Slovenská technická univerzita v Bratislave
Fakulta Elektrotechniky a Informatiky
Študijný odbor INFORMATIKA

Radovan Semančík

Ochrana privátnych sietí proti útokom z Internetu

Dokumet k diplomovému projektu "Ochrana proti prienikom v dátových sieťach"

máj 1999

Obsah

1 Úvod

Medzinárodná počítačová sieť Internet sa od svojich počiatkov v 60-tych rokoch prudko rozvíjala až do podoby akú poznáme dnes. Internet sa stal mnohoúčelovou sieťou, ktorá je využívaná na získavanie obchodných informácií, ponuky služieb, zábavu, osobnú aj profesionálnu komunikáciu a na mnoho iných účelov. Funkčnosť tejto rôznorodej siete je však vo veľkej miere založená na vzájomnej dôvere účastníkov, poskytujúc len minimálne prostriedky na zabezpečenie toho, čomu sa v poslednom čase začína hovoriť *informačná bezpečnosť*.

Čoraz viac organizácií si uvedomuje, že pripojenie sa k tejto gigantickej sieti sa stáva nutnosťou na plnohodnotnú komunikáciu so svojimi partnermi a prísun aktuálnych informácií z okolitého sveta. Až donedávna si len niekoľko odborníkov uvedomovalo, aké riziká môžu vzniknúť pri pripojení sa k sieti Internet.

Predpokladá sa, že čitateľ má základné znalosti z oblasti počítačových sietí, konkrétne TCP/IP sietí. Ďalej sa predpokladajú základné znalosti činnosti operačných a informačných systémov ako aj bežných služieb siete Internet (E-mail. WWW. FTP, atď).

Anglické termíny použité v práci sú uvedené *kurzívou*. Veľká väčšina týchto termínov je v texte preložená, ak existuje slovenský ekvivalent alebo zmysluplný preklad. Výnimkoj je slovo “firewall”, ktorého slovenský ekvivalent neexistuje. Toto slovo sa používa v tomto tvare v celej publikácií.

2 Protokoly rodiny TCP/IP a bezpečnosť

Rodina protokolov TCP/IP sa stala najpoužívanejším protokolovým systémom pre veľké prepájané siete - internety. Už od prvopočiatkov svojho návrhu boly tieto protokoly orientované hlavne na funkčnosť. Bezpečnostné prostriedky boli do týchto protokolov pridávané dodatočne a ako bude neskôr popísané ani zďaleka neriešia všetky problémy.

Bezpečnosť akéhokoľvek systému možno vyjardiť pomocou troch základných vlastností: dostupnosti (*availability*), privátnosti (*confidentiality*) a integrity (*integrity*). Porušením aspoň jednej z týchto vlastností znamená porušenie celkovej bezpčnosti systému. Útoky zamerané na porušenie dostupnosti sa nazývajú "vyradenie z činnosti" (*denial of service*). Útoky zamerané na porušenie privátnosti alebo integrity sú v prostredí Internetu väčšinou klasifikované ako "prieniky" (*penetration*).

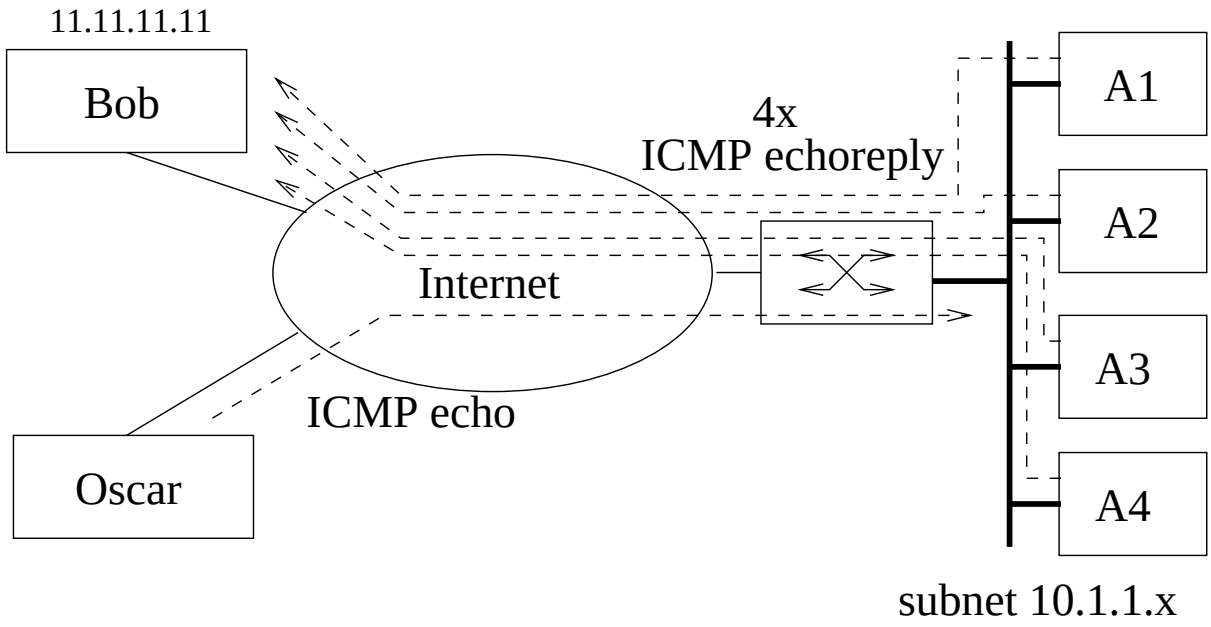
Útoky využívajúce chyby protokolov do štvrtej (transportnej) úrovne sú väčšinou zamerané len na vyradenie z činnosti, pretože bez znalosti protokolu vyššej úrovne nie je možné získať veľké výhody. Útoky na protokoly vyššej úrovne (väčšinou aplikačné protokoly) majú charakter prieniku, časté sú však aj útoky zamerané na vyradenie z činnosti.

2.1 Vyradenie z činnosti

Útoky zamerané na vyradenie z činnosti (*denial of service*, *DoS*) majú za cieľ odopretie legitímneho prístupu k zdroju alebo službe. Väčšinou sú realizované vyčerpaním všetkých dostupných zdrojov, ktoré sú nevyhnutné na realizáciu služby alebo prístup k nej. Tieto útoky sú väčšinou ľahko realizovateľné a ťažko sa im dá zabrániť, napriek tomu však väčšinou nepredstavujú vážnu hrozbu.

2.1.1 ICMP bombardovanie

Správy protokolu ICMP (Internet Control Message Protocol, [9]) slúžia na základné ovládanie a diagnostikovanie sietí založených na protokoloch rodiny TCP/IP a sú ich neoddeliteľnou súčasťou. ICMP protokol však neposkytuje ani základné bezpečnostné prostriedky a preto je ho možné zneužiť na neoprávnené ciele. Najčastejšie zneužívanými ICMP správami sú správy *ICMP redirect* a *ICMP host/network unreachable*. Tieto správy informujú svojho príjemcu o zmene smerovania v sieti a o nedosiahnuteľnosti vzdialeného uzla alebo siete. Správa *ICMP redirect* sa dá vhodne využiť na manipuláciu smerovacích tabuliek cieľovej stanice a tak vyradiť jej komunikáciu po sieti nesprávnym prenastavením smerovania. Táto technika sa navyše dá využiť aj na uľahčenie útoku *IP spoofing* popísaného v kapitole 2.2.2. Správy *ICMP host/network unreachable* sa dajú využiť na uzavretie existujúcich spojení cieľového uzla vhodným manipulovaním s obsahom správ. Pomocou techniky *IP spoofing* je možné jednoducho nasimulovať takúto



Obrázok 1: Smurfing

správu, tak ako keby ju odoslal jeden z legitímnych zdrojov týchto správ (napr. smerovač) a tým dosiahnuť okamžité uzatvorenie spojenia (útok *nuke*).

Ďalším útokom založeným na využití ICMP správ je *smurfing* [2]. Tento útok je založený na posielaní *ICMP echo* správ so sfalšovanou zdrojovou IP adresou na *broadcast* adresu rozsiahlej siete. Príklad takéhoto útoku je znázornený na obrázku 1. Útočník z uzla OSCAR vyšle falošný *ICMP echo* paket so zdrojovou adresou uzla BOB. Tento paket má cieľovú adresu nastavenú na *broadcast* adresu siete s veľkým počtom uzlov. V našom príklade je to sieť 10.1.1.x, takže cieľová adresa paketu bude 10.1.1.255. Každý aktívny uzol na tejto sieti prijme *ICMP echo* paket a bude sa snažiť naň odpovedať. Keďže zdrojová adresa v tomto pakete bola adresa uzla BOB, všetky uzly na sieti 10.1.1.x pošlú *ICMP echoreply* paket uzlu BOB. Pri dostatočne veľkom počte uzlov toto môže viesť k zahlteniu uzla BOB, keďže tento dostane všetky pakety približne v rovnakom čase. Rovnako táto záplava paketov môže viesť k zahlteniu liniek medzi uzlom BOB a sieťou 10.1.1.x. Veľká výhoda tohto útoku je, že každý útočníkov paket sa znásobí počtom aktívnych uzlov na sprostredkujúcej sieti (počet uzlov A). Ochrana proti tomuto útoku je účinná len na smerovači siete 10.1.1.x, uzol BOB sa proti útoku nemôže účinne brániť inak ako zakázaním *ICMP echoreply* paketov, čo vedie k obmedzeniu diagnostických možností.

Väčšine týchto útokov sa nedá priamo zabrániť. Ich rozsah sa však dá obmedziť pomocou vhodnej konfigurácie smerovačov siete a uplatnením príslušnej bezpečnostnej politiky. Tieto protiopatrenia sú detailnejšie popísané v kapitolách 4.2 a 4.1.

2.1.2 Aplikačné bombardovanie

Technika aplikačného bombardovania (application bombardment) je založená na vyčerpaní dostupných zdrojov na uzle poskytujúcom určitú službu. Útočník vytvorí veľký počet požiadaviek na službu, ktorá je náročná na prostriedky na cieľovom uzle. Na príklade servera s operačným systémom UNIX to môže byť napríklad SMTP server *sendmail* alebo iný pamäťovo alebo procesorovo náročný obslužný program služby, ktorý sa spustí pri každej novej požiadavke. Pri úspešnom útoku vznikne situácia, keď uzol bude mať všetky dostupné prostriedky obsadené falošnými požiadavkami na služby a pre legitímnu požiadavku na službu už nebude mať voľné prostriedky a odmietne ju.

Tak ako v predchádzajúcom prípade ani v tomto neexistuje univerzálne a jednoduché riešenie problému tohto útoku. Istá možnosť je implementácia obmedzení založených na zdrojových IP adresách požiadaviek, ale ani to nie je spoľahlivá metóda pri použití techniky *IP spoofing*.

2.1.3 SYN záplava

SYN záplava (*SYN flooding, [5]*) je technika založená na zaplavovaní cieľového uzla čiastočne otvorenými TCP spojeniami. Na strane cieľového uzla je polootvorené spojenie asociované s dátovou štruktúrou, ktoré zaberá drahocené prostriedky jadra operačného systému. Táto dátová štruktúra zaberá prostriedky na niekoľko minút, kým je konečne uvoľnená. Pomocou záplavy veľkého množstva SYN paketov je možné na cieľovom uzle vytvoriť veľké množstvo čiastočne otvorených spojení za krátky čas a tým alokovať až kritické množstvo "privilegovaných" prostriedkov operačného systému. Takéto rýchle vyčerpanie prostriedkov vedie pri menej stabilných operačných systémoch až k celkovému zlyhaniu operačného systému (tzv. "crash"). SYN pakety majú pre útočníka výhodu v tom, že sú malé a preto je možné využiť aj relatívne úzke prenosové pásmo na účinný *SYN flooding* útok.

Možnosť obrany proti záplave SYN paketov je značne obmedzená. Niektoré spôsoby ochrany sú popísané v kapitole 4.2.

2.1.4 Chyby implementácií TCP/IP

Kvalita implementácií protokolov rodiny TCP/IP sa značne líši. Niektoré implementácie nesledujú dokonale špecifikácie protokolov TCP/IP a obsahujú chyby, ktoré môže útočník využiť na vyradenie cieľového uzla z činnosti. Jedným z prvých útokov tohto typu bol útok nazvaný *ping of death* ([3]) podľa programu *ping* používanom na diagnostiku siete pomocou ICMP správ *ICMP echo* a *ICMP echoreply*. Útok využíva veľké ICMP pakety, ktoré po prijatí zraniteľným systémom spôsobia pretečenie vyrovnávacích pamätí a prepísanie

kritických štruktúr postihnutého operačného systému. Ďalší útok bol zameraný na chybu implementácie protokolu TCP v operačnom systéme Microsoft Windows. Tento útok bol pomenovaný *winnuke* a zakladal sa na fakte, že spomínaný operačný systém nevedel korektne spracovať dáta mimo TCP kanál (out of band data). Po prijatí týchto dát sa operačný systém začal správať nekorektne a nestabilne.

Chyby implementácie protokolov sa odstraňujú relatívne jednoducho, je však k tomu potrebná spolupráca výrobcu operačného systému. Hlavný problém je v tom, že tieto chyby sa ľahko využívajú a nie všetci správcovia systémov ich včas odstraňujú.

2.2 Impersonifikácia

Útoky založené na impersonifikácií využívajú falšovanie identity legitímneho používateľa prostriedku alebo služby útočníkom. Dopady útokov používajúcich tieto techniky sú veľmi vážne, keďže umožňujú útočníkovi neobmedzený prístup k prostriedkom, ktoré by mal k dispozícií legitímny používateľ.

2.2.1 Premenovanie stanice

Premenovanie stanice je najmenej náročná technika útoku. Zakladá sa na zmene IP adresy pracovnej stanice a tak získaniu všetkých privilégií založených na kontrole IP adries. Kontrolu IP adries ako jediný autentifikačný mechanizmus používajú napríklad protokoly NFS, SMTP, rlogin, rsh, atď. V prípade, že pracovná stanica obete je pred útokom aktívna, je ju možné vyradiť jedným z útokov zameraných na vyradenie z činnoti popísaných v kapitole 2.1. Na úspešnú realizáciu takéhoto útoku však musí byť útočník na rovnakej podsieti ako jeho obeť alebo musí vhodne manipulovať so smerovacími tabuľkami okolitých smerovačov.

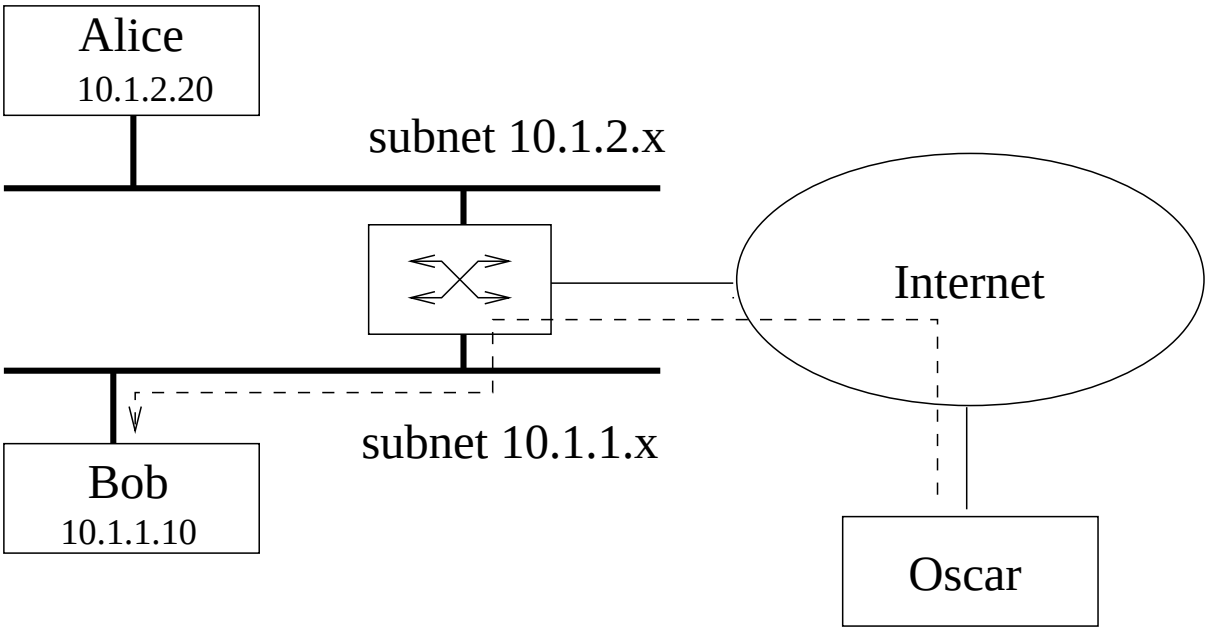
Tento útok je schopný realizovať aj menej skúsený útočník s vhodným prístupom k lokálnej sieti. Niektoré techniky ochrany proti tomuto útoku sú popísané v kapitole 4.8.

2.2.2 IP spoofing

Technika *IP spoofing ([5])* sa zakladá na falšovaní IP paketov so zámerom získať výhodu pri použití "výhodnejšej" zdrojovej adresy. Výhodnosť tejto IP adresy môže spočívať v tom, že jej obeť útoku dôveruje, falšovanie slúži na prechod cez filtre firewallu alebo slúži len na maskovanie reálneho zdroja útoku.

Bližšie túto techniku ilustruje obrázok 2. Uzol BOB je nakonfigurovaný tak, že dôveruje uzlu ALICE, čiže na uzle BOB sa už nerobí dodatočná kontrola prístupu, ak pristupuje užívateľ z uzla ALICE[1]. Uzol OSCAR sa snaží tento vzťah dôvery využiť a vytvorí paket

[1] Toto nastavenie zodpovedá napríklad službe *rlogin* alebo *NFS*.



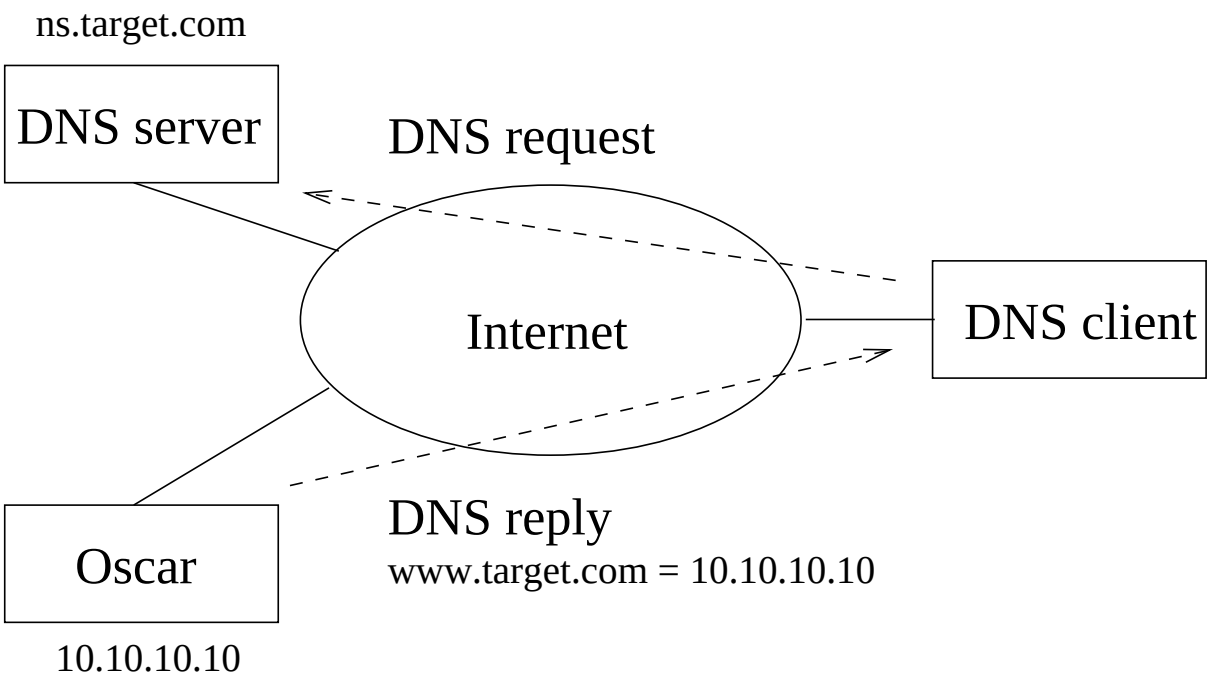
Obrázok 2: IP spoofing

so žiadosťou na nadviazanie TCP spojenia (SYN paket) so zdrojovou adresou uzla Alice (10.1.2.20) a cieľovou adresou uzla Bob (10.1.1.10) a vyšle ho do siete. Paket bude sieťou smerovaný podľa cieľovej adresy tak ako to naznačuje čiarkovaná čiara na obrázku. Uzol Bob po prijatí paketu odpovie paketom (SYN-ACK), ktorý bude doručený uzlu Alice. Uzol Alice však takéto spojenie na uzol Bob neotváral a tak bude paket ignorovať. Útočník na uzle Oscar musí uhádnuť sekvenčné číslo, ktorým uzol Bob odpovedal uzlu Alice, čo sa však pri niektorých implementáciach dá ľahko odvodiť od sekvenčných čísel predchádzajúcich spojení. Oscar potom pošle ďalší sfalšovaný paket (ACK paket) pre uzol Bob so zdrojovou adresou uzlu Alice a tým sa vytvorí spojenie. Uzol Bob toto spojenie vidí ako keby bolo iniciované uzlom Alice a preto nerobí žiadne ďalšie opatrenia na jeho zabezpečenie. Aj keď útočník na uzle Oscar nevidí odpovede uzla Bob, môže týmto jednostranným spojením dosiahnuť svoje zámery. Napríklad útokom na službu rlogin môže vykonávať príkazy ľubovoľného používateľa systému Bob.

Bližšie informácie o útokoch na sekvenčné čísla, predikcií sekvenčných čísel a metódach obrany možno nájsť v [1].

2.2.3 Ovplyvňovanie DNS

Internetový doménový systém mien (*Domain Name System*, DNS) je určený na mapovanie doménových mien na ich príslušné IP adresy. Na svoju funkciu používa hlavne UDP datagramy, čiže komunikáciu bez nadviazania spojenia. Útok na systém DNS je založený na vytváraní falošných paketov podobne ako tomu bolo pri technike *IP spoofing*. Tento raz



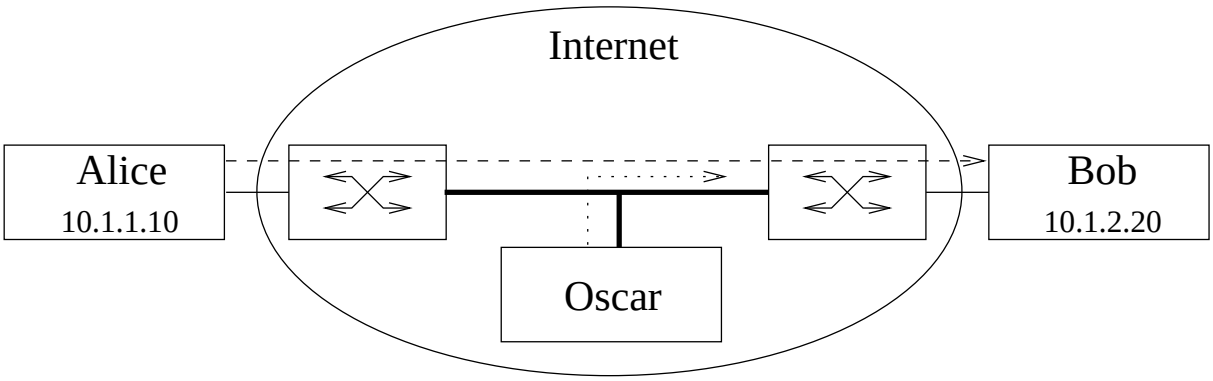
Obrázok 3: DNS spoofing

sa však vytvára falošná odpoveď na legitímnu požiadavku na rozlíšenie doménového mena. Útočník môže do takejto falošnej odpovede vložiť vlastnú IP adresu a tak impersonifikovať uzol, s ktorým sa chcel systém obete spojiť.

Tento spôsob útoku je bližšie znázornený na obrázku 3. Na tomto obrázku znázornený DNS klient je uzol v sieti obete zodpovedný za mapovanie doménových mien na IP adresy (*DNS name resolver*). Pri legitímnej požiadavke na zistenie adresy uzla *www.target.com* sa obráti s požiadavkom na DNS server *ns.target.com*. Útočník na uzle OSCAR môže vo vhodný časový okamih odpovedať falošným datagramom[2] so zdrojovou adresou zodpovedajúcou serveru *ns.target.com*, ktorá bude obsahovať falošné mapovanie mena *www.target.com* na IP adresu 10.10.10.10, čo je IP adresa uzla OSCAR. Keď sa niektorý uzol zo siete obete bude pri žiadaní WWW stránky odkazovať na meno www.target.com, spojí sa s uzlom s IP adresou 10.10.10.10, čo je uzol OSCAR a tento uzol mu poskytne falošnú WWW stránku obsahujúcu zavádzajúce informácie. Na zlepšenie účinku tejto techniky je možné server *ns.target.com* zahltiť alebo vyradiť z prevádzky aby nemohol včas odpovedať a zmariť útok. Prípadná možnosť monitorovania komunikácie DNS client – DNS server pomáha určiť vhodný časový okamih na spustenie útoku.

Ochranu proti tomuto útoku poskytuje rozšírenie služby DNS o bezpečnostné prvky (DNSSEC), ktoré je bližšie popísané v kapitole 4.5. Niektoré aplikačné protokoly (napr. SSL, SSH) riešia ochranu proti impersonifikácií vlastnými prostriedkami takže nie sú voči tomuto útoku zraniteľné.

[2]Služba DNS pracuje vo väčšine prípadov nad protokolom UDP.



Obrázok 4: Vkladanie paketov na siťové médium, prevzatie spojenia

2.2.4 Prevzatie spojenia

Prevzatie spojenia (*connection hijacking*) je technika zameraná na zmocnenie sa otvoreného legitímneho spojenia. Táto technika umožňuje pomocou falšovania paketov prevzať spojenie po tom ako prebehla úvodná autentifikácia a tak nadobudnúť práva používateľa ktorý spojenie autentifikoval. Tento útok má všetky charakteristiky útoku IP spoofing popísaného v kapitole 2.2.2, umožňuje však obísť aj úvodnú autentifikáciu. Prevzatie spojenia je aplikácia vkladania vhodných paketov na sieťové médium (*packet insertion*) tak ako to zobrazuje obrázok 4. Uzol ALICE vytvoril legitímne spojenie s uzlom BOB (čiarkovaná čiara). Útočník je umiestnený na uzle OSCAR, ktorý sa nachádza na trase po ktorej je spojenie ALICE–BOB transportované. Vo vhodnom okamihu po prebehnutí prvotnej autentifikácie na tomto spojení útočník začne posielať uzlu BOB pakety so zdrojovou adresou uzla ALICE (bodkovaná čiara na obrázku 4) ako keby to boli normálne TCP segmenty spojenia ALICE–BOB. Útočník môže odpočúvať odpovede uzla BOB a tak má úplnú kontrolu nad pôvodným spojením ALICE–BOB. Na zvýšenie efektivity útoku môže byť tesne pred začiatkom útoku uzol BOB zahltený alebo odstavený z prevádzky vhodným útokom zameraným na vyradenie z činnosti ako sú popísané v kapitole 2.1.

Vkladanie paketov sa nemusí obmedzovať len na TCP segmenty ako tomu bolo v prechádzajúcom príklade. Rovnako účinné je vkladanie aj v prípade IP fragmentov, kde sa táto technika dá využiť aj na oklamanie detekčného systému (*IDS*, kapitola 4.7) alebo firewallu.

Je dôležité si uvedomiť, že ani samotná silná autentifikácia (popísaná v kapitole 4.6) tento problém nerieši, keďže spojenie je možné prebrať až po jej prebehnutí. Tento problém je možné uspokojivo vyriešiť len zavedením techník zaručujúcich integritu ako je napríklad šifrovanie so spätnou väzbou alebo MAC (Message Authentication Code).

2.2.5 Falšovanie správ elektronickej pošty

Manipulácia so správami elektronickej pošty a konkrétne ich falšovanie (*e-mail forging*) je jedna z najjednoduchších a pritom najúčinejších techník impersonifikácie. Táto technika je založená na vytvorení falošnej e-mail správy a jej odoslaní príjemcovi pomocou SMTP protokolu. Na ilustráciu jednoduchého použitia tejto techniky je uvedený príklad ako ju môže realizovať ktorýkoľvek bežný používateľ moderného operačného systému.

```
evil% telnet mail.victim.com 25
Trying xxx.xxx.xxx.xxx...
Connected to mail.victim.com.
Escape character is '^]'.
220 mail.victim.com.sk ESMTP Sendmail 8.8.7/8.6.9 ready at Sat, 19 Dec 1998
11:43:32 +0100
HELO mail.whitehouse.gov
250 mail.victim.com Hello evil.com [yyy.yyy.yyy.yyy]
MAIL From: president@whitehouse.gov
250 president@whitehouse.gov... Sender ok
RCPT To: victim@victim.com
250 victim@victim.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: Your competition
Tu je vhodné doplniť ostatné potrebné hlavičky

Dear sir,

blah blah blah

Sincirely, Mr. President
.
250 LAA00736 Message accepted for delivery
QUIT
221 mail.victim.com closing connection
Connection closed by foreign host.
evil%
```

Tento útok je možné realizovať aj takmer úplne neznalým útočníkom a jeho detekcia je pri veľkom objeme elektronickej pošty značne náročná. Skutočná IP adresa odosielateľa

sa síce uloží do hlavičiek obálky e-mail správy, táto informácia sa však pri čítaní pošty jej konečným príjemcom nezobrazuje. Niekedy je dokonca možné použiť na odosielanie pošty rovnaké IP adresy ako by použil legálny používateľ (napr. dial-up prístup cez ISP) a tak už nie je technicky možné rozlíšiť legitímnu správu od falošnej.

Ochranou proti tomuto útoku je šifrovanie správ a metódy elektronického podpisu správ popísané v kapitole 4.5.

2.3 Techniky útokov

V nasledujúcich častiach budú popísané bežné techniky používané útočníkmi na získanie neoprávneneého prístupu do informačných systémov. Niektoré z týchto techník sú veľmi často používané a niektoré z nich sú založené viac na teoretickom ako praktickom základe. Každá z týchto techník je však plne realizovateľná a môže byť súčasťou terajšieho alebo budúceho útoku.

2.3.1 Mapovanie služieb

Mapovanie služieb a sietí (tzv. *portscanning*) slúži útočníkovi na "mapovanie terénu" siete obete. Táto technika poskytuje útočníkovi informácie o aktívnych uzloch na sieti, aktívnych poskytovaných službách, verziách obslužných programov a operačných systémov a mnoho iných dôležitých informácií. Na základe týchto informácií môže útočník identifikovať slabé miesta v informačnom systéme, ktorými môžu byť napríklad zastaralá vezria operačného systému alebo obslužného programu (*daemon-a*).

Jedna z najpoužívanejších techník je mapovanie dostupných uzlov pomocou ICMP správ *echo/echoreply* podobne ako to robí program *ping* a následné mapovanie otvorených TCP portov pomocou pokusov o pripojenie sa na každý z nich. Niektoré ďalšie techniky používajú na mapovanie SYN a FIN pakety, na mapovanie UDP portov sledujú výskyt ICMP správ oznamujúcich neexistenciu služby a využívajú možnosť servera FTP protokolu otvárať spojenia (tzv. *bouncing scans*). Bližší popis týchto techník je možné nájsť v dokumentácií [6].

Vyspelejšie techniky môžu byť použité aj na mapovanie filtračných pravidiel firewallu a uzlov za firewallom ako je bližšie popísané v dokumente [7].

2.3.2 Prienik

Po zmapovaní cieľovej siete a možných jej vstupných bodov nasleduje samotný prienik do jej infraštruktúry. Prienik sa väčšinou realizuje získaním dostatočných privilégií na jednom z uzlov siete. Definícia "dostatočných privilégií" sa môže značne líšiť podľa

druhu uzla a zámeru útoku. Ak je dotyčným uzlom napr. uzol s operačným systémom UNIX, tieto "dostatočné privilégiá " sú väčšinou privilégiá používateľa *root*, avšak pri operačnom systéme Microsoft Windows 95 a podobných je dostatočným privilégiom spustenie požadovaného procesu.

Na realizáciu prieniku a získanie týchto privilégií sa využívajú niektoré z nasledujúcich techník:

Využitie programátorskej chyby: využíva sa chyba v niektorom obslužnom programe operačného systému alebo v samotnom operačnom systéme. Veľká väčšina takýchto prienikov je založená na nedostatočnej kontrole vstupných údajov do obslužných programov. Často nastáva chyba pretečenia vyrovnávacích pamätí (*buffer overflow*) ktorá je založená na pretečení premennej vytvorenenj na zásobníku a vedie k prepísaniu obsahu zásobníku a tak aj návratovej adresy funkcie. Prevencia proti týmto chybám nie je jednoduchá keďže jazyk C ako najpoužívanejší jazyk na systémové programovanie neposkytuje žiadne podporné prostriedky na detekciu týchto chýb.

Využitie zlej konfigurácie uzla: V niektorých prípadoch sa stáva, že uzol pripojený do siete je nedostatočne nakonfigurovaný alebo je nakonfigurovaný nedostatočne kvalifikovanou osobou. Niektoré systémy prichádzajú k zákazníkovi nakonfigurované "štandardným" spôsobom, čo zahŕňa napríklad "dobre známe" používateľské a servisné heslá, prílišnú dôveru okolitým uzlom siete alebo implicitné aktivovanie nepotrebných a málo bezpečných služieb. Viac podrobností a ďalšie detaily o bezpečnostnej politike možno nájsť v kapitole 4.1.

Využitie ľudskej chyby: Ľudia v záujme uľahčenia a urýchlenia práce niekedy zabúdajú aj na základné bezpečnostné praktiky. Jedným z bežných príkladov je výber jednoduchých alebo stále rovnakých prístupových hesiel. Ak je prístupové heslo založené na skutočnom mene alebo prezývke používateľa, je jednoduché ho uhádnuť. Ak je heslo jedného používateľa rovnaké na všetkých uzloch, na ktoré má prístup, stačí kompromitovať jeden z uzlov a útočník má prítup aj na všetky ostatné uzly. Niekedy je bežné dokonca vytváranie prístupových účtov bez hesiel. Ďalšou pomerne rozšírenou praktikou je vytváranie "dočasných" prístupových privilégií, ktorých "dočasnosť" nie je dodržovaná. Príkladom môže byť vytváranie účtov stážistom alebo hosťujúcim špecialistom, na ktorých zrušenie sa zabudne, alebo zdielanie zdrojov pracovnej stanice do lokálnej siete bez obmedzenia prístupu. V tomto prípade môžu byť dokumenty na ich obvyklom úložnom mieste (servery) akokoľvek dobre ochránené, ich ochrana stráca na účinku v momente keď si používateľ vytvorí lokálnu kópiu dokumentu na svojej pracovnej stanici. Väčšine ľudských chýb je

možné zabrániť kvalitnou bezpečnostnou politikou a jej dôsledným vynucovaním ako je to popísané v kapitole 4.1.

Použitie hrubej sily: "Hrubá sila" (*brute-force) je* spôsob útoku na bezpečnostné machanizmy, ktorý sa snaží posupným skúšaním možností odhaliť správne hodnoty parametrov, ktoré zabezpečia útočníkovy prístup k cieľovému systému. Do tejto kategórie patria slovníkové útoky na heslá, hľadanie klúčov šifrovacích algoritmov, atď. Najčastejšie používané a aj najúčinnejšie sú práve slovníkové útoky na heslá, keďže používatelia si často vyberajú heslá založené na bežných slovách.

V praxi sa väčšinou používa kombinácia týchto techník na realizáciu účinného útoku na uzol. Napríklad útočník môže využiť heslo založené na krstnom mene jedného z používateľov na získanie bežného prístupu na UNIXový uzol a potom programátorskú chybu v jednom z obslužných programov nainštalovaných na tomto uzle na získanie privilégií *root*.

Súčasťou prieniku je aj zahladenie stôp, ktoré mohol prienik zanechať. Toto sa týka napríklad "čistenia" systémových log súborov, účtovacích a auditovacích záznamov.

2.3.3 Zabezpečenie pozícií

Po samotnom prieniku má už útočník dostatočné privilégiá na vykonanie svojho zámeru na uzle. Jeho cieľom však môže byť úplne iný uzol a práve kompromitovaný uzol môže byť len prostredníkom v útoku väčšieho rozsahu. Útočník má väčšinou záujem využívať výhody práve získaných privilégií aj v budúcnosti, pričom technika práve vykonaného útoku to buď neumožňuje (veľké riziko odhalenia) alebo je veľmi nepohodlná a neistá. Napríklad používateľ si môže svoje ľahko uhádnuteľné heslo zmeniť na niečo zložitejšie a útočník tým stratí prístup k uzlu alebo správca systému nainštaluje opravu programátorskej chyby, ktorú útočník využíval. Ďalšie riziká môžu pre útočníka vyplývať z jeho odhalenia či už náhodného alebo úmysleného.

Na zabezpečenie si neistých pozícií na práve napadnutom uzle slúžia programy nazývané zadné dvierka (*backdoor*) a trójske kone (*trojan*). Zadné dvierka sú programy, ktoré umožňujú útočníkovi kedykoľvek vstúpiť do systému tak, že premostia všetky bežné mechanizmy kontroly prístupu. Ako príklad môže slúžiť upravený program *login* v operačnom systéme UNIX, ktorý pustí bez zadania hesla každého, kto sa prihlási ako "hacker" a udelí mu práva používateľa *root*. Takýchto zadných dvierok môže útočník na uzol nainštalovať niekoľko, aby tak minimalizoval šancu ich odstránenia napríklad pri bežnom obnovovaní systémového softvéru. Trójske kone na druhej strane chránia útočníka pred rizikom odhalenia. Sú to programy, ktoré nahrádzajú bežné diagnostické programy operačného systému. Tieto programy sú však modifikované tak, že úmyselne nezobrazujú aktivity útočníka. Príkladom môže byť upravený príkaz *ps* v operačnom systéme UNIX, ktorý

zobrazuje všetky bežiace procesy. Tento príkaz môže byť modifikovaný tak, že nebude zobrazovať procesy spustené útočníkom. Podobne príkaz *ls* na zobrazenie obsahu adresára nebude zobrazovať súbory patriace útočníkovi. Takto možno modifikovať väčšinu bežných programov[3].

Súbory programov oboch typov sú voľne dostupné pre bežne používané operačné systémy a nevyžadujú od ich používateľov hlboké znalosti operačných systémov. Pre operačný systém Linux je napríklad k dispozícií súbor zadných dvierok a trójskych koňov pod názvom *root-kit* ktorý umožňuje dostatočne dobre zamaskovať útočníka pred neskúseným alebo nepozorným správcom. Rozšírenie tohto balíka na ostatné podobné operačné systémy je len otázkou času. Pre veľmi rozšírený operačný systém Microsoft Windows 95/98 je voľne k dispozícií produkt pod názvom Back Orifice [8], ktorý umožnuje vzdialenému útočníkovi manipulovať s týmto systémom ešte lepšie ako keby bol osobne za jeho konzolou. Tento program je navyše pre bežného používateľa Windows úplne neviditeľný a dokáže sa transparentne prenášať na hosťovských binárnych súboroch a neviditeľne inštalovať podobne ako vírus.

Riešením, ktoré obmedzuje útočníka v takejto modifikácií prostredia operačného systému a aplikácií je systém kontroly integrity, ktorý býva väčšinou systémom na detekciu neželaných aktivít (*Intrusion Detection System, IDS*) popísaných v kapitole 4.7.

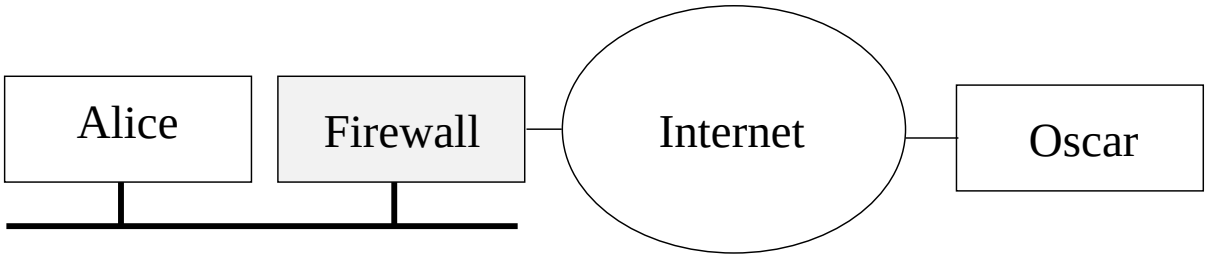
2.3.4 Odpočúvanie

Je bežné, že nie je možné zaútočiť priamo na uzol, ktorý obsahuje požadované informácie ale je nutné využiť niektorý zo slabšie zabezpečených uzlov siete ako prostredníka útoku. Útočník väčšinou získa dostatočné pozície na tomto uzle a z neho potom vedie ďalšie útoky. Tento uzol sa volí väčšinou tak, aby jeho umiestenie alebo spôsob používania poskytli útočníkovi výhody. Takýto pomocný uzol je výhodný ak si útok vyžaduje prekonanie firewallu a je takmer nevyhnutný pri prekonávaní demilitarizovaných zón.

Ak je tento pomocný uzol na rovnakej podsieti ako cieľový uzol a hardvér lokálnej siete to dovolí, je možné použiť diagnostické prostriedky siete na odpočúvanie komunikácie cieľového uzla s okolím. Takéto odpočúvanie je možné napríklad v sieťach typu *ethernet* za pomoci *promiskuitného módu* sieťového adaptéra, ktorý umožňuje prijímať všetky rámce na segmente[4]. Tento prístup je možné využiť na odpočúvanie terminálových spojení správcu cieľového uzla a tak získať prístupové parametre správcu systému (jeho prístupové meno a heslo) alebo aspoň získať informácie, ktoré uľahčia ďalší útok. Tieto informácie

[3]Toto neplatí len pre systémy distribuované spolu so zdrojovým kódom (*open source*) ale aj pre ostatné systémy. Nie je závažný technický problém vykonať pôvodný program a z jeho výstupu odfiltrovať "neželanú" informáciu o aktivite útočníka.

[4]tzv. *sniffing*. Jeho účinok sa podstatne obmedzí ak je použitý sieťový prepínač (*switch*), pozri kapitola 4.8.



Obrázok 5: Skytý kanál

môžu obsahovať napríklad zoznam uzlov, ktorým cieľový uzol dôveruje (*rlogin*, *rsh*, *NFS* a pod.) alebo zoznam používateľských účtov z e-mail správ.

Na odpočúvanie a zhromažďovanie informácií je možné použiť aj programy typu *trójsky kôň*. Napríklad pomocou upraveného programu *su* v operačnom systéme UNIX je možné zistiť heslá používateľov, ktorý tento príkaz používajú (hlavne používateľa *root*) a je značná šanca že títo používatelia budú mať rovnaké heslá aj na ostatných systémoch. Ďalším príkladom môže byť odpočúvanie pseudozariadenia *tty* alebo modifikovaný príkaz *telnet*, čo prináša rovnaké výsledky ako odpočúvanie sieťovej komunikácie.

2.3.5 Skryté kanály

Keď sa útočník dostane k informáciám ktoré hľadá, musí ich presunúť z miesta kde sú uložené na miesto kde k nim bude mať stály sprístup. Ak bol prienik realizovaný interaktívnym spojením je prirodzené využiť toto spojenie aj na presun informácií priamo na pracovnú stanicu útočníka. V niektorých prípadoch však útočník nemá k dispozícií spojenie zo svojou pracovnou stanicou. Takýto prípad môže nastať napríklad ak útočník získa metódou sociálneho inžinierstva dočasný fyzický prístup k informácií alebo jeho útok je realizovaný pomocou neinteraktívneho programu, napríklad trójsky kôň ukrytý v pomocnom programe poslanom správcovi systému v správe elektronicke pošty alebo vystavenom na FTP serveri.

V takýchto prípadoch musí útočník vytvoriť kanál smerom od úložiska informácie k pracovnej stanici útočníka alebo k pomocnému uzlu. V mnohých prípadoch je toto triviálna úloha, keďže väčšina systémov nepredpokladá hrozbu vo vnútornej "bezpečnej" zóne. V niektorých prípadoch to však nie je také triviálne, najmä ak sa jedná o systémy s oddelenými bezpečnostnými úrovňami (MLS alebo CMW) alebo ak je na predpokladanej ceste umiestnený dobre konfigurovaný kvalitný firewall. Tieto zariadenia nedovoľujú nekontrolovaný tok údajov ani smerom do vnútornej siete a ani smerom von z nej. Pre lepšiu ilustráciu techniky použitia skrytých kanálov predpokladajme konfiguráciu siete podľa obrázku 5. Firewall na obrázku je nakonfiguraný tak, že medzi vnútornou a vonkajšou sieťou prepúšťa len ICMP správy *echo* a *echoreply*. Útočníkov zámer je presunúť sú-

bor z vnútornej siete (z uzla ALICE) na vonkajšiu (na uzol OSCAR). Podľa špecifikácie protokolu ICMP [9] je do tela paketu ICMP echoreply skopírovaných 64 bajtov z pôvodného ICMP echo paketu. Útočník môže upraviť operačný systém na uzle ALICE tak, že namiesto skopírovania týchto dát z predchádzajúceho ICMP echo paketu tam vloží údaje z exportovaného súboru. Na vonkajšiej sieti potom už len stačí poslať sekvenciu legitímnych ICMP echo paketov smerom k systému ALICE, sledovať prichádzajúce pakety a vyberať požadovanú informáciu. V kombinácií so samoopravným kódom je to relatívne rýchly a spoľahlivý skrytý kanál. Modifikovať samotný operačný systém nemusí byť vždy jednoduchá úloha, takéto skryté kanály sa však dajú realizovať aj jednoduchšie v prostrediach, ktoré vynucujú slabšie obmedzenia na komunikáciu smerom von. Informácia sa dá napríklad exportovať pomocu *URI* používaných protokolom *HTTP*. V tomto prípade je možné informáciu zakódovať do adresy žiadanej stránky, napríklad:

```
http://oscar.evil.com/hack.cgi?data=A15C9F578D2C5A6DFF05
http://oscar.evil.com/hack.cgi?data=DD5E4C65AC4DF83E6D56
```

Postupnosťou takýchto žiadostí sa po častiach exportuje celý súbor. Nevýhoda tohto spôsobu je jeho nápadnosť. Dlhá postupnosť podobných žiadostí o stránky je ťažko prehliadnuteľná v záznamoch používania protokolu *HTTP* na firewalle. Na druhej strane je realizácia takéhoto kanála triviálne jednoduchá a vyžaduje len priemerné schopnosti útočníka.

Možností na vytváranie skrytých kanálov sú veľmi veľké a ich realizácia môže siahať od časového modulovania ACK segmentu v protokole TCP až po vytváranie prirodzene vyzerajúcich e-mail správ obsahujúcich skrytú informáciu[5]. Obmedzenie všetkých skrytých kanálov je veľmi náročné v väčšinou vyžaduje rozsiahle zmeny štruktúry systému. Vhodným výberom a konfiguráciou sieťových zábran (firewallov, aplikačných brán, atď.) je možné realizáciu takýchto kanálov podstatne sťažiť.

2.3.6 Sociálne inžinierstvo

Človek ako taký je väčšinou najslabším článkom akejkoľvek bezpečnostnej infraštruktúry. Ľudské chyby a skutočnosť že ľudia sa málokedy riadia presne podľa predpisov robia z ľudskej obsluhy informačných systémov veľmi lákavý cieľ. Sociálne inžinierstvo je technika zameraná na získavaní informácií pomocou presviedčania a podvádzania ľudského personálu.

Menej kvalifikovaný personál môže ľahko uveriť telefonátu z "technického oddelenia" so žiadosťou o prezradenie hesla nutného na odstráneniu nejakej závady. Aj technicky kvalifikovaný zamestnanec iste rád poskytne technické údaje o vnútornej sieti organizácie

[5]Napríklad použitie spojenia "bol som" znamená binárnu 1 a spojenie "som bol" znamená binárnu 0.

novému "kolegovi", ktorý dostal od neobľúbeného riadiaceho pracovníka ťažkú úlohu s krátkym časovým termínom. Možností ako podvodom získať požadované informácie je veľa a väčšinou jediné potrebné zariadenie na "útok" je telefón.

Obranou proti týmto útokom je dostatočné školenie personálu a vybudovanie prirodzených a bezpečných pravidiel spolupráce rôzneho personálu.

3 Hrozby a následky útokov

Útoky popísané v predchádzajúcej kapitole pôsobia dojmom, že pripojenie k sieti Internet prináša značné riziko a veľa problémov. Nemusí to byť nevyhnutne tak, ak si uvedomíme že značná časť popísaných útokov vyžaduje vhodné podmienky (napr. možnosť odpočúvať spojenie) a značne kvalifikovaného a motivovaného útočníka. Vhodne zvolené a kvalitne nakonfigurované bezpečnostné zariadenia a mechanizmy môžu odvrátiť väčšinu útokov a značne znížiť riziko prameniace z Internetového pripojenia. Táto kapitola sa bude zaoberať zhodnotením prostredia a podmienok súčasných organizácií, rizikami, ktoré podstupujú a následkami aplikácie hrozieb útokov.

Podľa štúdií realizovaných organizáciou Computer Security Institute ([10]) hrozba počítačovaj kriminality rok čo rok dramaticky rastie. Pripojenie do Internetu označilo ako častý zdroj útokov 57% organizácií pričom pri interných hrozbách to bolo len 55%.

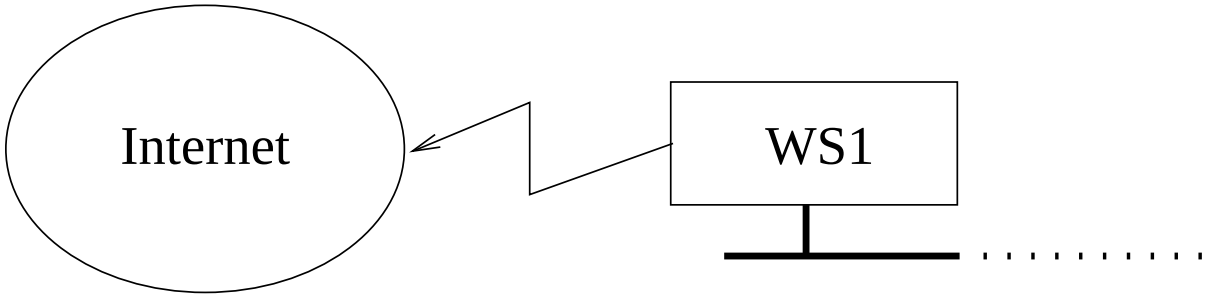
3.1 Prípadové štúdie

V nasledujúcich troch príkladoch bude zhodnotené ohrozenie a potreby malej, strednej a veľkej organizácie vzhľadom na hrozby prameniace z pripojenia k Internetu.

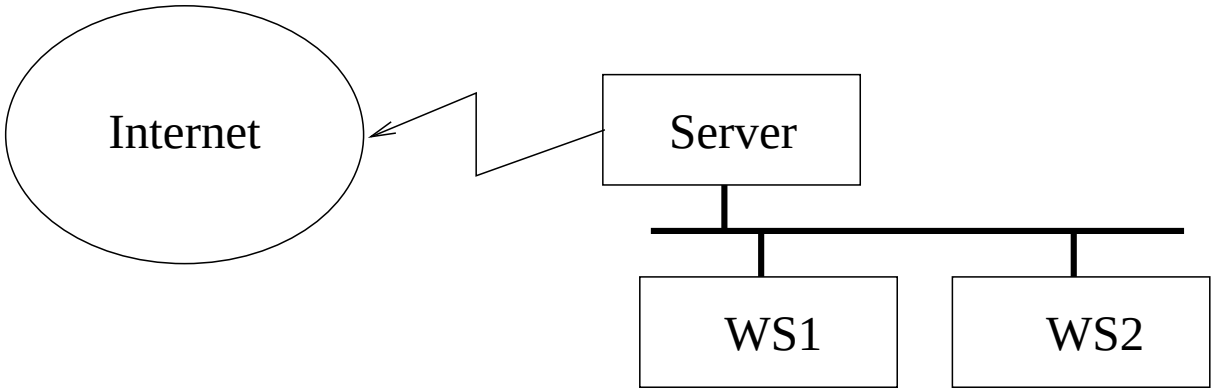
Terminológia použitá v týchto štúdiách je neformálna. Použitie formálnejšej terminológie by si vyžadovalo oveľa viac faktov a zdĺhavý proces ich zhromažďovania je ďaleko mimo rozsah tejto práce. V reálnych bezpečnostných štúdiách stredných a veľkých organizácií je použitie formálnej a strojovo spracovateľnej metodiky takmer nutnosť. Na podporu takýchto metodík boli vyvinuté automatizované systémy rizikovej analýzy, ktorých najvýznamnejšími zástupcami na našom trhu sú systémy MELISA, RiskPac a CRAMM. Všetky tieto systémy používajú podobnú metodiku a aj technickú realizáciu bezpečnostných projektov, MELISA je však jediný z týchto systémov prispôsobený pre naše jazykové podmienky. Postup projektu načrtnutý v kapitole 4.9 je tiež založený na metodike vedenia bezpečnostného projektu ako ju definuje systém MELISA [31].

3.1.1 Malá organizácia

Sieť malej organizácie väčšinou tvorí niekoľko pracovných staníc a jeden súborový server. Údaje sú ukladané na pevných diskoch pracovných staníc poprípade na disku servera. Pracovné stanice a súbory na nich a na serveri buď nie sú vôbec chránené alebo sú chránené jednoduchými heslami. Na spracovanie informácií sa väčšinou používajú široko dostupné kancelárske softvérové balíky. Prevládajúci operačný systém pracovných staníc je Microsoft Windows 95 (alebo obdobný) a prevládajúci operačný systém servera je Microsoft Windows NT.



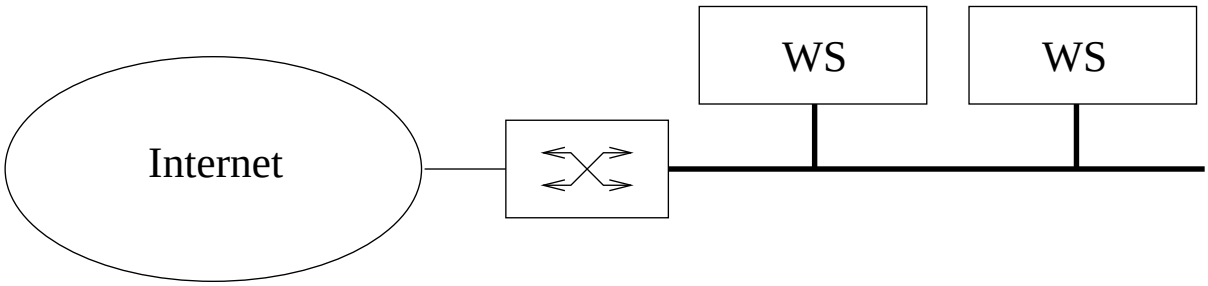
Obrázok 6: Pripojenie jednej pracovnej stanice



Obrázok 7: Pripojenie siete komunikačným serverom

Štruktúra pripojenia organizácie k sieti Internet je väčšinou realizovaná individuálnym pripojením jednej pracovnej stanice (obrázok 6) alebo inštaláciou "komunikačného servera" (obrázok 7). V oboch prípadoch sa jedná o pripojenie komutovanou linkou využívajúc buď štandardný modem alebo ISDN pripojenie. Spojenie je budované na žiadosť, väčšinou automaticky pri požiadavke komunikácie s Internetom. Spojenie je rušené po istom intervale nečinosti. V prípade pripojenia komunikačným serverom, môže túto úlohu zastávať buď samostatný vyhradený server alebo príslušný softvérový balík nainštalovaný na súborovom serveri organizácie. Celkovo možno zabezpečenie organizácie hodnotiť ako veľmi nízke.

Cena informácií uložených na pracovných staniciach a serveri organizácie je relatívne nízka. Prezradenie niektorých obchodných informácií malej organizácie môže spôsobiť problémy, málokedy však býva pre organizáciu kritické. Dostupnosť informácií je možné efektívne zabezpečiť zálohovaním na vymeniteľné médiá vzhľadom k malému objemu dát. Integritu informácií dokáže narušiť len skúsenejší útočník a keďže sa v takejto organizácií väčšina aktivít realizuje buď ručne alebo aspoň s ľudskou kontrolou, je malá pravdepodobnosť, že porušenie integrity nebude všas odhalené. Organizácia má svoje prezentačné WWW stránky umiestnené väčšinou na prenajatom mieste u svojho poskytovateľa služieb Internetu (*ISP*), ktorý je väčšinou vybavený kvalitnejším technickým zariadením



Obrázok 8: Pripojenie lokálnej siete do Internetu pomocou pevnej prenajatej linky

aj kvalifikovanejším presonálom ako samotná organizácia.

Motivácia útočníkov je vzhľadom k malej cene informácií v organizácií nízka. Väčšinou pôjde o jednoduché útoky zamerané na vyradenie z prevádzky, ktoré majú veľmi malý dopad vzhľadom na predpoklad že pripojenie k Internetu nie je strategický zdroj organizácie. Spojenie do Internetu je aktívne len v pracovnom čase, mimo neho teda hrozí len minimálne ohrozenie počas automatickej výmeny dávkových informácií (e-mail, news, atď).

Celkové ohrozenie takejto organizácie je malé. V každom prípade by však mali byť aktivované všetky bezpečnostné mechanizmy, ktoré používaný komunikačný softvér umožňuje. V prípade pripojenia komunikačným serverom je vhodnejšie použiť vyhradený server a to najlepšie s operačným systémom typu UNIX (Linux) alebo Microsoft Windows NT. Všetky komponenty pripojenia do Internetu by mali byť inštalované kvalifikovanou osobou čo by malo zaručiť ich správnu konfiguráciu. Dôraz tiež treba klásť na správnu voľbu poskytovateľa služieb Internetu (*ISP*).

3.1.2 Stredná organizácia

Organizácie strednej veľkosti má spravidla vybudovanú lokálnu počítačovú sieť (LAN) dostatočnej kvality. Pripojenie tejto siete do Internetu je vo väčšine prípadov realizované pevnou prenajatou linkou.Toto spojenie je trvalé a zaručuje stálu konektivitu. Spojenie ústia pevnej linky a lokálnej siete je väčšinou realizované jednoúčelovým smerovačom. Moderné smerovače používané vo väčšine inštalácií sú dobre hardvérovo aj softvérovo vybavené, ich konfigurácia a plné využitie ich možností však vyžaduje skúsenú ososbu. Pracovné stanice a servery v lokálnej sieti organizácie majú v niektorých prípadoch adresy vyčlenené na používanie v intranetoch (napr. 192.168.x.x alebo 10.x.x.x). V takýchto prípadoch smerovač realizuje preklad sieťových adries (Network Address Translation, NAT alebo tiež "masquerading"). V niektorých inštaláciach má smerovač nastavené prístupové zoznamy (Access Control Lists) a obmedzujú premávku na sieti podobne ako paketový filter (screening router). Zabezpečenie spojenia pevnou linkou je vo veľkej miere závislé od kvalitne zvládnutej konfigurácie smerovača a serverov vystavených do Internetu.

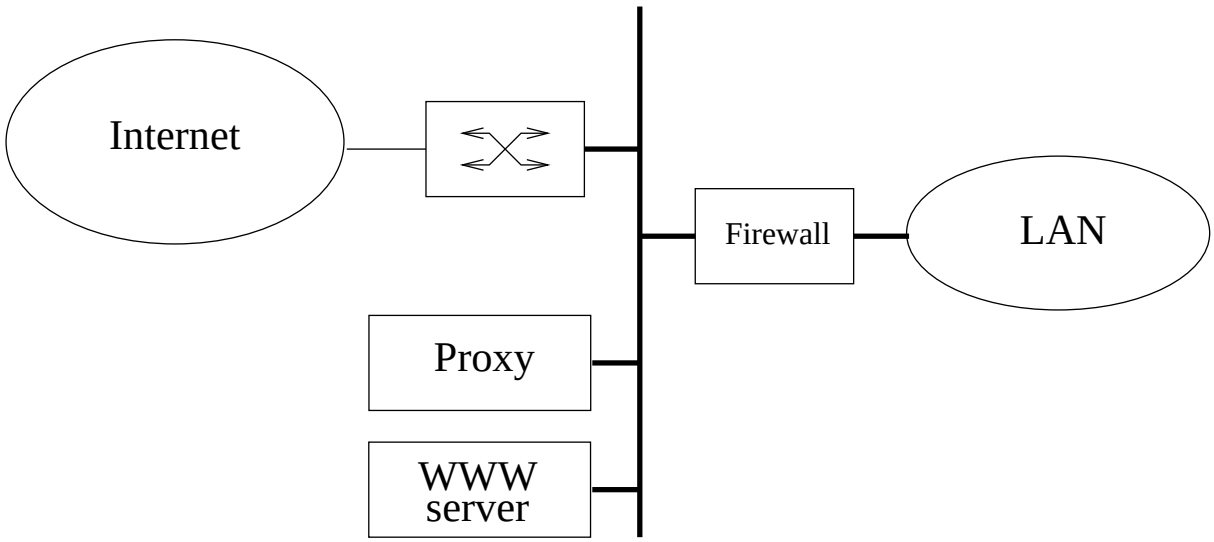
Väčšina dôležitých informácií strednej organizácie je uložená v súboroch na súborových serveroch organizácie a v databázach. Cena týchto informacií je veľmi variabilná, väčšinou sa však medzi nimi vyskytujú aj veľmi cenné firemné informácie. Niektoré informácie môžu dokonca podliehať zákonnej ochrane, ako je to pri osobných informáciach zamestnancov a zákazníkov alebo pri štátnom alebo služobnom tajomstve. Takmer žiadne z týchto dôležitých informácií nemusia byť a ani nie sú prístupné z Internetu a väčšinou sú aj systémy, na ktorých sú uložené, fyzicky oddelené od systémov poskytujúcich informácie do Internetu. Ohrozenie dôležitých informácií spočíva najmä v ich prezradení a možnosti ich zničenia. Zálohovanie niektorých druhov často sa meniacich informácií (účtovacie, žurnálové a auditačné údaje) môže činiť značné problémy. Určovanie ceny informácií v mnohých prípadoch však nie je triviálna úloha a je potrebné uvažovať o vyhotovení analýzy hodnôt a rizík. Viac o vedení bezpečnostných projektov je uvedené v kapitole 4.9.

Konkurencia na trhu v oblasti stredných firiem je dostatočne veľká aby sa vytvorili podmienky na dostatočnú motiváciu útočníka. Informácie uložené vo väčšine firiem predstavujú lákavý zdroj obchodných informácií poskytujúcich konkurenčnú výhodu. Pevné pripojenie k Internetu poskytuje stále pripojenie a tak je možné útok realizať mimo pracovného času a teda s minimálnym rizikom okamžitého odhalenia. Pri vhodnom časovaní má útočník k dispozícií dokonca niekoľko dní na útok a zahladenie jeho stôp. Nedostatočne alebo nekvalifikovane konfigurované zariadenia (smerovač, servery) nepredstavujú takmer žiadnu prekážku útoku.

Celkové ohrozenie organizácie závisí hlavne na dostatočnom využití inštalovaných technických prostriedkov a cene uložených informácií. Vo väčšine prípadov je však toto ohrozenie značné. Inštalovaný smerovač by mal mať možnosť vytvárania prístupových zoznamov (Access Control Lists) a mali by byť správne nakonfigurované. Správne nastavenie týchto zoznamov nie je triviálna záležitosť a táto úloha by mala byť zverená dostatočne kvalifikovanej osobe. Dôslednosť treba dodržovať aj pri konfigurácií serverov s údajmi vystavenými do Internetu (napr. WWW serverov).

3.1.3 Veľká organizácia

Veľké organizácie sa pripájajú k sieti Internet väčšinou vysokorýchlostnými ($\geq$ 128 kbps) pevnými linkami. Medzi Internetom a vnútornou sieťou organizácie sa takmer vo všetkých prípadoch vytvára špeciálna sieť, nazývaná demilitarizovaná zóna (DMZ). Spojenie linky z Internetu a DMZ je väčšinou realizované výkonným sperovačom s využitím jeho bezpečnostných funkcií (filtrovanie paketov). Na DMZ sú umiestnené systémy, ktoré k svojej činnosti potrebujú prístup aj do Internetu aj do privátnej siete. Na vnútornej strane DMZ je umiestnený kvalitný firewall, ktorý v niektorých prípadoch vykonáva aj kontrolu ob-



Obrázok 9: Pripojenie siete veľkej organizácie pomocu DMZ

sahu. Je takmer nevyhnutné, aby vnútorná sieť organizácie mala adresy pridelované z rozmedzia určeného pre privátne intranety. Preklad adries (NAT) sa väčšinou realizuje na vonkajšom smerovači a je staticky nastavený len na niekoľko nevyhnutných uzlov v sieti DMZ. Pri správnej konfigurácií sieťových zariadení a vhodnom zabezpečení serverov na DMZ je bezpečnosť takéhoto zapojenia relatívne vysoká. Pravdepodobnosť úspešného prieniku útočníka až do privátnej siete je veľmi malá.

Väčšina dôležitých informácií organizácie je uložená v privátnej sieti na veľkých súborových a databázových serveroch. Cena týchto informácií býva vysoká, jej presná hodnota sa však veľmi ťažko zisťuje. Samotná komplexnosť organizácie, jej vnútorných vzťahov a zlá viditeľnosť informačných tokov značne sťažujú analýzu hodnôt. Spoločným prvkom v týchto organizáciach však býva značné riziko prezradenia informácií a v niektorých odvetviach (financie) je značné aj riziko porušenia integrity informácií. Strata dostupnusti sa väčšinou nespája s veľkým rizikom, keďže väčšina dôležitých informácií je pravidelne zálohovaná a archivovaná.

Motivácia útočníkov je v tomto prípade najvyššia. Veľké objemy finančných tokov vo veľkých organizácia lákajú neželaný záujem. Na druhej strane je však organizácia navonok dobre zabezpečená a externí útočníci bez spolupráce s internými osobami nepredstavujú veľké riziko.

Celkové externé zabezpečenie takejto organizácie je dostačujúce. Interné zabezpečenie však býva minimálne a preto vnútorný nepriateľ predstavuje hlavné riziko veľkej organizácie. Budovanie bezpečnostnej infraštruktúry organizácie je dlhodobá a nákladná úloha, aj vďaka samotnej vnútornej komplexnosti a malej viditeľnosti procesov riadenia organizácie.

3.2 Legislatívne požiadavky

Výber vhodného bezpečnostného riešenia ovplyvňujú okrem strategických zámerov organizácie aj iné požiadavky, ktoré samotná organizácia nemôže ovplyvniť. Takýmito požiadavkami sú aj legislatívne požiadavky všeobecne záväzných právnych predpisov. V SR sú to najmä zákon NR SR č. 100/1996 zb. o štátnom a služobnom tajomstve a šifrovej ochrane informácií [11] a zákon NR SR č. 52/1998 zb. o ochrane osobných informácií v informačných systémoch [12]. Posledne sponínaný predpis sa dotýka takmer každej organizácie, pretože organizácie počas svojej činnosti zhromažďujú množstvo osobných údajov (o zákazníkoch, partneroch, atď.). Priamo informačnej bezpečnosti sa týka §10 tohto zákona (52/1998), ktorý definuje zodpovednosť za bezpečnosť osobných údajov v informačnom systéme. Podľa tohto paragrafu sú prevádzkovatelia informačného systému povinní prijať primerané technické a organizačné opatrenia na zaručenie bezpečnosti osobných údajov pod hrozbou pokuty do výšky až 1 000 000 Sk. Všeobecné ustanovenia zneužitia informácií a informačného systému definuje zákon NR SR č. 140/1961, Trestný zákon, v znení neskorších zmien a doplnkov.

4 Metódy obrany a ochrany

Prostriedky zabezpečenia počítačovej siete a informačného systému slúžia na minimalizáciu rizík a s nimi spojených finančných strát. Nasledujúce kapitoly sa budú zaoberať organizačnými a technickými prostriedkami na minimalizáciu a manažment spomínaných rizík.

4.1 Bezpečnostná politika

Bezpečnostná politika je súbor pravidiel a rozhodnutí, ktorý definuje povolené a nepovolené akcie účastníkov systému a reakcie na ne. Jednoducho povedané, definuje kto môže robiť aké operácie a čo sa stane, keď vykoná niečo čo vykonať nesmie.

Bezpečnostná politika je asi najviac zanedbávanou časťou bezpečnostnej infraštruktúry vo väčšine organizácií, pritom je jednou z jej najdôležitejších súčastí. Ani ten najlepší firewall neochráni sieť proti útoku, ak je nakonfigurovaný podľa zlej bezpečnostnej politiky. Ak bezpečnostná politika organizácie umožňuje pracovníkom používať vlastné modemy na *dial-in* prístup do podnikovej siete, útočník sa nemusí obťažovať prelamovať demilitarizovanú zónu. Kvalitne postavená a vyvážená bezpečnostná politika je kľúčovým prvkom dobrej bezpečnostnej infraštruktúry.

Spôsob formulácie bezpečnostnej politiky sa bude značne líšiť v závislosti od veľkosti a zvyklostí v organizácií. Malé organizácie môžu zredukovať bezpečnostnú politiku na niekoľko viet, ktoré sú odovzdávané ako ústne inštrukcie medzi zamestnancami. Stredná organizácia môže formulovať bezpečnostnú politiku neformálne na jeden list papiera pričom vo veľkej organizácií to môže predstavovať hrubý zväzok interných smerníc a nariadení.

V ďalších kapitolách bude popísané ako možno konkrétnymi úpravami technickej časti bezpečnostnej politiky dosiahnuť aspon čiastočnú ochranu proti útokom popísaným v kapitole 2.

4.1.1 Filtrovanie na hranici siete

Funkciu ochrany siete na jej hranici vykonávajú hlavne firewally a filtrujúce smerovače, preto táto kapitola bude zameraná hlavne na aspekty ich správnej konfigurácie.

Ako bolo popísané v kapitole 2.1, ICMP pakety predstavujú pre sieť značné riziko. Ich vhodným obmedzením na hranici siete sa môže odolnosť siete voči útokom podstatne zlepšiť. Nevýhodou ich blokovanie je však strata istej časti funkčnosti hlavne diagnostických služieb siete. Blokovanie ICMP paketov tiež prispieva k zakrytiu vnútornej štruktúry siete, keďže sťažuje niektoré metódy mapovania sieťových prostriedkov.

Dôležitú úlohu medzi metódami blokovania paketov na hranici siete zastávajú takzvané "*anti-spoofing*" filtrovacie pravidlá. Tieto pravidlá zabraňujú uzlu z vonkajšej siete, aby sa vydával za uzol z vnútornej siete pomocou techniky *IP Spoofing* popísanej v kapitole 2.2.2. Toto filtrovanie však nezabraňuje uzlu z vonkajšej siete, aby sa maskoval za iný uzol z vonkajšej siete, to je už mimo kontroly smerovača na hranici siete. Detailnejší popis nastavenia *anti-spoofing* pravidiel smerovača sa nachádza v kapitole 4.2.

Okrem firewallov sa na hranici siete nachádzajú aj aplikačné brány a proxy servery. Hlavnou úlohou týchto zariadení je zabezpečiť dodatočnú bezpečnostnú vrstvu a tiež zakryť štruktúru vnútornej siete. Servery pre spracovanie správ elektronickej pošty (mail exchangers) a FTP/HTTP proxy servery zakrývajú štruktúru vnútornej siete pred pohľadom z vonkajšku. Uzol vo vonkajšej sieti vidí komunikáciu vždy len s jednou IP adresou. Poštové servery môžu prepisovať hlavičky a obálky správ elektronickej pošty tak, aby zakryli prihlasovacie mená (login names) a mená lokálnych serverov. Čím menej informácií o štruktúre vnútornej siete útočník získa, tým je menšie riziko úspešného útoku.

4.1.2 Zabezpečenie serverov

Servery sú uzly siete ktoré poskytujú služby. Niektoré z týchto služieb však môžu skrývať riziko prezradenia informácií alebo možnosť prieniku útočníka v dôsledku chyby návrhu alebo implementácie služby. Z týchto dôvodov by mali byť servery obmedzené len na poskytovanie minimálnej sady služieb. Pri zvlášť zraniteľných službách (napr. *rlogin*) by sa mala prehodnotit možnosť ich náhrady za ekvivalentné služby s lepšími bezpečnostnými vlastnosťami.

Na prístup k službám sa v súčastnosti najviac používa autentifikácia heslom. Vhodná politika správy hesiel môže podstatne zlepšit celkovú bezpečnosť autentifikácie heslom. Vhodne zvolená doba životnosti a dĺžka hesla spolu s vynucovaním dostačujúcej zložitosti hesla dostatočne zabraňujú úspešným útokom zameraným na uhádnutie hesla. Treba ešte podotknúť, že heslo je dôležitá autentifikačná informácia a preto by sa nemalo prenášať sieťou nechránené (v otvorenej forme). Z tohto dôvodu je lepšie sa zamerať na protokoly poskytujúce heslu a aj celej následnej komunikácií kryptografickú ochranu.

Ďalším podstatným rizikom pre servery je nechcené zavlečenie zadných vrátok. Správca servera má za úlohu udržovať server funkčný a k tejto jeho úlohe tiež patrí inštalácia nového softvéru. Ak je tento softvér získaný z nedôveryhodného zdroja (napr. z FTP servera v Internete) je možnosť, že okrem funkcií, ktoré ma tento softvér poskytovať, pribudnú zadné dvierka pre prípadného útočníka. Preto k dobrým praktikám správcu systému patrí kontrola integrity získaného softvérového balíka pred jeho inštaláciou. Väčšina renomovaných firiem poskytuje metódy na overenie integrity ich produktov kryptografickými metódami (napr. kryptografická *hash* funkcia MD5).

Na zabránenie rýchlych a automatizovaných útokov je tiež veľmi dobré snažiť sa zakryť skutočnú identitu servera. To hlavne zahŕňa odstraňovanie čísel verzií a identifikácie výrobcu[6] z rôznych uvítacích správ služieb a odstraňovanie služieb, ktoré sú určené práve na poskytovanie systémových informácií (napr. *netstat*, *sysstat*, *finger*).

4.1.3 Nedôvera sieti

Ako už bolo spomenuté, siete založené na TCP/IP neboli navrhované s dôrazom na bezpečnosť. Metódy *IP spoofing* a *DNS spoofing* umožnujú impersonifikovať IP adresy a doménové mená. Preto protokoly založené na kontrole IP adries a doménových mien nemožno považovať za bezpečné. V prípadoch keď je nutné kontrolovať prístup vzhľadom na meno alebo adresu vzdialeného uzla, je nutné doplniť túto kontrolu o kryptografické metódy podobne ako to robia protokoly SSH alebo SSL. Siete TCP/IP neposkytujú ani záruku integrity TCP spojenia, preto sa treba orientovať na protokoly, ktoré si zaručujú vlastnú integritu kryptografickými metódami (zreťazené šifrovanie alebo MAC).

Jeden z najpoužívanejších protokolov, ktorého jediná bezpečnosť je založená na doménových menách a IP adresách je protokol SMTP určený na prenos elektronickej pošty. Ako bolo ukázané v kapitole 2.2.5, falšovanie správ elektronickej pošty je jednoduché. Preto je vhodné uviesť do používania jeden z protokolov zabezpečujúcich autenticitu, intergitu a privátnosť prenášaných správ. Viac podrobností je možné nájsť v kapitole 4.5.

4.2 Firewally a smerovače

Firewally, smerovače a prístupové zariadenia svojím umiestnením na okrajoch siete a medzi sieťami poskytujú dobrú možnosť implementácie časti bezpečnostnej politiky. Pre toto ich významné postavenie je vhodné venovať zvýšenú pozornosť ich bezpečnostným vlastnostiam. V tejto kapitole budú popísané jednotlivé druhy firewallov a bezpečnostných vlastností smerovačov podľa princípu ich činnosti. Ďalej bude popísaná odporučnená konfigurácia firewallu tak, aby zabraňovala bežným útokom popísaným v kapitole 2 a základné čtry vnútornej architektúry firewallu a ich vplyv na odolnosť firewallu.

4.2.1 Bezstavový paketový filter

Bezstavový paketový filter vykonáva kontrolu paketov na základe ich hlavičiek a vo veľmi obmedzenej miere aj na základe ich obsahu. Filter si nezachováva o paketoch žiadnu informáciu[7] a preto nemôže rozhodnúť o tom, či paket je súčasťou aktívneho spojenia, či bol vyžiadaný alebo či patrí do autorizovanej relácie. Kontrola prístupu sa v takýchto

[6] Ak odstraňovanie takýchto informácií nie je v rozpore s licenčnými podmienkami produktu.

[7] Okrem účtovacích informácií, tie sa však nepoužívajú na riadenie kontroly prístupu.

Tabuľka 1: Filtrovacie pravidá bezstavového paketového filtra

	Zdroj	Cieľ	Protokol	Port	Príznaky	Akcia
1	10.1.0.0/16	*	TCP	*	*	ALLOW
2	*	10.1.1.10	TCP	80	*	ALLOW
3	*	*	TCP	*	not SYN	ALLOW
4	*	*	*	*	*	DENY

firewalloch vykonáva na základe aplikovania jednoduchých pravidiel, ktoré sú väčšinou viazané na informácie z IP a TCP respektíve UDP hlavičiek paketu. Pravidlá sú väčšinou aplikované sekvenčne a prvé aplikovateľné pravidlo rozhoduje o povolení či zamietnutí paketu. Časť tabuľky pravidiel typického bezstavového filtra je Tabuľke 1. Ako vidieť, tento filter rozhoduje o prepustení paketu na základe zdrojovej a cieľovej adresy, typu prenášaného protokolu, čísla cieľového portu a príznakov protokolu. Firewall je umiestnený na hranici siete 10.1.x.x. Bezpečnostná politika, ktorú tieto pravidlá implementujú znie: "povoliť všetky spojenia zo siete von, zakázať všetky spojenia do siete okrem spojenia na server 10.1.1.10 na port 80". Pravidlo č. 1 povoľuje akýkoľvek TCP paket z vnútornej siete. Pravidlo č. 2 povoľuje TCP pakety s cieľovou adresou 10.1.1.10 a cieľovým portom 80. Pravidlo č. 3 povoľuje akékoľvek TCP pakety bez nastaveného príznaku SYN[8], čo zaručuje možnosť odpovede na spojenia otvorené z vnútornej siete. Posledné pravidlo určuje "implicitné správanie" tiež označované ako "policy". Toto pravidlo zakazuje všetko, čo nebolo predchádzajúcimi pravidlami explicitne povolené.

Nevýhodou bezstavových filtrov je fakt, že sa len veľmi ťažko dajú dokonale prispôsobiť požadovanej bezpečnostnej politike. V predchádzajúcom príklade museli byť povolené všetky non-SYN pakety do vnútornej siete na to, aby sa zaručila funkčnosť otvorených spojení, čo môže predstavovať vážnu hrozbu. Na druhej strane zakázanie týchto paketov by odporovalo bezpečnostnej politike, pretože by nebolo možné vytvoriť funkčné obojsmerné spojenie. Konfigurácia bezstavového paketového filtra nemusí byť vždy jednoduchá, hlavne ak musí implementovať komplexnú bezpečnostnú politiku. Pri konfigurácií ľahko vznikajú chyby, ktoré sa veľmi ťažko detekujú. Medzi výhody bezstavových filtrov patria vysoká efektivita, malé zdržanie pri kontrole paketov, jednoduchá implementácia a veľká dostupnosť množstva implementácií na rôznych platformách. Bezstavové filtre možno jednoducho paralelizovať a násobiť rovnakými metódami ako smerovače.

[8]Príznak SYN označuje otváranie nového spojenia. V tomto prípade ako aj vo väčšine reálnych firewallov sa paket s nastavenými príznakmi SYN aj ACK nepovažuje za "SYN paket" ale za "ACK paket".

Tabuľka 2: Príklad filtrovacích pravidiel stavového filtra

	Zdroj	Cieľ	Protokol	Služba	Akcia
1	10.1.0.0/16	*	TCP	*	ALLOW
2	*	10.1.1.10	TCP	http	ALLOW
3	10.2.0.0/16	10.1.0.0/16	TCP	john@ftp	ALLOW
4	*	*	*	*	DENY

4.2.2 Stavový paketový filter

Stavový filter pracuje podobne ako bezstavový, s tým rozdielom, že si zachováva stavovú informáciu o spojeniach, reláciach a pod., ktorá je vytváraná na základe analýzy prechádzajúcich paketov. Pomocou tejto stavovej informácie sa môže firewall jednoduchšie a presnejšie rozhodnúť, či skúmaný paket porušuje bezpečnostnú politiku alebo nie. Stavový filter podobne ako bezstavový čerpá väčšinu informácií zo základných protokolových hlavičiek (IP, TCP, UDP), vo veľkej miere sa však využíva aj dátová časť na kontrolu obsahu spojení (*content security*, pozri kapitola 4.2.4). Stavové filtre tiež môžu rozoznávať väčšiu škálu aplikačných protokolov, pretože si vedia pomocou stavovej informácie skompletizovať relevantnú časť TCP spojenia. Konfigurácia stavového filtra je tiež jednoduchšia, pretože jeho filtrovacie pravidlá viac zodpovedajú "prirodzenému" jazyku bezpečnostnej politiky. Príklad filtrovacích pravidiel stavového filtra ukazuje Tabuľka 2. Tieto pravidlá implementujú podobnú bezpečnostnú politiku ako v predchádzajúcom príklade, s dodatkom "povoliť prístup užívateľa JOHN zo siete 10.2.x.x na FTP-servery na vnútornej sieti". Pravidlo č. 1 implementuje povolenie všetkých spojení z vnútornej siete von. Keďže používame stavovú informáciu, nie je potrebné ďalšie pravidlo na povolenie paketov v opačnom smere, firewall ich automaticky povolí, ak patria k otvorenému spojeniu iniciovanému z vnútornej siete. Pravidlo č. 2 povoľuje prístup na server 10..1.1.10 na porte 80 (http port). Pravidlo č. 3 implementuje povolenie prístupu užívateľa JONH zo siete 10.2.x.x na vnútorné FTP-servery. Keďže firewall je schopný skompletizovať si relevantnú časť riadiaceho spojenia FTP protokolu, môže povoliť prístup len užívateľovi, ktorý sa príkazom USER protokolu FTP autentifikuje ako JOHN. Podobne môže firewall zabezpečiť aj povolenie dátových spojení pre prenos súborov sledovaním príkazov PORT protokolu FTP, pričom ostatné podobné spojenia zostanú zakázané. Posledné pravidlo zabezpečuje implicitné správanie, ktoré zakáže všetko čo nie je povolené predchádzajúcimi pravidlami.

Výhody stavového filtra sú zrejmé z predchádzajúceho opisu. Dokáže sa dobre prispôsobiť bezpečnostnej politike, ľahko sa konfiguruje a vo väščine prípadov zostáva plne transparentný pre sieťové protokoly. Jeho nevýhody sú spôsobené nutnosťou udržovať stavovú informáciu, čo spôsobuje problémy pri výpadkoch a dynamickom smerovaní. Ak má sieť viac vstupných bodov, môže sa stať, že pakety odpovede neprídu do siete tou istou

cestou ako vyšli požiadavky. Tu vzniká potreba zdieľania stavovej informácie medzi viacerými firewallmi, čo môže značne ovplyvniť výkon a spoľahlivosť stavových firewallov. Podobné problémy vznikajú pri paralelizácií a násobnosti s cieľom zvýšiť výkon alebo spoľahlivosť. Implementácia stavových filtrov je značne náročná a preto je výsledná cena produktov relatívne vysoká v porovnaní s bezstavovými filtrami.

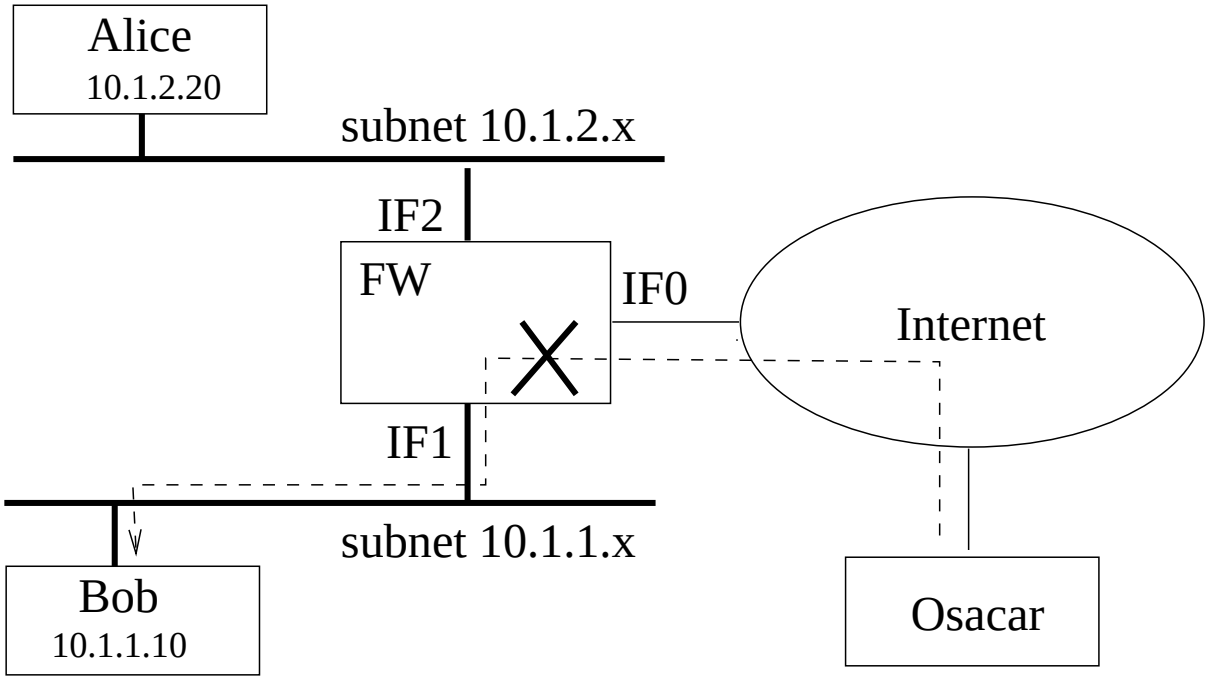
4.2.3 Aplikačná brána

Aplikačná brána sa líši od paketových filtrov hlavne v tom, že vôbec nesmeruje pakety. Kým paketové filtre pracujú na sieťovej (IP) vrstve[9] rodiny protokolov TCP/IP, aplikačná brána pracuje na úrovni aplikačných protokolov *nad* transportnými protokolmi TCP a UDP. Aplikačná brána nie je pre sieť transparentná. Aplikácie a používatelia musia vedieť že aplikačná brána existuje, aby mohli získať prístup do chránenej časti siete. Príkladmi aplikačných brán sú veľmi rozšírené HTTP-Proxy servery alebo Mail Relay servery. Ako už bolo povedané, aplikačná brána nie je transparentná. Každá aplikácia musí mať na aplikačnej bráne svoj modul, ktorý je schopný porozumieť aplikačnému protokolu a implementovať relevantnú časť bezpečnostnej politiky vzhľadom na daný aplikačný protokol. Štandardné aplikácie, ako sú napríklad klientské programy služieb FTP a Telnet, je síce s väčšinou aplikačných brán možne používať ďalej, ich použitie je však nepohodlné. Používateľ musí vedieť adresu brány, musí sa prihlásiť najprv na bránu a potom až na cieľový uzol, spojenia sa ťažko automatizujú vzhľadom na rôzne druhy aplikačných brán, atď.

Na druhej strane však aplikačná brána poskytuje najvyššiu relatívnu bezpečnosť, keďže priamo nesmeruje pakety a môže dokonale analyzovať aplikačný protokol. Okrem toho sa pakety prechádzajúce aplikačnou bránou "regenerujú" - fragmenty sú zlúčené, rozšírenia TCP/IP[10] sú potlačené. Prípadný útok na implementáciu rodiny protokolov TCP/IP dopadne len na aplikačnú bránu a nie na žiaden uzol za ňou. Ako základ aplikačnej brány možno použiť univerzálny operačný systém (UNIX, Windows NT) posilnený vhodnou konfiguráciou a inštaláciou dodatočných bezpečnostných modulov a aplikácií. Niektoré protokoly a aplikačný softvér už priamo podporujú aplikačné prány, ako napríklad HTTP protokol a WWW prehliadače priamo podporujú HTTP-Proxy servery. V takomto prípade je implementácia aplikačnej brány priamočiara a nenáročná.

[9] S prípadnou analýzou výšších vrstiev. Rozhodnutie o povolení respektíve zakázaní paketu sa však realizuje prostriedkami sieťovej vrstvy.

[10] Napríklad source routing option.



Obrázok 10: Ochrana proti útoku *IP spoofing*.

4.2.4 Konfigurácia fiewallu

Najdôležitejšou časťou pri umiestňovaní firewallu je jeho konfigurácia. Je dokonca dôležitejšia ako kvalita samotného firewallu. Aj ten najhorší[11] ale zato dobre nakonfigurovaný firewall ochráni sieť lepšie ako drahý a "bezpečný" firewall ktorého konfigurácia bola zanedbaná a povoľuje takmer všetko. Konfiguráciu firewallu by mal vždy vykonávať kvalifikovaný odborník, ktorému sú jasné princípy sieťových protokolov a ich vzájomné vzťahy. Kvalita konfigurácie firewallu sa dá len veľmi ťažko testovať, preto odhalenie nedostatkov konfigurácie je extrémne náročná úloha. Ak je firewall "uzavretejší" a povoľuje menej služieb ako by mal, dá sa to ľahko detekovať pretože zakázané služby prestanú pracovať. Ak je však firewall "otvorenejší" a povoľuje viac služieb ako by mal, pravdepodobne to nikto nespozoruje až kým nebude neskoro a nenastane prienik firewallom.

Konfigurácia firewallu by mala implementovať relevantnú časť bezpečnostnej politiky organizácie, preto bude veľká časť konfigurácie firewallu závislá práve od detailov tejto bezpečnostnej politiky. Niektoré črty sú však takmer pri všetkých firewalloch rovnaké, pretože implementujú ochranu proti niektorých bežným útokom. Ochrana proti útoku *IP spoofing* je jedným z takýchto prípadov. Podstatov tejto ochrany je filtrovať pakety, ktoré sa objavia na takom vstupnom rozhraní, kam sa evidentne nemali ako dostať. Príklad použitia ochrany proti útoku *IP spoofing* je ilustrovaný na obrázku 10. Útočník OSCAR sa

[11] "Najhorší" vo význame kvality a bohatosti vlastností samotného softvérového produktu bez konfigurácie.

Tabuľka 3: Nastavenie filtrovacích pravidiel na ochranu pred útokom *IP spoofing*.

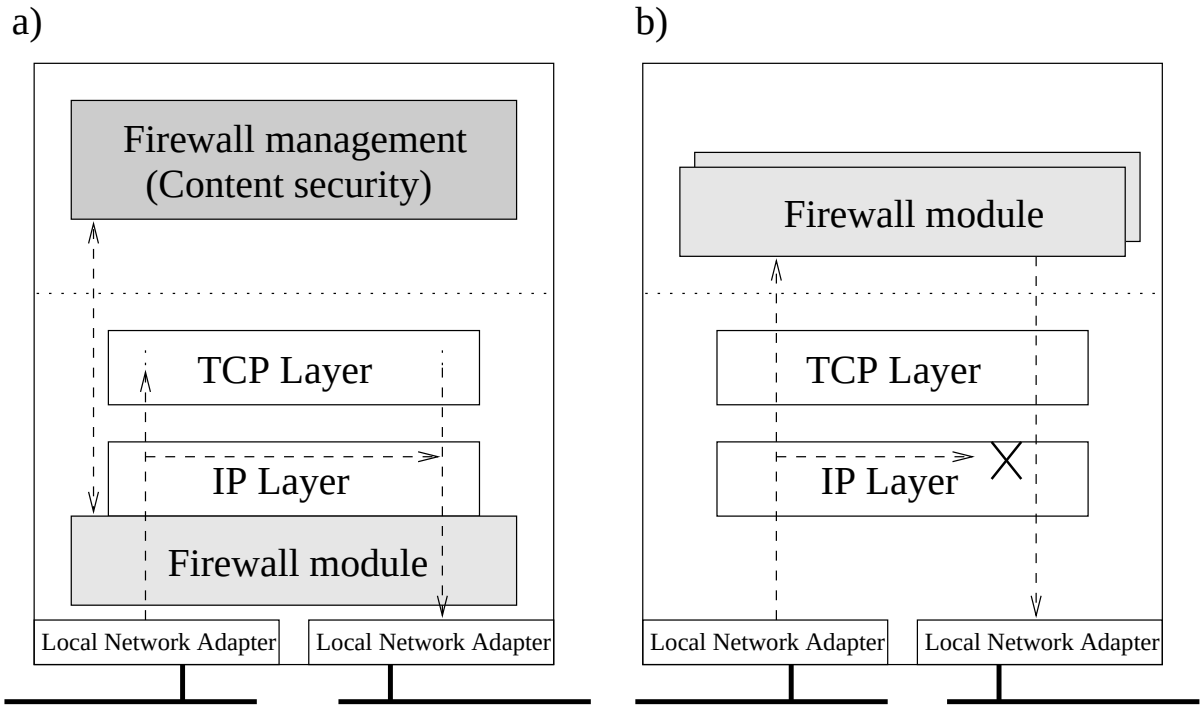
Zdroj	Cieľ	Rozhranie	Protokol	Port	Akcia
10.1.2.0/24	*	IF0	*	*	DENY
10.1.1.0/24	*	IF0	*	*	DENY
10.1.2.0/24	*	IF1	*	*	DENY
10.1.1.0/24	*	IF2	*	*	DENY

snaží oklamať uzol BOB paketom, ktorého zdrojová adresa patrí uzlu ALICE (podrobnejšie pozri kapitola 2.2.2). Firewall FW detekuje prítomnosť paketu so zdrojovou adresou 10.1.2.20 na rozhraní IF0. Paket s touto zdrojovou adresou sa na toto rozhranie nemohol nijako dostať, keď sieť 10.1.2.x je pripojená k rozhraniu IF2 firewallu a nie je na nej žiaden iný smerovač. Firewall tento paket neprepustí. Nastavenie relevantnej časti filtrovacích pravidiel pre tento prípade je zachytené v tabuľke 3. Tieto pravidlá je však možné implementovať len ak firewall dovoľuje filtrovanie paketov pri *vstupe*, tj. na vstupnom rozhraní a dovoľuje vo filtrovacích pravidlách uviesť aj vstupné rozhranie. Niektoré firewally generujú ochranu proti *IP spoofingu* samé, treba im však nastaviť rozsahy povolených IP adries pre jednotlivé sieťové rozhrania.

Vhodnou konfiguráciou firewallu sa dá čiastočne brániť aj proti ICMP bombardovaniu a útokom typu *smurf*. Najúčinnejším riešením je povoliť len minimálne nutné množstvo ICMP paketov. Zakázanie ICMP paketov s diagnostickými vlastnosťami (*echo*, *echoreply*, atď.) prispeje aj k lepšiemu utajeniu vnútornej štruktúry siete. Zakázanie paketov typu *directed broadcast* zabraňuje útočníkom využiť vašu sieť ako prostredníka pre útok typu *smurf*.

4.2.5 Architektúra firewallov

Väčšina momentálne dostupných paketových filtrov je založená na bežných operačných systémoch, ktorých jadro je viac či menej modifikované. Táto modifikácia väčšinou spočíva vo vložení filtrovacieho modulu do sieťového podsystému, konkrétne do podsystému spracovania protokolovej rodiny TCP/IP. Filtrovací modul je takmer výlučne umiestňovaný medzi linkovou (*Local Network Adapter Layer*) a sieťovou (*IP Layer*) vrstvou, kde umožňuje zachytiť maximum informácií bez toho, že by musel byť závislý na hardvérových sieťových prostriedkoch. Inak je to však pri aplikačných bránach. Aplikačná brána sa spolieha na kvalitu implementácie sieťového subsystému hosťovského operačného systému a jej moduly bežia takmer výlučne ako užívateľské procesy. Rozdiel medzi štruktúrou paketového filtra a aplikačnej brány zobrazuje obrázok 11. V prípade paketového filtra paket vstúpi cez sieťový adaptér (*Local Network Adapter*) a jeho ovládač odovzdá paket filtrovaciemu modulu (*firewall module*). Tento modul rozhodne o osude paketu a v klad-

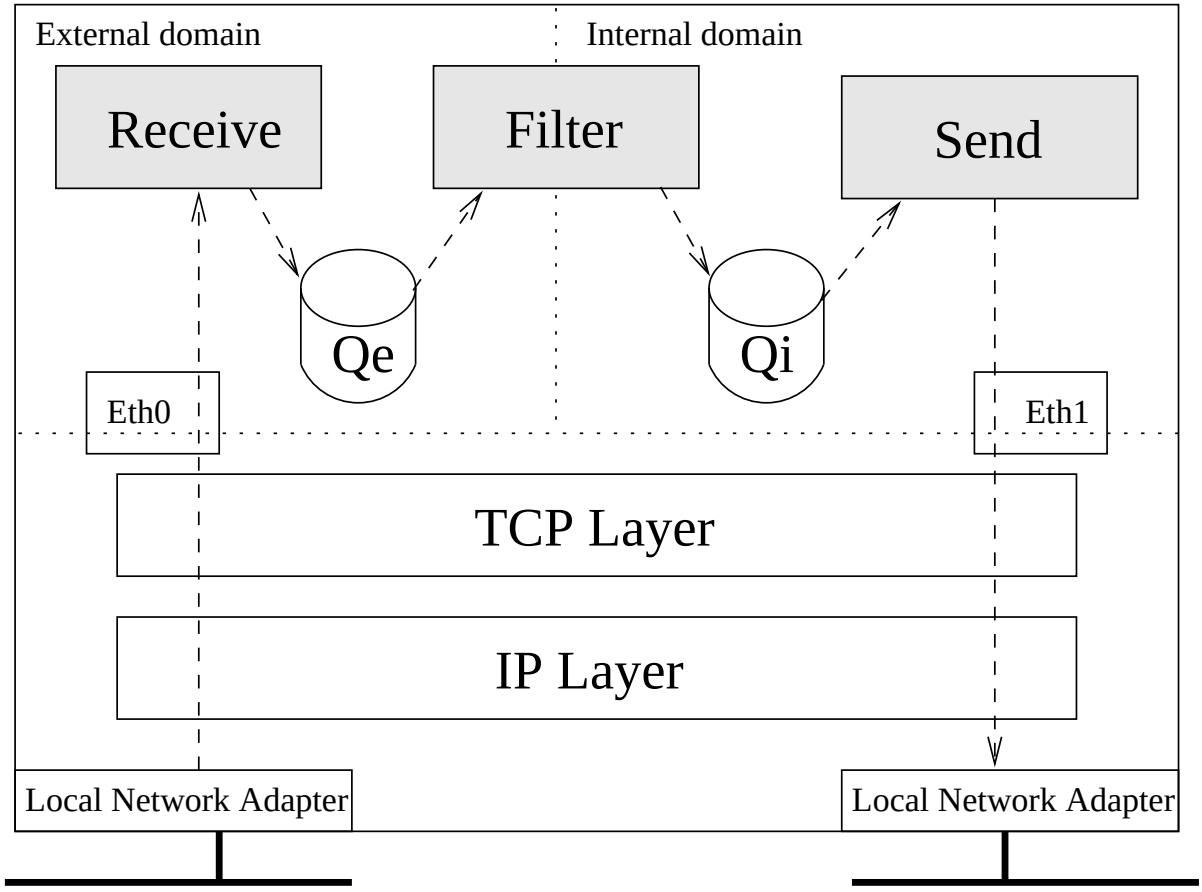


Obrázok 11: Architektúra a) paketového filtra a b) aplikačnej brány.

nom prípade ho posunie štandardnej IP vrstve, kde podlieha normálnemu smerovaniu. Pri vysielaní paketu do siete znova prechádza cez filtrovací modul. Nastavenie filtrovacieho modulu je riadené užívateľským procesom (*firewall management*) pomocou špeciálneho kanálu[12]. Užívateľský proces môže pri stavových firewalloch poskytnúť tiež služby kontroly obsahu (*content security*). Aplikačná brána v plnej miere využíva štandardné jadro operačného systému a štandardný sieťový subsystém. Jediná podstatná zmena oproti bežným bránam je fakt, že smerovanie paketov na IP vrstve je vypnuté. Všetky spojenia končia alebo začínajú v niektorom z procesov firewallu.

Niektoré firewally však nespoliehajú na ochranu bežného operačného systému. V poslednom čase sa začínajú aj v komerčnej oblasti objavovať operačné systémy vyššej bezpečnostnej úrovne. Tieto operačné systémy poskytujú povinnú kontrolu prístupu (*Mandatory Access Control*, MAC), ktorá na rozdiel od štandardnej kontroly prístupu (*Discretionary Access Control*, DAC) neumožňuje procesom manipulovať s prístupovými právami. MAC navyše implementuje bezpečnostné domény, ktorých informačný tok je oddelený priamo operačným systémom a môžu ho realizovať len privilegované procesy. Implementáciu MAC pre aplikačnú bránu ilustruje obrázok 12. Obrázok znázorňuje časť podsystému na spracovanie pošty. Sú definované dve bezpečnostné domény: interná (internal domain) a externá (external domain). Sieťové logické zariadenia (*Eth0* a *Eth1*) sú priradené do jednotlivých domén, rovnako ako aj fronty správ (Qe a Qi). Procesy na

[12]Týmto kanálom väčšinou býva znakové pseudozariadenie.



Obrázok 12: Povinná kontrola prístupu (MAC) v aplikačnej bráne.

Tabuľka 4: Porovnanie spôsobov práce firewallov.

Systém	Spôsob práce	Poznámka
CheckPoint FireWall-1	stavový paketový filter	Možnosť použiť externé servery na kontrolu a modifikáciu obsahu.
Cisco PIX	stavový paketový filter	
Linux 2.0.x	bezstavový paketový filter	
Linux 2.1.x	bezstavový paketový filter	Možnosť zapojiť externý modul na kontrolu obsahu.
Cisco IOS Firewall Feature Set	bezstavový paketový filter	Vzťahuje sa na tvz. "access-lists".
TIS firewall toolkit	aplikačná brána	FWTK je súbor aplikačných brán pre bežný OS (UNIX)
sendmail, qmail, ...	aplikačná brána	Bežné MTA. Dajú sa použiť v prostredí firewallu.
squid, apache, ...	aplikačná brána	Bežné HTTP proxy. Dajú sa použiť v prostredí firewallu.
Berkeley Internet Name Daemon (BIND)	aplikačná brána	Bežný DNS server. Obsahuje vlstnosti na použitie v prostredí firewallu.

prijímanie (RECEIVE) a odosielanie (SEND) pošty sú každý priradený vo svojej doméne. Mimo tejto domény nemajú žiadne práva. V žiadnom prípade sa nemôže stať, že proces SEND by mal prístup k zariadeniu *Eth0*. Jediný proces, ktorý môže komunikovať medzi doménami je proces filtrovania pošty (FILTER).

Rozdelenie procesov do domén je možné zjemniť ešte uplatnením prostriedkov štandardnej kontroly prístupu v rámci domén, alebo modifikáciou systému smerom k presnejšej špecifikácií práv procesov pre jednotlivé domény (čítanie, zápis, atď.). Názvy jednotlivých produktov obsahujúcich túto technológiu sa značne líšia. Väčšinou sa operačné systémy a podobné produkty obsahujúce MAC označujú ako "Trusted" (napr. "Trusted Solaris", "Trusted Oracle", atď.), pri firewalloch sa však vyskytuje aj označenie "Type Enforcement"[17]. Každý produkt certifikovaný podľa TCSEC alebo ICSEC na úroveň B1 a vyšie obsahuje MAC.

Architektúry a spôsoby filtrovania firewallov rôznych výrobcou sa líšia. Niektoré produkty zhŕňa Tabuľka 4. Za povšimnutie stojí, že aj bežné softvérové komponenty ako je napríklad *sendmail* alebo *BIND* obsahujú črty, ktoré sa dajú výhodne využiť v prostredí firewallov.

Tabuľka 6: Parametre testovaných firewallov

	Cisco 4000	PC-Linux
Základná doska	Cisco 4000	Compaq, ISA BUS
Procesor		Intel i486 DX/2
Sieťové adaptéry	Ethernet expansion card	2x 3c509, ISA
Sieťové médium	10Mb/s Ethernet, UTP	
Úložné zariadnie		HDD 120MB
Operačný systém	Cisco IOS	Linux 2.2.4
Firewall	IOS Firewall Feature Set	Linux ipchains
Spôsob filtra	bezstavový filter	bezstavový filter

Tabuľka 7: Výsledky merania priepustonosti testovaných firewallov.

	Cisco 4000	PC-Linux
FTP prenos, **bez filtrovania**	1000KB/s	800KB/s
Zaťaženie procesora	6%	20%
Odhad priepustnosti (*bing*)	4,8 Mb/s	3,7 Mb/s
Odhad priepustnosti (FTP)	8,2 Mb/s	6,5 Mb/s
FTP prenos, **s filtrovaním**	1000KB/s	800KB/s
Zaťaženie procesora	8%	25%
Odhad priepustnosti (*bing*)	4,8 Mb/s	3,7 Mb/s
Odhad priepustnosti (FTP)	8,2 Mb/s	6,5 Mb/s

4.2.6 Výkon firewallových systémov

Na ilustráciu výkonu firewallových systémov som vykonal test priepustnosti dvoch veľmi používaných firewallov nižšej kategórie. Prvý z nich je modulárny smerovač Cisco 4000 s operačným systémom IOS. Druhým testovaným systémom je bežný počítač triedy PC s operačným systémom Linux. Hardvérové a softvérové parametre testovaných zariadení sú uvedené v Tabuľke 6. Firewall bol umiestnený medzi dvoma segmentami siete Ethernet 10BaseT. Na každom z týchto segmentov bol umiestnený testovací uzol. Oba testovaciu uzly boli bežné počítače triedy PC s výkonným prosesorom Pentium II a dostatočným množstvom operačnej pamäte (min 32MB), aby sa čo najviac vylúčilo skreslenie spôsobené testovacími stanicami. Tieto stanice boli založené na zbernici PCI a obsahovali PCI sieťové adaptéry 3c590. Jeden z testovacích počítačov (FTP server) bol založený na operačnom systéme Linux 2.2.4 a druhý (klient) na operačnom systémem Microsoft Windows NT 4.0. Priepustnosť bola meraná časom prenosu súboru dĺžky 50MB službou FTP medzi testovacími stanicami a odhadom priepustonosti na základe merania rozdielov oneskorení ICMP paketov programom *bing*. Výsledky merania sú zhrnuté v Tabuľke 7. Z tabuľky vidieť, že nie je podstatný rozdiel v prenose firewallu bez filtrovania a s filtrovaním. Tento fakt je zrejme zapríčinený nevyťaženosťou procesora firewallov. Filtrovanie realizu-

Tabuľka 8: Filtrovacie pravidá firewallu Linux ipchains

No	zdroj	port	cieľ	port	protokol	ackcia	voľby
1	10.0.1.0/24	*	10.0.2.0/24	*	ICMP	ACCEPT	Bidirect
2	10.0.1.0/24	*	10.0.2.0/24	*	! TCP	DENY	Bidirect
3	10.0.1.0/24	*	10.0.2.0/24	telnet	TCP	DENY	Bidirect
4	10.0.1.0/24	*	10.0.2.0/24	finger	TCP	DENY	Bidirect
5	10.0.1.0/24	*	10.0.2.0/24	ftp	TCP	ACCEPT	
6	10.0.1.0/24	*	10.0.2.0/24	*	TCP	ACCEPT	Bidirect, ! SYN
7	10.0.2.0/24	ftp-data	10.0.1.0/24	1024:	TCP	ACCEPT	SYN
default policy			DENY				

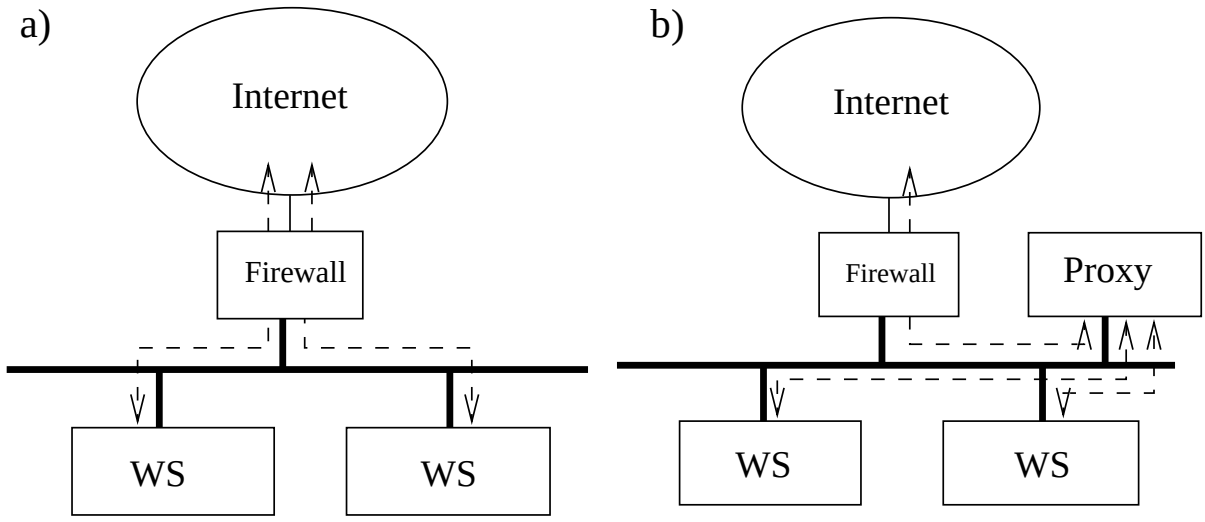
Tabuľka 9: Filtrovacie pravidlá firewallu Cisco IOS

akcia	protokol	zdroj	maska	cieľ	maska	rozšírenie
permit	icmp	10.0.1.0	0.0.0.255	10.0.2.0	0.0.0.255	
permit	icmp	10.0.2.0	0.0.0.255	10.0.1.0	0.0.0.255	
deny	tcp	10.0.1.0	0.0.0.255	10.0.2.0	0.0.0.255	eq telnet
deny	tcp	10.0.1.0	0.0.0.255	10.0.2.0	0.0.0.255	eq finger
permit	tcp	10.0.1.0	0.0.0.255	10.0.2.0	0.0.0.255	eq ftp
permit	tcp	10.0.1.0	0.0.0.255	10.0.2.0	0.0.0.255	established
permit	tcp	10.0.2.0	0.0.0.255	10.0.1.0	0.0.0.255	gt 1024
deny	ip	any		any		

je v hlavnej miere procesor systému, takže v prípade jeho nízkeho vyťaženia filtrovanie ovplyvní priepustnosť len minimálne[13]. V testovaných systémoch však boli použité len jednoduché filtrovacie pravidlá a je dosť pravdepodobné, že komplexné filtrovacie pravidlá by mohli vyťažiť procesor systému nad únosnú hranicu a tým ovplyvniť priepustnosť firewallu. Filtrovacie pravidlá použité na oboch systémoch sú sumarizované v Tabuľkách 8 a 9.

Priepustnosť systému s operačným systémom Linux je asi o 20% nižšia ako systému Cisco 4000. Je to zrejme spôsobené nízkou priepustnosťou zbernice ISA, ktorá je základom hardvérovej architektúry použitého počítača PC. Ďalším zaujímavým faktom je značná ochýlka odhadov programu *bing* a odhadov vypočítaných z priepustnosti dátového kanála FTP. Táto odchýlka je zrejme spôsobená nepresnosťou programu *bing* pri nízkych časoch odozvy (cca 1ms). Z výsledkov meraní programu *bing* je však zrejmé, že doba odozvy pri použití filtrovania sa rapídne nezmenila oproti stavu bez použitia filtrovania.

[13] V skutočnosti je tento vplyv nemerateľný na 10Mb/s ethernet sieťach.



Obrázok 13: Použitie jedného firewallu na obranu siete

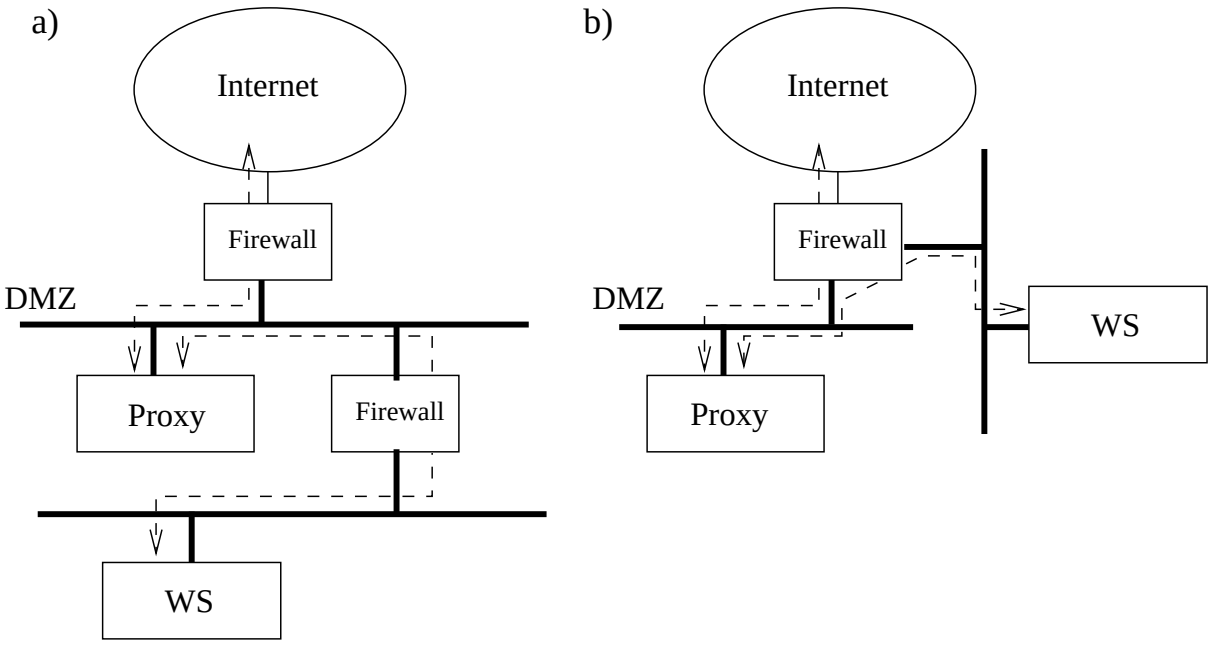
4.3 Návrh obrany siete

Firewally, filtrujúce smerovače a podobné zariadenia dokážu čiastočne oddeliť od seba dve siete. Vhodným návrhom štruktúry siete a nastavenia sieťových zariadení a uzlov je možné dosiahnuť účinnú koncepciu zabezpečenia siete a vhodne realizovať navrhnutú bezpečnostnú politiku. Znásobovaním a ukrývaním jednotlivých prvkom možno dosiahnuť oveľa lepšiu bezpečnostnú úroveň ako keby bol každý z týchto prvkov použitý samostatne. V tejto kapitole bude ukázané ako je možné tieto stavebné prvky využiť na vytvorenie bezpečnej ochrany siete.

4.3.1 Jednoduchý firewall

Pre nižší stupeň požadovanej bezpečnosti postačuje umiestnenie jedného firewallu medzi lokálnu privátnu sieť a Internet. Takúto konfiguráciu ukazuje obrázok 13. V prípade a) slúži firewall len na obmedzenie služieb prístupných na jednotlivých staniciach. Stanice sú však priamo prístupné z internetu a preto sú zraniteľné. V prípade b) je inštalovaný proxy server a filtrovacie pravidlá firewallu sú modifikované tak, že nepovoľujú priamy prístup na stanice z Internetu. Priamo prístupný je jedine proxy server. Aj tu je však isté riziko v tom, že pri prieniku na proxy server má útočník neobmedzený prístup na privátnu sieť.

V tomto prípade postačuje jednoduchý bezstavový firewall. Väčšina moderných smerovačov má zabudované obmedzené vlastnosti firewallu, takže väčšinou nie sú potrebné takmer žiadne dodatočné investície.



Obrázok 14: Demilitarizovaná zóna

4.3.2 Demilitarizovaná zóna

V prípade potreby vyššieho stupňa bezpečnosti je nutné fyzicky oddeliť siete na ktorých sa nachádza proxy server a pracovné stanice koncových užívateľov. Ako už bolo uvedené, takto vytvorená sieť, ktorá predstavuje medzistupeň medzi Internetom a privátnou sieťou sa nazýva *demilitarizovaná zóna* (DMZ). Spojenie s Internetom je filtrované jedným alebo dvoma firewallmi a aplikačnou bránou (proxy serverom). Najčastejšie používané konfigurácie demilitarizovanej zóny sú ilustrované na obrázku 14. Prípad a) používa na oddelovanie sietí dva nezávislé firewally, kým v prípade b) je použitý len jeden firewall. Fyzické oddelenie sietí slúži ako dôležitá prekážka pri prieniku na proxy server. Na rozdiel od použitia jednoduchého firewallu nie je pri prieniku na proxy server vnútorná sieť priamo vystavená útoku. Na demilitarizovanú zónu je možné vystaviť aj servery, ktoré poskytujú verejné služby Internetu, ako sú napríklad WWW alebo FTP servery. Riziká spojené s prevádzkou týchto serverov len minimálne ovplyvnia vnútornú sieť.

4.3.3 Proxy servery

Proxy servery sú v podstate špecializované aplikačné brány, ktoré sa snažia okrem zlepšenia bezpečnostných vlastností zväčšiť aj efektivitu a výkon komunikácie. Väčšina proxy serverov poskytuje svoje úložné a výpočtové kapacity na zlepšenie efektivity práce koncových klientov. Príkladom môže byť HTTP proxy server, ktorý ukladá do vyrovnávecej pamäte často používané stránky a tak skracuje priemerný čas odozvy. Na podobnom princípe pracuje aj DNS proxy, ktoré si drží v pamäti vybavené DNS požiadavky kým

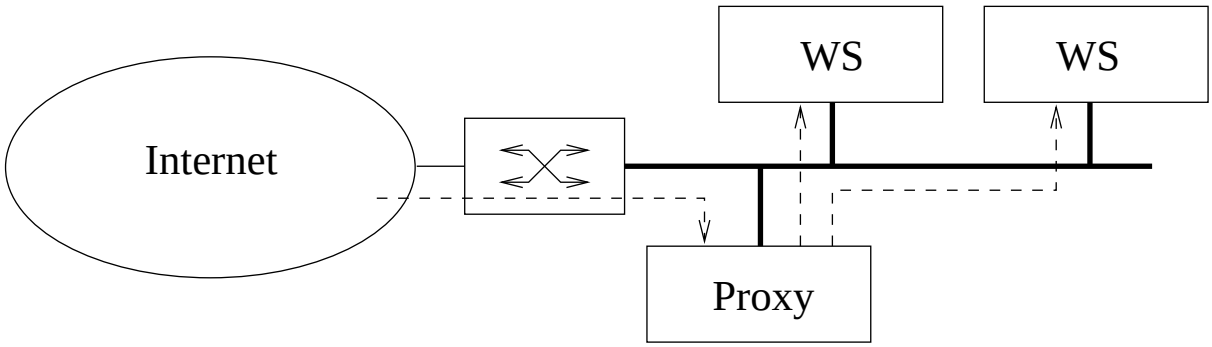
nevyprší ich platnosť. V prípade DNS požiadavky na meno, ktoré má DNS server v pamäti sa rapídne skracuje doba odozvy. Naším hlavným záujmom sú však bezpečnostné črty proxy serverov, preto si ich v nasledujúcich odstavcoch prejdeme podrobnejšie.

HTTP a FTP proxy Ako už bolo povedané, HTTP proxy zvyšuje efektivitu prenosu ukladaním transportovaných objektov do vyrovnávacej pamäte, čo je väčšinou hlavný dôvod jej implementácie aj mimo DMZ. Okrem toho však majú jednu veľmi užitočnú vlastnosť: skrývajú vnútornú štruktúru siete za jednu jedinú IP adresu[14]. Všetky prístupy viditeľné z vonkajšieho sveta sa totiž zdajú prichádzať len z proxy servera a nie su v nich zahrnuté takmer žiadne informácie o koncových pracovných staniciach. Okrem toho HTTP a FTP proxy umožňujú obmedzovať transportované objekty. Takto je možné efektívne implementovať reštriktívnu časť bezpečnostnej politiky zameranú na obmedzenie prístupu vlastných používateľov na stránky s neetickým alebo pracovne nerelevantným obsahom. Podobne je možné tieto obmedzenia limitovať časovo, aby zamestnanci mohli prezerať "nerelevantné" stránky len po pracovnom čase.

DNS server Domain Name System (DNS) server umiestnený v DMZ značne znižuje dobu odozvy a rovnako ako ostatné proxy servery skrýva štruktúru vnútornej siete. DNS proxy server umiestnený v DMZ sa však často používa aj ako externý DNS server na primárnu obsluhu DNS zón organizácie. V takomto prípade sa doporučuje uviesť v zónach len potrebný minimálny počet záznamov, ktoré musia byť viditeľné zo strany Internetu a ostatné (vnútorné) záznamy presunúť na *vnútorný* DNS server, ktorý je mimo DMZ. V prípade publikovania vnútorných DNS záznamov do Internetu by útočník získal značnú výhodu prehľadávaním záznamov DNS zón organizáacie. Aj v prípade rozdelenia vonkajšieho a vnútorného DNS sa však doporučuje obmedziť prenos zónových súborov (zone transfer) len na IP adresu sekundárneho DNS servera [18].

Mail relay Server, ktorý sa stará o transport elektronickej pošty sa nazýva *Mail Relay* alebo *Mail Transfer Agent* (MTA). Úlohou takéhoto servera je prijať poštu, dočasne uložiť a odoslať ju smerom ku koncovému príjemcovi. Okrem týchto funkcií môže MTA vykonávať aj ďalšie, bezpečnostne veľmi významé funkcie. Jednou z týchto funkcií je prepisovanie hlavičiek a obálky správy tak, aby sa zakryli všetky informácie o štruktúre vnútornej siete. Napríklad pri odosielanej správe sa prepíše adresa odosielateľa zo *semancik@storm.alert.sk* na *semancik@alert.sk* a tým sa zakryje meno pracovnej stanice odosielateľa. Na druhej strane pri príjme správ sa môže kontrolovať, či správa má korektnú adresu odosielateľa (napr. či jeho doména existuje) a či odosielateľ nie je na

[14]Prevádzkovatelia WWW serverov, ktorý zarábajú na prezentovaní reklamy, budú mať na túto "výhodu" asi iný názor.



Obrázok 15: Príklad bezpečného pripojienia siete k Internetu

čiernom zozname[15]. MTA môže obmedzovať maximálnu dĺžku správy alebo automaticky kontrolovať obsah správy na prítomnosť vírusov, atď. Pri použití bežných MTA sa doporučuje venovať zvýšenú pozornosť ich konfigurácií, pretože väčšina moderných MTA má vzhľadom na svoju flexibilitu pomerne zložitú konfiguráciu [19].

4.3.4 Príklad bezpečného pripojienia siete k Internetu

V tejto kapitole je popísaný príklad štruktúry siete a konfigurácie sieťových prvkov pre bezpečné pripojenie siete strednej organizácie k Internetu. Pripojenie je realizované prenajatým okruhom (pevnou linkou), ktorý je logicky ukončený v smerovači. Túto situáciu ilustruje obrázok 15. Vnútorná sieť organizácie používa adresy z rozsahu vyčleneného pre privátne siete. Pre sieť tejto organizácie sú vhodné adresy typu 192.168.x.x, ktoré môžu reprezentovať 256 sietí triedy C. Pridelenie niektorých dôležitých adries je uvedené v Tabuľke 10. Smerovač realizuje statický preklad sieťových adriesmedzi vnútornou a vonkajšou adresou proxy servera. Vonkajšia adresa samerovača a proxy servera musí byť pridelená z rozsahu verejných adries Internetu. Toto pridelenie realizuje takmer výlučne poskytovateľ služieb Internetu (ISP). Proxy server slúži ako aplikačná brána pre všetky bežné služby Internetu (FTP, HTTP, E-Mail, atď). Tento server môže slúžiť aj ako firemný WWW server pre publikovanie dokumentov organizácie verejnosti. Pre pracovné stanice je k dispozicií takmer celý rozsah privátnych IP adries, s malou rezervou pre ďalšie prípadné servery. Smerovač pracuje súčasne aj ako jednoduchý bezstavový firewall. Filtrovacie pravidlá navrhnuté pre smerovač sú uvedené v tabuľke 11. V prípade že je nutné priame spojenie pracovnej stanice do Internetu, je nutné na prístupovom smerovači nastaviť preklad vnútorných (privátnych) IP adries na verejné. V tomto prípade bude zrejme výhodný dynamický preklad a získanie väčšieho množstva IP adries od poskytovateľa služieb Internetu.

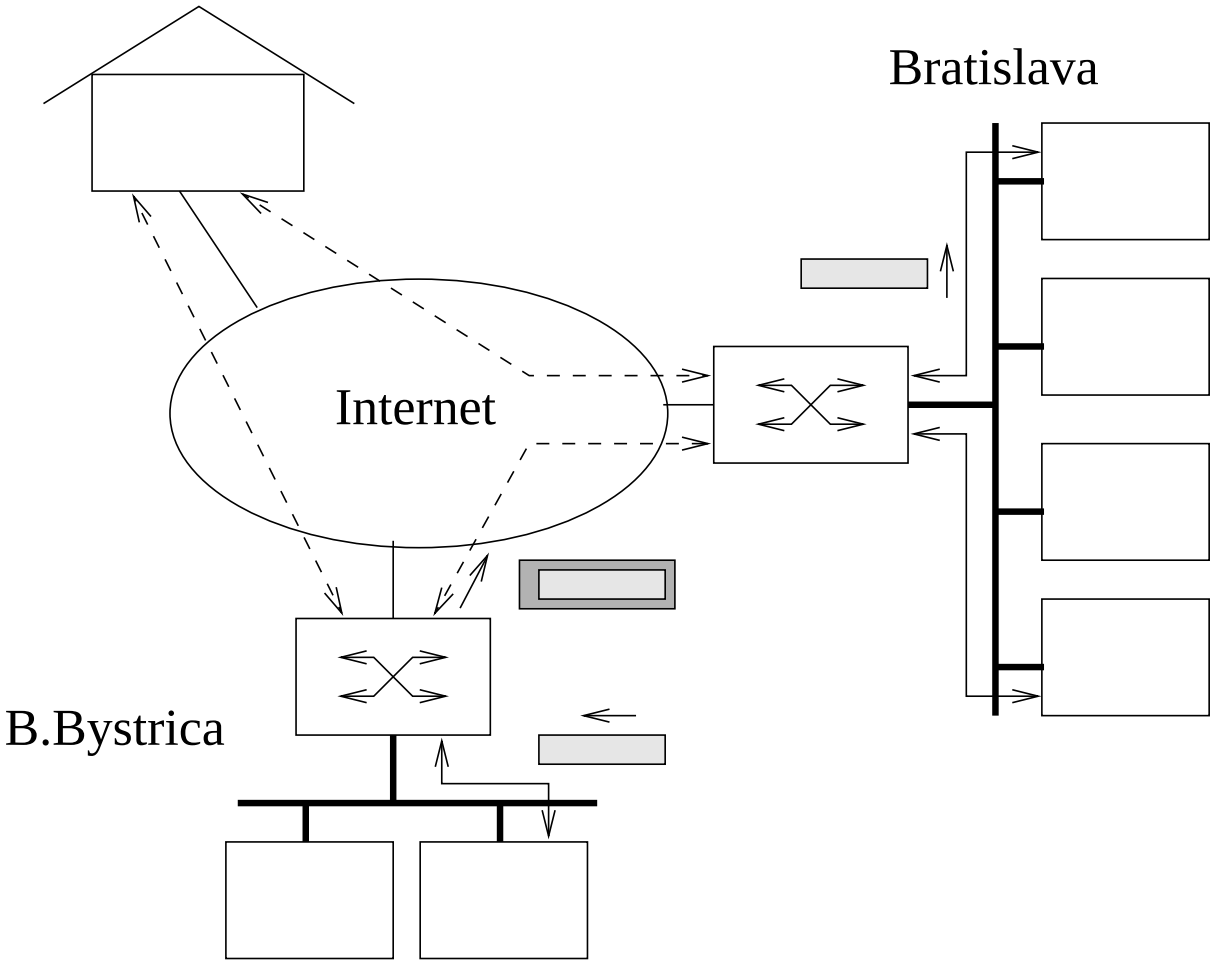
[15] Väčšinou sa jedná o zoznamy *"spammerov"*, čiže odosielateľov masovej nevyžiadanej pošty.

Tabuľka 10: Pridelenie IP adries

Uzol	IP adresa
smerovač vonkajšia	1.2.3.1 *(pridelí ISP)*
smerovač vnútorná	192.168.1.1
Proxy	192.168.1.2
Proxy vonkajšia	1.2.3.2 *(pridelí ISP)*
Pracovné stanice	192.168.1.10-192.168.255.254

Tabuľka 11: Filtrovacie pravidlá smerovača

akcia	protokol	zdroj	cieľ	port/voľby	poznámky
permit	tcp	any	192.168.1.2	smtp	povolenie prijímania pošty
permit	tcp	any	192.168.1.2	http	HTTP spojenia z Internetu firemný WWW server
permit	tcp	192.168.1.2	any	smtp	SMTP spojenia pre odosielanie pošty
permit	tcp	192.168.1.2	any	http	HTTP spojenia z proxy do Internetu
permit	tcp	192.168.1.2	any	ftp	FTP spojenia z proxy do Internetu
permit	tcp	any	any	established	povolenie všetkých otvorených spojení
permit	tcp	any	192.168.1.2	> 1024	povolenie spätných spojení pre FTP
deny	ip	any	any		implicitný zákaz



Obrázok 16: Príklad virtuálnej privátnej siete

4.4 Virtuálne privátne siete

Technológia virtuálnych privátnych sietí rozširuje technológiu tunelovania sieťových protokolov a umožňuje spájanie priestorovo vzdialených sietí pomocou verejných dátových sietí. Virtuálne privátne siete poskytujú vzdialený prístup a prepájanie vzdialených lokálnych sietí s podstatne nižšími nákladmi ako sú nutné na zriaďovanie prenajatých dátových okruhov a telefonický vzdialený prístup [21].

Typický príklad virtuálnej privátnej siete (*virtual private network*, VPN) ilustruje obrázok 16. Lokálne siete pobočiek v Bratislave a Banskej Bystrici sú spojené využitím Interetovej konektivity týchto pobočiek. Na okrajových smerovačoch týchto sietí sa pakety patriace do tejto virtuálnej privátnej siete zabalia do bežných Internetových paketov a zašifrujú. Na obrázku znázorňuje čiarkovaná čiara šifrované spojenie a plná čiara otvorené spojenie. Šifrovanie prebieha na okrajových smerovačoch, ktoré môžu byť na tento účel vybavené špeciálnym hardvérom. Pre koncové stanice sa virtuálna privátna sieť javí úplne rovnako ako skutočná privátna sieť. Jedinou výnimkou je stanica mobilného používateľa

(na obrázku 16 vpravo hore), kde sa o širovanie stará priamo jeho stanica, vybavená špeciálnym softvérom.

Najzávažnejším problémom pri vývoji a implementácií virtuálnych privátnych sieti je manažment kľúčov[16]. Pri rozsiahlej sieti totiž množstvo kľúčového materiálu stúpa exponenciálne s počtom uzlov. Manuálna výmena kľúčového materiálu prestáva byť reálna už pri malom počte vzájomne prepojených lokálnych sietí[17]. Rôzny dodávatelia technológií viturálnych privátnych sietí riešia tento problém rôzne, od manuálne distribuovaného hlavného kľúča ("master key") ktorý chráni distribúciu a pravideľnú výmenu kľúčov až po použitie elektronických certifikátov. Rôzne riešenia problému manažmentu kľúčov je hlavná príčina rozsiahle nekompatibility implementácií virtuálnych privátnych sietí. Túto nepriaznivú situáciu sa pokúša riešiť niekoľko štandardov, ktoré budú popísané v nasledujúcich kapitolách.

4.4.1 Proprietárne protokoly

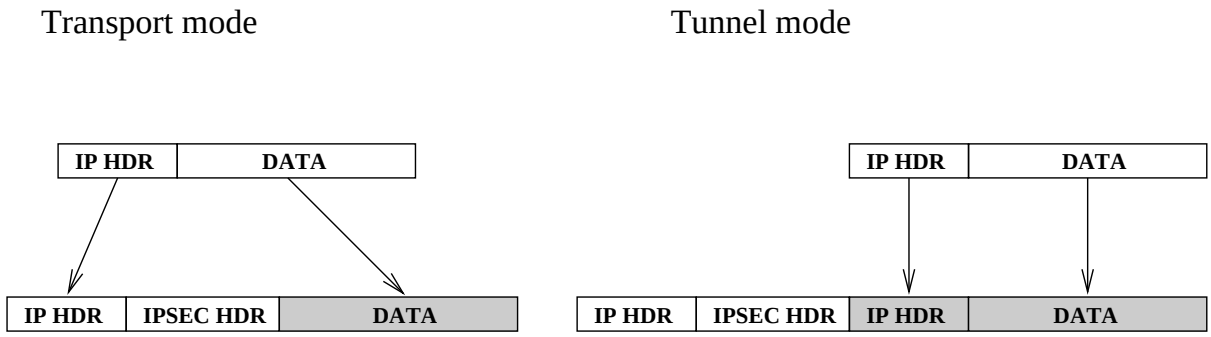
Postupom času ako vznikla nutnosť chrániť informácie prenášané Internetom vzniklo množstvo jednoúčelových protokolov na riešenie tohto problému. Niektoré z nich sa udržali až do súčastnosti, ale vo veľkej miere ustupujú v prospech viac štandardizovaným protokolom. Proprietárne protokoly pre ochranu virtuálnych privátnych sietí vyvíjali hlavne dodávatelia firewallov a smerovačov. Tieto protokoly boli viazané prevažne len na jeden šifrovací algoritmus a jeden mechanizmus manažmentu kľúčov.Tento mechanizmus bol dosť často založený na manuálnej výmene klúčového materiálu, buď manuálnym prepisovaním človekom alebo prenosom na čipových kartách.

4.4.2 SKIP

Protokol SKIP (Simple Key Management for Internet Protocols, [25]) bol vyvinutý ako otvorený štandard firmou SUN Microsystems. Protokol definuje zapúzdrenie IP paketov a ich ochanu šifrovaním ako aj spôsob manažmentu kľúčov. Obsah paketov môže byť šifrovaný niekoľkými symetrickými šiframi. Kľúčový materiál sa získava pomocou Diffie-Hellmanovej výmeny kľúčov. SKIP pracuje s podpísanými hodnotami verejných častí Diffie-Hellamanovej výmeny kľúčov, tvoriacimi istý druh certifikátov.

Protokol SKIP je pomerne rozšírený v inštaláciach firmy SUN Microsystems, ostatní výrobcovia sa však začínajú prikláňať k novšiemu a flexibilnejšiemu štandardu IPsec.

[16] Všeobecné problémy kryptografie popisuje kapitola 4.5.
[17] Najmä pokiaľ sa kľúče pravidelne menia, čo je vždy odporučovaný prístup.



Obrázok 17: Módy práce IPsec.

4.4.3 IPsec

Štandard IPsec (Internet Protocol Security extension) je súbor bezpečnostných mechanizmov spolupracujúcich na rozšírení štandardného prokolu IP o bezpečnostné vlastnosti. Jeho zámerom je doplnenie mechanizmov IP protokolu, ktoré zaručia privátnu, nenarušenú a autentifikovanú komunikáciu dimenzovanú na široké použitie v celej sieti Internet. Bezpečnostné vlastnosti sú založené na metódach modernej kryptografie a formáty a mechanizmy sú postavené na dobre osvedčených štandardoch.

Základom štandardu IPsec sú dve rozšírenia IP protokolu AH a ESP [22]. Rozšírenie AH (*Authentication Header*, [23]) slúži na zabezpečenie autenticity a integrity informácií, naproti tomu rozšírenie ESP (*Encapsulatig Security Payload*, [24]) zabezpečuje privátnosť informácií. Je možné používať tieto rozšírenia každé samostatne ale aj spolu[18]. Ochrana informácií môže byť realizovaná v transportnom (*transport mode) alebo* tunelovom móde (*tunnel mode*). Transportný mód nechráni privátnosť informácií v hlavičke, len obsah paketu. Tunelový mód pracuje podobne ako štandardný IP tunel, pridáva však bezpečnostné funkcie, chráni kompletne celý paket. Spôsob práce oboch týchto módov znázorňuje obrázok 17. Sivé časti obrázku znázorňujú šifrovanú respektíve autentifikovanú časť paketu. Pri použití tunelového módu sa vygeneruje nová IP hlavička, kým pri transportnom móde sa použije pôvodná IP hlavička. Je zrejmé že transportný mód je efektívnejší (má menšiu réžiu) kým tunelový mód poskytuje potencionálnemu útočníkovi menej informácií.

Kľúčový materiál a algoritmus na šifrovanie a autentifikáciu sa pri použití IPsec vyberá pomocu *bezpečnostných asociácií* (*security association*, SA). Bezpečnostná asociácia je jednosmerná relácia medzi dvoma uzlami, ktorá definuje použité algoritmy a ich parametre. Je určená pomocu cieľovej adresy paketu a *indexu bezpečnostných parametrov* (*Security Parameter Index*, SPI). SPI je náhodne vybrané jedinečné číslo, obsiahnuté v IPsec hlavičke. Pri odosielaných paketoch systém prehľadá tabuľku podľa cieľovej adresy

[18]Rozdelenie IPsec na dve základné rozšírenie IP protokolu bolo zrejme motivované zákazom šifrovania v niektorých krajinách (napr. Francúzko). V týchto krajinách môže byť využívané rozšírenie AH na zabezpečenie autenticity a integrity, pričom ESP a šifrovanie nebude použité.

paketu a nájde zodpovedajúce číslo SPI. Toto číslo uvedie v IPsec hlavičke paketu a paket sa zašifruje a odošle. Pri prijatí paketu sa podľa čísla SPI nájde v tabuľke zodpovedajúci kľúčový materiál a špecifikácia algoritmov a paket sa rozšifruje.

Samotný štandard IPsec nedefinuje vytváranie bezpečnostných asociácií, to je ponechané na vyšší protokol manažmenu kľúčov. Ako štandardný protokol pre manažment kľúčov bol vybratý protokol ISAKMP/Oakley[19]. Tento protokol vytvára bezpečný, autentifikovaný kanál, pomocou ktorého potom dohaduje bezpečnostné asociácie medzi dvoma entitami.

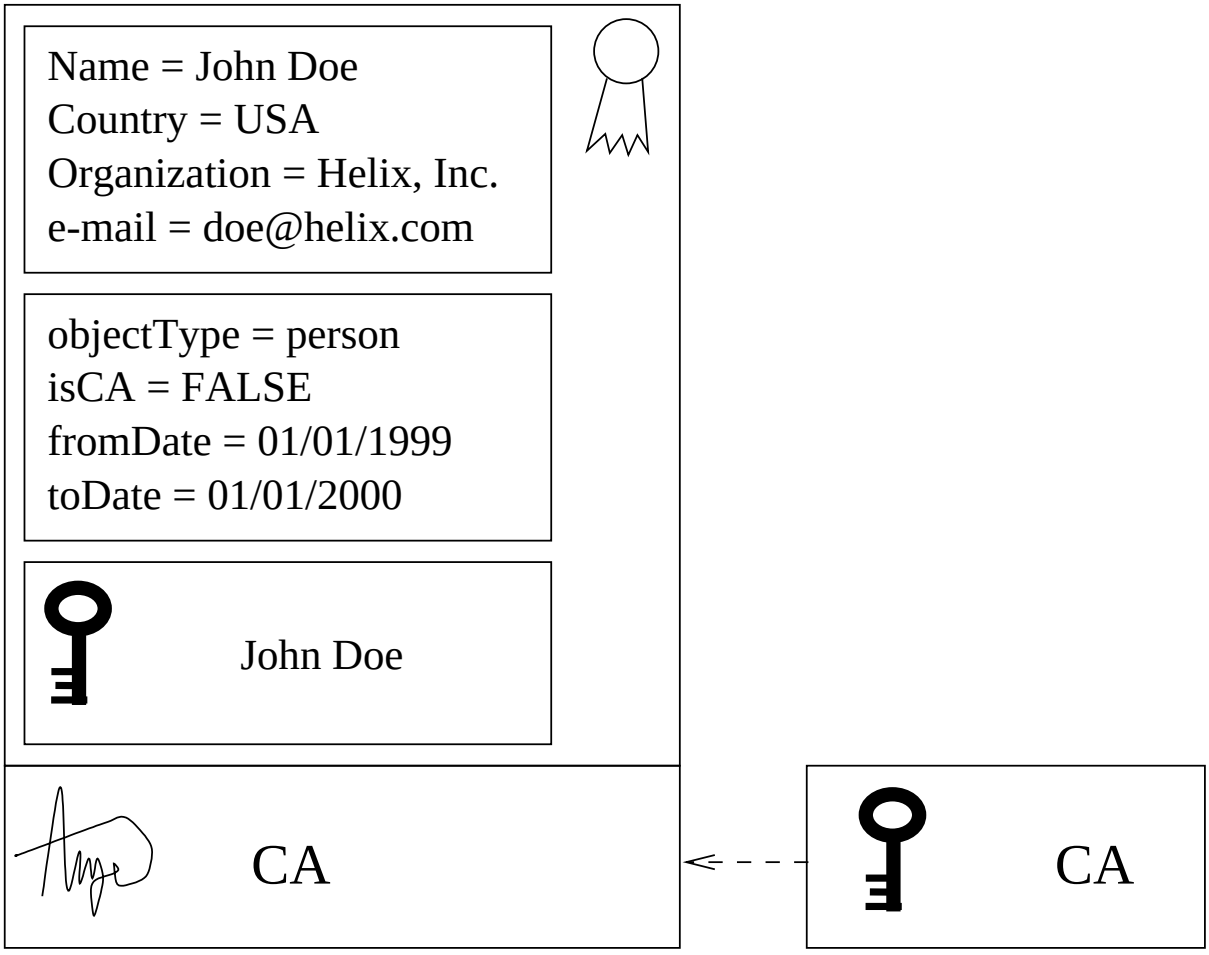
4.5 Kryptografická infraštruktúra

Slovo *kryptografia* je pre väčšinu ľudí totožné so slovom šifrovanie a spája sa s ochranou privátnych informácií. Kryptografia je však ďaleko viac ako len šifrovanie správ aby ich nemohol nepriateľ prečítať. Dnešná kryptografia ponúka okrem metód zaručenia privátnosti aj množstvo autentifikačných techník, manažment kľúčov, digitálne podpisy a časové značky a množstvo iných techník [20]. Šifrovanie by bolo zbytočné, ak by sme nedokázali chrániť a distribuovať šifrovacie kľúče. Distribúcia kľúčov by bola zbytočná, ak by sme nemohli zaručiť, že kľúč sa dostal len tam kam sa dostať mal, teda bez autentifikácie a zaručenia autenticity prepravovaného materiálu. V nasledujúcich kapitolách bude popísané, ako sa tieto metódy modernej kryptografie využívajú na skvalitnenie počítačovej bezpečnosti.

4.5.1 Certifikáty a certifikačné autority

Certifikátom v oblasti kryptografickej ochrany informácií sa nazýva väzba medzi identitou (objektom) a kľúčovým materiálom patriacim tejto identite. V konkrétnom prípade by certifikát mohol viazať meno, priezvisko, a elektronickú adresu istej ososby s jej verejným kľúčom. Okrem toho certifikát zvyčajne obsahuje aj dodatočné informácie o tom, na aké oblasti sa certifikácia vzťahuje (napr. či certifikovaný objekt môže alebo nemôže sám vydávať ďalšie certifikáty). Väzba medzi identitou, kľúčovým materiálom a dodatočnou informáciou sa realizuje elektronickým podpisom *certifikačnej autority*. Približnú štruktúru certifikátu ilustruje obrázok 18. Certifikát vydala autorita "CA" pre osobu menom JONH DOE z organizácie HELIX, INC. so sídlom v USA a adresou *doe@helix.com*. Certifikát je platný od 1.1.1999 do 1.1.2000 a nemôže slúžiť ako certifikát podradenej certifikačnej autority. Integrita autenticita certifikátu je zaručená elektronickým podpisom certifikačnej autority "CA".

[19]ISAKMP/Oakley bol vybraný spomedzi ostatných obdobných protokolov (SKIP, Photuris) najmä vďaka svojej flexibilite, čo však na druhej strane prináša jeho pomerne vysokú internú zložitosť.



Obrázok 18: Štruktúra elektronického certifikátu

Keďže certifikačné autority sú centralizované, prezradenie ich súkromného kľúča môže spôsobiť veľké škody. Z tohto dôvodu majú certifikačné autority kľúče veľkej dĺžky (najmenej 2048 bitov) a zavádzajú špeciálne procedúry na ochranu svojho kľúčového materiálu. Tento materíal sa uchováva buď na systémoch fyzicky izolovaných od počítačovej siete alebo v špeciánych zariadeniach nazývaných CSU (Certificate Signing Unit). Zariadenia CSU sú jednoúčelové hardvérové zariadenia určené na uchovávavnie kľúčov a podpisovanie certifikátov. Prístup k takémuto zariadeniu je väčšinou podmienený súčastným prezentovaním niekoľkých rôznych prístupových predmetov, ktoré vlastní niekoľko ľudí. Veľká dĺžka kľúča certifikačnej autority pomáha chrániť ho pred útokom hrubou silou, keďže tento kľúč ma veľmi dlhý čas trvanlivosti[20]. Ak má byť certifikát zneplatnený pred skončením doby jeho platnosti, certifikačná autorita ho umiestni na zoznam odobratých certifikátov (*certificate revocation list*, CRL). Používatelia, ktorí požadujú vysokú úroveň dôvery v certifikát môžu kontrolovať tento zoznam vždy pri používaní certifikátu, ktorý certifikačná autorita vydala. Presné umiestnenie zoznamu odobatých certifikátov je väčšinou uvedené priamo v certifikáte.

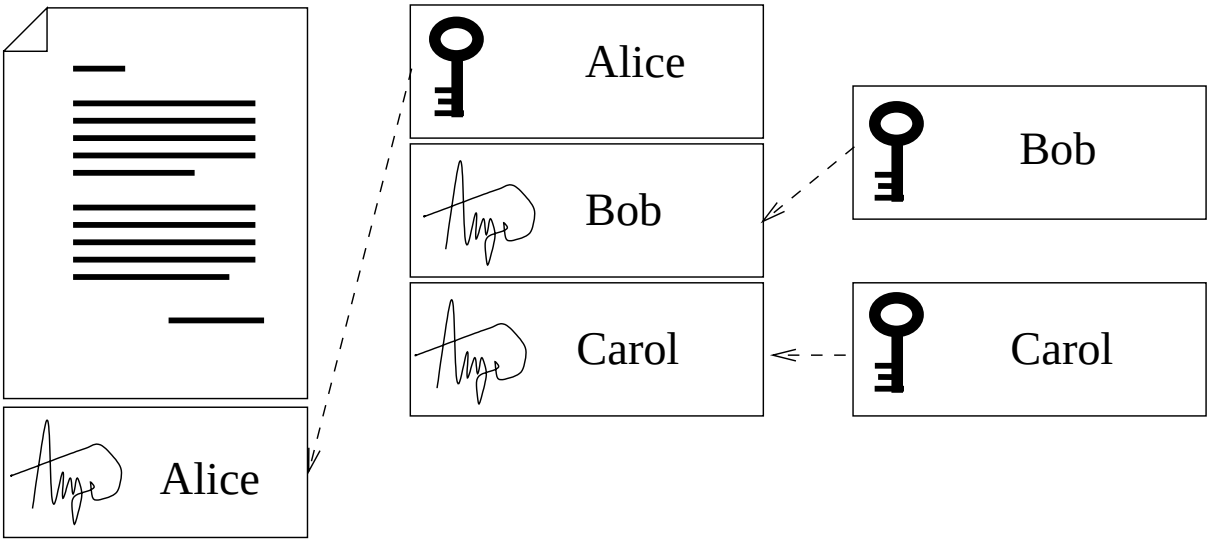
Každá certifikačná autorita by mala publikovať dokument opisujúci proces certifikovania a pravidlá overovania identity certifikovaných objektov. Na základe takéhoto dokumentu je možné rozhodnúť o stupni dôvery v konkrétnu certifikačnú autoritu. Taktiež je bežné, že certifikačná autorita má niekoľko kľúčov a každým z nich produkuje certifikáty rôznej bezpečnostnej úrovne. Toto platí hlavne pri verejných certifikačných autoritách na Internete.

4.5.2 Šifrovanie správ elektronickej pošty

Väčšina protokolov pre transport elektronickej pošty je zameraná takmer výlučne na funkčnosť a implementujú len minimum bezpečnostných prvkov. Správy elektronickej pošty sú prenášané v otvorenej forme, bez zabezpečenie integrity a autenticity. Na tento stav sa snažia reagovať systémy realizujúce šifrovanie správ elektronickej pošty spôsobom *end-to-end*, čiže priamo v poštových systémoch odosielateľa a príjemcu správy. Odosielateľov systém správu podpíše a/alebo zašifruje a odošle, správa sa prenesie štandardným systémom elektronickej pošty a doručí sa príjemcovi. Príjemcov systém zistí, že správa je zabezpečená a pred zobrazením ju rozšifruje a overí podpis odosielateľa. Najzložitejšou časťou je manažment kľúčov, pretože momentálne nie práve najbezpečnejší Internet neposkytuje metódy bezpečného transportu kľúčového materiálu.

Tento problém sa viac či menej úspešne snažilo riešiť niekoľko poštových zabezpečovacích systémov, z ktorých sú momentálne rozšírené už len dva: Pretty Good Privacy

[20]Bežne je to niekoľko rokov, pri nutnosti zabezpečiť autenticitu dokumentov v archívoch aj niekoľko desiatok rokov.



Obrázok 19: Podpis a verejný kľúč v systéme PGP

(PGP) a S/MIME. Ostatné systémy upadli do zabudnutia hlavne vďaka nízkej prepracovanosti manažmentu kľúčov a slabej podpore výrobcov[21]. V nasledujúcich odstavcoch si tieto dva systémy bližšie predstavíme.

Pretty Good Privacy Systém Pretty Good Privacy (PGP) je súbor programov na šifrovanie a podpisovanie správ elektronickej pošty a bežných súborov, ktorý obsahuje aj základné nástroje pre generovanie a správu kľúčového materiálu.

PGP používa model "pavučiny dôvery" (*web of trust*), kde každý účastník systému svojím podpisom zaručuje autenticitu cudzieho kľúčového materiálu. Pri vyhodnocovaní dôvery elektronického podpisu sa potom prechádzajú všetky tieto podpisy na kľúči a podľa dôvery, ktorú používateľ vložil na jednotlivých účastníkov, sa vyjadrí celková dôvera podpisu. Príklad podpisu a verejného kľúča je ilustrovaný na obrázku 19. Správu napísala Alice, podpísla ho svojim elektronickým podpisom, ktorý je pripojený k správe. Tento podpis je možné overiť pomocou jej verejného kľúča. Autenticitu Alicinho kľúča potvrdzujú svojimi podpismi Bob a Carol. Alicin kľúč môže byť bezpečne vystavený na verejnom mieste (napr. Alicinej WWW stránke), pretože jeho integritu zaručujú elektronické podpisy. Keď chceme overiť, že túto správu naozaj napísala Alice, Musíme vložiť istý stupeň dôvery v kľúč Boba alebo Carol. V systéme PGP sa jednotlivým týmto identitám (ako sú Bob a Carol, tzv. *introducers*) priraďuje stupeň dôvery a výsledná dôvera v podpis je potom založená na istej matematickej operácií nad stupňami dôvery v identity, ktoré kľúč podpísali. V reálnom prípade môžu byť vzťahy medzi týmito identitami veľmi komplikované a prepletené. Preto pre tento spôsob distribúcie dôvery vznikol názov

[21]Podobne dopadol aj návrh štandardu IETF *Privacy Enhance Mail* (PEM) a jeho nasledovník PEM-MIME (MOSS).

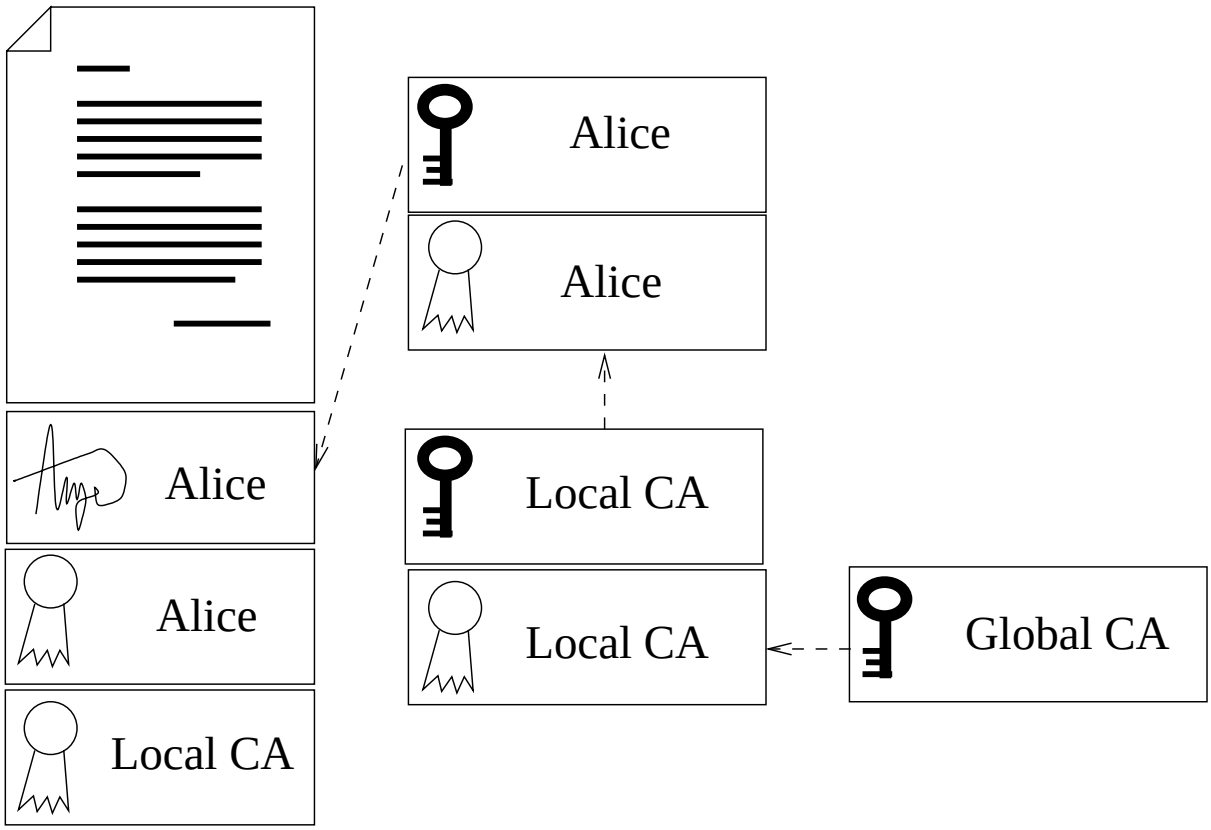
"pavučina" dôvery.

Takýto distribuovaný systém sa hodí do prostredí, kde nie je žiadna prirodzená autorita schopná zabezpečiť dobrú autenticitu kľúčov a jednotliví účastníci sa aspoň sčasti osobne poznajú a sú vo fyzickom kontakte. Distribúcia dôvery predstavuje isté riziko pri vyhodnocovaní autenticity kľúča, pretože prideľovanie stupňov dôvery v jednotlivé elektronické idetity je realizované len na báze úsudku účastníkov.

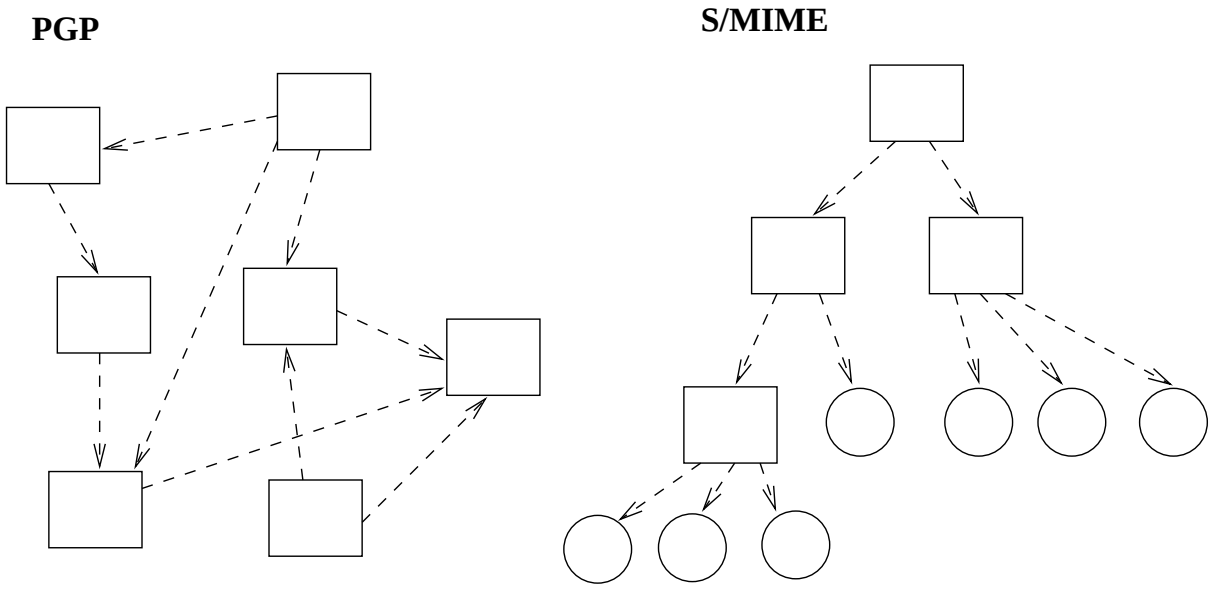
S/MIME S/MIME (Secure Multipurpose Internet Mail Extension) je bezpečnostný protokol elektronickej pošty založený na niekoľkých široko používaných a dobre overených štandardoch (MIME, PKCS a X.509, [20]). Tento protokol umožňuje šifrovať a podpisovať elektronickú poštu a spravovať kľúčový materiál vo forme certifikátov. Je založený na štandardných šifrovacích algoritmoch ako sú napríklad RSA, DES, RC4, RC5, MD5. Ich počet a parametre nie sú obmedzené a môžu sa časom vyvíjať. Správy sú šifrované symetrickou šifrou, ktorej náhodne generovaný kľúč je chránený asymetrickou šifrou. Podobne je to aj pri podpise, kde asymetrická šifra chráni výsledok kryptografického *hash*-u správy. Správa kľúčov protokolu S/MIME je centralizovaná a hierarchizovateľná. Systém je založený na hierarchí certifikačných autorít (CA), ktoré overujú identitu účastníkov a vydávajú *certifikáty* zaručujúce autenticitu kľúčového materiálu. Príklad správy v systéme S/MIME je ilustrovaný na orázku 20. Správu napísala Alice, ktorá k nej pripojila aj svoj elektronický podpis. Identitu Alice overila lokálna certifikačná autorita "Local CA", ktorá jej vydala certifikát. Tento certifikát potvrdzuje väzbu medzi Alicinou identitou (uvedeneou v certifikáte) a jej verejným kľúčom. Identita lokálnej certifikačnej autority je potvrdená certifikátom globálnej certifikačnej autority "Global CA". Certifikát Alice a lokálnej certifikačnej autority pripojí Alica ku správe, ktorú odošle príjemcovi. Príjemcovi na spoľahlivé overenie podpisu stačí znalosť kľúča globálnej certifikačnej autority, nemusí dôverovať kľúču lokálnej certifikačnej autority a ani Alicinmu, ich autenticitu zaručujú certifikáty.

Takýto hierarchický systém je vhodný do prostredí s hierarchickou štruktúrov kde sú vytvorené prirodzené centrá autority. Ideálne uplatnenie nachádza v podnikovom prostredí a prostredí komerčného Internetu. Malý počet certifikačných autorít najvyššej úrovne umožňuje distribúciu ich kľúčového materiálu priamo s aplikáciami elektronickej pošty.

Celkové porovnanie modelov dôvery PGP a S/MIME je načrtnuté na obrázku 21. Na tomto obrázku sú štvorcami zobrazené entity schopné podpisovať kľúče iných entít (certifikačné autority) a kruhmi sú zobrazené entity, ktoré nemôžu podpisovať cudzie kľúče.



Obrázok 20: Správa, podpis a certifikáty v systéme S/MIME



Obrázok 21: Porovnanie siete dôvery PGP a S/MIME

4.5.3 SSL/TLS

Komunikácia pomocou transportného protokolu TCP nie je zabezpečená pred zámerným zneužitím, pridaním ďalšej vrstvy nad TCP je však možné zabezpečiť bezpečnostné služby. Takúto vrstvu[22] zabezpečuje protokol SSL (Secure Socket Layer, [13]), zavedený firmou Netscape. Protokol SSL zabezpečuje integritu a šifrovanie spojenia pomocou symetrickej kryptografie, ktorej relačné kľúče sú vymieňané pri inicializácií spojenia a sú chránené asymetrickou šifrou. Protokol SSL zabezpečuje aj vzájomnú autentifikáciu účastníkov spojenia pomocou overovania certifikátov verejných kľúčov šifier chrániacich úvodnú výmenu relačných kľúčov. Protokol SSL používa štandardné certifikáty vo formáte X.509.

K vzniku a rozšíreniu protokolu SSL prispela hlavne potreba bezpečnej komunikácie medzi WWW serverom a prehliadačom. Na ochranu tejto komunikácie vznikol protokol HTTPS, ktorého základ tvoril protokol SSL. Neskôr sa tento protokol začal používať aj na zabezpečenie iných služieb a dnes už tvorí *de facto* štandard v poskytovaní bezpečnostných služieb na transportnej úrovni protokolov TCP/IP.

Na rozšírení protokolu SSL pracuje pracovná skupina IETF, ktorá má za úlohu špecifikovať štandard TLS (Transport Layer Security) na zabezpečenia spojení na transportnej vrstve [14].

4.5.4 Bezpečnostné rozšírenia DNS

Systém doménových mien Internetu (*Domain Name System*, DNS) je široko používaný systém na mapovanie doménových mien uzlov siete na ich korešpondujúce sieťové (IP) adresy. Jeho najväčšou nevýhodou je však absolútna absencia bezpečnostných služieb, čo negatívne prispieva k jeho dôveryhodnosti. Tent problém sa snaží riešiť štandard DNSSEC [**?**, **?**], definujúci bezpečnostné rozšírenia systému DNS. Tento štandard definuje mechanizmy pre distribúciu kľúčov pomocou systému DNS a na autentifikáciu zdroja dát, DNS transakcií a žiadostí.

Na distribúciu kľúčov slúži špeciálny typ údajov (*resource record,* RR) "KEY RR". Takto uložené kľúče možno využiť pri dohadovaní bezpečnostných asociácií pomocou protokolov štandardu IPsec (ISAKMP/Oakley, pozri kapitola 4.4.3). Distribúcia kľúčového materiálu pomocou DNS vyžaduje malú réžiu za predpokladu malej frekvencie zmeny hlavných kľúčov (*master keys*).

Zaručenie zdroja dát v zónach systému DNS slúži typ záznamu "SIG RR". Pomocou tohto záznamu sa realizujú elektronické podpisy objektov uložených v zónach DNS a tým sa zaručuje ich pôvod. Autentifikáciu pôvodu je možné sledovať prechádzaním hierarchie systému DNS a autenticitu každého stupňa hierarchie kryptograficky overiť.

[22] V podste sa jedná o časť patriacu do relačnej vrstvy, ktorú model TCP/IP nemá.

4.6 Autentifikácia

Proces deklarovania a dokazovania identity objektu sa nazýva autentifikácia. Autentifikácia prebieha keď sa nahlasujete do systému pomocou hesla alebo keď v banke predkladáte občiansky preukaz. Je zrejmé, že falšovaním autentifikačného procesu je možné sa vydávať za akúkoľvek osobu a tým získať jej plné práva. Toto je hlavný dôvod prečo je autentifikačný systém tak dôležitý a prečo je veľmi často cieľom útoku.

Autentifikácia sa podľa spôsobu dokazovania identity objaktu delí na tri základné skupiny:

Niečo viem. Autentifikačnému systému predkladám dôkaz o tom, že mám znalosť o istej informácií. Sem patrí autentifikácia všetkými druhmi hesiel a PIN čísel. Heslo sa systému predkladá buď priamo v otvorenej forme, alebo sa pri dokazovaní jeho znalosti vyžaduje istý spôsob interakcie (systémy výzva - odpoveď).

Niečo mám. Predkladám dôkaz o vlastníctve istej veci. Do tejto kategórie patria všetky systémy čipových a magnetických kariet, prístupových kalkulátorov a hardvérových kľúčov. Dôkaz o vlastníctve predmetu sa väčšinou realizuje nepriamo dokazovaním vlastníctva informácií na predmete uložených (prístupové kalkulátory) alebo poskytnutím celého predmetu na preskúmanie (karty s magenetickým prúžkom).

Niečo som. Dokazujem svoju identitu pomocou svojho neoddeliteľného materiálneho základu. Všetky biometrické metódy patria do tejto kategórie a dokazujú identitu človeka na základe jeho vonkajších telesných znakov (zrenica, dúhovka, odtlačok prstu) alebo jeho životných prejavov (analýza reči, podpisu).

V praxi sa jednotlivé tieto triedy navzájom kombinujú, aby sa tak dosiahol celkový vyšší stupeň bezpečnosti autentifikačného procesu. Na príklade systému bankomatov je skombinovaná autentifikácia vlastníctvom magnetickej karty a znalosťou PIN kódu. V ďalších kapitolách budú podrobnejšie popísané jednotlivé najpoužívanejšie autentifikačné systémy.

4.6.1 Pevné heslá

Autentifikácia pomocou pevného hesla je najjednoduchšia a najstaršia metóda dokazovania identity. Pri tejto metóde má objekt pridelené pevné heslo, ktoré sa bežne nemení a pri autentifikácií toto heslo v otovorenom tvare[23] prezentuje. Najväčším problémom tejto metódy je možné prezradenie hesla pasívnym odpočúvaním komunikačného kanálu.

[23]Pod "otvoreným tvarom" sa myslí že informácia potrebná na autentifikáciu (*credentials*) sa v čase nemení. Do tejto kategórie patria aj autentifikačné systémy ktoré túto informáciu kryptograficky počítajú čisto na základe užívateľom vloženého hesla.

Heslový materiál sa na cieľovom systém väčšinou neukladá v otvorenej forme, ale fo forme kryptografickej sumy vytvorenej nad otvoreným heslom. Takto zabezpečené heslá nie sú priamo prezradené ani pri prieniku na cieľový systém.

4.6.2 Heslá na jedno použitie

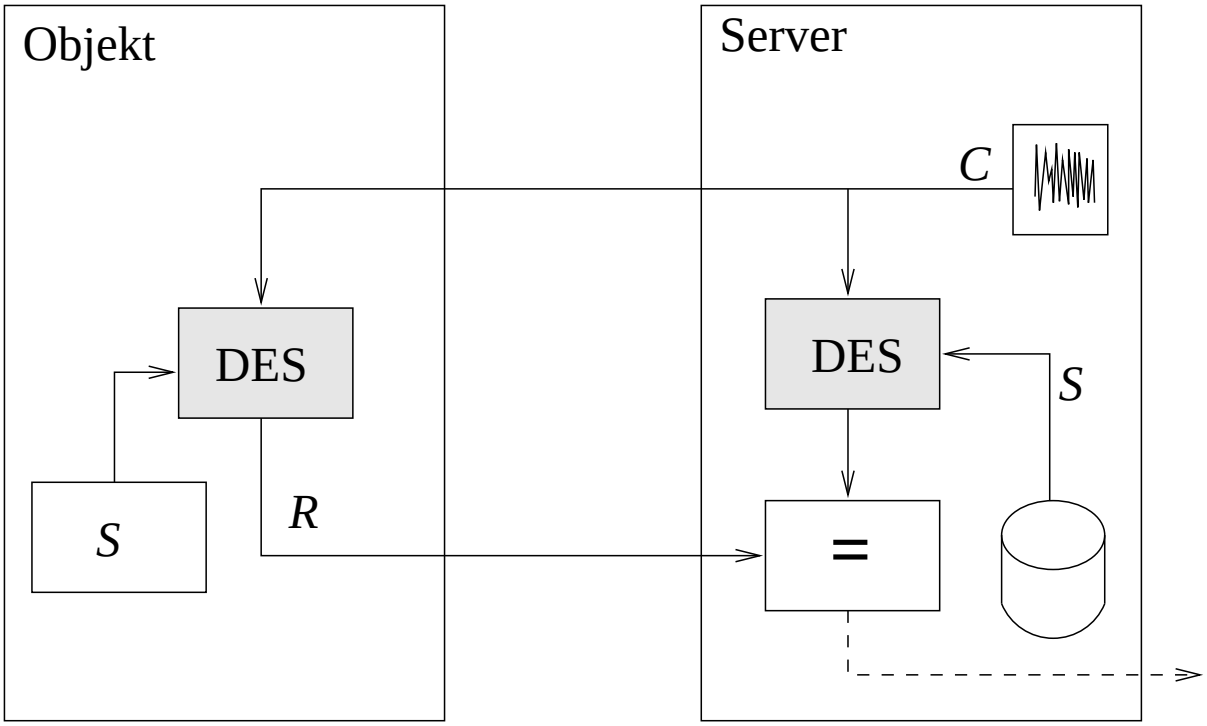
Ako už sám názov hovorí, táto autentifikačná procedúra sa zakladá na prezentovaní jednorazového hesla cieľovému systému. Pri druhom a ďalšom prezentovaní tohto hesla už autentifikácie neprebehne úspešne, preto tento systém nie je citlivý na pasívne odpočúvanie komunikačného kanála. Jednorazové heslá sú väčšinou generované na základe prvotného zieľaného tajomstva, ktoré musí byť iniciálne nakonfigurované na oboch stranách autentifikačného systému. Synchronizácia jednorazových hesiel sa väčšinou realizuje pomocou hardvérového zariadenia s presným reálnym časom alebo tak, že autentifikačný server poskytne sekvenčné číslo hesla, ktoré očakáva. Poskytnutie informácie autentifikačným serverom však tento sytém približuje kategórií výzva-odpoveď.

Reálne sa systém jednorazových hesiel realizuje distribuovaním zoznamu hesiel autentifikovaným objektom bezpečným kanálom. Keď objekt vyčerpá všetky heslá na zozname, musí si zaobstarať nový zoznam. Prvým rozšíreným autentifikačným systémom s heslom na jendo použitie bol S/KEY [26] od firmy Bellcore, ktorý bol založený na sekvencií aplikovania kryptografickej sumy MD5 na zdieľané tajomstvo.

4.6.3 Výzva - odpoveď

Pri systéme výzva-odpoveď (*challenge-response)* autenfikačný server poskytne istú informáciu ktorú musí autentifikovaný objekt pretransformovať určitým spôsobom dokazujúcim že vlastní tajnú informáciu. Táto transformácia sa väčšinou zakladá na kryptografických technikách a má vlastnosť nevratnej funkcie. Príklad takéhoto autentifikačného systému ukazuje obrázok 22. Server pošle objektu náhodne vygenerovanú výzvu (*challenge*) C. Objekt po jej obdržaní túto výzvu zašifruje pomocou algoritmu DES s tajným kľúčom S. Tento kľúč predstavuje zdieľané tajomstvo a jeho vlastníctvo sa objekt snaží dokázať serveru. Zašifrovanú odpoveď R (*response)* pošle objekt serveru. Server vykoná tú istú operáciu nad výzvou C a svojím uloženým kľúčom S. Ak sa výsledok tejto operácie zhoduje s odpoveďou, objekt musí naozaj vlastniť tajný kľúč S a tak je jeho identita dokázaná.

Tento spúsob autentifikácie vyžaduje isté kryptografické schopnosti na strane autentifikovaného objektu a tak je pre priamu autentifikáciu osôb takmer nepoužiteľný. Jeho princíp sa však veľmi často využíva v prístupových predmetoch a softvérových systémoch.



Obrázok 22: Autentifikácia pomocou výzvy a odpovede

4.6.4 Prístupové predmety

Prístupový predmet (*access token) je* prenosné harvérové zariadenie, ktorého vlastníctvom sa dokazuje identita objektu, ktorý ho vlastní. Prístupové predmety sú buď čisto pamäťové (karta s magentickou páskou) alebo obsahujú aj procesnú jednotku (*SmartCard*). Každý prístupový predmet počas autentifikačného procesu prezentuje isté informácie, ktoré môžu ale nemusia byť založené na externom vstupe informacií do predmetu (PIN, výzva, atď.).

Pamäťové prístupové predmenty majú za úlohu si zapamätať isté údaju (číslo účtu, heslá, atď.) a pri autentifikácií tieto údaje doslovne prezentovať. Bezpečnosť pamäťových prístupových predmotov je závislá hlavne na obtiažnosti vyrobenia kópie prístupového predmetu, čo zväčša pri tomto druhu predmetov nebýva náročná úloha. Pamäťové prístupové predmenty slúžia viac na zlepšenie pohodlia autentifikačného procesu ako na zlepšenie jeho bezpečnosti.

Prístupové predmety s procesnou jednotkou vo väčšine prípadov implementujú niektorú modifikáciu autentifikácie pomocou výzvy a odpovede, kde tajnú informáciu tvorí kombinácia sériového čísla predmetu a vlastníkom zadaného PIN čísla. Špeciálnym prípadom týchto predmetov sú prístupové predmety založené na reálnom čase, kde do procesu namiesto výzvy od autentifikačného servera vstupuje aktuálna hodnota reálneho času.

Technické prevedenie prístupových predmetov sa na prvý pohľad líši riešením rozhrania medzi predmetom a výpočtovým systémom. Magnetické a čipové karty a bezkontak-

tné predmety potrebujú špeciálne čítacie zariadenia, infra-červené prístupové predmety vedia komunikovať pomocou štandardného infračerveného rozhrania IrDA a prístupové kalkulátory potrebujú na prenos informácie zásah človeka, ktorý informáciu manuálne prepíše. Zložitejšie prístupové predmety sú väčšinou fyzicky chránené proti prezradeniu chránenej informácie autodeštrukčným mechanizmom. Autentifikačné systémy pracujúce s prístupovými predmetmi veľmi často kombinujú ich použitie s autentifikáciou pomocou hesla alebo PIN (ak to nevykonáva priamo prístupový predmet) a tak chránia systém pred následkami odcudzenia prístupového predmetu.

Prístupové predmenty sa v prostredí Internetu začali využívať len nedávno, a to hlavne v sfére bankovníctva a finančníctva. Prekážkou ich vysokého nasadenia je ich zatiaľ vysoká cena a vzájomná nekompatibilita produktov rôznych výrobcov.

4.6.5 Biometria

Biometrické metódy sa snažia identifikovať osobu na základe skúmania jej hmotnej podstaty alebo jej životných prejavov. K biometrickým metódam patria všetky metódy analýzy odtlačkov prstov, sietnice, dúhovky, geometrie ruky, hlasu, podpisu a mnoho ďalších metód. Ich takmer jednoznačným spoločným faktorom je relatívne vysoká spoľahlivosť a nutnosť použitia dodatočných hardvérových prostriedkov (snímač odtlačkov prstov, a pod.) čo spôsobuje vysoké náklady na prevádzku biometrického systému. Využitie nachádzajú hlavne v systémoch kde sa požaduje vysoká úroveň bezpečnosti. Ich použitie pri autentifikácií logického vstupu do informačného systému (*login)* bolo až donedávna zriedkavé. Klesajúce ceny špeciálneho hardvéru však sľubujú perspektívny rozvoj týchto metód, keďže ich používanie je aj pri ich vysokej úrovni bezpečnosti dostatočne pohodlné[24].

4.7 Systémy pre detekciu prieniku

Počítačová bezpečnosť sa stáva veľmi komplexnou a náročnou disciplínou. Množstvo vedomostí a informcií nutných k udržaniu dostatočne dobrého stavu bezpečnosti prudko rastie. Útočníkov pribúda a ich efektivita stúpa. Dokážu sa združovať a spolupracovať. Držať stráž nad podnikovou sieťou prestáva byť v ľudských silách. Automatizované zariadenia na detekciu prieniku (*Intrusion Detection Systems*, IDS) majú nahradiť niektoré ľudské činnosti a doplniť ich strojovou spoľahlivosťou a rýchlosťou. IDS je zariadnie, ktoré sleduje dôležité udalosti na sieti alebo uzle a snaží sa rozhodnúť či tieto udalosti sú porušením bezpečnostnej politiky alebo nie. Na realizáciu takejto rozhodovacej činnosti musí mať IDS dostatok "inteligencie", čiže jeho analytický modul musí pracovať ako

[24]Navyše neexistuje možnosť aby používateľ zabudol heslo alebo stratil predmet, keďže svoje autentifikačné znaky nosí stále so sebou.

expertný systém. Podľa spôsobu činnosti analytického modulu sa systémy pre detekciu prieniku delia na:

Detekcia zneužitia (*misuse detection*): Systém rozoznáva porušenie bezpečnostnej politiky pomocou identifikovania *signatúr útoku*. Signatúra útoku je presne definovaná postupnosť udalostí zameraných na zneužitie slabého miesta systému. Tento systém pracuje na základe vyhľadávania vzoriek vo vstupnom prúde udalostí.

Detekcia štatistických anomálií (*statistical anomaly detection*): Systém sleduje správanie systému za normálnych podmienok počas dlhej doby a vytvorí si štatistický model sledovaného prostredia. Útok je detekovaný ako odchýlka (anomália) momentálneho správania sa prostredia k odvodenému modelu správania.

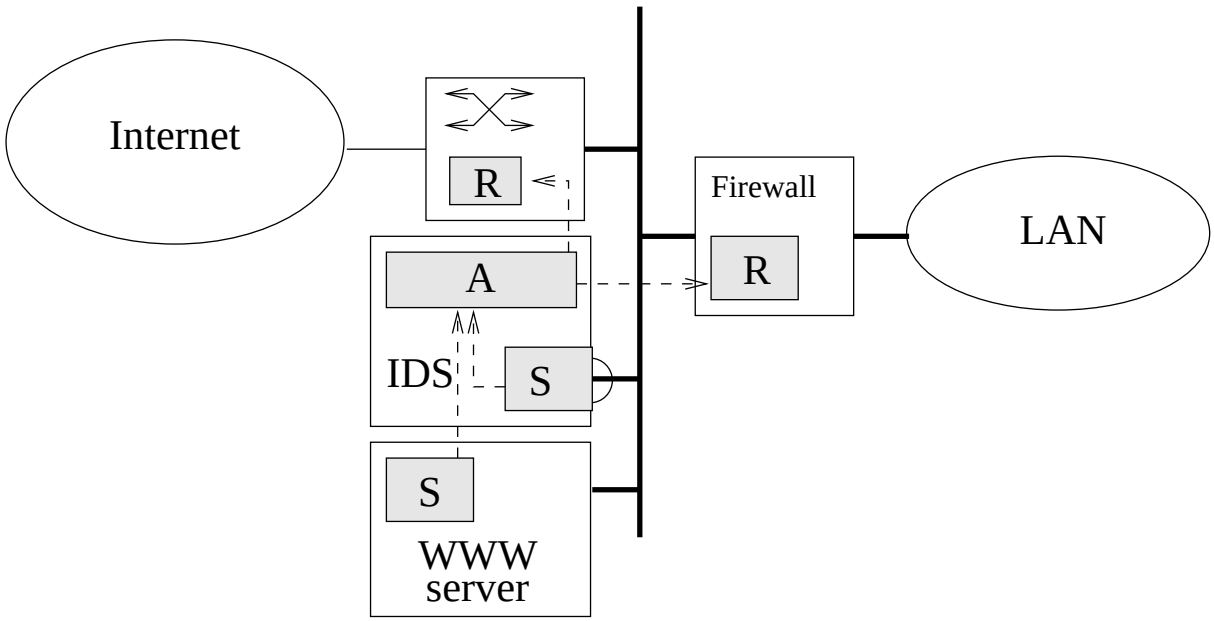
Okrem analytického modulu je tiež dôležitý modul senzorov. Tento modul poskytuje analytickému modulu prúd udalostí založených na sledovaní prostredia. Podľa spôsobu zberu dát senzorickým modulom sa IDS systémy delia na:

Sieťové (*network-based*) senzory: Senzor zberá údaje získané odpočúvaním siete. Snaží sa dekódovať zachytené protokolové dátové jednotky a na ich základe produkovať prúd udalostí pre analytický modul.

Uzlové (*host-based*) senzory: Senzor zberá údaje z prostredia operačného systému uzla. Monitoruje stav uzla a činnosť užívateľov a procesov a na ich základe produkuje udalosti pre analytický modul. Veľmi často sa na tento účel používa sledovanie záznamov systémového auditu (*audit trails*).

Posledným dôležitým modulom systému IDS je výkonný modul. Tento modul zabezpečuje oznámenie zistených skutočností obsluhe, poprípade vykonanie automatických akcií na zabránenie prieniku.

Väčšina doterajších systémov IDS bola monolitická. Senzorický modul, analytický modul a výkonný modul boli integrované do jediného produktu. Vo väčšine prípadov bolo celé takéto zariadenie zamerané len na jeden špecifický typ analýzy a zberu informácií, napríklad veľmi bežné sú sieťové systémy IDS založené na detekcií zneužitia vyhľadávaním signatúr útoku v TCP/IP paketoch. Príkladom takéhoto systému je NetRanger firmy Cisco [28]. V poslednom čase sa však začínajú objavovať aj distribuované IDS systémy. Tieto systémy môžu pracovať na viacerých uzloch a používať naraz viac princípov analýzy a senzorických systémov na zvýšenie spoľahlivosti detekcie útoku. Príkladom takéhoto systému je AAFID vytvorený ako súčasť projektu COAST na Purdue University [29].



Obrázok 23: Príklad IDS systému založeného na CIDF

4.7.1 Spoločná architektúra pre IDS

Detekčné systémy IDS sa pomaly začínajú presadzovať na trhu. Ich väčšinou privátna architektúra a vlastné komunikačné protokoly však neumožňujú efektívnu spoluprácu systémov IDS. Na riešení tohto problému pracuje široko obsadená pracovná skupina. Táto skupina pracuje na projekte s názvom "Common Intrusion Detection Framework" (CIDF, [30]). Projekt je zameraný na vytvorenie špecifikácie spoločnej architektúry a komunikačných protokolov na spoluprácu rôznych systémov IDS, senzorov, analyzátorov a výkonných modulov. Táto architektúra by mala umožňovať stavať rozsiahle a účinné systémy pre detekciu útokov a realizáciu protiopatrení na základe modulov rôznych výrobcov. Príklad takéhoto systému ilustruje obrázok 23. Senzorický modul na WWW serveri sleduje operačný systém uzla a generuje udalosti vo všeobecnom formáte, ktoré potom posiela analytickému modulu na uzle IDS. Senzorický modul na uzle IDS odpočúva sieť demilitarizovanej zóny a produkuje udalosti vo všeobecnom formáte pre analytický modul. Analytický modul spracováva informácie z dvoch zdrojov a preto môže zaručiť vyšiu spoľahlivosť výsledkov analýzy. V prípade detekcie útoku pošle analytický modul podnet na vykonanie protiopatrenia na výkonné moduly umiestnené na prístupomov mserovači a firewalle. Pritom každý modul môže pochádzať od iného výrobcu.

Zaujímavá črta modelu CIDF je v tom, že komunikácia nemusí byť striktne jednosmerná. Napríklad ak analytický modul príde k záveru, že udalosti zo senzora na WWW serveri naznačujú možný útok, môže sa aktívne spýtať druhého senzora, či nespozoroval podozrivú aktivitu, ktorá by domnienku o útoku podporila. Model CIDF zaručuje vysokú

flexibilitu pri dodržaní spoločného formátu výmeny správ.

4.8 Hardvérové a nízkoúrovňové zabezpečenie

Niektoré riziká porušenia bezpečnosti informačného systému je možné efektívne eliminovať na najnižších vrstvách logickej štruktúry systému. Fyzické zabezpečenie komunikačných kanálov sa stále ukazuje ako značne efektívna metóda zabezpečenia privátnosti komunikácií. Je to najmä vďaka bohatým skúsenostiam v odbore fyzickej bezpečnosti v porovnaní s relatívne mladou disciplínou bezpečnosti informačnej. Podobný prístup môžeme často pozorovať aj pri zabezpečovaní centralizovaných systémov typu klient - server. Veľké centrálne servery sú väčšinou dobre fyzicky chránené vzhľadom k ich vysokej cene a riziku odcudzenia a návrhári informačných systémov spoliehajú na túto fyzickú ochranu aj pri návrhu bezpečnostných mechanizmov. Veľmi často využívaný prístup je obmedzenie softvérových servisných činností len na konzolu systému, vyžadujúc si tak fyzickú prítomnosť správcu v chránenom priestore kde sa výpočtový systém nachádza.

Sieťové zariadenia tiež bývajú fyzicky chránené proti neoprávnenému prístupu, v zbernicových sieťach je však dôležitý problém šírenia informácií ku všetkým staniciam siete. V najpoužívanejších sieťach typu Ethernet je však možné tomuto šíreniu predísť používaním sieťových prepínačov (*network switch*) ktoré šíria informácie len selektívne od zdroja k cieľu, čím sa minimalizuje riziko odpočúvania. Použitie prepínača však nie je dokonalým riešením, pretože väčšinu moderných prepínačov je možné konfigurovať vzdialene a obsahujú možnosť nastaviť niektorý z portov do "monitorového" režimu, čo stále umožňuje odpočúvanie informácií. Pri vhodnom zabezpečení prístupu do konfigurácie prepínača je však toto nebezpečenstvo možné minimalizovať.

4.9 Bezpečnostný projekt

Zavádzanie bezpečnostnej ifraštruktúry v organizáciách je dlhý, náročný a nákladný proces, ktorý si vyžaduje prísne systematický prístup. Bezpečnostné aspekty sa priamo dotýkajú strategických zámerov každej organizácie a porušenie bezpečnosti ogranizácie môže vážne ohroziť jej zámery a dokonca aj samotnú jej existenciu. Napriek tomu je informačná bezpečnosť vo väčšine organizácií riešená *ad hoc* bez celkovej koordinácie a systémového prístupu. Riešenie informačnej bezpečnosti by sa malo držať zásad vedenia bezpečnostného projektu, aby sa v maximálnej miere zlepšila efektivita bezpečnostných systémov a znížili náklady, ktoré sú v sfére informačnej bezpečnosti oproti iným oblastiam informatiky relatívne vysoké.

Žiaden systém sa nedá zabezpečiť na 100%. Náklady potrebné na zvýšenie bezpečnosti systému rastú exponenciálne s úrovňou jeho zabezpečenia. Úlohou bezpečnostného

projektu je nájsť vyváženie medzi nákladmi na zlepšenie stavu bezpečnosti systémov a reziduálnym rizikom porušenia bezpečnosti. V nasledujúcich kapitolách budú v hrubých črtách uvedené jednotlivé etapy bezpečnostného projektu. Tieto etapy sú z časti prebrané z metodiky bezpečnostného projektu navrhnutej pre použitie automatizovaného systému rizikovej analýzy MELISA [31].

4.9.1 Inicializácia projektu

Najdôležitejšie pri bezpečnostnom projekte je to, aby nakoniec nezostal len projektom. Na presadenie zmien, ktoré projekt navrhne je nutné už pri jeho vytváraní zainteresovať členov vrcholového manažmentu organizácie. V tejto prípravne etape sa vytvára *výbor riadenia projektu*, ktorý sa skladá z odborníkov na informačnú bezpečnosť ako aj zástupcov manažmentu organizácie. Výbor riadenie projektu musí mať dostatočnú právomoc presadiť navrhnuté zmeny. Na vypracovaní samotného projektu sa budú podieľať členovia *pracovnej skupiny*, ktorí budú vypracovávať samotný projekt a koordinovať zavádzanie vybraných protiopatrení.

Súčasťou inicializácie projektu je aj pripravenie jednotlivých účastníkov projektu na jeho priebeh formou školení a prezentácií a uviesť členov výboru riadenia projektu a ostatné zainteresované osoby do oblasti informačnej bezpečnosti.

Výstupom etapy inicializácie projektu je pripravený výbor riadenia projektu a pracovná skupina projektu.

4.9.2 Analýza hodnôt

Náplňou analýzy hodnôt je identifikovať *aktíva* informačného systému, ich možné ohrozenia a dopady týchto ohrození na strategické zámery organizácie. Aktíva informačného systému tvoria informácie, predmety a osoby, ktoré sú nevyhnutné pre plnenie strategických zámerov organizácie. Po identifikácií aktív sa analýzujú možné zdroje ohrozenia aktív (agresori a hazardy) a stupeň akým môžu tieto zdroje ohrozenia na aktíva vplývať. Ohrozenie aktív sa premietne na stupnicu ohrozenia strategických zámerov organizácie. Keď už je zrejmé ktoré strategické zámery organizácie môže byť ohrozené a aký je stupeň ich ohrozenia, môžeme syntetizovať požadované úrovne zabezpečenia jednotlivých aktív. Počas analýzy hodnôt sa väčšinou realizuje aj modelovanie bezpečnostne relevantných komponentov systému. Tento model sa neskôr využíva na simulovanie dopadu protiopatrení na celkovú bezpečnostnú úroveň organizácie.

Výsledkom analýzy hodnôt je zjednodušený model systému a úrovne požadovaných bezpečnostných parametrov pre organizáciu ako celok alebo jednotlivé aktíva.

4.9.3 Analýza zraniteľnosti

Pod pojmom analýza zraniteľnosti sa myslí analýza súčasného stavu bezpečnostných vlastností bezpečnostne relevantných komponentov systému. V rozsiahlej organizácií sa takáto analýza realizuje prostredníctvom dotazníkov generovaných pre každý relevantný systém. Tieto dotazníky obsahujú otázky ohľadne dôležitých inštalačných a konfiguračných parametrov informačných alebo fyzických sytémov. Koordináciu celého procesu vyplňovania dotazníkov riadi pracovná skupina projektu. Dotazníky sa väčšinou spracúvajú automatizovane na základe modelu systému z predchádzajúce etapy. Výsledkom vyhodnotenia dotazníkov je celková momentálna úroveň bezpečnosti organizácie.

4.9.4 Protiopatrenia

Do tejto etapy vstupujú výsledky predchádzajúcich dvoch etáp. Rozdiel medzi požadovanou úrovňou bezpečnosti (výsledok analýzy hodnôt) a momentálnou reálnou úrovňou bezpečnosti (výsledok analýzy zraniteľnosti) je reziduálna úroveň bezpečnosti. Návrhom vhodných protiopatrení v tejto etape sa pracovná skupina projektu snaží minimalizovať reziduálnu úroveň bezpečnosti. Účinnosť jednotlivých protiopatrení sa simuluje na pripravenom modeli systému. Pracovná skupina väčšinou vypracuje niekoľko možných riešení, ktoré potom schvaľuje výbor riadenia projektu. Vybrané riešenie sa realizuje.

4.9.5 Bezpečnostný audit

Po realizácií vybraných protiopatrení nastupuje fáza overenia funkčnosti bezpečnostných mechanizmov systému. Auditori overujú reálnu (nie modelovanú) účinnosť protiopatrení, bezpečnostných systémov, pravidiel a metodík. Bezpečnostný audit je vysoko formalizovaná a dobre dokumentovaná procedúra. Výsledkom auditu je spáva o skutočnej súčastnej úrovni bezpečnosti organizácie.

4.9.6 Dohľad a údržba

Bezpečnostný projekt je nikdy nekončiaca procedúra. Stále nasadzovanie nových technológií, zmeny v organizácií a spôsobe práce sa odrážzjú aj na bezpečnostných charakteristikách systému. Na účinný dohľad nad bezpečnosťou organizácie je nutné na túto funkciu vyčleniť samostatného pracovníka alebo samostatné oddelenie zodpovedné *priamo* len vrcholovému manažmentu organizácie.

5 Syntéza riešení

V predchádzajúcich kapitolách boli popísané hrozby pre privátne siete a niektoré metódy obrany týchto sietí. Niektoré z popísaných metód však neposkytujú dostatočnú ochranu a iné sú zase veľmi nákladné. Táto kapitola sa snaží zhrnúť možnosti na obranu siete a odporučiť riešenia bežných problémov.

Všetky organizácie, ktoré plánujú brať otázku informačej bezpečnosti vážne, by mali otvoriť bezpečnostný projekt tak ako to opisuje kapitola 4.9. Pre úspešný priebeh celého projektu je nutné dôsledne prejsť všetky kroky, aj keď v malej organizácií niektoré z nich budú mať formu prípravy krátkeho neformálneho dokumentu. Dôsledné dodržovanie postupu bezpečnostného projektu minimalizuje možnosť bežných fatálnych chýb (nadhodnotenie alebo podhodnotenie bezpečnostných potrieb). Hlavný dôraz formálnej časti bezpečnostného projektu by mal byť na vytvorení prakticky aplikovateľnej bezpečnostnej politiky. Táto by mala mať formu oficálneho dokumentu schváleného vedením organizácie.

Súčasťou bezpečnostného projektu by mala byť analýza rizík a syntéza riešení s rozpracovaným plánom protiopatrení. Vo veľkej organizácií je bezpečnostný projekt takéhoto rozsahu naozaj jediné prijateľné riešenie na zaručenie dostatočnej bezpečnostnej úrovne. Pre malú organizáciu je však možné definovať všeobecné pravidlá pre budovanie alebo prestavbu informačných systémov a počítačových sietí:

Snažiť sa čo najviac oddeliť verejnú a privátnu časť siete. Systémy poskytujúce verejné služby (napr. verejný WWW server) a komponenty interného informačného systému (napr. vnútorný súborový server) by mali byť umiestnené minimálne na rôznych počítačoch a pokiaľ možno tieto počítače by mali byť na rôznych sieťach. Za zváženie stojí výstavba silnej demilitarizovanej zóny (kapitola 4.3.2).

Používať štandardné a perspektívne technológie. Použitie technológií spľňajúcich otvorené štandardy minimalizuje riziko zlej architektúry technologického základu a poskytuje záruku interoperabilty zariadení viacerých výrobcov. Pri výbere technológií je lepšie vyberať všeobecnejšie technológie (napr. IPsec namiesto SKIP) a technológie podporujúce infraštruktúru (napr. S/MIME namiesto PGP).

Zohľadniť možnosti integrácie. Je výhodnejšie vyberať riešenia, ktoré sa ľahšie integrujú do momentálnej architektúry informačného systému a siete organizácie. Napríklad je výhodnejšie vybrať implementáciu VPN, ktorú podporuje výrobca sieťových zariadení použitých vo vašej sieti (napr. IPsec ak používate smerovače CISCO) alebo používať technológie ktoré môžu navzájom spolupracovať pomocou dobre definovaných štandardov (SSL a S/MIME namiesto SSH a PGP).

Nezabezpečovať zbytočne. Príliš silná ochrana siete má tendenciu stať sa veľmi nepohodlnou. Personál, ktorý je nútený denne používať bezpečnostné prostriedky sa bude snažiť uľahčiť si prácu obchádzaním bezpečnostných mechanizmov. Príliš vysoká úroveň bezpečnosti môže byť rovnako škodlivá ako príliš nizka úroveň.

Po úspešnom uvedení bezpečnostných mechanizmov do praxe sa bezpečnostný projekt nekončí. Naďalej je nutné stále monitorovanie systémov a iniciovanie pravidelného bezpečnostného auditu. Bezpečnostná úroveň organizácie časom samovoľne klesá a preto je nutné jej stále zvyšovanie. V tejto fáze sa výrazne prejavia výhody systémových, štandardných a integrovaných riešení.

6 Záver

Táto práca sa snažila uviesť čitateľa do problematiky informačnej bezpečnosti zameranej hlavne na TCP/IP siete. Nie je to kompletný návod na zabezpečenie siete, skôr prehľad možných rizík prameniacich z pripojenia sa k modernej informačnej diaľnici. Práca dáva prehľad o technológiách a metodikách, ktoré sa bežne používajú pri zabezpečnovaní informačných systémov a počítačových sietí vôbec. Práca bola písaná v dobrej viere pomôcť zorientovať sa v neprehľadnej problematike informačnej bezpečnosti.

Referencia

[1] Bellovin, S.: RFC 1948 Defending Against Sequence Number Attacks,1996.

[2] CERT Advisory CA-98.01, "Smurf" IP Denial-of-Service Attacks.
http://www.cert.org/advisories/CA-98.01.smurf.html

[3] CERT Advisory CA-96.26, "Denial-of-Service Attack via ping".
http://www.cert.org/advisories/CA-96.26.ping.html

[4] CERT Advisory CA-97.28, "IP Denial-of-Service Attacks".
http://www.cert.org/advisories/CA-97.28.Teardrop_Land.html

[5] CERT Advisory CA-96.21, "TCP SYN Flooding and IP Spoofing Attacks".
http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html

[6] Nmap, The Network Mapper, http://www.insecure.org/nmap.

[7] Goldsmith, D. - Schiffman, M. : Firewalking.
http://www.genocide2600.com/~tatooman/unix-audit/firewalk

[8] skupina "Cult of the Dead Cow": Back Orifice Windows Remote Administration Tool.
http://www.cultdeadcow.com/tools/bo.html

[9] Postel, J.: RFC0792 Internet Control Message Protocol, September 1981.

[10] Computer Security Institute: Cyber attacks rise from outside and inside corporations, Marec 1999.
http://www.gocsi.com/prelea990301.htm

[11] Zákon NR SR 100/1996 Z.z. o ochrane štátneho tajomstva, služobného tajomstva, o šifrovej ochrane informacií a o zmene a doplnení Trestného zákona v znení neskorších predpisov

[12] Zákon NR SR 52/1998 Z.z. o ochrane osobných údajov v informačných systémoch

[13] Freier, A. - Karlton, P. - Kocher, P.: The SSL Protocol Version 3.0, Internet draft, November 1996.
http://home.netscape.com/eng/ssl3/draft302.txt

[14] IETF Transport Layer Security working group.
http://www.ietf.org/html.charters/tls-charter.html

[15] Eastlake, D. - Kafman, C.: RFC2065 Domain Name System Security Extensions, Január 1997.

[16] Chapman, Brent D.- Zwick, Elizabeth D.: Building Internet Firewalls; O'Reilly & Associates, 1995.

[17] Secure Computing Corporation: Type Enforcement for Firewalls [WP-102.1], June 1998.

[18] Internet Software Consortium: BIND, Berkeley Internet Name Domain, Marec 1999. http://www.isc.org/bind.html

[19] Sendmail, Mail Transfer Agent.
http://www.sendmail.org/

[20] RSA Laboratories: Answers to Frequently Asked Questions About Today's Cryptography, 1996.

[21] Check Point Software Technologies Ltd.: Redefing Vurtual Private Network, Marec 1998.

[22] Atkinson, R.: RFC1825 Security Architecture of the Internet Protocol, August 1995.

[23] Atkinson, R.: RFC1826 IP Authentication Header, August 1995.

[24] Atkinson, R.: RFC1827 IP Encapsulating Security Payload, August 1995.

[25] Aziz, A. - Peterson, M.: Design and Implementation of SKIP, SUN Microsystems, Jún 1995.

[26] Remsing, Steve: S/KEY One Time Passwords.
http://lhea.gsfc.nasa.gov/~srr/skey_info.html

[27] Bellovin, Steve M.: There Be Dragons, August 1992.

[28] Cisco Systems, NetRanger - Enterprise-scale Network Intrusion Detesction System, Data Sheet, 1998.

[29] Balasubramaniyan, J. S. - Garcia-Fernandes, J. O. - Isacoff, D. - Spafford, E. - Zamboni, D.: An Architecture for Intrusion Detection using Autonomous Agents; COAST Project, Máj 1998.

[30] Khan, C. - Porras, P. A. - Staniford-Chen, S. - Tung, B.: A Common Intrusion Detection Framework, Júl 1998.

[31] Conseil et Formation Systeme: MELISA, metodická príručka, SOFLAB a.s., 1998.