LTE transport network security

Jason S. Boswell
Head of Security Sales, NAM
Nokia Siemens Networks
New evolved Networks - new security needs

Walled Garden Transport & Protocols
- E1 / T1
- ATM
- MTP
- SCCP
- TUP / ISUP……

Open IP based Networks
Carrier Grade Ethernet
IP / SIP / …

Enforcing Ciphering and Integrity Protection

Manual network enrollment
- Manual commissioning on site
- Fully pre-planned network configuration
- Pre-planned transport relations
- pre-planned security peers

Self Organizing Networks
- Plug and Play
- Automated network configuration
- Automated network integration
- Automated connection establishment

Enforcing Network Element Authentication

Public IP threats

“All IP” networks

“SON” networks

“All IP” networks

mature networks

mature networks

Proprietary – NSN Security / May 2012

© Nokia Siemens Networks
So why do we need new 3GPP standards?

In the past - Protected by proprietary protocols and a closed environment

From 3G to LTE

Now - We have IP outside of the operator buildings – large threat footprint in small cell deployments

Radio Access Transport is now IP Based

Non IP transport traffic

IP transport traffic

Internet Operator Services

Internet Operator Services

3G

LTE

IPSec in tunnel mode between Security Gateways
IPSec profile and configuration

TS 33.210 - Network Domain Security

TS 33.401 - Security Architecture
- Defines IPSec for S1-MME & X2 Control plane and S1 & X2 User plane
- IKEv2 certificates based authentication
- Authentication by Public Certificates

TS 33.310 - Authentication Framework
- Specifies rules for Cross Certification between operators

© Nokia Siemens Networks

Proprietary – NSN Security / May 2012
3GPP Standardization Background

TS 33.210
Network Domain Security
• IPSec in tunnel mode between Security Gateways
• IPSec profile and configuration

TS 33.310
Authentication Framework
• Specifies rules for Cross Certification between operators

TS 33.401
Security Architecture
• Defines IPSec for S1-MME & X2 Control plane and S1 & X2 User plane
  • IKEv2 certificates based authentication
  • Authentication by Public Certificates
Security threats to Radio Access transport of LTE

- Denial of Service
- eNodeB spoofing
- Eavesdropping of user traffic
- Unauthorized access of eNodeB and other network equipment
Business impact of materialized threats on Radio Access transport of LTE

- Loss of Revenue
- Contractual Penalties
- Damage to Image

Radio Access Transport In LTE

Subscribers canceling their Subscription
LTE Transport Security Solution Overview

Base stations have IPSec support. *needs to be native/on-board for compliance

Business Benefits

- Risk mitigation of
  - Service unavailability (caused by DoS)
  - Eavesdropping of user traffic
  - Unauthorized access of network elements
  - eNodeB spoofing
- OPEX effective solution that enables strong mutual authentication to establish secure connections between network elements
- Multi-vendor capable Transport Security and PKI solution that can be integrated to existing infrastructure

© Nokia Siemens Networks  Proprietary – NSN Security / May 2012
Malicious end-user activity
Can have many forms …

Spoofing
IP address spoofing, Caller ID spoofing …

Man-in-the-Middle (MITM)
Eavesdropping, chosen-ciphertext attack, substitution attack, replay attack

Denial-of-Service (DoS)
SYN flood, LAND attack, Smurf attack, Ping of death, Teardrop attack …

Distributed Denial-of-Service (DoS)
Botnets/Dosnets, peer-to-peer attacks, Distributed Reflected DoS (DRDoS) attacks like ICMP echo request and DNS amplification attacks …

© Nokia Siemens Networks
Proprietary – NSN Security / May 2012
LTE Architecture Overview

PKI is applied to
• Authenticate network elements
• Authorize network access
• Protect integrity and confidentiality on transport path for all planes (control/user/management/sync)
Closing Points

3GPP compliant Certificate Authority and IPSec solution (TS 33.210, TS 33.401, TS 33.310)

Maintain CIA – Confidentiality, Integrity & Availability even in “high risk” environments

Efficient operation through automated certificate life cycle management and complete integration into O&M systems.

LTE Transport security ensured w/out compromising performance, design, flexibility or manageability of the network

Cost savings through zero footprint installations w/ inbuilt IPSec + Plug & Play deployment

Highest security across all layers

User plane

Control plane

Management plane

© Nokia Siemens Networks

Proprietary – NSN Security / May 2012