link22

Kedjad autentisering med smarta kort och TLS

Bakgrund

link22 AB utvecklar, inför och vidmakthåller IT-säkerhets- och systemlösningar till kunder inom offentlig sektor och större organisationer. Våra kunder återfinns inom svensk försvarsindustri, underrättelseorganisationer och svenska myndigheter. Gemensamt för våra kunder är högt ställda krav på sekretess, integritet och tillgänglighet för system som hanterar sekretessbelagd information. Identifiering, autentisering och spårbarhet hanteras med smarta kort och PKI-lösningar.

Uppsatsbeskrivning

En vanlig metod för att skydda information i en klient-server-arkitektur är att skapa en krypterad tunnel från klient till server där kommunikationen skyddas med en gemensam sessionsnyckel. Sessionsnyckeln förhandlas fram i en handskakningsalgoritm som föregås av en identifiering och autentisering av motstående part. I ett PKI-baserat system används certifikat med tillhörande asymmetriska nycklar, exempel på kryptografiskt protokoll som används är TLS 1.2.

I vissa tillämpningar är det önskvärt att bilda kedjande anslutningar där klient A kopplar upp sig via en krypterad tunnel till server B som i sin tur kopplar upp anslutning till server C och så vidare. Ett problem som uppstår är att certifikatet som används för att identifiera klient A inte används när tunneln från B till C skapas. Önskvärt vore att A:s certifikat används även för tunneln från B till C.

Vi behöver finna en metod för att hantera kedjade anslutningar när TLS 1.2 används som kryptografiskt protokoll. Denna metod behöver sedan analyseras ur flera olika aspekter, däribland dess kryptografiska egenskaper och begränsningar, metodens komplexitet och prestanda samt potentiella svagheter och attackvektorer.

Förväntat resultat

Examensarbetet förväntas leda till en analys av den problematik och de möjligheter som finns vid implementation av kedjad autentisering över TLS. Vi tror att en egen konceptimplementation, eller utökning av en existerande lösning, är nödvändig för en fullgod analys.

Omfattning och kvalifikationer

Examensarbetet omfattar 30 hp för en person. Studenten behöver goda kunskaper inom programmering (C/C++) samt ha läst kurser inom informationssäkerhet, mjukvarusäkerhet, kryptografi eller motsvarande.

Kontaktperson

Jakob Pogulis
jakob.pogulis@link22.se
072 – 921 59 97