Bezpečnost dat v informatice

Data security in informatics

Václav Chytil

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Václav CHYTIL**
Osobní číslo:	**A07608**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost dat v informatice (Bezpečné zpracování dat a bezpečná komunikace prostředky výpočetní techniky)**

Zásady pro vypracování:

1. **Zpracujte literární zdroje z oblasti datové bezpečnosti.**
2. **Stanovte cíle práce, metody a pracovní hypotézy.**
3. **V rámci praktické části zmapujte současné metody ochrany dat v jednotlivých oblastech – software, hardware, management.**
4. **Zanalyzujte vybrané prostředky pro ochranu dat a zhodnoťte jejich účinnost.**
5. **Na základě provedené analýzy zformulujte závěrečná doporučení v oblasti aplikace datové bezpečnosti.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **STŘIHAVKA, Marek: Vaše bezpečnost a anonymita na Internetu. 1. vyd. Brno: Computer Press, 2001. 84 s. ISBN 80-72265-86-5.**
2. **ERICKSON, Jon: Hacking umění exploitace. Překlad Marek Střihavka. 1. vyd. Brno: Zoner Press, 2005. 263 s. ISBN 80-86815-21-8.**
3. **SZOR, Peter: Počítačové viry analýza útoku a obrana. Překlad Marek Střihavka. 1. vyd. Brno : Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.**
4. **ZELENKA, Josef. Ochrana dat: kryptologie. Vyd. 1. Hradec Králové: Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.**
5. **PŘIBYL, Jiří; KODL, Jindřich. Ochrana dat v informatice. Vyd. 1. Praha: Vydavatelství ČVUT, 1996. 299 s. ISBN 8001016641.**

Vedoucí bakalářské práce: **RNDr. Ing. Miloš Krčmář**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tématem této bakalářské práce je „Bezpečnost dat v informatice“. V teoretické části jsou popsány jednotlivé prostředky užívané k ochraně dat a vysvětluje terminologii škodlivého softwaru.

Praktická část se věnuje praktickému použité prostředků zabezpečení dat. Také vysvětluje princip některých hrozeb a navrhuje opatření jak jim čelit.

Klíčová slova: datová bezpečnost, malware, bezpečnost, šifrování, záloha, firewall

ABSTRACT

The theme of this thesis is „Data security in informatics“. The theoretical part describes the various means used to protect data and explains the terminology of malicious software.

The practical part is devoted to practical devices used in data security. It also explains the principle of some of the threats and it recommends measures to deal with them.

Keywords: data security, malware, safety, encryption, backup, firewall

Poděkování

Rád bych poděkoval RNDr. Ing. Miloši Krčmářovi za jeho rady, vstřícnost a ochotu. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi od nich dostávalo během tvorby této práce i celého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Dnešní svět je závislý na rychlém a snadném přístupu k informacím víc, než kdy před tím. Ochrana znalostí a přenášených zpráv byla v minulosti jednodušší, protože informace byly buď uložené v paměti člověka, nebo byla existence zprávy omezena jednoznačně definovanou, fyzickou polohou nosiče. Takovou informaci jsme mohli snadno kontrolovat a ochránit pouze fyzickým zabezpečením samotného nosiče informace. V dnešní době jsou informace sice pořád závislé na nějakém fyzickém zařízení, ale změnily se možnosti přístupu k nim - můžeme je zpřístupnit prakticky z libovolného místa naší planety. Existuje velký počet komunikačních cest a prostředků, které mohou být použity i k neoprávněnému přístupu k informacím, a stále vznikají nové.

Zabezpečení dat je neustálý boj a naneštěstí se bojiště této informační války mění velmi rychle a je stále obtížnější sledovat nové trendy a prostředky ochrany dat. Zvlášť pro lidi, kteří se pravidelně nepohybují v oblasti informačních technologií je orientace v metodách zabezpečení dat obtížný úkol. Právě proto jsem se snažil napsat tuto práci srozumitelným jazykem, kterému porozumí i běžní uživatelé. Většina publikací z oblasti datové bezpečnosti je totiž možná až zbytečně podrobná. Ty srozumitelné bývají roztroušené po celém internetu nebo po různých časopisech a nenabízí komplexní pohled na celou problematiku.

Byl bych rád, kdyby se má bakalářská práce stala nejen prací odbornou, ale zároveň i srozumitelnou pro „běžného smrtelníka“ mimo obor IT. S tímto cílem tedy budu tvořit následující řádky.

I. TEORETICKÁ ČÁST

1 KRYPTOGRAFIE

Kryptografie neboli šifrování je jedním z nejúčinnějších prostředků ochrany dat. V minulosti byla kryptografie používána výhradně pro vojenské účely nebo diplomatickou komunikaci, ale s rozšířením osobních počítačů se dostala do každodenního života. Šifrování má dnes široké použití sahající od šifrování kabelové televize až po zabezpečení přísně tajných dokumentů.

1.1 Vymezení základních pojmu kryprografie

Protože je oblast datové bezpečnosti široký a specifický obor, je důležité nejprve definovat a vysvětlit některé pojmy z této oblasti: [6, s. 12]

- Kryptologie je samostatná vědní disciplína, která zastřešuje kryptografii, kryptoanalýzu a někdy se uvádí, že obsahuje i steganografii. Kryptologii chápeme jako vědu o informační celistvosti, konkrétně tento obor zahrnuje tvorbu kryptografických technik, vymezení podmínek jejich praktického využívání a zkoumání okolnosti kryptografických algoritmů proti kryptoanalytickým útokům.
- Kryptografie se zabývá matematickými metodami se vztahem k takovým aspektům informační bezpečnosti, jako je důvěrnost a integrita dat či autentizace entit a původ dat.
- Steganografie se zabývá úpravou informace způsobem, jehož účelem je skrýt existenci zprávy, přičemž samotná zpráva může být napsána nebo předána ve srozumitelné podobě.
- Kryptoanalýza je „opakem“ kryptografie – kryptoanalytici se v její „klasické“ podobě snaží získat ze zašifrované zprávy její původní podobu nebo alespoň část utajovaných informací, resp. prolomit šifrovací algoritmus.
- Kryptografické protokoly jsou postupem, jak využít celého potenciálu šifrovacího algoritmu, tedy jak provést šifrování nejvhodnějším způsobem.
- Kryptografický systém je systém, jehož funkcí je kryptografická transformace otevřeného textu (nechráněného textu) na šifrovaný text (chráněný text).

1.2 Moderní kryptografie

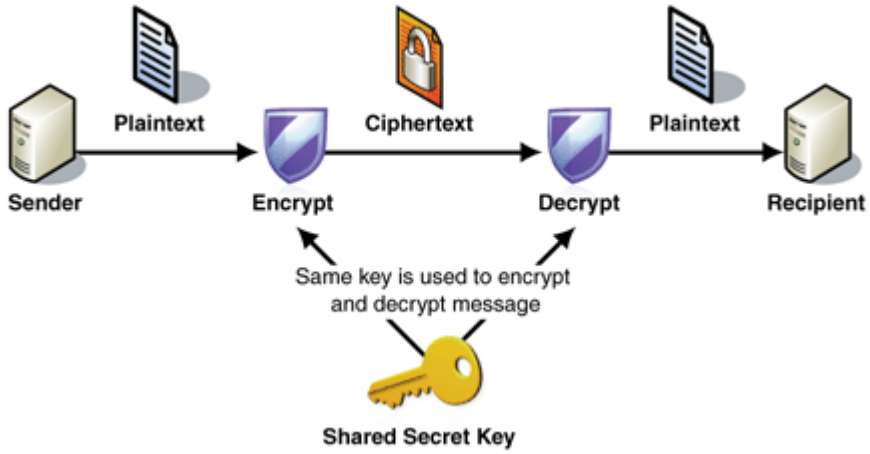
Narozdíl od starších monoalfabetických a polyalfabetických šifer využívá moderní kryptografie velké rychlosti počítačů. Proces šifrování a dešifrování se znalostí klíče je pro počítač jednoduchá úloha, ale dešifrovat zprávu bez klíče je velmi náročný úkol.

1.3 Proudové šifry

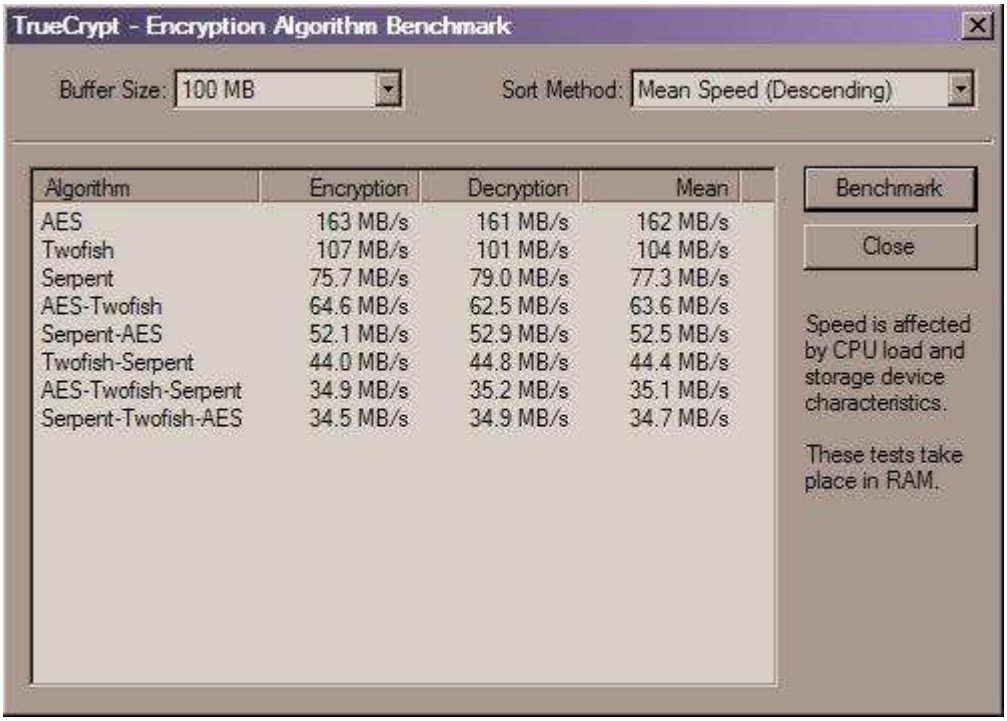
Tyto symetrické algoritmy se používají především u komunikačních systémů, kde je potřeba udržet souvislost datového toku nebo tehdy, kdy předem neznáme délku textu. Proudové šifry používají klíče různé délky a data šifrují po jednotlivých bitech. Délka klíče není omezena a klíč tedy může být dokonce i stejně dlouhý jako samotná zpráva. Proudové šifry se vyznačují snadnou hardwarovou implementací. I když bývají podstatně jednodušší než blokové algoritmy, mohou být stejně bezpečné nebo i bezpečnější. Například Vernamova šifra, používající jen jednoduchou funkci XOR, je při správném použití nerozluštitelná. Podoba zprávy vytvořená z šifrovaného textu je závislá pouze na klíči. Nevýhodou je dlouhý klíč, který navíc nelze použít vícekrát. V případě zadržení zprávy i zašifrovaného textu lze snadno získat klíč.

1.4 Symetrické blokové šifry

Symetrické blokové šifry jsou typické šifry moderní doby, které k šifrování i dešifrování používají stejný klíč a data šifrují v blocích. Bloky i klíče mohou mít různou délku. Šifrování v blocích je složitější než šifrování po jednotlivých bitech a zvyšuje bezpečnost algoritmu. Používání bloků navíc umožňuje použití matematických operací dat uložených v maticích, a tak otvírají další možnosti pro šifrovací algoritmy. Dnešní počítače zvládají šifrování symetrickou blokovou šifrou velmi rychle, rychlost algoritmu AES dosahuje na dnes už běžných počítačích přes 150 MB/s, což je srovnatelné s možnostmi pevných disků.



Obr. 1. schéma činnosti symetrické šifry

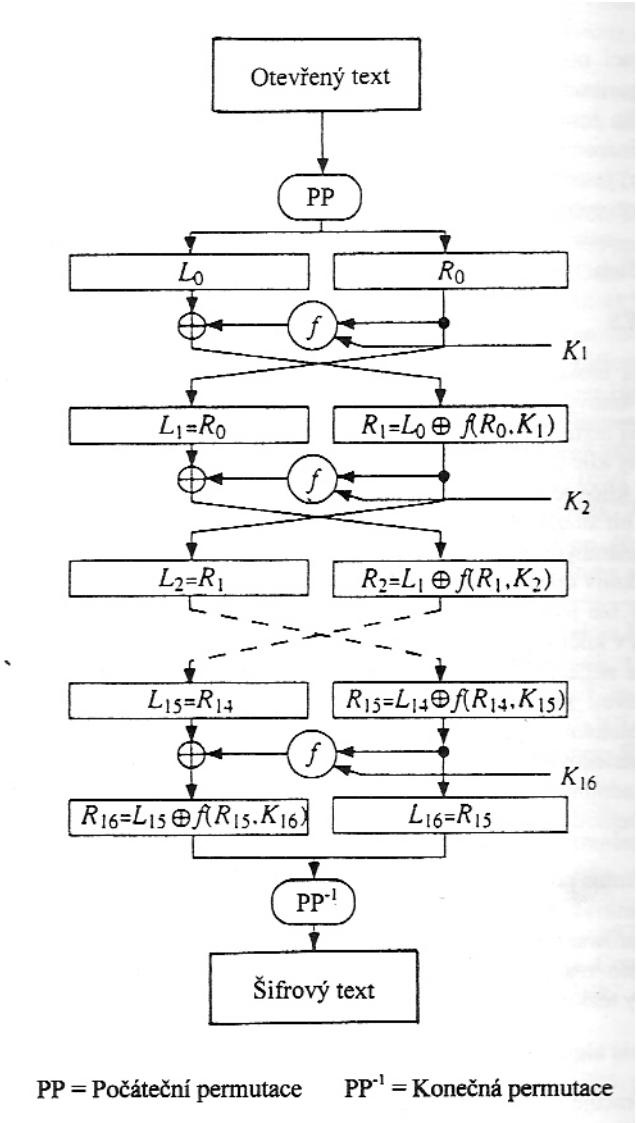


Obr. 2. tabulka rychlosti symetrických algoritmů

1.4.1 DES

DES (Data Encryption Standard) je šifrovací standard, jenž byl zaveden v roce 1976 Institutem standardů a technologií (National Institute of Standards and Technology), který je součástí ministerstva obchodu Spojených států amerických. Tento standard používá šifrovací algoritmus známý jako DEA (data encryption algorithm), který byl původně vyvinut společností IBM pod názvem Lucifer. Konečná podoba algoritmu je výsledek spolupráce IBM, NIST a NSA. Původně navrhovaná varianta algoritmu Lucifer používala délku klíče 128 bitů a 128 bitové bloky, nakonec však byla použita délka pouze 64 bitů,

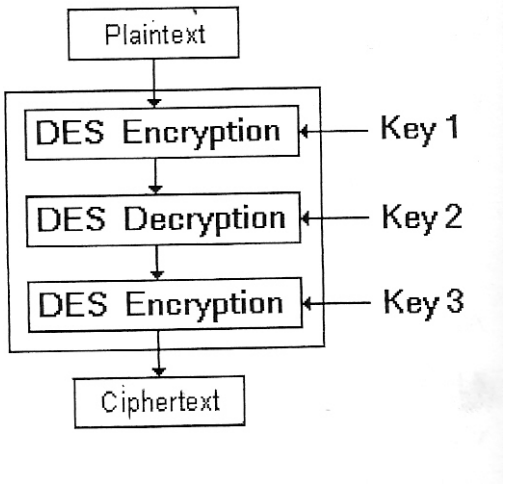
z toho pouze 56 efektivních. NSA spolupracovala s firmou IBM na zesílení algoritmu proti všem útokům kromě útoku hrubou silou. Délka klíče 56 bitů byla kritizována jako nedostatečná už v době vzniku standardu, přesto ale tento algoritmus odolával až do roku 1998. DES pracuje s 64-bitovými bloky otevřeného textu. Po počáteční permutaci je blok rozdělen na pravou a levou polovinu, každou o délce 32 bitů. Poté následuje 16 kol identických operací, nazývaných funkce f, v nichž dochází ke kombinaci dat s klíčem. Po šestnáctém kole se levá a pravá polovina spojí a konečná permutace (inverzní počáteční permutace) algoritmus zakončí. [6, s. 69]



Obr. 3. podrobné schéma algoritmu DES [2]

1.4.2 Triple DES

Triple DES, známý i jako 3-DES nebo TDES, je zesílená varianta šifrovací normy DES. Samotný šifrovací algoritmus neprošel žádnou změnou, ale šifrování dat probíhá třikrát, s použitím tří klíčů. Základní schéma se skládá z procesu šifrování, dešifrování a opětovného šifrování. Protože proces dešifrování probíhá jiným klíčem, nejde o dešifrování ve smyslu převodu šifrovaného textu na původní text, ale o převod jednoho šifrovaného textu na jiný. V podstatě jde opět o proces šifrování, avšak s opačnou posloupnosti kroků. Další šifrování probíhá podle použité varianty s použitím buď s použitím stejného klíče jako u prvního procesu šifrování nebo s použitím třetího klíče. Obě tyto varianty se dají považovat za bezpečné, protože odstraňují největší nedostatek šifrovací normy DES - nedostatečnou délku klíče. Přestože je 3-DES považován za bezpečný šifrovací systém, existují v dnešní době kvalitnější a efektivnější alternativy.



Obr. 4. základní schéma algoritmu 3-DES [2]

1.4.3 AES

AES, neboli Advanced Enryption Standard (pokročilý šifrovací standard) je bloková symetrická šifra nahrazující zastaralý DES a 3-DES, která byla vybrána na základě výběrového řízení vypsaného v roce 1997. Základní podmínkou byla délka klíče minimálně 128 bitů a délka bloku minimálně 128 bitů. Do soutěže bylo přihlášeno 15 různých algoritmů a do finále se dostalo pět. Byli to Rijndael, Serpent, Twofish, RC6 a MARS. Algoritmy byly důkladně prozkoumány, vyhodnoceny jejich klady i zápory a v roce 2002

byl vybrán algoritmus Rinjdael. Rijndael má nastavitelnou délku klíče i bloku 128, 192 nebo 256 bitů a šifrování probíhá v závislosti na délce klíče v 10, 12 nebo 14 kolech. Tento algoritmus kombinuje bezpečnost, rychlost, flexibilitu a hardwarovou implementaci, a právě pro svoji flexibilitu a rychlost byl Rijndael vyhlášen vítězem. Algoritmus AES si našel široké použití v hardwarových zařízení i na úrovni softwaru.

1.4.4 Serpent

Serpent je bloková šifra, která používá klíč o délce 128, 192 nebo 256 bitů a bloky o délce 128 bitů. Na rozdíl od algoritmu Rijndael probíhá výpočet v 32 kolech. Tento algoritmus je bezpečnější, ale pomalejší než Rijndael. To byl také důvod k odsunutí algoritmu Serpent na druhé místo. 14 kol výpočtu bylo podle porotců dostatečné množství. Tvůrci algoritmu Serpent namítali, že jde o nadhodnocení bezpečnosti pro případné nové typy útoků, ale nebyli vyslyšeni.

1.4.5 Twofish

Twofish je další kandidát na AES. Jako ostatní kandidáti používá 128 bitů dlouhé bloky a 128 až 256 bitů dlouhý klíč. Co se týká poměru rychlosti a bezpečnosti, Twofish je kompromis mezí Rijndael a Serpent. Výpočet probíhá v 16 kolech.

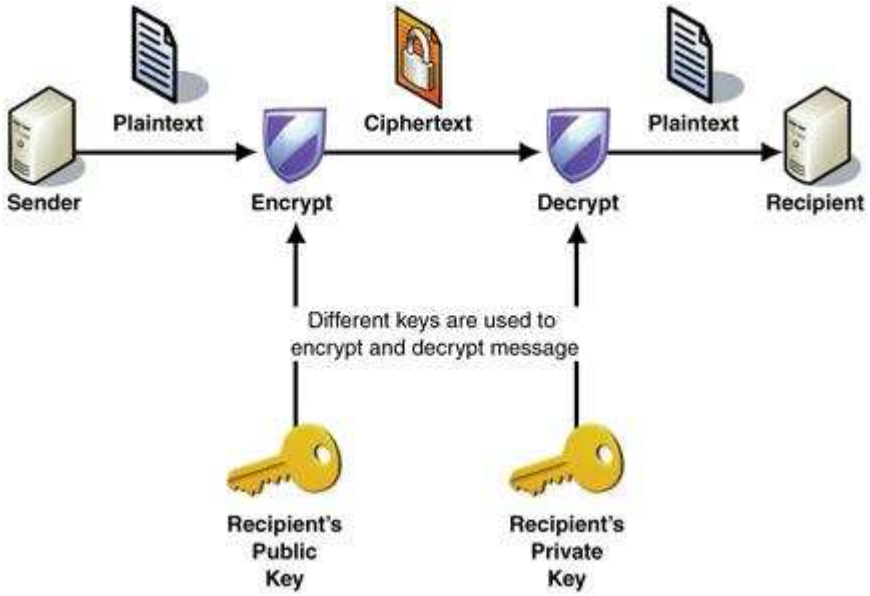
1.4.6 GOST

GOST je symetrický šifrovací algoritmus vyvinutý Sovětským svazem, který byl původně určený jen pro státní správu. Používá 256 bitů dlouhý klíč a výpočet probíhá v 32 kolech. Samotný výpočet v jednotlivých kolech je velmi jednoduchý, ale tuto jednoduchost vyvažuje velkým počtem kol. Tento algoritmus ale pomalu stárne a kvůli malé délce jednotlivých bloků (64 bitů) by jeden klíč neměl být použit k šifrování více než 2^{32} bloků dat stejného kontextu, což odpovídá 34,3 GB dat.

1.5 Kryptografie s veřejným klíčem

Kryptografie s veřejným klíčem používá k šifrování i dešifrování dva různé klíče. Jeden klíč je veřejný, ten slouží pouze k šifrování zprávy pro určitého příjemce a druhý je soukromý klíč, kterým lze zprávu pouze dešifrovat. Mezi veřejným a soukromým klíčem ale existují matematické vztahy, které před útokem hrubou silou vyloučí velkou část všech

možných soukromých klíčů, a proto je nezbytné použít velkou délku klíče. To se bohužel projeví v rychlosti těchto algoritmů, které jsou oproti symetrickým algoritmům velmi pomalé. Nejčastěji se používají k elektronickému podpisu nebo v hybridních systémech, které používají asymetrickou kryptografii k bezpečné distribuci klíče pro symetrické šifrování.



Obr. 5. schéma činnosti asymetrické šifry

1.5.1 RSA

RSA algoritmus byl první algoritmus, který byl vhodný k podpisu zprávy i k samotnému šifrování. Algoritmus vyvinuli Ron Rivest, Adi Shamir a Leonard Adleman. (Zkratka RSA jsou první znaky jejich příjmení.) Je založený na obtížnosti rozkladu velkých čísel na prvočíselné dělitele. To ale značně omezí a zmenší klíčový prostor, protože počet prvočísel je narozdíl od počtu kominací všech čísel relativně malý. Minimální délka bezpečného klíče je 1024 bitů.

tabulka 6 – Porovnání bezpečnosti

Blokové šifry	RSA	Eliptické křivky
56	417	105
64	682	120
80	1464	149
86	1881	161
109	4047	206

Obr. 6. porovnání délky klíčů odpovídající bezpečnosti [2]

1.5.2 DSA

Digital signature algorithm (algoritmus digitálního podpisu) je asymetrický algoritmus určený především k digitálnímu podpisu dokumentů. Algoritmus je založený na obtížnosti řešení úlohy diskrétního logaritmu. Podpis dokumentu probíhá rychleji než jeho ověřování. Délka klíče je ve specifikacích omezena na 1024 bitů a v následujících letech se očekává prolomení tohoto algoritmu.

1.5.3 ECDSA

Tento algoritmus je obdoba DSA, ale k šifrování využívá eliptické křivky. Výhodou tohoto algoritmu je vysoká bezpečnost v porovnání s délkou klíče.

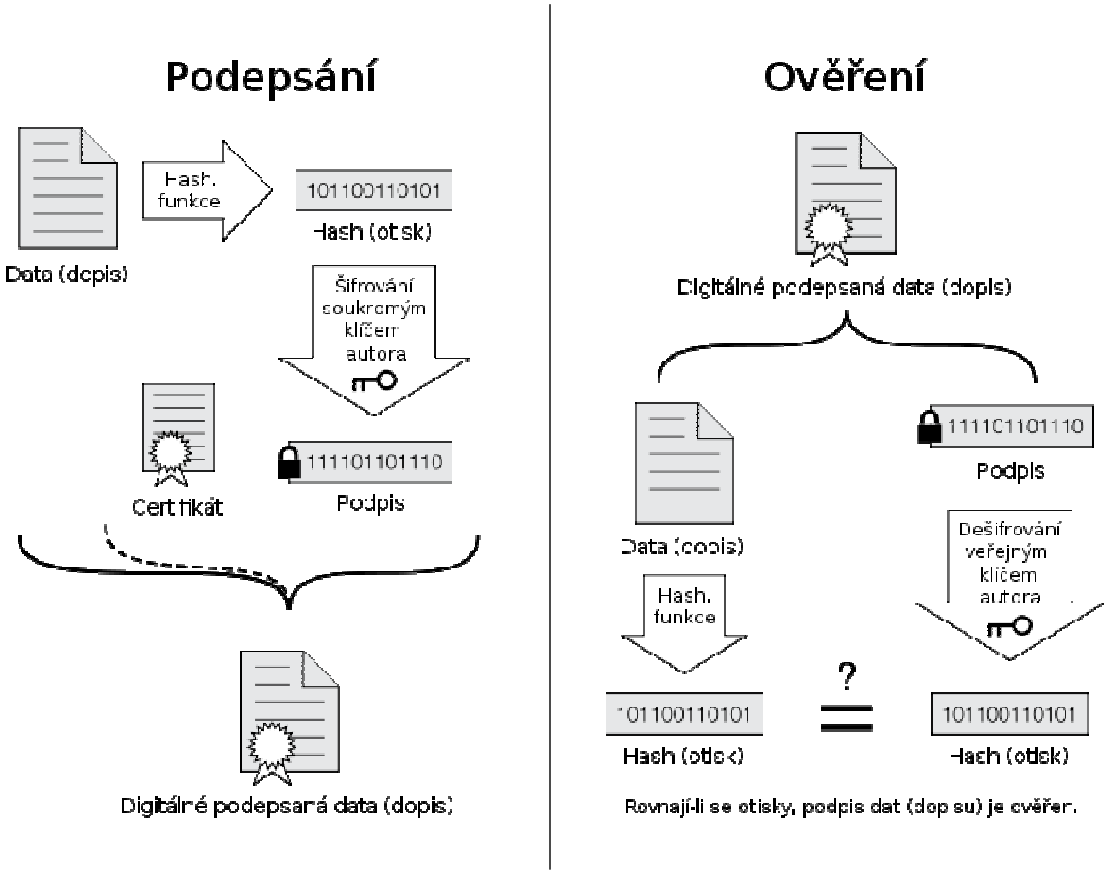
1.5.4 Pohlig-Hellman

Jde o obdobný algoritmus jako RSA, používá ale dva soukromé klíče. Z jednoho klíče lze snadno odvodit druhý klíč. Jeho výhoda je odolnost proti útoku se znalostí původního textu, avšak je pomalejší než jiné algoritmy se soukromým klíčem, a proto se v praxi nepoužívá.

1.6 Elektronický podpis

Elektronický podpis je proces ověření adresáta dokumentu a jeho pravosti. Kombinuje hash funkce a asymetrické algoritmy. Nejprve se vytvoří otisk dokumentu

pomocí hash funkce, výsledek se zašifruje soukromým klíčem odesilatele a podepsaný dokument se odešle. Příjemce odšifruje podpis veřejným klíčem odesilatele (tím získá otisk dokumentu, který vytvořil odesilatel), vytvoří vlastní otisk dokumentu a hodnoty porovná. Pokud se hodnoty shodují, jde o autentický dokument. Když se hodnoty neshodují, je dokument upravený nebo ho odeslal někdo jiný.



Obr. 7. schéma principu elektronického podpisu

1.7 HASH

Hash funkce je šifrovací algoritmus, jehož funkce umožňuje pouze zašifrovat data, ale ze zašifrovaného textu už nelze získat původní text. Vstupní text může mít libovolnou délku, ale výstup hash funkce má vždy délku stejnou. Většinou má výsledek délku v řádech stovek bitů, ale jeho délka není v podstatě omezena. Protože má délka výstupu hash funkce pevnou délku a jsou použity jednosměrné matematické operace, je informace původního textu v podstatě zničena. Ideální hash algoritmus je takový, u kterého sebemenší změna vstupního textu způsobí změnu celého výsledku. Hash funkce se v praxi používají

k vytvoření otisku dokumentu, detekci chyb, ukládání hesel nebo k tvorbě šifrovacích klíčů.

1.8 Bezpečnost kryptografických prostředků

Až do vynálezů počítačů byl neustálý boj mezi tvůrci kryptografických prostředků a kryptoanalytiky. Dlouhou dobu byla výhoda na straně kryptoanalytiků a téměř žádná šifra nezůstala nerozluštitelná. Rychlost šifrování i rychlost kryptoanalýzy byla značně omezena lidským faktorem. S rozšířením počítačů bylo snadné vytvořit proces, který je se znalostí klíče velmi rychlý, ale bez znalosti klíče už je prolomení algoritmu velmi obtížné. U dnes již zastaralých algoritmů byla délka klíče značně omezena výpočetní rychlostí počítačů, v dnešní době se však používají dlouhé klíče, které mají doslova astronomický počet variací. I když byly některé moderní algoritmy mírně oslabeny nebo byl vymyšlený útok proti zjednodušeným algoritmům, k prolomení celého algoritmu za reálnou dobu se nikdo ani nepřiblížil. Případný útok hrubou silou proti symetrickému algoritmu s délkou klíče 256 bitů naráží již na limity fyzikálních zákonů a potřebná energie činí takové útoky nemožné. Počet možných kombinací klíče v závislosti na jeho délce je exponenciální funkcí, zatímco rychlost šifrování roste jen lineárně. Případné zdvojnásobení délky klíče je poměrně snadné, rychlost šifrování se sníží na polovinu, ale počet kombinací vzroste z 2^{256} na 2^{512}, což je 2^{256} krát víc. Kdyby například existovalo 10^9 počítačů, které by vyzkoušely 10^{15} klíčů za sekundu, trval by útok hrubou silou na 256 bitů dlouhý klíč $7{,}8 \times 10^{45}$ let.

Útoky proti samotným algoritmům nebo klíčům jsou prakticky vyloučeny, existují jiné cesty k prolomení systému. Nejjednodušší způsoby získání utajovaných informací je tzv. rubber-hose cryptoanalysis (pendreková kryptoanalýza), která spočívá v získání klíče násilím, nebo metoda zvaná purchase-key attack, u kterého si klíč jednoduše koupíme úplatkem. Další metody využívají jiných slabin celého systému a může jít o odposlouchávání, nasazení agenta, použití malwaru (keylogger, trojský kůň, backdoor, spyware...) nebo třeba získání hlavního klíče.

1.9 Současné trendy a budoucnost kryptografie

Od konce studené války probíhá proces privatizace kryptografie, který bude velmi pravděpodobně pokračovat i nadále, kryptografie tak bude čím dál více součástí běžného života. S rozvojem mobilních zařízení, jako jsou například notebooky nebo inteligentní

mobilní telefony, je třeba dbát především na flexibilitu kryptografických algoritmů a protokolů. Převážně v oblasti mobilních komunikačních technologií se dá očekávat upřednostňování flexibilního softwarového řešení kryptografie, protože vylepšení softwaru je jednodušší a levnější než přebudování celé komunikační sítě. Rozvoj kryptografie může ohrozit vývoj kvantových počítačů, které by teoreticky mohly vyzkoušet všechny klíče za velmi krátkou dobu. Vývoj takových počítačů se zatím potýká s problémy a vůbec není jisté, zda bude plně funkční kvantový počítač vůbec fungovat.

2 MALWARE

Malware - jinými slovy škodlivý software, nebo i škodlivý kód - je jakýkoli program, část programu nebo script, který je vytvořený za účelem škodit. Malwarem je infikovaná podstatná část počítačů, přesto není nutné panikařit. Pojem „škodlivé účinky“ je velmi široký a velká část malwaru způsobuje jen zanedbatelné škody. Podle dostupných údajů je až 30% počítačů chráněných antivirovým programem nakaženo malwarem. Toto vysoké číslo není překvapivé, jelikož většina uživatelů, kteří mají počítač v domácnosti, pravidelně podceňuje základní pravidla prevence a slepě spoléhají jen na ochranu antivirového programu. U firemních počítačů nebo počítačů zkušených a pozorných uživatelů se dá očekávat toto procento nakažených počítačů významně nižší.

2.1 Typy malwaru

Jak se vyvíjel obor výpočetní techniky, měnily se i programové podmínky, zranitelná místa počítačů a spolu s nimi se vyvíjel samozřejmě i malware. Můžeme jej klasifikovat podle různých kritérií, např. dle způsobu šíření, charakteru možné škody či dle struktury malwaru. Nejčastěji se používá následující dělení.

2.1.1 Virus

Když se řekne škodlivý software, většina lidí i z řad „laiků“ si vybaví právě počítačový virus. Ostatní typy škodlivého softwaru bývají často mylně považovány za viry, i když tato kritéria nesplňují. Počítačový virus je významová analogie běžného, biologického viru. Kritéria, podle kterých se pozná počítačový virus, jsou schopnost sebereplikace (kopírování sama sebe) a nutnost hostitelského souboru. I když je virus nejznámější typ malwaru, je v poslední době nahrazován jinými typy se specifickým zaměřením nebo se složitou strukturou.

2.1.2 Trojský kůň

Trojský kůň je malware, který je součástí jiného programu. Tento program plní svou běžnou funkci, avšak bez vědomí uživatele také způsobuje různé škody. Trojské koně jsou poměrně nebezpečné, protože je v podstatě nainstaluje sám uživatel. Při instalaci programu se totiž může objevit požadavek na udělení výjimky ve firewallu, například z důvodu

aktualizace programu. Uživatel pak může v dobré víře povolit škodlivému programu připojení k internetu a otevře tak brány svého počítače trojskému koni.

2.1.3 Červ

Červ je malware, který ke své činnosti nepotřebuje hostitelský program a šíří se prostřednictvím počítačové sítě. Po infikování počítače převezme kontrolu nad komunikačními prostředky, které posléze používá k dalšímu šíření nebo k plnění své funkce. Červ může plnit stejné funkce jako trojský kůň, ale šiří se bez nutnosti zásahu ze strany uživatele. Narozdíl od trojských koní je potenciálně nebezpečnější (šíří se sám pomocí sítě), ale na druhou stranu je také snadněji rozeznatelný. U propracovaných trojských koní bývá obtížné rozpoznat, co je žádoucí funkce programu a co již nikoliv.

2.1.4 Backdoor

Malware typu backdoor vytváří zadní vrátka, která umožní vzdálený přístup k počítači. Napadení takovým malwarem často předchází větší útok proti počítačovému systému, a proto je vhodné napadený počítač důkladně zkontrolovat, zvlášť když jde o firemní počítače s důvěrnými informacemi.

2.1.5 Adware

Adware se často nepočítá mezi malware, nebo je zařazován pod spyware. Jeho účel je specifický a často má škodlivé účinky, a proto si adware zaslouží plnou pozornost. Adware je složenina slov advertising-supported software, neboli reklamou podporovaný software. Adware na první pohled nevypadá jako klasické počítačové viry, ale může způsobit značné škody: často mění domovskou stránku bez souhlasu uživatele, přesměrovává spojení, otvírá vyskakovací okna nebo i přímo vytváří falešné výstražné zprávy operačního systému. Adware bývá méně škodlivý než ostatní malware a je finančně lukrativní pro své distributory. Adware bohužel často odkazuje na zavirované internetové stránky, vytváří zadní vrátka, nebo je přímo součástí podvodu.

2.1.6 Spyware

Tento zástupce malwaru je velmi nebezpečný a může způsobit značné škody. Spyware neohrožuje integritu dat, ale přímo bezpečnost informačního systému. Instaluje

keyloggery, odesílá hesla a přihlašovací jména, vyhledává a ukládá šifrovací klíče nebo odesílá celé soubory. Spyware je hlavním prostředkem pro získávání hesel, krádeže identity, krádeže informací nebo i při stalkingu. Často mívá podobu rootkitu a skrývá svou aktivitu. Jeho odstranění bývá komplikované a obyčejné antivirové programy nemusí stačit.

2.1.7 Exploit

Exploit není škodlivý kód plánovitě napsaný za účelem škodit. Exploit je nějaká chyba v programu, která vznikla buď nedopatřením nebo přehlédnutím chyby, kterou je možné zneužít k neoprávněnému přístupu k počítačovému systému nebo k datům. Sám exploit není přímo malware, protože není vytvořený s úmyslem škodit, ale toto označení se používá i k označení škodlivého programu nebo kódu, který takové chyby využívá. S exploity se nejčastěji setkáváme v operačních systémem, a to hlavně ze dvou důvodů. Operační systém je velmi komplexní software. Čím je systém složitější, tím je vyšší pravděpodobnost chyby a kvůli rozsahu se jen obtížně kontrolují drobné chyby, které nezpůsobují chyby v rámci normálního provozu. Druhý důvod je ten, že právě přes operační systém se útočník může dostat k datům nebo může i dálkově ovládnout počítač. Nejčastěji se o exploitech mluví v souvislostech s operačním systémem MS Windows, avšak tyto chyby jsou přítomny i v jiných operačních systémech. MS Windows je nejpoužívanější operační systém a je tedy zcela logické, že právě na něj se soustředí převážná část útoků. I když jsou exploity v programu nevyhnutelné, je možné riziko minimalizovat pravidelnými aktualizacemi, kvalitním antivirovým programem, firewallem a především účinnou prevencí.

2.1.8 Rootkit

Rootkit je sada softwarových prostředků sloužící k zamaskování své aktivity nebo i jiného malwaru před antivirovým programem, operačním systémem či před samotným uživatelem. Napadený operační systém se na první pohled chová zcela běžně, a tak je detekce rootkitů problematická. K jejich odhalení je nezbytná podrobnější znalost rutinního chodu operačního systému. Rootkity nejčastěji napadají API (application programming interface, rozhraní pro programování aplikací), jsou postavené mezi hardware a operační systém, a proto je k jejich stoprocentnímu odstranění potřeba přeinstalovat operační systém.

2.1.9 Keylogger

Tyto nebezpečné programy bývají součástí i jiného malwaru, jako například rootkitů, červů nebo trojských koní. Keylogger je určen k detekci stisknutých kláves a k jejich ukládání nebo i odeslání. Z takových údajů je možné podle znaku „@“ najít a rozpoznat emailovou adresu a heslo, které bývá napsané nejčastěji ihned po emailové adrese. Keyloggery velmi často zatěžují procesor (občas i 100% výkonu procesoru), pevný disk nebo síťové zařízení, čímž na sebe uživatele PC upozorní. Škodlivé následky můžeme eliminovat použitím firewallu, který filtruje příchozí i odchozí komunikaci.

2.1.10 Dialer

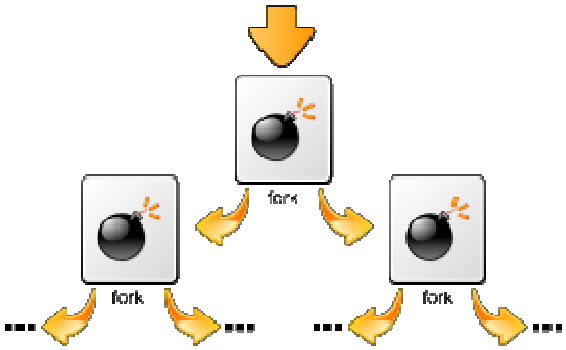
Tento malware přesměrovává vytáčené číslo v případě modemového připojení k internetu přes drahé telefonní linky. S nástupem digitálního připojení k internetu (ASDL, WI-FI,) dialer téměř vymizel. Štafetu po něm převzal URL injector, který přesměrovává web adresy a v podstatě krade výdělek z reklamy.

2.1.11 URL injector

Jak jsem již zmiňoval dříve, tento malware přesměrovává připojení k určité internetové stránce. Nejčastěji je používán k reklamním účelům (platba za zobrazení reklamy), ale může být použit i k jiným, nebezpečnějším formám útoku, jako například přesměrování na podvodné nebo zavirované stránky.

2.1.12 Wabbit

Historie tohoto vzácného malwaru sahá do šedesátých let, kdy se na počítačích začal objevovat program zvaný „Králík“. Sám o sobě neškodil, nenapadal další počítače a jen kopíroval sám sebe. Škodlivý byl až následný pokles výkonu a úložné kapacity. Tento typ malwaru je možné snadno upravit k působení škod, jako například DoS útoky typu „Fork bomb“. Tato metoda útoku používá řetězovou reakci, kdy jeden proces spustí další dva, ty spustí další 4, až dojde k zastavení celého systému nebo služby. Běžné routery, síťové prvky nebo programy již bývají běžně odolné proti podobným útokům.



Obr. 8. fork bomb

2.2 Rizika malwaru pro data

Malware se od počátku používání počítačů velmi změnil. Původně šlo jen o žerty, které pouze obtěžovaly a zpomalovaly chod počítače, avšak postupem času se účel změnil. Malware se záhy začal využívat k destruktivním účelům, kterých dosahoval mazáním souborů, smazáním systému souborů nebo i šifrováním pevného disku. V poslední době se malware začal komercializovat a jeho hlavním účelem se stal zisk. Dnešní rizika jsou především krádež identity, získávání hesel, získávání čísla kreditních karet, zneužívání vzdálených počítačů k dalšímu šíření malwaru nebo přímo ke krádeži informací. Cíle jednotlivých typů malwaru se mohou lišit, nejčastěji to však bývá jeden nebo i více z následujících:

- umožnit vzdálený přístup k počítači

Malware se pokusí umožnit vzdálený přístup k počítači jedné osobě nebo okruhu lidí. I po odstranění škodlivého kódu může být v bezpečnosti počítače díra, kterou lze zneužít.

- automatické posílání spamů

Nejčastěji jde o červy nebo trojské koně, které rozesílají emaily či jiné nevyžádané zprávy. Mohou také automaticky přidávat odkaz za každou odeslanou zprávu nebo i přílohu k emailu. Napadenému počítači tento malware nemusí vysloveně škodit, ale uživatel tohoto počítače často ztrácí důvěru v e-mailové služby nebo se jeho emailový nebo jiný účet může dostat na jednu z mnoha černých listin. Poté často nezbývá nic jiného, než si nechat zkontrolovat a vyčistit počítač a založit si zcela nové účty různých komunikačních služeb.

- krádež dat

Toto je spolu s mazáním souborů největší riziko malwaru pro datovou bezpečnost. Krádež dat může být dlouhou dobu nezjištěna a v takovém případě hrozí únik důvěrných informací nebo i know-how společnosti. Může být tedy ohrožena prosperita společnosti a v důsledky i její samotná existence. Za tímto účelem se používají backdoory, trojské koně, keyloggery, spyware nebo rootkity. Největší riziko způsobují cílené útoky kombinující více typů malwaru.

- stahování dat z internetu

Infekce downloaderu může být začátek většího útoku na počítačovou síť. Existují specializované trojské koně, které stahují další malware, buď náhodně, nebo i cíleně. Mohou vytvořit zadní vrátka, jako například otevřít port určený k přijímání dat.

- úprava nebo mazání souborů v počítači

Destruktivní malwary jsou naštěstí v dnešní době v útlumu, ale stále se vyskytují. Mohou způsobit značné škody, které se však dají zmírnit pravidelným zálohováním dat. I když je hlavním cílem dnešních virů zisk, nevyplatí se toto riziko podcenit. Záloha může obnovit data, ale rozhodně ne všechna. Práce provedená před další zálohou může být nenávratně zničena a čas potřebný k nahrání zálohovaných dat také není zanedbatelný. Úprava souborů může mít různé motivy. Může jít o nově infikovaný soubor, činnost rootkitu nebo vytváření zadních vrátek.

- sledování aktivity počítače

Do této kategorie patří sledování prohlížených internetových stránek, spuštěných aplikací, činnost keyloggeru i sledování jiných činností. Pokud je taková činnost malwaru zaměřena cíleně, může způsobit rozsáhlé škody, zvlášť když jde o průmyslovou špionáž. Používá se i k legálnímu sledování činnosti vlastních zaměstnanců a ke kontrole jejich práce.

- způsobit chybu systému

Malwarem způsobená systémová chyba většinou pouze „obtěžuje“ uživatele, avšak za určitých okolností může způsobit ztrátu neuložených dat. Takové ztrátě dat můžeme zabránit používáním softwaru s automatickou zálohou v reálném čase, jako například MS

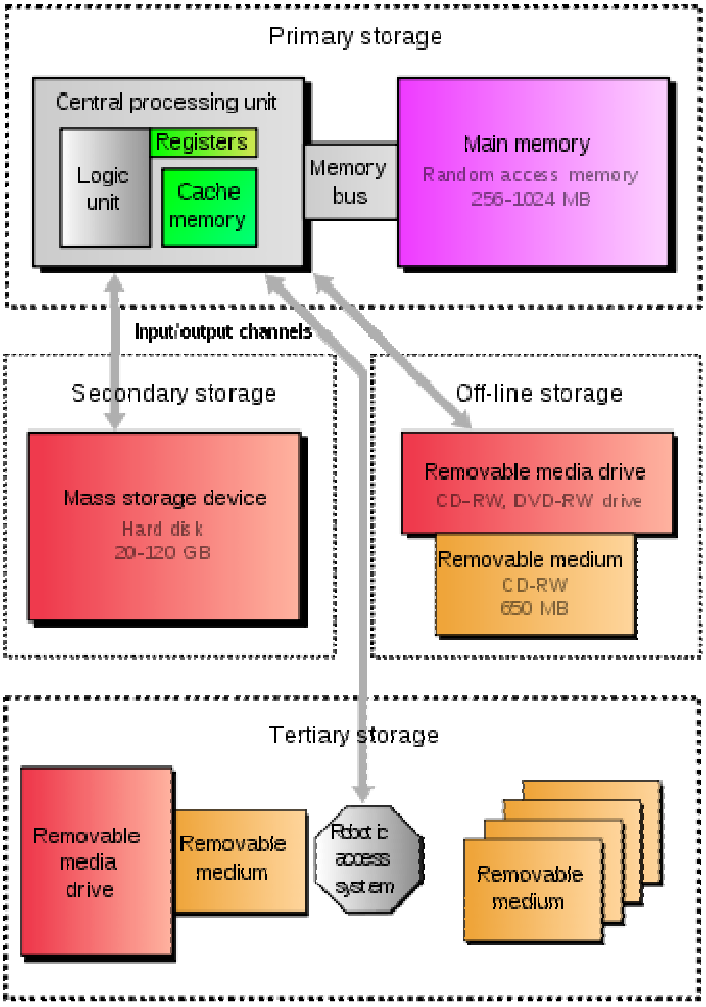
office. V případě počítačových sítí nebo serverů jsou následky vážnější, neboť v takových aplikacích a přidružených službách je stěžejní spolehlivost.

2.3 Současné trendy a budoucnost malwaru

Vývoj nelze zastavit - a to platí i o škodlivém softwaru. Současné trendy jsou spojené především se současným rozvojem sociálních sítí, kde se rozmáhá určitý typ spywaru. Lidé na Facebooku, což je nejmasověji využívaná sociální síť současnosti, bývají často až příliš sdílní, otevření, velmi neopatrní a důvěřiví. Vyvinuly se nové techniky, které používají sociální inženýrství za účelem získávání osobních informací, emailů, telefonů a jiných informací osobního charakteru. Tyto metody jsou často legální, protože uživatel přímo povolí přístup ke svému profilu, ale protože je jejich účelem získávání a zneužití (nejčastěji prodej) osobních informací nebo kontaktů, můžeme tyto aplikace považovat za škodlivý software. Další vývoj lze očekávat v oblasti mobilních telefonů a bezdrátových sítí. I když se flexibilita a schopnosti nových mobilních telefonů blíží běžným osobním počítačům, jejich zabezpečení se často podceňuje.

3 DATOVÁ ÚLOŽIŠTĚ A ZÁLOHA DAT

Protože data musí být někde uložena, je spolehlivost datových úložišť, na kterých jsou uložena, základním předpokladem datové bezpečnosti. Datová úložiště lze kategorizovat podle několika kritérií, ale v souvislosti s datovou bezpečností je nejvhodnější dělení podle vzdálenosti od procesoru. Tento systém třídění dělí datová úložiště na primární, sekundární a terciální. Primární úložiště jsou zařízení přímo propojená s CPU, jako například vyrovnávací paměť procesoru nebo paměť RAM. Primární paměťová zařízení jsou závislá na napájení a neslouží k trvalému uložení dat, jejich spolehlivost tedy přímo souvisí se spolehlivostí celého počítače. Sekundární zařízení jsou propojena s CPU prostřednictvím řadičů, nejčastěji pomocí sběrnice nebo různých portů. Jsou určena k trvalému uložení velkého objemu dat. Jsou pomalejší než primární úložiště a k trvalému uchování dat nepotřebují napájení. Patří zde pevné disky, flash disky, diskety nebo optická média. Poslední skupina, terciární zařízení, jsou taková zařízení, která nejsou trvale připojena a k jejich použití je potřeba lidské činnosti. Patří sem magnetické pásky, nepřipojené externí pevné disky nebo uskladněné optické disky. Terciární zařízení slouží převážně k archivaci aktuálně nepotřebných dat nebo k zálohování dat.



Obr. 9. rozdělení datových úložišť

3.1 Stručný přehled datových úložišť

Rozhodl jsem se napsat stručný výčet datových úložišť, která mají vliv na datovou bezpečnost. Uvedu jejich základní popis, princip funkce a zhodnotím výhody a nevýhody těchto zařízení.

3.1.1 RAM

RAM, známá jako operační paměť počítače, je primární datové úložiště sloužící k dočasnému uložení dat, která mají být v případě potřeby okamžitě k dispozici, nebo dat, se kterými se v daném okamžiku pracuje. Paměť RAM je dvojího typu. Statická RAM (SRAM) je tvořena transistory (6 tranzistorů na jeden bit) a nepotřebuje pravidelnou obnovu. K udržení dat potřebuje jen velmi malý proud, řádově µW. Narozdíl od dynamické RAM je výroba náročnější a hustota dat menší, a proto se v počítačích používá především

jako vyrovnávací paměť, například cache procesoru. SRAM má dobu odezvy v řádu několika ns. Dynamická RAM (DRAM) je tvořena pouze tranzistorem a kondenzátorem na jeden bit, což umožňuje výrobu velkokapacitních paměťových čipů, ale elektrický náboj v kondenzátorech se musí pravidelně obnovovat, jinak se za určitý čas vybije. Vzhledem k velké hustotě dat občas dochází k nežádoucí změně jednotlivých bitů, které mohou způsobit chybu programu a mohou vést k systémové chybě. Proto se vyrábí varianta operační paměti s ECC (Error-Correcting Code memory), která umožňuje detekci a opravu jedné chyby v 64 bitovém bloku paměti a detekovat (bez opravy) až dvě chyby. I když je taková paměť pomalejší a dražší, je její použití vhodné v aplikacích, kde je potřeba stoprocentní spolehlivost, jako například servery. DRAM má dobu odezvy v desítkách nanosekund, nejčastěji okolo 40-60 ns.

Obr. 10. paměťový modul RAM

3.1.2 Pevný disk

Pevný disk (HDD, Hard Disc Drive) je sekundární datové úložiště, pracující na základě magnetického záznamu a umožňující trvalé uložení dat. První pevný disk byl představen roku 1956 společností IBM. V osobních počítačích se začal používat v osmdesátých letech, kdy začal rychlý růst kapacity a pokles ceny. Pevný disk se skládá z ploten, hlav a elektroniky. Každý disk má až pět kovových nebo skleněných ploten pokrytých magneticky měkkou vrstvou, které se otáčí velkou rychlostí, od 5400 do 15000 otáček za minutu. Pevný disk má několik hlav, nejčastěji dvě hlavy na jednu plotnu. Hlavy jsou v dnešních discích poháněny lineárním elektromotorem. Každý pevný disk disponuje

elektronikou, která zajišťuje správný pohyb hlav, čtení, zápis, opravu chyb, organizaci dat, vstup a výstup. Adresace dat byla u pevných disků podle fyzické polohy dat, ve formátu cylinder-head-sector, (česky stopa-hlava-sektor nebo válec-povrch-výseč). U disků větší kapacity se tento systém adresace nepoužívá. Dnešní pevné disky používají adresaci LBA (logical block addressing). Ten čísluje jednotlivé bloky dat postupně od nuly. Protože už adresace neurčuje fyzickou polohu dat a počet sektorů v jednotlivých stopách se liší, rozhoduje o pořadí operací elektronika pevného disku.

Obr. 11. vnitřek pevného disku

3.1.3 FDD

Hovorově disketová mechanika, floppy disk drive, je výraz, který označuje zařízení používající přenosné diskety. Původně byly diskety $5^1/_4$ palců velká, plochá a pružná média s kapacitou 360 kB nebo 1,2 MB. Postupem času se zvýšila hustota záznamu a disk byl zmenšen na $3^1/_2$ palce. Změnil se i původně ohebný obal na pevný plastová kryt a čtecí a záznamová část byla opatřena posuvným kovovým krytem. Kapacita těchto disků byla 360 kB, 720 kB a později až 1,44 MB. I když je jejich kapacita už nedostačující, stále se s nimi můžeme setkat i v praxi, nejen v „IT muzeu“.

3.1.4 SSD disk

Solid state drive je zařízení, které používá stálou elektronickou paměť. Nejvíce se podobá RAM paměti a flash paměti, ale je uzpůsobeno k rychlému zápisu a čtení. Oproti klasickým pevným diskům je poměrně drahý, ale je mechanicky odolnější a má rychlejší přístupovou dobu. Používá se nejčastěji v malých a přenosných zařízeních, kde je potřeba odolnost proti otřesům, malá velikost nebo nízká spotřeba.

Obr. 12. SSD disk

3.1.5 Flash disk

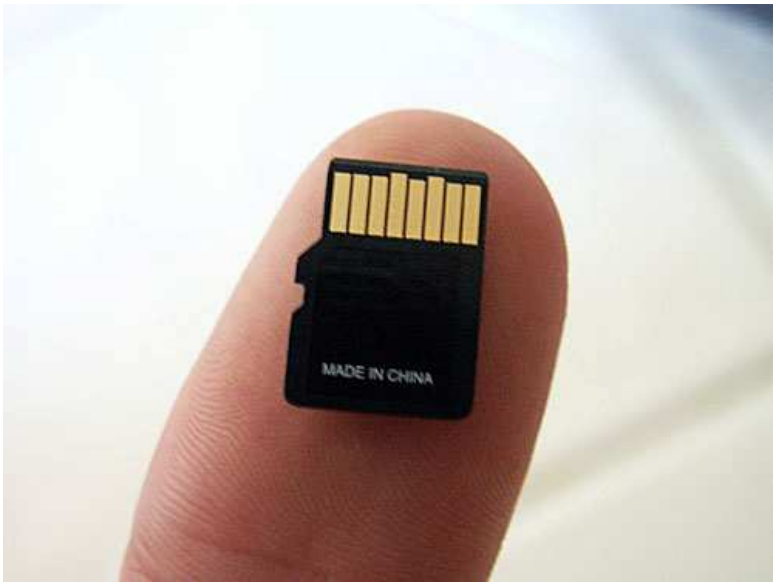
Flash paměť je trvalá elektronická, programovatelná, respektive vymazatelná paměť. Hlavní výhoda je velká kapacita v porovnání s velikostí a flexibilita. Nevýhodou je pomalý zápis, který je způsoben nutností vymazání části paměti a jejího následného naprogramování. Jeho nevýhoda je omezený počet přepsání, po kterém paměť přestává fungovat. Mívají kapacitu v řádu jednotek a desítek GB.

3.1.6 CD/DVD/BLU-RAY

Jde o optická média, která jsou obvykle používána k ukládání filmů, hudby nebo k zálohování dat. Zápis je v porovnání s rychlostí čtení pomalý proces, který probíhá pomocí laserového paprsku. Ten způsobuje změnu odrazivosti povrchu, která je použita k definici logické jedničky a nuly. CD DVD a BLU-RAY se liší především hustotou záznamu. Existují i přepisovatelné varianty, které mají nízkou rychlost zápisu a většinou se před použitím musí smazat. Přístupová doba bývá i několik sekund.

3.1.7 SD

SD karty, neboli secure digital, je obdoba flash paměti, která je v podobě malé paměťové karty. Nejčastěji se používají v malých zařízení, jako například fotoaparáty, mobilní telefony nebo mp3 přehrávače. Existují různé varianty, které se liší především kapacitou a velikostí.



Obr. 13. paměťová karta SD-micro

3.2 Vlivy jiného HW na bezpečnost dat

Datová bezpečnost je velmi komplexní problém a není moudré zanedbat vliv hardwaru na bezpečnost uložených dat, především jejich integritu. Největší vliv na bezpečnost dat má zdroj počítače, základní deska a výše popsaný pevný disk. V menší míře může integritu dat ovlivnit i ostatní HW nebo jeho části, jako například řadič pevných disků.

3.2.1 Zdroj počítače

V počítači se pojmem zdroj neoznačuje přímo zdroj elektrické energie, ale zařízení, které převádí střídavé síťové napětí na stejnosměrné napětí různých voltáží. Zdroj počítače přivádí elektrickou energii do různých zařízení jako je základní deska, pevné disky, display nebo i do grafické karty. Důležité vlastnosti každého zdroje jsou výkon, účinnost, bezpečnostní prvky, počet výstupů a typy výstupních konektorů. Existují i záložní zdroje, které napájí počítač v případě výpadku z baterií.

3.2.2 Základní deska

Základní deska je základní hardware každého počítače. Umožňuje komunikaci všech ostatních zařízení s procesorem. Obsahuje procesor, paměť RAM, přídavné karty, konektor k připojení pevných disků a jiná zařízení. Na základní desce bývá často integrována zvuková karta, řadiče pevných disků, grafická karta a různé řadiče vstupu a výstupu.

3.3 Záloha dat a archivace

Důležitost zálohování snad ani nemusím připomínat. Záloha dat a archivace mají různý účel, jsou to velmi podobné pojmy, a navíc používají podobné technické prostředky. Právě kvůli společným technickým prostředků při jejich realizaci je zmiňuji v rámci jednoho oddílu své bakalářské práce. Jak k zálohování tak k archivaci se používají především terciární a sekundární datová úložiště. Pro účely zálohování je nejdůležitější spolehlivost zařízení pro účely archivace, dále je velmi důležitá i životnost zařízení a nároky na skladování. Nejčastěji se používají magnetické pásky, pevné disky, lokální i vzdálené servery a v menší míře i optická média. Ať již použijeme jakýkoli prostředek, můžeme zálohování kategorizovat do tří základních typů.

3.3.1 Plná záloha

Tento typ zálohy spočívá v záloze všech dat, nejčastěji v pravidelných časových intervalech. Původně se z důvodu časové a technické náročnosti procesu zálohování používal jen tento typ, ale s rozvojem rychlých datových médií a počítačových sítí začal rozvoj rychlých a snadných metod zálohování. Tento způsob se dnes používá jako základ zálohy, pokud nebyla vytvářena hned od vzniku systému.

3.3.2 Přírůstkové zálohování

U tohoto způsobu zálohování se k plné záloze přidávají pouze data vytvořená od minulé zálohy. Tyto přírůstky jsou na sobě závislé a při chybě jednoho přírůstku není možné obnovit následující přírůstky. Výhoda tohoto způsobu zálohy je úspora místa.

3.3.3 Rozdílové zálohování

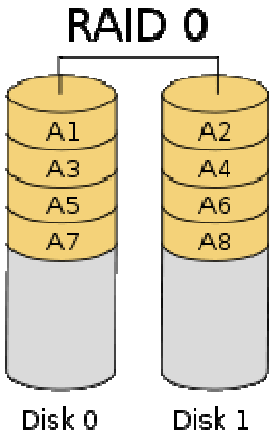
Jak již název napovídá, rozdílová záloha zaznamenává rozdíl dat od plné zálohy. Tyto rozdíly jsou na sobě nezávislé a k obnově dat stačí plná záloha a libovolný přírůstek. Jde o kompromis mezi plnou a přírůstkovou zálohou.

3.4 RAID

Tato čtyři písmena značí „Redundant Array of Independent Disks“. Většinou se tato zkratka překládá do češtiny jako vícenásobné diskové pole nezávislých disků, ale tento překlad není ideální, protože vynechává slovo redundant – nadbytečný, které je k pochopení základních principu nezbytné. RAID používá ukládání nadbytečných dat na jednotlivé pevné disky, což umožní budoucí opravu vzniklých chyb. Existuje velký počet typů tohoto systému, které používají vytváření duplicitních dat na více pevných discích, vytváří kontrolní součty nebo kombinují různé metody.

3.4.1 RAID 0

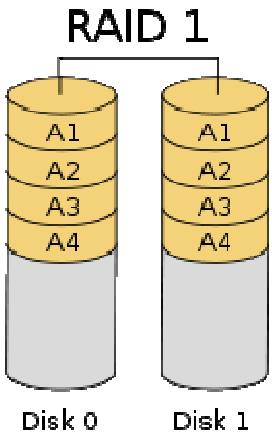
Tento typ není tak úplně RAID, protože neukládá žádná nadbytečná data a nezvyšuje bezpečnost, ba dokonce ji přímo snižuje. Využívá paralelního ukládání dat na více pevných discích za účelem zvýšení rychlosti čtení a zápisu (stripování dat). Teoreticky se rychlost zvýší tolikrát, kolik je v poli disků, v praxi je však zvýšení rychlosti menší. Činnosti disků je nutné koordinovat, což nezbytně vede k omezení přístupové doby a rychlost samotné sběrnice také není neomezená. Použitý hardware musí být schopný zpracovávat data rychleji, než je součet rychlostí disků. Další omezující faktor je průměrná velikostí souborů a velikostí sektoru. I když nejde přímo o RAID, je podporován stejnými řadiči jako jiné typy, často se kombinuje s ostatními konfiguracemi RAID a právě proto se mezi RAID počítá.



Obr. 14. princip činnosti RAID 0

3.4.2 RAID 1

Nejbezpečnější konfigurace RAID vytváří kopii pevného disku v reálném čase. Stejná data jsou ukládána na dva různé disky, při výpadku jednoho disku je tak k dispozici druhý. Tyto disky jsou použitelné i při selhání řadiče RAID, protože jde o dva obyčejné disky s normální strukturou dat. Pro takové ukládání dat potřebujeme dva pevné disky stejné kapacity a získáme celkovou kapacitu jen jednoho z nich.



Obr. 15 . princip činnosti RAID 1

3.4.3 RAID 2

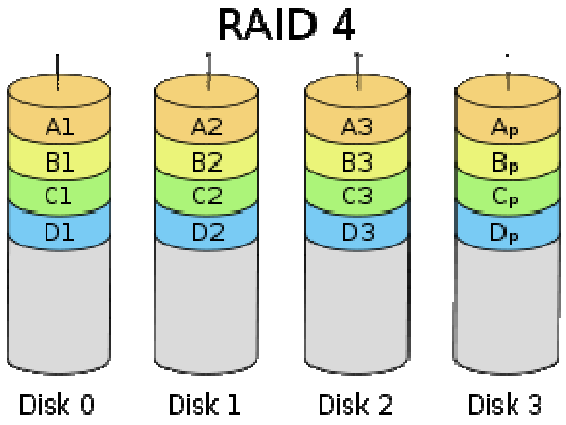
Raid 2 stripuje data po jednotlivých bitech a ukládá kontrolní součet Hammingovým kódem na paritní disky. Rychlost rotace disků je synchronizována. V praxi se RAID 2 moc nepoužívá, protože používá velký počet paritních disků a propustnost dat je malá.

3.4.4 RAID 3

Data jsou stripována po bajtech a kontrolní součty (XOR) jsou ukládány na samostatný disk. RAID 3 umožňuje rekonstruovat data při výpadku jednoho disku. Paritní disk je však nejvíce zatěžován a zpomaluje tedy rychlost všech zbývajících.

3.4.5 RAID 4

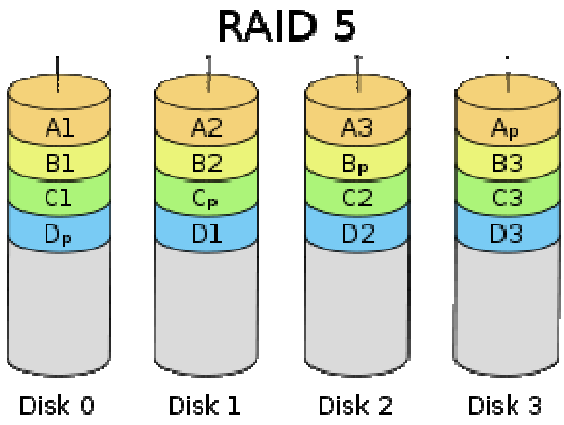
Obdobná funkce jako RAID 3, ale data se ukládají po blocích.



Obr. 16. princip činnosti RAID 4

3.4.6 RAID 5

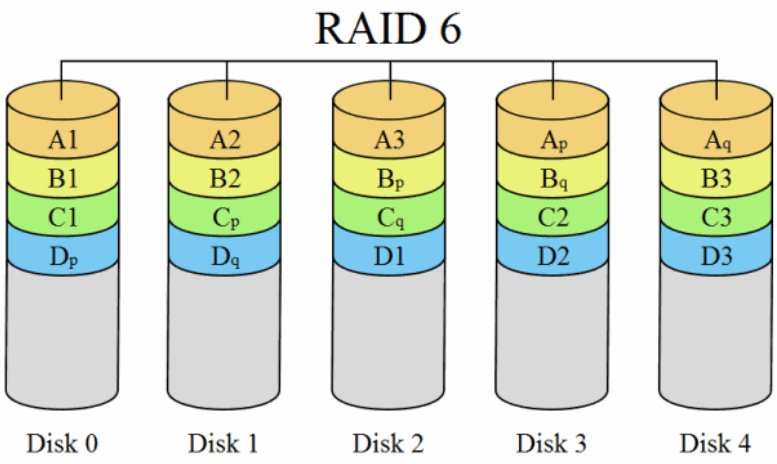
RAID 5 stripuje data po blocích a parita je ukládána střídavě na všechny disky. Protože se parita ukládá na všechny disky, není rychlost limitována rychlostí paritního disku. RAID 5 má nejlepší poměr samotných dat k celkové kapacity všech disků a velkou rychlost.



Obr. 17. princip činnosti RAID 5

3.4.7 RAID 6

Jde o RAID 5 se zvýšenou schopností opravy dat. Ke každému bloku se ukládají dvě různé parity, a tak je možné opravit chyby dvou disků.



Obr. 18. princip činnosti RAID 6

4 POČÍTAČOVÁ SÍTĚ

Možnost propojení a spolupráce více počítačů je dnes jednou z nejdůležitějších funkci počítačů. V dnešní době existují různorodá využití společné práce velkého počtu počítačů. Jde jednak o drobnosti jako je sdílená složka a společné hraní počítačových her, tak o obrovské vědecké projekty, na kterých spolupracují stovky tisíc počítačů. Za zmínku stojí vědecký program SETI určený k hledíní mimozemského života, který v roce 1999 spustil rozsáhlý projekt distribuovaných výpočtů, ke kterému se může přihlísit libovolný počítač. Projekt byl velmi úspěšný a vedl k vytvoření projektu BOINC, který nemá definovaný účel a mohou ho využít různé projekty. Jednou z možností jeho využití je například i tvorba tzv. duhových tabulek, které jsou jednou z účinných metod kryptoanalýzy.

4.1 Typy sítí podle rozlehlosti

Nejpoužívanější rozdělení počítačových sítí je podle fyzického rozsahu jejich struktury.

4.1.1 PAN

Personal area network, neboli osobní síť je nejméně rozlehlou sítí určenou k propojení různých osobních zařízení. Přenos probíhá nejčastěji bezdrátově a maximální vzdálenost přenosu je velmi malá. Důležitá je především odolnost proti rušení, kontinuita spojení, snadná konfigurace a nízká spotřeba. Nejznámějšími zástupci jsou IrDA a bluetooth.

4.1.2 LAN

Jedná se o lokální síť menšího rozsahu, nejčastěji v rámci jednoho objektu, například domácnost, kancelář nebo celou budovu. Lokální síť je často připojena k rozsáhlé síti za pomocí routeru. Důležitá je především přenosová rychlost a spolehlivost.

- Ethernet

Ethernet je nejrozšířenější kabelové propojení lokální sítě, které umožňuje rychlé připojení počítačů na vzdálenost řádu několik stovek metrů až několik kilometrů. Síťový

řadič ethernet je běžnou součástí základních desek počítače, což značně snižuje náklady na vybudování systému lokální sítě.

- Wi-fi

Je to bezdrátová technologie, která si získává popularitu hlavně u přenosných zařízení. Současný vývoj této technologie je velmi rychlý a v sítích malého rozsahu (domácnost, malá kancelář apod.) výrazně vytlačuje kabelové propojení.

4.1.3 WAN

WAN je síť velkého rozsahu, která často přesahuje hranice měst, států nebo i kontinentů. Může propojovat jak jednotlivé lokální sítě, tak i jednotlivé počítače. Nejrozsáhlejším a nejznámějším zástupcem je internet, což je globální počítačová síť, která používá komunikační protokoly rodiny TCP/IP. Internet je neoddělitelnou součástí života každého současného obyvatele naší planety. Internet slouží k mnoha účelům, je zdrojem informací či zábavy a v poslední dekádě se výrazně zapojil i do business sféry či mezilidské komunikace. Spolu s výhodami a novými příležitostmi však internet přinesl i nové hrozby a formy zločinu.

II. PRAKTICKÁ ČÁST

5 OCHRANA DAT PŘED ZNIČENÍM NEBO POŠKOZENÍM

Zabezpečení dat před zničením nebo poškozením je základ datové bezpečnosti, protože bez samotných dat postrádají ostatní metody jejich ochrany smysl. Důležitý je pojem integrita dat, který označuje celistvost dat. Můžeme zde zahrnout nejenom stav, kdy jsou přečtená data shodná s uloženými, ale i pravost a nezaměnitelnost dat nebo i celistvost jejich struktury. V této kapitole se budu zabývat především metodami, které mohou zabránit ztrátě, zničení nebo poškozením dat. Data jsou vždy přítomná na nějakém nosiči, datovém médiu. Tato datová média mají určitou životnost a spolehlivost, se kterou musíme počítat.

5.1 Výběr hardwaru počítače

Data může ohrozit i samotný hardware počítače. Jak datová média, tak i jiný hardware má určitou chybovost, která může způsobit škody. Vliv na bezpečnost dat má zdroj počítače a základní deska. Výběr tohoto hardwaru závisí na účelu počítače a požadované spolehlivosti. Základní deska počítače propojuje všechny ostatní části počítače. Případné selhání základní desky může vést i k poškození uložených dat, protože jsou pevné disky nejčastěji připojené k základní desce. Základní deska by v každém případě měla obsahovat teplotní čidla, která slouží k monitorování kritických prvků, jako je například procesor. Tato čidla lze nastavit, aby se základní deska vypnula v případě, kdy se teplota důležitých součástí základní desky blíží kritické teplotě. To platí částečně i o zdroji počítače, který také může obsahovat teplotní čidla. Důležité je zvolit dostatečně výkonný zdroj s vysokou účinností. Výkon zdroje časem klesne vlivem stárnutí a pokud není vybrán zdroj s jistou výkonnostní rezervou, může docházet k přetěžování zdroje nebo k nedostatečnému zásobování počítače elektrickou energií. Účinnost zdroje hraje roli v zahřívání zdroje a v jeho životnosti, protože se elektrické ztráty přeměňují na teplo.

Obr. 19. základní deska

5.2 Použití datových médií

Nejčastější metoda ochrany integrity dat je zálohování. Když data existují na více médiích současně, velice to sníží pravděpodobnost jejich zničení. Můžeme použít celou řadu médií, od optických disků, přes externí pevné disky až po vzdálenou zálohu na nějakém serveru.

- Optická média

Optická média jsou vhodná k zálohování a archivaci kvůli snadné použitelnosti, přenositelnosti a snadné archivaci. Jejich nevýhoda je především v pomalém zápisu a v závislosti životnosti na okolních vlivech. Životnost optických médií je závislá na způsobu jejich uložení a na jejich archivaci, protože samotný záznamový povrh není krytý před působením vzduchu a vlhkosti, jak je to například u pevného disku, který má pevný kryt. Jsou citlivá na mechanické poškození spodní vrstvy, na čistotě spodní plochy a na působení UV záření, prachu a vlhkosti. Životnost omezuje i kvalita záznamu. Potenciální životnost těchto médií je až na 100 let, ale tato hodnota platí pouze za naprosto ideálních podmínek. V praxi se může pohybovat v rozmezí 5-20 let.

- Pevný disk

Nesporná výhoda pevného disku je pevný kryt, který kryje samotné záznamové plotny. Pevné disky mají velkou hustotu dat, velkou kapacitu a rychlost zápisu i čtení je

vysoká. Nevýhoda je možnost poškození dat působením mechanických vibrací v okamžiku zápisu.

- Externí pevný disk

Externí pevné disky jsou konstrukčně velmi podobné pevným diskům. Nabízí snadné připojení pomocí portu USB a některé typy umožňují i automatickou zálohu stisknutím jediného tlačítka na disku. Jsou také náchylné k otřesům, ale existují i varianty, které jsou odolné i proti pádu.

- SSD

SSD disky fungují jako velká, trvalá elektronická paměť. Mývají velkou kapacitu, i když menší než pevné disky. Výhodou je absence pohybujících se součástek a rychlost zápisu. Problém je cena, která je vzhledem ke kapacitě poměrně vysoká.

- Magnetické pásky

Ideální médium k zálohám velkého rozsahu je právě magnetická páska. Má velkou kapacitu, dlouhou životnost, ale na druhou stranu má dlouhou přístupovou dobu. Magnetické pásky nejsou vhodné k zálohování menších a rychle se měnících systémů.

- Disková pole

RAID je vhodný způsob zálohy dat, který funguje v reálném čase. Místo obyčejného kopírování dat funguje naprosto automaticky. Nejvhodnější je RAID 1, 5 nebo 6. Raid 1 podporují i běžné osobní počítače, ale raid 5 nebo 6 už mohou vyžadovat speciální diskový řadič. Nejčastější použití rozsáhlejších diskových polí je v serverech. Zvlášť u použití varianty 5 a 6 je zapotřebí kvalitní diskový řadič. Některé diskové řadiče umožňují používat v módech 5 a 6 ještě jeden náhradní disk, na který jsou v případě poruchy automaticky obnovována data. Podrobněji jsem se diskovým polím věnovat již v teoretické části.

- Využití vzdálených serverů

Existují společnosti, které prodávají a pronajímají místo na vzdálených serverech, speciálně určených k zálohování dat. I když takové řešení ušetří spoustu práce s nákupem, instalací a provozem vlastních záložních mechanismů, vzdáme se kontroly. Tato metoda zálohování je založena na důvěře a spolehlivosti provozovatele a nezbývá nám nic jiného, než věřit v zabezpečení našich dat. Také je třeba zajistit bezpečný přenos dat, nejlépe s pomocí kryptografie.

6 OCHRANA PC PŘED MALWAREM

Použití antivirového programu je dnes běžný standart. Existuje velký počet kvalitních antivirových programů a některé z nich jsou dokonce pro použití v domácnosti zdarma. Ochrana před malwarem ale nezávisí pouze na antivirovém programu, ale i na internetovém prohlížeči, operačním systému, zabezpečení počítačové sítě, ale hlavně závisí na uživateli. Nejdůležitější je vyvarovat se rizikovému chování, jako je prohlížení nedůvěryhodných internetových stránek, instalace softwaru z nedůvěryhodného zdroje nebo i otevírání emailových příloh od neznámých adresátů.

6.1 Funkce antivirového programu

Antivirový program nebrání malwaru v jejich činnosti přímo, ale detekuje jejich přítomnost v souborech a skriptech. Když najde škodlivý kód, zabrání spuštění souboru nebo skriptu a varuje uživatele. Protože je v každém počítači velký počet souborů, kontroluje antivirový program především spuštěné, kopírované, stáhnuté nebo jinak „aktivní“ soubory. Kompletní antivirový scan všech souborů počítače je velmi pomalý, přesto by se však měla provádět jako periodická pravidelná kontrola. Antivir kontroluje i zdrojový kód internetových stránek a vyhledává v něm potenciálně nebezpečný kód. Antivirový program je vhodné doplnit o kvalitní firewall a případně i specializovaný software určený k ochraně před spywarem a adwarem. Až v kombinaci antivirového programu s firewallem a opatrným uživatelem dosáhneme efektivní ochrany před malwarem.

6.2 Firewall

Nestačí jen kontrolovat obsah souborů, ale je nutné kontrolovat a řídit i přijímání a odesílaní dat počítačovou sítí. Firewall spravuje síťovou komunikaci různých počítačů a nastavuje pravidla síťové komunikace. Ke kvalitní ochraně musí být nastavená pravidla, podle kterých se určuje, kterému programu bude povoleno odesílání a přijímání dat a kterému ne. I v případě firewallu by se měl uživatel vyvarovat rizikovému chování, jako například častému vypínání firewallu nebo povolení připojení neznámých programů k síti.

Existují i softwarové produkty, které zasahují i mimo oblast funkce obyčejného firewallu nebo antivirového programu. Například Comodo Firewall obsahuje funkci

defense+, která kontroluje rizikové chování procesů, jako například vytváření nových procesů, přístupu k chráněným registrům, pokusu o zpřístupnění programu v paměti a jiné podezřelé aktivity. Comodo Firewall se může „naučit“ běžný provoz počítače a poté varuje jen v případě neobvyklých situací. Tato funkce vyžaduje pokročilé znalosti uživatele, ale dokáže zabránit škodám, kterým nezabrání antivirový program ani firewall.

6.3 Preventivní chování uživatele

Nejlepší, ale také často podceňovanou ochranou před malwarem je prevence. Když se vyvarujeme nebezpečným a rizikovým aktivitám, můžeme riziko infekce malwarem výrazně minimalizovat. Zmínil bych především pozornost a opatrnost uživatele, protože nejnebezpečnější situace vznikají právě nepozorností nebo nedůsledností uživatele.

6.4 Rizikové chování

V této kapitole shrnu nejčastější rizikové chování a možnosti prevence před infekcí malwarem, nebo i jinými škodami.

6.4.1 Otevírání neznámých emailů

Email od neznámého odesilatele nebo email s podezřelým obsahem bychom nikdy neměli otevírat. Ke spolehlivému rozeznání podezřelých emailů nejsou potřebné rozsáhlé znalosti a stačí pouze opatrnost a zdravý rozum. Tyto emaily jsou často napsané anglicky nebo jsou špatně přeložené automatickým překladačem, bývají velmi stručné (například jen „To musíš vidět“) a nebo vůbec nedávají smysl. Může napovědět i emailová adresa odesilatele, která může obsahovat klíčová slova jako „noresponse, no-replay, discount, -20%“ a další. Pokud takový email obsahuje přílohu, jde pravděpodobně o hoax (nepravdivou, lživou informaci) nebo o počítačový virus. Zvlášť rizikové jsou soubory s příponou .vbs, které mohou obsahovat nebezpečný skript.

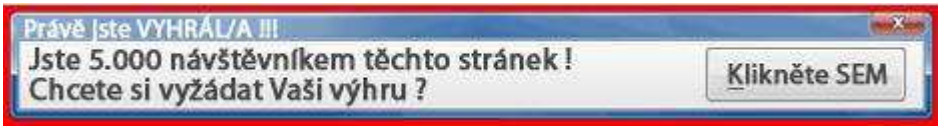
6.4.2 Instalace nedůvěryhodného SW

Software z neznámého zdroje bychom nikdy neměli instalovat. Jde především o freeware programy, které jsou k dispozici na různých serverech, které umožňují sdílení nebo stahování právě takových programů. Většinou mají neznámého výrobce, nebo jeho výrobce není známá společnost. Tyto programy nenabízí žádnou záruku spolehlivosti a

mohou obsahovat malware, nejčastěji trojské koně. Takové programy mohou chtít při instalaci povolit výjimku ve firewallu z důvodu aktualizace. V mnohých případech pak může sám uživatel povolit malwaru přístup k internetu.

6.4.3 Navštěvování rizikových internetových stránek

Malware se nejčastěji nachází na stránkách s velmi lákavým obsahem. Může jít o pornografii, nákupy zdarma, výherní loterie, počítačové hry, stahování zdarma nebo jiný lákavý obsah. I když samotné tyto stránky nemusí přímo obsahovat škodlivý kód, velmi často obsahují velké, barevné a blikající odkazy na zavirované nebo podvodné stránky, nebo automaticky otevírají nová okna prohlížeče na těchto stránkách. Vyhnout se takovým stránkám je jednoduché. Stačí neklikat na podezřelé odkazy na internetových, jako například „máte nepřečtenou zprávu“ nebo „blahopřejeme, jste miliónty návštěvník“.



Obr. 20. typický podvodný banner

6.4.4 Počítač přístupný ostatním osobám

Zvlášť v případech používání osobního počítače v domácnosti k pracovním účelům je třeba se zamyslet nad tím, jestli vůbec bude počítač přístupný ostatním členům rodiny a za jakých podmínek. Tím se totiž vlastník počítače částečně vzdává kontroly nad použitím počítače, protože nemůže neustále sledovat a kontrolovat aktivitu ostatních členů rodiny na počítači. Pokud se takový počítač stane nějakým typem veřejného počítače, je závažný problém jen otázka času. Takový počítač bývá totiž kvůli velkému tranzitu různých programů, her a dokonce i malwaru značně nespolehlivý. Případné škody lze zmírnit šifrováním, zavedením druhého operačního systému, pravidelným zálohováním dat, ale takový počítač už nemůžeme považovat za úplně bezpečný.

6.4.5 Další hrozby z internetu

Jak se zvětšuje vliv internetu na každodenním životě, je zneužití internetu k vlastním cílům čím dál tím lákavější a výnosnější. V dnešní době existují na internetu i jiné hrozby než malware, jako například krádeže identity, peněz nebo i krádeže elektronických účtů.

V poslední době ale existuje poměrně nové riziko používající sociální sítě v kombinaci se sociálním inženýrství. Budu se věnovat hlavně hrozbám krádeží identity, osobních údajů a některým jednoduchým a účinným metodám prevence.

6.5 Krádež identity

Se vzrůstajícím počtem údajů identifikujících určitou osobu roste i riziko, že tyto informace někdo zneužije k vlastnímu užitku. Čísla kreditních karet, čísla bankovních účtů, telefonní čísla a spousta dalších informací o nás se někde válí na internetu. Když se tyto informace dostanou do nepovolaných rukou, může nás to stát víc než jen nějakou tu tisícovku. Pokud jsou totiž naše informace použity například k páchání trestné činnosti, může mít tento problém následky třeba i v osobním nebo společenském životě. Mezi nejžádanější krádeže informací patří především čísla kreditních karet, hesla, PIN kódy, domovní adresy, emailové adresy, telefonní čísla, data narození, rodná čísla, čísla řidičského průkazu nebo detaily o úvěrech. Některé z těchto údajů nejsou používány přímo ke krádežím peněz, ale i k prodeji. Vždyť který lichvář by nechtěl vědět emaily, adresy, telefonní čísla nebo stávající dluhy ostatních? Tyto informace jsou často určeny k volnému prodeji. Velká část lidí si tyto informace nijak nehlídá a často je poskytují i dobrovolně, třeba i na požádání.

6.6 Ochrana internetového bankovnictví

Internetové bankovnictví je dnes velmi oblíbenou službou. Komu by se chtělo chodit do banky a ještě platit další poplatky, když máme internet. Jenže internetové bankovnictví láká zloděje úplně stejně jako samotné banky, pošty a spořitelny. Internetové bankovnictví je docela dobře chráněné, ale kde je lidský faktor, tam je i riziko selhání. Nejpoužívanější zabezpečení internetového bankovnictví používá víc než jeden způsob autentizace, například kód odeslaný na mobilní telefon, magnetickou kartu nebo i klíčový soubor.

- phishing

Tato metoda je založena na rozesílání emailů, které mají donutit adresáta poslat osobní informace. Tyto emaily mohou mít i změněnou hlavičku emailu, takže to vypadá, jako by email poslala třeba banka. Takový email mívá nejčastěji čtyři části. Obecný pozdrav (paní, pane,...), uvedení hrozby (smazání Vašeho účtu, počítačový virus), žádost o osobní informace (telefon, číslo účtu) a odkaz (většinou podezřele dlouhý). Můžeme tomu

zabránit firewallem, antivirovým programem a hlavně opatrností. Nejdůležitější je nikdy neposílat takové osobní informace emailem.

- Pharming

Pharming je sofistikovaná podvodná metoda. Napadá Domain Name System (DNS), který je zodpovědný za překlad URL adres na jejich skutečné číselné adresy. Když v internetovém prohlížeči zadám adresu, počítač se připojí k DNS serveru, který najde adresu požadované internetové stránky. V podstatě jde o nějaký druh spojovatelky. Když je ale informace na DNS serveru změněna, mohu skončit na úplně jiné internetové stránce, ale v prohlížeči se zobrazí správná URL adresa. Metoda Pharming používá právě tohoto k přesvědčení obětí podvodu, aby zadali osobní číslo a PIN. Útok může být proveden i změnou nastavení DNS serveru v počítači, k čemuž může posloužit malware. Tato metoda je obdoba útoku man-in-the-middle, česky „muž mezi“. Tomu může zabránit antivirový program, který dokáže kontrolovat nastavení adresy DNS serveru.

6.7 Metody ochrany osobních údajů

Snad nejúčinnější prevencí je zase opatrnost a rozumné uvažování. Jednoduchým zákazem ukládání a automatického vyplňování hesel v prohlížeči můžeme předejít možnému ohrožení. Nejen že jsou tato hesla automaticky vyplňována, ale jsou i uložena někde v počítači. Internetové prohlížeče umožňují jejich ochranu nějakým hlavním heslem, ale této možnosti zase většina uživatelů neví nebo nejsou ochotní při každém spuštění prohlížeče zadávat heslo. Tato hesla je možné v prohlížeči (například Mozilla Firefox) velmi snadno zobrazit, a to i s uživatelskými jmény i s internetovou adresou účtu. Používání této funkce je lepší se vyvarovat, protože k získání těchto informací stačí jen krátký přístup k počítači. Toto riziko můžeme omezit například vyžádáním uživatelského hesla po zrušení spořiče obrazovky, což znemožní tyto informace rychle a jednoduše zjistit. Nejlepší je ale nepoužívat vyplňování hesel. Můžeme použít i šifrování, který může zabránit úniku citlivých údajů i v případě krádeže počítače. Další, ještě účinnější metodou, je osobní informace neukládat, neodesílat nezabezpečeným informačním kanálem a už vůbec takové informace nezveřejňovat na internetu, zvlášť na sociálních sítích.

6.8 HOAX

HOAX je výraz pro lživou nebo poplašnou zprávu, která se šíří nejčastěji pomocí emailové komunikace. Tyto zprávy mohou obsahovat nebezpečné rady, podvodné prosby o pomoc, počítačové viry nebo mohou jen uživatele obtěžovat. Další problém těchto zpráv je, že zbytečně zatěžují servery. Když tyto zprávy posíláme dalším lidem, můžeme ztratit jejich důvěru, nebo se dokonce může stát, že naše emailová adresa bude zařazena na nějaký černý list. Naše zpráva pak může být automaticky zařazena mezi spamy. Typický HOAX má naštěstí několik prvků, podle kterých ho můžeme spolehlivě rozpoznat.

- Popis nebezpečí

Nejčastěji počítačový virus

- Popis možné škody

Počítačový virus, který spálí pevný disk počítače

- Uvedení důvěryhodného zdroje

Microsoft varuje, uvádí zdroj CNN a podobné

- Výzva k dalšímu rozeslání

Nejtypičtější je pro HOAX právě výzva k dalšímu rozeslání

6.9 Riziko sociálních sítí

Velký boom sociálních sítí s sebou přináší i rizika. Lidé jsou na sociálních sítích velmi otevření, přátelští a neopatrní. Je třeba si uvědomit, že k informacím uložených v mém profilu mají k dispozici všichni přátelé, ale i různé aplikace nebo hry, kterým takový přístup povolíme. Jako příklad popíši jednu podezřelou aplikaci, která na facebooku koluje. Tato aplikace umožňuje odpovědět na osobní otázky o nějakém příteli. Problém je, že odpovědi na otázky jsou přístupné pouze v případě, že aplikaci povolíme přístup k informacích o vlastním účtu. Aplikace má již 5 000 000 uživatelů (tj. minimálně 5 000 000 emailových adres), a tento počet se pořád zvyšuje. A proč to vlastně funguje? Může za to zvědavost. Kdo by nechtěl vědět, co si o něm říkají ostatní. A to někteří lidé mají na svém účtu nejenom emailovou adresu, ale i rok narození, adresu, vzdělání a zaměstnání, oblíbené sporty, záliby a nebo osobní fotky. O prodeji těchto informací (u této konkrétní aplikace) neexistuje žádný důkaz, avšak dokážu si představit, jakou hodnotu mají tato data např. pro marketingové společnosti. Já osobně doporučuji použít k účtu na

facebooku nově vytvořený email, na který klidně mohou přicházet spamy nebo jiná „havěť“. V žádném případě není vhodné zadávat do profilu žádné osobní informace, nebo aspoň omezit přístup k těmto informacím.

Obr. 21. povolení přístupu k informacím o účtu

7 ZABEZPEČENÍ LOKÁLNÍ SÍTĚ

Lokální sítě zažily v poslední době velký rozvoj, hlavně v oblasti bezdrátových sítí. S nimi se vyvíjely i způsoby jejich ochrany. Samotný boom technologie wi-fi byl tak rychlý, že se nutnost zabezpečení těchto sítí zatím nevžila stejně jako antivirová ochrana. U těchto sítí jde především o snadné připojení, málokdo zkrátka přemýšlí o zabezpečení své sítě. Velká část lidí se připojí automaticky k libovolné dostupné bezdrátové síti, aby se mohli připojili k internetu. V případě nezabezpečených sítí vím z vlastní zkušenosti, že převážnou část majitelů notebooku, například studentů, neodradí ani výstražná zpráva, že jde o nezabezpečenou síť.

7.1 Bezpečnost připojení k wi-fi

Bezdrátové připojení je sice pohodlné, ale také méně kontrolovatelné, než propojení kabelem. Kabel je možné fyzicky zkontrolovat a zabezpečit, ale elektromagnetické záření se volně šíří prostorem. Byly zavedeny technologie šifrování a autentizace, podobně jako zavedené DES nebo AES, ale narozdíl od zmíněných symetrických algoritmů má zabezpečení bezdrátových sítí jen krátkou životnost. [7]

Obr. 22. wi-fi router

7.1.1 WEP

Wired Equivalent Privacy je první používané zabezpečení bezdrátových sítí. První verze používá 40 bitů dlouhý klíč a 24 bitový inicializační vektor, ale nakonec byla zvýšena délka klíče na 104 bitů. WEP používá proudovou šifru a klíč by se neměl opakovaně používat k šifrování velkého množství dat. Právě proto existuje inicializační vektor, který funguje podobně jako SALT. Ten je ale velmi krátký a existuje 50% šance opakování stejného vektoru každých 5000 odeslaných datových paketů. V roce 2001 byla zveřejněna kryptoanalýza, která využívá odposlechu komunikace. Touto metodou je možné zjistit klíč za několik minut. WEP už je dávno překonaný, ale hardwarová zařízení jej stále podporují a pořád se v menší míře používá.

7.1.2 WPA a WPA2

Wi-Fi Protected Access (WPA) a WPA2 jsou komunikační protokoly, které postupně nahrazují starý WEP. WPA používá stejná algoritmus jako WEP (RC4), ale inicializační vektor má délku 48 bitů a klíč je 128 bitů dlouhý. Používá automaticky se měnící klíč (TKIP), který má zabránit možnému útoku. Jeho pokročilá verze WPA2 je dnes už standardem pro bezdrátová zařízení a nabízí velkou bezpečnost. WEP2 přidává algoritmus CCMP, který je odvozený od AES. WPA nebo WPA2 obsahuje i kontrolu integrity dat kontrolním součtem.

7.1.3 Komu není rady, tomu není pomoci

Bohužel je z dostupných odhadů vidět, že až 40% uživatelů nepoužívá vůbec žádné zabezpečení wi-fi, protože o něm buď neví, nebo ho považují za příliš složité. Asi polovina z těchto lidí spoléhá jen na svůj firewall, který ale nemůže zabránit uživateli ve vědomém odesílání nešifrovaných dat. Naštěstí v roce 2007 vzniky WPS (Wi-fi Protected Setup), což je software určený k usnadnění nastavení WPA2. Umožňuje automatické zabezpečení stisknutím jednoho tlačítka nebo pomocí zadání PIN kódu. Ruční nastavení je sice bezpečnější kvůli kontrole, ale protože je tento produkt zaměřen na skupinu uživatelů, kteří nepoužívají žádné zabezpečení, je to krok správným směrem.

7.2 Zabezpečení vlastní bezdrátové sítě

V předchozí kapitole jsem vysvětlil zabezpečení wi-fi z pohledu uživatele, který se chce připojit k existující síti. Protože jsou ale bezdrátové sítě čím dál víc používány v kancelářích i domácnostech, nejčastěji z důvodu připojení k internetu, budu věnovat pozornost také vytvoření a nastavení bezdrátové sítě. Wi-fi routery jsou již poměrně levné a nabízí celou řadu možných nastavení, kterými lze téměř vyloučit zneužití sítě.

7.2.1 Výběr routeru

Na trhu je spousta routerů, které liší cenou, rychlostí připojení, dosahem signálu i různým příslušenstvím. Otázka vhodného výběru není jednoduchá, protože záleží především na konkrétní situaci. Nejlepší rada je vybírat podle poměru cena, dosah a rychlost. Instalace je většinou podrobně popsaná v příručce a se samotnou instalací nebývá problém. Routery používají standardní nastavení, které umožňuje rychlé připojení bez nutnosti dlouhého nastavování. Pokud ale chceme bezpečnou síť s připojením k internetu, musíme věnovat pozornost některým bezpečnostním prvkům.

7.2.2 Nastavení přístupového hesla

Snad první rada pro zabezpečení routeru je změna přihlašovacího jména a hesla. Standardní nastavení bývá většinou jméno „admin“ nebo „administrátor“, a heslo bývá „admin“, „123456“ nebo třeba jméno výrobce routeru. K routerům se základním heslem se dá snadno připojit a změnit (nejčastěji odstranit) bezpečnostní prvky, nebo se k němu může snadno někdo tajně připojit. Silné heslo je první bariérou, kterou musí případný útočník překonat.

7.2.3 Změna IP adresy

IP adresa routeru bývá v převážné většině případů standardně nastavena na 192.168.0.1. Ponechání této adresy usnadní komukoli změnu nastavení routeru, protože zadáním této adresy do internetového prohlížeče se počítač připojí k nastavení routeru. Pokud je ještě použité základní heslo, je to ještě jednodušší. Toto nastavení taky částečně určuje IP adresu všech připojených počítačů, která se liší pouze posledním číslem. Změna této základní adresy značně zkomplikuje útočníkovi práci.

7.2.4 Nastavení SSID

SSID je v podstatě jméno bezdrátové sítě. Standardně je vysíláno a uvidí ho každý, kdo je v dosahu signálu. Pokud nechceme poskytovat volné připojení všem kolemjdoucím, je vhodné SSID nevysílat. Každý, kdo se chce poté přihlásit, musí vědět, že je v blízkosti router a musí znát SSID. Je to další nastavení, které komplikuje útočníkům práci.

7.2.5 Nastavení bezpečnosti připojení

Toto je snad nejdůležitější nastavení wi-fi routeru. Prakticky všechny routery již umožňují WPA2, a tak rozhodně doporučuji zvolit tuto variantu. V případě nutnosti, třeba nějakého staršího počítače, může být použit i WPA. Rozhodně ale není vhodné zvolit šifrování WEP nebo dokonce šifrování vypnout. K wi-fi se notebooky připojí třeba jen do vzdálenosti dvaceti metrů, ale s kvalitní anténou je možné signál přijímat na větší vzdálenost. S kvalitní anténou je možné zachytit na průměrném pražském sídlišti až několik desítek sítí.

7.2.6 Filtry klientů

Toto je nastavení, které spolu s šifrováním téměř úplně zabrání případnému nabourání do počítačové sítě. Převážná většina routerů umožňuje filtrování podle MAC adresy síťové karty počítače, která je pro každou síťovou kartu unikátní. Můžeme povolit připojení pouze jednotlivým počítačům, které v síti chceme. Je možné i jednotlivým počítačům určit stálou IP adresu podle MAC adresy síťového adaptéru. To nám umožní jednoznačně definovat, který počítač se může připojit k síti a jakou bude mít IP adresu. To může usnadnit i nastavení firewallu.

7.2.7 Wi-fi a firewall

Kvalitní firewally umožňují podrobné nastavení povolené a zakázané komunikace mezi jednotlivými počítači v síti. Pokud používáme síť nejen k připojení k internetu, ale i třeba ke sdílení některých složek, můžeme s pomocí firewallu jednoznačně určit, které počítače si mohou vyměňovat informace. To je možné nastavit podle MAC adresy nebo IP adresy. Správnou kombinací nastavení firewallu a routeru můžeme zabránit škodám i v případě, že se někomu podaří nabourat do bezdrátové sítě, protože firewall neumožní

jeho počítači zpřístupnit soubory ve sdílených složkách (nesouhlasí jeho MAC adresa ani IP adresa).

7.3 Zabezpečení drátové sítě

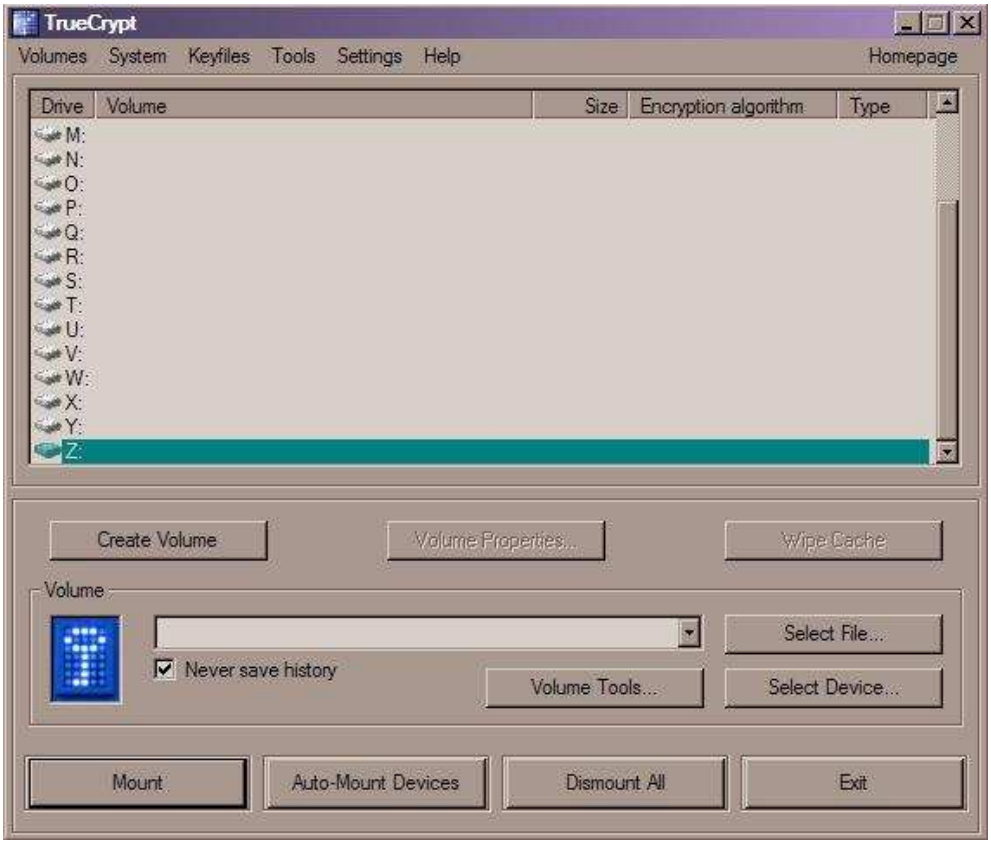
U drátových sítí je možné fyzicky zkontrolovat datové trasy, a proto je zde situace jednodušší než u bezdrátových sítí. Důležitá je hlavně autentizace uživatelů v síti a obecná pravidla firewallu. U rozsáhlejších sítí (třeba kancelářská budova) je vhodné vést záznamy o síťových aktivitách jednotlivých uživatelů.

8 VYUŽITÍ KRYPTOGRAFIE K OCHRANĚ DAT

Správným použitím kryptografie můžeme zabránit zneužití dat, a to i v případě, že data nebo i celý počítač padnou do nesprávných rukou. K zabezpečení uložených dat se používá symetrické kryptografie, šifrování se symetrickým klíčem probíhá nejčastěji šifrováním celých souborů a složek, nebo vytvořením virtuálního disku. K zabezpečení komunikace se používají převážně hybridní systémy, které kombinují symetrické algoritmy, asymetrické algoritmy a někdy i elektronický podpis. Použití asymetrických algoritmů na všechny odesílaná data je velmi pomalé, a tak se zpráva šifruje symetrickým algoritmem a asymetrický algoritmus se používá pouze k zabezpečené symetrického. Ten může být zvolen náhodně, protože je součástí odesílaných dat, a tak nehrozí budoucí zneužití klíče. Nejpoužívanější zástupci šifrovacího softwaru jsou Truecrypt a PGP.

8.1 Truecrypt

Program truecrypt je free-source software určený k symetrickému šifrování dat. Truecrypt nenabízí kromě šifrování žádné doplňkové funkce a je úzce specializovaný na šifrování za provozu počítače. Jeho zdrojový kód je přístupný a může být v případě pochybnosti kontrolován. V minulosti byl jeho zdrojový kód několikrát důkladně zkoumán odborníky a nebyla zjištěna žádná slabina programu nebo zadní vrátka. Program umožňuje několik velmi zajímavých možností, které u jeho konkurentů nejsou obvyklé. Těmito funkcemi jsou klíčové soubory, kaskádové šifrování a skryté svazky.



Obr. 23. grafické rozhraní programu Truecrypt

8.1.1 Základní funkce programu

Truecrypt patří mezi programy vytvářející virtuální disk, který uloží do zašifrovaného souboru libovolného názvu. Umožňuje i šifrování celých, systémových i nesystémových disků. Truecrypt pro soubor svazku automaticky navrhne svou příponu .tc, ale tato přípona zbytečně upozorňuje na přítomnost i umístění šifrovaného souboru. Tento soubor, ve kterém se nachází virtuální disk, je až na prvních 512 bitů (SALT) celý zašifrovaný. SALT je série náhodných čísel, u Truecryptu je to 512 bitů, které se spolu s heslem podílí na tvorbě klíče. Protože Truecrypt šifruje/dešifruje pouze požadovaný souboru, probíhá čtení i zápis dat v reálném čase, bez nutnosti čekat na odšifrování celého souboru. Data se nikdy nevyskytují na disku v původní podobě, jsou odšifrována a šifrována v paměti počítače.

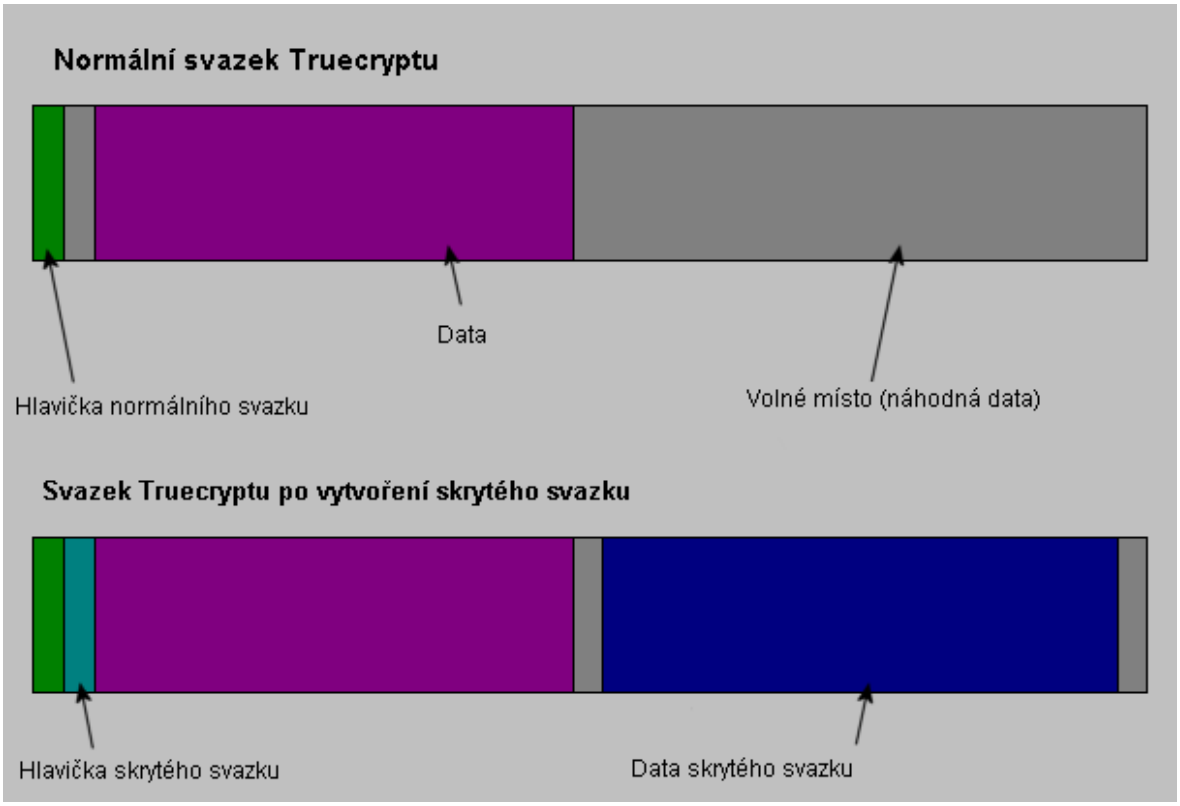
8.1.2 Tvorba klíče

Tvorba šifrovacího klíče je u programů, které vytváří virtuální disk, nejdůležitější proces ovlivňující bezpečnost programu. Soubor virtuálního disku má jednoznačně definovanou strukturu a na určitých místech mají všechny tyto soubory stejná data, což je

možné použít jako základ kryptoanalýzy. Z tohoto důvodu Truecrypt používá složitě generované dva klíče. První klíč (klíč hlavičky) je generován z hesla, náhodných čísel (SALT) a případně i z klíčových souborů a je používán jen k odšifrování hlavičky s druhým klíčem (hlavní klíč). Protože je klíč generovaný i na základě 512 bitů dlouhého náhodného čísla, existuje pro každé heslo 2^{512} možných klíčů, což prakticky vylučuje slovníkový útok proti klíči. Klíč hlavičky je použit jen k odšifrování hlavičky a ihned poté je z paměti počítače vymazán.

8.1.3 Skrytý svazek

Truecrypt umožňuje vytvoření skrytého svazku uvnitř normálního svazku, takže jde v podstatě o steganografii. Tato funkce využívá toho, že se volné místo i šifrovaná data jeví jako náhodná data a nelze je od sebe rozlišit. Tento skrytý svazek je přítomný v místě, kde se nachází volné místo normálního svazku. Při zadání hesla normálního svazku se zobrazí pouze data hlavního svazku, existenci skrytého svazku není možné odhalit jiným způsobem, než zadáním jeho správného hesla.



Obr. 24. formát kontejneru programu Truecrypt

Účel skrytého svazku je zabránit úniku informací v případě, že jsme donuceni prozradit heslo nebo soubor odšifrovat. Aby tato metoda byla účinná, musí být v normálním svazku uložené takové informace, které přesvědčí případného narušitele o tom, že má to, co hledal. Při práci s hlavním svazkem skrytý svazek neodhalí ani sám Truecrypt a hrozí jeho nechtěné přepsání. Program nabízí funkci ochrany skrytého svazku, kdy zadáme obě hesla a Truecrypt zabrání přepsání skrytého svazku.

8.1.4 Klíčové soubory

Použití této funkce velmi zvýší bezpečnost hesla a vlastně i celého šifrování. Klíčový soubor může být libovolný soubor, jehož obsah se bude podílet na tvorbě klíče spolu s heslem. Takový soubor může mít libovolnou délku, ale maximálně 1,048,576 bajtů (1 MB) je použito k tvorbě klíče. Klíčový soubor může být použit i samostatně, bez hesla. Důležité ale je, aby nebyl změněn klíčový soubor, protože by v takovém případě nebylo možné zachránit šifrovaná data. Jako klíčový soubor se nedoporučují systémové soubory, dokumenty a jiné soubory, u kterých lze předpokládat jakoukoli změnu obsahu. Použití klíčových souborů znemožní útoky na hesla. Bez klíčového souboru je heslo bezcenné a naopak. Klíčový soubor je ale nutné zabezpečit. Nejvhodnější je použít soubor, který je skrytý mezi jinými soubory, například zvukový soubor s příponou mp3. Z názvu souboru by nemělo být poznat, že jde o klíčový soubor.

8.1.5 Administrátorské heslo v truecryptu

Truecrypt nemá přímou funkci správcovského hesla, ale můžeme toho docílit správným použití funkce zálohy hlavičky. Jak jsem již zmiňoval, heslo, SALT a klíčové soubory pomocí hash funkce vytvoří klíč hlavičky, kterým odšifruje hlavičku s hlavním klíčem. Hlavní klíč je náhodně zvolený, pro konkrétní šifrovaný svazek neměnný klíč, kterým se šifruje celý svazek kromě SALTu a hlavičky. Když vytvoříme nový svazek, bude vytvořený hlavní klíč, který bude šifrovaný nějakým heslem, dejme tomu, že to bude „hlavní heslo 1“. Následně zálohujeme hlavičku svazku, kterou i s heslem bezpečně uchováme, například ve firemním trezoru. Potom zvolíme možnost „změnit heslo“, zadáme „hlavní heslo 1“ a necháme zaměstnance, aby si zvolil vlastní heslo, třeba „moje heslo“. Tím dojde k v paměti počítače k odšifrování hlavičky prvním heslem, následně se zašifruje novým heslem a touto novou hlavičkou se přepíše ta původní. V tento okamžik může data přečíst pouze zaměstnanec. V případě potřeby je ale možné celou hlavičku

nahradit tou bezpečně uloženou v trezoru, který obsahuje ten stejný hlavní klíč, který je ale zašifrovaný jiným, známým heslem.

Zpřístupnění dat hlavním heslem vyžaduje přepsání hlavičky, a tak je tento proces vhodný jako nouzové řešení nebo jako pojistka pro případ, kdy zaměstnanec není schopný nebo ochotný zpřístupnit svou práci zaměstnavateli.

8.1.6 Šifrování nesystémového disku

Truecrypt umožňuje i šifrování celého disku, dokonce i disku s operačním systémem. Celý šifrovaný disk je velmi podobný virtuálnímu disku, má dokonce stejnou strukturu. Rozdíl je v tom, že celý šifrovaný svazek není jeden určitý soubor, ale přímo celý disk. Samotný systém souborů je šifrovaný a bez načtení svazku programem Truecrypt vypadá takový disk jako neformátovaný disk plný náhodných dat. Až načtením tohoto svazku je možné pracovat s uloženými daty.

8.1.7 Šifrování disku s operačním systémem

Truecrypt umožňuje šifrovat celý disk i s operačním systémem, ale toto řešení není zrovna šťastné. Truecrypt nahraje malý zaváděcí program na MBR (master boot record, hlavní spouštěcí záznam) na první stopu pevného disku. Problém je, že MBR ani první stopa disku nemusí být prázdné. V MBR jsou uloženy třeba informace o logických jednotkách a první stopu disku může používat třeba program určený k volbě operačního systému. Truecrypt automaticky předpokládá, že jsou tato místa volná. Šifrování disku s operačním systémem programem Truecrypt může způsobit problémy. Lepší je tedy šifrovat až uložená data a operační systém nechat nešifrovaný.

8.1.8 Zhodnocení programu Truecrypt

Tento program patří mezi kvalitní software a navíc je zdarma. Používá silné algoritmy, šifruje všechna data ve svazku a dokonce celý tento svazek se navenek jeví jako náhodná data. Protože jde ale o open-source, je důležité tento program stáhnout z důvěryhodného zdroje, např. z oficiálních stránek výrobce: http://www.truecrypt.org/. Zdrojový kód je dostupný a tudíž i náchylný k neoprávněným změnám. Na těchto internetových stránkách je původní verze programu, která je navíc elektronicky podepsaná. Podle elektronického podpisu můžeme ověřit pravost naší kopie programu, kterou pak

můžeme bez starostí nainstalovat. Celkově je tento program považován za bezpečný a zatím není znám případ jeho prolomení, jenž by nebyl způsobený nedbalostí uživatele nebo jinými metodami, které jeho funkci obejdou. Program je kvalitní doplněk počítače, který při správném použití dokáže ochránit všechna důležitá data před krádeží nebo zneužitím.

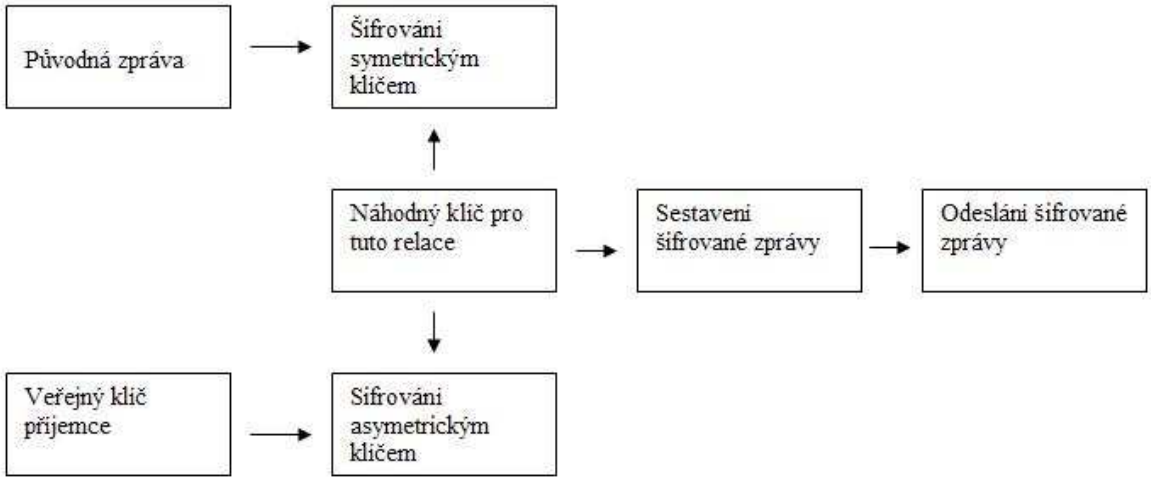
8.2 PGP

PGP je zkratka pro Pretty Good Privacy, v češtině „Docela dobré soukromí“. Jde o profesionální softwarový produkt nabízející širokou škálu různých nástrojů k bezpečnému uložení dat a komunikaci. Umožňuje i vytváření šifrovaných virtuálních disků jako Truecrypt, ale má i spoustu dalších funkcí. Umožňuje správu soukromých a veřejných klíčů, elektronický podpis a šifrování emailů, šifrování ICQ, bezpečné mazání souborů, vytváření samodešifrovacích souborů i šifrování celého disku. Tyto funkce umožňují i jiné, freeware programy, ale PGP má tu výhodu, že tyto funkce kombinuje v jednom balíku služeb. Nové a placené verze PGP mají kvalitní grafické rozhraní, které je celkově příjemné, jednoduché a přehledné. Funkce šifrovaných virtuálních disků je podobná jako u Truecryptu, proto se zaměřím především na popis zabezpečení emailové komunikace a v menší míře také na doplňkové služby programu.

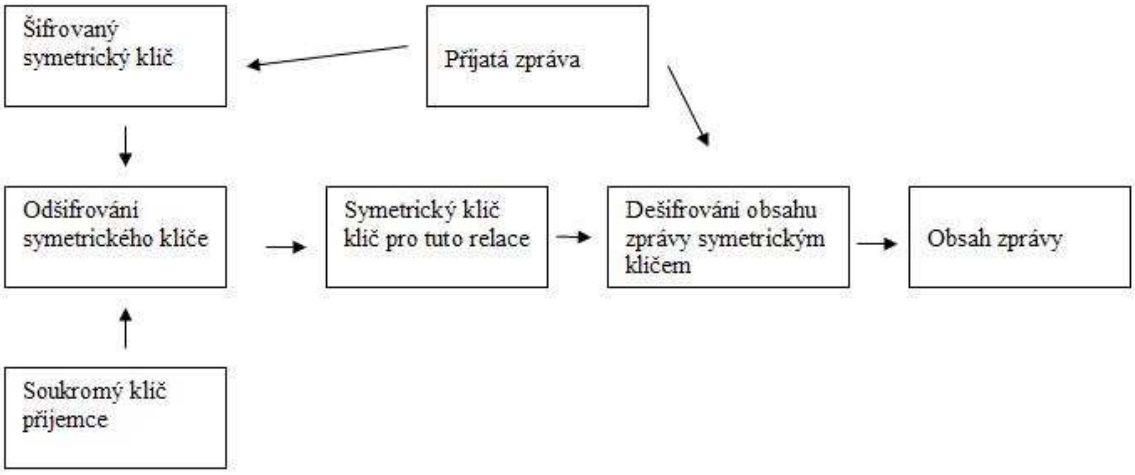
Obr. 25. grafické rozhraní programu PGP desktop 10.1.1

8.3 Postup šifrování emailové komunikace

PGP používá hybridní systém šifrování komunikace, který kombinuje rychlost symetrických algoritmů s klíčovou bezpečností systémů s veřejným klíčem. Na první pohled se může zdát, že je to kompromis mezi bezpečností a rychlostí, ale bezpečnost tohoto systému není nijak snížena. Zpráva je nejprve zašifrována náhodně vytvořeným symetrickým klíčem, který je pro každou šifrovanou zprávu jedinečný. Tento klíč následně zašifruje odesílatel veřejným klíčem příjemce, přidá ho ke zprávě a to odešle. Příjemce svým osobním klíčem, který zná pouze on, odšifruje symetrický klíč a ten odšifruje text zprávy. Hlavní výhoda tohoto systému je v tom, že symetrický klíč nemusí znát předem ani jeden z účastníků komunikace a tento klíč může odšifrovat pouze příjemce.



Obr. 26. postup šifrování komunikace s programen PGP



Obr. 27. postup dešifrování komunikace s programem PGP

8.4 Další užitečné funkce PGP

- Skartovačka dat

PGP shredder je užitečná pomůcka, která slouží k bezpečnému a trvalému vymazání souborů. Za normálních okolností se při mazání souboru smaže jen záznam o poloze souboru na disku, který se označí jako volné k přepsání. Samotná data ze souboru ale na disku pořád existují a je možné je i obnovit. PGP shredder soubor smaže a několikrát ho přepíše. Počet přepsání souboru lze nastavit, ale tři přepsání bohatě stačí k bezpečnému odstranění souboru. PGP shredder umožňuje automatické bezpečné smazání souborů při vyprázdnění koše.

- Samodešifrovací archivy

V případě potřeby rychlého zašifrování a dešifrování několika souborů nebo složek umožňuje PGP vytvořit samorozbalovací, šifrované archiv. Ten se při spuštění zeptá na heslo a na místo, kam má svůj obsah odšifrovat. Vytváření těchto archivů je usnadněno panelem PGP u vlastností souboru. Tato funkce je vhodná k rychlému šifrování jednotlivých souborů a složek nebo i k snadnému a bezpečnému odesílání souborů v příloze emailu.

- Správa klíčů

Správa klíčů je v PGP jedna z nejdůležitějších funkcí. Klíčový pár je uložený a šifrovaný symetrickým algoritmem, aby mohl být použít pouze oprávněnou osobou a aby bylo zabráněno zkopírování klíče. Velmi užitečná je i možnost zveřejnění veřejného klíče prostřednictvím specializovaných serverů.

- Elektronický podpis

PGP umožňuje i elektronický podpis souborů. Protože PGP běžně používá hash funkce i asymetrickou kryptografii, je implementace elektronického podpisu docela samozřejmá.

8.5 Proč si vybrat PGP

PGP doporučuji uživatelům, kteří chtějí co nejlépe zabezpečit svá data i svou komunikaci, ale chtějí to dělat rychle, jednoduše a přehledně. Neexistuje služba programu PGP, kterou by neumožňoval i jiný software, a to stejně kvalitně a zdarma. Jejich nedostatek je především složitá funkce a nároky na uživatele. K pokrytí všech funkcí PGP by bylo potřeba hned několik programů, které by se musely používat jednotlivě. S programem PGP se velmi příjemně pracuje a lze ho doporučit jak velkým či malým firmám, tak i běžným uživatelům, kteří berou bezpečnost svých dat vážně.

9 BEZPEČNOSTNÍ PRVKY OPERAČNÍHO SYSTÉMU MICROSOFT WINDOWS

Operační systém Microsoft Windows je v dnešní době nejpoužívanější operační systém. Je široce používán jak zkušenými uživateli, tak i těmi nezkušenými. Problematice bezpečnosti tohoto operačního systému se věnuji především z toho důvodu, že velká část uživatelů tohoto operačního systému spoléhá na jeho bezpečnost, aniž by věděli, jaké je jeho standardní nastavení a jaké bezpečnostní prvky tento produkt nabízí. Velký počet lidí se mě pravidelně ptá na otázku zabezpečení počítače pomocí uživatelských účtů. A má odpověď je často velmi překvapí. Systém uživatelských účtů je určen převážně k autentizaci jednotlivých uživatelů a ve standardním nastavení skoro žádnou bezpečnost nenabízí.

9.1 Uložení hesla uživatelských účtů

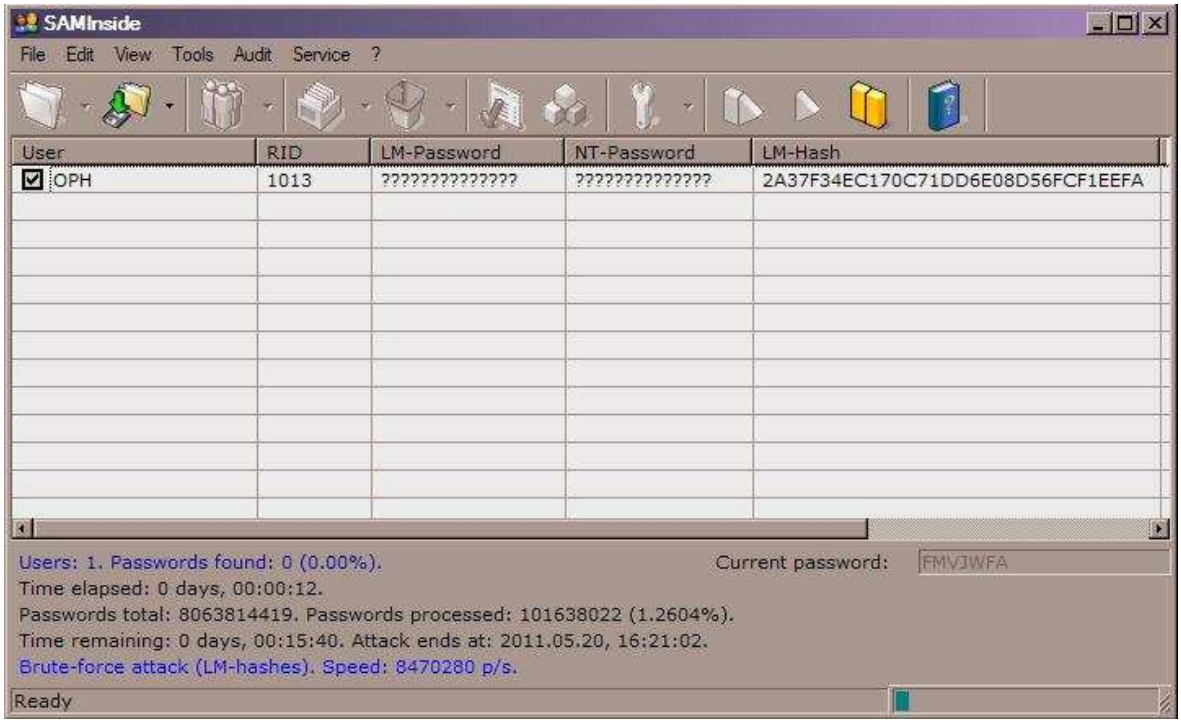
I když je Windows kvalitní produkt, nemůže ochránit své uživatele před jejich neznalostí. Většina běžných uživatelů slepě věří v absolutní bezpečnost a neprolomitelnost uživatelských účtů a jejich hesel. OS Windows umožňuje silné zabezpečení účtů i šifrování složek, ale o těchto funkcích převážná většina uživatelů vůbec neví. Protože jsou informace o uživatelských účtech a heslech uloženy na pevném disku počítače, je třeba tyto informace zabezpečit. Už jen samotné uložení informací o heslech omezuje bezpečnost uživatelů, protože co je fyzicky přítomné na pevném disku, jde i přečíst nebo přepsat. Windows používá ke správě uživatelských účtů SAM (security account manager), který ukládá informace o účtech a heslech. Je to databáze, která ukládá uživatelská jména a hash hodnotu hesel v databázi. Tato databáze je sice šifrovaná, ale protože je operační systém limitován hranicemi samotného počítače, musí být tento klíč uložený v blízkosti počítače, buď přímo na pevném disku, na disketě nebo flashdisku a nebo se generuje pomocí hesla. V prvním případě, kdy je klíč na pevném disku, dokáže tyto informace zpřístupnit i jiný počítačový program než operační systém. Uložení klíče na disku je standardní nastavení operačního systému. V SAM souboru je uložena jen zašifrovaná hodnota hesla (hash), ale tyto informace je možné přečíst (a později analyzovat), nebo dokonce i přepsat. Existují prostředky, které dokáží docela rychle nalézt odpovídající heslo, nebo ho dokonce rovnou přepsat. Windows používá dva typy hash algoritmů. První je docela bezpečný NTLM algoritmus. Druhý hash algoritmus je LM hash, který používá Microsoft Windows i

v nejnovějších verzích, který má ale několik zásadních slabin. Důvod jeho používání je zpětná kompatibilita s některými programy, ale systém ukládání hesel je tak bezpečný, jak je bezpečný jeho nejslabší článek. Operační systémy Windows Vista a Windows 7 stále umožňují použití LM hash, ale naštěstí je tato možnost již standardně vypnuta.

9.1.1 LM hash

LM hash pracuje následujícím způsobem. Nejprve převede heslo pouze na velká písmena, což eliminuje velkou část všech kombinací. Heslo je doplněno hodnotami „null“, aby mělo právě 14 znaků. Toto heslo je následně rozděleno na dvě sedmimístná hesla, což sníží počet možných kombinací na velmi malý počet. Počet všech kombinací hesla s pevnou délkou je roven C^n, kde *C* je počet možných znaků a *n* je počet míst. Tato dvě hesla jsou použita k vytvoření dvou DES klíčů, které se zapíší do SAM souboru jako dvojice.

Jako příklad uvedu výpočet počtu kombinací všech hesel, která obsahují malá písmena, velká písmena a čísla. Počet všech možných kombinací hesla je 62^{14}, což je $1{,}24 \times 10^{25}$. V prvním kroku jsou malá písmena převedena na velká, počet kombinací se sníží na 36^{14}, to se rovná $6{,}14 \times 10^{21}$. To ale není vše. Heslo se rozdělí na dvě sedmimístná, počet kombinací se sníží na pouhých 36^7, to je $7{,}84 \times 10^{10}$ kombinací. Původní počet kombinací všech hesel se tím pádem zmenší na nepatrný zlomek původního počtu. Dvoujádrový procesor s taktovací frekvencí 2,1Ghz vyzkouší a porovná 8 500 000 takových hesel za sekundu a všechna výše uvedená hesla vyzkouší za 2 hodiny a 30 minut. Heslo složené jen z písmen spolehlivě najde za pouhých 16 minut.

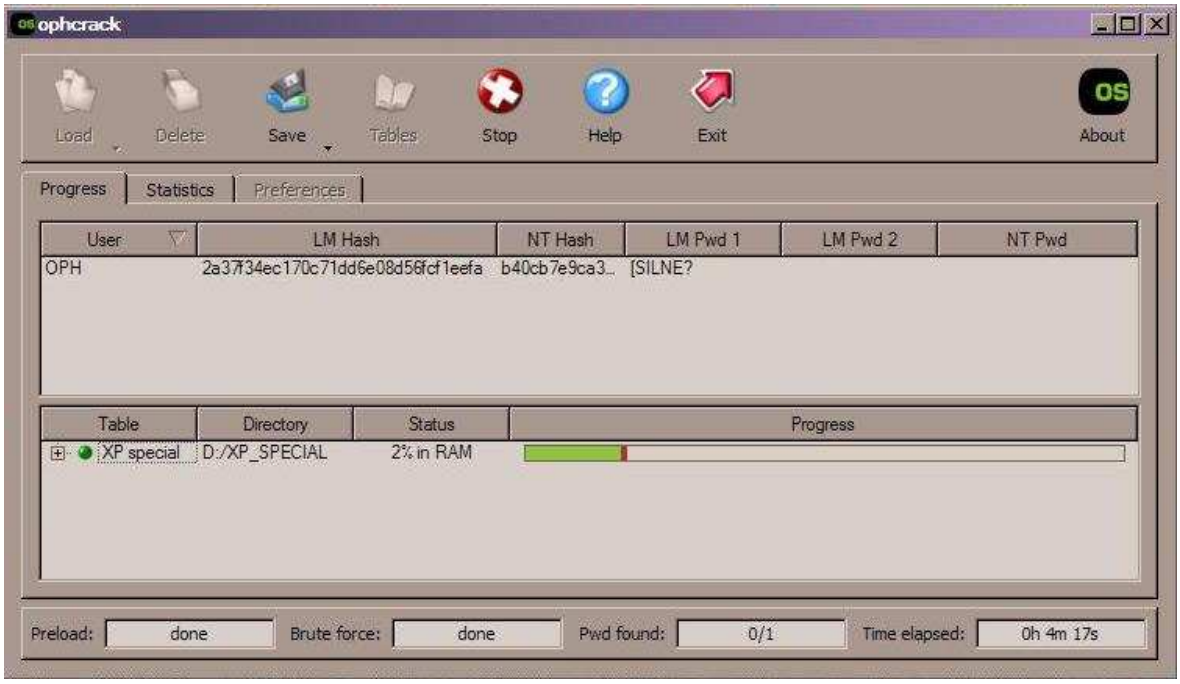


Obr. 28. útok hrubou silou na hesla

9.1.2 Funkce programu Ophcrack

Ophcrack je specializovaný software určený výhradně k překonávání hesel uživatelských účtů operačního systému Windows XP, ale je částečně použitelný i pro Windows Vista. Samotný program není nelegální. Nelegální je až případné překonávání cizích hesel. Ophcrack je možné použít i legálně, třeba k hledání zapomenutého hesla. Program využívá tzv. duhové tabulky. Samotné hash funkce jsou sice jednosměrné, ale tento problém můžeme snadno obejít tak, že předem vypočítáme hash hodnoty všech hesel nebo jen části hesel (slovníkový útok) a zapíšeme je do tabulky. Hash hodnotu v tabulce vyhledáme a přečteme příslušné heslo. Samotné SAM soubory jsou při provozu operačního systému Windows nepřístupné, a tak je Ophcrack spouštěn z bootovacího CD s operačním systémem Linux. Po startu program najde systémový klíč (soubor syskey), přečte SAM soubor a začne vyhledávat hesla z tabulky. Program je dodáván s tabulkou hesel obsahujících čísla a písmena, která má pouhých 380 MB. Existují i rozsáhlejší tabulky, které obsahují poměrně velký počet znaků. Tabulka, která zahrnuje 95 znaků (včetně mezery) má velikost 7,5 GB. Microsoft Windows XP sice používá ještě jednu, poměrně silnou hash funkci, ale ta je počítána ze stejného hesla. K použití programu musíme znát systémový klíč nebo musí být na disku počítače.

Provedl jsem test rychlosti tohoto programu, při kterém jsem hledal poměrně silné heslo [silnE?/]01 18 . První polovina hesla byla nalezena za 5 minut a 33 sekund a druhá za 10 minut a 45 sekund. Prohledání celé tabulky (7,5GB) trvalo 22 minut a 49 sekund.



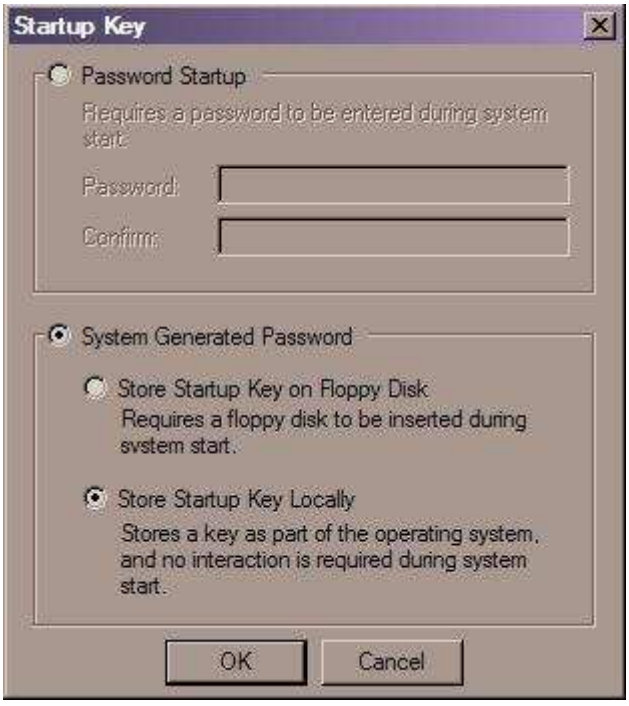
Obr. 29. program Ophcrack v činnosti

9.2 Přepsání SAM souboru

Tato metoda je ještě jednodušší než dlouhé vyhledávání hesla z databáze. Když je možné najít a přečíst hash hodnoty hesla, je určitě možné tyto hodnoty i přepsat. Není nic jednoduššího, než si zvolit vlastní heslo, vytvořit jeho hash hodnotu a touto hodnotou přepsat tu původní. Tato metoda je závislá na znalosti systémového klíče, stejně jako Ophcrack.

9.3 Zabezpečení systémového klíče

Systémový klíč slouží k zabezpečení databáze s uloženými hesly a některých klíčových částí operačního systému symetrickým šifrovacím algoritmem. Od verze Windows XP je systémový klíč používán automaticky, i když je standardně uložen na pevném disku. Existence systémového klíče a jeho nastavení bohužel není široce známá mezi uživateli. Existují tři různá nastavení, která můžeme nastavit přímo v registrech operačního systému nebo použitím programu syskey.exe.



Obr. 30. nastavení zabezpečení systémového klíče

- Klíč na lokálním disku

První a standardní nastavení ukládá systémový klíč na pevném disku počítače. Toto nastavení je uživatelsky pohodlné, protože nevyžaduje vložení hesla nebo souboru s klíčem. Toto nastavení nemusí nutně snižovat datovou bezpečnost, záleží na preferencích uživatele.

- Klíč na disketě

Druhé nastavení ukládá systémový klíč na přenosnou disketu. Toto nastavení vyžaduje disketu v disketové mechanice. Je možné použít i USB disk, ale k tomu je zapotřebí menší zásah do operačnímu systému. Je nutné operačnímu systému „vnutit“ že má USB disk označení A:, které se standardně používá pouze pro disketovou mechaniku. Uložení systémového klíče na disketu nebo i USB disk není příliš vhodné, protože diskety i USB disky nejsou stoprocentně spolehlivá datová média. V případě jejich poškození nebo ztráty může uživatel přijít o důležitá data. Výhodou je, že klíč není přítomný na pevném disku počítače.

- Šifrování klíče pomocí hesla

U této možnosti je systémový klíč sice přítomný na pevném disku, ale je šifrovaný pomocí hesla. Použitý algoritmus používá klíč délky 128 bitů. Samotný systémový klíč je

vytvořen generátorem náhodných čísel a není možný jiný útok, než útok hrubou silou nebo slovníkový útok. Slovníkovému útoku na heslo můžeme zabránit dostatečně dlouhým a složitým heslem.

9.4 Šifrování souborů

Microsoft Windows přímo umožňuje i šifrování dat na disku. Používá hybridní systém jako PGP, ale systém veřejného a soukromého klíče je využíván k šifrování jednotlivých souborů na disku. Tento systém používá hned několik klíčů. Ke generování klíče, kterým se odšifruje soukromý klíč uživatele, je použito uživatelské heslo, což omezuje bezpečnost tohoto systému. Tento hybridní systém slouží k šifrování i dešifrování souborů jednoho uživatele, takže jde prakticky o složitější variantu symetrického šifrování. K samotnému šifrování používá AES s 256 bitů dlouhým klíčem. Proto je vhodnější použít jiný, lépe kontrolovatelný software, jako například Truecrypt nebo PGP. Tato funkce začíná být zajímavá až u operačního systému Windows 7, který používá RSA s klíčem dlouhým až 16384 bitů nebo algoritmus, který používá eliptické křivky (ECC) s klíčem dlouhým 512 bitů.

9.5 Zbytkové riziko

Žádný systém není nepřekonatelný. I když správné nastavení systémového klíče zabrání velkému počtu možných útoků, pořád je možné tento systém překonat. Největší nebezpečí je infekce rootkitem, který může upravit nebo obejít kritické procesy operačního systému. Když není systémový klíč přímo na pevném disku, pořád je nutné tento klíč přečíst z diskety nebo vytvořit v paměti počítače. I SAM soubor se musí při startu počítače odšifrovat a uložit do paměti počítače k dalšímu použití. Případný rootkit může tyto procesy napadnout nebo upravit a následně získat a uložit systémový klíč, nebo ho dokonce i odeslat počítačovou sítí. Takový útok je naštěstí velmi náročný na znalosti útočníka, závisí na jeho technických a softwarových prostředcích a většinou vyžaduje i fyzický přístup k počítači. Další a jednodušší možností je instalace keyloggeru, kamery nebo rootkitu, pomocí kterých zjistíme heslo. Proto je důležité chránit počítač i kvalitním antivirovým programem, firewallem a hlavně si dát pozor a věnovat se prevenci, o které jsem psal již dříve.

ZÁVĚR

Mým cílem bylo poskytnout ucelenou práci z oblasti datové bezpečnosti. Věnoval jsem se nejen samotnému popisu základních termínů, ale tyto poučky jsem se snažil aplikovat do praxe a nabídnout svůj pohled na problematiku a svá doporučení na zabezpečení dat.

V teoretické části jsem se věnoval škodlivému softwaru, vymezil jsem jeho základní formy a systematicky jsem popsal využívané prostředky k zabezpečení dat různého charakteru. Následně jsem v části praktické dal tyto poznatky do souvislosti a spolu s vlastními zkušenostmi jsem se snažil nabídnout konkrétní řešení, jak data ochránit pomocí softwaru, hardwaru a také osobním přístupem k prevenci. Právě kombinace všech těchto prostředků je totiž tím nejefektivnějším způsobem, jak se vyhnout zneužití svých dat. I ten nejsofistikovanější software je vždy nutno doplnit o svědomitého uživatele, který zná možná rizika a nástroje na jejich eliminace umí správně využít. Byl bych proto rád, kdyby tato bakalářská práce dokázala i běžného uživatele PC upozornit na rizikové oblasti a nabídnout možná řešení.

V průběhu tvorby této práce jsem si uvědomil, že právě datová bezpečnost je mi blízká a chtěl bych se této problematice věnovat i v budoucnosti, jelikož bude výzvou srovnat a udržet krok s těmi, kteří se nezdráhají využít chyb a neznalostí lidí ve svůj prospěch.

SEZNAM POUŽITÉ LITERATURY

[1] ERICKSON, Jon: Hacking - umění exploitace. Preklad Marek Strihavka. 1. vyd. Brno : Zoner Press, 2005. 263 s. ISBN 80-86815-21-8.

[2] JAŠEK, Roman. Informační a datová bezpečnost. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006. 140 s. ISBN 80-7318-456-7.

[3] PRIBYL, Jirí; KODL, Jindrich. Ochrana dat v informatice. Vyd. 1. Praha : Vydavatelství CVUT, 1996. 299 s. ISBN 8001016641

[4] STRIHAVKA, Marek: Vaše bezpecnost a anonymita na Internetu. 1. vyd. Brno : Computer Press, 2001. 84 s. ISBN 80-72265-86-5.

[5] SZOR, Peter: Pocítacové viry - analýza útoku a obrana. Preklad Marek Strihavka. 1. vyd. Brno : Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.

[6] ZELENKA, Josef. Ochrana dat : kryptologie. Vyd. 1. Hradec Králové : Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

Internetové zdroje:

[7] *Security-Portal.cz | Bezpečnost • Hacking • Komunita* [online]. 2005-03-17 [cit. 2011-05-22]. WiFi sítě a jejich slabiny. Dostupné z WWW: <http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny>.

[8] SCHNEIER, Bruce. Schneier on Security [online]. 2000 [cit. 2011-05-17]. Dostupné z WWW: <http://www.schneier.com/>.

SEZNAM OBRÁZKŮ