IMPROVET

Informačná a sieťová bezpečnosť

Miguel Soriano

Autori: Miguel Soriano
Názov diela: Informačná a sieťová bezpečnosť
Preložil: Miloš Drutarovský
Vydalo: České vysoké učení technické v Praze
Spracoval(a): Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, 166 27, Česká republika
Tel.: +420 2 2435 2084
Tlač: (iba elektronická)
Počet strán: 79
Vydanie: 1.

ISBN 978-80-01-05299-0

Oponent: Dušan Levický

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

Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie. Táto publikácia reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii.

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
+	Výhody
–	Nevýhody

ANOTÁCIA

Tento modul obsahuje informácie pre základnú orientáciu študentov v oblasti informačnej a sieťovej bezpečnosti.

CIELE

Modul poskytuje základné informácie o informačnej a sieťovej bezpečnosti, t.j. informácie ako je možné zabezpečiť informačnú a sieťovú bezpečnosť, ako chrániť osobný počítač a ako zmierniť dôsledky rôznych typov bezpečnostných ohrození. Modul tiež obsahuje stručný prehľad kryptografie s verejným kľúčom a symetrickej kryptografie. Záver kurzu obsahuje základné informácie o sieťovej bezpečnosti, zabezpečených protokoloch, firewalloch a systémoch na sledovanie prienikov (intrusion detection systems), ako aj informácie o štandardných riešeniach pre zabezpečenie bezpečnosti v bezdrôtových sieťach.

LITERATÚRA

[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

Informačná bezpečnosť nie je len o detekcii vírusov, zabránení prístupu hackerom a nezvyšovaní rozosielania nevyžiadaných hromadných mailov (spamov). Informačná bezpečnosť zahrňuje tiež prácu so zamestnancami a manažmentom firiem s cieľom zabezpečiť, aby boli oboznámení s aktuálnymi hrozbami a metódami ako chrániť využívané informácie a systémy. Pojmy informačná bezpečnosť, počítačová bezpečnosť a sieťová bezpečnosť sú často využívané ako ekvivalentné. Tieto oblasti často súvisia a sledujú spoločný cieľ – zabezpečenie dôvernosti, integrity a dostupnosti informácie; avšak existujú jemné odlišnosti, ktorými sa líšia.

Informačná bezpečnosť znamená ochranu informácii a informačných systémov pred neoprávneným prístupom, využívaním, odhalením, narušením, modifikáciou, analýzou, kontrolou, zaznamenávaním alebo deštrukciou.

Počítačová bezpečnosť je všeobecný pojem pre množinu nástrojov navrhnutých na ochranu spracovávaných a ukladaných dát ako aj na zmarenie útokov hackerov.

Sieťová bezpečnosť je všeobecný pojem pre množinu nástrojov navrhnutých na ochranu dát počas ich prenosu.

Pojem internetova bezpečnosť je často využívaný v spojitosti s Internetom. Tento pojem zahrňuje aj koncepciu zabezpečenia ochrany voči okolitému prostrediu (perimetric security), čo je všeobecný pojem pre množinu nástrojov navrhnutých na ochranu prostriedkov privátnych sieti voči ich využívaniu alebo zneužívaniu užívateľmi z iných sietí (externého prostredia).

Rozdiely medzi informačnou bezpečnosťou, počítačovou bezpečnosťou a sieťovou bezpečnosťou spočívajú v prístupe k subjektu, metodike a oblastiach na ktoré sa sústredia. Informačná bezpečnosť sa koncentruje na dôvernosť, integritu a dostupnosť dát nezávisle od ich formátu, ktorými môžu byť: elektronický, tlačený, prípadne iný formát. Počítačová bezpečnosť sa sústreďuje na zabezpečenie dostupnosti a správnej činnosti počítačových systémov bez ohľadu na typ počítačom uloženej alebo spracovávanej informácie. Sieťová bezpečnosť sa zameriava na ochranu dát počas ich prenosu.

1.2 Zdroje bezpečnostných rizík

Bezpečnostné riziká počítačových systémov a sietí sú omnoho širšie ako len dobré známe počítačové vírusy a eliminácia týchto rizík sa v súčasnosti stáva prioritou. Nová generácia vandalov a zlodejov dát v sieťovom prostredí nemusí mať fyzický kontakt s obeťou. Dáta je možné ľahko kopírovať, prenášať, modifikovať alebo zničiť. Dôsledkom uvedených skutočností je mimoriadna komplikovanosť kriminálneho prostredia: neexistencia stôp, identifikácia páchateľov je takmer nemožná, ich zadržanie je ešte komplikovanejšie a legálny rámec často neposkytuje adekvátne zabezpečenie spravodlivosti v tejto oblasti kriminality.

Povaha Internetu, ktorý pracuje v reálnom čase pridáva tomuto druhu kriminality ďalší rozmer – bezprostrednosť.

Aj keď existuje mnoho zdrojov bezpečnostných problémov, existujú tri hlavné zdroje slabých miest, ktoré vytvárajú bezpečnostné problémy:

- technická slabina,
- slabina bezpečnostných zásad,
- konifuračná slabina.

Samozrejme bolo by možné do zoznamu pridať aj slabiny človeka a prípadne aj ďalšie, našim cieľom je však predovšetkým koncentrácia na zdroje problémov, ktoré po ich identifikácii je možné manažovať, monitorovať a zlepšovať v rámci bezpečnostnej stratégie.

Technická slabina

Každé technické zariadenie má nejaké známe alebo neznáme prirodzené slabiny alebo zraniteľné miesta, ktoré môžu byť využité dostatočne motivovaným útočníkom. Niektoré slabiny sú široko publikované v médiách, pretože sú spojené s dobre známymi produktmi. Užívatelia by však nemali podľahnúť falošnej ilúzii, že nejaký produkt je bezpečný pokiaľ o jeho slabinách zatiaľ nepočuli. Skutočnosť, že sa nikto nezaujíma o prelomenie nejakého produktu neznamená nevyhnutne, že produkt je bezpečný.

Ako ďalšie môžme spomenúť nasledujúce slabiny:

- Internetové protokoly neboli pôvodne navrhnuté na dosiahnutie bezpečnosti. V súčasnosti sa v množstve produktov od rôznych dodávateľov využívajú najlepšie bezpečnostné praktiky a bezpečnostné služby s cieľom minimalizácie rizík, ktoré vyplývajú z prirodzenej podstaty využívaného komunikačného prostredia.
- Počítačové a sieťové operačné systémy. Bez ohľadu na výrobcu alebo či sa jedná o nejaký otvorený štandard alebo uzavretý firemný (proprietary)

produkt, každý *operačný systém (OS)* má zraniteľné miesta, ktoré je potrebné udržiavať s využitím záplat (patches), aktualizácií a ich dôsledného uplatňovania v praxi.

- Slabiny sieťových zariadení. Sieťové zariadenia môžu mať zraniteľné miesta, ktoré často nazývame bezpečnostné „diery“, a ktoré je možné zneužiť. Záplaty a aktualizácie OS by mali byť vždy dôsledne aplikované s cieľom eliminovať alebo zmierniť známe bezpečnostné problémy.

Slabiny bezpečnostných zásad

Slabina bezpečnostných zásad sú základným zdrojom problémov, ktorý vo firemnom prostredí neodvratne vedie k bezpečnostným ohrozeniam sieťových systémov. Nasledujúce príklady opisujú problémy zásad, ktoré môžu negatívne ovplyvniť firemný počítačový systém:

- Neexistencia písomných bezpečnostných zásad. Neexistencia dokumentovaného a prijatého plánu znamená, že bezpečnostné snahy sa vyvíjajú a sú uplatňované (ak vôbec) pokusným spôsobom.

- Neexistencia plánu na obnovu po haváriách. Bez vhodného plánu je úsilie v boji proti sieťovému útoku – alebo počas mimoriadnych udalostí ako napr. požiar, záplavy, alebo zemetrasenie – ponechané na posúdení a skúsenostiach konkrétneho personálu. Aj najlepšie zaškolený a najskúsenejší personál môže prijať nerozumné rozhodnutia, pokiaľ je konfrontovaný s neočakávanými katastrofickými udalosťami.

- Neexistencia zásad pre softvérové a hardvérové aktualizácie a zmeny. Bez ohľadu na to, či je motiváciou zvýšenie produktivity alebo obnova systému, každé pridanie alebo aktualizácia softvéru alebo hardvéru môže prispieť k vytvoreniu neočakávanej zraniteľnosti systému. Pridanie neautorizovaného bezdrôtového prístupového bodu do siete môže otvoriť „zadné vrátka“ na prístup k sieti a firemným prostriedkom. Podobne, neautorizovaný šetrič obrazovky môže zaznamenávať heslá, užívateľské ID a ďalšie informácie pre potenciálneho útočníka.

- Nedostatočné monitorovanie bezpečnosti**.** Dokonca aj v prípade vytvorenia zabezpečenej siete vedie nerealizovanie monitorovania prístupov do siete a prebiehajúcich procesov, alebo slabá kontrola používateľských účtov k vytvoreniu nových zraniteľných miest a rozšíreniu neautorizovaného využívania. Najhorším prípadom je nerozpoznanie, že takýto vážny únik nastal alebo dokonca stále prebieha.

- Politika zamestnanosti**.** Častá zmena zamestnancov, nižšie ako typické platy a nedostatočné možnosti školení môžu vplývať na bezpečnosť zamestnaním nových, neoverených a nedostatočne kvalifikovaných pracovníkov na pozície odborníkov a zodpovedných zamestnancov.

- Interné zásady**.** Ležérne pracovné postoje a praktiky často vytvárajú pokušenia a relatívne bezpečné prostredie pre oportunisov, ktorí sa chcú realizovať . Je to syndróm „Všetci sme tu ako jedna rodina“. Bohužiaľ, aj najlepšie rodiny majú

svoju čiernu ovcu. Podobne rivalita, ohováranie, mocenské boje alebo skryté boje v kolektíve môžu viesť k bezpečnostným problémom alebo odvedeniu pozornosti zamestnanov a následnému neodhaleniu bezpečnostných problémov.

Konfiguračná slabina

Mnoho sieťových zariadení má preddefinované nastavenia, ktoré preferujú vysoký výkon alebo ľahkú inštaláciu bez dôrazu na bezpečnostné dôsledky. Inštalovanie bez adekvátneho dôrazu na potrebu modifikácií týchto nastavení môže viesť k vážnym bezpečnostným problémom. Medzi najčastejšie konfiguračné problémy patria:

- neefektívny zoznam na riadenie prístupu neumožňuje blokovať nežiaduci prenos,
- preddefinované, chýbajúce alebo neaktualizované heslá,
- nevyužívané porty alebo služby sú ponechané aktívne,
- užívateľské ID a heslá sa vymieňajú v otvorenom (nezašifrovanom) tvare,
- slabo chránený alebo nechránený vzdialený prístup prostredníctvom Internetu alebo komutovaných sietí.

Sledovanie oznámení a doporučení dodávateľov v kombinácii s priemyselnými novinkami umožňuje identifikovať najčastejšie, všeobecne známe ohrozenia, pričom tieto zdroje často tiež obsahujú informácie o vhodných protiopatreniach na ich elimináciu.

1.3 Klasifikácia útokov

Bezpečnostné útoky môžu byť charakterizované ako rôzne druhy systematických aktivít s cieľom znížiť alebo narušiť bezpečnosť. Z tohto pohľadu môže byť útok definovaný ako systematické ohrozenie realizované entitou zámerným, premysleným a racionálnym spôsobom.

Počítačové siete môžu byť napadnuteľné mnohými hrozbami a množstvom útokov ako:

- Sociálne inžinierstvo, v rámci ktorého sa niekto pokúša získať prístup s využitím sociálnych prostriedkov (predstierajúc, že je legitímny užívateľ systému alebo administrátor, podvodným získanímtajnýché informácií a pod.)
- Wardialing (názov odvodený z filmu WarGames), v ktorom niekto využíva počítačový softvér a modem na hľadanie počítačov vybavených modemami, ktoré odpovedajú na výzvy a poskytujú potenciálnu cestu na prístup do firemných sietí.
- Útoky využívajúce odmietnutie služby (DoS - Denial-of-Service), zahŕňajú všetky typy útokov zameraných na ochromenie počítača alebo siete takým spôsobom, že legitímny užívateľ počítača alebo siete ich nemôže využívať.
- Protokolovo-orientované útoky, ktoré využívajú výhody známych (alebo neznámych) slabín v sieťových službách.
- Útoky na hostiteľský počítač, ktoré pri útoku využívajú zraniteľnosť niektorých operačných systémov alebo spôsobu, ako je systém inštalovaný a administrovaný.
- Hádanie hesiel; heslá sú postupnosti symbolov, zvyčajne pričlenené k užívateľskému menu, čím poskytujú mechanizmus na identifikáciu a autentizáciu konkrétneho užívateľa. Na takmer všetkých platformách si užívatelia heslá volia. Toto presúva bremeno bezpečnosti na koncového užívateľa, ktorý buď nepozná alebo sa nezaujíma o náležité bezpečnostné praktiky. Zvyčajne platí, že heslá, ktoré sa ľahko pamätajú je rovnako ľahké uhádnuť. Útočníci majú niekoľko spôsobov, ako môžu efektívne hádať jednoduché heslá a prekonať tak túto prekážku.
- Odpočúvania všetkými spôsobmi, zahrňujúce neoprávnené čítanie e-mailových správ, súborov, hesiel a ďalších informácií prostredníctvom odpočúvania sieťovej komunikácie.

Bezpečnostné útoky môžu byť rozdelené do dvoch hlavných kategórií:

- pasívne útoky,
- aktívne útoky.

1.4 Pasívne útoky

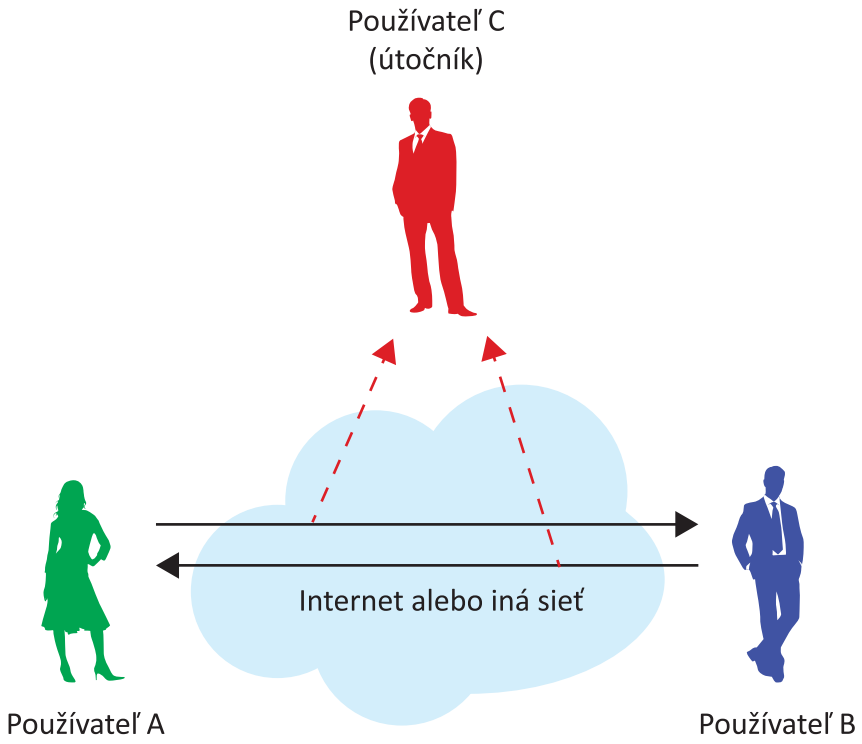
Pasívne útoky sa pokúšajú zistiť alebo využiť informáciu zo systému bez ovplyvňovania systémových prostriedkov. Pasívny útok je taký, pri ktorom útočník iba monitoruje komunikačný kanál. Pasívny útočník len ohrozuje dôvernosť dát. Povaha pasívnych útokov je založená na odpočúvaní alebo monitorovaní prenosu. Cieľom útočníka je získanie informácie, ktorá je prenášaná.

S obsahom správ a analýzou prevádzky súvisia dva typy pasívnych útokov:

- Odpočúvanie**.** Vo všeobecnosti väčšina sieťovej komunikácie prebieha v nezabezpečenom formáte (tzv. „otvorený text“), ktorý umožňuje útočníkovi, ktorý získal prístup k prostriedkom siete „načúvať“ alebo interpretovať (čítať) dáta vymieňané prostredníctvom siete. Schopnosť odpočúvajúceho monitorovať sieť je vo všeobecnosti najväčší bezpečnostný problém s ktorým je konfrontovaný administrátor v podniku. Bez využitia silných šifrovacích techník založených na kryptografii môžu byť dáta čítané inými osobami počas ich prenosu sieťou.

- Analýza prevádzky (traffic analysis)**.** Zodpovedá procesu odpočúvania a analýzy správ s cieľom odvodiť informáciu zo vzorov prenášaných dát. Môže byť realizovaná dokonca aj v prípade, že správy sú šifrované a nemôžu byť útočníkom dešifrované. Všeobecne platí, že čím väčší počet správ je možné sledovať alebo zachytiť a uložiť, tým viac informácií môže byť z prevádzky odvodených.

Nasledujúci obrázok ukazuje model pasívneho útoku.



Model pasívneho útoku

1.5 Aktívne útoky

Aktívne útoky sa pokúšajú modifikovať systémové prostriedky alebo ovplyvniť ich činnosť. Pri tomto type útoku sa útočník snaží vymazať, pridať, alebo nejakým iným spôsobom pozmeniť prenos informácie kanálom. Aktívny útočník ohrozuje integritu dát a autentifikáciu ako aj dôvernosť.

Aktívne útoky zahŕňajú určitú formu modifikácie dátového toku alebo vytvorenie falošného toku a je ich možné rozdeliť do šiestich kategórií:

- **Predstieranie identity (masquerade).** Je to typ útoku, pri ktorom útočník predstiera, že je autorizovaným užívateľom systému s cieľom získať prístup do systému alebo získať väčšie privilégia než na ktoré má autorizáciu.

- **Opakovanie.** Pri tomto type útoku je platný dátový prenos úmyselne alebo podvodne opakovaný alebo oneskorený. Toto je dosiahnuté buď pôvodcom správy alebo útočníkom, ktorý zachytil dáta a opäť preposlal, eventuálne ako časť útoku s predstieraním identity.

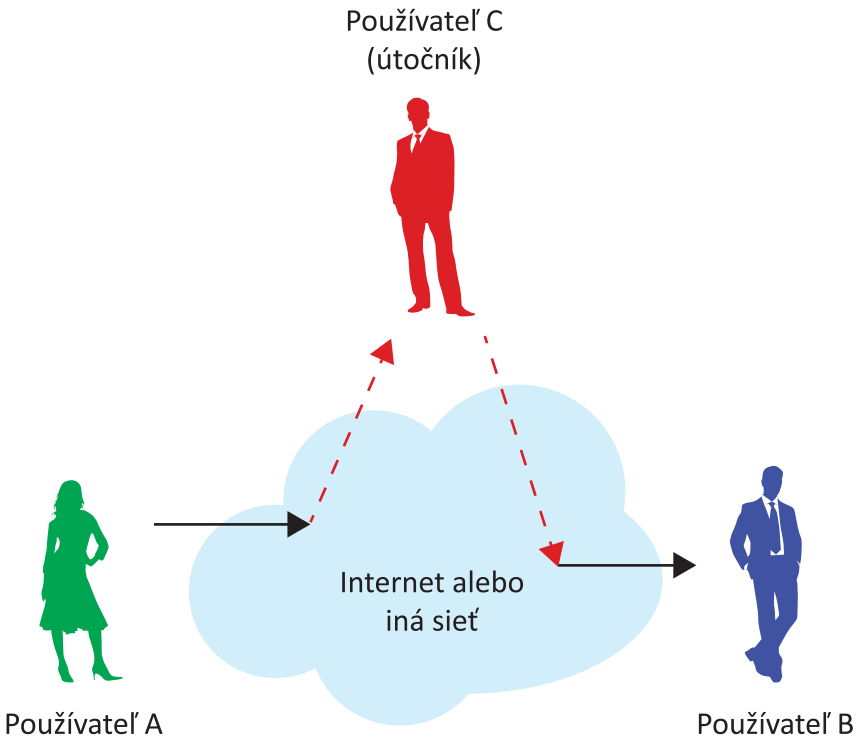
- **Modifikácia správ**. Útočník odstráni správu zo sieťovej komunikácie, pozmení ju a opätovne vloží do komunikačného kanála.

- *Útok zo stredu (MitM - Man in the Middle attack*). Pri tomto type útokov narušiteľ preruší komunikáciu medzi dvomi stranami, zvyčajne koncovým užívateľom a web stránkou. Útočník môže využiť získanú informáciu na krádež identity alebo iný typ podvodu.

- *Odmietnutie služby (DoS- Denial of Service)* a *distribuované odmietnutie služby (DDoS - Distributed Denial of Service) útoky*. DoS útok je incident počas ktorého je používateľovi alebo organizácii odoprená služba alebo prostriedok, ktoré by za normálnych okolností boli k dispozícii. Pri distribuovanom odmietnutí služby útočí veľký počet kompromitovaných systémov (niekedy nazývaných botnet) na jeden cieľ.

- *Pokročilé trvalé ohrozenie (APT - Advanced Persistent Threat)*. Je sieťový útok počas ktorého neautorizovaná osoba získa prístup do siete a ostáva dlhodobo neodhalená. Zámerom APT útoku je tajne získať dáta a nie spôsobiť škodu sieti alebo organizácii. APT útoky sú smerované na organizácie v sektoroch kde sa pracuje s cennými informáciami ako sú národná obrana, priemysel a finančný sektor.

Nasledujúci obrázok ukazuje príklad aktívneho útoku (konkrétne útok s pozmenením správy).



Aktívny útok s pozmenením správy

1.6 Útočníci: ciele a správanie

Útočník alebo votrelec je jednotlivec ktorý získa, alebo ktorý sa snaží získať neautorizované práva alebo neautorizovaný prístup do informačného systému.

Existuje viacero prístupov k spôsobu klasifikácie útočníkov. Základné vlastnosti použité pre klasifikáciu odlišných typov útočníkov môžu byť rozdelené do nasledujúcich skupín podľa:

- polohy útočníka vzhľadom k systému na ktorý útočí,
- odbornosti vedeného útoku,
- úmyslu, s ktorým k útoku pristupujú.

Z pohľadu polohy útočníka existujú dva odlišné typy útočníkov:

- vnútorný útočník (insider),
- vonkajší útočník (outsider).

Vnútorný útočník je obvykle osoba, ktorá má prístup do internej počítačovej siete a je teda legitímny užívateľ, ktorý sa pokúša získať neautorizovaný prístup k dátam, systémovým prostriedkom a službám alebo zneužíva autorizované dáta.

Vonkajší útočník je obvykle osoba, ktorá nemá autorizovaný prístup do internej počítačovej siete a ktorá chce preniknúť do tejto siete využívajúc jej zraniteľné miesta alebo bezpečnostné diery.

Podľa odbornosti vedeného útoku možno útočníkov rozdeliť na:

- amatérov,
- profesionálov.

Skupina amatérov vykonáva menej nebezpečné útoky ako skupina profesionálov. Tieto útoky sú adekvátne ich nízkej úrovni vzdelania a vybavenia technickými prostriedkami.

Skupina profesionálov je zvyčajne tvorená špičkovými počítačovými odborníkmi, ktorí majú prístup k špecializovaným prostriedkom a ktorí sú odborne vyškolení a skúsení. V praxi to znamená, že sú schopní uskutočniť veľmi nebezpečné útoky s vážnymi dôsledkami pre počítačové systémy a siete.

Veľmi diskutovanou otázkou je delenie útočníkov na:

- hackerov,
- crackerov.

Hacker je osoba s dobrými resp. výbornými IT znalosťami, ktorá sa často podieľa na významných softvérových projektoch a ktorej vedomosti a know-how sú užitočné pri hľadaní zraniteľných miest a bezpečnostných dier navrhovaných systémov. Činnosť hackera je prospešná a užitočná. Existujú dokonca hackerské kódexy, ktoré opisujú ich správanie.

Cracker je osoba ktorá dokáže obchádzať protipirátske ochrany počítačových programov a ktorá využíva svoje znalosti neetickým spôsobom. Existuje však viacero definícií tejto skupiny útočníkov, ktoré zdôrazňujú odlišné stránky ich aktivít.

Existujú však aj iné skupiny útočníkov, najväčšia z nich je skupina **scriptkiddies**. Táto skupina útočníkov je tvorená užívateľmi s nízkou úrovňou IT zručností. Útoky realizované uvedenými útočníkmi využívajú skripty obsahujúce kódy využívajúce zraniteľnosť IS. Útočníci aplikujú tieto skripty bez hlbšej analýzy, avšak škodlivé efekty týchto aktivít zvyčajne majú vážne následky. Táto forma útokov je veľmi častá a nebezpečná.

1.7 Ako sa môžme chrániť?

Táto sekcia odporúča domácim užívateľom nasledujúce praktiky:

Používajte silné heslá

Heslá sú často jedinou ochranou používanou v systéme. Užívateľské ID je iba nejaké meno a neumožňuje overiť identifikáciu, avšak heslo priradené k ID užívateľa funguje ako identifikátor. Heslá sú tak kľúčmi do siete a ako také by mali byť adekvátne chránené. Firewally a systémy na detekciu prienikov nemajú žiadny význam ak boli Vaše heslá kompromitované.

Silné heslo je také, ktoré nemôže byť nájdené v žiadnom slovníku – anglickom ani zahraničnom. Znamená tiež, že heslo nemôže byť ľahko uhádnuteľné. Dlhšie heslá sú ťažšie odhaliteľné alebo prelomiteľné ako kratšie.

Nasledujúci zoznam pravidiel by mal byť využívaný pri vytváraní silných hesiel:

- **Použite nezmyselnú kombináciu písmen:** Najlepšie heslá sú také, ktoré pôsobia ako úplne nezmyselné. Napríklad ak vezmeme anglickú frázu „Don't expect me to behave perfectly and wear that sunny smile" a použijeme iba prvé písmená každého slova, naše heslo sa bude javiť ako *demtbpawtss*.

- **Použite kombináciu malých a veľkých písmen:** Heslá by mali obsahovať nejaké veľké písmená umestnené niekde inde ako na začiatku a mali by obsahovať aj číslice.

- **Dlhšie heslá sú lepšie:** Heslo by malo mať dĺžku aspoň 8 znakov.

- **Heslá by sa mali periodicky meniť:** Dokonca aj najlepšie heslá by sa mali pravidelne meniť (povedzme každých 60 dní), aby sa zabránilo ich dlhodobému využívaniu v prípade, že sú prelomené. Mnoho operačných systémov umožňuje nastavenie tohto pravidla pre každého užívateľa. Užívateľ zvyčajne posudzuje takúto prax ako nepohodlnú, ale dodržiavanie tohto pravidla poskytuje zvýšenú bezpečnosť.

- **Nastavujte nové heslá namiesto opakovaného používania stále tých istých**: Tie isté heslá by nemali byť užívateľom využívanév rámci jedného roka alebo dokonca počas 18 mesiacov.

- **Nepoužívajte znaky klávesnice, ktoré nasledujú na klávesnici za sebou**: Je potrebné sa vyhnúť využívaniu hesiel ako qwerty, 12345678, alebo asdfghj, Aj keď takéto heslá sa zdajú nezmyselné, obsahujú vzory znakov nasledujúcich na klávesnici za sebou a programy na prelamovanie hesiel ich zistia v priebehu niekoľkých sekúnd.

- **Zaobchádzajte s heslami ako s prísne tajnými informáciami**: Všetky heslá by mali byt chránené a nemali by sa zdieľať. Mnohí užívatelia si zapisujú heslá na poznámkové štítky pripnuté k počítaču alebo ich uložia pod ich klávesnicu. Týmto nikoho neoklame!

Heslá na úrovni koreňových (root) a administrátorských práv sú pre votrelca kľúčmi k ovládnutiu systému. Systémoví administrátori s *koreňovými* právami, t.j. bez akýchkoľvek obmedzení a možnosťami realizovať akékoľvek zmeny, by mali mať najsilnejšie heslá a používať najprísnejšie pravidlá na ich zmenu a kontrolu ich opätovného používania. Je doporučené dodržiavať nasledujúce pravidlá:

- Zapísať všetky koreňové heslá a bezpečne ich uložiť: Ak potom administrátor nie je na nejakú dobu dostupný alebo náhle ukončí pracovný pomer, heslá nebudú navždy stratené. Existujú síce programy na obnovu hesiel, avšak v prípade krízových situácii nie je dobré sa na nich spoliehať.

- Zmeniť VŠETKY užívateľské heslá ak existuje podozrenie, že koreňové heslo bolo kompromitované**:** Ak neznáma osoba mala prístup k heslám s koreňovými alebo administrátorskými právami, je nemožné garantovať, že nedošlo ku krádeži všetkých hesiel.

Podobne, ak nejaký užívateľ má podozrenie, že jeho heslo bolo ukradnuté alebo kompromitované, užívateľ by mal heslo okamžite zmeniť a oznámiť to zodpovednej osobe vo firme.

Vždy používajte softvér na antivírusovú ochranu

Antivírusový softvér nie je vždy 100-percentne efektívny, ale je lepší ako vôbec žiadna ochrana. Aktivita väčšiny bežných vírusov nie je pre užívateľa jasne viditeľná, a teda ak užívateľ nemá žiadny antivírusový softvér, pravdepodobne ani nezistí, že jeho počítač je infikovaný.

Antivírusový softvér sa skladá z dvoch častí: *skenovacieho jadra* (*scanning engine*) a súborov s príznakmi (*signature files*). Je nevyhnutné pravidelne aktualizovať skenovacie jadro ako aj súbory s príznakmi, bez aktualizácie stráca antivírusový softvér efektivitu. Softvérový program má zvyčajne príkaz na *aktualizáciu*, prípadne je možné získať aktualizácie z web stránky výrobcu softvéru.

Skenovacie jadro informuje softvér ako a čo má skenovať, súbor s príznakmi je v podstate databáza známych vírusov a ich účinkov. Skenovacie jadro porovnáva súbory na počítači so vzormi známych vírusov v súbore príznakov. Súbor príznakov obsahuje vzory známych príznakov. Antivírusový softvér má tendenciu generovať falošné alarmy, čo je relatívne malou nepríjemnosťou za ochranu, ktorú užívateľovi poskytuje.

Keď sa vo svete objavia nové vírusy, výrobcovia antivírusových softvérov poskytujú aktualizácie súborov s príznakmi na zahrnutie nových variantov vírusov. Občas je potrebné aktualizovať aj skenovacie jadro. Ak je jedna časť programu aktualizovaná a iná nie, celok jednoducho nefunguje správne.

Na dosiahnutie maximálnej úrovne ochrany je nevyhnutné inštalovať antivírusový softvér na individuálne pracovné stanice ako aj na všetky servery a ďalšie počítače pripojené do siete. Je to jediný spôsob ako detegovať vírusy vo všetkých vstupných bodoch. Všetky prenosné média ako USB kľúče, CD média, ... by pred použitím v systéme mali byť preskenované. Ak je antivírusový softvér inštalovaný

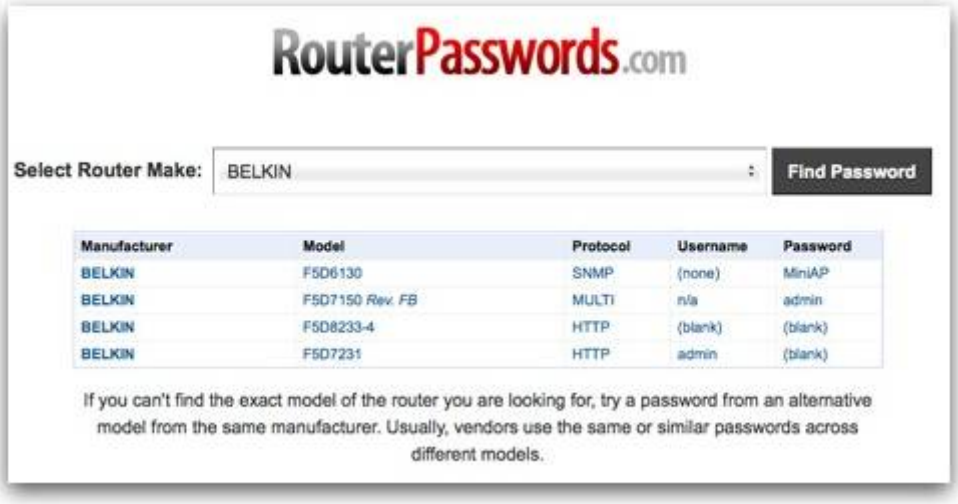
na serveroch realizujúcich Internetové brány (gateways), softvér môže zachytiť vírusy prichádzajúce z vonkajšieho prostredia.

Vždy zmeňte prednastavené konfigurácie

Inštalácia systému z dodaných médií a ponechanie štandardnej prednastavenej konfigurácie je pravdepodobne jedna z najčastejších chýb, ktorej sa užívatelia dopúšťajú pri konfigurovaní siete. Štandardné konfigurácie majú často prednastavené administrátorské účty a heslá ktoré hackeri na celom svete poznajú. Toto pravidlo platí aj pre smerovače (routers), rozbočovače (hubs), prepínače (switches), operačné systémy, emailové systémy, a ďalšie serverové aplikácie ako napr. Databázy a web servery.

Preddefinované konfigurácie obsahujú často okrem známych hesiel aj viaceré bezpečnostné diery, ktoré by mali byť ošetrené dostupnými bezpečnostnými záplatami. Pred uvedením každého počítača do prevádzky by mali byť mená preddefinovaných účtov a ich prístupové heslá zmenené a mali by byť tiež aplikované všetky bezpečnostné záplaty. Časová investícia v tejto fáze inštalácie môže ušetriť mnoho času a problémov v budúcnosti.

Nasledujúci obrázok ukazuje príklad hesiel, ktoré bývajú prednastavené na niektorých smerovačoch.



Príklad prednastavených hesiel smerovača

Používajte firewally

Užívateľom sa odporúča využívať nejaký firewallový nástroj. Votrelci sústavne skenujú systémy domácich užívateľov a hľadajú známe zraniteľné miesta. Sieťové firewally (založené na softvérovej alebo hardvérovej platforme) poskytujú určitý stupeň ochrany voči týmto útokom, Avšak žiadny firewall nemôže detegovať alebo zastaviť všetky útoky a preto nie je dostatočné nainštalovať firewall a následne ignorovať ďalšie bezpečnostné opatrenia.

Neotvárajte neznáme emailové prílohy

Pred otvorením ľubovoľnej emailovej prílohy sa uistite, že poznáte pôvodcu dát. Nestačí, že Vám email prišiel zo známej adresy. Napríklad vírus Melissa sa rozšíril práve preto, že prichádzal zo známych adries. Škodlivý (malicious) kód môže byť šírený prostredníctvom počítačových hier alebo inak lákavých programoch.

Počas otvárania priloženého súboru je dôležité zachovávať nasledujúce procedúry:

1. uistiť sa, že definície vírusov sú aktuálne,
2. uložiť súbor na pevný disk,
3. preskenovať súbor použitím antivírusového softvéru,
4. otvoriť súbor.

Na zvýšenie ochrany je možné pre otvorením súboru odpojiť počítač od siete.

Dodržiavanie týchto krokov zredukuje, avšak nie úplne eliminuje možnosť, že nejaký škodlivý kód nachádzajúci sa v prílohe sa môže rozšíriť z Vášho počítača na ďalšie.

Nespúšťajte programy získané z neznámych zdrojov

Nikdy nespúšťajte nejaký program pokiaľ neviete, že bol vytvorený osobou alebo firmou, ktorej dôverujete. Neposielajte programy neznámeho pôvodu priateľom alebo spolupracovníkom len preto, že sú zábavné – môžu obsahovať trójske kone.

Aplikujte dostupné bezpečnostné záplaty na všetky aplikácie vrátane operačných systémov

Predajcovia softvéru zvyčajne poskytujú záplaty pre ich softvér po objavení nového zraniteľného miesta. Dokumentácia väčšiny produktov opisuje metódu ako získať aktualizácie a záplaty.

Niektoré aplikácie automaticky preverujú dostupnosť aktualizácii, ak takúto možnosť softvér nemá, je absolútne nevyhnutné periodicky kontrolovať dostupnosť aktualizácií.

Vypnite počítač alebo ho odpojte od siete ak ho nepoužívate

Vypnite počítač alebo odpojte jeho sieťové rozhranie pokiaľ ho nepoužívate. Útočník nemôže na Váš počítač útočiť ak počítač nie je zapnutý alebo je kompletne odpojený od siete.

Realizujte pravidelné zálohy kritických dát a vytvorte štartovací disk

Vytvorte záložné kópie dôležitých súborov na vymeniteľných médiách. Používajte softvérové zálohovacie nástroje ak sú dostupné, a uložte záložné disky niekam mimo počítača. Okrem toho, na zabezpečenie obnovy v prípade bezpečnostných narušení alebo poruchy pevného disku, je veľmi výhodné vytvoriť štartovací disk na CD, ktorý v prípade takejto udalosti pomôže ľahko obnoviť inštaláciu počítača. Samozrejme takéto CD by malo byť vytvorené pred bezpečnostným incidentom.

1.8 Zhrnutie

V tejto kapitole boli ako prvé uvedené niektoré dôležité pojmy: informačná bezpečnosť, počítačová bezpečnosť a sieťová bezpečnosť, ako aj rozdiely medzi týmito pojmami. Následne boli prezentované niektoré príčiny nedostatočnej ochrany informácií a rozdelené bezpečnostné útoky a typy útočníkov na základe rôznych kritérií. V závere boli opísané najvhodnejšie postupy, ktoré domácemu užívateľovi umožňujú zvýšiť úroveň jeho ochrany.

2 Škodlivý softvér a antivírusy

2.1 Pojem škodlivý softvér (malvér)

Škodlivý softvér (**malvér**) je všeobecný pojem označujúci ľubovoľný škodlivý alebo otravný softvér inštalovaný v systéme a navrhnutý tak, aby umožnil zneužiť počítač vykonaním nežiaducich činností bez vedomia užívateľa.

Spustenie malvéru môže spôsobiť rozvrat činnosti počítača a môže byť tiež využité na získanie citlivých informácií alebo získanie neautorizovaného prístupu do počítačového systému. Malvér nie je to isté ako chybný softvér, ktorý má síce legitímne využitie, obsahuje však škodlivé chyby o ktorých sa nevedelo pred jeho uvoľnením.

V skutočnosti sú počítačové vírusy podmnožinou v rámci väčšej rodiny malvéru podobne, ako ďalšie príklady červov (worms), trójskych koňov, advéru (adware), odpočúvacieho softvéru - spajvéru (spayware), rootkitov (rootkits) a pod....

V súčasnosti je väčšina malvéru šírená prostredníctvom Internetu. Jedna z najbežnejších metód je známa ako „spusť stiahnutím“ (“drive-by download”). Realizuje stiahnutie a spustenie škodlivého súboru napríklad z Webu alebo spustením prílohy prijatej prostredníctvom emailu, napríklad ako škodlivý PDF súbor. V mnohých prípadoch je užívateľ oklamaný aby veril, že nejaký program alebo dáta sú pre neho užitočné, napr. ako softvér, ktorý prehráva video. V iných prípadoch je infikovanie maskované a užívateľ musí navštíviť Web stránku, ktorá využíva zraniteľnosti Web prehliadača na stiahnutie a spustenie malvéru. Okrem toho, takmer všetky internetové protokoly, ako napr. P2P alebo priame zasielanie správ (instant messaging), môžu byť využité na distribúciu malvéru. Je tiež dôležité si uvedomiť, že malvér sa môže šíriť prostredníctvom médií na ukladanie dát, napr. šírenie prostredníctvom USB kľúčov je dnes veľmi bežné.

2.2 Antivírusový softvér

Antivírus alebo antivírusový softvér je využívaný na prevenciu, detekciu a odstránenie malvéru vrátane počítačových vírusov, počítačových červov, trójskych koňov, spajvéru, advéru a ďalších. Na zabezpečenie efektívnosti antivírusového softvéru je potrebná jeho pravidelná aktualizácia. Bez nej nie je chopný zabezpečiť kvalitnú ochranu voči novým vírusom.

Odstránenie vírusu je pojem označujúci vyčistenie počítača. Existuje niekoľko metód odstraňovania:

- odstránenie kódu v infikovanom súbore, ktorý zodpovedá vírusu,
- odstránenie infikovaného súboru,
- karanténa infikovaného súboru, čo predstavuje jeho presunutie do oblasti, kde nemôže byť spúšťaný.

V praxi sú využívané rôznorodé stratégie.

Detekcia na základe vzorov zahrňuje hľadanie známych dátových vzorov (podpisov) vo vykonateľnom kóde. Vírusy sa množia nakazením „hostiteľskej aplikácie“, t.j. prekopírovaním časti vykonateľného kódu do existujúceho programu. Aby sa zabezpečila ich plánovaná funkčnosť, vírusy sú naprogramované tak, aby nenakazili ten istý súbor viac krát. Dosahujú to vložením postupnosti bajtov do nakazenej aplikácie, ktoré umožňujú overiť, či aplikácia už bola nakazená. Táto postupnosť bajtov sa nazýva vzor alebo podpis vírusu (virus signature). Antivírusové programy využívajú tento jedinečný podpis každého vírusu na jeho detekciu. Táto metóda sa nazýva detekcia na základe vzorov a je najstaršou metódou využívanou antivírusovými softvérmi. Táto metóda však neumožňuje detegovať vírusy, ktoré zatiaľ neboli analyzované tvorcom antivírusového softvéru. Okrem toho, tvorcovia vírusov do nich často vkladajú rôzne techniky maskovania, čo spôsobuje, že detekcia na základe podpisu vírusu je komplikovaná alebo často aj nemožná. Na detekciu takýchto ohrození môže byť využitý heuristický prístup.

Jeden z heuristických prístupov využíva všeobecné podpisy a umožňuje identifikáciu nových alebo variantov existujúcich vírusov hľadaním škodlivého kódu, alebo malých modifikácií takého kódu v analyzovaných súboroch. Heuristická metóda zahrňuje analýzu správania aplikácie s cieľom odhaliť aktivity podobné tým, ktoré majú známe vírusy. Tento typ antivírusových programov tak umožňuje odhaliť vírusy dokonca aj v prípadoch, keď antivírusová databáza nebola aktualizovaná. Na druhej strane heuristické prístupy majú náchylnosť generovať falošné alarmy.

Bez ohľadu na užitočnosť antivírusového softvéru môže mať jeho využívanie aj nevýhody. Antivírusový softvér môže ovplyvniť výkonnosť počítača. Neskúsení užívatelia môžu mať problém porozumieť výzvam a možnostiam, ktoré im antivírusový softvér prezentuje. Ich nevhodné rozhodnutia môžu viesť k narušeniu bezpečnosti.

2.3 Rozdelenie malvéru

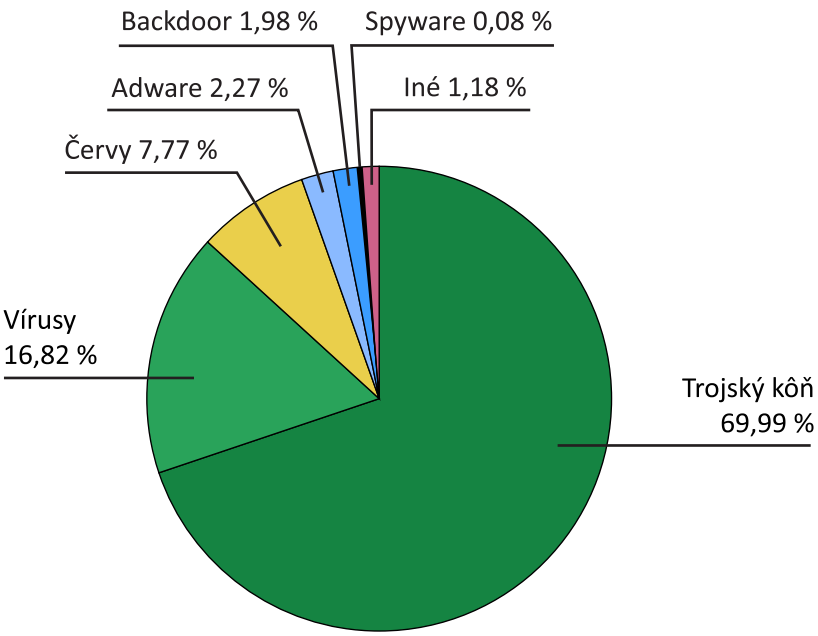
Malvér je možné rozdeliť rôznymi spôsobmi na základe rozdielnych kritérií: mechanizmu šírenia, metód inštalácie do systému, spôsobu vzdialeného riadenia, a pod. V súčasnosti existujúce malvéry majú veľa vlastností a tak sú zvyčajne delené na základe niektorej ich hlavnej vlastnosti. Môže to byť napr. trójsky kôň so schopnosťami rootkitu, ktorý je schopný ukrývať sa aj pred pokročilými užívateľmi a bezpečnostnými protiopatreniami. Môže tiež byť využitý na prihlásenie do siete nakazených počítačov, ktoré sú vzdialene riadené. Zároveň môže zobrazovať reklamy a monitorovať klávesnicu, takže by mohol byť súčasťou rodín softvérov typu advér a monitorov klávesnice (keyloggers). Takže bol by to trójsky kôň-rootkit-botnetadvér-monitor klavesnice … Všetko v jednom ! V skutočnosti je tento príklad celkom bežný.

Prvé rozdelenie malvéru je založené na základe potreby hostiteľského súboru na jeho šírenie.

Nasledujúce štyri druhy malvéru zodpovedajú malvéru, ktorý na svoje šírenie vyžaduje hostiteľské súbory:

- skryté vstupy (trap doors),
- logické bomby (logic bombs),
- trójske kone (trojan horses),
- vírusy (viruses).

Nasledujúci obrázok ukazuje rozdelenie malvérov podľa kategórií (zdroj: Panda Security)



Rozdelenie malware do kategórií
16. marca, 2011

zdroj: Panda Security

Typy malvérov

Dva druhy malvéru, ktoré na šírenie nevyžadujú hostiteľský súbor sú:

- červy (worms),
- zombie (zombies).

Skryté vstupy sú utajené vstupy do programu, ktoré umožňujú získať prístup do systému obchádzaním mechanizmov bezpečnosti. Uvedené vstupy boli používané programátormi najmä pri ladení a testovaní programov. Skryté vstupy umožňovali obchádzať najmä mechanizmy autentizácie počas ladenia a testovania programu z dôvodu urýchlenia týchto procesov, a programátor tak získal špeciálne privilégia. Tieto skryté vstupy vyhľadáva škodlivý softvér a obchádza mechanizmy bezpečnosti, čím vzniká vážne softvérové ohrozenie počítačového systému.

Logické bomby predstavujú najstarší druh škodlivého softvéru, ktorý predstavuje softvérové ohrozenie. Je to softvérintegrovaný do legitímneho programu, ktorý sa aktivizuje pri splnení určitých podmienok. Príkladom takýchto podmienok môže byť prítomnosť, resp. neprítomnosť určitého typu súboru v predvolený deň, týždeň, špecifický dátum alebo štart určitej aplikácie. Logická bomba môže spôsobiť straty, resp. škody v IS, napr. vymazať určité súbory, zastaviť prebiehajúci výpočet, atď.

Trójske kone sú programy, resp. príkazy, ktoré vykonávajú určité užitočné funkcie, a ktoré okrem toho vykonávajú v pozadí nežiaduce a deštrukčné účinky, napr. vymazanie dát. Špeciálnym prípadom tohto typu škodlivého softvéru je

špehovací softvér (spajvér), ktorý zbiera heslá zadávané z klávesnice, zisťuje aké stránky sú navštevované, aký softvér je používaný a odosiela uvedené informácie po Internete na zadané miesta.

Vírusy sú programy, ktoré sú schopné pripojiť sa k inému programu, resp. súboru a vykonávať nežiaduce činnosti. Na svoje šírenie vyžadujú iné súbory, ktoré sú vírusom modifikované. Vírusy majú teda schopnosť napádať iné súbory, šíriť sa a narušať IS.

Červ má schopnosť šíriť sa z jedného počítačového systému na iný počítačový systém pokiaľ sú tieto systémy pripojené do počítačovej siete. Šírenie červov sa najčastejšie realizuje pomocou emailových klientov, resp. cez určité služby, ktoré ponúkajú týmto klientom.

Zombia je druh škodlivého softvéru, ktorý sa šíri cez počítačovú sieť (Internet) a po úspešnom prieniku do počítačového systému umožňuje prevziať diaľkovú kontrolu nad napadnutým systémom. Niekoľko počítačov napadnutých rovnakým druhom tohto škodlivého softvéru vytvára botnet. Botnet možno riadiť z jedného vzdialeného počítača tak, aby vykonávali rovnaké príkazy. To umožňuje realizovať útok typu *DDoS*.

2.4 Životný cyklus vírusu

Životný cyklus vírusu tvoria štyri fázy:

- fáza nečinnosti (formant phase),
- fáza šírenia (propagation phase),
- fáza aktivácie (triggering phase),
- výkonná fáza (execution phase).

Vo fáze nečinnosti je vírus v kľudovom stave, teda neprejavuje žiadnu aktivitu. Je potrebné poznamenať, že nie každý druh vírusu má túto fázu.

Vo fáze šírenia vírus umiestňuje svoju identickú kópiu do iného programu, resp. do určitého sektora disku. Teda každý infikovaný program obsahuje klon vírusu, ktorý je schopný sa ďalej šíriť.

Vo fáze aktivácie je vírus uvedený do aktívneho stavu. Táto fáza je inicializovaná rôznymi okolnosťami, resp. stavmi infikovaného programu.

Vo výkonnej fáze vírus vykonáva činnosť, ktorá bola naprogramovaná pri vytvorení vírusu. Ide obvykle o deštrukčné činnosti, ktoré vedú k stratám a škodám v napadnutom počítačovom systéme.

2.5 Zhrnutie

V tejto kapitole bol vysvetlený pojem škodlivého softvéru – malvéru, ktorý bol rozdelený na základe rôznych kritérií: spôsobu šírenia, metód inštalácie, hlavnej vlastnosti a pod. Boli tiež opísanéfázy životného cyklu vírusov. Okrem toho kapitola opisuje niekoľko techník používaných na vyčistenie infikovaného počítača. Keďže tieto techniky vyžadujú detekciu malvéru, boli uvedené rôzne prístupy typicky využívané na jeho detekciu.

3 Služby bezpečnosti a mechanizmy bezpečnosti

3.1 Služby bezpečnosti

Služba bezpečnosti je taká služba, ktorá zabezpečí primeranú bezpečnosť systémov alebo prenosov dát. Služby bezpečnosti sa realizujú pomocou bezpečnostných mechanizmov v súlade s bezpečnostnou stratégiou.

Počas viac ako dvadsiatich rokov boli *dôvernosť(confidentiality), integrita (integrity) a dostupnosť (availability)* (známe tiež ako **CIA** triáda) základnými princípmi informačnej bezpečnosti.

Neskôr boli k týmto základným CIA atribútom pridané ďalšie elementy informačnej bezpečnosti. Týmito elemntami sú **autentizácia (authentication), riadenie prístupu (acccess control), ochrana proti odmietnutiu (non-repudiation), and ochrana súkromia (privacy).** Avšak táto klasifikácia je medzi odborníkmi na bezpečnosť stále diskutovaná.

3.2 Dôvernosť

Dôvernosť je vlastnosť, ktorá zaručuje, že informácia nebude dostupná neautorizovaným subjektom (organizáciám, ľuďom, počítačom, procesom). Nikto nebude schopný čítať dáta okrem špecifického subjektu (alebo subjektov) pre ktorý (ktoré) boli dáta určené. Informácia zahrňuje dátový obsah, veľkosť, existenciu, komunikačné parametre a pod.

Dôvernosť je požadovaná ak:

- dáta sú ukladané na nejaké médium (napr. na pevný disk), ktoré môže byť čítané neautorizovaným subjektom,
- dáta sú archivované pomocou zariadenia (napr. na pásku), ktorá sa môže dostať do nepovolaných rúk,
- dáta sú prenášané prostredníctvom nezabezpečených sietí.

Okrem toho, vezmúc do úvahy rafinovanosť a schopnosti motivovaných útočníkov, musí byť v súčasnosti dôvernosť všetkých citlivých dát zabezpečovaná pomocou **kryptografických techník**. Podobne ako pri zabezpečení integrity dát vyžaduje zabezpečenie dôvernosti dobŕe zvládnutie podstaty vhodných algoritmov a kľúčov.

3.3 Integrita dát

Integrita dát je ochrana dát voči vytvoreniu, pozmeneniu, vymazaniu alebo nahradeniu neautorizovanými subjektmi (organizáciami, ľuďmi, počítačmi, procesmi). Narušenie integrity je vždy spôsobené aktívnymi útokmi. Presnejšie, integrita súvisí s dôveryhodnosťou informačných zdrojov.

Integrita dát je zárukou nemennosti: dáta (prenášané alebo uložené) neboli nepozorovane modifikované či už poruchou alebo zámernou škodlivou aktivitou. Samozrejme takéto zaistenie je nevyhnutné v každom druhu podnikania alebo v prostredí elektronického obchodovania, je však nvyhnutné aj v mnohých iných aplikáciách a činnostiach.

Integrita informačného systému zahrňuje iba udržiavanie informácie o jeho stave – dobrý alebo zlý, bez ohľadu na tom, čo bolo zo systému vyslané alebo do neho nahrané. Na zmarenie zámernej manipulácie s dátami nejakým motivovaným útočníkom, ktorého cieľom je modifikácia dát s cieľom ich zneužitia, je potrebné využiť **kryptografické techniky.** Preto musia byť pri spolupráci medzi entitou ktorá poskytuje integritu dát a entitou, ktorá ju využíva, použité vhodné algoritmy a kľúče.

3.4 Dostupnosť

Dostupnosť je vlastnosť mať včasný prístup k informáciám. Napríklad porucha pevného disku alebo DoS útok spôsobujú prerušenie dostupnosti. Akékoľvek oneskorenie, ktoré presahuje očakávanú úroveň oneskorenia systému môže byť označené ako prerušenie dostupnosti. Informačný systém, ktorý nie je dostupný keď je potrebný, je prinajmenšom tak zlý ako žiadny. Situácia môže byť ešte horšia podľa toho, ako je organizácia na fungovaní počítača a komunikačnej infraštruktúry závislá.

Dostupnosť, podobne ako ďalšie aspekty bezpečnosti, môže byť ovplyvnená čisto technickými problémami (napr. nefunkčnosť časti počítača alebo komunikačného zariadenia), prírodnými vplyvmi (napr. vietor alebo záplavy), alebo zásahom človeka (neúmyselným alebo zámerným).

Aj keď relatívne riziká spojené s uvedenými príčinami závisia na konkrétnych súvislostiach, všeobecným pravidlom je že človek je ich najslabším článkom. Preto je kritická predovšetkým schopnosť a ochota každého užívateľa využívať dátový systém bezpečne.

3.5 Autentizácia

Autentizačná služba je zameraná na zabezpečenie, že komunikujúcim entitám je poskytnutá záruka a informácia o príslušných identitách komunikujúcich partnerov (ľudí, počítačov, procesov).

V prípade jednoduchej správy, ako napr. varovania alebo signálu alarmu, je úlohou autentizačnej služby zaručiť prijímateľovi, že správa je zo zdroja, z ktorého tvrdí, že je.

Prípady prebiehajúcej komunikácie, akým je napr. pripojenie terminálu ku vzdialenému počítaču, sú spojené s dvoma aspektmi. Prvý, v čase nadviazania spojenia služba zaisťuje, že dve komunikujúce entity sú autentické, teda každá entita je tá, za ktorú sa vydáva. Druhý, služba musí zabezpečiť, že do komunikácie nezasahuje tretia entita tak, že predstiera, že je jednou z dvoch oprávnených strán, s cieľom neautorizovaného vysielania alebo príjmu.

3.6 Riadenie prístupu

Riadenie prístupu je ochrana informačných zdrojov alebo služieb pred prístupom alebo využívaním neautorizovanými subjektmi (organizáciami, ľuďmi, počítačmi, procesmi). Riadenie prístupu sa vzťahuje na zabránenie neautorizovaného používania zdroja (t.j. táto služba riadi, kto môže mať prístup k určitým zdrojom, za akých podmienok sa môže prístup realizovať, a čo môže pristupujúci so zdrojmi vykonávať).

Na získane tejto služby musí byť každá entita snažiaca sa o prístup najskôr identifikovaná , alebo autentizovaná, aby jej prístupové práva mohli byť prispôsobené individuálne. Na lepšie pochopenie riadenia prístupu je dôležité definovať nasledujúce pojmy:

- oprávnenia – práva na prístup alebo využívanie prostriedkov alebo služieb,
- zásady – oprávnenia na riadenie prístupu jednotlivých entít,
- subjekty – entity využívajúce oprávnenia pre riadenie prístupu,
- objekty / ciele – prostriedky alebo služby prístupné/využívané subjektmi,
- delegovania – presun oprávnení pre riadenie prístupu medzi hlavnými subjektmi (administrátormi),
- autorizácia – presun oprávnení pre riadenie prístupu z hlavných subjektov na subjekty.

Zoznamy na riadenie prístupu (ACLs - Access control lists) sú najtypickejším ochranným mechanizmom poskytujúcim túto službu.

3.7 Ochrana proti odmietnutiu dát

Bezpečná komunikácia vyžaduje integráciu služieb, ktoré zabezpečujú generovanie digitánych informácií umožňujúcich rozhodnúť spory v prípadoch sieťových chýb alebo nekorektného správnia sa entít počas výmeny digitálnych informácií medzi dvoma alebo viacerými účastníkmi.

Ochrana proti odmietnutiu dát (non-repudiation) je služba bezpečnosti, ktorá využíva tieto dôkazy na poskytnutie ochrany voči popretiu jednou z entít zúčastnených na komunikácii, že participovala na celej komunikácii alebo jej časti.

Ochrana proti odmietnutiu dát je služba bezpečnosti, ktorá garantuje, že odosielateľ správy nemôže neskôr poprieť, že správu odoslal a že príjemca nemôže poprieť, že správu prijal.

Zahrňuje ochranu proti odmietnutiu pôvodu (t.j. dôkaz, že správa bola zaslaná špecifickým účastníkom) a ochranu proti odmietnutiu príjmu (t.j. dôkaz, že správa bola prijatá špecifickým účastníkom).

- *NRO (non-repudiation of origin)* poskytuje dôkazy prijímateľom, že správa bola zaslaná vysielajúcim, ktorý to tvrdí.
- *NRR (non-repudiation of receipt)* poskytuje dôkazy zasielajúcim, že určený prijímateľ správu prijal.

Typické ochranné mechanizmy sú: osvedčenie tretím subjektom (notarization), časové značky (timestamps), digitálne podpisy (digital signatures) a potvrdzovacie služby(confirmation services).

3.8 Ochrana dát

Ochrana dát je služba bezpečnosti umožňujúca jedincovi zabezpečiť právo obmedziť, aké informácie o ňom sú zhromažďované, ako sú používané a kto ich využíva.

Zvýšená možnosť zdieľania informácií v otvorených sieťach ako Internet vedie k novým spôsobom akými môže byť súkromie (privacy) narušené; nové technológie vytvárajú nové spôsoby získavania informácií, čo môže mať niektoré negatívne dôsledky na zachovanie súkromia. Využívanie techník dolovania dát (data maining) a príchod rôznych vyhľadávacích nástrojov vytvorili podmienky na ľahké získavanie a zhromažďovanie dát o jednotlivcoch z veľkého množstva zdrojov.

V mnohých svetových databázach existuje také obrovské množstvo informácií, že jednotlivec nemá praktické možnosti dozvedieť sa o nich alebo kontrolovať informácie o sebe, ktoré môžu iní vlastniť alebo k nim mať prístup. Takéto informácie môžu byť potenciálne predané ďalším za účelom zisku a/alebo použité na účely neznáme alebo neschválené jednotlivcami, ktorých sa to týka. Pojem práva na súkromie získal na dôležitosti spolu s nárastom systémov na zber informácií.

Súkromie - hlavný záujem užívateľov Internetu je možné rozdeliť do tých oblastí:

- aké súkromné informácie môžu byť s niekým zdieľané,
- či je možná výmena správ bez toho aby k nim mal prístup aj niekto iný,
- či a ako je možné zasielať správy anonymne.

Navyše sa možnosti sledovania polohy mobilných zariadení neustále zlepšujú a problémy súvisiace so súkromím narastajú, keďže pozícia užívateľa a jeho preferencie tvoria osobné informácie a ich nevhodné použitie narúša súkromie užívateľa.

Existuje mnoho spôsobov ako chrániť súkromie užívateľa na Internete. Napríklad, emaily môžu byť šifrované, prehľadávanie webových stránok ako aj ďalšie online aktivity by mali byť realizované prostredníctvom anonymizérov, tiež nazývaných mix siete (mix nets). Mix siete môžu byť využité na zabránenie poskytovateľom Internetových služieb aby zistili, ktoré stránky niekto prezeral a s kým komunikuje.

3.9 Mechanizmy bezpečnosti

Mechanizmus bezpečnosti je proces, ktorý implementuje služby bezpečnosti založené na hardvérových (technických), softvérových (logických), fyzických a administratívnych prístupoch. Mechanizmy bezpečnosti podporujú služby bezpečnosti a realizujú špecifické aktivity na ochranu proti útokom alebo výsledkom útokov.

Mechanizmy bezpečnosti sa delia na tie ktoré sú implementované v špecifických vrstvách protokolov a tie, ktoré nie sú presne zviazané s konkrétnou vrstvou protokolu alebo služby bezpečnosti.

K základným mechanizmom bezpečnosti patria:

- šifrovanie (encipherment),
- digitálny podpis (digital signature),
- riadenie prístupu (access control),
- integrita dát (data integrity),
- výmena autentizačnej informácie (authentication exchange),
- vypĺňanie medzier (traffic padding),
- riadenie smerovania (routing control),
- osvedčenie tretím subjektom (notarization).

Šifrovanie je mechanizmus zabezpečujúci utajenie informačného obsahu správy, s využitím určitých matematických algoritmov, ktoré transformujú správu do formy, ktorá nie je čitateľná neautorizovanými subjektmi.

Digitálny podpis je mechanizmus, ktorý využíva kryptografickú transformáciu dát na zabezpečenie autentizácie zdroja a integrity dát a chráni proti odmietnutiu.

Riadenie prístupu zahrňuje širokú triedu mechanizmov, ktoré zabezpečujú riadenie a kontrolu prístupových práv k systémovým prostriedkom a službám. Tento mechanizmus zahrňuje autorizáciu na prístup k vybraných prostriedkom a službám.

Integrita dát zahrňuje širokú triedu mechanizmov kontroly integrity prenášaných dát, alebo toku dát.

Výmena autentizačnej informácie je mechanizmus zabezpečujúci overenie identity používateľa prostriedkami výmeny informácie.

Vypĺňanie medzier je mechanizmus, ktorý realizuje vkladanie dodatočných bitov do medzier v dátových tokoch s cieľom znemožniť analýzu toku dát.

Riadenie smerovania je mechanizmus, ktorý umožňuje selekciu fyzických prenosových ciest pre určité dáta a dovoľuje zmenu smerovania, najmä ak sa očakáva narušenie bezpečnosti. Tento mechanizmus tiež zahrňuje ochranu voči okolitému prostrediu (perimeter security).

Osvedčenie tretím subjektom je mechanizmus, ktorý využíva dôveryhodný tretí subjekt na zabezpečenie určitých aspektov výmeny dát.

Ochrana voči okolitému prostrediu je mechanizmus, ktorý umožňuje akceptovanie alebo zamietnutie dát zasielaných z alebo na konkrétne adresy alebo služby umiestnené mimo lokálnej siete.

3.10 Služby bezpečnosti – mechanizmus mapovania

Jednotlivé služby bezpečnosti môže byť potrebné implementovať s využitím viacerých a rozličných mechanizmov bezpečnosti. Nasledujúca tabuľka znázorňuje vzťah medzi službami bezpečnosti a mechanizmami bezpečnosti.

	Šifrovanie	Digitálny podpis	Riadenie prístupu	Integrita dát	Výmena autentizačnej informácie	Vypĺňanie medzier	Riadenie smerovania	Osvedčenie tretím subjektom
Autentizácia	√	√			√			
Riadenie prístupu			√					
Utajenie	√					√	√	
Integrita dát	√	√		√				
Nepopierateľnosť		√		√				√
Dostupnosť			√	√				
Súkromie	√					√	√	

Bezpečnostné služby a mechanizmy

3.11 Zhrnutie

Komunikácia vyžaduje integráciu rôznych služieb s cieľom zaistiť adekvátnu bezpečnosť prenosu dát. V tejto kapitole boli uvedené najdôležitejšie služby bezpečnosti (dôvernosť, integrita, dostupnosť, autentizácia, riadenie prístupu, ochrana proti odmietnutiu dát a ochrana súkromia) a uvedené mechanizmy bezpečnosti potrebné na poskytovanie takýchto služieb. V podstate týmito mechanizmami bezpečnosti sú: šifrovanie, digitálne podpisy, riadenie prístupu, integrita dát, výmena autentizačnej informácie, vypĺňanie medzier, riadenie smerovania a osvedčenie tretím subjektom. V závere bolo konštatované prepojenie medzi službami bezpečnosti a mechanizmami bezpečnosti.

4 Základy kryptografie

4.1 Úvod

Kryptografia je silný matematický nástroj na boj proti mnohým typom bezpečnostných hrozieb. Mnoho bezpečnostných aplikácii v skutočnosti využíva kryptografiu a jej možnosti na šifrovanie a dešifrovanie dát.

Šifrovanie je vedná disciplína o zmene dát takým spôsobom, že pre neautorizovanú osobu sú tieto dáta nezrozumiteľné a bezcenné. Dešifrovanie je konvertovanie dát späť do ich originálnej formy.

Kryptografia umožňuje ukladať citlivé informácie alebo ich prenášať nezabezpečenými sieťami (ako Internet) tak, že nemôžu byť čítané niekým okrem určeného adresáta. Kryptografia sa v súčasnosti stala priemyselným štandardom na poskytovanie informačnej bezpečnosti, dôvery, riadenie prístupu k prostriedkom a elektronickým transakciám.

Táto technológia je využívaná v každodenných aktivitách ako sú volania pomocou mobilného telefónu, platení pomocou kreditnej alebo debetnej karty, vyberaní peňazí z bankomatu alebo počas prihlasovania sa na počítač pomocou hesla.

Kryptografický algoritmus alebo šifra je matematická funkcia použitá v procese šifrovania a dešifrovania. Kryptografický algoritmus využíva jeden alebo niekoľko kľúčov – nejaké slovo, číslo, alebo frázu – na zašifrovanie otvoreného textu (plaintext). Ten istý otvorený text šifruje na odlišné zašifrované texty (ciphertexts), ak sú použité odlišné kľúče. Bezpečnosť zašifrovaných dát úplne závisí na dvoch okolnostiach: sile kryptografického algoritmu a utajení kľúča.

Silný kryptografický algoritmus musí splňovať nasledujúce kritéria:

- Nesmie existovať iný spôsob na získanie otvoreného textu ak nie je známy kľúč ako je útok metódou totálnych skúšok (brute force attack), t.j. testovanie všetkých možných kľúčov až pokiaľ nie je nájdený správny kľúč.
- Počet možných kľúčov musí byť taký veľký, že je výpočtovo nerealizovateľné aplikovať metódu totálnych skúšok v čase, ktorý je na útok k dispozícii.
- Čokoľvek sa zašifruje, musí byť vrátené do pôvodnej formy počas dešifrovania s kľúčom určeným na dešifrovanie.
  V tejto knihe budeme skúmať **čo šifrovanie realizuje**. Budú uvedené základné pojmy využívané v šifrovaní a skúmaný model šifrovania. Avšak **nad rámec** tohto dokumentu je:
  - **ako šifrovanie funguje**; základné návrhy šifračných algoritmov.
  - **ako môže šifrovanie zlyhať**, ako môžu byť šifrovacie algoritmy nalomené s využitím kryptoanalýzy.

4.2 Rozdelenie kryptografických algoritmov

Kryptografické algoritmy je možné rozdeliť na:

Algoritmy so symetrickým alebo tajným kľúčom. Tieto algoritmy využívajú pre šifrovanie aj dešifrovanie ten istý kľúč. Algoritmus **AES** (*Advanced Encryption Standard*) je príkladom symetrického kryptosystému, ktorý sa široko využíva.

Kryptografia s verejným kľúčom alebo asymetrická kryptografia je systém, ktorý využíva na šifrovanie vhodný pár kľúčov: verejný kľúč, pomocou ktorého sa dáta šifrujú a zodpovedajúci súkromný kľúč na dešifrovanie. Aj keď táto dvojica kľúčov konkrétneho páru je matematicky zviazaná, je výpočtovo nemožné odvodiť súkromný kľúč z verejného kľúča. Používateľ alebo entita zverejňuje verejný kľúč pre všetkých, utajuje však súkromný kľúč. Ktokoľvek, kto vlastní verejný kľúč, môže informácie šifrovať, ale nie dešifrovať. Iba osoba, ktorá má zodpovedajúci súkromný kľúč môže informáciu dešifrovať.

Základnou výhodou asymetrickej kryptografie je umožnenie komunikovať bezpečne aj bez predchádzajúcej výmeny kľúčov zabezpečeným kanálom. Odosielateľ a príjemca nemusia prostredníctvom bezpečného kanálu zdieľať žiadne tajné kľúče; celá dostupná komunikácia využíva len verejné kľúče a žiadny súkromný kľúč nie je vysielaný alebo zdieľaný.

4.3 Terminológia

Otvorený text je správa, ktorá musí byť vyslaná k príjemcovi.

Zašifrovaný text je výstup, ktorý je generovaný zašifrovaním otvoreného textu.

Šifrovanie je proces zmeny formy otvoreného textu takým spôsobom, že aktuálna správa je nezrozumiteľná.

Dešifrovanie je opakom šifrovania; je to proces získania správy otvoreného textu z jej zašifrovanej formy (zašifrovaný text) . Tento proces konvertuje zašifrovaný text na otvorený text.

Kľúč je nejaké slovo, číslo, alebo reťazec, ktorý je použitý na šifrovanie otvoreného textu alebo dešifrovanie zašifrovaného textu.

Kryptoanalýza je veda o lúštení („lámaní") kódov a šifier.

Hašovacie (hash) algoritmus je algoritmus, ktorý konvertuje textový reťazec ľubovoľnej dĺžky na reťazec pevnej dĺžky.

Šifra je kryptografický algoritmus, t.j. matematická funkcia používaná na šifrovanie a dešifrovanie.

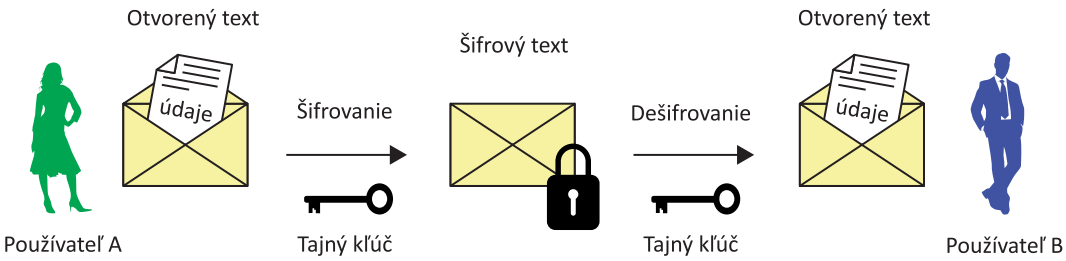
Dešifrátor konvertuje zašifrovaný text na ekvivalentný otvorený text pomocou nejakého šifrovacieho zariadenia.

Kľúčový manažment – proces v rámci ktorého je kľúč vytváraný, ukladaný, chránený, zasielaný, nahrávaný, používaný a vymazaný.

4.4 Symetrické šifry

Proces šifrovania a dešifrovania informácie s využitím jediného kľúča je známy ako šifrovanie s tajným kľúčom alebo symetrická kryptografia. V symetrickej kryptografii môžu byť kľúče použité na šifrovanie otvoreného textu a dešifrovanie zašifrovaného textu identické (typická situácia) alebo medzi oboma kľúčmi existuje jednoduchá transformácia. Hlavným problémom symetrických algoritmov je že odosielateľ a príjemca sa musia dohodnúť na spoločnom kľúči. Na výmenu tajného kľúča medzi odosielateľom a príjemcom je potrebný bezpečný kanál.

Proces použitia symetrickej šifry je nasledovný: Užívateľ A chce zaslať nejakú správu užívateľovi B a zároveň chce, aby len užívateľ B bol schopný správu prečítať. Na zabezpečenie prenosu užívateľ A vygeneruje tajný kľúč, zašifruje správu pomocou tohto kľúča a zašle správu užívateľovi B. Užívateľ B potrebuje na prečítanie správy použitý tajný kľúč. Užívateľ A môže odovzdať tajný kľúč užívateľovi A použitím nejakého (bezpečného) spôsobu, ktorý je dostupný. Po získaní tajného kľúča je užívateľ B schopný dešifrovať správu a získať pôvodnú správu.



Model šifrovania so symetrickým kľúčom

Šifrovací algoritmus musí spĺňať nasledujúce vlastnosti:

- **Difúzia (diffusion):** každý bit otvoreného textu ovplyvňuje mnoho bitov zašifrovaného textu a každý bit zašifrovaného textu je ovplyvnený mnohými bitmi otvoreného textu.
- **Konfúzia (confusion):** je nevyhnutné vyhnúť sa štruktúrovaným vzťahom (zvlášť lineárnym) medzi otvoreným textom a zašifrovaným textom/kľúčom, ktoré sú využiteľné známymi útokmi.
- Zašifrovaný text by mal vyzerať náhodne a mať dobré štatistické vlastnosti.
- **Jednoduchosť (simplicity).**
- **Výkonnosť (efficiency):** mal by byť extrémne rýchly v hardvérových aj softvérových implementáciách na širokej škále platforiem.

Najčastejšie využívané symetrické šifry sú:

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

Hlavným problémom symetrickej kryptografie je, že proces prenosu kľúčov k príjemcovi je zdrojom bezpečnostných rizík. Posielanie tajného kľúča cez Internet v emailoch nie je bezpečné. Ústne odovzdanie tajného kľúča telefónom je ohrozované odpočúvaním. Podobne, zasielanie konvenčnou poštou zvyšuje riziko prezradenia.

Bezpečnostné riziká obsiahnuté v symetrickej kryptografii boli do značnej miery prekonané použitím asymetrickej kryptografie. Symetrické šifry sú často využívané na šifrovanie dát na pevných diskoch. Osoba šifrujúca dáta vlastní (symetrický) kľúč privátne a neexistuje problém s distribúciou kľúča.

4.5 Asymetrická kryptografia

Asymetrická kryptografia sa rozvinula s cieľom poskytnúť riešenia na bezpečnostné problémy spojené so symetrickou kryptografiou. Metóda rieši problém symetrického kľúča použitím **dvoch kľúčov** namiesto jedného. Asymetrická kryptografiavyužíva pár kľúčov. V tomto procese je jeden použitý na šifrovanie a druhý na dešifrovanie.

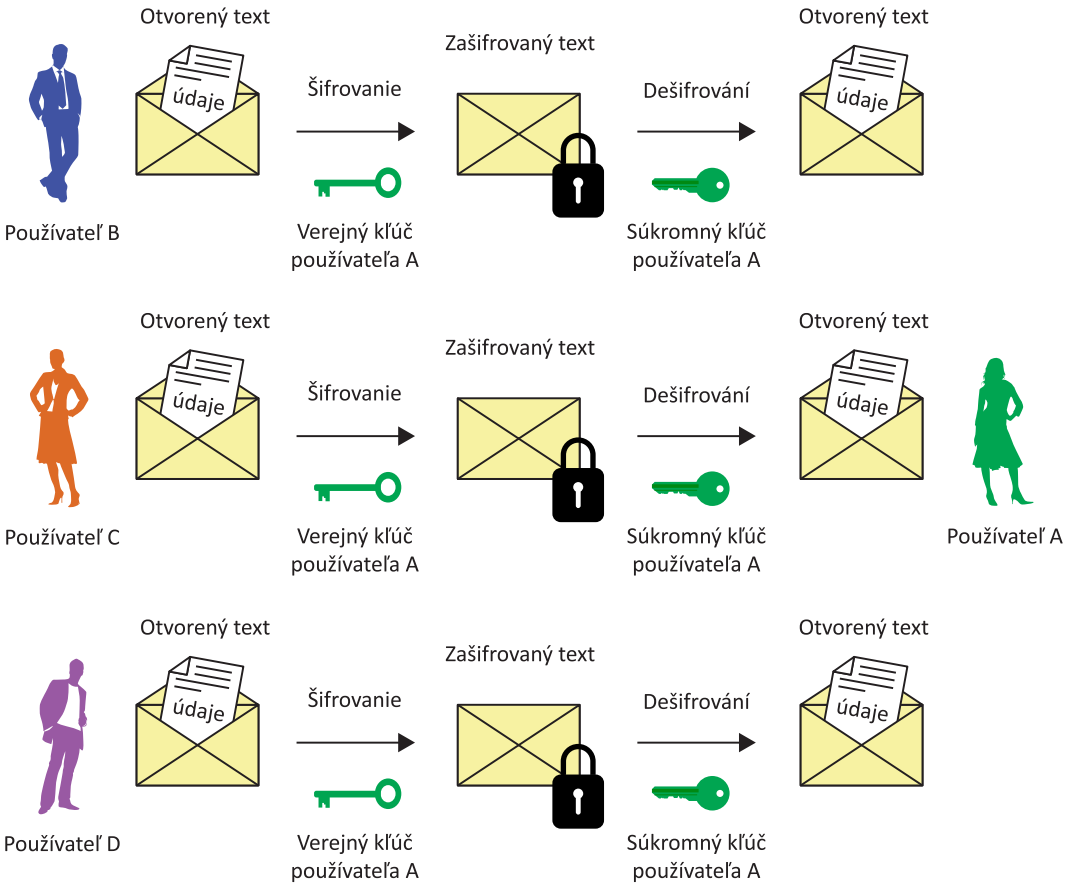
Tento proces je známy ako kryptografia s verejným kľúčom alebo asymetrická kryptografia, pretože v tomto procese sú na skompletizovanie procesu potrebné oba kľúče. Tieto dva kľúče sú súhrne známe ako **kľúčový par**. V asymetrickej kryptografii je jeden z kľúčov voľne šíriteľný. Tento kľúč sa nazýva **verejný kľúč** a používa sa pri šifrovaní. Preto sa táto metóda šifrovania nazýva tiež šifrovanie s verejným kľúčom. Druhým kľúčom je **súkromný kľúč** a používa sa pri dešifrovaní. Súkromný kľúč sa nešíri. Tento kľúč, ako vyplýva aj z jeho názvu, je privátny pre každú komunikujúcu entitu. Je dôležité zdôrazniť, že verejný a súkromný kľúč sú spolu previazané, ale je prakticky nemožné odvodiť súkromný kľúč len zo znalosti verejného kľúča.

Najznámejším algoritmom s verejným kľúčom je **RSA**.

4.6 Aký je princíp kryptogarfie s verejným kľúčom?

Využitie šifrovania s verejným kľúčom na poskytnutie dôvernosti

Nech napr. užívateľ B chce poslať nejakú správu užívateľovi B. Užívateľ B zašifruje správu s verejným kľúčom užívateľa A, a užívateľ A dešifruje správu pomocou jeho súkromného kľúča. Keďže kľúčový pár je komplementárny, iba pomocou súkromného kľúča užívateľa A je možné správu dešifrovať. Ak niekto iný zachytí šifrovaný text, nebude schopný dešifrovať ho, pretože iba súkromný kľúč užívateľa A je možné použiť na dešifrovanie. Táto metóda neposkytuje žiadnu autentizáciu, že správa prichádza od užívateľa B, pretože verejný kľúč užívateľa A je verejne známy. Avšak, metóda naozaj poskytuje dôvernosť pre zaslanú správu, pretože len užívateľ A ju môže dešifrovať.



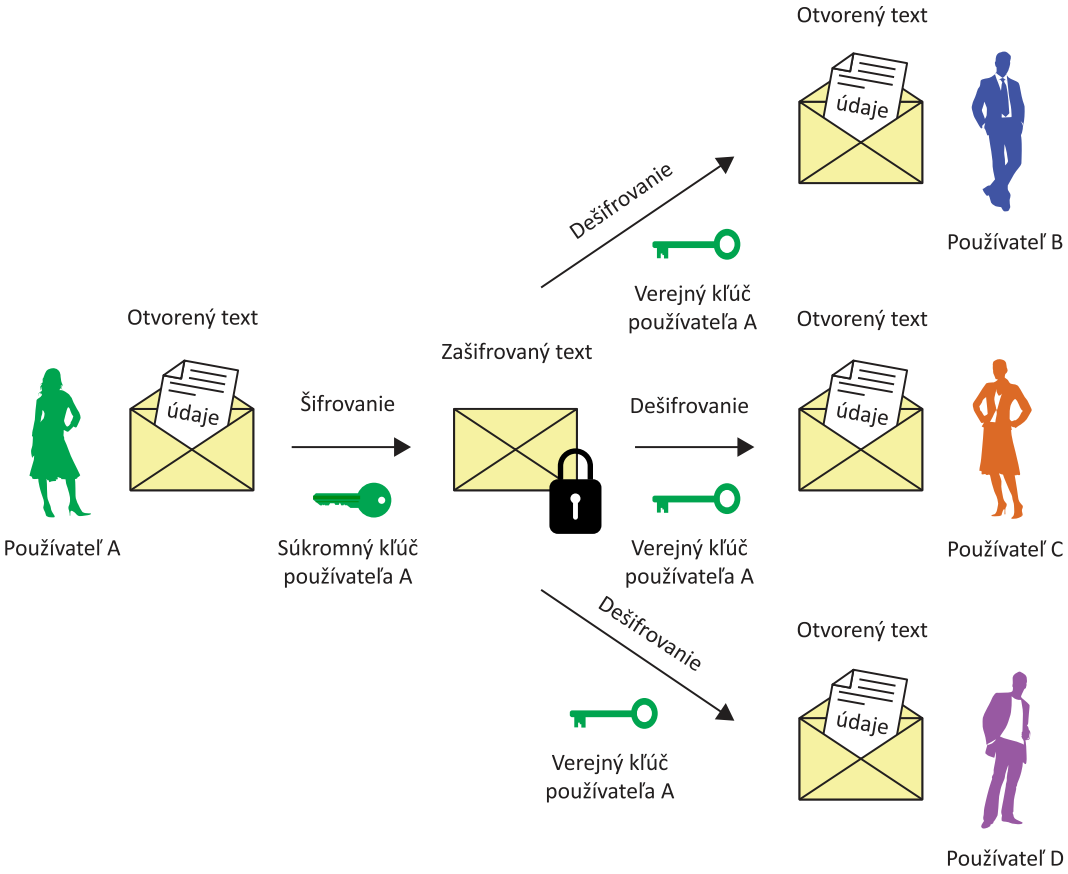
Model šifrovania s verejným kľúčom (poskytujúci dôvernosť)

Uvedená metóda veľmi jasne naznačuje, že dáta zasielané nejakému užívateľovi stačí zašifrovať verejným kľúčom príjemcu, ak je požadovaná ich dôvernosť. Podobne, dešifrovanie môže byť realizované iba súkromným kľúčom, ktorý musí poskytnúť príjemca dát. Takto môžu byť správy vymieňané bezpečne. Odosielateľ a príjemca nemusia zdieľať nejaký spoločný kľúč ako to bolo v prípade

symetrického šifrovania. Celá otvorená komunikácia využíva iba verejné kľúče a žiadny súkromný kľúč nie je prenášaný alebo zdieľaný.

Využitie šifrovania s verejným kľúčom na poskytnutie autentizácie

Na autentizáciu musí užívateľ A zašifrovať správu svojim súkromným kľúčom a užívateľ B dešifruje správu pomocou verejného kľúča užívateľa A. Táto metóda poskytne autentizáciu, že správa prišla od užívateľa A, neposkytuje však dôvernosť, pretože verejný kľúč užívateľa A je verejne známy. Preto každý, kto má verejný kľúč užívateľa A môže správu dešifrovať.



Model šifrovania s verejným kľúčom (poskytujúci autentizáciu)

Využitie šifrovania s verejným kľúčom na poskytnutie autentizácie a dôvernosti

Na súčasné poskytnutie dôvernosti a autentizácie musí užívateľ B zašifrovať otvorený text najskôr svojim súkromným kľúčom, čím poskytne autentizáciu. Následne užívateľ B použije verejný kľúč užívateľa A na zašifrovanie správy, čím poskytne dôvernosť.

Nevýhodou systému je veľká časová náročnosť a zložitosť, keďže šifrovanie a dešifrovanie musí byť realizované štyri krát, a dĺžka verejného kľúča je značná (od 1024 bitov do 4096 bitov).

4.7 Hybridné systémy: Kombinácia symetrického a asymetrického šifrovania

Nevýhodou používania **šifrovania s verejným kľúčom** je to **pomerne pomalý proces šifrovania**, keďže dĺžky kľúčov sú značné (od 1024 bitov do 4096 bitov). **Symetrické šifrovanie** je podstatne **rýchlejšie**, keďže dĺžky kľúčov sú výrazne menšie (od 40 bitov do 256 bitov). Na druhej strane v prípade symetrického šifrovania existuje problém prenosu kľúča. Obe tieto techniky je možné využiť spoločne a vytvoriť lepšiu metódu šifrovania. Týmto spôsobom je možné využiť spojené výhody and prekonať individuálne nevýhody.

Konkrétne, hybridný systém využíva algoritmus s verejným kľúčom na bezpečné zdieľanie kľúčov pre symetrické šifrovanie. Konkrétna správa je následne šifrovaná použitím tohto (symetrického) kľúča a zaslaná príjemcovi. Keďže metóda zdieľania (symetrického) kľúča je bezpečná, symetrický kľúč využívaný na šifrovanie sa mení pre každú zasielanú správu. Z tohto dôvodu sa niekedy nazýva kľúč relácie (session key). Znamená to, že ak by bol kľúč relácie kompromitovaný, útočník by mohol čítať len správu šifrovanú týmto kľúčom. Na dešifrovanie ďalších správ by útočník musel získať ďalšie kľúče relácií.

Kľúč relácie, šifrovaný algoritmom s verejným kľúčom, a správa (ktorá ma byť odoslaná) šifrovaná symetrickým algoritmom, sú automaticky kombinované do jedného balíka. Príjemca používa svoj súkromný kľúč na dešifrovanie kľúča relácie a následne využíva kľúč relácie na dešifrovanie správy. Mnoho aplikácií využíva práve tento systém.

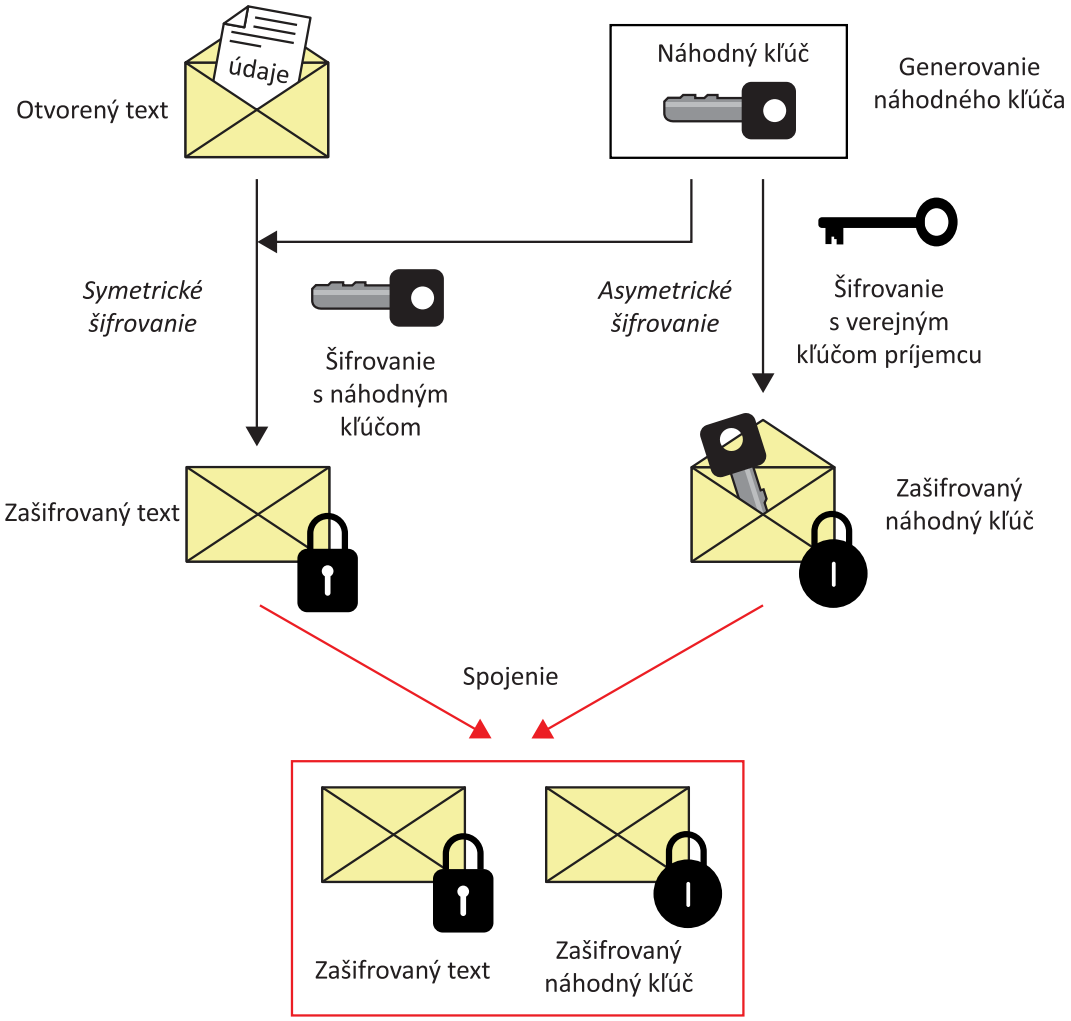
Jednotlivé dátové operácie v rámci kombinovanej techniky sú:

1. Šifrovanie otvoreného textu pomocou symetrickej šifry a náhodného kľúča.

2. Šifrovanie len náhodného kľúča pomocou asymetrického šifrovania a verejného kľúča príjemcu. Následné zaslanie zašifrovaného náhodného kľúča príjemcovi. Príjemca môže u seba dešifrovať náhodný kľúč s využitím svojho súkromného kľúča.

3. Následné zaslanie aktuálne zašifrovaných dát. Zašifrované dáta môžu byť dešifrované pomocou súkromného kľúča príjemcu, ktorý tvorí pár s verejným kľúčom príjemcu, ktorý bol použitý na zašifrovanie náhodného kľúča.

Nasledujúci obrázok ilustruje uvedený proces.



Model hybridného šifrovania (poskytujúci dôvernosť)

Kombinovaná technika šifrovania je v praxi široko využívaná. Je použitá napr. v **SSH** (*Secure Shell*) na zabezpečenie komunikácie medzi klientom a serverom a v programe **PGP** (*Pretty Good Privacy*) na posielanie emailov. Je však predovšetkým jadrom protokolov **TLS** (*Transport Layer Security*), ktoré sú široko využívané Web prehliadačmi a Web servermi na zabezpečenie podpory zabezpečeného komunikačného kanálu pri vzájomnej komunikácii.

4.8 Hašovacie funkcie

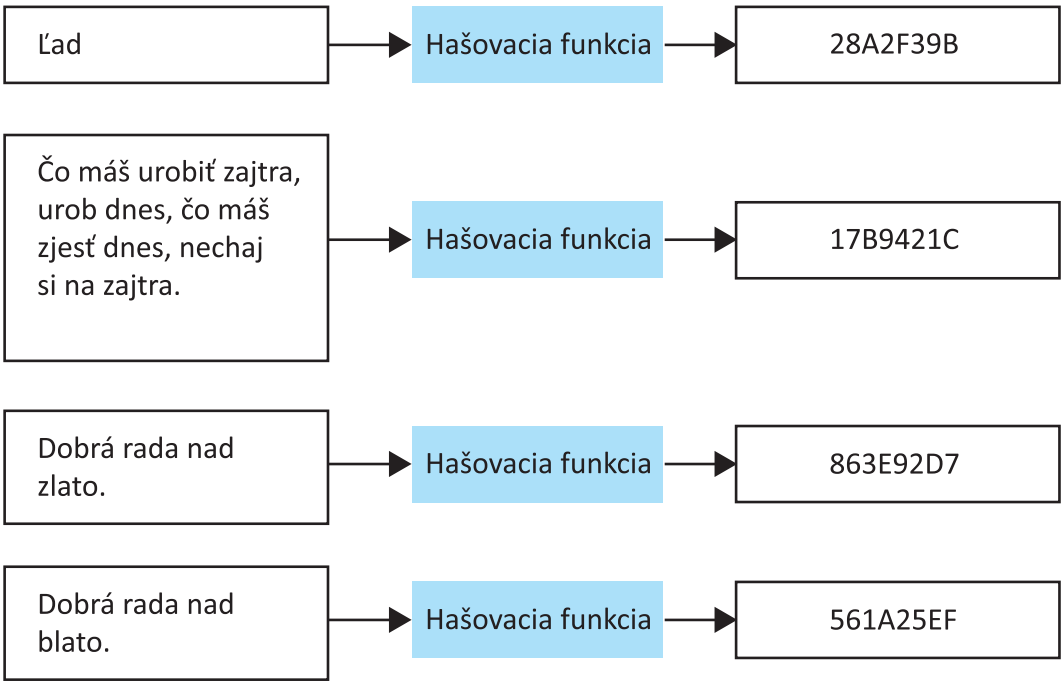
Hašovacia funkcia je transformácia, ktorej vstupom je správa *m* s premenlivou dĺžkou a výstupom reťazec pevnej dĺžky, ktorý sa nazýva hašovací kód *h* (teda platí, $h = H(m)$). Ľubovoľná zmena vstupných dát spôsobí (s veľmi vysokou pravdepodobnosťou) zmenu hašovacieho kódu. Hašovacie funkcie ktoré majú iba uvedenú vlastnosť majú množstvo všeobecných výpočtových aplikácií, avšak v prípade ich využitia v kryptografii sú na nich kladené dodatočné požiadavky.

Základné požiadavky na kryptografickú hašovaciu funkciu sú:

- jej vstup môže mať ľubovoľnú dĺžku,
- jej výstup má pevnú dĺžku,
- je ľahké určiť hašovací kód pre ľubovoľnú správu,
- hašovacie funkcie sú jednocestné (one-way), čo znamená, že je výpočtovo nerealizovateľné vytvoriť správu, ktorá má požadovaný hašovací kód,
- je nemožné modifikovať nejakú správu tak, aby sa jej hašovací kód nezmenil,
- je odolná voči kolízii (collision-free), čo znamená, že je výpočtovo nemožné nájsť dve odlišné správy (x,y) také, že $H(x) = H(y)$.

Hašovací kód stručne reprezentuje dlhšiu správu alebo dokument z ktorého bol vypočítaný. Výťah zo správy (message digest) ako „digitálny otlačok (digital fingerprint)“ väčšieho dokumentu.

Hlavnou aplikáciou kryptogarfickej hašovacej funkcie je zabezpečenie *digitálnych podpisov*. Navyše, otlačok je možné zverejniť bez toho aby bol odhalený obsah dokumentu, z ktorého otlačok vznikol.



Hašovacia funkcia

4.9 Digitálny podpis

Digitálne podpisy sú najdôležitejším výstupom prác na asymetrickej kryptografii , a poskytujú množinu bezpečnostných funkcií, ktoré by bolo náročné alebo doknca nemožné implementovať s využitím iných techník.

Digitálny podpis je elektronický podpis, ktorý môže byť využitý na autentizáciu identity odosielateľa správy alebo osoby podpisujúcej dokument, a eventuálne tiež na zabezpečenie integrity správy.

Digitálne podpisy sa ľahko prenášajú a nemôžu byť napodobnené niekým iným. Majú možnosť zabezpečiť, že originálne podpísaná správa po prijatí nemôže byť odosielajúcim odoprená.

Digitálne podpisy vychádzajú z klasických rukou realizovaných podpisov, ktoré sú využívané na potvrdenie vlastníckych práv alebo potvrdenie obsahu správy. Rukou realizované podpisy by mali mať nasledujúce vlastnosti:

- podpis je bezpečný – podpis by nemal byť napodobniteľný a akýkoľvek potenciálny pokus na napodobnenie podpisu (signature forgery) by mal byť ľahko odhaliteľný,
- podpis umožňuje autentizáciu – podpis jednoznačne identifikuje vlastníka podpisu, ktorý podpísal dokument bez obmedzenia a z vlastnej vôle,
- podpis je neprenosný – podpis je súčasťou dokumentu a neautorizovaný subjekt nie je schopný presunúť podpis na iný dokument,
- podpísaný dokument je nemenný – dokument nemôže byť po jeho podpise zmenený a modifikovaný,
- podpis je nepopierateľný – vlastník podpisu nemôže poprieť podpísanie podpísaného dokumentu.

V praxi nie žiadna z týchto požiadaviek u rukou realizovaných podpisov dôsledne splnená a podpis môže byť zdiskreditovaný alebo porušený. Všetky uvedené vlastnosti by mali mať aj digitálne podpisy.

Existujú však niektoré problémy spojené s praktickou realizáciou digitálnych podpisov. Digitálne súbory je možné ľahko kopírovať a časť nejakého dokumentu môže byť presunutá do iného dokumentu, pričom podpísaný dokument môže byť ľahko modifikovaný. Preto musia byť pre digitálny podpis sformulované dodatočné požiadavky:

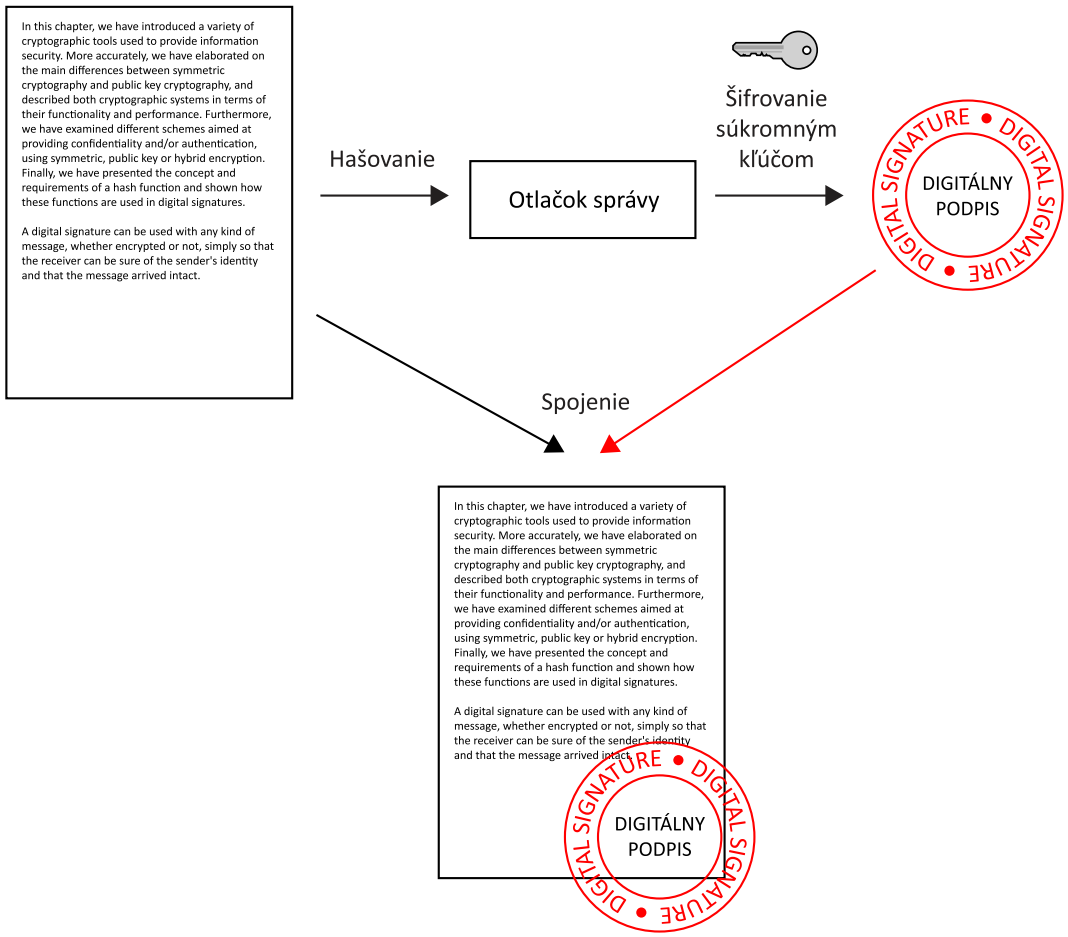
- podpis musí mať bitový formát ktorý závisí na správe ktorá je podpisovaná,
- podpis musí využívať nejakú jedinečnú informáciu o odosielateľovi, aby sa zabránilo falšovaniu aj odopretiu podpisu,

- realizácia a implementácia digitálneho podpisu musí byť relatívne ľahko realizovateľná,
- falšovanie digitálneho podpisu musí byť výpočtovo nerealizovateľné, a či už nemožnosťou vytvorenia novej správy pre existujúci digitálny podpis, alebo nemožnosťou vytvorenia falošného digitálneho podpisu pre nejakú správu,
- musí byť praktické uchovávať kópiu digitálneho podpisu v archívoch.

Digitálny podpis môže byť použitý pre ľubovoľnú správu, či už je šifrovaná alebo nie, aby sa príjemca mohol uistiť o identite odosielateľa a overiť že správa dorazila neporušená.

Existuje niekoľko využiteľných schém pre digitálne podpisy. Jedna z najakceptovanejších schém využíva hašovacie funkcie. V jej prípade musí užívateľ, ktorý chce digitálne podpísať nejaký dokument, vykonať nasledujúce kroky:

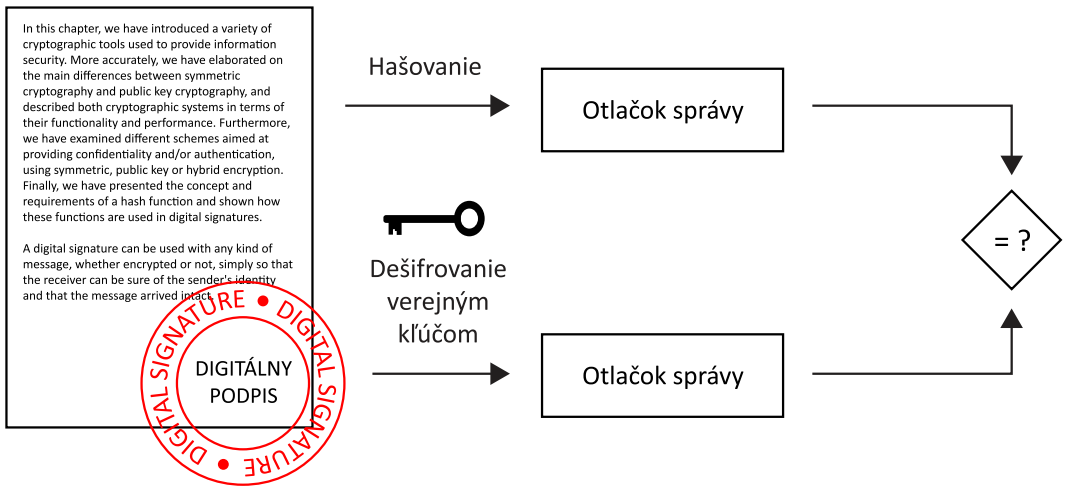
- určiť hašovací kód dokumentu, ktorý ide podpísať,
- použitím asymetrického šifrovania a súkromného kľúča odosielateľa zašifrovať získaný hašovací kód , čím získa digitálny podpis,
- pripojiť digitálny podpis k dokumentu.



Model digitálneho podpisu na báze hašovacej funkcie

Príjemca môže verifikovať autenticitu tohto digitálneho podpisu realizáciou nasledujúcich krokov:

- určiť hašovací kód dokumentu (bez digitálneho podpisu),
- použitím asymetrického šifrovania a verejného kľúča odosielateľa dešifrovať digitálny podpis, čím získa digitálny otlačok správy,
- porovnať výsledky získané v predchádzajúcich dvoch krokoch.



Verifikačný postup pre digitálny podpis na báze hašovacej funkcie

Ak sú otlačky správy získané v predchádzajúcich dvoch krokoch rovnaké, príjemca bude vedieť, že podpísané dáta neboli zmenené.

4.10 Zhrnutie

V tejto kapitole bol uvedený rad kryptografických nástrojov na zabezpečenie informačnej bezpečnosti. Presnejšie boli uvedené základné rozdiely medzi symetrickými šiframi a kryptografiou s verejným kľúčom, boli opísané oba kryptografické systémy z pohľadu ich funkčnosti a výkonnosti. Ďalej boli vyšetrované rôzne schémy umožňujúce poskytnúť dôvernosť a/alebo autentizáciu s využitím symetrického, asymetrického alebo hybridného šifrovania. V závere bol prezentovaný pojem hašovacia funkcia, naznačené požiadavky kladené na kryptografické hašovacie funkcie a ukázané ako sú tieto funkcie využité v digitálnych podpisoch.

5 Digitálne certifikáty a manažment kľúčov

5.1 Distribúcia verejných kľúčov

Digitálne podpisy predstavujú jedno z primárnych využití kryptografie s verejným kľúčom. Pre správy zasielané nezabezpečeným kanálom dáva príjemcovi správne implementovaný digitálny podpis dôvod veriť, že správa bola naozaj zaslaná odosielateľom, ktorý to o sebe tvrdí. V mnohých aspektoch sú digitálne podpisy ekvivalentne rukou realizovaným podpisom, avšak správne implementované digitálne podpisy je ťažšie falšovať ako ručné. Overenie digitálneho podpisu vyžaduje znalosť verejného kľúča odosielateľa. Preto je mechanizmus distribúcie kľúčov v praxi absolútne nevyhnutný.

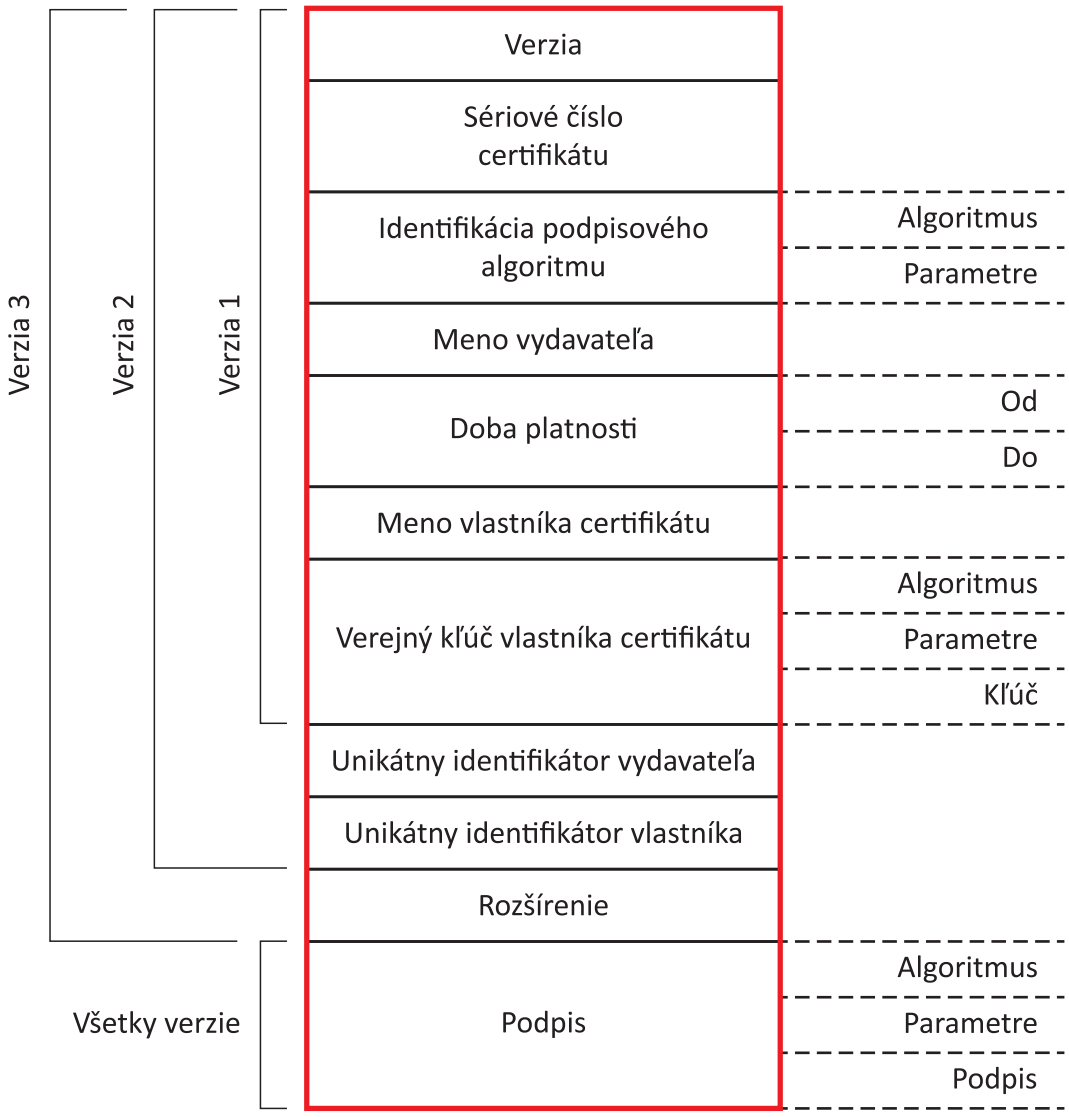
Najakceptovanejší spôsob realizácie výmeny kľúčov využíva digitálne certifikáty.

5.2 Pojem digitálneho certifikátu

Digitálny certifikát je elektronický dokument, ktorý využíva digitálny podpis **na vzájomne prepojenie vrejného kľúča s identitou** – informáciami o mene osoby alebo organizácie, ich adrese, atď.

Certifikát je možné použiť na verifikáciu, že verejný kľúč patrí nejakému jedincovi. Digitálny certifikát je dátová štruktúra, ktorá obsahuje verejný kľúč subjektu alebo vlastníka certifikátu ako aj identifikačné údaje vlastníka certifikátu, časovú pečiatku určujúcu platnosťou certifikátu a ďalšie údaje z certifikačnej autority. Táto štruktúra je podpísaná privátnym kľúčom *certifikačnej autority* (**CA**) a každý užívateľ má možnosť overiť autenticitu obsahu certifikátu použitím verejného kľúča certifikačnej autority.

Na nasledujúcom obrázku je zobrazená štruktúra digitálneho certifikátu:

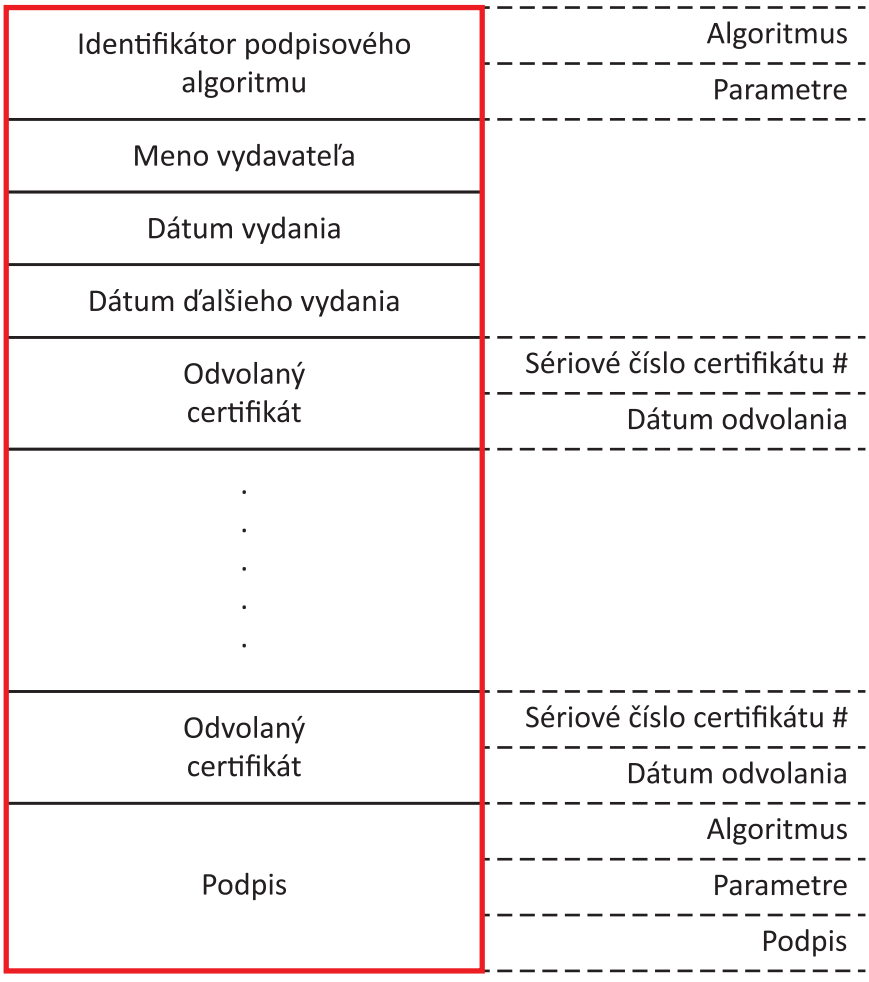


Štruktúra digitálneho certifikátu

5.3 Mechanizmy odvolania certifikátu

Digitálny certifikát môže byť odvolaný ak napr. už uživateľ nie je vlastníkom privátneho kľúča (napr. ak token obsahujúci jeho privátny kľúč bol odcudzený) a teda privátny kľúč bol kompromitovaný. Certifikát môže byť tiež odvolaný ak sa odhalí, že *certifikačná autorita* (**CA**) nesprávne vydala nejaký certifikát bez rešpektovania požiadaviek bezpečnostnej politiky.

Najbežnejším mechanizmom na verifikáciu, či nejaký certifikát bol odvolaný, je založený na využití *zoznamu odvolaných certifikátov* (**CRL-** *certificate revocation list*). CRL je zoznam certifikátov (alebo presnejšie zoznam sériových čísel certifikátov), ktoré boli odvolané a teda sa na nich nedá spoliehať. CRL je vždy vydávaný CA, ktorá vydáva zodpovedajúce certifikáty a je generovaná a publikovaná periodicky, často v definovanóm intervale. Každá CA preto potrebuje nejaký CRL.



Štruktúra zoznamu odvolaných certifikátov

5.4 Zhrnutie

V tejto kapitole boli naznačené problémy distribúcie verejných kľúčov a využitie digitálnych certifikátov ako najrozšírenejšej metódy na riešenie tohto problému. Tiež bol ilustrovaný problém odvolania certifikátu a poskytnutý opis mechanizmov založených na CRL.

6 Bezpečnosť sieťových služieb

6.1 TLS

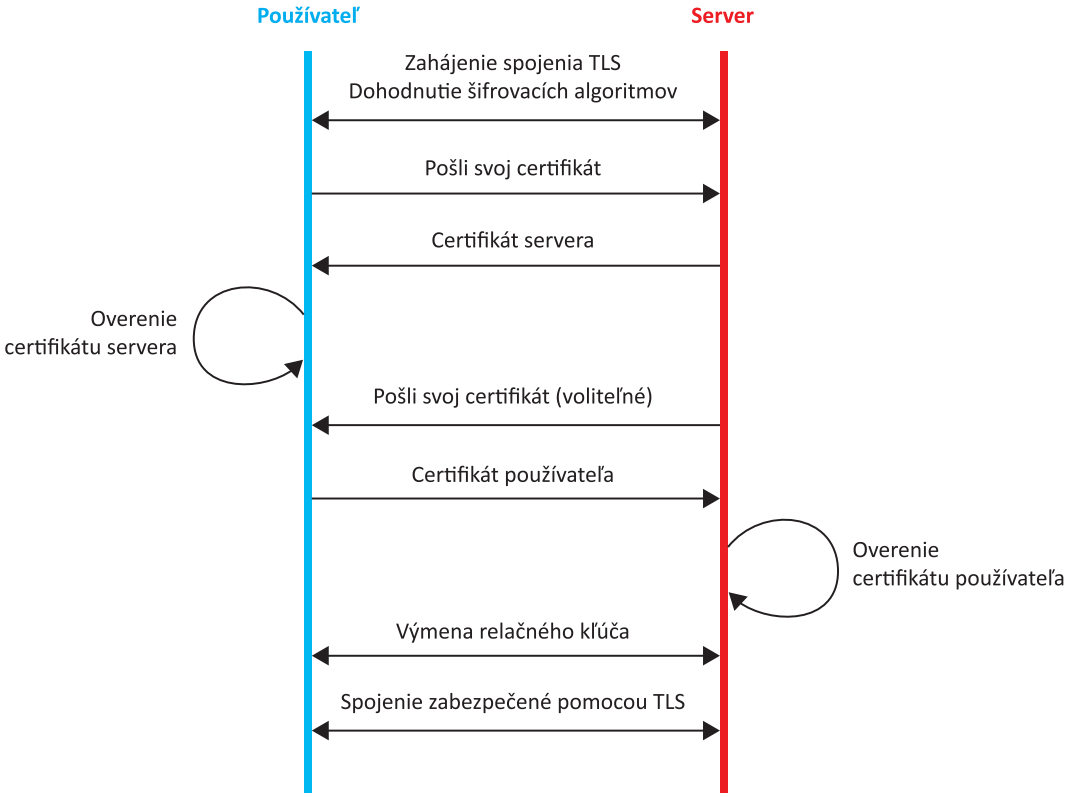
TLS (*Transport Layer Security*) je štandardný internetový protokol, ktorý zabezpečuje bezpečnú komunikáciu pri využívaní Internetu. Základným cieľom tohto protokolu je poskytnutie dôvernosti a integrity dát medzi dvomi komunikujúcimi aplikáciami. Významným je používanie TLS na zabezpečenie WWW (World Wide Web) prenosov realizovaných pomocou **HTTP vo forme HTTPS**, ktoré umožňujú bezpečnú realizáciu obchodných elektronických transakcií. Stále viac využívaný protokol **SMTP** (*Simple Mail Transfer Protocol*) je tiež zabezpečený pomocou TLS.

TLS je široko využívaný v takých aplikáciách ako prezeranie web stránok, elektronickej pošte, internetové faxovanie, priame zasielanie správ a prenosu hlasu internetovým protokolom **VoIP** (*voice-over-IP*).

TLS je založený na staršej **SSL** (*Secure Sockets Layer*) špecifikácii vyvinutej firmou Netscape Communications. Oba protokoly (TLS a SSL) využívajú kryptografické algoritmy a certifikáty s verejným kľúčom na overenie identity koncových komunikujúcich bodov a na výmenu kľúčov. Takáto autentizácia je voliteľná, ale vo všeobecnosti je vyžadovaná, aspoň pre jednu z dvoch komunikujúcich strán.

Tiež využívajú symetrické šifry na dosiahnutie dôvernosti, a autentizačné kódy správ (message authentication codes) na zabezpečenie integrity správ. Symetrická kryptografia je využívaná na šifrovanie dát. Pre každé spojenie sú generované jedinečné kľúče, pričom sa využíva vopred dohodnuté zdieľané tajomstvo. Dohadovanie tohto zdieľaného kľúča je bezpečné a spoľahlivé: dohodnutý kľúč nie je dostupný odpočúvajúcim, a pre všetky autentizované spojenia kľúč nemôže byť získaný dokonca ani útočníkom, ktorý realizuje aktívny útok medzi komunikujúcimi účastníkmi (útok zo stredu). Okrem toho, žiadny útočník nemôže modifikovať dohadovaciu fázu komunikácie bez toho aby jeho útok nebol detegovaný účastníkmi komunikácie.

Nasledujúci obrázok zjednodušene ukazuje, ako je vytváraná TLS relácia.



Vytvorenie relácie protokolu TLS

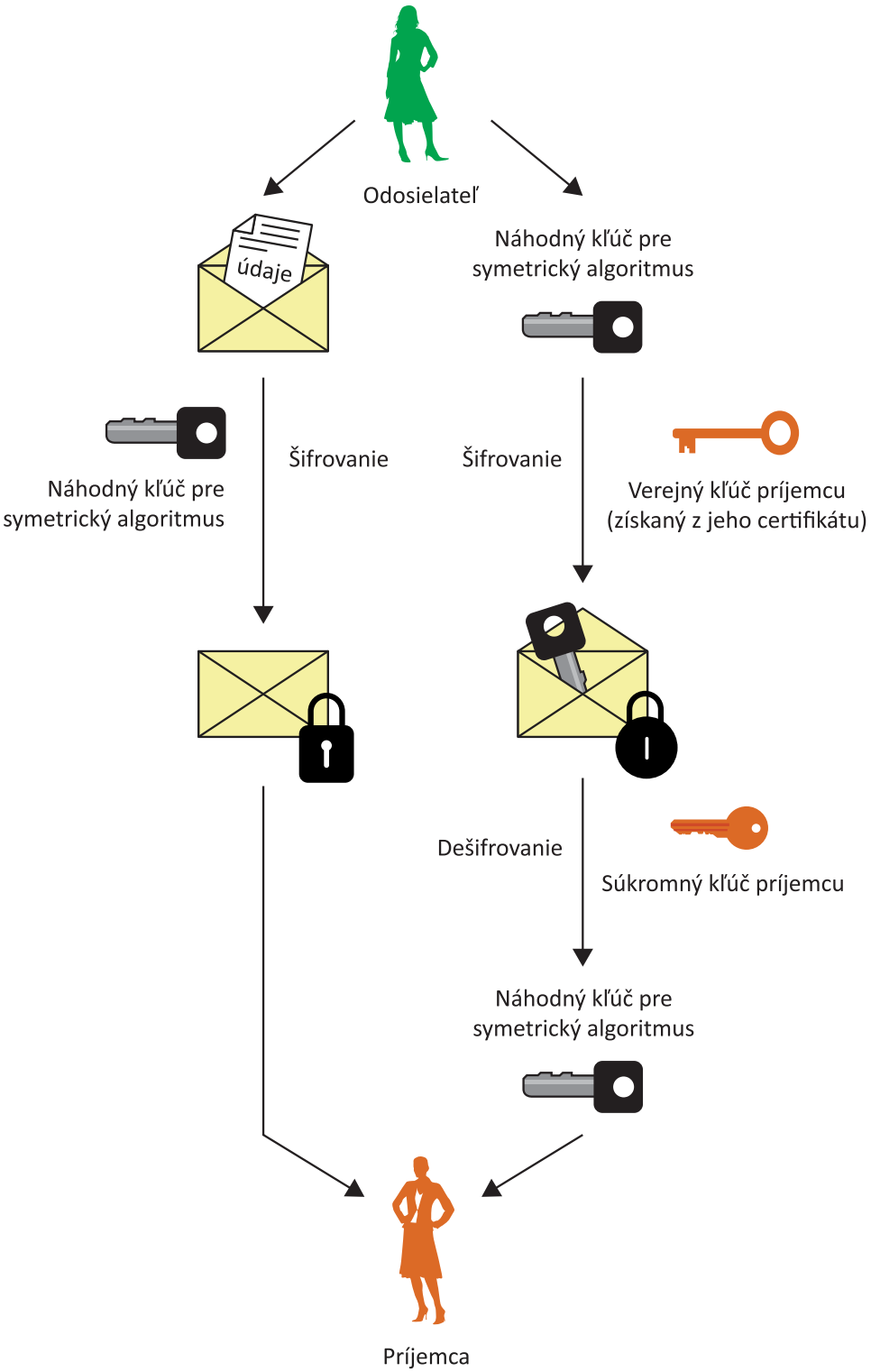
6.2 Zabezpečenie emailov

Zvyčajne je pri zasielaní emailov ich obsah nechránený a každý ich môže čítať. Je to podobné ako pri zasielaní pohľadníc: každý, komu sa dostanú do rúk ich môže čítať. Aby boli dáta zasielané prostredníctvom emailov dôverné a/alebo autentické, musia byť šifrované. V prípade dôvernosti môže správy dešifrovať len určený príjemca a všetci ostatní vidia len nezmyselný text.

Najakceptovanejšími mechanizmami poskytujúcimi zabezpečenie emailov sú **S/MIME** a **PGP**.

S/MIME je štandard, ktorý poskytuje nasledujúce kryptografické služby bezpečnosti pre aplikácie elektronického zasielania správ: autentizáciu, integritu správ, ochranu proti odmietnutiu zdroja (použitím digitálnych podpisov) a dôvernosť dát (použitím šifrovania). Používanie **S/MIME vyžaduje** digitálne certifikáty.

Nasledujúci obrázok ukazuje, ako sa S/MIME využíva na zabezpečenie dôvernosti.



Zabezpečenie dôvernosti pomocou S/MIME

6.3 Zhrnutie

V tejto kapitole boli stručne predstavené dva bezpečnostné protokoly (TLS a S/MIME), ktoré využívajú kombináciu asymetrickej a symetrickej kryptografie. V oboch prípadoch je autentizácia poskytnutá prostredníctvom digitálnych certifikátov a šifrovanie užívateľských dát je realizované pomocou symetrickej kryptografie.

7 Ochrana voči okolitému prostrediu

7.1 Úvod do firewallov

Jedno z najviac rozšírených a opisovaných bezpečnostných opatrení využívaných na Internete je „firewall". Firewally získali povesť všeobecného lieku na mnoho, ak nie na všetky, bezpečnostné problémy Internetu. Avšak nie sú všeliekom. Firewally sú len ďalším nástrojom pri hľadaní vhodných nástrojov systémovej bezpečnosti. Úroveň bezpečnosti, ktorú firewall poskytuje sa môže meniť podobne, ako sa môže meniť bezpečnosť konkrétneho počítača. Existujú tradičné súvislosti medzi bezpečnosťou, jednoduchým používaním, cenou, zložitosťou, atď.

Firewall je zariadenie používané na zabezpečenie vnútornej siete organizácie. Tento spôsob ochrany je realizovaný oddelením internej siete od vonkajšieho okolia, alebo Internetu. Všetky správy vstupujúce do alebo odchádzajúce z internej siete cez firewall sú skúmané s cieľom analyzovať, či tieto správy spĺňajú špecifické bezpečnostné pravidlá.

Pred inštaláciou firewallu musí organizácia, ktorá plánuje ochranu pomocou firewallu, mať pravidlá, ktoré zabezpečia ochranu jej majetku, počítačových systémov, osobných informácií a ďalších citlivých dát. Táto množina pravidiel tvorí bezpečnostnú politiku. Bez tohto dokumentu nie je možné pomocou firewallu sieť zabezpečiť.

Firewall môže realizovať dve činnosti. Môže buď blokovať komunikáciu, alebo ju povoliť. Všetka komunikácia z internej siete do vonkajšej siete (Internetu) je zvyčajne povolená, ale ak je bezpečnostnou politikou zakázaná, môže niekedy brániť spojeniam na nedôveryhodné stránky alebo miesta považované za bezpečnostnú hrozbu alebo pre organizáciu inak nevhodné. Naopak, komunikácia iniciovaná z Internetu do internej siete je zvyčajne zakázaná. V ďalších moduloch bude diskutované, ako firewally tento cieľ dosahujú a ako sú v tejto činnosti efektívne. Taktiež budú diskutované výhody a nevýhody firewallov.

7.2 Systémy na detekciu prienikov

Zabezpečovanie bezpečnosti sa stáva čoraz náročnejšie, pretože potenciálne techniky útokov sú stále prepracovanejšie. Zároveň novým útočníkom stačia na realizáciu útoku menšie technické schopnosti, keďže v minulosti úspešné metódy sú ľahko dostupné prostredníctvom Webu. *Systémy na detekciu prienikov* (**IDS - *Intrusion Detection Systems***) sa vyvíjajú ako odpoveď na neustále sa zvyšujúci počet útokov na hlavné počítačové systémy, stránky a siete.

IDS je system na mmenežovanie bezpečnosti počítačov a sietí. IDS zbiera a analyzuje informácie z rôznych miest v rámci počítača alebo siete s cieľom identifikovať potenciálne bezpečnostné narušenia, vrátane zneužitia (útoky z vnútra organizácie) a prienikov (útoky z externého prostredia).

IDS využíva určenie slabých miest, čo je technika vyvinutá na ohodnotenie bezpečnosti nejakého počítačového systému alebo siete.

Funkcie na detekciu prieniku zahŕňajú:

- monitorovanie a analýzu aktivít užívateľa a systému,
- analýza systémových konfigurácií a zraniteľnosti,
- ohodnotenie integrity systému a súborov,
- schopnosť rozpoznať vzory typických útokov,
- analýza vzorov abnormálnej aktivity,
- sledovanie narušenia užívateľských zásad.

Systém na detekciu prienikov (**IDS**) sleduje všetku do vnútra smerujúcu a odchádzajúcu sieťovú aktivitu a identifikuje podozrivé príznaky, ktoré môžu indikovať nejaký sieťový alebo systémový útok, pomocou ktorého sa niekto pokúša preniknúť do systému alebo kompromitovať ho.

Existuje niekoľko spôsobov kategorizácie IDS:

Detekcia zneužitia vs. detekcia anomálii

- **Detekcia zneužitia:** IDS analyzuje získané informácie a porovnáva ich voči veľkej databáze „podpisov“ útokov (attack signatures). V podstate, IDS hľadá nejaký špecifický útok, ktorý už bol dokumentovaný. Technika na detekciu prienikov založená na podpise útoku ja založená na hľadaní „podpisov“ (nejaká typická charakteristická postupnosť útoku) vo všetkej komunikácii, ktorá prechádza sieťou. Umožňuje aj detekciu útokov na aplikačnej úrovni. Podobne ako systémy na detekciu vírusov, softvér na detekciu zneužitia je len taký dobrý ako je dobrá databáza podpisov útokov, voči ktorým porovnáva pakety a tak systém zahrňuje aj údržbu a aktualizáciu databázy podpisov

útokov. Častá aktualizácia tejto databázy v zariadeniach, ktoré využívajú túto technológiu tak má najvyššiu dôležitosť pre úspešné využitie tejto techniky.

- **Detekcia anomálii:** systémový administrátor definuje základný alebo normálny stav sieťovej prevádzky, výpadky a typické veľkosti paketov. Detektor anomálii monitoruje sieťové segmenty porovnávaním ich stavu so základným a vyhľadáva anomálie.

Sieťovo-orientované vs. počítačovo-orientované systémy

- *Šieťovo-orientované (NIDS - Network-based system)*: individuálne pakety prechádzajúce sieťou sú analyzované. NDIS môže zdetegovať škodlivé pakety navrhnuté tak, aby boli prehliadnuté jednoduchými filtračnými pravidlami firewallu.

- *Počítačovo-orientované systémy (HIDS)*: IDS overuje všetky aktivity na každom individuálnom počítači.

Pasívne systémy vs. reaktívne systémy

- *Pasívne systémy*: IDS deteguje potenciálne bezpečnostné narušenia, zaznamenáva informácie a signalizuje výstrahy.

- *Reaktívne systémy*: IDS reaguje na podozrivé aktivity odhlásením užívateľa alebo reprogramovaním fireallu tak, aby blokoval sieťovú prevádzku z predpokladaného škodlivého zdroja.

Nasledujúci obrázok ukazuje schému siete s firewallom a IDS.

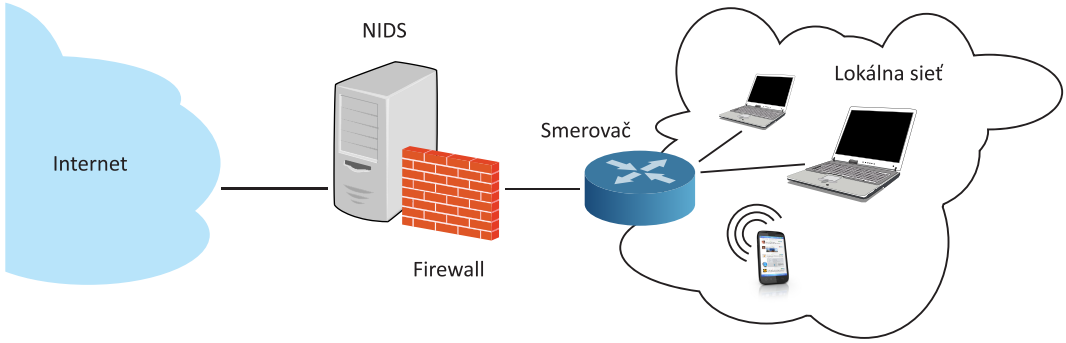


Schéma siete s firewallom a IDS

IDS sa líši od firewallu v tom, že firewall vyhľadáva aktivity na to aby zastavil ich vykonávanie. Firewall obmedzuje prístup medzi sieťami aby zabránil prienikom a nesignalizuje útoky z vnútra siete. IDS vyhodnocuje podozrivé vniknutia ktoré nastali a signalizuje ich alarmom. IDS sleduje tiež útoky, ktoré vznikajú vo vnúti siete.

7.3 Zhrnutie

V tejto kapitole boli diskutované typické riešenia prijaté s cieľom poskytnúť ochranu voči okolitému prostrediu (perimeter security). Táto ochrana predtavuje množinu hardvérových, softvérových a pragmatických bezpečnostných postupov, ktoré poskytujú určitú úroveň ochrany voči škodlivým aktivitám z okolitého prostredia. Okrem toho boli opísané hlavné vlastnosti firewallov a systémov na sledovanie prienikov, a tieto boli klasifikované v závislosti na rôznych kritériách.

8 Bezpečnosť bezdrôtových sietí

8.1 Bezdrôtové siete

Bezdrôtové siete (**WLAN**) sú v súčasnosti veľmi populárne, pretože podporujú mobilitu v rámci rozsahu bezdrôtovej siete a bezdrôtových pripojení koncových zariadení.Toto ponúka možnosť využívať sieť služieb a Internetu takmer všade a využíť dátovú a hlasovú komunikáciu.

Výhody bezdrôtovej komunikácie predstavujú však tiež vysoké bezpečnostné riziká vyplývajúce z dostupnosti rádiových signálov v rámci dosahu bezdrôtovej siete. Z týchto dôvodov je bezpečnosť bezdrôtových pripojení veľmi aktuálna téma.

WLAN bezpečnosť zahrňuje tieto dôležité úlohy:

- *zabezpečenie dôvernosti* alebo šifrovanie obsahu komunikácie,
- *autentizácia užívateľa* alebo riadenie sieťového prístupu.

Je dôležité poznamenať, že takmer všetky typy útokov vo WLAN sieťach sú vedené z vnútornej siete.

8.2 Bezpečnosť bezdrôtových sietí

Bezpečnosť bezdrôtových sietí zahrňuje tieto hlavné oblasti:

- **autentizácia,**
- **dôvernosť,**
- **manažment kľúčov.**

Autentizácia je proces, ktorým sa užívateľ pripája do WLAN siete; výsledkom je úspešné alebo neúspešné pripojenie užívateľa.

Dôvernosť vo WLAN sieťach je realizovaná s využitím šifrovania. Najčastejšie využívané algoritmy šifrovania sú **RC4** (**WEP**) a **AES** (**WPA2**).

Manažment kľúčov zahŕňa distribúciu a generovanie kľúčov.

8.3 WEP Protokol

WEP (*Wired Equivalent Privacy*) protokol je používaný ako voliteľný doplnok IEEE štandardu 802.11a/g/b a je navrhnutý na riadenie prístupu do WLAN a zabezpečenie dôvernosti prenášaných dát.

Zahrňuje služby na zabezpečenie autentizácie a dôvernosti:

- **WEP autentizácia**
  WEP autentizácia môže byť realizovaná dvoma spôsobmi, ktorými sú:
  - otvorená autentizácia,
  - zdieľaný kľúč.

Otvorená systémová autentizácia využíva iba sieťový identifikátor SSID. SSID nie je heslo, je to iba identifikátor bezdrôtovej siete. *Bezdrôtový prístupový bod* (**WAP -** *Wireless Access Point*) vysiela tento identifikátor v intervale každých niekoľko sekúnd.

V otvorenom autentizačnom móde užívateľ vysiela autentizačný rámec 802.11, ktorý obsahuje identifikačné dáta užívateľa. WAP kontroluje ID užívateľa a rámec potvrdzujúci alebo zamietajúci prístup do WLAN je zasielaný späť užívateľovi.

Zdieľaný autentizačný WEP kľúč využíva 40-bitový zdieľaný tajný kľúč, ktorý je identický pre všetkých WLAN užívateľov a je distribuovaný ku všetkým užívateľom nejakým bezpečným spôsobom. Autentizácia overuje identitu sieťovej karty koncového zariadenia.

- **WEP šifrovanie**

WEP protokol používa symetrickú šifru RC4, ktorá využíva na šifrovanie dát 64- alebo 128-bitový kľúč. Kľúč je zložený z tajného 40- alebo 104-bitového kľúča a 24-bitového *inicializačného vektora* (**IV**).

WEP protokol je napadnuteľný známymi útokmi (monitorovanie aktivity, metóda totálnych skúšok, opakovaný útok, atď. …) a šifra RC4 bola prelomená v roku 1996.

8.4 WPA Protocol

WPA (*Wi-Fi Protected Access*) protokol bol prijatý v roku 2002 s cieľom eliminovať zraniteľnosť WEP protokolu. Tento protokol bol prijatý ako prechodné riešenie, keďže v tom čase už prebiehali práce na novom štandarde IEEE 802.11i (schválenom v roku 2004). WPA protokol je podmnožinou 802.11i štandardu, takže implementácia 802.11i štandardu nevyžaduje žiadne zmeny v technických prostriedkoch. Zmeny sú nevyhnutné len na úrovni softvéru alebo firmvéru.

Podobne ako WEP protokol používa aj WPA protokol šifru RC4, využíva však ďalšie nové bezpečnostné mechanizmy. Hlavné časti WPA protokolu sú:

TKIP (*Temporary Key Integrity Protocol*),

- *kontrola integrity správy* (**MIC -** *Message Integrity Check*),
- riadenie prístupu založené na 802.1x štandarde s **EAP protokolom** (*Extensible Authentication Protocol*).

8.5 802.11i (WPA2) protokol

802.11i štandard, tiež nazývaný WPA2, kombinuje mechanizmy 802.1x a TKIP. Tento štandard používa 128-bitovú blokovú šifru AES.

Štandard 802.11i má zo štrukturálneho pohľadu podobnú štruktúru ako WPA a prináša nové vlastnosti ako napr. CCMP protokol a selektívnu incializáciu autentizácie, ktorá zaručuje rýchly a bezpečný roaming medzi prístupovými bodmi.

Hlavné mechanizmy služby bezpečnosti štandardu 802.11i sú:

- autentizácia,
- šifrovanie,
- integrita.

8.6 Zhrnutie

V tejto kapitole boli prezentované bezpečnostné rizika spojené s využívaním bezdrôtových komunikačných sietí. V prípade bezdrôtovej LAN boli prijaté rôzne riešenia zabezpečenia, aj keď niektoré z nich, napr. WEP protokol sú napadnuteľné radom útokov. Najakceptovanejším riešením na zabezpečenie rôznych bezpečnostných požiadaviek pre tento scenár je použitie štandardu 802.11i známeho tiež ako WPA2.