Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2014

Aleksi Nurmi

VERKKOPELAAMISEN TIETOTURVA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

2014 | 27

Ohjaaja Pasi Iivonen

Aleksi Nurmi

VERKKOPELAAMISEN TIETOTURVA

Opinnäytetyön aiheena on kertoa verkkopelaamisesta, siihen liittyvistä tietoturvakohdista ja tutkia miten verkossa pelaaminen on kehittynyt nykyaikana. Työssä selitetään mitä verkossa pelaaminen tarkoittaa, mitkä tekijät uhkaavat pelaajien käyttäjätilien eheyttä ja mitkä ovat mahdolliset pelaamiseen kohdistuvat häiriötekijät.

Opinnäytetyössä käytetään lähteinä pääasiassa eri verkkosivustoja ja omaa kokemusta verkkopelaamisesta.

Teoriaosuudessa selvitetään, mitä erilaisia keinoja on olemassa, joilla verkkorikolliset yrittävät anastaa pelaajien käyttäjätilejä, ja käydään läpi näiden toimintatapaa. Lisäksi selvitetään, miten pelitilien tietoturvaa on yritetty parantaa pelifirmojen taholta.

Opinnäytetyössä esitellään myös tietomurtotapauksia, jotka ovat kohdistuneet pelipalveluja ylläpitäviin peliyrityksiin. Osuudessa läpikäydään nykyaikaisten verkkopelien liiketoimintamallia ja miten se kasvattaa pelitilien rahallista arvokkuutta mikromaksujen muodossa sekä vaikutusta rikollisuuden kasvuun.

Työ osoittaa, että oman pelitilinsä turvallisuutta voi parantaa. Sitä ei kuitenkaan pelaaja yksin voi taata vaan vastuu kuuluu myös peliyhtiöille.

ASIASANAT:

Tietoturva, verkkopelaaminen, verkkorikollisuus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data communications

2014 | 27

Instructor Pasi Iivonen

Aleksi Nurmi

ONLINE GAMING SECURITY

The subject of this thesis was to discuss online gaming and security matters relating to it as well as give an overview on how online gaming has developed over the time. The thesis explains what playing games online means and which factors threaten user accounts or possibly disrupt the player's gaming experience.

The source material was mainly based on various Internet sites and personal experience.

The theoretical part presents the various methods cybercriminals use to try steal player user accounts and the way the methods work. In addition this part explains how the game companies have tried to improve their data security.

The thesis also introduces security breach cases where game companies have had their servers attacked. This part also presents the modern type of business model in online games and the way it raises the value of game accounts due to microtransactions and the effect on increasing Internet crimes.

The thesis shows that one can improve the security of his game accounts. However the player is not solely responsible for securing his accounts because part of this responsibility also concerns the game companies.

KEYWORDS:

Data security, online gaming, cybercrime

SISÄLTÖ

KUVAT

LYHENTEET

ADSL	Asymmetric Digital Subscriber Line (ADSL 2014.)
FPS	First Person Shooter (Video game genres 2014.)
ISDN	Integrated Services Digital Network (ISDN - Integrated services digital network 2014.)
MMORPG	Massively Multiplayer Online Role-Playing Game (Video game genres 2014.)
MOBA	Multiplayer Online Battle Arena (Video game genres 2014.)
SRP	Secure Remote Password (Secure remote password protocol 2014.)
SSL	Secure Sockets Layer (SSL – Secure sockets layer 2014.)
SYN/ACK	Synchronized/Acknowledgement (The Cert Division 2014.)

1 JOHDANTO

Opinnäytetyön aihevalinta juurtaa juurensa omasta mielenkiinnostani ja harrastuksestani peleihin ja erityisesti verkossa pelaamiseen. Alkuun oli vaikea keksiä ideaa opinnäytetyön aiheeksi. Todettuani ettei vastaavaa pelaamista käsittelevää työtä löytynyt, päädyin itseäni kiinnostavaan aiheeseen. Lähestyin aiheideaa verkkopelaamisesta tietoturvallisuuden ja verkkopelien kehityksen tutkimisen kannalta.

Nykyaikaisen yhä kehittyvän verkkoliikennetekniikan ja tietokonetekniikan avulla videopelaaminen verkossa on kasvattanut suosiotaan koko ajan ja sillä on suuri markkinaosuus viihdemaailmassa. Pelaaminen ei nykyään ole enää tyypillisesti nuorten miesten harrastus vaan se on ottanut jalansijaa kaikenikäisten ihmisten vapaa-ajanvietossa. Pelejä voi pelata verkkoselaimella, taulutietokoneella, kännykällä, pöytätietokoneella tai pelikonsolilla.

Pelaamisen suuren suosion kasvaminen tuo myös mukanaan lisää rikollisia, jotka yrittävät varastaa tai vahingoittaa käyttäjätilejä. Tarkoitukseni onkin opinnäytetyössä käydä läpi erilaiset pelaajia ja pelialaa uhkaavat tai häiritsevät tekijät ja ilmiöt.

Pohdin työssä myös verkkopelien sisäiseen ekonomiaan liittyviä tekijöitä kuten pelivaluuttojen kauppaamista sekä millaisia yhteiskunnallisia ilmiöitä se voi luoda.

2 VERKKOPELAAMINEN

2.1 Yleistä

Verkkopeli on verkkoyhteyden kautta pelattava videopeli. Se voi tarkoittaa yksin pelattavia pelejä tai monen pelaajan pelejä, jotka yhdistävät pelaajia samalle peliserverille eli palvelimelle pelaamaan yhdessä tai vastakkain. Verkossa pelattiin 90-luvulla käyttäen ISDN-sovittimia yhdistämään puhelinverkon läpi pelipalvelimille. Tämä yhteys oli kuitenkin erittäin hidas, parhaimmillaan vain 56 kilotavua sekunnissa. Lähiverkoissa pelaaminen ei kärsinyt hitaasta nopeudesta ja pelaajat kokoontuivat joskus tietokoneidensa kanssa pelaamaan samaan lähiverkkoon. ADSL-yhteydet alkoivat yleistymään kotitalouksissa 2000-luvun taitteessa ja niiden tuomat jopa 24 megatavun tiedonsiirtonopeudet mahdollistivat nykyaikaisten monen pelaajan verkkopelien yleistymisen.

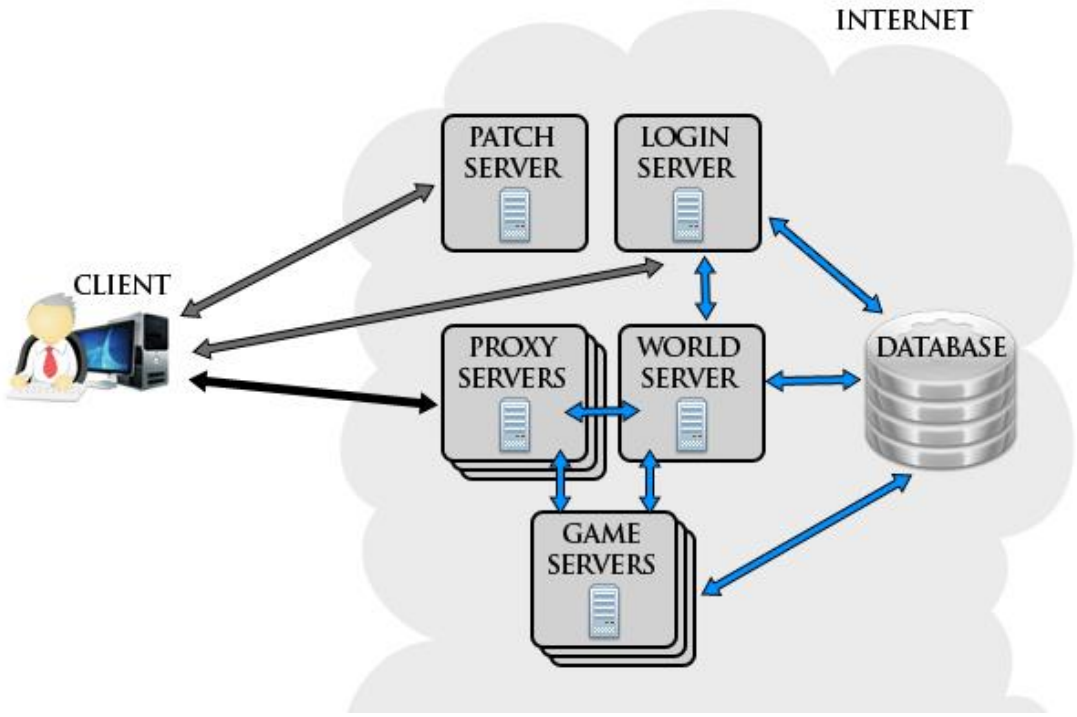
Verkkopelaamisen kuuluvat myös pelikonsolit, kuten Sony PlayStation tai Microsoft Xbox. Ensimmäinen konsoleille luotu verkkoympäristö oli japanilaisen Sega peliyhtiön luoma Sega Meganet vuonna 1990. Konsoliverkkojen tarkoitus on myydä digitaalisessa muodossa pelejä, jakaa pelipäivityksiä sekä tuoda pelaajat yhteen pelaamaan. Nykyään toiminnassa olevat konsoleiden verkot ovat muun muassa 2006 julkaistu Sony PlayStation Network ja Microsoftin Xbox Live, julkaistu 2002. (Online console gaming 2014.)

Verkkomoninpelit voidaan jakaa eri tyyppikategorioihin. Yleisimpiä näistä ovat esimerkiksi MMORPG, FPS ja MOBA. MMORPG tarkoittaa useiden pelaajien roolipelaamista omilla avatareilla suurissa pelimaailmoissa. Roolipeleissä yleensä pääintressinä on oman hahmon kehittäminen paremmaksi. Suosituin MMORPG-tyylinen peli on World of Warcraft, jonka ensimmäinen versio julkaistiin 2004. Se edelleen nauttii monien miljoonien pelaajien suosiosta. FPS on pelaajien välistä sotimista aseilla ensimmäisestä persoonasta kuvattuna. Nykyään suuren suosion saavuttaneet MOBA-pelit tarkoittavat reaaliaikaista strategiataistelua kahden joukkueen välillä. Nämä pelit ovat yleensä kuvattuna

lintuperspektiivistä antaen paremman strategisen näkymän pelikartan tapahtumista.

2.2 Arkkitehtuuri

Yksinkertaisuudessaan verkkopelien palvelinarkkitehtuuri on pelaajien yhdistäminen samalle peliserverille. Tähän sisältyy monta eri vaihetta. Alla olevassa kuvassa 1 on tyypillinen toimintaperiaate käyttäjän yhdistämisestä verkkopeliin.



Kuva 1. Pelipalvelimien arkkitehtuuri. (MMO RPG 2013.)

Pelipalvelimien täytyy palvella yhtäaikaisesti jopa tuhansia pelaajia ja tämä vaatii suuren määrän eri tarkoituksiin määriteltyjä laitteita. Arkkitehtuuriin kuuluu lisäksi palomuureja ja muita suojia hyökkäyksiä tai häiriöitä vastaan, joita kuvassa ei ole esitettynä.

Pelaaja kirjautuu ensin käyttäjätunnuksellaan ja salasanallaan kirjautumispalvelimelle, joka hoitaa ainoastaan tätä toimintoa. Hyväksytyn kirjautumisen jälkeen pelaaja voi tarvittaessa päivittää pelinsä uudempaan versioon. Se tapahtuu päivityksiä varten luodussa serverissä. Nämä kaksi yhteyttä palvelimille ovat väliaikaisia ja katkeavat toiminnon suorittamisen jälkeen.

Seuraavaksi pelaaja yhdistetään välittäjäpalvelimille, jotka kontrolloivat pakettiliikennettä käyttäjien ja varsinaisen peliserverin välillä. Näin itse peliserveri ei kuormitu yhteyksien hallinnasta ja se voi keskittää resurssit pelimaailman ylläpitämiseen. Pelaaja yhdistetään välittäjäpalvelimen kautta varsinaiseen pelimaailmaan. Niin sanottu World Server on ikään kuin peliserveriklusterin yhdistäjä, jonka toimintoja voi olla esimerkiksi pelissä oleva chat-palvelu. Database tarkoittaa kaiken pelissä olevan tiedon tietokantaa, josta palvelimet ammentavat mm. pelimaailman ja muun grafiikan. Mitä suurempi pelaajamäärä, sitä enemmän peli vaatii palvelimia toimiakseen vakaasti. Pelaaja voi joutua odottamaan palvelimelle pääsyä, jos kirjautumispalvelin ruuhkautuu liian suuresta pelaajamäärästä. (MMO RPG 2013.)

3 TIETOTURVAUHAT

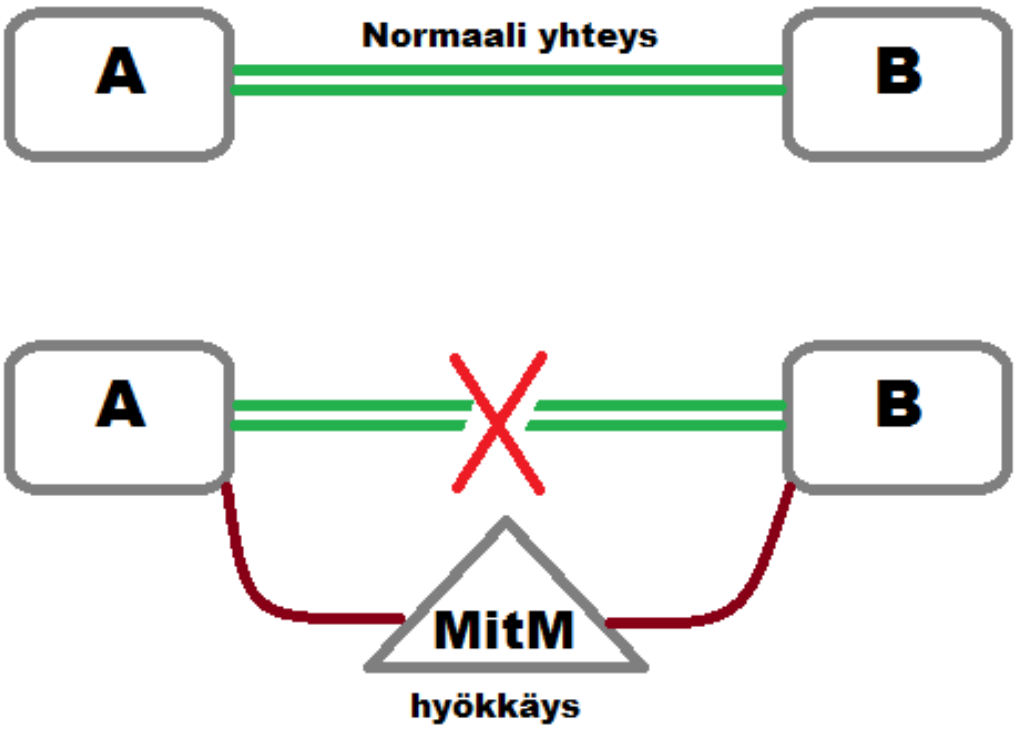
3.1 Tietojenkalastelu

Tietojenkalastelulla tarkoitetaan verkkorikollisten harjoittamaa verkkourkintaa (eng. *phishing*), jolla yritetään kalastella uhrien luottamuksellisia tietoja. Näitä tietoja voivat olla käyttäjien henkilötiedot, luottokorttitiedot sekä käyttäjätilien salasanat. Tavallisesti tietojen tavoittelulla on takana taloudellisen hyödyn saaminen. Urkintaa suoritetaan erilaisilla pikaviestimillä ja sähköposteilla, jotka naamioidaan näyttämään aidoilta ja saapuneeksi luotettavilta lähettäjiltä. Pelitilien käyttäjätunnuksia yritetään kalastella esimerkiksi pelifirmojen logoilla varustetuilla sähköpostiviesteillä, jotka saattavat suoraan pyytää tietoja tai ne sisältävät linkkejä valheellisiin kirjautumissivuihin. Phishing-mailin tunnistaminen onnistuu tutkimalla lähettäjän osoitetta lähdekoodista. Phishing on eniten käytetty keino haalia asiakastietoja verkkopeleissä sen yksinkertaisuuden takia, koska se luottaa uhrin heikkouskoisuuteen ja vähäiseen valppauteen. Vaikka pelitilit eivät itsessään ole välttämättä varastamisen arvoisia pelkkien pelien takia, voi usein tilitietoihin sisältyä pelaajan luottokorttitiedot. (Symantec 2014.)

3.2 Välimieshyökkäys

Välimieshyökkäys eli man-in-the-middle tapahtuu, kun kahden tietokoneen välille tunkeutuu hyökkääjä, joka ikään kuin salakuuntelee näiden välistä tiedonvaihtoa. Hyökkääjä asettuu käyttäjän ja kohteen tietojen välittäjäksi ja yleensä toimii uhrien huomaamatta. Se kerää esimerkiksi käyttäjätunnuksia ja salasanoja teeskennellen aitoa viestin kohdetta ja voi muuttaa kohteelle tarkoitetun dataliikenteen viestien sisältöä omaksi edukseen. Tällaisia hyökkäyksiä vastaan on olemassa verkkoprotokollia kuten SSL, jonka avulla kahden osapuolen välille ei pääse ylimääräisiä ei-todennettuja tahoja. Välimies

voi esimerkiksi asettua kuuntelemaan salaamattomassa Wifi-verkossa olevaa käyttäjää. (Huan-rong ym. 2009, 1464-1470.)



Kuva 2. Välimieshyökkäys.

Kuvassa 2 esiintyy ensin normaali verkkoyhteys kahden laitteen A ja B välillä. Sen alapuolella on yhteys, jonka on välimieshyökkääjä on katkaissut ja luonut uuden yhteyden kulkemaan hänen kauttaan.

3.3 Näppäilyn tallentajat

Näppäilyn tallentajat (eng. *keylogger*) ovat vakoiluohjelmia, joiden tarkoitus on tallentaa kaikki käyttäjän näppäimistön painallukset. Ne tallentavat jokaisen näppäimen painalluksen kryptattuun logitiedostoon ja lähettävät tiedon

eteenpäin verkon välityksellä ulkopuoliselle taholle. Niiden avulla on mahdollista saada käsiin pelitilien kirjautumistiedot ellei käytössä ole kertakäyttöisiä salasanoja. Ne voivat myös tallentaa sähköpostiviestejä tai osoitteita. Ohjelman toiminta on yleensä huomaamatonta. Automaattiset lomakekentän täydentäjät kirjautumisessa estävät haittaohjelman toiminnan, mutta paras keino suojautua on ajaa säännöllisin väliajoin haittaohjelmien poisto-ohjelma. (Keylogger 2014.)

3.4 Palvelunestohyökkäys

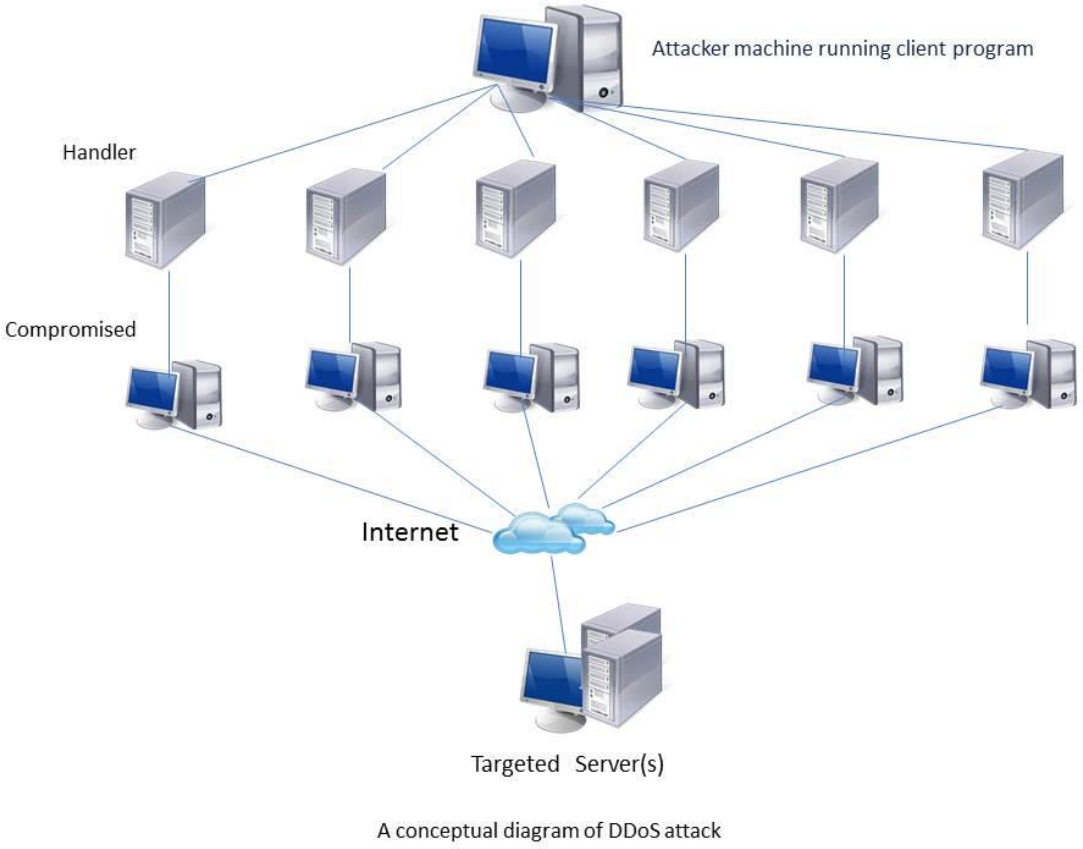
Palvelunestohyökkäys eli DOS on hyökkäys, jonka tarkoituksena on estää uhria pääsemästä käsiksi johonkin palveluun tai resurssiin. Se saattaa ilmetä verkkosivujen latautumisen hitaudella tai internetyhteyden katkeamisella. Hyökkäystapoja on erilaisia. Tulvahyökkäyksessä pyritään käyttämään mahdollisimman paljon uhrin koneen rajallisia resursseja, esimerkiksi tulvaamalla sähköpostipalvelin tuhansilla viesteillä. Toinen hyökkäystyyppi on verkkoprotokollien häiritseminen ja liikenteen ohjaaminen eri reittien kautta tai väärään osoitteeseen.

Yleisin metodi häiritä verkkoliikennettä on SYN-floodaus eli tulvaaminen. Ennen kuin asiakasohjelma ja serveri luovat yhteyden toisiinsa tapahtuu ns. kolmitiekättely. Asiakasohjelma lähettää SYN-paketin, jonka jälkeen palvelin vastaa takaisin lähettämällä SYN/ACK varmistukseksi, että paketti saapui. Asiakasohjelma lähettää vielä varmistuspaketin takaisin palvelimelle. SYN-floodauksessa hyökkääjän tietokone lähettää SYN-paketteja palvelimelle niin paljon, että odottavien yhteyksien lista palvelimella täyttyy. Tämä pakottaa palvelimen nollaamaan yhteydet, joka aiheuttaa yhteyden katkeamisen pelaajan ja peliserverin välillä. (The Cert Division 2014.)

Palvelunestohyökkäyksiä saatetaan käyttää erityisesti kilpailullisissa peleissä toisen pelaajan pois pelipalvelimelta saamiseksi tai jopa häiritsemään lähiverkkoon järjestettyä peliturnausta.

Hyökkäyksen voi toteuttaa yhdellä koneella tai botneteillä. Botnet tarkoittaa monen samankaltaisen internettiin kytketyn ohjelman verkkoa, jotka ohjelmoidaan suorittamaan tiettyjä toimintoja kuten voimakkaita palvelunestohyökkäyksiä. Tällaista hyökkäystä kutsutaan hajautetuksi palvelunestohyökkäykseksi. Botnetia käyttävä hyökkääjä tartuttaa muiden internetkäyttäjien tietokoneita viruksilla ja troijalaisilla ja voi halutessaan hyödyntää näitä tartunnan saaneita koneita eli ns. orjakoneita tehtävissään pommittamaan valittua verkkokohdetta.

Kuvassa 3 on kuvaus tyypillisestä hajautetusta palvelunestohyökkäyksestä eli DDoS:ista. Hyökkääjä käskee ”handler”-koneitaan, jotka voivat olla esimerkiksi kaapattuja webpalvelinkoneita, lähettämään käskyn troijalaisilla saastuneisiin tietokoneisiin. Jokaisen handlerin alaisena voi olla 1000 yksityisen käyttäjän konetta ja ne voivat osallistua hyökkäykseen käyttäjien huomaamatta. Tämä kaapattujen tietokoneiden verkko on botnet, joka suorittaa palvelunestohyökkäyksiä määriteltyyn uhriin, esimerkiksi johonkin pelipalvelimeen. (Prolexic 2014.)



Kuva 3. DDOS eli hajautettu palvelunestohyökkäys. (E-zest 2012.)

3.5 Autentikaatio

Blizzard Entertainment -peliyhtiö loi autentikaattorityökalun pelaajilleen, joka antaa lisäturvaa pelitilien turvallisuuteen. Se on fyysinen pieni laite, joka generoi digitaalisen numerokoodin ja koodi syötetään peliin sisäänkirjautumisen yhteydessä. Laite estää hyökkääjän pääsyn kohteen tilille, vaikka tämä tietäisi kirjautumistiedot. Autentikaattori hyödyntää kahden tekijän todennusta eli autentikaatioon vaaditaan laitteen generoima numerosarja sekä tilin salasana, jonka käyttäjä tietää. Yksi numerokoodi on validi vain minuutin ajan, minkä jälkeen se mitätöityy. Autentikaattorista luotiin myös mobiilisovellus, joka toimii

samaan tyyliin luoden kertakäyttöisen numerosarjan mobiililaitteeseen. (Battlenet authenticator 2014.)

Kuva 4. Fyysinen autentikaattori. (Battlenet authenticator 2014.)

Kuvassa 4 on Blizzardin avaimenperä-autentikaattorilaite, jossa ruudulle on generoitu digitaalinen varmennekoodi.

Toisen tekijän todennuksessa voidaan käyttää myös kertakäyttöisiä sähköposteja tai mobiilitekstiviestejä. Esimerkkinä Google Gmailissa on mahdollisuus liittää SMS-varmennus sähköpostiin kirjautumiseen.

Autentikaattori ei kuitenkaan ole täysin varma tapa suojautua tilivarkaudelta.

Vuonna 2014 Blizzard Entertainment raportoi troijalaisesta, joka pystyi ohittamaan kahden tekijän autentikaation. Jotkut käyttäjät olivat ladanneet tietämättään troijalaisella saastuneen ohjelmaversion suositusta pelin lisäosaohjelmasta Curse Client. Troijalainen loi välimieshyökkäyksen, jolla

salakuunteli pelaajien käyttäjätunnuksen, salasanan ja jopa autentikaattorin numerosarjan. Pelaaja sai yrittäessään kirjautua sisään virheilmoituksen, jonka aikana hyökkääjä pääsi itse tilille sisään. Tällaisen hyökkäyksen estämiseksi ehdotetaan, että toisen autentikaatiovaiheen tulisi tapahtua eri kanavan kautta. Paras keino kuitenkin on olla asentamatta mitään vieraita kolmannen osapuolen ohjelmia. (Gonsalves 2014.)

Monen tekijän todennuksessa käyttäjän aitouden todistamiseen käytetään useaa eri tapaa. Yksi tapa on salasanan tai PIN-koodin syöttäminen esimerkiksi verkkopankissa asioitaessa. Pelkkä käyttäjänimi ja salasana itsessään eivät riitä tarvittavan turvallisuuden takaamiseksi, joten todentamiseen lisätään toinen tekijä, kuten Blizzardin autentikaattoriväline. Kolmas esimerkki henkilön aitouden todentamisesta voi olla biometrinen tunnistautuminen, kuten sormenjälkitunnistus. Biometrinen tunnistus ei ole vielä käytössä pelialalla. (Multi-factor authentication 2014.)

3.6 Huijaaminen peleissä

Yksinpeleissä huijauksien käyttö on ollut yleistä jo peliteollisuuden alkutekijöistä lähtien. Pelien tekijät loivat alunperin huijauskoodit pelien testausta varten helpottaakseen testaustyötä, mutta koodit yleistyivät nopeasti myös pelaajien käyttöön. Ne saattoivat antaa mahdollisuuden esimerkiksi muuttaa pelien hahmojen ulkoasua tai auttaa tasojen päihittämisessä. Moninpeleissä kuitenkin huijaaminen yritetään kitkeä pois eri esto-ohjelmilla, jotta huijauksien käyttäjä ei pilaa muiden pelaajien pelikokemusta tai saa yliotetta vastustajasta, varsinkin kilpailuhenkisissä moninpeleissä.

Yksi tällainen työkaluohjelma on Even Balance Inc –yhtiön luoma PunkBuster. Se skannaa reaaliajassa tietokoneen muistia ja etsii mahdollisia tunnettuja huijausskriptejä tai kolmannen osapuolen ohjelmia. Pelaajien koneilta lähetetään nopeaan tahtiin useita kryptattuja tilanneraportteja PunkBusterin serverille, joka löytäessään rikkeen, voi poistaa pelaajan peliserveriltä ja estää

tämän uudelleenyhdistämisen palvelimelle. Pelipalvelimilla toimii myös ylläpitäjiä, joille voi kuvankaappauksilla ilmoittaa epäillyistä huijausten käyttäjistä. (Even Balance 2014.)

Peliyhtiö Blizzard Entertainment käyttää esimerkiksi suositussa World of Warcraft verkkomoninpelissä Warden-huijauksenestotyökalua. Pelin ollessa päällä Warden skannaa muut auki olevat ohjelmat ja kerää näistä dataa, jonka se lähettää Blizzardin servereille vertailtavaksi tunnettuihin huijausohjelmiin. Jotkut käyttäjät ovat väittäneet Wardenia vakoiluohjelman kaltaiseksi haittaohjelmaksi, koska se kerää pelaajien tietokoneista henkilökohtaista informaatiota. Blizzard vastasi näihin väitteisiin sanomalla, ettei Warden kerää mitään henkilökohtaista yksilötietoa ja että ohjelma keräsi vain mahdollisia todisteita huijauksien käytöstä. Suurin osa pelaajista kuitenkin hyväksyy tämän ohjelman käytön, jos se pitää huijaavat pelaajat poissa. (Ward 2005.)

Suuri amerikkalainen peliyhtiö Valve myös hyödyntää peliservereillään omaa huijauksenestoa VAC:ia eli Valve Anti-Cheat. Se tutkii pelaajan tietokoneelta peliin vaikuttavia kolmannen osapuolen ohjelmia tai muokattuja pelitiedostoja. Jos ohjelma havaitsee huijausrikkeen, se poistaa pelaajan serveriltä pysyvästi. Tyypillisiä huijauskeinoja Valven peleissä ovat esimerkiksi ”aimbot”, joka auttaa pelaajaa aseella tähtäämiseen, tai ”wallhack”, jonka avulla näkee pelitasojen seinien läpi muiden pelaajien liikkeet. On olemassa kuitenkin palvelimia, joissa VAC ei ole käytössä. Epävirallisten lähteiden mukaan VAC on antanut porttikiellon jopa yli 2 miljoonalle pelaajalle. (Valve Corp. 2013a.)

4 CASE WORLD OF WARCRAFT

Tässä luvussa selvitetään, miten eri keinoin pelaaja voi käytännössä parantaa World of Warcraft -pelitilinsä tietoturvaa.

Salasana

Salasana on ensisijainen keino, jolla tilejä turvataan. Jotta salasana olisi tarpeeksi vahva, tulee sen olla vähintään 8 merkkiä pitkä. Mitä pidempi salasana, sitä turvallisempi. Sen tulee sisältää pieniä ja suuria kirjaimia sekä numeroita. Salasana ei kuitenkaan anna paljoa turvaa pelitilille. Yleensä World of Warcraft -tileihin kohdistuvissa hyökkäyksissä tunkeutuja tietää jo käyttäjätiedot etukäteen.

Autentikaattori

Blizzard-peliyhtiö tarjoaa pelaajilleen mahdollisuuden autentikaattoriin. Ilmaisen mobiiliversion älypuhelimeen voi ladata Blizzardin verkkosivujen kautta. Sovelluksen asentamisen jälkeen se kytketään toimimaan käyttäjätilin kanssa pelaajan käyttäjätiliasetuksista. Autentikaattorikoodin kyselyn voi asettaa toimimaan joka kirjautumisen yhteydessä tai esimerkiksi 30 päivän välein. Yhteensopivat puhelimien käyttöjärjestelmät ovat iOS, Android ja Windows Phone 7. (Battle.net 2014.)

Kuvassa 5 on kuvakaappaus mobiiliautentikaattorin Android-versiosta, jossa näkyy yksi sovelluksen tuottamista kertakäyttöisistä digitaalisista numerokoodeista.

Kuva 5. Mobiiliautentikaattori. (Play Google 2013.)

SMS Protect

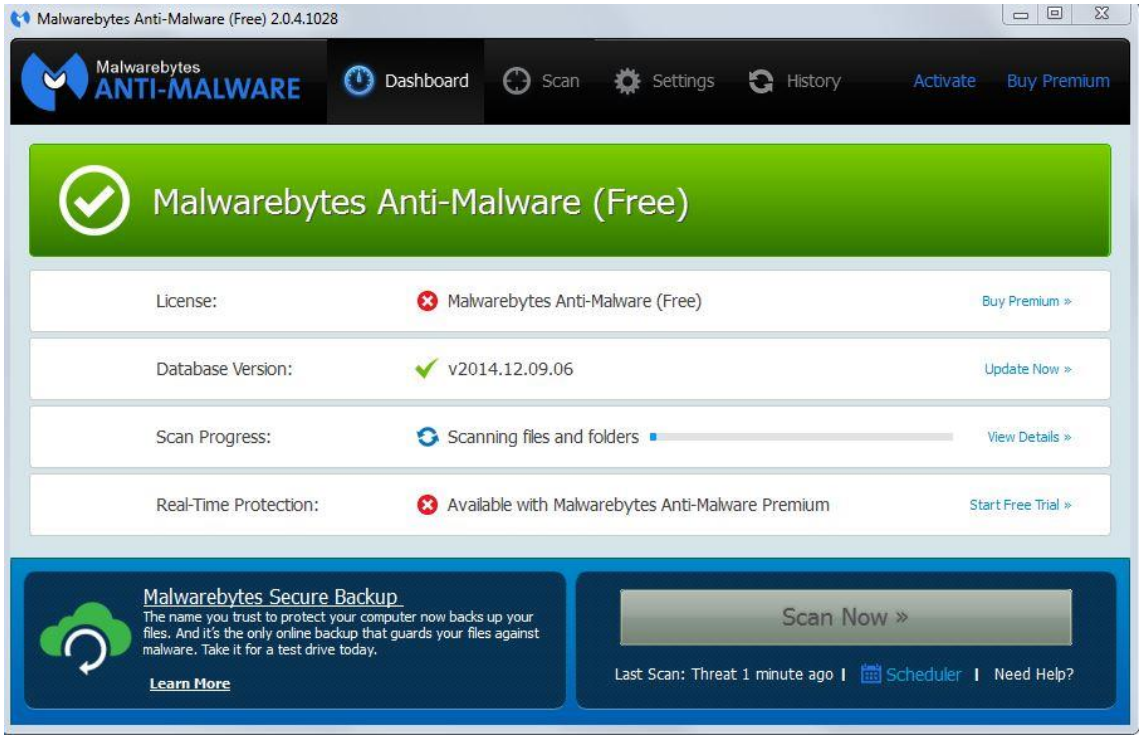
SMS Protect on Blizzardin tarjoama tekstiviestivarmennuspalvelu. Se on yksinkertainen ja toimii ikään kuin pelitilin vahtina. Sen on tarkoitus hälyyttää tekstiviesti-ilmoituksella, jos pelitiliin tehdään muutoksia. Esimerkiksi jos tili menee lukkoon liian monesta kirjautumisyrityksestä tai salasana vaihdetaan. Palvelun saa kytkettyä päälle Blizzardin verkkosivulta tiliasetuksista. (Battle.net 2014.)

Haittaohjelmat

Yleisin tapa menettää World of Warcraft -pelitili on käyttäjätunnuksien paljastuminen verkkorikollisille haittaohjelmien kautta. Tietojakalastelevien troijalaisten ja vakoiluohjelmien takia tietokoneella kannattaa ylläpitää aktiivisesti suojaavaa anti-virus ja anti-malwareohjelmaa, jota ajaa säännöllisin välein. Malware tarkoittaa suomeksi haittaohjelmaa. Esimerkkinä

haittaohjelmien poisto-työkaluna Malwarebytes Anti-Malware, joka löytää ja poistaa haittoja, joita tavallinen anti-virus ei ehkä löydä. Omakohtaisena kokemuksena ilmaisversio Malwarebytesistä on erinomainen.

Ikäviltä haittaohjelmilta välttyy, kun ei asenna mitään epävirallisia kolmannen osapuolen ohjelmia. Kaikki sähköpostit, jotka tulevat World of Warcraft tai Blizzard Entertaiment -nimisiltä lähettäjiltä tai näin otsikoituina, kannattaa huolellisesti tarkistaa. Blizzard ei koskaan kysy pelaajiensa salasanoja tai tunnistustietoja sähköpostitse tai pelin chat-palveluissa.



Kuva 6. Kuvakaappaus Malwarebytes Anti-Malware –ohjelmasta.

5 KÄYTTÄJÄTILIEN ARVO

5.1 Pelitilien rahallinen arvo

Viime vuosina on yleistynyt verkkopeleissä liiketoimintamalli, jossa pelien sisällä voi tehdä ostoksia oikealla rahalla. Ostot koskevat pelin lisäsisältöä, kuten omalle avatarille muuten saamattomissa olevia esineitä tai bonuksia. Pelissä saattaa esimerkiksi olla asia, jonka saavuttamiseen kuluisi normaalisti paljon peliaikaa, mutta sen saa hankittua samantien lataamalla pelitilille lisää rahaa. Tätä mallia hyödyntävät pelit ovat usein jopa ilmaisesti ladattavia ja pelintekijät tekevät liikevoittonsa ns. mikromaksusuorituksilla. Aikaisemmin tavallisempi maksutustapa verkkomoninpeleissä oli kiinteät kuukausimaksut, mutta nykyään yhä useampi uusi verkkomoninpeli on ilmaiseksi pelattava ja ne keskittyvät pienempiin vapaaehtoisiin pelaajaostotapahtumiin. Ymmärtäisin pelien tekijöiden huomanneen, että näillä mikromaksuilla kasvaa pelaajien rahankäyttö sekä ilmaiseksi hankittavat pelit edesauttavat houkuttelemaan uusia pelaajia.

Kun pelaaja on hankkinut tililleen rahallisesti arvokkaita asioita, nostaa se pelitilin arvokkuutta. Tämän takia verkkorikolliset yrittävät päästä käsiksi pelien käyttäjätileihin siirtääkseen varat itselleen. Erityisesti massiiviroolipelit käyttävät paljon mikromaksuja, joten ne ovat arvokkaita tilejä rikollisten myydä pimeillä markkinoilla eteenpäin.

Vuonna 2011 perustettiin pelaamisen suoratoistopalvelu Twitch.tv, joka ylläpitää 60 miljoonan käyttäjän kuukausikävijämäärää. Kuka tahansa henkilö voi aloittaa peliensä striimaamisen eli suoratoiston ilmaiseksi. Sivulla on chat-palvelu, jonka avulla katsojat voivat keskustella keskenään tai kommunikoida esiintyvän pelaajan kanssa. Twitch on vastaavanlaisten sivustojen suosituin ja sen osti Amazon.com syksyllä 2014 yli miljardilla dollarilla. F-secure uutisoi tapauksesta, jossa chatissa ollut bot-käyttäjä linkkasi toistuvasti linkkiä haitalliselle sivustolle ja mainosti valearvontaa, josta osallistuja kykenisi voittamaan pelien virtuaaliesineitä. Valearvontasivulla käyttäjää pyydettiin ilmoittamaan nimi ja sähköpostiosoite, mutta todellisuudessa tietokoneelle asentui haitallinen

ohjelma. Ohjelman tarkoitus on suorittaa eri komentoja, joilla se saa haltuunsa käyttäjän Steam-tilin ja voi aloittaa myymään sekä suorittamaan arvokkaiden virtuaaliesineiden siirtämistä hyökkääjän omalle Steam-tilille. Varastettujen esineiden arvo voi liikkua jopa tuhansissa euroissa. (F-secure 2014.)

5.2 Pelivaluuttojen myynti

Aasiassa ja etenkin Kiinassa on pelien sisäisten ekonomioiden luoma ilmiö ”kullan” keräys ja sen myynti. Kulta voi olla pelimaailmassa käytettävää valuuttaa, jolla pelaaja ostaa muilta pelaajilta tavaroita tai palveluja. Useissa verkkopeleissä on olemassa peleissä toimivat omat kaupat, joissa pelaajat voivat keskenään myydä esineitä ja määritellä hinnat näille. Kullankerääjät myyvät halukkaille pelaajille kultaa oikean maailman valuuttaa vastaan. Tällainen toiminta saattaa häiritä pelien sisäistä ekonomiaa ja luoda inflaatiota kullan ostoarvolle. Pelien tekijät ei hyväksy tätä toimintaa ja se on vastoin määrättyjä palveluehtosopimuksia.

The Guardian -lehden uutisartikkelissa vuonna 2011 kerrottiin kiinalaisesta vankien työleiristä, joissa vangit pakotettiin pelaamaan verkkopeliä ja keräämään kultaa vankileirin vartijoille, jotka myivät kullat eteenpäin oikeaksi rahaksi omiin taskuihinsa. Jos vanki ei saavuttanut päivän keräystavoitetta, sai hän fyysisen rangaistuksen. Kullankeräys peleissä on suhteellisen uusi ilmiö ja siihen liittyvä lainsäädäntö on edelleen epäselvää. (Vincent 2011.)

Kullankeräyksen alamaailma on kasvanut nopeaan tahtiin verkkomoninpelien suuren suosion takia. Aasiassa toimii ns. hikipajoja joissa ihmiset tekevät työkseen kullankeräystä, koska siitä saa useasti enemmän rahaa kuin esimerkiksi tehtaassa työskentelystä. Pelit saattavat myös olla helppo keino rikollisten rahanpesuun.

6 PELIYHTIÖT

6.1 Yritysten tietojärjestelmien tietomurrot

Suurimmat peliyhtiöt eivät ole säästyneet kyberhyökkääjiltä. Viime vuosina on raportoitu pelipalvelimien asiakastietokantojen hakkeroinnista. Rikolliset havittelevat ensisijaisesti pelaajien luottokorttitietoja.

Vuonna 2012 Blizzard Entertainment varoitti pelaajia sattuneesta tietomurrosta, joka kohdistui yrityksen sisäiseen verkkoon. Hyökkääjä sai käsiinsä käyttäjien sähköpostiosoitteita, kryptattuja salasanoja sekä mobiili- ja fyysisten laiteautentikaattorien kryptattuja koodeja. Blizzard käyttää salasanasuojauksessaan SRP-protokollaa ja se mainitsi salasanojen murtamisen olevan erittäin vaikeaa ja epätodennäköistä, mutta kehoitti silti asiakkaitaan vaihtamaan varmuudeksi salasanojaan. (Kirk 2012.)

Sony Online Entertaimentille tapahtui vuonna 2011 suuri tietomurto, kun 77 miljoonan Sonyn hallitseman Facebook-pelien käyttäjien tilitiedot varastettiin. Tiedot koostuivat nimistä, osoitteista, luottokorttitiedoista ja salasanoista. Kiusalliseksi tilanteen Sonyn kannalta teki se, että se kertoi tapahtumasta vasta viikkoa myöhemmin. Tapahtumien korvaamiseksi Sony jakoi pelaajille ilmaista pelisisältöä sekä ilmoitti parantavansa tietoturvallisuutta. Sony haastettiin oikeuteen monelta taholta ja oikeudenkäynti päätettiin sopimukseen, jossa se joutui maksamaan 15 miljoonan dollaria korvauksia. Asiakkaat joiden tietoja todistettavasti käytettiin rikollisesti hyväksi, saivat myös korvauksia. Sony jakoi lisäksi ilmaisia Playstation 3 -pelejä hyvittääkseen pelaajia. (CRN 2014.)

Tällaisissa tapauksissa vastuu on kokonaan peliyhtiöiden puolella, koska pelaaja ei itse ole syyllinen asiakastietojen vuotamiseen.

6.2 Moninpelialustat

Moninpelialustat ovat tietokoneelle asennettavia sovelluksia. Niiden kautta myydään digitaalisesti pelejä, pelataan niitä ja ne toimivat viestintävälineenä pelaajien kesken. Pelialustojen avulla tapahtuu myös pelien päivitykset uusimpiin versioihin. Suurimpia tällaisia palveluohjelmia ovat Valven Steam, Electronic Arts -pelifirman Origin ja Blizzard Entertainmentin Battle.net, joiden tarkoitus on yhdistää pelifirmojen omat pelit yhden käynnistysalustan alle. Myös Ubisoft-pelitalo kehitti oman sovelluksensa Uplay, joka yhdistää konsolipelaajat, tietokonepelaajat sekä sosiaalisen median.

Steam-pelialustassa on mahdollista käyttää Steam Guard -toimintoa. Se toimii lisäturvana käyttäjänimelle ja salasanalle. Jos käyttäjätilille yritetään kirjautua ennalta tuntemattomasta laitteesta, se vaatii erityiskoodin. Koodi lähetetään tilinomistajan sähköpostiosoitteeseen. Uusi laite voidaan koodin onnistuneen syöttämisen jälkeen lisätä tunnistettujen laitteiden listaan ja koodia ei enää kysytä tältä laitteelta. Tunnistetuille laitteille ei ole määrättyä maksimimäärää. (Valve Corp. 2013b.)

Ubisoftia on kritisoitu tyylistä vaatia pelejään olemaan yhteydessä internetiin, vaikka nämä pelit eivät olisi verkkomoninpelejä vaan yksinpelejä. Suositun The Sims -pelisarjan neljännen osan julkaisu kärsi tästä, koska pelipalvelimet eivät pystyneet käsittelemään tarpeeksi pelaajia ja peliin ei pystynyt kirjautumaan. Verkkomonipeleissä on yleistä, että uuden pelin julkaisupäivänä palvelimet ovat ylikuormittuneita ja pelaajat joutuvat jonottamaan peliin pääsyä. Omakohtaisena kokemuksena kohtasin tämän ongelman Blizzardin Diablo 3 -pelissä sen julkaisupäivänä vuonna 2012. Peli antoi virheilmoituksen lähes jokaiselle pelaajalle kirjautumisessa, joka ilmoitti palvelimien olevan liian kiireisiä ja kehoitti yrittämään sisäänpääsyä myöhemmin. Ongelma ei kestänyt ainoastaan tunteja vaan jopa kokonaisia päiviä ilman, että pelin ostaneet pääsivät pelaamaan.

7 YHTEENVETO

Opinnäytetyön kirjoittaminen oli aluksi melko haasteellista aiheen rajauksen suhteen, mutta idea selkiytyi kun tutki lähteitä tarkemmin. Opinnäytetyön aiheeseen oli vaikea löytää mitään nykyaikaista kirjallisuutta, joka käsittelisi etenkin verkossa pelaamista eikä pelkästään pelejä yleisesti tai pelien tekoa. Jouduin siis turvautumaan suureksi osin verkkolähteisiin. Kaikki lähdemateriaali mitä työssä käytettiin oli englanniksi.

Ei ole keinoa suojata täysin verkossa pelaamisen tietoturvaa. Aina on olemassa uusia kokemattomia pelaajia, jotka eivät ole tietoisia erilaisista uhista, joilla huijarit tilejä yrittävät anastaa. Vaikka pelitilit turvattaisiin sataprosenttisesti pelintekijöiden puolesta, liittyy pelaajaan aina omat sosiaaliset riskinsä kuten sähköpostihuijaukset tai epämääräisiä palveluja peleissä myyvät huijarit.

Mitä pelien tulevaisuuden kehitykseen tulee, uskon pelialan yhä kasvavan ja kehittyvän enemmän. Markkinoille tulee vuosien kuluessa okuläärilaitteita, joille luodaan virtuaalipelimaailmat ja ne saadaan liitettyä mahdollisesti myös verkkoon. Nykyajan nuoret lapset saavat jo pienenä kosketuksen peleihin taulutietokoneiden ja älypuhelimien kautta, joten tulevaisuus pelialalla näyttää jatkuvan.

Työni kautta lukija voi oppia uutta peleistä ja verkossa pelaamisesta ja niihin liittyvistä tietoturvauhista. Tietoja etsiessäni opin paremmin ymmärtämään tietoturvauhkia tai häiriöitä ja näiden toimintatapoja liittyen peleihin.

LÄHTEET

ADSL 2014. Webopedia. Viitattu 6.12.2014 http://www.webopedia.com/TERM/A/ADSL.html.

Battle.net 2014. Battle.net Authenticator. Viitattu 6.12.2014 https://us.battle.net/support/en/article/battlenet-authenticator.

Battle.net Authenticator 2014. Wowwiki. Viitattu 2.10.2014 http://www.wowwiki.com/Battle.net_Authenticator.

Battle.net 2014. Battle.net SMS Protect. Viitattu 6.12.2014 https://us.battle.net/support/en/article/battlenet-sms-protect.

The Cert Division 2014. Denial of Service Attacks. Viitattu 19.9.2014 http://www.cert.org/historical/tech_tips/denial_of_service.cfm#3A1.

CRN 2014. Sony Agrees to $15 million Payout, Free PS3 games In Playstation Breach Settlement. Viitattu 20.8.2014 http://www.crn.com/news/security/300073160/sony-agrees-to-15-million-payout-free-ps3-games-in-playstation-breach-settlement.htm.

Even Balance, Inc. 2014. Info. Viitattu 20.8.2014 http://www.evenbalance.com/index.php?page=info.php.

E-zest 2012. Stop ddos-attacks. Viitattu 1.12.2014 http://www.e-zest.net/blog/stop-ddos-attacks.

F-secure 2014. A Twitch of Fate: Gamers Shamelessly Wiped Clean. Viitattu 10.10.2014 http://www.f-secure.com/weblog/archives/00002742.html.

Gonsalves, A. 2014. World of Warcraft attack highlights two-factor authentication weakness. CSO. Viitattu 5.9.2014 http://www.csoonline.com/article/2134279/social-engineering/world-of-warcraft-attack-highlights-two-factor-authentication-weakness.html.

Huan-Rong, T.; Rou-Ling, S. & Wei-Qiang K. 2009. Wireless intrusion detection for defending against TCP SYN flooding and man-in-the-middle attack. IEEE Conference Publications, 1464-1470.

ISDN – integrated services digital network 2014. Webopedia. Viitattu 6.12.2014 http://www.webopedia.com/TERM/I/ISDN.html.

Keylogger 2014. Webopedia. Viitattu 20.10.2014 http://www.webopedia.com/TERM/K/keylogger.html.

Kirk, J. 2012. Blizzard Entertainment Warns of Password Breach. PC World. Viitattu 20.8.2014 http://www.pcworld.com/article/260696/blizzard_entertainment_warns_of_password_breach.html.

MMO RPG 2013. A Journey Into MMO Server Architecture. Viitattu 12.11.2014 http://www.mmorpg.com/blogs/FaceOfMankind/052013/25185_A-Journey-Into-MMO-Server-Architecture.

Multi-factor authentication 2014. Wikipedia. Viitattu 3.10.2014 http://en.wikipedia.org/wiki/Multi-factor_authentication.

Online console gaming 2014. Wikipedia. Viitattu 1.11.2014 http://en.wikipedia.org/wiki/Online_console_gaming.

Play Google 2013. Battlenet authenticator. Viitattu 6.12.2014 https://play.google.com/store/apps/details?id=com.blizzard.bma&hl=fi.

Prolexic 2014. What is DDoS denial of service. Viitattu 2.12.2014 http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html.

Secure Remote Password protocol 2014. Wikipedia. Viitattu 6.12.2014 http://en.wikipedia.org/wiki/Secure_Remote_Password_protocol.

SSL – Secure Sockets Layer 2014. Webopedia. Viitattu http://www.webopedia.com/TERM/S/SSL.html.

Symantec 2014. Security 1:1 – Part 5 – Online gaming fraud, scam and phishing. Viitattu 22.10.2014 http://www.symantec.com/connect/articles/security-11-part-5-online-gaming-fraud-scam-and-phishing-attempts.

Valve Corp. 2013a. Valve Anti-Cheat System (VAC). Viitattu 21.10.2014 https://support.steampowered.com/kb_article.php?ref=7849-Radz-6869.

Valve Corp. 2013b. Steam Guard. Viitattu 5.12.2014 https://support.steampowered.com/kb_article.php?ref=4020-ALZM-5519.

Video game genres 2014. Wikipedia. Viitattu 1.12.2014 http://en.wikipedia.org/wiki/Video_game_genres.

Vincent, D. 2011. China used prisoners in lucrative internet gaming work. The Guardian. Viitattu 15.11.2014 http://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam.

Ward, M. 2005. Warcraft game maker in spying row. BBC News. Viitattu 21.10.2014 http://news.bbc.co.uk/2/hi/technology/4385050.stm.