HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost sustava trenutnih poruka

CCERT-PUBDOC-2007-01-180

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Sustavi trenutnih poruka (eng. IM - *Instant Messaging*) omogućuju komunikaciju dvaju korisnika u stvarnom vremenu putem pisanih poruka. Poruke se između računala dvaju korisnika prenose računalnom mrežom, najčešće Internetom. Brojne prednosti IM sustava pred konvencionalnim načinima komunikacije, kao što su telefon ili elektronička pošta, učinile su ove sustave vrlo popularnima. Oni danas nisu samo sredstvo neformalne komunikacije već i alat za unaprjeđivanje suradnje među zaposlenicima brojnih tvrtki.

Osnovna karakteristika većine IM sustava je njihova skalabilnost, mogućnost rukovanja velikim brojem klijenata, koja je često postignuta na račun sigurnosti. Niti jedan besplatni IM sustav nema mogućnost enkripcije, a većina posjeduje određene mogućnosti zaobilaženja tradicionalnih korporativnih vatrozida, što administratorima otežava kontrolu njihova korištenja. Nesigurno rukovanje korisničkim zaporkama, mogućnost krivotvorenja korisničkih računa i izvođenja napada uskraćivanjem usluga česte su značajke ovih sustava. IM sustavi su dobar medij za širenje računalnih crva, virusa i drugih zlonamjernih aplikacija: oni su sveprisutni, osiguravaju komunikacijsku infrastrukturu, posjeduju liste korisnika koje mogu poslužiti za pronalaženje novih meta i često ih je moguće jednostavno programirati.

U nastavku dokumenta dan je općenit opis IM sustava, navedene su najčešće sigurnosne prijetnje i njihove osnovne značajke te kratak opis metoda sprečavanja širenja računalnih crva ovim sustavima. Dokument završava sigurnosnim preporukama za korištenje IM sustava i zaključkom.

2. Princip rada IM aplikacija

IM sustavi unaprjeđuju komunikaciju i olakšavaju suradnju jer, za razliku od elektroničke pošte, pružaju informaciju o tome je li sugovornik raspoloživ. Postavljanjem statusa korisnik može ostale korisnike obavijestiti kako je povezan, povezan ali zauzet ili povezan, ali nije uz računalo. Zbog toga komunikacija putem IM sustava može biti manje napadna od telefonske komunikacije, što je jedan od glavnih razloga rasta njezine popularnosti u poslovnim okruženjima. Ipak, neki popularni IM sustavi ne omogućuju slanje poruka korisnicima koji nisu povezani (eng. *offline message*) pa njih nije moguće koristiti kao manje formalni nadomjestak elektroničkoj pošti.

Kod ranih IM sustava pojedinačna slova su se kod sugovornika pojavljivala čim bi bila unesena, a i brisanje slova se prenosilo u stvarnom vremenu. Zbog toga je ovaj način komuniciranja više sličio telefonskom razgovoru nego razmjeni pisama. Moderni IM sustavi najčešće prenose cijeli redak teksta tek nakon prelaska u novi red.

Razgovore vođene pomoću IM sustava moguće je, za razliku od telefonskih razgovora, pohraniti i naknadno pregledavati. Spremanje razgovora daje IM sustavima postojanost koja karakterizira elektroničku poštu i koja omogućuje brzu, sigurnu i postojanu razmjenu podataka kao što su URL adrese ili odlomci dokumenata. Poznato je i da korištenje IM sustava uvelike poboljšava, u današnjem svijetu jako korisnu, vještinu strojopisa.

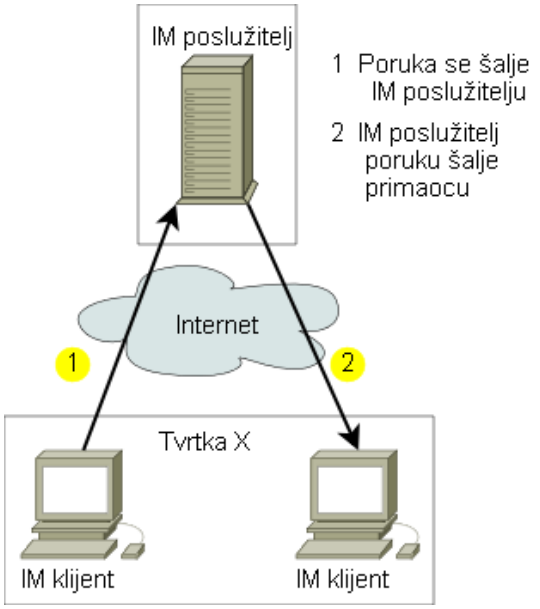
2.1. Komunikacijski modeli IM sustava

Prema načinu povezivanja i prenošenja poruka IM sustavi dijele se na:

- sustave temeljene na klijent-poslužitelj odnosu,
- P2P (eng. *Peer to Peer*) IM sustave i
- F2F (eng. *Friend to Friend*) IM sustave.

2.1.1. IM sustavi temeljeni na klijent-poslužitelj odnosu

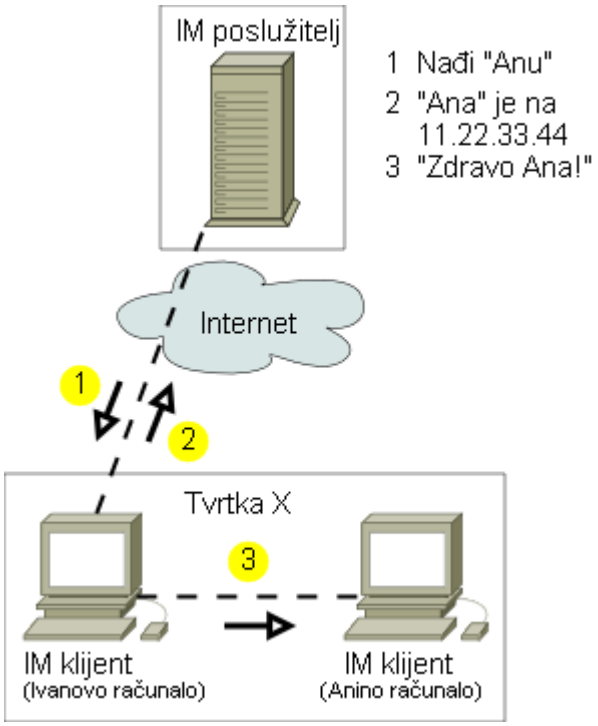
Gotovo svi IM sustavi sastoje se od poslužitelja i klijentskih aplikacija, ili kraće klijenata. Svaki korisnik na svome računalu, stolnom, prijenosnom ili ručnom, instalira klijenta, koji se nakon pokretanja povezuje s poslužiteljem te provjerava tko je od korisnika s liste povezan (eng. *on-line*) i raspoloživ za razgovor. Poruke se kod ovakvih sustava ne šalju izravno s pošiljateljevog računala na primateljevo, već se prijenos poruka vrši preko IM poslužitelja, kako je prikazano na slici Slika 1. Kod većine ovakvih sustava komunikaciju među klijentima izrazito je lako prisluškivati.



Slika 1: Primjer IM sustava temeljenog na klijent-poslužitelj odnosu

2.1.2. P2P IM sustavi

Postoje i implementacije distribuiranih IM sustava temeljenih na izravnom povezivanju klijenata, bez posredovanja poslužitelja (eng. *peer-to-peer*). Kod takvih se sustava za utvrđivanje povezanosti pojedinih korisnika koriste DHT (eng. *Distributed Hash Table*) tablice ili se za lociranje korisnika koristi IM poslužitelj nakon čega se uspostavlja izravna veza među klijentima, kao na slici Slika 2.



Slika 2: Primjer P2P IM sustava s poslužiteljem

Ako se oba klijenta nalaze unutar poslovne mreže ovakvi sustavi pružaju veću razinu sigurnosti u odnosu na IM sustave temeljene na klijent-poslužitelj jer poruke u ovom slučaju ne putuju Internetom.

2.1.3. F2F IM sustavi

Posljednja konfiguracija IM sustava temelji se na tzv. F2F (eng. *friend-to-friend*) mrežama kod kojih se svaki korisnik izravno povezuje s „prijateljima“ sa svoje liste „prijatelja“ i kod kojih je moguće povezivanje s „prijateljevim prijateljima“. Ovo je zapravo podvrsta P2P IM sustava. Iako su P2P i F2F IM sustavi otporniji na pogreške i kvarove, te unatoč dodatnim mogućnostima umrežavanja koje postoje kod F2F IM sustava, IM sustavi temeljeni na klijent-poslužitelj odnosu ipak su znatno više zastupljeni.

2.2. Organizacija IM poslužitelja

IM sustavi mogu biti organizirani oko jednog ili više poslužitelja. U slučaju korištenja većeg broja poslužitelja, pojedini među njima mogu imati sve ili samo neke funkcionalnosti nužne za rad IM sustava.

2.2.1. IM sustavi s jednim poslužiteljem

Jedan poslužitelj se kod ovakvih sustava brine za stvaranje korisničkih računa, autorizaciju korisnika i pružanje svih IM usluga. Postojanje samo jednog poslužitelja olakšava upravljanje sustavom i omogućuje postizanje više razine sigurnosti. IM sustavi s jednim poslužiteljem nisu skalabilni i zbog toga mogu imati problema s posluživanjem velikog broja korisnika.

2.2.2. Umnoženi poslužitelji

Kod IM sustava s umnoženim poslužiteljima svaki poslužitelj ima sve funkcionalnosti nužne za rad sustava. Poslužitelji su međusobno povezani čime je omogućena međusobna komunikacija korisnika povezanih na različite poslužitelje. Radi se umnoženoj varijanti IM sustava s jednim poslužiteljem.

2.2.3. Distribuirani IM sustavi

Distribuirani IM sustavi temelje se na raspodijeli zadataka među poslužiteljima. Pojedini poslužitelji tako mogu biti zaduženi za stvaranje novih korisničkih računa ili prijavu korisnika dok druga skupina poslužitelja upravlja prijenosom poruka među klijentima. Sustav je moguće izgraditi i tako da postoji više poslužitelja s istom ulogom. Ovo su najkompleksniji IM sustavi sa značajnim zahtjevima na infrastrukturu.

2.3. Dodatne mogućnosti IM sustava

Osim slanja poruka, IM sustavi korisnicima pružaju i brojne dodatne mogućnosti kao što su razmjena datoteka, programiranje klijenata ili održavanje web stranica. Ove mogućnosti čine IM sustave praktičnijima, ali i ranjivijima.

2.3.1. Prijenos datoteka pomoću IM sustava

Prijenos datoteka vrši se izravno između korisnika, bez prolaska datoteka kroz IM poslužitelj, kako bi se smanjili zahtjevi na propusnost mreže pružatelja IM usluga. To znači da se kod prijenosa datoteka uvijek koristi konfiguracija prikazana na slici Slika 2. Trenutno niti jedan od zastupljenijih IM sustava ne omogućuje enkripciju datoteka prenošenih među klijentima.

2.3.2. Programiranje IM sustava

Mnogi IM sustavi omogućuju korisnicima upravljanje pojedinim mogućnostima svoga IM klijenta pomoću programskog koda pisanog Visual Basic, JavaScript ili nekim drugim programskim jezikom. Iako praktična, ovakva mogućnost olakšava automatsko širenje računalnih crva i drugih prijetnji. Programirani IM klijenti mogu kontaktirati druge korisnike, slati datoteke, mijenjati vlastite postavke te izvoditi druge potencijalno štetne radnje.

2.3.3. Ostale mogućnosti IM sustava

Proizvođači svojim IM sustavima, zbog izrazito velike konkurencije, neprestano dodaju nove mogućnosti. ICQ klijent, na primjer, sadrži web poslužitelj koji korisnicima omogućuje održavanje manje web stranice izravno s vlastitog stolnog računala. Zlonamjerni korisnici mogu napadima na tako postavljenu web stranicu kompromitirati računalo na kojemu se izvodi web poslužitelj, odnosno IM klijent.

Neki noviji IM sustavi imaju omogućuju održavanje video i web konferencija, implementiraju VoIP (eng. *Voice over IP*) protokol, omogućuju dijeljenje radne površine (eng. *desktop sharing*) te reprodukciju IP radio i IPTV sadržaja.

3. Sigurnosne prijetnje IM aplikacijama

Niska razina sigurnosti IM sustava dovodi do velikog broja sigurnosnih prijetnji i raznolikih mogućnosti njihova iskorištavanja.

3.1. Prisluškivanje

Kako većina IM sustava ne vrši enkripciju mrežnog prometa, zlonamjerni korisnik može prisluškivati razgovor dvaju IM klijenata presretanjem i analizom mrežnog prometa ili korištenjem neke druge tehnike. Moguće je prisluškivati IM sustave temeljene na klijent-poslužitelj odnosu kao i P2P IM sustave.

3.2. Otimanje korisničkih računa

Mnogi IM sustavi ranjivi su na napade otimanjem korisničkih računa. Napadač koji uspješno provede takav napad može preuzeti IM identitet napadnutog korisnika u razgovoru s drugim korisnicima. Na nekoliko web stranica dostupni su alati i upute za izvođenje ovakvih napada. Većina IM sustava pruža malu ili nikakvu zaštitu korisničkih zaporki. Neki sustavi zaporke čuvaju na klijentskim računalima. U nekim slučajevima te datoteke su kriptirane, a u drugima nisu. Na pojedinim web stranicama postoje upute za probijanje enkripcije datoteka s korisničkim zaporkama nekih IM sustava.

Otimanje korisničkih računa moguće je provesti na više načina. Jedan od njih je slanje trojanskog konja koji nakon pokretanja pronalazi korisničke podatke i šalje ih napadaču. Napadač može preuzeti ulogu korisnika i preusmjeravanjem veze ili njenim otimanjem. Ako napadač, hineći poslužitelja, klijentu pošalje poruku o prekidanju veze ista će na poslužitelju ostati otvorena te zlonamjernom korisniku omogućiti preuzimanje IM identiteta zavaranog korisnika.

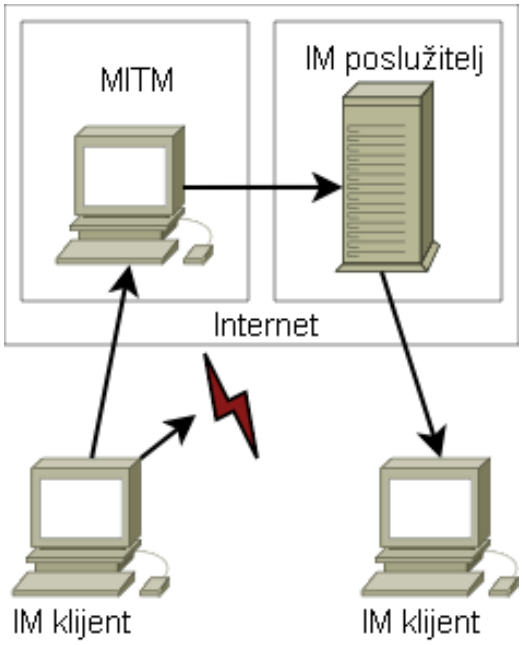
Korisnici s liste prijatelja korisnika čiji je IM račun otet mogu biti navedeni na otkrivanje potencijalno osjetljivih podataka ili na pokretanje zlonamjernih aplikacija pa je zbog toga ovakav napad opasan, kako za njih, tako i za korisnika čiji identitet je ukraden.

3.3. Neovlašten pristup podacima

Kao sve Internet aplikacije, tako i IM sustavi mogu sadržavati sigurnosne propuste koji omogućuju udaljene napade na ranjivo računalo. Napadima prepisivanja spremnika ili slanjem posebno oblikovanih mrežnih paketa udaljeni zlonamjerni korisnik može steći pristup računalu na kojem se izvodi ranjivi IM klijent. Brojne mogućnosti modernih IM klijenata povećavaju vjerojatnost pojavljivanja sigurnosnih nedostataka.

3.4. Napad preusmjeravanjem IM prometa

Napadač koji uspije preusmjeriti IM promet (eng. MITM - *Man-in-the-Middle*) tako da se postavi između klijenta i poslužitelja, kao na slici *Slika 3*, može analizirati i mijenjati poruke ili sprečavati njihovo dostavljanje.



Slika 3: Napad preusmjeravanjem IM prometa

3.5. Računalni crvi i višestruke prijetnje

Višestruke prijetnje (eng. *blended threats*) zajednički je naziv za skupinu napada koji, kombinirano izvedeni, povećavaju učinjenu štetu i/ili brzinu svog širenja. Primjer takve prijetnje je korištenje računalnog crva i virusa, uz istovremeno iskorištavanje ranjivosti računalnih i mrežnih sustava, kako bi se postigla zlouporaba koja ne bi mogla biti posignuta zasebnim korištenjem bilo koje od navedenih tehnika/ranjivosti.

Neka svojstva IM sustava omogućuju širenje računalnih crva i ugrađenih prijetnji. Ovdje se, u prvom redu, misli na slijedeće:

- IM sustavi osiguravaju robustan komunikacijski kanal među računalnim sustavima svojih korisnika.
- Liste prijatelja unutar IM sustava mogu biti iskorištene za širenje računalnih crva među korisnicima.
- Neke IM sustave moguće je programirati, što zlonamjernim aplikacijama pruža prilagodljivo sredstvo širenja.

Višestruka prijetnja prilagođena napadu na IM sustave bi, zbog njihove sveprisutnosti, mogla u samo nekoliko sati zaraziti na desetke milijuna osobnih i poslovnih računala. Na zaraženim računalima programski crv može brisati podatke, instalirati druge zlonamjerne aplikacije i otkrivati potencijalno osjetljive informacije neovlaštenim korisnicima.

Računalni crvi i višestruke prijetnje mogu se IM sustavima širiti:

- prijenosom zlonamjerno oblikovanih datoteka (zahtjeva sudjelovanje korisnika),
- zlouporabom mogućnosti njihova programiranja,
- slanjem posebno oblikovanih URL adresa (zahtjeva sudjelovanje korisnika),
- iskorištavanjem sigurnosnih propusta unutar IM klijenata ili
- iskorištavanjem ranjivosti operacijskih sustava ili nekih često korištenih aplikacija.

Postoje deseci računalnih crva koji se šire putem IRC (eng. *Internet Relay Chat*) IM sustava. Ovi su crvi programirani skriptnim programskim jezikom koji se distribuira zajedno s IRC klijentom i uglavnom djeluju na sljedeći način:

1. Korisnik čije je računalo zaraženo pridružuje se grupi i započinje razgovor.
2. Kako se nezaraženi klijenti pridružuju grupi, crv ih uočava i šalje im kopiju sebe u obliku datoteke koja sadrži skriptu. Kod nekih crva se korisniku koji je primio takvu datoteku nudi njezino otvaranje, a kod drugih korisnik ne prima nikakvu obavijest o primljenoj datoteci.
3. Kada crv zarazi novo računalo ciklus se ponavlja.

Uz IRC crve postoji i cijeli niz crva prilagođenih širenju pomoću pojedinih IM sustava namijenjenih Windows operacijskim sustavima. Niti jedan od njih dosad se nije uspio značajnije proširiti, ali njihovo postojanje ukazuje na općenitu ranjivost IM sustava.

3.6. Trojanski konji

Većina popularnih IM sustava omogućuje dijeljenje datoteka ili postoje dodaci i zakrpe za dodavanje takve mogućnosti. Uspješno postavljen trojanski konj može neograničenim dijeljenjem svih datoteka udaljenom napadaču omogućiti neovlašten pristup ranjivom računalu. Korištenje IM sustava za širenje trojanskih konja ima nekoliko prednosti za napadače:

- ime napadnutog računala se ne mijenja čak ni u slučaju korištenja dinamičke IP adrese,
- napadač dobiva obavijest kada je žrtva povezana na poslužitelj,
- nije potrebno otvarati dodatni mrežni port, već je moguće komunicirati s ranjivim računalom preko već otvorenih IM mrežnih portova, što otežava zaustavljanje vatrozidom.

Osim trojanskih konja koji omogućuju neovlašten pristup tvrdom disku napadnutog računala postoje i varijante koji svome tvorcu šalju prikupljene informacije kao što su podaci o operacijskom sustavu, korisničke zaporke ili IP adresa ranjivog računala. Slanjem IM poruke moguće je zaraženom računalu naložiti izvođenje, prethodno programiranih, neovlaštenih radnji.

3.7. Iskorištavanje sigurnosnih nedostataka IM sustava

Sigurnosni nedostaci IM sustava mogu biti iskorišteni za širenje računalnih crva i ugrađenih prijetnji, za izvođenje napada uskraćivanjem usluga ili za napade na IM poslužitelj.

3.7.1. Napadi uskraćivanjem usluga

Napadači mogu slanjem velikog broja TCP/IP paketa zagušiti IM poslužitelje i tako onemogućiti slanje valjanih poruka. Isto tako, slanjem velikog broja poruka jednom IM klijentu moguće je izvršiti napad uskraćivanjem usluga samo nad jednim korisnikom.

3.7.2. Napadi na IM poslužitelje

Veliki se napori ulažu u povećanje sigurnosti IM klijenata, ali jednako je važno, ako ne i važnije, ukloniti mogućnosti napada na IM poslužitelje. Zlonamjeran korisnik koji neovlašteno stekne pristup IM poslužitelju može lako prisluškivati sve razgovore, oteti bilo koji korisnički račun, izvesti napad uskraćivanjem usluga ili proširiti zlonamjerne aplikacije.

4. Sprečavanje širenja crva IM sustavima

Širenje računalnih crva IM sustavima moguće je spriječiti ili ograničiti:

- privremenim gašenjem poslužitelja,
- isključivanjem pojedinih klijenata,
- primjenom algoritma gušenja ili neke njegove varijante te
- provođenjem CAPTCHA testova.

4.1. Privremeno gašenje poslužitelja

Centralizirana struktura IM sustava čini ovu jednostavnu metodu zaustavljanja IM crva vrlo uspješnom. Postupak se sastoji od sljedećih koraka.

1. gašenje IM poslužitelja,
2. analiza uočenog računalnog crva i pisanje zakrpe namijenjene klijentskim aplikacijama, a koja uklanja mogućnost širenja crva i njegova zlonamjernog djelovanja na već zaraženim računalima,
3. prisilna nadogradnja svih klijenata prilikom sljedećeg povezivanja na poslužitelja, nakon njegova paljenja.

Nedostaci ove metode su obustavljanje IM usluga tijekom analize otkrivenog crva i pripreme zakrpe te činjenica da IM crvi mogu započeti epidemiju drugih crva, koji iskorištavaju ranjivosti operacijskog sustava i koji se šire elektroničkom poštom ili nekim drugim sredstvom. Gašenje IM poslužitelja imat će malo učinka na takvu epidemiju.

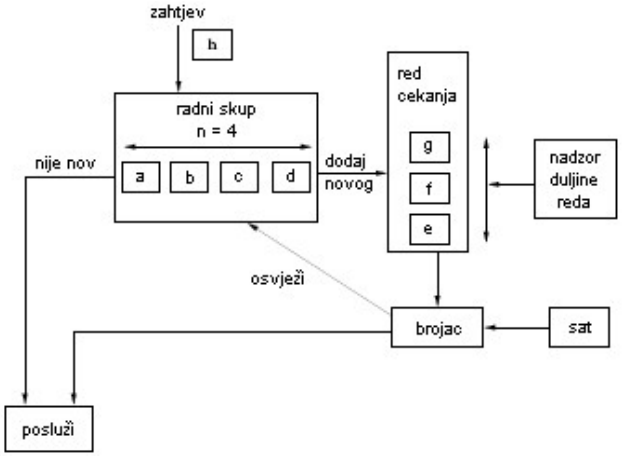
4.2. Privremeno isključivanje najpovezanijih klijenata

Mreže IM korisnika su nerazmjerne (eng. *scale free*) pa se isključivanjem relativno malog broja najpovezanijih klijenata, odnosno klijenata s najvećim listama prijatelja, može značajno povećati promjer mreže i tako usporiti širenje crva. Najpovezaniji klijenti, tzv. čvorovi (eng. *hub*) ostali bi izvan IM mreže do izdavanja zakrpe. Ovaj pristup ne sprečava širenje crva, već ga samo usporava i to diskriminirajući korisnike.

4.3. Algoritam gušenja

Algoritam gušenja (eng. *throttling*) temelji se na činjenici da se komunikacija kojom se šire računalni crvi značajno razlikuje od normalne IM komunikacije. Korisnici razgovaraju sa sporo promjenjivim podskupom korisnika sa svoje liste prijatelja dok IM crvi šalju poruke svim povezanim korisnicima s liste. Algoritam funkcionira tako da održava *radni skup* kontakata s kojima je korisnik razgovarao u određenom vremenskom periodu i onemogućuje slanje više od jedne poruke u vremenskoj jedinici novom korisniku, tj. korisniku s liste prijatelja koji se ne nalazi u radnom skupu. Svaki puta kada korisnik pokuša poslati poruku, primateljeva oznaka ('h' na slici Slika 4) se uspoređuje s onima iz radnog skupa. Ako se spomenuta oznaka već nalazi u radnom skupu poruka se odmah šalje, a u suprotnom se postavlja u *red čekanja* i šalje kasnije. Moguća je implementacija u kojoj se poruka u svakom slučaju šalje odmah, a u red čekanja se samo bilježe poruke poslane novim korisnicima, tako da zapravo nema kašnjenja u slanju poruka. Stariji zapisi se iz reda čekanja uklanjaju periodički, a isto tako se osvježava stanje radnog skupa. Ako rad čekanja preraste dozvoljenu veličinu, algoritam

pretpostavlja da se radi o pokušaju širenja IM crva, blokira sve poruke prema novim korisnicima te od korisnika traži potvrdu valjanosti poruka iz reda čekanja.



Slika 4: Shematski prikaz algoritma gušenja

Osnovni nedostaci ovog jednostavnog algoritma su:

- U slučaju postavljanja preniskog praga veličine reda čekanja učestala potreba za potvrđivanjem valjanosti poruka može biti smetnja korisnicima i razlog odbacivanja algoritma od strane IM zajednice.
- Blokiranje poruka, u slučaju prekoračenja veličine reda čekanja, do potvrde njihove valjanosti uzrokuje kašnjenje koje je u suprotnosti s načelima sustava trenutnih poruka.
- Kompromitiranje algoritma moguće je razvojem crva koji umjesto korisnika potvrđuje valjanost poruka.
- Ovaj algoritam ne uzima u obzir grupne razgovore ili sobe za razgovore u kojima se poruke istovremeno šalju većem broju korisnika.
- Implementacija algoritma na strani IM poslužitelja zahtjeva određenu količinu memorije za svakog korisnika.
- Moguća je pojava crva koji bi pratio komunikaciju korisnika te izgradio vlastiti radni skup. Pažljivim slanjem poruka takav crv bi se mogao proširiti na sve korisnike iz radnog skupa, kao i na ostale korisnike iz liste prijatelja, bez prekoračivanja veličine reda čekanja.

4.4. Selektivni algoritam gušenja

Primjenom algoritma gušenja samo na poruke koje sadrže URL adrese te na zahtjeve za prijenos datoteka značajno bi se smanjili negativni učinci ovog algoritma na performanse IM sustava jer ove poruke predstavljaju manji dio ukupnog broja poruka. Normalne tekstualne poruke šalju se bez kašnjenja i nema praga koji uvodi potrebu potvrđivanja njihove valjanosti. Kod prijenosa datoteka učinak algoritma gušenja dodatno je umanjen činjenicom da njihov prijenos ionako nije trenutan.

4.5. CAPTCHA

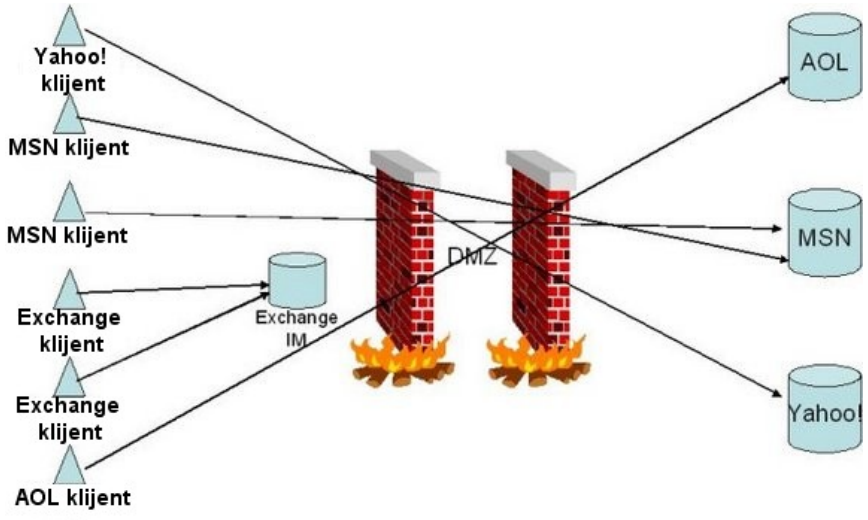
Provođenjem CAPTCHA (eng. *Completely Automated Public Turing test to tell Computers and Humans Apart*) testa nad pošiljaocima zahtjeva za prijenos datoteka ili poruka koje sadrže URL adrese, moguće je u velikom broju slučajeva otkriti šalje li poruku stvarna osoba ili računalni crv. Smanjenje performansi nije značajno zbog slabe učestalosti ovakvih poruka. CAPTCHA testove automatski stvara IM poslužitelj ili klijentska aplikacija primaoca. Ljudi ih lako rješavaju dok su algoritmi za njihovo rješavanje izrazito složeni te je vjerojatnost nasumičnog pogađanja točnog odgovora gotovo zanemariva.

5. Sigurnosne preporuke za korištenje IM sustava

Navedene ranjivosti IM sustava moguće je neutralizirati ili barem umanjiti pravilnim korištenjem vatrozida, antivirusnih aplikacija, VM (eng. *Vulnerability Management*) alata, ispravnim podešavanjem IM klijenata i poslužitelja te pravovremenom primjenom zakrpi.

5.1. Blokiranje IM poruka vatrozidom tvrtke

Mnoge tvrtke žele blokirati komunikaciju nesigurnim IM sustavima vlastitim, već postavljenim, vatrozidom. To najčešće nije moguće jer uobičajeni vatrozidi ne mogu zaustaviti promet posljednje generacije popularnih IM sustava u koje su ugrađeni brojni mehanizmi njihova probijanja.
Svim IM klijentima izvorno je postavljeno više IP adresa za povezivanje na poslužitelje. Mnoge tvrtke postavljaju vatrozide tako da blokiraju sve Internet usluge osim male skupine nužnih usluga (na primjer SMTP za elektroničku poštu, HTTP za pregled web stranica i DNS) čemu su tvorci IM klijenata doskočili tuneliranjem prometa preko uobičajeno dozvoljenih protokola.



Slika 5: Većina IM klijenata pokušava zaobići vatrozide u pokušaju povezivanja na poslužitelje

Primjerice, mnogi će klijenti, ako imaju poteškoća s povezivanjem na poslužitelj, pokušavati s njime stupiti u kontakt preko mrežnog porta 80. Ovaj port se uobičajeno koristi za pristup web stranicama pa je kod većine vatrozida promet preko njega dopušten. U opisanom slučaju IM klijent vatrozidu izgleda kao još jedan web preglednik, ali se njegov promet sastoji od IM naredbi, a ne HTTP naredbi kao kod web preglednika.
Kako bi se blokirao IM promet kroz vatrozid potrebno je spriječiti povezivanje klijenata na poslužitelje. To je jedino moguće učiniti dodavanjem IP adresa (npr. 11.22.33.44) ili imena (npr. *instantmessageserver.chatservice.com*) poslužitelja svih IM sustava čije korištenje se želi spriječiti na listu usluga koje vatrozid blokira. Ako se uzme u obzir da neki IM sustavi (npr. IRC) imaju mogućnost povezivanja na više nezavisnih poslužitelja, ova metoda može iziskivati opsežno istraživanje.

5.2. Blokiranje IM prijenosa datoteka vatrozidom tvrtke

Prijenos datoteka IM sustavima mnogo je lakše blokirati od prometa IM poruka jer se datoteke prenose izravno među korisnicima, bez posredovana IM poslužitelja koji može biti prilagođen zaobilaženju vatrozida.
Najbolji način za blokiranje neželjenog prijenosa datoteka vatrozidom je zabranjivanje prometa preko portova koje u tu svrhu koriste popularni IM sustavi. Takvom zabranom neće biti onemogućen prijenos datoteka među klijentima unutar tvrtke. Međutim, neki IM sustavi posjeduju mogućnosti maskiranja i kod prijenosa datoteka. Zbog toga, a i zato što mnogi vatrozidi ne provjeravaju sadrži li IM promet

datotekama računalne viruse, potrebno je instalirati antivirusne aplikacije na svim računalima unutar tvrtke, kako bi se na vrijeme otkrile i uklonile sigurnosne prijetnje proširene na ovaj način.

5.3. Određivanje pravila korištenja IM sustava

Brojne ranjivosti javnih IM sustava čine ih nepodobnim za poslovnu komunikaciju. Zbog toga je potrebno zabraniti njihovo korištenje unutar tvrtke, ako ne u potpunosti onda barem što se tiče poslovne komunikacije.

5.4. Postavljanje osobnih vatrozida

Osobni vatrozidi mogu biti postavljeni tako da onemogućuju komunikaciju neovlaštenih programskih paketa preko Interneta. Vatrozidi postavljeni na osobnim računalima mogu biti puno uspješniji u blokiranju IM prometa od vatrozida tvrtke zbog toga što je kod njih moguće dodatno prilagoditi postavke za pojedine aplikacije.

5.5. Postavljanje IM poslužitelja unutar tvrtke

Tvrtkama se savjetuje postavljanje jednog ili više sigurnih IM poslužitelja unutar tvrtke te prilagodba svih klijenata tako da se povezuju isključivo na njih. Na taj način se interna IM komunikacija odvija iza vatrozida tvrtke. Postoje brojni komercijalni, ali i besplatni, IM sustavi posebno prilagođeni korištenju u tvrtkama.

5.6. Preporučene postavke IM klijenata

U slučaju korištenja vanjskog IM sustava unutar tvrtke potrebno je odabrati sustav koji primjenjuje enkripciju i podesiti IM klijente tako da:

- primaju poruke samo od korisnika koji se nalaze na listi prijatelja ili kojima je to izričito dozvoljeno (time se sprečava povezivanje udaljenih napadača i slanje zlonamjerno oblikovanog programskog koda),
- prihvaćaju datoteke samo od korisnika s liste prijatelja i uz prethodan upit,
- koriste dostupne antivirusne alate za pregledavanje primljenih datoteka, ako je ta mogućnost podržana.

IM korisničke račune zaposlenika preporučeno je prilagoditi tako da nisu navedeni na javnim poslužiteljima. Time se dodatno smanjuje mogućnost neželjenih zahtjeva za pokretanjem razgovora.

5.7. Korištenje VM alata

Korištenjem VM (eng. *Vulnerability Management*) alata moguće je promjene osjetljivih IM postavki učiniti nedostupnima. Takvi alati administratorima omogućuju uvid u eventualna kršenja pravila korištenja IM sustava i odgovarajuće intervencije nad računalima na kojima se odvija nedozvoljena aktivnost. Osim navedenog, VM alati administratorima olakšavaju pronalaženje nenadograđenih i/ili ranjivih inačica IM klijenata te utvrđivanje koriste li zaposlenici propisane antivirusne aplikacije i vatrozide.

5.8. Zaštita privatnosti

Prilikom stvaranja IM korisničkog računa preporuča se odabrati korisničko ime koje ne odaje osobne informacije. Na primjer bolje je odabrati korisničko ime '*StariPunker*' nego '*HrvojeHorvat*'. Tako odabrano ime ne treba javno obznanjivati niti ga odavati nepoznatim korisnicima. Neki IM sustavi povezuju adresu elektroničke pošte s IM korisničkim imenom što može rezultirati povećanim brojem neželjenih elektroničkih pisama. Osjetljive informacije, kao što su brojevi kreditnih kartica i zaporke, ne treba otkrivati tijekom IM razgovora. Slanje osobnih IM poruka s posla također nije preporučano zbog toga što nadređeni mogu imati ovlasti za njihovo pregledavanje.

6. Zaključak

Efikasnost i praktičnost komunikacije čine IM sustave sve važnijim alatom brojnih tvrtki. Nedostatna razina sigurnosti ovih sustava, s druge strane, dovodi u pitanje sigurnost računalnih sustava i povjerljivih podataka tvrtki i pojedinaca koji ih svakodnevno koriste, bilo u poslovne ili u privatne svrhe.

Pravilnim korištenjem IM sustava, koji dodatno sadrže više sigurnosnih elemenata, vjerojatnost uspješnog napada može se značajno umanjiti. U slučaju velikih tvrtki to mogu biti i komercijalni IM sustavi posebno prilagođeni takvoj upotrebi. Pored toga, potrebno je primijeniti i druga sredstva zaštite računalnog sustava kao što su vatrozidi, VM sustavi i antivirusne aplikacije.

Rast uporabe IM sustava u poslovnim okruženjima uvelike će povećati efikasnost pojedinih zaposlenika i cijelih tvrtki, ali samo primjenom odgovarajućih sigurnosnih mjera bit će moguće u potpunosti iskoristiti njihove mogućnosti.

7. Reference

[1] Neal Hindocha: Instant Insecurity: Security Issues of Instant Messaging, http://www.securityfocus.com/infocus/1657, siječanj 2007.

[2] 10 tips for safer instant messaging, http://www.microsoft.com/athome/security/online/imsafety.mspx, siječanj 2007.

[3] Frank Thorsberg: How Secure Is Instant Messaging?, http://www.pcworld.com/article/id,103721-page,1/article.html, siječanj 2007.

[4] Paul Korzeniovski: Instant Messanging Opens New Security Holes, http://www.technewsworld.com/story/33271.html, siječanj 2007.

[5] Mindi McDowell, Allen Householder: Using Instant Messaging and Chat Room Safely, http://www.us-cert.gov/cas/tips/ST04-011.html, siječanj 2007.

[6] Symantec Enterprise Security: Securing Instant Messaging, http://www1.cs.columbia.edu/~angelos/worm05/imworms.pdf, siječanj 2007.

[7] Nigel Williams, Joanne Ly: Securing Public Instant Messaging (IM) At Work, CAIA Technical Report 040726A, 2004

[8] Mohammad Mannan, Paul C. van Oorschot: On Instant Messaging Worms, Analysis and Countermeasures, WORM'05, 2005