Joonas Kanninen

VoIP ja tietoturva

Tietotekniikan kandidaatintutkielma

30. toukokuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joonas Kanninen

Yhteystiedot: joonas.p.kanninen@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: VoIP ja tietoturva

Title in English: VoIP and security

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 18+0

Tiivistelmä: VoIP-teknologian laajentuvan käytön myötä sen tietoturvasta tulee entistä ajankohtaisempaa. Tämän kirjallisuuskatsauksen tavoitteena on luoda yleinen käsitys VoIP-teknologian sisällöstä, sitä hyödyntävistä hyökkäyskeinoista ja kyseisiä hyökkäyksiä vastustavista puolustuskeinoista. Hyökkäyskeinoihin tutustuessa ilmenee, että muista Internet-sovelluksista tuttuja hyökkäyksiä voidaan toteuttaa myös VoIP:lla. Hyökkäyksissä saatetaan hyödyntää lisäksi VoIP:n omia ominaisuuksia. Vastaavasti hyökkäyksiltä puolustautuessa voidaan hyödyntää sekä muille Internet-sovelluksille kehitettyjä keinoja, että puheen ominaisia piirteitä.

Avainsanat: VoIP, Voice over Internet Protocol, tietoturva

Abstract: As the use of VoIP technology expands, its security becomes increasingly relevant. The purpose of this literature review is to create a general understanding of VoIP technology, attacks utilising VoIP and methods for defending against aforementioned attacks. An examination into the methods of attack reveals that familiar attacks from other Internet applications can be imported to VoIP. Attacks can also utilise VoIP's own properties. Similarly, defence can also utilise methods imported from other Internet applications along with the characteristic properties of speech.

Keywords: VoIP, Voice over Internet Protocol, security

Termiluettelo

IP	Internet Protocol. Verkkokerroksen protokolla.
VoIP	Voice over Internet Protocol.
TCP	Transmission Control Protocol. Kuljetuskerroksen protokolla.
UDP	User Datagram Protocol. Kuljetuskerroksen protokolla
RTP	Real-time Transport Protocol. Sovelluskerroksen protokolla. Käytetään reaaliaikaisen datan lähettämiseen.
ITU	International Telecommunication Union.
ITU-T	ITU Telecommunication Standardization Sector.
IETF	Internet Engineering Task Force.
H.323	ITU-T:n määrittelemä merkinantoprotokolla.
RAS	Registration Admission and Status protocol. H.323:n alainen protokolla käyttäjän hallinnollisiin toimiin.
H.225	H.323:n alainen protokolla puhelun perustamisen ja purkamisen signalointiin.
H.245	H.323:n alainen protokolla terminaalin kykyjen neuvotteluun ja puhelunhallintaan.
SIP	Session Initiation Protocol. IETF:n määrittelemä merkinantoprotokolla.
DoS	Denial of Service. Palvelunestohyökkäys.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys.

Kuviot

Sisällys

1 Johdanto

VoIP-teknologiaa hyödyntävät sovellukset ovat tulleet osaksi monien elämää viimeistään koronapandemian myötä lisääntyneen etätyöskentelyn parissa. Yksi esimerkki tällaisesta sovelluksesta on Zoom, joka ilmestyi pandemian myötä kuin tyhjästä aktiiviseen käyttöön muun muassa koulutuksessa ja yrityksissä. Jo ennen pandemiaa VoIP on ollut aktiivisessa käytössä esimerkiksi Skypen ja Discordin muodossa, joista jälkimmäinen on pandemian myötä laajentanut videopeliharrastajiin keskittyvästä yleisemmäksi keskustelusovellukseksi. VoIP-palveluja tarjoavat myös muun muassa monista älypuhelimista löytyvät WhatsApp ja Telegram. Dantun ym. (2009) mukaan avaintekijöitä yritysten houkuttelemisessa VoIP:n pariin ovat alhaisemmat kustannukset ja suurempi joustavuus. Azad, Morla ja Salah (2018) nimeävät kohtuuhintaisuuden syyksi VoIP:n tilaajamäärien valtavalle kasvulle julkaisuaan edeltäneiden vuosien aikana.

”VoIP (Voice over IP) tarkoittaa puheensiirtoa Internet-protokollaan (IP) perustuvissa verkoissa.” (Karila 2005) Se hyödyntää useita eri osa-alueista vastaavia protokollia, jotka yhdessä mahdollistavat puhelun käymisen kahden tai useamman käyttäjän välillä. Tässä tutkielmassa käsitellään VoIP:tä tietoturvanäkökulmasta, jonka merkitys tulee kasvamaan entistä suuremmaksi VoIP:n käytön lisääntyessä. Luvussa 2 käsitellään joitain VoIP:n käyttämiä keskeisiä protokollia. Luvussa 3 käsitellään neljää hyökkäyskeinoa, jotka hyödyntävät VoIP:tä. Luvussa 4 käsitellään joitain keinoja, joilla luvun 3 hyökkäyskeinoja vastaan voidaan puolustautua.

2 Voice over Internet Protocol

Tässä luvussa käsitellään VoIP:n keskeisiä protokollia. Dantu ym. (2009) luokittelevat VoIP-protokollat laajasti kahteen ryhmään: mediankuljetusprotokollat ja merkinantoprotokollat.

2.1 Median kuljetus

Gooden (2002) mukaan tyypilliset Internet-sovellukset käyttävät TCP/IP -protokollapinoa, kun taas VoIP käyttää RTP/UDP/IP -protokollapinoa. Keskeisin ero TCP:n ja UDP:n välillä on se, että TCP varmistaa pakettien pääsyn perille, tarvittaessa esimerkiksi lähettämällä saman paketin useamman kerran. Goode lisäksi tarkentaa, että TCP/IP ei sovi reaaliaikaiseen viestintään kuten puheen lähettämiseen, koska sen kuittaus/uudelleenlähetys -ominaisuus johtaisi liiallisiin viiveisiin. RTP on sovelluskerroksen protokolla reaaliaikaisen datan kuten äänen lähettämiseen pakettiverkkoa pitkin. RTP:n tukena käytetään myös RTCP-protokollaa, jonka ensisijainen tehtävä on tarjota palautetta RTP:n tarjoaman palvelun laadusta. Tässä tutkielmassa RTP, RTCP, UDP, TCP ja IP -protokollia ei syvemmin käsitellä.

2.2 Merkinanto

Puhelun muodostamiseen, hallitsemiseen ja purkamiseen käytetään erilaisia merkinantoprotokollia. Näistä keskeisimpiä ovat H.323 ja SIP. Karapantazis ja Pavlidou (2009) jakavat merkinantoprotokollan roolin neljään funktioon:

- Käyttäjän paikantaminen: Soittajan tarvitsee ensin löytää soitettavan sijainti.
- Session perustaminen: Soitettava päättää hyväksyykö, hylkääkö vai uudelleenohjaako puhelun.
- Session neuvottelu: Puheluun osallistuvien päätepisteiden pitäisi suostua yhtenäisiin ominaisuuksiin sessiossa.
- Puheluun osallistujien hallinta: Se antaa päätepisteille mahdollisuuden liittyä tai poistua olemassaolevasta sessiosta.

2.2.1 H.323

Aluksi IP-puheluissa käytettiin merkinantoon H.323-protokollaa, jonka ITU-T on määritellyt. Karilan (2005) mukaan ITU:ssa määriteltiin ensin piirikytkentäisiin videoneuvotteluihin H.320-merkinantoprotokolla, jonka pohjalta H.323-protokolla kehitettiin pakettiverkoissa käytettäväksi. H.323 on sarja erilaisia protokollia, jotka tukevat ääni-, video- ja datasovelluksia, kertovat Karapantazis ja Pavlidou (2009). Heidän mukaan se sisältää kolmenlaista vuorovaikutusta, joista ensimmäiseen kuuluu käyttäjän hallinnolliset toimet. Näitä suorittaa RAS (Registration Admission and Status protocol). Toisen vastuulla on puhelun perustamisen ja purkamisen signalointi, joita hoitaa H.225-protokolla. Kolmas käsittelee terminaalin kykyjen neuvottelun ja puhelunhallinnan, jotka hoitaa H.245.

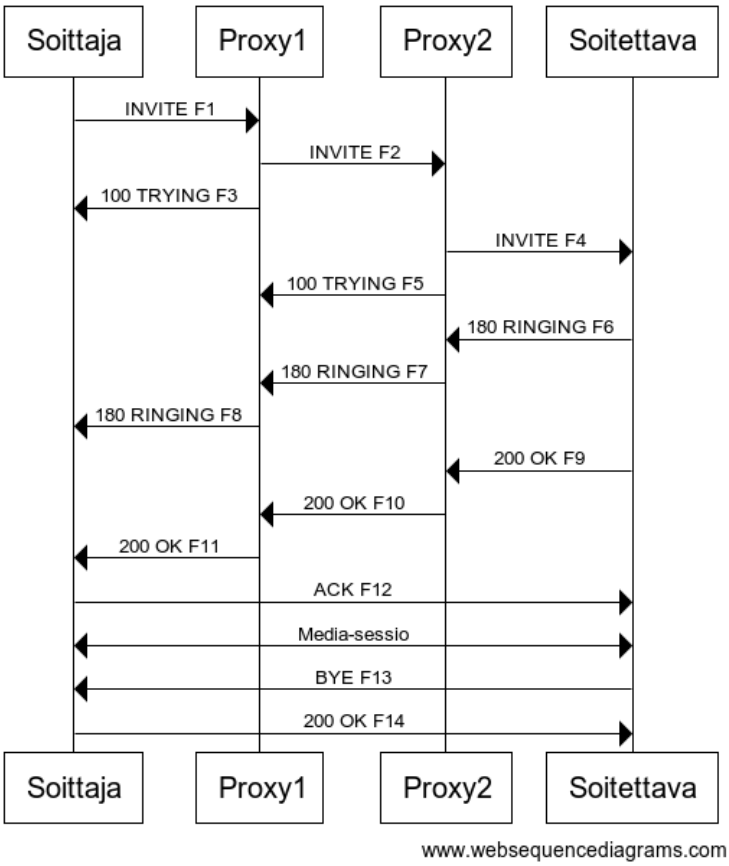
2.2.2 SIP

SIP (Session Initiation Protocol) on IETF:n kehittämä sovelluskerroksen protokolla, joka voi muodostaa, hallita ja purkaa multimediasessioita. Sillä voi myös kutsua käyttäjiä olemassaoleviin sessioihin. Rosenbergin ym. (2002) mukaan se tukee viittä multimediasessioiden muodostuksen ja purkamisen osa-aluetta:

- Käyttäjän paikantaminen: Viestintään käytettävän kohdejärjestelmän määrittäminen.
- Käyttäjän saatavuus: Soitetun osapuolen kommunikaatiohalukkuuden selvittäminen.
- Käyttäjän kykenevyys: Käytettävien median ja mediaparametrien määrittäminen.
- Session perustaminen: Soittaminen, sessioparametrien määritteleminen soitetulle ja soittavalle osapuolelle.
- Session hallinta: Sessioiden siirron ja purkamisen sisällyttäminen, sessioparametrien muokkaaminen ja palveluiden kutsuminen.

”WWW-ohjelmoijat on helppo kouluttaa SIP-ohjelmointiin.” (Karila 2005, s. 28) Yksi syy tähän on se, että SIP on syntaksiltaan samanlainen kuin WWW:ssä käytetty HTTP (Hypertext Transfer Protocol).

SIP-verkosto koostuu SIP-domaineista. Näistä jokainen sisältää ainakin välityspalvelimen (proxy) ja rekisterinpitäjän (registrar). SIP-domainista voi myös löytyä muita elementtejä, kuten esimerkiksi uudelleenohjauspalvelin.



Kuvio 1. Esimerkki SIP-session perustamisesta

Kuviossa 1 on esimerkki SIP-session perustamisesta. Kuvion Soittaja on rekisteröitynyt Proxy1-nimiselle välityspalvelimelle ja Soitettava on rekisteröitynyt Proxy2-nimiselle välityspalvelimelle. Soittaja ei soittaessaan tiedä Soitettavan tai tämän välityspalvelimen sijaintia, joten se lähettää INVITE-viestin häntä palvelevalle Proxy1-palvelimelle. Proxy1 selvittää Proxy2:n sijainnin esimerkiksi DNS-haun avulla ja ohjaa INVITE-viestin Proxy2:lle, joka ohjaa sen edelleen Soitettavalle. Soitettavan SIP-laite lähettää 180 RINGING-vastauksen takaisin Soittajalle ja vastatessaan lähettää perään 200 OK -viestin. Tässä kohtaa Soittaja ja Soitettava tietävät toistensa sijainnit, joten Soittaja lähettää kuittauksen suoraan Soitettavalle ja puhelu alkaa. Puhelun lopettaessaan Soitettava lähettää Soittajalle BYE-viestin, jonka Soittaja kuittaa ja puhelu päättyy. Yksityiskohtaisempi selitys löytyy dokumentista RFC3261 (Rosenberg ym. 2002, s.12 alkaen).

3 Hyökkäyskeinoja

Tässä luvussa käsitellään neljää kirjallisuudessa esiintynyttä hyökkäyskeinoa, joissa VoIP-teknologiaa voidaan hyödyntää.

3.1 Palvelunestohyökkäykset

Palvelunestohyökkäyksessä (DoS, Denial of Service) tarkoituksena on estää tai rajoittaa oikean käyttäjän pääsyä palveluun tai resursseihin. ”DoS-hyökkäykset muodostavat ehkä suurimman uhan yritysten VoIP-systeemeihin.” (Phithakkitnukoon, Dantu ja Baatarjav 2008, suomennos oma) Kohteena voisi olla esimerkiksi verkkosivu, tietokanta tai jokin kriittinen osa VoIP-infrastruktuuria. Hajautetussa palvelunestohyökkäyksessä (DDoS, Distributed Denial of Service) hyökkäys tulee samanaikaisesti usealta eri lähettäjältä, jolloin esimerkiksi yksittäisen lähetysosoitteen estäminen ei pysäyttäisi koko hyökkäystä.

VoIP-infrastruktuuriin hyökätessä kohteena voi olla esimerkiksi SIP-välityspalvelin. Sen tehtävänä on ohjata esimerkiksi jonkin yrityksen lähettämiä tai vastaanottamia SIP-paketteja eteenpäin niiden vastaanottajalle. Yksi SIP:n tehtävistä on aloittaa puhelu soittajan ja soitettavan välillä. Palvelunestohyökkäyksen estäessä pääsyn SIP-välityspalvelimelle eivät kyseistä palvelinta käyttävät käyttäjät kykenisi siis soittamaan tai vastaanottamaan uusia VoIP puheluja lainkaan, ellei heillä ole käytössään jotain vaihtoehtoista reittiä merkinannolle. Sisalem, Kuthan ja Ehlert (2006) jakavat SIP-palvelimiin kohdistuvien hyökkäysten lähestymistavat kahteen kategoriaan:

- Väsytyshyökkäykset (engl. brute force): SIP-palvelimelle muodostetaan suuri määrä uniikkeja sessioita, jotka kuluttavat palvelimen rajallista muistia.
- Rikkinäiset sessiot (engl. broken sessions): Väsytyshyökkäyksissä muistia kuluu vain vuorovaikutuksen ajan. Muistin kulutusta voidaan tehostaa muodostamalla vain osittainen sessio. Hyökkäyksen kohteen ollessa tilallinen (engl. stateful) SIP-palvelin, palvelin ylläpitää session tilaa ja jää odottamaan vastaanottajan vastausta. Jos vastausta ei tule, palvelin joutuu ylläpitämään tilaa ainakin 3 minuuttia samalla kun se yrittää uudelleenlähettää viestiään.

3.1.1 SIP INVITE Flooding

Rosenberg ym. (2002, s. 27) ovat määritelleet SIP:lle kuusi erilaista metodia: REGISTER, INVITE, ACK, CANCEL, BYE ja OPTIONS. REGISTERiä käytetään yhteystietojen rekisteröintiin, INVITE, ACK ja CANCEL käytetään session perustamiseen, BYE session purkamiseen ja OPTIONS kykyjen tiedustelemiseen. Erilaisissa laajennuksissa voidaan myös määritellä muita metodeja. ”INVITE ja OPTION ovat SIP -protokollan ainoat metodit, jotka aloittavat session.” (Hussain ja Naıt-Abdesselam 2011, suomennus oma, OPTION oletettavasti viittaa OPTIONS-metodiin.) Käytännössä tämä tarkoittaa sitä, että välityspalvelin tai viestin vastaanottajan laite joutuvat reagoimaan jokaiseen INVITE tai OPTIONS -viestiin, mikä kuluttaa resursseja. Esimerkiksi ennen session perustamista lähetettyihin ACK-viesteihin ei reagoitaisi mitenkään, sillä palvelin tai vastaanottaja eivät odottaisi kuittauksia elleivät ne ole lähettäneet jotain kuitattavaa. INVITE-viestiin palvelin reagoisi aiemmin esillä olleen kuvion 1 mukaisesti ohjaamalla viestin vastaanottajalle, jonka laite alkaisi esimerkiksi soimaan ilmoittaakseen käyttäjälle puhelusta. Hyökkääjä voisi samanaikaisesti lähettää ison määrän INVITE-viestejä esimerkiksi joko yhdelle vastaanottajalle, tai useammalle samaa välityspalvelinta käyttävälle käyttäjälle. Käyttäjän näkökulmasta tilannetta voisi visualisoida esimerkiksi seuraavanlaisesti:

- Yrityksellä on toimisto, jossa toimii kymmentä puhelinta päivystämässä kolme työntekijää.
- Päivystäjien tehtävänä on muun muassa sopia puhelimen välityksellä tavaran myynnistä ja kuljetuksista.
- Yhtäkkiä kaikki kymmenen puhelinta alkavat soimaan samanaikaisesti.
- Puheluun vastattaessa se katkeaa ja puhelin alkaa soimaan uudestaan.

Niin kauan kuin tilanne jatkuu, toimisto ei välttämättä pysty vastaanottamaan tai aloittamaan yhtäkään oikeaa puhelua, mikä olisi yrityksen toiminnan kannalta haitallista.

3.2 Fraasintunnistus

Wright ym. (2008) ovat kehittäneet menetelmän tunnistaa puhuttuja fraaseja salatuista VoIP-paketeista, joiden audio on koodattu käyttämällä muuttuvan bittinopeuden koodekeita. Koo-

dekki valikoi jokaiselle paketille sopivan bittinopeuden saavuttaakseen sopivan tasapainon äänenlaadun ja verkon kaistanleveyden välillä. Tämä pienentää liikkuvan datan määrää huomattavasti samalla tiputtaen laatua vain vähän jos ollenkaan. Koska lopullinen bittinopeus perustuu koodattuun audioon, on bittinopeuksien perusteella mahdollista kääntäen selvittää alkuperäistä audiota. Menetelmän tehokkuuden arvioimiseen on määritelty kaksi mittaria: precision ja recall. Precision mittaa todennäköisyyttä, että raportoitu osuma on oikea. Recall mittaa todennäköisyyttä, että algoritmi löytää haetun fraasin, kun salattu puhe sisältää kyseisen fraasin. Ihanteellisessa hakualgoritmissa molemmat arvot olisivat mahdollisimman lähellä lukua 1.0, joka vastaa 100% todennäköisyyttä. Wrightin ym. tulosten mukaan menetelmä saavuttaa keskimäärin arvot 50% (recall) ja 51% (precision). Joitain fraaseja tunnistaessa arvot ylittävät 90%. Noin 50% todennäköisyys saattaa kuulostaa matalalta, mutta se koskee salattua puhetta, jota saatetaan käytännössä pitää täysin murtamattomana.

3.3 Roskaposti

Quittek ym. (2008) määrittelevät roskapostin (engl. spam, Spam over Internet Telephony) ei-toivottuina Internet-puheluina. Heidän mukaansa ei-toivottuja puheluita ilmenee jo perinteisessä puhelinverkossa pääosin puhelinmyyjien toteuttamana, mutta niiden määrää rajoittaa perinteisen puhelun suhteellisen korkea hinta. Rosenbergin, Jenningsin ja Petersonin (2008, s. 5) mukaan SIP:tä hyödyntävän roskapostin lähettäminen on neljä suuruusluokkaa halvempaa, kuin perinteiset puhelinmyyjien soitot. Roskapostia lähetettäessä Internetin välityksellä kustannuksia voidaan myös ulkoistaa saastuttamalla kolmansien osapuolten laitteita viruksilla, jolloin roskapostista voi tulla lähettäjän kannalta lähes ilmaista. Lähetys voidaan toteuttaa perinteiseen tyyliin, jossa soittaja henkilökohtaisesti puhuu kohteelle, tai esimerkiksi levittämällä etukäteen äänitettyä puhetta isona massana.

3.4 Kalastelu

Hong (2012) jakaa kalasteluhyökkäyksen (engl. phishing) kolmeen vaiheeseen:

1. Mahdolliset uhrit saavat syöttiviestin.
2. Uhri toteuttaa viestissä ehdotetun toimenpiteen esimerkiksi menemällä väärennetylle

verkkosivulle, asentamalla haittaohjelman tai vastaamalla arkaluontoisilla tiedoilla.

3. Rikollinen muuttaa varastetun informaation rahaksi.

Hong jatkaa, että suurin osa sähköpostia käyttävästä kalastelusta hyödyntää sosiaalisia tekniikoita huijatakseen loppukäyttäjiä. Esimerkkeinä annetaan kiireellisyyden välittäminen huomion harhauttamiseksi ja ahneuteen sekä muihin tunteisiin vetoaminen. Sähköpostin tekstimuotoon verrattuna puheeseen sisältyy paljon enemmän tunnedataa, jota voidaan hyödyntää uhrin tunteisiin vetoamiseen. Esimerkiksi kiireellisyyttä voidaan luoda esiintymällä vihaisena esimiehen esimiehenä ja tunteisiin voidaan vedota esiintymällä itkua pidättelevänä lapsena.

Käynnissä oleva puhelinkeskustelu luo jo itsessään erilaisen kiireellisyyden tunteen kuin sähköposti. Sähköpostia saatetaan pitää luonnostaan alemman kiireellisyyden kommunikaatiovälineenä, jossa odotettu reaktioaika on kiireimmillään vastaanottopäivän aikana. Tyypillisessä puhelinkeskustelussa molemmat osapuolet ovat samanaikaisesti läsnä vähintäänkin uhrin näkökulmasta. Tällöin normaaliin käytökseen kuuluu se, että hyökkääjä sanoo sanottavansa ja jää sitten odottamaan vastausta. Jos hyökkääjän ehdottama toimenpide vaatisi normaalisti tarkoin harkittua päätöksentekoa, saattaa uhri jäädä hetkeksi miettimään, mutta tilanne jää silti päälle. Puhelussa hyökkääjä voi myös pyrkiä lisäämään uhriin kohdistuvaa painetta esimerkiksi aggressiivisella hengittämisellä tai etenevästi hankaloituvalla itkun pidätyksellä.

4 Puolustuskeinoja

Tässä luvussa käsitellään kolmea keinoa, joita voidaan hyödyntää edellisen luvun hyökkäyksiltä puolustautuessa.

4.1 SIP-otsikon muokkaus

SIP-rekisterinpitäjä ylläpitää tietokantaa käyttäjistä ja heidän senhetkisistä IP-osoitteista, jotka se saa käyttäjien lähettämistä REGISTER-viesteistä. Hussain ja Naıt-Abdesselam (2011) ehdottavat, että REGISTER-viestiin voitaisiin lisätä otsikkokenttä ”Critical Number”. Sen arvona oleva luku kuvaisi suurinta määrää soittajia, jotka käyttäjä kykenee käsittelemään helposti. Jos käyttäjään kohdistuvien viestien määrä on pienempi tai yhtä suuri kuin käyttäjän CN (Critical Number), välityspalvelin ohjaa saamansa INVITE-viestit normaaliin tapaan käyttäjälle. Jos viestien määrä on suurempi, se voi esimerkiksi laittaa soittajan jonoon tai kokonaan estää puhelun. Tällöin käyttäjään kohdistuva palvelunestohyökkäys ei kykenisi ylikuormittamaan tämän VoIP-laitetta.

Oikea soittaja saattaisi silti joutua odottamaan jonossa pitkään, mutta hän kuitenkin pääsee ennemmin tai myöhemmin perille, kunhan välityspalvelin kykenee jatkamaan toimintaansa. Oikeiden soittajien jonotusta voisi yrittää helpottaa esimerkiksi päästämällä heidät suoraan jonon eteen tai kehittämällä jonkinlaisen priorisointialgoritmin jonotusjärjestelmän tueksi.

4.2 VoIP-pakettien täydentäminen

Wright ym. (2008) ehdottavat fraasintunnistuksen ehkäisyyn yhdeksi keinoksi VoIP-pakettien täydentämisen yhtenäiseen pituuteen. Täydentäessä paketit 128 bitin monikertoihin fraasintunnistuksen tehokkuus sai arvot 0.15 (recall) ja 0.16 (precision). 256 bitin monikerroilla molemmat arvot olivat 0.04. Ilman täydentämistä vastaavat arvot olivat keskimäärin 0.5 ja 0.51, joten täydentämisellä on lupaava vaikutus. Vaikutuksen hinta on suurempi kaistanleveyden kulutus.

4.3 Käyttäjien todennus

Yksi keino roskapostina lähtevien VoIP-puheluiden estämiseen on puhelun osapuolten todentaminen. Kun puhelun muodostaminen vaatii ensin soittajan identiteetin todentamisen, voidaan roskapostia tuottavat käyttäjät lisätä esimerkiksi johonkin tietokantaan ja jatkossa estää automaattisesti. Kun soittokelpoisia identiteettejä on käytössä rajallinen määrä, roskapostin lähettäjä ei voi vain luoda sadoittain uusia identiteettejä toimintansa jatkamiseen.

Todentamista voidaan hyödyntää myös kalasteluhyökkäysten estämiseen. Suurena massana lähetettäviin yleisiin kalastelupuheluihin voidaan puuttua samalla tavalla kuin roskapostiin. Tarkemmin kohdennetuissa kalasteluhyökkäyksissä ilman todentamista tai muuta vastaavaa esimerkiksi yrityksen toimitusjohtajaa esittävän hyökkääjän tarvitsee vain saada uhri uskoteltua hänen identiteetistään, mikä saattaa olla hyvinkin helppoa ottaen huomioon, että uhri ei välttämättä tiedä työpaikkansa ylimmästä johdosta muuta kuin nimet ja heidän paikkansa yrityksen hierarkiassa. Todennuksen kanssa hyökkääjän tarvitsisi huijata hyökkäysten estoon varta vasten luotua laitteistoa, mikä saattaa käytetyistä todentamiskeinoista riippuen olla hyvin hankalaa tai jopa mahdotonta.

4.3.1 TAES

Hou, Han ja Novak (2020) ovat ehdottaneet soittajien todentamiseen TAESia, jonka nimi vaikuttaisi tulevan lyhenteenä kuvauksesta ”Two-factor Authentication with End-to-End Security”. Se hyödyntää kahta todennusmekanismia: allekirjoituksen todentaminen äänikanavaa pitkin ja puhujan tunnistaminen. Ensimmäinen mekanismi varmistaa, että soittaja on numeronsa omistaja. Toinen mekanismi varmistaa soittajan identiteetin. Siinä puhujan äänenjäljen (engl. voice-print, ilmeisesti puheversio sormenjäljistä) tunnusomaiset parametrit sarjallistetaan ja lisätään digitaaliseen todistukseen. Samalla samojen parametrien avulla luodaan avain todistuksen salaamiseen. Teoksen julkaisuhetkellä puhuja on onnistuttu tunnistamaan 72% todennäköisyydellä. Tämä tulee luultavasti paranemaan sitä mukaan, kun TAESia kehitetään pidemmälle.

5 Yhteenveto

Tässä tutkielmassa tutustuttiin alustavasti neljään VoIP:tä hyödyntävään hyökkäyskeinoon: palvelunestohyökkäyksiin, fraasintunnistukseen, roskapostiin ja kalasteluun. Näistä fraasintunnistus on mielenkiintoinen, koska sillä on mahdollista lähes kokonaan kiertää pakettien salaus. Palvelunestohyökkäykset, roskaposti ja kalastelu taas tulevat todennäköisesti kasvamaan entistä suuremmiksi ilmiöksi sitä mukaan, kun VoIP-teknologian kehityksen myötä sen käytöstä tulee entistä kustannustehokkaampaa. Tutkielmassa myös käsiteltiin edellä mainituille hyökkäyskeinoille vastineeksi kolmea puolustuskeinoa, joista kaksi ensimmäistä ovat sen verran yksinkertaisia, että jopa harrasteleva ohjelmoija kykenisi ne toteuttamaan. Valitettavasti tämän tutkielman käsittelemät puolustuskeinot eivät yksinään riitä estämään kaikkia VoIP:n tietoturvaongelmia, eivätkä välttämättä edes kaikkia tässä tutkielmassa esiteltyjä ongelmia. Tutkielma kuitenkin antaa alustavan esimerkin siitä, mitä tietoturvaongelmia VoIP:stä voi löytyä ja miten niitä vastaan voi lähteä puolustautumaan.

Yksi hyödyllinen tutkimusaihe tulevaisuuden kannalta voisi olla VoIP-pakettien täydentäminen fraasintunnistuksen ehkäisemiseksi. Sitä voidaan kaistanleveyttä uhraamalla ehkäistä jo hyvin, mutta jatkotutkimuksesta saattaisi syntyä jokin keino, jolla samat hyödyt saadaan aikaiseksi tehokkaammalla kaistanleveyden kulutuksella.

Lähteet

Azad, Muhammad Ajmal, Ricardo Morla ja Khaled Salah. 2018. “Systems and methods for SPIT detection in VoIP: Survey and future directions”. *Computers & Security* 77:1–20. https://doi.org/10.1016/j.cose.2018.03.005.

Dantu, Ram, Sonia Fahmy, Henning Schulzrinne ja Joao Cangussu. 2009. “Issues and challenges in securing VoIP”. *computers & security* 28 (8): 743–753. https://doi.org/10.1016/j.cose.2009.05.003.

Goode, Bur. 2002. “Voice over internet protocol (VoIP)”. *Proceedings of the IEEE* 90 (9): 1495–1517. https://doi.org/10.1109/JPROC.2002.802005.

Hong, Jason. 2012. “The state of phishing attacks”. *Communications of the ACM* 55 (1): 74–81. https://doi.org/10.1145/2063176.2063197.

Hou, Dai, Hao Han ja Ed Novak. 2020. “TAES: Two-factor Authentication with End-to-End Security against VoIP Phishing”. Teoksessa *2020 IEEE/ACM Symposium on Edge Computing (SEC),* 340–345. IEEE. https://doi.org/10.1109/SEC50012.2020.00049.

Hussain, Intesab, ja Farid Naıt-Abdesselam. 2011. “Strategy based proxy to secure user agent from flooding attack in SIP”. Teoksessa *2011 7th International Wireless Communications and Mobile Computing Conference,* 430–435. IEEE. https://doi.org/10.1109/IWCMC.2011.5982572.

Karapantazis, Stylianos, ja Fotini-Niovi Pavlidou. 2009. “VoIP: A comprehensive survey on a promising technology”. *Computer Networks* 53 (12): 2050–2090. https://doi.org/10.1016/j.comnet.2009.03.010.

Karila, Arto T. 2005. *Internet-puhelut (VoIP): selvitys.* Liikenne-ja viestintäministeriö. http://urn.fi/URN:ISBN:952-201-332-3.

Phithakkitnukoon, Santi, Ram Dantu ja Enkh-Amgalan Baatarjav. 2008. “Voip security—attacks and solutions”. *Information Security Journal: A Global Perspective* 17 (3): 114–123. https://doi.org/10.1080/19393550802308618.

Quittek, Juergen, Saverio Niccolini, Sandra Tartarelli ja Roman Schlegel. 2008. “On spam over internet telephony (SPIT) prevention”. *IEEE Communications Magazine* 46 (8): 80–86. https://doi.org/10.1109/MCOM.2008.4597108.

Rosenberg, Jonathan, Cullen Jennings ja J Peterson. 2008. *The session initiation protocol (SIP) and spam.* Tekninen raportti. RFC 5039, January. https://doi.org/10.17487/RFC5039.

Rosenberg, Jonathan, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley ja Eve Schooler. 2002. *RFC3261: SIP: session initiation protocol.* https://doi.org/10.17487/RFC3261.

Sisalem, Dorgham, Jiri Kuthan ja Sven Ehlert. 2006. “Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms”. *IEEE Network* 20 (5): 26–31. https://doi.org/10.1109/MNET.2006.1705880.

Wright, Charles V, Lucas Ballard, Scott E Coull, Fabian Monrose ja Gerald M Masson. 2008. “Spot me if you can: Uncovering spoken phrases in encrypted voip conversations”. Teoksessa *2008 IEEE Symposium on Security and Privacy (sp 2008),* 35–49. IEEE. https://doi.org/10.1109/SP.2008.21.