HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost Skype alata

CCERT-PUBDOC-2007-10-208

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

Skype je međunarodno popularan alat za komuniciranje putem Interneta. On nudi funkcionalnost standardnog *instant messaging* (IM)klijenta, ali je najveću popularnost ipak stekao zahvaljujući funkcionalnosti IP telefona. Iako postoji velik broj klijenata koji nude slična rješenja uporabe VoIP (eng. *Voice over IP*) protokola, većina njih se pokazala se nedovoljno dobrima (uglavnom zbog loše kvalitete veze) te ne mogu zamijeniti klasičan telefon.

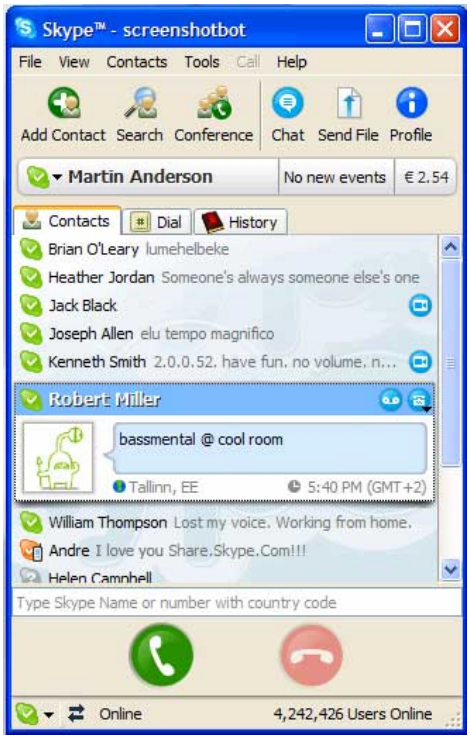
Skype se upotrebom vlastitog, još uvijek tajnog rješenja tog problema i besplatnom distribucijom aplikacije nametnuo kao najbolje rješenje te ubrzo postao vrlo popularan. Nakon incijalno velikog interesa javnosti, Skype je u fokus ponovno došao nedavno, kada je korisnicima njegova usluga bila nedostupna čak nekoliko dana zbog sigurnosnih problema u alatu i poslužiteljima za podršku. Tek nakon tog događaja pojavilo se pitanje: "Koliko je Skype ustvari siguran i trebaju li njegovi korisnici biti na oprezu kada ga koriste?" Odgovor na to pitanje tema je ovog dokumenta.

2. Općenito o *Skype* alatu

Skype je alat za telefoniranje i *instant messaging* putem Interneta. Temelji se na P2P (eng. *Peer To Peer*) infrastrukturi i vlastito razvijenim komunikacijskim protokolima koji djeluju povrh VoIP protokola. Skype P2P mreža razvijena je oko središnjeg poslužitelja koji sadrži podatke o Skype korisnicima i omogućuje njihovo pronalaženje u mreži Međutim, sama komunikacija između korisnika ne odvija se preko tog poslužitelja.

Skype korisnicima uz male naknade omogućuje i uspostavljanje poziva prema fiksnim ili mobilnim telekomunikacijskim mrežama bilo gdje u svijetu. Budući da su naknade za takvo telefoniranje još uvijek puno manje od onih za ostvarenje takvog poziva unutar klasične telekomunikacijske mreže, Skype je stekao veliku popularnost.

Skype se odlikuje i izuzetno jednostavnim sučeljem (*Slika 1*) te visokom pouzdanošću čak i u situacijama u kojima brzina Internet veze nije velika. Tako se može sasvim normalno ostvariti telefonski poziv preko modemske veze od 56 kbit/s.



Slika 1. Skype korisničko sučelje

Autori Skype alata su Niklas Zennstrom i Janus Friis, nekadašnji osnivači P2P KaZaA sustava za razmjenu datoteka, a alat je danas u vlasništvu kompanije eBay. Prema trenutno raspoloživim podacima Skype alat je preuzet sa službene stranice više od 38 milijuna puta i ima više od 7 milijuna registriranih korisnika. Skype svakog dana koristi više od 2 milijuna ljudi, od čega je u svakom trenutku više od njih milijun priključeno na mrežu. Skype alatom je dosad ostvareno 2,7 milijardi minuta besplatnih poziva između dva Skype klijenta, a u tu brojku nisu uračunati pozivi koji se naplaćuju, tj. pozivi prema telekomunikacijskim mrežama.

Treba primijetiti kako je popularnosti Skype alata pridonijela i mogućnost njegovog korištenja na nekoliko operacijskih sustava (Windows, Mac OS, Linux, Pocket PC) čime je pokriveno gotovo cijelo tržište korisnika osobnih računala. Osim što je potpuno besplatan, Skype je lišen reklamnih poruka i *spyware* programa koji korisnike često odvraćaju od korištenja besplatnih programa. Osnovni prihod Skype ostvaruje naplatom dodatnih usluga - poziva ostvarenih prema telekomunikacijskim mrežama.

2.1. Usporedba *Skype* alata s ostalim VoIP alatima

Postoji nekoliko definiranih i uglavnom međusobno nekompatibilnih protokola za prijenos glasa putem Interneta. ITU standard H.225 definira protokol za glasovne i video telekonferencije, IETF je prihvatio nekompatibilan protokol nazvan SIP (eng. *Session Initiation Protocol*), dok je Cisco razvio vlastiti protokol nazvan SCCP (eng. *Skinny Client Control Protocol*).
Skype također koristi zasebno rješenje. Protokol se temelji na središnjem poslužitelju koji omogućuje uspostavu veze sa Skype korisnicima. Nakon što je veza uspostavljena, sva se komunikacija odvija izravno između klijenata.
U usporedbi s ostalim VoIP alatima Skype se razlikuje u nekoliko značajnih činjenica:

- Skype je vrlo popularan – samo u prvom tjednu nakon objavljivanja u kolovozu 2003. godine 60 000 ljudi je preuzelo alat. Danas Skype broji milijune korisnika.
- Korištenje Skype klijenta i Skype P2P mreže je besplatno . Naplaćuje se samo korištenje dodatnih usluga kao što su „SkypeOut“ i „SkypeIn“ koje koriste pristup vanjskim telekomunikacijskim mrežama.
- Skype je značajno lakši za korištenje. Instalacija Skype klijenta je izrazito jednostavna – osim odabira korisničkog imena nije potrebna druga konfiguracija sustava. Osim toga, za razliku od drugih VoIP sustava, Skype će raditi čak i ako se korisnik nalazi iza vatrozida ili NAT (eng. *Network Address Translation*) sustava.
- Skype koristi impresivnu tehnologiju komprimiranja govorenog zvuka. Ona mu daje pouzdanost i kvalitetu koja čak nadmašuje neke tradicionalne telefonske sustave ako se koristi putem širokopojasne veze prema Internetu.
- Osim telefonije Skype podržava i *instant messaging*, pretraživanje i prijenos datoteka.
- Skype komunikacija je enkriptirana. Za razliku od obične telefonije i ostalih VoIP sustava, prema tvrdnjama Skype-a, sva komunikacija je enkriptirana ključevima od minimalno 128 bita što onemogućava bilo kakvo presretanje i prisluškivanje komunikacije.

3. Analiza rada *Skype* sustava

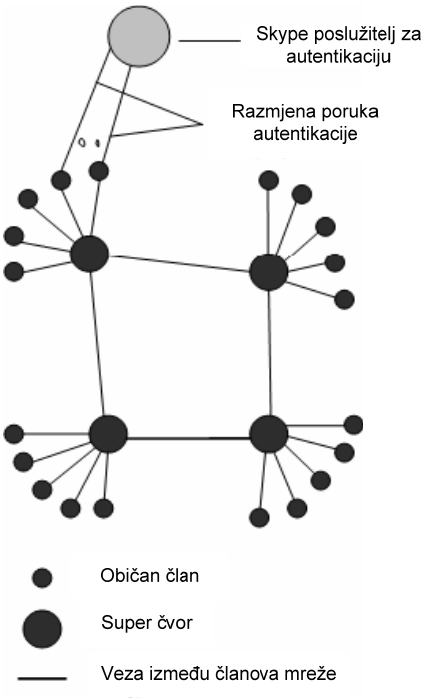
Skype sustav ima dvije osnovne komponente:

- Skype P2P mrežu i
- Skype klijente.

Komponente su detaljnije opisane u sljedećim poglavljima.

3.1. Skype P2P mreža

Skype P2P mreža se satoji od dvije vrste članova – obični članovi (eng. *Ordinary host*) i super čvorovi (eng. *Super Node*). Običan član je bilo koji Skype klijent za uspostavu poziva i slanje poruka. Super čvor je Skype klijent koji se nalazi na rubu Skype P2P mreže, tj. član kojeg samo jedan običan član dijeli od kraja mreže. Bilo koji član koji ima javnu IP adresu, dovoljno memorije i kapaciteta procesora, te dovoljno brzu vezu prema Internetu može postati super član.



Slika 2. Izgled Skype P2P mreže

Svaki običan član mora se povezati preko super čvora na Skype P2P mrežu, te se registrirati i uspješno proći kroz proces autentikacije Skype poslužitelja. Iako poslužitelj za autentikaciju nominalno nije član Skype P2P mreže on je njen važan element jer se na njemu pohranjuju sva korisnička imena i zaporke. Tim poslužiteljem se osigurava jedinstvenost Skype korisničkih imena unutar Skype P2P mreže.

Osim poslužitelja za autentikaciju u Skype mreži ne postoji niti jedan središnji poslužitelj. Informacije o statusu pojedinih korisnika (*on-line* ili *off-line*) nisu centralizirane, već se pohranjuju i distribuiraju pomoću ostalih članova mreže. Korisničke pretrage također se ne obavljaju na središnjem poslužitelju već se distribuiraju putem članova mreže.

Zaobilaženje NAT i vatrozidnih sustava su važne funkcije Skype sustava. Iako zbog zaštićenosti sustava nije točno utvrđen princip rada tih funkcija pretpostavlja se da koristi neku varijantu STUN protokola za utvrđivanje tipa NAT i vatrozidnog sustava.

Skype je mreža dinamičkog karaktera pa svaki Skype klijent mora održavati listu koja sadrži podatke o dostupnim super čvorovima mreže. Ta lista se u Skype sustavu naziva *host cache* (HC) i sadrži podatke o IP adresi i broju priključaka super čvorova, a pohranjuje se u unutar *Windows Registry* zapisa člana mreže.

Za komunikaciju unutar mreže koristi se TCP protokol za prijenos signalizacijskih informacija, a UDP i TCP protokoli za prijenos podataka. Pritom se signalizacijski podaci i sami podaci govora/poruka ne prenose preko jednakih priključaka.

3.2. Skype klijent

Skype klijent ima sljedeće funkcionalnosti:

- prati promet na određenim priključcima za detekciju dolaznog poziva,
- održava listu super čvorova (*host cache - HC*),
- koristi širokopojasne kodere/dekodere,
- održava listu kontakata,
- enkriptira podatkovni promet i
- utvrđuje nalazi li se iza NAT ili vatrozidnog sustava.

Za praćenje prometa Skype klijent otvara TCP i UDP priključke koje korisnik odabere prilikom instalacije klijenta na osnovu predloženih vrijednosti. Naime, tijekom instalacije Skype klijent slučajnim odabirom korisniku predlaže brojeve priključaka, što je jedna od njegovih posebnosti jer

ostali VoIP protokoli (primjerice, SIP) imaju definirane uobičajene priključke za TCP ili UDP promet. Povrh spomenutih Skype klijent otvara i dodatne priključke (HTTP i HTTPS priključci 80 i 443), ali se oni konfiguracijom klijenta mogu isključiti bez utjecaja na njegov rad.
HC lista je lista IP adresa i broja priključaka super čvorova Skype P2P mreže. Ovu listu kreira i periodički osvježava Skype klijent. Održavanje liste je ključno za rad Skype sustava i ona mora sadržavati barem jedan važeći zapis. Važeći zapis je zapis koji sadrži i IP adresu i broj priključka super čvora koji je trenutno aktivan u mreži. HC lista se pohranjuje unutar Windows registry zapisa i to na sljedećoj lokaciji: HKEY_CURRENT_USER / SOFTWARE / SKYPE /PHONE / LIB / CONNECTION / HOSTCACHE. Eksperimentalno je utvrđeno da ta lista sadrži maksimalno 200 zapisa. Bitno je primijetiti da Skype klijent ne može spriječiti svoj prijelaz iz običnog člana u super čvor unutar mreže.
Skype klijent vjerojatno koristi iLBC, iSAC kodere/dekodere za kodiranje zvuka no to nije službeno potvrđeno već se pretpostavka temelji na partnerskom odnosu između Skype-a i kompanije GlobalIPSound koja proizvodi spomenute kodere. Eksperimentalno je utvrđeno da Skype prenosi frekvencijski pojas od 50 – 8000 Hz što je uobičajeni pojas za širokopojasne kodere. Za ostvarenje poziva razumne kvalitete Skype klijentu je dovoljna Internet veza od samo 2 kbyte/s dok u standardnim uvjetima za glasovni poziv koristi od 3 do 16 kbyte/s.
Listu kontakata Skype klijent također pohranjuje unutar *Windows Registry* zapisa, ali je ta lista enkriptirana i digitalno potpisana. Lista se pohranjuje samo lokalno na računalu i ne postoji njena kopija na središnjem poslužitelju. Ako korisnik pristupa Skype mreži s drugog klijenta/računala morat će rekonstruirati svoju listu kontakata.
Skype klijent koristi AES enkripciju s ključem dužine 256 bita što daje maksimalno 1,1 x 1077 mogućih ključeva. U procesu dogovora za utvrđivanje simetričnih AES ključeva za zaštitu komunikacije Skype klijent koristi RSA enkripciju s ključevima dužine od 1536 do 2048 bita. Pritom javne ključeve dodijeljene korisniku digitalno potpisuje Skype poslužitelj za autentikaciju.
Pretpostavlja se da Skype klijent koristi varijaciju STUN (eng. *Simple Traversal of UDP through NAT*) i TURN (eng. *Traversal Using Relay NAT*) protokola za dobivanje informacija o tipu NAT ili vatrozidnog sustava iza kojeg se nalazi, ali zbog zaštićenosti sustava to nije moguće potvrditi.

4. Sigurnosni aspekt rada *Skype* alata

Sigurnost nekog sustava nije apstraktna osobina koja može biti nezavisno proocijenjena. Kako bi se ocijenio stupanj sigurnosti Skype alata, potrebno je uzeti u obzir specifične sigurnosne prijetnje i onda utvrditi pruža li Skype zaštitu od njih.
Povrh toga sigurnosna analiza Skype sustava se dodatno usložnjuje jer sigurnost alata ovisi o sigurnosti samog računala na kojem je on instaliran, kao i sigurnosti mreže putem koje Skype klijent pristupa Skype P2P mreži. Osim toga Skype protokol je tajan i zaštićen, a jedine dostupne informacije o njemu potječu od proizvođača ili su dobivene reverznim inženjeringom.
Povrh toga napisanog, Skype klijent se može automatski osvježavati što znači da se njegova sigurnost može mijenjati ovisno o inačici koja se trenutno koristi.
Uzevši u obzir sve navedene čimbenike, mogu se identificirati sljedeće bitne kategorije za ocjenu sigurnosti Skype sustava:

- Privatnost – dozvoljava li Skype prisluškivanje razgovora nekome izvan sustava?
- Autentičnost – ako se inicira poziv prema nekom korisniku, jamči li Skype autentičnost tog korisnika?
- Dostupnost – može li se Skype veza između korisnika uspostaviti uvijek kada su oba korisnika povezana na Internet ili može doći do situacije kada su oba korisnika priključena na sustav, ali jedan drugog ne vide? Može li se razgovor koji je u tijeku prekinuti?
- Izdržljivost – ako se Skype infrastruktura ošteti ili prekine na neki način, mogu li Skype korisnici još uvijek međusobno komunicirati?
- Otpornost – ako se Skype infrastruktura ošteti ili prekine na neki način do te razine da Skype više ne radi, mogu li Skype korisnici na jednostavan način uspostaviti međusobnu vezu?
- Integritet razgovora – gubi li Skype dijelove razgovora? Jesu li datoteke koje se prenose Skype sustavom prenesene u cijelosti i neoštećene.
- Integritet sustava – kako korištenje Skype alata utječe na ostale aplikacije na korisnikovom računalu?

Ocjena sigurnosti Skype-a u svakoj od navedenih kategorija bit će dana u sljedećim poglavljima.

4.1. Privatnost

U skladu s izjavama svojih autora, čini se da Skype koristi enkripciju. Istinitost ove primjedbe može se utvrditi analizom paketa koje Skype šalje. Iz njih se, naime, ne može na jednostavan način otkriti sadržaj komunikacije.

Napravljena je analiza jedne uspostave poziva koja je pokazala sljedeće:

- Za autentikaciju korisnika koristi se inačica HTTP protokola kojom se ostvaruje veza s središnjim poslužiteljem za autentikaciju (*ui.skype.com* - koji se navodno nalazi u Amsterdamu).
- Za komunikaciju s ostalim Skype klijentima koristi se izmijenjena inačica HTTP protokola.
- Za prijenos razgovora, poruka ili datoteka koristi se vlastito razvijeni kriptirani protokol.

Unatoč kriptiranju cjelokupne komunikacije Skype klijenata, analizom prometa moguće je raspoznati uspostavljanje interakcije između dvaju klijenata. To znači da čak i neovlašteni korisnici Skype P2P mreže mogu iz analize prometa otkriti kada neki korisnik zove drugog. Nije poznato da li Skype sustav članovima mreže daje mogućnost praćenja cjelokupnog prometa unutar Skype P2P mreže ili je njima vidljiv samo dio ukupnog prometa mreže.

Sigurnost kriptiranih podataka ovisi o mnogo čimbenika kao što su kriptografski algoritmi, mehanizam razmjene ključeva, implementacija protokola koji koriste kriptografiju, itd. Skype tvrdi da koristi RSA algoritam za razmjenu ključeva i 256-bitni AES algoritam za enkripciju komunikacije. Budući da implementacija tih algoritama kao ni dizajn njihovih certifikata i autentikacijskog sustava nisu javni, ne može se sa sigurnošću reći da su navedeni algoritmi uopće implementirani, a pogotovo nije moguće dati realnu ocjenu kvalitete primijenjene implementacije, kao ni opće sigurnosti koju ona pruža.

S druge strane može se sa sigurnošću reći da je Skype sigurniji od većine današnjih VoIP sustava jer oni uopće ne nude enkripciju. Međutim, ukoliko se komunikacija tih VoIP sustava ostvari povrh VPN mreže tada oni vjerojatno postaju sigurniji od Skype sustava.

Postoje i drugi sigurnosni aspekti Skype alata vezani uz privatnost :

- Iako izgleda da Skype klijent ne zapisuje ili arhivira glasovne pozive, on uobičajeno pohranjuje IM poruke osim ako korisnik izričito ne isključi tu opciju. Te arhivirane poruke mogu potencijalno postati meta napadačima putem raznih *spyware* ili drugih alata kojima se može preuzeti kontrola nad drugim računalom.
- Budući da su svi Skype korisnici priključeni na isti „oblak" svaki Skype korisnik može vidjeti da li je neki drugi korisnik trenutno priključen na mrežu ili ne.
- Čini se da Skype sustav pokušava razmjenjivati pakete izravno između sudionika razgovora. Ako izravan put između komunicirajućih subjekata nije ostvariv, klijent pokušava pakete razmjenjivati preko drugih računala uključenih u Skype mrežu – super čvorova. Nije poznato može li super čvor pratiti promet koji se kroz njega ostvaruje. Skype tvrdi da to nije moguće zbog upotrebe enkripcije, ali to nije moguće provjeriti.

4.2. Autentičnost

Svaki Skype korisnik ima korisničko ime i zaporku, te registriranu adresu elektroničke pošte za slučaj da zaboravi zaporku. Ti podaci se prilikom autentikacije šalju do autentikacijskog poslužitelja, ali nije potpuno jasno na koji način. Naime nije poznato u kojem točno obliku i na koji način korisničko ime i zaporka putuju kroz Skype P2P mrežu do poslužitelja za autentikaciju. S obzirom da se za prijenos koriste drugi članovi Skype P2P mreže potencijalno su mogući sljedeći napadi:

- Moguće je da neki član Skype P2P mreže uspije uhvatiti korisničko ime i zaporku drugog korisnika.
- Ako se za pristup Skype P2P mreži koristi zlonamjeran pružatelj Internet usluga on može preusmjeriti promet prema zlonamjerno oblikovanom Skype super čvoru da bi se domogao korisničkih podataka.
- Nije isključena ni mogućnost lažne autentikacije pomoću koje se neki član mreže priključuje na sustav s nekim korisničkim imenom za koji zaporka uopće ne postoji.

Ako se radi o glasovnoj komunikaciji tada će korisnici vrlo lako uočiti lažno predstavljanje, međutim ako se samo razmjenjuju IM poruke onda ta vrsta verifikacije nije primjenjiva. Unatoč svemu navedenom može se reći da Skype jamči jednaku razinu autentičnosti kao i većina sustava koji se temelje na korisničkom imenu i zaporci. U takvim sustavima većina korisnika ima kontrolu nad svojim korisničkim računom, ali uvijek postoji određeni mali broj korisnika čiji se korisnički podaci zlorabe.

4.3. Dostupnost

Klasična telekomunikacijska mreža ima impresivnu dostupnost od 99,99905 %. Internet mreža, iako izvorno zamišljena kao mreža koja može djelovati čak i u situaciji kad neki njen dio ne radi ipak ne pruža tako visoke razine dostupnosti. U slučaju Skype P2P mreže dostupnost Internet mreže ipak ne predstavlja kritičnu točku dostupnosti sustava.
Rad Skype sustava temelji se na autentikaciji svih korisnika koji pristupaju Skype P2P mreži, a autentikacija se obavlja na središnjem poslužitelju. To znači da ako središnji poslužitelj iz nekog razloga prestane biti dostupan ili prestane s radom, cijela mreža, tj. cijeli Skype sustav također ne mogu raditi. Dokaz za to je prezentiran nedavno kada je baš zbog problema s autentikacijskim poslužiteljem cijeli Skype sustav bio nedostupan većini korisnika nekoliko dana. Općenito, svaki sustav čiji rad se temelji ne središnjem poslužitelju imat će ovakav problem.

4.4. Izdržljivost

Često se čuje tvrdnja da je Internet dizajniran tako da izdrži i nuklearnu katastrofu. Činjenica je da su paketne mreže dizajnirane tako da dva čvora u mreži mogu komunicirati čak i kad izravna veza između njih ne postoji. Osobina sustava koja mu omogućuje nastavak rada čak i u situaciji u kojoj je oštećen naziva se izdržljivost (eng. *survivability*).
Internet mreža pružateljima usluga daje pravo izbora o tome koliko će njihova usluga biti izdržljiva. Ako neka organizacija poveže svoj poslužitelj elektroničke pošte na Internet jednom DSL linijom onda će u slučaju otkazivanja te linije ova usluga biti nedostupna. Ako pak odluči taj poslužitelj povezati s dvije DSL linije onda će sustav preživjeti pad bilo koje od te dvije linije.
Izdržljiviji sustavi su u pravilu skuplji nego sustavi s jednom točkom prekida, a rijetko kada pružaju značajno bolju funkcionalnost. Taj je čimbenik često presudan kod pružatelja usluga i korisnika Interneta te oni najčešće ne implementiraju izdržljive sustave. Vezano uz Skype sustav, nije poznato mogu li Skype poslužitelji za autentikaciju podnijeti probleme u radu Internet mreže ili neki mrežni napad.

4.5. Otpornost

Paketne mreže same po sebi pokazuju izuzetnu otpornost.
Skype sustav je, kao i većina drugih VoIP sustava, upravo zbog specifičnih zahtjeva sročenih u vrijeme dizajna, izuzetno otporan na prekid u lokalnoj mreži. Dok god se korisnik može registrirati u Skype mrežu njegova lokacija u mreži nije bitna.

4.6. Integritet razgovora

Mjere za očuvanje integriteta razgovora uspostavljenog unutar Skype mreže su potpuno nepoznate. Skype ne daje nikakva jamstva u tom pogledu pa je sasvim moguće da se u toku razgovora neki njegovi dijelove izgube ili ispremiješaju prije nego što stignu na odredište. Isto vrijedi i za prijenos datoteka i IM poruka – Skype ne jamči njihov integritet tijekom prijenosa.
U praksi međutim sve funkcionira prilično dobro pa se razgovori, poruke i datoteke prenose bez grešaka. Jedina iznimka od ovakvog ponašanja javlja se kad se Skype veza uspostavlja preko 802.11 bežične mreže jer tada dolazi do značajnog pada kvalitete prijenosa govora.

4.7. Integritet sustava

Mrežni administratori su s razlogom zabrinuti kada korisnici unutar njihove mreže preuzimaju i koriste programsku potporu čije korištenje može imati nepoznat utjecaj na rad mreže (ugrožena sigurnost, povećan promet i td.).

Što se Skype klijenta tiče, vezano uz količinu prometa, razloga za zabrinutost ne bi trebalo biti. Budući da su Skype razgovori ograničeni na prijenos glasa, maksimalni promet koji bi neki Skype super čvor mogao dodati na postojeći Internet promet je jednak dvostrukom broju razgovora koje super čvor prenosi pomnoženim s opsegom potrebnim za prijenos jednog razgovora. Budući da je opseg za prijenos jednog razgovora relativno malen, ukupna količina dodatnog prometa ne bi trebala biti značajna, osim ako se ne radi o prijenosu velikog broja razgovora. Trenutno nije poznato postoji li ograničenje na broj poziva koji se mogu prenositi putem jednog super čvora.
Skype klijent bi također mogao biti i izvorište *Spyware* programa. Iako njegovi kreatori tvrde da ne sadrži nikakav *Spyware*, nije sasvim sigurno govore li istinu, kao ni hoće li tu tvrdnju s vremenom promijeniti.
Moguće je također da Skype klijent sadrži i određene ranjivosti kojih njegovi korisnici nisu svjesni. Međutim, treba imati na umu da rizici koji dolaze uz upotrebu Skype sustava vjerojatno nisu drugačiji od rizika koje donosi korištenje drugih sličnih aplikacija. Čak štoviše, Skype vjerojatno predstavlja i manji rizik jer se primarno upotrebljava za ostvarenje glasovnih veza.
Ako se ipak počne koristiti za prijenos datoteka rizik se značajno povećava jer, za razliku od drugih sličnih alata, Skype nema ugrađenu antivirusnu zaštitu koja automatski kontrolira dolazne i odlazne datoteke.

5. Ranjivosti *Skype* sustava

U zadnje vrijeme otkriveno je nekoliko ranjivosti Skype sustava:

- Sigurnosni propusti Skype klijenta koji zlonamjernim korisnicima dozvoljavaju rušenje Skype klijenta i pokretanje proizvoljnog programskog koda na računalu na kojem se klijent nalazi.
- Sigurnosni propust koji Skype korisnicima omogućava pokretanje prijenosa datoteka bez pristanka druge strane, ali samo ako se prijenos događa između dva klijenta koji su već uspostavili povjerenje (tj. verificirali su jedan drugog).

Kao što je vidljivo spomenuti sigurnosni propusti (kao i većina ranije otkrivenih) uglavnom se ne odnose na Skype sustav nego na Skype klijent i to ih čini manje važnim. Jedino što je zabrinjavajuće kod većine propusta Skype klijenta je činjenica da se velik broj njih manifestira na svim platformama što govori o tome da su svi Skype klijenti utemeljeni na vrlo sličnom kodu. To i izuzetna popularnost čini ih potencijalno atraktivnom metom napadača.
Iako su otkrivene ranjivosti Skype klijenta relativno opasne, one nisu zabrinule Skype korisnike. Ono što je diglo veliku buku i srušilo povjerenje mnogih Skype korisnika bila je ranjivost Skype sustava koja je uzrokovala njegovo rušenje i nedostupnost korisnicima kroz nekoliko dana u kolovozu ove godine.
Iako se inicijalno smatralo da je uzrok pada sustava problem s autentikacijskim poslužiteljem, to se na kraju pokazalo netočnim. Također, pokazalo se netočnim i prvobitno objavljeno objašnjenje koje pad sustava dovodi u vezu s novoobjavljenim Windows sigurnosnim zakrpama. Nakon rješenja problema, koje se po ocjeni većine korisnika nije dogodilo dovoljno brzo, pojavilo se i konačno službeno objašnjenje koje ukratko opisuje razlog pada sustava.
Velik broj ponovnih pokretanja Windows računala u kratkom vremenskom roku, uzrokovanih instalacijom Windows sigurnosnih zakrpa, narušio je integritet Skype P2P mreže. To je dovelo do enormnog povećanja zahtjeva za autentikaciju što je pak zbog manjka trenutno raspoloživih resursa unutar Skype P2P mreže dovelo do lančane reakcije s kritičnim posljedicama. Automatski restauracijski mehanizmi Skype P2P mreže koji su u prošlosti uspjeli riješiti problem nedostatka P2P resursa nisu mogli obnoviti mrežu u nastalim uvjetima koji su ovaj put bili izuzetno nepovoljni.
Drugim riječima algoritam za alokaciju resursa nije se mogao dovoljno brzo prilagoditi okolnostima u kojima se jako brzo mijenjaju kako količina prometa tako i struktura Skype P2P mreže te je zaglavio i doveo do raspada mreže. Da bi se problem riješio bilo je potrebno ručno stabilizirati jezgru Skype P2P mreže kako bi se omogućio njen daljnji rad.
Kao što je vidljivo iz opisanog, najopasnije ranjivosti Skype sustava nisu ranjivosti klijenata nego ranjivosti Skype P2P mreže koja, čini se, ipak nije baš toliko otporna na opterećenja i pouzdana koliko se mislilo.

5.1. Sigurnosne preporuke za korištenje

Budući da na sigurnost i otpornost Skype P2P mreže korisnici Skype sustava ne mogu utjecati, preporuke dane u ovom odlomku vezane su uz sigurnost Skype klijenta. Da bi Skype komunikacija bila sigurnija preporučuju se sljedeće akcije:

- Pobrinuti se da računalo na kojem se koristi Skype bude očišćeno od *Spyware* i *Adware* programa, crva, virusa kao i od programa za udaljenu kontrolu.
- Korisničko ime i zaporka koji se koriste za pristup Skype sustavu ne smiju se koristiti ni u koju drugu svrhu.
- Korisničko ime koje se koristi za pristup Skype sustavu ne bi trebalo jednostavno odavati identitet korisnika, tj. ne bi trebalo biti izravno povezano s korisnikovim imenom, zanimanjem ili nazivom tvrtke u kojoj radi.
- Korisničko ime i zaporka koji se koriste za pristup Skype sustavu bi se trebali redovito mijenjati ako se Skype koristi za diskusiju o osjetljivim pitanjima. Promjena korisničkog imena otežava potencijalnim napadačima praćenje aktivnosti korisnika dok promjena zaporke skraćuje vrijeme dostupno za izrabljivanje eventualno probijene zaporke.
- Skype korisnici trebali bi pretpostavljati da Skype komunikacija može u bilo kojem trenutku postati nedostupna te bi trebali uvijek imati rezervne načine komuniciranja.
- Ne treba uvijek vjerovati da je osoba koja se predstavlja kao određeni Skype korisnik danas ista osoba koja se tako predstavljala jučer. Moguće je da netko sjedi za računalom te osobe i koristi računalo bez dozvole stvarnog vlasnika ili da je netko ukrao korisnikov identitet. Uvijek treba pokušati neovisno o Skype-u verificirati identitet osobe s kojom se komunicira, pogotovo ako se namjerava razmjenjivati osjetljive podatke.
- Iako Skype tvrdi da se njihovim sustavom za prijenos govorne komunikacije ne može prenijeti virus, nema dokaza za tu tvrdnju. U stvarnosti prepisivanje spremnika u dekoderu govora može napadaču omogućiti pokretanje proizvoljnih naredbi na računalu s kojim je Skype klijent bio u kontaktu. Također Skype se može koristiti za prijenos datoteka koje mogu sadržavati viruse ili *Spyware* programe.
- Iako je Skype razgovor kritpiran on se dekriptira na odredištu. Ne može se utvrditi snima li taj razgovor osoba na odredištu. Korištenje kriptirane komunikacije nije zamjena za pažnju o izgovorenim riječima.

6. Zaključak

Općenito gledano Skype sustav nudi znatno veću razinu sigurnosti nego klasična telefonska linija, ali s druge strane nešto manju razinu sigurnosti nego VoIP sustavi realizirani povrh VPN veza. Budući da nijedan takav VoIP sustav nije toliko raširen i jednostavan za korištenje kao Skype on se nameće kao najčešće rješenje za ostvarenje govorne komunikacije. S druge strane tu je stalna doza sumnje koja proizlazi iz načina realizacije Skype sustava proizišlog iz tehnologije P2P mreža koje su se gotovo uvijek vezale uz dijeljenje podatkovnih sadržaja i to ne uvijek legalnih. Baš zbog tog porijekla i zbog potpune tajnosti detalja implementacije Skype sustava mnogi sumnjaju u sigurnost i pouzdanost Skype mreže i komunikacije koja se njome ostvaruje.
Međutim iskustvo ne govori u prilog tim sumnjama jer do danas nisu otkrivene značajne mane Skype sustava niti je zabilježeno značajnije kompromitiranje Skype komunikacije. Osim jednog pada sustava Skype nisu obilježili sigurnosni skandali pa dok se to ne dogodi on ostaje jedan od sigurnih i jeftinih načina za uspostavu komunikacije.

7. Reference

[1] Analiza rada *Skype* sustava, http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf , rujan 2004.
[2] Sigurnost *Skype*-a, http://www.cs.huji.ac.il/labs/danss/p2p/resources/Skype-security.pdf , siječanj 2005.
[3] Ranjivosti *Skype*-a, http://www.theregister.co.uk/2005/10/25/skype_vuln/ , listopad 2005.