Nasjonal sikkerhetsmyndighet

IT-veiledning for ugradert nr 14 (U-14)
Oppdatert: 2016-09-30

Transport Layer Security (TLS)

Sikring av kommunikasjon med TLS

Beskrivelse av grunnleggende tiltak for sikring kommunikasjon over usikre nett ved hjelp av TLS

Dette dokumentet er NSMs anbefaling for grunnleggende sikring av overføring av informasjon mellom ulike systemer.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20. mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse	**Sivil telefon/telefax**	**Militær telefon/telefaks**	**Internettadresse**
Postboks 14	+47 67 86 40 00/+47 67 86 40 09	515 40 00/515 40 09	www.nsm.stat.no
1306 BÆRUM	**E-postadresse**		
POSTTERMINAL	post@nsm.stat.no		

Innhold

1 Innledning

Transport Layer Security (TLS) er en kryptografisk protokoll som ivaretar autentisitet, integritet og konfidensialitet av kommunikasjon. TLS legger seg over *Transmission Control Protocol* (TCP) og kan benyttes av ulike protokoller, applikasjoner og tjenester som har behov for sikret kommunikasjon. Dette dokumentet beskriver TLS og anbefaler hvordan TLS skal benyttes.

NSM anbefaler at mest mulig kommunikasjon benytter TLS for autentisering, integritets- og konfidensialitetsbeskyttelse. Dette vil sikre enorme mengder data over Internett, hvor fortsatt under halvparten av kommunikasjonen er sikret.

Det er en forutsetning at den man tar kontakt med (tjener) autentiserer seg. I noen tilfeller bør også den som tar kontakt (klient) autentisere seg. Når parten(e) er autentisert, vil man etablere integritets- og konfidensialitetsbeskyttet kommunikasjon.

I tillegg til å sikre ønsket trafikk, må man hindre uønsket, kryptert kommunikasjon. Uønsket, kryptert kommunikasjon kan skjule kompromittering og eksfiltrering av informasjon. Bare kommunikasjon som organisasjonen kjenner til og godkjenner bør tillates.

For systemer som ikke kan benytte TLS eller hvor risikovurdering tilsier at spesifikke tiltak ikke kan implementeres for sikring av informasjon, anbefaler NSM å se på andre protokoller eller mekanismer som kan tilby sikker kommunikasjon.

Kontaktpunkt for denne veiledningen er post@nsm.stat.no. Vennligst bruk veiledningens navn som emne. Kommentarer og innspill mottas med takk.

2 Om TLS

Ulike aktører har tilgang til ulike deler av Internett og det har vist seg at en rekke ulike aktører avlytter kommunikasjonen over Internett. I tillegg har en rekke sårbarheter i programvare og protokoller, gjort det enklere å manipulere og få tilgang til informasjon og systemer.

Krypteringsprotokollen TLS er den vanligste løsningen for autentisering, integritets- og konfidensialitetsbeskyttelse av kommunikasjon mellom ulike systemer over usikre kanaler. TLS befinner seg på applikasjonslaget, og de mest kjente anvendelsene av TLS er HTTPS, SMTP over TLS, STARTTLS og OpenVPN.

TLS er en videreutvikling av *Secure Sockets Layer (SSL)* som ble publisert i 1995. SSL 3.0 var siste versjon av SSL og kom i 1996. I 2014 ble SSL-protokollen knekt og forkastet i 2015 gjennom RFC 7568.

Bruken av TLS-protokollen deles opp i to faser[1]:

1) Etablering av sikker forbindelse mellom klient og tjener
    a. Valg av protokoll og kryptografiske algoritmer
    b. Autentisering av server (og eventuelt klient) basert på sertifikat
    c. Utveksling av kryptografiske parametere
    d. Etablering av krypteringsnøkkel for sesjonen
2) Utveksling av applikasjonsdata over den sikre forbindelsen

Første fase skjer hovedsak i klartekst. Det betyr at i tillegg til informasjon som IP-adresser, kan sertifikater som utveksles i etableringsfasen avlyttes.

Når TLS er etablert for en tjeneste, vil informasjonen overføres uten at andre som har tilgang til linjene trafikken passerer gjennom, kan se innholdet. TLS gir samme beskyttelse mot avlytting på lokale nett, som mot avlytting på Internett.

[1] Basert på U-03, kapittel 2.2

3 Anbefalte tiltak

NSM anbefaler at TLS benyttes i størst mulig grad, da protokollen er tilgjengelig i mange ulike systemer og tjenester. I mange tilfeller vil det å benytte TLS bety å «aktivere» TLS i applikasjonen eller tjenesten man ønsker å sikre. Det er likevel viktig at man konfigurerer protokollen korrekt.

Tjeneren bør kreve TLS-tilkobling for å være sikker på at man benytter TLS. På denne måten vil klienter som prøver å etablere usikker forbindelse, bli sperret. I tillegg til å hindre usikre klienter, vil man på denne måten få oversikt over hvilke klienter som ennå ikke er konfigurert til å benytte TLS.

Benytt STARTTLS dersom man ikke kan kreve at TLS skal benyttes. Dette er en protokoll som prøver å «oppgradere» enhver type usikker forbindelse til sikker, ved at man spør om kryptert forbindelse er tilgjengelig ved oppkobling. Dermed vil man kunne sørge for at sikre klienter får sikker forbindelse, mens ikke-oppdaterte klienter får etablert forbindelse. Siden protokollen er opportunistisk, betyr det at om uvedkommende hindrer forespørselen om oppgradering til kryptert forbindelse, vil forbindelse bli etablert ukryptert og kommunikasjonen kan avlyttes.

3.1 Kryptografiske tiltak

Benytt nyeste versjoner av TLS-protokollen. Nyeste versjoner av TLS-protokollen tilbyr mer sikkerhet og NSM anbefaler TLS versjon 1.2. Dette er siste tilgjengelige versjon og NSM vil anbefale at versjon 1.3 tas i bruk så snart den er ferdigstilt. Dersom man benytter oppdatert programvare og installerer tilhørende sikkerhetsoppdateringer vil disse protokollene normalt være tilgjengelige. Dersom disse protokollene ikke er tilgjengelige bør program- og maskinvare erstattes. Merk at TLS som regel befinner seg i en rekke ulike implementasjoner på en datamaskin. Foruten operativsystem, kan programmer som nettlesere, epost-klienter og Java-kjøremiljøet ha egne TLS-implementasjoner.

Benytt sikre kryptografiske mekanismer. Sikre kryptografiske mekanismer som moderne algoritmer med tilfredsstillende nøkkellengder bør benyttes. *NSM Cryptographic Requirements*[2] lister opp NSMs anbefalte og aksepterte kryptomekanismer. For bruk i TLS, samt i andre kryptoprotokoller, benyttes såkalte *cipher suites*. Dette er pakker med ulike kryptomekanismer, som spesifiserer hvilke mekanismer som benyttes for autentisering, integritetsbeskyttelse, nøkkeletablering og konfidensialitetsbeskyttelse.

(Perfect) forward secrecy bør være støttet av ovennevnte *cipher suite*. Dette hindrer at kompromittering av langtidsnøkler medfører kompromittering av sesjonsnøkler; altså dersom den private nøkkelen til sertifikatet i et system blir kompromittert, vil ikke tidligere kommunikasjon mot systemet være kompromittert.

Autentisert kryptering bør være støttet av ovennevnte *cipher suite*. Autentisert kryptering er integritetsbeskyttet konfidensialitetsbeskyttelse og sørger for at man kan være sikker på at mottatte data kommer fra den autentiserte motparten.

[2] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

Benytt sertifiserte og minimalistiske implementasjoner. Foruten at TLS-mekanismene, inkludert kryptoalgoritmer, er funksjonelt riktige, bør de være evaluert og sertifisert for å kunne ha tillit til dem. Aktuelle evaluerings- og sertifiseringsordninger er *Common Criteria* og *FIPS 140-2*.

Implementasjonene bør være minimalistiske. Alle komponenter introduserer nye sårbarheter og for å ikke introdusere ekstra sårbarheter, bør funksjonalitet som ikke benyttes, ikke være tilstede i implementasjonen.

Samtidig må all funksjonalitet for TLS være implementert. Dette inkluderer funksjonalitet for verifikasjon av sertifikater. Dette er nærmere beskrevet i kapittel 3.4.

Benytt maskinvarebaserte kryptomoduler. Private nøkler bør forvaltes i *maskinvarebaserte kryptomoduler*. Maskinvarebaserte kryptomoduler har som regel robuste implementasjoner. Disse gir sterke nøkler ved hjelp av sterk nøkkelgenerering, god beskyttelse og korrekt bruk av nøklene.

For systemer med høy belastning benyttes gjerne maskinvarebaserte kryptomoduler da dette er ressurskrevende i generelle prosessorer, men systemer med lav belastning bør også bruke slike maskinvarebaserte kryptomoduler for høyere tillit.

Benytt klientsertifikater for to-veis autentisering. To-veis autentisering bør benyttes i sensitive systemer. Dermed autentiserer både tjener og klient seg med sertifikater før sikker kommunikasjon etableres.

3.2 Digitale sertifikater

Digitale sertifikater benyttes for å etablere sikre forbindelser. Sertifikatene identifiserer tjeneren (og eventuelt klienten) og spesifiserer bruksområde og gyldighetsperiode til sertifikatet.

Benytt en tiltrodd sertifikatutsteder. Siden digitale sertifikater benyttes for å identifisere tjenester, er det viktig at man har tiltro til disse.

NSM anbefaler sertifikatutstedere som:

- er underlagt norsk lovgivning
- sjekker eieren av sertifikatet før utstedelse (*extended validation*)
- offentliggjør alle utstedte sertifikater (*certificate transparency*)

Verifiser digitale sertifikater før bruk. Sertifikater må verifiseres før sikre forbindelser etableres. Informasjon om sertifikatet er trukket tilbake bør tilbys i oppkoblingen. På denne måten vil klienten få tilsendt både tjenerens sertifikat og sertifikatets statusinformasjon ved oppkobling. For å hindre at sertifikater som ikke lenger er gyldige benyttes, bør *OSCP Must-Staple* benyttes.

Spesifiser hvilke sertifikater og sertifikatutstedere som skal benyttes. *Certificate Pinning* bør benyttes for å spesifisere hvilke sertifikatutstedere eller sertifikater som er gyldige mot bestemt tjenester. Dette gjør det vanskelig å benytte forfalskede sertifikater.

3.3 Tiltak for klienter

Ikke benytt TLS-inspeksjon på klienter. Ulike «sikkerhetsprodukter» installerer programvare for å inspisere TLS-kommunikasjon på klientside. Eksempler på dette er anti-skadevare- og foreldrekontrollprogramvare. Dette medfører at sikkerhetsmekanismene som tilbys fra operativsystem eller nettleser omgås og dermed reduserer sikkerheten til TLS. TLS-inspeksjon på klienter bør derfor unngås.

Fjern ikke-tiltrodde sertifikatutstedere. Ulike TLS-implementasjoner, som operativsystem, nettleser og kjøremiljø har ulike lister over sine tiltrodde sertifikatutstedere. En nettleser må normalt stole på en rekke sertifikatutstedere, mens en VPN-klient kun trenger å stole på én. Sertifikatutstedere man ikke stoler på, bør fjernes fra disse listene. Siden en datamaskin kan ha en rekke ulike TLS-implementasjoner, vil dette være en formidabel oppgave. Det vil være nyttig å begrense bruken av sertifikater fra ikke-tiltrodde sertifikatutstedere ved hjelp av verifikasjonsverktøy. Dette er nærmere beskrevet i neste kapittel.

3.4 Verifikasjonstiltak

Sikkerhetsovervåkning bør implementeres for å verifisere at tiltak for å styrke TLS er implementerte og effektive. Løsninger som overvåker TLS-oppkoblinger kan gi verdifull informasjon om sikkerhetstilstanden i systemet. Slike løsninger kan blant annet verifisere hvilke sertifikater og sertifikatutstedere som utveksles og benyttes i oppkoblingsfasen, og hvilken TLS-versjon og hvilke kryptografiske mekanismer som tilbys og tas i bruk. På denne måten kan man stoppe trafikk som ikke møter organisasjonens retningslinjer.

Vedlegg A Dokumenthistorie

2016-03-02	Dokument ble opprettet.
2016-09-06	Intern høring.
2016-10-01	Publisering.