OULUN AMMATTIKORKEAKOULU

Heikki Kallankari

TLS ja palvelimien turvallisuuden arviointi

TLS ja palvelimien turvallisuuden arviointi

Heikki Kallankari
Opinnäytetyö
Syksy 2020
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittely, Järjestelmäasiantuntijuus

Tekijä(t): Heikki Kallankari
Opinnäytetyön nimi: TLS ja palvelimien turvallisuuden arviointi
Työn ohjaaja(t): Teppo Räisänen
Työn valmistumislukukausi ja -vuosi: Syksy 2020 Sivumäärä: 27 + 1 liite

---

Tämän opinnäytetyön tarkoituksena on avata TLS-tekniikan taustaa perusteiden, kehityskaaren sekä siinä käytetyn tekniikan osalta. Työssä käydään myös läpi muutamia protokollaan kohdistuneita tunnetuimpia haavoittuvuuksia. Tutkimusosuudessa tarkastellaan sadan suosituimman .fi -päätteisten sivustoiden tietoturvan tilaa uusimman TLS 1.3 -version osalta. Lisäksi avataan tutkimuksessa käytetyn työkalun toimintalogiikkaa yhden sivuston osalta. Aineistona työssä käytettiin alan tunnettujen toimijoiden julkaisuja, teknisiä dokumentteja, aiheesta suoritettuja tutkimuksia sekä tutkimuksessa käytetyn työkalun dokumentaatiota.

Opinnäytteen ensimmäisessä kappaleessa käydään läpi Transport Layer Security -protokollan perusteet, kehityskaari sekä uusimman 1.3 version tuomat tärkeimmät muutokset. Toisessa kappaleessa kerrotaan protokollan tekniikasta tarkemmin. Kolmas kappale käsittelee tunnetuimpia protokollan haavoittuvuuksia hyödyntäneitä hyökkäyksiä.

Opinnäytteen tavoitteena on toimia lukijalle tietopakettina TLS-protokollan toiminnasta sekä sen sisällöstä. Työ valikoitui aiheeksi vaihto-opintojen aikana suoritettujen tietoturvakurssien sytyttämän mielenkiinnon vuoksi. Aiheen teknisyyden vuoksi työ on kirjoitettu mahdollisimman selkeästi niin, ettei lukijan tarvitse olla aiheeseen syvemmin perehtynyt. Työ on kirjoitettu IT-alaa opiskeleville tai alasta kiinnostuneille henkilöille.

Tutkimusosuuden johtopäätöksenä voidaan sanoa, että tietoturvan tila uusimman TLS version osalta on keskinkertainen, mutta seuraa kuitenkin aiemmissa tutkimuksissa esille tullutta trendiä. Tutkimuksen data on anonymisoitu.

Asiasanat: Tietojenkäsittely, tietoturva, salaus, varmenteet, verkkohyökkäykset

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Data Sciences, Option of Systems Administration

---

Author(s): Heikki Kallankari
Title of thesis: TLS and auditing server security
Supervisor(s): Teppo Räisänen
Term and year when the thesis was submitted: Autumn 2020
Number of pages: 27 + 1 appendix

The purpose of this thesis is to inspect the TLS protocol. This is done by taking a closer look at its basics, development technical aspects and some of the most infamous vulnerabilities that affect the protocol. The study part of the thesis conducts a look at the current usage of the latest 1.3 version by collecting and analyzing data from the top 100 .fi websites.

The first chapter of the thesis is about the basics, development and the changes brought by the latest version. Second part takes a closer look at the technical aspects. The third part is dedicated to some of the vulnerabilities affecting TLS.

This thesis tries to be as succinct as possible in its object of showcasing the subject of study. The writers hope is to convey information in a way that is understandable to readers wishing to learn more about the subject. Such as students and hobbyists.

The study results show that the current usage of TLS version 1.3 is less than satisfactory. However, it follows the trend shown by earlier studies conducted on the subject.

Keywords: Information technology, Information security, Encryption

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tarkastella Transport Layer Security (TLS) -protokollan sisältöä ja sen toimintaa sekä avata palvelimien tietoturvan tilan tarkasteluun käytettäviä keinoja. TLS on jatkokehitetty versio SSL-protokollasta, se julkaistiin vuonna 1999. (Cloudflare, viitattu 22.4.2020.) Opinnäytteen tutkimusosuudessa tutkitaan Suomen top 100 -sivuston TLS-asetusten tilaa. Erityisesti kiinnittäen huomiota uusimman 1.3 version käytön yleisyyteen.

Opinnäytteen aihe valikoitui vaihto-opinnoissa käymistäni tietoturvaan perehtyvistä opinnoista alkaneesta kiinnostuksesta aihetta kohtaan. TLS-protokollassa on kattavasti erilaisia tekniikoita, joita olen opiskellut opintojeni aikana. Lisäksi aihe tuntuu olevan hieman tuntematon jopa tietotekniikan parissa työskentelevien ihmisten parissa.

Yksityisyyden takaaminen, datan oikeudellisuuden varmentaminen ja turvallinen kommunikointi internetissä ovat tietoturvan peruspilareita sekä välttämättömyyksiä maailmassa, jossa yksityisten ihmisten data on suuri liiketoiminnan kohde. Ilman toimivaa salausta ei tietoturvaa pystytä takaamaan, eikä ihmisen oikeutta yksityisyyteen olisi olemassa.

Tietoturva on hyvin ajankohtainen aihe. Syksyllä 2020 tapahtunut Valvomon tietomurto paljasti, mitä pahimmillaan voi tapahtua, mikäli tietoturvaa laiminlyödään organisaatioissa. Tietoturva tuntuukin olevan Suomessa laajemman huomion kohteena kuin koskaan aiemmin.

2 TRANSPORT LAYER SECURITY

Tässä luvussa tarkastellaan Transport Layer Security -protokollaa. Esittelyssä edetään perusteista luvussa 2.1, kehitykseen luvussa 2.2 sekä uusimman version esittelyyn luvussa 2.3.

2.1 Perusteet

Transport Layer Security eli TLS, on laajasti internetin kommunikaatiossa käytetty tietoturvaprotokolla. Sen ensisijainen käyttökohde on tiedon salaaminen web sovellusten ja palvelimien välillä. Sitä voidaan käyttää myös muissa internet kommunikaatioiden muodoissa kuten sähköposteissa, VoIP-puheluissa sekä pikaviestimissä.

TLS sai alkunsa kansainvälisten standardien järjestön IETF (Internet Engineering Task Force) ehdotuksesta. Ensimmäinen versio julkaistiin vuonna 1999 (Cloudflare, viitattu 22.4.2020).

Peruskäyttäjälle TLS-tekniikka tulee näkyviin useimmin HTTPS-protokollan kautta. Tällöin selaimet ilmoittavat sivuston olevan salattu, yleensä lukko ikonin avulla.

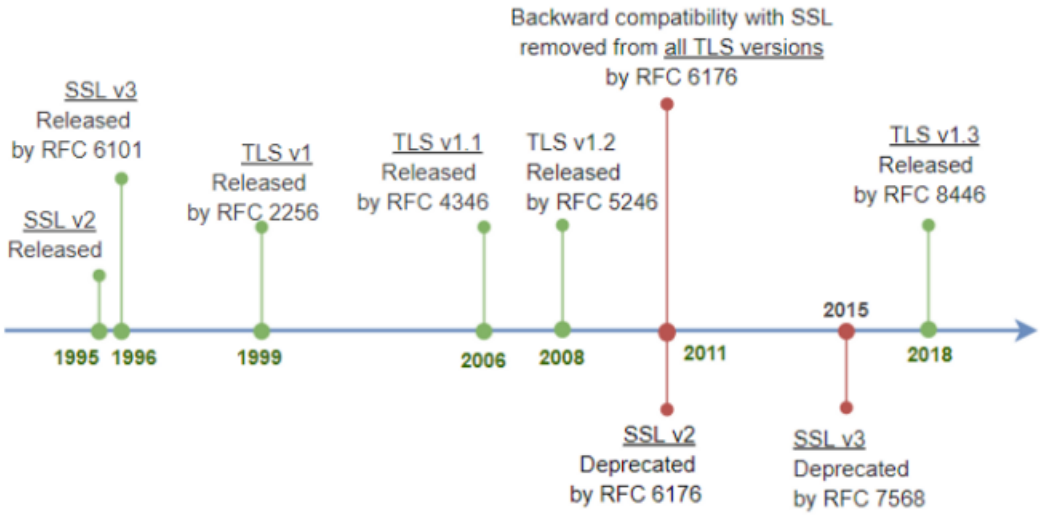
Kuva 1 Chrome selaimen ilmoitus HTTPS-protokollan käytöstä.

2.2 Kehitys

TLS on evoluutio protokollasta Secure Sockets Layer (SSL). SSL on alkujaan Netscape -yhtiön vuonna 1995 kehittämä protokolla. SSL-protokollaa ei nykyisellään enää päivitetä, eikä sen käyttöä suositella sen sisältämien haavoittuvuuksien takia.

Koska TLS ja SSL ovat niin lähellä toisiaan, on tavallista, että termit sekoitetaan tai niitä vaihdetaan keskenään. Käytännössä kun kuulet puhuttavan SSL-salauksesta, on nykyään useimmiten kyseessä kuitenkin TLS-protokolla (Cloudflare, viitattu 22.4.2020).

Kehityskaaren aikana vanhempia versioita on ensin suositeltu poistettavan käytöstä, sekä myöhemmin suurien toimijoiden mukana suoraan poistettu hyväksyttyjen listalta. Käytännössä tämä tarkoittaa sitä, että esimerkiksi Googlen kehittämän Chromium-ydintä käyttävät selaimet, joihin kuuluvat muun muassa Chrome ja Edge, eivät enää tue vanhempia salausversioita kuin TLS 1.2. (Google, viitattu 23.4.2020) Kuvassa 2 esitellään versiohistoriaa tarkemmin.



Kuva 2. Versiohistorian aikajana. (Medium.com, viitattu 22.4.2020)

2.3 Versio 1.3

Versio 1.3 on TLS-protokollan ensimmäinen suurempi kunnostus. Sen tarkoituksena on päivittää protokollaa salauksen ja nopeuden osalta, sekä pudottaa pois vanhoja haavoittuvia salauskeinoja.

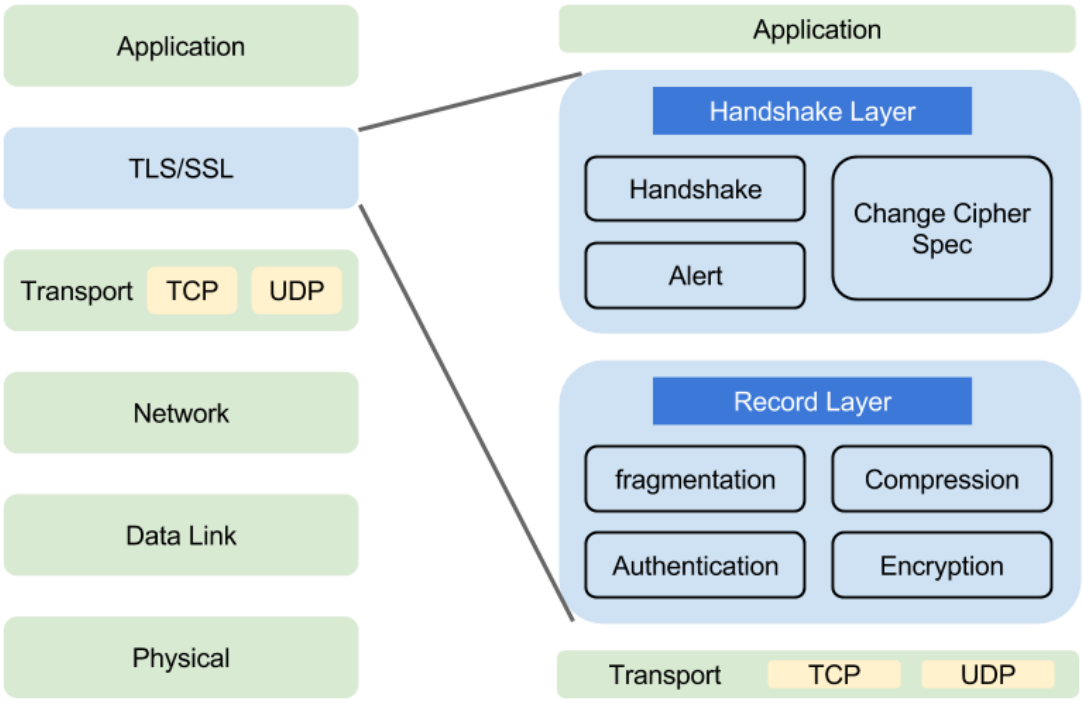
Uusimman version kehityksen tavoitteiksi IETF määräsi kättelyn latenssin vähentämisen, kättelyn aikaisen salauksen lisäämisen, poikkiprotokollaisten hyökkäysten vastaisen lujuuden lisäämisen sekä vanhojen perinnöllisten ominaisuuksien vähentämisen. (IETF, viitattu 20.5.2020.)

Suurin muutos salauksen osalta on RSA-salauksen pudottaminen pois versiosta 1.3. Tämä jättää ainoaksi hyväksytyksi salausprotokollaksi Diffie-Hellman-salauksen. Muutoksella haluttiin taata Forward Secrecy-ominaisuus, sekä parantaa kättelyn latenssia, sillä tämä mahdollistaa Zero round trip -kättelyn. (Cloudflare 2018, viitattu 14.12.2020.)

Uusimmassa versiossa muokattiin myös yhteyksien jatkamisen mekaniikkaa. Versiossa 1.3 palvelimen ja asiakkaan yhteinen salaisuus mahdollistaa istunnon jatkamisen samalla yhteisellä avaimella. (Cloudflare 2018, viitattu 14.12.2020.) Versio 1.3 onkin suurin muutos internetissä käytettyyn salaukseen pitkään aikaan.

3 TEKNIIKKA

TLS toimii OSI-mallissa kerroksien neljä ja viisi välissä, eli kuljetus ja ohjelma kerroksissa. OSI eli Open Systems Interconnection on ISO (International Organization for Standardization) -organisaation kehittämä tapa erilaisten tietoliikennejärjestelmien kommunikaation mallintamiseen. Kuvassa 3 havainnollistetaan TLS-protokollan kohdat OSI-mallissa.

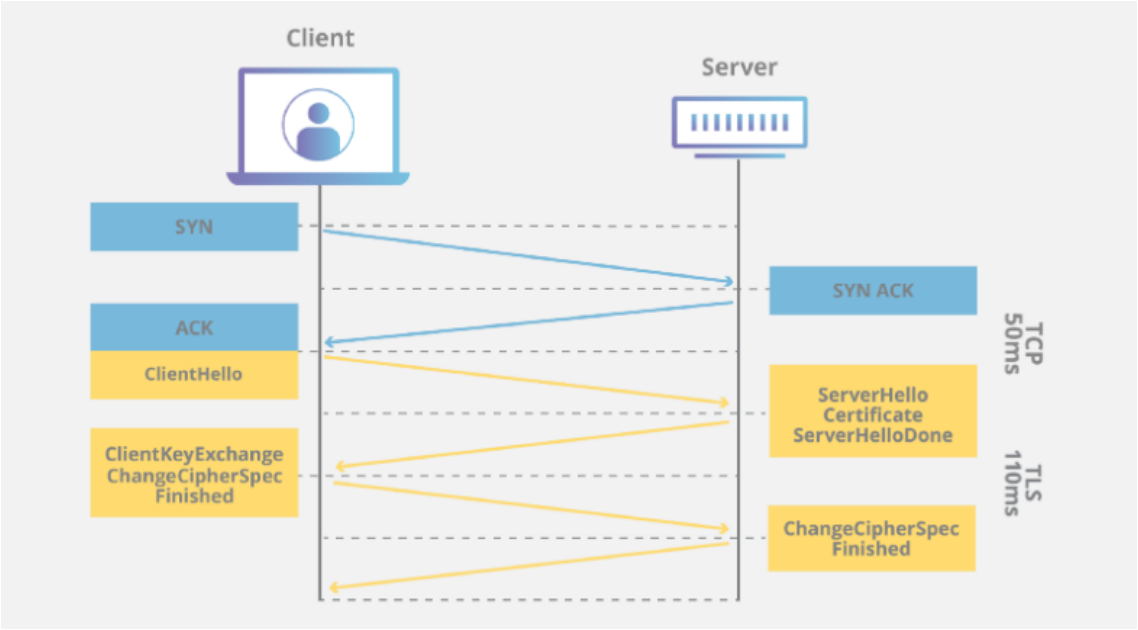


Kuva 3 TLS OSI-mallin osana. (Ilan Benichou, Eleven-labs, viitattu 1.6.2020.)

3.1 TLS-kättely

Jotta websivusto tai ohjelma voi hyödyntää TLS-tekniikkaa, tulee sen käytössä olla luotettavan tahon myöntämä sertifikaatti. Sertifikaatin myöntäjää kutsutaan nimellä Certificate Authority, eli lyhyesti CA. Sertifikaatti voidaan myöntää joko henkilölle tai organisaatiolle. Sertifikaatti sisältää tietoja palvelun omistajasta, sekä palvelimen julkisen avaimen. Kättelyssä voidaan hyödyntää sekä RSA- (Rivest–Shamir–Adleman), että DHE (Diffie–Hellman ephemeral) -salauksia.

Mikäli molemmilla osapuolilla on kunnollinen sertifikaatti, käynnistetään TLS-yhteys käyttämällä TLS-kättelyä (TLS handshake). Kättelyssä palvelin ja asiakas vaihtavat tietoja käytetystä TLS versiosta, salaus kokonaisuuksista, todentavat sertifikaatit sekä luovat kryptograafiset avaimet tulevalle tiedonvaihdolle. Kättelyn perimmäinen tarkoitus onkin luoda pohja alkavalle kommunikaatiolle käyttäjän ja palvelun välillä. Kuvassa 4 on kättelyn toiminta graafisessa muodossa.

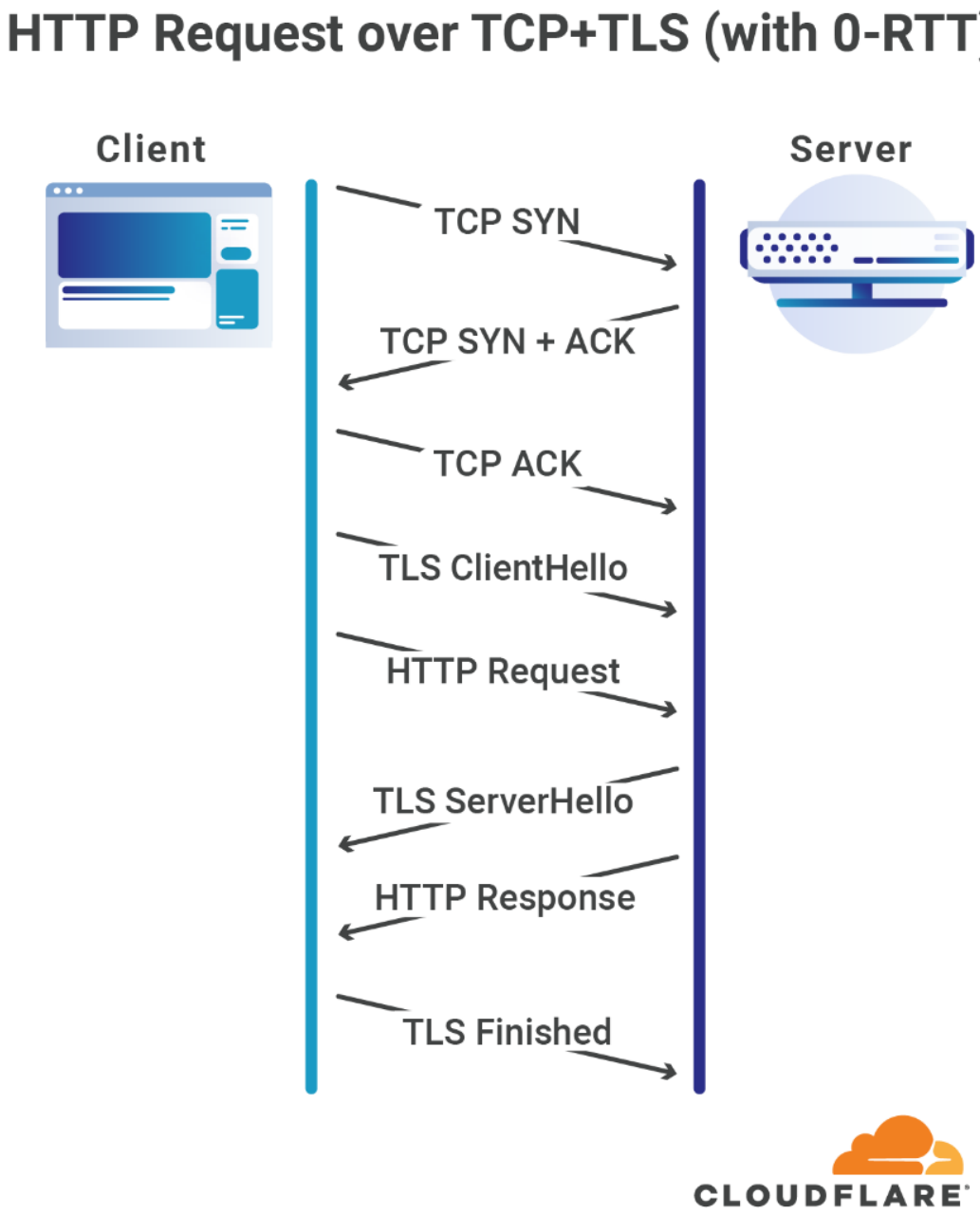


Kuva 4 TLS handshake. (Cloudlare 2020, viitattu 19.8.2020)

Suurin muutos versiossa 1.3 edellisiin versioihin nähden on juuri kättelyssä. Versio 1.3 mahdollistaa ns. Zero Roundtrip (0-RTT) -kättelyn käytön, jossa asiakas voi aloittaa datan, kuten http-pyyntöjen, lähettämisen jo ennen kuin TLS-kättely on kokonaan lopussa. Tällä on suuri vaikutus yhteyksien muodostamisen latenssiin.

0-RTT-kättelyn ideana on käyttää asiakkaan ja palvelimen edellisten TLS-kättelyiden varastoitua dataa uusien yhteyksien muodostamiseen. Tällä voidaan ohittaa yhteyden salausavaimien laskeminen jokaiselle yhteydelle ennen kuin palvelimelle voidaan keskustella. (Cloudflare, 2019, viitattu 26.11.2020.)

Muutos sinällään on hyvä ja nopeuttaa yhteyden muodostamista huomattavasti. On kuitenkin huomattava sen luoma uhka, sillä 0-RTT ei tue Forward Secrecy -ominaisuutta. Kuvassa 5 havainnollistetaan http-pyyntö salattuna käyttäen TLS- ja 0-RTT-tekniikoita.



Kuva 5 http-pyyntö sisältäen TLS-kättelyn käyttäen Zero Roundtrip -tekniikkaa. (Cloudlfare 2019, Haettu 26.11.2020)

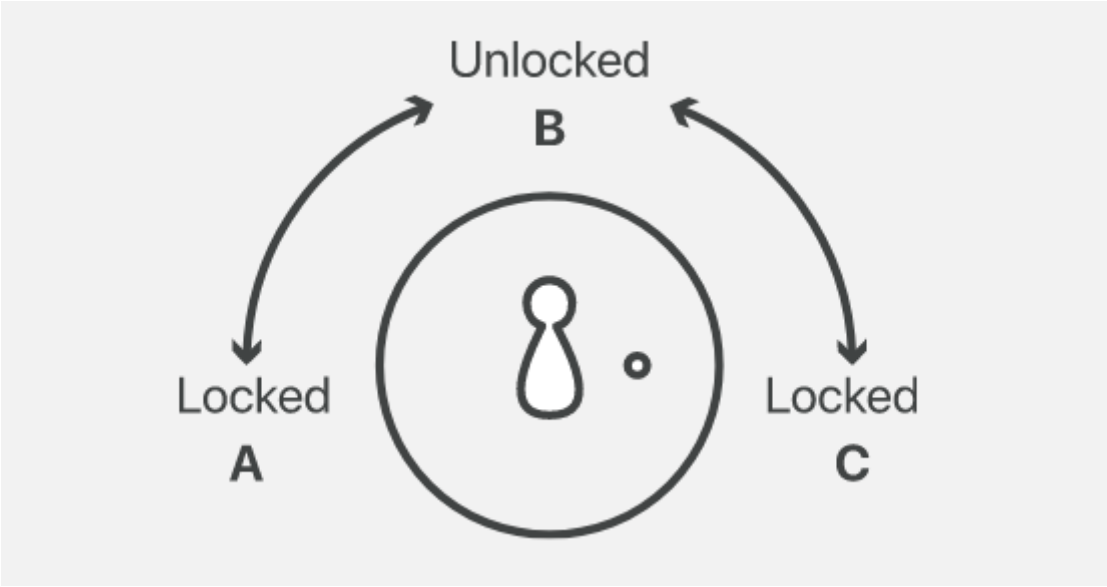
3.2 Forward Secrecy

Forward Secrecy tai Perfect Forward Secrecy on osa TLS-protokollan avainten vaihtoa, joka takaa, että jokainen luotu yhteysavain on uniikki ja itsenäinen. Käytännössä tämä tarkoittaa sitä, että mikäli yksityinen avain vuotaisi hyökkääjälle, ei salausavaimilla päästä käsiksi edellisten yhteyksin tietoihin. Ennen Forward Secrecy -tekniikan käyttöönottoa oli siis teoriassa mahdollista yksityistä avainta käyttämällä nähdä kaikkien sillä tehtyjen yhteyksien käyttäjän ja palvelimen välisten yhteyksien vanha data. Forward Secrecy nojaa Diffie-Hellman Ephemeral (DHE) -salaukseen kertakäyttöisten avainten luonnissa. (Namecheap 2019, viitattu 3.10.2020.)

3.3 Salaus

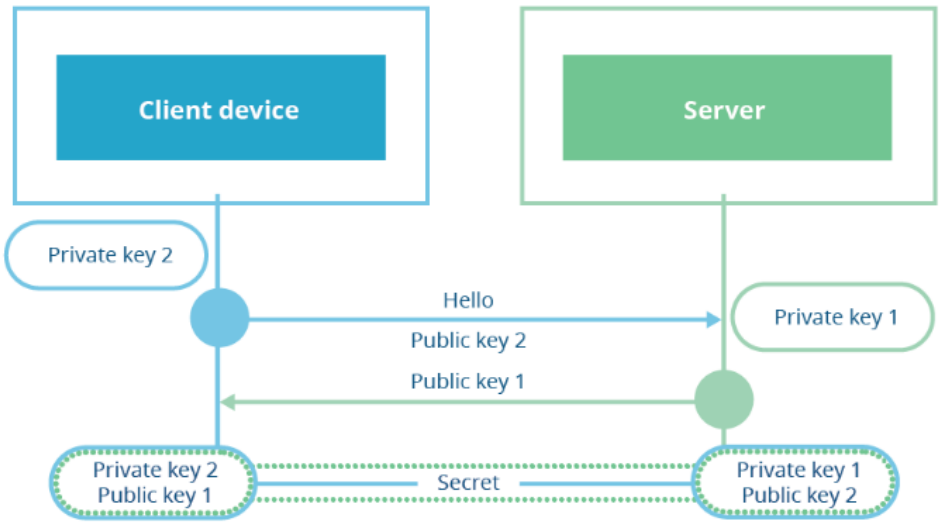
TLS-protokollassa käytetty salaus on avainpareihin perustuva tekniikka, jota kutsutaan nimellä Public Key Encryption (PKE). Avainpari koostuu julkisesta avaimesta (public key) sekä salaisesta yksityisestä avaimesta (private key). Julkisella avaimella salattu data voidaan avata vain yksityisellä avaimella ja yksityisellä salattu julkisella. TLS-salauksessa julkinen avain on osa SSL/TLS-sertifikaattia, joka on julkisesti saatavilla. Yksityinen avain taas asennetaan palvelimelle. (Cloudflare 2020, viitattu 14.12.2020.)

PKE-salaus saattaa tuntua vaikealta ymmärtää. Se voidaan kuitenkin havainnollistaa helposti yksinkertaisen kuvan avulla ks. Kuva 6. Kuvan lukossa asennossa A ollessaan se voidaan avata vain avaimella C ja vastaavasti toisinpäin. Lukko voidaan lukita kummalla tahansa avaimella mutta vain toinen avain voi avata sen. Tätä kutsutaan asymmetriseksi salaukseksi, sitä käytetään RSA-tekniikassa.



Kuva 6 PKE asymmetrinen salaus havainnollistettuna. A ja C kuvaavat Julkista ja Yksityistä avainta. (Cloudflare 2020, viitattu 15.12.2020.)

DHE- ja RSA-salauksien suurin ero on siinä, miten yhteinen salaisuus luodaan. RSA-salauksessa asiakas luo yhteisen salaisuuden omasta satunnaistetusta datastaan. Tämä tarkoittaa sitä, että kaikki jatkossa tehty keskustelu voidaan avata samalla avaimella. DHE-salauksessa asiakas ja palvelin laskevat yhdessä kertakäyttöisen avaimen etukäteen kättelyssä sovittujen parametrien mukaan. Tätä kutsutaan symmetriseksi salaukseksi. (Cloudflare 2020. viitattu 15.12.2020.) Kuvassa 7 on esitetty DHE yhteisen salaisuuden muodostaminen kättelyn aikana.

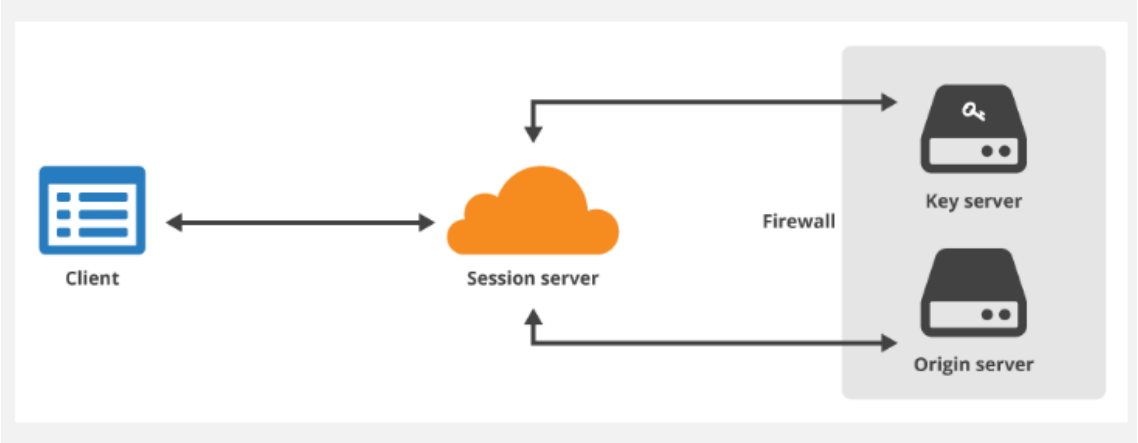


Kuva 7 DHE-kättely esitettynä. Asiakas ja palvelin laskevat yhteisen salaisuuden. (Cloudflare, Nick Sullivan 2018, viitattu 15.12.2020.)

3.4 Keyless SSL

TLS-kättelyssä käytetty salaus voidaan suorittaa myös avaimettomasti (keyless SSL). Avaimettomaksi tätä tekniikka kutsutaan siksi, että palveluntarjoaja ei koskaan näe käyttäjän yksityistä avainta. Yleensä tämä on käytössä vain silloin, kun yritys tai järjestö on ulkoistanut SSL-salauksen esimerkiksi pilvipalveluun, eikä yrityksen yksityistä avainta voida luovuttaa pois yrityksen sisältä.

Normaalissa kättelyssä yksityinen avain jouduttaisiin luovuttamaan palveluntarjoajalle, mutta avaimeton tekniikka mahdollistaa sen, ettei avainta luovuteta pois, vaan se säilyy sisäisesti avainpalvelimen avulla. Tämä siis vaatii yrityksellä olevan erillinen avainpalvelin, joka hoitaa salauksen kättelyn aikana ja muodostaa istuntoa varten avaimen (session key) ks. kuva 8. (Cloudflare 2020, viitattu 15.12.2020.)



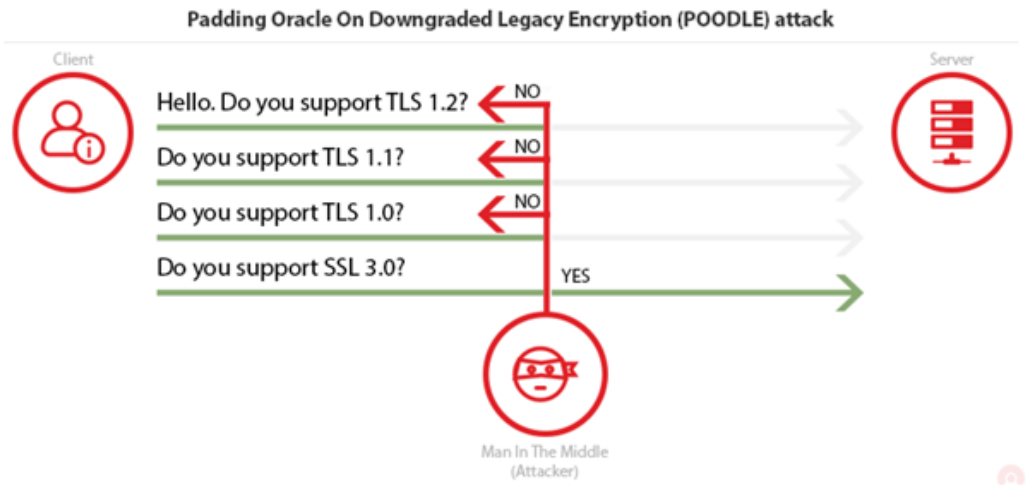
Kuva 8 Avaimeton SSL havainnollistettuna. (Cloudflare 2020, viitattu 15.12.2020.)

4 HAAVOITTUVUUDET

Tässä työssä käydään läpi viisi tunnetuinta SSL/TLS-haavoittuvuutta. Haavoittuvuuksien monimutkaisen ja teknisen luonteen vuoksi työssä kerrotaan niistä vain lyhyesti.

4.1 POODLE

Padding Oracle On Downgraded Legacy Encryption eli POODLE on 2014 lokakuussa julkaistu hyökkäys, joka hyväksikäyttää vanhentuneen SSL 3.0 -version haavoittuvuutta. Hyökkäys oli nimensä mukaisesti osoitettu Oracle -yhtiön palvelimiin, jotka vielä silloin tukivat vanhentunutta SSL 3.0 -versiota.



Kuva 9 Kuinka POODLE-hyökkäys toimii. (Acunetix 2019, viitattu 1.12.2020)

POODLE-hyökkäys toimii siten, että hyökkääjä kaappaa asiakkaan kättelyn ja suorittaa Man In The Middle (MITM) -hyökkäyksen esiintymällä palvelimena, kunnes asiakas suostuu alentamaan yhteyden käyttämään SSL 3.0 -protokollaa. (Acunetix 2019, viitattu 1.12.2020.) Kuvassa 9 on graafinen esitys toiminnasta.

4.2 BEAST

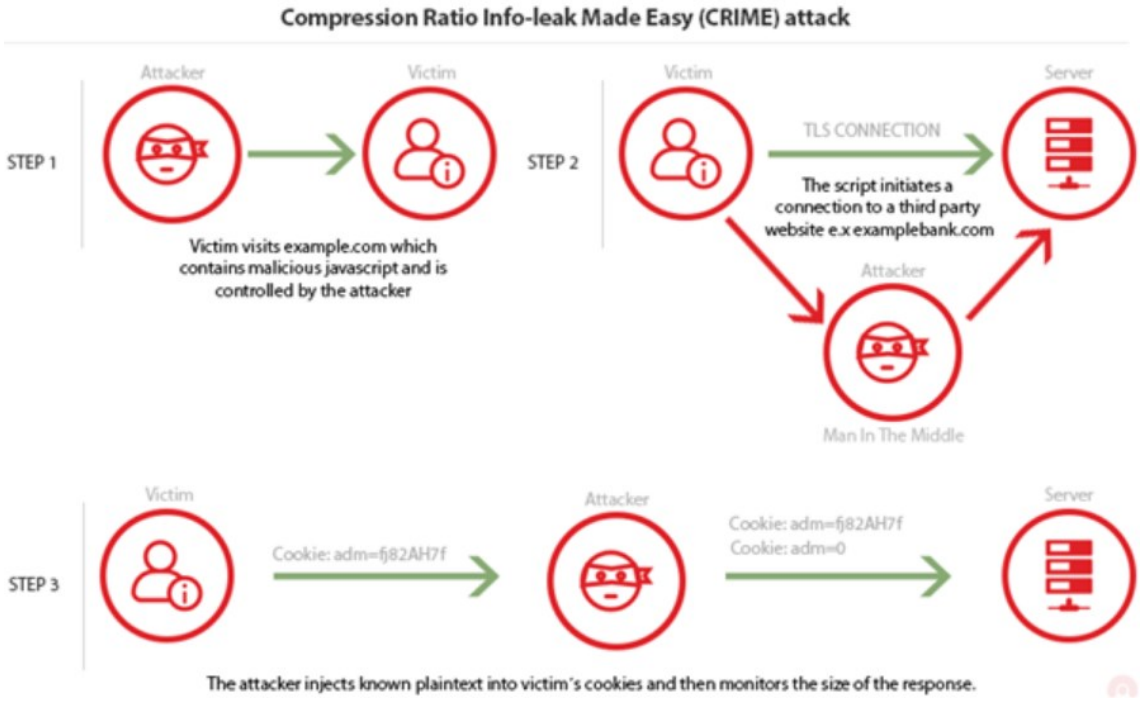
BEAST – eli Browser Exploit Against SSL/TLS on vuoden 2011 syksyllä esille tullut hyökkäys. Se keskittyy SSL 3.0 ja TLS 1.0 sekä näitä vielä vanhempien versioiden haavoittuvuuksiin. Hyökkääjä voi tätä haavoittuvuutta käyttäen saada kahden osapuolen välistä salaamatonta dataa. (Acunetix 2019. Viitattu 8.12.2020.)

Hyökkäys on pohjimmiltaan perinteinen Man-in-the-middle (MITM) -hyökkäys. Näissä hyökkäyksissä jokin kolmas osapuoli saa käyttöönsä kahden järjestelmän välistä dataa. MITM-hyökkäykset ovat helposti toteutettavia, sillä niitä hyödyntäviä työkaluja on laajasti saatavissa. (Globalsign 2017, viitattu 9.12.2020)

4.3 CRIME

CRIME – eli Compression Ratio Info-leak Made Easy, on TLS-pakkaukseen kohdistettu hyökkäys. Pakkaus metodi on TLS-kättelyn Client Hello -viestin osa. Pakkaus metodin sisällyttäminen ei ole pakollista Client Hello -viestissä ja yhteys voidaan muodostaa ilman sitä. Pakkaus esiteltiin SSL/TLS-protokollassa keinona pienentää kommunikaation viivettä. (Acunetix 2019, viitattu 8.12.2020.)

CRIME hyökkäys perustuu pakkauksen tapaan korvata toistuvia tavuja. Tätä hyödyntämällä hyökkääjä voi kokeilemalla arvata oikeita tuloksia, sillä palvelimen vastauksien koon perusteella voidaan päätellä, onko testattu tavu oikein. Käytännössä hyökkäys toimii parhaiten selainten istuntojen Cookie arvojen selvittämisessä. Esimerkiksi verkkopankki istuntojen kohdalla. Kuvassa 10 on esitetty mahdollinen skenaario käyttäjän verkkopankkitietoihin käyttämällä hyväksi CRIME-haavoittuvuutta.



Kuva 10 CRIME-hyökkäys käyttäjän verkkopankin lähettämää Cookieta käyttäen. (Acunetix 2019, viitattu 8.12.2020)

4.4 BREACH

BREACH - eli Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext, on hyvin samankaltainen kuin edellisen kappaleen CRIME-hyökkäys. Tästä poiketen se on kuitenkin osoitettu HTTP-pakkaukseen.

Tässäkin tapauksessa on kyse MITM-hyökkäyksestä. Hyökkääjä harhauttaa kohteensa yhdistämään kolmannen osapuolen TLS-protokollaa käyttävälle sivustolle. Haavoittuvuutta käyttäen hyökkääjä voi tarkkailla kohteensa palvelimelle lähettämää dataa. (Acunetix 2019, viitattu 8.12.2020.)

Tämä hyökkäys on kohdistettu web-ohjelmiin ja sen estäminen on pitkälti ohjelman kehittäjän harteilla. Mikäli ohjelma ei peitä käyttäjän lähettämää dataa on hyökkäys mahdollista. (Acunetix 2019, viitattu 8.12.2020.)

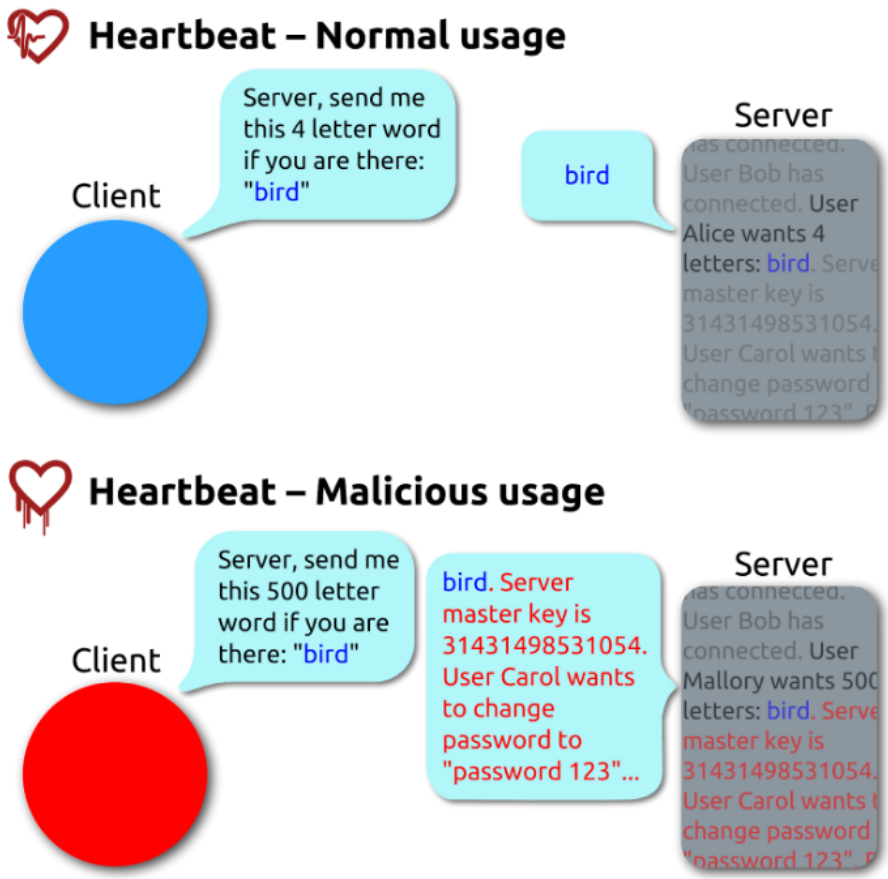
4.5 Heartbleed

Heartbleed on kriittinen haavoittuvuus, joka löydettiin yleisesti käytetystä OpenSSL-kirjastosta vuonna 2014. Haavoittuvuus käyttää hyväkseen tekniikan osaa, joka pitää asiakkaan ja palvelimen

välisen yhteyden aktiivisena. Heartbleed ei ole suoranaisesti TLS-protokollan aiheuttama haavoittuvuus, vaan kyse on OpenSSL-kirjaston viasta. (Synopsys/Heartbleed.com 2020, viitattu 8.12.2020.)

Tekniikka toimii siten, että asiakas lähettää palvelimelle paketin, jossa on dataa ja datan koosta kertova tieto. Palvelin vastaa tähän palauttamalla asiakkaalle saman paketin. (Acunetix 2019, viitattu 8.12.2020.) Tekniikka muistuttaa sydämen sykäystä, josta se on saanutkin nimensä.

Haavoittuvuudessa asiakas lähettää palvelimelle paketin dataa, jonka koon määre on väärä. Palvelin vastaa tähän palauttamalla asiakkaan paketin ja lisäksi omassa muistissaan ollutta dataa, koska vastauspaketin koon on vastattava asiakkaan pyyntöä. (Malwarebytes 2020, viitattu 8.12.2020.) Kuvassa 11 on graafinen esitys haavoittuvuuden toiminnasta käytännössä.



Kuva 11 Heartbleed-haavoittuvuuden toiminta. (Malwarebytes 2020, viitattu 8.12.2020)

Muista tässä opinnäytteessä esitellyistä poiketen, Heartbleed-haavoittuvuus on edelleen valitettavan yleinen. Korjaaminen vaatii OpenSSL-päivitystä palvelimen osalta, ja tämä ei jossain tapauksissa ole helppoa tai mahdollista.

5 TUTKIMUS

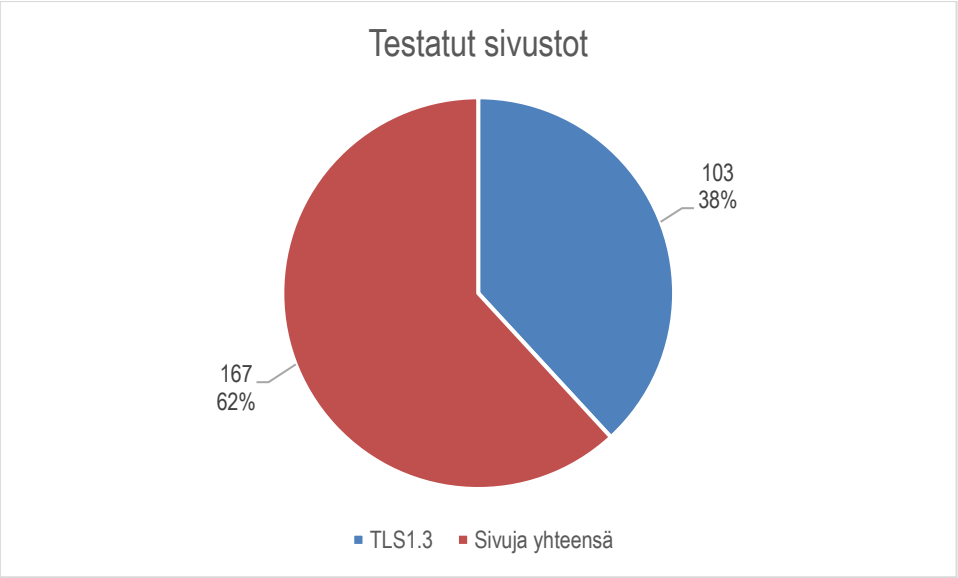
Tämän opinnäytteen tutkimuksen tavoitteena on tarkastella sadan suosituimman .fi päätettä käyttävän internetsivuston TLS tietoturvan tasoa käyttäen vapaassa jakelussa olevaa Qualys SSLlabs -yhtiön kehittämää rajapintaa, sekä sitä käyttävää työkalua.

Käyttämäni työkalu **drwetter/testssl.sh** on Linux Shell -skripta, jolla voidaan automatisoida suuri määrä hakuja osoitteista, sekä tulostaa lopputulos ihmisen luettavassa muodossa haluttujen parametrien mukaan. Työkalu on vapaassa jakelussa GPL-2.0-lisenssin alla.
Tutkimuksen pohjana tarvittava data hankittiin Domaintyper.com -palvelusta.

Työkalu testaa jokaisen sivuston tietoturvan haluttujen parametrien mukaan. Jokaisesta sivustosta luodaan tiedosto, jotka yhdistämällä saadaan suuri tietomäärä, joka on kuitenkin ihmisluettavissa sekä käsiteltävissä Excel Powerquery -ohjelmaa käyttäen. Tätä suurempi datamäärä, tai tarkempi analyyttinen tarkastelu, vaatisi jonkin toisen metodin käyttöä. Saamalleni tietomäärä on kuitenkin vielä hallittavissa yksinkertaisilla työkaluilla. Tässä opinnäytteessä esitelty tutkimusdata on anonymisoitu. Tutkimuksen data TLS 1.3 -version käytön yleisyyden osalta on esitetty Liitteessä 1.

5.1 TLS 1.3 käytön yleisyys

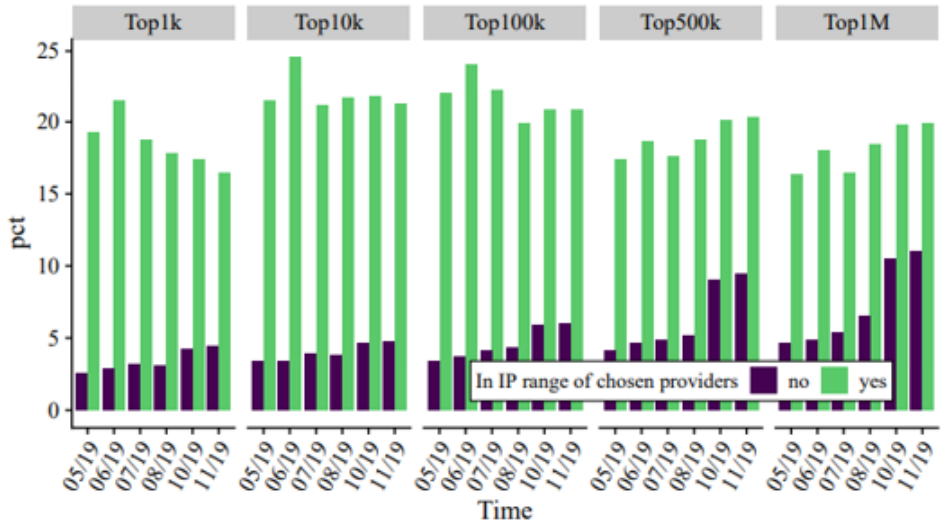
Erityisessä tarkkailussa oli uusimman TLS 1.3 -version hyödyntäminen palveluissa. Jotta SSLlabs -rajapintaa hyödyntävät työkalut voivat antaa sivustolle korkeimman mahdollisen arvosanan A, tulee sivuston tukea uusinta versiota.



Kuva 12, TLS version 1.3 käyttö kaikista testatuista sivuista sekä niiden alasivuista.

Kerätystä datasta käy ilmi, että 38 % testatuista sivustoista käyttää TLS 1.3 -versiota kokonaan tai osittain. Luku on yllättävän matala, sillä uusin versio on ollut julkaistuna tutkimuksen ajankohtana jo noin kaksi vuotta.

Tarkastelemalla ylikansallisen tutkimusryhmän dataa vuodelta 2019, voidaan todeta, että kasvu on kuitenkin jokseenkin odotettavissa. Uusien versioiden käyttöä hidastaa tiuha päivitystahti, joka aiheuttaa kuormitusta ja ongelmia ylläpitäjille sekä mahdolliset komplikaatiot vanhempien sovelluksien toimivuuden kanssa. Kuvassa 14 on graafi version 1.3 käytön yleisyydestä tutkimuksesta vuodelta 2019. Data on suurimpien palveluntarjoajien ylläpitämistä sivuista.



Kuva 13 TLS 1.3 Käytön tutkimus vuodelta 2019. (Holz, Hiller, Amann & al. 2019, viitattu 4.12.2020)

5.2 Turvallisuuden analysointi

Tässä kappaleessa käydään läpi tutkimuksessa käytetyn työkalun yhdelle sivustolle suorittama analyysi tarkemmin. Ohjelma tarkistaa ja tulostaa käyttäjän valitsemien parametrien mukaan raportin haetusta palvelusta. Tässä tapauksessa tarkasteltu palvelu on siis internetsivusto. Yläotsikoilla id, severity ja finding ohjelma listaa testatun osion, tietoturvan tason sekä mahdollisia lisätietoja. CVE ja CWE ovat lyhenteitä termeistä Common Vulnerability Enumeration sekä Common Weakness Enumeration. Näiden avulla merkitään MITRE-yhtiön ylläpitämien haavoittuvuustietokantojen käyttämiä numerointeja.

Riveillä 4–12 työkalu tarkistaa tarjotut SSL/TLS-versiot sekä niiden tason. Mikäli protokollaa ei tueta kokonaan tai tarjotaan heikompi tilalle, myös siitä ilmoitetaan. Riveillä 13–20 tarkistetaan palvelun tarjoamat salauskirjastot. Ohjelma tarkistaa OpenSSL-kirjaston tarjoamia osia. Riveillä 21–23 tarkistetaan Forward Secrecy. Työkalu ilmoittaa myös käytetyt salaukset. Rivit 24–43 ovat työkalun

suorittamaa haavoittuvuuksien tarkistusta. Työkalu ilmoittaa tietoturvan tilan sekä mahdollisia huomioita kyseisestä haavoittuvuudesta. Haavoittuvuuksien osalta ilmoitetaan myös niille annettu CVE-numerointi. Kuvassa 12 esitetään työkalun antama testitulos yhden sivuston osalta.

1	id	port	severity	finding	cve	cwe
2	service	443	INFO	HTTP		
3	pre_128cipher	443	INFO	No 128 cipher limit bug		
4	SSLv2	443	OK	not offered		
5	SSLv3	443	OK	not offered		
6	TLS1	443	INFO	not offered		
7	TLS1_1	443	INFO	is not offered		
8	TLS1_2	443	OK	offered		
9	TLS1_3	443	INFO	not offered + downgraded to weaker protocol		
10	NPN	443	INFO	offered with h2, http/1.1 (advertised)		
11	ALPN_HTTP2	443	OK	h2		
12	ALPN	443	INFO	http/1.1		
13	cipherlist_NULL	443	OK	not offered		CWE-327
14	cipherlist_aNULL	443	OK	not offered		CWE-327
15	cipherlist_EXPORT	443	OK	not offered		CWE-327
16	cipherlist_LOW	443	OK	not offered		CWE-327
17	cipherlist_3DES_IDEA	443	INFO	not offered		CWE-310
18	cipherlist_AVERAGE	443	LOW	offered		CWE-310
19	cipherlist_GOOD	443	OK	offered		
20	cipherlist_STRONG	443	OK	offered		
21	FS	443	OK	offered		
22	FS_ciphers	443	INFO	ECDHE-RSA-CHACHA20-POLY1305-OLD ECDHE-RSA-AES256-GCM-SHA3		
23	FS_ECDHE_curves	443	OK	prime256v1 secp384r1 secp521r1 X25519		
24	heartbleed	443	OK	not vulnerable, no heartbeat extension	CVE-2014-	CWE-119
25	CCS	443	OK	not vulnerable	CVE-2014-	CWE-310
26	ticketbleed	443	OK	not vulnerable	CVE-2016-	CWE-200
27	ROBOT	443	OK	not vulnerable	CVE-2017-	CWE-203
28	secure_renego	443	OK	supported		CWE-310
29	secure_client_renego	443	OK	not vulnerable	CVE-2011-	CWE-310
30	CRIME_TLS	443	OK	not vulnerable	CVE-2012-	CWE-310
31	BREACH	443	OK	not vulnerable, no gzip/deflate/compress/br	CVE-2013-	CWE-310
32	POODLE_SSL	443	OK	not vulnerable, no SSLv3	CVE-2014-	CWE-310
33	fallback_SCSV	443	OK	no protocol below TLS 1.2 offered		
34	SWEET32	443	OK	not vulnerable	CVE-2016-	CWE-327
35	FREAK	443	OK	not vulnerable	CVE-2015-	CWE-310
36	DROWN	443	OK	not vulnerable on this host and port	CVE-2016-	CWE-310
37	DROWN_hint	443	INFO	Make sure you don't use this certificate elsev	CVE-2016-	CWE-310
38	LOGJAM	443	OK	not vulnerable, no DH EXPORT ciphers,	CVE-2015-	CWE-310
39	LOGJAM-common_primes	443	OK	no DH key with <= TLS 1.2	CVE-2015-	CWE-310
40	BEAST	443	OK	not vulnerable, no SSL3 or TLS1	CVE-2011-	CWE-20
41	LUCKY13	443	LOW	potentially vulnerable, uses TLS CBC ciphers	CVE-2013-	CWE-310
42	winshock	443	OK	not vulnerable	CVE-2014-	CWE-94
43	RC4	443	OK	not vulnerable	CVE-2013-	CWE-310

Kuva 14 Yhden sivuston testitulos

6 POHDINTA

Opinnäytteessä tarkasteltiin TLS-protokollaa kehityksen, tekniikan ja tietoturvan osalta. Kohteena olevan tekniikan laajuuden vuoksi jouduttiin aiheen joitain osia käymään läpi pintapuolisesti kuitenkin niin, että lukijalle välittyisi kokonaisuudesta hallittu kuva. Tekniikka on yksi tärkeimmistä ja käytetyimmistä tietoturvan muodoista internetissä ja sähköisessä kommunikaatiossa, joten koin aiheen tähdelliseksi nostaa esille varsinkin, koska perusopinnoissa TLS jäi hyvin pintapuoliseksi raapaisuksi.

Tässä opinnäytteessä esitellyt haavoittuvuudet tulivat valikoiduksi niiden saavuttaman tunnettavuuden ja niiden hyödyntämien tietoturva-aukkojen vakavuuden vuoksi. On huomattava, että Heartbleed-haavoittuvuus on osittain edelleen paikkaamatta useissa palvelimissa, sillä se vaatii OpenSSL toteutuksen päivittämistä mikä voi olla hankalaa tai jopa mahdotonta mikäli käytössä on siihen kytketty vanhempi ohjelmisto.

TLS tekniikka aiheena olisi niin laaja, että opinnäytteeseen varattu aika ja resurssit eivät sen läpikäymiseen riitä. Mikäli aiheeseen haluaa todella paneutua, vierähtäisi aikaa reilusti enemmän. Opinnäytettä kirjoittaessa onkin herännyt mielenkiinto suorittaa aiheesta tutkimusta edelleen mahdollisten jatko-opintojen parissa. Jatkokehitystä voisi ajatella suuremman datamäärän keräämisen sekä TLS 1.3 -version nopeuden testauksen osalta.

Jälkeenpäin ajateltuna tutkimuksesta saisi kokonaisvaltaisemman ja datan osalta tarkemman, mikäli tiedon keruu tutkimusta varten olisi aloitettu opintojen aikana. Opinnäytettä tehdessä aihe tuli entistä tarkemmin tutuksi varsinkin tekniikoiden osalta. Lisäksi tieteellinen tutkimus sekä tiedon ilmaiseminen lyhyesti olivat asioita, jotka tulivat työtä tehdessä tutuiksi.

Opinnäytettä työstäessä vallinneiden poikkeusolojen ja henkilökohtaisten ongelmien vuoksi aikataulu meni kirjoittamisen osalta pitkäksi. Alkuperäisenä ajatuksena oli suorittaa opinnäytteen tutkimus yritysyhteistyössä. Tämä kuitenkin peruuntui pandemian vuoksi. Opinnäyte kuitenkin onnistui mielestäni ongelmista huolimatta kohtalaisen hyvin.

LÄHTEET

Acunetix 2019. TLS Security 6: Examples of TLS Vulnerabilities and Attack. Hakupäivä 1.12.2020. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/

Cloudflare 2020. How Does Public Key Encryption Work? | Public Key Cryptography and SSL Hakupäivä 14.12.2020. https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/

Cloudflare 2020. What is TLS (Transport Layer Security)? Hakupäivä 22.4.2020. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

Cloudflare 2020. What is SSL | SSL definition. Hakupäivä 22.4.2020 https://www.cloudflare.com/learning/ssl/what-is-ssl/

Cloudflare 2019. Even faster connection establishment with QUIC 0-RTT resumption. Hakupäivä 26.11.2020. https://blog.cloudflare.com/even-faster-connection-establishment-with-quic-0-rtt-resumption/

Cloudflare, Nick Sullivan 2018. A Detailed Look at RFC 8446 (a.k.a. TLS 1.3). Hakupäivä 14.12.2020. https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/

Globalsign 2017. What is a Man-in-the-Middle Attack and How Can You Prevent It? Hakupäivä 8.12.2020 https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack

Google 2020. Deprecations and removals in Chrome 84. Hakupäivä 23.4.2020 https://developers.google.com/web/updates/2020/05/chrome-84-deps-rems

Ilan Benichou, Eleven Labs 2020. Understanding SSL/TLS: Part 1 – What is it?. Hakupäivä 1.6.2020
https://blog.eleven-labs.com/en/understanding-ssltls-part-1/

IETF 2013. TLS 1.3 Wish List. Hakupäivä 20.5.2020
https://www.ietf.org/proceedings/87/slides/slides-87-tls-5.pdf

Medium 2020. Making Sense of SSL/TLS. Hakupäivä 1.6.2020
https://medium.com/demystifying-security/making-sense-of-ssl-tls-b600133f52bc

Namecheap 2019. Perfect Forward Secrecy. What it is? Hakupäivä 3.10.2020.
https://www.namecheap.com/support/knowledgebase/article.aspx/9652/38/perfect-forward-secrecy-what-it-is#:~:text=Forward%20Secrecy%20(also%20known%20as,the%20session%20keys%20used%20in

Ralph Holz, Jens Hiller, Johanna Amann, Abbas Razaghpanah, Thomas Jost, Narseo Vallina-Rodriguez, Oliver Hohlfeld, 2020. Tracking the deployment of TLS 1.3 on the Web: A story of experimentation and centralization. Hakupäivä 12.6.2020.
https://ralphholz.science/publications/TrackingTheDeploymentOfTls13OnTheWebAStoryOfExperimentationAndCentralization.pdf

Synopsys, Heartbleed.com 2020. Hakupäivä 8.12.2020
https://heartbleed.com/#:~:text=The%20Heartbleed%20Bug%20is%20a,used%20to%20secure%20the%20Internet.

LIITTEET

TLS 1.3 testitulokset liite 1

	B	C	D	E	F	G
1	service	site	port	INFO	HTTP	Column
2	TLS1_3	site 1	443	INFO	not offered + downgraded to weaker protocol	
3	TLS1_3	site 2	443	INFO	not offered + downgraded to weaker protocol	
4	TLS1_3	site 3	443	OK	offered with final	
5	TLS1_3	site 4	443	OK	offered with final	
6	TLS1_3	site 5	443	OK	offered with final	
7	TLS1_3	site 6	443	OK	offered with final	
8	TLS1_3	site 7	443	INFO	not offered + downgraded to weaker protocol	
9	TLS1_3	site 8	443	INFO	not offered + downgraded to weaker protocol	
10	TLS1_3	site 9	443	OK	offered with final	
11	TLS1_3	site 10	443	INFO	not offered + downgraded to weaker protocol	
12	TLS1_3	site 11	443	INFO	not offered + downgraded to weaker protocol	
13	TLS1_3	site 12	443	OK	offered with final	
14	TLS1_3	site 13	443	OK	offered with final	
15	TLS1_3	site 14	443	OK	offered with final	
16	TLS1_3	site 15	443	OK	offered with final	
17	TLS1_3	site 16	443	OK	offered with draft 28, draft 27, draft 26, final	
18	TLS1_3	site 17	443	OK	offered with final	
19	TLS1_3	site 18	443	OK	offered with final	
20	TLS1_3	site 19	443	OK	offered with final	
21	TLS1_3	site 20	443	INFO	not offered + downgraded to weaker protocol	
22	TLS1_3	site 21	443	INFO	not offered + downgraded to weaker protocol	
23	TLS1_3	site 22	443	OK	offered with draft 28, draft 27, draft 26, final	
24	TLS1_3	site 23	443	INFO	not offered + downgraded to weaker protocol	
25	TLS1_3	site 24	443	INFO	not offered + downgraded to weaker protocol	
26	TLS1_3	site 25	443	INFO	not offered + downgraded to weaker protocol	
27	TLS1_3	site 26	443	INFO	not offered + downgraded to weaker protocol	
28	TLS1_3	site 27	443	OK	offered with final	
29	TLS1_3	site 28	443	OK	offered with final	
30	TLS1_3	site 29	443	INFO	not offered + downgraded to weaker protocol	
31	TLS1_3	site 30	443	INFO	not offered + downgraded to weaker protocol	
32	TLS1_3	site 31	443	INFO	not offered + downgraded to weaker protocol	
33	TLS1_3	site 32	443	OK	offered with final	
34	TLS1_3	site 33	443	OK	offered with final	
35	TLS1_3	site 34	443	OK	offered with final	
36	TLS1_3	site 35	443	OK	offered with final	
37	TLS1_3	site 36	443	OK	offered with final	
38	TLS1_3	site 37	443	INFO	not offered + downgraded to weaker protocol	
39	TLS1_3	site 38	443	OK	offered with final	
40	TLS1_3	site 39	443	INFO	not offered + downgraded to weaker protocol	
41	TLS1_3	site 40	443	OK	offered with final	
42	TLS1_3	site 41	443	INFO	not offered + downgraded to weaker protocol	
43	TLS1_3	site 42	443	INFO	not offered + downgraded to weaker protocol	
44	TLS1_3	site 43	443	OK	offered with final	
45	TLS1_3	site 44	443	OK	offered with final	
46	TLS1_3	site 45	443	OK	offered with final	
47	TLS1_3	site 46	443	OK	offered with final	
48	TLS1_3	site 47	443	INFO	not offered + downgraded to weaker protocol	
49	TLS1_3	site 48	443	INFO	not offered + downgraded to weaker protocol	
50	TLS1_3	site 49	443	INFO	not offered + downgraded to weaker protocol	
51	TLS1_3	site 50	443	OK	offered with final	
52	TLS1_3	site 51	443	OK	offered with final	
53	TLS1_3	site 52	443	OK	offered with final	
54	TLS1_3	site 53	443	OK	offered with final	
55	TLS1_3	site 54	443	OK	offered with final	
56	TLS1_3	site 55	443	OK	offered with final	
57	TLS1_3	site 56	443	OK	offered with final	
58	TLS1_3	site 57	443	INFO	not offered + downgraded to weaker protocol	
59	TLS1_3	site 58	443	INFO	not offered + downgraded to weaker protocol	
60	TLS1_3	site 59	443	INFO	not offered + downgraded to weaker protocol	
61	TLS1_3	site 60	443	OK	offered with final	
62	TLS1_3	site 61	443	OK	offered with final	
63	TLS1_3	site 62	443	OK	offered with final	
64	TLS1_3	site 63	443	INFO	not offered + downgraded to weaker protocol	
65	TLS1_3	site 64	443	INFO	not offered + downgraded to weaker protocol	
66	TLS1_3	site 65	443	OK	offered with final	
67	TLS1_3	site 66	443	OK	offered with final	
68	TLS1_3	site 67	443	OK	offered with final	
69	TLS1_3	site 68	443	OK	offered with final	
70	TLS1_3	site 69	443	OK	offered with final	
71	TLS1_3	site 70	443	OK	offered with final	
72	TLS1_3	site 71	443	OK	offered with final	
73	TLS1_3	site 72	443	OK	offered with final	
74	TLS1_3	site 73	443	INFO	not offered + downgraded to weaker protocol	
75	TLS1_3	site 74	443	OK	offered with final	
76	TLS1_3	site 75	443	OK	offered with final	
77	TLS1_3	site 76	443	OK	offered with final	
78	TLS1_3	site 77	443	OK	offered with final	
79	TLS1_3	site 78	443	INFO	not offered + downgraded to weaker protocol	
80	TLS1_3	site 79	443	OK	offered with final	

81	TLS1_3	site 80	443	OK	offered with final	
82	TLS1_3	site 81	443	INFO	not offered + downgraded to weaker protocol	
83	TLS1_3	site 82	443	INFO	not offered + downgraded to weaker protocol	
84	TLS1_3	site 83	443	INFO	not offered + downgraded to weaker protocol	
85	TLS1_3	site 84	443	INFO	not offered + downgraded to weaker protocol	
86	TLS1_3	site 85	443	INFO	not offered + downgraded to weaker protocol	
87	TLS1_3	site 86	443	INFO	not offered + downgraded to weaker protocol	
88	TLS1_3	site 87	443	OK	offered with final	
89	TLS1_3	site 88	443	OK	offered with final	
90	TLS1_3	site 89	443	OK	offered with final	
91	TLS1_3	site 90	443	OK	offered with final	
92	TLS1_3	site 91	443	INFO	not offered + downgraded to weaker protocol	
93	TLS1_3	site 92	443	INFO	not offered + downgraded to weaker protocol	
94	TLS1_3	site 93	443	INFO	not offered + downgraded to weaker protocol	
95	TLS1_3	site 94	443	INFO	not offered + downgraded to weaker protocol	
96	TLS1_3	site 95	443	INFO	not offered + downgraded to weaker protocol	
97	TLS1_3	site 96	443	INFO	not offered + downgraded to weaker protocol	
98	TLS1_3	site 97	443	OK	offered with final	
99	TLS1_3	site 98	443	OK	offered with final	
100	TLS1_3	site 99	443	OK	offered with final	
101	TLS1_3	site 100	443	OK	offered with final	
102	TLS1_3	site 101	443	INFO	not offered + downgraded to weaker protocol	
103	TLS1_3	site 102	443	OK	offered with final	
104	TLS1_3	site 103	443	OK	offered with final	
105	TLS1_3	site 104	443	OK	offered with final	
106	TLS1_3	site 105	443	OK	offered with final	
107	TLS1_3	site 106	443	INFO	not offered + downgraded to weaker protocol	
108	TLS1_3	site 107	443	INFO	not offered + downgraded to weaker protocol	
109	TLS1_3	site 108	443	OK	offered with final	
110	TLS1_3	site 109	443	OK	offered with final	
111	TLS1_3	site 110	443	OK	offered with final	
112	TLS1_3	site 111	443	OK	offered with final	
113	TLS1_3	site 112	443	OK	offered with final	
114	TLS1_3	site 113	443	OK	offered with final	
115	TLS1_3	site 114	443	OK	offered with final	
116	TLS1_3	site 115	443	INFO	not offered + downgraded to weaker protocol	
117	TLS1_3	site 116	443	INFO	not offered + downgraded to weaker protocol	
118	TLS1_3	site 117	443	INFO	not offered + downgraded to weaker protocol	
119	TLS1_3	site 118	443	INFO	not offered + downgraded to weaker protocol	
120	TLS1_3	site 119	443	CRITICAL	connection failed rather than downgrading to SSL	
121	TLS1_3	site 120	443	OK	offered with final	
122	TLS1_3	site 121	443	OK	offered with final	
123	TLS1_3	site 122	443	INFO	not offered + downgraded to weaker protocol	
124	TLS1_3	site 123	443	INFO	not offered + downgraded to weaker protocol	
125	TLS1_3	site 124	443	INFO	not offered + downgraded to weaker protocol	
126	TLS1_3	site 125	443	OK	offered with final	
127	TLS1_3	site 126	443	OK	offered with final	
128	TLS1_3	site 127	443	OK	offered with final	
129	TLS1_3	site 128	443	OK	offered with final	
130	TLS1_3	site 129	443	INFO	not offered + downgraded to weaker protocol	
131	TLS1_3	site 130	443	INFO	not offered + downgraded to weaker protocol	
132	TLS1_3	site 131	443	INFO	not offered + downgraded to weaker protocol	
133	TLS1_3	site 132	443	INFO	not offered + downgraded to weaker protocol	
134	TLS1_3	site 133	443	INFO	not offered + downgraded to weaker protocol	
135	TLS1_3	site 134	443	INFO	not offered + downgraded to weaker protocol	
136	TLS1_3	site 135	443	INFO	not offered + downgraded to weaker protocol	
137	TLS1_3	site 136	443	OK	offered with final	
138	TLS1_3	site 137	443	INFO	not offered + downgraded to weaker protocol	
139	TLS1_3	site 138	443	OK	offered with final	
140	TLS1_3	site 139	443	OK	offered with final	
141	TLS1_3	site 140	443	OK	offered with final	
142	TLS1_3	site 141	443	OK	offered with final	
143	TLS1_3	site 142	443	OK	offered with final	
144	TLS1_3	site 143	443	OK	offered with final	
145	TLS1_3	site 144	443	OK	offered with final	
146	TLS1_3	site 145	443	OK	offered with final	
147	TLS1_3	site 146	443	OK	offered with final	
148	TLS1_3	site 147	443	OK	offered with final	
149	TLS1_3	site 148	443	OK	offered with final	
150	TLS1_3	site 149	443	OK	offered with final	
151	TLS1_3	site 150	443	INFO	not offered + downgraded to weaker protocol	
152	TLS1_3	site 151	443	INFO	not offered + downgraded to weaker protocol	
153	TLS1_3	site 152	443	OK	offered with final	
154	TLS1_3	site 153	443	OK	offered with final	
155	TLS1_3	site 154	443	OK	offered with final	
156	TLS1_3	site 155	443	OK	offered with final	
157	TLS1_3	site 156	443	INFO	not offered + downgraded to weaker protocol	
158	TLS1_3	site 157	443	INFO	not offered + downgraded to weaker protocol	
159	TLS1_3	site 158	443	OK	offered with final	
160	TLS1_3	site 159	443	OK	offered with final	

161	TLS1_3	site 160	443	OK	offered with final	
162	TLS1_3	site 161	443	OK	offered with final	
163	TLS1_3	site 162	443	OK	offered with final	
164	TLS1_3	site 163	443	OK	offered with final	
165	TLS1_3	site 164	443	OK	offered with final	
166	TLS1_3	site 165	443	OK	offered with final	
167	TLS1_3	site 166	443	OK	offered with final	
168	TLS1_3	site 167	443	OK	offered with final	