Kryptolåda

Inledning

Detta dokument beskriver en kryptolåda som kan sättas med utsida mot det publika Internet (enligt Internetspecifikationen) och på sin insida erbjuda paketförmedling enligt Internetspecifikationen med trafikskydd och textskydd.

En kryptolåda ska givet en paketförmedlingstjänst enligt Internetspecifikationen kunna hitta andra kryptolådor för att upprätta relevanta koppel.

Bakgrund och syfte

Inom och mellan vissa organisationer finns fristående nätverk som är baserade på internetteknologi, men logiskt skilda från internet. Användningen av dem motiveras ofta med högre krav till tillgänglighet och driftsäkerhet än vad som påstås vara möjligt med förbindelser över internet. Två exempel på sådana nät är SGSI och Sjunet. På grund av hur de fristående näten realiseras tekniskt kan de paradoxalt nog ha fler felkritiska systemdelar (eng. single points of failure) än motsvarande internetbaserade lösningar. Det kan exempelvis bero på att de är beroende av en enda infrastrukturleverantörs tekniska system, där de kan dela kablar, kopplingsutrymmen, nätverksutrustning med mera med internet.

Kryptolådan ska göra det möjligt och enkelt att använda internet för verksamhetskritisk kommunikation på ett sätt som överensstämmer med internets arkitekturprinciper. Förbindelsen mellan två kryptolådor och den information som skickas mellan dem ska skyddas med avseende konfidentialitet, riktighet, tillgänglighet och äkthet enligt nedanstående tabell.

Utöver funktionaliteten i ett vanligt VPN-krypto ska kryptolådan klara överbelastningsattacker (DOS-attacker) med en trafikmängd motsvarande full linjehastighet på lådans internetsida. (I skrivande stund upp till 400 Gbps.) Projektet saknar budget att skapa en produkt. Inledningsvis ska en specifikation tas fram. Specifikationen ska gå att använda för att ta fram ett proof-of-concept.

Avhängighet

Detta dokument är beroende av Internetspecifikation.

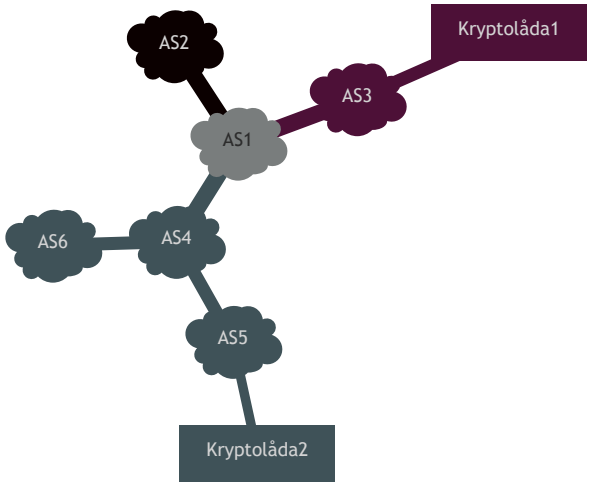
Begrepp

- **DoS-skydd:** Denial-of-service skydd från trafik som kommer från det publika Internet. En del av trafikskyddet.

- **Trafikskydd:** Ibland benämnt *signalskydd*, rör skydd av trafikflöden och behandlar bland annat störsändningar, falska meddelanden, och hoppande frekvenser / mottagaradresser.
- **Textskydd:** Ofta benämnt som kryptering, rör att skydda meddelandeinnehållet även om en antagonist kan läsa trafiken.

Arkitektur

Övergripande hanterar arkitekturen för kryptolåda krypterad end-to-end trafik mellan två godtyckligt valda platser på Internet. Se arkitekturskiss för exempelritning av arkitekturen.



Figur 1: Arkitekturskiss

En kryptolåda kan både skicka och ta emot paket. Inkommande paket ska vara adresserade till kryptolådan

Tunnelidentiteter består av en kombination av:

- protokoll
- mottagaradress (IPv6)
- mottagarport

TODO: Vad är begärandet av en ny adress en del av? Använder vi bara prefix från Internetspecifikationen och växlar mellan dem, eller ska vi lägga till hur man begär nya adresser via DHCP-PD eller en hel BGP-snurra?

TODO: Vem begär ny tunnelidentitet? Ska vi ha en kontrollenhet / annat som har ansvar att upprätthålla tunnlar osv.

TODO: Mesh, vilken del beslutar om hur vi bygger vårt mesh?

TODO: Kontrollplan?

Funktionalitet

Användare som vill koppla samman IPv6-nätverk på ett sätt som uppfyller ovan nämnda säkerhetskrav kan använda kryptolådan. Lådans kryptotextsida ansluts till internet och tilldelas en /64-adressrymd. Lådans klartextsida ansluts till en router på det interna (skyddade) nätverket. Kryptolådan tillhandahåller en lager 2-anslutning till klartextsidan på en eller flera andra kryptolådor. Över den anslutningen kan de anslutna routrarna skicka godtycklig trafik, inklusive routinginformation.

Konfidentialitet, riktighet och äkthet i trafiken tillses genom kryptering med en lämplig autentiserad symmetrisk kryptoalgoritm (ChaCha20-Poly1305?) I det enklaste användningsfallet har två kryptolådor en delad hemlighet som används för att generera en sessionsnyckel med t.ex. HKDF. Sekvensnumrering används för att detektera återuppspelningsattacker.

Skydd mot överbelastningsattacker

Systemen på kryptolådans klartextsida skyddas mot överbelastningsattacker genom den autentiserade krypteringen.

En överbelastning av kryptolådan kommer emellertid få effekten att alla system som skyddas av den blir otillgängliga. För att skydda mot detta använder kryptolådan sig av hoppande adresser. Med ett visst intervall (typiskt sett något hundratal millisekunder) byter kryptolådan adress. Intervallet kan vara en systemparameter eller förhandlas mellan två lådor i samband med sessionsinitieringen, t.ex. genom mätning av RTT.

Paket till andra destinationsadresser än nuvarande eller närmast föregående adress kastas. För att kunna genomföra en överbelastningsattack som mättar kryptolådans förmåga att dekryptera meddelanden måste en motståndare kunna sniffa äkta trafik från en annan kryptolåda och ställa om sin överbelastningstrafik till den nya adressen inom något hundratal millisekunder.

Kryptolådan använder statistiska metoder för att identifiera källadresser som skickar stora mängder obehörig trafik och använder DDoS Open Threat Signaling (DOTS) för att tillse att trafiken filtreras så tidigt så möjligt i nätverket.

Adresshoppningen kan exempelvis realiseras genom att de 64 lägsta bitarna i output från AES(k, CT), där k är en nyckel genererad från del delade hemligheten mellan två kryptolådor och CT är klartexten genererad enligt tabellen nedan.

Ett alternativ till att använda låd-id är att förhandla fram en separat nyckel för varje riktning vid handskakningen. Kryptolådorna måste ha gemensam tid med en noggrann-

het som är signifikant bättre än adressintervallet. Den föreslås erhållas genom NTS. Användning av MJD och tid sedan midnatt eliminerar problem med skottsekunder, UNIX-epochs osv.

Nödvändiga systemparametrar

- Tilldelat /64-nät på kryptotextsida
- Tilldelat /64-nät för motparternas kryptotextsidor (strikt taget endast nödvändigt för ena parten i en tvåvägsförbindelse)
- Delad hemlighet (en per motpart)
- Adressintervall
- Adress till NTS-server (och certifikatkedja)
- DOTS-parametrar

Proof-of-concept

Ett fungerande proof of concept ska minst ha följande funktionalitet: * Sessionsinitiering över förbindelsen med hjälp av delad hemlighet och HKDF. * Krypterad och autentiserad överföring av data mellan klartextsidorna på två kryptolådor. * Hoppande IPv6-adresser på kryptotextsidan. * Filtrering av obehöriga paket med hjälp av destinationsadress (adresshoppning) och autentiserad kryptering.

Kvarvarande frågor och observationer

- Antalet samtidiga sessioner kommer att påverka prestandan. Det typiska användningsfallet kommer att vara en eller en handfull sessioner.
- Ska kryptolådan erbjuda skydd mot trafikanalys (fyllnadssignalering)?
- Hur hanteras out-of-order packets mht. sekvensnumreringen?
- Är det nödvändigt att skicka NDP-paket med nya adresser för att inte få packet loss vid adresshoppningen? Hur lång tid innan adressbyte i så fall?
- Kan vi ta bort gamla adresser ur neighbortabellen med NDP?
- När måste man byta nyckel för adresshoppningen? Även om man har observerat en viss adress så är sannolikheten *nästan* lika stor att den dyker upp igen. Med tanke på hur ofta/sällan de byts så borde det räcka något decennium eller så, men det borde kontrollräknas.
- Beskriv någon hyfsat effektiv statistisk metod för att identifiera källadresser som skickar stora mängder överbelastningstrafik. (För det är inte praktiskt genomförbart att hålla en lista på alla i minnet.)

DoS-skydd

Denial-of-service skyddet ska se till att kryptolådan ej kan sättas ur funktion genom designade trafikströmmar. Detta görs genom att kryptolådor ska klara av ett fullt trafikflöde enligt dess datalänklager.

TODO: Givet korrekt protokoll, port och adress så lämnar DoS över till trafikskydd?

- **Krav:**
  - DoS-skyddet **ska** filtrera bort all trafik som inte är adresserad till aktiv kryptografisk tunnel.
  - DoS-skyddet **ska** upprätthålla full tillgänglighet vid datalänkslagrets fulla trafikhastighet.

Trafikskydd

TODO: Vad gör trafikskyddet i den här lösningen?

TODO: De flesta protokoll idag gör en kombo av trafikskydd och textskydd. Vill vi dela upp dem? Antar att det finns fördelar med att kunna dela upp dem även fast de flesta implementationer sköter trafik och textskydd tillsammans.

- **Krav:**
  - Trafikskyddet **ska** meddela DoS-skyddet aktiva tunnelidentiteter.

Textskydd

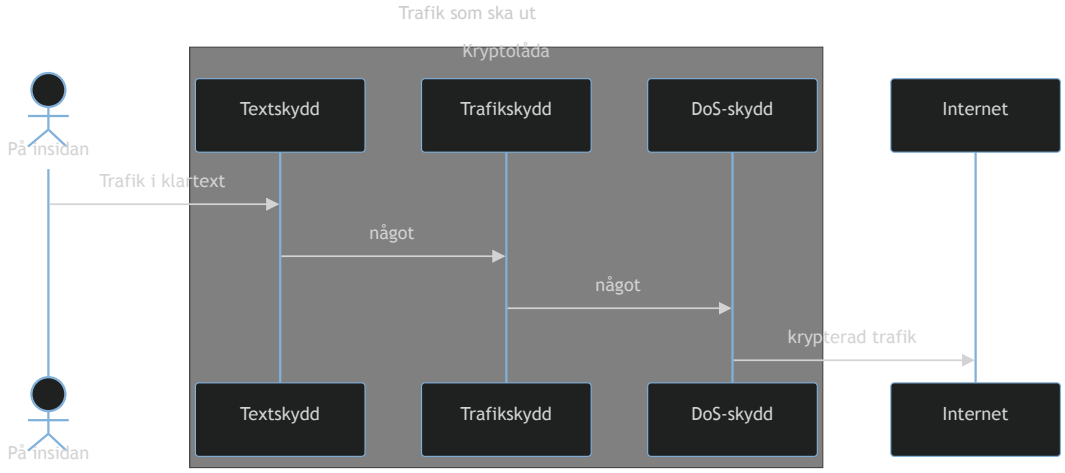
TODO: Hur mycket valfrihet ska finnas för textskyddet? Får användare välja vad som helst?

- **Krav:**
  - Textskyddet **ska** meddela trafikskyddet aktiva tunnelidentiteter.

Exempel

Från klient på insidan till trafik på utsidan

TODO: Reffa internetspecifikationen. På insidan så ska en klient inte se någon skillnad.



Figur 2: Trafik som går från klient

Trafik utifrån in till klient

TODO: Hur sker avskalning av skydd?

Verifikation

TODO: Ta fram mätbara krav på kryptolådan

Proof of concept

TODO: Ta fram PoC? Ev raspberry pi / liten referensdesign som man kan bygga och testa?

Annat

TODO: Hur hanterar vi kvantsaker? Ex nyckelutbyte över annan rutt än Internet?

Från tidigare spec

Frequency hopping

Kan man använda de sista 64-bitarna i en IPv6-adress för frequency hopping på ett bra sätt?

Vilket sliding window behöver vi för att hoppa effektivt?

Kryptosystem

För de användare som tidigare använt fasta förbindelser eller någon form av VPN-tjänst tillhandahåller Fem små hus-infrastrukturen ett kryptosystem. Kryptosystemet ger skydd mot obehörig trafik, avlyssning och överbelastningsattacker.

Kryptosystemets princip är att det överför Ethernet-paket mellan två punkter genom att man kapslar in det krypterade Ethernet-paketet i ett IPv6-paket som skickas över infrastrukturen. Olika metoder används för att skydda kryptots ändpunktsadresser mot överbelastningsattacker. Har man flera korresponderande motparter via samma krypto identifieras de med ett VLAN per motpart.

Kryptot ansluts till infrastrukuren med 100/400Gbit och tjänsten mot användaren är förmedling av Ethernet-paket med 100/10Gbit-anslutning. Maximal överförd lager 2-Ethernet-MTU är 8210 byte.

För detaljspecifikation av kryptot, se del 4 som tas fram av en separat arbetsgrupp.

En enklare form av tunnling, motsvarande MPLS, är att använda L2TPv3 över IPv6. Funktionaliteten finns i de flesta kommersiella routrar och kan i vissa fall kombineras med routerns kryptofunktion.