Univerza v Ljubljani

Fakulteta za elektrotehniko

ZAŠČITA OMREŽIJ IN NAPRAV

Podiplomski študij

Porazdeljeni informacijski sistemi in celovitost podatkov

Miha Smolnikar

Miha.Smolnikar@guest.arnes.si

Ljubljana, 30. 5 .2006

Kazalo

Kazalo slik

Kazalo tabel

1. Uvod

2. Protokol IPsec in navidezna zasebna omrežja

Večina znanih protokolov za prenos podatkov v omrežjih IP ima za zagotavljanje zaščite precej omejen manevrski prostor, zato sta se v zadnjem času uveljavili predvsem dve obliki zaščite:

- *lokalne rešitve* v obliki požarnih zidov in
- namenske *aplikacijske rešitve*, ki zagotavljajo varnost le določenim aplikacijam (npr. elektronsko bančništvo).

Protokol IPsec (angl. Internet Protocol Security) je protokol, ki omogoča celovit pristop pri zaščiti prenosa podatkov v omrežjih IP. Poleg zaščite pred napadalci in prisluškovalci omogoča tudi gradnjo navideznih zasebnih omrežij (angl. Virtual Private Network - VPN).

Protokol IPsec se v protokolnem skladu enako kot protokol IP umešča v omrežni sloj. Za aplikacijski sloj je torej popolnoma transparenten, kar pomeni, da je vrsta podatkov ki jih ščitimo poljubna. Pomembno je tudi, da je protokol IPsec del protokola IPv6, zato lahko v prihodnosti pričakujemo njegovo splošno rabo. Ne glede na to, pa lahko brez težav deluje tudi v omrežjih IPv4. IPsec temelji na šifriranju in ovijanju (angl. encapsulation) prometa za namen prenosa preko IP omrežja [8]. Njegov nabor storitev obsega:

- kontrolo dostopa,
- avtentikacijo izvora podatkov,
- zaupnost (šifriranje),
- nepovezavno celovitost in
- delno zaupnost prometnega pretoka.

Deluje lahko v transportnem ali tunelskem načinu delovanja. V slednjem je s tuneliranjem paketov omogočena tudi gradnja navideznih osebnih omrežij. O navideznosti govorimo zato, ker več zasebnih omrežij uporablja isto fizično infrastrukturo, omrežja pa so ločena na omrežnem nivoju. Pri gradnji navideznih zasebnih omrežij, je uporaba protokola IPsec primerna oz. upravičena tudi zaradi hkratne zaščite podatkov. Omenimo morda le še, da IPsec omogoča zaščito tudi zgolj določenega tipa povezave (npr. FTP povezave).

2.1 Delovanje protokola IPsec

Protokol IPsec vsebuje več postopkov in protokolov:

- protokoli varnosti,
- protokoli upravljanja s ključi in
- algoritmi avtentikacije in šifriranja.

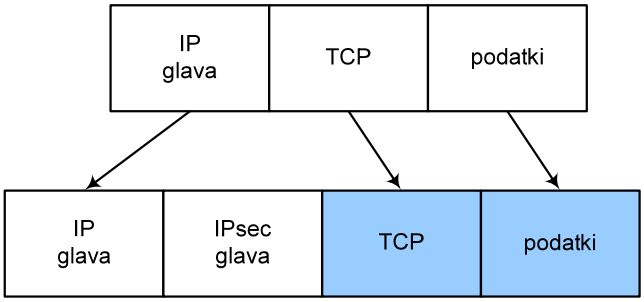
Izbire zadnjih IPsec sam po sebi ne omejuje, kakor tudi ni obvezen protokol upravljanja s ključi. Pri vsaki IPsec zvezi, pa se uporablja vsaj en protokol varnosti;

AH (Authentication Header) in/ali ESP (Encapsulating Security Payload), s čimer s zagotovimo avtentikacijo izvora podatkov in vsebine paketov, ter šifriramo podatke.

Kot že rečeno, sta možna dva načina delovanja, ki ju podrobneje predstavimo v nadaljevanju.

2.1.1 Transportni način delovanja

Transportni način je osnovni način delovanja protokola IPsec. Omogoča zgolj povezave med pari končnih uporabnikov oz. naprav in z njim torej ne moremo povezati dveh omrežij. Uporablja se za zaščito protokolov višjih nivojev, saj se šifrira samo koristna informacija oz. tovor, ne pa glava IP paketa. Transformacijo paketa iz izvornega IP protokola v protokol IPsec prikazuje slika 1.



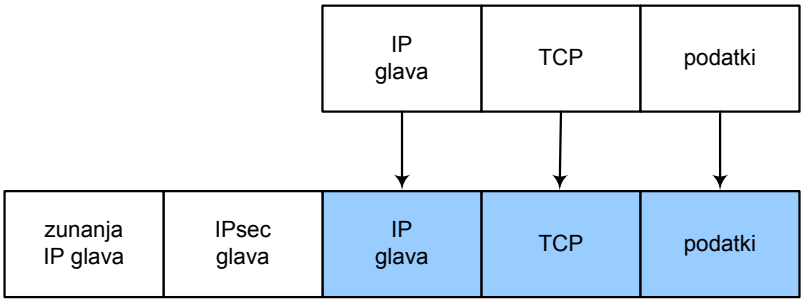
Slika 1:Transformacija IP paketa v transportnem načinu delovanja

IP glava zagotavlja paketu IPsec enake pogoje potovanja po omrežju, kot jih imajo vsi ostali IP paketi. Z modro polja na sliki pa predstavljajo del paketa, ki ga je mogoče šifrirati oz. mu dodati avtentikacijske podatke.

2.1.2 Tunelski način delovanja

Transformacijo IP paketa v tunelskem načinu delovanja prikazuje slika 2. Takoj opazna posebnost je zunanja glava paketa, ki omogoča tuneliranje. Na oddajni strani se celotni izvorni paket, vključno z glavo, naloži v paket IPsec, ki nato po omrežju potuje v skladu z navodili zunanje glave.

Z zunanjo glavo je omogočena uporaba poljubnih naslovov v originalnem paketu, kar je zelo uporabno pri gradnji navideznih zasebnih omrežij. V primeru uporabe učinkovitega šifriranja podatkov tako prisluškovalec lahko vidi le zunanjo glavo in tako lahko sklepa le o začetni in končni točki tunela, ne more pa ugotoviti kdo sta resnični pošiljatelj in prejemnik. Poleg tega je prisluškovalcu skrit tudi TCP paket, na podlagi katerega bi lahko sklepal o vrsti podatkov.



Slika 2: Transformacija IP paketa v tunelskem načinu delovanja

Tunelski način delovanja torej omogoča povezovanje omrežij, povezovanje končnih uporabnikov in kombinacijo obeh možnosti.

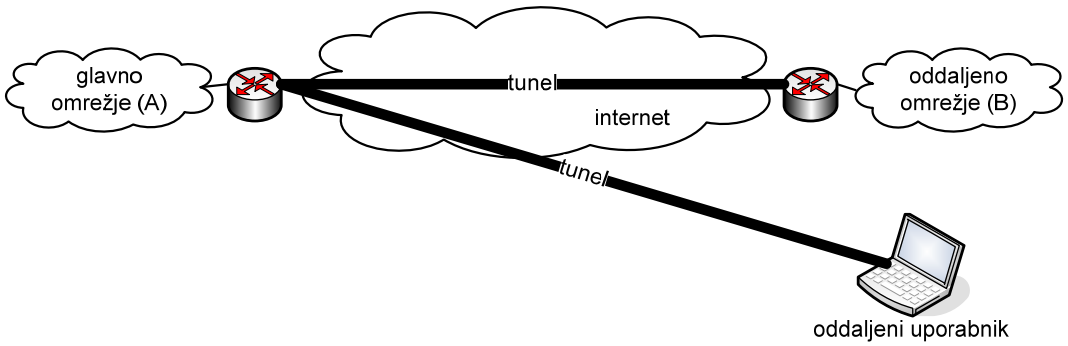
2.2 Navidezna zasebna omrežja

Internet se je razvil v pomembno poslovno orodje, ki omogoča izmenjavo velikih količin podatkov. Sem spadajo tudi podatki kritičnih aplikacij poslovnega procesa, ki so strogo zaupni (npr. finančne transakcije). Zaradi potrebe po zaščiti teh podatkov, ki se prenašajo po javnem omrežju je prišlo do razvoja navideznih zasebnih omrežij. Ta omogočajo, da je omrežje posamezne organizacije z ostalim svetom povezano le toliko, kot je to nujno potrebno.

V omrežjih IP pravimo protokolom, ki omogočajo realizacijo zgoraj opisanih funkcionalnosti, tunelski protokoli. In eden izmed takih je lahko tudi IPsec.

Kot je bilo povedano že pri opisu tunelskega načina delovanja IPsec protokola, lahko s tunelskimi povezavami povežemo več lokalnih omrežij ali končnih uporabnikov. Pri tem mora imeti vsako lokalno omrežje svojo povezavo oz. prehod v Internet, ki mora samo tuneliranje omogočati. Pomembna posledična lastnost takih omrežij je, da imajo lahko vsa sodelujoča omrežja zasebne omrežne naslove, javni naslov pa ima le prehod, ki je povezan v internet.

Primer konkretne izvedbe navideznega privatnega omrežja prikazuje slika 3.



Slika 3: Navidezno zasebno omrežje

Pod narisano shemo si lahko predstavljamo podjetje, ki deluje na dveh lokacijah in do čigar zaupnih podatkov dostopa tudi nek oddaljen uporabnik. Predpostavimo,

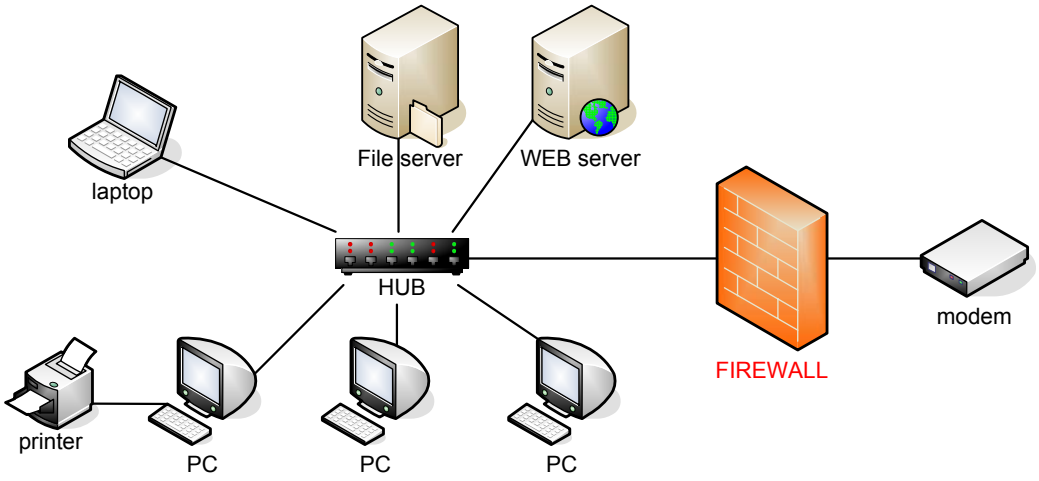
da pri obeh lokalnih omrežjih uporabljamo zasebne naslove in da je A glavno omrežje. V tem primeru lahko omrežje B deluje povsem samostojno, ali pa je podrejeno omrežju A.

Samostojno delovanje omrežja B si predstavljamo tako, da računalniki tega omrežja uporabljajo tunel kadar komunicirajo z računalniki v glavnem omrežju (omrežju A), za komunikacijo z drugimi računalniki v Internetu pa izkoriščajo usmerjevalnik, ki mora v tem primeru podpirati funkcijo prevajanja naslovov (angl. Network Address Translation - NAT). V podrejenem načinu delovanja omrežja B računalniki tega omrežja uporabljajo tunel vedno, kadar komunicirajo z računalnikom, ki ni del samega lokalnega omrežja. V tem primeru usmerjevalnik za vstop v omrežje B deluje tudi kot požarni zid, saj prepušča le pakete, ki pridejo skozi tunel.

S stališča varnosti je očitno boljše podrejeno delovanje, se pa na ta način poveča promet skozi javno omrežje in obremenitev prehoda v glavno omrežje.

3. Požarni zid

Poleg uporabe protivirusnih programov, je najpogosteje uporabljena zaščita pred vdori v računalnik uporabljen požarni zid oz. pregrada (angl. firewall). Z njimi skušamo nepooblaščenim preprečiti dostop do računalnika. Za zaščito enega samega računalnika ponavadi uporabljamo požarni zid, ki ga dobimo že skupaj z operacijskim sistemom ali pa uporabimo katerega od za to namenjenih programov. Če želimo zaščititi celotno lokalno računalniško omrežje, je priporočljivo namestiti požarni zid v obliki posebne strojne opreme, nameščene med lokalno omrežje in svetovni splet. Še več, v nekaterih močno zavarovanih sistemih lahko ločimo več nivojev požarnih zidov, ki razdelijo lokalno omrežje na bolj in manj zavarovane predele. Strežniki, skozi katere kako podjetje komunicira s svetom, so tako postavljeni v nekoliko manj zaščiteno območje, kjer je na volj lažja komunikacija s spletom, vendar pa je zaščita pred vdori le delna. Strežniki, na katerih se zbirajo zaupni podatki, ki imajo za podjetje visoko vrednost, pa so postavljeni v zaščiteno območje omrežja, do katerega je dostop mogoč le iz izbranih in močno zavarovanih računalnikov. Omenimo še, da požarni zidovi v večini primerov delujejo dvosmerno. To pomeni, da ne le varujejo notranjega omrežja pred vdori od zunaj, temveč da omogočajo tudi omejevanje omrežnega prometa navzven, iz notranjega omrežja v zunanje.



Slika 4: Značilna postavitev požarnega zidu med lokalno omrežje in svetovni splet

3.1 Izvor izraza 'požarni zid'

Večje stavbe poznajo požarne pregrade, ki ob ognjeni stihiji nepredušno ločijo posamezne prostore in s tem zmanjšajo nevarnost, da bi ogenj uničil celotno poslopje in s tem ogrozil vse, ki so v stavbi. Ta gradbena prvina je postala navdih za računalniški sistem, ki podobno kakor požarna pregrada stavbo ločuje na dva dela, ločuje dva dela omrežja. Izraz sistem smo uporabili zato, ker za požarne sisteme velja, da so lahko izdelani kot strojna ali programska oprema, oziroma

najpogosteje kot kombinacija obojega. V zadnjem času vse bolj priljubljena vrsta požarnih zidov so t.i. osebni požarni zidovi (angl. personal firewall). Kot lahko sklepamo že iz imena ti varujejo posamezen računalnik proti zunanjemu omrežju, ki je lahko bodisi krajevno ali prostrano.

3.2 Protokoli

Preden si ogledamo, kako požarni zidovi delujejo, se moramo v grobem seznaniti z naravo delovanja omrežja. Računalniki, povezani v omrežje, si med seboj izmenjujejo podatke. Da je to mogoče, se morajo med seboj poznati. Način prepoznavanja naprav v omrežju, ugotavljanja njihovih naslovov in samo izmenjavo podatkov določajo protokoli. To so pravila, ki v celoti določajo način izmenjave podatkov med napravami v omrežju. Skupine protokolov določajo vrsto omrežja. Danes je v računalniških omrežjih daleč najpogostejši sklad protokolov TCP/IP, na katerem temelji tudi delovanje interneta. Čeprav so bila omrežja TCP/IP zasnovana za vojaške potrebe, za komunikacije po teh omrežjih še zdaleč ne moremo trditi, da so varne. V veliki večini temeljnih protokolov, ki se uporabljajo v omrežju, je pojem varnosti zelo površno zastopan. To je posledica dolge zgodovine, saj je bil internet, kakršnega ga poznamo in uporabljamo, zasnovan že pred desetletji. Njegovi tvorci pa so se takrat ukvarjali predvsem z robustnostjo, saj je omrežje moralo delovati tudi, ko bi bili lahko številni deli omrežja poškodovani. Taka zasnova je tudi omogočila neverjetno širitev in današnjo prevlado interneta, saj so protokoli brez posebnih težav prenesli tisočkrat in tisočkrat večje obremenitve. S širitvijo interneta pa so seveda nastale tudi potrebe po večji varnosti. Razvitih je bilo kar nekaj protokolov (npr. IPsec), ki omogočajo večjo stopnjo varnosti, vendar pa se ti bodisi še niso uveljavili, bodisi niso prešli v množično uporabo. V času tega prehodnega obdobja bomo torej za zagotovitev varnosti še morali posegati po uporabi požarnih zidov.

Naprave, ki so del omrežja TCP/IP, imajo vsaka svoj naslov. Določen je z enolično t.i. IP številko (ang. IP number). Navadno jo zapišemo s kvartetom osembitnih števil, ločenih s piko (npr. 194.249.231.85). Pogosteje od njih sicer uporabljamo njihova pripadajoča simbolična oz. domenska imena, kot je npr. *www.ijs.si*, vendar se moramo zavedati, da je to le zato ker si taka imena ljudje mnogo lažje zapomnimo, računalniki pa le te prevedejo nazaj v številko IP s pomočjo posebnega protokola DNS. Kot vemo, lahko v omrežje povezan računalnik počne več stvari. Tipičen scenarij uporabe je, da medtem ko brskamo po spletu, prejemamo in pošiljamo tudi elektronska sporočila, v ozadju pa najverjetneje ves čas izmenjujemo datoteke. Številka IP tako ne zadošča, da bi v celoti določili povezavo med dvema napravama v omrežju. Pomemben del naslova je še številka vrat (ang. port number). Ta se lahko giblje v meji od 1 do 65535. Povezavo med dvema napravama tako v celoti določa kombinacija dveh številk IP in dveh številk vrat na vsaki strani. Simbolično lahko povezavo zapišemo takole s številkama IP, ki jima za dvopičjem sledi še številka vrat:

198.16.35.14:1572 ↔ 195.96.196.249:80

Številke vrat ponavadi delimo na dobro znana vrata (ang. well-known port numbers), ki so praviloma na območju 1-1023 in začasna vrata, ki obsegajo preostalo območje. Dobro znana vrata olajšajo vzpostavitev povezave, saj pripadajo posameznemu protokolu. Za spletne strani, ki jih prenaša protokol

HTTP, so tako predpostavljena dobro znana vrata, oštevilčena s številom 80. Za prenos datotek s protokolom FTP se uporabljajo vrata 21, elektronska sporočila s protokolom SMTP pošiljamo prek vrat 25, sprejemamo pa jih v primeru protokola POP3 prek vrat 110. Seveda pa opisana vrata s protokolom niso dokončno predpisana. Spletni strežnik npr. lahko posluša nove povezave na katerihkoli prostih vratih. Kot smo videli iz zgornjega zgleda, oznaka vrat na obeh straneh povezave ni nujno ista. Velja, da na dobro znanih vratih poslušajo le strežniki, medtem ko se odjemalci z njimi povezujejo prek začasnih vrat. To nam omogoča, da se npr. povežemo z več spletnimi strežniki hkrati. Še več, strežniki na dobro znanih vratih le poslušajo nove povezave. Ko odjemalca sprejmejo, se dogovorita za začasna vrata, na katera preklopi strežnik, tako da lahko na dobro znanih vratih posluša še naprej. Ta postopek nam omogoča tudi, da se z istim strežnikom povežemo večkrat. Na primer pri ogledu neke spletne strani, nam spletni brskalniki hkrati ob prenosu besedila z istega strežnika prenašajo tudi slike.

Zaključimo lahko, da nam oznaka vrat tako ne pove dosti o samem protokolu, ki poteka na posamezni povezavi. Da bi posamezno povezavo lahko spoznali in razumeli, kaj se na njej pravzaprav dogaja, moramo poznati še vrsto protokola, ki se na njej uporablja. Protokole, ki se uporabljajo v omrežju, razvrščamo v sloje (angl. layers). Sloj podrobneje opredeli vlogo protokola in sega od fizične (nosilec za prenos informacije) do aplikativne ravni (storitve omrežja).

3.3 Vrste požarnih zidov

Glede na sloj protokola, kjer požarni zid opravlja svoje delo, jih navadno delimo na naslednje tri vrste:

1. paketni filtrer (angl. packet filter),
2. nadomestni strežnik (ang. proxy server ali application-level gateway),
3. vmesni strežnik (angl. circuit-level gateway),
4. analiza stanja (ang. stateful inspection)

Poudarimo, da posameznega sodobnega požarnega zidu ni mogoče preprosto uvrstiti v eno izmed naštetih kategorij, saj praviloma uporablja kombinacijo večih pristopov. Opišimo v nadaljevanju posamezne vrste požarnih zidov.

3.3.1 Paketni filter

Paketni filtri so učinkovita zaščita, ki deluje na povezovalnem sloju. Ker so podatki, ki se izmenjujejo v omrežju, različnih dolžin, protokoli uporabljajo pakete, ki jih drugega za drugim izmenjujejo, dokler vsebina ni prenesena v celoti. Posamezen paket ne vsebuje le koščka podatka, temveč tudi podatke o svojem izvoru in cilju. Paket je nekakšna ovojnica, ki podatek obda z oznako protokola, parom številk IP in vrat pošiljatelja ter parom številk IP in vrat prejemnika. Paketni filtri izkoriščajo podatke v ovojnici paketa in se na njihovi podlagi odločajo, ali bodo določen paket prepustili, zavrnili ali zavrgli. Delovanje paketnega filtra je v marsičem podobno delovanju usmerjevalnika (angl. router).

Učinkovitost paketnega filtra je odvisna od pravil, ki mu jih moramo predpisati, preden lahko opravlja svoje delo. Pravila so seznam preizkusov, ki jih mora vsak posamezen paket prestati, preden se odloči o njegovi usodi. S stališča varnosti je veliko bolje, če izhajamo iz temeljnega pravila, ki vse pakete zavrne, potem pa le tega nadgrajujemo z natančnimi pravili posameznih dovoljenj, ki promet od zunaj prek določenih vrat prepuščajo v le enega izmed računalnikov v krajevnem omrežju. Tak pristop se izkaže za mnogo efektivnejšega, kot pa če izhajamo iz situacije v kateri moramo razmišljati o vseh prepovedih. Princip je uporaben tudi v nasprotni smeri komunikacije, kjer uporabnikom znotraj krajevnega omrežja dovolimo povezavo v splet le prek s pravili določenih vrat.

Za zgled si poglejmo sledeč primer pravil. Zunanjemu svetu pri dostopu do našega lokalnega omrežja dovolimo le dostop do spletnega strežnika (številka IP 192.168.0.5) in strežnika FTP (192.168.0.2), uporabnikom znotraj naše lokalne mreže pa omogočimo dostop do zunanjega strežnika e-pošte (215.16.33.15) in vseh spletnih strežnikov:

Zunanje omrežje → Notranje omrežje

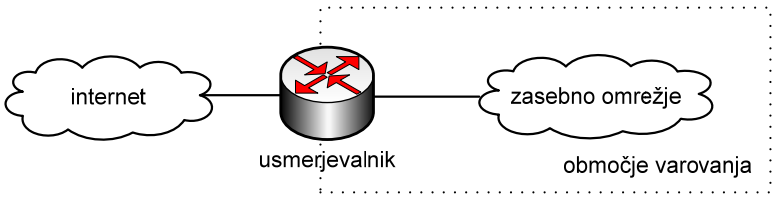
Zunanje omrežje		Notranje omrežje		Politika
IP	Vrata	IP	Vrata	
..*.*	*	192.168.0.5	80	DOVOLI
..*.*	*	192.168.0.2	21	DOVOLI
..*.*	*	*.*.*.*	*	ZAVRNI

Notranje omrežje → Zunanje omrežje

Notranje omrežje		Zunanje omrežje		Politika
IP	Vrata	IP	Vrata	
..*.*	*	215.16.33.15	25	DOVOLI
..*.*	*	215.16.33.15	110	DOVOLI
..*.*	*	*.*.*.*	80	DOVOLI
..*.*	*	*.*.*.*	*	ZAVRNI

Paketni filter bo po vrsti, od zgoraj navzdol, preverjal seznam pravil, dokler za posamezni paket ni popolnoma prepričan, kam sodi. Če mu ne ustreza nobeno od pravil, pristane pri temeljnem pravilu, ki zavrača vse.

Pravila lahko določajo, da se posamezen razred paketov prepusti, v nasprotnem primeru pa ga požarni zid lahko tiho ali glasno zavrne. V slednjem primeru pošlje obvestilo o izvoru zavrnjenega paketa. Vidimo, da so paketni filtri popolnoma odvisni od pravil, ki določajo varnostno politiko. Taki požarni zidovi delujejo hitro in so za uporabnike, katerih paketi so skladni s pravili, neopazni. Paketni filtri so zato pogost že kar del operacijskega sistema. Osnovni princip delovanja prikazuje slika 5.



Slika 5: Paketni filter

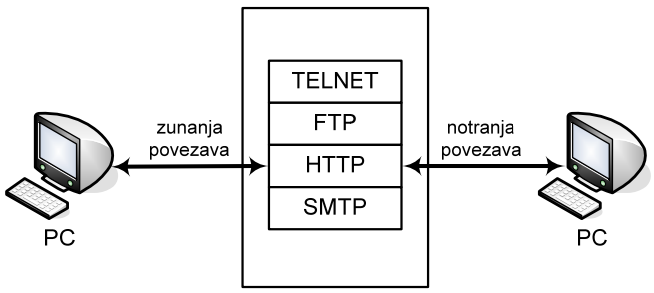
Žal imajo paketni filtri veliko pomanjkljivost. Vsebino paketa je namreč mogoče popačiti. Napadalec lahko prikrije svoj izvor tako, da spremeni svojo številko IP z drugo, za katero je ugotovil, da je v tabeli pravil dovoljena. Tak napad, imenovan tudi IP spoofing, je razlog, da se paketni filtri v učinkovitem požarnem zidu nadgradijo z dodatnimi omejitvami.

3.3.2 Nadomestni strežnik

Da bi lahko presegli omejitve paketnega filtra, se moramo pomakniti više po slojih omrežnih protokolov. Nadomestni strežnik ne preučuje prometa le na sloju posameznih paketov, temveč sledi njihovemu zaporedju. Deluje na aplikacijskem sloju, saj se zaveda podrobnosti protokola, torej upošteva tudi zaporedje paketov. Osnovno delovanje ponazarja slika 6.

Vsaka povezava ima fazo vzpostavitve. V tej fazi se izmenjujejo paketi, ki so še posebej označeni. Požarni zid, kot vedno, stoji med obema deloma povezave. V trenutku, ko prispe zahteva za vzpostavitev povezave, prevzame vlogo druge strani in se postavi v vlogo nadomestnega poslušalca. Če ugotovi, da je bilo z zaporedjem paketov vse v redu, sklene povezavo med obema stranema. Požarni zid vodi tabelo pravilno vzpostavljenih povezav ves čas njihovega trajanja.

Zaradi učinkovitosti lahko požarni zid po uspešni vzpostavitvi povezave opusti preverjanje protokola in slepo posreduje pakete med obema stranema. Delovanje je sicer hitrejše, a tak pristop spet ogroža varnost, saj lahko napadalec izkoristi tako vzpostavljeno povezavo in vanjo naknadno vriva zlonamerne pakete, ki lahko izkoriščajo razpoke v sistemu varnosti. Pogostejši pristop, ki omogoča večjo varnost, je stalno spremljanje paketov. Ker požarni zid pozna tudi protokol, ki se uporablja na posamezni povezavi, lahko brez težav zazna naknadno vrinjene nepravilne pakete.



Slika 6: Nadomestni strežnik

Nadomestni strežnik opravlja še eno storitev, ki znatno izboljša varnost krajevnega omrežja. Ker tak požarni zid vzpostavlja povezave v imenu drugih naprav, so vsi računalniki v notranjem omrežju navzven nevidni. Zunaj jih namreč predstavlja požarni zid s svojim zunanjim naslovom IP. Požarni zid seveda vodi seznam vzpostavljenih povezav in lahko na podlagi številke vrat ugotovi, kateremu računalniku na notranji strani je paket v resnici namenjen. Tej storitvi pravimo tudi prevajanje naslovov (angl. Network Address Translation - NAT).

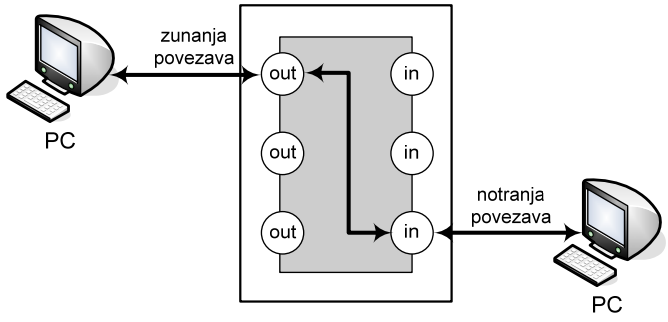
Pravila, ki jih uveljavlja prehod uporabe, so lahko tu precej podrobnejša kakor pri paketnem filtru. Ker ima vsak protokol na višjem sloju specifične ukaze, lahko prehod uporabe prilagodimo tako, da prepušča le določene. Še več, pri naprednejših požarnih zidovih lahko taka pravila uveljavljamo izbirno, le za določene skupine uporabnikov.

Glede na namen je zato pri nekaterih prehodih uporabe potrebna prijava uporabnika. Požarni zid s tem ni več neviden za uporabnika, ki se mora najprej ustrezno predstaviti z uporabniškim imenom in geslom.

Nadomestni strežniki morajo poznati podrobnosti protokola in opravljati vse delo v imenu zaščitene naprave. To lahko podaljša čas obdelave in omeji uporabnost omrežja, če nadomestni strežnik katerega od zanimivih protokolov ne pozna. Po drugi strani pa ima nadomestni strežnik lahko tudi možnost medpomnjenja, saj lahko za določen čas shrani posamezne vsebine in jih naknadnim odjemalcem posreduje brez povezovanja z zunanjim virom.

3.3.3 Vmesni strežnik

Ta vrsta požarnega zidu deluje na transportnem sloju z vzpostavljanjem dveh TCP povezav za posredovanje prometa med pošiljateljem in prejemnikom. Pri njuni komunikaciji se nato na paketni ravni vrši odločitev o tem kateremu paketu bo prehod preko zidu bodisi dovoljen, bodisi zavrnjen. Delovanje ponazarja slika 7.



Slika 7: Vmesni strežnik

Slabost takega požarnega zidu je, da so primerni samo za TCP vrsto povezav, saj UDP komunikacije niso povezavno orientirane.

3.3.4 Analiza stanja

Nadomestni strežniki ponujajo učinkovito zaščito, a jih je v nekaterih primerih nekoliko nerodno uporabljati. Nadalje nekateri menijo, da pravo varnost lahko zagotavlja le vmesni strežnik, ki dejansko posreduje pakete med dvema paroma povezav, vendar pa to v omrežni promet včasih vnaša nepotrebno zapletenost, sam proces pa je lahko uporabniku preveč opazen.

Zgornje slabosti poskuša odpraviti požarni zidovi, ki opravljajo analizo stanja prometa. Ti še vedno opravljajo vse predstavljene vloge zaščite, a hkrati ohranjajo neposredno povezavo med zunanjim in notranjim omrežjem. Podobno kakor nadomestni strežniki opravljajo preverjanje pravilne vzpostavitve povezave in prevajanje naslovov omogočajo tudi zavračanje specifičnih ukazov posameznih protokolov. Od njih pa jih ločuje analiza podrobnosti posameznega protokola. Namesto na dejanske protokole se analiza stanja zanaša na posebne algoritme, ki spremljajo vzorce bitov v paketih. S tem so lahko požarni zidovi z analizo stanja teoretično veliko bolj učinkoviti pri odkrivanju zlonamernih paketov, poleg tega pa jih ni treba prilagajati vsakemu posameznemu protokolu in so uporabnikom nevidni.

3.4 Izvedbe požarnih zidov

Postopki preverjanj, ki jih izvajajo požarni zidovi, se lahko izvajajo v programski kodi ali strojni opremi (slika 8). Slednja ponuja večje udobje, saj je po prilagoditvi pravil tak požarni zid popolnoma avtonomen in vedno na voljo. Ker je zgrajena z namenskimi vezji, svoje delo opravlja zelo učinkovito. Nekoliko težje je nadgrajevati njene zmogljivosti, saj smo vezani na enega ponudnika in njegovo podporo. Na drugi strani imamo sodobno programsko opremo, ki opravlja enakovredne naloge, in včasih omogoča še večjo stopnjo zaščite, saj lahko postopke preverjanja dopolnimo še z drugimi (npr. protivirusnimi) programi. Paziti moramo le na zmogljivosti računalnika, v katerem je tako programje nameščeno. Večji omrežni promet in zahtevna preverjanja lahko upočasnijo še tako zmogljiv računalnik.

Slika 8: Strojna izvedba požarnega zidu (levo), uporabniški vmesnik programskega požarnega zidu (desno)

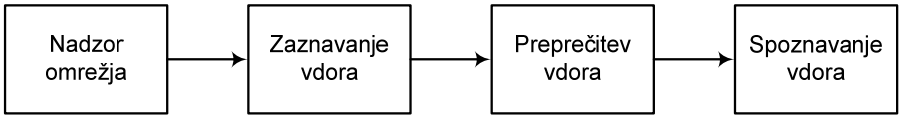
Posebna vrsta so osebni požarni zidovi, ki jih pogosto uporabljamo za zaščito enega samega računalnika. Pri teh je treba paziti, da so dvosmerni, da nas torej ne varujejo le pred vdori iz zunanjega omrežja, temveč preprečujejo tudi delovanje vohunske programske opreme in črvov, ki lahko zlorabijo naš računalnik za posredovanje zasebnih podatkov ali razpošiljanje nezaželene e-pošte navzven. Paziti je treba tudi na zahtevnost filtrov, saj nekateri osebni zidovi omogočajo podrobno analizo stanja, ki lahko uporabnika upočasni celo pod mejo uporabnosti.

Danes so cene osebnih usmerjevalnikov za širokopasovna omrežja, ki obsegajo strojni požarni zid, že tako nizke, da se jih splača omisliti si, čeprav smo (zaenkrat) v omrežje povezani le z enim računalnikom. Visoka stopnja varnosti je praviloma zagotovljena že brez posebnega prilagajanja. Po potrebi pa jih lahko podrobno prilagodimo. Večina v ta namen ponuja lasten spletni strežnik, skozi katerega preprosto spreminjamo pravila zaščite. Če imamo v domačem omrežju več računalnikov, pa je nakup tega strojnega dodatka še bolj upravičen. Navadno v isti napravi dobimo poleg usmerjevalnika in požarnega zidu še strežnik DHCP za preprosto dodajanje novih naprav, možnost samodejne prijave spremenljivega naslova IP v dinamične strežnike DNS in prehod za vzpostavitev navideznih zasebnih omrežij (angl. Virtual Private Networks - VPN).

4. Sistemi za zaznavanje in preprečevanje vdorov

Sistemi za zaznavanje in preprečevanje vdorov (angl. intrusion detection/protection systems) so sistemi, ki zaradi svojega načina delovanja omogočajo implementacijo visokega nivoja varnosti v omrežju.

Vsebino teh sistemov bomo predstavili preko opisa delovanja. Osnovna filozofija delovanja sistemov sloni na verigi prikazani na sliki 9.



Slika 9: Osnovni koraki v delovanja sistemov za zaznavanje in preprečevanje vdorov

Začnemo torej z nadzorom omrežja oz. prometa, ki se po njem prenaša. Ko na osnovi pregledovanja prometa zaznamo nekaj kar bi lahko bil vdor, na osnovi definirane politike ustrezno reagiramo. Reakcije so lahko preprečitev prometa, beleženje dogodka, alarmiranje skrbniku itd. Na koncu se v koraku spoznavanja vdora želimo iz preteklega dogodka nekaj naučiti in s tem dodatno definirati politiko ukrepanja za nadaljnje poskuse napadov.

4.1 Zaznavanje vdorov

Kot že rečeno, kadar želimo zaznati poskuse vdorov moramo opazovati omrežni promet. Za to pa jasno potrebujemo dostop do omrežja, iz česar posledično sledi, da lahko sistem za zaznavanje vdorov nadzira le tisti del omrežja, kjer se tudi sam nahaja. Nadalje lahko pri procesu pregledovanja ločimo sisteme na take, ki promet zgolj spremljajo (mu prisluškujejo) in na take, skozi katere promet tudi dejansko poteka.

V želji, da bi dosegli čim višji nivo sposobnosti odkrivanja vdorov, se poslužujemo različnih tehnik zaznavanja napadov. Vedno pa lahko potencialne napade ločimo v dve skupini:

- Pri poskusu vdoru je uporabljen *znan način napada* na neko *znano varnostno pomanjkljivost določene aplikacije*, ki je še nismo ustrezno zavarovali.
- Pri poskusu vdora je uporabljena popolnoma *nova tehnika napada*, na bodisi znano ali neznano varnostno pomanjkljivost določene aplikacije.

Predstavimo ju podrobneje v nadaljevanju.

4.1.1 Zaznavanje znanih napadov

Napade, ki pri poskusih vdora uporabljajo znane tehnike, je s sistemi za zaznavanje vdorov relativno preprosti odkriti. Vse kar pri tem potrebujemo je le baza znanih vdorov. Vsak znan poskus napada uporablja določeno zaporedje paketov oz. vsebin v paketih in vse kar moramo narediti je, da celoten promet pregledujemo in če v prometu najdemo iskana zaporedja paketov s predpisano vsebino, ustrezno ukrepamo. Uporabljen je torej podoben princip, kot ga uporabljajo protivirusni sistemi, ki jih opisujemo v poglavju 5.

Problem pri takšnem načinu delovanja je velika možnost lažnih alarmov. Natančneje, pri napadih, ki so v bazi napadov natančno specificirani ni problemov, saj ob odkritju iskanega zaporedja paketov oz. ukazov gotovo odkrili poskus vdora oz zlorabe omrežja. Problematična pa so tista zaporedja paketov oz. ukazov, ki so enaka tistim , ki jih specifikacije ne določajo zelo specifično. Odkritje takih sekvenc nam predstavlja le potencialne poskuse napada.

Če si za primer ogledamo primer znanega virusnega napada 'I LOVE YOU' iz leta 2000, pri katerem je najbolj pomembno, da preprečimo možnost širjenja okužbe, lahko ugotovimo sledeče. Okužba se širi preko elektronske pošte s sporočilom, ki na določenem mestu vsebuje to besedno zvezo. Če bi na primer v okviru prenašanega prometa iskali zgolj to besedno zvezo, bi lahko sprožili veliko število lažnih napadov. Pomembno je torej, da v zaporedju paketov ali ukazov ne iščemo le določene besedne zveze, temveč tudi da vemo v katerih delih posameznih paketov kaj iščemo. Za izbran primer se moramo omejiti na iskanje besedne zveze zgolj v imenih k sporočilu pripetih datotek. S tem količino lažnih alarmov močno znižamo.

Pri odkrivanju znanih napadov smo torej omejeni na obstoječo uporabljano bazo napadov. Za maksimalno izkoristek tega načina odkrivanja napadov je zato pomembno sprotno obnavljanje oz. osveževanje baze.

4.1.2 Zaznavanje neznanih napadov

Zgoraj opisani način odkrivanja znanih napadov je sicer učinkovit, vendar pa v sodobnih sistemih za zaznavanje vdorov žal ni zadosten. Želimo si namreč zaznati tudi še neznane poskuse vdorov.

Pri tem si lahko pomagamo s standardi in protokoli, ki se uporabljajo v okviru IP protokola. Napadi namreč v veliko primerih bazirajo prav na zlorabi teh protokolov. Recimo, da izbran protokol v danem trenutku predvideva določen podatek (npr. glede na njegovo obliko ali velikost), mi pa mu posredujemo nekaj drugega. Če aplikacija v takem primeru nima ustreznih mehanizmov, ki to takoj ugotovili napačnost rabe protokola, se lahko zgodi da aplikacija preneha delovati tako kot je bila napisana in na osnovi našega nepričakovanega posega izvaja neke druge akcije. Tipičen primer takšnega načina napada je t.i. Buffer-overflow. Pri njem aplikaciji posredujemo več podatkov, kot jih pričakuje in tipično se višek teh podatkov nenadzorovano zapiše v spomin aplikacije. Če ta presežek podatkov spretno oblikujemo, lahko nepooblaščeno dosežemo, da aplikacija izvaja nekaj povsem drugega, kot je bilo mišljeno.

Z nadzorom in pregledovanjem prometa moramo torej zagotoviti, da se aplikacije in servisi uporabljajo tako kot je predpisano. Če temu ni tako, lahko zaznamo potencialne znake napada tudi če nam le ta ni znan vnaprej.

Jasno je tudi v teh primerih možnost za proženje lažnega alarma velika, vendar pa vseeno manjša ko v prejšnjem primeru. Proženje alarma na osnovi teh sistemov zaznavanja je namreč pogosto koristno tudi če ne gre za poskus vdora, ampak je neka aplikacija npr. le uporabljena drugače kot je bilo mišljeno.

Do sedaj opisani sistemi za preprečevanje napadov so sicer učinkoviti, še vedno pa imajo eno slabo lastnost. Praviloma namreč delujejo le v okviru znanih aplikacij oz. standardov. Problem se torej pojavi, kadar želimo v omrežju uporabiti neko lastno aplikacijo, ki smo jo npr. sami razvili. Sistem nam zanjo ne more ponuditi nabora znanih napadov, in prav tako ne more sklepati na anomalije uporabe standardov in protokolov. Sklenemo torej lahko, da morajo sistemi za zaznavanje napadov ponujati mehanizme, kjer lahko sami definiramo parametre, ki okarakterizirajo potencialne načine napadov na aplikacijo.

4.2 Preprečitev vdora

Jasno je, da nam sistem, ki napad le prepozna, ni pa ga sposoben preprečiti ne more biti v prav veliko pomoč. Tako imamo tudi pri tehnikah preprečitve napadov, v odvisnosti od njihove vrste, več načinov.

Glede na različne možnosti postavitve, lahko govorimo o dveh možnih načinih preprečevanja vdorov:

- **Pasivni način**, zgolj spremlja promet v omrežju. Sam promet se torej ne prenaša prek sistema za zaznavanje in preprečevanje vdorov.
- **Aktivni način**, pri njem gre celoten promet dejansko prek sistema za zaznavanje in preprečevanje vdorov.

Pasivni način lahko še nadalje delimo na dve podkategoriji, vendar pa več o tem v nadaljevanju, kjer vsakega od načinov podrobno predstavimo.

4.2.1 Spreminjanje politike (pasivno spremljanje prometa)

Najenostavnejši način preprečevanja napadov je preko samodejne prekonfiguracije preostalih varnostnih mehanizmov.

Kot že rečeno, sisteme za zaznavanje vdorov uporabljamo zato, ker ostali sistemi ne spremljajo ustrezno prometa na aplikativnem nivoju. Če torej nek sistem uporabljamo lahko predpostavimo prisotnost rizičnega prometa. Tipično torej uporabljamo nek drug varnostni sistem (npr. požarni zid), kjer promet za določeno aplikacijo prepuščamo, sistem za zaznavanje vdorov pa vsebinsko nadzira promet v okviru te aplikacije.

V primeru, da sistem zazna napad oz. poskus vdora, lahko v primeru ustrezne konfiguracije sistema in pa drugih varnostnih mehanizmov (npr. požarnega zidu) ,

izvedemo samodejno prijavo na ta varnostni sistem in prekonfiguriramo filtrirne sisteme tako, da promet za aplikacijo, ki je napadena ni več mogoč.

Ideja je v osnovi preprosta, za učinkovito rabo pa je potrebno zagotoviti sledeče:

- Uporabljati moramo sistem za zaznavanje vdorov in požarni zid, ki takšno delovanje omogočata
- Varnostno politiko moramo sestaviti pazljivo, saj lahko s takšnim načinom dela zelo hitro omogočimo t.i. denial-of-service napad, pri katerem lahko nekdo drug na relativno lahek način doseže nedostopnost našega informacijskega sistema.

4.2.2 TCP reset (pasivno spremljanje prometa)

V primeru TCP prometa lahko uporabimo lastnost zaključevanja sej. TCP promet je namreč t.i. smerni promet, kjer se paketi med dvema mrežnima elementoma ne prenašajo vsak zase, ampak so vsi del ustrezne TCP seje. To pomen, da recimo uporabnik prične s komunikacijo, TCP sejo. Strežnik mu na to komunikacijo odgovarja in svoje odgovore posreduje v okviru iste TCP seje. Eden izmed parametrov na podlagi katerega se ta seja je zaporedna številka (angl. sequence number). Vsakič, ko v okviru določene TCP seje posredujemo sogovorniku paket, povemo kakšno zaporedno številko pričakujemo v odgovoru in paket, ki ta odgovor predstavlja mora seveda podatek o tej številki vsebovati. TCP seja na koncu zaključi tako, da uporabnik ali strežnik komunikacijo zaključita s t.i. TCP-reset paketom.

Sistem za zaznavanje vdorov lahko tako v določenih primerih zaustavi sporno komunikacijo. Če recimo uporabnik prične uprabljato neko aplikacijo, ki za komunikacijo uporablja TCP protokol in to počne na način, ki za sistem za zaznavanje vdorov predstavlja napad, lahko sistem strežniku posreduje 'lažen' TCP-reset paket in ga tako prepriča, da je seja zaključena.

Ideja zveni enostavna, mnogo manj enostavna pa je njena implementacija. Sistem za zaznavanje napadov mora biti namreč dovolj spreten, da pravočasno zazna napad, ugotovi ustrezne zaporedne številke in potem tem številkam ustrezno posreduje strežniku TCP-reset paket. Sistem ne deluje v primerih, ko:

- se napad izvede in zaključi še preden sistem reagira, ali ko
- zaradi napačne zaporedne številke strežnik ignorira posredovani TCP-reset paket in
- jasno takrat, ko komunikacija ne temelji na TCP protokolu.

4.2.3 Zavračanje prometa (aktivno spremljanje prometa)

Sistem za zaznavanje vdorov lahko postavimo tudi tako, da se celoten promet prenaša preko njega. V tem primeru je preprečevanje vdorov preprostejše, saj mora sistem v danem trenutku zgolj zavreči ustrezen paket in torej za to ne potrebuje samega strežnika ali požarnega zidu, kot v zgornjih dveh primerih.

S stališča uspešnosti preprečevanja napadov je takšna tehnika uporabe sistema še najbolj učinkovita.

5. Zlonamerni programi

Zlonamerni programi (angl. malicious software, malware), so programi napisan z namenom škoditi uporabniku oziroma škodljivo vplivati na delovanje nekega informacijskega sistema.

Terminologija na tem področju je problematična, saj lahko opazimo pomanjkanje splošno sprejetih izrazov in tudi dejstvo, da se mnoge od obravnavanih kategorij med seboj prekrivajo. Nekaj osnovnih in bolj uveljavljenih terminov, skupaj s pripadajočimi razlagami, podaja tabela 1.

Ime	Opis
Virus	Zlonamerni program s sposobnostjo samorazmnoževanja.
Črv (angl. Worm)	Zlonamerni program, ki se razširja v računalniških omrežjih in se pri tem samodejno razmnožuje.
Časovna bomba (angl. Time bomb)	Zlonamerni program, ki se sproži ob določenem času.
Logična bomba (angl. Logic bomb)	Zlonamerni program, ki se sproži ob določenem dogodku.
Trojanski konj (angl. Trojan horse)	Zlonamerni program z navidezno koristno funkcijo, npr. kot arhivski program, igra, protivirusni program.
Stranska vrata (angl. Backdoor, Trapdoor)	Nedokumentiran, skriven način dostopa do programa, običajno izdelan za potrebe vzdrževalcev programov.
angl. Downloader	Program, ki namesti nove programe na napaden terminal.
angl. Spammer program	Program, ki samodejno razpošilja neželeno/nadležno pošto.
Program preplavljanja (angl. Flooder)	Program za napadanje omrežij s preplavljanjem (angl. Denial of Service attack)
angl. Keyloggers	Program za beleženje na tipkovnici pritisnjenih tipk.
Zombi (angl. Zombie)	Program aktiviran na okuženem računalniku, namenjen proženju napadov na druge računalnike.
angl. Adware	Program, ki nam samodejno prikazuje oglase.
angl. Spyware	Program, ki zbira podatke o uporabniku in jih nato brez njegove vednosti posreduje tretji osebi.

Tabela 1: Terminologija na področju zlonamernih programov

Delimo jih lahko v dve skupini; na tiste, ki za svoje delovanje potrebujejo program v katerega se naselijo in na samostojne oz. neodvisne programe. Med prve

štejemo npr. viruse, logične bombe in stranska vrata; med druge pa črve in zombije.

V nadaljevanju so podrobneje razložene skupine zgoraj naštetih vrst zlonamernih programov.

5.1 Računalniški virusi

Programi, ki se brez vednosti uporabnika sami razmnožujejo in se skrivajo v računalniških zapisih in datotekah, spadajo med viruse. Njihovo obnašanje je podobno obnašanju bioloških virusov, ki se širijo po celicah organizma. Od tod izhaja tudi njihovo ime. Datoteke, ki vsebujejo viruse, imenujemo okužene datoteke.

V znanstvenih krogih se je ideja o računalniškem programu, ki deluje podobno kot biološki virus pojavila, pojavila sredi sredi 70. let prejšnjega stoletja. Prvi program, ki je lahko okužil druge programe je nek študent izdelal leta 1980. Od tega leta dalje je bilo odkritih že več kot 80.000 različnih virusov, pri čemer je 99% okužb posledica le nekaj sto različnih virusov, ki jih danes najdemo razširjene med uporabniki. Leta 1982 se je pojavil prvi računalniški virus, ki se je preko okuženih disket razširil izven laboratorijev. Imenoval se je *Elk Cloner*, okužil pa je sisteme z operacijskim sistemom Apple DOS 3.3.

Leta 1995 je Izrael postal prva država, ki je uzakonila kazni proti avtorjem virusov.

5.1.1 Vrste računalniških virusov in njihovi načini širjenja

V splošnem velja, da računalniške viruse izdelujejo nadarjeni programerji, pogosto imenovani tudi hekerji. Ni namreč preprosto napisati programa, ki kopira samega sebe z vstavljanjem v druge datoteke, pri čemer mora zaobiti vse najnovejše varnostne ukrepe v računalniških omrežjih in operacijskih sistemih, ter pri tem narediti še nekaj škode. Kljub temu lahko preprost virus izdela tudi nekdo, ki ni vešč programiranja, saj za ta namen obstajajo različni namenski programi. Virusi se prožijo na izbran način in naredijo škodo glede na želje njegovega izdelovalca. Tako lahko danes tudi uporabnik računalnika brez programerskih izkušenj izdela virusni program, ki se na primer sproži na njegov rojstni dan in na okuženih računalnikih izpiše '*Vse najboljše!'*. Širjenje takega virusa pa bo najverjetneje zelo hitro ustavljeno, saj imajo dandanes ze skoraj vsi računalniki nameščen kak protivirusni program, ki tak virus zlahka odkrije. V ta namen obstajajo tudi programi, ki viruse mutirajo, in jih torej naredijo neprepoznavne za protivirusne programe, vse dokler niso ti nadgrajeni z ustreznimi popravki.

Kljub slabemu slovesu, ki ga imajo virusi in njihovi avtorji v javnem mnenju, lahko med virusi najdemo tudi neškodljive ali celo 'dobre' viruse, ki jih avtorji pišejo bodisi da opozorijo na določene pomanjkljivosti sistemov ali celo popravijo okužene programe in brišejo druge viruse, bodisi imajo avtorji izdelavo virusov za svoj kreativni hobi in jih izdelujejo brez škodljivih vplivov.

Poleg tega, da bi viruse lahko delili na dobre in slabe, jih zaradi dejstva, da jih je velika večina slabih pogosteje delimo po načinu širjenja. V tem primeru jih v

grobem lahko razdelimo na *običajne viruse*, *črve* in *trojanske konje*. Predstavimo v nadaljevanju vsak tip nekoliko podrobneje.

Običajni računalniški virus

Običajni računalniški virus se skrije v datoteke in se z njihovo pomočjo širi. Ko uporabnik tako prenese okuženo datoteko v svoj računalnik (n primer z disketo, USB ključem, zgoščenko ali prek spleta) in jo požene, ga s tem okuži. Okužba se zgodi tako, da virus po aktiviranju poišče nove za okužbo primerne datoteke (lahko tudi na sosednjih računalnikih v lokalnem omrežju), jih okuži in začne s povzročanjem škode. Lahko se virus naloži tudi le v pomnilnik in v ozadju spremlja dogajanje v računalniku. V tem primeru ponavadi poskuša okužiti vsako datoteko s katero pride v stik uporabnik oz. operacijski sistem. Za običajne računalniške viruse torej lahko rečemo, da če jih ne aktiviramo (z zaganjanjem okužene datoteke), jih sicer lahko imamo v računalniku, vendar nam zaradi neaktivnosti ne morejo povzročiti škode.

Poseben primer običajnih virusov so **makrovirusi**, ki se širijo s pomočjo dokumentov programskega paketa Microsoft Office in so se pojavili sredi 90. let. Z njimi so najpogosteje okuženi dokumenti programov Word in Excel, v katerih so skriti makroukazi. Ti se z odprtjem dokumenta samodejno sprožijo in makrovirus kopirajo še v druge dokumente na disku.

Črv

Črvi, se od običajnih računalniških virusov razlikujejo po tem, da za širjenje ne potrebujejo človeka, ki bi jih npr. z nalaganjem datoteke zagnal. Za širjenje namreč uporabljajo računalniško omrežje na primer tako, da razpošljejo po elektronski pošti vsem, ki jih imamo v elektronskem imeniku. Postopek se nato ponovi pri vsakem prejemniku virusa in se verižno nadaljuje. Tudi, če črv sam ne povzroča škode na posameznem terminalu, lahko že samo njegovo širjenje povzroči težaves prometom v računalniškem omrežju.

Trojanski virus (konj)

Trojanski virusi, pogosto imenovani tudi trojanski konji, so programi so ponavadi na prvi pogled videti nenevarni ali celo koristni, v resnici pa vsebujejo zlonamerno kodo. Prejemniki trojanskega virusa običajno verjamejo, da so program dobili iz zaupanja vrednega vira. Najbolj zahrbten primer trojanskega virusa je program, ki se predstavlja kot protivirusni program, v resnici pa v računalnik sam prinese virus. Ta vrsta virusov je dobila ime po trojanskem konju, ki so ga Grki med trojanskimi vojnami podarili obleganim prebivalcem Troje in iz katerega so ponoči skrivaj zlezli vojaki ter odprli mestna vrata oblegovalcem.

V preteklosti, ko so bile diskete pogosto uporabljan medij povezanost računalnikov v mreže ali splet pa prej redkost kot pravilo, so se virusi širili predvsem z medsebojno izmenjav dokumentov na disketah. Nekateri virusi so za širjene uporabljali celo zagonski sektor diskete in v tem primeru je do okužbe računalnika

prišlo ob zagonu računalnika v katerem je bila pozabljena disketa. S široko uporabo spleta je način širjenja virusov preko prenosnih medijev skoraj popolnoma izginil, virusi pa so zaradi hitrejšega razširjanja po omrežjih postali še resnejša grožnja.

5.1.2 Škodljivo delovanje virusov

Virus, kot že rečeno, običajno ne more narediti škode, dokler ga uporabnik ne sproži. Proženje se izvede z zagonom datoteke ali odpiranjem dokumenta. Danes se to najpogosteje zgodi preko elektronske pošte in sicer ob odpiranju priponk. Še zlasti moramo biti pozorni na datoteke s končnicami EXE,COM, BAT, DOC, XLS, SCR in VBS. Odpiranje datotek s končnicami TXT, GIF in JPG (npr. *holiday.jpg*) bi moralo biti varno, vendar včasih pošiljatelj pravo končnico skrije tako, da ji doda še eno (npr. *holiday.jpg.exe*), ki jo nekateri programi za branje elektronske pošte skrijejo.

Ko uporabnik kakorkoli aktivira virus, pride čas, da ta opravi svoje škodljivo poslanstvo. Tu obstajajo med virusi velike razlike, saj je rezultat okužbe omejen le z domišljijo tistega, ki ga je izdelal. Večina virusov se namesti v računalnikov pomnilnik in se začne razmnoževati, šele potem pa začnejo s povzročanjem škode. To povzročanje škode je z namenom, da bi uporabnik težje odkril vir okužbe, pogosto sproženo šele čez nekaj časa, na primer na nek poseben datum ali na točno določeno uporabnikovo dejanje. Kot že rečeno nekateri virusi ne naredijo nič škodljivega in so dokaz, da njihov način širjenja deluje. Najpreprostejši imajo tako le sposobnost razmnoževanja, s čimer v določenem zasedejo ves razpoložljiv pomnilnik in s tem ustavijo delovanje sistema. Nekoliko bolj nagajivi virusi na primer pomešajo črke na ekranu ali pri izpisu na tiskalniku, izpišejo določeno besedilo, zaigrajo neko skladbo ali pa v primeru makrovirusa v nek dokument na vsako stran dodajo npr. logotip izdelovalca virusa. Najnevarnejši virusi pa so tisti, ki uničujejo datoteke na računalniku. To lahko storijo z neposrednim brisanjem datotek operacijskega sistema, uporabniških datotek, s formatiranjem diska ali z brisanjem zapisa Master Boot Record, ki je bistven za pravilno branje podatkov iz diska. Še bolj zviti virusi, z namenom da njihovega obstoja sploh nebi opazili, počasi brišejo podatke naključne podatke iz datotek. Tako podatki postopoma skoraj neopazno izginjajo, računalnik pa iz neznanih razlogov vedno slabše deluje. V zadnjem času so se pojavili tudi virusi, ki datotek ne izbrišejo, ampak jih zašifrirajo tako, da jih uporabnik ne more več prebrati. Obenem pa uporabnik računalnika dobi obvestilo, da bo program za dešifriranje dobil proti plačilu ustreznega zneska. Za vse zgoraj opisane primere lahko tako ugotovimo, da se pogosto izdelovanje varnostnih kopij lahko izkaže za zelo pomembno.

Virusi lahko poleg tega, da so neškodljivi ali škodljivi za sistem ali podatke, služijo tudi vohunjenju. Takšni virusi ob sprožitvi namestijo v računalnik t.i. stranska vrata (angl. back door), skozi katera lahko nekdo na daljavo opazuje ali celo nadzoruje računalnik. Napadalec lahko tako na primer računalnik z namenom pridobitve uporabniškega imena in gesla nekaj časa opazuje, potem pa s krajo identitete prevzame nadzor. Virus bi v tem primeru beležil pritiske na tipke računalnikove tipkovnice in jih sporočal napadalcu.

5.1.3 Načini zaščite pred računalniškimi virusi

Ker v splošnem ni načina, s katerim bi lahko ugotovili prisotnost virusa, čeprav nekateri virusi sami opozorijo nase, se v boju proti računalniškim virusom poslužujemo namenskih t.i. protivirusnih programi, ki periodično preverjajo ali kakšna datoteka v računalniku morda vsebuje virus. Kot že rečeno obstaja tako več tipov virusov kot tudi njihovih načinov širjenja, ki so se skozi zgodovino spreminjali. So pa bili virusi skozi vso svojo zgodovino najbolj pogosto pisani za operacijski sistem Microsoft Windows. Razlog za to gre iskati predvsem v tem, da je najbolj razširjen, gotovo pa obstajajo tudi nekateri drugi razlogi. Virusi se pojavljajo tudi na drugih operacijskih sistemih res pa je, da so na nekaterih zelo redki.

Preden se posvetimo načinom zaščite pred virusi si poglejmo še kateri so tipični znaki na podlagi katerih lahko sumimo, da je naš računalnik okužen:

- samodejna izključitev ali ponovni zagon računalnika,
- močno upočasnjeno delovanje računalnika,
- izginjanje datotek, za katere smo prepričani, da smo jih shranili,
- izginjanje odsekov diska,
- pojav naključnih napak na zaslonu ali izpisu tiskalnika,
- 'sesuvanje' programov, ki so prej brezhibno delovali …

Prvi korak v obrambi pred virusi je redno nadgrajevanje in posodabljanje operacijskega sistema. S tem se zmanjša število varnostnih lukenj, skozi katere bi se lahko prikradli virusi. Najbolj pomembno orodje za boj proti virusom pa so protivirusni (ali tudi antivirusni) programi. Njihova glavna Naloga je, da iščejo sledi znanih virusov v vseh za njih primernih datotekah. Če virus najdejo, ga morajo biti sposobni izolirati od sistema (pogosto se na tem področju uporablja izraz karantena) ali pa ga na željo uporabnika virus pobrisati iz datoteke, oz če to ni mogoče, izbrisati celo datoteko. Prav tako, kot za operacijske sisteme tudi za protivirusne programe velja, da jih je potrebno posodabljati in s tem osveževati bazo poznanih virusov s podatki o najnovejših. Pri tem opravilu nam večina programov omogoča avtomatsko posodabljanje virusov ob določeni uri ali ob zagonu računalnika.

Seveda se lahko zgodi, da tudi redno posodabljanje ni dovolj hitro za preprečitev okužbe. V tem primeru je potrebno namestiti popravek za konkreten virus kar najhitreje, ko le ta postane dostopen. Ti primeri nastopijo, kadar virus za svoje širjenje izkoristi varnostno luknjo v operacijskem sistemu ali uporabniški programski opremi. Takrat je njegovo širjenje lahko tako hitro, da v nekaj urah okuži ogromno število računalnikov po vsem svetu.

Poleg opisanih postopkov občasnega pregledovanja datotek s protivirusnim programom je priporočljiva tudi namestitev t.i. ščita, to je programa, ki sproti preveri vsako pognano, odprto ali preneseno datoteko. Na tem mestu pri sprotnem pregledovanju pa smo prišli še do zadnjega, a gotovo tudi zelo pomembnega obrambnega mehanizma pri obrambi pred virusi. Gre za, če ji lahko tako rečemo, *'psihologijo radovednosti'*, ko uporabnik zavestno zažene nek program, ki ga je na primer dobil kot priponko k elektronski pošti. Do tega problema najpogosteje pride

ko odpove sprotno preverjanje uporabnik pa misli, da je sporočilo prišlo od vira, ki mu zaupa. V resnici pa je virus maskiral naslov pošiljatelja z nekim iz imenika naključno izbranim naslovom.

V večni tekmi med virusi in protivirusnimi programi, ki se verjetno ne bo nikoli končala, se razvijalci slednjih trudijo odkriti metode, ki ne bi zgolj preverjale prisotnosti znanih virusov, ampak bi samodejno odkrivale vedenjske vzorce virusov in jih posledično odstranjevale po vzoru biološkega imunskega sistema. To je tem težje ob dejstvu, da so se sodobni virusi ob kopiranju (spet po vzoru bioloških procesov) sposobni vsakokrat nekoliko spremeniti (mutirati). Med sumljive vzorce obnašanja bi tu lahko šteli razna nepredvidena poseganja programov v register operacijskega sistema, ali pa akcije nekega procesa ob vsakokratnem zagonu računalnika. Še posebej težko se je ubraniti virusov, ki se pred odkritjem na različne načine zavarujejo. Nekateri tako v svoje škodljivo delovanje vključijo tudi spremembe protivirusnega programa samega. Torej, kakor tudi evolucija v milijardah let ni našla popolnega imunskega sistema, tudi v računalništvu ne smemo pričakovati, da bomo pred računalniškimi virusi kdaj popolnoma varni.

5.2 Vohunski programi

Programi, ki brez naše vednosti in nadzora stikajo po podatkih v našem sistemu, jih zbirajo in dostavljajo tistemu, ki ga ti podatki zanimajo, so lahko zelo nadležni in tudi nevarni.

Ogledali si bomo, kakšne vrste okužb z namenom vohunjenja poznamo in podali nekaj nasvetov, kako se pred temi okužbami zavarovati. Že na tem mestu si moramo namreč priznati, da je večina okužb povezana s premajhno ozaveščenostjo uporabnikov, ki težave v zvezi s tem odkrijejo bodisi prepozno, ali pa jih pripisujejo drugim vzrokom.

Opozorimo še, da čeprav samodejno razmnoževanje ni lastnost vohunskih programov, le ti pogosto deluje skupaj z virusi (predvsem trojanskimi konji), ki smo jih opisali v prejšnjem razdelku. Na opise je zato je potrebno gledati kot celoto. V skupino vohunskih programov štejemo čiste vohunske programe (angl. spyware), oglasne programe (angl. adware), klicni programi (angl. dialers), ugrabitelje (angl. hijackers) in vsiljene orodne vrstice (angl. toolbars).

Preden pa se lotimo opisa vsakega od teh povejmo, da so tudi t.i. piškotki (angl. cookies), ki so majhne datoteke z omejenim naborom podatkov že lahko znajdejo v razredu oglasnih ali celo vohunskih programov. V te datoteke na disku uporabnika, spletne strani sicer shranjujejo podatke, preko katerih ga ob njegovem naslednjem obisku prepoznajo. V osnovi gre torej za pozitivno usmerjeno tehnologijo, ki pa jo je mogoče zlorabiti tudi v vohunske namene.

5.2.1 Čisti vohunski programi

Vohunske programi so programi, ki proti naši volji in ponavadi tudi brez naše vednosti zbirajo podatke o našem sistemu. Največkrat so to podatki o sistemu

samem, nanj nameščenih programih, uporabniških imenih in geslih, naslovih v elektronskem imeniku, seznamih obiskanih spletnih strani …

Čistokrvni vohunski programi se v sistem namestijo brez naše vednosti, z drugim uporabniškim programom ali pod pretvezo nekega 'nepogrešljivega' programa. Tako se pogosto zgodi, da neka spletna stran za uspešno nalaganje zahteva namestitev npr. nekega popravka ali orodja za ogled. In če tak program namestimo se pogosto izkaže, da je bila v sistem vnesena okužba.

Lep primer takega programa je *Bonzi Buddy* (slika 10), ki pod pretvezo prijazne opice, ki nam pomaga pri računalniških opravilih, v ozadju pa pritajeno beleži podatke o našem sistemu.

Slika 10: Primer vohunskega programa Bonzi Buddy

Čeprav smo trojanske konje že predstavili v poglavju o računalniških virusih, so hkrati izrazit zgled vohunskega programiranja, še posebej kadar zbirajo uporabniška imena in gesla, ki jih pošiljajo v oddaljene strežnike. Je pa res, in to je tudi razlog zakaj smo trojenske konje predstavili v poglavju o virusih, da se vohunsko programje v neki točki močno razlikuje od virusov. Namreč, vohunski program se bo morda res naselil v računalnik, ne da bi o tem obvestil uporabnika, a pri tem ne bo imel samorazmnoževalnih nagnjen, medtem ko se bo virus hotel razširiti tudi v druge računalnike.

5.2.2 Oglasni programi

Oglasni programi so od vohunskih precej manj nevarni, so pa zato toliko bolj moteči. Uporabniku namreč na zaslonu proti njegovi volji prikazujejo oglase v različnih oblikah.

Oglasni programi se v sistem največkrat namestijo s kakšnimi drugimi uporabnimi programi, kot so npr. kodeki za predvajanje filmov. Najbolj znan primer takega oglasnega programa je *GAIN*, ki se na primer namesti skupaj s kodekom DivX in se kot večina ostalih takih programov ne pusti zlahka odstraniti.

5.2.3 Klicni programi

Med množico vohunskih programov so še posebej zahrbtni in nevarni t.i. Klicni programi ali klicatelji, ki se brez vednosti uporabnika namestijo na računalnik,

potem pa prek modema kličejo izbrane plačljive telefonske številke. To pa lahko privede do visokih računov na strani uporabnika oz. do nepoštenih zaslužkov na drugi strani.

Statistike kažejo, da se klicni programi prikradejo v sistem večinoma prek internetnih strani z erotično vsebino in da pri namestitvi največkrat uporabijo trojanskega konja, ki jim omogoči namestitev brez kakršnegakoli opozorila.

5.2.4 Ugrabitelji in vsiljevalci orodnih vrstic

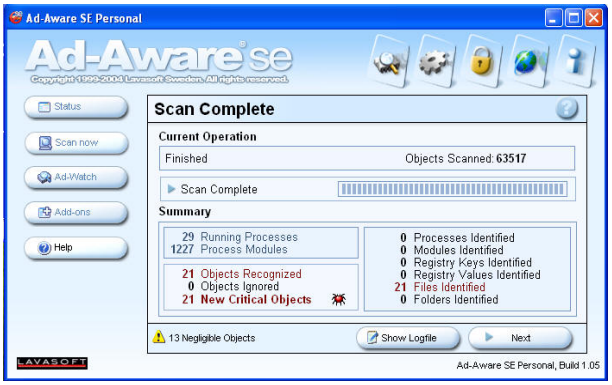
Za ugrabitelje je značilno, da prevzamejo nadzor nad deli uporabnikovega spletnega brskalnika. Najpogostejši simptomi so zamenjana domača stran, dodana ali zamenjana iskalna vrstica, preusmerjanje na določene spletne strani in pa preprečitev ogleda določenih spletnih strani.

Skoraj praviloma velja, da ugrabitelji napadajo izključno Microsoftov Internet Explorer.

5.2.5 Zaščita

Oglejmo si nekaj zgledov nenavadnega obnašanja sistema, ob katerih lahko posumimo na prisotnost vohunskih programov:

- ob zagonu sistema se odpre spletni brskalnik z neko oglasno stranjo,
- spremenjena je privzeta domača stran spletnega brskalnika,
- spremenjena je vsebina seznama priljubljenih spletnih povezav,
- slaba odzivnost sistema …



Slika 11: Primer uporabniškega vmesnika protivohunskega programa

Odgovor na vprašanje, zakaj se moramo zavarovati pred vohunskimi programi, se že glede na vse zgoraj omenjene neposredne nevšečnosti zdi trivialen. Pa vendar se je potrebno zavedati še vrste pomembnejših problemov, ki nam jih le ti lahko povzročijo. Teoretično je namreč mogoče prek vohunskih programov pridobiti kakršnokoli informacijo iz sistema, vključno z uporabniškimi imeni in gesli, številkami kreditnih kartic itn. Poglavitni problem je torej varnost.

Najbolje se proti vohunskim programom zavarujemo tako, da jih sploh ne dobimo. Najbliže k temu stanju približamo s previdno uporabo spleta, z rednimi posodobitvami operacijskega sistema in z namestitvijo požarnega zidu, ki nas opozarja na vsakršen promet v sistem in iz njega. V kolikor se v sistem vseeno prikrade vohunski program pa potrebno pomoč poiskati pri specializiranih programih za odkrivanje in odstranjevanje teh programov. Primer uporabniškega vmesnika enega izmed takih programov prikazuje slika 11.

6. Neželena elektronska pošta

Svetovni splet je odličen medij za pošiljanje sporočil v elektronski obliki, saj pošiljatelju v primerjavi s klasično pošto ne povzroča praktično nobenih stroškov. Je pa s pomočjo posebne programske opreme mogoče 'z enim samim klikom' poslati sporočilo milijonom uporabnikov. Kadar prejemniki takih sporočil ne želijo prejemati, gre za neželena oglasna sporočila (angl. spam).

Sporočila vrste spam so ena največjih nevarnosti interneta, saj lahko povzročijo škodo na več ravneh. Prav gotovo so v veliko nadlogo prejemnikom, saj jim povzročajo precejšnjo izgubo časa, ko se morajo prebiti čez velike količine sporočil. Poleg tega, tudi močno obremenjujejo računalniška omrežja s podatkovnim prometom, iz česar sledi , da so primerna tudi za napade za zavrnitev storitve (angl. Denial of Service – DoS), včasih imenovane tudi napad s preplavljanjem (angl. flooding). Gre za napade na ciljne računalniške sisteme povzročene s pretiranim in večinoma nesmiselnim prometom, ki ga ciljni sistemi ne morejo obdelati v razumnem času in zato odpovejo.

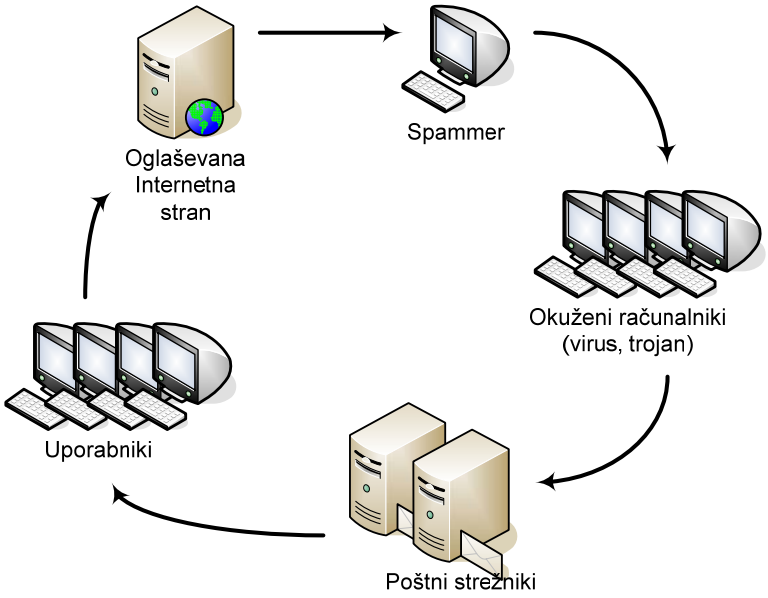
Množično pošiljanje oglasnih sporočil krši pravila skoraj vseh ponudnikov dostopa do svetovnega spleta in ponavadi vodi do ukinitve elektronskega naslova, s katerega so bila sporočila poslana. Takšno početje v večini držav zakonsko prepovedano, kar pa prenekaterih od tega početja ne odvrne, saj gre v tem poslu za velike zaslužke.

Razširjevalci množičnih elektronskih sporočil najdejo naslove v različnih bazah podatkov, na spletnih straneh, v forumih, pri ponudnikih dostopa do spleta in z uganjevanjem. Kot vir pošiljanja uporabijo vsakokrat drug elektronski naslov. Tako lahko pride tudi do situacije, ko se pošiljatelj neželene elektronske pošte prikaže svojo identiteto z naslovom nekega legitimnega uporabnika. Temu se nato obeta najmanj kup jeznih odgovorov žrtev poslanega sporočila, veliko število obvestil o nedostavljivosti sporočil, lahko pa ga doleti tudi ukinitev elektronskega naslova.

6.1 Pošiljanje spama

Prvi način pošiljanja spama, priljubljen predvsem v zadnjem času, je posredovanje spama s pomočjo računalnikov okuženih z virusom. Naloga takega virusa je, da uporabi elektronski naslov uporabnika in pošilja neželeno elektronsko sporočilo s tega naslova. Takemu računalniku hekerji pravijo 'zombi'. Ker je v tem primeru sporočilo poslano iz okuženega računalnika, se pravega pošiljatelja ne da izslediti iz zapisov poti, po kateri je sporočilo potovalo. To pa dodatno otežuje preprečevanje spama.

Začaran krog, ki ga tvori pošiljanje neželenih elektronskih sporočil prikazuje slika 12. Scenarij po je tak: Pošiljatelj oglasnega sporočila razširi virus, ki iz okuženih računalnikov pošilja sporočila vrste spam. Ta spodbudijo nekatere uporabnike, da obiščejo oglaševano spletno stran in se morda odločijo za nakup oglaševanega izdelka. Lastnik oglaševane spletne strani nato del dobička nameni pošiljateljem spama.



Slika 12: Začaran krog pošiljanja oglasnih sporočil

Drug način pošiljanja spama vključuje zlorabo brezplačnih in prosto dostopnih strežnikov za elektronsko pošto, kot je npr. Hotmail. Račune na teh servisih si pošiljatelji spama ustvarjajo s pomočjo algoritmov, ki si izmišljajo uporabnike, ki naj bi bili lastniki teh naslovov. Ponudniki so zato, v želji preprečiti takšne zlorabe, na mnogih spletnih straneh, kjer si uporabniki lahko ustvarijo elektronski naslov dodali polje za prepoznavo niza znakov. Ljudje takšne nize zlahka prepoznamo, računalniki pa imajo brez posebnih postopkov za prepoznavo pisave s takšnimi nizi težave. Primer prikazuje slika 13.

Slika 13: Niz za računalnik težko prepoznavnih znakov

6.2 Preprečevanje spama

Ko so sporočila vrste spam razposlana, jih lahko zaustavimo šele ob dospetju na poštni strežnik ali na samem odjemalniku elektronske pošte. Tam so običajo nameščeni ustrezni filtri, ki preverjajo prihajajoča elektronska sporočila.

Najpreprostejši filtri preprečujejo prejemanje sporočil iz določenih spletnih domen, ki so znan vir spama. Naprednejši in v zadnjem popularnejši filtri uporabljajo za preprečevanje spama t.i. bayesov filter, ki temelji na verjetnosti pojavljanja določenih besed v sporočilih. Če sporočilo npr. vsebuje veliko besed, ki se pogosto pojavljajo v spamu (npr. Viagra) in hkrati malo besed, ki se uporabljajo v običajnih sporočilih, je verjetnost, da je sporočilo tipa spam, velika. Vendar pa so

se pošiljatelji tudi na te filtre že dodobra prilagodili, saj nekatera sporočila tipa spam sedaj vsebujejo dolga zaporedja besed, ki nimajo zveze s spamom (npr. izsek leposlovne literature).

Spamu se je torej težko izogniti, vseeno pa lahko poskusimo z naslednjimi ukrepi:

- Preventivno se je treba izogibati javnemu objavljanju svojega elektronskega naslova.
- Na sporočila spam ne pošiljamo odgovorov, saj s tem pošiljatelju le pokažemo, da je naš naslov še dejaven.
- Uporabimo fiter sporočil tako na poštnem strežniku, kot na odjemalcu elektronske pošte.

6.3 M-SPAM, SPIM, SPIT …

Zlivanje komunikacijskih tehnologij je v zadnjem času omogočilo širitev neželenega oglaševanja tudi v druge komunikacijske kanale, ki jih vsakodnevno uporabljamo.

Nove oblike spama so tako:

- M-SPAM - so neželena SMS sporočila,
- SPIM - so neželena sporočila na področju neposrednega sporočanja (angl. instant messaging) in
- SPIT – so neželena (glasovna) sporočila na področju internetne telefonije.

Ena izmed zadnjih tehnik učinkovitega spletnega sporočanja je tudi tehnologija RSS (angl. Really Simple Syndication, Rich Site Summary). Namenjena je popolnejšemu, uporabniško prilagojenemu sporočanju. Glede na to, da na primer nekatera podjetja to tehnologijo že spretno uporabljajo za oglaševanje, je vprašanje, ali bo prav tako postala tarča neke vrste spama in se bodo posledično tudi zanjo začeli razvijati filtri in drugi zaščitni mehanizmi.

7. Kraja zasebnih podatkov

Že z dosedanje obravnave najrazličnejših trikov in prevar, ki jih hekerji uporabljajo z namenom povzročitve najrazličnejših napadov lahko sklenemo, da so le ti vedno bolj iznajdljivi in sofisticirani. S tem se povečuje tudi preteča nam nevarnost in posledično tudi pomembnost zavedanja in poučenosti na tem področju.

Ugotovimo lahko tudi, da postajajo tehnike napadov vse bolj multifunkcionalne in jih torej ne moremo direktno uvrstiti med npr. viruse ali vohunske programe. V tem poglavju si poglejmo nekaj takih tehnik, ki jih hekerji uporabljajo za krajo zasebnih podatkov. Natančneje, opisali bomo skupino napadov, pri katerih hekerji od uporabnikov pridobijo njihove zasebne podatke (npr. uporabniška imena in gesla, številke kreditnih kartic …) in nato z njimi vdrejo v ciljni sistem. Mednje največkrat prištevamo: spoofing, phishing in pharming.

7.1 Spoofing

Pojem spoofing ima najširši pomen in v splošnem pomeni lažno predstavljanje uporabnika. Njegova raba se najpogosteje nanaša na pošiljanje elektronskih sporočil, kjer ponazarja metodo za potvarjanje elektronskega naslova pošiljatelja, s čimer heker dobi vstop v sisteme, kamor elektronsko sporočilo sicer ne bi bilo prepuščeno.

7.2 Phishing

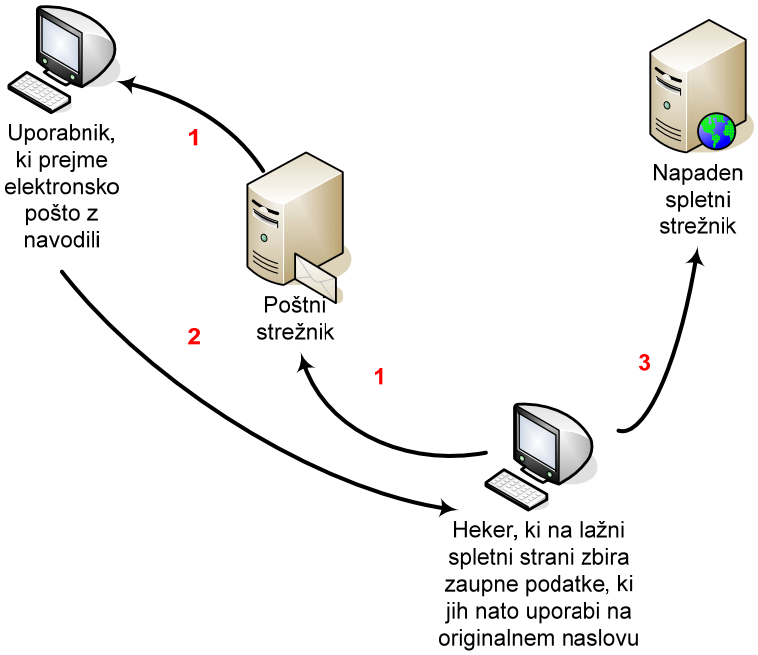
Phishing je vrsta internetne prevare, s katero napadalec s kombinacijo uporabe elektronske pošte in lažnih spletnih strani, pridobi zaupne podatke uporabnikov.

Ime metode je skovanka iz angleških besed password (geslo), harvesting (požeti) in fishing (ribariti), kar bi v slovenščino lahko prevedli kot *ribarjenje za gesli*. Nekateri izvor besede povezujejo tudi s starejšo metodo napadov, imenovano 'phone phreacking', s katero so hekerji, zaradi nekonsistentnosti javnega telefonskega omrežja, le tega včasih uporabljali za brezplačne telefonske klice.

V prvem koraku prejme žrtev takšnega napada elektronsko sporočilo, ki je videti, kot da je prišlo s popolnoma legitimnega naslova uglednega in znanega podjetja (npr. x@ime_banke.com). Zadeva sporočila je ponavadi naključno generirana, navezuje pa se na ime ustanove (npr.: Pomembno_obvestilo – ime_banke). Sporočilo se zdi popolnoma pristno, poleg tega pa je vsebina napisana tako, da takoj pritegne uporabnikovo pozornost in mu da vedeti, da gre za izjemno pomembno sporočilo. Prejemnik je tako npr. obveščen, da je nujno potrebna potrditev njegove identitete prek spletne strani, ali pa npr. da je zaradi vse pogostejših zlorab nujna zamenjava njegovega vstopnega gesla. Scenariji sporočil so precej podobni, vsi pa imajo isti cilj – pretentati prejemnika sporočila in od njega izvabiti zaupne podatke, s katerimi se bo lahko pošiljatelj sporočila okoristil.

Skupna lastnost vseh takih sporočil je tudi, da vsebujejo povezavo do lažne spletne strani, prek katere naj bi uporabnik posredoval prevarantskemu podjetju

zaupne podatke. Kar pri celotni zadevi najbolj zavede uporabnike, je to, da niti pomislijo ne, da so potencialna žrtev zlorabe, saj nikakor ne morejo podvomiti v pristnost prejetega sporočila niti v verodostojnost spletne strani, na katero so preusmerjeni, ko kliknejo na povezavo v sporočilu. Zaradi uporabe logotipov in drugih grafičnih simbolov, se namreč lažna spletna stran in elektronsko sporočilo tako v izgledu kot tudi v funkcionalnosti namreč popolnoma ujemata s spletno stranjo ali s pismom legitimnega podjetja.



Slika 14: Phishing napad

Omenjeno vrsto prevar je v bistvu zelo enostavno izvesti, saj so ponarejanje pošiljateljevega naslova, prikrivanje prave povezave (napadalci s skripti spremenijo naslov, ki ga uporabnik vidi v brskalniku tako, da se zdi, kot da je pravi; npr. http://www.banka.com/) in zajem podatkov, relativno preprosto opravilo. Slike, logotipi in stilske lastnosti, ki se uporabljajo na lažnih straneh in v posredovani e-pošti, pa so tako ali tako vsem uporabnikom dostopne na originalnih straneh. Napadalci si tako razmeroma preprosto in brez velikega naprezanja poskušajo pridobiti dostop npr. do bančnih računov nič hudega slutečih uporabnikov. Končni cilj prevar, pri katerih uporabnik posreduje zaupne podatke tretjim osebam, je v izbranem primeru seveda kraja denarja. Princip je ponazorjen na sliki 14.

7.3 Pharming

Poleg napadov phishing se v zadnjem času pojavlja vse več napadov, ki imajo prav tako zanimivo ime – pharming. Tudi tu gre za obliko napada, s katerim želijo napadalci pridobiti zaupne podatke uporabnikov.

Beseda pharming je skovanka iz angleških besed farming (kmetovati) in pharmaceutical (farmacevtski), ki v biotehnologiji pomeni vzrejo gensko spremenjenih živali.

Napadi phishing, kot že rečeno, temeljijo predvsem na *privabljanju* uporabnikov na lažne spletne strani s pomočjo elektronskih sporočil. Za razliko od njih, napadi pharming ne temeljijo na privabljanju, oz. bi lahko rekli, da so *napadi brez vabe (elektronskega sporočila)*. Gre namreč za neposredne napade na DNS-strežnike ali na datoteko o gostiteljih (hosts) v uporabnikovem računalniku. Posledica tovrstnih napadov je, da so uporabniki nevedoč, preusmerjeni na zlonamerne spletne strani, četudi so v naslovno vrstico brskalnika pravilno vnesli URL-naslov strani, ki so jo želeli obiskati. Ker so lažne spletne strani največkrat spet popolne kopije originalnih, uporabniki niti opazijo ne, da so na lažnem naslovu in da se v ozadju dogaja v bistvu nekaj škodljivega. Ravno to nevednost pa izkoriščajo napadalci, saj od uporabnikov na lažni strani ni težko izvabiti zaupnih podatkov.

Preden podrobneje razložimo potek napada, si za lažje razumevanje poglejmo osnovno delovanje DNS (Domain Name System/Server) strežnikov. Le ti skrbijo za pretvarjanje imenskih naslovov domen v pripadajoče internetne IP naslove. Predstavljamo si jih torej lahko kot nekakšne telefonske imenike za domene. Ko želi uporabnik obiskati določeno spletno stran, se zahteva po obisku iz njegovega računalnika posreduje DNS strežniku, ki poskrbi za prevod spletnega naslova v IP naslov (npr. www.neka_domena.si = 1.1.1.1). Na podlagi te pretvorbe nato DNS strežnik preusmeri uporabnika na spletno stran, ki jo je želel obiskati. Če strežnik zahtevka po pretvorbi ne more razrešiti, ga posreduje drugemu strežniku in tako dokler računalnik ne dobi nazaj ustreznega IP naslova. Kot si lahko mislimo, je bil DNS sistem uveden predvsem zaradi tega, ker si ljudje mnogo lažje zapomnimo neko ime, kot pa numeričen niz.

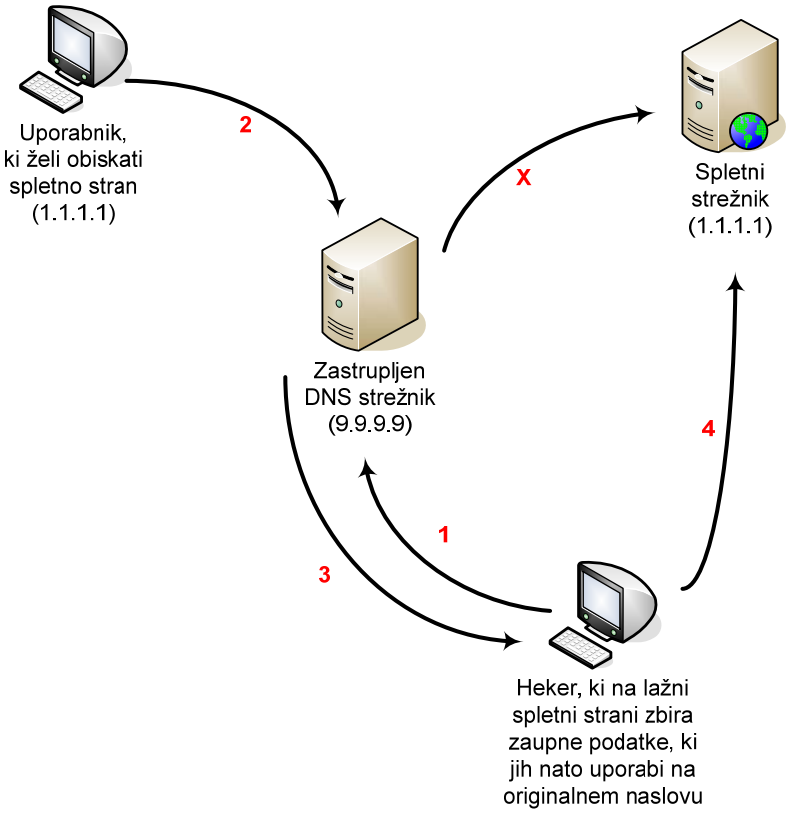
Kot že rečeno poznamo dve različici napadov pharming; lokalni napad na posamezen računalnik in neposredni napad na sam DNS strežnik.

7.3.1 Napad na DNS strežnike

Za neposredne napade na DNS strežnike je značilno, da prizadenejo vse uporabnike, ki dostopajo do napadenega strežnika. Izvedejo se s kompromitiranjem DNS sistema in so poznani tudi pod imenom DNS poisoning (zastrupljanje). Ker so torej usmerjeni v strežnik in ne na posamezne uporabnike, lahko v kratkem času dosežejo veliko žrtev, ki jih preusmerijo na zlonamerne strani.

Če je DNS-strežnik, ki pretvarja spletne in e-poštne naslove v numerične nize, zastrupljen, to pomeni, da vsebuje napačne povezave med imeni domen in pripadajočimi IP-številkami. Zaradi tega pride do nepravilnega razreševanja IP naslovov in s tem do preusmeritev uporabnikov na napačne strani kljub pravilno vnesenim URL naslovom. Posledica zastrupitve DNS strežnika je, da se imenskemu zapisu domene priredi lažna IP številka (npr. www.neka_domena.com ni več 1.1.1.1 ampak 9.9.9.9). Če bo torej uporabnik odtipkal naslov www.neka_domena.com, bo ne da bi to sploh vedel, preusmerjen na lažno spletno stran 9.9.9.9. Ta bo na videz po vsej verjetnosti popolna kopija originalne spletne strani, na kateri bo napadalec od uporabnika skušal izvabiti podatke, ki jih bo

lahko kasneje uporabil za zlorabo na originalni spletni strani. Postopek je prikazan na sliki 15.



Slika 15: Pharming napad

7.3.2 Napad na datoteko o gostiteljih

Medtem ko je za neposredne napade značilno, da prizadenejo vse uporabnike, ki dostopajo do napadenega strežnika, je za lokalne napade značilno, da so mnogo lažje izvedljivi in še učinkovitejši od prvih. Vse kar mora napadalec storiti, je 'le' spremeniti datoteko hosts v uporabnikovem računalniku (v primeru operacijskega sistema Windows imeniku C:\Windows\system32\drivers\...) in ustvariti lažno spletno stran, na katero bo uporabnik preusmerjen.

Napadalci pridejo do datotek hosts z vdorom, ali pa jo prepišejo s pomočjo različnih virusov ali trojanskih konjev, ki jih največkrat dobimo kar prek e-pošte. Datoteka hosts je napadalcem zanimiva zato, ker v uporabnikovemu računalniku shranjuje najpogosteje obiskane IP naslove in njim pripadajoče URL naslove, s čimer nam prihrani vsakokratno iskanje poti do spletne strani v DNS strežniku. Če napadalcu uspe prepisati oziroma opremiti datoteko hosts z lažnimi naslovi, bo uporabnik tudi ob pravilnem vnosu URL naslova preusmerjen na lažno stran, ki jo je ustvaril napadalec.

8. Viri

[1] S. Tomažič, 'Varnost v telekomunikacijah in kako jo zagotoviti', Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, maj 2003.

[2] W. Stallings, Cryptography and network security: principles and practice, Prentice Hall, Upper Saddle River (New Jersey), USA, 2005.

[3] E. Cole, R. Krutz, J. W. Conley, Network Security Bible, Wiley Publishing, Indianapolis, USA, 2005.

[4] D. Trček, Managing information systems security and privacy, Springer, Berlin, Heidelberg, New York, 2006.

[5] M. Y. Rhee, Internet Security : Cryptographic Principles, Algorithms and Protocols, John Wiley & Sons, West Sussex , England, 2003.

[6] B. Schneier, Secrets and lies: digital security in a networked world, John Wiley, New York, USA, 2000.

[7] R. Sušnik, S. Tomažič, Uporaba protokola IPsec v omrežjih IP.

[8] R. Kolar, 'Varnost v IP VPN omrežjih z uporabo tehnologije IPsec', Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, maj 2003.

[9] S. Tomažič, Varne komunikacije preko interneta.

[10] M. Trampuš, M. Ciglarič, T. Vidmar, Formalizacija varnostnih politik.

[11] V. Ban, 'Sistem za zaznavanje vdorov v IP omrežjih', Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, maj 2003.

[12] B. Štular, 'Varnostna analiza tehnologij za navidezna zasebna omrežja', Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, maj 2003.

[13] Revija Moj Mikro

[14] Revija Monitor

[15] Revija Življenje in tehnika

[16] http://en.wikipedia.org/