Consortium

CASSIDIAN · ERNW Living Security. · Fraunhofer SIT · Hochschule Augsburg University of Applied Sciences · Nokia Siemens Networks · RWTH AACHEN UNIVERSITY

ASMONIA

Attack analysis and Security concepts for MObile Network infastructures supported by collaborative Information exchAnge

SPONSORED BY THE
Federal Ministry of Education and Research

Threats and Risks for 4G Mobile Communication Networks and Terminals

Peter Schneider
Nokia Siemens Networks Research

ASMONIA Workshop - Heidelberg

29.03.2011

Overview

- Federal Ministry for Education and Research - call for proposals: Need for " ... Analyse der Gefährdungen von 4G Netzen..."

  → "Gefährdung": danger/endangerment/hazard/threat/…

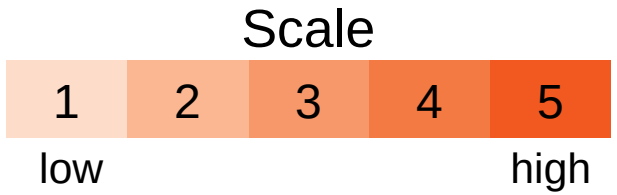
☐	hazard analysis [tech.]		die **Gefährdungsanalyse**
☐	threat analysis [law]		die **Gefährdungsanalyse**
☐	vulnerability analysis [law]		die **Gefährdungsanalyse**

from dict.leo.org

- It's about strenghtening networks against deliberate attacks.
- ASMONIA focus: Detecting attacks
  - What to look for → What are the most relevant threats/attack types - which of them cause the high risks?
  - Where to look → What are the most endangered parts of the network - where are the high risks?

Threat and Risk Analysis (TRA) Method

- checked: a number of ISO/3GPP/ETSI/ITU documents
- individual approach chosen:
  - around 10 generic threats
    - flooding an interface, eavesdropping, compromise via management interface, theft of service, …
  - around 20 assets (network elements, network parts)
  - per asset and threat: assess
    - likelihood of attack
    - overall vulnerability of the asset
    - impact on the network



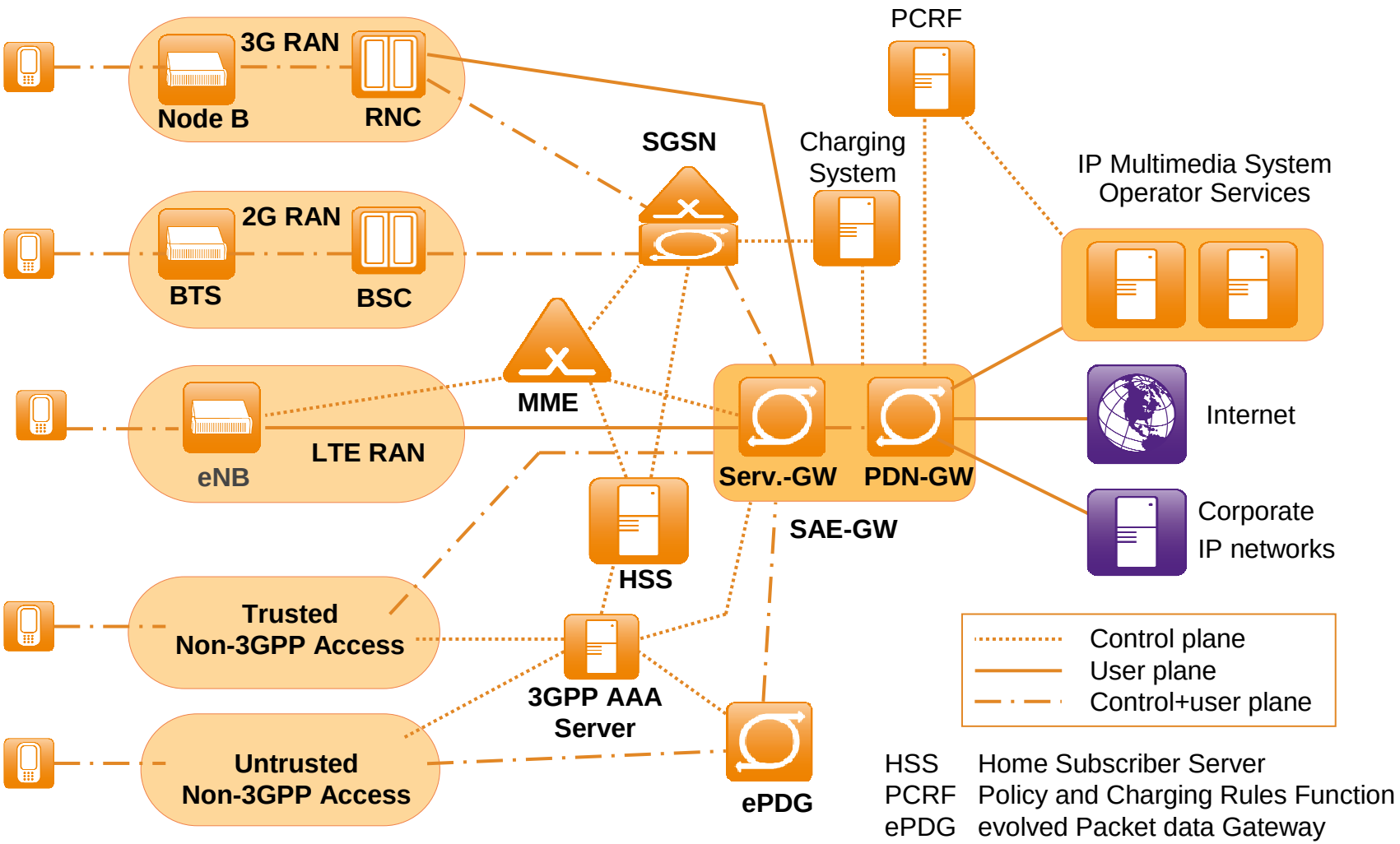
➔RISK = likelihood * vulnerability * impact

3GPP Network Generations

3GPP: 3.Generation Partnership Project (organization in charge of mobile network standards).

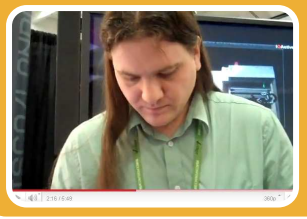
2G	GSM Global System for Mobile Communications	Circuit Switched (CS) Base Transceiver Station (BTS), Base Station Controller (BSC), Mobile Switching Center
2.5G	GPRS General Packet Radio Service	Packet Switched (PS) → IP services GSM RAN (Radio Access Network) SGSN - GGSN (Serving - Gateway GPRS Support Node)
3G	UMTS Universal Mobile Telecommunications System	CS + PS new RAN: • Node B • Radio Network Controller (RNC) TDM/ATM/IP transport options
4G	LTE/SAE Long Term Evolution / System Architecture Evolution	PS only (no more circuits!) new RAN: evolved Node B (eNB) new Core: • Mobility Management Entity (MME) • SAE-Gateway (SAE-GW)

3GPP 4G Mobile Network



HSS Home Subscriber Server
PCRF Policy and Charging Rules Function
ePDG evolved Packet data Gateway

3GPP Security Architectures

2G	GSM	network authenticates mobile (shared secret) radio interface encryption (e.g. algorithm A5/1) → still prevents widespread technical fraud but: concepts are weak according to todays standards  **Chris Paget** RSA conference March 2010 Eavesdropping GSM calls with a fake Base Station
3G	UMTS	mutual authentication network – mobile (shared secret) strong radio interface encryption/integrity protection cryptographic protection on core interfaces specified (IPsec) → has proven remarkably resilient against security analyses, still seems fully adequate for 3G networks
4G	LTE/SAE	builds on UMTS security, enhancements to account for • changed architecture • new service and business environment

Ranking of Threats

Threat	Risk
Compromise via management interface	38
Malicious insider	36
Compromise via implementation flaw	23
Flooding an interface	16
Crashing a network element	14
Eavesdropping (user plane)	13
Theft of service	13
Eavesdropping (control plane)	12
Traffic modification (control plane)	9
Data modification on a network element	8
Unauthorized data access	8
Traffic modification (user plane)	7

Ranking of Network Elements (critical ones)

Asset	Risk
HeNB (4G home base station, "femto-cell")	29
SAE-Gateway	21
IP Multimedia System	20
Operation and Maintenance Servers	19
GGSN (Gateway GPRS Support Node)	19
IP/MPLS Router (e.g. core site router)	19
eNB (4G base station)	19
DNS-Server	18
ePDG (evolved Packet Data Gateway)	17
PCRF (Policy and Charging Rules Function)	17

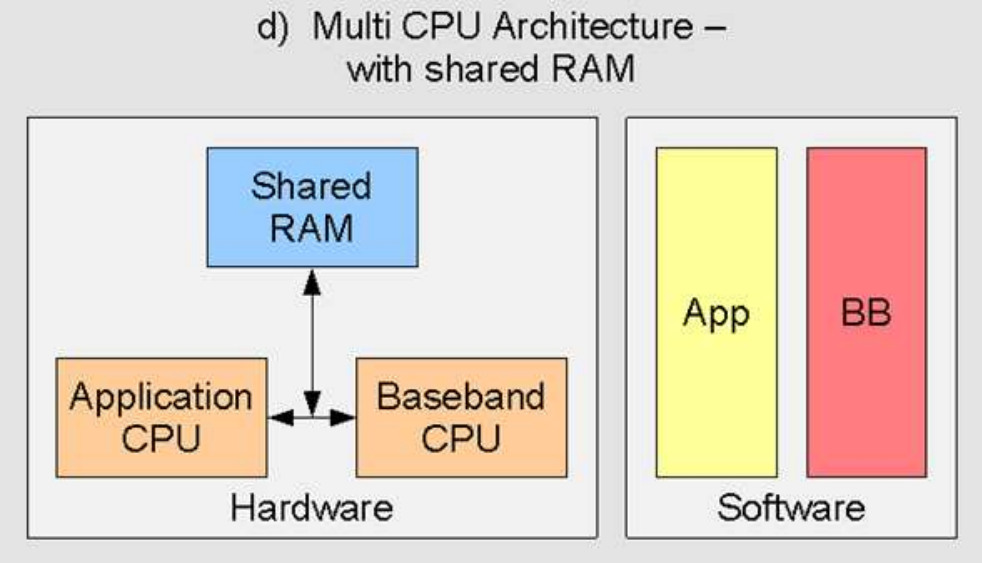
Ranking of Network Elements (less criticals ones)

Asset	Risk
Circuit-Switched Core Network Domain	14
Web-Proxy	14
Charging Systems	14
HSS (Home Subscriber Server)	13
Mobility Management Entity	12
SGSN (Serving GPRS Support Node)	12
HeNB-Gateway	11
EIR (Equipment Identity Register)	11
3GPP AAA-Server/Proxy	10

Mobile Terminals

- generic threats assessed, but they are not fully adequate
- main threat: compromise
  - strong impact on user
  - relevant for the network in case many terminals are affected

➔ mobile botnets



➔ both application and baseband part can be abused!

Further Work

- Terminals: more work on *how* they can get compromised
- Networks:
  - explore some more "remote" areas
  - have a more detailed look at some critical spots
- More pentests

➔ Another TRA document is due 02/2012

- The prose TRA document is on www.asmonia.de
  (http://www.asmonia.de/deliverables/D5.1_I_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf)
- Acknowledgements to the co-authors of the TRA document:
  André Egners, Enno Rey, Sascha Wessel