IMPROVET

Zabezpečení informací a sítí

Miguel Soriano

Autor: Miguel Soriano
Název díla: Zabezpečení informací a sítí
Přeložil: Tomáš Vaněk
Vydalo: České vysoké učení technické v Praze
Zpracoval(a): Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 2 2435 2084
Tisk: (pouze elektronicky)
Počet stran: 82
Vydání: 1.

ISBN 978-80-01-05296-9

Recenzent: Jiří Stibor

Innovative Methodology for Promising VET Areas
http://improvet.cvut.cz

Program celoživotního učení

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
+	Výhody
–	Nevýhody

ANOTACE

Účelem tohoto kurzu je poskytnout studentům důležité základní znalosti z oblasti informační a síťové bezpečnosti.

CÍLE

V tomto kurzu jsou prezentovány základy informační a síťové bezpečnosti, tj. jak lze informační a síťovou bezpečnost zajistit, jak chránit osobní počítač a jak zmírnit bezpečnostní hrozby různých typů. Kurz rovněž obsahuje stručný přehled kryptografických metod a algoritmů využívajících veřejných a tajných klíčů. Dále zde studenti naleznou základní informace týkající se síťové bezpečnosti – konkrétně bezpečnostních protokolů, firewallů, systémů pro odhalování průniku, jakož i standardních řešení pro zajištění bezpečnosti bezdrátových sítí.

LITERATURA

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security Fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Sikorski, Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press, February 2012

[6] Michael Goodrich, Roberto Tamassia: Introduction to Computer Security, 2010

[7] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[8] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Obsah

1 Úvod

1.1 Úvod

Informační bezpečnost se nezabývá jen tím, jak zastavit šíření virů, jak se bránit hackerům nebo jak potírat spam v emailech. K informační bezpečnosti patří také práce se zaměstnanci i s pracovníky managementu, abychom získali jistotu, že jsou si všichni vědomi současných hrozeb, jakož i způsobů, jak mohou chránit své informace a systémy. Pojmy informační bezpečnost, počítačová bezpečnost a síťová bezpečnost se často používají jako synonyma. Mezi těmito oblastmi existují mnohé vazby a jejich cíle jsou společné, tj. ochrana důvěrnosti, integrity (celistvosti) a dostupnosti informací; přesto jsou však mezi nimi drobné odlišnosti.

Informační bezpečnost znamená ochranu informací a informačních systémů před neoprávněným přístupem, využíváním, vyzrazením, narušením, pozměňováním, prohlížením, sledováním, zaznamenáváním či zničením.

Jako počítačová bezpečnost se společně označuje celá škála nástrojů určených k ochraně zpracovávaných a ukládaných dat a k boji proti záměrům hackerů.

Síťová bezpečnost je taktéž společné označení pro množinu nástrojů určených k ochraně dat během jejich přenosu.

V souvislosti s Internetem se často používá termín internetová bezpečnost. Toto označení navíc zahrnuje i pojem zabezpečení perimetru (tzn. hranic střežené oblasti), což je opět společný název pro množinu nástrojů určených k ochraně zdrojů v privátní síti před uživateli z jiných sítí.

Rozdíly mezi informační bezpečností, počítačovou bezpečností a síťovou bezpečností spočívají především v přístupu, v použitých metodách a v oblastech, na něž se soustředíme. Informační bezpečnost se zabývá důvěrností, integritou a dostupností dat, bez ohledu na jejich formu: elektronickou, tištěnou, či jinou. Počítačová bezpečnost se může zaměřovat na zajištění dostupnosti a správné funkce počítačového systému, bez ohledu na informace v něm uložené nebo jím zpracované. Síťová bezpečnost se týká ochrany dat během jejich přenosu.

1.2 Příčiny nedostatečné bezpečnosti

Nedostatečná bezpečnost počítačových systémů a sítí sahá mnohem dále než jen k dobře známým počítačovým virům, a v současnosti je považována za prioritu. Ve světě propojeném sítěmi již nová generace vandalů a zlodějů dat nepotřebuje mít fyzický kontakt s obětí. Data lze snadno kopírovat, přenášet, pozměnit nebo zničit. V důsledku toho pak bývá místo činu velmi nepřehledné: nejsou zde žádné stopy, identifikace pachatelů je téměř nemožná, a jejich dopadení tím spíše; právní rámec navíc neobsahuje vhodná ustanovení, která by tento typ trestné činnosti dostatečně postihovala.

Jelikož na Internetu se vše odehrává v reálném čase, získává tento typ trestné činnosti novou kvalitu: je dílem okamžiku.

Ačkoli mají bezpečnostní problémy mnoho příčin, můžeme vyjmenovat alespoň tři kategorie slabých míst, která těmto problémům otevírají vrátka:

- slabá místa technologie,
- slabá místa v pravidlech,
- slabá místa v konfiguraci.

Samozřejmě bychom mohli k tomuto výčtu přidat i lidské slabosti a některé další, ale naším cílem je soustředit se na takové typy problémů, které můžeme nejen rozpoznat, ale také řešit, sledovat a přijmout k nim nezbytná opatření v rámci dané bezpečnostní strategie.

Slabá místa technologie

Každá technologie má svá slabá či zranitelná místa, ať už známá, nebo neznámá, která může dostatečně motivovaný útočník zneužít. Některá z nich se dostávají do obecného povědomí i díky médiím, zvláště jedná-li se o dobře známý software či zařízení. Avšak neklamme se – jiné produkty ještě nemusejí být bezpečné jen proto, že jsme o jejich nedostatcích dosud neslyšeli, a ani nezájem hackerů nemusí automaticky svědčit o tom, že daný produkt je bezpečný.

Uveďme si několik příkladů slabých míst:

- Internetové protokoly nebyly navrženy s ohledem na bezpečnost. V dnešní době se ke snížení rizik vyplývajících z povahy síťového prostředí využívá osvědčených postupů a zabezpečovacích služeb v kombinaci s produkty celé řady výrobců.
- Počítač a síťové operační systémy. Nezáleží na výrobci ani na tom, zda se jedná o systém založený na otevřených standardech, nebo proprietární – každý *operační systém (OS)* má určitá zranitelná místa, která je nutno ošetřit pomocí oprav (tzv. záplat), aktualizací a doporučených postupů.

- Slabá místa síťových prvků. Síťové prvky či zařízení mohou mít zranitelná místa, která obvykle označujeme jako bezpečnostní díry. Proto je důležité, aby byly opravy a aktualizace operačního systému (např. **IOS** – *Internetworking Operating System* – operační systém síťových prvků firmy Cisco) instalovány a doporučené postupy aplikovány vždy, jakmile jsou k dispozici; známé problémy tak mohou být odstraněny, případně lze alespoň zmírnit jejich dopady.

Slabá místa v pravidlech

Jako slabá místa v pravidlech souhrnně označujeme opatření přijatá firmou (nebo nedostatečnost opatření) vedoucí bezděčně, avšak nevyhnutelně k ohrožení bezpečnosti síťového systému. Z následujících příkladů je zřejmé, jak mohou určité nedokonalosti v pravidlech nepříznivě ovlivnit vlastnosti podnikového počítačového systému:

- Neexistují psaná bezpečnostní pravidla. Neexistuje-li náležitě zpracovaný a řádně schválený plán, znamená to, že bezpečnostní zásady se teprve vyvíjejí a jsou v praxi naplňovány (pokud vůbec) nanejvýš formou „nejlepší snahy“ („best-effort“).

- Neexistuje plán obnovy po havárii. Není-li stanoven plán obnovy, musí se do boje proti síťovému útoku (případně živelné pohromě, jakou je například požár, povodeň nebo zemětřesení) zapojit ti zaměstnanci, kteří jsou právě nablízku, se svými znalostmi a zkušenostmi. I nejlépe vyškolení pracovnicí s bohatými zkušenostmi však mohou učinit chybná rozhodnutí, ocitnou-li se tváří v tvář nenadálé krizové situaci.

- Neexistují pravidla pro přidávání a změny softwaru a hardwaru. Ať už je cílem zvýšení produktivity, nebo jen zábava – každé přidání či změna softwaru nebo hardwaru může mít za následek nečekaná bezpečnostní rizika. Přidání neschváleného bezdrátového přístupového bodu do sítě může rázem otevřít ne vrátka, ale přímo vrata do podnikové sítě a k jejím zdrojům. Neznámý spořič obrazovky může zase pro útočníka potají shromažďovat hesla, uživatelská jména a další informace.

- Neprovádí se bezpečnostní kontrola**.** I když je síť vybudována jako bezpečná, může vést nedostatečná kontrola záznamů a procesů ke vzniku a rozvoji bezpečnostních slabin a neoprávněného využívání zdrojů. Nejhorším případem je, když ani závažné ztráty nejsou vůbec rozpoznány a může k nim docházet i nadále.

- Zaměstnanecká politika**.** Velká míra fluktuace, nižší ohodnocení a nedostatek vzdělávacích příležitostí se mohou projevit na bezpečnosti sítě tak, že se noví, nedostatečně prověření a nezkušení zaměstnanci dostávají do funkcí, k nimž patří rozhodovací pravomoci a odpovědnost.

- Vnitřní politika**.** Laxní přístupy a postupy často přispívají ke vzniku pokušení, jakož i poměrně bezpečného prostředí pro ty, kdo hledají jen svůj vlastní prospěch. Hovoříme o syndromu „jsme tu všichni jako rodina“. Bohužel, i některé z nejlepších rodin mají ve svém středu zloděje. Podobně i rivalita,

pomlouvání, boje o moc nebo zápasy v bahně mohou zapříčinit bezpečnostní rizika, případně odvést pozornost, takže skutečné problémy zůstanou neodhaleny.

Slabá místa v konfiguraci

Mnohá síťová zařízení mají výchozí nastavení, které jsou volena s ohledem na maximální výkonnost nebo snadnou instalaci, avšak bez ohledu na bezpečnostní rizika. Není-li při jejich instalaci věnována náležitá pozornost úpravě těchto nastavení, mohou následně nastat vážné problémy. Mezi běžné chyby konfigurace patří například:

- neefektivní seznamy přístupových pravidel, které nedokáží blokovat určený provoz,
- výchozí, zcela chybějící nebo stará hesla,
- nepotřebné porty nebo služby, které jsou ponechány aktivní,
- uživatelská jména a hesla zasílaná jako otevřený text,
- nedostatečně chráněný vzdálený přístup prostřednictvím Internetu nebo telekomunikačních sítí.

Sledování zpráv a doporučení zveřejňovaných výrobcem nám spolu s průmyslovým zpravodajským servisem může pomoci odhalit nejčastější a nejznámější slabá místa, a obvykle se takto dozvíme i o vhodných způsobech jejich nápravy.

1.3 Klasifikace útoků

Bezpečnostní útoky můžeme popsat jako různé druhy systematických činností zacílených na snížení nebo narušení bezpečnosti. Z tohoto hlediska je možno útok definovat jako systematickou hrozbu způsobenou nějakou entitou, a to uměle, úmyslně a inteligentně.

Počítačové sítě jsou zranitelné a mohou být vystaveny mnoha typům hrozeb spojených s mnoha typy útoků, jakými jsou například:

- Sociální inženýrství – snaha získat společenskými kontakty přístup k systému (např. předstíráním, že daná osoba je oprávněným uživatelem či správcem systému, úmyslné klamání lidí s cílem vyzvědět utajované informace atp.).
- Zlomyslná volání – využití počítačového softwaru a modemu k vyhledávání počítačů připojených k telefonní síti, jejichž modem automaticky přijímá příchozí volání, čímž potenciálně otevírá přístup do podnikové sítě.
- Útoky typu odmítnutí služby – všechny typy útoků, jejichž cílem je zahltit počítač nebo síť takovým způsobem, aby je oprávnění uživatelé nemohli použít.
- Útoky založené na protokolech – využívají známá (i neznámá) slabá místa síťových služeb.
- Útoky na hostitelské počítače – zaměřují se na zranitelná místa konkrétních operačních systémů, případně na způsob, jakým je systém nakonfigurován a spravován.
- Odhadování hesel – jako heslo označujeme posloupnost znaků (obvykle svázanou s uživatelským jménem), která slouží k identifikaci a autentizaci konkrétního uživatele. Prakticky na všech počítačích si uživatelé volí hesla sami. Odpovědnost za bezpečnost tedy leží na koncových uživatelích, kteří často zásady bezpečného chování buď neznají, nebo na ně nedbají. Obecným pravidlem je, že hesla, která jsou snadno zapamatovatelná, lze snadno uhodnout. Útočníci mají několik způsobů, jak při odhadování hesel postupovat a tuto překážku překonat.
- Odposlouchávání všeho druhu, včetně kradení e-mailových zpráv, souborů, hesel a dalších informací přenášených po síti.

Bezpečnostní útoky můžeme rozdělit do dvou hlavních kategorií:

- pasivní útoky,
- aktivní útoky.

1.4 Pasivní útoky

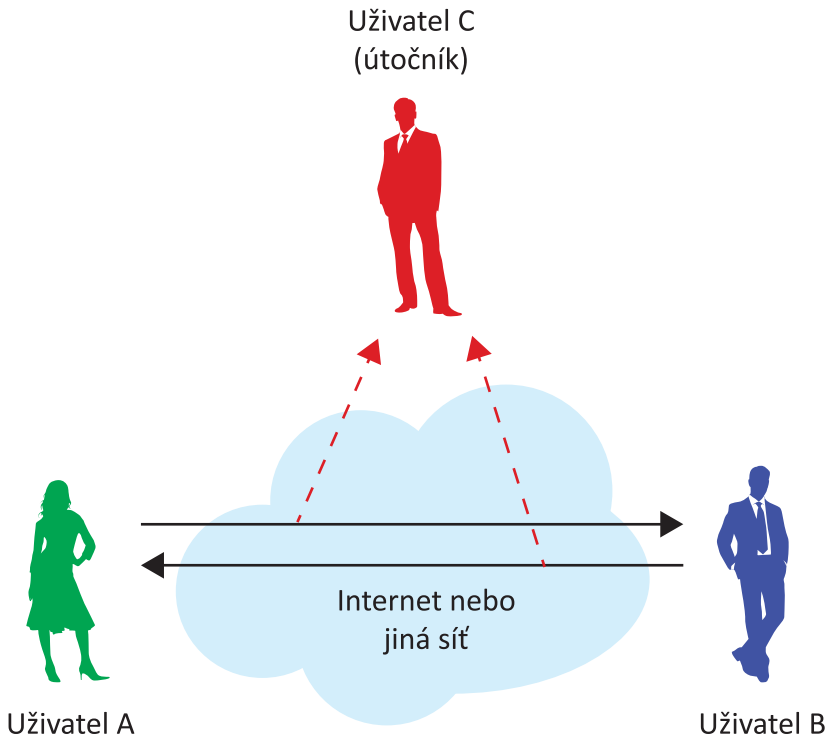
Cílem pasivních útoků je získat nebo využít informace ze systému, nemají však vliv na systémové prostředky. Při pasivním útoku útočník pouze monitoruje komunikační kanál a ohrožuje důvěrnost dat. Povaha pasivních útoků tedy spočívá v odposlouchávání či monitorování přenosu s cílem získat přenášené informace.

Rozeznáváme dva typy pasivních útoků, které jsou zaměřeny jednak na obsah zpráv, jednak na analýzu provozu:

- Odposlouchávání**.** Většina síťové komunikace probíhá v nezabezpečeném formátu, tedy v podobě otevřeného (nešifrovaného) textu; to umožňuje útočníkovi, který získal přímý přístup k přenosové cestě v síti, aby „naslouchal“, čili interpretoval (četl) přenášená data. Možnost odposlechu síťového provozu je, obecně vzato, největší bezpečnostní problém, se kterým se setkávají správci podnikových sítí. Nejsou-li použity silné šifrovací služby založené na bezpečných kryptografických principech, mohou ostatní uživatelé zcela volně číst data přenášená v síti.

- Analýza provozu. V tomto případě jde o zachycování a zkoumání přenášených zpráv s cílem odvodit určité informace z typického průběhu komunikace. To je možno provádět i v případě, kdy jsou zprávy šifrovány a nelze je dešifrovat. Obecně platí, že čím větší je počet zpráv, které jsou takto sledovány, nebo dokonce zachyceny a uloženy, tím více poznatků můžeme ze síťového provozu vyvodit.

Obrázek 1 ukazuje model pasivního útoku.



Obr. 1 – Model pasivního útoku

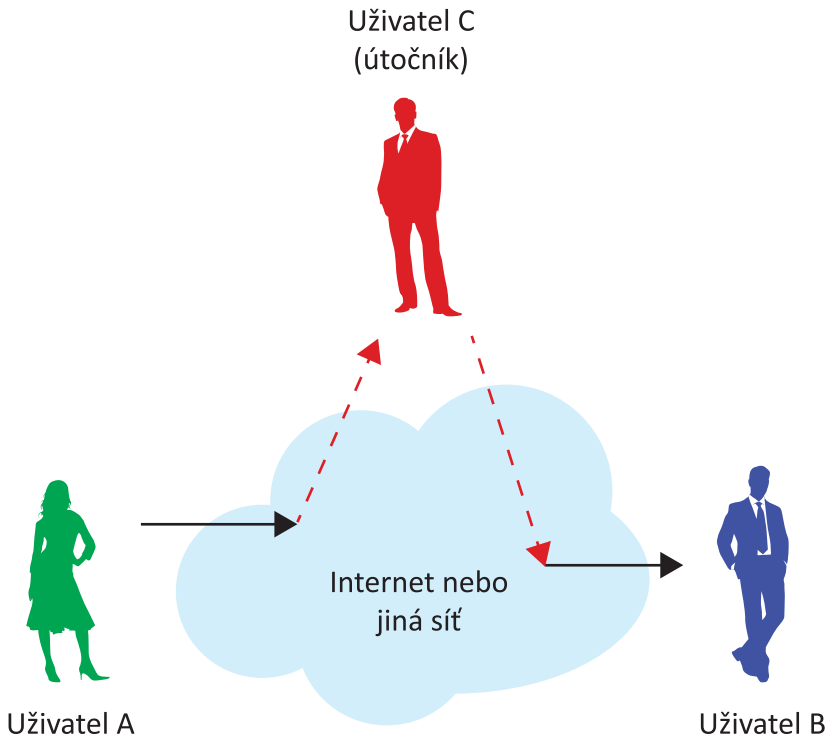
1.5 Aktivní útoky

Aktivní útoky se pokoušejí měnit systémové prostředky nebo ovlivnit jejich funkčnost. Při tomto typu útoku se útočník snaží data přenášená příslušným kanálem odstranit, přidat nebo jinak měnit. Aktivní útočník ohrožuje integritu dat, jakož i autentizaci a důvěrnost.

Součástí aktivních útoků je nějaká změna datového toku nebo vytvoření toku falešného. Tyto útoky můžeme rozdělit do následujících šesti kategorií:

- **Maškaráda.** Jedná se o typ útoku, kdy útočník předstírá, že je oprávněným uživatelem, a jeho cílem je získat přístup k systému, případně větší uživatelská práva, než jaká mu náležejí.
- **Přehrání zprávy.** Při tomto druhu útoku je původní zpráva zlomyslně (podvodně) opakována nebo zpožděna. To provede buď odesílatel, nebo útočník, který data zachytí a znovu odvysílá, například v rámci útoku typu maškaráda.
- **Pozměnění zprávy**. Útočník odstraní zprávu ze síťového toku, pozmění ji a znovu ji do sítě vyšle.
- *Člověk uprostřed* (**MitM –** *Man in the Middle*). Útočník odposlouchává komunikaci mezi dvěma stranami – obvykle mezi koncovým uživatelem a webovým erverem. Útočník může takto získané informace zneužít ke zcizení identity nebo k jiným podvodům.
- *Odepření služby* (**DoS –** *Denial of Service*) a *Distribuované odepření služby* (**DDoS –** *Distributed DoS*). Útok typu odepření služby (DoS) je incident, při němž uživatel nebo organizace přijde o služby poskytované určitým zdrojem, které by za normálních okolností měly být k dispozici. V případě distribuovaného odepření služby využívá útočník velké množství napadených počítačů (tzv. botnet) k zahlcení cílového systému.
- *Trvalá významná hrozba* (**APT –** *Advanced Permanent Threat*). Jedná se o útok, při němž neoprávněná osoba získá přístup k síti a zůstane po dlouhou dobu neodhalena. Cílem útoku APT je obvykle krádež dat, nikoli přímé poškození sítě nebo jejího vlastníka. APT útoky se zaměřují na organizace působící v odvětvích, kde se pracuje s cennými informacemi (jako je např. armáda, průmysl či finančnictví).

Obrázek 2 ukazuje příklad aktivního útoku (konkrétně útok s pozměněním zprávy).



Obr. 2 – Aktivní útok s pozměněním zprávy

1.6 Útočníci, jejich cíle a chování

Útočník či narušitel je osoba, která získá, případně se snaží získat větší než přidělená práva nebo neoprávněný přístup k informačnímu systému.

Útočníky můžeme řadit do různých kategorií podle mnoha hledisek. Základní kritéria používaná pro tuto klasifikaci jsou následující:

- umístění útočníka vzhledem k napadenému systému,
- úroveň útoku,
- cíle útoku (proč je útok prováděn).

Z hlediska umístění rozlišujeme dva typy útočníků:

- vnitřní útočník – insider,
- vnější útočník – outsider.

Insider je obecně osoba, která má přístup k vnitřní počítačové síti; je tedy oprávněným uživatelem, avšak pokouší se získat neoprávněný přístup k datům, systémovým prostředkům a službám, případně zneužívá data, která jsou mu v rámci běžných oprávnění přístupná.

Outsider je obecně osoba, která nemá oprávnění k přístupu do vnitřní počítačové sítě, chce do ní však proniknout; k tomu využívá zranitelná místa nebo bezpečnostní díry.

Podle kvalitativní úrovně útoku dělíme útočníky rovněž do dvou hlavních skupin:

- amatéři.
- profesionálové.

Amatéři provádějí méně nebezpečné útoky než profesionálové, neboť mívají nižší kvalifikaci a horší vybavení.

Profesionálové jsou obvykle špičkoví počítačoví odborníci, kteří mají přístup ke specializovaným zdrojům, jsou vysoce kvalifikovaní a mají velké zkušenosti. V praxi to znamená, že jsou schopni vést velmi nebezpečné útoky s vážnými následky pro počítačové systémy a sítě.

Pokud jde o klasifikaci útočníků, je značně diskutovaným tématem jejich rozdělení do následujících dvou skupin:

- hackeři,
- crackeři.

Hacker má dobré až vynikající dovednosti v oblasti IT, často se podílí na významných softwarových projektech a jeho znalosti a know-how jsou užitečné při vyhledávání zranitelných míst a bezpečnostních děr ve vyvíjeném systému. Jeho činnost je tedy prospěšná a užitečná. Existují dokonce i kodexy (psaná pravidla) pro chování hackerů.

Cracker umí překonat protipirátské ochrany počítačových programů a využívá své znalosti neetickým způsobem. Existuje však více definic této skupiny útočníků, které zdůrazňují odlišné oblasti jejich činnosti.

Existují i jiné skupiny útočníků. Největší z nich jsou tzv. **scriptkiddies** (doslova „děti se skripty“). Jedná se o uživatele s nízkou úrovní dovedností v oblasti IT. Ke svým útokům využívají skripty (jednoduché programy) obsahující kódy zaměřené na zneužívání zranitelných míst informačních systémů. Tyto skripty používají, aniž by znali hlubší podstatu jejich fungování; dopady jejich činnosti jsou však obvykle závažné. Jedná se o nejčastější a nejnebezpečnější typ útoků.

1.7 Jak se lze chránit?

V této kapitole jsou uvedena některá doporučení pro domácí uživatele.

Používejte silná hesla

Heslo je mnohdy jedinou ochranou daného systému. Uživatelské jméno samo o sobě nemůže sloužit k ověření totožnosti, avšak heslo ve spojení s uživatelským jménem jako identifikátor funguje. Hesla jsou tedy klíčem k vaší síti, a proto byste je měli co nejlépe chránit. Firewally a systémy detekce průniku jsou k ničemu, pokud dojde k vyzrazení vašich hesel.

Silné heslo je takové, které nelze nalézt v žádném slovníku – českém, anglickém ani jiném, tedy, heslo, které není snadné uhodnout. Je samozřejmě těžší odhadnout nebo prolomit delší hesla nežli krátká.

Následuje seznam pravidel pro nastavení silného hesla:

- **Použijte nesmyslnou kombinaci písmen:** Nejlepší hesla jsou zcela nesmyslná (taková, která nemají žádný věcný význam). Vezmeme-li například větu „Neočekávejte ode mne dokonalé chování a zářivý úsměv“ a použijeme-li jen první znak každého slova, dostaneme heslo *nomdcazu*.

- **Smíchejte velká a malá písmena:** Heslo by mělo obsahovat velké písmeno někde jinde než na začátku, a mělo by se v něm vyskytovat také číslo.

- **Delší hesla jsou lepší:** Délka hesla by měla být alespoň 8 znaků.

- **Hesla byste měli pravidelně měnit:** Dokonce i ta nejlepší hesla by měla být pravidelně měněna (řekněme po 60 dnech), neboť při dlouhodobém používání se zvyšuje riziko prolomení. Řada operačních systémů umožňuje nastavit toto pravidlo pro všechny uživatele. Uživatelům se to nejspíš bude zdát nepohodlné, ale jde o zajištění bezpečnosti.

- **Vymýšlejte nová hesla namísto opakovaného užívání starých:** Uživatel by neměl znovu použít stejné heslo po dobu alespoň jednoho roku, nebo dokonce 18 měsíců.

- **Nepoužívejte jako heslo posloupnost písmen, která jsou na klávesnici za sebou:** Je třeba vyhýbat se používání takových hesel, jako je QWERTY, 12345678, nebo asdfghj. I když vypadají nesmyslně, jsou tvořena podle jasného vzoru po sobě jdoucích znaků na klávesnici počítače, a pro crackera není problém prolomit je za několik sekund.

- **Zacházejte s hesly jako s přísně tajnou informací:** Všechna hesla by měla být chráněna, nikoli sdělována druhým! Řada uživatelů si píše hesla na poznámkové lístečky nalepené na počítač nebo si je dává pod klávesnici. Tím ale nikoho neošálí!

Superuživatelská a administrátorská hesla jsou pro útočníka jako klíče od království. Správci systému s právy superuživatele (root) – tedy bez jakýchkoli

omezení přístupu a s možností provádět jakékoli změny – by proto měli mít ta nejsložitější hesla a nejpřísnější pravidla pro jejich změny a opětovné použití. Doporučuje se dodržování následujících pokynů:

- Zapište si všechna administrátorská hesla a zamkněte je do trezoru: I když se pak stane, že správce je nějakou dobu například v pracovní neschopnosti nebo náhle opustí zaměstnání, není heslo nenávratně ztraceno. Existují sice programy pro obnovu hesel, ale není dobré spoléhat na ně v tísni.

- Změňte VŠECHNA uživatelská hesla, jestliže existuje podezření na vyzrazení hesla administrátorského**:** Nelze zaručit, že nebyla zcizena všechna hesla, pokud se neznámá osoba zmocnila hesla superuživatele nebo administrátora.

Obdobně, pokud má řadový uživatel podezření, že heslo bylo zcizeno nebo vyzrazeno, měl by své heslo okamžitě změnit a oznámit událost tomu, kdo ve firmě odpovídá za bezpečnost.

Vždy používejte antivirový program

Antivirový software nemusí být sice stoprocentně účinný, ale je to lepší než zůstat zcela bez ochrany. Přítomnost nejběžnějších virů není nijak nápadná, takže pokud uživatel nemá žádný antivirový program, pravděpodobně ani netuší, že jeho počítač je napaden.

Antivirový software se skládá ze dvou částí: *skenovacího programu* a *souboru signatur*. Je třeba pravidelně aktualizovat obě tyto části, jinak antivirový program přestane být účinnou ochranou. Program má obvykle volbu pro aktualizaci, případně lze dostupnost aktualizací kontrolovat na webových stránkách výrobce.

Skenovací program řídí antivirovou kontrolu počítače, zatímco soubor signatur je vlastně databáze známých virů a popisu jejich chování. Skenovací program porovnává soubory na vašem počítači se známými viry v souboru signatur. Antivirový software občas spustí falešný poplach, ale to je jen malá daň za poskytovanou ochranu.

Když se objeví nové viry, výrobci antivirového softwaru vydávají aktualizace souborů signatur, které obsahují nový kmen. Občas je třeba aktualizovat i samotný skenovací program. Je-li jedna část softwaru aktualizovaná a druhá zastaralá, nebude celek fungovat správně.

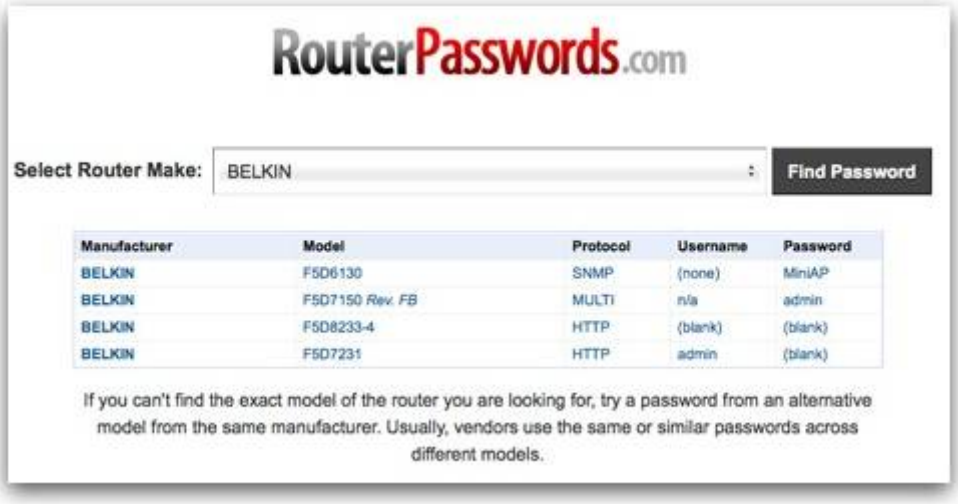
Aby byl zajištěn nejvyšší stupeň ochrany, je třeba instalovat antivirový software jak na jednotlivých pracovních stanicích, tak na všech serverech a ostatních počítačích v síti. To je jediný způsob, jak lze detekovat viry ve všech vstupních bodech. Veškerá vyměnitelná média, jako jsou USB disky, CD atd., mají být před použitím v daném systému prověřena. Je-li antivirový software nainstalován na serverech fungujících jako brány k Internetu, může zachytit viry (infiltrace) přicházející z vnějších připojení.

Vždy změňte výchozí nastavení

Základní instalace systému s ponecháním výchozích nastavení je pravděpodobně jedna z nejčastějších chyb, kterých se lidé dopouštějí při oživování sítí. Ve výchozí konfiguraci obvykle existuje výchozí administrátorský účet s výchozím přístupovým heslem, a hackeři na celém světě tyto údaje znají. To platí pro směrovače, rozbočovače, přepínače, operační systémy, systémy elektronické pošty, jakož i další serverové aplikace, například databáze a webové servery.

Kromě toho, že výchozí konfigurace počítačových systémů obsahují známá hesla, je v nich také mnoho bezpečnostních děr, které je nutno ošetřit. Dříve než je jakýkoli počítač připojen k síti, je třeba změnit výchozí jména účtů i hesla a instalovat všechny bezpečnostní aktualizace. Trocha času, kterou v této chvíli věnujeme úpravám systému, nám může ušetřit spoustu pozdějších starostí.

Obrázek 3 ukazuje příklad hesel, která bývají nastavena jako výchozí na některých směrovačích.



Obr. 3 – Příklad výchozích hesel směrovače

Používejte firewall

Důrazně se doporučuje používat nějaký typ firewallu. Narušitelé vytrvale slídí po domácích systémech, zda se v nich nevyskytují známá zranitelná místa. Síťové firewally (ať už softwarové, nebo hardwarové) poskytují určitou míru ochrany před těmito útoky. Žádný firewall však nemůže odhalit nebo zastavit všechny útoky, takže nestačí jen nainstalovat firewall a ignorovat všechna ostatní bezpečnostní opatření.

Neotevírejte neznámé přílohy e-mailů

Před otevřením jakékoliv přílohy e-mailu j třeba se ujistit, zda známe zdroj těchto dat. Nestačí však, že pošta přichází z důvěryhodné adresy. Virus Melissa se šíří

právě proto, že je odeslán z adresy dobře známé. Škodlivý kód může být rozesílán v zábavných nebo lákavých programech.

Při otevírání přiložených souborů je důležité dodržovat následující postup:

1. ujistěte se, že instalovaná virová databáze je aktuální,
2. uložte soubor na lokální disk,
3. prověřte soubor antivirovým programem,
4. soubor otevřete.

Dodatečným bezpečnostním opatřením může být, že před otevřením souboru odpojíte počítač od sítě.

Respektování těchto doporučení sníží, avšak ne zcela odstraní riziko, že škodlivý kód obsažený v příloze se bude moci šířit z vašeho počítače do jiných počítačů.

Nespouštějte programy neznámého původu

Nikdy nespouštějte žádný program, pokud s jistotou nevíte, že pochází od osoby nebo společností, které důvěřujete. Programy neznámého původu také neposílejte přátelům ani spolupracovníkům jen proto, že jsou zábavné – mohou totiž obsahovat trojské koně.

Bez prodlení aktualizujte všechny aplikace i operační systém

Výrobci softwaru obvykle vydávají opravy, jakmile je objeveno zranitelné místo. Dokumentace k většině programů obsahuje návod, jak aktualizace a opravy získat.

Některé aplikace automaticky kontrolují dostupné aktualizace; v ostatních případech je naprosto nezbytné dostupnost aktualizací pravidelně kontrolovat.

Když počítač nepoužíváte, vypněte jej nebo odpojte od sítě

Když počítač nepoužíváte, vypněte jej nebo odpojte kabel od síťového rozhraní. Útočník nemůže váš počítač napadnout, pokud je vypnutý nebo zcela odpojený od sítě.

Pravidelně zálohujte důležitá data a vytvořte si spouštěcí disk

Uchovávejte kopie důležitých souborů na výměnných médiích. Používejte dostupné nástroje pro zálohování a ukládejte disky se zálohou na jiné místo, než kde je počítač. Kromě toho je více než vhodné vytvořit si spouštěcí disk (CD), který vám usnadní obnovu konfigurace počítače po narušení bezpečnosti nebo selhání pevného disku. Tento disk je samozřejmě nutno vytvořit dříve, než k podobné události dojde.

1.8 Shrnutí

V této kapitole jsme se nejprve seznámili s několika důležitými pojmy, jimiž jsou informační bezpečnost, počítačová bezpečnost a síťová bezpečnost, a uvedli jsme si, jaké jsou mezi nimi rozdíly. Poté jsme si uvedli některé příčiny nedostatečného zabezpečení informací a roztřídili si typy bezpečnostních útoků a útočníků podle různých hledisek. Nakonec jsme probrali oddíl shrnující doporučení, jak mohou domácí uživatelé zlepšit ochranu svých systémů.

2 Škodlivý software a antivirové programy

2.1 Pojem škodlivého softwaru (malwaru)

Škodlivý software (malware) je obecný termín označující jakýkoliv zlomyslný nebo obtěžující software, který je navržen tak, aby počítač zneužíval prováděním nechtěných činností bez vědomí či souhlasu uživatele.

Spuštění malwaru může způsobit narušení činnosti počítače; může být také využito ke shromažďování citlivých informací nebo k získání neoprávněného přístupu k počítačovým systémům. Malware není totéž co vadný software (tedy software, který má legitimní účel, ale obsahuje potenciálně škodlivé chyby, které nebyly odhaleny před zahájením jeho distribuce).

Počítačové viry jsou vlastně podmnožinou v rámci širší rodiny malwaru, stejně jako ostatní druhy, jako například červi, trojské koně, adware, spyware, rootkity atd.

V současnosti se většina malwaru šíří prostřednictvím Internetu. Jeden z nejběžnějších způsobů je znám jako „drive-by download“ (což bychom mohli přeložit jako stažení mimoděk) – dojde ke stažení a spuštění škodlivého souboru například prostřednictvím webového prohlížeče nebo otevřením přílohy e-mailu (dejme tomu škodlivého souboru PDF). Uživatelé jsou často podvedeni a věří, že určitý program nebo datový soubor jim může být užitečný (například software pro přehrávání videa). Jindy je zase infekce před uživatelem skryta – stačí jen navštívit webovou stránku, která zneužívá zranitelné místo ve webovém prohlížeči ke stažení a spuštění malwaru. K distribuci malwaru však může být využit téměř každý internetový protokol, včetně P2P (Peer-to-peer) nebo instant messagingu (chat). Dále je třeba mít na paměti, že fyzická zařízení pro ukládání dat mohou rovněž sloužit k šíření malwaru (velmi častým případem je jeho distribuce prostřednictvím USB flash disků).

2.2 Antivirový software

Antivirus neboli antivirový software se používá k prevenci, detekci a odstranění škodlivého softwaru, včetně (nikoli však pouze) počítačových virů, červů, trojských koní, spywaru a adwaru. Aby byl účinným nástrojem, měl by být pravidelně aktualizován – jinak nemůže zajistit ochranu proti novým virům.

Odstranění viru je termín používaný pro vyčištění počítače. Existuje několik metod, kterými se provádí:

- odstranění kódu, který odpovídá viru, z infikovaného souboru,
- odstranění (smazání) infikovaného souboru;
- uložení infikovaného souboru do karantény, což znamená jeho přesunutí do umístění, odkud nemůže být spuštěn.

Obvykle se využívá celá řada různých strategií.

Detekce podle signatury zahrnuje vyhledávání známých vzorů v programovém kódu. Viry se reprodukují infikováním „hostitelských aplikací“, což znamená, že kopírují část spustitelného kódu do napadeného programu. Aby byla zajištěna jejich plánovaná funkce, jsou viry naprogramovány tak, aby neinfikovaly tentýž soubor vícekrát. Proto přidávají do infikované aplikace informaci (několik byte), aby si mohly zkontrolovat, zda již byla napadena – tuto informaci označujeme jako signaturu viru. Antivirové programy využívají k detekci virů právě tento podpis, který je pro každý virus jiný. Tato metoda se nazývá detekce podle signatury, a jde o nejstarší metodu používanou antivirovými programy; neumožňuje však detekovat viry, které výrobce antivirového softwaru dosud nemá ve svém archivu. Programátoři navíc často dávají virům maskovací schopnosti, což detekci signatury ztěžuje, či dokonce znemožňuje. Určitou pomoc v boji proti těmto hrozbám nabízejí heuristické postupy.

Jeden z heuristických postupů, metoda generické signatury, umožňuje identifikovat nové viry nebo varianty stávajících virů tak, že vyhledává v souborech známé nebo mírně modifikované části škodlivého kódu. Heuristická metoda zahrnuje analýzu chování aplikací za účelem zjištění podobného chování, jaké má známý virus. Tento typ antivirových programů tedy umožňuje detekovat viry i v případě, že virová databáze není aktuální; na druhé straně jsou však náchylné k falešným poplachům.

Ať už je antivirový program jakkoli užitečný, může mít i své nevýhody. Může snížit výkonnost počítače. Nezkušení uživatelé mohou mít také potíže s pochopením zobrazovaných hlášení a nabízených řešení; nesprávné rozhodnutí pak může vést k narušení bezpečnosti.

2.3 Rozdělení malwaru

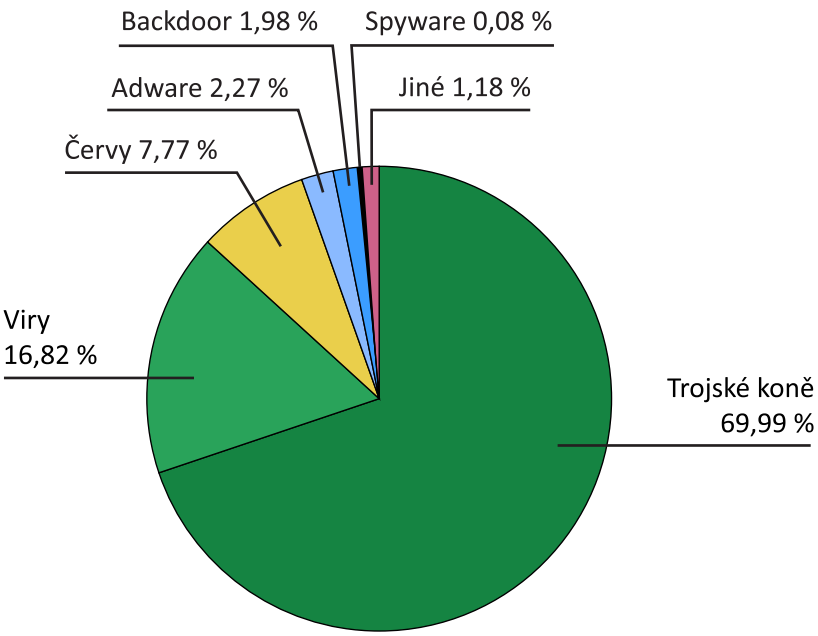
Malware můžeme třídit různými způsoby podle různých kritérií, kterými jsou například způsob šíření, metoda instalace do systému, způsob ovládání na dálku atd. V současné době mívají jednotlivé druhy malwaru mnoho funkcí, takže jsou obvykle klasifikovány podle funkce hlavní. Můžeme mít například, trojského koně s funkcemi rootkitu, takže může zůstat skrytý před zkušenými uživateli i bezpečnostními mechanismy. Může jít také o zaváděcí program v síti infikovaných počítačů, které jsou dálkově ovládány. Zároveň může zobrazovat reklamy a zaznamenávat stisky kláves, takže by patřil i do rodin adwaru a keyloggerů. Byl by to tedy trojský kůň-rootkit-bot-adware-keylogger ... Vše v jednom! V praxi jsou takové případy docela běžné.

První klasifikace malwaru je založena na nezbytnosti hostitelského souboru pro šíření.

Následující čtyři druhy škodlivého softwaru potřebují pro své šíření hostitelské soubory:

- zadní vrátka (backdoor),
- logické bomby,
- trojské koně,
- viry.

Obrázek 4 ukazuje rozdělení malwaru podle kategorií (zdroj: Panda Security)



Rozdělení malware do kategorií
16. března, 2011

zdroj: Panda Security

Obr. 4 – Druhy malwaru

Další dva typy škodlivého softwaru hostitelský soubor k šíření nepotřebují. Jsou to:

- červi,
- zombie.

Zadní vrátka jsou tajné vstupy do programu, které umožňují přístup k systému bez nutnosti projít bezpečnostními mechanismy. Tyto přístupy jsou používány programátory během ladění programu, kdy má programátor zvláštní oprávnění. Tyto padací dveře jsou vyhledávány škodlivým softwarem a mohou být použity pro obcházení bezpečnostních mechanismů. Důsledkem pak je závažná softwarová hrozba pro počítačový systém.

Logické bomby jsou nejstarší druh malwaru, který představuje softwarovou hrozbu. Jedná se o software, který je zakomponován do běžného programu a aktivuje se při splnění určitých podmínek. Jedním z příkladů těchto podmínek může být přítomnost nebo nepřítomnost určitého souboru v okamžiku, kdy nastane určený den, týden nebo datum. Logická bomba může způsobit ztrátu nebo poškození dat v informačním systému – tedy vymazat určité soubory, zastavit běžící výpočetní aplikace atd.

Trojské koně jsou programy nebo příkazy, které vykonávají užitečné postupy nebo procesy, ale zároveň provádějí škodlivé aktivity na pozadí – například mazání dat. Zvláštním případem tohoto druhu škodlivého softwaru je spyware, který shromažďuje hesla zadaná z klávesnice, informace o navštívených

webových stránkách, druh softwaru, který je používán na daném počítači, či informace zasílané přes Internet.

Viry jsou programy, které se připojují k jiným programům nebo souborům a mohou provádět nepovolené činnosti. Pro své šíření potřebují hostitelský soubor, který je virem pozměněn. Viry mohou napadnout další soubory, šířit se dále a poškodit informační systém.

Červ se může šířit z jednoho počítačového systému do druhého, pokud jsou tyto systémy propojeny sítí. Šíří se převážně s využitím e-mailových klientů nebo prostřednictvím služeb těmito klienty nabízených.

Zombie je škodlivý software, který se šíří prostřednictvím sítě. Po jeho úspěšném průniku do počítačového systému je možno infikovaný počítač dálkově ovládat a spravovat. Případ, kdy je několik počítačů infikováno stejným druhem škodlivého softwaru se schopností dálkového ovládání označujeme jako botnet. Botnet tak může být ovládán z jednoho vzdáleného počítače a dokáže využívat jednotlivé infikované počítače (zombie) k provádění stejných příkazů. To pak umožňuje realizovat útoky označované jako *Distribuované odepření služby (DDoS)*.

2.4 Životní cyklus virů

Životní cyklus virů má čtyři fáze, jimiž jsou

- latentní fáze (nečinnost),
- fáze šíření,
- fáze aktivace,
- fáze provedení (aktivita).

V **latentní fázi** zůstává virus neaktivní, tzn. neprovádí žádnou činnost. Je však třeba poznamenat, že ne všechny viry tuto fázi ve svém životním cyklu mají.

Ve **fázi šíření** umístí virus identickou kopii sebe sama do jiného programu nebo do určitých oblastí na disku. Každý infikovaný program obsahuje nyní klon viru, který se může samostatně šířit.

Ve **fázi aktivace** je virus aktivován. Tato fáze může být spuštěna na základě různých podmínek nebo stavů infikovaného programu.

Ve **fázi provedení** virus vykonává činnost, pro kterou byl naprogramován. Obvykle jde o činnosti destruktivní, které mohou způsobit ztrátu či poškození dat v infikovaném počítačovém systému.

2.5 Shrnutí

V této kapitole jsme si vysvětlili pojem škodlivého softwaru (malwaru) a roztřídili jsme si jej podle různých kritérií: způsobu šíření, způsobu instalace, charakteristických vlastností, atd. Dále jsme prozkoumali jednotlivé fáze tvořící životní cyklus virů. Kapitola také popisuje několik způsobů používaných pro čištění (léčení) infikovaných počítačů. Jelikož tyto metody vyžadují detekci malwaru, představili jsme si i některé strategie, které se pro detekci často využívají.

3 Bezpečnostní služby a mechanismy

3.1 Bezpečnostní služby

Bezpečnostní služba je taková služba, která zajišťuje odpovídající bezpečnost systémů nebo datových přenosů. Bezpečnostní služby jsou realizovány pomocí bezpečnostních mechanismů ve shodě s bezpečnostními zásadami.

Již od devadesátých let dvacátého století se za základní principy informační bezpečnosti považují *důvěrnost, integrita* a *dostupnost* (podle anglických názvů „confidentiality, integrity, availability“ označované společně jako „trojice **CIA**“).

Později byly k těmto třem základním atributům přidány další prvky informační bezpečnosti – **autentizace, řízení přístupu, neodmítnutí** a **soukromí**. Tato klasifikace je však stále předmětem debat mezi bezpečnostními experty.

3.2 Důvěrnost

Důvěrnost znamená ochranu informací před vyzrazením nepovolaným entitám (jimiž mohou být organizace, lidé, stroje či procesy). Nikdo kromě oprávněné entity (či entit) nesmí mít k určeným datům přístup. Informací rozumíme kromě obsahu dat i jejich velikost, existenci, charakteristické parametry komunikace atd.

Důvěrnost je vyžadována:

- jestliže jsou data uložena na médiu (např. pevném disku počítače), ke kterému může mít přístup neoprávněná osoba,
- jestliže jsou data zálohována na zařízení (například pásku), která mohou padnout do rukou neoprávněné osoby,
- jestliže jsou data přenášena nechráněnou sítí.

Vzhledem k vysoké úrovni a schopnostem dnešních útočníků je navíc nutno pro zajištění důvěrnosti všech citlivých dat použít **kryptografické techniky**. Stejně jako v případě zajištění integrity dat je třeba, aby se komunikující entity shodly na použití vhodných algoritmů a klíčů.

3.3 Integrita dat

Integritou dat rozumíme ochranu před vytvořením, změnou, smazáním, kopírováním nebo opakovaným získáním dat neoprávněným entitami (jimiž mohou být organizace, lidé, stroje či procesy). Porušení integrity je vždy způsobeno aktivními útoky. Integrita je svázána s důvěryhodností informačních zdrojů.

Integrita dat znamená ujištění o jejich neměnnosti – tedy že data (přenášená nebo uložená) nebyla nezjistitelným způsobem změněna, ať už omylem, nebo záměrně. Je zřejmé, že takové ujištění je nezbytné pro podniková prostředí nebo elektronický obchod všeho druhu; i v mnoha jiných oblastech je však přinejmenším žádoucí.

Integrita informačního systému má zajistit pouze uchování informace beze změny, tedy tak, jak byla do systému přenesena či vložena, ať už je sama o sobě správná, nebo chybná. Chceme-li motivovanému útočníkovi zabránit v záměrné manipulaci s daty a v dosažení jeho cíle, kterým je pozměnění obsahu dat pro jeho vlastní prospěch, je nutno použít **kryptografické techniky**. Je třeba, aby se entita, která má integritu dat zajišťovat, a entita, která chce být o integritě dat ujištěna, shodly na použití vhodných algoritmů a klíčů.

3.4 Dostupnost

Dostupnost znamená možnost včasného přístupu k informacím. Například havárie pevného disku nebo útok typu odepření služby mají za následek narušení dostupnosti. Každé zpoždění, které přesahuje předpokládaný limit pro danou službu, může být rovněž chápáno jako narušení dostupnosti. Mít informační systém, který není dostupný v okamžiku, kdy jej potřebujete, je někdy horší než nemít žádný. Záleží na tom, jak dalece se daná organizace stala závislou na funkční počítačové a komunikační infrastruktuře.

Podobně jako jiné aspekty bezpečnosti může být i dostupnost ovlivněna jak čistě technickými příčinami (např. selháním součástí počítače nebo komunikačního zařízení), tak přírodními jevy (např. větrem nebo vodou) či lidským faktorem (náhodně nebo záměrně).

Zatímco relativní rizika spojená s těmito kategoriemi závisí na konkrétním kontextu, obecným pravidlem je, že nejslabším článkem jsou lidé. (Proto je také klíčovým prvkem schopnost a ochota každého uživatele používat datový systém bezpečným způsobem.)

3.5 Autentizace

Podstata autentizace spočívá v tom, že komunikujícím entitám je poskytnuta jistota a informace o skutečné identitě komunikujících partnerů (lidí, strojů, procesů).

Při přenosu jediné zprávy, jakou je například výstražný nebo poplašný signál, spočívá funkce služby autentizace v ujištění příjemce, že zpráva skutečně pochází z toho zdroje, který jako svůj zdroj uvádí.

V případě probíhající interakce, jakou je například připojení terminálu k hostitelskému počítači, se jedná o dva aspekty. Zaprvé, ve fázi navazování spojení služba zaručuje, že obě entity jsou autentické, tzn. že každá z nich je tou, za kterou se prohlašuje. Zadruhé, služba musí zajistit, aby do spojení nebylo možno zasáhnout takovým způsobem, že by se třetí strana mohla podvodně vydávat za jednu z obou stran legitimních za účelem neoprávněného vysílání nebo příjmu informací.

3.6 Řízení přístupu

Řízení přístupu je ochrana informačních zdrojů nebo služeb před přístupem nebo využíváním ze strany nepovolaných entit (organizací, lidí, strojů, procesů). Můžeme tedy říci, že řízení přístupu zabraňuje neautorizovanému využívání určitého zdroje (tzn. tato služba kontroluje a určuje, kdo má přístup k jakým zdrojům, za jakých podmínek k nim může přistupovat a jakým způsobem je může využívat).

Má-li tato služba splnit svůj účel, musí být každá entita pokoušející se získat přístup nejprve identifikována (autentizována), aby jí mohla být přidělena odpovídající přístupová práva. Chceme-li řízení přístupu lépe porozumět, je důležité znát následující pojmy:

- oprávnění – práva přistupovat ke zdrojům nebo službám či využívat je,
- nositelé – entity vlastnící oprávnění,
- subjekty – entity uplatňující (vykonávající) oprávnění,
- objekty / cíle – zdroje nebo služby, k nimž subjekty přistupují nebo je využívají
- delegování – převod oprávnění mezi nositeli,
- autorizace – převod oprávnění z nositelů na subjekty.

Seznamy přístupových pravidel (**ACL –** *Access Control List*) jsou nejčastěji používaným ochranným mechanismem pro řízení přístupu.

3.7 Neodmítnutelnost

Bezpečná komunikace musí zahrnovat službu odpovědnou za vytváření digitálních důkazů, které mohou být využity při řešení sporů vzniklých v případě chyby sítě nebo nesprávného chování entit při výměně digitálních informací mezi dvěma nebo více stranami.

Neodmítnutelnost je bezpečnostní služba, která využívá digitální důkazy tak, aby žádná entita účastnící se komunikace nemohla popřít, že se účastnila celé této komunikace nebo její části.

Neodmítnutelnost je bezpečnostní služba zajišťující, aby odesílatel zprávy nemohl později popřít, že zprávu odeslal, a aby příjemce nemohl popřít, že zprávu přijal.

To zahrnuje neodmítnutí původu (tj. důkaz, že zpráva byla odeslána konkrétní stranou) a neodmítnutí příjmu (tj. důkaz, že zpráva byla konkrétní stranou přijata).

- **NRO** (*Non repudiation of origin* - neodmítnutí původu) poskytuje příjemcům důkaz, že zpráva byla odeslána uváděným odesílatelem.
- **NRR** (*Non repudiation of receipt* **-** neodmítnutí příjmu) poskytuje odesílateli důkaz, že určený příjemce zprávu přijal.

Typickými ochrannými mechanismy jsou certifikované ověření, časová značka, digitální podpisy a potvrzovací služby.

3.8 Ochrana osobních údajů

Ochrana osobních údajů je bezpečnostní služba, která umožňuje jednotlivcům zachovat si právo na kontrolu a rozhodování, jaké informace o nich jsou shromažďovány, jak jsou využívány a kdo je využívá.

V otevřené síti, jakou je Internet, mohou rozšířené možnosti sdílení informací zároveň vést k novým způsobům, jak může být narušeno soukromí. Nové technologie otevírají nové cesty, jak sbírat informace, což může mít negativní dopady na zachování soukromí. Možnost využití dolování dat a nástup různých vyhledávačů vytvářejí podmínky pro snadné shromažďování dat o jednotlivcích z mnoha různých zdrojů.

V mnoha databázích po celém světě je uloženo tolik informací, že jedinec prakticky nemá možnost znát či kontrolovat všechny informace o své osobě, které ostatní mají nebo k nim mohou získat přístup. Tyto informace by mohly být prodány jiným osobám za účelem zisku a/nebo použity k účelu pro dotyčnou osobu neznámému či dokonce nepřijatelnému (a jí postihovanému). Pojem ochrany osobních údajů nabyl na významu v souvislosti s rozmachem informačních systémů.

V prostředí Internetu můžeme soukromí jakožto jednu z priorit uživatelů chápat v souvislosti s následujícími otázkami:

- jaké osobní údaje lze sdílet a s kým,
- zda lze zprávy předávat, aniž by jejich obsah znala třetí osoba,
- zda a jak lze zprávy posílat anonymně.

Dalším problémem jsou rostoucí možnosti pro určování a sledování polohy mobilních zařízení, a tedy rostoucí ohrožení soukromí jejich uživatelů, protože pozice uživatele a jeho chování představují osobní údaje a jejich nevhodné použití narušuje soukromí.

Existuje mnoho způsobů, jak chránit soukromí uživatelů na Internetu. Například e-maily je možno šifrovat; prohlížení webových stránek, stejně jako jiné on-line aktivity, by mělo být prováděno beze stop s využitím anonymizérů, tzv. směšovacích sítí. Tyto směšovací sítě mohou být využity k tomu, aby poskytovatel připojení k Internetu nemohl sledovat, jaké stránky uživatel navštěvuje a s kým komunikuje.

3.9 Bezpečnostní mechanismy

Bezpečnostní mechanismus je proces implementace bezpečnostních služeb s využitím řešení technického (hardware), logického (software), fyzického nebo administrativního charakteru. Bezpečnostní mechanismy podporují bezpečnostní služby a vykonávají určité činnosti sloužící k ochraně před útoky nebo jejich následky.

Bezpečnostní mechanismy dělíme na ty, které jsou implementovány ve zvláštním protokolu příslušné vrstvy, a ty, které nejsou specifické pro konkrétní protokolovou vrstvu či bezpečnostní službu.

K základním bezpečnostním mechanismům patří:

- šifrování
- digitální podpis
- řízení přístupu
- integrita dat
- výměna autentizačních informací
- provozní výplň
- řízení směrování
- certifikované ověření

Šifrování je mechanismus zaměřený na ochranu informačního obsahu zprávy využívající matematických algoritmů, které transformují data do takové podoby, jež jsou pro neoprávněné subjekty nečitelná.

Digitální podpis je mechanismus, který využívá kryptografickou transformaci datové jednotky k prokázání pravosti zdroje a integrity dat, potažmo k ochraně před podvrhy.

Řízení přístupu zahrnuje různé mechanismy, které se opírají o používání přístupových práv ke zdrojům. Pro přístup k některým zdrojům využívá autorizaci.

Integrita dat zahrnuje celou řadu mechanismů používaných k zajištění neporušenosti datové jednotky nebo datového toku.

Výměna autentizačních informací je mechanismus určený k ověření identity subjektu na základě výměny informací.

Provozní výplň je mechanismus, který vkládá bity do mezer v datovém toku s cílem zmařit pokusy o analýzu provozu.

Řízení směrování umožňuje výběr konkrétních fyzicky bezpečných tras pro přenos určitých dat a umožňuje změny směrování, zejména při podezření na narušení bezpečnosti. Tento mechanismus zahrnuje také zabezpečení perimetru.

Certifikované ověření je mechanismus, který používá služeb důvěryhodné třetí strany k zajištění určitých vlastností výměny dat.

Zabezpečení perimetru je mechanismus, který umožňuje přijetí nebo odmítnutí dat pocházejících z (či odesílaných na) konkrétní adresy nebo služby mimo místní síť.

3.10 Bezpečnostní služba – mapování mechanismů

Jednotlivé bezpečnostní služby mohou ke své implementaci vyžadovat více různých bezpečnostních mechanismů. Obrázek 5 ilustruje vztah mezi bezpečnostními službami a bezpečnostními mechanismy.

	Šifrování	Digitální podpis	Řízení přístupu	Integrita dat	Autentizační výměna	Provozní výplň	Řízení směrování	Certifikované ověření
Autentizace	√	√			√			
Řizení přístupu			√					
Utajení	√					√	√	
Integrita dat	√	√		√				
Nepopiratelnost		√		√				√
Dostupnost			√	√				
Soukromí	√					√	√	

Obr. 5 – Bezpečnostní služby a mechanismy

3.11 Shrnutí

Komunikace vyžaduje integraci různých služeb s cílem zajistit odpovídající zabezpečení datových přenosů. V této kapitole jsme představili nejdůležitější bezpečnostní služby (důvěrnost, integritu, dostupnost, autentizaci, řízení přístupu, neodmítnutí a soukromí) a seznámili se s bezpečnostními mechanismy potřebnými k poskytování těchto služeb. Bezpečnostní mechanismy jsou v zásadě tyto: šifrování, digitální podpisy, řízení přístupu, integrita dat, výměna autentizačních informací, provozní výplň, řízení směrování a notářské ověření. Na závěr jsme si ujasnili vztah mezi bezpečnostními službami a mechanismy.

4 Základy kryptografie

4.1 Úvod

Kryptografie je matematická věda zabývající se metodami utajování smyslu zpráv do podoby, jež neoprávněným osobám znemožňuje zjistit jejich obsah. Řada bezpečnostních aplikací je ve skutečnosti založena na využití kryptografických algoritmů (tj. matematických transformačních funkcí) k šifrování a dešifrování dat.

Šifrování je proces (transformace) zabývající se takovou změnou dat, aby pro nepovolanou osobu, která získá k zašifrovaným datům přístup, byla tato data nečitelná a bezcenná. Dešifrování je pak převod dat zpět do původní podoby.

Kryptografický šifrový systém (tvořený šifrováním, dešifrováním a klíčem) umožňuje ukládání citlivých informací nebo jejich přenos nezabezpečenými prostředími (jako je například celosvětová síť Internet) tak, aby je nemohl přečíst nikdo kromě oprávněného příjemce. Kryptografické šifrové systémy jsou dnes již standardem pro zajištění informační bezpečnosti, důvěryhodnosti, řízení přístupu ke zdrojům i elektronických transakcí.

Tuto techniku používáme při každodenních činnostech, jako je volání z mobilního telefonu, placení kreditní nebo debetní kartou, výběr hotovosti z bankomatu nebo přihlašování k počítači pomocí hesla.

Kryptografický algoritmus, nebo též šifra, je matematická funkce používaná během šifrování a dešifrování. Kryptografický algoritmus pracuje ve spojení s jedním nebo několika klíči (kterými může být slovo, číslo nebo řetězec) s cílem zašifrovat prostý (otevřený) text. Použijeme-li pro zašifrování stejného otevřeného textu různé klíče, dostaneme různé šifrové texty. Bezpečnost šifrovaných dat zcela závisí na dvou faktorech – na síle kryptografického algoritmu a na utajení klíče.

Silný kryptografický algoritmus musí splňovat následující kritéria:

- Nesmí existovat žádný způsob, jak najít otevřený text (čitelná data), pokud klíč není znám, kromě hrubé síly, tzn. zkoušení všech možných klíčů až do nalezení klíče správného.
- Počet možných klíčů musí být tak velký, že je z hlediska dostupného výpočetního výkonu nemožné uskutečnit úspěšný útok hrubou silou v rozumném čase.
- Cokoliv je provedeno během šifrování, musí být transformováno zpět do původního stavu během dešifrování pomocí stejného klíče. V tomto kurzu se budeme zabývat tím, **co šifrování dělá**. Představíme si základní pojmy týkající se šifrování a prozkoumáme model šifrování.

- Následující témata však spadají **mimo rámec** tohoto dokumentu:
  - **jak šifrování funguje**, základní principy návrhu šifrovacích algoritmů,
  - **jak může šifrování selhat**, jak prolomit šifrovací algoritmy pomocí kryptoanalýzy.

4.2 Klasifikace kryptografických algoritmů

Kryptografické algoritmy můžeme klasifikovat takto:

Algoritmy se symetrickým čili tajným klíčem, u nichž se používá jediný klíč jak pro šifrování, tak pro dešifrování. Příkladem běžně používaného kryptografického systému se symetrickým klíčem je *standard AES* (*Advanced Encryption Standard*).

Algoritmy s veřejným čili asymetrickým klíčem, u nichž se využívá dvojice klíčů: veřejný klíč pro šifrování dat a jemu odpovídající soukromý (tajný) klíč pro dešifrování. Ačkoli jsou oba klíče z téhož páru matematicky spojeny, je výpočetně nemožné odvodit soukromý klíč z klíče veřejného. Uživatel (nebo obecně jakákoliv *entita*) oznámí svůj veřejný klíč světu (např. na k tomu určeném veřejně přístupném serveru), avšak soukromý klíč si uchová v tajnosti. Každý, kdo má k dispozici veřejný klíč, může nějakou informaci zašifrovat, ale ne dešifrovat. Dešifrovat ji může pouze osoba, která má odpovídající soukromý klíč.

Hlavním přínosem kryptografických systémů (tzv. *kryptosystémů*) založených na algoritmech s veřejným klíčem je, že umožňují bezpečnou výměnu zpráv i entitám (např. osobám), které doposud nepoužívaly žádná bezpečnostní opatření. Odesílatel a příjemce si nemusejí posílat tajné klíče prostřednictvím zabezpečených kanálů; veškerá komunikace využívá pouze veřejné klíče, a žádný soukromý klíč není nikam přenášen ani nikomu sdělován.

4.3 Terminologie

Otevřený text je zpráva, která má být předána příjemci. Bývá také označován jako *prostý text*.

Šifrový text je výstup, který vznikne šifrováním otevřeného textu.

Šifrování je proces, při němž je obsah otevřeného textu změněn takovým způsobem, že původní zpráva je skryta.

Dešifrování je opak šifrování; je to proces zpětného získání zprávy tvořené otevřeným textem z jeho šifrované podoby (šifrového textu) – jinak řečeno, převod šifrového textu na otevřený text.

Klíč je slovo, číslo, nebo řetězec; používá se k zašifrování otevřeného textu nebo k dešifrování šifrového textu.

Kryptoanalýza je věda zabývající se prolamováním kódů a šifer.

Hašovací algoritmus je algoritmus, který převede textový řetězec libovolné délky na řetězec pevné délky.

Šifra je kryptografický algoritmus, tj. matematická funkce používaná pro šifrování a dešifrování.

Luštění převádí šifrový text na ekvivalentní otevřený text pomocí šifrovacího systému.

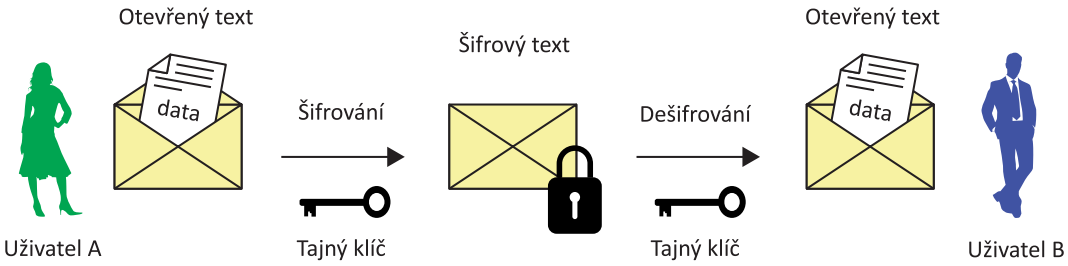
Správa klíčů je proces, v rámci kterého je klíč vygenerován, uložen, chráněn, přenášen, načítán, používán a zničen.

4.4 Kryptosystém se symetrickým klíčem

Proces šifrování a dešifrování pomocí jediného klíče je znám jako kryptosystém (někdy též kryptografie) s tajným či symetrickým klíčem. Klíče v takovém systému používané k šifrování otevřeného textu a k dešifrování šifrového textu mohou být identické (obvyklý případ), nebo může být dána jednoduchá transformace pro přechod mezi dvěma klíči. Hlavním problémem algoritmů se symetrickými klíči je, že odesílatel a příjemce si musí dohodnout společný klíč. Pro výměnu tajného klíče mezi odesílatelem a příjemcem je také nutný *zabezpečený komunikační kanál*.

4.5 Jak funguje symetrický kryptosystém?

Princip použití kryptosystému se symetrickým klíčem je následující: Uživatel A chce poslat zprávu uživateli B a chce mít jistotu, že pouze uživatel B bude schopen zprávu přečíst. Aby byl přenos bezpečný, uživatel A vygeneruje tajný klíč, zašifruje zprávu pomocí tohoto klíče a odešle ji uživateli B. Uživatel B potřebuje získat tentýž tajný klíč, aby mohl zašifrovanou zprávu přečíst. Uživatel A může tajný klíč předat uživateli B pomocí jakýchkoli dostupných prostředků. Jakmile uživatel B obdrží tajný klíč, může zprávu dešifrovat, aby získal její původní znění.



Obr. 6 – Model šifrování se symetrickým klíčem

Vlastnosti, které musí šifrovací algoritmus splňovat, jsou následující:

- **Difúze:** každý bit otevřeného textu ovlivňuje mnoho bitů šifrového textu a každý bit šifrového textu je ovlivněn mnoha bity otevřeného textu,
- **Konfúze:** je nutno zabránit vzniku strukturovaných vztahů (zejména lineární závislosti) mezi otevřeným textem a šifrovým textem / klíčem, neboť takové vztahy jsou využívány známými typy útoků.
- Šifrový text má mít náhodný charakter a dobré statistické vlastnosti.
- **Jednoduchost.**
- **Účinnost:** je velmi rychlý vzhledem k použitému hardwaru a softwaru na mnoha různých platformách.

Mezi nejpoužívanější algoritmy s tajným klíčem patří:

- *Data Encryption Standard* (**DES**)
- *Advanced Encryption Standard* (**AES**)

Hlavním problémem symetrické kryptografie je, že proces přenosu klíče k příjemci je vystaven bezpečnostním rizikům. Sestavení *bezpečného kanálu* tedy není triviální proces, protože posílání tajného klíče přes Internet v e-mailové zprávě není bezpečné, při telefonickém sdělení klíče hrozí odposlech, stejně tak při zaslání běžnou poštou existuje riziko zachycení zprávy atp.

Bezpečnostní rizika, kterými trpí kryptosystém s tajným klíčem, byla do značné míry překonána kryptografickým systémem s klíčem veřejným. Symetrické systémy se často používají k šifrování dat na pevných discích. Osoba, která šifrování provádí, klíč zná, a v tomto případě není třeba řešit problém týkající se distribuce klíčů.

4.6 Kryptosystém s veřejným klíčem

Kryptosystém (někdy též kryptografie) s veřejným klíčem vznikl v reakci na bezpečnostní problémy kryptografie symetrické. Tato metoda řeší uvedené problémy použitím **dvou klíčů** namísto jediného. Kryptosystém s veřejným klíčem tedy používá dvojici klíčů – jeden pro šifrování a druhý pro dešifrování.

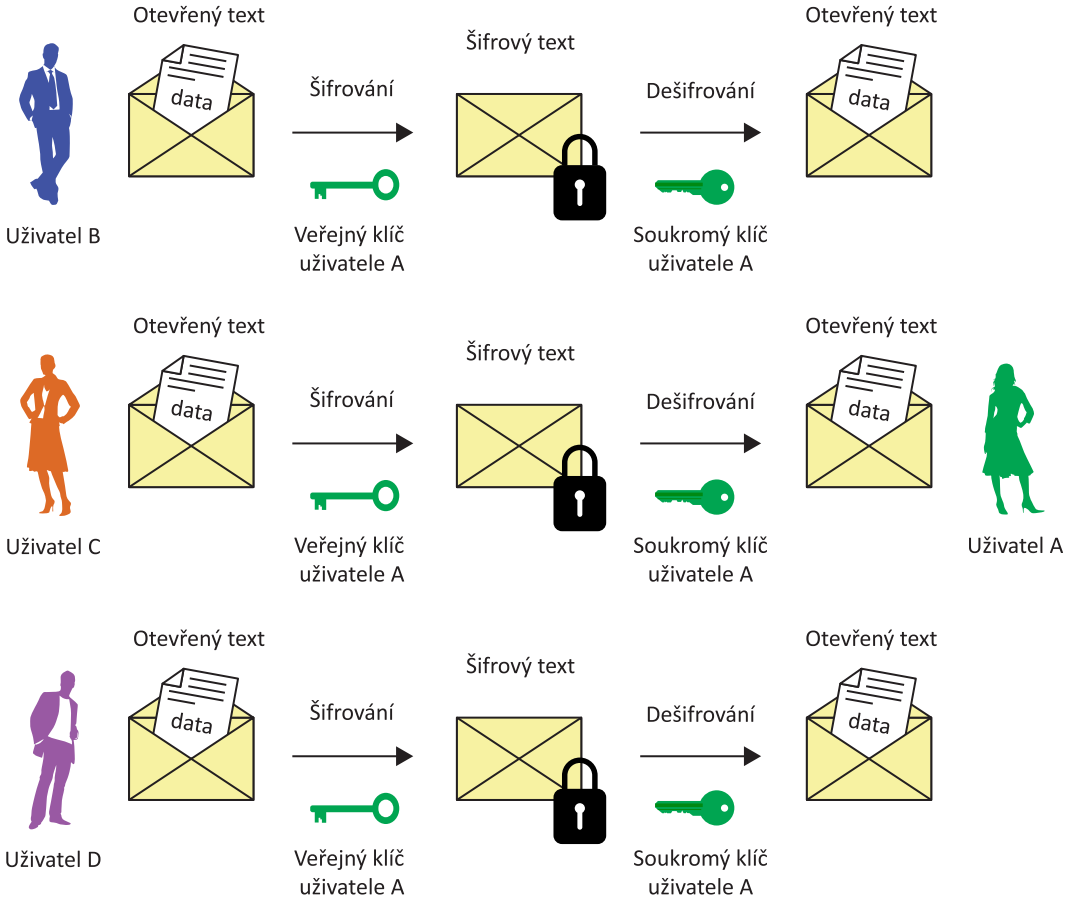
Kryptosystém s veřejným klíčem se rovněž označuje jako asymetrický kryptografický systém, protože k dokončení procesu je zapotřebí obou klíčů. Tyto dva klíče jsou známy jako **dvojice klíčů**. V asymetrické kryptografii je jeden z klíčů volně šiřitelný – nazývá se **veřejný klíč** a používá se pro šifrování. Proto se tato metoda také označuje jako šifrování s veřejným klíčem. Druhým klíčem je **tajný** neboli **soukromý klíč** a používá se pro dešifrování. Soukromý klíč nesmí být šířen; jak název napovídá, je soukromý pro každou komunikující entitu. Je třeba zdůraznit, že veřejný a soukromý klíč jsou spolu svázány, ale je prakticky nemožné odvodit soukromý klíč na základě znalosti veřejného klíče.

Nejběžnější algoritmus využívající veřejného klíče je **RSA**, jehož název je zkratka odvozená z prvních písmem příjmení jeho autorů, jimiž jsou: *Rivest, Shamir, Adleman*).

4.7 Jak funguje asymetrický kryptosystém?

Jak šifrování s veřejným klíčem poskytuje důvěrnost

Vezměme si příklad, kdy uživatel B chce poslat zprávu uživateli A. Uživatel B zašifruje zprávu veřejným klíčem uživatele A, a uživatel A dešifruje zprávu pomocí svého soukromého klíče. Vzhledem k tomu, že dvojice klíčů jsou komplementární (navzájem se doplňují), může být k dešifrování daného souboru použit jen soukromý klíč uživatele A. Pokud někdo jiný zachytí šifrový text, nebude schopen jej dešifrovat, protože k tomu lze použít pouze soukromý klíč uživatele A. Tato metoda neposkytuje žádnou autentizaci, tedy ověření, že zpráva přichází skutečně od uživatele B, protože veřejný klíč uživatele A je veřejně známý. Poskytuje však zprávě důvěrnost, protože pouze uživatel A ji může dešifrovat.



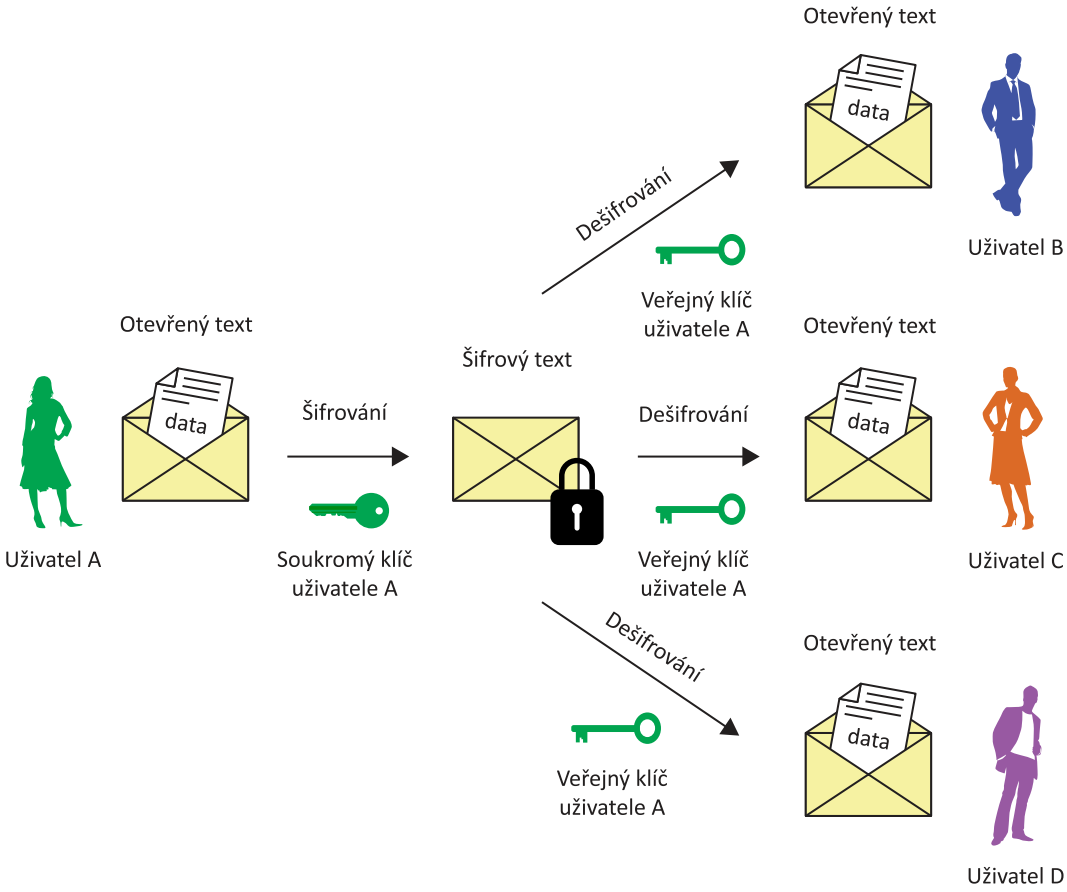
Obr. 7 – Model šifrování s veřejným klíčem (zajištění důvěrnosti)

Tato metoda jasně ukazuje, že data, která zasíláte nějakému uživateli, mohou být zašifrována pouze pomocí veřejného klíče příjemce, pokud má být zajištěna důvěrnost. A naopak, dešifrování může být provedeno pouze pomocí soukromého klíče, který vlastní příjemce dat. Výměna zpráv tedy může být bezpečná. Odesilatel a příjemce nemusí mít k dispozici stejný klíč, jako je tomu v případě

symetrického šifrování. Veškerá komunikace probíhá pouze s použitím veřejného klíče, a žádný soukromý klíč není nikam přenášen ani nikomu sdělován.

Jak šifrování s veřejným klíčem poskytuje autentizaci

Chceme-li zajistit autentizaci, musí uživatel A zašifrovat zprávu svým soukromým klíčem a uživatel B ji bude dešifrovat pomocí veřejného klíče uživatele A. Tato metoda bude poskytovat autentizaci, tedy ověření, že zpráva pochází od uživatele A, avšak nezaručuje důvěrnost, protože veřejný klíč uživatele A je veřejně známý. Proto může danou zprávu dešifrovat každý, kdo zná veřejný klíč uživatele A.



Obr. 8 – Model šifrování s veřejným klíčem (zajištění autentizace)

Jak šifrování s veřejným klíčem poskytuje autentizaci i důvěrnost

Aby byla zajištěna jak důvěrnost, tak autentizace, musí uživatel B zašifrovat otevřený text nejprve pomocí svého soukromého klíče, což zajistí autentizaci. Poté použije uživatel B k dalšímu zašifrování zprávy veřejný klíč uživatele A, což zajistí důvěrnost.

Nevýhodou tohoto systému je, že celá operace bude časově náročná a složitá, neboť šifrování a dešifrování s veřejným klíčem musí být provedeno celkem čtyřikrát, přičemž délka klíče veřejného klíče je poměrně značná (1024 až 4096 bitů).

4.8 Hybridní systém: kombinace symetrického a asymetrického šifrování

Nevýhodou **šifrování s veřejným klíčem** je, že jde o **značně pomalý proces**, jelikož délka klíčů je velká (1024 až 4096 bitů) a matematické operace s takto velkými čísly jsou velmi pomalé. Při porovnání obou procesů zjistíme, že **šifrování se symetrickým klíčem** je podstatně (o dva až tři řády) **rychlejší**, protože délka klíče je menší (64 až 256 bitů); na druhé straně zde však existuje problém týkající se přenosu klíče. Obě metody mohou být použity společně, a nabízejí tak ještě lepší způsob šifrování. Tak můžeme využít kombinace výhod a odstranit nevýhody.

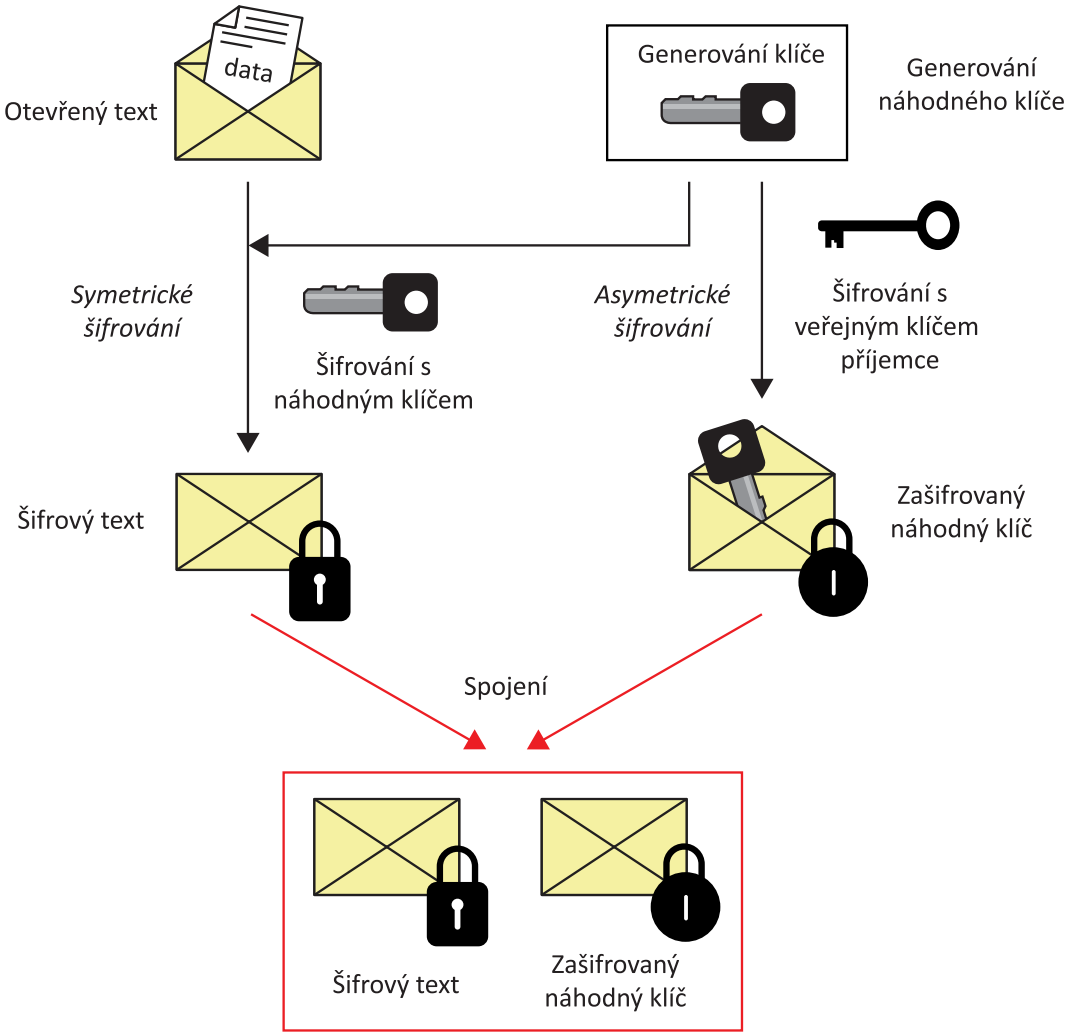
Konkrétně – hybridní systém využívá algoritmus veřejného klíče k bezpečnému sdílení tajného klíče symetrického šifrovacího systému. Samotná zpráva je pak zašifrována pomocí tohoto klíče, a následně odeslána příjemci. Vzhledem k tomu, že metoda pro sdílení klíče je bezpečná, mění se pro každou odeslanou zprávu symetrický klíč použitý k šifrování. Z tohoto důvodu je někdy označován jako klíč relace (session key). To znamená, že pokud je klíč relace zachycen, může útočník přečíst pouze jednu zprávu šifrovanou pomocí tohoto klíče. Pokud by chtěl dešifrovat ostatní zprávy, musel by zachytit i klíče dalších relací.

Klíč relace, zašifrovaný pomocí algoritmu s veřejným klíčem, a odesílaná zpráva, zašifrovaná pomocí symetrického algoritmu, jsou automaticky spojeny do jediného datového balíčku. Příjemce použije svůj soukromý klíč k dešifrování klíče relace, a pak použije klíč relace k dešifrování zprávy. Mnoho aplikací používá právě tento systém.

Postupné kroky při datové transakci s využitím kombinované metody jsou následující:

1. Zašifrování otevřeného textu pomocí symetrické šifry a náhodného klíče.
2. Zašifrování pouze tohoto náhodného klíče pomocí veřejného klíče příjemce (asymetrické šifrování). Nyní je zašifrovaný náhodný klíč odeslán příjemci. Příjemce nyní může na své straně dešifrovat náhodný klíč pomocí svého soukromého klíče.
3. Odeslání samotných zašifrovaných dat. Zašifrovaná data lze dešifrovat pomocí klíče, který byl zašifrován pomocí veřejného klíče z dvojice asymetrických klíčů.

Tento proces ilustruje následující obrázek 9.



Obr. 9 – Model hybridního šifrování (zajištění důvěrnosti)

Popsaná kombinovaná metoda šifrování je široce využívána. Používá ji například *Secure Shell* (**SSH**) k zabezpečení komunikace mezi klientem a serverem nebo **PGP** (*Pretty Good Privacy*) pro odesílání zpráv. Především je to ale srdce protokolu *Transport Layer Security* (**TLS**), který používají webové prohlížeče a webové servery k udržování zabezpečeného komunikačního kanálu mezi sebou navzájem.

4.9 Hašovací funkce

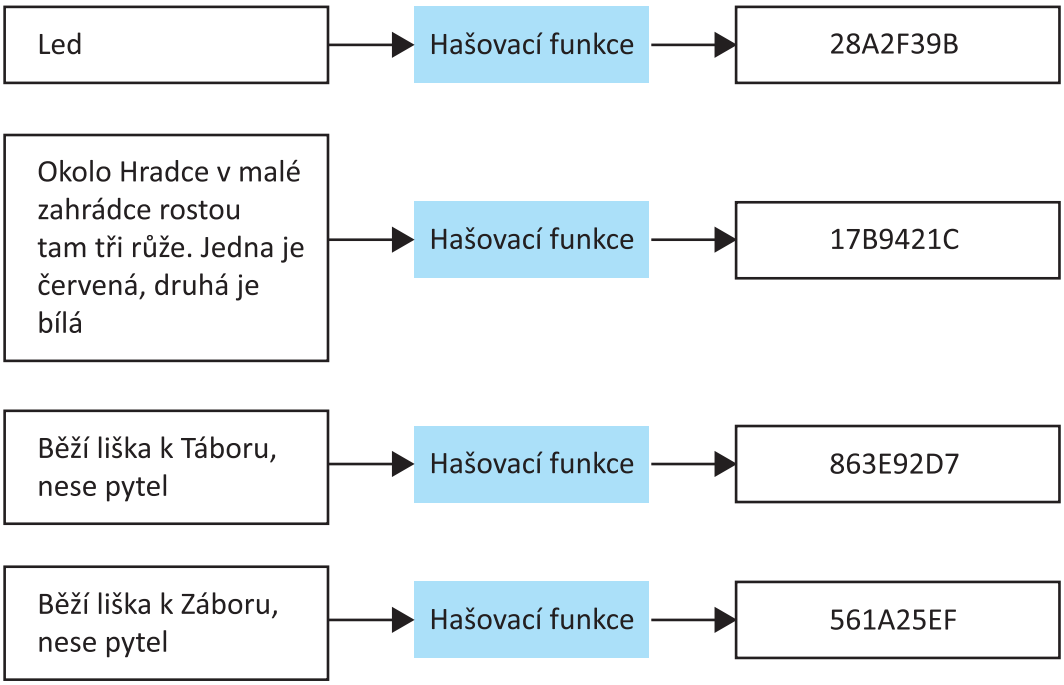
Hašovací funkce je transformace, která zpracovává bloky vstupních dat *m* o různé velikosti a vrací řetězec pevné velikosti, který se nazývá hodnota haše *h* (tedy platí, že $h = H(m)$). Jakákoliv změna vstupních dat bude mít (s velmi vysokou pravděpodobností) za následek změnu hodnoty haše. Hašovací funkce právě s touto vlastností mají nejrůznější uplatnění v obecných výpočetních aplikacích, ale pokud se využívají v kryptografii, jsou hašovací funkce obvykle voleny tak, aby měly nějaké další důležité vlastnosti.

Základní požadavky kladené na kryptografickou hašovací funkce jsou následující:

- vstup může mít libovolnou délku,
- výstup má pevnou délku,
- je snadné vypočítat hodnotu haše pro danou zprávu,
- hašovací funkce jsou jednosměrné, tzn. je výpočetně nemožné vytvořit zprávu, která má danou hodnotu haše,
- není možné upravit zprávu, aniž by se změnila hodnota jejího haše,
- je bezkolizní, tzn. je výpočetně nemožné najít dvě různé zprávy (x, y) tak, aby platilo $H(x) = H(y)$.

Hodnota haše představuje zhuštěnou podobu delší zprávy nebo dokumentu, ze kterého byl vypočítán. O tomto stručném výtahu můžeme uvažovat jako o „digitálním otisku“ většího dokumentu.

Hlavní využití kryptografické hašovací funkce leží v oblasti poskytování *digitálních podpisů*. Kromě toho lze tento otisk zveřejnit, aniž by byl vyzrazen samotný obsah dokumentu, z něhož je odvozen.



Obr. 10 – Hašovací funkce

4.10 Digitální podpis

Digitální podpisy jsou nejdůležitějším ovocem úsilí věnovaného kryptografii s veřejným klíčem, a disponují řadou bezpečnostních funkcí, které by bylo obtížné realizovat jiným způsobem.

Digitální podpis je variantou elektronického podpisu, který je realizován pomocí asymetrické kryptografie a může být použit k ověření identity odesílatele zprávy nebo signatáře dokumentu, a případně i k zajištění integrity zprávy.

Digitální podpisy lze snadno přepravovat a nemůže je napodobit nikdo jiný. Schopnost zajistit, aby byla původní podepsaná zpráva doručena, zároveň znamená, že odesílatel nemůže později snadno popřít její odeslání.

Digitální podpisy jsou založeny na vlastnoručních podpisech, které jsou používány pro potvrzení vlastnických práv nebo obsahu zpráv. Vlastnoruční podpisy by měly mít následující vlastnosti:

- Podpis je bezpečný – podpis by neměl být napodobitelný, a případné pokusy o padělání by mělo být možné snadno odhalit.
- Podpis usnadňuje autentizaci – podpis jednoznačně identifikuje vlastníka, který podepsal dokument svobodně a vědomě.
- Podpis je nepřenosný – podpis je součástí dokumentu, a neoprávněný subjekt není schopen přenést podpis do jiného dokumentu.
- Podepsaný dokument nelze měnit – dokument nelze měnit a upravovat poté, co byl podepsán.
- Podpis je nepopiratelný – držitel podpisu nemůže popřít, že podepsaný dokument skutečně podepsal.

V praxi však žádná z těchto vlastností nebývá u vlastnoručních podpisů důsledně splněna, což může vést k diskreditaci nebo poškození. Digitální podpisy by měly mít všechny uvedené charakteristiky.

Existují však určité problémy spojené s praktickou realizaci digitálních podpisů. Digitální soubory lze snadno kopírovat, část dokumentu může být přenesena do jiného dokumentu a podepsaný dokument lze snadno pozměnit. Proto je nutno specifikovat další požadavky kladené na digitální podpis:

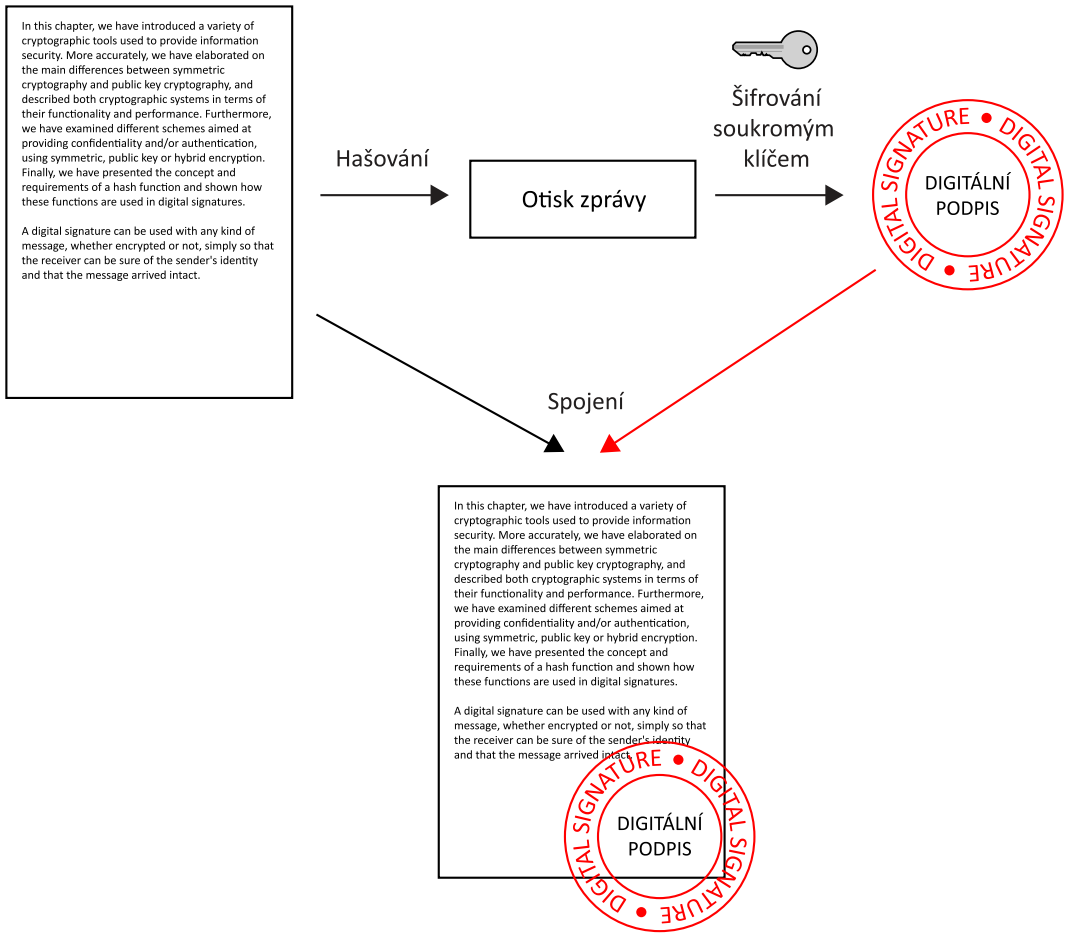
- Podpis musí být bitová posloupnost, která je závislá na obsahu podepsané zprávy.
- Podpis musí využívat nějakou informaci, která je jedinečná pro daného odesílatele, aby se předešlo padělání a popírání autentičnosti.
- Realizace a implementace digitálního podpisu musí být poměrně snadná.

- Padělání digitálního podpisu musí být výpočetně neproveditelné, ať už jde o pokus vytvořit novou zprávu k existujícímu digitálnímu podpisu, nebo vytvořit padělaný digitální podpis k dané zprávě.
- Musí být praktické ponechat si kopii digitálního podpisu v datovém úložišti.

Digitální podpis může být použit pro jakýkoliv druh zprávy, ať už je šifrovaná, nebo ne, jednoduše tak, aby si příjemce mohl být jist identitou odesílatele i neporušeností doručené zprávy.

Existuje několik možných schémat pro digitální podpisy. Jedno z nejvíce uznávaných je založeno na hašovacích funkcích. V tomto případě jsou kroky uživatele, který chce digitálně podepsat dokument, následující:

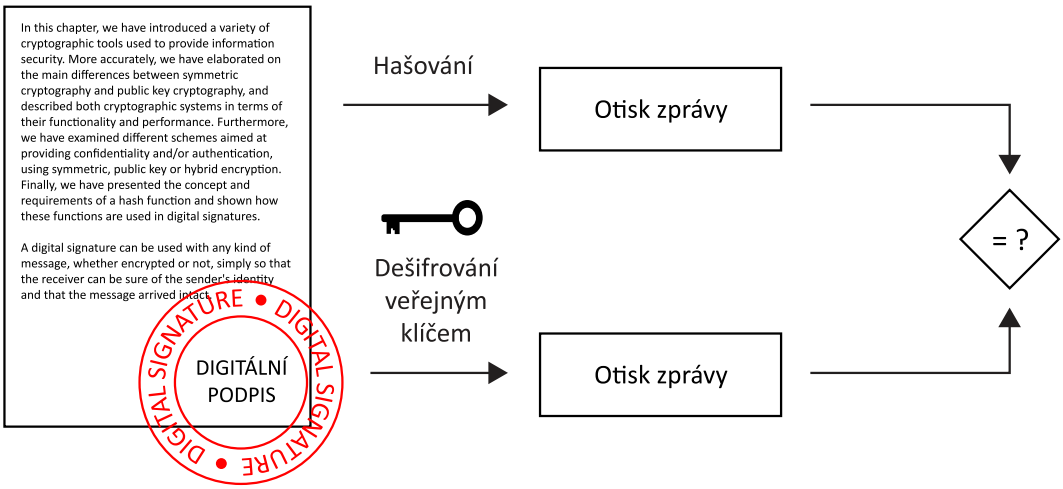
- Určit hodnotu haše dokumentu, který má být podepsán.
- Pomocí asymetrické šifry zašifrovat haš s použitím soukromého klíče odesílatele, čímž dostaneme digitální podpis.
- Přidat digitální podpis do dokumentu.



Obr. 11 – Model digitálního podpisu založeného na otisku (haš)

Příjemce si může ověřit pravost tohoto digitálního podpisu následujícími kroky:

- Vyhodnotit haš dokumentu (bez digitálního podpisu).
- Pomocí asymetrické šifry dešifrovat digitální podpis odesílatele s použitím veřejného klíče odesílatele, čímž dostaneme otisk zprávy.
- Porovnat výsledky získané v předchozích dvou krocích.



Obr. 12 – Proces ověření digitálního podpisu založeného na otisku (haš)

Pokud jsou otisky zprávy získané v obou krocích stejné, bude příjemce vědět, že podepsaná data nebyla pozměněna.

4.11 Shrnutí

V této kapitole jsme si představili řadu kryptografických nástrojů používaných k zajištění informační bezpečnosti. Přesněji vzato jsme se zabývali hlavními rozdíly mezi symetrickou kryptografie a kryptografií s veřejným klíčem a popsali si oba kryptografické systémy z hlediska jejich funkčnosti a výkonnosti. Dále jsme prozkoumali různé možnosti zajištění důvěrnosti a/nebo autentizace s využitím symetrického šifrování, veřejného klíče nebo hybridního šifrování. Nakonec jsme se seznámili s pojmem hašovací funkce a ukázali jsme si, jak se tyto funkce využívají v digitálních podpisech.

5 Digitální certifikáty a správa klíčů

5.1 Distribuce veřejných klíčů

Digitální podpisy představují jeden z hlavních způsobů využití kryptografie s veřejným klíčem. U zpráv odesílaných přes nezabezpečený kanál dává správně implementovaný digitální podpis příjemci dobrý důvod předpokládat, že zpráva byla odeslána uváděným odesílatelem. V mnoha ohledech jsou digitální podpisy rovnocenné tradičním ručně psaným podpisům – zfalšovat řádně provedený digitální podpis je však mnohem obtížnější. Pro účely ověření digitálního podpisu je nutné znát veřejný klíč odesílatele. Z tohoto důvodu je naprosto nezbytné, aby byl definován mechanismus distribuce klíčů.

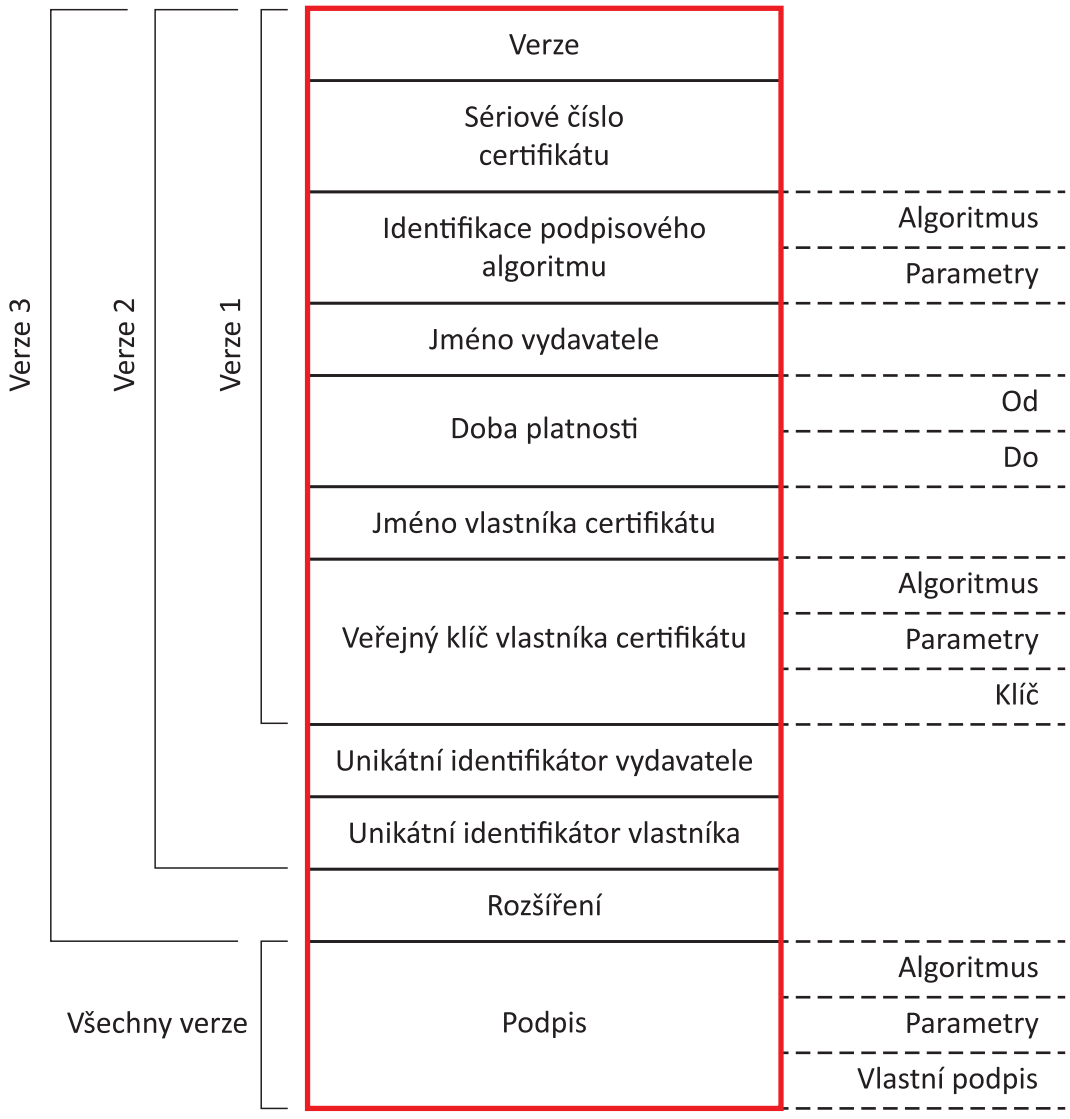
Nejčastěji způsob distribuce veřejných klíčů je založen na využití digitálních certifikátů podle standardu X.509.

5.2 Pojem digitálního certifikátu

Digitální certifikát je elektronický dokument, který obsahuje digitální podpis, a jeho účelem je **svázat veřejný klíč s identitou** dané osoby – tedy s informacemi, jako je jméno osoby nebo název organizace, adresa a podobně.

Certifikát může být použit k ověření, že veřejný klíč náleží dané osobě. Digitální certifikát je datová struktura, která obsahuje veřejný klíč subjektu nebo držitele certifikátu, jakož i identifikační údaje držitele certifikátu, časové razítko udávající dobu platnosti certifikátu a další údaje přidané *certifikační autoritou* (**CA**). Tato struktura je podepsána s použitím soukromého klíče certifikační autority, a každý uživatel si může ověřit autentičnost obsahu certifikátu pomocí veřejného klíče certifikační autority.

Obrázek 13 ukazuje strukturu digitálního certifikátu.

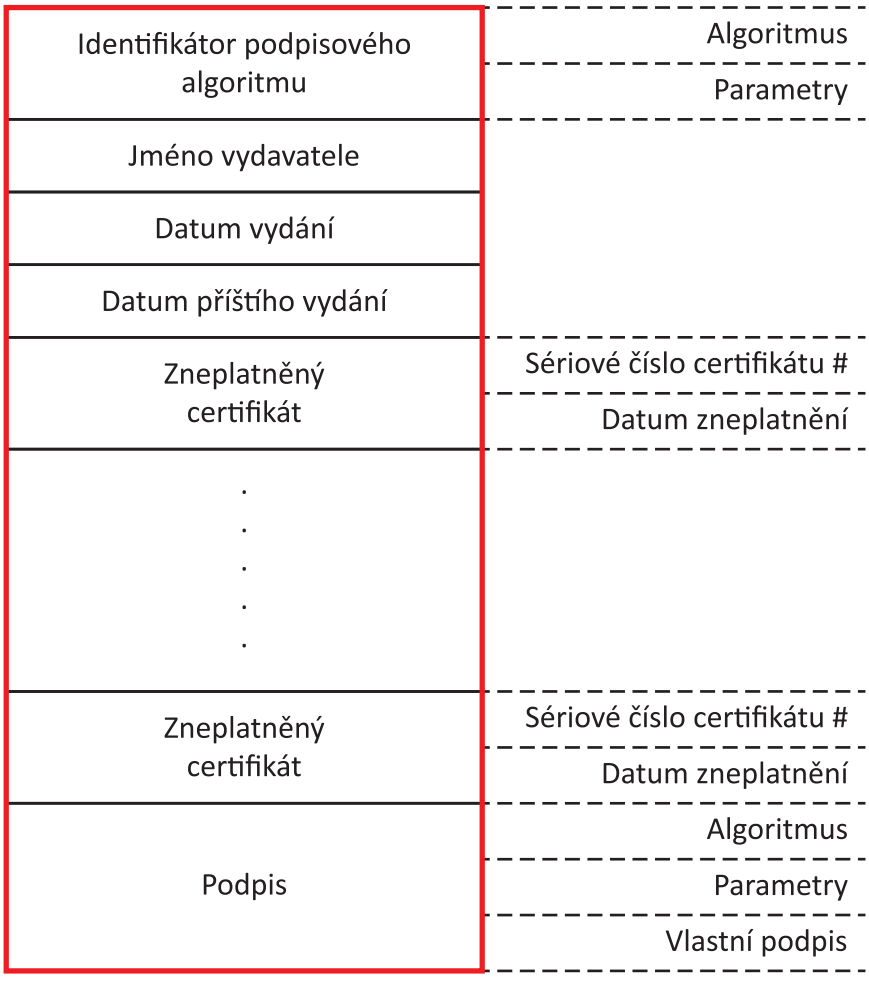


Obr. 13 – Struktura digitálního certifikátu

5.3 Proces zneplatnění certifikátu

Platnost digitálního certifikátu může být zrušena (revokována), například jestliže uživatel již není výhradním vlastníkem soukromého klíče (obvykle následkem jeho ztráty nebo odcizení) – pak se předpokládá, že soukromý klíč byl vyzrazen. Certifikát může být zrušen také tehdy, zjistí-li se, že *certifikační autorita* (**CA**) jej vydala nesprávně, v rozporu s požadavky bezpečnostních zásad.

Nejběžnější mechanismus pro ověření, zda byla platnost certifikátu zrušena, je založen na použití revokačního seznamu (**CRL** – *Certificate Revocation List*). CRL je seznam certifikátů (nebo, přesněji řečeno, seznam sériových čísel certifikátů), které byly zrušeny, a proto by neměly být přijímány. CRL vždy vydává ta CA, která vydala i příslušné certifikáty. CRL je generován a zveřejňován pravidelně, obvykle v určených časových intervalech. Každá CA tedy potřebuje CRL.



Obr. 14 – Struktura revokačního seznamu (CRL)

5.4 Shrnutí

V této kapitole jsme se seznámili s problematikou distribuce veřejných klíčů a s používáním digitálních certifikátů jakožto nejvíce přijímaným řešením tohoto problému. Dále jsme popsali problém revokace certifikátů a uvedli, jak funguje mechanismus založený na CRL.

6 Bezpečnost síťových služeb

6.1 TLS

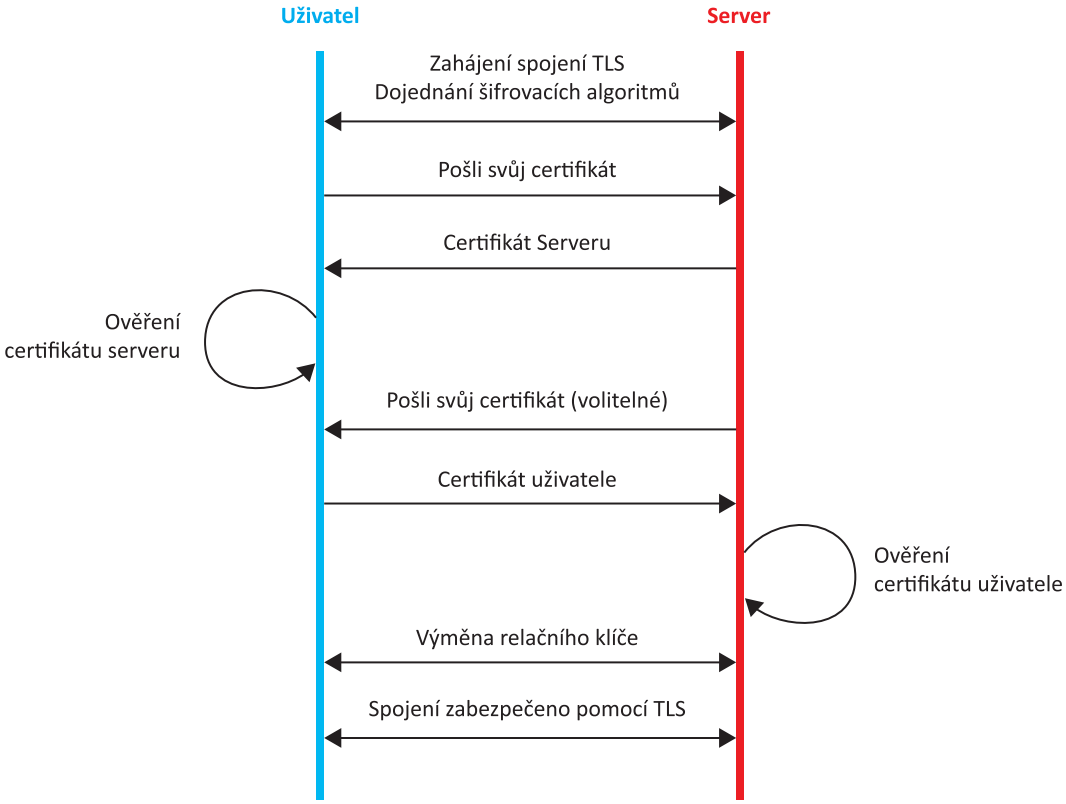
Transport Layer Security (**TLS**) je standardní internetový protokol, který poskytuje zabezpečení komunikace v Internetu. Hlavním účelem tohoto protokolu je zajištění důvěrnosti a integrity dat mezi dvěma komunikujícími aplikacemi. Nejvýznamnější použití TLS spočívá v zabezpečení World Wide Web provozu přenášeného s využitím protokolu **HTTP**, čímž vzniká **HTTPS** umožňující bezpečné elektronické obchodní transakce. Ve stále větší míře bývá pomocí TLS chráněn i *Simple Mail Transfer Protocol* (**SMTP**).

TLS je ve velké míře využíván v aplikacích pro prohlížení webových stránek, elektronickou poštu, internetové faxování, instant messaging a *Voice-over-IP* (**VoIP**).

TLS je založen na starších specifikacích *Secure Sockets Layer* (**SSL**) vypracovaných společností Netscape Communications. Oba protokoly (TLS a SSL) využívají kryptografické algoritmy a certifikáty s veřejným klíčem pro ověření totožnosti koncových bodů a pro výměnu klíčů. Tuto autentizaci lze nastavit jako nepovinnou, avšak obecně je vyžadována alespoň pro jednu z obou komunikujících entit.

Oba také používají symetrické šifrování pro zajištění důvěrnosti a **MAC** funkce (*Message Authentication Code*) pro zajištění integrity zpráv. Symetrická kryptografie je použita pro šifrování dat. Klíče pro toto symetrické šifrování jsou generovány zvlášť pro každé spojení a jsou založeny na dříve sjednaném sdíleném tajemství. Sjednávání tohoto sdíleného klíče je zabezpečené a spolehlivé: sjednaný klíč není možno odposlechnout, a při žádném autentizovaném spojení nemůže útočník klíč získat, ani pokud se nachází v cestě spojení (útok typu Man in the Middle). Navíc žádný útočník nemůže pozměnit komunikaci při sjednávání klíče, aniž by byl takový pokus odhalen účastníky komunikace.

Obrázek 15 zjednodušeně ukazuje, je navazována relace TLS.



Obr. 15 – Navázání relace protokolu TLS

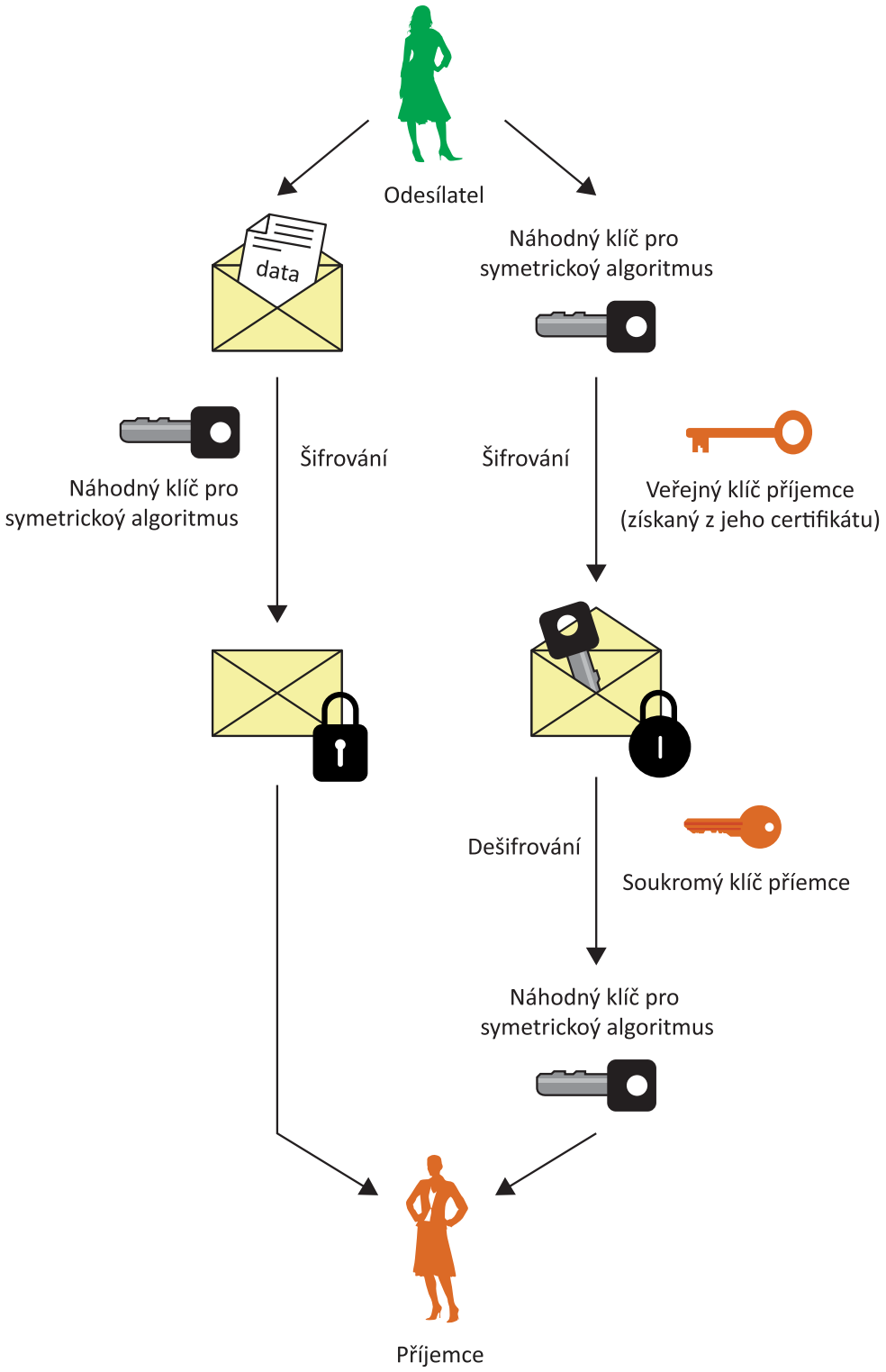
6.2 Bezpečnost elektronické pošty

Když je odesílána e-mailová zpráva, její obsah je obvykle otevřen pro každého. E-mail je jako posílání pohlednice: každý, kdo ji dostane do rukou, si ji může přečíst. Chcete-li zachovat důvěrnost a/nebo autentičnost dat posílaných e-mailem, je nutno je zašifrovat. Pokud jde o důvěrnost, bude pouze oprávněný příjemce schopen zprávu dešifrovat, zatímco ostatní uvidí jen nesmyslnou změť znaků.

Mezi obvyklé mechanismy sloužící k zabezpečení e-mailu patří **S/MIME** (*Secure Multipurpose Internet Mail Extension*) a **PGP**(*Pretty Good Privacy*)

S/MIME je standard, který poskytuje následující kryptografické zabezpečovací služby pro aplikace elektronického přenosu zpráv: autentizace, integrita zpráv, nepopiratelnost původu (pomocí digitálních podpisů) a důvěrnost dat (pomocí šifrování). Použití **S/MIME** vyžaduje digitální certifikáty.

Obrázek 16 ukazuje, jak se S/MIME využívá pro zajištění důvěrnosti.



Obr. 16 – Zajištění důvěrnosti pomocí S/MIME

6.3 Shrnutí

V této kapitole jsme si stručně představili dva bezpečné protokoly (TLS a S/MIME), které využívají kombinaci veřejného klíče a symetrické kryptografie. V obou případech je autentizace založena na použití digitálních certifikátů a šifrování uživatelských dat se provádí prostředky symetrické kryptografie.

7 Vnější zabezpečení

7.1 Firewally

Jedním z nejčastěji nasazovaných a propagovaných bezpečnostních opatření pro použití v internetu je „firewall“. Firewally si získaly pověst obecného všeléku na mnohé, ne-li všechny bezpečnostní problémy Internetu. Nejsou však jimi. Je to jen jeden z nástrojů v boji o zabezpečení systému. Úroveň zabezpečení, kterou firewall poskytuje, se může měnit, stejně jako úroveň zabezpečení konkrétního stroje. Objevují se zde tradiční kompromisy mezi bezpečností, snadností použití, výší nákladů, složitostí atd.

Firewall je zařízení sloužící k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení pomocí předem definovaných pravidel pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla dříve zahrnovala pouze identifikaci zdroje a cíle dat (zdrojovou a cílovou adresu sítě/zařízení) a zdrojový a cílový port. V současné době však moderní firewally pracují rovněž s informacemi o stavu spojení a se znalostí kontrolovaných protokolů.

Dříve nežli je firewall nainstalován, je vhodné, aby si příslušná organizace stanovila soubor pravidel s cílem zajistit ochranu svých aktiv, počítačových systémů, osobních údajů a dalších citlivých dat. Tento soubor pravidel nazýváme též *zásadami zabezpečení*. Tento dokument zajistí, že budou v celé firemní síti dodržována jednotná pravidla, kterými se budou správci zařízení při jejich nastavování řídit.

Firewall může fungovat dvěma základními způsoby – buď může komunikaci blokovat, nebo ji povolovat. Je důležité si uvědomit, že pro zabránění šíření jakýchkoliv síťových ilegálních aktivit, je vždy výhodné kontrolovat jak provoz do sítě přicházející, tak i provoz ze sítě odcházející.

Firewally lze kategorizovat následovně:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou protokolů

Paketové filtry jsou nejjednodušší a nejstarší formou zabezpečení provozu. Pracují pouze s informace o zdrojové a cílové adrese a portu, tj. na třetí (síťové) a čtvrté (transportní) vrstvě ISO/OSI modelu. Mezi jejich výhodu patří jejich rychlost, takže tento princip se používá dodnes.

Aplikační brány neboli *Proxy servery*, slouží ke kontrole spojení iniciovaných klientskými aplikacemi. Brána funguje jako prostředník mezi klientem a cílovým

serverem, takže původní spojení rozdělí na dvě: klient–brána a brána–server, což umožňuje filtrovat požadavky na nežádoucí cílová zařízení. Kontrola se tedy provádí na sedmé (aplikační) vrstvě ISO/OSI modelu.

Stavové paketové filtry si oproti klasickým paketovým filtrům ukládají i informace o povolených spojeních, které využívají pro rychlejší vyhodnocení dalších paketů, které s již povoleným paketem (resp. spojením) souvisejí. To je nejenom rychlejší, ale zároveň zefektivňuje konfiguraci, neboť stačí nastavit jeden směr a pakety odpovědí již budou automaticky povoleny.

Stavové paketové filtry s kontrolou protokolů jsou moderní stavové paketové filtry, které kromě informací o stavu spojení a schopnosti dynamicky otevírat porty pro řídící a datová spojení složitějších známých protokolů, umožnují kontrolovat i spojení na aplikační úrovni známých dat a protokolů. Lze tak například odhalit pokus o spojení hypertextového protokolu (HTTP), kdy se nejedná o požadavek na WWW server, nýbrž o tunelování jiného protokolu (jiná aplikace snažící se komunikovat na stejném portu).

7.2 Systémy detekce průniku

Zajišťování bezpečnosti je čím dál obtížnější, protože technologie použitelné pro vedení útoků jsou čím dál sofistikovanější; současně potřebují začínající útočníci méně technických schopností, jelikož popis osvědčených metod je snadno přístupný na webu. Systémy pro detekci průniku (**IDS –** *Intrusion Dection System*) jsou proto vyvíjeny v reakci na rostoucí počet útoků vedených proti významným stránkám a sítím.

Systémy detekce průniků monitorují síťový provoz, pracují s databází signatur a pomocí heuristické analýzy odhalují vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení (např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.) Jejich cílem je detekce neobvyklých aktivit, které by mohly vést k narušení bezpečnosti v operačním systému nebo počítačové síti, a též možný aktivní zásah proti nim.

IDS využívá hodnocení zranitelnosti (někdy označované jako skenování), což je technologie vyvinutá pro posuzování bezpečnosti počítačového systému nebo sítě.

Mezi funkce pro odhalování průniku patří:

- monitorování a analýza uživatelských i systémových aktivit,
- analýza systémových konfigurací a zranitelných míst,
- posuzování integrity systému a souborů,
- schopnost rozpoznat vzorce chování typické pro útoky,
- analýza nezvyklých vzorců chování,
- sledování porušování uživatelských zásad.

Systém pro detekci průniku (**IDS**) kontroluje veškeré síťové aktivity v příchozím i odchozím směru a vyhledává podezřelé vzorce chování, které mohou ukazovat na síťový nebo systémový útok, tedy pokus o průnik do systému či o jeho ohrožení.

Existuje několik hledisek, podle nichž můžeme IDS dělit:

Detekce zneužití a detekce anomálií

- **Detekce zneužití:** IDS analyzuje shromažďované informace a porovnává je s rozsáhlou databází, která obsahuje signatury útoků. IDS v podstatě hledá popis konkrétního útoku, který již byl zaznamenán. Metoda detekce průniku založená na signatuře útoku spočívá v hledání „podpisů“ (posloupností znaků typických pro útok) ve veškeré komunikaci přenášené sítí. Tato metoda umožňuje odhalit útoky na aplikační úrovni, a to i tehdy, jsou-li v souladu s protokolovými standardy pro komunikaci mezi aplikacemi; v tomto smyslu

tedy vlastně doplňuje dekódování meziaplikačních protokolů. Podobně jako systém pro detekci virů, i software pro detekci zneužití je z hlediska spolehlivosti odkázán na databázi obsahující signatury útoků, se kterou porovnává přenášené pakety; tím je dána nutnost tuto databázi udržovat a často aktualizovat.

- **Detekce anomálií:** správce systému definuje základní či normální stav z hlediska zatížení sítě, poruch, protokolu a typické velikosti paketů. Detektor anomálií monitoruje síťové segmenty, porovnává jejich stav se stavem normálním a hledá anomálie.

Systémy založené na síti a založené na hostitelském počítači

- *Systém založený na síti (***NIDS** – *Network IDS)*: NIDS analyzuje pakety přenášené sítí, takže monitoruje více hostitelů (zařízení) najednou. NIDS dokáže detekovat škodlivé pakety, které jsou navrženy tak, aby je jednoduchá filtrovací pravidla firewallu neodhalila.

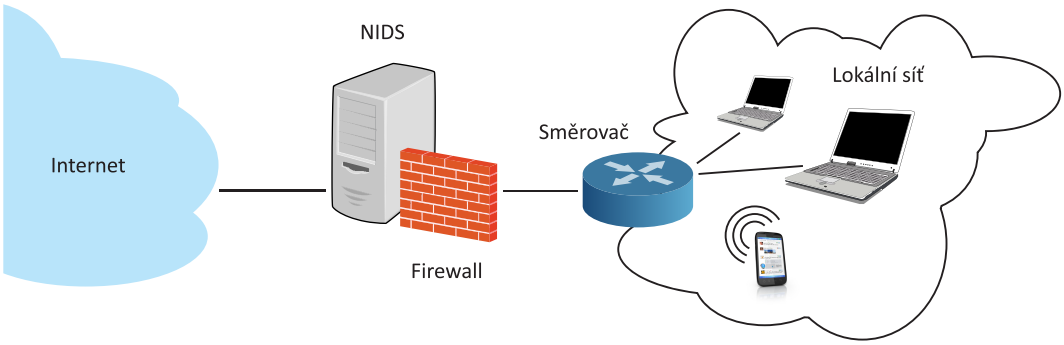
- *Systém založený na hostitelském počítači (***HIDS –** *Host-based IDS)*: HIDS je ve formě softwarového programu (tzv. agenta), který s cílem odhalit útoky monitoruje v rámci daného počítače (hostitele) jeho aktivity pomocí analýzy systémových volání, činnosti aplikací, úprav na souborovém systému apod.

Pasivní systém a aktivní detekční systém

- *Pasivní systém detekce*: IDS detekuje potenciální narušení bezpečnosti, zaznamenává informace a signalizuje výstrahu. Výhoda je, že zařízení není umístěno v cestě provozu, ale síťový provoz se na něj kopírován (zrcadlen). V případě podezření provede pouze příslušné oznámení (email, zpráva SNMP trap apod.)

- *Aktivní systém detekce (Systém prevence)*: Aktivní IDS běžně označovaný jako *Intrusion Prevention System (IPS)* reaguje na podezřelou aktivitu, mimo pasivního ohlášení (jako IDS) aktivně, např. odhlášením uživatele nebo přeprogramováním příslušného síťového zařízení (typicky firewallu) s cílem zablokovat síťový provoz z podezřelého (potenciálně škodlivého) zdroje. Zařízení IPS je vždy umístěno v cestě provozu, aby bylo možné aktivně zabránit šíření podezřelých paketů v síti. Tím ale vytváří potenciální úzké hrdlo, a přispívá tak k celkovému zpoždění při přenosu zpráv. Moderní IPS jsou však navrženy tak, aby zpoždění paketů při jejich zpracování (kontrole), bylo minimální (řádově jednotky až desítky mikrosekund).

Obrázek 17 ukazuje schéma síťového systému prevence (NIPS) s firewallem.



Obr. 17 – Schéma NIPS (aktivního NIDS) s firewallem

IDS se liší od firewallu v tom, že firewall omezuje přístup mezi sítěmi, aby předešel průniku, přičemž ale neupozorňuje na útok vedený zevnitř sítě. IDS vyhodnocuje podezření na průnik, jakmile se vyskytne, tak signalizuje poplach. IDS hlídá také útoky, které přicházejí zevnitř systému pomocí analýzy síťové komunikace a heuristické analýzy vzorců chování jednotlivých síťových entit.

7.3 Shrnutí

V této kapitole jsme diskutovali o typických řešeních používaných pro zabezpečení perimetru. Zabezpečením perimetru rozumíme soubor hardwarových, softwarových a programových bezpečnostních pravidel, která poskytují určité úrovně ochrany proti škodlivým aktivitám zvenčí. Dále jsme si popsali hlavní charakteristické vlastnosti firewallů a systémů pro detekci průniku uvedli jsme si klasifikaci těchto systémů podle různých hledisek.

8 Bezpečnost v bezdrátových sítích

8.1 Bezdrátové sítě

Bezdrátové sítě (**WLAN –** *Wireless Local Area Network*) jsou v dnešní době velmi populární, protože v rámci svého dosahu umožňují mobilitu a bezdrátové připojení koncových zařízení. To umožňuje využívat síťové služby a Internet pro datovou a hlasovou komunikaci téměř všude.

Výhody, které bezdrátová komunikace přináší, však zároveň představují i vysoká bezpečnostní rizika vyplývající z dostupnosti rádiového signálu v dosahu bezdrátové sítě. Právě proto je zabezpečení bezdrátového připojení tak aktuálním tématem.

Zabezpečení WLAN zahrnuje tyto důležité body:

- **zajištění důvěrnosti** čili šifrování obsahu sdělení,
- autentizaci uživatele čili řízení přístupu k síti.

Je třeba si uvědomit, že v sítích WLAN přicházejí útoky téměř všech typů zevnitř sítě.

8.2 Bezpečnost v bezdrátových sítích

Zabezpečení bezdrátových sítí zahrnuje tyto hlavní oblasti:

- **autentizaci,**
- **důvěrnost,**
- **správu klíčů.**

Autentizace je proces, během kterého se uživatel přihlašuje do WLAN sítě; výsledkem je pak úspěšné nebo neúspěšné přihlášení uživatele.

Důvěrnost je v sítích WLAN zajištěna pomocí šifrování. Nejpoužívanějšími šifrovacími algoritmy jsou **RC4** (**WEP**) a **AES** (**WPA2**).

Správa klíčů zahrnuje distribuci a generování klíčů.

8.3 Protokol WEP

Protokol **WEP** (*Wired Equivalent Privacy*) se používá jako volitelný doplněk standardu IEEE 802.11a/g/b a je určen pro řízení přístupu k WLAN s cílem zajistit důvěrnost přenášených dat.

Poskytuje služby autentizace a důvěrnosti:

- **Autentizace WEP**
  Autentizaci WEP lze provést dvěma metodami; jsou to:
  - otevřená autentizace,
  - sdílený klíč.

Systém otevřené využívá pouze SSID identifikátor sítě. SSID není heslo, nýbrž jen identifikátor (označení) bezdrátové sítě. *Bezdrátový přístupový bod* (**WAP** – *Wireless Access Point*) vysílá tento identifikátor periodicky vždy po několika sekundách.

V režimu otevřené autentizace odešle uživatel autentizační rámec 802.11, který obsahuje identifikační údaje daného uživatele. WAP kontroluje uživatelské ID a posílá zpět uživateli rámec potvrzující nebo odpírající přístup k síti WLAN.

Autentizace WEP se sdíleným klíčem využívá tajný 40bitový sdílený klíč, který je stejný pro všechny uživatele WLAN a je jim všem distribuován tajným způsobem. Při autentizaci se vlastně ověřuje totožnost síťové karty v koncovém zařízení.

- **Šifrování WEP**

Protokol WEP využívá symetrické šifrování RC4; pro šifrování dat je použit 64bitový nebo 128bitový klíč. Klíč se skládá z tajného 40bitového nebo 104bitového klíče a 24bitového *inicializačního vektoru* (**IV**).

Protokol WEP není odolný vůči známým typům útoků (monitorování aktivity, hrubá síla, opakovací útok atd.) a šifra RC4 byla prolomena již v roce 1996.

8.4 Protokol WPA

Protokol **WPA** (Wi-Fi Protected Access) byl přijat v roce 2002, aby překonal nedostatky protokolu WEP. Tento protokol byl dočasným řešením, protože v té době již započaly práce na novém standardu IEEE 802.11i (který byl přijat v roce 2004). Protokol WPA je z hlediska funkčnosti podmnožinou standardu 802.11i, takže implementace 802.11i nevyžaduje žádné změny technického vybavení (pouze změny softwaru nebo firmwaru).

Stejně jako protokol WEP, používá také i WPA šifru RC4, ale obsahuje nové bezpečnostní mechanismy. Hlavní součásti protokolu WPA jsou:

- *Temporary Key Integrity Protocol* (**TKIP**),
- *Message Integrity Check* (**MIC**),
- Řízení přístupu založené na standardu 802.1x s protokolem **EAP** (*Extensible Authentication Protocol*).

8.5 Protokol 802.11i (WPA2)

Standard 802.11i, označovaný též jako WPA2, spojuje mechanismy 802.1x a TKIP. Tento standard používá 128bitovou blokovou šifru AES.

Z hlediska uspořádání má 802.11i podobnou strukturu jako WPA a přichází s novými funkcemi, jako je například protokol CCMP a volitelná předautentizace, což zajišťuje rychlé a bezpečné přecházení mezi přístupovými body.

Hlavní mechanismy a bezpečnostní služby standardu 802.11i jsou:

- autentizace,
- šifrování,
- integrita.

8.6 Shrnutí

V této kapitole jsme si shrnuli bezpečnostní rizika spojená s používáním bezdrátových komunikačních sítí. V případě bezdrátových sítí LAN byla přijata různá bezpečnostní řešení, přestože některá z nich (např. protokol WEP) jsou snadno napadnutelná různými typy útoků. Nejvíce přijímané řešení pro zajištění různých bezpečnostních požadavků spočívá v použití standardu 802.11i (označovaného též jako WPA2).

9 Shrnutí

Tento dokument podává přehled o různých aspektech informační a síťové bezpečnosti. Je rozdělen do osmi částí.

První z nich je úvod, který se snaží čtenáře motivovat ohledně potřeby chránit data a síťovou komunikaci. Jsou zde uvedeny některé příčiny nedostatečné datové a síťové bezpečnosti spolu s různými základními mechanismy, jejichž použití by uživatelé měli zvážit pro svou vlastní ochranu. Dále je součástí této kapitoly základní klasifikace typů útoků.

Druhá část je věnována škodlivému softwaru a antivirům. Je zde představen pojem škodlivého softwaru a uvedena jeho klasifikace podle několika kritérií: způsobu šíření, metody instalace do systému, hlavní funkce atd. Kapitola dále popisuje různé metody léčení (čištění) infikovaného počítače. Jelikož tyto metody vyžadují detekci malwaru, jsou zavedeny různé strategie běžně používané pro detekci. Dokument obsahuje i základní informace o antivirovém softwaru, s důrazem na nutnost udržovat jej aktuální.

Třetí část je zaměřena na bezpečnostní služby a mechanismy. Nejdůležitější bezpečnostní služby (důvěrnost, integrita, dostupnost, autentizace, řízení přístupu, neodmítnutí a soukromí) jsou zde představeny spolu s bezpečnostními mechanismy nezbytnými pro poskytování těchto služeb. Kromě toho je zde vysvětlena souvislost mezi bezpečnostními službami a mechanismy.

Čtvrtá část obsahuje základní informace o různých kryptografických nástrojích používaných k zajištění informační bezpečnosti. Tato kapitola vysvětluje hlavní rozdíly mezi symetrickou kryptografií a kryptografií s veřejným klíčem, a srovnává oba typy algoritmů z hlediska jejich funkcí a výkonu. Poté je zde vysvětlen pojem hašovací funkce a požadavky na ni kladené, jakož i použití těchto funkcí v systému digitálního podpisu.

Pátá část je zaměřena na problematiku distribuce veřejného klíče. Je zde představen i pojem digitálních certifikátů, jelikož se jedná o nejrozšířenější metodu, jaká je k tomuto účelu využívána. Dále je stručně nastíněna problematika revokace certifikátů.

Šestá část obsahuje krátký popis dvou zabezpečených protokolů (TLS a S/MIME). Oba využívají kombinaci veřejného klíče a symetrické kryptografie, a vyžadují použití digitálních certifikátů.

Sedmá kapitola se zabývá zabezpečením perimetru. Jsou zde představeny základní prvky (firewally a systémy detekce průniku – IDS). Kromě toho jsou systémy IDS klasifikovány podle různých kritérií.

Osmá a poslední část je věnována bezpečnostním rizikům spojeným s používáním bezdrátových komunikačních sítí. Byla vyvinuta různá bezpečnostní řešení, přestože některá z nich (např. protokol WEP) jsou snadno napadnutelná různými typy útoků. Nejvíce přijímané řešení pro zajištění různých bezpečnostních požadavků spočívá v použití standardu 802.11i (označovaného též jako WPA2).