OULUN SEUDUN
AMMATTIKORKEAKOULU

Mikko Tervahauta

LTE-VERKON S1-RAJAPINNAN MONITOROINTI

LTE-VERKON S1-RAJAPINNAN MONITOROINTI

Mikko Tervahauta
Opinnäytetyö
Kevät 2012
Tietokonetekniikan koulutusohjelma
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietokonetekniikan koulutusohjelma, langaton tietoliikenne

Tekijä: Mikko Tervahauta
Opinnäytetyön nimi: LTE-verkon S1-rajapinnan monitorointi
Työn ohjaaja: Kari Jyrkkä
Työn valmistumislukukausi ja -vuosi: Kevät 2012 Sivumäärä: 34 + 4

Työn tehtävänä oli laatia Rugged Tooling Oy:n toteuttamalle LTE-verkon rajapintojen monitorointiratkaisulle testaussuunnitelma. Aihe rajattiin koskemaan monitorointiratkaisun, Rugged Statisticsin eli RUSTin, toiminnallista testausta, suorituskykytestausta ja näihin testeihin tarvittavan testimateriaalin tuottamista. Tavoitteena oli toteuttaa testitapaukset, joiden pohjalta RUSTin eri toiminnallisuuksien vaatimusmäärittelyn mukainen toiminta saadaan yksikäsitteisesti testattua ja RUSTin suorituskyky määritettyä.

Testaussuunnitelmaa ryhdyttiin laatimaan RUSTin vaatimusmäärittelydokumentin perusteella. Ensimmäisinä tutustuttiin RUSTin toiminnallisuuksiin eli S1-rajapinnassa käytettävän IPsec-salauksen purkamiseen ja tietoliikenteen kaappaamiseen RPCAP- ja NetFlow-etäkaappausmenetelmillä. Tämän tietopohjan perusteella suunniteltiin näiden toiminnallisuuksien ja RUSTin suorituskyvyn testaamista varten yksityiskohtaiset, vaihe vaiheelta etenevät testitapaukset, testien suorittamiseen tarvittavien laitteiden ja ohjelmistojen käyttöohjeet sekä testeihin tarvittavat testimateriaalit.

Työn tuloksena saatiin valmiiksi RUSTin testaussuunnitelma. Suunnitelmaa tullaan käyttämään ja jatkokehittämään osana RUSTin kehitystä. Testaussuunnitelma on liitteenä ainoastaan Rugged Toolingille jäävässä opinnäytetyön versiossa.

Asiasanat: LTE, S1-rajapinta, IPsec, RPCAP, NetFlow, toiminnallinen testaus, suorituskykytestaus

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Information Technology, wireless telecommunication

---

Author: Mikko Tervahauta
Title of thesis: Monitoring the LTE S1 interface
Supervisor: Kari Jyrkkä
Term and year when the thesis was submitted: Spring 2012 Pages: 34 + 4

The purpose of the thesis was to produce a test plan for Rugged Tooling's embedded LTE interface monitoring solution, Rugged Statistics or RUST. The subject was limited to handle the functional and performance testing of said equipment and the production of the necessary test material. The goal was to produce test cases as grounds from which the functionality, according to the requirement specification, and the performance of RUST could unambiguously be tested.

The test plan is based on RUST requirement specification. First it was necessary to learn all the functionalities of RUST, i.e. the decrypting of IPsec algorithms used in the LTE S1 interface and the remote capturing of IP traffic via RPCAP and NetFlow. Based on this knowledge the detailed, step-by-step test cases for testing the functionality and the performance of RUST were created and assembled as the testing plan.

The plan will be utilized and developed further as part of the development of RUST. The test plan is included only with the version of this thesis that is intented for Rugged Tooling ltd.

Keywords: LTE, S1 interface, IPsec, RPCAP, NetFlow, functional testing, performance testing

ALKULAUSE

Tämä opinnäytetyö tehtiin keväällä 2012 Rugged Tooling Oy:lle. Tehtävänä oli laatia Rugged Toolingin toteuttaman verkkomonitorointiratkaisun testaussuunnitelma.

Haluan kiittää Rugged Tooling OY:n toimitusjohtaja Vinski Bräysyä opinnäytetyön aiheen sekä osa-aikaisen työpaikan tarjoamisesta. Kiitokset Kari Jyrkälle opinnäytetyöni sisällönohjauksesta ja Tuula Hopeavuorelle tekstinohjauksesta. Ammattikorkeakoulun kolmena viimeisenä vuotena luokkamme ryhmänohjaajana toiminutta Riitta Rontua haluan kiittää tuesta ja kannustuksesta opintojeni aikana. Antoisista työpäivistä tahdon kiittää Rugged Toolingin työntekijöitä Esa Pesosta, Mikko Karjalaista, Saku Wennerstrandia ja Katri Siivolaa, minkä lisäksi erityiskiitoksen loistavasta vertaistuesta esitän opiskelijatoverilleni Katariina Moilaselle.

Oulussa 20.5.2012

Mikko Tervahauta

SISÄLLYS

SANASTO

3GPP	3rd Generation Partnership Project, usean standardointijärjestön yhteistyöorganisaatio, joka huolehtii matkapuhelinjärjestelmien spesifiointityöstä
AES-CBC	Advanced Encryption Standard with Cipher-block Chaining, yksi IPsecin käyttämistä salausmenetelmistä
CN	Core Network, tietoliikenneverkon runko
eNB	Evolved NodeB tai eUTRAN NodeB, LTE-järjestelmän tukiasemaa vastaava verkkoelementti
EP	Elementary Procedure, S1 Application Protocol muodostuu EP:ista
EPC	Evolved Packet Core, runkoverkon LTE-spesifinen osa, pitää sisällään MME:n, S-GW:n, PDN GW:n ja PCRF:n
E-RAB	eUTRAN Radio Access Bearer, eNB:n ja EPC:n välillä dataa kuljettava entiteetti
eUTRAN	Evolved UMTS Terrestrial Radio Access Network, eNB:iden ja UE:ien muodostama kokonaisuus, LTE:n ilmarajapinta
GPRS	General Packet Radio System, pakettipohjaisen datan välittäjä GSM- ja WCDMA-verkoissa
GTP	GPRS Tunneling Protocol, GPRS-tunnelointiprokotolla
GTP-U	GTP User Data Tunneling, GPRS-tunnelointiprotokolla käyttäjädatalle
GSM	Global System for Mobile Communications, niin sanottu 2G eli toisen sukupolven matkapuhelinjärjestelmä

HSS	Home Subscriber Server, käyttäjätietojen päätietokanta, suorittaa autentikointia ja valvoo käyttäjien käyttöoikeuksia eri verkkoresursseihin
IPsec	Internet Protocol Security, IP-liikenteen tietoturvallisuudesta huolehtiva protokollapino
IPv4	Internet Protocol Version 4, Internetin verkkokerroksen protokollan versio 4
IPv6	Internet Protocol Version 6, Internetin verkkokerroksen protokollan versio 6
LTE	Long Term Evolution, GSM- ja UMTS-järjestelmiä seuraava matkapuhelinjärjestelmäsukupolvi
MME	Mobility Management Entity, EPC:n kontrollisanomista huolehtiva verkkoelementti
NAS	Non-Access Stratum, IP-protokollapinon verkkokerrokseen verrattavissa oleva kerros UMTS- ja LTE-järjestelmien langattoman tiedonsiirron protokollapinossa
OFDMA	Orthogonal Frequency Division Multiple Access, radiorajapinnan monikäyttötekniikka
PCAP	Packet Capture, pakettikytkentäisen verkon informaation sisältämien elementtien kaappaus analysointitarkoituksessa
PCRF	Policy and Charging Rules Function, huolehtii muun muassa laskutuksen kontrolloinnista
PDN GW	Packet Data Network Gateway, liittää EPC:n muihin pakettidataverkkoihin
RAN	Radio Access Network, luo tietoliikenneyhteyden UE:n ja CN:n välille

RNC	Radio Network Controller, aiempien matkapuhelinjärjestelmäsukupolvien käyttämä verkon kontrollielementti tukiaseman ja muun verkon välissä
RPCAP	Remote Packet Capture, PCAP:n alalaji, mahdollistaa pakettien etäkaappauksen
S1AP	S1 Application Protocol, S1-rajapinnan verkkokerroksen signalointiprotokolla
S1-MME	S1 Control Plane Interface, S1-rajapinnan kontrolliviestien puolisko
S1-U	S1 User Plane Interface, S1-rajapinnan käyttäjädatan puolisko
SC-FDMA	Single Carrier Frequency Division Multiple Access, radiorajapinnan monikäyttötekniikka
SCTP	Stream Control Transmission Protocol, kuljetuskerroksen protokolla
S-GW	Serving Gateway, käyttäjädatasta huolehtiva verkkoelementti EPC:ssa
TOS	Type of Service, yksi IPv4-otsikon kentistä
3DES	Triple Data Encryption Standard, yksi IPsecin käyttämistä salausmenetelmistä
UDP	User Datagram Protocol, yksinkertainen datanvälitysprotokolla
UE	User Equipment, päätelaite, esimerkiksi matkapuhelin
UMTS	Universal Mobile Telecommunication System, niin sanottu 3G eli kolmannen sukupolven matkapuhelinjärjestelmä

1 JOHDANTO

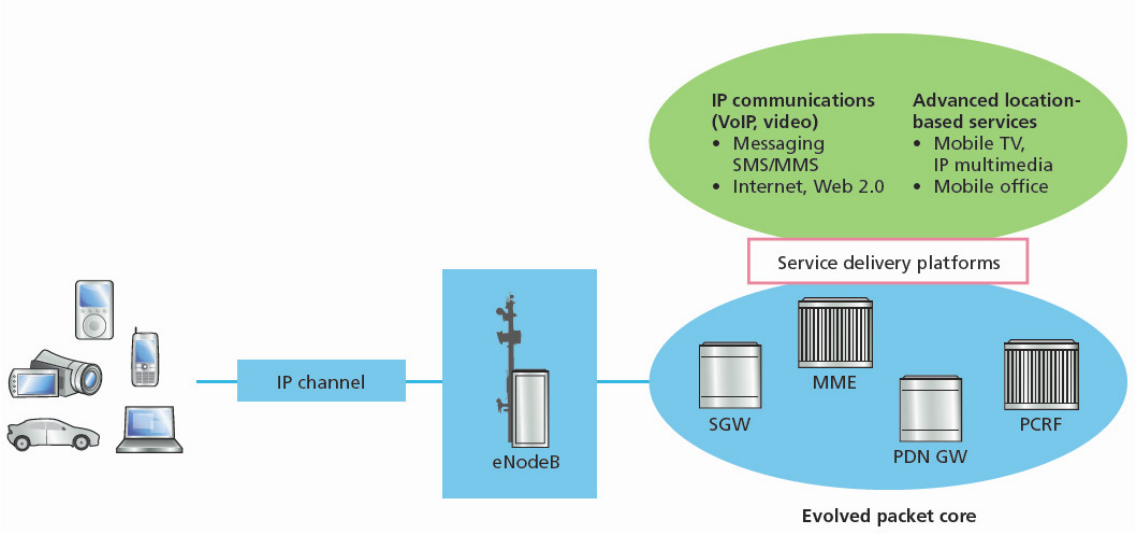
Long Term Evolutionilla (LTE) tarkoitetaan GSM:n ja UMTS:n aloittaman jatkumon seuraavaa vaihetta, seuraavaa matkapuhelinsukupolvea. Sen suurimpia muutoksia edellisiin sukupolviin verrattuna on järjestelmän välittämän tietoliikenteen siirtyminen pois perinteisestä piirikytkentäisestä siirtotavasta käyttämään IP-pohjaista pakettikytkentäistä tekniikkaa.

Rugged Tooling OY on oululainen IP-verkkojen sulautettuihin suuren tarkkuuden testaus-, validointi- ja monitorointiratkaisuihin erikoistunut yritys. RUST on Rugged Toolingin Octeon-verkkoprosessorilla toteuttama sulautettu LTE-verkon monitorointiratkaisu, jota voidaan käyttää LTE:n S1-rajapinnassa kulkevien kontrollisanomien ja käyttäjädatan kokonaisvaltaiseen tarkkailuun. Tietoliikenteen tarkkailemiseksi RUST suorittaa monitoroimansa tietoliikenneyhteyden kontrolliliikenteelle RPCAP- ja käyttäjädatalle NetFlow-etäkaappauksen. Tämän lisäksi se purkaa IPsec-salaukset kaappaamastaan tietoliikenteestä, mikä mahdollistaa eteenpäin lähetettävän datan suodattamisen sen sisältämän tiedon perusteella.

Tämän opinnäytetyön aiheena oli RUSTin testauksen suunnittelu. Tarkoituksena oli suunnitella testitapaukset RUSTin toiminnallista testausta ja suorituskykytestausta varten eli laatia testaussuunnitelma, jonka pohjalta RUSTin toiminnallisuudet saadaan kattavasti todettua toimiviksi ja suorituskyky määritetyksi. Tämän lisäksi tehtävänä oli tuottaa näiden testien tarvitsemat testimateriaalit.

2 LONG TERM EVOLUTION

LTE eli Long Term Evolution hyödyntää tiedonsiirrossaan uusia radiorajapinnan monikäyttötekniikoita, MIMO-tekniikkaa eli useampia lähetys- ja vastaanottoantenneja sekä tiedonsiirtokanavilla 20 MHz:n maksimikaistanleveyttä UMTS:n 5 MHz:n maksimikaistanleveyden sijaan. LTE:n uudistunutta runkoverkko-osaa kutsutaan nimellä Evolved Packet Core ja se koostuu Mobility Management Entitystä, Serving Gatewaysta, Packet Data Network Gatewaysta ja Policy and Charging Rules Functionista (kuva 1). (1.)



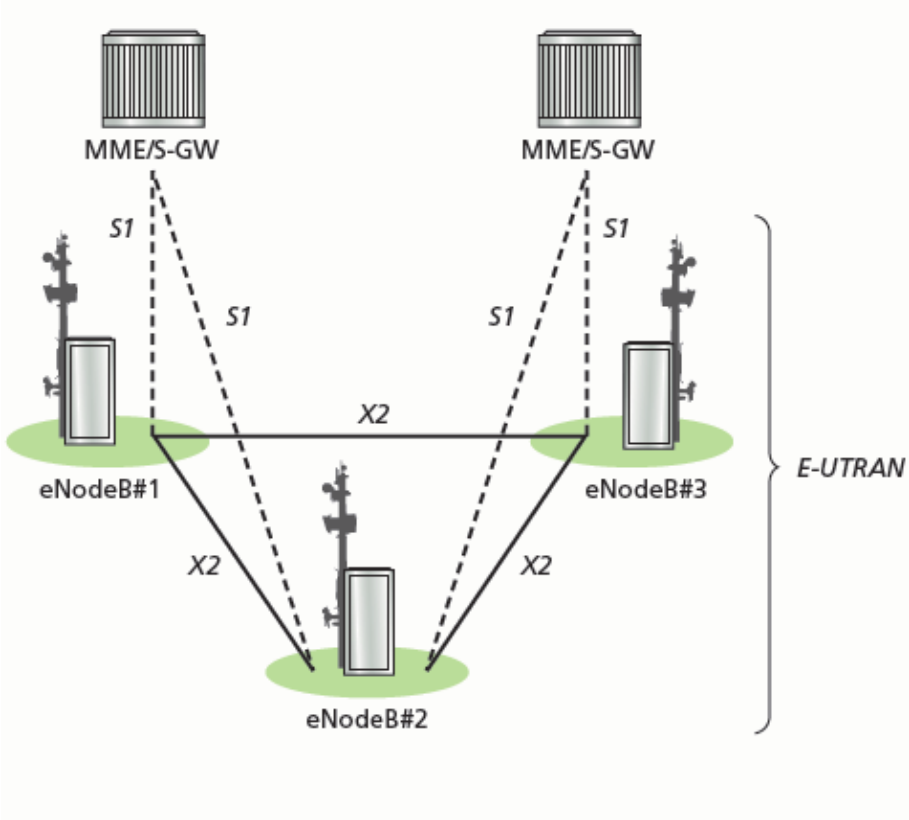
KUVA 1. LTE-arkkitehtuuri (3)

Uusien menetelmien vuoksi LTE:llä saavutetaan suurempi tiedonsiirtokapasiteetti ja -nopeus sekä parempi radiotaajuuksien käytön tehokkuus verrattuna aiempiin toteutuksiin. Lisäksi verkon rakennetta on pyritty yksinkertaistamaan tiedonsiirron viiveiden minimoimiseksi, jotta entistä nopeammat datayhteydet ovat ylipäätään mahdollisia. LTE on takaisinpäin yhteensopiva aiempien järjestelmien kanssa ja sen teknologioiden kehittämisestä ja ylläpidosta huolehtii 3rd Generation Partnership Project. (1.)

2.1 LTE-verkon osat

2.1.1 eNodeB

LTE:n Evolved NodeB on GSM-järjestelmän tukiasemaa ja UMTS-järjestelmän NodeB:tä vastaava verkkoelementti, joka hoitaa mobiilin User Equipmentin kanssa keskustelemisen radiorajapintaa hyväksikäyttäen. Uusina monikäyttötekniikkoina eNB hyödyntää verkosta UE:lle päin OFDMA:ta ja UE:lta verkkoon päin SC-FDMA:ta. Aiemman sukupolven toteutuksista poiketen se ei tarvitse erillistä Radio Network Controlleria, vaan verkonohjaukselliset elementit on tältä osin toteutettu osana eNB:tä. Muista verkkoelementeistä se on yhteydessä toisiin eNB:ihin X2-rajapinnan ja Mobility Management Entityyn sekä Serving Gatewayhin S1-rajapinnan kautta (kuva 2). (2.)



KUVA 2. eUTRAN-arkkitehtuuri (3)

2.1.2 Mobility Management Entity

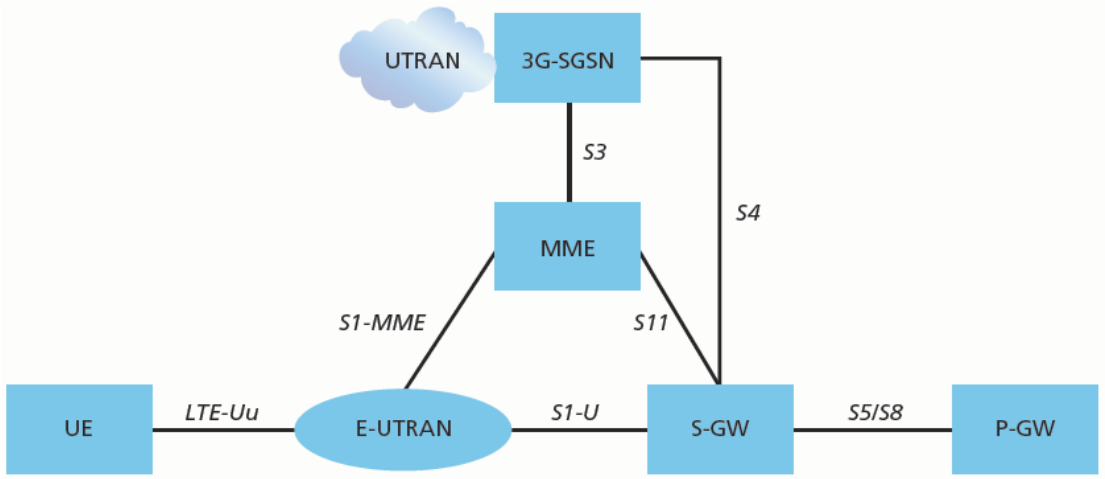
Mobility Management Entity on LTE-verkon kontrollielementti, ja se suorittaa signalointiin ja ohjaukseen liittyviä tehtäviä. Yksittäinen MME kykenee hoitamaan tuhansien eNB:iden tarvimat toimenpiteet. Se hallinnoi UE:ien pääsyä verkkoyhteyksille ja verkkoresurssien allokointia sekä hoitaa idle-tilassa olevien UE:ien paikannusta verkossa, idle-tilassa olevien UE:ien kutsumista, roamingiin liittyvien rajoitusten toteutumista sekä handovereiden järjestelyä UE:n siirtyessä GSM- tai UMTS-verkon palveltavaksi. Se hoitaa myös käyttäjän autentikoinnin yhdessä Home Subscriber Serverin kanssa ja valitsee UE:n käyttämän Serving Gatewayn. (4.)

2.1.3 Serving Gateway

Serving Gateway huolehtii käyttäjädatan, esimerkiksi puheen, välittämisestä eNB:ltä EPC:lle, minkä lisäksi se pitää yllä tietoa UE:n liikkuvuudesta käyttäjärajapinnan osalta kahden eNB:n välisessä handoverissa sekä UE:n vaihtaessa GSM- tai UMTS-verkkoon. S-GW hoitaa lisäksi MME:n kutsuman idle-tilassa olevan UE:n datan puskuroinnin, kunnes data voidaan välittää UE:lle sen vaihdettua active-tilaan. (4.)

2.2 S1-rajapinta

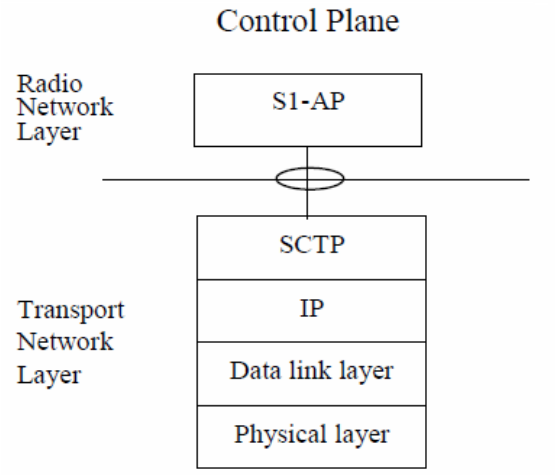
Tietoliikenne eNB:iden ja EPC:n välillä tapahtuu S1-rajapinnan kautta. Se tukee eUTRAN Radio Access Bearereiden luontia, ylläpitoa ja vapauttamista, LTE:n sisäisiä ja matkapuhelinverkkojen välisiä handovereita, UE:iden erottamista toisistaan protokollatasolla käyttäjäkohtaisen hallinnoinnin mahdollistamiseksi, NAS-viestien välittämistä UE:n ja EPC:n välillä, paikannuspyyntöjen ja -tietojen välittämistä UE:n ja EPC:n välillä sekä resurssien varaamista pakettidatayhteyksien käyttöön. Liikenteen välittymisestä S1-rajapinnassa huolehtii S1 Application Protocol. S1-rajapinta jakautuu kahtia kontrolliliikenteen hoitavaan S1-MME:hen ja käyttäjädatan välittävään S1-U:hun (kuva 3), joissa kulkevaa tietoliikennettä RUSTilla on siis tarkoitus monitoroida. (5.)



KUVA 3. LTE-järjestelmän rajapinnat (3)

2.2.1 S1-MME-rajapinta

Kontrollisanomat S1-rajapinnassa välittävän S1-MME-rajapinnan protokollapino koostuu fyysisestä kerroksesta, siirtokerroksesta, IP-kerroksesta ja SCTP-kerroksesta (kuva 4). Protokollapinon päällä toimii S1-rajapinnan signaloinnista vastaava S1AP. (5.)

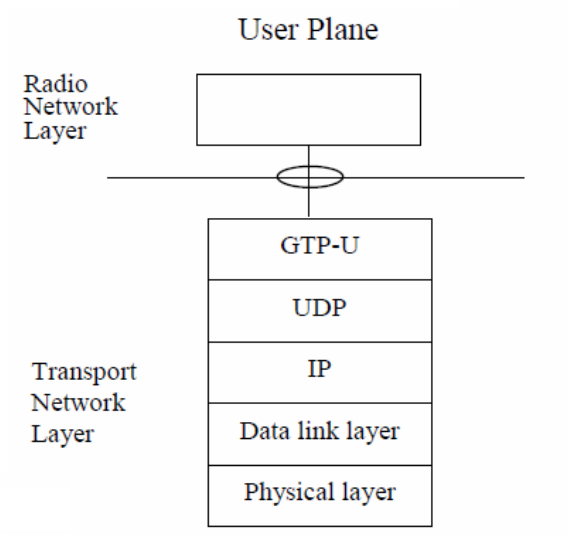


KUVA 4. S1-MME-rajapinnan protokollapino (5)

RUST suodattaa S1-MME-rajapinnasta halutut paketit ennaltamäärättyjen sääntöjen perusteella ja lähettää ne eteenpäin RPCAP-menetelmällä jatkokäsittelyä varten.

2.2.2 S1-U-rajapinta

Käyttäjädatan välityksen S1-rajapinnassa hoitavan S1-U-rajapinnan protokollapino koostuu fyysisestä kerroksesta, siirtokerroksesta, IP-kerroksesta, UDP-kerroksesta ja GTP-U-kerroksesta (kuva 5) (5). RUST purkaa S1-U-rajapinnan tietoliikenteestä ennaltamäärättyjen sääntöjen perusteella halutut paketit NetFlow 9 -formaattiin ja lähettää ne eteenpäin NetFlow-kerääjälle jatkokäsittelyä varten.



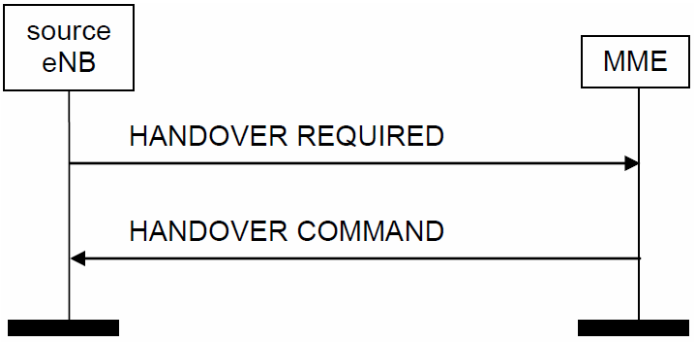
KUVA 5. S1-U-rajapinnan protokollapino (5)

2.2.3 S1 Application Protocol

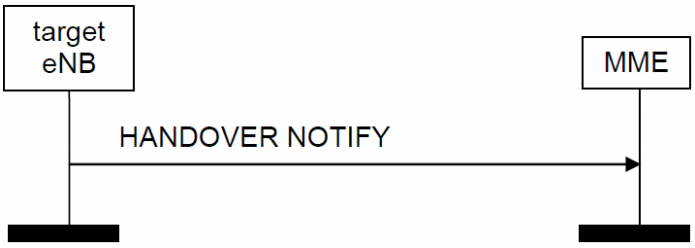
S1AP eli S1 Application Protocol huolehtii S1-rajapinnan tietoliikenteen toiminnasta. Sen tehtäviin kuuluu S1-rajapinnan ylläpito, E-RAB:ien hallinnointi, eNB:iden ja EPC:n välisen tiedonsiirron aloittamiseen liittyvät toimenpiteet, active-tilassa olevien UE:iden handovereiden hallinta, active-tilassa olevien UE:iden kutsuminen, NAS-viestien välitys UE:n ja EPC:n välillä, UE:n paikkatiedon välittäminen MME:lle, RAN-informaation välitys kahden RAN noden välillä ja tunnelointi CDMA2000-järjestelmään. (6.)

S1AP muodostuu joukosta Elementary Procedureja. EP on eNB:n ja EPC:n välisen kommunikoinnin yksikkö, viesti, joista on tarkoitus muodostaa kokonaisia sekvenssejä, joilla S1AP hallinnoi S1-rajapinnan tietoliikennettä. EP on mahdol-

lista muodostaa itsenäisenä, ja niitä voidaan ajaa myös rinnakkain. Ne jaetaan kahteen osaan: luokkaan 1, jonka EP:t on määritelty pyyntö-vastauspareina, ja luokkaan 2, jonka EP:t on määritelty yksittäisinä viesteinä. Luokan 1 EP:n vastausviesti on aina tieto pyynnön sisältämän toimenpiteen onnistumisesta tai epäonnistumisesta, kun taas luokan 2 EP:t ajatellaan aina onnistuneiksi. Liitteessä 1 on esitetty kaikki luokan 1 EP:t ja liitteessä 2 kaikki luokan 2 EP:t. Esimerkkinä eNB:n ja MME:n välisestä luokan 1 EP:lla tapahtuvasta kommunikoinnista on kuvassa 6 esitetty handoverin aloitus ja esimerkkinä luokan 2 EP:llä tapahtuvasta kommunikoinnista kuvassa 7 on onnistuneesta handoverista ilmoittaminen. (6.)



KUVA 6. Handoverin aloittaminen (6)



KUVA 7. Onnistuneesta handoverista ilmoittaminen (6)

Nämä Elementary Procedure -viestit on mahdollista purkaa S1-MME-rajapinnasta ja saada näkymään vaikkapa Wiresharkissa, jolloin niistä voidaan tehdä johtopäätöksiä verkon toimivuudesta.

3 IP-LIIKENTEEN TIETOTURVALLISUUS

IPsec:llä eli Internet Protocol Securityllä tarkoitetaan IP-protokollan käyttämiä autentikointia ja salausta toteuttavia osia. IPsec toimii IP-protokollapinon verkkokerroksella suojaten datavirtoja lähettäjän ja vastaanottajan tietokoneiden välillä, minkä lisäksi sillä on mahdollista suojata myös laajempia kokonaisuuksia, esimerkiksi lähiverkkoja, mikäli tietoliikenne ohjataan ulos tästä kokonaisuudesta yhden pisteen kautta. Lähetettävästä paketista voidaan haluttaessa salata vain hyötykuorma, jolloin IP-otsikkokenttä pysyy salaamattomana, tai koko paketti voidaan salata, jolloin salatun IP-paketin päälle lisätään uudet otsikkokentät, joilla varmistetaan paketin perillepääsy. (7.)

IPsec-standardi on avoin standardi, jonka virallisesta dokumentoinnista vastaa Internet Engineering Task Force IETF. Se käyttää useita protokollia tietoliikenteen turvaamisessa: Authentication Header -protokolla todentaa pakettien alkuperän ja takaa niiden eheyden, Encapsulating Security Payload -protokolla tarjoaa pakettien alkuperän todentamisen, pakettien eheyden takauksen sekä pakettien salauksen ja Security Associations -protokolla kahden aiemmin mainitun toimintaan tarvittavat algoritmit ja tiedot. (7.)

RUSTin toiminnan kannalta näistä protokollista oleellisin on ESP (kuva 8), sillä pakettien alkuperä on LTE-verkoissa varmuudella tiedossa jo muutenkin, eikä AH-protokollan tarjoamalle pelkälle alkuperän varmistukselle ilman pakettien salausta ole käyttöä.

Offsets	$Octet_{16}$	0								1								2								3							
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Security Parameters Index (SPI)*																															
4	32	*Sequence Number*																															
8	64	*Payload data*																															
...	...																																
...	...									*Padding (0-255 octets)*																							
...	...																	*Pad Length*								*Next Header*							
...	...	*Integrity Check Value (ICV)*																															
...	...	...																															

KUVA 8. Encapsulating Security Payload -pakettirakenne (8)

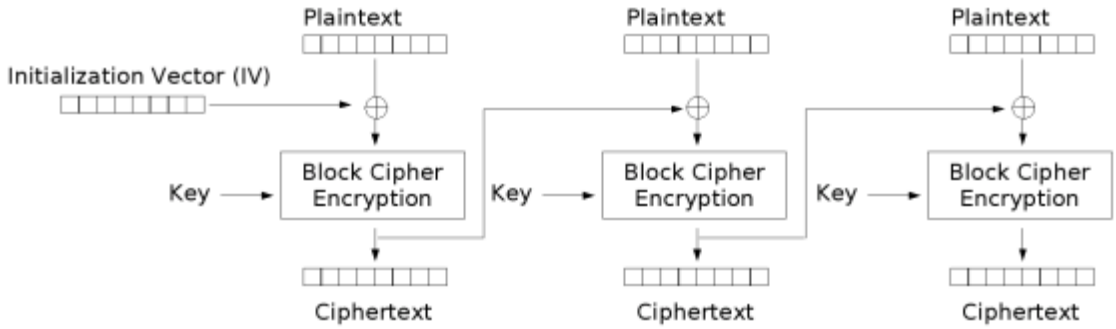
Security Parameters Index -kentässä on sattumanvarainen 32-bittinen luku, jota käytetään yhdessä kohde-IP-osoitteen kanssa tunnistamaan käytetty Security Association eli lähettäjän ja vastaanottajan välinen tietoturvallisuuskäytäntö. Sequence Number -kenttä sisältää juoksevan numeron, jolla estetään uudelleenlähetyshyökkäyksiä. Payload Data on ESP-paketin sisältämä, salattu hyötydata, jonka perään lisätään sopiva määrä Paddingia, ”tyhjää dataa”, jotta paketti olisi ESP-salausblokin mittainen. Pad Length -kenttä kertoo Paddingin pituuden, Next Header -kenttä seuraavan otsikkokentän tyypin ja Integrity Check Value -kenttä sisältää koko paketin pituuden tarkistustiedon paketin eheyden varmistamiseksi. (7.)

IPsec käyttää salauksessa kolmea salausalgoritmia, joista RUSTin kannalta oleellisia ovat AES-CBC ja 3DES-CBC, joita käytetään dataliikenteen salaamisessa. Jotta tietoliikenneyhteyden pakettien suodattaminen kaappaamista varten niiden sisältämän datan perusteella olisi mahdollista, täytyy pakettien salaus kyetä ensin purkamaan. RUST tukee sekä AES-CBC- että 3DES-CBC-salausten purkua, jolloin sitä on mahdollista käyttää näitä salauksia käyttävien pakettien suodattamiseen. Tämän lisäksi RUST purkaa myös ESP-paketin sisältä mahdollisesti löytyvät tunneloinnit, jolloin paketteja voidaan suodattaa lähetystä varten myös tunnelointien sisältä löytyvien tietojen perusteella.

3.1 AES-CBC-salausalgoritmi

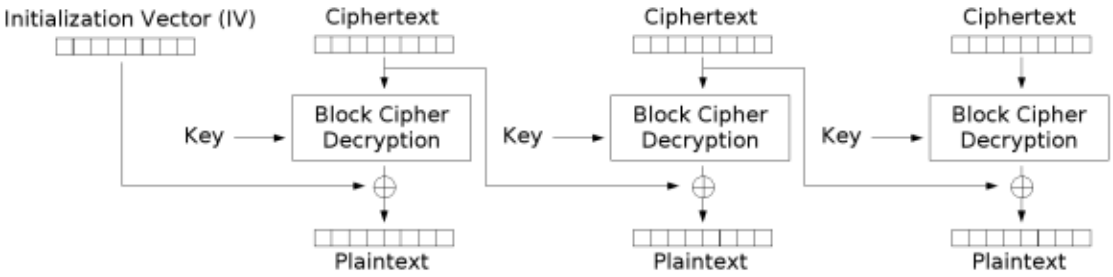
Advanced Encryption Standard on symmetrisen avaimen lohkosalausalgoritmi eli sekä tiedon salaus että salauksen purku suoritetaan samalla avaimella. Salausavain voi olla joko 128-, 192- tai 256-bittinen. Tiedon salaus tapahtuu sarjana muutoskierroksia, joissa algoritmiin syötettyä salaamatonta dataa muokataan tiettyjen vaiheiden kautta, kunnes haluttu kierrosmäärä tulee täyteen. Kierrosten lukumäärä riippuu salausavaimen pituudesta: 128-bittisellä avaimella suoritetaan 10, 192-bittisellä avaimella 12 ja 256-bittisellä avaimella 14 muutoskierrosta. Jokaiselle muutoskierrokselle lasketaan oma kierrosavain niin sanotun Rijndaelin avainjärjestyksen mukaan. (9.)

CBC eli Cipher Block Chaining on salauksenparannusmenetelmä, jossa jokaiselle salattavalle selväkieliselle lohkolle tehdään XOR-operaatio edellisen jo salatun lohkon kanssa (kuva 9). Ensimmäistä lohkoa salattaessa käytetään Initialization Vectoria, koska edellistä jo salattua lohkoa ei vielä ole olemassa.



KUVA 9. Tiedon salaus CBC-menetelmällä (11)

Myös salauksen purun yhteydessä suoritetaan vastaavat XOR-operaatiot (kuva 10).



Kuva 10. Salauksen purku CBC-menetelmällä (11)

CBC-menetelmän salauksenparannus perustuu siihen, että jokaisen salattavan lohkon salaus on riippuvainen kaikista siihen mennessä käsitellyistä lohkoista. (10.)

3.2 3DES-CBC-salausalgoritmi

Triple Data Encryption Standard on lohkosalausalgoritmi, joka nimensä mukaisesti suorittaa salattavalle datalle DES-lohkosalausalgoritmin vaiheet kolme kertaa. DES-salaus itsessään on jo todettu riittämättömäksi sen avainten lyhyy-

den vuoksi, mutta 3DES-toteutuksella samaa menetelmää voidaan kuitenkin vielä käyttää hyödyksi. Yhden DES-salausavaimen pituus on 56 bittiä, joita tarvitaan jokaiselle salattavalle lohkolle kolme, ja salauslohkon koko on 64 bittiä. (12.)

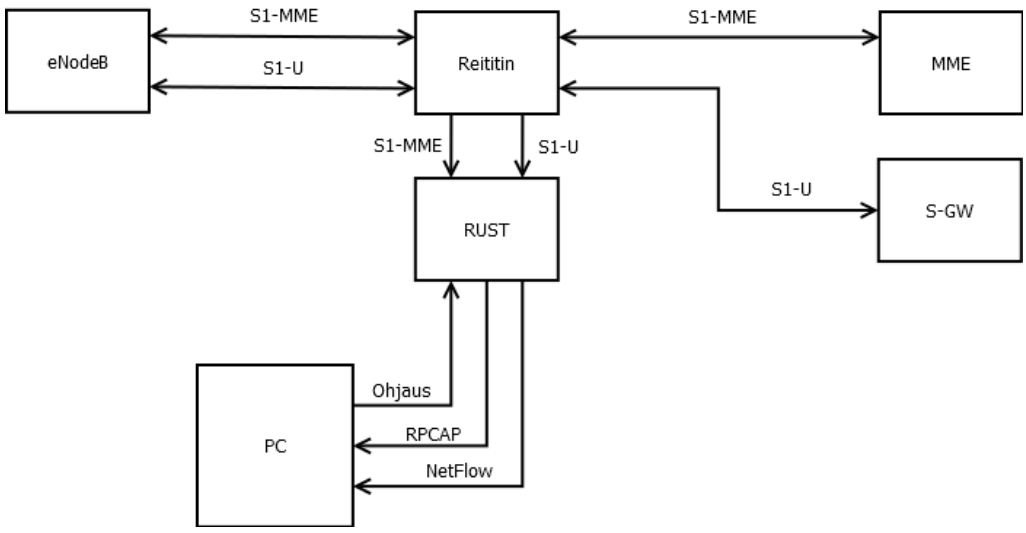
3DES-salauksessa salattavalle datalle suoritetaan ensin DES-salaus ensimmäisellä avaimella, sen jälkeen DES-salauksen purku toisella avaimella ja tämän jälkeen vielä DES-salaus kolmannella avaimella. 3DES-salauksen purku taas tapahtuu päinvastaisessa järjestyksessä: ensimmäisenä suoritetaan DES-salauksen purku kolmannella avaimella, sen jälkeen DES-salaus toisella avaimella ja viimeisenä DES-salauksen purku ensimmäisellä avaimella. (12.)

S1-rajapinnan tietoliikenteen salauksessa myös 3DES-salauksen yhteydessä käytetään AES-CBC-kappaleessa kuvattua CBC-parannusmenetelmää (7).

4 TIETOLIIKENTEEN MONITOROINTI

Jotta jonkin tietoliikenneyhteyden yli liikkuvaa dataa voitaisiin analysoida, täytyy se ensin pystyä kaappaamaan. Tällä tarkoitetaan useimmiten samassa lähiverkossa tapahtuvan tietoliikenteen nauhoittamista ja analysointia tarkoitukseen varatulla ohjelmistolla tai laitteistolla. Kaappaus voidaan tehdä myös etäratkaisuna, jolloin kohdeverkosta lähetetään jollakin laitteella, tässä tapauksessa RUSTilla, halutut paketit jatkokäsittelyä varten eteenpäin tietokoneelle, jonka ei välttämättä tarvitse olla samassa lähiverkossa. Kaappausjärjestelmä voi, järjestelmästä riippuen, joko tallentaa analysoimastaan tietoliikenneyhteydestä vain haluttuja statistiikkatietoja, esimerkiksi käyttäjävoiden lukumäärän, tai tallentaa kaiken siinä liikkuvan datan tiedostoon tai tietokantaan myöhempää analysointia varten. Kaapattavaa dataa voidaan kaappauksen yhteydessä tai jälkeenpäin myös suodattaa monin eri tavoin, esimerkiksi käytettävän protokollan tai eri protokollakerrosten osoitteiden perusteella.

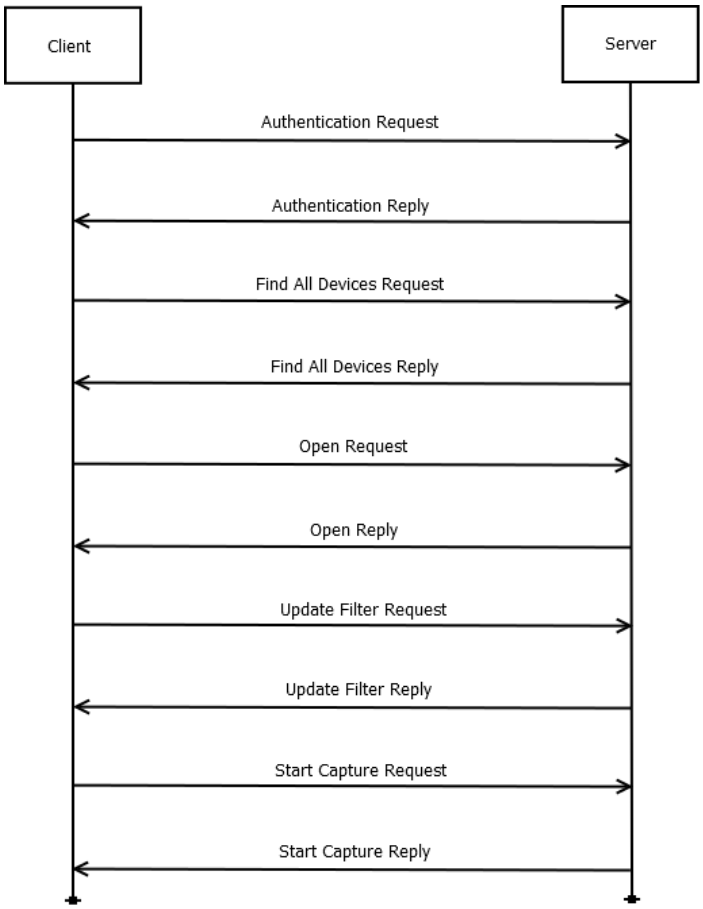
RUST suorittaa S1-MME:n kontrollisanomien kaappaukset RPCAPilla ja S1-U:n käyttäjädatan kaappaukset NetFlow-protokollalla ennaltamäärättyjen sääntöjen perusteella jostakin verkon solmukohdasta monistetusta tietoliikenteestä (kuva 9). Sääntönä voi olla esimerkiksi tietty lähde- tai kohdeosoite, ja nämä säännöt saadaan kaappaukset vastaanottavalta tietokoneelta.



KUVA 9. RUSTin toiminta

4.1 Remote Packet Capturing

RPCAP eli Remote Packet Capturing mahdollistaa tietoliikenteen kaappauksen etätoteutuksena. RPCAP-järjestelmä koostuu kahdesta erillisestä prosessista, palvelimesta joka kaappaa paketit ja asiakkaasta joka vastaanottaa ne. Etäkaappauksen hallintaan käytetään RPCAP-signalointia (kuva 10), jolla kaappauksen vastaanottava tietokone ohjaa kaappauksen suorittavaa laitetta tekemään tietokoneen pyytämiä toimintoja. (13.)

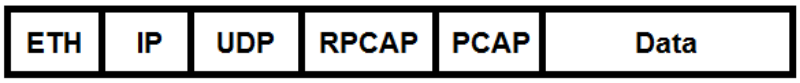


KUVA 10. Esimerkki RPCAP-signaloinnista

Authentication-viesteillä varmistetaan, että palvelimen kanssa keskustelevalla asiakkaalla on käyttöoikeus palvelimen kaappauspalveluun. Find All Devices -viesteillä palvelin välittää asiakkaalle listan rajapinnoista, joista kaappausta on mahdollista suorittaa. Open-viesteillä asiakas pyytää palvelinta avaamaan jonkin rajapinnan kaappausta varten. Update Filter -viesteillä voidaan päivittää pal-

velimen pakettien suodattamisen määrittävää asetustiedostoa ja Start Capture -viesteillä aloitetaan pakettien kaappaaminen ja edelleenlähetys. (14.) Update Filter -viestit eivät ole käytössä RUSTissa, vaan RPCAPin pakettisuodatin on korvattu Rugged Toolingin omalla, suorituskykyisemmällä suodatinratkaisulla.

Kohdeverkossa olevalla palvelimella, RUSTilla, suodatetaan tietoliikenteestä halutut paketit, joihin liitetään edelleenlähettämistä varten tarvittava lisäinformaatio: ethernet-, IP-, UDP-, RPCAP- ja PCAP-otsikkokentät (kuva 11). Tämän jälkeen ne lähetetään eteenpäin analysointia varten tietokoneelle, jonka ei tarvitse olla samassa lähiverkossa.



KUVA 11. Edelleenlähetettäviin paketteihin lisättävät otsikkokentät

RPCAP-otsikkokentällä kerrotaan kaapatut paketit vastaanottavalle taholle, miten paketit tulee käsitellä. Se sisältää kaikille RPCAP-otsikkokentille yhteisen osan (kuva 12) lisäksi myös erillisellä kentällä määriteltävän toisen osan, joka puolestaan sisältää jonkin signalointiviestin tiedot. VER-kentällä määritetään käytettävä RPCAP-versio, TYPE-kentällä määritetään RPCAP-otsikkokentän toisen osan tyyppi, VALUE-kenttä on joidenkin toisen osan tyyppien käyttämä kenttä ja PLEN-kentässä on kerrottu paketin sisältämän datan pituus. (14.)

KUVA 12. RPCAP-otsikkokentän yhteinen osa

Mikäli kyseessä on kaapattua dataa sisältävä paketti, on otsikkokentän toinen osa rpcap_pkthdr-tyyppiä (kuva 13), jossa timestamp_sec-kenttä sisältää aikaleiman sekuntiosan, timestamp_usec-kenttä aikaleiman mikro- tai nanosekuntiosan, caplen-kenttä kertoo hyötydatan pituuden, len-kenttä kertoo koko paketin pituuden ja npkt-kenttä sisältää juoksevan pakettinumeron (14).

timestamp_sec(32)	timestamp_usec(32)	caplen(32)	len(32)	npkt(32)

KUVA 13. rpcap_pkthdr-otsikkokenttä

RPCAP-kaapatut paketit vastaanottava tietokone purkaa pakettien sisältämän hyötydatan protokollakerrokset libpcap-formaattiin, jolloin pakettien sisältöä voidaan tutkia esimerkiksi Wireshark-ohjelmalla.

4.2 NetFlow

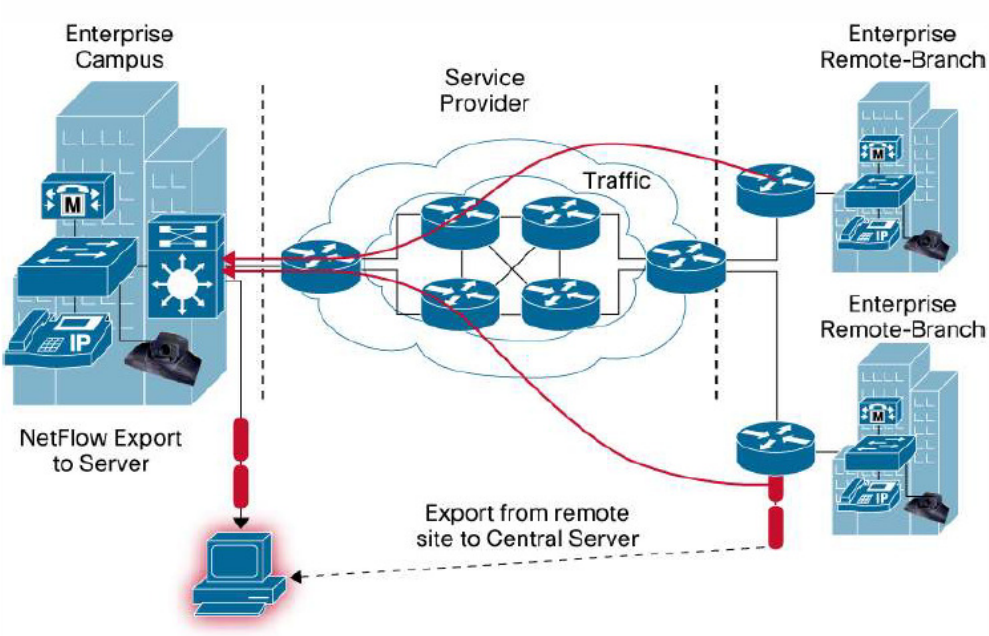
NetFlow on Cisco Systemsin kehittämä tietoliikenneverkkojen monitorointiin tarkoitettu protokolla. Sillä voidaan tarkkailla yksityiskohtaisesti esimerkiksi verkkoliikennettä käyttäviä sovelluksia, verkkoresurssien käyttöä, turvallisuusnäkökulmia ja verkkomuutoksien aiheuttamia ilmiöitä. NetFlow'n tuottamaa tallennetta kutsutaan flow-tallenteeksi, ja flow puolestaan on määritelty yhdensuuntaiseksi pakettien sekvenssiksi, jossa kaikilla paketeilla on sama kulkurajapinta, lähtö- ja kohdeosoite, IP-protokolla, lähtö- ja kohdeportti sekä TOS. (15.)

NetFlow'n tuorein versio on versionumeroltaan 9. Sen suurimpia muutoksia aiempiin NetFlow-versioihin on ohjelmiston käyttämän tallennusformaatin muuttuminen template-pohjaiseksi. NetFlow-kaappaukseen kykenevä laite tai järjestelmä kasaa kaappaamastaan datasta edelleenlähetystä varten vientipaketin, joka koostuu paketin otsikkokentästä ja sen perässä tulevasta, yhdestä tai useammasta, FlowSetistä (kuva 14). FlowSet on yleisnimitys paketin otsikkokenttää seuraavalle tallenteiden joukolle, ja sen sisältö voi olla joko template-tyyppiä (Template FlowSet), jolloin se sisältää informaatiota sitä seuraavista FlowSeteistä, tai varsinaista dataa (Data FlowSet). (16.)

Packet Header	Template FlowSet	Data FlowSet	Data FlowSet	.....	Template FlowSet	Data FlowSet

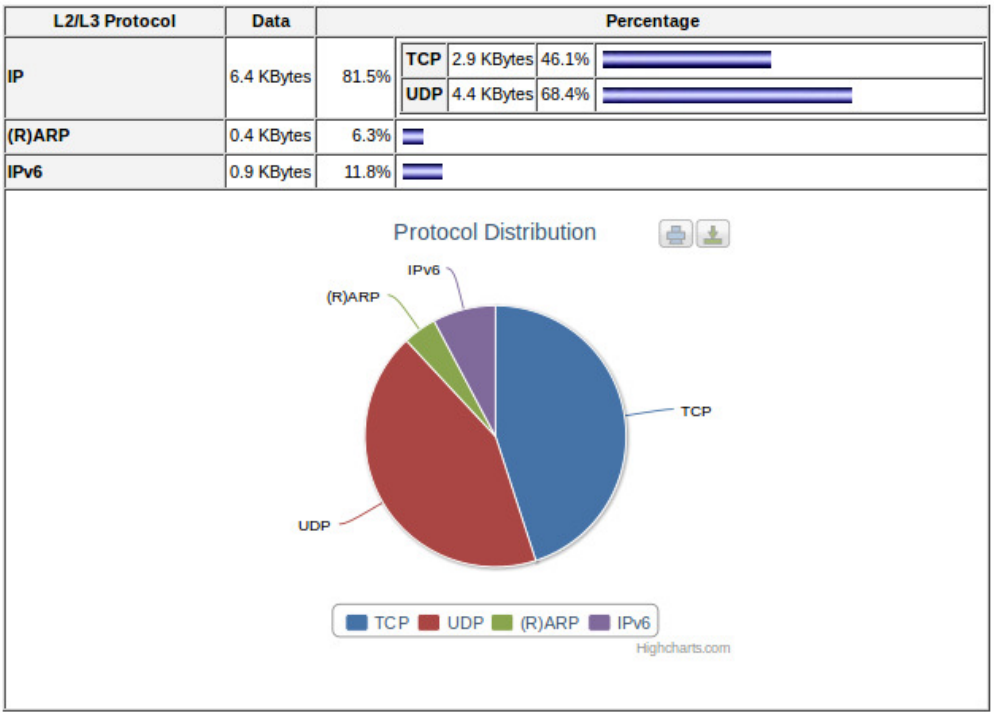
KUVA 14. NetFlow 9:n vientipaketin rakenne (16)

Kaappauksen suorittanut ja vientipaketin kasannut laite tai järjestelmä, tässä tapauksessa RUST, lähettää joukon vientipaketteja eteenpäin NetFlow-kerääjälle, joka on tyypillisimmin palvelin (kuva 15).



KUVA 15. NetFlow-kaappauksen toteutus esimerkkiverkossa (15)

Kerääjä kasaa vientipaketeista Data FlowSet -tallenteet niihin liittyvän Template FlowSetin ohjeiden perusteella ja muodostaa niistä raportteja esimerkiksi liikenne- tai turvallisuusanalyysia varten (kuva 16). (16.)



KUVA 16. Esimerkki NetFlow 9 -raportista

4.3 Aikaleimaus

Tämän opinnäytetyön yhteydessä aikaleimalla tarkoitetaan kaapattuun pakettiin lisättävää tietoa kaappauksen tapahtumahetkestä. Aikaleima on siis käytännössä paketit kaappaavan järjestelmän systeemikellon hetkellinen arvo. Aikaleimaus on mahdollista toteuttaa joko ohjelmallisesti tai erillisenä rautatoteutuksena.

Siirryttäessä yhä nopeampiin tietoliikenneverkkoihin muodostuu pakettien kaappauksen yhteydessä ongelmaksi aikaleimojen tarkkuus: pakettien saapumisten aikavälit voivat olla reilusti alle mikrosekunnin ja ne pitäisi silti pystyä yksikäsitteisesti aikaleimaamaan saapumisjärjestyksessä. Ohjelmallisissa toteutuksissa aika tarkistetaan aikaleimausta varten ohjelmaa suorittavan käyttöjärjestelmän kellosta, jonka näyttämää aikaa puolestaan joudutaan jatkuvasti korjaamaan. Nämä korjaukset saattavat olla kerrallaan jopa millisekuntien hyppäyksiä, jolloin pakettien aikaleimajärjestys saattaa mennä täysin sekaisin.

Tätä ongelmaa voidaan, ainakin sulautetuissa järjestelmissä, korjata suorittamalla aikaleimaus erillisellä laitetoteutuksella, jonka kelloa korjataan jatkuvasti mahdollisimman pienin askelin eikä se näin vaikuta aikaleimauksien järjestykseen. RUSTin toteutuksessa käytetyssä Octeon-verkkoprosessorissa on aikaleimaukselle edellä mainitun kaltainen erillinen laitetoteutus, jolloin aikaleimojen tarkkuuden suhteen ei pitäisi ilmetä ongelmia.

5 RUST

RUST eli Rugged Statistics on Rugged Tooling Oy:n toteuttama Caviumin Octeon-verkkoprosessorilla toimiva rajapinta-analysaattorisovellus. Tässä opinnäytetyössä RUSTilla on tarkoitus monitoroida LTE:n S1-rajapintaa, mutta jatkokehitysmahdollisuudet myös muille rajapinnoille ovat varsin realistiset. RUSTia on mahdollista käyttää joko monitoroitavan tietoliikenteen päätepisteenä tai tietoliikennettä edelleenlähettävänä verkkoelementtinä. Päätepistemoodissa monitoroitava tietoliikenne välitetään RUSTille jostakin verkon solmukohdasta kopioituna (kuva 9) ja kaappaukset suoritetaan tästä monistetusta tietoliikenteestä. Edelleenlähetysmoodissa monitoroitava tietoliikenne kulkee RUSTin läpi ja kaappaukset suoritetaan tästä läpimenevästä tietoliikenteestä. Edelleenlähetysmoodia ei ole tässä opinnäytetyössä käsitelty, sillä se ei realistisesti liity RUSTin toimintaan LTE-verkossa. (17.)

Jotta LTE-verkon tietoliikenteen suodattaminen monitorointia varten olisi mahdollista tehdä tietoliikenteen parametrien avulla, täytyy RUSTin purkaa IP-verkoissa käytettävät salaukset. RUST purkaa S1-rajapinnassa käytetyistä salauksista AES-CBC- ja 3DES-CBC-salaukset, mutta ei HMAC-SHA1-salausta, jota käytetään lähinnä tiedon alkuperän varmentamiseen eikä se näin ollen ole RUSTin toiminnan kannalta oleellinen. Salausten purkamisen jälkeen RUSTilla voidaan kaapata rajapinnan tietoliikenteestä halutut paketit suodattamalla tietoliikennettä RUSTin pakettisuodattimella ennalta määrättyjen sääntöjen perusteella. Sääntöjen laatimiseen on olemassa oma syntaksinsa ja yksittäinen sääntö voi olla esimerkiksi jokin käytetty protokolla, esimerkiksi TCP tai UDP, tai lähde- tai kohde-IP-osoite. RUSTilla on mahdollista suorittaa tietyllä säännöllä pelkkä RPCAP-kaappaus, pelkkä NetFlow-kaappaus tai molemmat. Myös salausten purkuun tarvittavat salausavaimet on mahdollista asettaa sääntökohtaisesti. (17.)

6 TESTAUSSUUNNITELMAN LAATIMINEN

Toiminnallisen testauksen tavoitteena on määrittävä, täyttääkö testattavan laitteen tai ohjelman eri toiminnallisuuksien toiminta sille asetetut vaatimukset. Toiminnallinen testaus suoritetaan yleisimmin niin sanotulla musta laatikko -menetelmällä, jolloin testattavan laitteen tai ohjelman sisäisestä toiminnasta ei tiedetä mitään, vaan tiedossa on vain testaukseen tarvittavat syötteet ja niitä vastaavat vaatimusmääritelmän mukaiset tulosteet. (18, s. 35.) Toiminnallista testausta suunniteltaessa täytyy normaalin toiminnan lisäksi ottaa huomioon myös ääritapaukset ja virhetilanteet, joiden aikana laitteen toiminnan tulisi epänormaalista tilanteesta huolimatta jatkua. Testitapaukset on hyvä suunnitella siten, että mukana on mahdollisimman laajasti erilaista testidataa – myös sellaisia syötteitä, joita laitteen tai ohjelman käyttöympäristössä ei suurella todennäköisyydellä tule koskaan esiintymään. Yhdessä testitapauksessa ei kannata yrittää testata mahdollisimman montaa asiaa, vaan laitteen tai ohjelman toiminnallisuus kannattaa jakaa järkevästi mahdollisimman pieniin kokonaisuuksiin. Toiminnallisen testauksen voidaan katsoa olevan valmis, kun kaikki laitteen tai ohjelman vaatimusmäärittelyn mukaiset toiminnallisuudet on kattavasti testattu. (19.)

Suorituskykytestauksen tavoitteena on määrittää testattavan laitteen suorituskyky oletettua käyttöympäristöä mahdollisimman hyvin vastaavassa testiympäristössä ja useissa laitteen oletetuissa, normaaleissa käyttötilanteissa. Testausta suoritetaan aloittamalla matalalla vaativuustasolla, josta testien vaativuutta nostettaan, kunnes suurin mahdollinen suorituskyky on saatu määritettyä kussakin tilanteessa. (19.)

Toiminnallisen ja suorituskykytestauksen toteuttaminen ei ole mahdollista ilman testien tarvitsemia testimateriaaleja. Testimateriaalilla tarkoitetaan tässä opinnäytetyössä RUSTiin testattaessa syötettäviä, realistista käyttötilannetta vastaavia datapaketteja, jotka sisältävät testitapauksesta riippuen joko kontrollisanomia tai käyttäjädataa. Opinnäytetyön tuloksena syntyneiden testitapausten tarvitsemia testimateriaaleja lähdettiin kokoamaan ennestään olemassa ollei-

den, pcap-formaatissa olevien Wireshark-nauhoitusten perusteella. Näistä nauhoituksista valittiin testitapausten suorittamiseen soveltuvia datapaketteja, joiden sisältöä vielä muokattiin tarvittaessa heksaeditorilla, jotta datapakettien sisältö olisi juuri haluttu.

Tämän opinnäytetyön aiheena ollut RUSTin testaussuunnitelma on laadittu IEEE-standardin 829-2008, Standard for Software and System Test Documentation, periaatteiden pohjalta. Testaussuunnitelman testitapausten perustana on RUSTin vaatimusmäärittelydokumentti. Esimerkkinä testaussuunnitelman sisältämästä testitapauksesta on liitteessä 3 esitetty testitapaus 3: AES-CBC-salaus. AES-CBC-salauksen purkaminen on olennainen osa koko RUSTin toimintaa tietoliikenteen kaappauksessa, joten sen toimivuus on hyvä testata varhaisessa vaiheessa. Testitapausta suunniteltaessa kannattaa ottaa huomioon testauksen mahdollinen suorittaja: testaajat voivat olla tietotasoltaan hyvin erilaisia, joten testitapaukseen tulisi sisällyttää kaikki tarpeellinen tieto juuri sen testin suorittamisen mahdollistamiseksi. Testitapauksen tarkoituksesta selviää testitapauksen määrittelemän testin kohde, tietyt testattavan laitteen tai ohjelman ominaisuudet. Testauksen suorittamiseen tarvittavan laitteiston kertominen kootusti etukäteen säästää testaajien aikaa, kun tarvittavan kokoonpanon komponentteja ei tarvitse lähteä testin vaiheista erikseen päättelemään. Ilman tietoa tarvittavista syötteistä testausta on mahdotonta lähteä suorittamaan ja odotetut tulokset ovat oltava tiedossa, jotta voidaan määrittää, läpäisikö laite tai ohjelma testin vai ei. Testin vaiheet on hyvä kuvata mahdollisimman yksityiskohtaisesti, jotta eri testaajien välillä olisi testin suorittamisessa mahdollisimman vähän eroavaisuuksia. Testitapausten ja testimateriaalikuvausten lisäksi testaussuunnitelmaan laadittiin myös yksityiskohtaiset käyttöohjeet kaikille testauksessa tarvittaville ohjelmistoille, jotta testauksen aloittaminen sujuisi mahdollisimman helposti.

Tämän opinnäytetyön tuloksena syntynyt RUSTin toiminnallisen testauksen suunnitelma on liitteenä opinnäytetyön Rugged Toolingille jäävässä versiossa.

7 YHTEENVETO

Työn tarkoituksena oli laatia testaussuunnitelma Rugged Tooling Oy:n toteuttamalle LTE-verkon rajapinta-analysaattorille. Testauksen toteutus rajattiin käsittelemään toiminnallista testausta eli testattavan laitteen, RUSTin, eri toiminnallisuuksien toimivuuden selvittämistä sekä RUSTin suorituskykytestaamista. Tämän lisäksi tuotettiin testauksen tarvimat testimateriaalit. Työssä oli alun perin tarkoitus myös toteuttaa testaussuunnitelman mukainen RUSTin testaaminen, mutta yrityksen projektien aikataulullisista syistä laitetta ei saatu valmiiksi ennen tämän opinnäytetyön valmistumista. Uusina asioina opinnäytetyön aikana tulivat vastaan ennen kaikkea testaussuunnitelman laatiminen ja tietoliikenneyhteyksien monitorointi pakettien kaappauksella, minkä lisäksi tietämykseni LTE-verkon toiminnasta syveni huomattavasti. Myös heksaeditorin käyttö pcap-tiedostomuodossa olleiden datapakettien muokkaamiseen oli uutta.

Työn tuloksena syntynyttä toiminnallisen testauksen suunnitelmaa varten ei tässä opinnäytetyössä ole selvitetty kaikkia mahdollisia ääritapauksia ja virhetilanteita, vaan suunnitelmaan määriteltiin RUSTin toiminnallisuuksien testaaminen normaalitilanteissa mahdollisimman kattavasti. Suorituskykytestaukseen suunniteltiin kattava testitapausten joukko, jolla RUSTin suoriutumista erilaisissa vaativissa tilanteissa voidaan mitata. Toiminnallisen testauksen jatkokehityksessä kannattaa panostaa eri virhetilanteiden selvittämiseen mahdollisimman kattavasti, jotta RUST toimii oikein ja kaatumatta myös verkon häiriötilanteissa. Suorituskykytestauksen osioon tullaan jatkossa laatimaan suorituskykytestejä vastaamaan mahdollisia uusia RUSTin käyttötarkoituksia. Yhtenä seuraavista kehitysvaiheista RUSTin testauksessa tulee myös olemaan testitapausten suorittamisen ja testitulosten validoinnin automatisointimahdollisuuksien selvittäminen ja automatisoinnin toteuttaminen.

Työn alkuvaiheessa jouduin pohtimaan omia aiemmin hyväksi havaitsemiani työskentelytapoja kriittisesti, sillä työnteon käynnistäminen osoittautui varsin hankalaksi. Aikaisemmin toiminut viimeisen illan menetelmä ei näin laajan projektin kanssa toiminut alkuunkaan – ennen itse laatimaani henkilökohtaista pro-

jektisuunnitelmaa raportin kirjoittamisessa tai testisuunnitelman laatimisessa ei tapahtunut edistymistä käytännössä lainkaan. Päivittäisen aikataulun valmistuttua pääsin viimein liikkeelle ja opinnäytetyön kirjoittaminen osoittautui lopulta mielekkääksi ja mukavaksi projektiksi.

LÄHTEET

1. 3GPP TR 25.913 V9.0.0 Release 9. 2010. Universal Mobile Telecommunications System (UMTS); LTE; Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN). Saatavissa: http://www.3gpp.org/ftp/Specs/html-info/25913.htm. Hakupäivä 6.4.2012.

2. 3GPP TS 36.300 version 10.7.0 Release 10. 2012. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. Saatavissa: http://www.3gpp.org/ftp/Specs/html-info/36300.htm. Hakupäivä 6.4.2012.

3. LTE Network Architecture. 2009. Alcatel-Lucent. Strategic White Paper. Saatavissa: http://www.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers%2FCPG0599090904_LTE_Network_Architecture_EN_StraWhitePaper.pdf&lu_lang_code=en_WW&REFERRER=. Hakupäivä 15.4.2012.

4. Introduction to Evolved Packet Core. 2009. Alcatel-Lucent. Strategic white paper. Saatavissa: http://lte.alcatel-lucent.com/locale/en_us/downloads/wp_evolved_packet_core.pdf. Hakupäivä 7.4.2012.

5. 3GPP TS 36.410 version 10.2.0 Release 10. 2011. LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 general aspects and principles. Saatavissa: http://www.3gpp.org/ftp/Specs/html-info/36410.htm. Hakupäivä 7.4.2012.

6. 3GPP TS 36.413 version 10.5.0 Release 10. 2012. LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application

Protocol (S1AP). Saatavissa: http://www.3gpp.org/ftp/Specs/html-info/36413.htm. Hakupäivä 7.4.2012.

7. Security Architecture for the Internet Protocol. 2005. Internet Engineering Task Force. Saatavissa: http://tools.ietf.org/html/rfc4301. Hakupäivä 17.4.2012.

8. IPsec. 2012. Wikipedia. Saatavissa: http://en.wikipedia.org/wiki/IPsec. Hakupäivä 17.4.2012.

9. Announcing the Advanced Encryption Standard. 2001. National Institute of Standards and Technology. Saatavissa: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Hakupäivä 30.4.2012.

10. Recommendation for Block Cipher Modes of Operation. 2001. National Institute of Standards and Technology. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf. Hakupäivä 30.4.2012.

11. Block cipher modes of operation. 2012. Wikipedia. Saatavissa: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation. Hakupäivä 30.4.2012.

12. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. 2008. National Institute of Standards and Technology. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf. Hakupäivä 30.4.2012.

13. Remote Capture. 2007. WinPcap. Saatavissa: http://www.winpcap.org/docs/docs_40_2/html/group__remote.html. Hakupäivä 25.4.2012.

14. RPCAP-otsikkotiedoston määritelmä. 2009. WinPcap. Saatavissa: http://www.winpcap.org/docs/docs_412/html/pcap-remote_8h_source.html. Hakupäivä 26.4.2012.

15. Introduction to Cisco IOS® NetFlow. 2007. Cisco Systems. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.pdf. Hakupäivä 8.4.2012.

16. Cisco IOS NetFlow Version 9 Flow-Record Format. 2011. Cisco Systems. Saatavissa: http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.pdf. Hakupäivä 8.4.2012.

17. Rugged Tooling Oy. 2012. RUST Software Requirement Specification.

18. IEEE Standard Glossary of Software Engineering Terminology. 1990. IEEE Std 610.12-199. Institute of Electrical and Electronics Engineers. Saatavissa: http://standards.ieee.org/findstds/standard/610.12-1990.html. Hakupäivä 9.5.2012.

19. IEEE Standard for Software and System Test Documentation. 2008. IEEE Std 829-2008. Institute of Electrical and Electronics Engineers. Saatavissa: http://standards.ieee.org/findstds/standard/829-2008.html. Hakupäivä 9.5.2012.

Elementary Procedure	**Aloitusviesti**	**Onnistuneen toimenpiteen vastausviesti**	**Epäonnistuneen toimenpiteen vastausviesti**
Handover Preparation	HANDOVER REQUIRED	HANDOVER COMMAND	HANDOVER PREPARATION FAILURE
Handover Resource Allocation	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE	HANDOVER FAILURE
Path Switch Request	PATH SWITCH REQUEST	PATH SWITCH REQUEST ACKNOWLEDGE	PATH SWITCH REQUEST FAILURE
Handover Cancellation	HANDOVER CANCEL	HANDOVER CANCEL ACKNOWLEDGE	
E-RAB Setup	E-RAB SETUP REQUEST	E-RAB SETUP RESPONSE	
E-RAB Modify	E-RAB MODIFY REQUEST	E-RAB MODIFY RESPONSE	
E-RAB Release	E-RAB RELEASE COMMAND	E-RAB RELEASE RESPONSE	
Initial Context Setup	INITIAL CONTEXT SETUP REQUEST	INITIAL CONTEXT SETUP RESPONSE	INITIAL CONTEXT SETUP FAILURE
S1 Setup	S1 SETUP REQUEST	S1 SETUP RESPONSE	S1 SETUP FAILURE
UE Context Release	UE CONTEXT RELEASE COMMAND	UE CONTEXT RELEASE COMPLETE	
UE Context Modification	UE CONTEXT MODIFICATION REQUEST	UE CONTEXT MODIFICATION RESPONSE	UE CONTEXT MODIFICATION FAILURE
eNB Configuration Update	ENB CONFIGURATION UPDATE	ENB CONFIGURATION UPDATE ACKNOWLEDGE	ENB CONFIGURATION UPDATE FAILURE
MME Configuration Update	MME CONFIGURATION UPDATE	MME CONFIGURAION UPDATE ACKNOWLEDGE	MME CONFIGURATION UPDATE FAILURE
Write-Replace Warning	WRITE-REPLACE WARNING REQUEST	WRITE-REPLACE WARNING RESPONSE	
Kill	KILL REQUEST	KILL RESPONSE	

Elementary Procedure	**Message**
Handover Notification	HANDOVER NOTIFY
E-RAB Release Indication	E-RAB RELEASE INDICATION
Paging	PAGING
Initial UE Message	INITIAL UE MESSAGE
Downlink NAS Transport	DOWNLINK NAS TRANSPORT
Uplink NAS Transport	UPLINK NAS TRANSPORT
NAS non delivery indication	NAS NON DELIVERY INDICATION
Error Indication	ERROR INDICATION
UE Context Release Request	UE CONTEXT RELEASE REQUEST
DownlinkS1 CDMA2000 Tunneling	DOWNLINK S1 CDMA2000 TUNNELING
Uplink S1 CDMA2000 Tunneling	UPLINK S1 CDMA2000 TUNNELING
UE Capability Info Indication	UE CAPABILITY INFO INDICATION
eNB Status Transfer	eNB STATUS TRANSFER
MME Status Transfer	MME STATUS TRANSFER
Deactivate Trace	DEACTIVATE TRACE
Trace Start	TRACE START
Trace Failure Indication	TRACE FAILURE INDICATION
Location Reporting Control	LOCATION REPORTING CONTROL
Location Reporting Failure Indication	LOCATION REPORTING FAILURE INDICATION
Location Report	LOCATION REPORT
Overload Start	OVERLOAD START
Overload Stop	OVERLOAD STOP

eNB Direct Information Transfer	eNB DIRECT INFORMATION TRANSFER
MME Direct Information Transfer	MME DIRECT INFORMATION TRANSFER
eNB Configuration Transfer	eNB CONFIGURATION TRANSFER
MME Configuration Transfer	MME CONFIGURATION TRANSFER
Cell Traffic Trace	CELL TRAFFIC TRACE
Downlink UE Associated LPPa Transport	DOWNLINK UE ASSOCIATED LPPA TRANSPORT
Uplink UE Associated LPPa Transport	UPLINK UE ASSOCIATED LPPA TRANSPORT
Downlink Non UE Associated LPPa Transport	DOWNLINK NON UE ASSOCIATED LPPA TRANSPORT
Uplink Non UE Associated LPPa Transport	UPLINK NON UE ASSOCIATED LPPA TRANSPORT

Testitapauksen numero ja nimi:

3: AES-CBC-salaus

Tarkoitus:

1. Testata AES-CBC-salauksen purkamisen toimivuus

Tarvittava laitteisto:

1. RUST
2. PC, jossa Wireshark, tcpreplay, rpcapd, RUSTin käyttöliittymätyökalu ja vähintään kaksi verkkokorttia
3. Testijärjestelmä, joka on rakennettu kohtien 1-2 laitteista seuraavasti:
- Yhdistä RUSTin portti E2 PC:n verkkokorttiin 1
- Yhdistä RUSTin portti E0 PC:n verkkokorttiin 2

Syötteet:

1. Testidataa, **handover_8_to_24_aes.pcap** (salattu avaimella 616573636263656e6372797074696f6e, avaimen pituus 128 bittiä)
2. Salauksenpurkusääntö: Filter: sip 10 and ip 10.44.34.8, key: 616573636263656e6372797074696f6e, key length: 128, algorithm: aes-128
3. Suodatussääntö: Filter: sctp, RPCAP: yes, Netflow: no

Odotettu tulos:

1. RUST purkaa AES-CBC-salauksen oikein, kun sille on annettu oikea salausavain

Vaiheet:

1. Käynnistä RUST uudelleen, säännöt nollautuvat
2. Käynnistä rpcapd verkkokortin 1 IP-osoitteeseen
3. Käynnistä käyttöliittymätyökalu
4. Syötä salauksenpurkusääntö (Syötteet 2.) RUSTille
5. Syötä suodatussääntö (Syötteet 3.) RUSTille
6. Tarkista käyttöliittymästä, että säännöt vastaanotettiin
7. Käynnistä Wireshark-nauhoitus RUSTin portista E2
8. Lähetä PC:ltä handover_8_to_24_aes.pcap RUSTille tcpreplay-ohjelmalla
9. Tarkista Wireshark-nauhoituksesta, että salauksen purku onnistui vertaamalla sitä alkuperäiseen salaamattomaan dataan (avaa handover_8_to_24.pcap Wiresharkissa)