Bezpečnost dat v informatice

Data Security in Computer Science

Jan Hraňo

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Hraňo**
Osobní číslo:	**A11018**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost dat v informatice (Bezpečné zpracování dat a bezpečná komunikace prostředky výpočetní techniky)**
Téma anglicky:	**Data Security in Computer Science (Secure Data Processing and Secure Computing Equipment Communications)**

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. **Analyzujte 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. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 190 s. ISBN 80-251-0106-1.**
2. **ENDORF, Carl. Detekce a prevence počítačového útoku. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.**
3. **HARRIS, Shon. Hacking: manuál hackera. 1. vyd. Praha: Grada, 2008, 399 s. ISBN 978-80-247-1346-5.**
4. **LUDVÍK, Miroslav a ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. Vyd. 1. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.**
5. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.**
6. **SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press, 2006, 608 s. ISBN 80-868-1504-8.**

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

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

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

ABSTRAKT

Tato bakalářská práce se zaobírá především tématikou informační bezpečnosti v počítačových technologiích. Teoretická část je rozdělena do několika kapitol. Na úvodních stranách je stručně rozebrána problematika dat. V dalších kapitolách se práce zabývá hesly, problematikou hackerů, tématikou škodlivého softwaru, šifrováním a ochranou počítačových sítí. Na závěr teoretické části práce řeší penetrační testování.

V praktické části se práce zaobírá metodami ochrany dat. V první kapitole praktické části práce popisuje hardwarové metody ochrany dat. V další kapitole popisuje softwarové metody ochrany dat. V následující kapitole rozebírá metody ochrany dat před zničením. V poslední kapitole se práce věnuje fyzické ochraně dat.

Klíčová slova: bezpečnost dat, šifrování, hesla, škodlivý software, penetrační testování, hardwarová ochrana dat, softwarová ochrana dat

ABSTRACT

This bachelor thesis mainly deals with the theme of information security in computer technology. The theoretical part is divided into several chapters. The opening pages briefly discussed the issue of data. In other chapters thesis deals with passwords, hackers issue, themed malicious software, encryption and protection for computer networks. At the end of the theoretical part thesis deals with penetration testing.

In the practical part thesis deals with methods of data protection. In the first chapter the practical part describes the hardware methods of data protection. The next chapter describes a software methods of data protection. The following chapter discusses about the methods of data protection against destruction. In the last chapter thesis deals with the physical protection of data.

Keywords: data security, encryption, passwords, malicious software, penetration testing, hardware data protection, software data protection

Poděkování

Chtěl bych poděkovat RNDr. Ing. Miloši Krčmáři za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce. Dále bych chtěl poděkovat celé své rodině a přítelkyni za podporu a pomoc při tvorbě této práce.

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

S postupem doby se pro nás stal počítač nedílnou součástí života, trávíme na něm více a více času, vyřizujeme přes něj nákupy zboží na internetu, ukládáme si firemní zprávy a jiné důležité věci, všechna tato data jsou pro nás velmi důležitá, proto vznikla potřeba je chránit. Ochrana dat je v dnešní počítačové době velmi rozšířené téma, v průběhu let docházelo k vývoji počítačů, vyvíjely se také počítačové viry a přibývaly útoky na data jiných lidí, bylo nutné najít metody, jak tato data, co nejlépe chránit. Mnoho lidí by mohlo povídat, proč je důležité chránit data, když o ně přišli výpadkem elektřiny, nebo počítačovým virem.

Přestože se téměř všichni lidé setkávají s počítači každý den, často ani nevědí, že existují hrozby, které by jim mohly uškodit, natož aby používali nějaké ochrany svého počítače. Člověk se o danou problematiku nemusí zaobírat do hloubky, ale měl by mít alespoň základní přehled, co všechno hrozí za hrozby a jak se proti nim chránit. Zásadně by také mohlo pomoct, kdyby lidé měli naučené základy, jak se chovat na internetu a jaké používat hesla. Útočníci jsou každým dnem vychytralejší a obyčejní lidé se proti nim stávají bezmocní, přestože existuje mnoho způsobů, jak se chránit. Není správné, aby útočníci kradli lidem údaje, které jim nepatří. Jedním z důvodů proč jsem si vybral tuto práci je, abych mohl informovat o způsobech, jak se chránit.

Cílem mé práce je seznámit čtenáře s metodami ochrany dat, ať už to je hardwarovým, softwarovým nebo fyzickým způsobem tak, aby i člověk, který se tímto tématem nezabývá, věděl, o co se jedná. Dalším cílem mé práce je sjednocení jednotlivých metod ochrany dat do logického celku.

.

I. TEORETICKÁ ČÁST

1 DATA

Data je možné definovat více způsoby v závislosti na oboru, ve kterém se vyskytují. V počítačové sféře data definujeme jako informace, které jsou přeloženy do vhodnější podoby pro zpracování a přenos. Pro počítač je to binární kód, který mu umožňuje rychlejší manipulaci s daty. V ostatních vědních oborech jsou data informace (zkušenosti, znalosti, vědomosti, pozorovaní), které byly nějakým způsobem zaznamenány (např. v knize, na papíře atd.). Data mohou být klidně i fakta, která máme uložena v mozku.

1.1 Význam dat

Data nám umožňují rychleji posílat informace přes internet, dovolují nám uchovávat naše vzpomínky, zkušenosti, fotografie a další. V podstatě obsahují téměř všechno vědění světa.

1.2 Data versus informace

Informace jsou výsledkem zpracování, manipulace a organizace dat takovým způsobem, že obohatí vědomosti příjemce. Data jsou souborem nesouvislých informací, které nemají žádný význam, dokud nejsou správně vyhodnoceny. Pokud je při jejich vyhodnocení objeven nějaký významný vztah mezi daty, je převeden na informace. A tato data mohou být použita k různým účelům.

1.3 Proč je důležité chránit data?

Data obsahují všechny informace světa od našeho data narození až po heslo k našemu bankovnímu účtu. V dnešní počítačové době jsou všechna data někde uložena, může to být server banky, firmy atd. Výhodou je, že se díky tomu můžeme dostat ke svému účtu z našeho počítače, vybrat si bankomat a další úkony, které nám zkracují čas, než když bychom museli danou banku sami navštívit. Na druhou stranu to nese nevýhodu, jelikož tato data jsou někde uložena, musí být také na dostatečné úrovni zabezpečená, pokud by nebyla nijak chráněna, měl by k našim údajům přístup naprosto každý, došlo by ke ztrátě peněz, odcizení identity a k dalším škodám, z toho důvodu je důležité tato data chránit.

1.4 Rozdělení rizik

Obecně můžeme rizika při ochraně dat rozdělit na dvě kategorie:

1. Security – zde můžeme zařadit jakékoliv napadení počítače cizí osobou, ať už vzdáleně z internetu, či lokálně přímo z daného počítače, či zařízení.
2. Integrity – jedná se o ztrátu dat vzniklou vlivem jiných faktorů, patří sem výpadky proudu, chyby počítače, chyba obsluhy, počítačové viry.

1.5 Způsoby ochrany

Možností jak se chránit je nespočet, ne všechna jsou však kvalitní a dostatečná. Jednotlivé způsoby ochrany můžeme rozdělit do softwarových metod, hardwarových metod. Tyto metody jsou popsány v praktické části této práce. Nejdůležitějšími body ochrany jsou:

- Komplexnost – ochrana musí být úplná, využít při ní všechny dostupné bezpečnostní prvky a způsoby ochrany.
- Kompatibilita – jednotlivé složky ochrany spolu musí bezvýhradně spolupracovat, nesmí dojít k tomu, že se některé z nich budou rušit.
- Efektivnost – umístit do systému jen takové bezpečností prvky, které jsou efektivní.
- Cenová přiměřenost - míra ochrany by měla odpovídat důležitost dat, je zbytečné chránit nákupní list, co máme doma uložen v počítači, několikatisícovou ochranou

2 HESLA

Hesla se používají téměř všude, ať už při přihlášení do operačního systému Windows, nebo při přihlášení na různorodé internetové stránky. Hesla jsou využívány k identifikaci uživatele. Pokud heslo neznáme, nebudou nám zpřístupněny určité funkce (nemožnost se přihlásit do systému Windows). Pokud heslo chceme používat, nejdříve musí být vytvořen účet, ke kterému bude toto heslo přiřazeno. Při vytváření účtu si vybereme uživatelské jméno a poté heslo, které k tomuto účtu náleží, tento účet je uložen buď v našem počítači (např. u systému Windows pro osobní počítač), nebo v databázi (internetové stránky, např. facebook). Pokud se chceme následně přihlásit k uživatelskému účtu, je potřeba znát naše uživatelské jméno a heslo.

2.1 Bezpečné heslo

Jedná se o heslo, které splňuje určité kritéria. Taková hesla by měla být všechna, která využíváme při přístupu k důležitým datům. Při vytváření bezpečného hesla bychom měli dbát na následující body:

- Délka hesla – čím je heslo delší, tím narůstá počet možných kombinací a díky tomu i doba nutná k jeho prolomení. Obecně je udáváno, že by heslo mělo mít alespoň osm znaků. Například pokud využijeme pouze čtyřmístné číslo, tak pomocí variací s opakováním si můžeme vypočítat, kolik dostaneme možných čísel: $V'(4{,}10) = 10^4 = 10000$. I když se může zdát 10000 jako velké číslo, pro hackery je v dnešní době možné čtyřmístné heslo složené pouze z číslic za pár sekund, protože výkon dnešních několika jádrových procesorů dovoluje na běžném počítači provést i 1000 kombinací za sekundu.
- Použité znaky – zase platí, čím větší množství znaků použijeme, tím je těžší heslo prolomit. Při tvorbě hesla máme na výběr z deseti číslic (0-9), padesáti dvou písmen abecedy (pokud použijeme velká i malá písmena, a-z, A-Z), také je možné použít znaky s diakritikou, nebo interpunkční znaménka, či speciální znaky. Tyto nadstandardní znaky bych ale nedoporučoval používat z důvodu toho, že většina zahraničních serverů je nedovoluje.
- Vhodná volba hesla – naše heslo by se nikdy nemělo shodovat s názvem účtu, protože to je jedna z prvních věcí, které hacker zkouší. Taktéž by nemělo obsahovat osobní informace jako například jméno našeho psa, manželky, rodné číslo, osobní

telefon atd., takové informace je možné použít, ale jen za určitých podmínek, které si ukážeme následně. V heslu by se také neměly vyskytovat často používané výrazy typu 123456, qwert a podobně.

Bezpečné heslo by tedy mělo být co nejdelší a s největším počtem různorodých znaků. Pro některé lidi může být velkým problémem zapamatování hesla, které má mnoho různorodých znaků, ale pokud použijeme určité pomůcky, stane se heslo snadněji zapamatovatelné. Pomůcek existuje mnoho, každý člověk může mít svou vlastní. Nyní uvedu příklad jedné z pomůcek, jejíž podstatou je přidání číslic a velkých a malých písmen do známého slova. Kdybychom použili pouze heslo karamely, tak by toto heslo bylo snadno zjistitelné, nyní využijeme naši pomůcku a přidáme námi snadno zapamatovatelné číslice na začátek a konec slova: 123karamely456, toto heslo stále není dostačující a tak přidáme navíc velká písmena na začátek a konec slova (je možno využít i jiného pravidla, například jen velká písmena uprostřed slova, ale tato metoda mi přijde jednodušeji zapamatovatelná) a písmeno „a“ nahradíme číslicí 4, písmeno „e“ nahradíme číslicí 3, dostáváme: 123K4r4m3lY456, toto heslo již je naprosto dostačující a snadno zapamatovatelné.

V následující tabulce máme přehled časů potřebných pro prolomení hesla, tuto tabulku jsem získal následovně. Nejdříve jsem si vypočítal počet variací pomocí variací s opakováním $V'(4{,}10) = 10^4 = 10000$, následně jsem toto číslo podělil výkonem, který je v našem případě 100, díky tomu jsem dostal čas potřebný pro prolomení hesla v sekundách. Časy, uvedené v tabulce, jsou pouze orientační, vždy závisí na různých faktorech například na výkonu daného počítače, či na propracovanosti programu, který je použit pro zjištění hesla.

Délka hesla	***Použité znaky***		
	0-9 10 znaků	**a-z, 0-9 36 znaků**	**a-z, 0-9, A-Z 62 znaků**
	Čas potřebný k prolomení hesla při výkonu 100 hesel za sekundu		
4	2 minuty	5 hodin	2 dny
5	17 minut	7 dní	4 měsíce
6	3 hodiny	8 měsíců	18 let
7	1 den	25 let	1120 let
8	12 dní	900 let	69200 let

Tab. 1: Orientační časy prolomení hesel

2.2 Bezpečnost hesla

Staráme se, aby naše heslo bylo co nejbezpečnější, používáme silné kombinace znaků, heslo si nikam neukládáme, přesto se může stát, že se někdo dostane k našemu heslu. Jak je to možné? Ve většině případů je na vině už tvůrce webové aplikace, který vytvořil systém tak, že nechává ukládat hesla v otevřeném čitelném formátu. Pokud se útočník dostane k této databázi, získá přístup a informace o všech uživatelích v databázi. Tento problém je možné lehce vyřešit. Tvůrce webové aplikace vytvoří takový systém, který bude do databáze ukládat pouze otisk hesel neboli hash, který je výsledkem speciální matematické funkce. Obecně tato funkce pracuje tak, že bere vstupní data a k nim vrací řetězec znaků o určitých vlastnostech. Mezi základní vlastnosti hashe patří:

- pro stejná vstupní data je stejný,
- má pevně stanovou délku,
- malá změna vstupních dat má za následek velkou změnu výsledku,
- neměli by existovat různá dvoje vstupní data se stejným hashem,
- z hashe by nemělo být nikdy možné rekonstruovat původní text.

Hashovacích funkcí existuje mnoho, avšak v dnešní době některé poskytují větší bezpečnost než jiné. Například hashovaní funkce MD5 byla již prolomena. Za bezpečnou hashovaní funkci se považuje SHA2 a vyšší z rodiny SHA algoritmů. Další možností, jak útočníkovy znesnadnit získání hesla, je umožnit na daném serveru zadání pouze omezeného počtu hesel při přihlášení. Pokud se bude snažit útočník uhádnout heslo a zadá ho třikrát po sobě špatně, dojde k provedení určitých operací například zablokování účtu a odeslání zprávy s unikátním kódem na telefon vlastníka účtu, který jej musí zadat, aby se bylo možné znovu přihlásit. Vlastník je díky této zprávě upozorněn, že se někdo snaží dostat na jeho účet a navíc útočník se už dále nemůže pokoušet o získání hesla. Další možností jak se bránit například před počítačovým programem, který se snaží uhádnout heslo, je použití CAPTCHI, což je Turingův test, který odlišuje počítače od lidí, ve většině případů ve formě obrázku deformovaného textu, tento obrázek počítač neumí přečíst. Útok probíhá následovně. Počítač zadá třikrát po sobě špatně heslo, objeví se CAPTCHA, tento obrázek počítač neumí přečíst, a tak je útok neúspěšný, pokud by uživatel zadal toto heslo třikrát po sobě špatně, přečte si CAPTCHU a zadá ji do příslušného pole, poté se může znovu přihlásit.

2.3 Uchování hesla

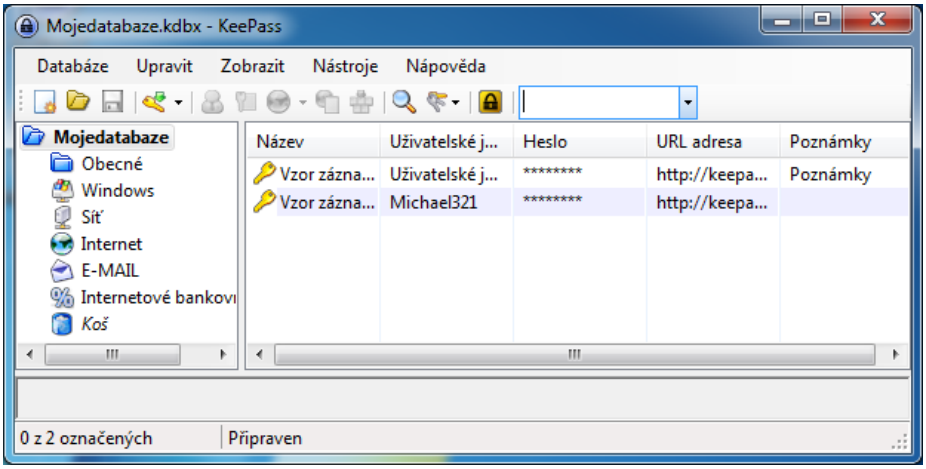
Heslo bychom nikdy neměli uchovávat u počítače například na papírku přilepeném na monitoru, nebo v diáři v šuplíku. Taktéž by nemělo být uloženo v počítači na ploše, či v nějakém snadno dostupném dokumentu. Pokud využíváme různorodá hesla a potřebujeme je mít pro případ zapomenutí někde uložena, můžeme využít programy pro správu hesel.

2.3.1 Programy pro správu hesel

Programů pro správu hesel existuje nespočet, liší se v nabízených funkcích. Každý z těchto programů má něco společného a to je hlavní heslo, které nás pustí v podstatě ke všem dalším heslům, které máme uložené v daném programu. Toto heslo by mělo být extra zabezpečené. V následujícím výčtu jsem vybral programy, které jsou pro uchování hesel nejvhodnější, ke každému jsem navíc napsal popis.

KeePass

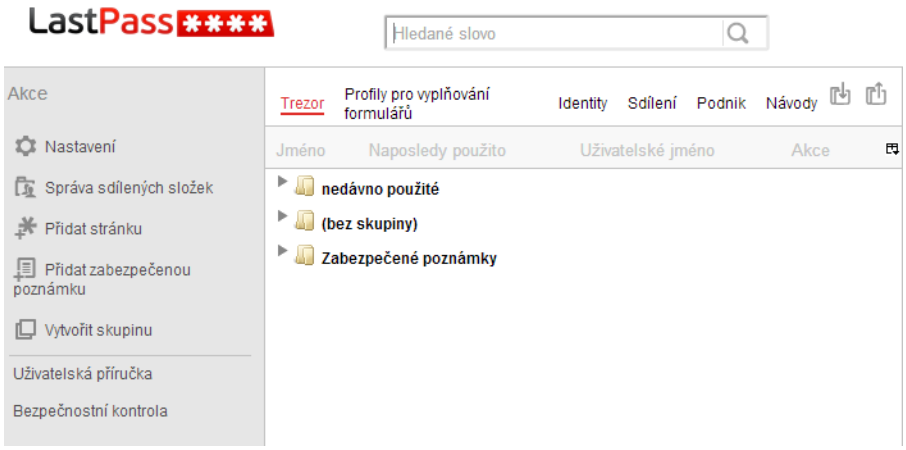
Jedná se o jeden z nejoblíbenějších programů pro správu hesel, program je open source (počítačový software s otevřeným zdrojovým kódem) a je zdarma. Program je velmi přehledný (viz. Obrázek 1.), vždy má uživatel přehled kam se co a jak ukládá. Každý uživatel má svoji vlastní databázi hesel (databázi je možné uložit na libovolné místo v počítači) a k ní vstupní heslo (je možné toto heslo brát i ze souboru). Jednotlivé záznamy se pak do databáze vkládají pomocí záložky upravit a vložit záznam, kde zadáme uživatelské jméno, heslo (je možno jej pro dodatečnou ochranu vygenerovat), adresu stránky, na které se bude dané heslo a jméno používat, případně poznámky a platnost hesla (pokud bychom chtěli heslo měnit po určitých časových intervalech).



Obr. 1: Prostředí programu KeePass

LastPass

Další velmi oblíbený program mezi uživateli, který slouží k ukládání hesel online, v podstatě je doplňkem k internetovým prohlížečům (Chrome, Internet Explorer, Firefox, Safari, Opera), do kterých se po stažení nainstaluje, pokud používáme více prohlížečů na jednom počítači, je možné nainstalovat tento doplněk do každého z nich. Takže se nemusí otevírat další externí program navíc. LasPass ukládá naši databázi hesel jak na internetový server programu, tak i na náš lokální disk (kdyby došlo k výpadku serveru, abychom stejně měli přístup k našim heslům). Hesla se ukládají do databáze programu při zadání jména a hesla na příslušné internetové stránce, čili není potřeba navíc nejdřív vytvářet záznamy v databázi, pří následující návštěvě stránky program poskytuje autodoplňovací funkci. Program navíc poskytuje funkci ukládání bezpečných poznámek, které se dá využití například k uložení licenčních klíčů k programům. Někteří uživatelé se bojí toho, že když jsou jejich data uložena na internetovém serveru, tak že by mohlo dojít k jejich odcizení, ale toto všechno je ošetřeno, jelikož veškeré přenosy jsou zašifrovány pomocí 256bitového AES (i naše lokální databáze). Navíc výrobce programu tvrdí, že jejich datové centrum je zabezpečeno na co nejvyšší úrovni, a pokud by i přesto došlo k odcizení dat, tak by stejně útočníkům byla tato data k ničemu, neboť při zabezpečení dat je použita kombinace dostatečně silných šifrovacích algortimů.



Obr. 2: Prostředí programu LastPass

3 HACKEŘI

Dříve termín hacker znamenal chytrého programátorského experta, avšak nyní odkazuje spíše na člověka, který umí získat neoprávněný přístup k dalším počítačům. Hacker si umí „hacknout“ jeho cestu přes úrovně zabezpečení počítačového systému nebo sítě. Toto hackování může být v jednodušší podobě zjištění hesla druhých, ale také ve složitější podobě napsání vlastního programu, který umí prolomit ochranný software systému druhých lidí. Hackeři jsou hlavním důvodem, proč bezpečnostní firmy musí pravidelně vydávat bezpečnostní aktualizace pro jejich programy. Někteří hackeři se spíše zaměřují na obyčejné lidi, jiní zase na velké firmy a organizace. Přestože pod pojmem hacker si většina lidí představí spíše člověka, který se snaží škodit, existují i takový, kteří naopak pomáhají. [7]

3.1 Typy hackerů

V podstatě je nemožné hodit všechny hackery do jedné kategorie. Důvody, které vedou hackery k hackování bezpečnosti stránky (či počítačového systému), mohou být různorodé, od ušlechtilých záměrů (například testování/zlepšování bezpečnosti simulací útoku) nebo neušlechtilé (testování hackerových dovedností, získání tajných informací) nebo dokonce z politických důvodů. Z těchto důvodů jsou hackeři rozdělování do skupin na základě jejich individuálních cílů a schopností. [7]

3.1.1 White hats

White hat hackeři (někdy také nazývaní jako etičtí hackeři) jsou lidé, kteří se nabourávají do bezpečnostních systémů, ale nečiní tak z neetických či škodlivých důvodů. Tito hackeři mají obvykle svůj jasně definovaný etický kodex a ve většině případů spolupracují s výrobci či vlastníky ke zlepšení objevených bezpečnostních slabin. Mnozí z nich po upozornění vlastníka, či výrobce bezpečnostního systému zveřejní po určitém čase tuto bezpečnostní slabinu na veřejnost, aby zajistili, že bude opravena. Tento termín je také používán pro hackery, kteří pracují na zlepšení návrhu a programového kódu bezpečnostních systémů. [7]

3.1.2 Black hats

Black hat hackeři jsou osoby, které neoprávněně pronikají do sítí a počítačů druhých lidí a také vytvářejí počítačové viry a škodlivý software. Tito hackeři se snaží být

na lepší technologické úrovni než white hat hackeři. Většinou se snaží najít cestu nejmenšího odporu, ať už v důsledku lidské chyby nebo lenosti, nebo k získání přístupu používají nové typy útoků. Black hat hackeři jsou často hackerskou komunitou označovány za „crackery“. Jejich hlavní motivací jsou peníze, které se snaží díky útoku získat. [7]

3.1.3 Grey hats

Grey hat hackeři jsou na pomezí mezi black hats a white hats. Tito hackeři také hledají zranitelná místa systému. Stejně jako white hat na toto zranitelné místo upozorní vlastníka, či výrobce. Ale jako black hat využije toto zranitelné místo a do tohoto bezpečnostního systému se bez schválení vlastníka dostane. Ve většině případů také bude nabízet opravení tohoto zranitelného místa, které objevil, za malý poplatek. [7]

3.2 Hackerské nástroje

Hackerské nástroje jsou programy nebo utility, které jsou navrženy tak, aby pomáhali hackerovy při hackování. Tyto nástroje mohou být také využívány k ochraně sítě nebo počítače. Hackerské nástroje jsou běžně používány k získání neoprávněného přístupu k počítači vložením škodlivého software a to převážně virů a trojských koní. Hackeři jsou velice kreativní a existuje nespočet nástrojů, které používají, vybral jsem však ty nejhlavnější.

3.2.1 Password crackers

Password crackers neboli prolamovače hesel patří mezi nejstarší nástroje, které využívají hackeři. Tyto nástroje, jak už z názvu vyplývá, slouží k prolomení hesel, která jsou používána k ochraně nebo autentizaci účtů uživatele. Jejich princip spočívá ve zkoušení různorodých kombinací znaků, které by mohly být heslem, pokud je heslo přijato, dojde k jeho odeslání hackerovi. Existují dva nejčastější typy útoku, které jsou uskutečňovány pomocí prolamovače hesel:

- Slovníkový útok (dictionary attack) – tento útok je založený na používání slov, která jsou uložena v takzvaném slovníku – databázi slov.
- Útok hrubou silou (brute force attack) – tento útok využívá generované kombinace vybraných znaků o určité délce a poté je zkoušeno, zda tyto kombinace nevyhovují zadanému heslu.

Kvalitní nástroje pro prolomení hesel mají v sobě obsaženy také slovník, který obsahuje slova, která by dle autora tohoto slovníku mohly být použita jako opravdové heslo. Čím kvalitnější slovník, tím je pravděpodobnější shoda s opravdovým heslem. Použití prolamovačů hesel je velmi jednoduché, jelikož většina z nich disponuje grafickým prostředím, ve kterém je možné nastavit parametry prolamování hesla. V dnešní době existuje mnoho na internetu volně dostupných prolamovačů hesel. Většina těchto nástrojů umožňuje ověřit zhruba 50000 hesel za sekundu na běžném počítači. Kvalitnější prolamovače, které jsou umístěny na výkonném počítači, jsou schopné ověřit až milión hesel za sekundu. Důležité faktory, které ovlivňují rychlost prolamovače jsou: [7]

- rychlost počítače, na kterém je nástroj používán,
- typ dat, která jsou prolamována,
- umístění dat,
- struktura zakódovaných dat.

3.2.2 Backdoors

Backdoors neboli zadní vrátka jsou kódy, které po instalaci na cílový počítač umožňují hackerovi vzdálené řízení tohoto počítače. Tyto zadní vrátka jsou formou trojského koně, který je popsán v kapitole 4. V dnešní době je tento nástroj velmi oblíben mezi hackery, protože jim poskytuje naprostou kontrolu napadeného stroje. Backdoors se nejčastěji instalují do cílového počítače. Pokud hacker objeví bezpečnostní díru v systému. Díky tomuto nástroji hacker naprosto obejde autentizaci systému. Většina hackerů instaluje backdoors na několik počítačů zároveň přes které pak podnikají útok na další počítače. Kvalitní backdoor je velmi těžké rozpoznat, navíc pokud je používán jen zřídka. Komunikaci mezi backdoors a hackerem je zprostředkovávána pomocí služby spuštěné na portu s vysokým číslem nebo také může být zamaskována jako například jako webový port 80 nebo terminálový přístup port 23 či kryptovaný kanál port 22. Tyto porty nejsou většinou odfiltrovány firewally, což umožňuje jejich přístupnost i přes bezpečnostní prvky sítě. Moderní backdoors využívají také protokolů některých komunikačních programů jako je ICQ či IRC. Jedním z nejznámějších backdoor programů je Back Orifice, který v jeho původní verzi umožňoval naprostou kontrolu nad operačním systémem Windows 95 a Windows 98. Po proniknutí do systému byl nainstalován jako .exe soubor a po startu počítače byl spuštěn jako běžná služba. Později došlo k jeho vylepšení na verzi Back

Orifice 2000 a bylo tak možné napadnou Windows NT a Windows 2000. Dalšími známými backdoor programy jsou NetBus / NetBus 2.0 Pro a SubSeven / Sub7. [7]

3.2.3 Skenery

Skenery jsou používány k nalezení otevřených portů počítače. Ke každému portu se váže i nějaká služba, která je díky tomuto portu přístupná. Skener hackerovi podává základní informace o cílovém počítači jako je například verze operačního systému. Pokud cílový počítač disponuje ochrannými prostředky, počítač může detekovat skenování, jež je pro něj předzvěstí potenciálního útoku, a provést bezpečnostní opatření jako například ukončení spojení s útočníkem na určitou dobu. Používanými programy jsou například Nmap, NetScan nebo SuperScan. Hlavní metodou, jak se bránit proti skenování, je použití IDS neboli systémů detekce narušení, tyto obranné systémy monitorují síťový provoz a snaží se odhalit podezřelé aktivity. Většina IDS je zdarma, za zmínku stojí například systém Snort nebo Suricata. [7]

3.2.4 Sniffery

Sniferry nebo také „čichače“ jsou nástroje, které slouží k odposlouchávání síťového provozu. Po skeneru se jedná o další nástroj, který neslouží přímo k útoku, ale k získávání informací pro útok. Hacker musí zvolit správné umístění snifferu v síti, aby získal potřebné informace. Sniffer pracuje tak, že přepne síťovou kartu do promiskuitního režimu, ve kterém systém obdržuje veškerá data (v normálním režimu nejsou předávána data systému, která nejsou určena pro síťovou kartu), která se na síti pohybují. Tyto data jsou dále zaznamenávány a analyzovány, například IP adresa, typ protokolu, MAC adresy a tak dále. Součástí analýzy je vyčlenění té části, ve které se nachází obsah přenášené zprávy. Díky tomu je možné odposlouchávat síť a získat tak přenášená hesla či jiné údaje. V dnešní době jsou často používanými programy například Ethereal, který je volně dostupný na internetu nebo také Ettercap a Dsniff. [7]

4 ŠKODLIVÝ SOFTWARE

Škodlivý software, také známý jako malware, je každý software, který nějakým způsobem škodí počítačovému systému. Malware může být ve formě červů, virů, trojských koní, spywaru, adwaru, atd., které kradou chráněná data, mažou dokumenty nebo přidávají software, který uživatel neschválil. [1]

4.1 Viry

Počítačový virus můžeme definovat jako program, nebo také kus kódu, který je vložen do počítače, nebo jiného zařízení bez vědomí uživatele a pracuje proti jeho vůli. Viry potřebují hostitelskou jednotku, aby se mohly šířit, pod hostitelskou jednotkou si můžeme představit soubory s příponou COM, EXE, SCR, VBS a další. Viry mohou infikovat jak soubory, tak i systémové prvky a dál se šířit, díky jejich schopnosti vlastní replikace. Jednoduchý virus, který je schopen se neustále replikovat, je poměrně snadné vyrobit. Přesto je stejně nebezpečný, protože pokud nebude rychle zastaven, při replikaci využije všechnu dostupnou operační paměť počítače či zařízení, což může vést až k zamrznutí systému. Viry tedy napadají soubory a tyto soubory jsou pak dále šířeny lidskou komunikací například emailem, či internetovým úložištěm. Ochranou proti virům jsou antiviry, které jsou popsány v praktické části. [6]

4.1.1 Bootviry

Nejdříve si vysvětlíme, co to je bootovací sektor. Bootovací sektor je vyhrazené místo na paměťovém médiu (pevný disk, usb disk, CD, DVD), které obsahuje bootovací program. Tento program slouží k načtení operačního systému. Je nemožné, aby počítač načetl operační systém bez bootovacího sektoru. Bootvir nejčastěji napadne počítač tak, že nahradí výchozí bootovací program svojí vlastní nakaženou kopií. Tento virus tedy napadá pouze systémové oblasti počítače. Bootvirus je schopný napadnout počítač pouze tehdy, je li používán k bootování počítače. [1]

4.1.2 Souborové viry

Souborové viry jsou jedním z nejčastěji používaných virů. Ve většině případů napadají soubory s příponou .exe nebo .com. Pokud je infikovaný soubor spuštěn, může být částečně nebo kompletně přepsán virem. Tyto viry se mohou šířit po celém systému.

Některé složitější varianty souborových virů umí i zformátovat pevný disk, díky čemu uživatel může přijít o všechna svá data. [1]

4.1.3 Multipartitní

Multipartitní viry dokážou napadat jak soubory, tak i systémové oblasti počítače, díky čemuž dokážou způsobit větší škody než ostatní viry. Tento virus nejdříve napadne bootovací sektor a po spuštění počítače a zavedení operačního systému z nakaženého boot sektoru napadne a začne škodit i na souborech, díky čemuž může převzít kontrolu nad celým počítačem. Multipartitní virus napadá počítač několikrát a v různých časech. [1]

4.1.4 Makroviry

Makroviry napadají kancelářské balíky s podporou maker. Makra jsou součástí těchto kancelářských softwarů například Visual Basic u Microsoft Office. Tyto viry se nejčastěji zaměřují na šablony, které nakazí a poté uživatel, který využije tuto nakaženou šablonu pro tvorbu nového souboru, nakazí i tento nový soubor. [1]

4.2 Červy

Počítačový červy jsou virům podobní v tom, že replikují svoje funkční kopie. Hlavní funkcí červa je ovládnutí prostředků pro síťovou komunikaci, které pak využívá, aby se mohl dále šířit, ale bývá také doplněn o sekundární funkce, které vykonávají činnosti podobné virům, například mažou soubory. Na rozdíl od virů, které vyžadují šíření infikovaného hostitelského souboru. Červy jsou samostatný software a nevyžadují hostitelský soubor nebo lidskou propagaci. Červ pro své šíření zneužívá zranitelnosti cílového systému nebo si dopomáhá metodami sociálního inženýrství. Červ vstoupí do počítače zneužitím zranitelnosti systému a využije jeho síťové funkce, což mu umožňuje cestovat bez jakékoliv pomoci. [6]

4.2.1 Emailový červy

Emailový červy pro své šíření využívají emailů. Pokud proniknou do emailové schránky uživatele a dostanou se k jeho kontaktům, jsou schopny se rozeslat ke všem kontaktům v adresáři uživatele. Pokud i tito uživatelé takový email otevřou, červ získá jejich kontakty a tak to stále pokračuje. Tento typ červa pak ve velkém zahlcuje síť. [6]

4.3 Trojští koně

Jedná se pravděpodobně o nejjednodušší typ škodlivého softwaru. Trojský kůň je destruktivní program, který se tváří jako neškodný. Na rozdíl od virů, trojští koně se nereplikují, ale jsou stejně nebezpeční jako viry. Jedním z nejzákeřnějších trojských koní je program, který tvrdí, že uživatele zbaví počítačových virů, ale místo toho tyto viry do počítače stahuje. Trojští koně spadají do kategorie sociálního inženýrství, protože se snaží uživatele obelhat, aby je nainstaloval. [6]

4.3.1 Trojští koně s funkcí hledání hesel

Trojští koně s funkcí hledání hesel jsou podtřídou trojských koňů, jejichž hlavní funkcí je hledání a odesílání hesel útočníkovy. Díky tomu získají citlivé údaje uživatelů, které následně mohou zneužít. Často také bývají kombinovány s funkcí zaznamenávání kláves[6].

4.3.2 Backdoors

Backdoors je další podtřídou trojských koňů, která slouží hackerovi jako cesta pro vzdálený přístup uživatele. Backdoors jsou více popsány v kapitole 3.1.2.

4.4 Speciální případy

Do této kategorie spadají jak programy, které neškodí v počítači uživatele, ale mohou způsobit paniku. Také sem spadají techniky, jež jsou využívány k odcizení osobních údajů uživatele.

4.4.1 Spyware

Spyware je spíše nepříjemností než hrozbu. Tento software odesílá statistická data o uživateli například počet navštívených webových stránek, či počet nainstalovaných programů. Tato data jsou poté zneužita pro cílenou reklamu, která může být značně nepříjemná. Umisťuje se například do zkušebních programů. O malware se jedná proto, že běží na systému uživatele bez jeho vědomí a může zhoršit běh programů. [1]

4.4.2 Adware

Už z názvu můžeme vyvodit, že adware něco přidává. Tím něčím jsou ve většině případů reklamy, které jsou přidány například jako vyskakující okna na webové stránky, nebo jako reklamy v programech. Některé aplikace a programy jsou nabízeny zdarma a uživatel odsouhlasí, že za poskytnutí dané aplikace zdarma se mu budou zobrazovat reklamy. Rozdíl mezi adwarem a spywarem je ten, že při instalaci programu, který obsahuje adware uživatel musí odsouhlasit, že takový program chce nainstalovat, kdežto spyware běží v systému uživatele bez jeho vědomí.

4.4.3 Hoax

Hoax není jako takový škodlivý software, spíše se jedná o poplašnou zprávu, či nevyžádaný email. Způsobuje strach, pochyby díky tomu že informuje o neexistujícím nebezpečí. Hoax ve většině případů obsahuje čtyři body. Popis nějaké nebezpečí, či popis problému (virus, injekční stříkačka v kině), poté co všechno toto nebezpečí může způsobit, nebo co se může stát, pokud bude ignorováno (vymazání dat, ohrožení dětí), dále pak odkaz na nějaký důvěryhodný zdroj (Microsoft, můj známý pracující v kině) a v poslední řadě výzvu k dalšímu rozesílání. Patří sem i různé petice, falešné prosby o pomoc, řetězové dopisy štěstí, a tak dále. Hlavním poznávacím znamení hoaxu je žádost o hromadné rozeslání dalším osobám.

4.4.4 Phishing

Phishing je podvodná technika, která je využívána k získání citlivých údajů uživatele. Phishing je odvozeno od slova fishing, což v angličtině znamená rybaření. Phising je podobný jako rybaření u jezera, ale místo chytání ryb se phisheři (lidé, kteří se zabývají phisingem) snaží „chytnout“ citlivé údaje uživatele. Phisheři rozesílají podvodné emaily, které se tváří jako opravdové emaily od legitimních společností jako například PayPal, eBay, Komerční banka. V emailu se většinou píše, že je potřeba aby si uživatel upravil své údaje na odkazu, který je k emailu přiložen. Nepozorný uživatel se bude snažit na podvodné stránce přihlásit a přitom dojde k odeslání jeho údajů phisherovi. Nepravost takových stránek jde poznat podle url adresy dané stránky, která se neshoduje s url stránky pravé.

4.4.5 Pharming

Pharming je další podvodná technika, jenž je podobná phisingu. Uživatel ale nemá ponětí, že se nachází na podvodné stránce, protože když zadá adresu správné stránky, tak je přesměrován na stránku podvodnou. Na této stránce zase zadá své citlivé údaje s vědomím, že se nachází na stránce správné. Tyto údaje jsou odeslány podvodníkovi, který je může zneužít. Pharming je oproti phisingu mnohem nebezpečnější, protože je často velmi náročné rozeznat podvodnou stránku od té pravé.

5 KRYPTOGRAFIE

Kryptografie neboli šifrování je hlavní způsob softwarové ochrany dat. Jedná se o proces šifrování informace takovým způsobem, že pouze osoba nebo počítač, která vlastní klíč může tuto informaci rozšifrovat. V šifrování jsou dva základní pojmy:

- Algoritmus – šifry můžeme považovat za algoritmy, což jsou posloupnosti kroků (návod), které vedou k zašifrování informace. Algoritmus poskytuje pokyny a rozsah určitých možných kombinací k vytvoření zašifrované informace.
- Klíč – šifrovací klíč pomáhá člověku nebo počítači upřesnit konkrétní přeměny informace na zašifrovanou informaci, či naopak při šifrování. Jedná se o posloupnost číslicových bitů, které pracují s algoritmem na šifrování a dešifrování informace.

Podle přenosu klíče rozlišujeme dva druhy kryptografie: symetrickou a asymetrickou.

5.1 Symetrická kryptografie

Využívá k šifrování a dešifrování pouze jediný klíč. Nejprve informaci zašifruje klíčem odesílatel, poté je informace přenesena k příjemci, který informaci pomocí stejného klíče dešifruje. Odesílatel a příjemce sdílí jeden klíč. Symetrické šifrování je jednodušší a rychlejší než asymetrické, ale jeho hlavní nevýhodou je, že obě strany si musí nějakým bezpečným způsobem vyměnit klíč. Symetrické šifry se rozdělují podle toho, jak přistupují k otevřenému textu na proudové a blokové. [5]

5.1.1 Proudové šifry

Kryptografický klíč a algoritmus jsou aplikovány na každý jeden bit, přičemž v jednom okamžiku je šifrován pouze jeden bit. Proudové šifry se používají tam, kde předem neznáme délku textu nebo potřebujeme udržet souvislost datového toku.

RC4

Tento šifrovací algoritmus vytvořil v roce 1987 Ron Rivest pro RSA Security. Jedná se o nejznámější proudovou šifru. RC4 může být použita pouze jednou, aby si udržela svoji kryptografickou bezpečnostní sílu. Je považována za velmi bezpečnou a je snadno implementovatelná jak softwarově, tak hardwarově. Využívá rozdílnou délku šifrovacího klíče, jenž se většinou pohybuje od 40 do 256 bitů.

5.1.2 Blokové šifry

Kryptografický klíč a algoritmus jsou aplikovány na blok dat (například 64 po sobě jdoucích bitů) najednou jako celek než na jednotlivé bity, jako je tomu u proudových šifer. Stejně velké bloky dat ve zprávě nejsou šifrovány stejným způsobem (což by značně usnadnilo dešifrování šifrovaného textu). Je běžné, že se šifrovaný text z předešlého bloku dat používá na další blok dat, který je v pořadí. To znamená, že dvě zprávy, které jsou šifrovány ve stejný den, nevytvářejí stejný šifrovaný text. Inicializační vektor odvozený z generátoru náhodných čísel je zkombinován s klíčem a textem v prvním bloku. Tím je zajištěno, že všechny výsledné bloky v šifrovaném textu neodpovídají těm, které vznikly při prvním šifrování.

AES

AES je zkratkou pro Advanced Encryption Standard neboli pokročilý šifrovací standard. AES nahradil překonaný algoritmus DES. AES má tři 128bitové blokové šifry s šifrovacími klíči o velikosti 128, 192 a 256 bitů. Velikost klíče není omezena, ale maximální velikost bloku je 256bitů. AES se vyznačuje vysokou rychlostí a používá se jak v hardwaru, tak i softwaru. [5]

Obr. 3: Proces symetrického šifrování

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 15, upraveno]

5.2 Asymetrická kryptografie

Odlišuje se od symetrické kryptografie v tom, že využívá dva klíče, veřejný a soukromý klíč. Nejdříve si příjemce vygeneruje dvojici klíčů, veřejný a soukromý, příjemce soukromý klíč uloží na důvěryhodné místo a veřejný klíč sdílí do světa.

Odesílatel si poté tento veřejný klíč vezme a zašifruje s ním informaci, kterou následně odešle, příjemce tuto informaci příjme a pomocí soukromého klíče ji dešifruje. [5]

RSA

Algoritmus RSA vyvinula společnost RSA Data Security. Tento algoritmus je založen na obtížnosti faktorizace velmi velkých čísel. Na základě tohoto principu, RSA šifrovací algoritmus využívá faktorizaci jako „padací dveře“ pro dešifrování, jelikož je velmi snadné vynásobit dvě velká čísla, ale správně je rozdělit už je velký problém. Odvození klíče RSA proto vyžaduje velké množství času a výpočetního výkonu. Jedná se o první algoritmus, který je vhodný pro podepisování i pro šifrování. Při dostatečné délce šifrovacího klíče je považován za bezpečný. Zatím za minimální bezpečnou délku je považováno 1024 bitů, ale to se může v blízké době změnit, proto je optimální využívat klíč s délkou alespoň 2048 bitů. Avšak s délkou klíče roste čas, který je nutný k šifrování a dešifrování[5].

DSA

Zkratka DSA znamená Digital Signature Algorithm neboli algoritmus digitálního podpisu. Spolu s RSA je jedním s nejvíce používaných algoritmů pro vytváření digitálního podpisu. DSA na rozdíl od ostatních algoritmů digitálního podpisu nešifruje hash zprávy pomocí soukromého klíče, ani nedešifruje pomocí veřejného klíče. Místo toho využívá jedinečnou matematickou funkci k vytvoření digitálního podpisu skládajícího se ze dvou 160bitových čísel, které jsou vytvořeny z hashe a soukromého klíče. Veřejný klíč je pak využíván k ověření podpisu. Na rozdíl od RSA je ale proces ověřování složitější.

Obr. 4: Proces asymetrického šifrování

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 15, upraveno]

6 POČÍTAČOVÉ SÍTĚ

Počítačová síť je skupina počítačových systémů nebo jiných hardwarových výpočetních zařízení, která je navzájem propojena prostřednictvím komunikačních kanálů, které usnadňují komunikaci a sdílení mezi širokou škálou uživatelů. Sítě například umožňují několika uživatelům sdílet jedno hardwarové zařízení (tiskárnu, skener), sdílení souborů, usnadňují přístup k informacím a podobně. Sítě jsou obvykle rozděleny do kategorií na základě jejich vlastností.

6.1 Klasifikace sítí

Počítačové sítě je možné rozdělit podle různých hledisek, tím nejčastějším je však jejich rozlehlost.

6.1.1 PAN

Personal Area Network zkráceně PAN můžeme přeložit jako osobní síť. Jedná se o síť, jež se nachází kolem individuální osoby, tedy pokrývá vzdálenost jen několik metrů. V této síti se obvykle nacházejí notebooky, mobilní telefony, nebo například PDA. Tyto sítě mohou být použity k přenosu souborů, včetně emailů, událostí v kalendáři, digitálních fotografií a hudby. USB a FireWire kabely obvykle spojují dohromady drátovou PAN.

6.1.2 WPAN

Jedná se o bezdrátovou variantu osobní sítě, na rozdíl od drátových PAN využívají k přenosu technologii Bluetooth, či případně infračervený port, ale ten se v dnešní době už téměř nevyužívá. [5]

6.1.3 LAN

Local Area Network zkráceně LAN můžeme přeložit jako lokální síť. Jedná se o počítačovou síť, která se nachází v malé zeměpisné oblasti jako jsou domy, školy, počítačové učebny, kancelářské budovy nebo skupiny budov. LAN je tvořena vzájemně propojenými pracovními stanicemi a osobními počítači, z nichž každý je schopen přístupu a sdílení dat a zařízení kdekoliv na síti. LAN jsou charakteristické vyššími komunikačními a datovými přenosy. Většina lokálních sítí je postavena s využitím levného hardwaru jako jsou ethernetové kabely, síťové adaptéry a rozbočovače.

6.1.4 WLAN

Jedná se o bezdrátovou metodu přenosu pro dva nebo více zařízení, které používají vysokofrekvenční rádiové vlny, a často také obsahuje přístupový bod k internetu. Je to bezdrátová varianta lokální sítě. Místo Ethernetových kabelů využívá pro přenos rádiových vln. Uprostřed WLAN je většinou umístěn bezdrátový router (nebo několik routerů, pokud se jedná o rozsáhlejší objekt), na kterém jsou umístěny vysílače a přijímače, které slouží ke komunikaci s dalšími zařízeními, jež disponují prostředky pro bezdrátovou komunikaci. [5]

6.1.5 MAN

Metropolitan Area Network zkráceně MAN můžeme přeložit jako metropolitní síť. MAN jsou podobné LAN, ale pokrývají celý areál nebo město. MAN jsou tvořeny spojením několik LAN. MAN poskytují vysoké přenosové rychlosti prostřednictvím vysokorychlostních nosičů jako jsou například optické kabely.

6.1.6 WAN

Wide Area Network zkráceně WAN můžeme přeložit jako rozlehlou síť. Tato síť pokrývá velmi velkou geografickou oblast. WAN propojuje různé menší sítě, včetně LAN a MAN. Díky tomu je zajištěno, že počítače a uživatelé na jednom místě můžou komunikovat s počítači a uživateli na jiných místech. WAN využívají taktéž pro přeno vysokorychlostní nosiče, ale i satelitní rádiové spojení.

6.2 Ochrana počítačových sítí

Ochrana počítačových sítí je obvykle prováděna správcem sítě nebo správcem systému, který implementuje bezpečnostní politiku. Softwarové a hardwarové prostředky ochrany dat, aby zajistil ochranu sítě a zdrojů, které jsou přístupné prostřednictvím této sítě, před neoprávněným přístupem. Pokud se jedná o firmu, tak také musí správce zajistit, aby zaměstnanci dané firmy měli přístup pouze k těm prostředkům, které potřebují k práci. Bezpečnostní síťový systém obvykle závisí na vrstvách ochrany, které se skládají z několika komponentů zahrnujících monitorování sítě, bezpečnostní software a hardware. Všechny komponenty spolu musejí pracovat, aby zvýšily celkovou bezpečnost počítačové sítě. Jednotlivé metody, jež se používají i k ochraně počítačových sítí jsou zmíněny v praktické části. Z hardwarových jsou to hlavně biometrické čtečky, čipové karty a

bezpečnostní tokeny. Ze softwarových jsou to firewally, antivirové programy, IDS a IPS a HoneyPots. [4]

6.2.1 Ochrana bezdrátových počítačových sítí

Ochranou bezdrátových počítačových sítí je myšlena preventivní činnost proti neautorizovanému přístupu nebo poškození počítače pomocí bezdrátových sítí. Mezi nejčastější typy zabezpečení bezdrátových sítí patří WEP a WPA. V dnešní době už mají snad všechny notebooky nainstalovanou bezdrátovou kartu, která slouží pro komunikaci bezdrátovou sítí. Schopnost připojit se kdekoliv, kde je signál bezdrátové sítě, představuje značnou pohodlnost a mobilitu. Avšak bezdrátové sítě jsou náchylné k odposlechům a jsou snadno zachytitelné. Hackeři přišli na to, že bezdrátová síť je snadno proniknutelná, a to i pomocí jiné bezdrátové technologie. V důsledku toho je velmi důležité, aby podniky, které využívají bezdrátovou síť, aby si stanovily efektivní bezpečnostní politiku. Avšak je důležité, aby i domácí uživatelé využívali ochrany. Jak již bylo zmíněno výše, mezi nejčastější typy ochrany patří WEP a WPA. [5]

WEP

Je zkratkou pro Wired Equivalent Privacy, což můžeme volně přeložit jako soukromý ekvivalentní drátovým sítím. Jedná se o bezpečnostní protokol pro bezdrátové lokální sítě WLAN, jenž je definován ve standardu 802.11b. WEP je navrženo tak, aby poskytovalo stejnou úroveň zabezpečení jako u drátových lokálních sítí. LAN jsou ze své podstaty bezpečnější než WLAN, protože LAN jsou chráněny díky jejich fyzické struktuře, jenž má některé nebo všechny části sítě uvnitř budovy, která může poskytovat ochranu proti neoprávněnému přístupu osob. WLAN nemají tuto fyzickou strukturu, protože jsou přenášeny pomocí rádiových vln a proto jsou náchylnější k útokům. WEP poskytuje zabezpečení pomocí šifrování dat na rádiových vlnách, díky čemuž jsou tato data chráněna při přenosu z jednoho koncového bodu do druhého. WEP využívá proudovou šifru RC4 s 40bitovým klíčem a 24bitový inicializačním vektorem, nebo 104bitovým klíčem a 24bitový inicializační vektorem. Pro kontrolu integrity používá algoritmus CR-32. Avšak toto zabezpečení bylo prolomeno již v roce 2001 a bylo nahrazeno zabezpečením WPA. [5]

WPA

Wi-Fi Protected Access zkráceně WPA, můžeme přeložit jako chráněný přístup k Wi-FI. Řeší jej standard IEEE 802.11i. WPA je Wi-Fi standard, jenž byl navržen, aby nahradil překonaný WEP. Je navržen tak, aby pracoval se stávajícími výrobky Wi-Fi, které využívali WEP (čili je to softwarový update na stávajícím hardwarovém zařízení). Oproti WEP vylepšuje šifrování dat, protože zahrnuje 128bitový TKIP (Temporary Key Integrity Protocol), který dynamicky vytváří nové klíče pro každý datový paket. Avšak v TKIP byla později nalezena bezpečnostní chyba a byl nahrazen CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), jenž byl definován ve WPA2. Data jsou u WPA šifrována stejnou proudovou šifrou RC4 jako u WEP, ale na rozdíl od něj využívá 128bitový šifrovací klíč a 48bitový inicializační vektor. Pro kontrolu integrity dat využívá MIC (Message Integrity Code). Přestože WPA vylepšilo bezpečnost oproti WEP, pokud je použito s TKIP, je ho snadné prolomit. Proto se nedoporučuje používat WPA v kombinaci s TKIP. [5]

WPA2

Jedná se o vylepšenou verzi WPA. Jeho cílem bylo dosáhnout úplné shody se standardem standard IEEE 802.11i, jenž bylo dosaženo u WPA pouze částečně, a vyřešit bezpečnostní chybu v 128bitovém TKIP, jenž je nahrazen ve WPA2 CCMP, který je založen na AES. WPA2 je v dnešní době považován za bezpečný. Existují dvě verze WPA2: WPA2-Personal a WPA2-Enterprise. WPA2-Personal chrání před neoprávněným přístupem k síti využitím nastaveného hesla. WPA2-Enterprise ověřuje uživatele pomocí serveru. WPA2 je zpětně kompatibilní s WPA. [5]

7 PENETRAČNÍ TESTOVÁNÍ

Penetrační testování je praktické testování počítačového systému, sítě nebo webové aplikace za účelem nalezení slabých míst, kterých by mohl útočník využít. Penetrační testy mohou být automatizovány pomocí softwarových aplikací, nebo mohou být prováděny ručně. Oba dva způsoby zahrnují proces získávání informací o cíli penetračního testu před testem, určení pravděpodobných míst průniku, pokus o prolomení skrze tyto místa a podání zprávy o zjištěních. Hlavním cílem penetračního testování je nalezení bezpečnostních nedostatků. Penetrační testování může být také použito pro zjištění, jak moc jsou dodržovány bezpečnostní politiky podniku, zda jej pracovníci dodržují a schopnost organizace identifikovat a reagovat na bezpečnostní incidenty. Penetrační testy jsou někdy nazývány jako útoky White hats, protože je provádějí „dobří lidé“. Přestože se v bezpečnostní komunitě často používá penetrační testování jako synonymum k hledání slabých míst, ale jsou to rozdílné pojmy. Při hledání slabých míst je také prováděno skenování, avšak po nalezení těchto míst se s nimi už dál nic neprovádí. Penetrační testování se však po nalezení slabých míst soustředí na jejich zneužití. Penetrační testování může být prováděno buď uvnitř organizace, nebo vně. [3]

7.1 Typy testů

Rozlišujeme tři druhy testů na základě jejich rozsáhlosti.

7.1.1 Red teaming

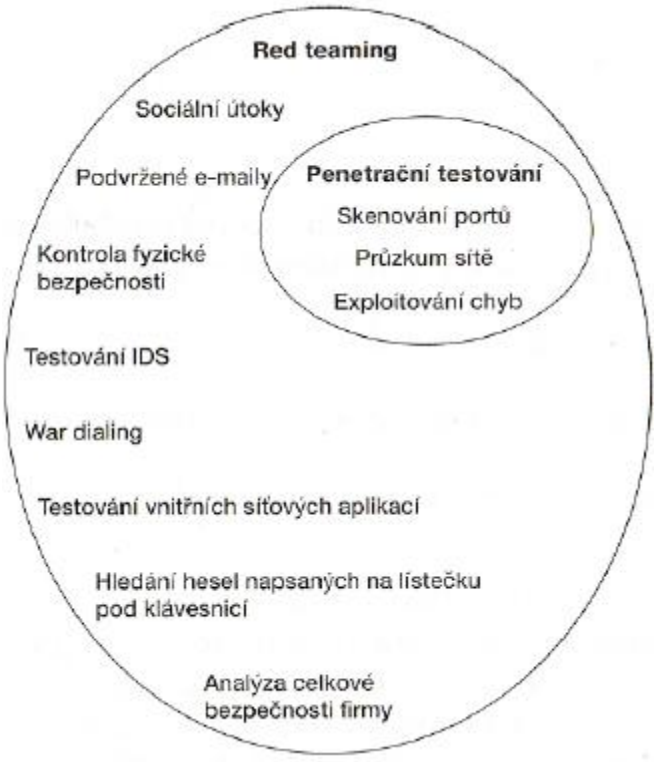
Pokud zákazník vyžaduje co nejširší pohled na bezpečnost jeho informací, využívá se širší analýza, která se nazývá red teaming. Výraz red team (červený tým) pochází z armády, kde se dobré straně říká blue team (modrý tým) a nepřátelské straně red team. Red teaming tedy můžeme považovat za simulaci nepřítele. Pokud má červený tým opravdu simulovat útok, nesmí mu být přiřazeny žádné výhody jako je síťová zástrčka, či kancelář ve výpočetní místnosti. Pokud se jedná o dobrý tým, musí si svou cestu najít sám a nejlépe skrytě, aby otestovali všechny možnosti včetně reakce na tento bezpečnostní incident. Kromě skenování portů a průzkumu sítě se provádí také testování webových aplikací a IDS, ale také sociální útoky a hledání dalších problémů firmy. [3]

7.1.2 Penetrační testování

Je to v podstatě podmnožina red teamingu, jenž zahrnuje převážně skenování portů, průzkum sítě a využívání chyb. Výstupem penetračního testování a red teamingu zpravidla bývá závěrečná zpráva, která poslouží jako seznam chyb a jsou v ní obsaženy pohovory s technickými zaměstnanci, kteří budou tyto chyby opravovat, a s vedením firmy. [3]

7.1.3 Systémové testy

Třetím typem testu jsou systémové testy. Tyto testy slouží k bezpečnostní analýze konkrétního systému nebo aplikace. Jedná se o nejsložitější typ testu, protože již nestačí poukázat na známé chyby, ale je nutné provést hloubkovou analýzu uvnitř systému nebo aplikace a nalézt uvnitř systému nové chyby, či špatné bezpečnostní předpoklady. Test tak může úspěšně odhalit, že například neoprávněný uživatel může zapisovat do systémových souborů. [3]



Obr. 5: Rozdíly mezi penetračními testy a red teamingem

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 3]

II. PRAKTICKÁ ČÁST

.

8 HARDWAROVÁ OCHRANA DAT

Jedná se o ochranu dat s využitím odpovídajících technických prostředků. Obecně je brána jako alternativa k softwarové ochraně, jež využívá hlavně metody šifrování, aby zabránila odcizení dat. Útočník, či vir může přesto tato data poškodit, aby je nebylo možné použít. Hardwarová ochrana dat nám poskytuje zabezpečení proti čtení a zápisu dat a neoprávněnému přístupu.

8.1 Biometrická ochrana

Využívá se k přístupu, či ověření osoby rozpoznávání určitých fyziologických znaků člověka, nelze použít jakékoliv znaky, které člověk má, tyto znaky musí splňovat určité kritéria a to především:

- Trvanlivost – daná charakteristika by se neměla měnit v průběhu času.
- Rozlišitelnost – pokud srovnáme každé dva lidi, tak musejí být v dané charakteristice dostatečně rozdílní.
- Univerzálnost – je potřeba, aby je každý člověk měl.
- Měřitelnost – musejí se dát množstevně změřit.

. V informačních technologiích se nejčastěji využívají fyziologické přístupy a to čtečka otisků prstů a rozpoznání obličeje.

8.1.1 Čtečky otisků prstů

Čtečky otisků prstů slouží k získání a porovnání otisku prstu uživatele. Nejdříve je senzorem sejmut otisk prstu pomocí různých technologií. Poté jsou vyhodnoceny daktyloskopické markanty, kterým jsou přidruženy indexy, následně jsou tyto indexy porovnány s databází. Existuje nespočet čteček otisků prstů. Každá z nich využívá jiného principu snímání prstů, některé jsou více bezpečné, jiné zase méně. Čtečky otisků prstů se obecně dělí do dvou kategorií: kontaktní a bezkontaktní.

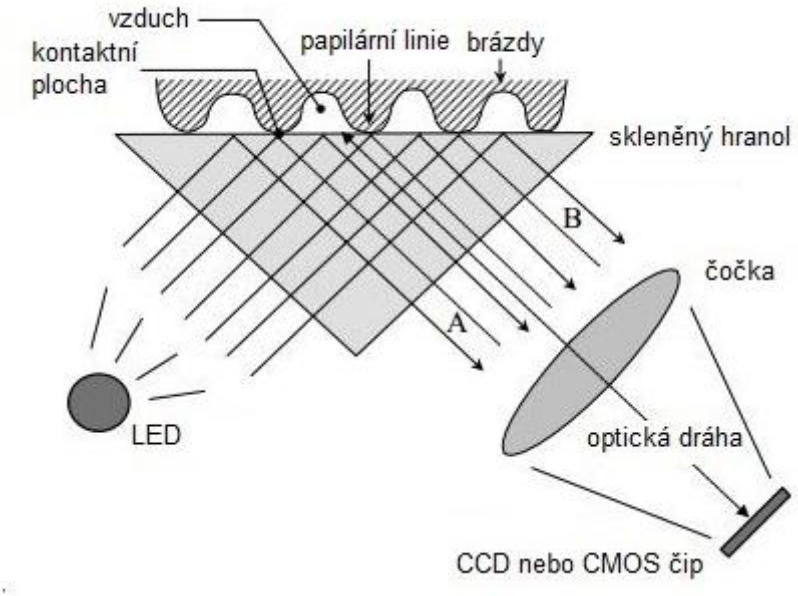
- Kontaktní - po uživateli je vyžadován kontakt se snímačem zařízení - musí k němu například přiložit prst.
- Bezkontaktní – po uživateli není vyžadován kontakt se snímačem zařízení, ale je vyžadována viditelnost mezi snímaným znakem a čtečkou a to na předem určenou maximální vzdálenost.

a) Optické

Optické čtečky otisků prstů využívají ke své činnosti působení světla.

Pracující na technologii FTIR s jedním hranolem

Jedná se o nejstarší typ čteček. Pracují na technologii FTIR – Frustrated Total Internal Reflection. Princip tohoto zařízení spočívá v tom, že uživatel přiloží prst nad skleněnou plochu. LED, která je umístěna v zařízení, vyšle světlo směrem k prstu, toto světlo se od prstu odrazí a následně je koncentrováno pomocí čočky na CCD nebo CMOS snímač, který obraz otisku zachytí. Četnost odraženého světla se odvíjí od hloubky papilárních linií a brázd (od papilárních linií se odráží světlo více, od brázd se odráží méně). Na množství odraženého světla má vliv i špína na prstech, případně na skle. Snímací čip je nastaven tak, že nezaznamenává odraz od brázd. Díky tomu, že zařízení pracující na technologii FTIR snímá trojrozměrný obraz povrchu prstu, nemůže být toto zařízení lehce překonáno přiložením fotografie, či vytisknutého obrázku otisku prstu. Pokud je prst při snímání velmi suchý, nevytvoří se jednotný a konzistentní dotyk s plochou snímání, proto někteří výrobci používají speciální povlak (nejčastěji ze silikonu), který zlepšuje kontakt pokožky se snímacím zařízením. [9]

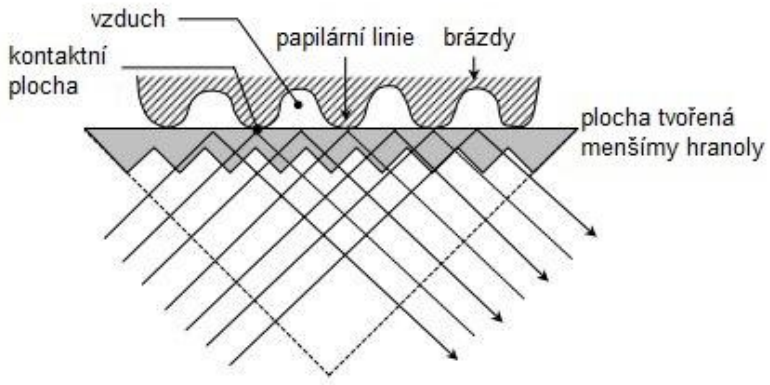


Obr. 6: Princip činnosti technologie FTIR s jedním hranolem

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

Pracující na technologii FTIR s několika hranoly

Čtečky, pracující na této technologii, nevyužívají jediného hranolu, ale plochy, která je tvořena několika menšími hranoly. Tato plocha je značně menší než u technologie FTIR s jedním hranolem. Díky tomu je na výrobu potřeba menší množství materiálu a tím je snížena i cena výroby. Přestože je plocha tvořená několika menšími hranoly znatelně menší, zůstává optická dráha stejná jako u FTIR s jedním hranolem. Výhodou vůči technologii s jedním hranolem je levnější výroba a menší rozměr. Nevýhodou je obvykle horší kvalita pořízených snímků. [9]

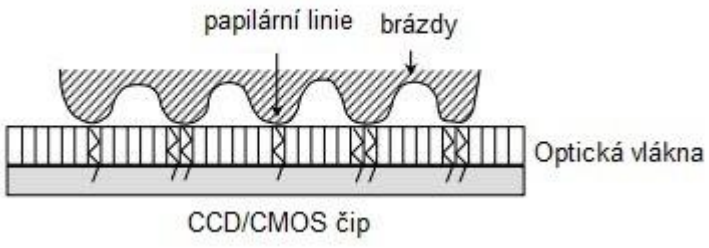


Obr. 7: Princip činnosti technologie FTIR s jedním hranolem

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

Využívající optická vlákna

Tyto čtečky otisků prstů využívají speciální desku tvořenou optickými vlákny (FOP – fiber optic plate). Princip zařízení spočívá v tom, že prst je v přímém kontaktu s vrchní stranou desky. Na spodní straně se nachází CCD nebo CMOS čip pevně spojený s deskou, jenž přijímá zbytkové světlo, které prošlo přes prst, přenášené pomocí skleněných vláken. Výhodou zařízení využívajících tuto technologii je znatelně menší rozměr než u FTIR technologií, jelikož přímo v desce, tvořenou optickými vlákny, se nachází snímací čip. Díky využití optických vláken odpadá také potřeba použití čoček, jelikož optická vlákna jejich funkci nahrazují. Nevýhodou je podstatně vyšší cena, z důvodu toho, že snímač musí pokrýt celou plochu desky. [9]

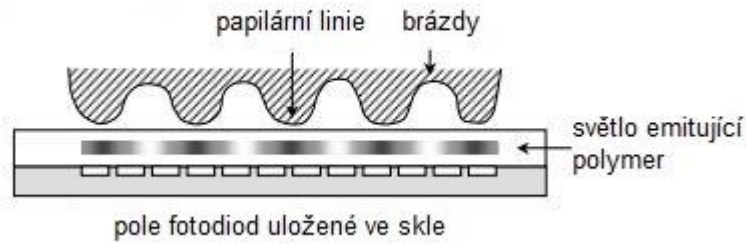


Obr. 8: Princip činnosti technologie využívající optického vlákna

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

Elektrooptické

Elektrooptické čtečky otisků prstů se skládají ze dvou hlavních vrstev, první vrstva obsahuje polymer, který při polarizaci správným napětím emituje světlo. Při přiložení prstu k polymeru se papilární linie dotýkají polymeru, ale brázdy ne, a tak není potenciál ve všech místech plochy stejný. Množství emitovaného světla se mění v závislosti na potenciálu plochy polymeru, což umožňuje vytvoření světelné reprezentace otisku prstu. Druhá vrstva, jež je pevně spojená s první, se skládá z fotodiodového pole (uloženého ve skle). Tato vrstva přijímá světlo, které je emitováno polymerem a přeměňuje jej na digitální obraz. Některé komerční senzory používají pouze první vrstvu, která emituje světlo, k vytvoření obrazu a standardní čočku a CMOS snímací čip pro získání a digitalizaci obrazu. Výhodou elektrooptických zařízení je jejich malý rozměr. Nevýhodou je kvalita pořízených snímků otisků prstů, jež se nedá srovnávat s technologií FTIR. [9]



Obr. 9: Princip činnosti elektrooptické technologie

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

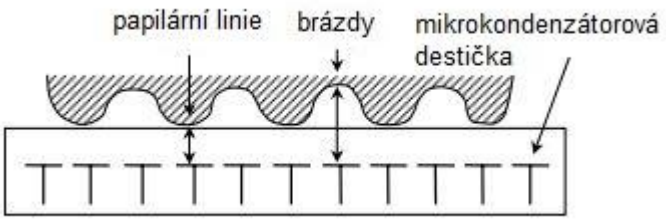
b) Pevné

Pevné čtečky otisků prstů jsou někdy také nazývány jako silikonové, jelikož obsahují silikonovou vrstvu, na kterou se přikládá prst. Všechny tyto čtečky otisků prstů se skládají z pole pixelů. Každý pixel představuje malý senzor. Podle toho, jak přeměňují

fyzický dotyk prstu na elektrický signál, se dělí na kapacitní, termální, rádiové a piezoelektrické.

Kapacitní

V dnešní době patří tato metoda mezi nejpoužívanější z pevných čteček otisků prstů. Kapacitní senzor se skládá z dvojdimenzionálního pole, které je tvořeno mikrokondenzátorovými destičkami, jež je zabudováno do silikonového čipu. Kůže prstu uživatele představuje druhou část každé mikrokondenzátorové destičky. Po přiložení prstu na čip vznikají malé elektrické náboje mezi povrchem prstu a každou kapacitní destičkou Velikost elektrického náboje závisí na vzdálenosti mezi povrchem kůže (papilárními liniemi, brázdami) a jednotlivou kapacitní destičkou. Papilární linie a brázdy mají rozdílné kapacity na různých destičkách. Výhodou této technologie je, že nemůže být oklamána přiložením obrázku, jelikož toto zařízení skenuje pouze trojrozměrný povrch. Další výhodou je možnost upravení elektrických parametrů pro nepříliš ideální pokožku (vlhké nebo suché prsty). Nevýhodou je neustálá potřeba čistit povrch senzoru od nečistot, další nevýhodou je, že reagují na elektrické výboje na konečcích prstů, avšak správnými opatřeními (uzemnění) je možné tuto nevýhodu eliminovat. [9]



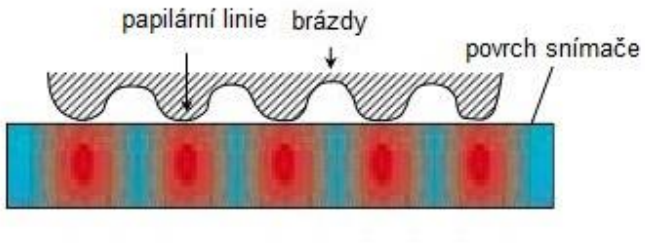
Obr. 10: Princip činnosti kapacitní technologie

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

Teplotní

Teplotní snímače jsou tvořeny pyroelektrickým materiálem, který generuje elektrický proud na základě teplotních rozdílů. Princip tohoto zařízení spočívá v tom, že papilární linie prstu, které jsou v kontaktu s povrchem snímače, mají rozdílnou teplotu než brázdy, které jsou od senzoru vzdáleny. Snímače jsou obvykle pomocí elektrického vyhříváni udržovány při vysoké teplotě, aby byl dosažen dostatečný teplotní rozdíl mezi papilárními liniemi prstu a povrchem snímače. Teplotní rozdíl zapříčiní to, že při kontaktu se snímačem dojde k vytvoření obrazu. Tento obraz ale brzy zmizí, protože se vyrovná teplota mezi prstem a snímačem. Proto může být nezbytná metoda přetáhnutí prstu

k získání kvalitního obrazu otisku prstu. Výhodou tohoto snímače je odolnost vůči elektrostatickému výboji, přiměřená pořizovací cena a malé rozměry. Nevýhodou je nižší kvalita pořízených snímků ve srovnání s ostatními snímači otisků prstů. [9]

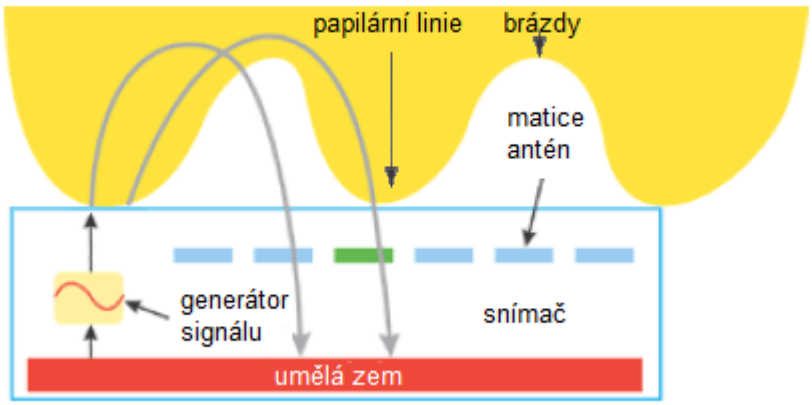


Obr. 11: Princip činnosti teplotní technologie

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

Rádiové

Princip tohoto snímače spočívá v tom, že je nejdříve do prstu vyslán signál pomocí vysílače nízkofrekvenčního signálu. Následně je tento signál snímán maticí miniaturních antén, které jsou umístěny rovnoběžně s plochou snímaného prstu. Síla signálu se mění v závislosti na vzdálenosti mezi kůží a anténní soustavou. Signál je rozdílný mezi papilárními liniemi, které se dotýkají plochy snímače a brázdami, které se nedotýkají. Výhodou tohoto snímače je, že pořizuje snímky ve vysoké kvalitě, je levný a odolný proti nečistotám. [9]



Obr. 12: Princip činnosti rádiové technologie

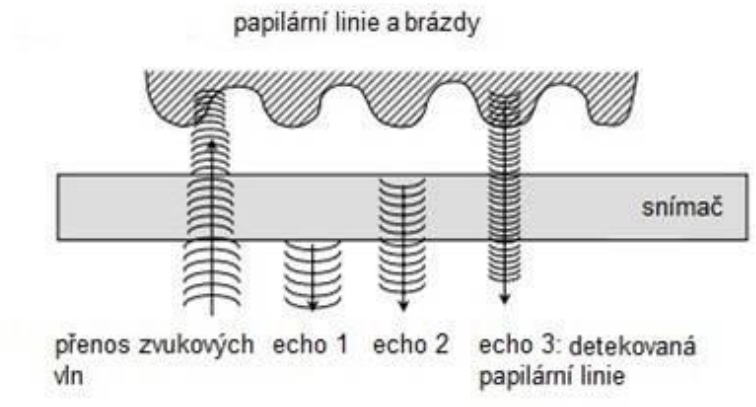
[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 10, upraveno]

Piezoelektrické

Piezoelektrické snímače jsou navrženy tak, aby vytvářely elektrický signál, pokud je na ně vytvářen mechanický tlak. Plocha snímače je tvořena nevodícím dielektrickým materiálem, který při dotyku prstu vytváří malý elektrický proud (tento jev se nazývá piezoelektrický). Síla generovaného signálu závisí na síle dotyku prstu na plochu snímače. Protože jsou papilární linie a brázdy v různých vzdálenostech od povrchu snímače, působí rozdílným tlakem na plochu snímače a tak vytvářejí rozdílné množství elektrického proudu. Naneštěstí tyto snímače postrádají citlivost pro detaily papilárních linií. Tento nedostatek lze vyřešit několika způsoby. Například umístit vodivostní membránu tvořenou maticí piezoelektrických tlakových senzorů na CMOS kameru se silikonovým čipem. Výhodou tohoto snímače je možnost jeho miniaturizace. [9]

c) Ultrazvukové

Ultrazvukové snímače pracující na principu vysílání akustických vln k otisku prstu a následném přijetím echo signálu (odraženého signálu). Z přijatého signálu je pak vytvořen obraz otisku prstu. Tyto snímače se skládají ze dvou hlavních částí z vysílače, který generuje krátké akustické impulsy, a přijímače, který tyto akustické impulsy, odražené od povrchu prstu, přijímá. Výhodou této metody je, že snímá podpovrchovou vrstvu kůže prstu, což znamená, že je odolný vůči špíně a potu na prstech. Nevýhodou tohoto snímače je jeho velká cena. [9]



Obr. 13: Princip činnosti ultrazvukové technologie

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 9, upraveno]

8.1.2 Rozpoznávání obličeje

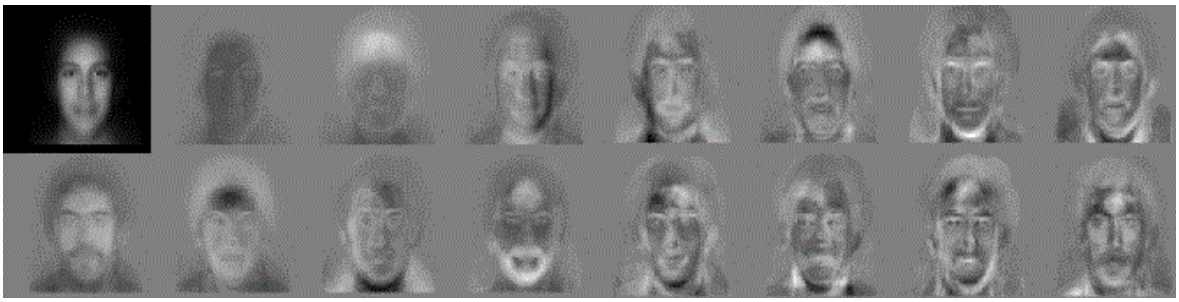
Využívají charakteristik obličeje snímané webkamerou, či integrovanou kamerou, které porovnávají s charakteristikami obličejů uložených v databázi. Rozlišujeme dva základní přístupy rozpoznání obličeje:

- Geometrický – vyhodnocuje rysy obličeje.
- Fotometrický – vyhodnocuje vzhled obrazu obličeje.

Existuje mnoho algoritmů, podle kterých daný program vyhodnocuje tvář. Obecně každý z nich vyhledává na tváři specifické znaky. Může to být například velikost očí, jejich umístění, velikost nosu, čela, úst. Nejběžnějšími algoritmy jsou:

Analýza hlavních částí (PCA)

Tvář každého člověka je možné rozdělit na tzv. eigenfaces (skupina vzorů tváří) a poté ji znovu složit. Všechny eigenface jsou vyjádřeny pouze číslem, čili se neukládá obrázek, ale pouze číslo. Tento algoritmus využívá normalizovaných obrázků, na kterých je předem dáno umístění významných bodů obličeje jako jsou oči, uši atd.… PCA provádí odstranění nadbytečných znaků. Tedy těch znaků, které jsou ve vztahu s jinými znaky. Díky této redukci dojde ke snížení znaků zhruba na tisícinu, což razantně usnadňuje klasifikaci a uložení databází, které by jinak byly příliš velké. Aby tento algoritmu správně pracoval, je nutné předem vytvořit databázi několika snímků každého uživatele. Na každém snímku má uživatel rozdílný výraz obličeje a jednotlivé snímky jsou pořízeny za různých osvětlení. Poté co je provedena detekce a lokalizace obličeje uživatele, dojde k tomu, že se vypočítají eigenvektory (informace o jednotlivých rysech obličeje, soubor těchto eigenvektorů pak tvoří eigenface). Všechny obličeje jsou reprezentovány lineární kombinací eigenfaces. Nejlepší eigenface je následně porovnán s databází. [14]



Obr. 14: Eigenfaces

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 14, upraveno]

Lineární diskriminační analýza (LDA)

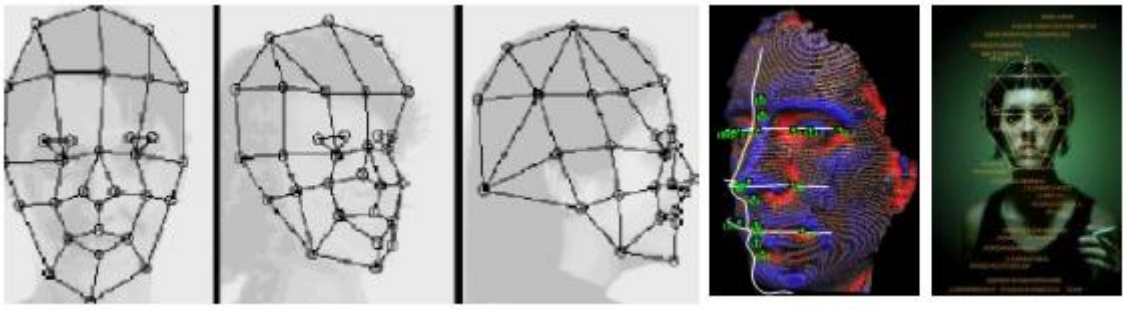
Tento algoritmus nejdříve roztřídí pořízené obrazy tváří do skupin. Poté na základě roztřídění maximalizuje rozdíly mezi jednotlivými skupinami a minimalizuje rozdíly v každé skupině. Každá výsledná skupina pak reprezentuje jednu třídu. Pro správné fungování tohoto algoritmu je potřeba databázi několika snímků obličeje každého uživatele. Tyto snímky by se měly lišit úhlem natočení obličeje, výrazem, nasvětlením scény a barvou pozadí. Pokud uživatel nosí brýle tak snímek s nimi i bez nich. Jak můžeme vidět na obrázku 15, snímky se řadí do dvojrozměrného pole. Obrazy jsou tříděny dle míry podobnosti, jež se určuje především pomocí očí, vlasů, brady, úst. [14]

Obr. 15: Příklad šesti tříd s využitím LDA

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 14]

Elastický srovnávací diagram (EBGM)

Jelikož ostatní metody nemohou uvažovat nelineární charakteristiky jako je osvětlení scény, natočení hlavy či výrazy tváře, bylo potřeba vytvořit algoritmus, který tyto charakteristiky bude umět snímat. Proto došlo k vytvoření elastického srovnávacího diagramu. Princip tohoto algoritmu spočívá v tom, že si na specifických místech obličeje (například koutky očí, úst, špička nosu) vytvoří uzlové body. Tyto body jsou následně propojeny, čímž jsou vytvořeny linie tváře v prostoru, všechny tyto propojené body tvoří souřadnicovou síť obličeje. Z každého obličeje, který je uložen v databázi, se vytvoří tzv. shlukový graf (FBG). Tento graf obsahuje různé pozice uzlových bodů. Algoritmus následně hledá shodné uzlové body snímaného obličeje s uzlovými body z některého snímku z FBG. [14]



Obr. 16: Síť vytvořená elastickým mapováním a obraz zpracovaný počítačem

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 14]

8.2 Hardwarové klíče

Zařízení, které se připojuje k počítači nebo laptopu většinou pomocí USB portu, v němž je naprogramován licenční klíč nebo jiný kryptografický zabezpečovací mechanismus. Využívá se ke zpřístupnění určitého softwaru, který do té doby, než je připojen hardwarový klíč, buď není celý přístupný, nebo jsou z části omezeny jeho funkce (např. nelze tisknout, ukládat soubory). Existují dva druhy hardwarových klíčů a to hardwarový odemykací klíč a obálkový hardwarový klíč. [8]

Hardwarový odemykací klíč

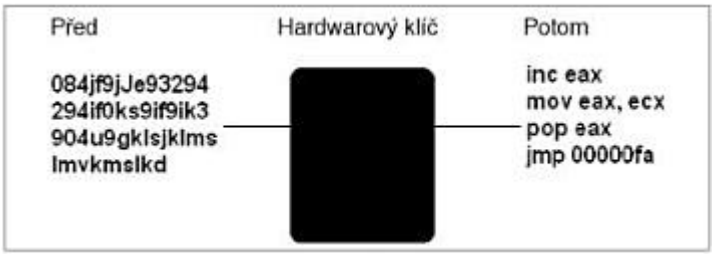
Tyto klíče v sobě obsahují malý ROM čip, jenž má pouze 10 nebo 20 bajtů paměti. V této paměti je umístěno sériové číslo či číselné heslo, jež software načte jako licenci. Princip je obdobný, jako když zadáváme sériové číslo při instalaci programu. Rozdíl je v tom, že toto sériové číslo je umístěno pouze v externím zařízení. Software, který vyžaduje použití hardwarového odemykacího klíče, se neustále dotazuje tohoto klíče na jeho platnost a na obsah jeho paměti ROM. Sériové číslo nebo číselné heslo většinou odkazuje na licenci, kterou vlastník k danému softwaru zakoupil. Pokud při používání softwaru dojde k odpojení hardwarového klíče či k vypršení licence dojde k ukončení softwaru nebo vypsaní varovného upozornění o ukončení platnosti. V některých případech se používá v hardwarových klíčích i šifrování. Například pokud klíč nebo sériové číslo funguje jako šifrovací klíč či heslo k odemknutí chybějících informací v daném softwaru. Bez toho aniž by byl připojen hardwarový klíč, není možno rozšifrovat informaci. Pokud by hacker chtěl překonat toto šifrování, musel by získat kopii softwaru a platnou kopii hardwarového klíče. [8]

Obr. 17: Hardwarový odemykací klíč od firmy Alvis

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 16]

Obálkový hardwarový klíč

Toto zařízení neobsahuje sériové číslo či číselné heslo na rozdíl od hardwarového odemykacího klíče, ale funguje jako dešifrovací mechanismus. Obálkový hardwarový klíč pracuje obdobně jako hardwarový odemykací klíč s tím rozdílem, že software, který je svázán s tímto klíčem, je zašifrovaný, aby ho bylo možné použít, je nutno připojit hardwarový klíč, který tento software dešifruje. Tento druh zabezpečení je velmi těžké obejít, protože nikdo neví, co tento klíč v podstatě dělá. Taktéž velmi ztěžuje zpětné programování. [8]



Obr. 18: Obálkový hardwarový klíč

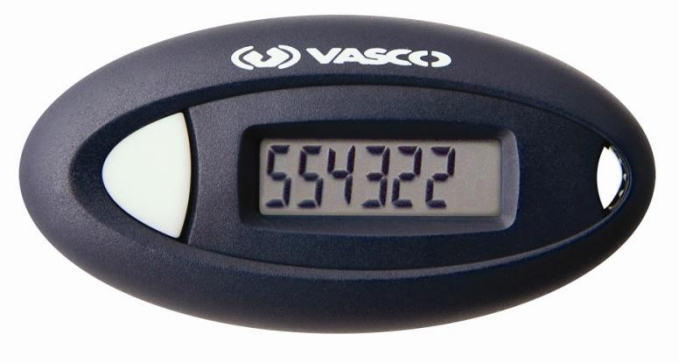
[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 8]

8.3 Bezpečnostní tokeny

Bezpečnostní token (někdy také nazýván jako autentizační token) je malé hardwarové zařízení, které uživatel nosí při sobě a díky tomuto zařízení je mu umožněn přístup k nějaké síťové službě. Toto zařízení může být ve formě čipové karty nebo může být vloženo do běžně používaného předmětu, například klíčenky. Bezpečnostní tokeny poskytují další úroveň zabezpečení pomocí metody dvojúrovňového ověřování (v angličtině známé jako two-factor authetization). První úroveň je tvořena osobním identifikačním číslem (PIN), které je známo pouze uživateli. Druhá úroveň je tvořena unikátním číslem generovaným bezpečnostním tokenem (toto číslo se v pravidelných intervalech pro každého uživatele mění, většinou to bývá každých 5 minut), které jedinečně identifikuje uživatele při přihlášení k dané službě.

a) Nekomunikující s počítačem

Tyto tokeny jsou vyrobeny ve formě zařízení s displejem. Na tomto displeji se zobrazuje jedinečné číslo generované zařízením. Tyto tokeny nemají žádné výstupy, tudíž je není možné připojit k počítači. Při přihlášení na požadovanou stránku uživatel nejdříve zadá jeho osobní identifikační číslo (PIN) a poté zadá číslo, které je zobrazeno na displeji, toto číslo se mění v různých časových intervalech v závislosti na výrobci. Časová synchronizace mezi autentizačním serverem a tokenem je provedena při výrobě zařízení. Bezpečnostní token je poháněn baterií, jejíž výdrž se liší od výrobce. Obvykle je to od tří do pěti let. Nevýhodou tokenů tohoto typu je, že může nastat situace, kdy dojde k rozdílu v synchronizaci se serverem a tím k nepoužitelnosti tokenu, v takovém případě je nutné navštívit výrobce zařízení, aby chybu opravil, případně poskytl nový token.



Obr. 19: Bezpečnostní token od firmy VASCO

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 17]

b) Komunikující s počítačem

Jak už z názvu vyplývá, tento typ bezpečnostních tokenů komunikuje s počítačem, dle provedení to může být buď drátově, nebo bezdrátově. Jejich princip spočívá v tom, že uživatel při přihlašování připojí token do počítače. Z toho tokenu jsou načteny potřebné data pro autentizaci uživatele a uživatel je přihlášen.

USB tokeny

USB tokeny připomínají USB paměť. Taktéž se připojují k počítači pomocí USB rozhraní. Na tomto tokenu většinou bývá natištěné unikátní sériové číslo, aby bylo možné identifikovat jeho vlastníka například při ztrátě. V jednodušším případě jsou v USB tokenu uložena autentizační hesla, pomocí nichž je uživatel po připojení USB tokenu a zadání osobního identifikačního čísla (PIN) autentizován. Ve složitějších případech obsahují také čip jako čipové karty a je na nich uložen privátní klíč, který se používá k šifrování a podepisování dat. Tento privátní klíč nejde z tokenu zkopírovat. Tyto tokeny mají také vestavěnou šifrovanou paměť a je možné do nich ukládat certifikáty.

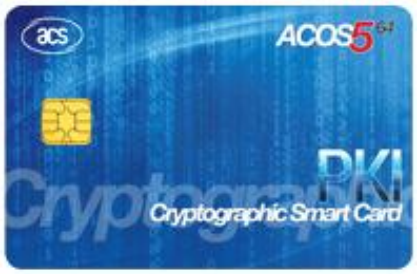
Obr. 20: USB token od firmy Safenet

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 18]

Čipové karty

Čipové karty jsou malé plastové karty s integrovaným obvodem – čipem. Tyto karty se k počítači nepřipojují, ale jsou snímány pomocí externího zařízení – čtečky čipových karet, která se nejčastěji připojuje k počítači pomocí USB rozhraní. Tyto čipové karty v nejjednodušším případě představují bezpečné úložiště autentizačních hesel, jejichž použití je vázáno na zadání osobního identifikačního čísla (PIN). Ve složitějších případech jsou na čipu čipové karty uloženy certifikáty a privátní klíč, které se využívají k autentizaci. Čipové karty, které podporují asymetrickou kryptografii, umožňují generovat

kryptografické klíče přímo na čipu a využít privátního klíče k vytvoření elektronického podpisu. Výhodou čipové karty je možnost natištění dalších poznávacích údajů na kartu například fotografie uživatele. Nevýhodou je pořizovací cena čtecího zařízení.



Obr. 21: Čipová karta od firmy ACS

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 19]

8.4 Hardwarové bezpečnostní moduly

Hardwarové bezpečnostní moduly (HSM), někdy také nazývané jako hardwarová bezpečnostní zařízení jsou fyzická bezpečnostní zařízení, která chrání a spravují digitální klíče pro silnou autentizaci. Tyto moduly jsou vyráběny buď jako zásuvný modul, který se připojuje pomocí PCI rozhraní do základní desky počítače nebo jako externí zařízení, které se připojuje k počítači pomocí USB kabelu nebo přímo k serveru pomocí ethernetového kabelu. Každý bezpečnostní modul obsahuje jeden nebo více zabezpečovacích kryptoprocesorových čipů, aby se zabránilo neoprávněné manipulaci s modulem. Hlavními cíly HSM je poskytnout bezpečné místo pro generování a ukládání šifrovacích klíčů. Taktéž pro šifrovací a dešifrovací operace, služby autentizace a elektronického podpis.

Obr. 22: Hardwarový bezpečnostní modul od firmy Oracle

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 20]

9 SOFTWAROVÁ OCHRANA DAT

Využívá softwarové možnosti pro ochranu dat. V podstatě se jedná o počítačové programy, které v počítači vykonávají činnost, která napomáhá k ochraně dat. Patří sem například firewally, antivirové programy, antispywarové programy, IDS a IPS, nebo také programy využívající šifrování.

9.1 Firewally

Brána firewall je systém navržený tak, aby zabránil neoprávněnému přístupu ať už do nebo z privátní sítě, hlavně intranetu. Firewall si můžeme představit jako zeď, která je mezi počítačem a internetem. Na jedné straně kontroluje informace, které přicházejí z internetu a sítě, a na straně druhé kontroluje informace, které odesílá počítač. Podle předem definovaných pravidel vyhodnocuje, které informace může počítač přijímat a které může odesílat. Díky kontrole informací firewall chrání počítač před útokem hackerů. Firewally bývají často součástí antivirových programů, či některých operačních systémů. Firewall by měl být na každém počítači, který je připojen k síti, či internetu. Firewally mohou být implementovány jak v hardwaru, tak i v softwaru, nebo v jejich kombinaci. [1]

Hardwarové a softwarové firewally

Firewally mohou být buď hardwarové nebo softwarové, ale ideální firewallová konfigurace se skládá z obou. Kromě omezení přístupu k počítači a síti, firewall také umožňuje zabezpečený vzdálený přístupu k privátní síti pomocí ověřovacích certifikátů a přihlášení. Hardwarové firewally je možné zakoupit jako samostatný produkt, ale často se také nacházejí jako součást širokopásmových routek (směrovačů). Hardwarové firewally jsou důležitou součástí komplexního zabezpečení systému, včetně sítě. Většina hardwarových firewallů má minimálně čtyři síťové porty pro připojení dalších počítačů, ale na trhu jsou řešení i pro velké a firemní sítě. Softwarové firewally jsou v počítači nainstalované jako každý jiný software a je možné je nastavit. Nastavení nám poskytuje částečnou kontrolu nad jeho ochrannými funkcemi. Softwarový firewall chrání počítač před útoky, které mají za cíl získat přístup či kontrolu nad počítačem, zvenčí.

Základní typy

Firewally se používají jak pro ochranu domácí, tak i firemní sítě. Typický firewallový program nebo hardwarové zařízení filtrují všechny informace přicházející prostřednictvím Internetu do sítě nebo počítačového systému. Existuje několik typů

firewallů, které zabraňují, aby se potenciálně škodlivé informace dostaly do počítače, či sítě.

Paketový filtr

Jedná se o nejstarší a nejjednodušší formu firewallu. Tento firewall sleduje každý příchozí či odchozí paket sítě a na základě pravidel definovaných uživatelem jej přijme, či odmítne. Pravidla stanovují z jaké adresy a portu na jakou adresu a port může být doručen procházející paket. Výhodou je vysoká rychlost zpracování. Nevýhodou tohoto firewallu je že kontroluje procházející spojení pouze na nízké úrovni, protože je schopný sledovat jednotlivé pakety bez možnosti hledání souvislostí mezi nimi. Také neumožňuje autentizaci vůči firewallu. [4]

Aplikační brány

Komunikace přes aplikační bránu probíhá ve formě dvou spojení. Na straně jedné je klient a na straně druhé je požadovaná služba, ke které se klient chce připojit. Nejdříve musí klient odeslat na aplikační bránu požadavek pro otevření spojení k dané službě. Aplikační brána tento požadavek zpracuje a spojení otevře. Vytvoří se tedy dvě spojení, jedno mezi klientem a aplikační bránou a druhé mezi aplikační bránou a cílovou službou. Všechny data tedy procházejí přes aplikační bránu, která rozhoduje, co se s nimi stane. Aplikační brána je tedy prostředníkem mezi klientem v jedné síti a službou v síti druhé. Díky tomu, že veškerá komunikace probíhá přes aplikační bránu, tak počítače, které jsou za firewallem jsou chráněny. Výhodou je možnost kontroly obsahu přenášených paketů, například pomocí antivirové kontroly, také je zde možné autentizovat uživatele, další výhodou je skrytí zdrojové adresy klienta. Nevýhodou jsou vyšší hardwarové nároky. [1]

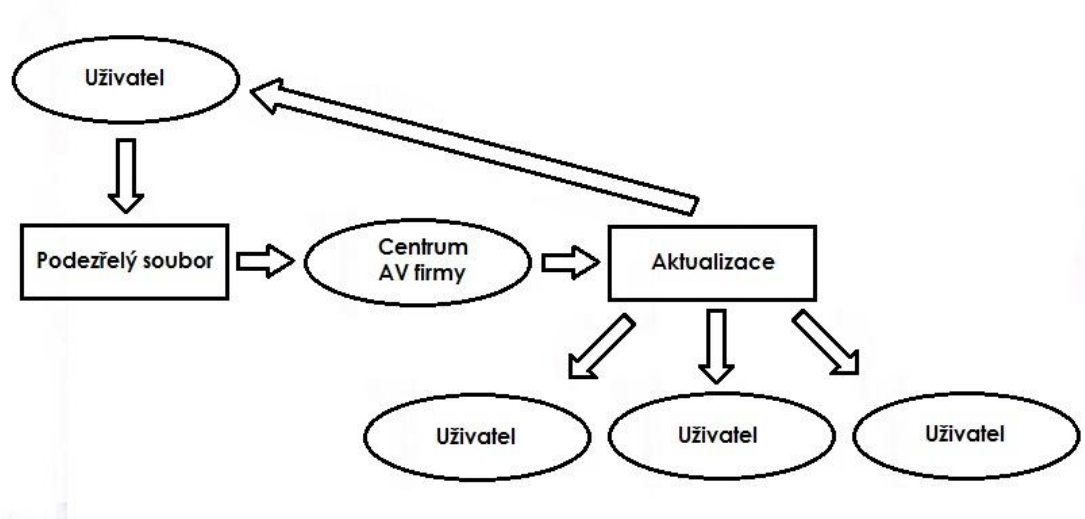
Stavové paketové filtry

Stavové paketové filtry pracují stejně jako paketové filtry, odlišují se od nich však tím, že si ukládají informace o povolených spojeních. Tyto informace pak využívají při rozhodování o budoucnosti paketů, čímž urychlují práci firewallů a celý ověřovací proces. Výhodou je tedy rychlost zpracování požadavků, snadná konfigurace a lepší možnost zabezpečení než u paketových filtrů. Nevýhodou je nižší úroveň zabezpečení oproti aplikační bráně. [4]

.

9.2 Antivirové programy

Antivirové programy vznikly z důvodu potřeby ochrany před počítačovými viry, v dnešní době však poskytují ochranu před většinou typů škodlivého softwaru. Jsou také základním prvkem komplexní ochrany dat, avšak pro celkovou ochranu je potřeba využít dalších prvků zabezpečení. Antivirových programů je mnoho, liší se v závislosti na použití, výbavě, či schopnosti rozpoznání virů a škodlivého softwaru. Mohou se vyskytovat buď ve formě celého bezpečnostního balíku (antivir, firewall, ochrana proti phisingu, atd.), který poskytuje mnoho funkcí, tak i ve formě scannerů, které jsou určeny pouze pro odstranění určitého typu viru a neposkytují další dodatečnou ochranu. Na trhu se nacházejí jak placené verze s možností volby licence pro domácího uživatele, mobilní telefon, či firmu, tak i verze zdarma (freeware). Placené verze poskytují funkce navíc, ale pro obyčejného uživatele postačuje verze zdarma. Nevýhodou antivirů, které poskytují funkci on-demand skenování, která běží na pozadí operačního systému, zabírá systémové prostředky, čímž se snižuje výkon počítače. Na nových počítačích s dostatečnou pamětí RAM pokles výkonu není poznat, ale na starších sestavách je znatelný. V reakci na nové hrozby jsou antivirové programy pravidelně aktualizovány, postup při aktualizaci můžeme vidět na obrázku 23. [6]



Obr. 23: Postup při aktualizaci antiviru

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 1]

a) Funkce antivirových programů

Funkcí, které poskytují antivirové programy, je mnoho, liší se od výrobce a verze. Vybral jsem tedy důležité funkce například on-demand scanner, on-access scanner, heuristickou analýzu, generickou detekci, kontrolu integrity, virovou databázi a karanténu.

On-demand scanner

Jedná se o kontrolu, která se spouští na podnět uživatele. Uživatel si může navolit parametry kontroly, mezi ně patří například typ kontroly (zda se bude jednat o rychlou nebo hloubkovou kontrolu), místo kontroly (celý lokální disk nebo vybrané složky), výjimky (které soubory mají být při kontrole přeskočeny), případně čas (kdy se má kontrola provádět, její pravidelnost, nebo jestli se má provést po restartu počítače). Bývá jak součástí antivirových programů, tak i ve formě scanneru bez dalších funkcí. [6]

On-access scanner

Tato kontrola je neustále spuštěna na pozadí, v rezidentní paměti, jsou kontrolovány všechny operace, které uživatel provádí například práce se soubory (otevírání, vytváření či zavírání), prohlížení webových stránek, či operace s archivy. Pokud je nalezen virus, dojde k vykonání přednastavené akce. Touto akcí může být odstranění viru bez vědomí uživatele, či znemožnění přístupu k postiženému souboru nebo zobrazení nabídky, která obsahuje informace o viru a možnosti, co s napadeným souborem dělat, například ho léčit, uložit do virového trezoru a podobně. [6]

Heuristická analýza

Jedná se o metodu, která slouží k detekci dosud neznámých virů a nových verzí známých virů. Většina antivirových programů, které využívají heuristickou analýzu, ji provádějí spuštěním programových příkazů pochybného programu nebo skriptu v rámci specializovaného virtuálního prostředí. Virtuální prostředí umožňuje antivirovému programu simulovat, co by se stalo v případě, že by se kód programu provedl v reálném prostředí. Příkazy jsou analyzovány, tak jak jsou prováděny, přičemž jsou sledovány podezřelé virové aktivity, jako je replikace, přepsání souborů, či pokus o skrytí existence podezřelého souboru. Pokud je zjištěna jedna nebo více virových aktivit, podezřelý soubor je označen jako potenciální virus a uživatel je upozorněn. Nevýhoda heuristické analýzy je to, že často produkují falešné poplachy. [6]

Generická detekce

Jedná se o další metodu pro detekci neznámých virů. Je postavena na předpokladu, že řada virů je z hlediska programové struktury podobná. Uplatňuje se především na viry z jedné „rodiny“ a na trojské koně, které byly vygenerovány pomocí nástrojů, popřípadě po menší úpravě starších verzí. Pokud jde o virus zcela nový, tak se ve většině případů používá spíše heuristická analýza, protože generická detekce má menší úspěšnost. [6]

Kontrola integrity

Kontrola integrity počítačových souborů patří mezi nejlepší generickou metodu. Jedná se o metodu, při které jsou porovnávány informace (kontrolní součet, atributy atd.) o souborech s informacemi z předchozí kontroly. Například on-demand kontrolory integrity jsou schopny spočítat kontrolní součet všech souborů pomocí vybraných známých algoritmů (např. MD4, MD5). Kontrola integrity poskytuje velmi rychlou kontrolu dat, zda nebyly napadeny. [6]

Virová databáze

Antivirový program obsahuje virovou databázi, ve které jsou obsaženy definice známých virů a jejich kódy. Aktuálnost databáze závisí na rychlosti reakce antivirové společnosti na nové hrozby. Aktuálnost databáze je klíčová v boji proti novým hrozbám, proto jako jeden z hledisek při výběru antivirového programu je rychlost reakce na novou hrozbu.

Karanténa

Karanténa je chráněný prostor, který využívá antivirový program. Do tohoto prostoru ukládá napadené soubory, aby nemohli nakazit další. V karanténě je možné nakažené soubory léčit, smazat nebo obnovit (pokud se jedná o falešný poplach).

b) Vybrané antivirové programy

Většina antivirových programů poskytuje licenci zdarma i licenci placenou. Na trhu se jich nachází nepřeberné množství. Nejpoužívanější antivirové programy, které byly používány v lednu 2004, můžeme vidět v tabulce 2. Vybral jsem dva programy, které jsou určeny pro domácího uživatele.

AVG AniVirus FREE 2014

Jedná se bezplatný antivirový program, který kromě antiviru také poskytuje ochranu odkazů a bezpečné odstranění souborů. Je zaměřen na domácího uživatele a určen pouze pro nekomerční použití. AVG nabízí možnost instalace doplňků například toolbaru, který se nainstaluje do prohlížeče internetu a pomocí něj je pak možné určit, zda je dané stránka bezpečná. Výhodou je automatická instalace aktualizací i přehledné uživatelské prostředí. Pokud je použit bez dalších přídavných doplňků, zatěžuje procesor počítače pouze minimálně. Při použití doplňků výrazně roste jeho náročnost. Nevýhodou jsou časté reklamy, které se nachází v programu a časté falešné poplachy.

Avast! Free Antivirus 2014

Jedná se o přímého konkurenta AVG AniVirus FREE 2014. Taktéž je zdarma pro nekomerční využití, ale vyžaduje do 30 dnů od instalace registraci, která je poté platná na jeden rok, po kterém se musí znovu obnovit. Kromě antivirového programu nabízí také antispyware ochranu, čištění prohlížečů a funkci kontroly softwaru. Výhodou oproti jiným antivirům je jeho antiphisingová funkce a lepší uživatelská podpora. Opět nabízí přívětivé uživatelské prostředí, které není zbytečně přeplácané. Umožňuje také naplánovat kontroly počítače. Jeho náročnost na výkon počítače se pohybuje kolem lepšího průměru. Kvalita detekce je na velmi dobré úrovni s minimem falešných poplachů.

Název antivirového programu	Procentuální podíl na trhu
Microsoft Security Essentials	16,3
avast! Free Antivirus	13,2
Windows Defender	6,2
Avira Free Antivirus	5,0
AVG Anti-Virus Free Edition	4,8
ESET Smart Security	4,6
Malwarebytes Anti-Malware Pro	4,2
AVG Internet Security	3,3
Kaspersky Internet Security	3,3
Norton Internet Security	3,1
ESET NOD32 Antivirus	2,8
COMODO Antivirus	2,7
McAfee VirusScan	2,5
Norton 360	2,3
avast! Internet Security	2,2
Symantec Endpoint Protection	1,9
Jiné	21,6

Tab. 2: Procentuální podíl antivirových programů na trhu leden 2014

[zdroj tabulky zahrnut v seznamu použité literatury, zdroj číslo 13, upraveno]

9.3 Antispywarové programy

Antispywarové programy jsou určeny k detekci a odstranění nežádoucích spyware programů (viz kapitola 4). Tento spyware detekují pomocí metod založených na pravidlech nebo na základě definic stažených souborů, které identifikují běžné spyware programy. Antispywarové programy mohou být použity k nalezení a odstranění spyware programů, které již byly nainstalovány do počítače uživatele, nebo také mohou poskytovat ochranu v reálném čase a zabránit tak stažení spyware. Antispywarové programy mohou být samostatným programem, nebo součástí jiných programů pro ochranu dat.

Vybrané antispywarové programy

Na trhu se nachází mnoho placených i neplacených antispywarových programů, ne všechny jsou však věrohodné a některé mohou být dokonce nebezpečné. Proto je dobré si před koupí, či stažením ověřit důvěryhodnost daného programu. Neplacené verze jsou většinou určeny pouze pro domácí použití. Vybral jsem zde programy, které jsou výkonné a ověřené uživateli.

Spyware Terminator

Jedná se o jeden z nejlepší antispywarových programů zdarma, přestože nabízí i placenou verzi. Verze zdarma je plnohodnotná a není nijak omezena. Má tři typy kontrol – rychlou (pro rychlou kontrolu počítače), úplnou (pro hloubkovou kontrolu počítače) a vlastní (pro kontrolu s nastavením vlastních parametrů). Taktéž nabízí ochranu v reálném čase či možnost naplánování automatických kontrol. Zajímavostí tohoto programu je, že umožňuje instalovat doplňky, které rozšíří funkce programu. Odstraňuje nejen spyware, ale také adware.

Spybot – Search & Destroy

Tento antispyware nabízí taktéž placenou i neplacenou verzi. Umožňuj detekci a odstranění spywaru, adware i trojských koní, dále poskytuje ochranu při prohlížení internetu. V placené verzi Home a Professional navíc poskytuje i antivirovou ochranu a ochranu v reálném čase. Program je přehledný a je ho snadné nainstalovat.

Ad-Aware

Jedná se o antispyware, který je přimo zabudovaný do antivirového programu, čímž poskytuje komplexní ochranu proti malwaru. Tento program nabízí tři placené verze a jednu zdarma. Ve verzi zdarma jsou dostupné funkce antiviru, antispywaru, ochrany

v reálném čase, bezpečné prohlížení, které slouží k ochraně uživatele před podezřelými stránkami. V placených verzích je pak dostupná ochrana bankovnictví či firewall. Ad-Aware taktéž nabízí jednoduché a přehledné uživatelské rozhraní a snadnou instalaci.

9.4 Systém detekce narušení IDS

Intrusion detection systems neboli systémy detekce narušení jsou obranné systémy, které monitorují síťový provoz a snaží se odhalit podezřelé aktivity. Můžeme je taktéž definovat jako soubor nástrojů, metod a zdrojů, které pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity. Jsou detekovány takové aktivity, které mohou být narušením, ale také nemusí. Detekce narušení není samotné ochranné opatření, ale pouze část celkového ochranného systému, jenž je nainstalován na určitém systému či zařízení. [2]

9.4.1 Typy IDS systémů

IDS systémy se dělí do tří kategorií. První kategorií jsou uzlově orientované systémy detekce narušení (host-based intrusion-detection systems, zkráceně HIDS), druhou kategorií jsou síťově orientované systémy detekce narušení (network-based intrusion-detection systems, zkráceně NIDS) a třetí kategorií jsou hybridní systémy zmíněných dvou kategorií. [2]

HIDS

Uzlově orientované systémy detekce narušení jsou tvořeny softwarem, který je nainstalován na jednotlivých počítačích v rámci systému. HIDS analyzuje příchozí a odchozí informace z počítače, na kterém je software detekce narušení nainstalován. HIDS poskytují funkce, které nelze získat s NIDS. Například HIDS je schopen monitorovat aktivity, které by měl být schopen vykonat pouze administrátor. Také umí monitorovat změny a pokusy o přepsání v klíčových souborech systému. HIDS umí také sledovat trojské koně a backdoor programy a umí zastavit jejich pokus o instalaci. HIDS neposkytují ochranu úplnou ochranu v reálném čase, ale pokud jsou nastaveny správně, tak se k ní blíží. [2]

NIDS

Síťově orientované systémy detekce narušení jsou často samostatné hardwarové zařízení, které obsahují síťové funkce detekce narušení. Většinou se skládají buď z hardwarových senzorů rozmístěných na různých místech po celé síti, nebo softwaru, jenž

je nainstalován na počítač připojený k síti, který analyzuje příchozí a odchozí datové pakety pohybující se v síti. NIDS je většinou levnější implementovat a jsou méně náročné na obsluhu, ale nejsou tak univerzální jako HIDS. [2]

9.5 Systém prevence narušení IPS

Intrusion prevention systems neboli systémy prevence narušení jsou dalším stupněm zabezpečovací technologie díky jejich schopnosti zajistit bezpečnost na všech systémových úrovních od jádra operačního systému až po síťové datové pakety. Kde IDS informuje o potenciálním útoku, tam se IPS snaží o jeho zastavení. Obrovským skokem oproti IDS je, že IPS je schopen zabránit známým příznakům útoků, ale i některým neznámým útokům díky jeho databázi chování generických útoků. IDS je spíše pasivní detekční a monitorovací systém a IPS je aktivní preventivní systém. [2]

9.5.1 Typy IPS systémů

IPS systémy mohou být buď uzlově orientované (host-based intrusion-prevention systems, zkráceně HIPS), nebo síťově orientované (network-based intrusion-prevention systems, zkráceně NIPS). [2]

HIPS

Uzlově orientované systémy prevence narušení se používají k ochraně serverů a pracovních stanic prostřednictvím softwaru, který běží mezi aplikacemi systému a jádrem operačního systému. Tento software je nastaven tak, aby na základě narušení, či příznaků útoků stanovil bezpečnostní pravidla. HIPS zachytí podezřelou aktivitu v systému a na základě předem stanovených pravidel rozhodne, zda tuto událost bude blokovat, či ji povolí. Zatímco HIPS jsou považovány za ty, které poskytují lepší ochranu než HIPS, tak cena instalace softwaru na každý server a pracovní stanici v organizaci může být velmi drahá. Navíc HIPS na každém systému musí být pravidelně aktualizován, aby poskytoval ochranu před novými hrozbami. [2]

NIPS

Síťově orientované systémy prevence narušení jsou řešením pro síťově založenou ochranu. NIPS zachytávají veškerý síťový provoz a monitorují podezřelé aktivity a události buď požadavky blokují, nebo předávají dál ty, které považují za legitimní. NIPS pracuje několika způsoby. Většinou balíčky nebo softwarové doplňky určují, jak konkrétní

řešení NIPS pracuje, ale obecně skenuje pro příznaky útoků, hledá protokolové anomálie, rozpoznává příkazy, které nejsou normálně prováděny v sítí a další. [2]

Rozdíly mezi IDS a IPS

IDS	IPS
Instalují se na segment sítě (NIDS) a uzel (HIDS).	Instalují se na segment sítě (NIDS) a uzel (HIDS).
V síti jsou pasivním prvkem.	Jsou zařazovány sériově (nejsou pasivní).
Nemohou analyzovat šifrovaný provoz.	Vhodnější pro ochranné aplikace.
Centrální správa řízení.	Centrální správa řízení.
Vhodnější pro detekci hackerských útoků.	Ideální pro blokaci webových znetvořenin.
Výstrahu vydávající produkt (reaktivní).	Blokující produkt (proaktivní).

Tab. 3: Rozdíly mezi IDS a IPS

[zdroj tabulky zahrnut v seznamu použité literatury, zdroj číslo 2, upraveno]

9.6 Programy využívající šifrování

Hlavním úkolem šifrovacího softwaru je šifrování a dešifrování informací/dat většinou pomocí komplexních matematických algoritmů. Jakmile jsou data zašifrována, je velmi obtížné tato data dešifrovat bez znalosti hesla, které bylo použito pro jejich zašifrování.

9.6.1 TrueCrypt

TrueCrypt je open source šifrovací software, který je určen pro operační systémy Windows, Linux a Mac OS. Díky tomu, že je TrueCrypt open source, je zaručeno, že je jeho kód bezpečný a neobsahuje žádné mezery v zabezpečení, které by mohly vést k narušení bezpečnosti. Podle serveru truecrypt.org je kód tohoto programu neustále hodnocen mnoha nezávislými výzkumníky, aby se zaručila jeho bezpečnost. TrueCrypt umožňuje on-the-fly šifrování (OTFE). On-the-fly šifrování je metoda, která slouží k zabezpečení dat na paměťovém zařízení počítače takovým způsobem, že zabezpečené informace, které se nachází na disku, jsou stále přístupné ověřenému uživateli. Charakteristickým znakem OTFE je, že informace jsou čteny a zapisovány zatímco jsou kódovány, což zaručuje, že nejsou v žádné chvíli nechráněny. TrueCrypt podporuje vícero šifrovacích algoritmů například AES, Twofish a Serpent, či jejich kombinace. Program

umožňuje vytvoření virtuálního disku, jenž je v podobě souboru, který je pak možné snadno připojit a pracovat s ním jako s kterýmkoliv diskem. Také umožňuje šifrovat celý diskový oddíl.

9.6.2 PGP

Pretty good Privacy neboli PGP je počítačový program, která slouží k šifrování a dešifrování dat. Poskytuje kryptografické soukromí a autentizaci pro datovou komunikaci. Využívá kombinace hashování, datové komprese, symetrické a asymetrické kryptografie. Každý krok používá jeden z mnoha podporovaných algoritmů. Každý veřejný klíč je svázán s uživatelským jménem nebo emailovou adresou. PGP také podporuje ověřování zpráv a kontrolu integrity, což nám umožňuje ověřit, zda byla zpráva pozměněna při přenosu a jestli byla opravdu odeslána osobou nebo subjektem, který tvrdí, že ji odeslal. Jelikož obsah zprávy je šifrován, jakákoliv změna zprávy povede při dešifrování příslušným klíčem k selhání. Odesílatel využívá PGP, aby vytvořil digitální podpis pro zprávu a to s použitím RSA nebo DSA algoritmů. Aby mohl být tento digitální podpis vytvořen, musí PGP spočítat hash z otevřeného textu a pak vytvořit digitální podpis z tohoto hashe s využitím soukromého klíče odesílatele.

9.7 HoneyPots

HoneyPot do češtiny přeloženo jako „hrnec medu“ je nástražný počítačový systém, který slouží buď k chytnutí hackera nebo ke sledování atypických či nových hackerských útoků. HoneyPots jsou navrženy tak, aby záměrně nalákaly a oklamaly hackera a identifikovaly nebezpečné aktivity prováděné na internetu. Jediný HoneyPots může napodobovat celý produkční systém, nebo dokonce celou počítačovou síť. Jedním z hlavních úkolů je získat informace od útočníka například jak útočí, na jaké data se zaměřuje. Při nasazení může být přístupný zvenčí, kdy je mu přidělen pro útočníka atraktivní DNS název, nebo nepřístupný, načež by na něj neměl směřovat žádný síťový provoz. Jednoznačnou výhodou HoneyPots je skutečnost, že při napadení nastrčeného systému pak hacker nemá čas útočit na opravdový systém. Existují dva typy HoneyPots Low-Interactive a High-Interactive. [4]

9.7.1 Low-Interactive (LIHP)

Tento typ je realizován pomocí softwaru, který předstírá jednu ze zranitelných služeb, o které se ví, že má bezpečnostní chybu, nebo je často náchylná k útokům.

Nevýhodou LIHP je skutečnost, že o útočníkovi zjistíme méně informací než při HIHP, protože je napodobována pouze jedna služba a ne celý systém, na kterém by mohl provádět mnohem více úkonů. Přesto výhoda tohoto systému spočívá v tom, že po útoku dostáváme snad čitelný výstup většinou ve formě textového souboru. [4]

9.7.2 High-Interactive (HIHP)

Tento typ bývá většinou realizován buď přímo na nezabezpečeném systému nebo na nějakém virtuálním stroji (VMWare). Výhodou HIHP je, že o útočníkovi zjistíme mnohem více informací než u LIHP, může to být například způsob napadení, do jakých souborů se snaží dostat nebo jak za sebou zahlazuje stopy. Z výhody avšak vyplývá i nevýhoda, aby bylo možné získat tyto informace, je potřeba provést hloubkovou analýzu napadeného systému, včetně síťového provozu, která je velmi časově náročná. [4]

10 OCHRANA DAT PŘED ZNIČENÍM

Data mohou být zničena několika způsoby. Mezi ty nejčastější patří jejich smazání nebo fyzické poškození nosiče, na kterém se data nachází. Smazání dat může nastat jak vlivem chyby systému tak i uživatele, případně jeho zlomyslností. Nosič dat může být poškozen fyzickým útokem, přírodní katastrofou, nebo také může po čase přestat fungovat. Ke zničení dat tedy může dojít kdykoliv, proto je důležité data před jejich zničením chránit, mezi nejčastější metody ochrany dat před zničením patří zálohování a duplikace dat.

10.1 Zálohování

Zálohování dat představuje proces, při kterém je kopie vybraných dat uložena na jiný datový nosič. Pokud dojde ke zničení původních dat, je možné tato data obnovit z jejich zálohy. Při obnovování dat jsou původní data přepsána zálohou, tedy jsou ztracena. Hlavní otázka zní: jak často zálohovat data? Jednak záleží, jestli se jedná o jednotlivce, kterému stačí zálohovat důležitá data jednou denně nebo firmu, která svá data zálohuje třeba každou hodinu. Zálohování by nemělo zbytečně zatěžovat systém, pokud se s ním pracuje (tudíž například u serverů se většinou zálohuje v nočních hodinách, kdy k nim přistupuje méně uživatelů), taktéž by mělo probíhat tak často, aby případná ztráta dat byla co nejmenší. Zálohovat by měl každý člověk, který nechce přijít o svá data, ve většině případů dojde k nějaké nepříjemné události, která má za následek ztrátu dat, v tu nejnevhodnější dobu. Pokud je to možné měli bychom také zálohovat na více míst najednou. [1]

a) Typy záloh

Existuje několik typů záloh, každá má svoje výhody a nevýhody. Při vytváření zálohy je dobré myslet na to, že každá zálohovaná data musí být někde uložena a měla by být do určité míry organizovaná. Jednoduchou organizaci záloh je možné provést pomocí listu papíru se seznamem všech zálohovacích médií (CD atd.) a daty, které jsou na nich uloženy. Sofistikovanější způsob organizace může být proveden například pomocí databáze záloh, do které si můžeme přehledně zapsat všechny důležité údaje a mít je kdykoliv k dispozici.

Plná záloha

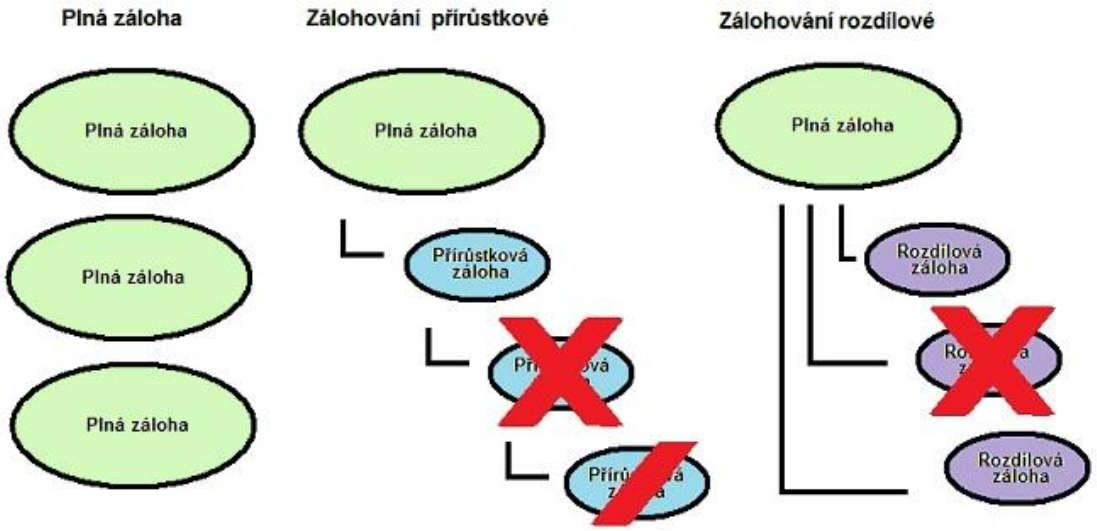
Tento typ zálohy představuje základ pro všechny ostatní zálohy, protože obsahuje veškerá data, která jsou vybrána k zálohování. Díky komplexnosti a soběstačnosti je plná záloha ideálním typem zálohy, avšak díky její časové náročnosti se příliš nevyužívá. Tato záloha je ve většině případů vytvářena každý týden či měsíc a to převážně v nočních hodinách. Výhodou této zálohy je, že nám poskytuje úplnou a rychlou obnovu všech souborů. Další výhodou je to, že ukládá data do jediného souboru, což nám umožňuje lepší správu úložného média. Nevýhoda představuje větší časovou náročnost a vyšší požadavky na úložný prostor v porovnání s ostatními typy záloh. V neposlední řadě tato záloha představuje bezpečnostní riziko, kdyby došlo k jejímu odcizení, může být ohrožena celá organizace. [11]

Přírůstková záloha - inkrementální

Přírůstková záloha si nejdříve vytvoří plnou zálohu na začátku zálohovacího procesu. Další záloha pak ukládá pouze změny, které se objevily od poslední zálohy (tedy je ukládán pouze přírůstek dat, která se nějakým způsobem změnila oproti původní úplné záloze). V pořadí třetí záloha pak následně uloží zase pouze změny oproti předešlé záloze. Nespornou výhodou této zálohy je mnohem rychlejší vytvoření zálohy oproti plné záloze, jelikož je ukládán pouze přírůstek a ne všechna data. Další výhodou je úspora místa oproti plné záloze. Nevýhoda představuje nemožnost obnovit data, která se nachází za poškozenou částí přírůstku, viz obr. 23. [11]

Rozdílová záloha – diferenciální

Rozdílová záloha taktéž na začátku zálohovacího procesu vytvoří jednu plnou zálohu. Další záloha je poté tvořena všemi soubory, které se změnily od poslední plné zálohy. Rozdíl mezi přírůstkovou a rozdílovou zálohou je takový, že přírůstková záloha ukládá v první řadě změny z hlavní plné zálohy a poté pouze změny z přírůstků, kdežto rozdílová záloha ukládá vždy všechny soubory, které se změnily od poslední zálohy. Pokud dojde k poškození jakékoliv rozdílové zálohy, nemá to vliv na ostatní zálohy. Výhodou rozdílové zálohy je kratší čas obnovení dat vůči přírůstkové záloze a rychlejší zálohování vůči plné záloze. Nevýhodou je větší náročnost na úložný prostor než je tomu u přírůstkové zálohy a pokud se zálohuje často, tak může přesáhnout požadovaný úložný prostor, který potřebuje plná záloha. [11]



Obr. 24: Schémata různých typů záloh

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 11]

b) Ukládací média

Ukládací média slouží k uložení zálohovaných dat. Existuje mnoho typů ukládacích médií, avšak každé se hodí na jiný typ použití. Liší se jak v cenových kategoriích, tak v poskytované úložné kapacitě a životnosti.

Magnetické pásky

Magnetické pásky jsou na trhu už více jak 60 let, do dnešní doby jsou nejpoužívanějším ukládacím médiem pro velké objemy dat. Používají se hlavně díky jejich výhodám, což je malá velikost, načež umožňují uložení velkého množství dat. Například firma Oracle v roce 2013 uvedla magnetickou pásku o velikosti 8,5 TB, také jsou snadno přemístitelné a umožňují snadné uložení mimo místo zálohy. Skladovat tyto pásky je možné až 30 let, což z nich činí ideální médium pro zálohování. V podnicích je možné použít robotizované systémy výměny médií, které zajišťuje automatickou výměnu médií. Nevýhodou je vysoká pořizovací cena čtecího a zapisovacího zařízení.

Pevné disky

Pevné disky se nachází v každém počítači, slouží k uložení a k práci s daty. V dnešní době jsou běžné a cenově dostupné (nejlevnější se pohybují kolem ceny 1500 Kč s DPH, květen 2014) pevné disky s kapacitou 1 TB a není problém se setkat i s disky s kapacitou 3 TB. Pevné disky se vyrábějí ve dvou variantách a to interní, které se nacházejí v počítačové skříni a připojují se k základní desce počítače, a externí, které se připojují k počítači pomocí USB rozhraní a jsou přenositelné. V dnešní době se jedná o

velmi rozšířený typ zálohovacího média, protože skoro každý člověk má počítač a v něm jeden, či více pevných disků. Proto není problém si přikoupit další, na který se budou zálohovat data. Výhodou je tedy jejich rychlost čtení a zápisu, kapacita, rychlé a snadné použití. Nevýhodou je náchylnost k mechanickému poškození.

Optické disky

Zapisovatelné CD, DVD či Blu-ray disky jsou běžně používány s osobními počítači, zpravidla jsou také levné. Nicméně kapacity a čtecí rychlosti těchto i jiných optických disků jsou obvykle řádově nižší než u pevných disků nebo magnetických pásek. Mnoho optický disků umožňuje pouze jednorázový zápis, což z optických disků dělá ideální médium pro archivační účely, protože data nelze změnit. Pro firmy, které vyžadují zálohu většího množství dat, je možné použít automatické systémy, které umožňují automatickou výměnu a skladování optických disků bez nutnosti zásahu člověka. Kapacita CD je 700 MB, pro jednovrstvé DVD 4,7 GB a pro Blu-ray disku až 50 GB. Ke čtení a zápisu na tyto disky je vyžadována čtecí mechanika. Výhodou je tedy cena optického disku, které se u CD a DVD pohybuje řádově v desítkách korun a u Blu-ray disků podle velikosti kolem 150 KČ za kus. Při správném zacházení s optickým diskem také jeho životnost, která při správných podmínkách může dosáhnout i několik desítek let.

Flash paměti

Jedná se o USB disky, které poskytují univerzálnost, rychlost a mobilitu, avšak umožňují pouze omezený počet zápisů a jsou náchylné ke ztrátě dat vlivem například statické elektřiny. Jsou tedy vhodné pouze pro domácí uživatele pro krátkodobou zálohu některých souborů. Výhodou je tedy hlavně jejich cena (například USB disk se standardem 3.0 od firmy Kingston o velikost 16 GB s rychlostí čtení 70 MB/s a zápisu 30 MB/s, který je navíc voděodolný, stojí zhruba 400 Kč s DPH), velikost a přenositelnost. Nevýhodou je jejich náchylnost ke ztrátě dat a omezený počet zápisů.

Vzdálená zálohovací služba

Rozšíření vysokorychlostního připojení k internetu umožnilo vznik online zálohovacích služeb. Tyto služby poskytují uložení zálohovaných dat do jejich online úložiště. Přenos dat probíhá pomocí internetu, tudíž rychlost zálohování je limitována rychlostí a vytížením připojení. Na jedné straně poskytují jednoduché použití, které nevyžaduje speciální technické prostředky. Navíc nám odpadá starost fyzického zabezpečení dat, jelikož se o tyto věci stará firma, která poskytuje tuto cloudovou službu.

Nevýhoda spočívá v tom, že nevidíme do zabezpečení dat, takže jej nemůžeme ovlivnit. Například nevíme, kdo všechno má přístup k těmto datům, nevíme, kde se fyzicky nacházejí, či jak je postaráno o data, které ze služby odstraníme. V neposlední řadě také nutnost zabezpečení přenosu dat, který může být odposloucháván jinými osobami.

Datové úložiště na síti

Anglicky označováno jako NAS (Network Attached Storage), jedná se o datové úložiště, které je ideálně připojené k lokální síti, ale jsou možná i jiná řešení (USB, FireWire, WLAN). V podstatě se jedná o klasický pevný disk, případně disky, s nezbytnými součástmi, které se starající se o oboustrannou komunikaci na bázi TCP/IP protokolu. Výhodou je tedy rychlý přístup k datům, vysoká kapacita, která se odvíjí od toho kolik a jaké pevné disky použijeme, nízké náklady.

Médium	Klady	Zápory	Vhodné pro	Nevhodné pro
Páska	Páskové kazety jsou relativně levné. Nelze je snadno přepsat.	Pomalý lineární přístup. Automatizované páskové knihovny mohou být velice nákladné.	Automatizovanou zálohu velkých datových serverů. Dlouhodobou archivaci.	Zálohu jednotlivých pracovních stanic a počítačů. Rychlou obnovu.
CD/DVD	Náhodný přístup. Levné pořízení. Téměř každý počítač má vypalovací mechaniku CD/DVD.	Omezená kapacita, což znamená výměnu disků při zálohování velkého objemu dat. Životnost.	Off-line zálohu jednotlivých počítačů a notebooků. Spouštěcí obnovovací disky. Dlouhodobou archivaci.	Zálohu serverů.
Paměťové karty/ flash	Jednoduché ovládání a ukládání. Není potřeba nic jiného než USB port nebo slot pro paměťové karty.	Snadný přepis, snadno se poškodí a ztratí. Omezená kapacita.	Náhodnou zálohu důležitých dokumentů a datových souborů.	Pravidelnou zálohu serverů nebo stolních/přenosných počítačů.
Externí pevný disk	Rychlý náhodný přístup. Kapacita. Nízké náklady.	Snadno přepisovatelné. Nesnadno přenosné.	Automatizovanou zálohu serverů a pracovních stanic v síti.	Zálohu velkých datových serverů. Dlouhodobou archivaci.
Síťové uložiště	Rychlý náhodný přístup. Vysoká kapacita. Nízké náklady.	Snadno přepisovatelné.	Automatizovanou zálohu serverů a pracovních stanic v síti.	Dlouhodobou archivaci.
Cloudové uložiště	Externě spravované prostředky.	Rychlost zálohování/obnovy omezena rychlostí připojení k internetu.	Zálohu notebooků mobilních uživatelů.	Zálohu/obnovu serverů.

Tab. 4: Porovnání médií pro zálohování a obnovu

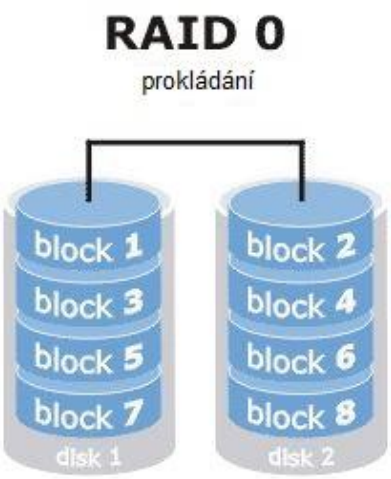
[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 11]

10.2 RAID

V minulosti označení RAID znamenalo vícenásobné pole levných disků (Redudant Array of Inexpensive Disks), ale v dnešní době je spíše odkazováno na vícenásobné pole nezávislých disků (Redudant Array of Independent Disks). Zatímco v minulosti používala zařízení pro ukládání dat pouze jeden disk, dnešní RAID využívají koordinovanou práci dvou nebo více disků k ukládání, čímž poskytují ochranu dat před poškozením či selháním pevného disku. Disková pole RAID jsou často využívána na serverech, kde je vyžadován neustálý provoz, pokud dojde k selhání jednoho disku, je možné ho okamžitě vyměnit za jiný. Existuje několik typů RAID, jednotlivé typy jsou označovány čísly (například RAID 1), každý z nich poskytuje jinou úroveň zabezpečení dat. Mezi nejpoužívanější patří RAID 0, RAID 1 a RAID 5. Je důležité si uvědomit, že RAID nenahrazuje zálohování dat.

RAID 0

Technicky vzato RAID 0 není RAID, protože neposkytuje datům žádnou ochranu (porucha jednoho disku znamená ztrátu dat), ale je takto obvykle vnímán. Řekněme, že máme tři disky. Místo toho, abychom data zapsali pouze na jeden disk, tak tyto data rozdělíme a zapíšeme jejich část na každý z těchto tří disků. První část je tedy uložena na první disk, druhá část na druhý disk, třetí část na třetí disk a čtvrtá znovu na první disk, a tak se to stále opakuje. Jedná se o metodu prokládání, jak můžeme vidět na obrázku 25. Při čtení dat nečteme pouze z jednoho disku, ale ze tří disků zároveň. Na konci jsou tato data zkombinována. Díky tomu, že čteme z několika disků zároveň je zvýšen výkon. Pokud dojde k poškození jednoho z těchto tří disků, jsou všechna data uložená na nich ztracena, protože jich kus bude chybět a nebudou celistvá. Výhodou RAID 0 je jejich výkon, jak čtecích tak zapisovacích operací. Taktéž zde není zpomalení výkonu způsobené kontrolou parit. Další výhodou je, že je využita kapacita všech disků. RAID 0 vyžaduje alespoň dva disky. **Výhody:** výkon, jak čtecích tak zapisovacích operací; žádné zpomalení výkonu způsobené kontrolou parit; využití celé kapacity všech disků; snadná implementace. **Nevýhody:** poškození jednoho disku zapříčiní ztrátu všech dat. **Ideální použití:** RAID 0 je ideální pro nekritické úložiště dat, kde je potřeba číst a zapisovat data velmi rychle například studio, které pracuje s programem Photoshop a velkými fotkami. [12]

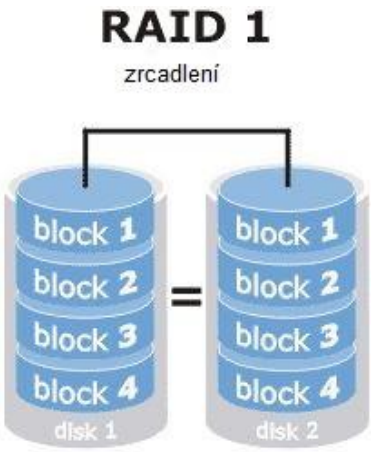


Obr. 25: RAID 0

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 12]

RAID 1

RAID 1 využívá metodu zrcadlení, kdy jsou ukládána stejná data na více disků najednou, jsou vyžadovány alespoň dva disky. Představme si, že máme dva disky. Uložíme data na jeden disk a ty samá data se uloží zrcadlově i na druhý disk. Myšlenka je, že pokud dojde k poškození jednoho z těchto dvou disků, pak máme disk druhý, který stále pracuje, čímž se zlepšuje dostupnost dat. RAID 1 také umožňuje zvýšení výkonu. Pokud vše pracuje správně, oba disky se točí a chovají normálně, tak při čtení čteme data ze dvou disků naráz, čímž se dvojitě zvyšuje výkon čtení. Zvýšení výkonu je pouze u čtení dat, ale ne u zápisu. RAID 1 systémy se často kombinují s RAID 0 pro zlepšení výkonu. RAID 1 vyžaduje alespoň dva disky. **Výhody:** RAID 1 poskytuje excelentní rychlost čtení (rychlost zápisu je srovnatelná s jedním diskem); pokud dojde k selhání jednoho disku, data nemusí být přestavěna, ale pouze zkopírována na náhradní disk; RAID 1 je velmi jednoduchá technologie. **Nevýhody:** efektivní úložná kapacita je pouze polovina kapacity celého disku, protože všechna data musejí být zapsány dvakrát; softwarové řešení RAID 1 ne vždy umožňuje nahrazení vadného disku při běhu serveru, v ideálním případě je použit hardwarový řadič. **Ideální použití:** RAID-1 je ideální pro kritické ukládání dat například pro účetní systémy; vhodný pro malé servery, ve kterých jsou použity pouze dva disky. [12]

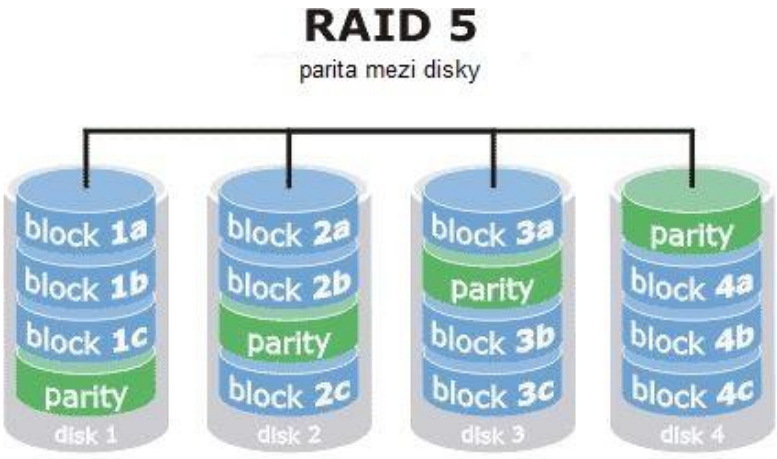


Obr. 26: RAID 1

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 12]

RAID 5

RAID 5 je nejběžněji používaným typem RAID, je podobný RAID 3 (využívá paritního disku, jenž je dopočítáván z ostatních disků), s tím rozdílem že parita (která slouží k obnovení dat při poruše disku) není uložena na jeden disk, ale je střídavě uložena na všechny disky. Pokud máme 4 disky jako na obrázku 27 a jeden z nich se porouchá, tak jsme schopni dopočítat chybějící data ze zbývajících tří disků. To znamená, že máme toleranci chyby jednoho disku, která nám zlepšuje dostupnost dat. **Výhody:** rychlost čtení dat. **Nevýhody:** selhání disku může mít vliv na propustnost dat; pomalejší rychlost zápisu dat (z důvodu, že musí být dopočítávána parita); komplexní technologie. **Ideální použití:** RAID 5 je všestranný systém, který kombinuje efektivní ukládání dat s kvalitním zabezpečením a slušným výkonem, je tedy ideální pro souborové a aplikační servery. [12]



Obr. 27: RAID 5

[zdroj obrázku zahrnut v seznamu použité literatury, zdroj číslo 12]

11 FYZICKÁ OCHRANA DAT

Fyzická ochrana dat slouží k fyzickému zabránění neautorizovaných lidí v přístupu k počítačům a informačním systémům, či zařízením. Ne všechny útoky na data musí pocházet z počítačové sítě. Některé podniky zapomínají na to, že i když zabezpečí svá data různými hardwarovými či sofwarovými způsoby, tak stále někdo může ukradnout zařízení, na kterém jsou tato data uložena, pokud nebudou chráněny i prostory, kde se zařízení nachazí. Útočnící nemusejí přicházet jen z „venčí“ podniku, ale mohou to být i nespokojení nebo chamtivý zaměstnanci.

11.1 PZTS

Jedním ze způsobů, jak zabránit neoprávněným osobám vstup do chráněných prostor je využití poplachových zabezpečovacích a tísňových systémů (PZTS). Jedná se o soubor technický prostředků, jejichž hlavním hlavním účelem je ochrana zdraví a majetku. PZTS se skládá z ústředny, ovládací klávesnice, detektorů a koncových zařízení. Vždy záleží na objektu, který se má chránit a do jakého stupně zabezpečení spadá. Projektant na zálakladě bezpečnostní analýzy navrhe systém, který bude chránit celý objekt a bude vyhovovat zákazníkovým potřebám. Daný objekt je možné rozdělit na subsystémy a zóny a vytvořit speciální režim zabezpečení pro dané místnosti, či celé patra, kde se zařízení, na kterých budou data umístěna, budou nacházet. PZTS je vhodné doplnit o mechanické zábranné systémy (MZS), do kterých spadají například zámkové systémy, bezpečnostní dveře, trezory a podobně. K PZTS je možné doplnit další systémy například CCTV a ACS.

11.2 CCTV

Pokud potřebujeme mít neustálý dohled nad chráněnými prostory, kde se naše data nachází, je možné využít uzavřeného televizního okruhu (CCTV) neboli kamerového systému. Díky vzdálenému přístupu umožňuje dohled nad rozsáhlými prostory buď v reálném čase nebo pomocí záznamu.

11.3 ACS

Systémy kontroly vstupu (ACS) slouží, jak už název napovídá, ke kontrole vstupu. Umožňují nám určit, kdo, kdy a kam může jít a zároveň tyto osoby evidují. Jejich hlavní činností je zabránění neoprávněným osobám do míst, kam nemají přístupové právo.

ZÁVĚR

Podařilo se mi splnit cíle stanové v úvodu, tedy popsat a logicky seřadit jednotlivé metody ochrany dat. Přesto jsem však nebyl schopen zahrnout naprosto všechny metody, protože daná problematika ochrany dat je velmi rozsáhlé téma a proto jsem popsal ty nejhlavnější metody ochrany dat. Jednotlivé metody jsou popsány výstižným způsobem, aby byl pochopen jejich účel. V praktické části jsem je roztřídil do čtyř hlavních kapitol a to hardwarové metody, softwarové metody, ochrana dat před zničením a fyzická ochrana dat. Některé prostředky ochrany dat můžou být ve formě jak hardwarové, tak softwarové. Aby byla zachována jejich přehlednost, jsou začleněny pouze v jedné z těchto kapitol na základě jejich častějšího použití v dané kategorii.

V hardwarové ochraně dat se můžeme setkat s několika problémy. Například po nákupu nového hardwaru nejsou jeho uživatelé často dostatečně seznámeni s tímto hardwarem, což může mít za následek jeho poruchu a nebo špatné vyhodnocování. Další problém vzniká při nákupu nekvalitních hardwarových prostředů, které mohou být snadno oklamány a tak neposkytují téměř žádnou ochranu. Avšak těmto chybám se lze vyhnout a to dostatečným seznámením uživatelů s novým hardwarem a volbou kvalitního hardwaru. Pokud se uživatel v těchto prostředcích neorientuje, vždy je možné se poradit s bezpečnostními odborníky.

V softwarové ochraně dat se také můžeme setkat s problémy. Hlavní problém některých uživatelů zahrnuje chybné posouzení ochrany. Tyto omyly zahrnují zbytečné využívání například dvou antivirových programů, které se v závislosti na sobě mohou rušit. Další problém je opět volba nekvalitního či nebezpečného softwaru. Na internetu se nachází nepřeberné množství produktů. Některé programy se můžou tvářit jako legitimní, ale místo, aby poskytovali ochranu, umožní útočníkovi přístup do systému. Doporučení v této oblasti platí obdobně jako u hardwarových prostředků. Je důležité vždy volit pouze ověřený software, testovaný nezávislými organizacemi. Abychom zabránili předimenzování ochrany systému, ve většině případů stačí nepoužívat dvě ochrany stejného typu (dva firewally, dva antivirové programy atd.).

Přestože se již na základních školách učí informatika, počítačová bezpečnost je často opomíjena. Větší zaměření na počítačovou bezpečnost by mohlo vést ke zvětšení vzdělanosti uživatelů a ke snížení jejich nebezpečného chování. Jednotlivé metody ochrany

dat se budou do budoucna nadále vyvíjet stejně tak jako hrozby. Potenciál však vidím v prostředcích, které budou umět reagovat a eliminovat i naprosto nové hrozby.

CONCLUSION

I managed to accomplish objectives defined in the intoduction – describe and logically arrange the particular methods of data protection. Nevertheless i was not able to cover completely all methods because this issue of data protection is very vast subject and that is the reason why i described only the most important methods od data protection. The individual methods are delineated by accurate manner so the purpose could be understood. The practical part is categorized into four main chapters namely hardware methods , software methods, protection of data against destruction and physical data protection. Some means of data protection can be in the both form hardware and software. In order to preserve its clear arrangement these means are integrated only in one of these chapters based on its more frequent application in that category.

In hardware data protection we can encounter several problems. For example after purchase a new hardware, its user often no familiar with that hardware, which may result in a malfuction or a bad evalution. Another problem arises after buying low-quality hardware, which can be easily deceived, so they do not provide almost any protection. However these mistakes can be avoided by an adequate familiarization users the new hardware and by a choise of quality hardware. If the user is not well informed in these products, he can always consult it with security experts.

In software data protection we can encounter several problems too. The main issue of some users includes incorrect evaluation of protection. These mistakes includes unnecessary use for example two antivirus programs, which might interfere each other. Another problem is again the choice of low quality or malicious software. On the Internet are many kinds of products. Some programs might seem legitimate, but instead of provision a protection it allows the attacker acces to the system. Recommendation in this area are similiar to advices about hardware resources. It is always important to choose only certified software, tested by independent organizations. To avoid oversizing system protection, in the most cases it is convenient not to use two protection of the same type (two firewalls, two anti-virus programs, etc.).

Although the information technology is taught at primary schools, the computer security is often neglected. Greater focus on computer security could lead to increase education of users and to reduce their dangerous behavior. The individual methods od data

protection will continue evolve in the future as well as threats. The future potential might be in resources which will be able to repond and eliminate even completely new threats.

SEZNAM POUŽITÉ LITERATURY

[1] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

[2] ENDORF, Carl. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

[3] HARRIS, Shon. *Hacking: manuál hackera*. 1. vyd. Praha: Grada, 2008, 399 s. ISBN 978-80-247-1346-5.

[4] LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. *Teorie bezpečnosti počítačových sítí*. Vyd. 1. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.

[5] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[6] SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Vyd. 1. Brno: Zoner Press, 2006, 608 s. ISBN 80-868-1504-8.

[7] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[8] CRAIG, Paul a Ron HONICK. *Softwarové pirátství bez záhad*. 1. vyd. Překlad Tomáš Hlaváč. Praha: Grada, 2008, 212 s. ISBN 978-80-247-1765-4.

[9] MALTONI, Davide, Dario MAIO, Anil JAIN a Salil PRABHAKAR. *Handbook of fingerprint recognition*. London: Springer, 2009, xvi, 494 s. ISBN 978-1-84882-253-5.

[10] Biometric Fingerprint Recognition. GUPTA, Pooja. *How to exam?* [online]. 2011 [cit. 2014-03-27]. Dostupné z: http://www.howtoexam.com/index.php?option=com_content&view=article&id=273:biometric-fingerprint-recognition&catid=793:materials-and-industrial-technology

[11] Zálohování a archivace dat v podnikovém prostředí – 5. díl, Typy záloh a jejich rotační schémata. JUNEK, Pavel. *Zálohování* [online]. 2013 [cit. 2014-04-30]. Dostupné z: http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-5-dil-typy-zaloh-a-jejich-rotacni-schemata/

[12] LEURS, Laurens. RAID level 0, 1, 3, 5 and 10: Advantage, disadvantage, use. *Prepressure.com* [online]. 2013 [cit. 2014-05-03]. Dostupné z: http://www.prepressure.com/library/technology/raid

[13] Antivirus Market Share Report January 2014. *OPSWAT: Software manageability and multiple engine scanning solutions* [online]. 2014 [cit. 2014-05-17]. Dostupné z: http://www.opswat.com/about/media/reports/antivirus-january-2014

[14] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2014-22-05]. Dostupné z WWW: http://www.biometrickypodpis.cz/PDF/biometricke_metody.pdf

[15] Data Confidentiality. *MSDN: Microsoft Developer Network* [online]. 2005 [cit. 2014-05-24]. Dostupné z: http://msdn.microsoft.com/en-us/library/ff650720.aspx

[16] ADI - ALVIS HWKLIC/USB - hardwarový klíč pro ALVIS, provedení USB. *ADI Global Distribution* [online]. 2014 [cit. 2014-05-28]. Dostupné z: http://www.adiglobal.cz/iiWWW/cz/produkty310.nsf/w/C2FCC47A7BF9CEB6C12575E8002D837A?OpenDocument

[17] VASCO Strong Two Factor Authentication - DIGIPASS GO 3. *VASCO Data Security - A World Leader in Strong Authentication* [online]. 2014 [cit. 2014-05-28]. Dostupné z: http://www.vasco.com/products/client_products/single_button_digipass/digipass_go3.aspx

[18] Safenet eToken 7300. *ASKON INTERNATIONAL s.r.o* [online]. 2012 [cit. 2014-05-28]. Dostupné z: http://www.askon.cz/Produkty/Autentizace/USB-Tokeny/Safenet-eToken-7300.html

[19] Smart Card - ACOS5 Cryptographic Smart Card. *ACS - Top PC-linked Smart Card Reader Supplier* [online]. 2014 [cit. 2014-05-28]. Dostupné z: http://www.acs.com.hk/en/products/17/acos5-64-cryptographic-smart-card/

[20] Crypto Accelerator 6000 PCIe Card. *Oracle: Hardware and Software, Engineered to Work Together* [online]. 2014 [cit. 2014-05-28]. Dostupné z: http://www.oracle.com/us/products/networking/ethernet/crypto6000-pcie/overview/index.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS Access Control System – systémy kontroly vstupu

AES Advanced Encryption Standard - pokročilý šifrovací standard

CCD Charge-coupled device - zařízení s nábojovou vazbou

CCMP Counter Cipher Mode with Block Chaining Message Authentication Code Protocol

CCTV Closed Circuit Television – uzavřené televizní okruhy

CD Compact Disc – kompaktní disk

CMOS Complementary metal–oxide–semiconductor - doplňující se kov-oxid-polovodič

DES Data Encryption Standard – standard šifrování dat

DSA Digital Signature Algorithm - algoritmus digitálního podpisu

DVD Digital Versatile Disc - Digitální víceúčelový disk

EBGM Elastic Bunch Graph Matching - elastický srovnávací diagram

FBG Face bunch graph - shlukový graf

FTIR Frustrated total internal reflection – narušený úplný vnitřní odraz

GB Gigabyte

HIDS Host-based intrusion detection system - uzlově orientované systémy detekce narušení

HIPS Host-based intrusion-prevention systems - uzlově orientované systémy prevence narušení

HSM Hardware security module – hardwarový bezpečnostní modul

IDS Intrusion detection systems - systémy detekce narušení

IEEE Institute of Electrical and Electronics Engineers - institut pro elektrotechnické a elektronické inženýrství

IP Internet Protocol – internetový protkol

IPS Intrusion prevention systems - systémy prevence narušení

LAN Local Area Network - místní síť

LDA Linear Discriminant Analysis - lineární diskriminační analýza

LED Light-Emitting Diode – dioda emitující světlo

MAC Media Access Control - řízení přístupu k médiu

MAN Metropolitan Area Network – metropolitní síť

MB Megabyte

NAS Network Attached Storage – datové úložiště na síti

NIDS Network-based intrusion-detection systems - síťově orientované systémy detekce narušení

NIPS Network-based intrusion-prevention systems - síťově orientované systémy prevence narušení

PAN Personal Area Network – osobní síť

PCA Principal Component Analysis - analýza hlavních částí

PGP Pretty Good Privacy – dost dobré soukromí

PIN Personal identification number – osobní identifikační číslo

PZTS Poplachové zabezpečovací a tísňové systémy

RAID Redudant Array of Independent Disks - vícenásobné pole nezávislých disků

RC Rivest's cipher – Rivestova šifra

SHA Secure Hash Algorithm - bezpečnostní hešovací algoritmus

TB Terabyte

TKIP Temporal Key Integrity Protocol

WAN Wide Area Network – rozlehlá síť

WEP Wired Equivalent Privacy – soukromý ekvivalentní drátovým sítím

Wi-Fi Wireless Fidelity - komunikační standard pro bezdrátový přenos dat

WLAN Wireless Personal Area Network – bezdrátová místní síť

WPA Wi-Fi Protected Access – chráněný přístup k Wi-FI

WPAN Wireless Personal Area Network – bezdrátová osobní síť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK