Nykyajan vakoiluohjelmat ja ”Discord-newspeakin” ongelma

Digitaalisen viestinnän historia

Ihmiskunnan tunnetun historian aikana viestejä on välitetty pitkien matkojen päähän monenlaisilla keinoilla. Ennen sähkön keksimistä viestejä on välitetty mm. savumerkein ja kirjekyyhkyjen kuljettamana. Sähkön keksimisen jälkeen yleistyivät sähkötys morseaakkosilla ja ihmisäänen kuljettaminen analogisena äänisignaalina – jälkimmäinen viestintätapa on yhä yleisessä käytössä ja tunnetaan nimellä ”*puhelin*”. Sähkötyksen merkitys viestinnässä on käytännössä hävinnyt digitaalisten automaattisesti viestejä välittävien tietokoneiden yleistyttyä.

Ensimmäiset digitaaliset viestintäohjelmat käyttivät yksinkertaisia protokollia ja usein asiakasohjelmaksi riitti pelkkä telnet-ohjelma. Jo vuonna 1982 kehitettiin yhä laajassa käytössä oleva SMTP-protokolla, jolla välitetään sähköpostiviestejä palvelimien välillä. Suomalaisen Jarkko Oikarisen vuonna 1988 kehittämä IRC-protokolla muodostui ensimmäiseksi laajempaan käyttöön vakiintuneeksi pikaviestiprotokollaksi.

Teknisten termien määritelmiä

Asiakasohjelma: Ohjelma, jonka käyttäjä asentaa tietokoneellensa palvelua käyttääkseen.

Palvelinohjelma: Ohjelma, joka asennetaan palvelintietokoneeseen, jonka kautta palvelun käyttäjät ovat yhteydessä toisiinsa.

Protokolla: Säännöstö, jota käyttäen asiakas- ja palvelinohjelmat vuorovaikuttavat keskenään.

Tietosisältö: Hyötykuorma, joka siirretään asiakkaalta toiselle protokollan avulla – kommunikaatio-ohjelman tapauksessa useimmiten käyttäjältä toiselle osoitettu viesti.

Päästä päähän -salaus: Tietosisältö salataan sen lähettävän asiakasohjelman toimesta ja salaus puretaan vasta vastaanottavan asiakasohjelman toimesta niin, että viestiä välittävällä palvelimella ei ole mahdollisuutta nähdä tietosisältöä salaamattomana.

Pikaviesti: Suomennos englanninkielisestä sanasta ”chat”.

Siltabotti: Botti, joka välittää viestejä kahden tai useamman eri keskustelukanavan välillä. Eri keskustelukanavat voivat käyttää eri protokollaa – botti voi välittää viestejä esimerkiksi IRC-kanavan ja Matrix-kanavan välillä.

Suljettujen ja vapaiden pikaviestimien erot

Ehkä merkittävin ero suljettujen ja vapaiden pikaviestimien välillä on nimen käyttötavassa. Suljettujen pikaviestimien nimi assosioidaan tavallisesti asiakasohjelmaan, kun taas vapaissa vaihtoehdoissa pikaviestimen nimellä tarkoitetaan itse protokollaa. Hyviä käytännön esimerkkejä ovat tunnetut pikaviestimet IRC ja Mumble, joista molemmille on olemassa useita asiakasohjelmia

eikä protokollan mukaan nimettyä asiakasohjelmaa ole ensinmainitulle edes olemassakaan. Voisi yleistäen sanoa, että vapaat pikaviestimet ovat ensisijaisesti vain protokollia, jotka toteutetaan joko palvelin- tai asiakasohjelman kontekstissa.

Suljetuissa pikaviestimissä protokolla on yleensä kokonaan dokumentoimaton ja sen vuoksi vaihtoehtoisten asiakasohjelmien tekeminen on hankalaa ja työlästä. Vaihtoehtoisten asiakasohjelmien käyttö saattaa olla myös kielletty käyttöehdoissa, kuten esimerkiksi Discordin tapauksessa on. Suljettu ja dokumentoimaton protokolla aiheuttaa sen, että kyseinen pikaviestin toimii käytännössä vain niillä laitteilla, joille virallinen asiakasohjelma on julkaistu. Vapaissa pikaviestimissä protokolla on avoin ja dokumentoitu, minkä ansiosta oman asiakasohjelman kirjoittaminen on helppoa. Yleisimpiin vapaisiin pikaviestimiin löytyykin asiakasohjelma käytännössä joka laitteelle.

Dokumentoimaton protokolla vaikeuttaa siltabottien tekemistä ja usein siltabotit ovat kokonaan kielletty suljettujen pikaviestimien käyttöehdoissa. Yleensä suljetun pikaviestimen bisnesideaan kuuluukin merkittävänä osana käyttäjien sulkeminen rajojensa sisään. Suljettuihin pikaviestimiin ei muutamia harvoja poikkeuksia lukuunottamatta pysty tekemään omaa palvelinta, vaan kaikki viestintä tapahtuu pikaviestimen kehittäjien ylläpitämän keskuspalvelimen kautta, mikä tekee suljetuista pikaviestimistä alttiimpia palvelunestohyökkäyksille ja totalitaaristen hallintojen harjoittamalle sensuurille.

Sanojen merkitysten muuttuminen markkinoinnissa

Suurin osa omisteisista suljetun lähdekoodin tietokoneohjelmista on voittoa tavoittelevien yritysten tuottamia. Markkinointi ei useinkaan ole aivan rehellistä – varsinkaan, jos kyse on tuotteesta, jonka toimintatapaa keskivertokäyttäjä ei täysin ymmärrä. Sama ilmiö on havaittavissa myös ohjelmistoissa, ja yksi käytetyimmistä valheellisen markkinoinnin keinoista on sanojen merkityksien muuttaminen omia tarkoitusperiä vastaavaksi. Pahimmassa tapauksessa sanojen uudenlainen käyttö vakiintuu vähitellen markkinoinnista yleiseen kielenkäyttöön, mikä on riskinä etenkin teknisen sanaston asiayhteyksissä, joissa markkinoinnin kohderyhmä usein oppii sanalle ensimmäisen merkityksen nimenomaan valheellisesta mainonnasta. Sanojen uusmerkitysten vakiintuminen normaaliin kielenkäyttöön tekee asioista entistäkin hankalampia käsittää.

Tyypillisesti termien harhaanjohtavassa käytössä pyritään latistamaan positiiviseksi miellettyjen sanojen merkityksiä. Esimerkiksi sanoja ”secure” tai ”(tieto)turvallinen” käytetään pikaviestimestä, jossa ei ole päästä päähän -salausta ja jossa kaikki viestit tallennetaan keskuspalvelimelle selkokielisinä – sanan uusi merkitys halutaan siis latistaa tarkoittamaan pelkästään sitä, että palvelimen ja asiakkaan välinen yhteys on salattu. Discord käyttää palvelun sisäisistä ryhmistä nimitystä ”palvelin” (englanniksi ”server”) tarkoituksena luoda mielikuva, että Discordiin voi kuka tahansa tehdä omia palvelimia. Tietenkään sillä ei oikeasti ole mitään tekemistä palvelimen kanssa – palvelin tarkoittaa ja on aina tarkoittanut rautatasolla palvelinohjelmaa ajavaa tietokonetta ja ohjelmistotasolla asiakasohjelmien yhteydenottoja kuuntelevaa ohjelmaa, eikä kumpikaan synny asiakasohjelmasta paria linkkiä klikkaamalla.

Käsitteelliset ongelmat tietoturvasta puhuessa

Viime vuosina etenkin suljetun lähdekoodin ohjelmistojen tietoturva on ollut laajasti otsikoissa. Vakoiluominaisuuksia on paljastunut muiden muassa Microsoftin ja Applen käyttöjärjestelmistä ja huolta on herättänyt maailman suosituimman sosiaalisen median Facebookin toimintansa

rahoittaminen myymällä tietoa käyttäjistään. Matkapuhelinverkkoja 5G-taajuuksille laajennettaessa moni maa boikotoi kiinalaista laitetoimittajaa Huaweita vakoiluepäilyjen vuoksi.

Keskustelu tietoturvasta ajautuu usein sivuraiteille tai käy kokonaan mahdottomaksi, koska sanojen merkitykset eivät ole selviä. Tietoturvaohjelmistoja myyvillä yrityksillä on jo kauan ennen ”discord-newspeakin” aikakautta ollut tapana markkinoida tuotteitaan kuin tietoturvaa olisi mahdollista ostaa kaupasta, mikä on jo ennestään tehnyt valistamisesta vaikeaa.

Pikaviestimien tietoturvan ymmärtäminen on mahdotonta, jos palvelimen käsite on epäselvä. Oleellisessa osassa ovat *salauksen* lisäksi se, onko *palvelin* luotettu vai ei, ja jos ei ole, niin näkeekö se *asiakkaiden* väliset viestit. Discord-newspeakin takia tyypillinen keskustelu tietoturvasta noudattaa seuraavaa kaavaa:

1: Ollakseen tietoturvallinen kommunikaatio-ohjelman pitää salata viestit käyttäjien välillä.

2: Discord käyttää salattua yhteyttä. Discord on siis tietoturvallinen.

1: Discord ei ole tietoturvallinen, koska sen salaus ei ole käyttäjien välinen. Salaus on vain käyttäjän ja palvelimen välillä ja viestit tallentuvat palvelimelle selkokielisenä. Todennäköisesti kaikki sinne kirjoittamasi viestit myydään mainostajien käyttöön.

2: Tein Discordiin oman *palvelimen* johon luotan, koska se on minun oma palvelin ja omaan palvelimeen voi luottaa! Kaiken lisäksi *palvelimen* tekeminen Discordiin on erittäin helppoa, sillä se onnistuu parilla klikkauksella clientistä! Ainoastaan ajastaan jälkeen jääneisiin paskaviestimiin pitää tehdä palvelin asentamalla joku ohjelma ja jättämällä tietokone päälle!

Mikä meni vikaan? Keskusteluosapuoli **2** tietää, että asiakas- ja palvelinohjelman välinen salaus on tietoturvan kannalta riittävä, jos palvelin on luotettu. **2** luulee perustamaansa Discord-ryhmää palvelimeksi ja päättelee sen perusteella, etteivät viestit voi päätyä ulkopuolisten käsiin. Discord kutsuu palvelun sisäisiä ryhmiä valheellisesti ”palvelimiksi”.

Muita esimerkkejä ”Discord-newspeakista” ja valheellisesta markkinoinnista

- Discord ilmoittaa webbisivuillansa käyttävänsä vain WebRTC- ja SSL-protokollaa ja pyrkii luomaan mielikuvan, että protokolla varsinaisena asiakas- ja palvelinohjelman välisenä säännöstönä on *vanhanaikainen*. Discordissa ei siis virallisesti ole mitään protokollaa asiakkaan ja palvelimen välillä. Sen perusteella jää epäselväksi, miten asiakkaan ja palvelimen välinen kommunikaatio Discordissa tapahtuu, mutta se on selvää, että Discord toteuttaa asian *modernilla* tavalla.
- Discord on virallisesti ilmoittanut betatestaajilleen, että Discordin asiakasohjelman kaatuilu johtuu siitä, että Discordin ”palvelimia” kohtaan tehdään palvelunestohyökkäyksiä.
- Discordin webbisivuilla on lause ”Discord <3 open source”, jonka perusteella Discordin luullaan yleensä olevan avointa lähdekoodia. Discord ei ole missään vaiheessa julkaissut lähdekoodejaan, eikä sitä ole julkaistu millään avoimen lähdekoodin lisenssillä.
- Useimmat kommunikaatio-ohjelmat markkinoivat itseään monialustaisina ja ”kaikilla laitteilla toimivina”, vaikka todellisuudessa asiakasohjelman saa yleensä vain tietyille Androidin versioille, Applen mobiililaitteille ja Windowsin x86-versiolle.

- Discord markkinoi itseään ”IRCin korvaajana” ja ratsastaa IRC-protokollaan liitetyillä positiivisilla mielikuvilla, jotka eivät päde Discordiin. Discord on myös markkinoinnissaan väittänyt kilpailevan Teamspeak-ohjelmiston palvelimien olevan maksullisia.