

doc. Ing. Pavel Šenovský, Ph.D.

Bezpečnostní informatika 1

skripta
8. vydání



Bezpečnostní informatika 1

8. rozšířené vydání

tento text neprošel jazykovou úpravou

©Pavel Šenovský, Ostrava, 2017

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků	5
Seznam tabulek	7
Úvod	9
1 Základní pojmy informatiky	13
1.1 Informace	13
1.2 Další vlastnosti informace	17
2 Programové vybavení PC	21
2.1 Členění software	21
2.2 Systémový software	22
2.3 Aplikační programy	25
2.4 Uživatelské programy	25
3 Škodlivý kód	27
3.1 Počítačový virus	27
3.2 Červi	29
3.3 Trojští koně	30
3.4 Hoax	32
3.5 Spyware a phishing	32
3.6 SPAM	35
3.7 Ochrana	35
4 Šifrování a elektronický podpis	41
4.1 Základní pojmy	41
4.2 Stručná historie šifrování	42
4.3 Substituční šifry	43
4.4 Kódy	45
4.5 Symetrické a asymetrické šifry	45
4.5.1 Blokované šifry	45
4.5.2 Proudové šifry	48
4.6 Asymetrické šifrování	49
4.6.1 RSA	49
4.6.2 DSA	50
4.6.3 ECDSA	51
4.6.4 Požadavky na nastavení parametrů algoritmů asymetrického šifrování	51
4.7 Elektronický podpis v zákonech	51
4.8 Bezpečné hašovací algoritmy	58
4.8.1 MD2 - 5	59
4.8.2 SHA	60
4.8.3 RIPEMD-160	61
4.8.4 WHIRPOOL	61
4.8.5 Doporučení k použití bezpečných hašovacích funkcí	62

5 Úvod do počítačových sítí	65
5.1 Rozdělení sítí	65
5.2 Kabeláž sítí	68
5.3 Síťová architektura ISO/OSI	69
5.4 Ostatní síťová zařízení	73
6 E-government	79
6.1 Základní registry	79
6.2 Elektronické podatelny	81
6.3 Datové schránky	82
7 Informační systémy veřejné správy	85
7.1 Stručná historie informačních systémů veřejné správy v ČR	85
7.2 Informační systémy veřejné správy	86
8 Kybernetická bezpečnost v ČR	89
8.1 Kybernetická bezpečnost	89
8.2 CERT a CSITR týmy a jejich význam	91
9 Rychlé informace	95
9.1 Úvod	95
9.2 Nařízení vlády 11/2002 Sb.	96
9.3 Nebezpečné látky – rychlé informace	98
10 Budoucnost výpočetní techniky aneb počítáme netradičně	105
10.1 DNA počítače	105
10.2 Kvantové počítače	106
10.3 Neuroprocesory	107
11 Telekomunikace	109
11.1 Legislativní rámec EU	109
11.2 Zákon o elektronických komunikacích (127/2005 Sb.)	112
Literatura	117
Seznam zkratk	123
Rejstřík	124

Seznam obrázků

1.1	Obecné schéma sdělovací soustavy	15
1.2	Informační nárůst demonstrováný na úložných kapacitách nutných pro jeho pokrytí (převzato z: [50])	17
1.3	Křivka stárnutí ideální informace	18
1.4	Stárnutí informací při uvažování okrajových podmínek	19
2.1	Uživatel v informačním systému	22
3.1	Celkový počet vzorků škodlivého kódu v databázi testovací laboratoře AV-Test (převzato z [37])	28
3.2	Phishing zaměřený na zákazníky České spořitelny - legendární <i>Drahoušek zákazník</i>	33
3.3	DNSSEC/TLSA Validator add-in for Web Browsers v MS Internet Explorer (převzato z [47])	34
3.4	Podíl různých verzí OS Android k 5. prosinci 2016 (převzato z [51])	38
4.1	Skytale (převzato z [27])	42
4.2	Šifrovací disk Leaona Battisty Albertiho (převzato z [42])	43
4.3	Přístroj Enigma s třemi rotory (převzato z [6])	44
4.4	Využití hashovacích funkcí při elektronickém podepisování dokumentů	53
5.1	Sběrníková topologie počítačových sítí	66
5.2	Topologie počítačových sítí token ring	66
5.3	Hvězdicová topologie počítačové sítě	67
5.4	Nejčastěji používané typy kabeláže v počítačových sítích (převzato z [65])	68
5.5	Komunikace v síti - pohled referenční model ISO/OSI	70
5.6	Switch Cisco Catalyst 2950	71
5.7	Nastavení formátu data a čísel ve Windows 7	73
5.8	6-ti diskový NAS TVS-671 společnosti QNap (převzato z: [28])	75
8.1	Typové rozložení řešení bezpečnostních incidentů týmu CSIRT.CZ v letech 2008-2011 (převzato z [45])	92
8.2	CSIRT týmy – mezinárodní spolupráce	93
9.1	Příklady použití barev pro značení	97
9.2	Příklady značek zákadu	97
9.3	Příklady značek výstrahy	98
9.4	Příklady značek příkazu	98
9.5	Příklady informativních značek	99
9.6	Značka CE dle protokolu PECA	100
9.7	Příklad Identifikátorů nebezpečné látky – převzato z databáze Nebezpečné látky 2005 [72]	100
9.8	Příklad Diamantu s vysvětlením významu – převzato z databáze Nebezpečné látky 2005 [72]	101
9.9	Třídy nebezpečnosti	102
9.10	Výstražné symboly	102
9.11	Výstražné symboly dle legislativy CLP	103

Seznam tabulek

4.1	Doporučení pro nasazení algoritmů blokových šifer (převzato z [62])	46
4.2	Doporučení pro nasazení algoritmů proudových šifer (převzato z [62])	48
4.3	Doporučení pro parametry asymetrických šifrovacích algoritmů (převzato z [62])	51
4.4	Doporučená podpisová schémata dle [34]	57
4.5	Použitelnost SHA algoritmů dle [34]	57
4.6	Vlastnosti hašovacích algoritmů SHA	61
9.1	Tabulka barev značek a světelných signálů (převzato z [19])	96

Úvod

Vážený studente, dostává se Vám do rukou učební text předmětu *Bezpečnostní informatika I.*

Mým cílem při psaní tohoto textu bylo, aby čtenatel získal základní přehled v oblasti informačních technologií a také otázek bezpečnosti, které jsou s nimi spojené. Text samotný není proto zaměřen na *informatiky*, ale spíše na lidi, kteří budou **Informační technologie (IT)** používat uživatelsky. Uživatelský přístup k problematice IT je trochu jiný - v našich úvahách o jednotlivých diskutovaných problémech nebudeme muset proto zacházet příliš do hloubky. To nás však samo o sobě nezabavuje nutností se s těmito technologiemi seznámit, zjistit jejich možnosti, ale také omezení, která jsou spojena s jejich použitím.

Moderní technologie jsou totiž často obklopeny z hlediska principu fungování řadou mýtů, pověr a nepochopení, které znesnadňují jejich správné použití, nebo u uživatelů vytvářejí neodůvodněná očekávání, která nemohou naplnit. Naše chápání, tedy způsob, jakým vnímáme informační technologie, přímo ovlivňuje způsob, jakým je budeme používat v praxi a v takovém případě za správné použití je pak zodpovědný, ten kdo je používá - tedy uživatel, nikoliv nutně IT specialista. S tím jak se zvyšuje penetrace stále pokročilejších technologií od počítačů až po chytré mobilní telefony a tablety, tím se také zvyšují nároky na jejich uživatele a to zejména z pohledu bezpečnosti, ochrany osobních údajů nebo citlivých dat uchovávaných na těchto zařízeních obecně.

Tento text vychází těmito požadavkům vstříc.

Organizace textu

Pro zpříjemnění čtení jsem se také rozhodl zpracovat tento text formou vhodnou pro „distanční vzdělávání“, tak aby práce s ním byla co možná nejjednodušší. Z tohoto důvodu je text jednotlivých kapitol segmentován do bloků.

Každá kapitola začíná náhledem kapitoly, ve kterém se dozvíte, o čem budeme v kapitole mluvit a proč. V bodech se pokusím shrnout, co byste po prostudování kapitoly měli znát a kolik času by Vám studium mělo zabrat. Mějte prosím na paměti, že tento časový údaj je pouze orientační, nebudte proto prosím smutní nebo naštvaní, když ve skutečnosti budete kapitole věnovat o něco méně nebo více času.

Za kapitolou následuje shrnutí, ve kterém budou zdůrazněny informace, které byste si rozhodně měli zapamatovat (určitě Vám ale neuškodí, pokud si jich zapamatujete více).

To, že jste správně pochopili probíranou látku, si budete moci ověřit pomocí kontrolních otázek a testů, které by Vám měly poskytnout dostatečnou zpětnou vazbu k rozhodnutí, zdali jít dále nebo si vyhradit delší čas na opakování.

Pokud studujete Bezpečnostní informatiku I v rámci celoživotního vzdělávání, tak v průběhu studia narazíte také na tzv. *korespondenční úkoly*. Tyto úkoly je potřeba vypracovat a v termínech daných Vaším studijním harmonogramem je odevzdat. Tyto korespondenční úkoly poslouží k Vašemu závěrečnému hodnocení.

Pokud jste studenty řádného studia v denní nebo kombinované studijní formě, pak i Vy narazíte na korespondenční úkoly, ale můžete je v klidu ignorovat – Vaše hodnocení bude provedeno na základě písemné zkoušky.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:

V novém (už šestém!) vydání skript jsem se rozhodl pro trošičku jiný způsob přípravy skript a celá jsem je přepsal v **Desktop Publishing (DTP)** systému L^AT_EX. Důvodem jsou některé schopnosti, které je s běžnými textovými procesory je možné dosáhnout pouze stěží a také to, že řada z vás bude studovat tento text přímo v počítači (tabletu, čtečce elektronických knih nebo mobilním telefonem) a v takovém případě budete chtít využít nejspíše všech schopností, která Vám tato zařízení poskytují.

Kolikrát jste si pomysleli - „jaké by to třeba bylo, kdybych mohl klepnout na jednu z těch divných



Průvodce studiem

Slouží pro seznámení studentů s látkou, která bude v kapitole probírána.



Čas nutný ke studiu

Představuje odhad doby, který budete potřebovat k prostudování celé kapitoly. Jedná se pouze o orientační odhad, neznepokojte se proto, pokud Vám studium bude trvat o něco déle nebo budete hotovi rychleji.



Vysvětlení, definice, poznámka

U této ikony najdete vysvětlující text, poznámku k probíranému tématu, která problém uvede do širších souvislostí, popřípadě důležitou definice.



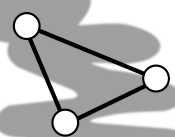
Kontrolní otázky

Na závěr každé kapitoly je zařazeno několik otázek, které prověří, zda jste problematice kapitoly dostatečně porozuměli. Pokud nebudete vědět odpověď na některou otázku, je to signál pro Vás, abyste se ke kapitole vrátili.



Příklad

Příklady obsahují praktické demonstrace diskutovaného problému.



Návaznosti

V tomto segmentu budou zmíněny další návaznosti probíraného tématu na další témata tohoto předmětu, ale také dalších předmětů.



Shrnutí

Obsahuje základní myšlenky kapitoly, kterým by měl být věnována zvláštní pozornost během studia.

zkratk (které informatici tak milují) a ona by mě přesmérovala automaticky na seznam zkratk“? Nebylo by lepší kdyby na daný literární pramen bylo možné se dostat přímo klepnutím na jeho číslo v textu, nebo aby jste nemuseli vybranou pasáž hledat přes čísla stránek, ale postačovalo by kliknout

**Přestávka**

Po obtížné části textu, nebo prostě občas jenom tak je nutné si udělat krátkou přestávku, načerpat síly k novému studiu.

na jméno kapitoly v obsahu?

Mě jako studentovy by se to líbilo a proto doufám, že je oceníte i Vy, protože všechny výše uvedené možnosti skriptu ve formátu **Portable Document Format (PDF)** obsahují. Aktivní odkazy jsou v textu zvýrazněny červenou (a v případě odkazů na literaturu zelenou) barvou.

Na konec skript byl přidán také rejstřík pojmů. Doporučuji, abyste jej v rámci přípravy na zkoušku prošli - zamyslete se nad tím, zda všechny pojmy, které jsem do něj zařadil, chápete a jste je schopni dát do souvislostí. Pokud ne je vedle pojmu odkaz na číslo stránky, kde je pojem probrán a Vy můžete rychle zaplnit případné mezery ve svých znalostech problematiky informačních systémů.

Přeji Vám, aby čas, který strávíte s tímto textem, byl co možná nejpříjemnější a abyste jej nepovažovali za ztracený.

doc. Ing. Pavel Šenovský, Ph.D.

Poznámka autora:

Právě držíte v rukou osmé rozšířené vydání skript. Je možné, že právě studujete na zkoušku, nebo jste se ke skriptům dostali pouze náhodou po delší době. Z tohoto důvodu by se Vám mohlo hodit stručné shrnutí změn mezi jednotlivými vydáními těchto skript.

Novinky v 5. vydání skript

1. Doplněna teorie informace o kódy, další drobné změny
2. Kapitola o šifrování byla doplněna o informace k možnosti nasazování algoritmů **Secure Hash Algorithm (bezpečný hašovací algoritmus) (SHA)** v čase pro generování certifikátů a základní informace o SHA-3.
3. Kapitola věnována peer to peer sítím byla podstatně přepracována (obecný úvod, architektura **Berkeley Open Infrastructure for Network Computing (BOINC)**, bezpečnostní aplikace).
4. Kapitola rychlých informací doplněna o základy značení dle evropské legislativy **Classification, Labelling and Packaging (klasifikace, označování a balení) (CLP)**.
5. Kapitola o Internetu – doplněny základní informace o IPv6

Novinky v 6. vydání:

1. sazba v \LaTeX
2. Drobné opravy a aktualizace v textu
3. Přepsána kapitola moderního symetrického a asymetrického šifrování, aby pokrývala celé spektrum použití

Novinky v 7. vydání:

1. změny v souvislosti se změnou koncepce předmětu Bezpečnostní informatika 1
2. doplněny kapitoly

- (a) Úvod do počítačových sítí
 - (b) E-government
 - (c) Informační systémy veřejné správy (ISVS)
 - (d) Kybernetická bezpečnost v ČR
3. některé kapitoly byly naopak odstraněny

Novinky v 8. vydání:

1. do kapitoly o škodlivém kódu byly doplněny některé informace o bezpečnosti mobilních telefonů/tabletů a zařízení **Internet of Things (IoT)**
2. provedeny změny v kapitole o šifrování za účelem modernizace textu a lepšího vysvětlení používaných postupů
3. doplněny informace o změnách v legislativě elektronického podpisu související s transpozicí evropské směrnice eIDAS do českého právního řádu
4. oblast podpisových schémat předělána dle požadavků normy ETSI TS 102 760-1 V2.1.1 (v předchozích vydáních byla využívána norma ve verzi V2.0.0)

Kapitola 1

Základní pojmy informatiky



Náhled kapitoly

Informace jsou základní hybnou silou dnešní společnosti, proto ji také někdy říkáme společnost informační. Z tohoto důvodu je nutné plně porozumět pojmům, jako je informace, informační technologie apod.

Po přečtení této kapitoly budete vědět

1. co je to informace, informační technologie ...
2. jak probíhají komunikační procesy

umět

1. rozlišit informace a data



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 30 minut.

1.1 Informace

Zamysleme se nad samotným pojmem informace, jelikož se tento pojem v běžném jazyce často používá, většina lidí si přibližně dokáže představit, co znamená. Pro naše účely však je nutné ymezit si tento pojem mnohem přesněji - což vyžaduje formální definici. Pojem informace můžeme definovat například takto:



Zapamatujte si

Informace je objekt nehmotné povahy, sdělení (zprávy), jehož základní vlastností je to, že u příjemce informace snižuje neurčitost.

Definice informace zmiňuje neurčitost, pokusme se ji tedy nějak definovat. Neurčitost neboli entropie, česky míra neznalosti (1.1) byla odvozena z počtu pravděpodobnosti C . Shanonem [61] obecně takto:

$$H = - \sum_{i=1}^n p_i \log_2 p_i \quad (1.1)$$

kde:

H ... entropie

p_i ... pravděpodobnost výskytu i -tého jevu

Takto definovaná entropie H znamená množství informací, které jsou nutné k jejímu úplnému odstranění, tedy úplnému odstranění neurčitosti u posuzovaného jevu.

Nejjednodušší informace je typu ANO-NE, TRUE-FALSE, 0/1 – nejjednodušší informace je jednotnou informací a říkáme mu jeden bit. Bit je odvozen z míry neurčitosti dvou stejně pravděpodobných jevů.

Toto si můžeme ověřit tak, že do vzorce (1.1) dosadíme hodnoty například pro hod mincí (1.2). Tedy pravděpodobnost p_i , že padne určitá strana mince je 0,5, takže:

$$H = - \sum_{i=1}^2 0,5 \log_2 0,5 = 1b \quad (1.2)$$

Ze vzorce vyplývá, že neurčitost je tím větší, čím větší je množina pravděpodobných výsledků. Na problém se můžeme podívat i z opačné strany - čím je problém složitější, tím větší množství informací je potřeba k tomu, aby byly odstraněny veškeré nejistoty (neurčitosti), které jsou s ním spojené. Informační entropie jako veličina má také širší použití - používají ji např. některé metody datamingu jako jsou rozhodovací pravidla nebo stromy pro identifikaci veličiny, která nejvíce přispívá k vysvětlení řešeného problému (a má tedy nejnižší entropii). Problematika datamingu výrazně přesahuje možnosti těchto skript, takže, pokud Vás problematika zaujala budete si muset počkat na předmět **Bezpečnostní informatika 3 (BI3)**, který je vyučován v prvním ročníku navazujícího studia.

Pro další úvahy je nutné si uvědomit rozdíl mezi **informacemi a daty** (údaji). Informace se nějaké sdělení, které u příjemce snižuje neurčitost – tuto vlastnost jsme už zmínili, pro rozlišení je ale nesmírně důležitá. Data, jako pojem, jsou mnohem obecnější – jedná se totiž o sdělení. Tato sdělení přitom mohou, ale nemusí snižovat neurčitost. Data tedy mohou, ale nemusí obsahovat informace.

Informace jsou tedy podmnožinou všech dat. Například seznam všech studentů VŠB-TUO můžeme považovat za data. Výběr všech studentů, kteří studují předmět **Bezpečnostní informatika 1 (BI1)**, však, pro mě jako pro vyučujícího tohoto předmětu, představují informace – snižují totiž u mě neurčitost v tom, kolik studentů budu vyučovat, kolik jich budu muset vyzkoušet, apod.

Pro informaci je typická nutnost nějaké úsilí (energie), které je nutno vynaložit, abychom informaci získali z dostupných dat a je přitom jedno, jestli zpracování probíhá ručně nebo automatizovaně pomocí nějakého informačního systému nebo analytického nástroje.

S informacemi souvisí také další pojem - *znalost*. Tento pojem je často nesprávně významově zaměňován s informací. Znalosti jsou získávány interpretací a organizací informací a jejich dalším použitím např. pro rozhodování. Výše uvedený demonstrační příklad se studenty předmětu BI1 by znalost mohl představovat výstup analýzy odpovědí písemných prací vypracovaných při zkoušce předmětu. Výsledek by poskytl znalosti o probíraných tématech, u kterých studenti více chybují a byl by využitelný pro upravení skript/přednášek předmětu.

S informatikou související pojem jsou **IT**. Pokud hovoříme o **IT**, obvykle máme na mysli automatizované nástroje pro sběr, přenos a vyhodnocování údajů.

IT jako pojem se ovšem používají také v přeneseném významu, který se může částečně překrývat s významem pojmu informatika nebo ještě lépe pojmem aplikovaná informatika. **Informatika** jako věda se zabývá především zkoumáním informací jako takových, jejich vlastností, shromažďováním, zpracováním – těmito problémy se zabývá především v teoretické rovině. IT se proti tomu zabývá spíše praktickou stránkou těchto problémů - tedy že informace jsou zpracovávány na počítačích, pomocí softwarových nástrojů, že tyto počítače lze propojovat do sítí apod. IT se tedy zabývá v podstatě stejnou oblastí ale z praktičtějšího (aplikačního) pohledu.

Dalším významným pojmem je **systém**, jedná se o pojem obecný v současné době často využívaný v různých významech. Systém bychom mohli obecně definovat jako souhrn prvků, které jsou vůči sobě v nějakém vztahu a vůči okolí působí jako celek.

Na **Informační systém (IS)** pak lze nahlížet optikou výše uvedené definice systému: jako na společné působení lidí (peopleware), zařízení (hardware), programů (software) a organizačních opatření (orgware), které pracují společně na splnění vytyčených cílů (za jakým byl informační systém nasazen).

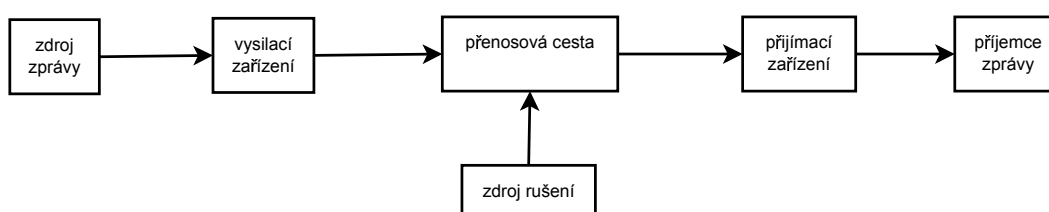
Taková definice odpovídá vymezení IS pomocí IT. IS přitom můžeme chápat i poněkud obecněji jako jakýkoliv systém, který slouží ke shromažďování, správě a vyhodnocování údajů ať již s pomocí

výpočetní techniky nebo například formou kartotéky apod. Taková definice odpovídá více chápání IS jako systému pracujícího nad databázovým systémem.

Konečně pojmem **databáze** rozumíme systém pro řízení báze dat, tedy systém, který umožňuje efektivní správu dat ve smyslu jejich pořizování, údržby, výběru a to tak, aby data byla v databázi pokud možno obsažena pouze jedenkrát (zamezení redundancím) a ve formě, která zaručí neustálou dostupnost a integritu dat. V češtině byly databázové systémy původně označovány jako **Systém řízení báze dat (SRBD)**, v současnosti se ale i v češtině používá souhrnné označení databázový systém nebo zkráceně databáze.

Ve vztahu k IS slouží databáze mimo jiné jako tzv. backend. Tedy IS si data, se kterými pracují, ukládají do různých databází a tím řeší všechny otázky konzistence udržovaných dat - stará se o ně databáze sama.

Už víme, že informace je objekt nehmotné povahy, víme také, že informační technologie nám umožňují s informacemi efektivněji pracovat – k tomuto účelu ale musí být tyto informace nějakým způsobem vyjádřeny fyzicky a přeneseny na místo určení ke zpracování. Procesu sběru, zpracování, uchovávání, přenosu a využívání informace říkáme **informační proces**. V průběhu informačního procesu může dojít ke zkreslení informace zejména v průběhu přenosu informace vlivem informačních šumů (viz obr. 1.1).



Obrázek 1.1: Obecné schéma sdělovací soustavy

Obr. 1.1 představuje obecné schéma sdělovací soustavy, které se v různých obměnách objevuje v řadě oborů od sociologie až po kybernetiku. *Zdroj zpráv* může představovat počítač stejně jako člověka, který produkuje zprávu a ta je zakódována ve *vysílacím zařízení* do podoby signálu vhodného pro přenos daným *sdělovacím kanálem*.

Signál se na místo určení přenáší prostřednictvím sdělovacího kanálu. V těchto kanálech může docházet k *šumům*, které informace deformují a snižují její efektivní množství. Prakticky šum působí tak, že modifikuje přenášený signál. Řada sdělovacích soustav je proti působení šumu do určité míry odolná. Pokud aplikujeme výše uvedené na běžnou konverzaci mezi lidmi, budou mít charakter vysílacího zařízení naše hlasivky, roli přímače bude hrát náš sluch. Signál bude mít vlnění šířeného vzduchem. Na tyto signály budou působit zdroje rušení ve formě zdrojů zvuku v naší blízkosti. Pokud je úroveň hluku v našem okolí nízká, nedělá nám obvykle problém porozumět podstatě sdělení, pokud však intenzita rušení přesáhne určitou mez, přestáváme postupně rozumět až do stavu kdy nejsme schopni odlišit přenášené sdělení od rušení.

V případě, komunikace dvou lidí je výhodou, že obě strany mohou vyhodnocovat průběžně kvalitu přenosu informace a reagovat, co se ale stane pokud přenos informace je realizován čistě pomocí výpočetní techniky. Počítače dnes nejsou (a nikdy nebyly) inteligentní, jak tedy v takovém případě zajistit, aby bylo možné rozhodnout, že přijaté signály byly zachyceny v přijatelné, interpretovatelné podobě? V historii se objevila celá řada algoritmů a postupů, které tento problém řeší, jedním z prvních bylo použití CRC algoritmů (**Cyclic redundancy check (kontrolní součty) (CRC)**). CRC algoritmy pracovaly tak, že pro bloky přenášených dat vypočítávaly číslo, to pak odeslaly spolu s daty. Po příjmu se provedl přepočítání přijatých dat a získané kontrolní součty se porovnály s těmi, které byly zaslány. Pokud se shodovaly, byla přijatá data korektní.

Hlavní nevýhodou CRC algoritmů je jejich jednoduchost - ta umožňuje snadno identifikovat náhodné narušení komunikačního procesu, v případě, že ale je proces komunikace narušen motivovaným útočníkem, např. hackerem, CRC přestávají plnit ochrannou úlohu, přenášená data je totiž možné pozměnit tak, aby jim nezměněný kontrolní součet odpovídal. Proto se pro účely ověření dnes používají spíše bezpečné hašovací algoritmy (**SHA**) nebo na nich založené algoritmy jako např. elektronický podpis. Tyto algoritmy již využívají některých postupů kryptografie, což činí jejich narušení značně obtížnější.

SHA, šifrováním a elektronickým podpisem se budeme zabývat v pozdějších kapitolách, nyní se

vraťme k podstatě signálu a jeho vyjádření a otázce, co to vlastně signál je? *Signál* je stav popřípadě proces látkového nebo energetického média. Signál je tedy tím kýženým fyzickým vyjádřením nehmotné informace. Aby nám signály dávaly nějaký význam, musíme je používat podle určitých pravidel, která jim tento význam přiřadí. Takové soustavě pravidel říkáme **kód**.

Každý kód se skládá z jednotlivých symbolů, kterými pokud je určitým způsobem zřetězíme za sebou můžeme vyjádřit zprávu. Seznamu přípustných symbolů kódu říkáme *abeceda*.

Kód je obvykle navrhován s ohledem na charakter informací, které budou přenášeny. Teoreticky můžeme hovořit o tzv. *optimálním kódu* – tedy takovém kódu, který právě postačuje pro přenesení dané informace. Takový kód ovšem není právě praktický, protože není univerzální. Z tohoto důvodu v běžně používaných kódech preferujeme určitou míru redundance. Jak si to představit? Použijme běžnou abecedu, kterou používáme každý den. Představme si situaci, že píšeme e-mail. Optimální kód bude takový, který bude obsahovat pouze ta písmena, která jsme v mailu potřebovali použít a žádná jiná. Co když ale v jiném mailu bude potřeba použít právě tato chybějící písmena?

Ve výpočetní technice se tento problém řeší použitím do určité míry univerzálními systémy kódování, které často označujeme jako znakové sady (např. **American Standard Code for Information Interchange (ASCII)**, **UCS Transformation Format (UTF-8)** a další). Znakové sady sice nezajistí úplnou celosvětovou znakovou kompatibilitu, ale regionálně fungují velmi dobře.

Vraťme se ke problematice kódování a abeced ještě obecně. Na základě entropie lze odvodit některé důležité vlastnosti použité abecedy a systému kódování. Konkrétně lze, za předpokladu, že pravděpodobnost výskytu každého symbolu abecedy je stejná, vypočítat maximální entropii abecedy H_{max} podle vzorce (1.1) a tuto veličinu pak použít pro určení *efektivity kódování*.

Efektivitu můžeme měřit pomocí relativní entropie h (1.3) nebo pomocí tzv. redundance kódu r (1.4). Relativní entropii rozumíme poměr entropie kódu použitého pro zakódování zprávy k maximální entropii celé abecedy. Výpočet relativní entropie provedeme podle vzorce (1.3).

$$h = \frac{H}{H_{max}} \quad (1.3)$$

Kde

h ... relativní entropie

H ... entropie reálně použité abecedy

H_{max} ... maximální entropie celé abecedy

Optimální kód by se logicky měl mít hodnoty H a H_{max} velmi podobné, proto by se relativní entropie měla blížit 1. Pokud relativní entropii odečteme od 1, získáme redundanci (nadbytečnost) kódu.

$$r = 1 - h = 1 - \frac{H}{H_{max}} \quad (1.4)$$

Kde

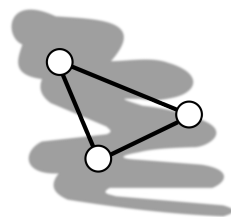
r ... redundance kódu

h ... relativní entropie

H ... entropie reálně použité abecedy

H_{max} ... maximální entropie celé abecedy

Pro signál platí, že jedna informace je vyjádřena minimálně jedním signálem (tedy jedním a více signály), zatímco jeden signál obsahuje maximálně jednu informaci.



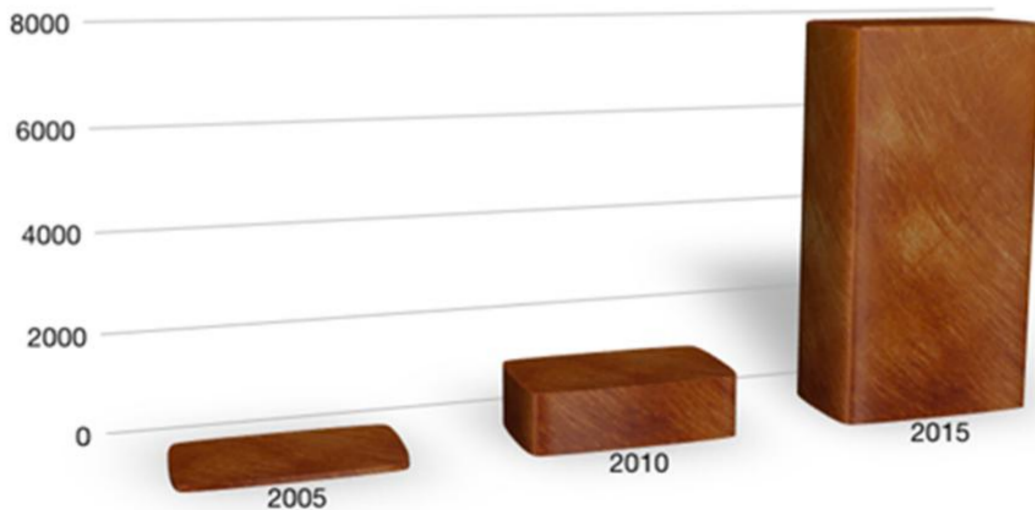
Návaznosti

Redundance je základním stavebním kamenem ochrany dat. Redundance je využívána např. v šifrování viz kapitoly věnované symetrickému a asymetrickému šifrování v těchto skriptech, popř. předmětu *Počítačové sítě a ochrana dat*.

Z historického hlediska můžeme uvažovat o celkovém množství informací, které jsou v daném okamžiku aktivně využívány. Intuitivně cítíme, že toto množství se neustále zvyšuje. To souvisí s rostoucím

množstvím informací, které jsme použili pro zlepšení poznávacích procesů (citlivější přístroje, výkonné počítače schopné zpracovávat velké objemy dat apod.).

M. Mertal na kongresu leteckého průmyslu v roce 1949 předpokládal, že nárůst informací v čase má exponenciální charakter. Tento předpoklad experimentálně dokázal roku 1955 D. S. Price. Graficky je informační nárůst zobrazen na obr. 1.2. V tomto případě je informační nárůst demonstrován úložnou kapacitou (stávající a předpokládanou) nutnou pro jeho pokrytí.



Obrázek 1.2: Informační nárůst demonstrovaný na úložných kapacitách nutných pro jeho pokrytí (převzato z: [50])

Je zřejmé, že exponenciální charakter informačního nárůstu nemůže pokračovat neomezeně dlouhou dobu, bude vždy omezen hranicí technických možností dané doby. S tím, jak se blížíme této hranici, dojde ke změně charakteru křivky informačního nárůstu. Ta nejprve ztratí svůj exponenciální charakter a bude růst dále již jen lineárně se stále zmenšujícím se sklonem, až se stabilizuje na určité úrovni a na této úrovni zůstane do doby, než dojde k průlomovému objevu, který znovu nastartuje informační nárůst. Charakter průlomu určí, jestli další nárůst bude spíše lineární nebo exponenciální.

Pohledem do minulosti lze vysledovat několik období prudkého informačního nárůstu následovaného z hlediska informací stabilním obdobím, jmenujme například antiku, renesanci a období průmyslové revoluce a v moderní době masivní nástup výpočetní techniky.

1.2 Další vlastnosti informace

Další podstatnou vlastností informace, je že její schopnost odstraňovat entropii v čase klesá. To znamená, že informace je užitečná pouze omezenou dobu, po jejímž uplynutí se stává nadbytečnou. Životnost informace je tedy časově omezená. V rámci zkoumání charakteru stárnutí informací se zavádí pojem *poločasu stárnutí*.

Poločas stárnutí informace lze definovat jako čas od zveřejnění informace do okamžiku poklesu počtu citací této informace na jednu polovinu ve srovnání s okamžikem maximální aktivity (užitečnosti) informace.

Tento čas není možné zjistit přesně a bude se lišit případ od případu. Při zjišťování přibližného poločasu stárnutí dané informace bereme v úvahu tzv. *zpětný poločas stárnutí* (hodnotíme tedy informaci, která již prošla celým svým životním cyklem) a ten potom používáme pro informace obdobného charakteru.

Ideální křivka stárnutí informace by mohla být vyjádřena následující rovnicí (1.5):

$$y = 1 - \left(\frac{a}{e^x} \cdot \frac{b}{e^{2x}} \right) \quad (1.5)$$

kde

$$a + b = 1$$

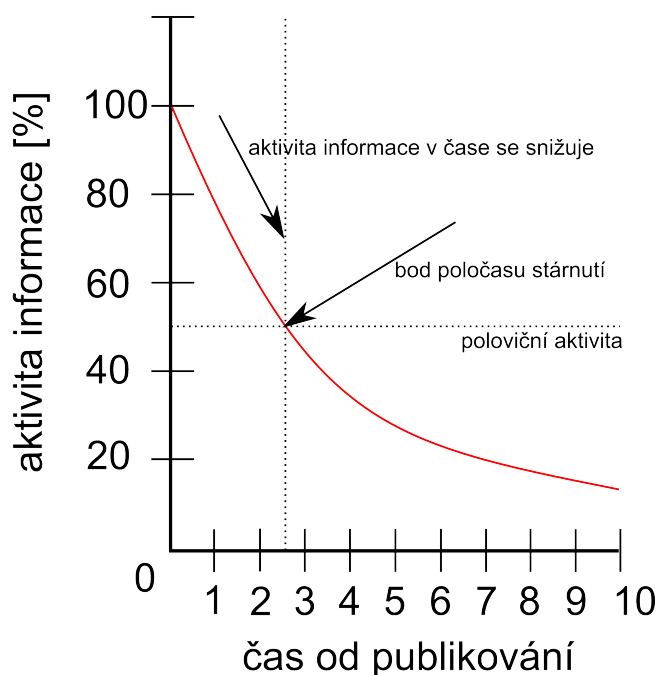
a, b ... jsou koeficienty, které určují progresivitu stárnutí

y ... hodnota kumulovaného procenta publikací v jednotlivých letech

x ... čas v dekadách

Jak by mohlo vypadat grafické znázornění stárnutí informací, je patrné z obrázku 1.3.

Poločas stárnutí informace



Obrázek 1.3: Křivka stárnutí ideální informace

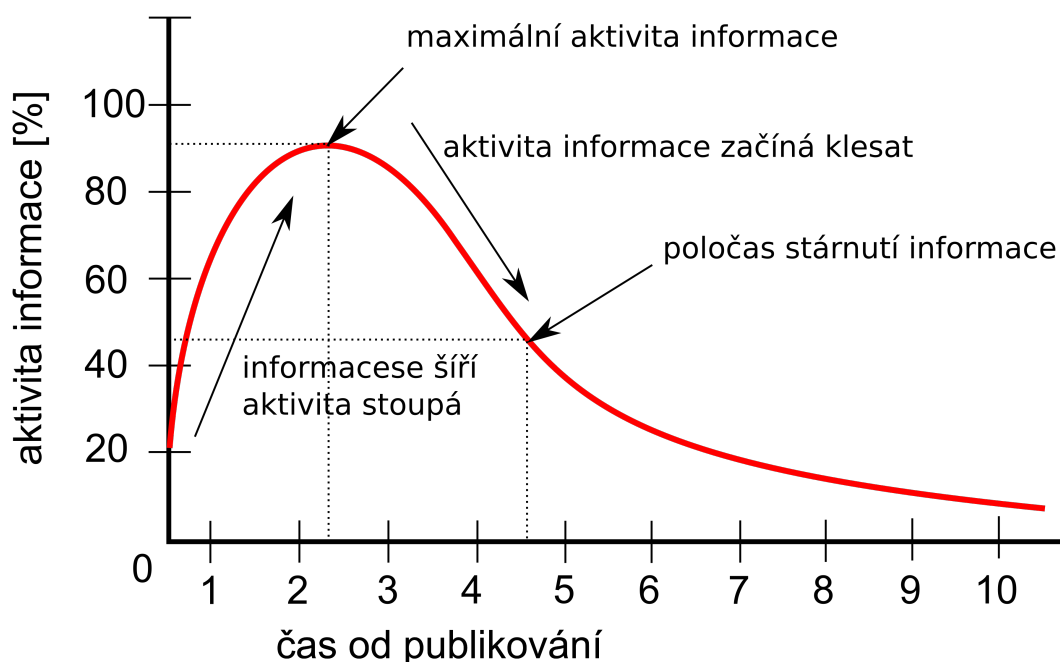
Obrázek 1.3 ukazuje stárnutí informace z nějakého vrcholu až takřka k nule. Je očividné, že tento obrázek neuvažuje tzv. *okrajové podmínky*. Informace po svém zveřejnění totiž není okamžitě na svém „vrcholu“, trvá nějakou dobu, než se dostane do širokého podvědomí a začne být aktivně využívána a projeví se tedy měřitelným způsobem v citacích, odkazech apod. Dále můžeme říci, že informace bez ohledu na její charakter se nerozšíří úplně všude - tedy aktivita informací v reálném světě nebude nikdy 100

Reálná informace proto bude nejprve z hlediska aktivity narůstat, s tím jak se bude postupně šířit, poté dojde ke kulminaci aktivity a následovat bude úpadek aktivity. Příklad takového životního cyklu naleznete na obrázku 1.4. Informace také nedosáhne nikdy úplného rozšíření, tudíž může se pouze blížit hodnotě 1, nikoliv jí dosáhnout.

Parametry křivky stárnutí informace se budou lišit pro jednotlivé obory lidské činnosti.

Obecně platí, že humanitně zaměřené obory mají delší poločas stárnutí informace, vysoce inovační obory, jako např. obor IT, pak mají extrémně rychlý životní cyklus informace.

Poločas stárnutí informace



Obrázek 1.4: Stárnutí informací při uvažování okrajových podmínek

Shrnutí

Informace je objekt nehmotné povahy, sdělení (zpráva), jehož základní vlastností je to, že u příjemce informace snižuje neurčitost.

Od *dat* se liší zejména nutností vynaložit určitou energii na získání informací.

Informace stárnou. Pro změření míry tohoto stárnutí byl zaveden pojem *poločas stárnutí informace*, jako doba od zveřejnění informace po dobu než počet nových odkazů na ni klesne na polovinu (ve srovnání s počátkem životního cyklu informace).

Kontrolní otázky

1. Definujte pojem data a srovnajte jej s pojmem informace.
2. Jak se určuje poločas stárnutí informace?
3. Jaké metody lze použít pro ověření poškození přijaté informace?
4. Proč při uvažování okrajových podmínek životního cyklu informace aktivita informace nejprve stoupá a teprve potom klesá?
5. Definujte informační entropii pomocí informace.

Správné odpovědi

1. Data jsou nadmnožinou informací. Jedná se o obecná sdělení, která u příjemce mohou, ale nemusí snižovat informační entropii. Z dat můžeme informace získat investicí energie – tedy aktivním zpracováním informací za účelem získání odpovědi na naše otázky.
2. Odhadem na základě empiricky změřených poločasů stárnutí informací podobného charakteru, které již prošly celým životním cyklem.
3. **CRC**, **SHA**, elektronický podpis.
4. Protože informace potřebuje nějaký čas pro rozšíření se a teprve potom začíná vlastně stárnout.
5. Informační entropie je množství informací, které je nutno získat pro kompletní odstranění neurčitosti určitého jevu.



Testi

1. základní jednotkou informace je jeden
 - (a) bit
 - (b) kilo bit
 - (c) mega bit
2. informace se obecně přenáší formou
 - (a) jedniček a nul
 - (b) dvojek a trojek
 - (c) signálů
3. množství informací ve společnosti roste
 - (a) lineárně
 - (b) exponenciálně
 - (c) logaritmičsky
4. základním omezením budoucího zvyšování množství informací ve společnosti je
 - (a) hranice technologických možností
 - (b) kapacita současných výpočetních strojů
 - (c) omezení není
5. IS se skládá z:
 - (a) Lidí, IT a org. norem
 - (b) Peopleware, software, hardware, orgware
 - (c) Lidí, výpočetní techniky, programů a organizačních pravidel

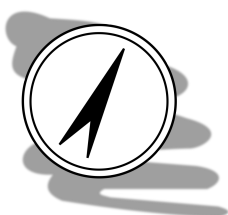


Správné odpovědi

1. a), 2. c), 3. b), 4. a), 5. všechny odpovědi správně

Kapitola 2

Programové vybavení PC



Náhled kapitoly

Software je hybnou součástí každodenního života drtivé většiny ekonomicky aktivních lidí. Je to také on, který představuje určité bezpečnostní riziko. Z tohoto důvodu si povíme něco o členění software do kategorií a tyto kategorie si vysvětlíme. Zároveň se podíváme do určité (omezené) míry i na bezpečnostní aspekty užití software.

Po přečtení této kapitoly budete vědět

1. co je to software
2. jak můžeme software dělit
3. co jsou databáze
4. jak vypadá XML soubor



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 30 minut.

Programové vybavení počítače tvoří rozhraní mezi počítačem (hardware) a lidskou bytostí (peopleware). Vzhledem k tomu, že se počítače staly nedílnou součástí každodenního života, je nezbytné se o něm něco málo dozvědět.

Na následujících stránkách se pokusím rozčlenit software do několika kategorií. Hranice mezi jednotlivými kategoriemi ovšem není úplně ostrá, berte prosím tedy následující stránky jako pokus začlenění problematiky SW do širšího kontextu.

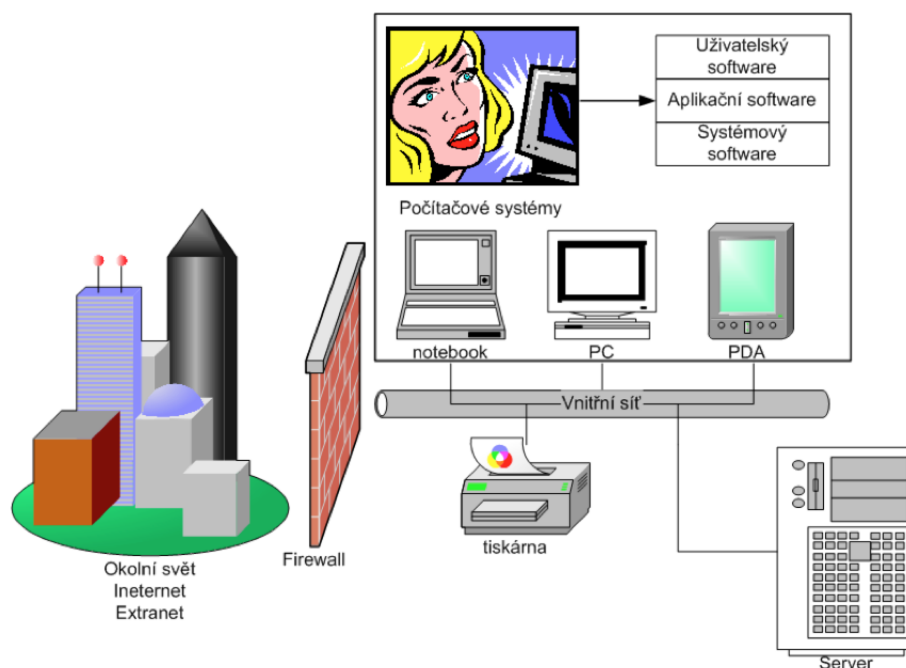
2.1 Členění software

Software lze členit podle mnoha různých charakteristik, pro základní rozlišení skupin software nám může posloužit následující členění podle účelu použití software:

1. systémové programy
2. aplikační programy
3. uživatelské programy

Základní filozofický rozdíl z hlediska bezpečnosti mezi výše uvedeným software je v tom, jakým způsobem se uživatelé a administrátoři staví k nakládání s ním.

Z hlediska administrace obvykle v podnikovém nasazení požadujeme, aby systémový software pro koncového uživatele fungoval jako černá skříňka – tedy koncový uživatel do nich nemůže zasahovat, jakýkoliv zásah může být fatální pro chod celého počítače.



Obrázek 2.1: Uživatel v informačním systému

Aplikační software vykonává „skutečnou, produktivní“ práci, za kterou je zaměstnanec placen. Možnosti konfigurace, změn tohoto typu software mohou proto být povoleny vyšší. Zároveň aplikační software funguje nad software systémovým, takže problém s jednou aplikací obvykle neohrožuje fungování systému jako celku (může ale být průvodním jevem hlubších problémů).

Konečně uživatelský software běží obvykle nad systémovou a aplikační vrstvou, škody, které je pomocí něho možno napáchat jsou tak omezené.

2.2 Systémový software

Do kategorie systémového software se řadí především:

1. operační systémy a jejich nadstavby
2. databázové systémy
3. testovací, diagnostické a antivirové programy

Operační systémy jsou specializované programy, které zabezpečují fungování samotného počítače. *Operační systémy* mají dvě základní funkce:

1. přidělování zdrojů (procesory, paměti, periferie),
2. zabezpečení komunikace člověk-počítač (hardware)

Na světě existují desítky, možná stovky různých operačních systémů, které se výrazně liší svými vlastnostmi. Pokusme se je rozčlenit do několika kategorií. Nejedná se samozřejmě o úplný výčet, při troše snahy bychom mohli nalézt další kritéria, podle kterých by bylo možné operační systémy členit jinak.

Dělení podle druhu počítače

1. superpočítače
2. servery
3. PC
4. tablety, smartphony

5. a další

Počítače v tomto případě dělíme podle velikosti. Dělení je ale možné použít také odlišné např. podle počtu uživatelů, které s operačním systémem mohou zároveň pracovat:

1. jednoúživatelské (**Desktop Operating System (DOS)**, Windows95, 98)
2. víceúživatelské (**Operační systém (OS)** UNIXového typu (klasické UNIX systémy, LINUX (**Linux is not Unix (Linux)**)), systémy na bázi **Berkeley Software Distribution (též Berkeley Unix) (BSD)** a další), Windows2000 a vyšší)

Současnou prací v tomto případě nemyslíme stav, kdy ze vzdáleného počítače spustíme nějakou aplikaci (aplikační servery), nebo využíváme nějakou službu (např. přístup na WWW stránky). Víceúživatelskou prací v tomto případě myslíme stav, kdy několik uživatelů ze vzdálených počítačových systémů pracuje s počítačem stejným způsobem jako by u něj seděli. V této oblasti tradičně kralují operační systémy odvozené od UNIX. Windows 2000 a XP v této oblasti umožňují nějaký vzdálený přístup, je ovšem otázka zda se takovýto přístup dá považovat za víceúživatelský.

Operační systémy lze členit také podle počtu úloh, které je možno zpracovávat současně.

1. monoprogramový (DOS, Windows 3.11)
2. multiprogramový (UNIX, Windows9x, 2000, XP, OS/2 . . .)

Procesor se při zpracování více úloh nerozdělí na několik menších, které by se staraly o jemu přidělené úlohy. Operační systém však přiděluje cykly procesoru podle činností, které jednotlivé úlohy po něm požadují. Vytvoří se tedy fronty požadavků jednotlivých úloh (programů), které se postupně vykonávají.

Procesorem ve výše uvedené definici se rozumí samostatná výpočetní jednotka tedy procesor nebo jádro procesoru v případě procesorů obsahujících více jader. Vícejaderné procesory se tedy chovají jako víceprocesorové systémy a vytvářejí pro každé jádro samostatné vlákno, na kterém se jednotlivé činnosti vykonávají.

Podle použité architektury lze OS členit na:

1. klasické
2. otevřené (např. dle POSIX standardu)

Portable Operating System Interface [for Unix] (POSIX) je standardem, který by měl zajistit hladkou interoperabilitu mezi jednotlivými zařízeními pracujícími s různými UNIXovými operačními systémy. Hladkou interoperabilitou se v tomto případě rozumí především schopnost zkompileovat, bez nutnosti provést další úpravy, programy pro různé verze UNIXových systémů.

Nadstavby operačních systémů

Slouží ke zkvalitnění komunikace člověk – počítač. Mezi tyto nadstavby byly například často zařazovány i Windows 3.11, protože ke své práci potřebovaly operační systém DOS. V dnešní době se jedná především o programy, které usnadňují práci se soubory a složkami jako jsou například Total Commander, Servant Salamander apod.

Do oblasti systémového software jsou také často zařazovány databázové systémy. Jedná se o systémy, které zabezpečují operace nad daty shromážděnými v tzv. bázi dat. Operacemi v tomto případě myslíme vkládání, editace a výmaz dat. Databázový systém umožňuje provádět výběry (filtrování dat) podle zadaných požadavků. Drtivá většina databázových systémů pro zabezpečení výběrů používá dotazovací jazyk **Structured Query Language (SQL)**, tedy česky strukturovaný jazyk pro dotazování.

Vedení dat v jednotné bázi dat umožňuje uchovávat data pouze efektivně na jednom místě. Toho se dosahuje tak, že související data jsou propojena. Tím pádem v databázi nevznikají nekonzistence v důsledku duplicit.

Typy

1. stromové (DBS/25)
2. síťové (IDMS)
3. relační
 - (a) „velké“ - ORACLE, INFORMIX, PROGRESS, MySQL, MS SQL Server
 - (b) „malé“ - dBASE, FoxPro, MS Access, Paradox, Clipper)
4. objektové (Matisse, NeoAccess . . .)
5. XML (Berkeley DB XML, Xyleme Zone Server, ...)

6. NoSQL databáze

Síťové a stromové databázové systémy ve výčtu uvádím pro úplnost, tyto systémy byly překonány v osmdesátých letech systémy relačními, které představují majoritní databázovou architekturu dneška.

V relačních databázích jsou data uchovávána v tabulkách s definovanou strukturou (sloupce tabulky), samotná data se pak vkládají do jednotlivých řádků tabulky. Každý řádek je v obvykle jednoznačně identifikovatelný pomocí *primárního klíče*. Tabulky samotné lze v databázi propojovat vazbami, nazývanými *relace* - odtud název relační databáze.

Objektové databázové systémy vycházejí z odlišnějšího pohledu na data - někdo by možná řekl intuitivnějšího pohledu. Filozofický přístup je následující: z reálné situace, o které potřebujeme shromážďovat data, vybereme několik objektů (například student, předmět ...) u těchto objektů pak zkoumáme jejich vlastnosti - data, která o nich lze evidovat a také způsob jakým se mají chovat v databázovém systému - metody. Objekty jsou potom shromážďovány v databázi.

Ačkoliv je z filozofického hlediska tento přístup možná intuitivní - prakticky příliš intuitivní není, což je také důvodem toho, že objektové databáze se příliš nerozšířily v praxi.

Extensive Markup Language (XML) v češtině znamená rozšiřitelný značkovací jazyk. XML vychází z toho, že řadu dat, které běžně vedeme v dokumentech lze intuitivně popsat pomocí značek. Například obchodní dopis by bylo možné popsat následovně:

```
<dopis>
  <adresat>
    <jmeno>Jan</jmeno> <prijmeni>Nepomu</prijmeni>
    <adresa>
      Ulice 15
      Ostrava
      702 00
    </adresa>
  </adresat>
  <vec>Konference ABC2015</vec>
  <teloDopisu> text dopisu </telo_dopisu>
</dopis>
```

Skutečný XML dokument by obsahoval ještě informaci o použití standardu XML, kódování znaků a případně i o použitém schématu. Pro nás je pouze podstatné, že takto strukturované dokumenty je jednodušší uchovávat a dále s nimi nějakým způsobem pracovat. Údaje v takovéto strukturované podobě mají obrovskou výhodu v tom, že je možné je uchovávat na jediném místě - v jediném souboru, což je hlavní rozdíl proti relačním databázím, které na vyjádření složitějších vazeb v datech mohou vyžadovat i větší množství propojených tabulek.

XML databáze lze ještě dělit podle toho, zda se jedná o „čistě“ XML databáze (umí zpracovávat data pouze v XML nebo se jedná o databáze relační s rozšířenou podporou XML, např. ve smyslu formátování výstupů, ale s vnitřním ukládáním dat do běžných propojených tabulek.

Konečně *NoSQL databáze* jsou databázovými prostředky, které úmyslně rezignovaly na členění ukládaných šablon do podoby tabulek. Zjednodušeně řečeno - všechna data se ukládají na „jednu hromadu“, se kterou se pak dále pracuje. Tento typ databází se hodí pro řešení úloh, na které již výkonově nepostačují databáze relační. Pro tyto problémy se vžil anglický název big data. Typickým příkladem mohou být data, na základě kterých nabízí vyhledávače, jako je např. Google Search nebo Microsoft Bing a další, výsledky svých vyhledávání. Indexace jednotlivých stránek do podoby tabulek již dávno není možná a databáze NoSQL nabízí elegantní řešení tohoto problému.

NoSQL databáze lze obecně použít všude tam, kde je nutno zpracovat obrovské množství různých dat.

Testovací a diagnostické programy

Slouží k prověřování správného fungování technických prostředků. (ScanDisc, nástroje pro defragmentaci disku apod. – součást operačního systému; komerční nástroje, které přinášejí něco „navíc“ např. Norton Utilities, O&O Defrag, diagnostické nástroje pro testování paměti – GoldenMemory apod.).

2.3 Aplikační programy

Programy orientované na řešení určitých tříd úloh v různých oblastech použití. Jsou méně obecné než programy systémové. Řeší třídu problémů určité třídy uživatelů. Jejich společnou vlastností je to, že jsou určeny obvykle pro velkou skupinu lidí, nezáleží přitom, zda je program šířen komerčně nebo nekomerčně.

Typy

1. Kancelářské balíky (**Microsoft (MS)** Office, LibreOffice ...)
2. ediční systémy **DTP** (např. Adobe PageMaker, InDesign, QuarkXPress, Ventura Publisher apod.)
3. statistický software (StatGrafik, MathLab, Statistica ...)
4. grafické systémy
 - (a) editace rastrové grafiky (např. fotografie) - PhotoShop, PaintShop Pro, Gimp, Corel PhotoPaint;
 - (b) editace vektorové grafiky - Corel Draw, Adobe Ilustrátor apod.
5. ekonomický software
6. (účetnictví, skladová evidence apod.)
7. řízení projektu (Project Management) - např. MS Project apod.
8. programy pro vývoj software **Computer Aided System Engineering (CASE)**
9. (LBMS, CASE 4/2, ArgoUML, SELECT SE apod.)
10. programy pro počítačově řízený návrh **Computer Aided Design (CAD)** (např. Autocad, Bentley Microstation)
11. a další.

2.4 Uživatelské programy

Mezi uživatelský software řadíme vše, co se jinač nevejde. Jedná se především o software, který si uživatel navrhuje sám (buď ho sám zprogramuje nebo naspecifikuje požadavky) za účelem zjednodušení svých pracovních činností.

Pro uživatelský software je typické, že je nemožné jej masově nasadit, protože úkoly které plní jsou příliš specifické.

Typicky se jedná o aplikace řešené makry MS Office, jednoúčelové kontrolní, exportní nebo importní programy, programy na kontrolu integrity dat, skripty pro hromadné zpracování údajů (jako je např. migrace dat na nový systém) apod.



Shrnutí

Software dělíme do tří základních skupin:

1. systémový,
2. aplikační a
3. uživatelský.

Nejběžnějšími představiteli systémového software jsou různé operační systémy, aplikačního různé kancelářské nástroje a uživatelského různé jednoúčelové, velmi specifické utility.

V dnešní době v oblasti databází stále ještě převažují tzv. relační databáze, ačkoliv poslední dobou získává značnou popularitu datový formát **XML**.

XML je obecný, samo-dokumentující se jazyk pro popis dat, který je binárně kompatibilní napříč operačními systémy.



Kontrolní otázky

1. Vyjmenujte alespoň tři operační systémy.
2. Zařaďte makro v MS Excel pro zpracování statistiky známek absolventů za rok 2004 do některé ze skupin software.
3. Jaké jsou hlavní úkoly databází?
4. Jaký typ databázových systémů se v dnešní době nejvíce používá?
5. Jaké jsou hlavní úkoly operačních systémů?



Správné odpovědi

1. Windows 7, Ubuntu, Debian, OS X, Android, iOS, Solaris, Symbian, ...
2. uživatelský software
3. uchovávat data na jednom místě, zabráňuje duplicitám, zabezpečuje operace nad daty (dle požadavků uživatelů)
4. relační
5. tvoří rozhraní mezi hardware a software, přidělují zdroje počítače



Testi

1. Mezi aplikační software patří
 - (a) Linux
 - (b) Corel Draw
 - (c) Autocad
2. XML znamená
 - (a) Rozšířitelný značkovací jazyk
 - (b) Rozšířený značkovací jazyk
 - (c) Rozsáhlý značkovací jazyk
3. Který typ databáze se již nepoužívá
 - (a) Relační
 - (b) Stromové
 - (c) objektové
4. Z hlediska stability počítače jako celku je nejdůležitější bezpečnost?
 - (a) Systémového software (SW)
 - (b) Aplikačního SW
 - (c) Uživatelského SW
5. Který SW je vyráběn masově (ve velkých šaržích)?
 - (a) Systémového software (SW)
 - (b) plikačního SW
 - (c) Uživatelského SW



Správné odpovědi

1. b) c), 2. a), 3. b), 4. a), 5. a) b)

Kapitola 3

Škodlivý kód



Náhled kapitoly

Viry a jiné druhy škodlivého kódu (malware) se v posledních letech staly široce diskutovaným problémem, problémem který ročně způsobuje škody v řádech několika miliard dolarů pouze v USA (**United States of America (USA)**). Přestože malware je s námi již několik desítek let a existuje celá řada nástrojů umožňující s ním bojovat, počet nových vzorků malware se poměrně výrazně zvyšuje viz 3.1. Tento trend je přitom nejspíše dlouhodobý a nezasahuje již pouze klasické počítače a notebooky, ale také tablety, „smart“ mobilní telefony popřípadě jinou spotřební elektroniku s připojením k Internetu.

Je proto nutné se na střetnutí s tímto problémem pečlivě připravit.

Po prostudování kapitoly budete

1. umět rozdělit viry podle funkčnosti
2. znát hlavní metody ochrany před škodlivým kódem
3. vědět co je to spam
4. vědět co je to phishing (rhybaření)



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně hodinu.

3.1 Počítačový virus

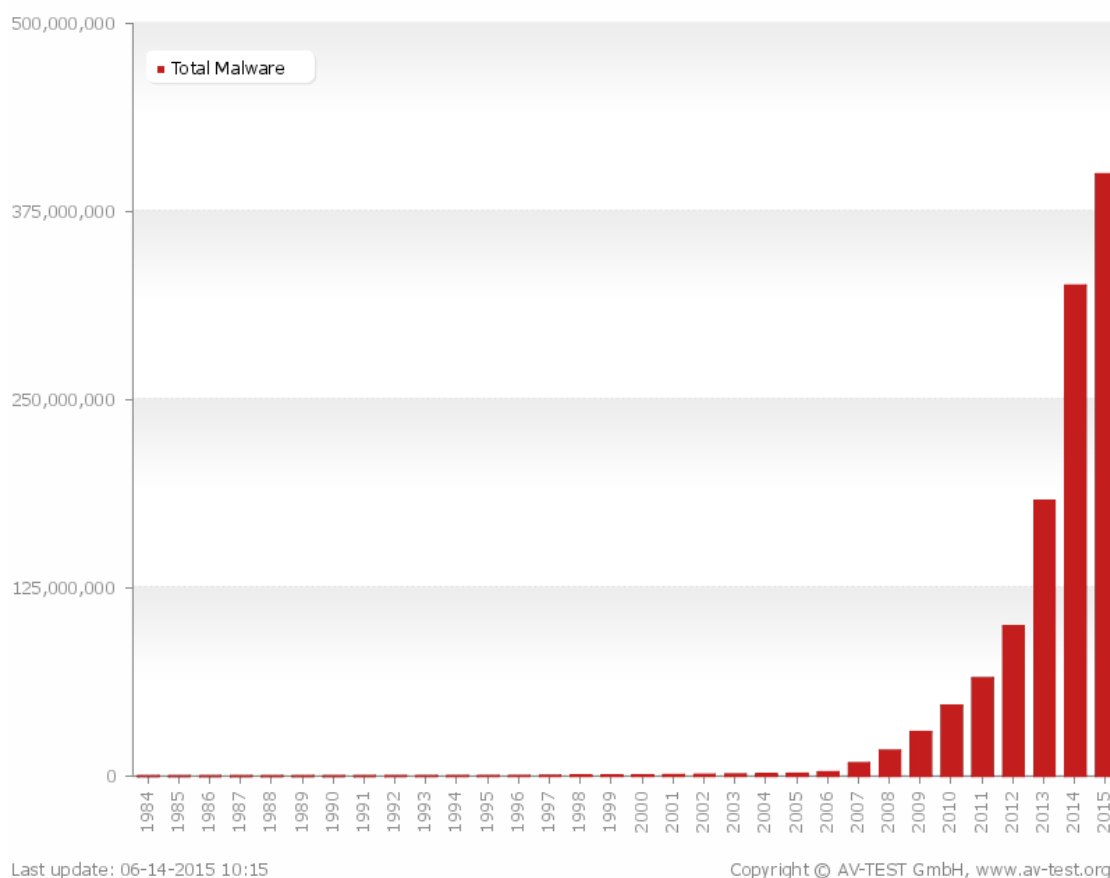
Virus většinou nepracuje okamžitě, ale pouze za určitých podmínek (ty určí autor viru).

Výše uvedená definice se týká pouze klasických souborových virů. Ačkoliv se i tyto druhy virů občas ještě objevují, v několika posledních letech představují závažné riziko počítačovým systémům spíše jiné druhy škodlivého kódu.

V průběhu doby se pojetí virů trochu změnilo, dnes je obvykle pojem počítačový virus chápán jako synonymum pro jakýkoliv škodlivý kód.

Činnost viru

1. zábavná (např. pozdrav k Velikonocům)
2. zhoubná (poškození nebo úplná destrukce dat na paměťovém médiu).
3. zneužívající (zneužívá počítač uživatele pro rozesílání spamu, útoky na jiné systémy, apod.)
4. špionážní (sleduje činnosti uživatele a o jeho aktivitách podává hlášení)



Obrázek 3.1: Celkový počet vzorků škodlivého kódu v databázi testovací laboratoře AV-Test (převzato z [37])



Zapamatujte si

Klasická definice říká, že počítačový virus je *zvláštní program, jehož chování připomíná chování biologických virů. Na paměťovém médiu vyhledává programy, které jsou nenakažené a ty pak „infikuje“. Připojí k danému programu další instrukce - vlastní virus - ten bude infikovat další programy.*

Z hlediska zamýšlené činnosti malware lze pozorovat výrazný posun v čase. Ještě v devadesátých letech minulého století byla převažující činností, zábava popř. destrukce. To odpovídalo autorům malware spíše samotářským, kteří tvořili malware za účelem pobavení sebe sama, prostě zvědavosti, zda je něco takového možné skutečně realizovat, popř. ve snaze pomstít se „zlému světu“.

Počátek století 21. je ve znamení profesionalizace autorů malware - ti již vědí, co je a není technicky možné (toho, co není technicky možné přitom zase tak moc není). Profesionalizací rozumíme fakt, že autoři malware, mají vývoj tohoto typu software jako svůj hlavní zdroj obživy. To ale v praxi znamená, že zábavná a destruktivní činnost z portfolia škodlivého kódu takřka vymizely, jelikož ovládnutí počítače a jeho využití pro účely útočníka je pro útočníka finančně podstatně výhodnější.

Autoři malware proto tvoří samotnou špičku uzavřených, vysoce organizovaných zločinných uskupení s mezinárodní působností, se kterými je velmi problematické odhalovat a stíhat.

Rozdělení:

1. viry souborové (dle definice výše)
2. červi (worms)
3. trojští koně (trojans, někdy také označované jako zadní vrátka – backdoor)
4. hoax

5. dialer
6. rootkit
7. spyware
8. ransomware
9. a další

Klasické viry (souborové) jsme si již definovali výše, jejich zastoupení v celkovém množství ročně vyvinutých virů se z dominantního podílu ještě v polovině devadesátých let minulého století rychle zmenšil prakticky na nulu dnes ve prospěch mnohem záluďnějších červů. Přesto ke vzdělání v této oblasti patří alespoň základní přehled o typech virů.

Tyto viry lze rozdělit podle jejich chování například následujícím způsobem:

1. *klasické* – dle definice bez dalších „vychytávek“. Detekce takového viru se děje pomocí tzv. *signatur*. Signatury obsahují kusy těla kódu viru, podle kterých je možno jednoznačně virus identifikovat.
2. *bootovací* – zavádí se do speciální oblasti disku tzv. boot sektoru. K aktivaci takového viru tedy dojde pokaždé při startování počítače. Některé počítače mají možnost zapnout funkci sledující přepis boot sektoru na úrovni **Basic Input Output System (BIOS)** a umožnit tak uživateli rozhodnout jestli zásah je oprávněný (např. během instalace operačního systému) nebo ne.
3. *Stealth* (skrývající se, neviditelné) – infikované soubory je možné odhalit podle toho, že se do nich přidal kód viru. Některé viry ovšem zůstávají rezidentní v paměti a v případě, že dojde ke „skenování“ infikovaného souboru pomocí antiviru tyto viry předloží soubor původní a proto mohou unikát i relativně dlouho detekci. Jedinou možností, jak se spolehlivě takového viru zbavit je nahrát systém s prokazatelně „čistého (nezavirovaného)“ disku - a provést likvidaci viru z něj. Rada výrobců antivirových produktů nabízí za tímto účelem záchranné CD.
4. *Polymorfní* – klasický vir se připojuje k souboru, tělo viru se pak soubor od souboru neliší. Antivirovému programu potom stačilo mít databázi takových změn – signatur viru – aby odhalil infekci. Polymorfní viry jsou ale jiné, obsahují náhodně generované části, které takovýto druh detekce znesnadňují, až znemožňují. Z tohoto důvodu vyvinuly antivirové firmy nástroje pro tzv. heuristickou analýzu. Kód jednotlivých souborů byl pomocí ní analyzován, zda neobsahuje instrukce, které by mohly být znakem viru. Pozitivem takové analýzy je, že umožňuje detekovat i nové antivirovému programu zatím neznáme viry, negativem je ale také možnost falešného poplachu – tedy situace kdy je soubor vyhodnocen jako zavirovaný ačkoliv je čistý.

3.2 Červi

Červi (worms) pro své šíření využívají jiný mechanismus obvykle založený na zneužití chyby v operačním systému, popřípadě v klientu e-mailu často spojeném i s určitou mírou sociálního inženýrství. Prvním masivně rozšířeným červem byl nechvalně známý *I love you virus*.

Jeho šíření bylo založeno na tom, že příjemce e-mailu s předmětem *I love you* si přečte přílohu e-mailu, čímž dojde k nakažení počítače. Podobným způsobem funguje i virus *Anna Kurniková*, který pro změnu slibuje příjemci v příloze obrázky populární ruské tenistky. V příloze je samozřejmě místo obrázků virus. Toto jsou typické příklady **sociálního inženýrství** pro šíření viru.

Dalším způsobem, o kterém jsem se zmínil je šíření s využitím chyby v operačním systému nebo v nějakém programu. Typickým představitelem této skupiny může být virus *Klez* nebo *Bugbear*. Oba viry využívají chyby v MS Internet Exploreru, která umožňuje, aby e-mail v **Hyper Text Markup Language (HTML)** formátu sám spustil svou přílohu. Tyto viry tedy apriori nepotřebují spolupráci uživatele, stačí, když si obě e-mail přečte a infekce je automatická.

Šíření viru se děje po napadení počítače automatickým rozesláním e-mailů na adresy, které jsou v adresáři klienta e-mailu. Někteří červi se navíc snaží analyzovat dokumenty na napadeném počítači a adresy hledat i tam. Zdaleka nejvíc virů se šíří právě tímto způsobem, objevilo se ale také několik zajímavých virů, které využívají chyb v jiných programech. Například ve své době široce medializovaný *Code Red* nebo *Nimda* pro své šíření využívaly aktivně chyby v MS **Internet Information Service (IIS)**. Infikovaly tedy nejprve veřejně přístupný web server a odtud se dostali pohodlně do vnitřní sítě společnosti.

Virus *Slammer* zase využil chyby v MS SQL Server. Tento virus měl také relativně dlouhou dobu pověst nejrychleji se šířícího viru, který kdy byl naprogramován. Toto vítězství však bylo pouze krátkodobé a již záhy jej o tuto pochybnou poctu připravil virus *MyDoom*.

Odborníci na virovou ochranu varují, že v současné době je možné naprogramovat počítačový vir tak, aby se masivně rozšířil celosvětově během deseti minut na několik milionů počítačů. Tento teoretický virus pojmenovali *Flash*.

Předpoklad takového masivního šíření je přitom relativně jednoduše splnitelný, je třeba vytipovat bezpečnostní chybu, pomocí které se virus bude šířit a vytipovat několik tisíc počítačů přístupným nějakou formou přes Internet (ať už přes e-mail nebo nějaký server), které mají být v prvních okamžicích napadeny. Další šíření se potom děje lavinovým efektem a bude omezeno pouze propustností přenosových tras.

V současnosti však tvůrci škodlivého kódu jdou trochu jiným směrem - s masivním šířením škodlivého kódu je totiž spojen pro jeho autora nepříjemný aspekt, vytváří totiž detekovatelné změny v síťovém provozu, což může vést k jeho odhalení a následnému odstranění, čemuž se autor červa chce vyhnout. Z tohoto důvodu je dnes autory červů většinou preferován pomalejší proces infikování cílových počítačů.



Zapamatujte si

Červi často využívají chyb v programech nebo samotném operačním systému. Moderní operační systémy jsou obrovské produkty a s velikostí jdou bohužel ruku v ruce i chyby. Tyto chyby pak představují zranitelnosti systému, které může autor malware zneužít pro infikování počítače. Společnosti vyvíjející operační systémy přitom evidují průměrnou dobu mezi nalezením a zveřejněním chyby v produktu do doby jeho zneužití například počítačovým virem. Ještě v roce 2000 tato doba byla okolo 400 dní, v roce 2005 to však bylo již pouze dni 40 a tato doba se dále zkracuje. To vyvíjí obrovský tlak na výrobce softwaru, kteří jsou z logiky věci podobně jako antivirové firmy o krok pozadu za autory virů.

Nejhorší variantou zranitelnosti jsou tzv. *zero-day zranitelnosti* (zranitelnosti nulového dne) - jedná se o zranitelnosti, které jsou aktivně zneužívány a zároveň na ně neexistuje „záplata“ od autora postiženého produktu.

3.3 Trojští koně

Trojští koně (trojans) nejsou počítačovými viry v pravém smyslu tohoto výrazu. Ve skutečnosti se jedná o plnohodnotné programy, které kromě toho co deklarují, že dělají také dělají i něco jiného – obvykle nežádoucího. Typickým příkladem trojského koně je program *BackOriffice*. Tento program deklaruje, že slouží pro vzdálenou správu počítače, tedy, že se oprávněný uživatel může připojit odkudkoliv ke svému počítači a pracovat s ním stejným způsobem, jako by u něj seděl.

Tuto činnost *BackOriffice* skutečně umožňuje, tou „přidanou“ funkcí, která ho řadí do kategorie trojských konů je to, že okamžitě po své instalaci na počítač se snaží upozornit svého tvůrce na to kde je nainstalovaný a umožnit mu tak plný přístup k napadenému počítači. Podobně fungujícím trojským koním říkáme *zadní vrátka* (*back door*).

Trojských koní existuje kromě zadních vrátek několik druhů. **Dialer** je vysvětlen v samostatném pojednání (viz níže), z určitého hlediska bychom tento druh programů mohli zařadit i mezi trojské koně.

Další sub-kategorií jsou tzv. *keylogery* – tedy programy, které slouží k zaznamenávání stisknutých kláves. Nebezpečí zneužití je tady očividné, tento druh programů bez problémů umožní útočníkovi získat přihlašovací jména a hesla, čísla kreditních karet apod., protože text zadávaný na klávesnici není většinou nijak chráněn (je dostupný v otevřené podobě). Existují i varianty tohoto typů trojského koně umožňující zachytávání také obrazovky samotné a pohybu myši na ní.

Detekce takových „virů“ je značně obtížná – programy totiž mohou mít legální užití, hranice v tomto případě co je považováno za běžný program a co za škodlivý kód je v mnoha případech značně tenká. To je také jeden z důvodů, proč se relativně dlouhou dobu firmy vyvíjející antivirové programy vyhýbaly detekci trojských koní - pravděpodobně v důsledku obav o výsledek případných soudních sporů. Dnes však již všechny používanější antivirové programy detekci trojských koní našťastí obsahují.

To že programy podobné *BackOriffice* mohou být použity pro naprosto legální dálkovou správu počítače je jasné, méně očividné je legální použití keylogerů. Pomocí takových aplikací může za určitých okolností např. zaměstnavatel kontrolovat, k jakým činnostem využívá zaměstnanec firemní

počítač. Tato oblast je však přísně regulována úřadem na ochranu osobních údajů v souladu s platnou legislativou.

Dialer je speciální druh programu, který po své instalaci připojuje dial-up připojení přes drahého, často zahraničního poskytovatele Internetu. Záludnost tohoto programu spočívá v tom, že toto připojování probíhá bez vědomí uživatele. Ohroženy jsou všechny formy vytáčeného připojení (dial-up i **Integrated Services Digital Network (ISDN)**, **General Packet Radio Service (GPRS)**), ohroženy naopak nejsou **Asymmetric Digital Subscriber Line (ADSL)**/**Very High Speed DSL (VDSL)**, wi-fi, mikrovlnné připojení, připojení pomocí kabelové televize, optického kabelu . . .

Kupodivu i přesměrování připojení mohla mít legální charakter, některé služby na Internetu (především pornografického charakteru) tímto způsobem financovala svůj provoz. Po připojení se na takovou stránku je uživatel upozorněn na přesměrování připojení i jeho důvod včetně ceny a je na samotném uživateli zda tento způsob připojení akceptuje. Doba největšího rozmachu tohoto typu malware však již pominula s nástupem široce dostupného vysokorychlostního připojení k Internetu, které je vůči činnosti dialeru imunní.

Dropper je trojským koněm, který slouží jako nosič dalšího škodlivého kódu. Po svém spuštění vypustí do systému několik dalších virů, trojských koňů a zajistí, aby se aktivovaly (došlo k infekci počítače těmito viry).

Downloader je skupina trojských koní, kteří mají podobný úkol jako trojské koně ve skupině dropper. Downloader však malware stahuje z nějakého předem určeného místa. Takoví trojští koně jsou mnohem nebezpečnější než předchozí skupina, protože autorovi umožňují lepší management škodlivého kódu, může jej aktualizovat s ohledem na případnou detekci nebo změnu požadované funkčnosti.

Trojan-proxy jsou trojské koně, které z napadeného počítače dělají proxy pro připojování k Internetu. Hacker, aby nemohl být jednoduše vystopován, nemůže systémy napadat ze svého počítače přímo, z tohoto důvodu využívá tzv. proxy serverů, přes které směřuje svůj internetový provoz a útočníkem z hlediska vysledovatelnosti se stává proxy server. Při časté změně proxy je velmi obtížné vysledovat, odkud ve skutečnosti přichází útok.

Proxy má také další vlastnost, která je zajímavá z hlediska využití autorem malware, tou je možnost směřovat síťový provoz dalších počítačů přes tento počítač. To útočnickovi umožňuje získávat citlivé informace o chování majitelů napadených systémů, které může dále využívat pro dosažení svých cílů.

Rootkity jsou poslední dobou často skloňovanou skupinou škodlivého kódu zejména v souvislosti s široce medializovanou kauzou Sony BMG a jejich rootkitem obsaženým na hudebních **Compact Disc (CD)**. Sony rootkity přibalovala v letech 2005 - 2007 do svých hudebních CD s cílem zabránit jejich kopírování na běžných PC (**Personal Computer (PC)**).

Rootkit je program, který slouží k zamaskování určitých aktivit na počítači. Původně se rootkity objevily v Unixových operačních systémech k maskování nelegální činnosti hackerů (login, nahrazování systémových knihoven apod.).

V dnešní době jsou rootkity problémem i v operačních systémech MS Windows. Z hlediska fungování je možné je rozdělit tzv. *user mode* a *kernel mode* rootkity. Nejčastějším případem tzv. user mode rootkitů je modifikace cest a úprava registrů tak, aby standardní moduly Windows nebyly schopny zobrazení těchto položek a přitom funkčnost zůstala zachována.

Kernel mode rootkity se staví mezi uživatele systému a jádro OS (kernel). Tímto způsobem získávají plnou kontrolu nad odezvou systémových knihoven, což používají pro skrývání sebe samých nebo další činnosti, která probíhá na napadeném počítači a má zůstat skrytá. Do této skupiny zařazujeme např. **Application Programming Interface (API) hooks**, kdy rootkit modifikuje výsledky volání API funkcí operačního systému s cílem zakrýt některá místa na disku, přítomnost procesů apod.

Rootkity jsou nebezpečné zejména tím, že neumožňují uživatelům plnou kontrolu nad svým systémem, tyto nekontrolované oblasti mohou být použity pro zamaskování nežádoucích aktivit. Zároveň je jejich detekce obtížná, obtížnější než u ostatních typů malware a často vyžaduje použití specializované detekční software a interpretaci jejich výsledků odborníkem na IT.

Zvláštní skupinu trojských koní, která se v poslední době objevila je tzv. **ransomware**. Tento typ škodlivého kódu se nainstaluje do počítače a následně zašifruje obsah disku. Uživateli je pak zobrazena výzva o zaplacení výkupného za data. Vzhledem k tomu, že tyto programy využívají silných šifrovacích algoritmů prolomení hrubou silou nebo nějakou známou zranitelností není v současnosti možné.

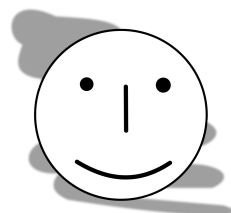
Typickým představitelem této skupiny malware je **Cryptolocker**, v některé z jeho variant. Platby v takovém případě obvykle probíhají přes některou z tzv. krptyoměn, jako je Bitcoin a podobně. Tento způsob platby je extrémně obtížné vysledovatelný, čehož autoři takových programů s oblibou využívají.

Metod sociálního inženýrství využívají ve svůj prospěch tzv. **rogue antivirus** (falešné antiviry). Ty využívají strachu uživatelů z případné infekce a nabízejí jim ke stažení antivirové programy údajně schopné kvalitně ochránit jejich počítač, což dokládají počtem imaginárních červů, virů a jiné havěti, které nadetekovaly ve Vašem počítači, se kterými se pak po instalaci statečně poperou. Běžní uživatelé mohou být zmateni častou podobou názvu produktu s věhlasným antivirovým programem a také grafická zdařilost **Graphical User Interface (GUI)** programu.

I v tomto případě je ochranou především obezřetnost uživatele a schopnost rozlišit, to co je a co není reálné.

3.4 Hoax

Hoax (humbuk) jsou zvláštní třídou virů, které ke svému šíření a činnosti využívají pouze sociální inženýrství. Jedná se zejména o varování proti počítačovým virům s přiloženým „návodem na jeho odstranění“, který bývá značně destruktivní. Tyto viry přímo počítají s tím, že se dostanou k uživatelům – „neodborníkům“, kteří v dobré víře ve snaze vypořádat se s neexistujícím virem jsou schopni „pomoci“ sobě i kolegům v širokém okolí.



Přestávka

Veselý, silně přehnaný příklad:

Dobrý den,

jsem Albánský virus. V Albánii je v současné době obtížná ekonomická situace, která se projevuje i v oblasti programování počítačových virů, proto Vás touto cestou prosím, abyste na svém počítači náhodně vybrali tři soubory a smazali je a potom mě přeposlali na všechny e-mailové adresy ve Vašem adresáři.

Děkuji

Albánský virus

Proti takovým virům v současné době neexistuje jiná obrana, než vzdělávání uživatelů v oblasti informačních technologií. Takovýto „poučený“ uživatel ví alespoň zhruba co možné je a co není a když si není jistý, má kontakt na systémového administrátora, kterého může požádat v případě potřeby o pomoc.

3.5 Spyware a phishing

Spyware

Opět se nejedná o počítačové viry v pravém slova smyslu. Řada programů freewarového charakteru v sobě obsahuje komponentu, která sleduje některé činnosti uživatele a tyto činnosti v periodických intervalech odesílá výrobci. Softwaru, který obsahuje takové komponenty, říkáme **spyware**.

Činnost těchto programů lze přirovnat k určité formě průzkumu. Jsou sledovány činnosti uživatele a ty jsou většinou anonymně odesílány zadavateli. Výrobce softwaru pak další vývoj financuje z výnosů takového průzkumu.

Na první pohled se jeví použití takových programů jako bezproblémové, bohužel není tomu tak vždy. Slídící komponenty totiž většinou nejsou transparentní – uživatel tedy neví, jaké informace jsou z jeho počítače odesílány, ani jak s nimi bude na místě určení dále naloženo. Dále některé z těchto komponent jsou z hlediska své činnosti poměrně „agresivní“ a jejich činnost tak může ovlivnit například připojení k Internetu – náhle se objevující pop-up okna pochybného charakteru, funkce chodu systému jako celku – neúnosné zpomalení počítače apod.

V dnešní době se spyware šíří také přímo přes Internet, pro své šíření využívá zejména chyb v prohlížečích **World Wide Web (WWW)** obsahu, které za určitých okolností umožňují instalovat programy na počítač bez souhlasu uživatele.

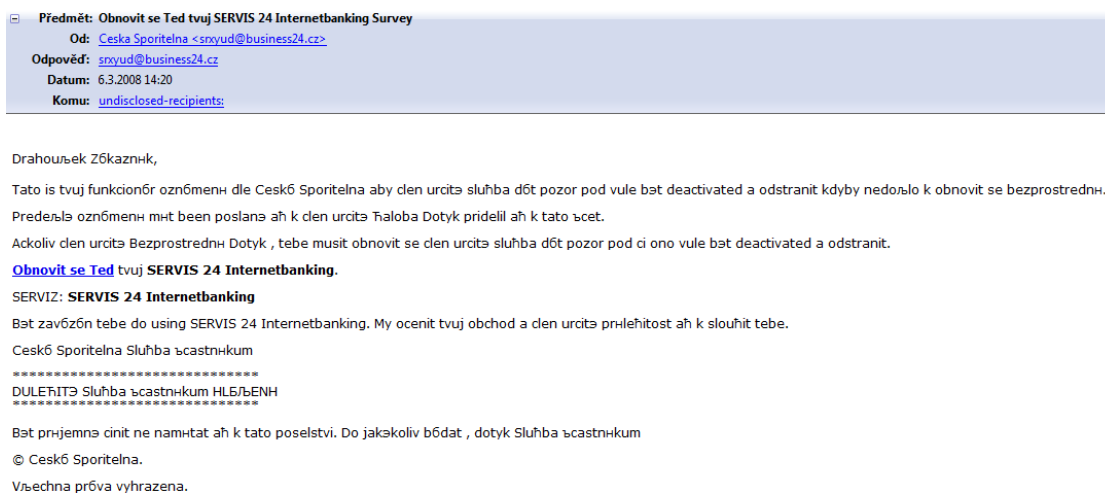
Zejména ve vnitropodnikových sítích je spyware považován za závažné ohrožení bezpečnosti sítě a s jako takovým je s ním nakládáno.

Phishing (rhybaření)

Slovem **phishing** (česky rhybaření – ne nejedná o překlep ani v anglické ani v české verzi slova) se označují e-maily, které mají přesvědčit čtenáře k sdělení citlivých údajů.

Útočník formuluje e-mail jazykově i vzhledově tak, aby u příjemce vytvořil dojem, že se jej snaží kontaktovat instituce, které za normálních okolností důvěřuje (např. banka). Uživatel je vyzván, aby se připojil na určité stránky a vyplnil tam své přihlašovací údaje nebo čísla kreditních karet. Útočník to odůvodňuje nutností ověřit platbu, pádem systému a nutností doplnění informací.

Takové informace mohou být zneužity pro vybrání konta oběti. Až donedávna bylo naší výhodou jazyková bariéra. 99 % podvodných mailů bylo totiž psáno v anglickém jazyce, a takováto komunikace banky s českým klientem je pro každého jasně krajně podezřelá. Koncem února 2006 se ale objevil první česky psaný phishing, ve kterém se jeho autor vydává za CityBank. Největšího mediálního úspěchu však dosáhl až phishing zaměřený na klienty České spořitelny, familiérně přezdívaný drahoušek zákazníků, viz 3.2.



Obrázek 3.2: Phishing zaměřený na zákazníky České spořitelny - legendární *Drahoušek zákazník*

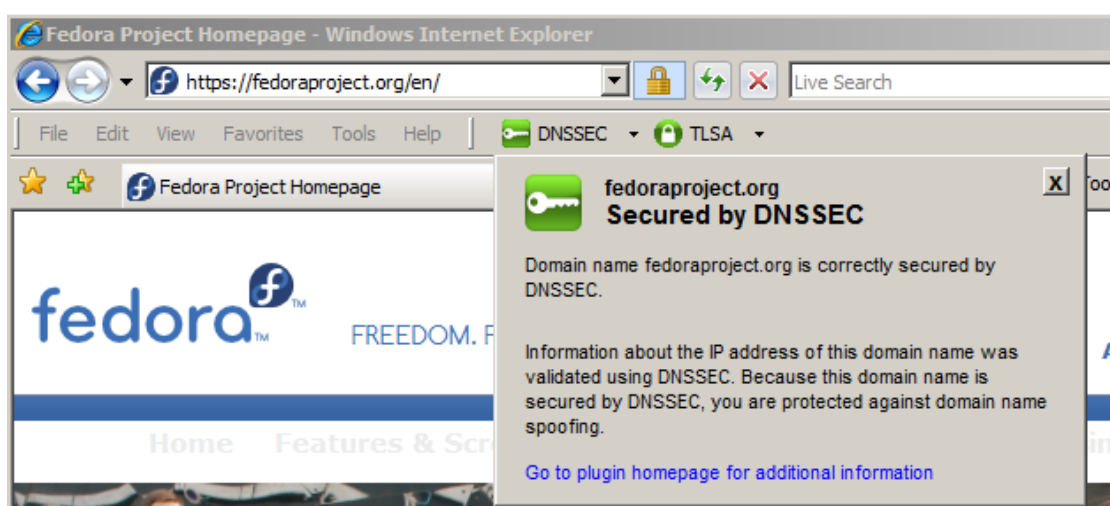
Dnes lze říci, že hračka, kterou pro autory phishingových útoků představoval český jazyk již byla překonána, řada v současnosti probíhajících útoků proto z jazykového hlediska není takto jednoduše identifikovatelná. Tím spíše je odpovědnost na nás jako koncových uživatelích systémů, aby nedošlo ke kompromitaci našich účtů. Nabízíme proto několik momentů, použitelných pro identifikaci a bezpečnou manipulaci s webovými službami.

1. zkontrolujte text mailu po jazykové stránce - máte z něj dobrý pocit?
2. zkontrolujte e-mail adresu odesílatele, zejména část za znakem @. Tato část e-mailové adresy má vazbu na doménu, ze které byl mail odeslán - přináleží skutečně očekávanému odesílateli nebo se jedná o nějakou generickou doménu jako je gmail.com, seznam.cz popř. se jedná o úplně jinou adresu?
3. test zdravého rozumu - pokud je po Vás v e-mailu žádáno něco, co je očividně nesmyslné, nebezpečné nebo sporné, s vysokou pravděpodobností se jedná o podvod. Typickým příkladem je žádost o zaslání přihlašovacích údajů apod.
4. pokud si nejste jisti ověřte si informaci, ale pozor - informaci je potřeba ověřit z odlišného zdroje, než ze sporného e-mailu. Pro ověření proto nepoužíváme odkazy, e-maily nebo telefonní čísla uvedené v takovém mailu - tyto informace získáme na oficiálních stránkách dané instituce nebo služby.

Do určité míry lze také ověřit validitu webových sídel nebo domén, na kterých se nacházejí. K tomuto účelu lze použít technologii **DNSSec**. Tato technologie je založena na elektronickém podpisu (principy elektronického podpisu jsou podrobněji vysvětleny v samostatné kapitole). Všechny změny v registru domén jsou tak v případě použití DNSSec elektronicky podepsány vlastníkem domény. Pro případného útočníka je tak mnohem obtížnější kompromitovat bezpečnost DNS.

Na úrovni koncového uživatele, který webové sídlo nebo službu bude používat, lze ověřit, zda doména je zabezpečena pomocí DNSSEC a také to, zda certifikát, který byl použit pro podepsání, přísluší k oficiálnímu vlastníku a byl vydán důvěryhodnou certifikační autoritou. Ověřování v takovém případě, ale nezabezpečuje přímo samotný webový prohlížeč, pro možnost ověření je potřeba doinstalovat vhodné rozšíření. Nejpoužívanějším pro tento účel je rozšíření sdružení CZ.NIC nazvané DNSSEC/TLSA Validator add-in for Web Browsers [47].

Validator je dostupný pro většinu z používaných webových prohlížečů. Určitou představu o funkci si je možné udělat z obr. 3.3.



Obrázek 3.3: DNSSEC/TLSA Validator add-in for Web Browsers v MS Internet Explorer (převzato z [47])

Stále častěji se objevuje také nebezpečná varianta phishingu nazvaná **vishing**. Samotné slovo vishing je tvořeno ze slov voice phishing, které charakterizují princip tohoto podvodného jednání. Podobně jako phishing je prvotní kontakt s případnou obětí proveden pomocí e-mailu, který se tváří jako e-mail od Vaší banky nebo poskytovatele nějakých služeb apod. Na rozdíl od phishingu, ale neodkazuje podvodný e-mail na podvržené stránky, ale obsahuje telefonní číslo.

Telefonní číslo přitom patří podvodníkovi, který z oběti dostane informace, které potřebuje. Případné oběti mají pro komunikaci přes telefon větší důvěru než pro komunikaci přes e-mail, o to je tento postup nebezpečnější.

Sítě botů

Trendem dnešní doby je propojování různých druhů škodlivého kódu. Objevilo se několik virů, které na napadené počítače instalovaly zároveň i trojského koně, nebo otevíraly porty pro pozdější zneužití tohoto počítače. Tento trend je v zásadě výsledkem značné profesionalizace tvůrců virů. Nejspíš také proto dnes prakticky vymizely čistě destruktivní viry.

Počítačům, které byly napadeny tak, aby poskytovaly přístup z vnějšku, se říká *zombie PC*, podobně jako jejich filmové protiklady mohou kdykoliv „vstát z mrtvých“ a začít ohrožovat okolí. Takové počítače mohou být využity např. skupinami hackerů pro útoky na další počítačové sítě, nebo mohou být zneužity rozesílateli nevyžádané pošty (SPAM) k distribuci, dalšími viry, jako místo průniku apod.

Takovým způsobem napadeným počítačům sdružených do sítí říkáme **sítě botů**. Tento název je odvozen od slova robot. Myšlenka vytváření botů není nijak nová. Prakticky byla realizována v podobě podobné té dnešní v rámci automatizace správy diskuzních **Internet Relay Chat (IRC)** kanálu. Kanály se svou možností téměř okamžitou komunikací mezi uživateli staly velmi populární. S nárůstem užívání, však narostl i objem prací moderátorů kanálů až se přišlo s myšlenkou, že většina činností, které moderátor kanálů provádí, se opakuje a tyto opakující se činnosti je možné automatizovat pomocí samostatných programků – botů. Ty se v kanále objevují jako uživatelé, ale místo konverzace se jim zasílají pokyny pro archivaci kanálu, vypsání pravidel pro uživatele apod.

Podobným způsobem fungují i sítě botů. Jejich úkolem je ale spravovat vzdálené počítače této sítě a ulehčovat hackerovi jeho činnost.

Infrastruktura určená k ovládní těchto sítí je často označována jako **Command and Control Infrastructure (C & C)**. Tato infrastruktura umožňuje, aby majitel sítě napadených počítačů mohl tyto centralizovaně ovládat ke svému prospěchu. Antivirové společnosti spolu orgány činnými v trestním řízení se naopak zaměřují na vyřazení této infrastruktury. Teprve při její nefunkčnosti existuje naděje na vyřazení celé sítě.

3.6 SPAM

SPAM neřadíme k počítačovým virům, nicméně pro úplnost jej tady doplňuji. SPAM by se dal česky popsat jako nevyžádané obchodní sdělení. Tvůrci spamu využívají toho, že elektronické šíření obchodních nabídek prakticky nic nestojí a proto je masově šíří všem lidem na které mají e-mail. Doufají přitom, že nějaké malé procento na tyto nabídky zareagují a zboží/službu si objednají.



Přestávka

Původ slova SPAM ve smyslu něčeho otravného je obvykle odvozován od jedné legendární scény z Monthy Pythonova létajícího cirkusu.

Díky moderním technologiím se na ni můžete podívat také vy:

<http://www.youtube.com/watch?v=anwy2MPT5RE&feature=related>

V řadě zemí je rozesílání spamu trestné. Ne jinak je tomu i v ČR, kde jsme měli donedávna jeden z nejprísnejších zákonů (alespoň co do definice SPAMu) na světě. U nás je SPAM definován v *zákoně 480/2004 Sb. o některých službách v informační společnosti* [31]. Jako SPAM je definováno jakékoliv obchodní sdělení, které nebylo předem vyžádáno. Toto poměrně přísné omezení bylo následně změkčeno předpokladem automatického souhlas s posíláním obchodních sdělení firm, se kterými měla v minulosti daná osoba nějakou formu obchodního vztahu (např. něco od ní zakoupila).

I v tomto případě jsou však na obchodní sdělení kladeny poměrně přísné nároky, především nutnost každé takové sdělení viditelně označit jako obchodní sdělení a přímo ve zprávě umožnit příjemci odhlásit se od odběru takových sdělení.

Nad dodržováním zákona bdí **Úřad pro ochranu osobních údajů (ÚOOÚ)**. Právě tento úřad přijímá podání pro porušení ustanovení zákona o některých službách v informační společnosti a může firmám tento zákon porušující udělit i opakovaně pokutu až 10 miliónů Kč. Logicky do působnosti úřadu spadají pouze společnosti, které působí v ČR a podléhají tedy právnímu řádu ČR.

Obecně existují dva základní principy, ke kterým se při definici co je to SPAM přistupuje:

1. opt-in
2. opt-out

Opt-in princip je prosazován v ČR, znamená, že odběratel musí předem souhlasit s posíláním obchodních sdělení. *Opt-out* princip platí třeba v USA a implicitně předpokládá souhlas se zasíláním obchodních sdělení, s tím že odběratel může kdykoliv požadovat ukončení zasílání (rozesílatel SPAMu ze zahraničí však na takový požadavek zpravidla stejně nereaguje).

Dá se říci, že potírání této nelegální činnosti se v celosvětovém měřítku nedaří. Legislativa je neúčinná, protože většina odesílatelů SPAMu operuje ze států, kde je jejich činnost legální a jsou tak prakticky nepostížitelní.

3.7 Ochrana

Výše uvedený přehled různých ohrožení je poměrně neveselý, zůstává jedna otázka - *jak se bránit?* Opatření, která můžeme přijmout lze rozdělit do dvou skupin a to konkrétně na opatření preventivní a opatření aktivní.

Preventivní opatření

Mezi preventivní opatření lze zařadit různá opatření vedoucí k minimalizaci možnosti infekce počítače (nebo obecně zařízení), které hodláme chránit. Základní opatření je omezení přístupu k zařízení neoprávněným osobám. Tyto možnosti jsou obvykle přímo integrální součástí operačního systému ve

formě správy uživatelských účtů. Všechny účty běžných uživatelů by měly být chráněny heslem. Pokud citlivé údaje jsou ukládány do jiných složek než uživatelského profilu, je potřeba nastavit v těchto složkách práva tak, aby do nich měl přístup pouze oprávněný uživatel.

Moderní operační systémy obsahují funkce umožňující transparentní oddělování běžných a administrátorských činností na počítači. V případě operačního systému Windows se jedná o **User Access Control (UAC)**, v případě Unixových systémů se jedná o mechanismus SU. Tyto mechanismy chrání proti škodám způsobenými neúmyslnými zásahy do operačního systému a proto by tyto mechanismy neměly být zakazovány.

Instalovány by měly být před instalací prověřeny - že skutečně dělají, co dělat mají (nejedná se o trojského koně) a také, že byly získány z důvěryhodného zdroje a tedy nemohlo dojít o jejich pozměnění. Pokud to daný operační systém podporuje, používejte pro instalaci repozitáře aplikací (OS Linux), App Store (Apple), Play Store (Android), Windows Store (Microsoft) apod. Aplikace v nich jsou auditovány a výše uvedené nástroje lze využít také ke zjednodušení údržby aplikací formou instalace aktualizací.

Instalován by měl být pouze takový software, který je skutečně používán. Sníží se tím jednak nároky na počítač, jednak se tím zmenší oblast, která může posloužit útočníkovi k napadení systému. Všechny instalované aplikace by měly být aktualizovány, priorita u aktualizací by měla být kladena na aktualizace aplikací, u kterých je známo, že velmi často slouží jako vstupní bod infekce:

1. operační systém samotný
2. velké kancelářské balíky (MS Office, LibreOffice a další)
3. runtime moduly pro spouštění některých aplikací: **Java Runtime Environment (JRE)**, Adobe Air, Adobe Flash, Adobe Shockwave
4. prohlížeče souborů **PDF**, především Adobe Reader
5. webový prohlížeč, bez ohledu na jeho výrobce

Někteří odborníci na počítačovou bezpečnost doporučují jako jednu z preventivních metod používat méně oblíbené, ale stále ještě dobře podporované operační systémy a programy - např. místo Adobe Reader používat Foxit Reader apod. Toto doporučení zdůvodňují menší atraktivností těchto produktů pro útočníky.

Aktivní opatření

Základním opatřením, především u systému Windows je instalace *antivirového programu*. V dnešní době je poměrně obtížné vydat autoritativní doporučení na to, který produkt je nejlepší, proto se spíše zaměříme na obecné vlastnosti a zdroje informací použitelné pro kvalifikované rozhodnutí.

Moderní antivirové programy by kromě klasických schopností detence (on-demand - sken na vyžádání, on-access - automatický sken při přístupu k souboru) měly obsahovat další komponenty pro úplnou ochranu uživatele. Výsadní postavení v těchto dodatečných komponentách hraje osobní firewall, který by měl uživatele chránit proti nežádoucímu síťovému provozu. Moderní firewall by měl být schopen kromě kontroly provozu v sobě mít také schopnosti kontroly aplikací, které tyto služby využívají (běžný firewall pouze filtrování provozu na základě IP adres a používaných portů).

Svůj význam mohou mít i moduly behaviorální analýzy s cílem zabránit, v případě proniknutí malware na počítač, napáchat škody. Takové moduly jsou často označovány zkratkou **Host Intruder Prevention System (HIPS)**. Některé bezpečnostní balíky obsahují i nástroj pro sandbox aplikací. *Sandbox* zjednodušeně řešeno zabraňuje aplikacím aby mohly zasahovat do dalších aplikací popřípadě operačního systému. Sandbox tedy slouží ke zpřísnění pravidel práce s aplikacemi nad rámec běžného systému práv a politik aplikovaných operačním systémem.

Na kvalitu jednotlivých bezpečnostních balíků lze také usuzovat z toho, jak si vedou v různých testech nezávislých testovacích laboratořích. Nejznámější jsou:

1. Test Virus Bulletin (VB100) [68]
2. AV-Test [1]
3. Matousec Proactive Security Challenge 64 [54]

Jako doplňkové nástroje mohou být použity detektory rootkitů - interpretace výsledků skenů je ale v jejich případě složitější. V případě, že existuje podezření na infekci počítače mohou mít význam i nástroje pro shromažďování údajů o spouštěných službách a aplikacích, jak je poskytují nástroje jako je **Farbar Recovery Scan Tool (FRST)** [8], **Random's System Information Tool (RSIT)** [21] nebo **DDS** [20]. Výsledkem funkce těchto produktů je vygenerování logu o fungování počítače, ze kterého

se dá identifikovat problém.

Kde aktualizovat?

Řada SW společností jako reakci na nebezpečí zneužití chyb v jimi vyvíjeném softwaru zavedla služby pro automatizované vyhledávání opravných balíčků. Microsoft zavedl tuto službu jako první s příchodem jejich operačního systému Windows 98 a tuto službu nazval jako Windows Update.

Tato služba zkontroluje registry na přítomnost aktuálních knihoven a sám nabídne opravné balíčky přehledně rozdělené do několika kategorií, dle závažnosti opravy. Podobnou službu zavedl Microsoft i pro svůj aplikační balík MS Office 2000 a vyšší. Tyto služby zde zmiňuji proto, že Windows a MS Office jsou hegemony ve své oblasti a jsou nainstalovány na až 90 % všech počítačů.

Podobné služby zavedly i jiné společnosti, například i společnosti Apple, Red Hat, Ubuntu a další pro své operační systémy. V případě těchto společností je podporována řada produktů třetích stran, což dále zvyšuje užitečnost těchto nástrojů.

Ostatní společnosti obvykle jednou za čas vydávají pro své produkty tzv. *Service Packy* (opravné balíčky), které dávají k dispozici na svých **WWW** stránkách. Většina softwarových společností neumožňuje automatickou detekci existence opravných balíčků. Vzhledem k závažnosti této problematiky se však počet společností, které automatické aktualizace nabízejí se zvyšuje.

Počítačová bezpečnost v prostředí monokultury Windows

V dnešní době jsme v situaci kdy podíl nejrůznějších verzí operačního systému Windows nasazovaných v segmentu **Small Office Home Office (SOHO)** je přes 90 %. Dá se tedy říci, že v této oblasti funguje monokulturní prostředí Windows, které s sebou nese minimální náklady na zaškolování pracovníků, pohodlnost použití těchto nástrojů apod. Bohužel to s sebou nese také negativa – zatímco se ročně objeví tisíce virů pro Windows pro Unixové operační systémy se jich objeví 100x méně.

Přitom nelze říci, že by operační systém Windows (alespoň jeho poslední verze) z bezpečnostního hlediska podstatně hůře navržen. Samotný fakt, že má takový tržní podíl z něj činí lákavý cíl pro tvůrce virů, mají tak totiž zajištěno, že potenciálních cílů bude dostatek.

V segmentu serverů má operační systém Windows má významné, nikoliv však monopolní postavení. Řada firem cíleně využívá serverů s různými operačními systémy. Tímto způsobem jednak optimalizuje náklady – vybrána je taková platforma, která je pro daný úkol vhodnější, jednak se optimalizuje i riziko, že zneužití jedné chyby určitého operačního systému povede k úplnému vyřazení celé sítě z provozu.

Podobná diverzifikace pravděpodobně v domácnostech hned tak nenastane. Z tohoto důvodu nelze do budoucna předpokládat, že by se objevila nějaká nová platforma, která by lákala tvůrce virů, a tím by poklesl virový nápor na běžného uživatele. O to náročnější je pak práce uživatele, který musí sám vyvinout úsilí, aby mohl pracovat bezpečně.

Co s bezpečností ostatních zařízení (mobilní telefony, tablety apod.)?

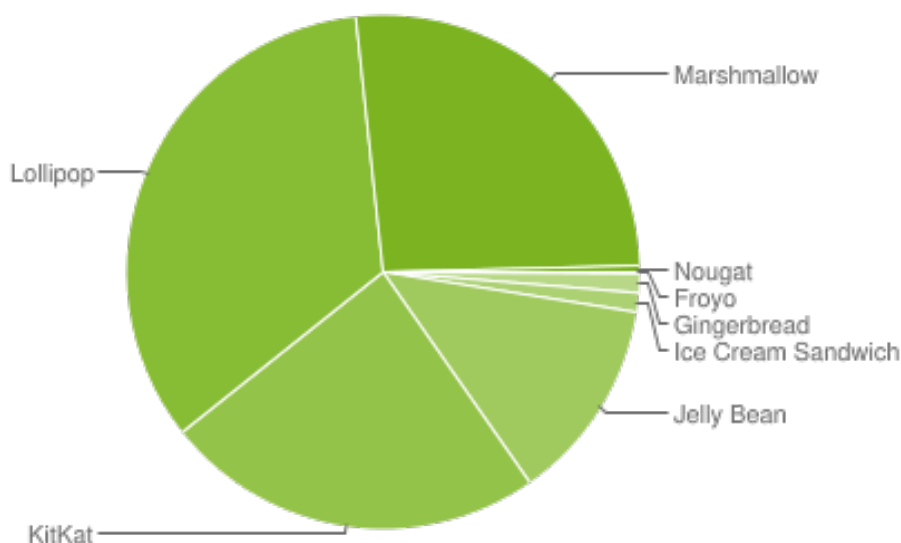
Pozor Výše uvedená pravidla a také problémy jsou typické nikoliv pouze pro počítače a notebooky, ale také další zařízení - u některých byste problém čekali: chytré mobilní telefony, tablety u jiných může být zranitelnost spíše překvapením: chytré hodinky nebo náramky, smart televize, routery, k síti připojené settop boxy, chytré žárovky, měřidla zámky.

Společným znakem těchto zařízení je to, že dosud jsme nebili nuceni zabývat se bezpečností těchto zařízení. Tato doba se ale mění, bezpečnostní hlediska využití těchto technologií již nelze pomíjet.

Významným problémem v tomto případě je, že opravování chyb není levné. V případě většiny používaných operačních systémů těchto zařízení jsou náklady rozděleny mezi společnost vyvíjející operační systém jako takový (např. Google v případě OS Android) a výrobce zařízení (např. Samsung, Lenovo, One+ a další). Výrobce pracuje tak, že vezme dostupný kód operačního systému a přizpůsobí jej pro zařízení (drivery, nadstavby OS a další). Následně takto připravenou verzi operačního systému pro podporovaná zařízení otestuje a pokud vše proběhne v pořádku zpřístupní verzi koncovým uživatelům zařízení.

Výše uvedený postup je ale drahý, proto jsou zejména lowendová zařízení podporována ze strany výrobce pouze po velmi omezenou dobu a obvykle pouze formou menších oprav. Lépe jsou pak podporována dražší zařízení, kde má výrobce výrazně větší prostor pro aktivní ochranu uživatele vytvořenou vyššími maržemi. Velmi dobře je situace viditelná např. z rozložení verzí OS Android, viz obr. 3.4.

Vzhledem k tomu, že Google v současnosti podporuje pouze OS ve verzi 5 nebo vyšší, prakticky to znamená, že přibližně 39 % zařízení s OS Android, které se aktivně připojují ke službě Google Play Store používalo nepodporovanou verzi operačního systému. Podíl nejnovějších verzí Android je



Obrázek 3.4: Podíl různých verzí OS Android k 5. prosinci 2016 (převzato z [51])

pak ve statistikách takřka zanedbatelný 0,4 % pro verzi Android 7, verze 7.1 se pak ve statistikách v současnosti neobjevuje (prosinec 2016).

I v novějších verzích OS Android pak výrobci telefonů, popř. tabletů neuvolňují nové verze OS okamžitě, ale s často poměrně dlouhým zpožděním.

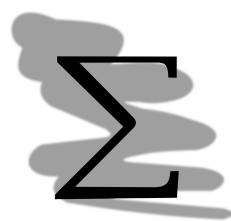
Situaci lze porovnat s podílem různých verzí operačního systému PC. Např. nepodporované Windows XP mají podle průzkumu NETMarketShare [56] na trhu podíl pouze 8,6 %, Windows Vista pak pouze 1,1 %. Pro novější verze je připravena cesta updatů, popř. upgradů OS.

Podobně závažná situace je u zařízení **IoT**. Podle analytiků BussinesInsider [52] je v současnosti připojeno k Internetu okolo 10 mld. zařízení. V roce 2020, jich ale k Internetu bude připojeno již 34 mld. Z tohoto počtu budou tradiční zařízení (PC, notebooky, telefony, tablety) tvořit přibližně jednu třetinu, zbývající většinu budou tvořit zařízení jako jsou chytré televize, set-top boxy, IP kamery, do datové sítě zapojená čidla teploty apod.

Zkušenosti z poslední doby ukazují, že bezpečnost těchto zařízení je přinejmenším sporná. Velké množství takových zařízení bylo použito v říjnu 2016 pro krátkodobé vyřazení služeb velkého amerického poskytovatele DNS služeb - společnost Dyn. Intenzita útoku **Distributed Denial of Services (DDoS)** dosáhla 1,6 Tbps (viz York [70], Schneier [60]).

Ochrana zařízení IoT je přitom složitější, jelikož na jedné straně nasazení umožňuje dosáhnout vyšší efektivity např. ve vytápění, výrobě a rozvodu elektřiny, popř. dalších služeb, jejich realizace by bez takových zařízení nebyla možná. Na straně druhé jelikož se jedná o nastupující technologie pracují výrobci s celou řadou neznámých včetně např. předpokládané době života takových zařízení a době podpory ze strany výrobce.

Zranitelnosti v současné generaci zařízení **IoT** naznačují, že do budoucna budou tato zařízení významným zdrojem rizik pro IT infrastrukturu jako takovou.



Shrnutí

Škodlivý kód je závažným a velmi složitým problémem dnešní doby. Mezi škodlivý kód řadíme počítačové viry, červy, trojské koně, spyware, rootkity.

Proti škodlivému kódu je nutné se bránit použitím specializovaného software – antivir, osobní firewall, detektory rootkitů apod. a také omezit použitelný vektor šíření škodlivého kódu instalací záplat a opravných balíčků k programům nainstalovaným na Vašem PC.



Kontrolní otázky

1. V čem spočívá nebezpečí rootkitů?
2. Co je to vektor šíření škodlivého kódu?
3. Mohou mít trojské koně nějaké legální opodstatnění?
4. Vyjmenujte alespoň tři metody aktivní ochrany proti škodlivému kódu.
5. Je spyware destruktivní?



Správné odpovědi

1. Skrývají některé činnosti před uživatelem a ten tak ztrácí úplnou kontrolu nad svým systémem.
2. Jedná se o způsob, kterým se daný škodlivý kód šíří, např. využití nějaké známé zranitelnosti operačního systému apod.
3. Ano, pokud slouží pro legální účely. Jejich legální užití je však značně omezené.
4. Použití antiviry, antispymware, detektorů rootkitů ...
5. Destrukce není primárním úkolem spyware. Bohužel se tento typ škodlivého kódu obvykle hluboko zavrtává do operačního systému, aby znesnadnil odhalení – odstranění, a to může být destruktivní z hlediska funkčnosti systému (tedy nikoliv aktivní výmaz dat).



Test

1. Keylogger zaznamenává
 - (a) Příchody a odchody zaměstnance do práce
 - (b) Stisky kláves
 - (c) Jaké programy jsou spuštěny
2. Klasické počítačové viry se vyskytují (jako podíl celkového škodlivého kódu)
 - (a) Převážně
 - (b) Tak napůl
 - (c) Skoro vůbec
3. Ve windows mi maximální bezpečnost zajišťuje účet s právy
 - (a) Administrátorskými
 - (b) Power user
 - (c) user
4. Instalovat opravy je potřeba
 - (a) Ignorovat
 - (b) Nainstalovat jak si vzpomenu
 - (c) Nainstalovat ihned co vyjdou
5. Pro detekci spyware mohou použít
 - (a) Antispymware
 - (b) Antivir
 - (c) Rootkit detektor



Správné odpovědi

1. b), 2. c), 3. c), 4. c), 5. a) b) (i když pouze omezeně)

Kapitola 4

Šifrování a elektronický podpis



Náhled kapitoly

Šifrování a elektronický podpis jsou moderními technologiemi, jejichž význam stále stoupá. To je také důvod, proč se s těmito technologiemi v této kapitole seznámíme i my.

Po přečtení kapitoly budete

Vědět

1. Co je šifra a elektronický podpis
2. Jak je jejich použití upraveno legislativně
3. Jaké jsou předpoklady bezpečnosti jednotlivých šifrovacích algoritmů popř. algoritmů elektronického podpisu



Čas pro studium

Tato kapitola je jedna z nejrozsáhlejších v těchto skriptech, zároveň obsahuje celou řadu nuancí a návazností, které by bylo vhodné během studia plně pochopit. Proto studium této kapitoly může zabrat i celý den.

4.1 Základní pojmy

Předtím než začneme se samotným výkladem šifrování jako takového zaměříme se na vysvětlení některých pojmů, které pak budou využity v dalším výkladu.

Šifrováním rozumíme obvykle proces převodu textu nebo dat z otevřené podoby do podoby šifrované. Účelem šifrování je tedy chránit text popř. data proti neoprávněnému přečtení.

Otevřeným textem/daty v tomto případě rozumíme text nebo data, která jsou přímo čitelná nebo interpretovatelná. Např. tento text je v češtině, není nijak chráněný, jedinou překážkou jeho pochopení proto mohou tvořit nové pojmy nebo myšlenky, se kterými čtenář dosud nepracoval.

Šifrovaný text předchozího odstavce by mohl vypadat např. následovně: Bgriřraýz grkgrz/qngl i gbzgb čřcngě ebmhzízr grkg arob qngn, xgreá wfbh čřzřb čvgryaá arob vagrecerbingryaá. Ancř. gragb grkg wr i čřsgvač, araí avwnx pueáačáý, wrqvabh čřrxázxbh wrub cbpubcraí zbudh gibřvg abié cbwzl arob zřšyraxl, fr xgreýzv čgraář qbřhq arcenpbiny.

Jak je vidět z předchozího odstavce, šifrovaný text není přímo čitelný/interpretovatelný. Pro jeho přečtení je vyžadována jistá znalost - *klíč*. V předchozím příkladu tvoří klíč identifikace algoritmu: Caesarova šifra s posunem abecedy o 13 znaků aplikovaná na všechny písmena bez interpunkce (písmena s interpunkcí a mezery zůstaly beze změn). K zašifrování byla použita jednoduchá webová aplikace Caesar cipher decryption tool [49].

S touto znalostí (použitého algoritmu a klíče) jsem schopen otevřený text zašifrovat a šifrovaný text zase dešifrovat.

Podle způsobu šifrování a množství klíčů, lze šifrovací algoritmy dále dělit viz další kapitoly těchto skript.

4.2 Stručná historie šifrování

Dá se říci, že šifrování je staré jako lidstvo samo, přinejmenším od vynálezu písma. První dokumentované použití šifry se datuje někdy okolo roku 1900 př. n. l. do oblasti starého Egypta, kde neznámý písař tvořil nápisy z nestandardních hieroglyfů.

Někdy k roku 1500 př. n. l. se datuje původ destičky z Mezopotámie se zašifrovaným návodem na výrobu glazur na keramiku.

Mezi 500 – 600 před naším letopočtem hebrejští učenci napsali knihu Jeremiášovu, pro kterou použili jednoduchou substituci nazývanou ATBASH, kdy použili obrácenou abecedu (místo A Z, B Y apod.).

Do roku 487 př. n. l. se datuje použití nástroje „skytale“ v Řeckém městském státě Sparta. Jednalo se o dřevěný kolík, na který se namotával úzký proužek kůže. Na tuto kůži se napsala zpráva, kůže se odmotala a poslala po poslovi na místo určení. Pro dešifrování zprávy potom bylo nutné mít kolík o správném průměru. Představu o vzhledu si můžete udělat z obr. 4.1.



Obrázek 4.1: Skytale (převzato z [27])

V období svého tažení (2. pol. 1. stol. před. n. l.) Gaius Julius Caesar pro komunikaci s Římem používal jednoduchou *substituční šifru* – jednotlivá písmena abecedy byla posunuta o tři znaky doprava.

V případě šifer ATBASH i Caesarovy abecedy otevřeného textu odpovídá právě jedna abeceda šifrovaného textu. Z toho důvodu je tento typ šifer označován jako šifry *monoalfabetické*.

Někdy mezi 725 a 790 byla napsána první teoretická kniha o šifrování, arabský učenec Abd al-Rahman al-Khalil ibn Ahmad ibn ‘Amr ibn Tammam al-Farahidi al-Zadi al-Yahmadi v ní psal o luštění kryptogramů, byl přitom inspirován svou prací luštitel pro Byzantského císaře. Do dnešní doby se bohužel tato kniha nedochovala, její obsah bych ale rekonstruován z knih dalších soudobých autorů, kteří části textu použili ve svých knihách.

Je zajímavé, že pro luštění použil metodu tzv. *známého textu*. Tedy uhodl několik slov na začátku zprávy. Tímto způsobem měl k dispozici pasáž textu v otevřené formě a jí odpovídající pasáž v podobě šifrované. Následně pouze hledal klíč, který převod mezi oběma formami umožňoval. Proces dešifrování tak mohl proběhnout velmi rychle. Obdobná metoda byla s úspěchem používána i během druhé světové války při luštění textů šifrovaných strojem Enigma.

V roce 1379 Gabrieli di Pavnice na žádost Klementa VII vytvořil jednoduchou substituční šifru spojenou s použitím jednoduchého kódu. Pro svou pohodlnost, se tato šifra používala v diplomatických sborech až do osmnáctého století.

1466 Leon Battista Alberti vynalezl a publikoval první polyabecední (polyalfabetickou) šifru. Pro snadné použití sestrojil šifrovací disk. Určitou představu o vzhledu a funkci šifrovacího disku si lze

udělat z obr. 4.2.



Obrázek 4.2: Šifrovací disk Leaona Battisty Albertiho (převzato z [42])

Polyalfabetické šifry pro šifrování využívají více než jednu šifrovací abecedu. V případě Albertiho šifrovacího disku k použití další abecedy došlo jednoduchým posunem vnitřní části šifrovacího disku. Klíč je při použití tohoto nástroje tvořen jednak šifrovacím diskem samotným, jednak znalostí o kolik se má disk posunout. Tento druh šifer byl prolomen až počátkem 19. století.

Blaise de Vigenère 1585 publikoval knihu o šifrování, ve které jako první zmiňuje koncept autoklíče, tedy šifry ve které šifrovací klíč je odvozen z předchozího písmene šifrované nebo otevřené zprávy. Tento způsob šifrování byl zapomenut a posléze v průběhu 19. století znovu vynalezen. Koncept použití autoklíče přetrval i do dnešních moderních šifer.

1917 americká vláda zaměstnala Williama Fredericka Friedmana, považovaného za duchovního otce kryptoanalýzy v USA, a jeho manželku, aby pro armádu luštili šifry.

1927 – 1933, v USA vládne prohibice, což vede k rozmachu organizovaného zločinu. Ruku v ruce s tím se začaly šifry používat utajení informací před konkurencí i policií. V reakci na to FBI zřídila oddělení, které se zabývá dešifrováním takových zpráv. Toto oddělení pracuje dosud.

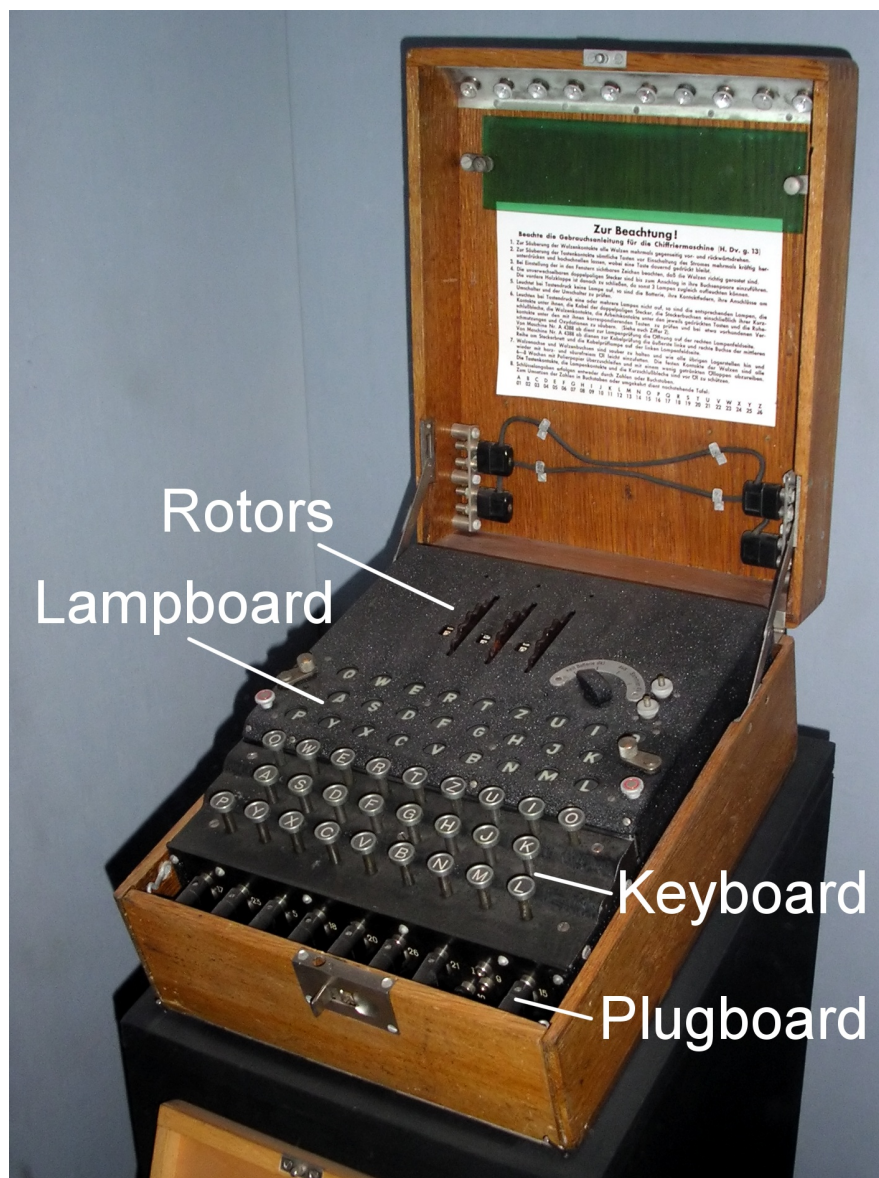
1933 – 1945 šifrovací stroj Enigma nasazen a masově využíván nacistickým Německem. Nasazení Enigmy předznamenává použití moderních technologií, jako základu bezpečnosti.

4.3 Substituční šifry

Substituční šifry fungují na tom principu, že písmena abecedy nahrazujeme podle předem stanovených pravidel za jiná písmena nebo znaky. Nejznámější substituční šifru vytvořil římský císař Caesar během svého tažení do Galie a během historie ji použil v modifikované verzi například i císař Augustus.

Caesarova šifra:

Otevřený text A B C D E F G ...
Šifrovaný text D E F G H I J ...



Obrázek 4.3: Příklad Enigma s třemi rotory (převzato z [6])

Na první pohled se jedná o šifru bezpečnou, jednotlivá písmena zprávy jsou nahrazována jinými písmeny tak aby výsledný text nebylo možné přečíst. Pokud se ale nad celým konceptem zamyslíme, zjistíme, že tomu tak není.

U každého jazyka je totiž frekvence výskytu různých písmen různá. Drobné rozdíly ve frekvenci použití písmen je možné vysledovat také v různých typech textu - např. mohou být rozdíly mezi textem odborným a beletrii. Tyto rozdíly jsou však méně významné, jelikož obvykle ovlivňují pořadí méně používaných písmen.

Na základě frekvenční analýzy otevřeného textu v daném jazyce je tedy možné seřadit písmena abecedy podle frekvence výskytu v textu a těm přiřadit znaky šifrované zprávy seřazené podle frekvence výskytu šifrovaných znaků bez nutnosti zkoumat o jaký druh substituce se jedná.

Výsledný dešifrovaný text může obsahovat chyby v některých méně používaných písmenech, ale měl by být čitelný.

Pro svou nízkou odolnost kryptoanalýze se záhy začaly objevovat pokročilejší šifry, které jsou tzv. *polyalfabetické*. Tyto šifry nepoužívají jedinou abecedu jako klasické substituční šifry, ale více abeced, přičemž tyto abecedy se střídají, obvykle po písmenu. Tímto způsobem se významně znesnadňuje frekvenční analýza textu (při použití dlouhého šifrovaného textu a malého počtu abeced je dešifrování však možné).

4.4 Kódy

Kódy rozumíme slova, která mají v běžném jazyku nějaký význam, ale my je používáme ve významu jiném. Pro úspěšné využití kódů se musí všichni účastníci komunikace předem dohodnout, jakým způsobem bude kódování probíhat – tedy zajistit, aby zakódovaná zpráva mohla být správným způsobem pochopena (dekódována).

Využití kódů lze za dodržení určitých bezpečnostních opatření považovat za bezpečnou i dnes. Pokud případný „špión“ nezná význam jednotlivých kódových slov, nemůže zprávu správně dešifrovat. Nebezpečí ale spočívá v tom, že při stálém využívání stejných kódů je možné vyzorovat u příjemce určité vzorce chování jako reakce na přijatou zprávu, ze kterého lze usuzovat na význam kódu.

Například ještě během první světové války se tento problém řešil použitím tzv. *kódových knih*. Kódová kniha obsahovala na každé stránce seznam klíčových slov pro zakódování. Po zakódování se stránka z knihy vytrhla a zničila – jednorázové kódy bez vlastnictví kódovací knihy prakticky není možné prolomit.

4.5 Symetrické a asymetrické šifry

Tématem symetrických a asymetrických šifer se dostáváme již k moderní kryptografii.

Symetrickými šiframi rozumíme šifry, které pro zašifrování i dešifrování zprávy využívají stejný klíč. Oproti asymetrickým jsou koncepčně starší. V případě Ceasarovy šifry byla klíčem znalost posunu abecedy (o 4 znaky doprava). Tato znalost postačuje pro zašifrování i dešifrování textu. Výhodou symetrických šifrovacích algoritmů je také relativně snadné hardwarové řešení a vysoká rychlost zpracování.

Typově lze symetrické šifrovací algoritmy rozdělit do dvou skupin: *blokové* a *proudové* (stream) šifrovací algoritmy. Hlavní rozdíl mezi nimi je v účelu šifrování.

Blokové šifry jsou koncepčně starší a slouží pro šifrování souborů, zpráv apod. Tento typ šifrovacích algoritmů pracuje tak, že zpracovává šifrovanou zprávu po blocích o určité délce - odtud název bloková šifra.

Proudové šifry jsou proti tomu jiné - jsou určeny pro šifrování datových proudů jejichž přesná délka není předem známa. Proudové šifry se používají pro šifrování datových přenosů, hovorů v mobilních telefonech apod.

4.5.1 Blokované šifry

První komerčně nasazená symetrická šifra byla vyvinuta v laboratořích IBM (konec 60. let) a byla nazvána *Lucifer*. Hned po uvedení na trh o systém projevil zájem některé pojišťovací společnosti s hustou sítí poboček, které v něm viděli efektivní prostředek pro zabezpečení komunikace s ústředím.

V roce 1973 americký **National Institute for Standards and Technology (NIST)** vypsal soutěž na navržení šifrovacího algoritmu pro použití ve státní správě. Do této soutěže IBM nabídla zdokonalenou verzi svého *Lucifera*. IBM v té době byla jedinou společností, která byla schopna nabídnout funkční odzkoušený systém pro šifrování a z tohoto důvodu také soutěž vyhrál.

Do finálního jednání se vedle NIST zapojila také **National Security Agency (NSA)**. Při jednání se přitom střetly dva proudy v koncepci nového standardu. První prosazoval maximální možnou bezpečnost jako prostředek pro maximální ochranu subjektů, které budou tuto šifru používat. Druhý proud prosazoval omezení bezpečnosti šifry tak, aby v případě zneužití šifry bylo technicky možné zašifrované údaje dešifrovat.

Výsledkem byl kompromis ve kterém se původně navrhovaná délka klíče 128 bitů zmenšila na 56 bitů a 23. listopadu 1976 byla šifra přijata pod názvem **Decryption Encryption Standard (DES)**.

Již těsně po uvedení šifry se objevily pochybnosti o její bezpečnosti, které ve svém důsledku vedly k vytvoření alternativního proudu v kryptografii a vyvinutí asymetrických šifer.

Již v roce 1994 mělo být možné za investice okolo 1 mil. dolarů sestavit počítač schopný dešifrovat DES hrubou silou za 3,5 hod., a to s předpokladem, že cena se každých 18 měsíců sníží na polovinu.

V dnešní době jsou reálně luštitelné šifry s klíčem 80-bitů. V reakci na tato odhalení byla v druhé polovině devadesátých let vypsána nová soutěž na standard nahrazující DES. Tato soutěž dnes již zná svého vítěze pod názvem **Advanced Encryption Standard (AES)**. NIST specifikaci tohoto algoritmu zveřejnil v rámci řady standardů **Federal Information Processing Standard (FIPS)**, konkrétně FIPS 197 [33].

Pro prodloužení životnosti šifry DES byla modifikována tak, aby zdvojnásobila bezpečnost této šifry a vytvořil se tak časový prostor pro pohodlný přechod na AES. Tato modifikace bývá označována jako **Triple DES (TDES)**, dnes se spíše používá označení **Triple Data Encryption Algorithm (TDEA)**. Algoritmus – viz doporučení NIST SP 800-67 Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher [39].

S koexistencí TDEA a AES se počítá až do roku 2030. Rok 2030 zde vystupuje jako rok mezní, do kterého všechny aplikace využívající TDEA musí zavést AES. Tak dlouhá doba (30 let) je stanovena pro to, že drtivá většina přechodů na AES bude prováděna v rámci zásadních změn používaných informačních systémů. Stávající systémy se tedy nechají „dožít“, aby byly postupně nahrazeny až se završí jejich životní cyklus. Tímto způsobem se zásadně omezí dodatečné náklady zavádění AES.

Zde zmíněné standardy samozřejmě nejsou jedinými symetrickými šiframi, které se všude po světě používají. Z těch ostatních je možné vyjmenovat například: BlowFish, IDEA apod. Pro jejich nasazování však existují určitá pravidla mající za cíl zajistit, že účel, za kterým je šifrování nasazeno bude zachován.

Z hlediska nasazení se rozlišuje obvykle mezi tzv. *legacy* a novými systémy. Legacy systémy jsou, systémy nebo programové prostředky, popř. technologie, které již byly vyvinuty, prakticky nasazeny a dále se již nevyvíjejí (resp. probíhá jejich běžná údržba, nedochází ale k přidávání nových vlastností). Tyto systémy v sobě obsahují určité technologické předpoklady, které ovlivňují jejich bezpečnost. U starších systémů jsme obvykle limitováni v možnostech výběru šifrovacího algoritmu. Tento algoritmus musí být totiž zaveden přímo v systému a jeho změna proto nemusí představovat triviální problém. Při použití legacy systémů jsme proto obvykle odkázáni na to, co systém podporuje a pokud je nabízená technologie nevyhovující, je často nutné systém jako celek nahradit systémem novým – který požadované technické vlastnosti již má.

U nových systémů nejsme obvykle omezovali určitou technologií, resp. lze specifikovat funkční požadavky na ni. Legacy systémy lze tedy vnímat jako systémy dosluhující, na které jsou kladeny menší bezpečnostní nároky, avšak s tím, že tyto systémy budou výhledově vyřazeny nebo nahrazeny systémem novým. Nové systémy by oproti tomu měly splňovat přísnější bezpečnostní parametry, protože se předpokládá, že budou dlouhodobě provozovány.

Určitá doporučení k použití šifrovacích algoritmů poskytuje **European Union Agency for Network and Information Security Agency (ENISA)**. Přehled používaných algoritmů blokových šifer s doporučeními (vydanými v roce 2013 [62]) pro nasazení je v tab. 4.1.

Tabulka 4.1: Doporučení pro nasazení algoritmů blokových šifer (převzato z [62])

	legacy	nové
AES	ano	ano
Camellia	ano	ano
TDES	ano	ne
Kasumi	ano	ne
Blowfish	ano	ne
DES	ne	ne

Tabulka 4.1 obsahuje některé šifrovací algoritmy, se kterými jsme se dosud nesečkali, podívejme se na ně nyní.

Algoritmus *Camellia* byl vyvinut v roce 2000 ve společnosti Mitsubishi a **Nipon Telegraph and Telephone Corporation (NTT)** v Japonsku. Tento algoritmus byl certifikován v rámci **Cryptography Research and Evaluation Committees (CRYPTREC)** ustaveném japonskou vládou pro certifikaci šifrovacích šifrovacích algoritmů pro použití na území Japonska a také v rámci Evropského projektu **New European Schemes for Signatures, Integrity and Encryption (NESSIE)**. *Camellia* podporuje šifrovací klíče délky 128, 192 a 256 bitů.

Standard je dostupný také ve formě **Request for Comment (RFC)** nezávislé standardizační entity **Internet Engineering Task Force (IETF)**, která se zabývá standardizací technologií používaných v celosvětové síti Internet. Konkrétně se jedná o standard RFC 3713 [55].

Šifrovací algoritmus *Kasumi* má široké použití v systémech **Universal Mobile Telecommunications System (UMTS)**, **Global System for Mobile Communications (GSM)** nebo **GPRS**. Tento algoritmus byl odvozen ze staršího algoritmu **MISTY1 (Mitsubishi Improved Security Technology (MISTY))**. Také algoritmus **MISTY1** byl vyvinut firmou Mitsubishi a byl jedním z „kandidátů“ na standardizaci v rámci **CRYPTREC**, v roce 2013, ale z posuzování vypadl. Samotný algoritmus *Kasumi* byl

navržen pro zajištění bezpečnosti v mobilních sítích třetí generace a byl certifikován v rámci **Security Algorithms Group of Experts (SAGE)**, které je součástí evropského certifikačního orgánu **European Telecommunication Standards Institute (ETSI)**.

Paradoxně je Kasumi proti MISTY1 zjednodušen. Důvodem byla příliš velká časová náročnost prováděných kryprovacích operací v rámci MISTY1 algoritmu. V roce 2010 byl publikován postup, který výrazně zjednodušuje útok na tuto šifru pomocí tzv. *útoků souvisejícími klíči*. Tento útok je založen na pozorování fungování šifrovacího algoritmu pomocí několika různých klíčů. Původní otevřeného textu sice na začátku procesu není známa, ale mezi klíči existují matematické souvislosti, které tyto klíče spojují, a které jsou známy útočníkovi. To výrazně zjednodušuje složitost útoku na šifrovací algoritmus jako takový.

Použití algoritmu Kasumi pro nové aplikace a systémy se nedoporučuje.

Algoritmus *Blowfish* navrhla v roce 1993 jedna z nejviditelnějších osobností počítačové bezpečnosti Bruce Schneier. Pro šifrování využívá klíče o velikosti 32 - 448 bitů. Základní slabinou algoritmu Blowfish je fakt, že pro něj existují tzv. *slabé klíče*, kterým je potřeba se vyhnout. Slabé klíče jsou v tomto případě všechny klíče o délce menší než 80 bitů. Výhledově by uživatelé měli přejít buď na algoritmus AES nebo na bezpečnější verze Blowfish nazvané Twofish nebo Threefish.



Fakta o Bruce Schneirovi

Když Bruce Schneier pozoruje kvantovou částici, zůstane ve stejném stavu dokud Bruce pozorování nedokončí.

Bruce Schneier umí prolomit šifrování eliptickými křivkami tím, že je ohne do podoby kruhu.

Žádná prvočísla nejsou, existují pouze taková čísla, u kterých Bruce Schneier nechce, abyste je faktorizovali.



Další „fakta“ o Bruce Schneierovi můžete zjistit z <http://www.schneierfacts.com/>.

Velikost klíče a bezpečnost

V této kapitole byla zmíněna celá řada šifrovacích algoritmů a různých velikostí šifrovacích klíčů. Z hlediska bezpečnosti obvykle platí, že čím větší je klíč, tím lépe jsou šifrovaná data chráněna. Při útoku hrubou silou totiž útočník musí pro odhalení klíče projít větší prostor, ve kterém může klíč být. Matematicky lze tuto skutečnost vyjádřit následovně (4.1):

$$p = \frac{a^k}{2} \quad (4.1)$$

Kde p je průměrný počet pokusů potřebných pro odhalení klíče. Tento počet pokusů je odvozen z velikosti použité abecedy a a velikosti klíče k . Se zvyšující se délkou klíče roste tedy složitost útoku exponenciálně. a^k přitom představuje úplný prostor (kombinace všech možných znaků), kde se může šifrovací klíč nacházet. /2 pak říká, že klíč se může nacházet jak v první tak v druhé polovině prohledávaného prostoru.

Z hlediska doporučené velikosti šifrovacího klíče existuje celá řada názorů - v současnosti se často doporučuje používat **šifrovací klíč o minimální velikosti 112 bitů** (viz např. [15]).

4.5.2 Proudové šifry

Zatímco blokové šifry jsou určeny pro šifrování souborů, e-mailů apod., šifry proudové jsou uzpůsobeny ochraně datových přenosů. Využívají se proto pro šifrování telefonních hovorů, šifrování připojení k síti WiFi apod. Jelikož šifrování proudovou šifrou pracuje v „skoro reálném“ čase, je tento typ šifer lépe optimalizován na rychlost.

Proudové šifry jsou z určitého pohledu považovány za méně bezpečné alespoň ve srovnání s šiframi blokovými. Vzhledem k tomu, že šifrovaný proud dat je časově omezen např. hovor uskutečněný pomocí mobilního telefonu délkou hovoru a šifrovací klíče se mění pro každou „session“. Je relativní slabost použitých algoritmů vyvážena častou obměnou šifrovacích klíčů, které naopak prolomení bezpečnosti znesnadňují.

I pro proudové šifry **ENISA** poskytuje doporučení [62], viz tab. 4.2.

Tabulka 4.2: Doporučení pro nasazení algoritmů proudových šifer (převzato z [62])

	legacy	nové
Rabbit	ano	ano
SNOW 3G	ano	ano
Trivium	ano	ne
SNOW 2.0	ano	ne
A5/1	ne	ne
A5/2	ne	ne
E0	ne	ne
RC4	ne	ne

Algoritmus *Rabbit* je definován ve standardu **IETF** RFC 4503 [40] a je také součástí standardu ISO/IEC 18033-4 [12]. Šifra byla poprvé prezentována v roce 2003 a standardizace v rámci RFC 4503 dosáhla v roce 2006. Algoritmus používá klíč o délce 128 bitů a 64-bitový iniciační vektor.

V současné době existuje dokumentovaný útok na algoritmus, který snižuje komplexitu útoku na 2^{158} , což je však při současných možnostech výpočetní techniky považováno stále za bezpečné (jako hranice bezpečnosti se v současnosti považuje komplexita útoku 2^{128}).

SNOW 3G je zdokonalenou verzí staršího algoritmu *SNOW 2.0*. K šifrování se používá klíč o délce 128 bitů a iniciační vektor o stejné velikosti. První verze algoritmu byla posuzována v rámci projektu **NESSIE**, verze 2.0 se stala součástí ISO/IEC 18033-4 [12]. Algoritmy se používají primárně v mobilních sítích třetí generace **UMTS**.

U těchto algoritmů jsou známy některé postupy snižující komplexitu útoku, nesnižují ji ale dost na to, aby algoritmy bylo nutné považovat za nebezpečné. Pro nové aplikace se přesto doporučuje implementovat spíše bezpečnější *SNOW 3G*.

Algoritmus *Trivium* je algoritmem nenáročným na systémové zdroje, který je standardizován v rámci ISO/IEC 29192-3 [13]. Svou konstrukcí je algoritmus obzvláště vhodný pro hardwarovou implementaci. Používá klíč i iniciační vektor o délce 80 bitů. U plně (standardizované) verze algoritmu nejsou sice známy žádné útoky snižující komplexitu možnosti prolomení šifry, avšak délka klíče 80 bitů naznačuje, že do budoucna nebude tento algoritmus schopen poskytovat dostatečnou úroveň bezpečnosti.

Algoritmus A5/1 byl původně pro užití v rámci **GSM** protokolu. Je iniciován pomocí 64-bitového klíče a známého 22-bitového iniciačního čísla. Až do roku 1994 byl tento algoritmus tajen. V roce 1994 unikly na veřejnost některé informace o tomto algoritmu, které posloužily k plné rekonstrukci algoritmu metodami reverzního inženýrství. V průběhu doby se objevila celá řada slabin tohoto algoritmu, z nichž některé mohly vést až k možnosti dešifrovat hovory v síti **GSM** v reálném čase.

Algoritmus A5/1 je proto často uváděn jako příklad nevhodnosti nasazení přístupu *security by obscurity* v klíčových technologiích. *Security by obscurity* u technologie rozumíme předpoklad, že technologie je bezpečná, pokud případný útočník neví, jak vnitřně funguje. Praxe však ukazuje, že tento předpoklad se nezakládá na pravdě a útočník může usuzovat na fungování algoritmu podle vnějšího chování algoritmu, především pomocí tzv. *postranních kanálů*.

Útok pomocí postranních kanálů se nesnaží nalézt slabiny v samotné algoritmu, ale ve způsobu jakým je implementován - např. časová náročnost práce algoritmu při zpracování různých dat, analýza odběru elektrické energie, úmyslné zavádění chyb do procesu zpracování a zkoumání reakce algoritmu apod.

Algoritmus A5/2 je oslabená verze algoritmu A5/1, které byla vyvinuta za účelem vývozu z USA. V 90. letech minulého století šifrovací algoritmy vyvinuté v USA podléhaly exportnímu embargu. Cílem tohoto embarga bylo zabránit k USA nepřátelským mocnostem získat silné šifrovací algoritmy, které by pak výrazně ztížily možnosti získávání zpravodajských informací z těchto režimů.

E0 je algoritmus používaný pro šifrování dat přenášených bezdrátovým přenosem pomocí bluetooth. Používá obvykle klíč o délce 128 bitů. Nejlepší známý útok je útok typu podmíněný korelační útok (conditional correlation attack) s komplexitou 2^{38} . Vzhledem ke komplexitě řešení není algoritmus E0 možné považovat nadále za bezpečný pro jakékoliv použití.

Konečně algoritmus RC4 je využíván v řadě protokolů jako např. **Transport Layer Security (TLS)**. Algoritmus navrhl v roce 1987 Ronald R. Rivest (jeden ze zakladatelů velmi známé společnosti RSA zabývající se bezpečnostními řešeními na bázi šifrování). Od doby zveřejnění algoritmu se objevila celá řada útoků, pro které tento algoritmus není možné doporučit k jakémukoliv dalšímu použití.

4.6 Asymetrické šifrování

Asymetrické šifry se od šifer symetrických výrazně liší. Jejich nástup umožnilo až masivní zavádění výpočetní techniky. Algoritmy asymetrického šifrování byly také odvozovány z odlišného základního modelového problému: *mějme kulatý stůl, u kterého probíhá debata, přitom každý účastník může slyšet vše co řekne u stolu kdokoliv jiný. Základním problémem v takovém prostředí je jak dohodnout klíč komunikace. Očividně jej není možné další osobě říct, protože bude odposlechnut a možná zneužit.*

Řešením tohoto problému je vyvinutí nové skupiny šifrovacích algoritmů, které nepoužívají totožný klíč pro šifrování a dešifrování komunikace, ale používají dvojici klíčů - *privátní* a *veřejný*. Tyto klíče jsou matematicky příbuzné, ale zároveň není možné je jeden z druhého odvodit. Kontrolu nad komunikací tak útočník může získat pouze získáním obou klíčů nebo vyřešením složitého faktorizačního úkolu, jehož obecné, efektivní algebraické řešení dosud není známo.

Pro účely elektronického podpisu je možno dle stávající právní úpravy použít jeden z následujících algoritmů. Jelikož elektronický podpis je aplikací asymetrického šifrování, může nám tento výběr posloužit stejně jako kterýkoliv jiný, ovšem s tím, že se nejedná o úplný výčet dostupných algoritmů.

1. RSA
2. DSA
3. ECDSA – F_p
4. ECDSA – F_m^2
5. ECGDSA – F_p
6. ECGDSA – F_m^2

4.6.1 RSA

Název RSA je odvozen od počátečních písmen jmen Ronald Rivest, Adi Shamir a Leonard Aleman, kteří tento systém v roce 1977 navrhli.

RSA algoritmus počítá s dvěma velkými prvočíslly p a q . Vynásobením těchto prvočísel čísel (viz rovnice 4.2) získáme číslo n , kterému říkáme modul.

$$n = p \cdot q \tag{4.2}$$

Zvolíme takové číslo e , které je menší než n a s matematicky příbuznými čísly našim prvočíslům p , q , tedy $(p-1)(q-1)$ nemá společného dělitele vyjma čísla 1. Mějme číslo d , takové aby $(ed-1)$ bylo dělitelné $(p-1)(q-1)$. Hodnoty e a d nazveme *veřejné* a *soukromé exponenty*.

Veřejný klíč potom tvoří čísla $(n; e)$, zatímco *privátní klíč* je tvořen čísly $(n; d)$.

Matematickému postupu, kterým lze získat čísla p a q z n se říká *faktorizace*. Bezpečnost RSA je založena na předpokladu, že při současném stavu lidského vědění, je faktorizace nesmírně obtížná a pro dostatečně velké čísla p a q je reálně nemožné ji provést.

Postup šifrování

Mějme dva subjekty Alici a Boba, kteří spolu chtějí komunikovat. Alice chce poslat Bobovi zprávu m . Alice proto zprávu m zašifruje do zašifrované podoby c , tak že $c = m^e \bmod(n)$, kde e a n jsou získány z Bobova veřejného klíče.

Bob, aby získal původní zprávu m , musí provést inverzní operaci $m = c^d \bmod(n)$, kde číslo d Bob získá ze svého privátního klíče.

Analogicky k tomuto postupu se provádí elektronické podepisování dokumentu. K podepsání ale nepoužijeme veřejný klíč adresáta, ale svůj soukromý klíč. Taková zpráva je dešifrovatelná pouze veřejným klíčem odesílatele.

V našem příkladě by to vypadalo následovně:

Alice podepíše dokument $c = m^d \bmod(n)$ (d a n Alice získá ze svého soukromého klíče).

Bob získá zprávu tak, že $m = c^e \bmod(n)$ (e a n Bob získá z veřejného klíče Alice).

Z hlediska bezpečnosti je tedy klíčové volba prvočísel p a q . Bylo dokázáno, že pokud délka (počet cifer) p je podstatně menší než délka q (viz 4.3), je proces faktorizace výrazně jednodušší.

$$l(p) \ll l(q) \quad (4.3)$$

Z toho důvodu je nutné zajistit, aby obě prvočísla si svou délkou přibližně odpovídala - rozdíl v délce by neměl přesáhnout 20 cifer, viz 4.4.

$$0, 1 < |l(p) - l(q)| \leq 20 \quad (4.4)$$

Je také známo, že pokud absolutní hodnota rozdílu prvočísel p a q je menší než čtvrtá odmocnina jejich součinu n (viz 4.5), existují metody pro snadnou faktorizaci (v tomto případě se jedná o Coppersmithovu metodu).

$$|p - q| < \sqrt[4]{n} \quad (4.5)$$

4.6.2 DSA

NIST publikoval algoritmus pro elektronický podpis (**Digital Signature Algorithm (DSA)**) jako součást standardu pro elektronický podpis [36] (**Digital Signature Standard (DSS)**). DSS byl vybrán NIST ve spolupráci s NSA jako standard pro digitální autentizaci pro vládní organizace USA. Tento standard byl přijat v roce 1994, s poslední verzí standardu z roku 2013.

DSS standard je zaměřen především na problematiku elektronického podpisu, algoritmy, které jsou v něm použity jsou ale využitelné i pro účely šifrování.

Parametry DSA:

1. $p \dots$ prvočíslo, kde $2^{L-1} < p < 2L$, kde L je násobkem 64.
2. $q \dots$ dělitel čísla $p - 1$, kde $2159 < q < 2160$
3. $g = h^{\frac{p-1}{q}} \bmod(p)$, kde h je jakékoliv celé číslo v intervalu $1 < h < p - 1$ takové aby $h^{\frac{p-1}{q}} \bmod(p) > 1$
4. $x, k \dots$ náhodně generované celé číslo v intervalu $0 < x, k < q$
5. $y = g^x \bmod(p)$

Čísla p, q a g mohou být veřejná a mohou dokonce být společná pro více uživatelů. Privátní klíč je x , veřejný y . Parametry x a k jsou využívány pouze pro vygenerování podpisu a musí být udržovány v tajnosti. Parametr k musí být vygenerován před každým podepsáním dokumentu.

Elektronický podpis s zprávou M se vygeneruje použitím rovnic:

$$r = (g^k \bmod(p)) \bmod(q) \quad (4.6)$$

$$s = (k^{-1}(SHA - 1(M) + xr)) \bmod(q) \quad (4.7)$$

Pro ověření pravosti podpisu se provede následující: Nechť M', r' a s' jsou čísla M, r, s , která obdržel adresát. Nejprve se provede kontrola r' a s' , zda $0 < r', s' < q$, v případě, že r' nebo s' podmínce nevyhoví, je podpis odmítnut. Samotný výpočet se provede pomocí rovnic:

$$w = s'^{-1} \bmod(q) \quad (4.8)$$

$$u_1 = ((SHA - 1(M'))w) \bmod(q) \quad (4.9)$$

$$u_2 = ((r')w) \bmod(q) \quad (4.10)$$

$$v = (((g)^{u_1} (y)^{u_2}) \bmod(p)) \bmod(q) \quad (4.11)$$

Pokud $v = r'$, potom je podpis ověřen.

4.6.3 ECDSA

Elliptic Curves Digital Signature Algorithm (ECDSA) znamená algoritmus elektronického podpisu založený na eliptických křivkách. Matematické základy navrhli pánové Victor Miller a Neal Koblitz někdy v polovině 80. let minulého století. Fungují analogicky ke zde již diskutovaným systémům veřejného klíče (například RSA).

Výhodou eliptických křivek je možnost jejich definice prakticky nad jakýmkoliv číselným oborem (reálných, přirozených, komplexních čísel). Eliptická křivka se skládá ze všech bodů v intervalu (x, y) které splňují podmínku (4.12):

$$y^2 = x^3 + ax + b \quad (4.12)$$

Bezpečnost algoritmů založených na eliptických křivkách je velmi podobná bezpečnosti algoritmu RSA – opět se vychází z tohoto, že faktorizace čísel je velmi obtížná. Pro úspěšné řešení algoritmu musíme vyřešit následující problém: *Mějme dva body G a Y na eliptické křivce jako je $Y = kG$, cílem je najít celočíselné k . Tento problém je často nazýván problémem diskrétního logaritmu eliptické křivky.*

Úvod do problematiky kryptografie založené na eliptických křivkách poskytuje článek [64].

V současné době výpočet obecného diskrétního logaritmu eliptické křivky je časově náročnější než například faktorizace, z tohoto důvodu jsou ECDS algoritmy srovnatelně bezpečné jako konvenční algoritmy elektronického podpisu zmiňované výše a to i s menší délkou klíče.

4.6.4 Požadavky na nastavení parametrů algoritmů asymetrického šifrování

Tato podkapitola obsahuje aktuální poznatky použitelné pro správné nastavení algoritmů asymetrického šifrování, což je základním předpokladem pro bezpečné použití algoritmů. Doporučení byla převzata z doporučení ENISA [62], viz tab 4.3.

Tabulka 4.3: Doporučení pro parametry asymetrických šifrovacích algoritmů (převzato z [62])

primitivum	parametry	min. legacy	min. nové
RSA problém	n, e, d	$l(n) \geq 1024$ $e \geq 3$ nebo 65537 $d \geq \sqrt{n}$	$l(n) \geq 3072$ $e \geq 3$ nebo 65537 $d \geq \sqrt{n}$
Finite Field DLP	p, q, n	$l(p^n) \geq 1024$ $l(p) > 160, l(q) > 160$	$l(p^n) \geq 3072$ $l(p) > 256, l(q) > 256$
ECDLP	p, q, n	$l(q) > 160$	$l(q) > 256$
Párování	p, q, n, d, k	$l(p^{k \cdot n}) \geq 1024$ $l(p) > 160, l(q) > 160$	$l(p^{k \cdot n}) \geq 3072$ $l(p) > 256, l(q) > 256$

4.7 Elektronický podpis v zákonech

Pravidla používání elektronického podpisu v České republice jsou upravena zákonem 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce [71], který nahrazuje do té doby platný zákon 227/2000 Sb. o elektronickém podpisu [32].



Změna legislativy 2016

Zákon o službách vytvářejících důvěru byl přijat v září 2016 a jeho přijetím odstartovalo dvouleté přechodné období, které by mělo umožnit plynulý přechod na nová technická řešení požadovaná legislativou. Z toho důvodu v následujícím textu budou rozebrány obě právní úpravy s vysvětleními rozdílů a důsledky.

Zákon v tomto systému definuje základní pojmy a postupy které souvisí s problematikou elektronického podpisu a jeho dalších aplikací např. časového razítka. Dalším úkolem zákona je zajištění hladké přeshraniční spolupráce tak, aby zaručený elektronický podpis (vydaný dle zákona) nebyl

platný pouze ve státu, který jej vydal. Pro účely interoperability se implementuje v podmínkách ČR Rozhodnutí Komise č. 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu [26].

Nová právní úprava je založena na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS) [17]. Už samotný název indikuje dva poměrně významné rozdíly. První je ve zvolené formě nařízení a druhé je v rozsahu řešené problematiky. Oproti původní právní úpravě je v tomto případě řešena i obecná problematika identifikace jedince nebo organizace a to v celém prostoru EU.



Nařízení EU vs směrnice EU

Směrnice EU [16] je závazná pro každý stát, kterému je určena, pokud jde o výsledek, jehož má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům. Prakticky se směrnice transponují ve stanoveném časovém období do právních řádů jednotlivých určených států EU formou, kterou daný stát pro daný účel zvolí, obvykle pomocí zákonů a vyhlášek.

Nařízení EU [16] má obecnou působnost, je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

Původní právní úprava pracuje s následujícími prostředky:

- elektronický podpis
- elektronická značka
- časové razítko

Nová právní úprava používá následující prostředky:

- elektronický podpis (ale odlišným způsobem zaručený)
- elektronická pečeť
- časové razítko (opět odlišným způsobem zaručené)
- elektronická identita
- webové certifikáty

Podívejme se nejprve na nové oblasti působnosti legislativy. Účelem právní úpravy používání *webových certifikátů* je pokus získat určitou kontrolu nad bezpečností webových služeb v technologiích jako je DNSSEC, protokolech https a dalších. Úprava problematiky webových certifikátů je zvláštní v tom, že je jednak nepovinná a jednak, že mezinárodní IT komunita toto nařízení více méně ignoruje. Přitom bez součinnosti s výrobcí operačních systémů, popř. výrobcí dalších softwarů jako jsou např. prohlížeče WWW není možno očekávat úspěch takové úpravy.

Účelem implementace *elektronické identity (eID)* je umožnit jednoznačně identifikovat všechny obyvatele EU bez ohledu na zemi původu. Nařízení eIDAS předpokládá postupné připojování jednotlivých členských států do tohoto systému. Vzájemné uznávání eID je v tomto případě budováno „zdola“ - tedy od jednotlivých členských států. Předpokládaný postup je následující:

1. členský stát vyvine za začlenění do svého právního řádu eID (národní eID např. formou elektronického občanského průkazu)
2. stát poskytne popis národního eID systému ostatním státům
3. stát oznámí národní systém eID Evropské komisi
4. systém eID bude zveřejněn v Úředním věstníku
5. vzájemné uznávání

Jak je z výše uvedeného postupu patrné, jedná se o dlouhodobý proces. Předpokládá se, že do fáze vzájemného uznávání se lze dostat do dvou let (od okamžiku schválení národního eID). Dvouleté období je však pouze odhadem, až čas ukáže zda a jak bude takové vzájemné uznávání fungovat.



eID - elektronický občanský průkaz (eOP)

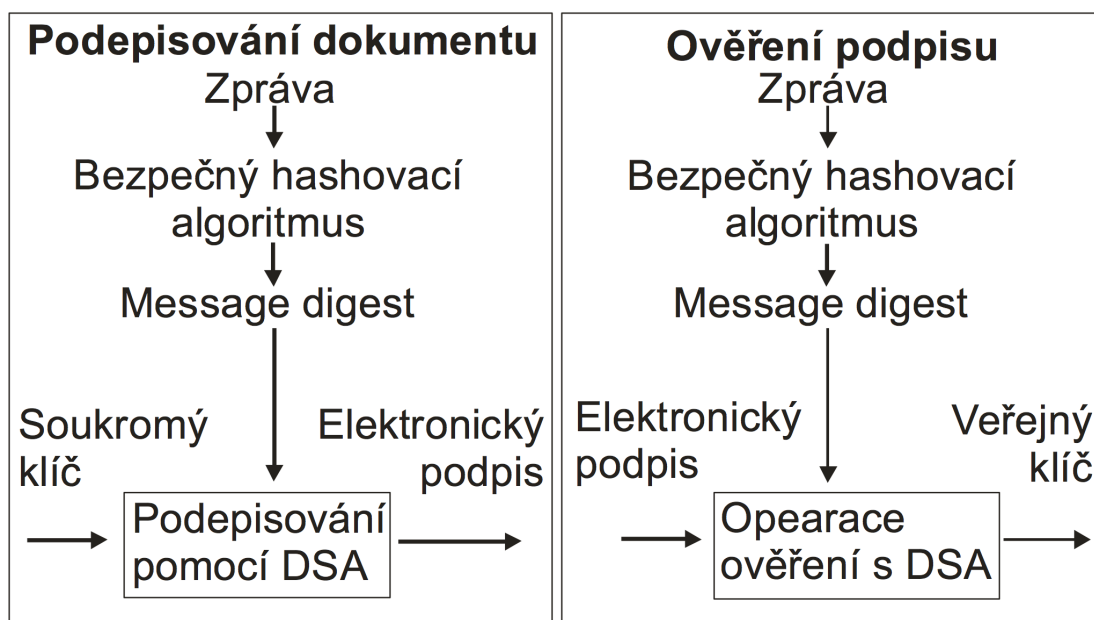
Problematika elektronické identity propojuje problematiku elektronického podpisu s problematikou e-governmentu (viz kapitola e-government). Již dnes je možno do eOP vybaveného kontaktním čipem nahrát osobní certifikát. Tuto službu poskytují oba hlavní poskytovatelé certifikačních služeb v ČR a to PostSugnum a První certifikační autorita.

Velmi důležitým pojmem, se kterým legislativa pracuje je *důvěra*. Znamená to, že cílem použití prostředků elektronického podpisu (a souvisejících prostředků) je dosažení určité úrovně důvěryhodnosti např. podepsané zprávy. Tuto důvěru lze pak využít např. pro zajištění vymahatelnosti podepsaných dokumentů apod.

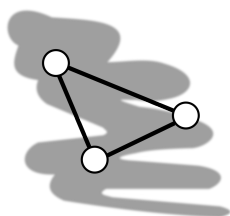
Úroveň důvěry je možno rozdělit do tří stupňů zajištěné odlišnými technickými prostředky:

1. *nízká úroveň* - tuto úroveň poskytují prostředky s omezenou mírou spolehlivosti ověření totožnosti, pro tuto úroveň je požadována minimálně jednofaktorová autentizace.
2. *značná úroveň* - tuto úroveň poskytují prostředky poskytující značnou míru spolehlivosti, pro tuto úroveň je požadována minimálně dvoufaktorová autentizace.
3. *vysoká úroveň* - prostředky nabízí vyšší míru spolehlivosti při ověřování totožnosti, pro tuto úroveň je požadováno využití takových prostředků, které chrání pro vyhotovení duplikátů a neoprávněné manipulaci.

Ve výše uvedeném seznamu se objevuje několikrát pojem *autentizace*, se kterým jsme se dosud nesetkali. Autentizací rozumíme proces, kterým uživatel prokazuje totožnost systému. Z předchozí kapitoly už víme jak technicky funguje elektronický podpis (podepisování např. dokumentu) i ověření tohoto podpisu. Pro připomenutí můžeme celý postup schématicky znázornit jako na obr. 4.4.



Obrázek 4.4: Využití hashovacích funkcí při elektronickém podepisování dokumentů



Bezpečné hashovací funkce

U elektronického podpisu se obvykle podepisuje pouze otisk (hash) zprávy, nikoliv zpráva celá. Jedním z důvodů je vysoká výpočetní náročnost celého procesu. Podrobnější informace o těchto funkcích můžete získat v kapitole *Bezpečné hashovací funkce* v těchto skriptech.

V předchozí kapitole nebyla řešena jedna velmi důležitá otázka: *jak zaručit, že veřejný klíč přináleží určité konkrétní osobě?*

K takovému ověření je potřeba nezávislá třetí strana, které budou ověřit jak podepisující, tak ověřující strana. Takovou úlohu hraje **Poskytovatel Certifikačních Služeb (PCS)**. V případě, že elektronicky podepsané dokumenty mají být právně závazné, je potřeba, aby tento PCS splňoval určitá bezpečnostní kritéria stanovená technickými normami. Nároky jsou kladeny na PCS také z pohledu např. archivace dokumentů apod.

Proces samotného vystavování elektronického podpisu funguje tak, že zájemce fyzicky navštíví PCS, který ověří jeho totožnost a vydá certifikát. Certifikát obsahuje data nutná ověření totožnosti

uživatele. Zároveň obsahuje také data, která umožňují elektronický podpis vytvářet (privátní klíč). Za správnost těchto dat PCS ručí a je také povinen zveřejňovat pravidelně seznamy vydaných certifikátů. Platnost certifikátu je časově omezena, obvykle na řádově měsíce až jeden rok. Kvalifikované certifikáty s delší dobou platnosti se obvykle nevydávají.

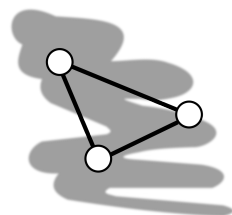
Vzhledem k vážným důsledkům, které může mít odcizení identity, což je mimochodem zločin, který se běžně stává všech vyspělých zemích a proto také u nás, jsou kladeny relativně vysoké požadavky na bezpečnost informačních systémů PCS.

Vraťme se zpět k autentizaci. Jsme v situaci, kdy si uživatel pořídil certifikát od PCS. Privátní klíč z něj pak udržuje v tajnosti a může jej použít pro podepisování dokumentů. Pokud privátní klíč není žádným dalším způsobem chráněn, pak identita uživatele je prokazována prostým vlastnictvím tohoto privátního klíče. Identita uživatele je tedy prokázána pouze jedním prostředkem - odtud označení *jednofaktorová autentizace*.

Dvoufaktorová autentizace používá dva způsoby ověření totožnosti uživatele. První je stejný, jako v předchozím případě, tedy privátní klíč. Tento klíč je však navíc sám chráněn zašifrováním. K použití tedy nestačí pouze vlastnictví privátního klíče, ale také znalost klíče jímž se dešifruje.

U značné i vysoké míry důvěry se předpokládá použití dvoufaktorové autentizace. Rozdíl mezi nimi je však v tom, že vysoká úroveň vyžaduje použití technického prostředku, jako jsou tokeny nebo bezpečnostní karty, které samy o sobě splňují jisté bezpečnostní požadavky stanovené normami.

Příkladem takového zařízení je TokenME italské společnosti Bit4id, který nabízí v ČR certifikační autorita PostSignum. Tento produkt prošel certifikací podle standardu Common Criteria na úroveň EAL4+ (Evaluation Assurance Level) [4] a splňuje požadavky na kryptografické moduly podle FIPS 140-2 [57].



Autentizace

Podrobnější informace o problematice *autentizace* můžete získat v předmětu *Počítačové sítě a ochrana dat*, který si můžete zvolit pro studium v třetím ročníku.

Elektronický podpis

Pro různé typy elektronických podpisů jsou vyžadovány různé stupně zabezpečení. Z tohoto pohledu můžeme rozdělit elektronické podpisy na čtyři typy (se stupňující se úrovní důvěryhodnosti):

1. prostý elektronický podpis (elektronický podpis bez přívlastku)
2. zaručený elektronický podpis (**Advanced Electronic Signature (AdES)**)
3. zaručený elektronický podpis, založený na kvalifikovaném certifikátu
4. kvalifikovaný elektronický podpis (**Qualified Electronic Signature (QES)**)

Elektronický podpis dle eIDAS mohou vytvářet jen a pouze fyzické osoby. Elektronický podpis je brán jako projev vůle podepisující osoby vůči podepisovanému dokumentu. Jedná se tedy o filozoficky stejný přístup jako v případě podepisování „papírových“ dokumentů.

Nejnižší úroveň zabezpečení, resp. žádnou úroveň zabezpečení poskytuje *prostý elektronický podpis*. Jako elektronický podpis slouží jakékoliv údaje připojené k podepisovanému dokumentu a používané jako podpis. Může se jednat např. o patičku emailu.



Prostý elektronický podpis jako patička e-mailu

... tělo e-mailu ...

S pozdravem

Pavel Šenovský

Katedra ochrany obyvatelstva

Fakulta bezpečnostního inženýrství

VŠB - Technická univerzita Ostrava

Podobným způsobem může být použit naskenovaný běžný podpis přiložený k dokumentu. V obou případech není splněn ani jeden stupeň úrovně důvěry, které byly uvedeny výše. Jinými slovy nikomu nic nebrání aby vytvořil libovolný dokument a tento typ podpisu k němu připojil. Tímto způsobem

podepsaný dokument proto ze své podstaty nemůže být natolik důvěryhodný, aby byl závazný (např. z hlediska vymahatelnosti takto podepsaných smluv).

Na druhou stranu prostý elektronický podpis používáme každý den, v rámci e-mailů, příspěvků na sociálních sítích apod., abychom se identifikovali - a k tomuto účelu prostý elektronický podpis plně postačuje.

Zaručený elektronický podpis pro operaci podepisování používá kryptografické algoritmy. Na certifikát, pomocí kterého se operace podepisování provádí, ale nejsou kladeny žádné nároky. Takový certifikát tedy může být vygenerován jakkoliv, můžeme si jej vygenerovat také sami pomocí nástrojů jako je PGP [22] nebo OpenSSL [23].

Jelikož jsou používány kryptografické algoritmy, je podpis samotný lépe zabezpečen. Problémem v tomto případě je ověření totožnosti podepisující osoby - pokud si podepisující osoba sama může vystavit certifikát (nebyly využity služby kvalifikovaného PCS), je tento způsob podpisu bezpečnější než podpis prostý? Odpověď zní ano i ne. Pro podepsání obchodní smlouvy tento druh elektronického podpisu nevytváří dostatečně silnou důvěru. Pokud ale tento druh podpisu použijeme uvnitř firmy a oddělení IT bude vykonávat služby PCS, ale nikoliv na takové úrovni aby jej bylo možné považovat za kvalifikovaného PCS, může být relativně levně dosažena vyšší úroveň důvěry podepisovaných vnitřní dokumentů organizace.

Zaručený elektronický podpis, založený na kvalifikovaném certifikátu se liší od předchozího případu využitím služeb kvalifikovaného PCS pro vytvoření certifikátu. Za totožnost podepisující osoby tedy ručí nezávislá třetí strana (nezávislá na podepisující osobě i osobě, která provádí ověření podpisu). Důvěryhodnost kvalifikovaného PCS je zajištěna kontrolou souladu způsobu fungování PCS s legislativou i relevantními technickými normami.

Prostředek použitý pro podepisování může být ale libovolný. Není zde tedy požadavek na to, aby certifikát byl bezpečně uložen na certifikovaném tokenu nebo obdobném zařízení. Tento typ elektronického podpisu je plně v souladu s požadavky dnes již zrušeného zákona o elektronickém podpisu. Úroveň důvěry v tomto případě je z pohledu legislativy po dobu trvání přechodného období (do září 2018) stejná jako u nejvyšší formy elektronického podpisu - *kvalifikovaného elektronického podpisu*.

Kvalifikovaný elektronický podpis je naopak standardem pro zajištění nejvyšší úrovně důvěry podle nařízení eIDAS. Pro dosažení této úrovně je nutné použití kvalifikovaného prostředku (např. tokenu). Po uplynutí přechodného období bude tento druh elektronického podpisu jako jediný použitelný pro oficiální komunikaci s úřady, popř. jiné úkony vyžadující vysoký stupeň důvěryhodnosti.

S pojmem elektronický podpis souvisí celá řada dalších pojmů.

Elektronická značka

Prvním z nich je tzv. *elektronická značka*. Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojeny k datové zprávě a:

1. jsou jednoznačně spojené s označující osobou a umožní její identifikaci pomocí certifikátu
2. byly vytvořeny pomocí nástrojů pro vytváření elektronických značek, které označující osoba může mít pod svou výhradní kontrolou.
3. jsou připojeny takovým způsobem, který umožní odhalit jakoukoliv následnou změnu zprávy

Naskýtá se otázka, čím se vlastně liší elektronický podpis od elektronické značky. Podle zákona se má za to, že před podpisem se podepisující osoba s dokumentem seznámila a podpisem se tak zaručuje za správnost údajů v dokumentu obsažených. Elektronický podpis je tedy chápán jako projev vůle fyzické osoby vůči podepisovanému dokumentu.

V případě elektronické značky se ale má za to, že zpráva byla označena bez předchozí kontroly obsahu zprávy - tedy něco podobného jako parafa v případě papírových dokumentů. Elektronickou značku obvykle používají automatizované systémy. Např. ji může použít **IS** pro do něj nahraný dokument, aby bylo možné zaručit, že dokument prošel daným systémem.

Z technického pohledu se používají pro označování dokumentů stejné algoritmy jako v případě elektronického podpisu. Rozdíl je zde tedy v právním důsledku akce označení dokumentu.

Elektronickou značku zavedl do ČR zákon o elektronickém podpisu a **nemá obdobu v nařízení eIDAS**. To znamená, že po uplynutí přechodného období nebude možné používat se stejnými právními důsledky jako dosud. Dopady jsou dnes ne úplně jasné. Elektronické značky se v současnosti využívají extenzivně v Informačním systému datových schránek (**Informační systém datových schránek (ISDS)**).

Elektronická pečeť

Elektronická pečeť je novým nástrojem zavedeným nařízením eIDAS. Elektronickou pečetí se opět rozumí údaje připojené k dokumentu (datové zprávě), které:

1. jsou jednoznačně spojeny s „pečetící“ organizací
2. byly vytvořeny pomocí nástrojů pro vytváření elektronických pečetí, které má pečetící organizace výhradně pod svou kontrolou
3. jsou připojeny takovým způsobem, který umožní odhalit jakoukoliv následnou změnu zprávy

Elektronickou pečeť mohou využívat pouze právnické osoby (včetně organizačních složek státu). Podobně jako v případě elektronické značky i v případě elektronické pečetí je odlišný význam. Elektronická pečeť není chápána jako projev vůle, ale pouze jako specifikace původu zapečetěného dokumentu.

Elektronickou pečeť tedy organizace mohou dávat pouze na dokumenty, kterých jsou původci.

I tento posun je logický, pokud jej srovnáme s filozofií použití běžného podpisu. I v případě podepisování smluv mezi dvěma právnickými osobami akt podpisu je vykonáván fyzickou osobou, která je k tomuto úkonu zmocněna - např. statutární zástupce nebo jím zmocněná osoba.

Z technického pohledu se používají pro zapečetění dokumentů stejné algoritmy jako v případě elektronického podpisu. Rozdíl je zde tedy v právním důsledku akce zapečetění dokumentu.

Časová razítka

Kvalifikovaným *časovým razítkem* se rozumí údaje připojené k datové zprávě vydaná poskytovatelem certifikačních služeb, která spojuje zprávu s určitým časovým okamžikem.

Časové razítko je velmi důležité například pro uzavírání smluv. Smlouvu uzavíráme k určitému datu. Použití elektronických prostředků by mohlo svádět k antidatování takových smluv (nebo jiných dokumentů). Z tohoto důvodu musí časové razítko vydávat poskytovatel certifikačních služeb, protože je nezávislý vůči podepisujícím stranám a je pod velmi přísnou kontrolou.

Poskytovatel musí ze zákona zajistit, aby čas odpovídal hodnotě koordinovaného světového času. Časové razítko si potom můžeme představit podobně jako například rádiové budíky, které se v pravidelných intervalech zachycují signál z vysílače přesného času a podle něho nastaví čas.

Velmi často je výhodné použít kombinaci časového razítka a elektronického podpisu. Použití může být např. ve formě elektronického podepsání dokumentu a aplikaci časového razítka. Tímto způsobem se dokument včetně elektronického podpisu spojí s určitým časem a je možno zkoumat, zda v té době podpis byl platný. Tedy zdali k času a datu „oražení“ dokumentu certifikát použitý k podpisu neexpiroval (neskončila jeho platnost) nebo nebyl předčasně revokován. Revokaci certifikátu lze ověřit proti seznamu revokovaných certifikátů.

Opačný postup než v předchozím případě - tedy dokument opatřit časovým razítkem a teprve následně elektronicky podepsat je také možný. Interpretace je ale rozdílná. Časová značka spojí dokument s určitým okamžikem, podepisující osoba pak získává jistotu, že podepisuje např. aktuální verzi dokumentu. Pozor v tomto případě ale časové razítko nevypovídá nic o času aktu podepsání.

Pokud jste dočetli až sem, pak Vás nepřekvapí, že pro časovou značku technicky je použit algoritmus elektronického podpisu. Ovšem s tím časovému označení se použije privátní klíč PCS a ověření pak proběhne proti jeho veřejnému klíči.

Podpisová schémata

Z předchozího textu již víme, že existuje celá řada prostředků a algoritmů, které lze elektronický podpis a obdobné služby použít. U kvalifikovaných PCS je ale jejich použití z hlediska algoritmů a jejich parametrů omezeno, aby byla zaručena dlouhodobá bezpečnost aplikací této technologie.

Kombinaci algoritmů použitelné pro elektronické podepisování a obdobné služby označujeme jako *podpisové schéma*. Schéma samotné je tvořeno:

- algoritmem elektronického podpisu,
- bezpečnou hashovací funkcí a
- paddingovou funkcí.

Algoritmy elektronického podpisu jsme se již zabývali, hashovacími funkcemi se budeme zabývat v samostatné kapitole, zbývá tedy *paddingová funkce*. Paddingové funkce zajišťují služby tzv. paddingu, tedy doplnění zprávy na určitou délku. Důvodem pro použití takových funkcí jsou blokové charakteristiky ostatních funkcí podpisového schématu. To znamená, že tyto funkce vyžadují pro svou práci, aby zpráva, kterou mají zpracovat, byla beze zbytku dělitelná na bloky o určité délce.

Jelikož délka zprávy může být různá je tento požadavek zajištěn použitím paddingové funkce, která „chybějící“ část bloku doplní.

Doporučená podpisová schémata jsou obsažena v tabulce 4.4.

Tabulka 4.4: Doporučená podpisová schémata dle [34]

Podpisové schéma	SHA	Paddingová funkce	DSA
SHA224-s-RSA	SHA224	Pozn.	RSA
SHA256-s-RSA	SHA256	Pozn.	RSA
RSA-PSS s MGF1SHA1 ident.		MGF1SHA1	RSA
RSA-PSS s MGF1SHA224 ident.		MGF1SHA224	RSA
RSA-PSS s MGF1SHA256 ident.		MGF1SHA256	RSA
SHA224-s-ECDSA	SHA224	-	ECDSA-Fp nebo ECDSA-F2m
SHA256-s-ECDSA	SHA256	-	ECDSA-Fp nebo ECDSA-F2m
SHA384-s-ECDSA	SHA384	-	ECDSA-Fp nebo ECDSA-F2m
SHA512-s-ECDSA	SHA512	-	ECDSA-Fp nebo ECDSA-F2m

Pozn.: Měla by být vybrána paddingové funkce pro algoritmus elektronického podpisu RSA:

1. emsa-pkcs1-v1.5
2. emsa-pkcs1-v2.1
3. emsa-pss
4. iso9796ds2
5. iso9796-din-rn
6. iso9796ds3

Pro jednotlivé algoritmy se přitom předpokládá časově omezená použitelnost pro vystavování certifikátů. Nejexponovanějším algoritmem z tohoto pohledu je algoritmus bezpečné hašovací funkce. Použitelnost definuje norma ETSI TS 102 176-1 [34] a znázorňuje ji také tabulka 4.5.

Tabulka 4.5: Použitelnost SHA algoritmů dle [34]

SHA funkce	1 rok	3 roky	6 let	10 let (odhad)
SHA 1	X	X	X	X
RIPEMD-160	X	X	X	X
SHA-224	O	O	O	?
SHA-256	O	O	O	?
SHA-384	O	O	O	O
SHA-512	O	O	O	O
Whirpool	O	O	O	O

Pozn.: O = použitelné, ? = neznámo, X = nepoužitelné

Časový údaj v letech je počítán od data vydání normy ETSI TS 102 176-1 V2.1.1 [34], tedy od roku 2011. Tyto číselné údaje jsou spíše orientačního charakteru a slouží jako vodítko PCS pro volbu optimálního preferovaného podpisového schématu podle doby platnosti vydaného certifikátu.

Lze tedy říci, že pro účely elektronického podepisování není možné použít bezpečné hashovací funkce SHA 1 a RIPEMD-160. Dlouhodobá bezpečnost „krátkých“ SHA třídy 2 (SHA-224 a SHA-256) je v současnosti nejistá a doporučuje se spíše použití SHA-512, tam kde je to možné.

Elektronické archívy

Elektronický podpis dle eIDAS je platný (ověřitelný) po dobu trvání platnosti certifikátu použitého pro podepsání dokumentu. Obvykle je tato doba relativně krátká - do jednoho roku. Po jejím uplynutí elektronický podpis není možno ověřit. V některých případech je ale žádoucí, aby schopnost ověření trvala déle. Jedná se zejména o případy systémů, které slouží pro dlouhodobou archivaci dokumentů.

Podpis/značka v takovém případě slouží mimo jiné také k ověření toho, že archivovaný dokument nebyl pozměněn nebo poškozen. Ke změnám může dojít úmyslně nebo prostou lidskou chybou, k

poškození pak může dojít třeba také v důsledku technického selhání, např. poškození sektoru na disku, v jehož důsledku nelze část dokumentu přečíst.

Elektronické archívy jsou proto z mnoha pohledů velmi specifické. Problematika vedení elektronických archívů není nová a existují technická řešení. Například **National Aeronautics and Space Administration (NASA)** se zabývá problematikou elektronického archivnictví někdy od roku 1966. Je také zakládajícím členem **Consultative Committee for Space Data Systems (CCSDS)** (založen 1982). Tato organizace se zabývá přijímáním standardů souvisejících s výzkumem vesmíru. Jeden z těchto standardů, konkrétně CCSDS 650.0-M-2: Reference Model for an **Open Archival Information System (OAIS)** [2], také označovaný jako magenta book¹, se zabývá právě problematikou archivací dokumentů a také archivnictvím obecně.

Tento standard byl také v roce 2003 vydán jako ISO 14721:2003 [10]. Cílem je navrhnout systém archivace dat jak v elektronické podobě, tak v podobě „papírové“, tak aby data byla přístupná cílové skupině uživatelů. K dosažení tohoto cíle vymezuje i organizační schémata jako souhrn lidí a pravidel pro archivaci odpovědnost a proces poskytování dat z archívu.

Jedná se tedy spíše o stanovení filozofie archivování než konkrétní návod se stanovením technologií k použití. Finální aplikace musí přitom mít funkce archívu a zároveň používat transparentní metody elektronického podepisování s dlouhodobou platností (např. podle ETSI TS 101 733 [7]). Zajištění právní vymahatelnosti dokumentů nebude možné bez dalších legislativních změn, které se však v současné době nepřipravují.



Zapamatujte si

Je třeba si uvědomit možnosti elektronického podpisu a způsobu jakým je jeho použití upraveno zákonem. V zásadě totiž existují dva druhy elektronického podpisu - takový, který je oficiální, lze ho použít pro komunikaci s úřady, podepisování smluv tedy splňující požadavky zákona. Pro certifikační autoritu zavádí zákon přívlástek *kvalifikovaná*.

Potom existují certifikační autority, které používají stejné nebo podobné algoritmy elektronického podpisu, nicméně se nesnaží splnit všechny požadavky zákona a prováděcích vyhlášek. Takový elektronický podpis samozřejmě není z právního hlediska použitelný např. pro uzavírání smluv, ale lze jej výhodně využít například v rámci podniků pro zvýšení bezpečnosti komunikace jeho zaměstnanců.

4.8 Bezpečné hašovací algoritmy

Hašovací funkce slouží k vytváření tzv. **Message Digest (MD)** jednotlivých souborů. Jedná se o matematické, jednosměrné funkce jejichž výsledkem je řetězec, unikátní pro každou zpracovávanou zprávu. Cílem je získat možnost ověřit, že zpráva, jejíž MD vlastněme, nebyla pozměněna. Message digest tedy můžeme přeneseně považovat za otisk prstu zprávy.

Samotný proces ověřování se provádí jednoduše tak, že se ze zprávy vygeneruje nový MD a ten je srovnán s MD původní.

Svou koncepcí vychází ze starších algoritmů pro vytváření kontrolních součtů (**CRC**). Problémem těchto algoritmů byla možnost jejich snadného falšování. Moderní hašovací funkce proto využívají metod šifrování. Možnost objevení dvou zpráv, které mají stejný MD samozřejmě nelze úplně vyloučit, u bezpečného algoritmu je však krajně nepravděpodobné. Možnosti vytvoření dvou zpráv mající totožný haš nazýváme *kolize*.

Bezpečnost hašovací funkce se definuje jako počet průchodů algoritmem (pokusů), které jsou nutné provést pro získání dvou zpráv se stejným MD. Bezpečnost je tedy odvozena od počtu operací, které je nutno provést pro prolomení bezpečnosti a získání kolizní zprávy. Tuto bezpečnost, někdy označovanou taktéž jako tzv. *bits of security*, vypočteme takto (4.13):

$$p = 2^{\frac{m}{2}} \quad (4.13)$$

kde p maximální počet výpočtů MD pro nalezení zprávy mající hledaný MD m délka výsledného hashe (MD) v bitech

¹označení je odvozeno z barvy přebalu normy

Bezpečnost hašovacích algoritmů zkoumáme z dvojího pohledu:

1. z pohledu hledání dvou libovolných různých zpráv, které mají stejný haš,
2. z pohledu hledání zprávy s konkrétním hašem.

Rozdíl mezi těmito dvěma přístupy je jasně viditelný na tzv. narozeninovém paradoxu. **Narozeninový paradox** říká [38]: *pokud je v místnosti 23 nebo více lidí, je více než padesátiprocentní šance, že nejméně dva z nich mají narozeniny ve stejný den.* Ve skutečnosti se nejedná o logický paradox, protože toto tvrzení je velmi lehce odvoditelné, spíše se jedná o paradox z pohledu prvotní úvahy většiny lidí, kteří se nad tímto problémem zamyslí.

Vysvětlení můžeme nalézt uvažováním inverzního problému - tedy, že žádný z přítomných lidí nemá narozeniny ve stejný den jako jiný (viz 4.14).

$$p'(n) = 1 \left(1 - \frac{1}{365}\right) \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) \quad (4.14)$$

kde n počet lidí v místnosti

Pravděpodobnost, že se v místnosti nacházejí dva lidé se stejným dnem narozenin (4.15)

$$p(n) = 1 - p'(n) \quad (4.15)$$

Pokud tedy hledáme dvě libovolné zprávy, které mají stejný haš, tak je to podobně jako pro hledání dvou libovolných lidí s narozeninami ve stejný den nesrovnatelně jednodušší než hledání zprávy, která má jeden konkrétní haš (člověka který se narodil v určité datum).

Bezpečnost hašovacího algoritmu je proto přímo odvislá od délky výsledného haše, tak jak stanovuje rovnice 4.13. Velikost haše nám stanovuje prostor, který je nutné prohledat, abychom narušili bezpečnost daného algoritmu.

Díky těmto vlastnostem si tyto algoritmy našly uplatnění v řadě oblastí:

1. ověření že během stahování souboru z Internetu nedošlo k chybě – uživatel si stáhne MD, vypočte MD staženého souboru a obě MD porovná
2. jako náhrada za heslo – do databází a souborů se neukládá heslo v čitelné ani zašifrované podobě, ale jeho MD. Po zadání hesla uživatelem se vypočte MD a porovná se s MD uloženým.
3. Součást elektronického podpisu – umožňuje zjistit, dokument opatřený elektronickým podpisem nebyl nijak změněn

V současné době existuje řada algoritmů, které se pro generování MD využívají, a některé z nich tady představím podrobněji. Bude se jednat především o algoritmy MD2, MD4 a MD5 vyvinuté firmou RSA a SHA-1 vyvinuté na MIT. Česká vyhláška pro použití elektronického podpisu také umožňuje využití algoritmu RIPEMD-160 autorů Hanse Dobbertina, Antoona Bosselaerse a Barta Preneela. Tyto algoritmy se liší jednak délkou generovaného MD (čím větší tím bezpečnější) i použitím různých technik ochrany.

Hašovací algoritmy MD2 – MD5, stejně jako SHA-1 byly přijaty organizací IETF jako RFC doporučení defacto standardy pro celosvětovou síť internet. První dokument RFC se objevil v roce 1969. Tehdy RFC dokumenty plnily funkci diskusní platformy rostoucí komunity kolem sítě **Advanced Research Projects Agency Network (ARPANET)** (předchůdce Internetu) o síťových protokolech a technologiích na ARPANET použitých.

4.8.1 MD2 - 5

MD algoritmy mají společné to, že upraví vstupní zprávu na určitou délku, pro kterou je v několika „kolech“ vypočítán MD. Výsledkem, je řetězec pevné délky, která je určena použitým algoritmem.

Zpracování tedy probíhá v pěti krocích:

1. doplnění zprávy na normalizovanou délku,
2. doplnění kontrolního součtu zprávy,
3. iniciace bufferu na počáteční hodnotu,
4. zpracování zprávy a
5. zaznamenání výsledku.

Z hlediska moderního návrhu hašovacích funkcí je přelomová MD4, která posloužila jako základ návrhu SHA-1 i RIPEMD. Novátorským principem je zde tzv. více-kolový systém. Na každý blok

zprávy se použije několik předem definovaných funkcí. Tímto způsobem se autoři celého algoritmu snažili znesnadnit statistickou analýzu výsledku těchto funkcí a tedy zabránění nalezení jiné zprávy mající stejně MD bez nutnosti provést p-výpočtů.

Závěry výzkumů z poslední doby ukazují, že délka haše 128 bitů, kterou využívají algoritmy MD2 – MD5 již nelze považovat za zcela bezpečné. Již v roce 1994 pánové Paul van Oorschot a Mike Wiener dokázali [59], že při investici 10 miliónů dolarů je možné sestavit počítač, který mohl dvě zprávy se stejným MD najít během měsíce. Přitom autoři očekávali, že náklady by se každých 18 měsíců snížily na polovinu.

Už v roce 1995 se ale ukázalo, že taková investice nebude vůbec nutná, protože algoritmus samotný obsahuje závažné zranitelnosti, které proces útoku výrazně zjednodušují a tím pádem také zrychlují. Tento útok zpracoval a také posléze publikoval německý kryptoanalytik Hans Dobbertin [48] napadl všechny tři kola zpracování MD4. Na běžném PC by útok na MD4 trval řádově několik sekund. MD4 se ovšem v době publikování už nepoužívalo - neboť o bezpečnosti tohoto algoritmu měly určité pochybnosti samotní autoři algoritmu, proto jej záhy nahradili o něco pomalejší, ale také výrazně bezpečnějším algoritmem MD5.

V roce 1996 Dobbertin publikoval úvahy o možném řešení MD5 aplikací stejných postupů, které použil pro prolomení MD4. Myšlenky Dobbertina, Orschota a Wiesnera dále rozvedli Číňané Xiaoyun Wang, Dengguo Feng and Xuejia Lai a Hongbo Yu [69] prokázali, že MD5 je skutečně nebezpečné a je možné najít během několika hodin dvě zprávy se stejným hashem. Proti způsobu, jakým autoři MD5 napadli nejsou imunní ani další hashovací funkce jako je SHA-0, RIPEMD a HAVAL-128.

Počátkem roku 2006 přispěl k řešení této problematiky i Vlastimil Klíma [53], který čínský útok dále urychlil až pod jednu minutu na průměrném testovacím notebooku.

4.8.2 SHA

Definován ve standardu **NIST FIPS 180-4 Secure Hash Standard (SHS)** [35]. Tento standard specifikuje hašovací algoritmy pro SHA-1, SHA-256, SHA-384 a SHA-512.

Standard 180-4 [35] byl sice aktualizován v roce 2012, jednalo se však o změny spíše kosmetické. Největší změny zavedl FIPS 180-2, který umožnil používat SHA třídy 2, které zahrnují algoritmy SHA-256, SHA-384 a SHA-512), zatímco původní norma umožňovala použití pouze algoritmu SHA-1.

Oproti srovnatelnému algoritmu MD5 je délka výsledného haše 160 bitů u SHA-1 a u ostatních algoritmů SHA ještě delší, z tohoto hlediska je tedy algoritmus SHA bezpečnější. Je však potřeba dodat, že všechny v současnosti normalizované algoritmy SHA filozoficky vycházejí z MD4, proto všechny také do určité míry trpí jejími neduhy, které činí z jejich bezpečnosti spornou otázku. Z tohoto důvodu také NIST ve spolupráci s NSA vypsal soutěž na SHA třídy 3, jejichž algoritmus by měl být razantně odlišný a algoritmus by tak neměl být zranitelný stejným typem útoků jako starší SHA algoritmy. Tuto soutěž vyhrál algoritmus *Keccak* a v roce 2015 byl tento algoritmus zveřejněn jako součást standardu FIPS PUB 202 [58]. V současnosti (počátek roku 2017) však SHA-3 není v praxi téměř používán.

Všechny stávající algoritmy lze rozdělit do dvou etap *preprocessing* a *výpočet haše*. V rámci preprocessingu se připravuje zpráva podobným způsobem jako u algoritmů MD (doplnění zprávy, iniciace počátečních nastavení). Při výpočtu haše se vytvoří message shedule a ten je pak použit spolu s funkcí, konstantami a operacemi s textovými bloky k iteračnímu vygenerování série haš hodnot.

Algoritmy jsou iterační, jednocestné hašovací funkce, které zpracují zprávu a vytvoří její MD. Algoritmy se přitom liší počtem bitů (bits of security), dále se liší délkou zpracovávaných textových bloků, které jsou užity v procesu hašování.

Aplikací čínského útoku (viz. část věnována funkcím MD) došlo zatím k zmenšení složitosti útoku na algoritmus SHA-1 ze 2^{80} na 2^{69} , v roce 2015 pak pak komplexita útoku poklesla na $2^{57,5}$ [63]. Z kryptografického pohledu je tedy SHA-1 prolomena a proto se použití tohoto algoritmu nedoporučuje. Algoritmus SHA-1 již byl také vyřazen z doporučených bezpečných hashovacích funkcí používaných v rámci podpisových schémat kvalifikovaných PCS. V průběhu let 2016 a 2017 také přestane většina WWW prohlížečů označovat webová sídla podepsaná certifikátem založeným na tomto algoritmu jako bezpečná.

Řešením je přechod na SHA třídy 2 (SHA-256 a vyšší), zejména pak SHA-512, kde větší délka výsledného haše poskytuje stále ještě vyšší záruku bezpečnosti.

Srovnání parametrů funkcí rodiny SHA je dostupné v tabulce 4.6.

Tabulka 4.6: Vlastnosti hašovacích algoritmů SHA

třída	algoritmus	délka zprávy [v bitech]	velikost bloku	velikost slova	velikost MD	bits of security
SHA-1	SHA-1	$<2^{64}$	512	32	160	80
SHA-2	SHA-256	$<2^{64}$	512	32	256	128
	SHA-384	$<2^{128}$	1024	64	384	192
	SHA-512	$<2^{128}$	1024	64	512	256
SHA-3	SHA3-224	-	1152	-	224	112
	SHA3-256	-	1088	-	256	128
	SHA3-384	-	832	-	384	192
	SHA3-512	-	576	-	512	256

4.8.3 RIPEMD-160

RIPEMD-160 [9] vychází z koncepce RIPEMD hashovacího algoritmu, který vznikl v rámci projektu Evropské unie **Race Integrity Primitives Evaluation (RIPE)** a reaguje na slabiny původního algoritmu, které objevil začátkem roku 1995 Hans Dobbertin. Zvyšuje délku výsledného hashe na 160 bitů a zvyšuje také počet kol.

Geografická oblast využití se omezuje zejména na státy Evropské unie a státy o vstup usilující. V USA je preferovaný algoritmus SHA. Na základě podrobné analýzy MD4 vznikl posílený algoritmus, který byl nazván RIPEMD.

RIPEMD se v zásadě skládá z dvou paralelních MD4, s dalšími vylepšeními v oblasti bitových operací a změnou pořadí slov zprávy. Jinak v zásadě zůstává algoritmus MD4 zachován, včetně výsledné délky hashe 128 bitů.

Po útoku Dobbertina v roce 1995, který našel slabiny ve dvou kolech algoritmu ze tří, začalo být jasné, že bude nutné algoritmus upravit. Dalším důvodem pro úpravu byla i možnost útoku hrubou silou viz. závěr podkapitoly věnované MD2 – MD5. 128 bitů v dnešní době neposkytuje záruku dostatečné bezpečnosti.

RIPEMD v žádné verzi v současnosti není součástí podpisových schémat kvalifikovaných PCS. Používání těchto algoritmu se již v praxi nedoporučuje.

4.8.4 WHIRPOOL

Funkce Whirpool má za sebou zajímavý vývoj. Byla navržena v roce 2000 Vincentem Rijmenem a Paulem S. L. M. Barettem, kteří ji přihlásili do výběrového řízení pořádaného v rámci projektu **NESSIE**, který funguje v rámci programu **Information Society Technologies (IST)** Evropské komise. Cílem projektu NESSIE je napomáhat standardizaci kryptografických primitiv a fungovat tak podobným způsobem pro Evropskou unii jako NIST pro USA.

Součástí tohoto projektu bylo i výběrové řízení pro hašovací funkce, které mělo mít podobný charakter jako výběrové řízení NIST pro výběr AES. Bohužel do výběrového řízení byla přihlášena pouze hašovací funkce Whirpool. Tato funkce logicky byla vybrána a posléze zavedena jako jeden z doporučených algoritmů do revidovaného normy ISO/IEC 10118-3:2004 [11].

Z hlediska implementace je zajímavé, že tato hašovací funkce používá vnitřní 512-bitovou blokovou šifru W .

Zpráva je doplněna tak, že na konec se doplní 1 (bit), potom x krát 0 (bit) a 256-ti bitové číslo reprezentující délku původní zprávy. Nuly se doplňují tak, aby celková délka zprávy byla dělitelná beze zbytku na 512-ti bitové bloky m_1, m_2, \dots, m_n .

Jednotlivé bloky jsou použity pro generování pracovních hodnot hashe H_0, H_1, \dots, H_n . Přičemž H_0 je před započítáním práce iniciováno na 512 nulových bitů.

Pro výpočet H_i je využita blok zprávy m_i , který je zašifrován pomocí šifry W s H_{i-1} jako klíčem. Na zašifrovaný blok zprávy je aplikována operace XOR s H_{i-1} a m_i . H_i je hledaný výsledek hašovací funkce Whirpool.

Celkově se jedná o hašovací funkci velmi bezpečnou. V současné době neexistují poznatky, které by vedly k jakémukoliv oslabení bezpečnosti této funkce.

4.8.5 Doporučení k použití bezpečných hašovacích funkcí

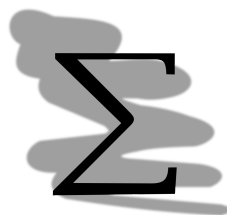
V současné době se používá několik desítek různých hašovacích algoritmů. Z hlediska zákona o elektronickém podpisu však můžeme použít pro vytváření plně kvalifikovaných certifikátů pouze některé algoritmy

1. SHA-2 (256, 384, 512) a
2. WHIRPOOL

Pro algoritmy SHA-1 a RIPEMD-160, ačkoliv nedošlo k úplnému prolomení jejich bezpečnosti, se doporučuje přechod k odolnějším algoritmům s delším výsledným hašem.

Z SHA algoritmů je doporučován zejména algoritmus SHA-512, jehož délka „bits of security“ poskytuje nejvyšší šanci na bezpečnost.

V současnosti platné normy však připouštějí použití i výpočetně méně náročných algoritmů, jako je SHA-256.



Shrnutí

Šifrování je staré jako písmo samo. Z hlediska techniky šifrování rozlišujeme dva typy šifrovacích algoritmů: *symetrické* a *asymetrické*.

Symetrické používají k zašifrování a dešifrování zprávy stejný klíč. Asymetrické naopak používají jiný klíč pro zašifrování a jiný pro dešifrování, využívá se pro to matematické příbuznosti obou klíčů.

Elektronický podpis a asymetrické šifrování jsou příbuzné, u obou se využívá dvojice klíčů a některé algoritmy (např. RSA) umožňují jak šifrovat tak podepisovat. U elektronicky podepisovaného dokumentu postupujeme tak, že vezmeme svůj soukromý klíč a použijeme jej na zprávu (nebo její haš), taková zpráva je ověřitelná pouze pomocí našeho veřejného klíče – za to, že veřejný klíč přináležejí určité osobě, odpovídá poskytovatel certifikačních služeb.

Asymetrické šifrování má za cíl chránit zprávu, před přečtením nepovolanou osobou, proto postupujeme opačně. Pro zašifrování zprávy použijeme veřejný klíč příjemce, zpráva je pak dešifrovatelná pouze s použitím privátního klíče – ten si každý uživatel tohoto typu šifrování udržuje v tajnosti.

Časová razítka, elektronické pečete a elektronické značky taktéž využívají postupů algoritmů elektronického podpisu. Elektronická značka se od podpisu liší právními důsledky - el. podpisem potvrzujeme (ručíme za) správnost dokumentu, el. značkou potvrzujeme, že nám dokument prošel rukama. Elektronická pečeť je určena organizacím a potvrzuje původ dokumentu. Časové razítko zase generuje nezávislá autorita časových razítek - je to jediný způsob jak zajistit prokazatelné ukotvení dokumentu v čase.

Bezpečné hašovací funkce jsou velmi důležitou avšak obvykle širokou veřejností ignorovanou problematikou. Na bezpečnosti těchto funkcí je založena bezpečnost elektronického podpisu, hesel apod. Výsledkem činnosti těchto funkcí je otisk zprávy, který je s vysokou pravděpodobností unikátní pro danou zprávu.



Kontrolní otázky

1. Proč nemůžeme substituční šifry v dnešní době považovat za bezpečné?
2. Jaký je rozdíl mezi symetrickým a asymetrickým šifrováním?
3. Popište postup použití privátního a veřejného klíče pro asymetrické šifrování.
4. Které bezpečné hašovací funkce je možné použít pro kvalifikovaný elektronický podpis v ČR?
5. K čemu slouží bezpečné hašovací funkce?

**Správné odpovědi**

1. Protože nemění frekvenční charakteristiky textu.
2. Symetrické šifrování používá jeden klíč pro zašifrování i dešifrování, asymetrické šifrování používá různé klíče pro šifrování a dešifrování.
3. Veřejný klíčem příjemce se zpráva zašifruje a privátním klíčem příjemce se dešifruje.
4. SHA třídy 2
5. Využití v rámci elektronického podpisu, náhrada šifrování hesel, kontrola integrity souborů ...

**Test**

1. Je možné za splnění určitých podmínek považovat použití kódů za bezpečné?
 - (a) Ano
 - (b) Ne
2. Skytale byla
 - (a) Substituční šifra
 - (b) Známý kód
 - (c) Šifrovací pomůcka
3. Který z následujících algoritmů lze použít pro asymetrické šifrování i elektronický podpis?
 - (a) RSA
 - (b) DSA
 - (c) ECDSA
4. Podpisové schéma tvoří
 - (a) DES, paddingová funkce, SHA
 - (b) DSA, paddingová funkce, SHA
 - (c) DEA, paddingová funkce, SHA
5. Elektronický podpis je ověřitelný
 - (a) Stále
 - (b) Po dobu jednoho roku
 - (c) Po dobu platnosti certifikátu

**Správné odpovědi**

1. a), 2. c), 3. a), 4. b), 5. c)

Kapitola 5

Úvod do počítačových sítí



Náhled kapitoly

V rámci této kapitoly se podíváme na základy problematiky počítačových sítí, zejména jaká zařízení na síti fungují a jakou plní funkci. Podíváme se také na specifika návrhu menších (domácích) sítí.

Po přečtení kapitoly budete

Vědět

1. jaké jsou vrstvy sítě
2. jaká zařízení se na síti vyskytují a jakou funkci plní



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 4 hodiny.

5.1 Rozdělení sítí

Počítačové sítě je možné dělit podle celé řady různých kritérií, např.:

- topologie
- charakteru komunikace
- oblasti, kterou síť pokrývá
- apod.

Topologií sítě se rozumí způsob, jakým jsou jednotlivé počítače do sítě zapojeny. Historicky topologií vznikla celá řada:

- sběrnice
- síť typu token ring (zapojení „do kruhu“)
- hvězdicová topologie
- hybridní topologie (např. stromové)

Sběrnice topologie je z dnešního pohledu, jako síťová topologie, překonaná (alespoň ve své čisté podobě). V rámci této topologie se koncová zařízení připojují ke sběrnici. Vizualně si lze tuto topologii představit jako na obr. 5.1.

Tento typ zapojení vyžaduje použití kabeláže, která tento typ zapojení umožňuje - obvykle se jedná o koaxiální kabel. Z tohoto kabelu se pomocí T-spojky provádějí odbočky pro jednotlivá koncová zařízení. Na obou zakončeních sběrnice je pak hlavní kabel zakončen tzv. terminátory, jejichž účelem je pohlcování volných signálů pohybujících se v síti.

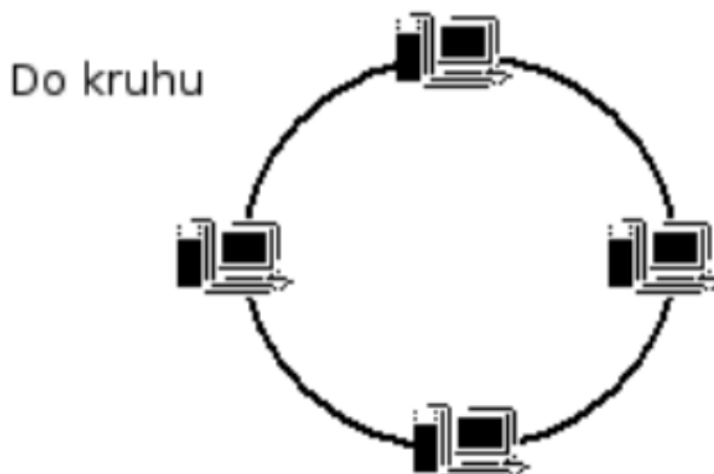


Obrázek 5.1: Sběrníková topologie počítačových sítí

Použití koaxiálního kabelu s sebou nese relativně malé přenosové rychlosti na sítích této topologie. Dalším problémem je také závislost na sběrnici jako takové - pokud dojde k přerušení kabelu dojde také k omezení dostupnosti sítě na počítačích tento kabel využívajících.

Tyto dva faktory vedly k tomu, že pro účely realizace sítí, se koaxiální kabeláž ani sběrníková topologie již nevyužívají.

Sítě typu **token ring** jsou z hlediska topologie zajímavé. Vizualně si je lze představit jako na obr. 5.2. Na první pohled by se mohlo zdát, že tento typ zapojení je prostou adaptací sběrníkové topologie, jenomže tomu tak není, protože zapojení do kruhu není fyzické, ale logické - je tedy implementováno softwarově, zatímco fyzicky je tato síť zapojena v *hvězdicové topologii* (viz níže).



Obrázek 5.2: Topologie počítačových sítí token ring

Fungování těchto sítí si lze představit tak, že určíme zdroj komunikace na síti a na jeho umístění položíme značku (token). Tuto značku postupně posunujeme v kruhu (ring) ve směru hodinových ručiček po jednotlivých počítačích v síti, až dojdeme k cíli komunikace.

Postup v kruhu je ale z hlediska efektivity síťového provozu poměrně problematický, proto se v praxi spíše používá hvězdicová topologie, popř. topologie hybridní.

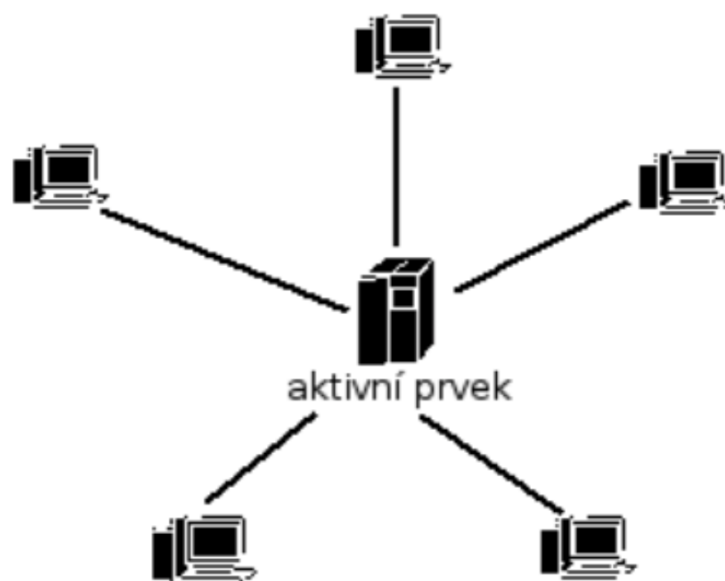
Vizuálně je možné si **hvězdicovou topologii** představit podobně jako na obr. 5.3.

V centru zapojení hvězdicové topologie je aktivní síťový prvek jako např. switch nebo router (viz podkapitola Síťová architektura ISO/OSI) a k němu jsou připojena jednotlivá další síťová zařízení. Připojení je realizováno pomocí dedikované (nesdílené) kabeláže. K tomuto účelu se obvykle využívá kabeláž známá pod názvem kroucená dvojlinka (twisted pair).

Hybridními topologiemi rozumíme kombinaci více typů topologií v rámci jediné sítě. Nejčastěji uváděným zástupcem tohoto typu topologií je *stromová topologie*, která kombinuje na nejnižší úrovni hvězdicové zapojení, aktivní prvky sítě jsou ale zapojovány pomocí sběrníkové topologie (pomocí zařízení hub nebo switch). Účelem hybridních topologií je umožnit stavbu rozsáhlejších sítí.

Podle oblasti, kterou síť pokrývá je možné typově síť rozdělit na síť:

- **Local Area Network (LAN)**
- **Wide Area Network (WAN)**
- **Metropolitan Area Network (MAN)**



Obrázek 5.3: Hvězdicová topologie počítačové sítě

- kontinentální
- celosvětové apod.

Nejčastěji používaným pojmem z výše uvedených jsou sítě **LAN**. Jedná se tzv. lokální síť. Lokálností se v tomto případě rozumí fakt, že síť je fyzicky realizována v jedné budově nebo areálu - tedy na jednom místě pro organizaci nebo domácnost. Sítě **WAN** jsou jiné - nikoliv nutně po technologické stránce, ale fyzickou lokací sítě.

Sítě WAN zasahují mnohem větší plochu než sítě LAN. Společným prvkem zůstávají použité technologie a vlastnictvím/uzitím sítě jedinou organizací. Pomocí WAN sítí se řeší problém vzájemného propojení sítí geograficky vzdálených lokací. Dobrým příkladem může být naše univerzita - její hlavní kampus je v Porubě, Ekonomická fakulta a Fakulta bezpečnostního inženýrství jsou ale fyzicky v odlišných částech města. Každá odlehlá lokace proto realizuje vlastní LAN síť a tyto sítě jsou pak propojeny do rozsáhlejší WAN sítě.

Propojování odlehlejších lokací může být realizováno různým způsobem, lze využít veřejné infrastruktury telefonního vedení (např. pro připojení pomocí ADSL nebo VDSL), pokud není požadována vysoká přenosová kapacita. V opačném případě lze propojení realizovat pomocí optických kabelů. Často je navíc v síti mezi takovými vzdálenými lokalitami síťový provoz analyzován pomocí systémů **Intruder Detection System (IDS)** nebo **Intruder Prevention System (IPS)**. Tímto způsobem je možné včas detekovat, popř. i zabránit šíření virových infekcí nebo propagaci útoku hackerů mezi jednotlivými lokalitami organizace.

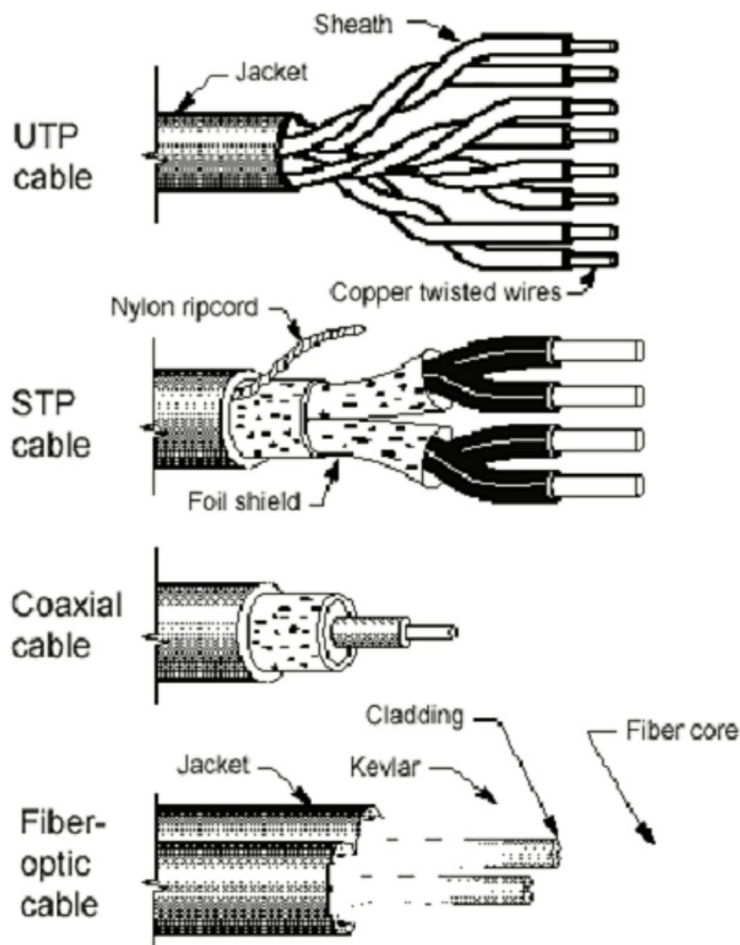
Sítě **MAN** je možno do určité míry připodobnit k veřejným infrastrukturám typu vodovody, kanalizace apod. Města si od budování metropolitních sítí slibují obvykle zvýšení zajímavosti pro větší investory, kteří se mohou na takovou síť připojit a získat tak vysokorychlostní připojení k Internetu, samozřejmě za úplaty. Fyzicky jsou takové sítě realizovány pomocí optických kabelů a nebo zřízením Wi-Fi hot spotů. Organizačně města budování a provoz takových sítí řeší zřízením dceřiných firem (s plným vlastnictvím města). Např. v Ostravě funguje tímto způsobem společnost Ova.net [24].

Představitelem **kontinentálních** sítí je např. síť CESNET2, rozvíjena sdružením CESNET. Jeho hlavním úkolem je výzkum v oblasti a vývoj v oblasti informačních a komunikačních technologií. Síť CESNET2 [3] propojuje pomocí vysokorychlostního připojení vzdělávací a výzkumné instituce v ČR a je připojena k podobně řešeným sítím zahraničím, zejména síť GÉANT, kterou lze považovat za evropskou páteř výzkumu, vývoje a vzdělávání.

Typickým představitelem celosvětové sítě je pak Internet.

5.2 Kabeláž sítí

Schématické znázornění nejčastěji používaných typů kabeláže je dostupné na obr. 5.4.



Obrázek 5.4: Nejčastěji používané typy kabeláže v počítačových sítích (převzato z [65])

Začít výklad můžeme u kabelu **koaxiálního**, tento kabel se v praxi pro konstrukci počítačových sítí již nepoužívá. Přesto se s ním lze setkat, zejména ve formě antén a také kabeláže analogových kamerových systémů. Signály jsou kabelem vedeny pomocí elektrických impulzů vedených měděným jádrem kabelu. Vzhledem k útlumu signálu je možná délka kabeláže omezená. Toto omezení se liší podle služeb, pro které bude kabel využíván a také použitím různých variant kabelu.

Koaxiální kabely se dodávají ve dvou variantách:

- tenké a
- tlusté

V tomto případě označení tlustý a tenký skutečně odpovídá tloušťce kabelu. Tlustší varianta má přibližný dosah 500 m a tenčí pak přibližně polovinu.

Kabel typu **kroucená dvojlinka** (twisted pair) je v současnosti nejpoužívanějším síťovým kabelem. Kabel tvoří celkem 8 kabelů které jsou zkrouceny po dvou (viz obr. 5.4) - odtud název kroucená dvojlinka. Zkroucení kabelů není samoúčelné, ale plní velmi důležitou funkci, zmenšuje totiž přeslechy mezi jednotlivými kabely a omezuje též elektromagnetické vyzařování kabelu do okolí.

I tento typ kabeláže se dodává v několika různých variantách. Základní členění je mezi variantou nestíněnou (**Unshielded Twisted Pair (UTP)**) a stíněnou (**Shielded Twisted Pair (STP)**). Stíněná varianta se vyznačuje výrazně nižší úrovní vyzařování kabelu, tato vlastnost je však vyvážena vyšší cenou takového kabelu.

Kabeláž tohoto typu je možno také dělit podle tzv. *kategorie*. Kategorie se označuje CatX, kde X představuje číslo kategorie. Vyšší čísla v pořadí odpovídají novějším a proto také rychlejším katego-

riím kabeláže. V současnosti je v praxi nejrozšířenějším druhem kabeláže typu Cat5 s přenosovými rychlostmi 100 Mbps (mega-bit za sekundu), popř. 1 Gbps (gigabit za sekundu). Hodnota 1 Gps je na horní hranici možností Cat5 kabelu.

Nové sítě jsou pak konstruovány pomocí kabeláže Cat6 nebo Cat7 umožňující přenosové rychlosti až 10 Gbps, ve vývoji je pak kabeláž umožňující ještě vyšší přenosové rychlosti (Cat8 až 40 Gbps). Skutečná rychlost sítě však není determinována pouze kvalitou kabeláže, ale také aktivními síťovými prvky, které síťový provoz řídí. Proto pokud např. switch podporuje přenosové rychlosti pouze 100 Mbps, vyšší rychlosti z něj skutečně nedostanete, byť by to kabeláž samotná třeba podporovala.

Z hlediska fyzických vlastností je maximální délka kabelu 100 m a není z něj možné provádět odbočky.

Posledním typem kabeláže, kterou se v této podkapitole budeme zabývat jsou **optické kabely**. Tento typ kabeláže se od předchozích výrazně liší, protože nepřenáší elektrické impulzy, ale impulzy světelné. Přenosové rychlosti, stejně jako maximální délka kabelu, jsou proto výrazně vyšší.

Optické vlákno samotné má průměr 8 - 10.5 μm , s ochranným pláštěm je pak na průměru přibližně 125 μm . Velmi malá tloušťka a relativně příznivá cena umožňuje, aby vlákno nebylo pokládáno samo, ale ve svazcích. Vzhledem k tomu, že mezi jednotlivými vlákny nevznikají interference mohou být v jednom svazku desítky, stovky nebo dokonce tisíce vláken.

I v případě použití optické kabeláže dochází k určitému útlumu signálů, vzhledem k tomu, že signály jsou v tomto případě světelné, je možno překlenout relativně velké vzdálenosti. Opět pro různé typy služeb se doporučují různé maximální délky kabelu, pro většinu služeb se jako bezpečná vzdálenost uvádí 50 km.

Hlavní použití kabeláže je pro překlenutí velkých vzdáleností - předpokládá se proto, že kabel bude tažen vně budov. Kabel je obvykle tažen v zemi.

5.3 Síťová architektura ISO/OSI



Upozornění

Tato podkapitola není z hlediska použité terminologie úplně korektní. Aby se autor vyhnul některým pokročilejším tématům (např. vysvětlování toho jak vypadá packet apod.), byl text zjednodušen až na samotnou „hranu“. Cílem této kapitoly je seznámit čtenáře primárně se základními síťovými zařízeními a jejich funkcí. Pro podrobnější informace o problematice lze doporučit např. server *Svět sítí* [65] nebo články na specializovaných serverech, např. [41].

Jedním z nejznámějších popisů síťové architektury je tzv. *referenční model ISO/OSI*. Tento model vznikl jako snaha o standardizaci síťové architektury. Ačkoliv proces standardizace se nepodařilo dotáhnout do úplně zdárného konce, je tento přístup v podstatě dodržován (s určitými odchylkami).

Referenční model se skládá ze sedmi na sebe navazujících vrstev:

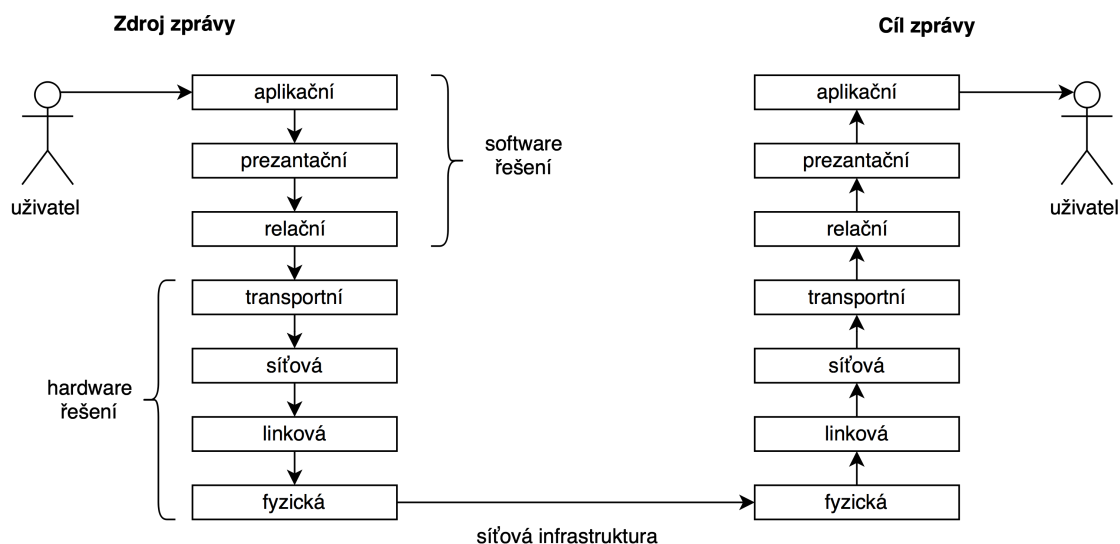
1. fyzická
2. linková
3. síťová
4. transportní
5. relační
6. prezentační
7. aplikační

Vrstvy 1 - 4 jsou exaktně definovány a výrobci síťových zařízení tyto definice poměrně přesně dodržují. Důvod odhalíme relativně jednoduše při pohledu na seznam vrstev, první vrstvy jsou spojeny s více s hardware. Odchylky v jejich realizaci by proto mohly snadno způsobit nekompatibilitu mezi zařízeními - zařízení na síti by prostě nemohla vzájemně komunikovat a to je samozřejmě nepřijatelné.

Zbylé tři vrstvy jsou spojeny spíše se síťovými protokoly, implementace protokolů různých výrobců se mohou v určitých aspektech lišit. Této vlastnosti lze dokonce využít pro tzv. *computer fingerprinting* (snímání otisku prstů počítače). Metoda funguje tak, že na cílový počítač se vyšle určitý požadavek a analyzuje se způsob jak vzdálený počítač na takový požadavek zareaguje. Jelikož odchylky v implementacích protokolů jsou známé, lze takto odhadnout např. jaký operační systém, popř. v jaké verzi

na počítači pracuje. Tento postup funguje obecně i pro programy, které nejsou součástí operačního systému, ale poskytují síťové služby.

Nyní se zaměříme na jednotlivé vrstvy modelu. Fungování vrstev nejprve znázorníme společně, viz obr. 5.5.



Obrázek 5.5: Komunikace v síti - pohled referenční model ISO/OSI

Jak z obr. 5.5 vyplývá, každý požadavek uživatele vyžadující síťovou komunikaci se propaguje operačním systémem od aplikace směrem k hardware, který pošle požadavek pomocí připojené síťové infrastruktury. Na straně příjemce se postupuje analogicky, ale popačně, tedy směrem od hardware interpretujícího požadavek nahoru až do aplikační vrstvy, která jej vyřídí.

Fyzická vrstva zajišťuje bitový přenos dat mezi zařízeními připojenými k síti. Na tuto vrstvu zařazujeme různé typy modemů, síťových karet apod., které toto připojení fyzicky zajišťují. Kromě toho, na této vrstvě fungují některá specializovaná zařízení, která mají svůj význam pro stavbu sítě jako takovou. Do této skupiny patří *repeatery* (opakovače)¹ a *huby* (rozbočovače).

Úkolem **repeaterů** je, jak naznačuje jejich název, zopakovat přenášený signál. Z výkladu o síťových kabelech již víme, že v kabeláži dochází k postupnému útlumu signálu se zvětšující se vzdáleností, kterou signál musí urazit. Z hlediska délky kabelu jsme proto omezeni. Repeater přijme signál, posílí jej a pošle dál. Z hlediska funkcí se tedy jedná o zařízení jednoduché, které je relativně levné, pracuje v reálném čase.

Huby neboli rozbočovače slouží pro propojování jednotlivých uzlů na síti. Pomocí hubu lze vyřešit problém použití různých typů kabelů (např. kroucená dvojlinka a optický kabel), jedná se také o základní prostředek pro hvězdicovou topologii sítě. Funguje tak, že signály přijaté na kterémkoliv portu jsou posíleny a přeposlány na zbývající porty (tedy dále do sítě). Zařízení připojená k hubu, pro která není komunikace určena je budou ignorovat - ozve se zpět pouze zařízení, kterému byla komunikace určena.

Z hlediska praktického se od použití postupně upouští, jelikož přeposílání komunikace do všech portů představuje neúměrně vysoké zatížení sítě, zejména tam, kde je do sítě zapojeno větší množství zařízení. Alternativu k použití hubu představují zařízení typu *switch*, tato zařízení fungují ale až na linkové vrstvě počítačové sítě.

Linková vrstva sítě zajišťuje přístup k přenosovému médiu a je odpovědná také za adresaci na fyzickém spojení. Na této vrstvě se pracuje s adresou, která je spojena přímo s hardware - tzv. MAC adresou (**Media Access Control (MAC)**). MAC adresa se skládá ze dvou částí - identifikátoru výrobce a sériového čísla zařízení. Tato adresa by proto měla být unikátní a to celosvětově.

Na úrovni linkové vrstvy pracují zařízení důležitá pro architekturu sítě, jedná se o zařízení typu *bridge* (můstek) a *switch* (přepínač), na který jsme narazili již při výkladu významu hubů.

¹ v praxi se používají spíše anglické názvy zařízení, než jejich české ekvivalenty

Switch v zásadě vypadá (viz obr. 5.6) a plní funkci jako hub, činí tak ale inteligentním způsobem. Jak je z obr. patrné, hlavním vizuálním prvkem jsou síťové porty, v tomto případě je jich 48. Z hlediska počtu portů se dodávají switche s počtem portů v násobcích osmi (tedy 8, 16, ..., 48). Počet 48 portů již lze pro praktické nasazení možno považovat za mezní.



Obrázek 5.6: Switch Cisco Catalyst 2950

V čem je tedy switch lepší než hub? Výhodou je, že si switch vytváří automatizovaně určitou představu o architektuře sítě - komunikaci proto nemusí přeposílat na všechny aktivní porty, ale pouze tam, kde se nachází cílové zařízení komunikace. Tímto způsobem se výrazně omezí síťový provoz aniž by utrpěla kvalita datových přenosů na síti.

Další výhodou je, že switch pracuje transparentně. Transparentností rozumíme to, že z hlediska funkce sítě se jedná o zařízení, které nemění data jím procházející, funguje automatizovaně a proto není potřeba v rámci komunikace switch adresovat (přímo oslovovat). Pro zařízení fungující na vyšších vrstvách počítačové sítě je tak switch prakticky neviditelný - nemusí se starat o to jak funguje.

Zařízení typu **bridge** slouží pro propojení (přemostění) různých sítí nebo jejich segmentů. Můstek musí mít povědomí o tom, zda adresát komunikace je v „jeho“ segmentu nebo ne. Tuto představu si vytváří transparentně na základě síťového provozu, který přes něj prochází. V případě, že adresát komunikace není v segmentu, ze kterého tato komunikace vzešla přepoše bridge komunikaci do všech připojených segmentů sítě.

Opět se tedy nejedná o příliš „inteligentní“ zařízení. Z hlediska praktického nasazení proto často nahrazováno buďto pomocí switchů nebo routerů.

Síťová vrstva zajišťuje adresaci v rámci sítě s více segmenty, Adresa je v tomto případě logická (není proto spojena přímo s hardware např. síťové karty). Nejčastěji používaným protokolem na této vrstvě sítě je *IP protokol*. Tento protokol je v současnosti používán ve dvou různých verzích, konkrétně IPv4 a IPv6. Hlavním rozdílem (ale ne jediným) mezi nimi je vzhled a počet IP adres, se kterými může protokol pracovat.

IPv4 adresa se skládá ze čtveřice čísel v intervalu 0 - 255 oddělených tečkami. Adresa samotná vypadá následovně např., 148.196.200.15. IPv4 tedy umožňuje použití 2^{32} (4 294 967 296) adres. Aby komunikace na síti fungovala, musí být zajištěno, aby použité IP adresy byly na síti unikátní - tedy neopakovaly se. V případě, že by se na síti vyskytly dvě různá zařízení se stejnou IP adresou, došlo by k tzv. konfliktu IP adres, který by se prakticky vyřešil tak, že první (dříve) připojené zařízení do sítě by tuto adresu mohlo používat a všechna další mají smůlu a zůstala by tedy bez připojení do sítě.

Prudký rozvoj Internetu jasně ukázal, že počet IP adres poskytovaný IPv4 je absolutně nedostačující - definitivní řešení pro představitelnou budoucnost představuje přechod IPv6. Předtím, než se trochu podíváme na novější IPv6, se podívejme ještě na některé adresy IPv4, popř. jejich rozsahy, které mají speciální význam.

Např. adresa 127.0.0.1 je tzv. *loopback adresa* - tedy adresa odkazující se sama na sebe. Existuje také několik rozsahů IP adres sloužících pro tzv. *privátní sítě*. Privátní síť rozumíme síť, která je neveřejná, tedy její jednotlivá koncová zařízení nemají veřejnou IP adresu. To znamená, že může existovat stovky sítí využívající stejné (privátní) IP adresy a přesto to nevyvolává síťové konflikty. Pokud takové zařízení ale má mít přístup na Internet nemůže se k němu připojit přímo, ale pouze prostřednictvím dalšího zařízení, jako je např. síťová maškaráda (NAT) apod.

Rozsahy adres privátních sítí jsou definované standardem RFC 1918 [25]:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

IPv6 adresa je tvořena osmi čtveřicemi čísel v šestnáctkové soustavě. IPv6 adresa by proto mohla vypadat následovně: fdce:9f6a:0995:0000:0000:0000:0000:0047. Prakticky to znamená, že k dispozici je 2^{128} adres, což je počet z dnešního pohledu nevyčerpatelný. IPv6 má ale také řadu dalších užitečných vlastností reagujících na změny ve způsobu využívání sítí:

- jumbo packets - podpora pro efektivní přenos větších souborů, popř. streamování
- podpora pro elektronické podepisování jednotlivých uzlů v síti (mělo by tak být obtížnější pro útočníka vydávat se za jiné zařízení)
- podpora šifrování komunikace
- a řada dalších

Na síťové vrstvě pracují **routery** (směřovače). Jedná se o zařízení, která mají jisté povědomí o architektuře sítě, tedy kde se co nachází, a snaží se směřovat síťový provoz tak, aby byl co možná nejefektivnější. Oproti zařízením typu bridge tedy nerozesílá komunikaci do všech připojených segmentů sítě, ale pouze tam, kde se skutečně nachází cílové zařízení.

Je zajímavé, že pro některé routery jsou označovány také jiným názvem - konkrétně *gateway*, tedy brána. Toto označení se někdy používá pro routery, které se starají o směřování síťové komunikace mezi sítí LAN a jejím okolím. Funkčně není mezi běžným routerem a gateway rozdíl - jedná se tedy spíše o historickou záležitost.

Přenosová vrstva zajišťuje spolehlivost přenosu dat po síti dle požadavků vyšších vrstev architektury ISO/OSI. V rámci této vrstvy sítě se poskytují dva druhy služeb a to tzv. *spojové* a *nespojové* služby.

Spojovými službami rozumíme takové, které zajišťují spolehlivost datových přenosů - jinými slovy obsahují kontrolu kvality síťové komunikace. Jde tedy o to, že spojová služba zajistí navázání spojení, odeslání a příjem dat a kontrolu toho, zda byla přijata všechna požadovaná data, a že přijatá data jsou v pořádku, např. že nebyla poškozena po cestě. Typickým představitelem protokolu spojových služeb je *TCP*.

Nespojové služby se oproti tomu vůbec nestarají o kvalitu spojení, tím pádem ale odpadá určitá režie, která činí tento typ služeb zajímavých pro aplikace zaměřené čistě na datové přenosy (např. Bittorrent). Kontrolu kvality, v případě potřeby, lze realizovat na vyšších vrstvách síťové architektury - především v aplikační vrstvě.

Typickým představitelem nespojových služeb je protokol *UDP*.

Spojová vrstva zajišťuje pravidla pro navázání a ukončování datových přenosů mezi uzly sítě. Příklady protokolů fungujících na spojové vrstvě, se kterými se lze setkat v praxi jsou:

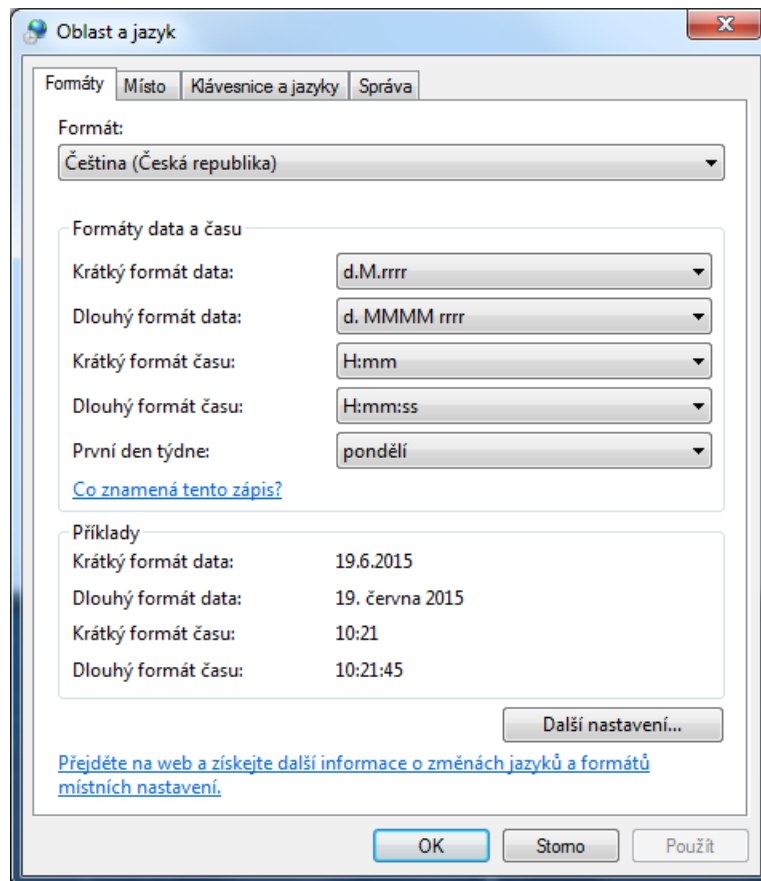
- **Network File System (NFS)** . používá se na síťových datových úložištích
- **SQL** - jazyk pro manipulaci s relačními databázemi
- **Remote Procedure Call (RPC)** - protokol starají se o manipulaci se vzdálenými zařízeními, např. nástroj vzdálená plocha využívá RPC.
- apod.

Pro protokoly pracující na spojové vrstvě je typické, že signalizují stav připojení, jsou schopné předávat příkazy, hlásit výsledek (ať už formou dat nebo chybového hlášení).

Prezentační vrstva je zodpovědná za formátování a syntaxi dat. Jde o to, že v různých kulturách se dělají věci různě. Vezměme si takovou banální věc jako je číslo. V ČR bychom číslo tisíc s dvěma desetinnými čísly mohli napsat třeba takto 1.000,00 nebo takto 1 000,00, ale v USA by zápis vypadal spíše 1,000.00 nebo 1 000.00. Tedy zatímco u nás se používá symbol desetinné čárky v USA se používá desetinná tečka, zatímco u nás se používá jako oddělovat tisíců tečka, v USA je to čárka. Takových rozdílů je obrovské množství v datech, v používaných písmenech (diakritika), speciálních znacích apod.

Tyto rozdíly nevznikly přes noc - jsou výsledkem dlouhodobého vývoje jazyků. Problémem je, že počítače nejsou vnitřně navrženy tak, aby se dokázaly s takovými rozdíly samy vypořádat. Uznávají pouze jednu definici čísla, data apod. Prezentační vrstva se proto stará o překlad údajů v těchto striktních definicích do podoby lokální specifik a zpět. O tento úkol se obvykle stará samotný operační systém. Ve Windows toto nastavení najdete například v Ovládacích panelech - Oblast a jazyk, viz obr. 5.7.

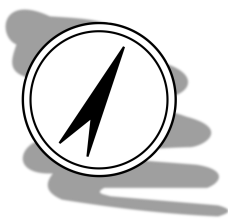
Na prezentační vrstvě mohou také nastat některé problémy v kompatibilitě. Tyto problémy vznikají tak, že tvůrce programu předpokládá použití určité specifické znakové sady nebo formátu čísel a



Obrázek 5.7: Nastavení formáty data a čísel ve Windows 7

nepočítá s tím, že např. existují státy, kde se nemluví anglicky (nebo japonsky nebo ... dosadte jiný více či méně oblíbený exotický jazyk). Takové problémové programy je často možno zprovoznit změnou nastavení formátu čísel nebo data, pokud jej tedy nutně musíte použít.

U **aplikační vrstvy** již pracujeme s běžnými aplikacemi, které nějakým způsobem pracují se sítí.



Nejdůležitější informace ze sítě

V této kapitole jsme toho probrali velké množství, ačkoliv všechny informace obsažené v textu jsou relevantní, některé jsou přece jenom důležitější než jiné. Věnujte proto obzvláště velkou pozornost zařízením typu: switch, router, protokolům IP a TCP (TCP/IP) a funkci prezentační vrstvy.

5.4 Ostatní síťová zařízení

Kromě síťových zařízení, kterými jsme se zabývali v předchozí podkapitole, na síti funguje celá řada dalších zařízení, o kterých byste měli mít určité povědomí. Pravděpodobně nejdůležitějším zařízením je *server*. Serverem rozumíme počítač, který je nastaven tak aby poskytoval na síti určité služby. K serveru se pak dálkově připojují další počítače - *klienti* a tyto služby využívají.

Servery lze členit podle různých kritérií, např. podle použitého operačního systému, jelikož prostor těchto skript je poměrně omezený zaměříme se na jiný druh členění - podle typů služeb, které server provozuje. Z tohoto pohledu lze rozlišovat:

- databázové servery
- WWW servery
- souborové

- tiskové
- aplikační
- atd.

Tento typ rozčlenění je potřeba chápat jako do určité míry virtuální. Technicky totiž nebrání nic tomu, aby jedno zařízení (server) neplnil všechny výše uvedené úlohy. K samostatnému řešení výše uvedených služeb nás vede především snaha provoz těchto služeb lépe zabezpečit a také lépe škálovat.

Lepším zabezpečením máme na mysli především to, že lze mnohem lépe specifikovat okruh uživatelů a způsobu užití serveru - zmenší se tak prostor zneužitelný pro případnou kompromitaci serveru pomocí malware nebo útokem hackera. Škálovatelností rozumíme přizpůsobení výkonu požadavkům uživatelů. Službu z tohoto pohledu lze provozovat na jediném serveru nebo v případě potřeby zátěž rozložit na serverů více (cluster serverů).

Nyní už blíže k jednotlivým typům serverů. **Databázový server** se stará o poskytování služeb systému řízení báze dat. Česky to znamená že klientům poskytuje data a umožňuje také jejich porřízení/editaci/výmaz. K tomuto účelu obvykle využívá jazyka SQL, o kterém jsme se zmínili již v předchozí podkapitole.

Jako představitele databázových serverů lze uvést např.:

- open source databázové servery
 - MySQL
 - PostgreSQL
 - a další
- proprietární databázové servery
 - Oracle
 - MS SQL Server
 - DB2
 - a další

WWW server poskytuje WWW stránky nebo jiné zdroje dostupné pomocí protokolu http nebo jeho šifrované varianty https. WWW stránky přitom mohou být *statické* (ve formátu html nebo xhtml) - v takovém případě jsou poskytovány jako jiné zdroje dostupné na Internetu (např. obrázky nebo videa) a nebo mohou být *dynamické*. Dynamičnost WWW stránky spočívá v tom, že obsah stránky se vygeneruje dynamicky pomocí skriptu na serveru, obvykle s využitím databázového backendu na základě požadavku který byl na server zaslán.

O spuštění a management výsledků skriptů se stará právě WWW server. V současnosti nejpopulárnější WWW servery jsou:

- Apache
- MS Internet Information Service
- Nginx

Souborové servery poskytují svým uživatelům prostor na disku - tento prostor se také někdy označuje jako disková kvóta. Souborové servery mohou být realizovány různě - mohou poskytovat WWW rozhraní pro manipulaci se soubory, pomocí FTP/FTPs nebo mohou využívat některý z protokolů pro mapování síťových zdrojů (např. ve Windows SMB). Mohou, ale také nemusí, být integrovány se systémy řízení identity uživatelů na síti. Integrace v tomto případě umožňuje „inteligentní“ přidělování diskových kapacit jednotlivým uživatelům nebo jejich skupinám.

Existují specializovaná zařízení, která se zaměřují pouze na poskytování diskových služeb. Taková zařízení často označujeme jako **Network Attached Storage (NAS)**. Taková zařízení umožňují domácnostem, malým a středním firmám efektivně spravovat relativně velké diskové kapacity. Představu o vzhledu NAS si lze udělat z obr. 5.8.

NAS zařízení se vyznačují použitím více disku (dva a více), které je možno propojit do diskového pole. Nastavování zařízení se obvykle děje pomocí WWW rozhraní.

Úkolem **tiskového serveru** je spravovat tiskárny a jejich tiskové úlohy. Použití tiskového serveru má tu výhodu, že správa tiskáren je centralizovaná, to umožňuje:

- nastavovat, kdo a na jaké tiskárně (popř. kdy) může tisknout
- lepší diagnostiku problémů s tiskárnami



Obrázek 5.8: 6-ti diskový NAS TVS-671 společnosti QNap (převzato z: [28])

- kontrolu vytíženosti tiskáren
- implementaci nástrojů pro monitoring nákladů spojených s tiskem
- a další

Použití tiskových serverů tedy představuje velmi efektivní nástroj umožňující efektivní správu všech aspektů použití tiskáren v organizace.

Aplikační server slouží pro zprostředkování aplikační logiky klientským počítačům. Co přesně to znamená? Klasické programy (tzv. thick (tlustý) klient) jsou provozované celé na klientském počítači. Tedy veškerá programová logika se provádí na běžném PC uživatele počítače. Tento způsob práce je, dalo by se říci, tradiční, je s ním ale spojena také řada nevýhod, zejména v okamžiku kdy takových klientů organizace provozuje stovky nebo tisíce a všechny je musí udržovat. Jakákoliv změna v aplikační logice se v takovém případě vyžádá provedení změn (distribuci upraveného programu) na všech klientských počítačích. Provedení takových změn je ale časově i finančně náročné. Nejedná se přitom nutně pouze o nutnost provedení změn v souvislosti s přidáním nějaké nové funkčnosti, ale také běžné údržby, podpory nových zařízení, opravy chyb apod.

Použití aplikačního serveru tyto problémy řeší pomocí konsolidace aplikační logiky na serveru. Na straně klienta zůstává pouze logika jeho přístupu k aplikační vrstvě na serveru. Veškeré změny v aplikační logice včetně oprav budou tak centralizované na serveru - řešíme tedy pouze jejich distribuci na server. Po provedení jeho aktualizace je nová verze programu dostupná okamžitě všem klientům.

Na síti se nachází také celá řada dalších zařízení, které plní různé funkce, některá z nich tady proto ještě zmíníme. První z nich je **Dynamic Host Cache Protocol (DHCP)**. DHCP je služba běžící na serveru, která se stará o přidělování IP adres klientským počítačům. Toto přidělování probíhá dynamicky, což znamená, že IP adresa se přiděluje na dobu určitou (hodiny až dny podle nastavení), a že adresa IP pro jednotlivé počítače v síti obvykle není stálá - mění se dynamicky podle toho, které IP adresy jsou právě k dispozici.

DHCP využívá toho, že v praxi je velmi nepravděpodobné, aby v jeden okamžik byla zapnuta všechna zařízení, která se v dané organizaci mohou připojit k síti. Vzniká tak určitý prostor pro to, aby organizace mohla manipulovat s relativně malým počtem veřejných IP adres pro větší množství zařízení. To je klíčová vlastnost počítačových sítí pracujících na bázi protokolu IPv4, jelikož již víme, že počet adres, které tento protokol má k dispozici, je značně omezený.

V protokolu IPv6 je sice podpora DHCP přítomna, ale jeho význam je menší a plní trošku odlišné úlohy.

Pro použití WWW (a nejenom jej) je klíčové použití **DNS (Domain Name Server (DNS))**. Úkolem DNS je zajistit překlad adresy IP na tzv. doménové jméno (např. www.vsb.cz). Bez doménových jmen bychom se museli k jednotlivým zdrojům dostávat přímým zadáním IP adresy - to by bylo jednak dosti

nepohodlné a také dosti problematické, protože moderní WWW servery jsou schopny na jedné IP adrese provozovat desítky nebo dokonce stovky webových sídel.

Domény se rozlišují podle tzv. řádů. Doména I. řádu je většinou spojena se státem (např. .cz) nebo tématem (např. .edu - vzdělávání). Z praktického hlediska může být vždy správce takové domény pouze jeden, v případě ČR je to sdružení CZ.NIC.

Doména II. řádu, vždy spadá pod některou doménu I. řádu. Registrace takové domény se provádí u tzv. registrátora domén. Takových registrátorů přitom může (a také je) v jednotlivých státech obvykle více. Žádost o registraci provádí předpokládaný uživatel domény. Žádosti se vyhová v případě, že je doména dostupná a byl zaplacen poplatek. Registrace je vždy časově omezena - obvykle na jeden rok. Za pronájem domény se platí každý rok.

Po expiraci domény (uplynutí doby na kterou byla doména zaplacená) je obvykle registrátorem poskytována určitá ochranná lhůta pro případ, že původní vlastník pouze zapomněl doménu zaplatit. V této lhůtě však již na doméně není dostupná webová prezentace původního vlastníka. Po uplynutí ochranné lhůty se doména vrací na běžný trh a může ji tak zakoupit kdokoli.

Příkladem domény druhého řádu může být např.: vsb.cz.

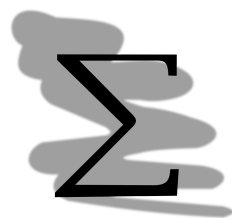
Doména III. řádu, někdy také nazývaná subdoména, se vytváří u domén II. řádu a může vypadat např. takto www.vsb.cz nebo fbi.vsb.cz. Za zřizování domén třetího řádu se již správci domény neplatí.

Posledním typem zařízení, které v této podkapitole zmíníme je **Network Address Translation (NAT)**. Někdy se pro NAT používají také odlišné názvy, např. síťová maškaráda a jiné. NAT řeší problém připojování privátních sítí k síti Internet. Jelikož na privátní síti jsou používány IP adresy, které nejsou nutné unikátní celosvětově - není možné privátní síť připojit k Internetu přímo (konečně proto je ta síť privátní). K připojení je nutné použít zařízení, které zprostředkuje toto připojení. Přesně tyto úkoly plní NAT.

NAT funguje tak, že umožňuje počítačům na privátní síti použít jeho veřejnou IP adresu k připojení k Internetu. Představit si to lze tak, že požadavky z koncových počítačů na privátní síti jsou směřovány přes NAT a teprve tam osloví cílové zařízení na Internetu.

NAT si pamatuje odkud požadavek vzešel a směřuje tam odpovědi ze zařízení na Internetu. Pro vzdálená zařízení, je ale NAT netransparentní - vidí a komunikují přímo pouze s ním, protože pouze NAT na dané síti má veřejnou IP adresu.

V okamžiku, kdy se plně do praxe nasadí IPv6, pozbude NAT smysl, jelikož IP adres bude dostupných tolik, že vlastní veřejnou IP adresu bude moci mít každé zařízení přítomné na síti a to celosvětově.



Shrnutí

Počítačové sítě lze členit podle různých vlastností nejčastější rozdělení ale rozlišuje síť LAN lokalizované v jedné budově nebo jednom areálu budov a síť WAN, které jsou schopny překlenout velké vzdálenosti mezi jednotlivými areály podniků.

Ze zařízení nezbytných pro konstrukci počítačových sítí je nutné zmínit *switch* sloužící pro propojení většího množství počítačů pomocí kabeláže. *Router* slouží pro směřování provozu na počítačových sítích, umožňuje tak propojovat různé segmenty sítí.

IP protokol umožňuje adresovat jednotlivá zařízení v síti pomocí IP adres. DNS je pak schopno tyto adresy překládat do podoby doménového jména (a zpět).



Kontrolní otázky

1. Co je účelem NAT?
2. Jakou funkci plní prezentační vrstva sítě?
3. K čemu slouží switch?
4. Jaká je funkce routeru?
5. Je možné z kroucené dvojlinky (kabel) vést odbočky?



Odpovědi

1. Účelem NAT je zprostředkovat připojení se k internetu počítačům přítomným v privátních sítích (počítačů nemajících veřejnou IP adresu).
2. Prezentační vrstva sítě se stará o převod údajů z podoby pochopitelné počítačem do podoby odpovídající lokálním specifikům (např. desetinná čárka nebo desetinná tečka).
3. Switch slouží pro připojení a komunikaci více počítačů do počítačové sítě.
4. Router směřuje síťový provoz. Slouží pro propojování jednotlivých segmentů sítě.
5. Ne.

Kapitola 6

E-government



Náhled kapitoly

Problematika e-governmentu je v ČR založena na několika základních pilířích, které v příštích dvou kapitolách postupně probereme. Jedná se:

- základní registry
- **informační systémy veřejné správy (ISVS)**
- datové schránky a elektronické podatelny
- ostatní nástroje

V této kapitole se zaměříme především na problematiku základních registrů a datových schránek, v kapitole příští pak probereme problematiku ISVS (informačních systémů ve veřejné správě).

Po přečtení kapitoly budete

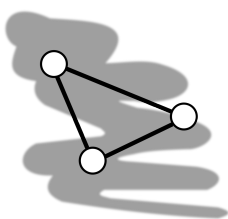
Vědět

1. co jsou to základní registry a jaké údaje udržují
2. jak fungují datové schránky
3. co jsou to elektronické občanské průkazy



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 2 hodiny.



Návaznost na elektronický podpis

Tato kapitola úzce navazuje na problematiku elektronického podpisu. Aby elektronická komunikace mezi orgány státní správy a firmami (popř. občany) byla důvěryhodná musí být dokumenty předávané např. datovými schránkami elektronicky podepsané. Před začátkem studia této kapitoly byste proto měli mít minimálně základní představu o tom, jak technicky funguje elektronický podpis a jak je jeho použití právně upraveno.

6.1 Základní registry

V roce 2009 byl přijat zákon 111/2009 Sb. o základních registrech [30], která definuje soubor základních registrů s informacemi o občanech. Základními registry ve smyslu tohoto zákona jsou:

1. Registr obyvatel
2. Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob)
3. Registr územní identifikace, adres a nemovitostí (registr územní identifikace)
4. Registr agend orgánů veřejné moci a některých práv a povinností (registr práv a povinností)

Tyto registry jsou určeny pro sdílení údajů mezi základními registry a mezi agendovými informačními systémy tak, aby tyto údaje byly udržovány pouze na jediném místě. Ostatní IS, které s těmito údaji pracují, jejich správnost dále nezkoumají.

Zajímavé je také to, že fyzické osoby, o kterých se agenda vede, jsou identifikovány pomocí ne-veřejného identifikátoru, který je navržen tak, že z něj nelze odvodit žádné osobní nebo jiné údaje vztahující se k dané osobě.

V registru obyvatel jsou vedeny následující informace:

- jméno a příjmení
- adresa/místo pobytu
- datum, místo o okres narození (+ stát u cizinců)
- datum, místo a okres úmrtí
- státní občanství
- čísla elektronicky čitelných identifikačních dokladů
- záznam o zpřístupnění datové schránky

Správce registru obyvatel je Ministerstvo vnitra.

V registru osob jsou vedeny následující údaje:

- obchodní jméno/jméno a příjmení u fyzických osob
- agendou identifikátor osoby
- datum vzniku/zápisu do evidence
- datum zániku/výmazu z evidence
- právní forma
- informace o zpřístupnění datové schránky
- statutární orgán
- právní stav
- adresa sídla
- datum zahájení/ukončení činnosti v provozovně
- adresa místa provozovny
- adresa místa pobytu

Správce registru osob je Český statistický úřad.

Registr územní identifikace obsahuje řadu údajů o území, ale také jednotlivých objektech, které jsou na něm postaveny. O území samotném jsou vedeny následující informace:

1. území státu,
2. území regionu soudržnosti
3. území vyššího územního samosprávného celku
4. území kraje
5. území okresu
6. správní obvod obce s rozšířenou působností
7. správní obvod obce s pověřeným obecním úřadem
8. území obce
9. území vojenského újezdu
10. správní obvod v hlavním městě Praze
11. území městského obvodu v hlavním městě Praze
12. území městské části v hlavním městě Praze
13. území městského obvodu a městské části územně členěného statutárního města
14. katastrální území
15. území základní sídelní jednotky
16. stavební objekt
17. adresní místo
18. pozemek v podobě parcely

O samotných objektech se pak shromažďují tyto informace:

1. měsíc a rok dokončení,
2. počet bytů u stavebního objektu s byty,
3. zastavěná plocha v m^2 ,
4. obestavěný prostor v m^3 ,
5. podlahová plocha v m^2 ,
6. počet nadzemních a podzemních podlaží,
7. druh svislé nosné konstrukce,
8. připojení na vodovod,
9. připojení na kanalizační síť,
10. připojení na rozvod plynu,
11. připojení na rozvod elektrické energie,
12. způsob vytápění a
13. vybavení výtahem.

Funkci editora vykonává obec, městský obvod nebo městská část územně členěného statutárního města, městská část hlavního města Prahy a kraj v přenesené působnosti.

V registru práv a povinností se eviduje především seznam činností a rolí, které vykonávají jednotlivé orgány veřejné moci. Správce registru je opět Ministerstvo vnitra.

V souvislosti s registry je zajímavé jedno datum a to konkrétně 1. 7. 2012. Od tohoto data totiž vstupují v platnost všechna ustanovení zákona o základních registrech v platnost. V praxi by to mělo znamenat, že úředník při komunikaci s občanem již nebude moci přímo od občana zjistit danou informaci, pokud je již obsažena v některém z registrů.

Myšlenka je to krásná, její praktická realizace však poněkud kulhá. Zdá se totiž že přechod na plnohodnotné využívání registrů nebude nijak snadný, neboť většina ISVS není připravena automatizovanou komunikaci s těmito registry. Připravilo se proto přechodné období, kdy informace ze základních registrů budou předávány poloautomatizovaně prostřednictvím datových schránek.

Předání bude vypadat tak, že úředník jeden-krát denně vypíše formulář požadující informace a ty pak následně odešle na místo určení prostřednictvím datových schránek. Žádost o informace bude vyřízena a informace se pošle žádajícímu úředníkovi zpět, opět prostřednictvím datové schránky.

Veškeré přístupy k registrům jsou navíc pečlivě evidovány. Občan tak má možnost požádat o výpis „aktivity“ v registrech týkající se jeho osoby. Může tak teoreticky zjistit, kdo (např. jaký úřad) se o jeho osobu zajímal. Slovo teoreticky je tady použito proto, že je ve výpisu aktivity velmi obtížné rozlišit automatizované zásahy systémů a jsou technického rázu, které jsou prováděny v celém systému, a situací, kdy byl dotaz proveden některým z úřadů na určitou osobu přímo. To výrazně snižuje užitečnost celého mechanismu.

Přes veškeré problémy se základní registry staly páteří, ze které čerpají prakticky všechny informační systémy používané ve státní správě.

6.2 Elektronické podatelny

Povinnost zřizovat elektronické podatelny byla stanovena vyhláškou 496/2004 Sb. o elektronických podatelkách. Samotné zřízení elektronické podatelny se dělo podle nařízení vlády 495/2004 Sb., kterým se provádí zákon č 227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů.

Uznávány jsou podané dokumenty, které splňují určité požadavky na formát zprávy (obvykle jsou podporovány formáty doc, xls, pdf a html – požadavky na formáty musí být také zveřejněny). U některých typů dokumentů je nutné pak ještě připojení elektronického podpisu, značky nebo časového razítka. Požadavky na tyto typy dokumentů jsou stanoveny samostatnými zákony a vyhláškami.

Zaslaná elektronická zpráva se na úřadu zaregistruje a je vyřízena v souladu s pravidly, která byly pro tento typ dokumentů přijaty.

Technicky se v podstatě nejedná o nic jiného než běžné schránky elektronické pošty, které prokazatelně přináležejí k určitému orgánu státní správy nebo samosprávy.

Elektronické podatelny se z hlediska technického i legislativního přežily a jak vyhláška 496/2004 Sb., tak nařízení vlády 495/2004 Sb. byly zrušeny zákonem 167/2012 Sb. Přesto některé obce nebo úřady elektronické podatelny ponechaly v provozu jako jednu z cest komunikace s občany.

Pro formální předávání dokumentů se pak většinou využívá služeb datových schránek nebo písemných podání (v „papírové“ podobě).

6.3 Datové schránky

Datové schránky byly přijaty v roce 2008 zákony 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů a 301/2008 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona 300/2008 Sb.

Pro funkčnost datových schránek jsou velmi důležité další navazující zákony a vyhlášky, především 191/2009 Sb. o podrobnostech spisové služby, 193/2009 Sb. o stanovení podrobností provádění autorizované konverze dokumentů a 194/2009 Sb. o stanovení podrobností užívání a provozování informačního systému.

Zákon 300/2008 definuje informační systém datových schránek a jeho využití. Na rozdíl od elektronické podatelny datová schránka funguje jinak. Není založena na technologii elektronické pošty, ale na existenci státem garantovaného informačního systému, kde každý uživatel má svůj prostor a také nástroje pro komunikaci, primárně s orgány státní moci, v omezené míře i dalšími uživateli datových schránek. Tímto způsobem odpadají problémy s identifikací uživatele, ale také problémy s doručovacími adresami, s vyzvedáváním pošty (listovních zásilek) apod.

Současným „technickým“ provozovatelem informačního systému datových schránek je Česká pošta.

Datové schránky mohou využívat orgány veřejné moci, právnické a fyzické osoby. Zřízení pro všechny typy uživatelů probíhá bezúplatně a to do tří dnů od podání žádosti. Použití datových schránek je přitom pro právnické osoby a orgány veřejné moci povinné a pro tyto zřízení datové schránky probíhá automaticky.

Fyzické osoby mohou využít služeb datových schránek nepovinně. Pokud si ale už datovou schránku zřídí, jsou orgány státní moci povinny s uživatelem komunikovat právě pomocí ní.

Datové schránky samotné zřizuje a spravuje Ministerstvo vnitra.

Uživatel k obsahu datové schránky přistupuje obvykle přes **WWW** rozhraní. Existují ale také desktopové aplikace, které umožňují s datovou schránkou pracovat také, často pohodlněji. Příkladem takové aplikace je Datovka 4 [46] vyvíjená sdružením CZ.NIC.

Veškeré zasláné dokumenty v rámci komunikace prostřednictvím datových schránek musí být elektronicky podepsány. Pasivní užití schránek je tak sice zdarma, ale v případě, že uživatel chce využívat datovou schránku pro zasílání dokumentů (není to ve všech případech povinné), musí získat patřičný certifikát od poskytovatele certifikačních služeb dle eIDAS. Tyto služby jsou již zpoplatněny.

V současné době je zatím většinou možná komunikace se státními orgány v „papírové podobě“ směrem podnik -> státní orgán, komunikace opačným směrem je však ze zákona možná pouze v elektronické podobě prostřednictvím datových schránek.

Jedinou výjimkou kdy i orgán veřejné moci může využít klasickou „papírovou“ formu je případ, kdy povaha dokumentu samotného zaslání v elektronické podobě, to neumožňuje. V současné době se tedy stále v papírové podobě přepravuje dokumentace s velkým rozsahem obrazového materiálu např. ze soudů apod.

Zasílání zpráv, faktur nebo v budoucnu jiných dokumentů právnickým nebo fyzickým osobám je přitom také zpoplatněno. Po několika letech provozu se nedá říci, že by právě posílání faktur mezi společnostmi pomocí datových schránek bylo nějak zvláště oblíbeno.

Pro zasílání zprávy je vždy vytvořena tzv. obálka s identifikačními údaji zprávy (tzv. metainformace o datové zprávě). Tato obálka se zasílá spolu se samotným souborem zprávy. Po uplynutí 10 dní, se zpráva automaticky považuje za přečtenou, se všemi právními důsledky, které to má. Uživatel datové schránky pak má možnost zprávu přečíst dalších 90 dní. Po uplynutí této doby je zpráva ze systému smazaná (pokud si uživatel nezaplátí dodatečnou službu nazvanou Datový trezor). V systému zůstane zachována pouze obálka datové zprávy obsahující

1. Kdo zprávu poslal
2. Komu ji poslal
3. Kdy ji poslal
4. Informaci zda a kdy byla přečtena
5. Název zprávy
6. Hash samotné zprávy

Pokud, tedy příjemce zprávy potřebuje zprávu zachovat pro pozdější použití, musí použít buď zpoplatněnou službu – tato služba ovšem neřeší expiraci certifikátu, kterým byla zpráva podepsána, a tedy možnost pozdějšího ověření pravosti zasláného dokumentu – nebo musí použít služeb tzv. *autorizované konverze dokumentů*.

Autorizovanou konverzi je možné provést na CzechPOINTu. Sestává se z ověření datové zprávy z hlediska validity elektronického podpisu (elektronické značky, elektronické pečeti, popř. časového razítka), následného tisku a zkontrolování souladu s původní zprávou. O celém procesu se vytvoří ověřovací doložka, která je uložena do centrálního úložiště. Celý proces tak připomíná proces standardního úředního ověřování dokumentů a jako takový je také zpoplatněn.



Platnost elektronického podpisu

Ověření dokumentu/datové zprávy je možné pouze po dobu platnosti certifikátu, který byl použit pro podepsání dokumentu.

Po uplynutí platnosti nebo revokaci certifikátu dokument/zprávu není možné ověřit bez ohledu na zákonné lhůty pro doručování zpráv do datové schránky a 90 denní ochranné lhůty pro archivaci zpráv. Takové zprávy již není možné ani autorizovaně konvertovat do listinné podoby.



Problém 24 hodin

S autorizovanou konverzí je spojován ještě jeden problém, který zasluhuje Vaši pozornost. Pro tento problém se vžil název *problém 24 hodin* a je spojován s procesem revokace certifikátu. Problém spočívá v tom, že v okamžiku, kdy osoba revokuje certifikát, PCS musí ověřit, že žádost je oprávněná, následně certifikát zařadí na seznam revokovaných certifikátů a ten zveřejní. Celá tato operace může zabrat až 24 hodin. Při autorizované konverzi se ověřuje zda certifikát použitý pro podpis není na aktuálně platném seznam revokovaných certifikátů. Tím ale není zaručeno, že certifikát nebyl revokován, ale aktualizovaný seznam revokovaných certifikátů ještě nebyl zveřejněn.

CzechPOINT tento problém přenáší na svého zákazníka upozorněním v průvodce konverzní doložky.

Do budoucna se uvažuje s možností dlouhodobého ověřování platnosti dokumentů uskladněných v datových schránkách. Předpokládá se přitom použití kombinace časového razítka a elektronického podpisu. Časové razítko umožní ukotvit dokument v čase a zkoumat, zdali v okamžiku zaslání zprávy byl certifikát použitý k podepsání zprávy v platnosti nebo ne.

Bohužel ani časové razítko nezajistí schopnost ověřování pro situace, kdy došlo k prolomení bezpečnosti použitého schématu elektronického podpisu, které by umožnilo padělání těchto dokumentů. Z tohoto důvodu se uvažuje o použití různých tzv. „solí“, které znesnadňují útoky, ale ani tento mechanismus nezaručuje dlouhodobou bezpečnost – zejména s uvážením možnosti úniku mechanismu generování solí.

Na ověřování dokumentů z datových schránek ale existuje ještě jeden pohled, který je v přímém rozporu s výše uvedeným názorem. Alternativní pohled pracuje s pojmem vyvratitelná domněnka pravosti, podle zákona 499/2004 Sb., o archivnictví a spisové službě. Domněnka pravosti totiž zjednodušeně říká, že dokument se považuje za pravý, pokud byl podepsán a není prokázáno, že by pravý nebyl.

Tento pohled se vůbec nezabývá platností certifikátů (ať už použitých pro podpisové operace nebo operace časového razítka) – dokument může platit věčně. To znamená, že na zájemci o zneplatnění dokumentu je důkazní břemeno prokázání toho, že dokument není pravý.

Takový přístup byl jednu dobu preferovaný státní správou. Dnes se však i státní správa spíše přiklání k nutnosti pečlivého udržování řetězce důvěry nutného pro technické zajištění zaručení pravosti elektronických dokumentů.



Elektronický podpis a datové schránky, zajímavosti a podrobnosti

Celá problematika elektronického podpisu a datových schránek je velmi zajímavá, bohužel však také velmi složitá a dynamicky se vyvíjející.

Pro zájemce proto doporučuji studium z dalších zdrojů. Začít doporučuji s podnětnými články Jiřího Peterky na lupa.cz [14].

Pozornost věnujte především článkům s nálepkou e-government, datové schránky, e-podpis a eIDAS (ačkoliv i ostatní články jsou nepochybně zajímavé).



Shrnutí

Základní registry jsou centrálně vedené databáze obsahující informace o občanech, osobách, nemovitostech a také jednotlivých agendách správních úřadů. Svým rozsahem se v podmínkách ČR jedná o nebývalý posun v oblasti e-governmentu, který se jinak nevyvíjí příliš dynamicky. Hlavní myšlenkou základních registrů je, že budou představovat důvěryhodný zdroj informací pro další agendy a systémy provozované veřejnou správou. Informace vedené v registrech proto občan nebude muset opakovaně hlásit na různých úřadech, ale prostě se načtou z těchto registrů.

Elektronickými podatelny rozumíme „virtuální“ místa, provozovaná orgány státní moci, kam je možné posílat oficiální komunikaci. V dnešní době se již do velké míry jedná o přežitek, jelikož úřady je možno kontaktovat jak elektronicky např. e-mailem (ideálně elektronicky podepsaným), tak pomocí datových schránek.

Datové schránky, přesněji řečeno *informační systém datových schránek* je systémem pro zaručenou komunikaci mezi úřady, úřady a osobami (právníckými nebo fyzickými) a osobami mezi sebou. Použití datových schránek je povinné pro úřady a také právnícké osoby (je povinné mít schránku a vybírat její obsah). Osoby fyzické si mohou datovou schránku nechat zřídit.

Pro komunikaci ze strany úřadů funguje tzv. doručovací fikce - tedy zpráva se po uplynutí určité doby považuje automaticky za přijatou se všemi právními důsledky, které to může mít, bez ohledu na to, zda ji ve skutečnosti někdo opravdu četl nebo ne.



Kontrolní otázky

1. Co řeší nařízení eIDAS?
2. Co rozumíme pojmem fikce doručení (u datových schránek)?
3. Jaké základní registry jsou provozovány v rámci ČR?



Odpovědi

1. Nařízení eIDAS řeší problematiku důvěryhodné identifikace fyzických a právníckých osob pro on-line služby provozované veřejnou správou v rámci celé EU.
2. Fikcí doručení rozumíme to, že po uplynutí stanovené doby předpokládá úřad, že jím zasláné podání bylo doručeno (se všemi právními důsledky) bez ohledu na to, zda k přečtení datové zprávy skutečně došlo nebo ne.
3. Registr obyvatel, registr osob, registr územní identifikace, registr práv a povinností.

Kapitola 7

Informační systémy veřejné správy



Průvodce studiem

V této kapitole se seznámíme s koncepcí informačních systémů ve veřejné správě (**ISVS**).

Po prostudování této kapitoly budete Vědět

- Jaké systémy považujeme za veřejné
- Jakým způsobem jsou **ISVS** sestavovány
- Jaké úlohy plní v této oblasti ministerstvo vnitra



Čas nutný pro studium

Pro prostudování této kapitoly budete potřebovat přibližně hodinu.

7.1 Stručná historie informačních systémů veřejné správy v ČR

Budování informačních systémů veřejné správy je spjato s nasazováním informačních technologií ve státní správě. Každá z institucí, která tyto systémy nasazovala tak činila proto, aby do určité míry automatizovala svou činnost a také získala jednotné úložiště, které by umožnilo sdílet data mezi pobočkami veřejných institucí.

Primárním cílem tak bylo zajistit plnění úkolů svěřených těmto institucím prostřednictvím v té době platné legislativy. To znamená, že každá instituce buduje vlastní, samostatné systémy, které nepředpokládají spolupráci se systémy jiných institucí nebo dokonce sdílení dat mezi nimi.

Slabiny této koncepce si vláda uvědomila už v roce 1996, kdy vzniká zákonem 272/1996 Sb. Úřad pro státní informační systém (ÚSIS). Ještě téhož roku měl být přijat další zákon, který tomuto úřadu měl definovat práva a povinnosti (tedy kompetence). Díky politickým turbulencím ale tento kompetenční zákon přijat nebyl a tak ÚSIS až do svého zániku zůstal „bezzubý“.

Výsledkem jeho práce tak bylo pouze několik spíše obecnějších dokumentů zabývajících se koncepcí informačních systémů ve veřejné správě.

Ke změně došlo až v roce 2000, kdy je přijat zákon 365/2000Sb. o informačních systémech veřejné správy, který ÚSIS ruší. Úkoly v oblasti **ISVS** tak přejímá nově zřízené Ministerstvo informatiky a Úřad pro veřejné informační systémy.

Úřad pro veřejné informační systémy dostává za úkol řešit především praktickou realizaci opatření v oblasti **ISVS**, zatímco Ministerstvo informatiky řeší oblast normalizace, vývoj legislativy apod.

Ministerstvo informatiky tak oblast řeší především návrhem standardů **ISVS**, které definují životní cyklus informačních systémů, jakým způsobem budou mezi nimi vyměňována data apod.

Poslední větší změna se udála v roce 2006, kdy zaniká Ministerstvo informatiky a jeho úkoly přebírá Ministerstvo vnitra. V rámci této transformace pozbývají platnost standardy **ISVS**, ve své původní podobě (tedy jako normy), některé z nich jsou ale přijaty ve formě vyhlášek v rámci nově přijaté legislativy ISVS.

7.2 Informační systémy veřejné správy

Informační systémy veřejné správy jsou definovány zákonem 365/2000 Sb. o informačních systémech veřejné správy. Tento zákon definuje **ISVS** jako soubor informačních systémů, které slouží pro výkon veřejné správy. Tedy v podstatě jakýkoliv informační systém, který je využíván orgány veřejné správy. Za **ISVS** jsou považovány i jiné informační systémy, které této definici nepodléhají. V takových případech tyto systémy do skupiny **ISVS** zařazuje nějaký jiný právní předpis (např. zákon o státní statistické službě, živnostenský zákon, apod.).

Naopak u některých informačních systémů, které by výše uvedenou definici splňovaly, se o **ISVS** nejedná a to opět ze zákona. Jedná se především o takové systémy, které nakládají s údaji takové povahy, že okruh užití těchto údajů by měl zůstat pouze v kompetenci daného orgánu.

Mezi **ISVS** proto neřadíme informační systémy používané zpravodajskými službami, Policí ČR, Vězeňskou službou, orgány činnými v trestním řízení, Národním bezpečnostním úřadem. Zákonu o **ISVS** také nepodléhají některé činnosti Ministerstva financí (v souvislosti s finanční kriminalitou) a Ministerstva obrany (v souvislosti s obranou státu).

Zákonu také nepodléhají orgány veřejné správy nebo právnické osoby (resp. **IS**, které provozují), které tyto **IS** využívají výlučně pro účely krizového řízení dle krizového zákona (240/2000 Sb.).

Specifické je také postavení Ministerstva vnitra, do jejíž gesce **ISVS** spadají. Ministerstvo vnitra má:

- kontrolní a tvůrčí pravomoci v této oblasti,
- působí v akreditaci a atestaci,
- stanovuje pravidla pro sdílení informací,
- vyjadřuje se k projektům **ISVS**,
- vydává věstník.

Pokud mají být finanční prostředky vynaložené na rozvoj **ISVS** vynaloženy efektivně, musí existovat místo, kde se tyto systémy (a jejich schopnosti) budou registrovat a orgán, který bude kontrolovat, že navrhovaný systém již není realizován a používán např. nějakým jiným orgánem státní správy. To znamená, že investice do pořízení nebo rozšíření **ISVS** není zbytečná.

Jednotlivé systémy musí být také vzájemně kompatibilní, pokud si mezi sebou mají vyměňovat informace. Tato kompatibilita by přitom měla jít až na co možná nejnižší úroveň – tedy na úroveň stanovení datového typu a rozsahu a také pravidel validace správnosti vyplněného údaje. Tyto definice pak musí být veřejně dostupné tak, aby je mohly správně do svých systémů implementovat další orgány státní správy. Těmto definicím a pravidlům souhrnně říkáme *referenční rozhraní*.

ISVS musí také splňovat určité bezpečnostní podmínky, s tím souvisí akreditace a atestace.

Akreditací rozumíme pověření nezávislé právnické osoby prováděním atestací **ISVS**. Akreditaci provádí Ministerstvo vnitra a může ji udělit pouze nezávislé právnické osobě (nezávislé na posuzovaných **ISVS**), která je zároveň členem mezinárodních sdružení zabývajících se akreditacemi.

V rámci akreditace se prověřuje zejména existence schválených akreditačních pravidel a také to, zda daná organizace má proces atestace odborně zajištěn kvalifikovaným personálem.

Atestace samotné pak provádí akreditované atestační středisko, které nesmí mít pohledávky vůči orgánům státní správy (nesplňovalo by podmínku nezávislosti). Atestace se provádí dvojího typu:

- posuzování dlouhodobého řízení **ISVS** a
- způsobilost k realizaci vazeb mezi systémy **ISVS**

Atestace se provádí vždy podle předem stanovených atestačních podmínek. Výsledkem atestace je protokol o zkoušce. Atest se uděluje vždy na dobu určitou a to maximálně na 5 let. Atest je však možno opakovaně prodlužovat a to maximálně o 2 roky.

Své úkoly v oblasti **ISVS** mají taktéž orgány státní správy a to především:

- spolupracují s Ministerstvem vnitra,
- předkládají Ministerstvu vnitra návrhy na pořízení nebo změnu informačních systémů,
- zajišťují vazby na jiné informační systémy pomocí referenčního rozhraní,

- zveřejňují číselníky,
- odstraňují nedostatky zjištěné v rámci kontrol.

Jakým způsobem konkrétně se výše uvedené činnosti provádějí, definují prováděcí vyhlášky tohoto zákona.

Vyhláška 469/2006 Sb. o informačním systému o datových prvcích definuje fungování informačního systému shromažďujícího informace o jednotlivých datových prvcích.

Datovým prvkem přitom rozumíme datovou položku a její popis. Účelem je, aby data vedená v informačních systémech veřejné správy vedla tato data stejně napříč systémy – a tyto systémy tak byly kompatibilní. Tento informační systém o datových prvcích je základním předpokladem pro možnost implementace referenčního rozhraní.

Předtím, než je tedy navržen nový datový prvek informačního systému, je konzultován **IS** o datových prvcích, zda už takový prvek neexistuje. Předem jsou už tak řešeny případné návaznosti mezi jednotlivými informačními systémy.

Vyhláška 528/2006 Sb. o informačním systému o informačních systémech veřejné správy definuje náležitosti informačního systému, který bude shromažďovat informace o existujících systémech veřejné správy. Takový systém umožňuje zjišťování, zda existuje **IS** s požadovanými vlastnostmi včetně toho, kde je takový systém nasazen.

Účelem takového systému je vytvořit prostředí motivující k efektivním investicím do IT. Organizace pořizující nebo modifikující **IS** tak nemůže činit svévolně, ale až poté co prokáže, že změna je nutná (v souvislosti s legislativními požadavky) a nejsou k dispozici takové systémy, které umožňují vedení potřebné evidence.

Vyhláška 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy se zabývá různými aspekty životního cyklu **ISVS** a zejména dat v něm obsažených. **IS** musí být spravován dlouhodobě – dokud bude trvat potřeba dat v něm obsažených. Z toho také vyplývá nutnost provádět plánování na pořízení nebo vytvoření informačního systému, ale také plány na udržení kvality poskytovaných služeb a bezpečnosti.

Základním dokumentem nutným k dosažení těchto cílů je *informační koncepce*, která se přijímá (na úrovni orgánu státní správy) na dobu určitou a tyto problémy by měla řešit.

Vyhláška 530/2006 Sb. o postupech atestačních středisek při posuzování dlouhodobého řízení **ISVS** stanovuje způsob, jak postupovat během atestace orgánů státní správy na jejich způsobilost dlouhodobě řídit své informační systémy. Atestace se zaměřuje především na hodnocení informační koncepce a provozní dokumentace provozovaných informačních systémů. Výsledkem atestace je certifikát s jedním z možných výsledků:

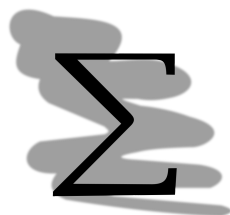
- splněno,
- splněno s výhradou,
- nesplněno.

Vyhláška 52/2007 Sb. o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb **ISVS** prostřednictvím referenčního rozhraní stanovuje způsob atestace způsobilosti orgánu státní správy realizovat vazby na jiné **ISVS** pomocí referenčního rozhraní.

Během atestace se hodnotí zejména soulad mezi implementací vazby a její soulad s dokumentací (viz. 469/2006 Sb.). Výsledkem atestace je certifikát s hodnocením splněno nebo nesplněno.

Vyhláška 53/2007 Sb. o referenčním rozhraní stanovuje povinnost používat v rámci **ISVS** vyhlášené datové prvky. Ovlivňuje také technologii, která bude použita pro výměnu informací mezi jednotlivými **ISVS** – předpokládá se totiž výměna pomocí jazyka XML.

Konečně vyhláška 64/2008 Sb. o přístupnosti garantuje přístupnost služeb **ISVS** také lidem se zdravotními postiženími.



Shrnutí

Informačními systémy veřejné správy (ISVS) rozumíme veškeré systémy využívané veřejnou správou pro vykonávání úkolů veřejné správy. Účelem legislativy ISVS je zajistit, aby jednotlivé IS implementované veřejnou správou:

- znovu „nevymýšlely kolo“ - tedy aby neřešily již vyřešené problémy
- byly vzájemně kompatibilní ve smyslu datových definic udržovaných údajů, které se objevují ve více systémech
- byly vyvíjeny pouze v případě, že je to opravdu nutné, tedy implementaci vyžaduje nová nebo změněná legislativa a neexistuje žádný systém, který by tyto požadavky plnil
- byly dlouhodobě udržitelné - tedy aby bylo možné IS dlouhodobě provozovat.

Koordináční úlohu v pro oblast ISVS má Ministerstvo vnitra, které jednak vede samo některé systémy zejména pak informační systém o informačních systémech ve veřejné správě (katalog používaných ISVS) a také vede IS datových prvků, obsahující definici datového prvku, která by měla být dodržena napříč jednotlivými systémy. Ministerstvo vnitra také akredituje atestační střediska, která hrají velmi důležitou roli v životním cyklu ISVS, atestují totiž jednotlivé úřady z hlediska schopnosti systémy dlouhodobě udržovat v provozu.



Kontrolní otázky

1. Co je to ISVS?
2. Jak probíhá atestace úřadu na schopnost dlouhodobě provozovat informační systém?
3. Co je to datový prvek ISVS?
4. Jaké úlohy plní v oblasti ISVS Ministerstvo vnitra?



Odpovědi

1. ISVS jsou všechny systémy provozované veřejnou správou pro plnění úloh jí svěřených platnou legislativou.
2. Atestace probíhá u akreditovaného atestačního střediska na základě žádosti úřadu. Atestuje se způsobilost k dlouhodobé udržitelnosti systému a také realizaci vazeb mezi různými systémy. Atestace je na dobu určitou, ale je možné podat žádost o její prodloužení.
3. Datový prvek je specifikace jména, datového typu a popisu údaje, který má být uložen v některém z ISVS. Účelem datového prvku je zajistit kompatibilitu mezi systémy za účelem výměny údajů mezi nimi.
4. Schvaluje pořízení nového ISVS, akredituje atestační střediska, vede informační systém o informačních systémech veřejné správy a informační systém o datových prvcích.

Kapitola 8

Kybernetická bezpečnost v ČR



Náhled kapitoly

Problematika kybernetické bezpečnosti, je již dlouhá léta skloňována ve všech pádech v soukromé sféře. Sféra veřejná ale po dlouhou dobu zůstávala stranou zájmu útočníků tak bezpečnostních expertů. V posledních letech se však situace výrazně změnila a jsme svědky výrazných posunů řízení kybernetické bezpečnosti jednotlivých států a také užšího zaměření se na ochranu řídicích systémů kritických infrastruktur.

V této kapitole se seznámíme se stavem řešení kybernetické bezpečnosti v ČR.

Po přečtení kapitoly budete

Vědět

1. jaké úlohy plní vládní a národní CSIRT tým
2. jaké je postavení kybernetické bezpečnosti s ohledem na ochranu kritické infrastruktury



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

8.1 Kybernetická bezpečnost

Dlouhou dobu byla otázka kybernetické bezpečnosti spíše doménou jednotlivých organizací - nebylo jasné patrné, že tuto problematiku je nutné řešit komplexněji i na té nejvyšší, tedy celostátní úrovni. Tento pohled se ale v průběhu posledních několika let změnil v souvislosti se změnou přístupu k ochraně kritické infrastruktury na straně jedné a odhalením řady dlouhodobých útoků, kterým musely čelit společnosti provozující významné prvky kritické infrastruktury i provozovatelé významných informačních systémů.

Z útoků, které by stálo za to zmínit, je možno zmínit např. Stuxnet nebo operaci Night Dragon. Stuxnet je malware zaměřený na fyzické poškození vybraných zařízení - konkrétně centrifug používaných pro obohacování uranu. Night Dragon byla operace kladoucí si za cíl kompromitaci sítí firem podnikajících v chemickém průmyslu USA, především pro účely získání intelektuálního vlastnictví společností, ale také plánů budov apod. V obou případech se předpokládá, že se jedná o tzv. *státem sponzorované útoky*, byť důkazy, že tomu tak skutečně bylo, chybí.

V poslední době také prakticky nemine týden, kdy by nebyl publikován nějaký případ velkého úniku informací nebo úspěšného útoku na významné počítačové síť. Změna celkové bezpečnostní situace v oboru IT tak nutně vedla ke změně postoje i v oblasti řešení této problematiky i na nejvyšší úrovni.

V ČR se problematiky kybernetické bezpečnosti ujalo Ministerstvo vnitra, později se ale hlavním garantem této problematiky stal **Národní bezpečnostní úřad (NBU)**, který má s touto problematikou podstatně větší praktické zkušenosti. Jako prvním krokem bylo zřízení národního CSIRT týmu (viz následující podkapitola) a později také Národního centra kybernetické bezpečnosti (**Národní centrum kybernetické bezpečnosti (NCKB)**), které je provozováno přímo v rámci NBÚ.

Hlavním účelem tohoto centra je provozovat vládní CERT České republiky GovCERT.CZ. Centrum plní také další úkoly, jako je spolupráce s obdobnými organizacemi v zahraničí, příprava bezpečnostních standardů pro různé kategorie organizací v ČR, osvěta, ale také výzkum a vývoj v oblasti kybernetické bezpečnosti.

Až do počátku roku 2015, ale centrum nemělo prakticky žádné pravomoci - 1.1.2015 ale vešel v platnost zákon 181/2014 Sb. o kybernetické bezpečnosti, který tuto situaci výrazně změnil. Zákon totiž legislativně zakotvuje postavení vládního a národního CSIRT týmu v ČR a stanovuje určité povinnosti některým osobám, zejména v oblasti povinnosti hlášení kybernetických bezpečnostních incidentů.

Jedná se zejména:

- orgány nebo osoby zajišťující významnou síť
- správci informačních systémů kritické informační infrastruktury
- správci významných informačních systémů

Významnou sítí se ve smyslu zákona rozumí síť, která zahrnuje systémy, zařízení a prostředky pro přenos signálů a vysílání, bez ohledu na druh přenášení informace, jejichž prostřednictvím je kybernetický prostor na území ČR propojen do zahraničí, nebo síť, které zajišťují připojení kritické informační infrastruktury ke kybernetickému prostoru.

Z definice významné sítě vyplývá, že v podmínkách ČR jich bude relativně málo. První půlka definice se týká připojení kybernetického prostoru ČR do zahraničí - bude se proto týkat zejména **Internet Service Provider (ISP)** a to jak těch, kteří připojují jednotlivce a firmy (např. Telefónica-O2, UPC a další) tak těch, kteří provozují specializované síť připojené do zahraničí, např. sdružení CESNET propojující vzdělávací a výzkumné instituce. Druhá půlka definice se týká kritické informační infrastruktury.

Kritickou infrastrukturou rozumíme obecně zvláštní kategorii systémů, které jsou kritické z hlediska udržení základních funkcí státu. Existuje řada definic, které pokrývají různé aspekty kritické infrastruktury (těmi se budete případně zabývat v jiných předmětech), pro účely tohoto předmětu si můžeme kritickou infrastrukturu nadefinovat jednoduše, jako systémy jejich vyřazení by vedlo k velkým ztrátám na životech, hospodářských škodách nebo jinému výraznému poškození zájmů ČR. Původní platná legislativa před zákonem o kybernetické bezpečnosti řešila problematiku kybernetické bezpečnosti v rámci odvětví *Komunikační a informační systémy*, kam spadají technologické prvky [18]:

- pevné sítě elektronických komunikací
- mobilní sítě elektronických komunikací
- sítě rozhlasového a televizního vysílání
- pro satelitní komunikaci
- pro poštovní služby
- informačních systémů

Problémem tohoto pohledu je zejména to, že řešeny jsou především technologické prvky, to odpovídá primárně fyzické ochraně těchto prvků. Problém kybernetické bezpečnosti je ale komplexnější, obsahuje sice složku fyzické ochrany, ale v případě, že daný systém je připojen k Internetu (a v některých případech i když připojen k internetu není) je možno jej kompromitovat čistě softwarovou cestou dálkově. Fyzická bezpečnost je proto sice důležitá a je nutné ji vždy řešit, avšak sama o sobě nemá dostatečný potenciál účinně ochránit zájmová aktiva proti plné škále hrozeb.

Zákon o kybernetické bezpečnosti proto definici kritické infrastruktury rozšiřuje o *systémy kritické informační infrastruktury*, které nejsou tak konkrétně vymezeny jako komunikační a informační systémy, neboť prostupují všechna odvětví kritické infrastruktury. Lze tedy dovodit, že v případě kritické informační infrastruktury se bude jednat o veškeré systémy IT (software i hardware), které řídí nebo „pohánějí“ systémy kritické infrastruktury.

Řízením v tomto případě rozumíme především systémy průmyslové automatizace, které fyzicky řídí výrobní nebo distribuční procesy. Součástí systémů kritické informační infrastruktury budou také systémy, které nespádají do oblasti průmyslové automatizace ale jsou přitom zodpovědné za zajištění fungování určitého odvětví kritické infrastruktury (např. v bankovníctví nebo pojišťovnictví).

Významným informačním systémem se ve smyslu zákona rozumí informační systém se zásadním významem pro fungování veřejné správy. Do této kategorie budou spadat zcela jistě systémy základních registrů, informačního systému datových schránek a některé z agendových systémů. Kritéria pro rozlišení toho, co do této definice spadá a co ne poskytuje v obecné rovině vyhláška 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích hovoří o systémech.

Zákon o kybernetické bezpečnosti dává do rukou NBÚ (prostřednictvím GovCSIRT.CZ) do rukou možnost vydávat varování stran odhalených zranitelností systémů nebo hrozící možnosti jejich zneužití (hrozícím útokem) a má právo také nařídit reaktivní a ochranná opatření.

Reaktivní opatření reaguje na probíhající útok - jeho cílem je útok zastavit a nebo omezit jeho dopady. Účelem *ochranného opatření* je preventivně zabránit nebo ztížit útok na zájmový systém.

Provedení opatření může nařídit NBÚ pouze zájmovým osobám (dle seznamu výše). Platnost nařízení je 3 dny od vyvěšení na úřední desce, ovšem s tím, že NKÚ má za povinnost pokusit se doručit nařízení do vlastních rukou. Zájmová osoba pak musí hlásit výsledek realizace nařízeného opatření.

Posledním, ale také nejmocnějším, nástrojem je možnost vyhlásit **stav kybernetického nebezpečí**. Tento stav je možné vyhlásit v případě, že je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací a tím by mohlo dojít k porušení/ohrožení zájmu České republiky ve smyslu zákona na ochranu utajovaných informací.

Během stavu kybernetického nebezpečí spadá pod pravomoc NKÚ širší skupina zájmových osob, které pak může taktéž nutit je spolupráci ve smyslu možnosti nařizování provedení opatření. Tento stav je může trvat maximálně jeden měsíc. V případě, že by nebezpečí trvalo déle může republika přejít do nouzového stavu dle běžné (ne IT legislativy).

8.2 CERT a CSIRT týmy a jejich význam

Jak bylo zmíněno v předchozí podkapitole, významnými hráči na poli kybernetické bezpečnosti jsou CERT a CSIRT týmy. Primárním úkolem takových týmů je především informování o možných hrozbách a také způsobu ochrany proti nim. Typově lze CERT/CSIRT týmy rozlišit následovně:

- vládní
- národní
- resortní
- týmy jednotlivých organizací

Státy obvykle mají pouze jeden vládní a jeden národní CERT/CSIRT tým. Ostatních týmů může být více. Z předchozí kapitoly víme, že funkci vládního týmu plní GovCSIRT.CZ provozovaný NBÚ v rámci NCKB, proto se zaměříme především na národní tým.

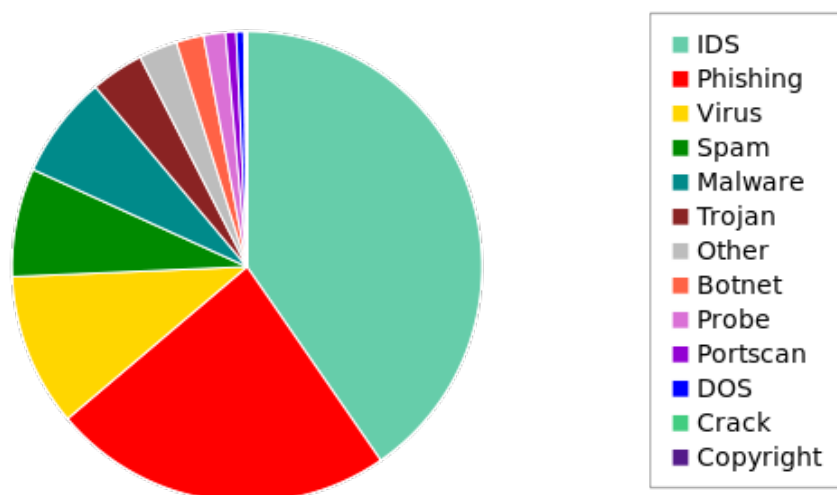
V České Republice roli národního **Computer Security Incident Response Team (CSIRT)** týmů zastává CSIRT.CZ provozovaný sdružením CZ.NIC od 1. ledna 2011. Obdobný národní tým v USA US-CERT vznikl už v roce 2008 (už od 80. let 20. století ale fungoval **Computer Emergency Response Team (CERT)** při Carnegie Mellon Univerzitě). V Polsku CERT.GOV.PL vznikl v roce 2008, na Slovensku CSIRT.SK byl zřízen nařízením vlády 479/2009 Sb. [29].

Role jednotlivých **CSIRT** týmů může být odlišná, například CSIRT.CZ popisuje [5] svoji roli následovně:

- Udržování zahraničních vztahů - se světovou komunitou **CSIRT** týmů a organizacemi, které tuto komunitu podporují.
- Spolupráce se subjekty v rámci ČR - **ISP**, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi.
- Poskytování služeb v oblasti bezpečnosti:
 - Řešení a koordinace řešení bezpečnostních incidentů
 - Osvětová a školicí činnost
 - Proaktivní služby v oblasti bezpečnosti

US-CERT definuje [66] své poslání jinak: Posláním US-CERT je zlepšit národní postavení v oblasti kyber bezpečnosti, koordinovat sdílení informací a proaktivní řízení kyber rizik ohrožující USA při ochraně ústavních práv Američanů. Vizí US-CERT je stát se důvěryhodným globálním vůdcem v oblasti kyber bezpečnosti – spolupracující, agilní a pružný v komplexním prostředí.

CSIRT týmy menších států pochopitelně nemohou aspirovat na vedoucí úlohu v oblasti IT bezpečnosti, ale řada činností by se měla překrývat. Činnost jednotlivých týmů lze zkoumat pomocí statistik a analýzou činnosti na domácích stránkách týmů. Rozložení řešených bezpečnostních incidentů týmu CSIRT.CZ je znázorněn na obr. 8.1.



Obrázek 8.1: Typové rozložení řešení bezpečnostních incidentů týmu CSIRT.CZ v letech 2008-2011 (převzato z [45])

Většinu bezpečnostních incidentů připadá na detekované průniky do sítí následované phishingovými útoky a napadení různými typy malware. **CSIRT** tým pracuje tak, že upozorní správce zdrojové sítě útoku a pomůže (informační podpora) případně s identifikací problému.



Postavení CSIRT.CZ

Národní tým CSIRT.CZ je zajišťován nestátní organizací - může se jednat o soukromou firmu, sdružení osob apod. Jelikož národní CSIRT tým může být pouze jeden, výběr organizace, která jeho provoz zajistí probíhá výběrovým řízením. To je celkem paradoxní situace, protože aby byl CSIRT tým funkční, musí spolupracovat se zahraničím. Aby mohl spolupracovat se zahraničím, musí být sdružen v některém mezinárodním uskupení takových týmů. Paradox spočívá v tom, že provoz CSIRT týmu je brán jako služba - smlouva se uzavírá proto na dobu určitou a poté se soutěž opakuje.

Teoreticky proto můžeme mít každých 5 let jiný národní CSIRT tým, který nemusí být funkční, neboť nebude mít uzavřenou spolupráci se zahraničím...

CERT.GOV.PL [44] kromě standardní minimální úrovně služeb (jak je realizována např. týmem CSIRT.CZ), poskytuje ještě aktuální informace, doporučené nástroje, doporučení na konfigurace systémů a také zpracovávání bezpečnostních incidentů ARAKIS-GOV [43].

CSIRT.SK jako slovenský národní **CSIRT** tým byl akreditován teprve v polovině roku 2011, přesto poskytuje oznámení a varování, základní návody a doporučení pro konfiguraci a zabezpečení IT aktiv.

Jako etalon toho, jaký typ informací může poskytovat CERT, lze použít US-CERT [67]. Tento národní tým poskytuje údaje o hrozbách a zranitelnostech, aktualizacích, ale také aktivitách a dalších zdrojích a to v úpravě pro techniky (IT odborníky), netechniky (domácí a podnikové uživatele), státní správu a samostatně řeší také bezpečnost řídicích systémů.

Bez ohledu na to, jaké přesné úkoly **CSIRT** tým dostává od svého zřizovatele, existují některé úkoly, které mají všechny týmy a to především sloužit jako místo pro reportování bezpečnostních incidentů a být nápomocni při jejich řešení. K tomuto účelu je ale vyžadováno, aby jednotlivé **CSIRT**

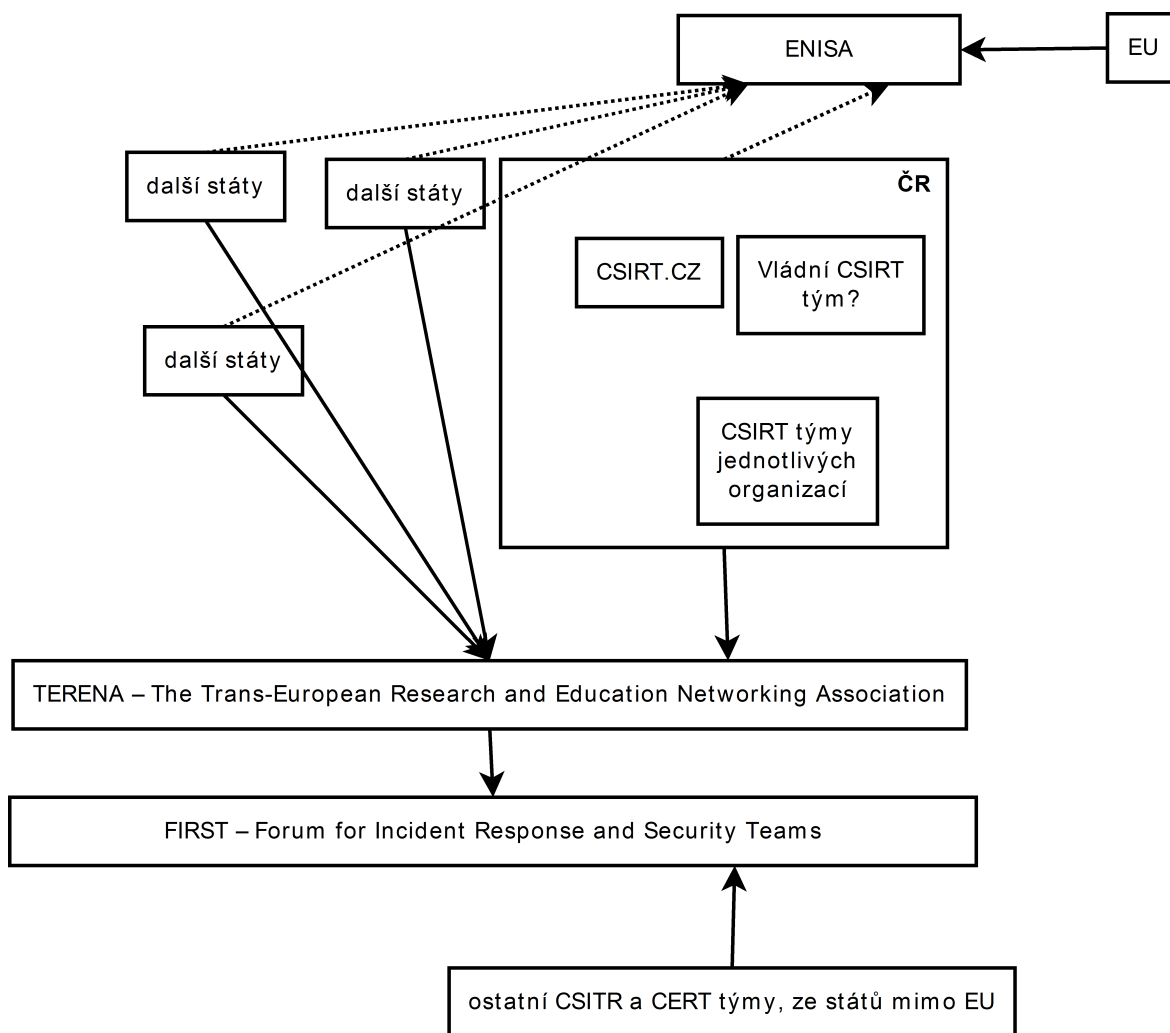
byly certifikovány, tedy aby někdo ručil za to, že **CSIRT** tým je skutečně určen pro řešení takových problémů, a zájemce o využití služeb tak získal určitou jistotu, že důvěrné informace o bezpečnostním incidentu nepadnou do nepovolaných rukou.

Pro tyto účely se uznávané **CSIRT** týmy sdružují do různých mezinárodních uskupení. Na úrovni EU funguje **ENISA** [?]. **ENISA** jako instituce je poradním orgánem Evropské komise v oblasti IT bezpečnosti, zabývá se také organizací konferencí, seminářů, školení a cvičení pro národní **CSIRT** týmy.

CSIRT týmy samotné se v Evropě sdružují do organizace **The Trans-European Research and Education Networking (TERENA)** [?] jako platformy zprostředkovávající výměnu bezpečnostně orientovaných informací, školení apod. mezi **CSIRT** týmy.

Samotná registrace je realizována pomocí mezinárodní organizace **Forum for Incident Response and Security Teams (FIRST)** [?]. Pro registraci je nutné, aby se za uchazeče o registraci zaručil nějaký již uznávaný člen fóra. Tímto způsobem se zajišťuje jeden z pilířů spolupráce – dobrá komunikace na mezinárodní úrovni. **CSIRT** tým tedy musí nejprve navázat „neformální“ spolupráci s jinými **CSIRT** týmy a teprve poté se může ucházet o registraci v rámci **FIRST**.

Schematicky si můžeme spolupráci na mezinárodní úrovni představit podobně jako na obr. 8.2.



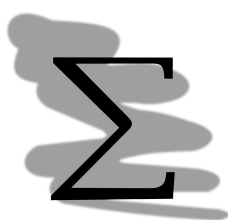
Obrázek 8.2: CSIRT týmy – mezinárodní spolupráce



Národní vs vládní CSIRT tým

Národní CSIRT tým slouží pro řešení bezpečnostních incidentů na národní úrovni. Jeho uživateli tak mohou být soukromníci, firmy, ale také slouží jako kontaktní místo pro zahraniční CSIRT týmy, které řeší bezpečnostní incidenty s přesahem do ČR.

Funkce vládního týmu je ale definována mnohem úžeji. Slouží pro řešení bezpečnostních incidentů ve státní správě popř. samosprávě. Vládní CSIRT tým je obvykle provozován státem a jako takový má ve veřejném sektoru mnohem větší pravomoci než národní CSIRT tým vůči sektoru privátnímu.



Shrnutí

Problematika kybernetické bezpečnosti je z hlediska legislativního řešení relativně mladá. Zákon o kybernetické bezpečnosti vešel v platnost teprve počátkem roku 2015. Zakotvuje postavení národního (CSIRT.CZ) a vládního (GovCSIRT.CZ) CSIRT týmu. Vládní tým je provozován Národním centrem pro kybernetickou bezpečnost (pod NBÚ).

Zákon dává možnosti NBÚ v případě ohrožení kritické informační infrastruktury popř. významných informačních systémů nařizovat opatření reaktivní a ochranná. V případě, že ohrožení přesáhne určitou mez, může být vyhlášen stav kybernetického nebezpečí dávající do rukou NBÚ možnost donutit ke spolupráci širší okruh zájmových osob. Tento stav může být vyhlášen maximálně na dobu jednoho měsíce.



Kontrolní otázky

1. Jaké jsou rozdíly v pravomocích národního a vládního CSIRT týmu?
2. Co rozumíme pojmem významný informační systém?
3. Co rozumíme pojmem významná síť?



Odpovědi

1. Národní CSIRT tým je primárně zaměřen na informování a spolupráci v oblasti běžných bezpečnostních incidentů, které nejsou zaměřeny např. na kritickou infrastrukturu. Národní CSIRT tým také nemá žádné faktické pravomoci.
2. Významným IS rozumíme, takové IS, bez kterých by veřejná správa nemohla vykonávat svou funkci (ve smyslu povinností uložených platnou legislativou).
3. Významnou sítí se rozumí takové sítě, které zajišťují připojení (datové, telekomunikace obecně) do zahraničí.

Kapitola 9

Rychlé informace



Náhled kapitoly

Problematikou rychlých informací vybočujeme lehce z oblasti informačních technologií a dostáváme se do mnohem obecnější oblasti. Rychlými informacemi máme na mysli použití barev, piktogramů apod., které na první pohled dávají informaci, která člověka nacházejícího se v dané oblasti nutná.

Po přečtení kapitoly budete

Vědět

1. jakým barvy se používají pro označování prostor a proč
2. proč jsou rychlé informace důležité
3. co všechno lze ještě zařadit mezi rychlé informace

Znát

1. vzhled nejběžnějších typů značek



Čas pro studium

Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

9.1 Úvod

Koncepce rychlých informací vychází z toho, jakým způsobem člověk vnímá barvy, tvary a zvuky. Jedná se vlastně o přímé dědictví od našich zvířecích předků. Všechny tyto vjemy jsou vyhodnocovány jako signály o různé intenzitě. Na našich pudech popřípadě výcviku záleží, jak na tyto signály budeme reagovat.

Tyto vjemy lze rozdělit do několika kategorií podle smyslů, které je přijímají:

1. hmat
2. čich
3. sluch
4. zrak
5. chuť

Z hlediska rychlých informací, tedy alespoň jejich formalizované podoby bychom mohli takřka vyloučit čich a chuť.

Ačkoliv ani ten případ s plynem není úplně bez rychlých informací. Do zemního plynu se schválně z důvodu jednoduchosti detekce přimíchávají chemická látka thiol, jelikož zemní plyn samotný je bez

**Přestávka****Poslední slova**

... hele cítím plyn ...

... jo, já ho taky cítím ... počkej, škrtnu zápalkou, ať vidíme, odkud to jde ...

nebo

Vidíš jak je ta smaženice dobrá? Ale je pravda, že ty žampiony vypadaly divně

...

chuti a zápachu. Právě thiol zajišťuje typickou „vůni“ zemního plynu. Toto by že se dalo považovat za jistý druh rychlé informace.

Zbývá nám tedy zrak, sluch a hmat. Hmat se může zdát být podobně nepoužitelný jako chuť a čich, ale nevidomí nebo slabozrací spoluobčané jsou nuceni na něj spoléhat. Do této kategorie můžeme zařadit např. speciální dlažbu s výstupky označující, že se nevidomý nachází na chodníku, zvukovou signalizaci na přechodu pro chodce a podobně.

Z hlediska rychlých informací nás především bude zajímat zrak a sluch. V případě zraku je to pak zejména schopnost barevného vidění.

Například červená – barva krve, byla signálem, že na daném místě se něco a je třeba dávat větší pozor popřípadě se místu kompletně vyhnout.

Z tohoto hlediska:

Červená barva – nebezpečná oblast

Žlutá barva – pozor, všimni si mě

Zelená barva – bezpečí, následuj mě a nic se ti nestane

9.2 Nařízení vlády 11/2002 Sb.

Pocity člověka z barev, které mohou být do značné míry individuální, nelze brát bez další normalizace. Právní předpis, který upravuje vzhled, umístění značek je nařízení vlády 11/2002 Sb. [19]. Barvy a jejich významy viz. tab. 9.1.

Tabulka 9.1: Tabulka barev značek a světelných signálů (převzato z [19])

Barva	Význam nebo účel	Pokyny a informace
červená	Značka zákazu	Nebezpečné chování
	Signalizace nebezpečí	Zastavit přerušit práci bezpečnostní pojistka opustit prostor
	Věcné prostředky PO a bezpečnostně požární zařízení	Označení a umístění
žlutá	Značka výstrahy	Buď opatrný
oranžová		Připrav se
zelenožlutá		Ověř si
modrá	Značka příkazu	Určité chování nebo postup Použij OOPP
zelená	Značka nouzového východu	Označení dveří, východů, cest,
	Značka první pomoci	zařízení, vybavení
	Bezpečí	Návrat k běžnému stavu

V praxi by například značení nějaké překážky (schod, kanálek upevněný na zemi pro vedení elektrické sítě apod.) vypadal podobně jako na obr. 9.1.

Značky zákazu jsou vyvedeny v kruhovém tvaru s červeným okrajem a červeně přeškrtnutou čírností, která je zakázána, viz například obr. 9.2.

Značky výstrahy jsou zpracovány v trojúhelníkovém tvaru se žlutým pozadím, černým okrajem se znázorněným symbolem nebezpečí, na které si takto značeném prostoru máme dát pozor (viz obr. 9.3).

Při použití barev černé a žluté



Při použití barev červené a bílé



Obrázek 9.1: Příklady použití barev pro značení



Kouření zakázáno

Zákaz výskytu
otevřeného ohně

Průchod pro pěší
zakázán

Obrázek 9.2: Příklady značek zákazu

Značky příkazu jsou kulovitého tvaru s modrým pozadím a graficky znázorněným co musí člověk udělat pro svou bezpečnost (viz obr. 9.4).

Informativní značky slouží pro označení únikových cest a nouzových východů nebo míst první pomoci a zařízení pro přivolání první pomoci (viz obr. 9.5).

Uvedené značky nejsou kompletním výčtem používaných značek, pouze jejich reprezentativním výběrem. Kompletní výčet je obsažen v přílohách nařízení vlády 11/2002 Sb. [19].

Bezpečnost ovšem není jediná oblast, kde se normalizované značení používá. Například protokol PECA (protokol k Evropské dohodě o posuzování shody a akceptaci průmyslových výrobků) ukládá výrobcům dávat na své výrobky značku CE jako rychlou informaci zákazníkovi, že daný výrobek splňuje základní požadavky nařízení vlády (viz. obr. 9.6).

Různých druhů značení je pravděpodobně stejně jako různých druhů lidské činnosti. Do kategorie rychlých informací bychom proto mohli zařadit například i značku Bio – označující ekologicky šetrně vyrobené potravinářské výrobky, nebo také punc vyražený na šperku pro rychlé určení drahého kovu, ze kterého byl vyroben.

Sluch je pro člověka stejně důležitý nebo možná důležitější smysl než zrak. Ucho jako sluchový orgán člověka je schopno ze zachycených zvuků zjistit směr odkud zvuk vychází a přibližnou vzdálenost zdroje zvuku. Člověk je také schopen si ve zmeti zdrojů vybrat jeden a ostatní zdroje „odfiltrovat“.

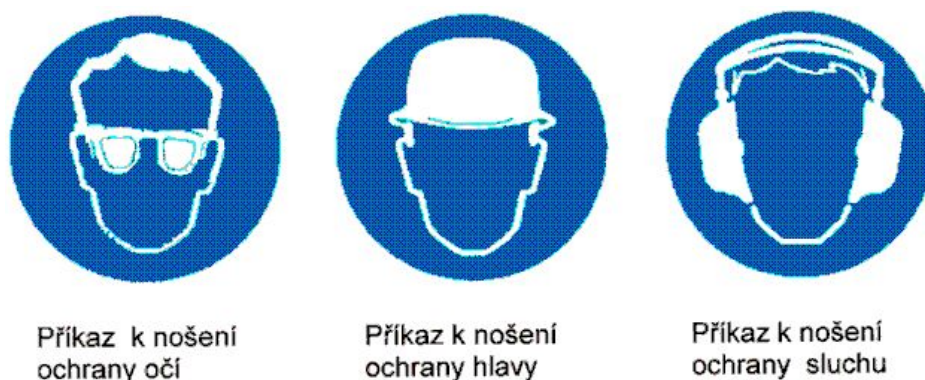
Zvukové signály jsou velmi často využívány pro poskytování rychlých informací. Klakson automobilu má jediný účel – říct tady jsem, dej na mě pozor. Mezi zvukové rychlé informace lze nepochybně zařadit například i sirény CO.

Je vědecky dokázáno, že člověk věnuje větší pozornost kombinovaným vjemům, tedy takovým vjemům, které zaznamenává více než jeden smysl. Na stejném principu je založeno i učení – je rozdíl, pokud si látku pouze čteme, a nebo zároveň k ní máme puštěnu audio nahrávku (např. výuka jazyků).

Tohoto principu využívají například i automobily záchranných služeb, které mají zároveň spuštěn maják i sirénu.



Obrázek 9.3: Příklady značek výstrahy



Obrázek 9.4: Příklady značek příkazu

Uvedené principy mají nepopíratelný význam pro návrh uživatelského rozhraní specializovaných systém, jejichž obsluha musí rychle reagovat na nějakou událost. Typicky se v průmyslu může jednat o vizualizace technologických procesů. Obsluha má k dispozici grafický výstup na obrazovku, který pro člověka přijatelným způsobem zobrazuje ukazatele sledovaného procesu. Přitom se neočekává, že by obsluha věnovala příliš pozornosti jednotlivým ukazatelům – sleduje pouze, zda se „nerozsvítila“ červená kontrolka signalizující, že něco není v pořádku.

V tomto okamžiku pracovník teprve studuje jednotlivé ukazatele a zjistí příčinu problému. Včasná indikace problému zabrání finančním ztrátám způsobeným například výpadky technologie apod.

9.3 Nebezpečné látky – rychlé informace

Jako základní identifikátory slouží tři položky a to *CAS číslo*, *ES číslo* a *indexové číslo*. *Indexové číslo* se udává ve tvaru **ABC-RST-VW-Y**, kde číslo ABC udává atomové číslo prvku charakterizujícího látku. Číslo RST představuje pořadové číslo v sérii ABC a VW označuje formu v jaké je látka dodávána na trh. Poslední číslo Y plní kontrolní funkci – jedná se o kontrolní součet, vypočítaný metodou ISBN.

ES číslo neboli tzv. *Einecs číslo*, se přiděluje látkám, které jsou na seznamech látek, který v ČR ze zákona udržuje Ministerstvo životního prostředí. Konkrétně se jedná o tři rejstříky: seznam nových látek ELINCS (400-010-9 a vyšší), seznam látek, které nadále nejsou považovány za polymery NLP (500-001-0) a seznam obchodovatelných látek (200-01-8). ES číslo je přitom přidělováno látce bez ohledu na to zda je hydratovaná nebo ne.

Z předchozích odstavců vyplývá, že ani ES ani indexové číslo nemohou zajistit jednoznačnou identifikaci látky, lze je však použít lépe než např. *UN kód*. Látku jednoznačně identifikuje *CAS číslo*.

CAS číslo je unikátní číselný identifikátor chemických sloučenin. CAS čísla jsou přidělována divizí American Chemical Society, která se nazývá Chemical Abstract Service, s cílem jednoznačně identifikovat kteroukoliv chemickou látku, která kdy byla popsána. Počátkem prosince 2005 takto bylo přiděleno více než 27 milionů čísel.



Únikový východ (vlevo)



Místo první pomoci



Nosítka

Obrázek 9.5: Příklady informativních značek

CAS číslo obsahuje tři části oddělené pomlčkou. První část se může skládat až z šesti číslic, druhá obsahuje dvě číslice a konečně třetí část obsahuje pouze jedinou číslici a slouží jako kontrolní součet.

UN číslo je čtyřciferný identifikátor nebezpečných látek a zboží v souvislosti s mezinárodní přepravou. UN čísla v intervalu 0001 – 3500 jsou přidělována výborem expertů pro přepravu nebezpečných materiálů při OSN (United Nations Committee of Experts on Transport of Dangerous Goods). Seznam UN čísel tyto experti zveřejnili v tzv. Oranžové knize (Recommendations on the Transportation of Dangerous Goods).

Kromě UN čísel se používají také tzv. NA čísla (North America (NA)), která jsou také známa pod označením DOT čísla. NA čísla přiděluje ministerstvo dopravy USA (Department of Transportation (DOT)). NA čísla jsou kompatibilní s UN čísly, v tom smyslu, že NA a UN čísla jsou totožná s výjimkou některých látek, které nemají UN číslo, ale mají NA číslo.

Identifikační číslo nebezpečnosti (dříve označováno jako tzv. Kemler kód), slouží k rychlému určení nebezpečí v případě havárie nebo požáru nebezpečných látek.

Tzv. HAZCHEM kód se používá zejména ve Velké Británii, ale pro jeho snadnou interpretovatelnost se postupně rozšířil i do dalších zemí. HAZCHEM kód je tvořen trojicí čísel udávajících hasivo – ochranu – evakuaci.

Značení prostřednictvím Diamantu prosadila v USA National Fire Protection Association (NFPA), vzhledem k tomu, že se jedná o jednoduchý a přitom spoustu informací poskytující systém, prosadil



Obrázek 9.6: Značka CE dle protokolu PECA

ID	Tisková sestava	CAS číslo	ES číslo	Indexové číslo
		108-24-7	203-564-8	607-008-00-9
Název				
Acetanhydrid				
Identifikační číslo nebezpečnosti		83	Hasivo	Ochrana Evakuace
UNKod		1715	HAZCHEM kód: 2	P

Obrázek 9.7: Příklad Identifikátorů nebezpečné látky – převzato z databáze Nebezpečné látky 2005 [72]

se tento způsob značení i mimo území USA.

Jednotlivé kvadranty Diamantu mají přitom následující význam:

1. modrá – zdraví
2. červená – nebezpečí požáru
3. žlutá – reaktivita
4. bílá – speciální ustanovení

Do každého kvadrantu s výjimkou bílého se přiřazuje číselné vyjádření nebezpečnosti, přičemž čím vyšší číslo, tím vyšší nebezpečí (ohrožení zdraví, požáru, ...).

V bílém kvadrantu jsou pak obsažena speciální ustanovení označovaná písmeny. Přeskrtnuté W (z technických důvodů v databázi pouze W) např. znamená zákaz použití vody pro sanaci látky.

ADR je Mezinárodní úmluva o pravidlech přepravy po silnici a *RID* je její obdoba pro železnici. Tato smlouva upravuje značení vybraných nebezpečných látek pro účely jejich přepravy.

Definuje tzv. *třídy nebezpečnosti*, které jsou vizualizovány na přepravních kontejnerech, cisternách apod. prostřednictvím nálepek, viz. obr. 9.9.

Legislativa u nás i ve světě také upravuje oblast označování látek výstražných symbolů a R a S větami.

R věty slouží pro bližší specifikaci nebezpečí, které představuje nebezpečná látka (R = risk). Pro bližší specifikaci ochranných opatření se používají tzv. *S věty* (S = safety). R a S věty jsou tvořeny označením R resp. S a číslem. Ke každé kombinaci označení a čísla je přiřazen výklad, např. R1 – výbušný v suchém stavu. Existují i tzv. kombinované R a S věty, např. R14/15 – prudce reaguje s vodou za uvolňování extrémně hořlavých plynů.

R2 - Nebezpečí výbuchu při úderu, tření, ohni nebo působením jiných zdrojů zapálení.

S2 - Uchovávejte mimo dosah dětí.

Obrázek 9.8: Příklad Diamantu s vysvětlením významu – převzato z databáze Nebezpečné látky 2005 [72]

S9 - Uchovávejte obal na dobře větraném místě.

V souvislosti s postupným náběhem chemické legislativy REACH se budou zavádět různé změny v pro specifikaci nebezpečí a proto R a S věty budou do roku 2015 kompletně nahrazeny *H* (*H* = Hazard) a *P* (*P* = Protection) *věťami*, kterých je více a jsou jiného znění, svým základním smyslem jsou ovšem stejné (*R* -> *H*, *S* -> *P*)¹.

Výstražné symboly jsou označeny písmenem, slovním popisem vlastnosti látky, která je považována za nebezpečnou a jejich grafickým znázorněním, např. *E* – výbušný. Platné výstražné symboly jsou zobrazeny na obr. 9.10.

Změně bude podroben i systém označování výstražných symbolů, viz. obr. 9.11. Tyto symboly budou univerzální a budou celosvětově platné celosvětově dohoda GHS, EU implementace je známa pod zkratkou CLP).

Systém rychlých informací může být součástí specializovaných informačních systémů např. pro záchranáře při zásahu pro zjištění vlivu uniklé chemické látky na zdraví apod.

¹ačkoliv základní filozofie zůstává stejná, samotné znění jednotlivých vět se mění



Obrázek 9.9: Třídy nebezpečnosti



Obrázek 9.10: Výstražné symboly



Obrázek 9.11: Výstražné symboly dle legislativy CLP

Shrnutí

Z hlediska legislativy jsou rychlé informace řešeny např.:

1. nařízením vlády 11/2002 Sb.
2. Mezinárodní úmluvou o přepravě nebezpečných látek ADR, RID
3. a dalšími právními normami a mezinárodními úmluvami (např. dohoda PECA)

Nařízení vlády rozlišuje čtyři druhy značek

1. zákazu
2. výstrahy
3. příkazu
4. informativní

Jednotlivé značky se liší tvarem a barvami.

Pro identifikaci nebezpečných látek lze využít UN, ES, CAS, indexová čísla, přitom pouze CAS číslo poskytuje jednoznačnou identifikaci nebezpečné látky.

Z hlediska bezpečnosti jsou důležité vlastnosti a způsoby ochrany před účinky nebezpečných látek identifikovány pomocí R a S vět, identifikačního čísla bezpečnosti, výstražných symbolů a nálepek. Legislativa REACH a především CLP zavádí vlastní systém výstražných symbolů a používá H a P věty pro specifikaci ohrožení látkami a možností ochrany před jejich negativními účinky.

Kontrolní otázky

1. Jaké jsou barvy nebezpečí, výstrahy a bezpečí?
2. Co jsou to R a S věty?
3. Jaké informace poskytuje Diamant?
4. Jak se liší UN a DOT čísla?
5. Jaké rychlé informace mohou být použity pro identifikaci škodlivých vlastností nebezpečných látek?



Správné odpovědi


1. nebezpečí – červená, výstrahy - žlutá, bezpečí – zelená
2. Identifikují riziko nebezpečné látky, S věty identifikují prostředky ochrany před účinky nebezpečné látky.
3. Ohrožení zdraví, nebezpečí požáru, reaktivita a speciální ustanovení (např. zákaz požití vody).
4. UN přijatá OSN, DOT přijatá Ministerstvem dopravy USA a obsahují UN čísla a některá další čísla pro další látky.
5. R nebo H věty, Diamant, HAZCHEM, identifikační číslo nebezpečnosti, výstražné symboly, třídy nebezpečnosti.



Test

1. Které z následujících čísel jednoznačně identifikuje nebezpečnou látku
 - (a) CAS
 - (b) ES
 - (c) UN



2.  je značka:
 - (a) zákazu
 - (b) výstrahy
 - (c) příkazu
3. Výstražné symboly obsahují
 - (a) Obrázek
 - (b) Písmeno nebezpečí, obrázek
 - (c) Písmeno nebezpečí, obrázek, popis rizika
4. Diamant obsahuje barvy
 - (a) Bílou, žlutou červenou, modrou,
 - (b) Bílou, modrou, černou, červenou
 - (c) Žlutou, červenou, fialovou, bílou
5. Číslo 0115 může být číslem
 - (a) CAS
 - (b) ES
 - (c) UN



Správné odpovědi

1. a), 2. b), 3. b), 4. a), 5. c)

Kapitola 10

Budoucnost výpočetní techniky aneb počítáme netradičně



Náhled kapitoly

V této kapitole se seznámíte s možnou budoucností IT. Budeme hovořit zejména o pokročilých výpočetních systémech na bázi DNA, kvantových počítačů nebo třeba neuročipů.

Po přečtení kapitoly budete

Vědět

1. co znamenají pojmy DNA počítač, kvantový počítač, neuro-procesor a proč se o nich má vůbec smysl bavit



Čas pro studium

Na prostudování této kapitoly budete potřebovat přibližně 60 minut.

10.1 DNA počítače

Výkladem o možné budoucnosti informačních technologií zakončíme exkurzi do světa informatiky. V kapitole 1 jsme si něco pověděli o informačním nárůstu a jeho limitujících faktorech. Jedním z těchto faktorů je hranice technologických možností. Z dnešního pohledu se zdá, že touto hranicí bude miniaturizace tranzistorů v procesorech. Podle některých odhadů může být této hranice dosaženo někdy za 20 možná 30 let, tedy s vysokou pravděpodobností ještě za našich životů.

Vyvinutí a nasazení úplně nových technologií může být novým impulsem, který odstartuje nové kolo inovací. O některých „nadějných“ technologiích se dozvíte něco v následujících odstavcích.

Začneme DNA počítači. Při výzkumu v této oblasti se vychází z toho, že v živých organismech slouží ke kódování informací nukleové kyseliny. Vlákno nukleové kyseliny se skládá z několika složek, z našeho hlediska nás však zajímá především jedna a to je tzv. dusíkatá báze. U DNA jde o adenin, guanin, cytosin a thymin, u RNA je thymin nahrazen uracilem. Jednotlivé dusíkaté báze dále budeme označovat jejich počátečními písmeny.

Některé z těchto dusíkatých bází jsou vůči sobě komplementární, tzn. že se mezi nimi vytváří pevná vazba:

A A G
T U C

Atraktivita použití DNA počítačů spočívá v masivním paralelismu při řešení zadané úlohy. Průkopníkem v této oblasti profesor Leopard Aleman, který pomocí DNA počítače řešil celkem dvě úlohy. V roce 1994 úspěšně vyřešil problém obchodního cestujícího a v nedávné době i problém výběru automobilu.

Problém obchodního cestujícího je následující: Obchodní cestující má předem stanovená města, která během své cesty navštíví, tuto návštěvu ale chce optimalizovat tak, aby přitom urazil co možná nejmenší vzdálenost.

Druhý Alemanův experiment se blíží svým zadáním běžnému lidskému myšlení. Mějme autobazar a zákazníka, který chce koupit auto. Zákazník má představu co chce přesně koupit, ovšem tato představa je velmi obtížně zpracovatelná pomocí standardních výpočetních prostředků: zákazník by chtěl Cadillac nebo auto s odklápěcí střechou nebo auto červené barvy. Pokud by se jednalo o Cadillac, musel by mít čtyři sedadla nebo uzamykatelný uzávěr k nádrži. A nakonec pokud by se jednalo o auto s odklápěcí střechou, nemělo by se jednat o Cadillac nebo by měl mít dvě sedadla. Zákazník ze sebe vychrlí ještě dalších 21 podmínek, prodejce si teď musí sednout a porovnat tyto podmínky s 1 milionem aut, která má k dispozici a vybrat z nich auto nebo auta, která podmínkám nejlépe vyhovují.

Pro člověka je takový problém neřešitelný. V případě řešení pomocí DNA počítače, by se vytvořili pomocí nukleových bází reprezentanti jednotlivých aut i požadavků zákazníka. Zajistí se, aby konce těchto samostatných vláken byly komplementární dle požadavků zákazníka a aby všichni reprezentanti byli zastoupeni v roztoku dostatečně-krát. Potom se vše pečlivě promíchá, aby se komplementární báze spojily, a výsledek se odfiltruje magnetismem, elektrolyzou apod.

Tedy požadovaný výsledek můžeme dostat, ale nemusíme, je pouze pravděpodobné, že díky tomu že jednotlivé komponenty byly v roztoku redundantně, dostaneme požadovaný výsledek. V tom spočívá výše zmíněný masivní paralelismus.

Zde představený počítač je jednoúčelový a jednosměrný – musí se připravit vstupní látky a ty se během výpočtu znehodnotí. Po ukončení výpočtu se musí tedy všechny látky zahodit a začít znovu.

Přesto je zajímavé zamyslet se nad složitostí problémů řešitelných tímto způsobem a srovnat jej se způsobem klasickým. Oba řešené problémy se řadí do kategorie problému NP- kompletních. Takové problémy rostou kvadratickou řadou s počtem prvků. Představte si složitost řešení problému obchodního cestujícího se sedmi městy a dvaceti městy. Pro paralelní počítače, kam se řadí i DNA počítače, se složitost problému zvyšuje pouze lineárně.

V Izraeli se pracuje na DNA počítači nové generace, který by dle požadavků byl schopen spojovat a rozpojovat jednotlivé báze tak aby k tomuto problému nedošlo, tento výzkum je však ještě v relativně raném stádiu.

Praktického nasazení DNA počítačů se nejspíše v příštích 20-ti letech nedočkáme.

10.2 Kvantové počítače

Kvantové počítače byly teoreticky odvozeny z kvantové fyziky někdy během 80. let minulého století. Se vznikem teoretických základů je spojováno jméno Richarda Feynmana. Další impuls pro výzkum se staly práce Petera Shorta z Bellových laboratoří, který navrhl první algoritmu, který takový by takový počítač mohl zpracovávat. Algoritmus řešil faktorizaci velkých čísel na prvočísla. Prakticky se to samozřejmě vzhledem k neexistenci takového počítače nikdy nevyzkoušelo.

Kvantové počítače pracují na principu kvantové fyziky. Ta mimo jiné říká, že jakékoliv měření vyvolává v prostoru kvantových jevů nevratné změny. Z tohoto důvodu kvantový počítač musí být úplně izolován od okolí, které by ho jinak ovlivnilo.

Podle kvantové fyziky totiž, dokud se na elektron nepodíváme, nevíme, kde se přesně nachází, ale což je závažnější, v určitém smyslu se nachází na více místech současně. V okamžiku, kdy se na něj podíváme, však tento zvláštní stav pomine a elektron uvidíme pouze na jednom z těchto míst.

Abychom se to shrnuli, klasický počítač pracuje se stavem se dvěma hodnotami 0/1. Přitom stav může mít pouze jednu hodnotu. Kvantová mechanika umožňuje elektronu, aby zaujal speciální stav, kterému se říká lineární superpozice obou stavů, který charakterizuje tzv. vlnová funkce. Zatímco tedy u klasických počítačů pracujeme s bity, u kvantových počítačů pracujeme s kvantovými bity neboli qbity. Díky tomu může celá soustava atomů ve všech 2^N stavech současně, kde N je počet bitů. Je tedy možné najednou prozkoumat velké množství možností.

V praxi je kvantový počítač tvořen částicemi, připraví se do výchozí podoby a nechá se pracovat – v okamžiku kdy se na něj podíváme, dojde ke kolapsu systému, po kterém jsme schopni odečíst výsledek, ale počítač není schopen dál pracovat, musí se „opravit“ do původního stavu.

V současné době se s kvantovými počítači experimentuje. Před několika lety oznámila IBM úspěch v podobě sestavení 5-ti qbitového počítače, což je samozřejmě pro praktické nasazení pořád málo.

V oblasti aplikace kvantové mechaniky obecně došlo k výraznějším pokrokům a dochází k nasazení tzv. kvantové kryptografie, která je svou fyzikální podstatou, alespoň dle současného stavu poznání, naprosto bezpečná.

Celkově se nedá očekávat, že by k výraznějšímu průlomů v oblasti kvantových počítačů došlo během příštích 10 let.

10.3 Neuroprocesory

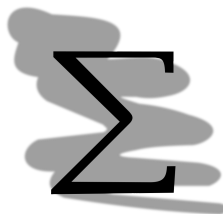
Lidský mozek resp. mozek obecně má úžasné vlastnosti. Umožňuje totiž svému nositeli zvládat nepřehledné množství často nepředvídatelných událostí a to vše v reálném čase. Například i podprůměrně inteligentní člověk se zvládne naučit řídit auto, ponechme stranou jak dobře podstatný je fakt že se to naučí. Uvědomme si, že toto dnes žádný počítač nezvládne.

Například soutěž před několika měsíci, v rámci které měla počítačem řízená vozidla překonat trať dlouhou asi 15 km, skončila naprostým krachem, kdy nejlépe jedoucí vozidlo se zastavilo na 1,5 km.

Z těchto důvodů se vážně uvažuje o možnosti propojit klasický čip a mozkovou tkáň resp. neuronovou síť mozku. V běžném mozku dochází k přenosu elektrických impulsů, vzruchů po tzv. axonech, které spojují jednotlivé neurony do sítě. Na základě zkušeností, učení dojde k posílení nebo naopak utlumení tohoto vzruchu. Spolupráce klasického procesoru a neuronové sítě pak spočívá ve speciální povrchové úpravě čipu, který je schopen takové impulsy vysílat i přijímat.

V současné době se s touto technologií experimentuje zejména v SRN, kdy pro experimenty jsou využívány neurony slimáků zejména vhodné pro svou velkou velikost, která usnadňuje manipulaci. Současné pokusy jsou schopny úspěšně signál odeslat z křemíkové části vzruch, ten převezme biologická část a vrátí jej zpět na čip.

Ačkoliv se podobně jako u DNA a kvantových počítačů popisovaných v této kapitole jedná o velmi nadějnou technologii, zbývá zde ještě mnoho nevyřešených problémů, které pravděpodobně v minimálně příštích deseti letech nedovolí nasadit ji do praxe.



Shrnutí

Některé typy problémů, jsou pomocí současné výpočetní techniky špatně řešitelné, jedná se zejména o tzv. N:P kompletní problémy – třída problémů, jejichž složitost roste exponenciálně. Pro řešení takových problémů bude nutné vyvinout buď nové algoritmy řešení, nebo nový hardware.

Mezi nadějně počiny v oblasti hardware řadíme DNA počítače, kvantové počítače a neuroprocesory.

DNA počítače využívají tzv. masivního paralelismu, kterým rozumíme fakt, že jednotliví reprezentanti částí problému jsou v DNA počítači přítomni mnohokrát. Samotný výpočet tak probíhá najednou smísením všech těchto reprezentantů a následným filtrováním výsledků.

Kvantové počítače využívají pro výpočty kvantové mechaniky, která na rozdíl od klasické výpočetní techniky nepočítá s bity a qbity. V klasické mechanice stav nastane nebo nenastane (0/1), v kvantové mechanice funguje (0/1/0 a 1).

Konečně neuroprocesory spojují klasické čipy s mozkovou tkání. Cílem je propojit výhody klasické výpočetní techniky a schopnosti uvažování živých organismů, především jejich schopnost abstrakce a kreativního vyhodnocování velmi složitých problémů.

Všechny výše uvedené technologie, jsou bohužel zatím ve stádiu výzkumu a komerčně pravděpodobně nebudou nasazeny příštích deseti až dvaceti letech.



Kontrolní otázky

1. Co jsou to N:P kompletní problémy?
2. Co rozumíme pojmem masivní paralelismus DNA počítačů?
3. Co je to neuroprocesor?
4. Proč říkáme, že kvantový počítač pracuje jako černá skříňka?
5. S jakými jednotkami pracuje kvantový počítač?



Správné odpovědi

1. Jsou to problémy, jejichž složitost roste minimálně exponenciálně.
2. Schopnost DNA počítačů provést výpočet najednou paralelně pro velké množství reprezentantů prvků problému.
3. Speciálně upravený procesor napojený na mozkovou tkáň s cílem vyměňovat si informace mezi čipem a tkání prostřednictvím elektrických impulsů.
4. Protože když se do ní podíváme, zhroutí se vlnová funkce a výpočet havaruje.
5. qbit



Test

1. DNA se skládá z následujících dusíkatých bází:
 - (a) A, T, U
 - (b) G, T, U
 - (c) A, T, G
2. DNA počítače jsou
 - (a) Jednopróblémové, jednorázové
 - (b) Vícepróblémové, jednorázové
 - (c) Jednopróblémové, stále použitelné
3. Speciálnímu případu nerozhodného stavu říkáme
 - (a) Super pozice
 - (b) Qbit
 - (c) Vlnová funkce
4. DNA a kvantové počítače jsou
 - (a) Běžně používány
 - (b) Občas používány
 - (c) Ve fázi vývoje
5. Neuroprocesory se úspěšně testovaly na
 - (a) Pijavicích
 - (b) Slimácích
 - (c) Lidech



Správné odpovědi

1. c), 2. a), 3. a), 4. c), 5. a) b)

Kapitola 11

Telekomunikace



Náhled kapitoly

V této kapitole se seznámíte s legislativním rámcem telekomunikací v České Republice a EU.

Po přečtení kapitoly budete

Vědět

1. Legislativní rámec telekomunikací v ČR a EU
2. Co znamenají pojmy ex ante, dominantní postavení, univerzální služba



Čas pro studium

Na prostudování této kapitoly budete potřebovat přibližně 60 minut.

11.1 Legislativní rámec EU

2002/21/ES – rámcová směrnice

Základní směrnici v oblasti telekomunikací EU je směrnice **European Parliament (EP)** a rady 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).

Vzhledem ke konvergenci telekomunikací, médií a informačních technologií (IT) vyžadují jednotný předpisový rámec. Tento rámec se skládá ze čtyř základních směrnic:

1. 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizované směrnice)
2. 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice)
3. 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě)
4. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

Všechny tyto směrnice se zabývají technickou stránkou telekomunikací a nikoliv regulací jejich obsahu. Regulací obsahu se zabývá směrnice 89/552/EHS a směrnice od ní odvozené. Legislativní rámec telekomunikací je relativně nový a právníci zabývající se touto oblastí uvádějí, že nová úprava podstatným způsobem zjednodušuje právní úpravu v této oblasti, nicméně, jak se ukáže v následujících odstavcích, to neznamená, že by právní úprava byla jednoduchá.

Z hlediska zařízení se směrnice také nevztahují na zařízení v oblasti platnosti směrnice 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody. Výše uvedené směrnice se však vztahují na zařízení pro digitální televizi.

Na služby v informační společnosti se vztahuje směrnice 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (směrnice o elektronickém obchodu).

Směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů a pravidel pro služby informační společnosti – definuje jako první směrnice pojem služby informační společnosti. Většina z těchto služeb nespadá pod legislativní rámec telekomunikací, protože nespočívají zcela nebo převážně na přenášení signálů po sítích elektronických komunikací.

Právní rámec se vztahuje:

1. hlasové telefonní služby
2. služby přenosu elektronické pošty
3. přístup k internetu apod.

Do právního rámce naopak nespadá:

1. regulace obsahu (např. televizního vysílání nebo rozhlasu)
2. úprava služeb poskytovaných přes Internet apod.

Rámec jako takový stanovuje základní požadavky na úpravu telekomunikací, zejména s ohledem na podporu „zdravé“ hospodářské soutěže v tomto odvětví. Prvním z těchto požadavků je požadavek na existenci nezávislého regulátora na trhu. Nezávislostí se zde myslí zejména požadavek na možnost odvolat se k nějaké třetí straně. Dle směrnice jí může být i soud.

Regulace jako taková by měla být pokud možno technologicky neutrální.

Radiové frekvence, jejich přidělování a převod se řídí rozhodnutím Evropského parlamentu (EP) a rady 676/2002/ES o předpisovém rámci pro politiku rádiového spektra v Evropském společenství (rozhodnutí o rádiovém spektru).

Za určitých okolností je nutné přistoupit k regulaci konkurenčního prostředí, tedy trhu. Jednou z těchto zvláštních okolností je, když některý účastník trhu získá tzv. významnou tržní sílu. Jako první se tento pojem vyskytl v 97/33/ES o propojení v odvětvích telekomunikací s cílem zajistit univerzální službu a interoperabilitu. Uplatněním zásad otevřeného přístupu k síti (ONP). Mnohem častěji se však využívá pojem vycházející z jurisdikátů soudního dvora a soudu prvního stupně ES – dominantní postavení.



Vysvětlení

Dominantní postavení má jedna nebo více firem pokud mezi nimi existuje strukturální nebo jiné vazby nebo také tehdy pokud struktura trhu vede ke koordinačním účinkům a tedy podporuje souběžné (spojené) protisoutěžní chování na trhu.

V tomto případě se ukládá regulačnímu orgánu povinnost regulovat tzv. ex ante. Ex ante regulace znamená, že trh je regulován takovým způsobem, aby fungoval jako předtím, než došlo k tržnímu selhání (v tomto případě získání dominantního postavením účastníkem trhu).

Všimněte si také, jakým způsobem je definice dominantního postavení sestavena, uvažuje totiž nejen se situací, kdy některý z účastníků získá dominantní tržní podíl, ale také situací, kdy dominantní postavení je založeno např. na vlastnění telekomunikační infrastruktury. To je třeba i případ Českého Telekomu (nynější Telefonicy O2), který své dominantní postavení zdědil ještě z dob komunismu.

EU jako celek bude v budoucnu zřizovat skupinu evropských regulačních orgánů pro sítě a služby elektronických komunikací jako vhodnou metodu spolupráce jednotlivých národních regulátorů a pokud možno jednotné regulační úpravě trhu EU jako celku.

Vnitrostátní regulační orgány mají povinnost podporovat hospodářskou soutěž s cílem, aby všichni uživatelé včetně např. tělesně postižených) měli maximální výhody výběru z hlediska služeb, ceny a kvality. Regulátor také může investičně podpořit rozvoj infrastruktury nebo inovací pokud by bez této podpory inovace nebyla realizována vůbec nebo se zpožděním. Regulátor také podporuje účinné využívání radiových frekvencí a zdrojů číslování a zajišťuje jejich účinnou správu.

Regulátor kromě řešení tržních selhání má i úlohu v rozvoji vnitřního telekomunikačního trhu EU a to zejména v oblasti odstraňování překážek pro zajišťování sítí elektronických komunikací na evropské úrovni. Zde patří i různá přeshraniční spolupráce, podpora zřizování a rozvoje transevropských sítí, zajišťování interoperability celoevropských služeb apod.

V oblasti rádiového spektra musí jednotlivé státy zajistit přidělování a kontrolu radiových frekvencí a to v souladu s rozhodnutím 676/2002/ES (viz výše).

Členské státy zajistí přidělování čísel, jmen a adres a to na základě tzv. národních číslovacích plánů. Tyto národní číslovací plány mají členské státy povinnost zveřejňovat, výjimky jsou možné pouze z důvodu možného ohrožení národní bezpečnosti.

2002/20/ES – autorizační směrnice

Cílem této směrnice je vytvořit právní rámec pro volné zajišťování sítí a poskytování služeb elektronických komunikací. Zabývá se požadavky pro získání oprávnění pro veškeré sítě a služby elektronických komunikací bez ohledu na to zda jsou poskytovány veřejnosti nebo ne.

Tato směrnice se nevyužívá pro přidělování radiových frekvencí s výjimkou zajišťování sítí nebo poskytování služeb elektronických komunikací (obvykle za úplatu), které se radiových frekvencí nebo provozu na nich týkají.

Využívání radiových vln (např. pro radioamatéry) upravuje směrnice 1999/5//ES.

Ustanovení upravující volný pohyb systému podmíněného přístupu a volného poskytování chráněných služeb, které jsou na takových systémech založeny, upravuje 98/84/ES o právní ochraně služeb s podmíněným přístupem a služeb tvořených podmíněným přístupem.

Udělování zvláštních práv může být nadále nezbytné pro užívání radiových frekvencí a čísel národního číslovacího plánů včetně tzv. zkrácených kódů. Práva k číslům mohou být předělována i z evropského číslovacího plánu, včetně virtuálního kódu země „3883“, který byl přidělen členským státům Evropské konference správ pošt a telekomunikací (CEPT).

2002/19/ES – Přístupová směrnice

Předmětem úpravy jsou mobilní telefonní sítě, sítě kabelové televize, sítě pro pozemní vysílání družicových sítí a sítí Internetu (používané pro přenos hlasu a obrazu, dat nebo faxu). Pro sítě takového typu musí být uděleno povolení dle autorizační směrnice nebo předchozích regulačních opatření.

Tato směrnice se vztahuje na dohody o přístupu a propojování mezi dodavateli služeb. Na neveřejné sítě (sítě, které neposkytují služby veřejnosti, např. vnitropodnikové) se tato směrnice nevztahuje, stejně jako na služby poskytování obsahu.

Regulační rámec má zajistit pokud možno kulturní rozmanitost, mediální pluralitu v oblasti telekomunikací. Počáteční předpisový rámec pro digitální televizi stanovuje směrnice 95/47/ES. Ustanovení v něm obsažená, se mají přezkoumávat na úrovni států s cílem zjistit, zda je důvod pro rozšíření povinnosti na zřizování nových bran (gateway), jako jsou elektronické programové průvodce (EPG) nebo rozhraní pro aplikační programy (API), tak aby se služby dostaly bez problému ke koncovému uživateli.

Směrnice také upravuje podmínky poskytnutí přístupu k infrastruktuře a to zejména u firem, které mají dominantní postavení na předmětném trhu. Povinnost zpřístupnit infrastrukturu je odůvodnitelná jako prostředek pro zachování hospodářské soutěže v daném segmentu trhu (žádná infrastruktura konkurence = žádná soutěž).

Regulátor při stanovení povinnosti však musí brát v úvahu i práva vlastníka infrastruktury, který do jejího vybudování a údržby investoval nějaké finanční prostředky. Tedy zpřístupnění by se mělo dít pouze s finanční nebo jinou náhradou. Vlastník infrastruktury by také měl mít možnost využívat tuto infrastrukturu v přiměřené míře ve svůj prospěch.

Regulace cen je možná pouze za předpokladu, že analýza trhu prokáže, že hospodářská soutěž je v určitém segmentu trhu neúčinná. Stanovené ceny by měly být přiměřené (dle směrnice 97/33/ES).

2002/22/ES – Směrnice o univerzálních službách



Náhled kapitoly

Univerzální službou se rozumí minimální rozsah služeb, které má možnost používat každý občan, včetně např. tělesně postižených.

Státy EU přijaly závazky v této oblasti v souvislosti s dohodou o základních telekomunikacích Světové obchodní organizace (WTO). Každý stát má podle této dohody vymezit druh povinnosti

univerzální služby dle svých potřeb. Tyto povinnosti pak nebudou považovány za protisoutěžní. V zásadě tedy může stát určit monopolního dodavatele univerzální služby.

Základním požadavkem, je poskytnout uživatelům na jejich žádost připojení k veřejné telefonní síti v pevném místě (jsou tedy vyloučení mobilní operátoři), za dostupnou cenu. Požadavek se omezuje na úzkopásmovou přípojku, je z ní tedy vyloučeno ISDN nebo třeba DSL. Přístup k telefonní síti by měl umožnit bezproblémový přístup k on-line službám, zejména pro komunikaci s orgány státní správy a samosprávy).

Součástí univerzální služby je zabezpečení dostatečného počtu telefonních automatů, a to zejména z toho důvodu, aby uživatelé měli přístup k číslu tísňového volání „112“ a to bezplatně. Účastnické seznamy a informační služba o účastnických číslech (telefonní seznam a informační linka) představují základní prostředek pro přístup k telefonní službě a jsou součástí povinnosti univerzální služby.

Směrnice také upravuje přenositelnost čísla. Jedná se o prostředek, který by měl umožnit uživatelům rozhodování se na základě kvality a ceny poskytovaných služeb. Před zavedením přenositelnosti, byl v zásadě tažen setrvačností – přechod k alternativnímu operátorovi by znamenal nemalé finanční náklady (pro firmy) na tisk nových propagačních materiálů, vizitek, reklamní kampaně apod.

Zajímavá je také koncepce tísňového čísla 112. Před nedávnem byl medializován spor mezi pražskými hasiči a zdravotní záchrannou službou o reklamní kampani na číslo 112, kdy hasiči podporují 112 a záchranná služba naopak existenci národních tísňových linek 15x. Záchranná služba argumentuje tím, že v případě, že se uživatel dovolá na číslo 112 a potřebuje okamžitou lékařskou pomoc, bude operátorem na čísle 112 přepojen na záchrannou službu a tam se mu teprve dostane pomoci. Doba přepojení přitom trvá 1 – 2 minuty. Jde o to, že na specializované lince se uživatel může dozvědět informace např. o resuscitaci, než dorazí záchranka.

Z hlediska směrnice je však číslo 112 prioritní s tím, že jednotlivé státy mohou, ale nemusí, používat národní tísňové linky. Z tohoto pohledu je tedy přístup HZS správný a problém časové prodlevy by se měl tedy řešit jinak, např. technickým opatřením, slučováním dispečinků apod.

11.2 Zákon o elektronických komunikacích (127/2005 Sb.)

Zákon o elektronických komunikacích byl přijat poměrně nedávno v rámci harmonizace práva ČR s prepisovým rámcem EU.

Jako regulátor byl v ČR ustanoven Český telekomunikační úřad (ČTU) se sídlem v Praze. V plnění zásad stanovených regulačním rámcem spolupracuje ČTU s Ministerstvem vnitra, které přebralo prakticky celou gesci dnes již zrušeného Ministerstva informatiky.

Komunikačními činnostmi se dle zákona rozumí

1. zajišťování sítí elektronických komunikací
2. poskytování služeb elektronických komunikací
3. a provozování přístrojů dle §73

Pro provoz komunikační činnosti musí fyzické osoby splnit následující podmínky: dosáhnout minimálně 18-ti let věku, být bezúhonné a být způsobilé k vykonávání právních úkonů. Fyzická osoba také nesmí mít závazky vůči orgánům státní správy.

Právnícké osoby musí splňovat podobné podmínky jako fyzické osoby. Omezení bezúhonnosti a právní způsobilosti přitom platí pro osobu nebo osoby oprávněné jednat jménem právnícké osoby.

ČTU uděluje tzv. všeobecné oprávnění. Jedná se o obecné opatření ČTU stanovující podmínky výkonu komunikační činnosti. Podmínky pro udělení všeobecného oprávnění se mohou týkat finančních příspěvků na provoz univerzální služby, požadavků na interoperabilitu, ochranu životního prostředí apod.

Pro podnikání v oblasti telekomunikací platí oznamovací povinnost.

Ze zákona také vyplývá povinnost ČTU spravovat rádiové spektrum. Rádiovým spektrem se přitom rozumí elektromagnetické vlnění o kmitočtech 9kHz – 3000GHz šířené prostorem bez zvláštního vedení (jinými slovy tedy vzduchem).

Správou se rozumí sestavování návrhu plánu přidělení kmitočtových pásem, přidělování volacích značek, identifikačních čísel a kódů a kontrola využívání rádiového spektra.

Kmitočty lze využívat pouze na základě individuálního oprávnění k využívání rádiových kmitočtů. Pro některé účely je k žádosti vyžadována licence dle zvláštního předpisu:

1. 231/2001 Sb. O provozování rozhlasového a televizního vysílání

2. 49/1997 Sb. O civilním letectví
3. 114/1995 Sb. O vnitrozemské plavbě
4. 61/2000 Sb. O námořní plavbě



Přestávka

Česká námořní plavba byla privatizována Viktoru Koženému.

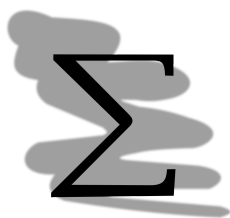
Úřad přednostně rozhoduje o udělování kmitočtů pro zajištění činnosti orgánů Ministerstva vnitra, BIS, Úřadu pro zahraniční styky a informace, Policie ČR, Vězeňská služba a justiční strážže ČR, HZS ČR a jednotek PO, Záchraně zdravotní službě a celním orgánům.

Kmitočtová pásma vyhrazená ministerstvu obrany pro vojenské účely mohou být pro tyto účely využívány bez nutnosti rozhodnutí o udělení oprávnění.

Za krizových stavů jsou podnikatelé zajišťující veřejné komunikační sítě povinni dle §12a zákona 240/2000Sb. a svých technicko – organizačních pravidel zabezpečit přístup k veřejné telefonní síti. Tento přístup je samozřejmě zpoplatněn. Pravidla, která si organizace přijímá sama, slouží k určení doby, za kterou je možno poskytnout přístup k síti a i ceny, která bude za využití sítě zaplacená.

Ministerstvo informatiky (MI) v oblasti elektronických komunikací předkládá vládě návrh státní politiky elektronických komunikací a po jejím schválení dohlíží nad její realizací. MI zabezpečuje mezinárodní vztahy v této oblasti na úrovni vlád, vládních i nevládních organizací s výjimkou těch, kde tímto úkolem byl pověřen ČTU. MI zodpovídá za plnění závazků vyplývajících z mezinárodních smluv a konečně vykonává státní statistickou službu.

Jelikož ministerstvo informatiky koncem roku 2007 zaniklo, přešly všechny jeho práva a povinnosti do gesce ministerstva vnitra.



Shrnutí

Telekomunikace jsou řešeny se na území EU jednotnými pravidly vymezenými směrnicemi EP a rady: rámcové, přístupové, autorizační, zvláštní směrnice a směrnice o univerzální službě.

Právní rámec se vztahuje na hlasové telefonní služby, služby přenosu elektronické pošty, přístup k internetu a podobně.

Regulace obsahu je spravována samostatnými pravidly.

Hlavním úkolem tohoto rámce je zajistit přístup k základním službám (univerzální služba), a zajistit, že trh se chová transparentně z hlediska hospodářské soutěže. Dalším cílem je zajistit plynulou přeshraniční spolupráci v této oblasti.

V ČR jsou tyto směrnice implementovány do zákona o elektronických komunikacích (127/2005 Sb.). Jako regulátor byl pro ČR stanoven Český telekomunikační úřad (ČTU). Z hlediska spolupráce na legislativě a mezinárodní spolupráce vstupuje do telekomunikací i Ministerstvo informatiky (MI).



Kontrolní otázky

1. které úřady mají povinnosti na úseku elektronických komunikací v ČR
2. Vyjmenujte zkrácené názvy alespoň dvou směrnic EU z oblasti elektronických komunikací
3. Pokuste se stanovit co je to univerzální služba.
4. Která čísla mají z hlediska práva větší význam 112 nebo 15x?
5. Co je přístup ex ante.



Správné odpovědi

1. ČTU, MI
2. Autorizační, přístupová, o univerzální službě, speciální
3. Základní hlasové a datové služby umožňující komunikaci s úřady.
4. 112, EU to tak chce a EU to tak bude mít i u nás
5. Překlad: Jako předtím – reguluje se s cílem dosáhnout stavu jako před dosažením dominantního postavení účastníka trhu nebo obecně nějakého tržního selhání.



Test

1. Které frekvence a telekomunikační služby schvaluje ČTU
 - (a) Všechny
 - (b) Žádné
 - (c) Všechny kromě armádních
2. Spolupracovat se zahraničními partnery na úseku telekomunikací má ze zákona povinnost
 - (a) Evropská komise
 - (b) MI
 - (c) ČTU
3. Univerzální služba obsahuje
 - (a) ISDN
 - (b) ADSL
 - (c) Základní hlasové a datové služby
4. Regulačním přístupem, kterým se snažíme dosáhnout situace na trhu předcházející tržnímu selhání, nazýváme
 - (a) Ex jure
 - (b) Ex ante
 - (c) Ex libris
5. Důvodem zavádění přenositelnosti telefonních čísel je
 - (a) Dobrá vůle operátorů
 - (b) Snaha pomoci koncovým zákazníkům
 - (c) Snaha otevřít rigidní trh konkurenci



Správné odpovědi

1. c), 2. b), 3. c), 4. b) 5. c)

Literatura

- [1] *AV-Test* [online]. [cit. 2013-12-18]. Dostupné z: <http://www.av-test.org/en/home/>
- [2] *CCSDS 650.0-M-2 - Reference Model for an Open Archival Information System (OAIS)* [online]. [cit. 2013-12-30]. Dostupné z: <http://public.ccsds.org/publications/archive/650x0m2.pdf>
- [3] *CESNET Komunikační infrastruktura* [online]. [cit. 2015-06-17]. Dostupné z: <http://www.cesnet.cz/e-infrastruktura/komunikacni/>
- [4] *Common Criteria* [online]. [cit. 2012-03-20]. Dostupné z: <https://www.commoncriteriaportal.org/>
- [5] *CSIRT.CZ O nás* [online]. [cit. 2012-03-16]. Dostupné z: <https://www.csirt.cz/page/882/onas/>
- [6] *Enigma* [online]. [cit. 2013-12-19]. Dostupné z: <http://en.wikipedia.org/wiki/File:EnigmaMachineLabeled.jpg>
- [7] *ETSI TS 101 733 V2.2.1 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)* [online]. [cit. 2013-12-30]. Dostupné z: http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
- [8] *Farbar Recovery Scan Tool* [online]. [cit. 2013-12-18]. Dostupné z: Farbar Recovery Scan Tool Download - Bleeping Computer
- [9] *The hash function RIPEMD-160* [online]. [cit. 2013-12-30]. Dostupné z: <http://homes.esat.kuleuven.be/~bosselae/ripemd160.html>
- [10] ISO 14721:2012 - Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model.
- [11] ISO/IEC 10118-3:2004 - Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions.
- [12] ISO/IEC 18033-4 Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers.
- [13] ISO/IEC 29192-3 Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers.
- [14] *Jiří Peterka* [online]. [cit. 2012-06-25]. Dostupné z: <http://www.lupa.cz/autori/jiri-peterka/>
- [15] *Keylength - NIST Report on Cryptographic Key Length and Cryptoperiod (2012)* [online]. [cit. 2017-01-2]. Dostupné z: <https://www.keylength.com/en/4/>
- [16] Konsolidované znění Smlouvy o fungování Evropské unie.
- [17] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES* [online]. [cit. 2016-08-15]. Dostupné z: <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>
- [18] *Nařízení vlády 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury.*
- [19] *Nařízení vlády č. 11/2002 Sb. kterým se stanoví vzhled a umístění bezpečnostních značek a zavedení signálů.*
- [20] *Návod na vytvoření logu z DDS* [online]. [cit. 2013-12-18]. Dostupné z: <http://forum.viry.cz/viewtopic.php?f=13&t=125171>
- [21] *Návod na vytvoření logu z RSIT* [online]. [cit. 2013-12-18]. Dostupné z: <http://forum.viry.cz/viewtopic.php?f=13&t=130786>
- [22] *OpenPGP* [online]. [cit. 2017-01-4]. Dostupné z: <http://openpgp.org/>
- [23] *OpenSSL* [online]. [cit. 2017-01-4]. Dostupné z: <https://www.openssl.org/>

- [24] *Ova.net* [online]. [cit. 2015-06-17]. Dostupné z: <http://www.ovanet.cz/>
- [25] *RFC 1918 - Address Allocation for Private Internets* [online]. [cit. 2015-06-19]. Dostupné z: <https://tools.ietf.org/html/rfc1918>
- [26] ROZHODNUTÍ KOMISE 2011/130/EU kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu.
- [27] *Skytale* [online]. [cit. 2013-12-19]. Dostupné z: <http://commons.wikimedia.org/wiki/File:Skytale.png>
- [28] QNAP. *TVS-671* [online]. [cit. 2015-09-2]. Dostupné z: <https://www.qnap.com/i/en/product/model.php?II=159>
- [29] Uznesenie vlády SR číslo 479/2009 k návrhu organizačného, personálneho, materiáľno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (CSIRT.SK) v SR.
- [30] ČESKO. *Zákon 111/2009 Sb. o základních registrech* [online]. [cit. 2016-04-18]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2009-111>
- [31] Zákon 480/2004 Sb., o některých službách v informační společnosti.
- [32] ČESKO. *Zákon 227/2000 Sb. o elektronickém podpisu* [online]. [cit. 2016-04-18]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2000-227>
- [33] *Specification for the Advanced Encryption Standard (AES)* [online]. Springfield, VA: NIST, 2001. 47 s. [cit. 2013-12-19]. Dostupné z: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [34] ETSI TS 102 176-1 V2.1.1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. 2011.
- [35] *FIPS PUB 180-4 - Secure Hash Standard (SHS)* [online]. [cit. 2013-12-30]. Dostupné z: <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>
- [36] *FIPS PUB 186-4 Digital Signature Standard (DSS)* [online]. [cit. 2013-12-20]. Dostupné z: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
- [37] AV-TEST. *Malware statistic* [online]. [cit. 2013-12-16]. Dostupné z: <http://www.av-test.org/en/statistics/malware/>
- [38] AZAD, Kalid. *Understanding the Birthday Paradox* [online]. [cit. 2013-12-30]. Dostupné z: <http://betterexplained.com/articles/understanding-the-birthday-paradox/>
- [39] BARKER, William C., BARKER, Elaine. *NIST SP800-67 Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher* [online]. [cit. 2013-12-19]. Dostupné z: <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>
- [40] BOESGAARD, M., VESTERAGER, M., ZENNER, E. *A Description of the Rabbit Stream Cipher Algorithm* [online]. [cit. 2013-12-19]. Dostupné z: <http://tools.ietf.org/search/rfc4503>
- [41] BOUŠKA, Petr. *Víte, jak pracuje switch?* [online]. [cit. 2015-06-18]. Dostupné z: <http://www.samuraj-cz.com/clanek/vite-jak-pracuje-switch/>
- [42] BUONAFALCE, Augusto. *Image of an Alberti Cipher Disk* [online]. [cit. 2016-12-21]. Dostupné z: https://commons.wikimedia.org/wiki/File:Alberti_cipher_disk.JPG
- [43] ARAKIS *agregacja, analiza i klasyfikacja incidentów sieciowych* [online]. [cit. 2012-03-16]. Dostupné z: <http://arakis.cert.pl/pl/index.html>
- [44] *CERT.GOV.PL - domácí stránky* [online]. [cit. 2012-06-16]. Dostupné z: <http://cert.gov.pl/portal/cer/>
- [45] *CSIRT.CZ: Incident handling statistics* [online]. [cit. 2012-03-16]. Dostupné z: <https://www.csirt.cz/files/csirt/statistics/stats.html>
- [46] CZ.NIC. *Datovka 4* [online]. [cit. 2017-01-7]. Dostupné z: <https://labs.nic.cz/cs/datovka.html>
- [47] CZ.NIC. *DNSSEC/TLSA Validator add-in for Web Browsers* [online]. [cit. 2015-06-16]. Dostupné z: <https://www.dnssec-validator.cz/pages/screenshots.html>

-
- [48] DOBBERTIN, Hans. Cryptanalysis of MD4. *Journal of Cryptology*. roč. 11, č. 4, s. 253–287. doi: 10.1007/s001459900047. ISSN 1432-1378.
- [49] EISELE, Robert. *Caesar cipher decryption tool • Code is poetry* [online]. [cit. 2016-12-21]. Dostupné z: <http://www.xarg.org/tools/caesar-cipher/>
- [50] GANTZ, John, REINSEL, David. *Extracting Value from Chaos* [online]. IDC, 2011. 12 s. [cit. 2013-11-1]. Dostupné z: <http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf>.
- [51] GOOGLE. *Dashboards | Android Developers* [online]. [cit. 2016-04-8]. Dostupné z: https://developer.android.com/about/dashboards/index.html?utm_source=suzunone
- [52] GREENOUGH, John. *How the „Internet of Things“ will impact consumers, businesses, and governments in 2016 and beyond* [online]. [cit. 2016-11-25]. Dostupné z: <http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10>
- [53] KLÍMA, Vlastimil. *Tunnels in Hash Functions: MD5 Collisions Within a Minute* [online]. [cit. 2013-12-30]. Dostupné z: <http://eprint.iacr.org/2006/105>
- [54] MATOUSEC. *Proactive Security Challenge 64* [online]. [cit. 2013-12-18]. Dostupné z: <http://www.matousec.com/projects/proactive-security-challenge-64/>
- [55] MATSUI, M., NAKAJIMA, J., MORIAI, S. *RFC 3713 A description of the Camellia Encryption Algorithm* [online]. [cit. 2013-12-19]. Dostupné z: <http://tools.ietf.org/html/rfc3713>
- [56] NET MARKET SHARE. *Operating System Market Share* [online]. [cit. 2016-12-21]. Dostupné z: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>
- [57] NIST. *FIPS 140-2 - Security Requirements for Cryptographic Modules* [online]. [cit. 2013-12-30]. Dostupné z: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [58] NIST. *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* [online]. Gaithersburg, NIST, 2015. 32 s. [cit. 2017-01-6]. Dostupné z: <http://dx.doi.org/10.6028/NIST.FIPS.202>.
- [59] OORSCHOT, P., WIENER, M. Parallel collision search with applications to hash functions and discrete logarithms [online]. In: *ACM Conference on Computer and Communications Security*. ACM Press, 1994, s. 210–218, [cit. 2013-12-30]. Dostupné z: <http://www.certainkey.com/dnet/acmccs94.pdf>.
- [60] SCHNEIER, Bruce. *Lessons From the Dyn DDoS Attack* [online]. [cit. 2016-11-25]. Dostupné z: https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html
- [61] SHANNON, C. E. A Mathematical Theory of Communication. *The Bell System Technical Journal*. 1948, roč. 27, č. 3, s. 379–423.
- [62] SMART, Nigel P. et al. *Algorithms, Key Sizes and Parameters Report* [online]. Brusel: ENISA, 2013. 96 s. [cit. 2013-12-19]. Dostupné z: <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>.
- [63] STEVENS, Marc, KARPMAN, Pierre, PEYRIN, Thomas. *Freestart collision for full SHA-1*. 2015.
- [64] SULLIVAN, Nick. *A (relatively easy to understand) primer on elliptic curve cryptography* [online]. [cit. 2013-12-20]. Dostupné z: <http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/>
- [65] SVĚT SÍTÍ. *Základy počítačových sítí* [online]. [cit. 2006-02-23]. Dostupné z: <http://svetsiti.cz>
- [66] US-CERT. *National Cyber Awareness System* [online]. [cit. 2012-06-25]. Dostupné z: <https://www.us-cert.gov/alerts-and-tips/>
- [67] *US-CERT - domácí stránky* [online]. [cit. 2012-03-16]. Dostupné z: <https://www.us-cert.gov/>
- [68] VIRUS BULLETIN. *VB100 comparative testing* [online]. [cit. 2013-12-18]. Dostupné z: <https://www.virusbtn.com/vb100/index>

-
- [69] WANG, Xiaoyun et al. *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD* [online]. [cit. 2013-12-30]. Dostupné z: <http://eprint.iacr.org/2004/199.pdf>
- [70] YORK, Kyle. *Dyn Statement on 10/21/2016 DDoS Attack* [online]. [cit. 2016-11-25]. Dostupné z: <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>
- [71] ČESKO. *297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce* [online].
- [72] ŠENOVSÝ, Pavel. *Databáze nebezpečných látek 2005 - Příručka uživatele*. Ostrava: SPBI, 2005. 65 s. ISBN 80-86634-79-5.

Slovník

AACS Advanced Access Content System.

AdES Advanced Electronic Signature.

ADSL Asymmetric Digital Subscriber Line.

AES Advanced Encryption Standard.

API Application Programming Interface.

ARPA Advanced Research Projects Agency.

ARPANET Advanced Research Projects Agency Network.

ASCII American Standard Code for Information Interchange.

AWS Amazon Web Services.

BI1 Bezpečnostní informatika 1.

BI3 Bezpečnostní informatika 3.

BIOS Basic Input Output System.

BOINC Berkeley Open Infrastructure for Network Computing.

BSD Berkeley Software Distribution (též Berkeley Unix).

C & C Command and Control Infrastructure.

CAD Computer Aided Design.

CASE Computer Aided System Engineering.

CC Common Criteria.

CCSDS Consultative Committee for Space Data Systems.

CD Compact Disc.

CEN Comité Européen De Normalisation (Evropská normalizační komise).

CERN Organisation européenne pour la recherche nucléaire.

CERT Computer Emergency Response Team.

CLP Classification, Labelling and Packaging (klasifikace, označování a balení).

CMCKG-PP Cryptographic module for CSP key generation services protection profile.

CMCSO-PP Cryptographic module for CSP signing operations - Protection profile.

CMCSOB PP Cryptographic module for CSP signing operations with backup - Protection profile.

CRC Cyclic redundancy check (kontrolní součty).

- CRYPTREC** Cryptography Research and Evaluation Committees.
- CSIRT** Computer Security Incident Response Team.
- CSS** Content Scrambling System.
- CWA** CEN Workshop Agreement.
- DARPA** Defence Advanced Research Project Agency.
- DDoS** Distributed Denial of Services.
- DES** Decryption Encryption Standard.
- DHCP** Dynamic Host Cache Protocol.
- DHT** Distributed Hash Table.
- DLP** Discrete Logarithm Problem.
- DNS** Domain Name Server.
- DOS** Desktop Operating System.
- DOT** Department of Transportation.
- DRM** Digital Rights Management.
- DSA** Digital Signature Algorithm.
- DSS** Digital Signature Standard.
- DTP** Desktop Publishing.
- DVD** Digital Versatile Disc.
- EAL** Evaluation Assurance Level.
- ECDLP** Elliptic Curves Discrete Logarithm Problem.
- ECDSA** Elliptic Curves Digital Signature Algorithm.
- ENISA** European Union Agency for Network and Information Security Agency.
- eOP** elektronický občanský průkaz.
- EP** European Parliament.
- ETSI** European Telecommunication Standards Institute.
- EU** Evropská unie.
- EULA** End User Licence Agreement.
- FIPS** Federal Information Processing Standard.
- FIRST** Forum for Incident Response and Security Teams.
- FRST** Farbar Recovery Scan Tool.
- FTP** File Transfer Protocol.
- GIF** Graphics Interchange Format.
- GPL** General Public License.
- GPRS** General Packet Radio Service.

- GSM** Global System for Mobile Communications.
- GUI** Graphical User Interface.
- HIPS** Host Intruder Prevention System.
- HTML** Hyper Text Markup Language.
- IDS** Intruder Detection System.
- IETF** Internet Engineering Task Force.
- IIS** Internet Information Service.
- IMP** Interface Message Processor.
- INWG** International Network Working Group.
- IoT** Internet of Things.
- IPS** Intruder Prevention System.
- IRC** Internet Relay Chat.
- IS** Informační systém.
- ISDN** Integrated Services Digital Network.
- ISDS** Informační systém datových schránek.
- ISP** Internet Service Provider.
- IST** Information Society Technologies.
- ISVS** informační systémy veřejné správy.
- IT** Informační technologie.
- JRE** Java Runtime Environment.
- LAN** Local Area Network.
- LGPL** Lesser GPL License.
- Linux** Linux is not Unix.
- MAC** Media Access Control.
- MAN** Metropolitan Area Network.
- MD** Message Digest.
- MISTY** Mitsubishi Improved Security Technology.
- MP3** MPEG-2 Audio Layer III.
- MS** Microsoft.
- NA** North America.
- NAS** Network Attached Storage.
- NASA** National Aeronautics and Space Administration.
- NAT** Network Address Translation.

- NATO** North Atlantic Treaty Organization.
- NBU** Národní bezpečnostní úřad.
- NCKB** Národní centrum kybernetické bezpečnosti.
- NCP** Network Control Protocol.
- NESSIE** New European Schemes for Signatures, Integrity and Encryption.
- NFPA** National Fire Protection Association.
- NFS** Network File System.
- NIST** National Institute for Standards and Technology.
- NSA** National Security Agency.
- NSF** National Science Foundation.
- NTT** Nipon Telegraph and Telephone Corporation.
- OAIS** Open Archival Information System.
- OS** Operační systém.
- P2P** peer to peer.
- PARC** Palo Alto Research Center.
- PC** Personal Computer.
- PCS** Poskytovatel Certifikačních Služeb.
- PDF** Portable Document Format.
- POSIX** Portable Operating System Interface [for Unix].
- QES** Qualified Electronic Signature.
- RFC** Request for Comment.
- RIPE** Race Integrity Primitives Evaluation.
- RPC** Remote Procedure Call.
- RSIT** Random's System Information Tool.
- RSS** RDF Site Summary.
- SAGE** Security Algorithms Group of Experts.
- SHA** Secure Hash Algorithm (bezpečný hašovací algoritmus).
- SHS** Secure Hash Standard.
- SOHO** Small Office Home Office.
- SQL** Structured Query Language.
- STP** Shielded Twisted Pair.
- SŘBD** Systém řízení báze dat.
- TDEA** Triple Data Encryption Algorithm.

TDES Triple DES.

TERENA The Trans-European Research and Education Networking.

TIFF Tagged Image File Format.

TLS Transport Layer Security.

UAC User Access Control.

UCS Universal Character Set.

UD United Devices.

UMTS Universal Mobile Telecommunications System.

URL Universal Resource Locator.

USA United States of America.

UTF-8 UCS Transformation Format.

UTP Unshielded Twisted Pair.

VDSL Very High Speed DSL.

W3C World Wide Web Consortium.

WAN Wide Area Network.

WU work unit.

WWW World Wide Web.

XML Extensive Markup Language.

ÚOOÚ Úřad pro ochranu osobních údajů.

ČR Česká republika.

[title=Seznam zkratek]

Rejstřík

- útok souvisejícími klíči, 47
- ČTÚ, 112
- časové razítko, 56
- šifra
 - asymetrická, 49
 - DSA, 50
 - ECDSA, 51
 - RSA, 49
 - kódy, 42
 - monoalfabetická, 42
 - polyalfabetická, 42
 - proudová, 48
 - substituční, 42
 - symetrická, 45
 - A5, 48
 - A5/1, 48
 - A5/2, 48
 - AES, 45
 - bloková, 45
 - Blowfish, 47
 - Camellia, 46
 - DES, 45
 - E0, 49
 - Kasumi, 46
 - MISTY1, 46
 - proudová, 45
 - Rabbit, 48
 - RC4, 49
 - SNOW 2.0, 48
 - SNOW 3G, 48
 - TDEA, 45
 - TDES, 45
 - Trivium, 48
- šifrování, 41
 - šifrovaný text, 41
 - kód, 45
 - klíč, 41
 - otevřený text, 41
 - škodlivý kód, 27
- AES, 45
- antivirový program, 36
- aplikační server, 75
- autentizace, 53
 - dvoufaktorová, 54
 - jednofaktorová, 54
- backdoor, 30
- big data, 24
- CERT, 91
- computer fingerprinting, 69
- CRC, 15
- CSIRT, 91
- data, 14
- databáze, 15, 23
 - objektové, 24
 - relační, 24
- datové schránky, 82
 - autorizovaná konverze, 82
 - CzechPOINT, 82
 - domněnka pravosti, 83
- datový prvek, 87
- DES, 45
- DHCP, 75
- dialer, 30
- DNA, 105
- DNA počítač, 105
- DNS, 75
- eID, 52
- eIDAS, 52
 - důvěra, 53
- elektronická identita, 52
- elektronická počef, 55
- elektronická podatelna, 81
- elektronická značka, 55
- elektronické archívy, 57
- elektronický občanský průkaz, 52
- elektronický podpis, 51
 - aplikace
 - DNSSec, 33
- elektronický podpis s dlouhou dobou působnosti, 58
- entropie, 13
 - relativní entropie, 16
- eOP, 52
- ex ante princip, 110
- faktorizace, 49
- firewall, 36
 - osobní, 36
- hašovací funkce, 58
 - kolize, 58
 - MD, 58

- MD2, 59
- MD4, 59
- MD5, 59
- Message Digest, 58
- RIPEMD, 61
- RIPEMD-160, 61
- SHA-1, 60
- SHA-2, 60
- SHA-3, 60
- WHIRPOOL, 61
- HIPS, 36
- hoax, 32

- informační koncepce, 87
- informační nárůst, 17
- informační proces, 15
- informační systém, 14
- informační systémy veřejné správy, 86
- informační technologie, 14
- informace, 13
 - poločas stárnutí, 17
 - stárnutí, 17
 - ideální křivka, 17
 - reálná křivka, 18
- informatika, 14
- IoT, 38
- IP adresa
 - privátní, 71
 - veřejná, 71
- IP protokol, 71
- IPv4, 71
- IPv6, 72
- IS, 14
- IT, 14

- kód, 16
 - redundance, 16
- kódování
 - efektivita, 16
 - kód, 16
 - optimální kód, 16
- kódové knihy, 45
- kabel
 - koaxiální, 68
 - kroucená dvojlinka, 68
 - optický, 69
 - STP, 68
 - twisted pair, 68
 - UTP, 68
- keylogger, 30
- klíč, 45
- klient, 73
- kritická informační infrastruktura, 90
- kritická infrastruktura, 90
- kvalifikovaný elektronický podpis, 55
- kvantový počítač, 106
- kybernetická bezpečnost, 89

- loopback adresa, 71
- MAC adresa, 70
- malware, 27
 - červ, 29
 - činnost, 27
 - heuristická analýza, 29
 - hoax, 32
 - rozdělení, 28
 - sítě botů, 34
 - signtura viru, 29
 - spyware, 32
 - trojský kůň, 30
 - backdoor, 30
 - dialer, 30
 - downloader, 31
 - dropper, 31
 - keylogger, 30
 - ransomware, 31
 - rogue antivirus, 31
 - rootkit, 31
 - trojan-proxy, 31
 - virus, 27
 - bootovací, 29
 - polymorfní, 29
 - stealth, 29
- Microsoft update, 37

- nařízení EU, 52
- narozeninový paradox, 59
- NAS, 74
- NAT, 71, 76
- NBU, 90
- NCKB, 90
- nebezpečné látky
 - ADR, 100
 - CAS číslo, 98
 - DOT čísla, 99
 - ES číslo, 98
 - H věty, 101
 - HAZCHEM, 99
 - identifikační číslo nebezpečnosti, 99
 - indexové číslo, 98
 - Kemler kód, 99
 - NA čísla, 99
 - P věty, 101
 - R věty, 100
 - RID, 100
 - S věty, 100
 - třídy nebezpečnosti, 100
 - UN kód, 98
 - výstražné symboly, 101
- nespojová služba, 72
- neuroprocesor, 107
- NoSQL, 24

- opatření
 - ochranné, 91

- reaktivní, 91
- operační systém, 22
 - nadstavby, 23
- přístupová směrnice, 111
- paddingová funkce, 56
- phishing, 32
- podpisové schéma, 56
- POSIX, 23
- poskytovatel certifikačních služeb, 53
- postranní kanály, 48
- privátní síť, 71
- problém diskrétního logaritmu eliptické křivky, 51
- prostý elektronický podpis, 54
- q-bit, 106
- ransomware, 31
- referenční model ISO/OSI, 69
- referenční rozhraní, 86
- rhybaření, 32
- rogue antivirus, 31
- rootkit, 31
- rychlé informace, 95
 - barvy, 96
 - informativní značky, 97
 - nebezpečné látky, 98
 - značky příkazu, 96
 - značky výstrahy, 96
 - značky zákazu, 96
- sítě
 - token ring, 66
- síťová zařízení
 - brána, 72
 - bridge, 71
 - gateway, 72
 - hub, 70
 - můstek, 71
 - opakovač, 70
 - přepínač, 70
 - repeater, 70
 - router, 72
 - směrovač, 72
 - switch, 70
- sítě
 - hvězdicová topologie, 66
 - hybridní topologie, 66
 - LAN, 67
 - MAN, 67
 - topologie, 65
 - WAN, 67
- sítě botů, 34
- Sandbox, 36
- security by obscurity, 48
- server, 73
 - databázový, 74
 - souborový, 74
- WWW, 74
- service pack, 37
- signál, 15
- slabý klíč, 47
- směrnice EU, 52
- sociální inženýrství, 29
- software
 - aplikační, 22, 25
 - systémový, 22
 - uživatelský, 25
- soukromý exponent, 49
- SPAM, 35
 - opt-in, 35
 - opt-out, 35
- spojová služba, 72
- spyware, 32
- SQL, 23
- stav kybernetického nebezpečí, 91
- substituční šifry, 43
- superpozice stavů, 106
- systém, 14
- TCP, 72
- TDEA, 45
- TDES, 45
- telekomunikace
 - rádiové spektrum, 112
 - regulační orgán, 110
 - regulační rámec, 109
- tiskový server, 74
- topologie
 - sběrnice, 65
- UDP, 72
- univerzální služba, 111
- významná síť, 90
- významný informační systém, 91
- veřejný exponent, 49
- vishing, 34
- vrstvy sítě
 - aplikační, 73
 - fyzická, 70
 - linková, 70
 - přenosová, 72
 - prezentační, 72
 - síťová, 71
 - spojová, 72
- webové certifikáty, 52
- Windows Update, 37
- XML, 24
- základní registry, 79
 - území, 80
 - obyvatel, 80
 - osob, 80

zákon o elektronickém podpisu, 51
zadní vrátka, 30
zaručený elektronický podpis, 55
zaručený elektronický podpis, založený na kvalifi-
kovaném certifikátu, 55
zero-day zranitelnost, 30
znaková sada, 16
znanost, 14
zranitelnost systému, 30