

Verkkovarmenteet yrityskäytössä

Tatu Erkinjuntti, Jussi Isosomppi, Eino Kupias, Saku Kähäri

Tietoturvan hallinta

ICT4TN026

**Työsuunnitelma**

# Tavoitteet ja lopputulokset

Projektin tavoite on tutkia erilaisia verkkoselaimissa käytettäviä varmenteita, niiden hyötyjä, mahdollisia haittoja sekä haavoittuvuuksia.

Projektissa on kaksi eri vaihetta, jotka seuraavat toisiaan.

Ensimmäisessä vaiheessa tutkitaan käytössä olevia varmenteita sekä pyritään hahmottamaan niiden välisiä eroja yrityskäytön kannalta. Projekti keskittyy tutkimaan kahta eri public key infrastructuren (PKI) piiriin kuluvaa menetelmää: Certificate Authorities (CA) sekä Web of Trust (WoT). Näiden osalta tulee myös tutkia varmenteissa käytettäviä salakirjoitusmenetelmiä, tässä tapauksessa pääasiallisesti X.509 sekä PGP. Lisäksi pyritään selvittämään varmenteiden käytön ongelmakohdat. Tämän kautta pyritään selvittämään, onko ongelma ehkäistävissä, sekä onko olemassa mahdollisia haavoittuvuuksia, jotka mahdollistaisivat sen hyväksikäytön.

Projektin toisessa vaiheessa on tarkoitus testata ensimäisessä vaiheessa löytyneitä ongelmakohtia, sekä pyrkiä hyväksikäyttämään tai ehkäisemään niitä.

Projektin alussa suunnitellut alustavat testit, joita on tarkoitus suorittaa toisessa vaiheessa:

* Varmenteen blacklistaus
* Välimieshyökkäys keinotekoisella varmenteella

Toisessa vaiheessa suoritettavat testit määräytyvät tarkemmin ensimmäisessä vaiheessa esiin tulleiden tietojen perusteella, joten alustavasti suunnitellut testit tarkentuvat tai muuttuvat myöhemmin projektin aikana. Tarkoitus on ottaa mukaan myös testejä, joita ei projektin alussa vielä hahmotettu käytettävän.

Projektin lopputuloksena on tarkoitus kehittää ohjeitus, jota voidaan soveltaa yrityksen näkökannasta.

Projektin loppuraportissa tullaan esittelemään, miten tutkimuksessa esiin tulleet tulokset on huomioitu ohjeistuksessa.

# Tehtävän rajaus

Projektin ei ole tarkoitus tutkia tai testava yritysten itse luomia varmenteita, tai varmenteita jotka eivät kuulu public key infrastructuren (PKI) piiriin. Projektin tarkoitus on tutkia ja testata vain varmenteita, joita käytetään verkkoselainpohjaisissa ratkaisuissa.

# Riskit ja niihin varautuminen

Koska projektissa on monta liikkuva osaa, on näiden osalta myös useampia riskejä jotka uhkaavat projektin onnistunutta loppuun saattamista.

Projektiryhmän jäsenen sairastuminen tai pois jääminen projektissa on riski, jota projektiryhmän on vaikea ennalta ehkäistä. Tähän tulee varautua hyvällä projektin dokumentoinnilla sekä projektiryhmän jäsenten perehtymisellä projektin eri osa-alueisiin, jotta mahdollinen projektiryhmän jäsenen väliaikainen tai pysyvä poisjääminen saadaan paikattua, eikä se näin aiheuta pysyvää haittaa projektille.

Työaika sekä sen rajallisuus on myös haaste projektin valmistumiselle. Jotta määritellyssä aikataulussa pysytään, tulee projektiryhmän jäsenten kesken jaettavat työtehtävät määritellä riittävän tarkasti, jotta niistä saadaan tavoitteen mukainen lopputulos. Tämä edesauttaa myös projektin aikataulussa pysymistä.

Koska varmenteiden käyttö tietoturvaratkaisuissa on yleistä, tulee tutkiminen rajata vain projektin tavoitteiden mukaisesti. Muuten on vaarana, että projektin tutkiminen eksyy tavoitteestaan, mikä johtaa epäoptimaaliseen työajan käyttöön.

# Työryhmä

Työryhmän jäsenet:

* Tatu Erkinjuntti
* Jussi Isosomppi
* Eino Kupias
* Saku Kähäri

# Työympäristö

Projekti tullaan pääsääntöisesti suorittamaan Haaga-Helian Pasilan kampuksen tiloissa.

# Aikataulu

| **Viikko** | **Työtehtävät** |
| --- | --- |
| vko 43 | Teorian tutkiminen |
| vko 44 | Teorian tutkiminen |
| vko 45 | Teorian tutkiminen |
| vko 46 | Testaus |
| vko 47 | Testaus |
| vko 48 | Testaus |
| vko 49 | Ohjeistuksen sekä projektin loppuraportin valmistelua. |
| vko 50 | Projektin loppuraportin esitteleminen. |

# Tehtävät, työmäärät ja lopputulokset

| **Tehtävät** | **Työmäärät** | **Lopputulokset** |
| --- | --- | --- |
| Public key infrastructure tutkiminen | 10 tuntia | parempi tietämys PKI:a |
| Käytettävien salakirjoitusmenetelmien tutkiminen (PGP, X.509) | 10 tuntia | Parempi ymmärrys käytettävistä salakirjoitusmenetelmistä |
| Web of Trust tutkiminen | 10 tuntia | parempi tietämys WOT:a |
| Certificate authorities tutkiminen | 10 tuntia | parempi tietämys CA:a |
| Kahden varmennemenetelmän vertailu, haitat sekä hyödyt | 15 tuntia | varmennemenetelmien haitat sekä hyödyt selvitetty |
| Ongelmakohtien tunnistaminen varmennemenetelmistä | 20 tuntia | Varmenteiden ongelmakohdat tunnistettu |

Vaihe 2 Alustavasti toiseen vaiheeseen suunnitellut tehtävät:

| **Tehtävät** | **Työmäärät** | **Lopputulokset** |
| --- | --- | --- |
| Suoritettaviena testien suunittelu | 25 tuntia | valmis testi suunnitelma |
| Testien toteutus | 50 tuntia | valitut testit suoritettu |
| Oheistuksen laatiminen | 12.5 tuntia | Valmis ohjeitus |
| loppuraportin laatiminen | 12.5 tuntia | valmis loppuraportti |

# Dokumentointi- ja versionhallintamenettelyt

Kaikki projektiin liittyvä dokumentointi tallenetaan, sekä jaetaan käyttäen projektin omaa Git repository:a. Tämä ylläpitää myös versionhallinan projektin dokumenteista.