Consortium

CASSIDIAN AN EADS COMPANY | ERNW Living Security. | Fraunhofer AISEC | Hochschule Augsburg University of Applied Sciences | Nokia Siemens Networks | RWTH AACHEN UNIVERSITY

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

SPONSORED BY THE
Federal Ministry of Education and Research

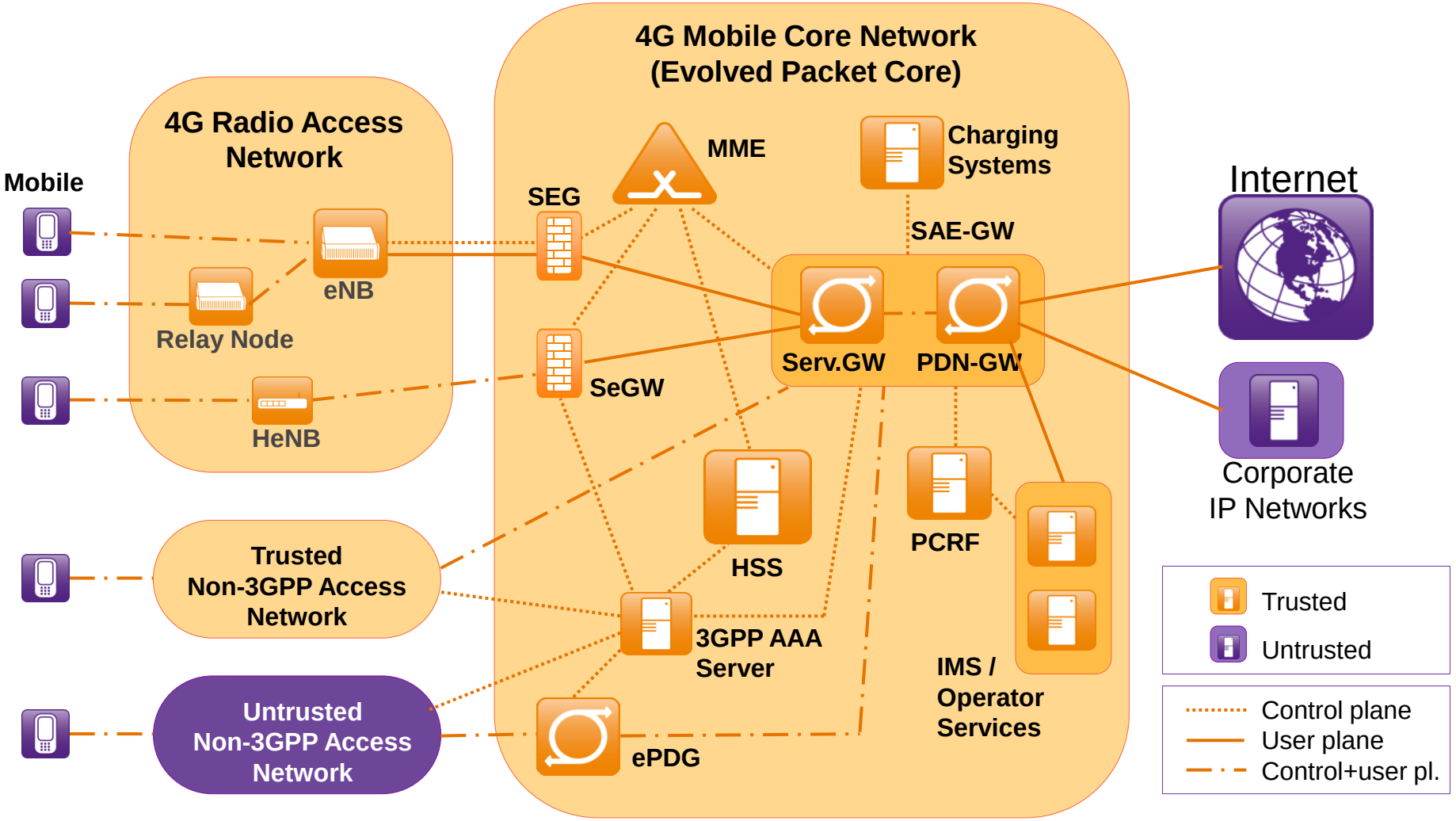
4G Mobile Networks At Risk

The ASMONIA Threat and Risk Analysis for 4G Mobile Networks

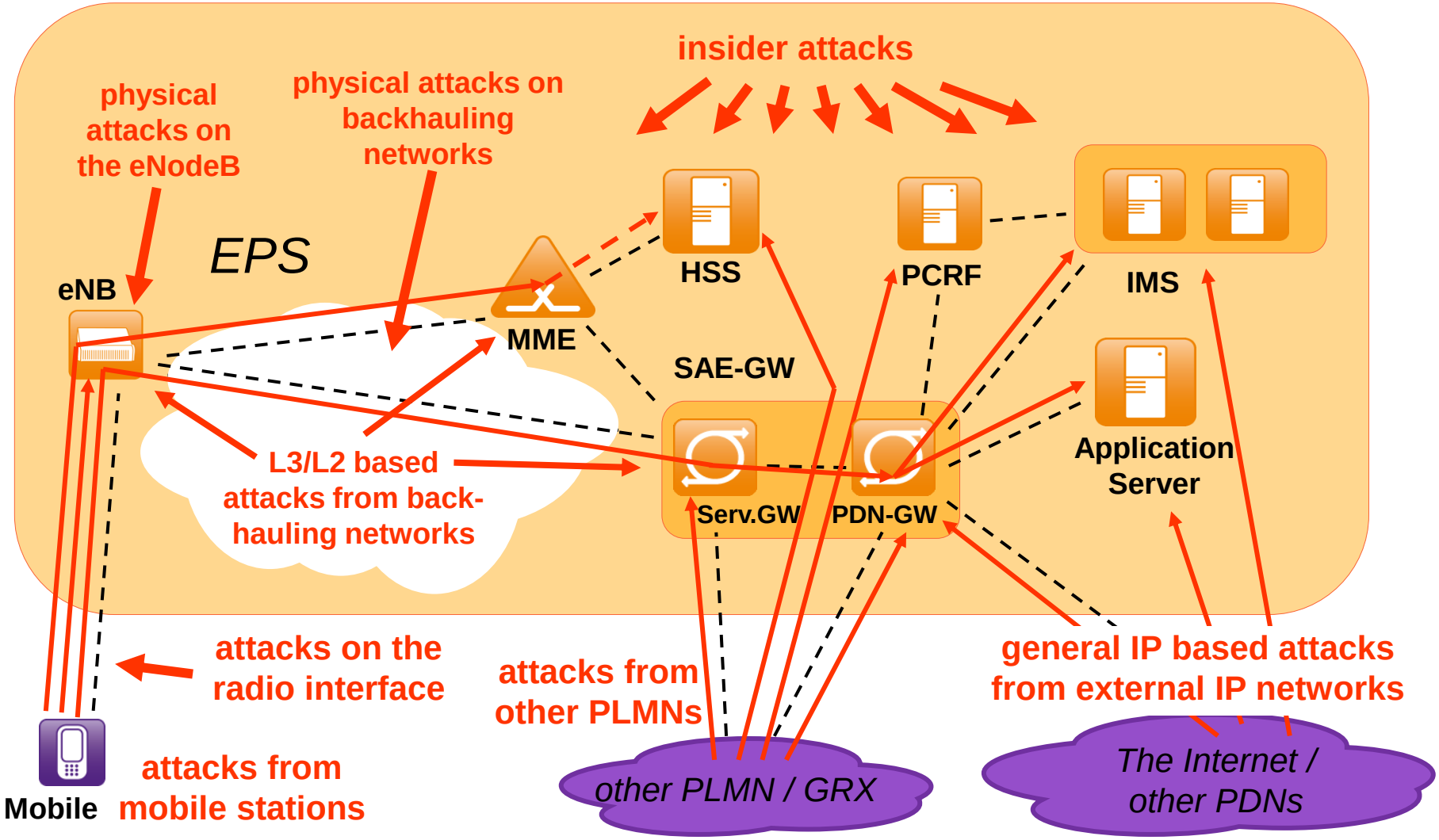
Peter Schneider
Nokia Siemens Networks Research

07.05.1203

3GPP 4G Mobile Network

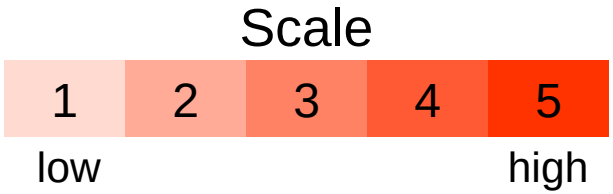


3GPP 4G Mobile Network



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

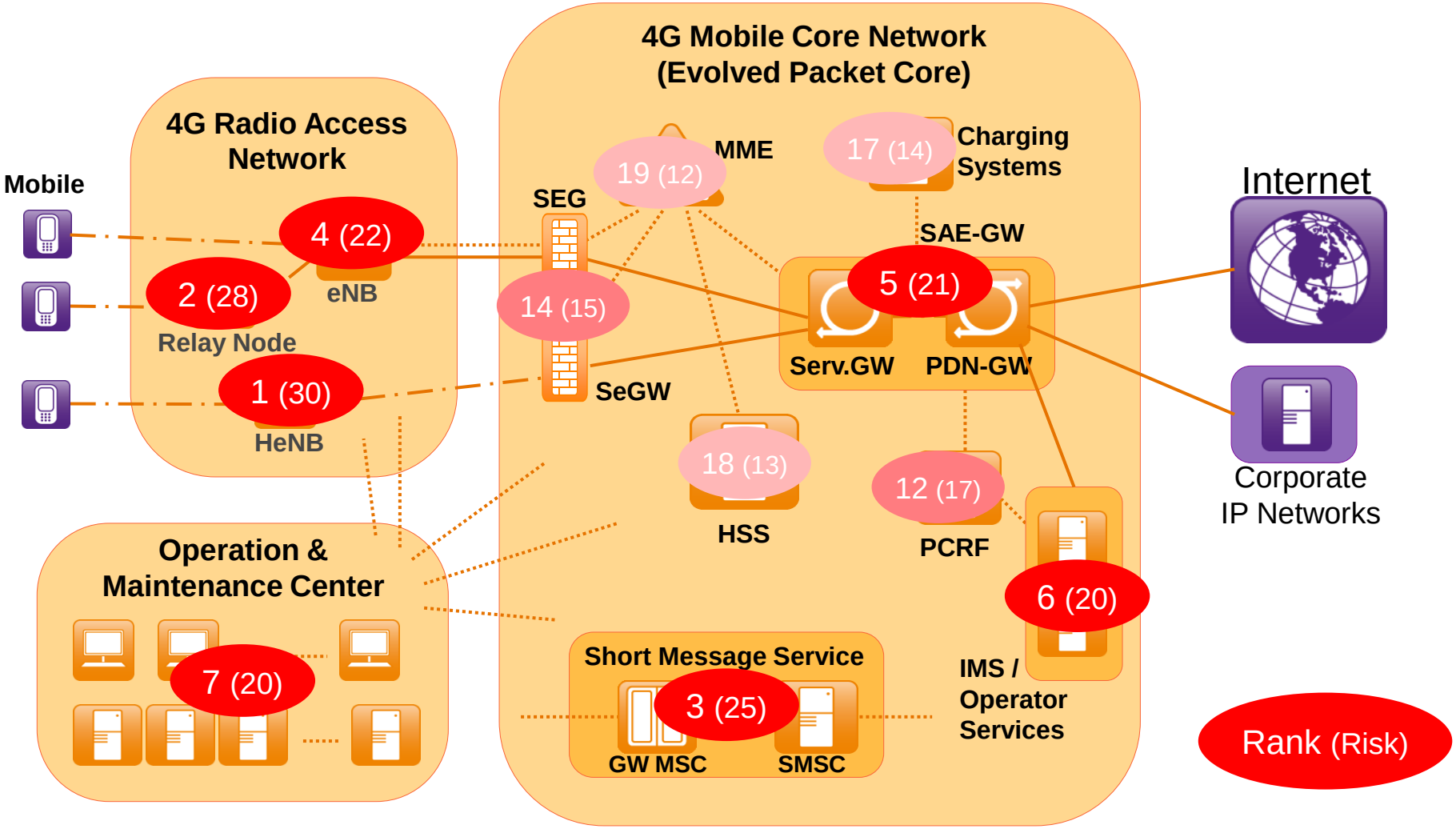


➔RISK = likelihood * vulnerability * impact

Ranking of Threats

Threat	Risk
Compromise via management interface	39
Malicious insider	33
Compromise via implementation flaw	26
Flooding an interface	19
Crashing a network element	16
Theft of service	15
Eavesdropping (user plane)	15
Eavesdropping (control plane)	13
Unauthorized access to data on a network element	10
Traffic modification (control plane)	10
Traffic modification (user plane)	9
Data modification on a network element	9

Ranking of Assets



Ranking of Network Elements (most critical ones)

Asset	Risk
HeNB (4G home base station, "femto-cell")	30
Relay Node	28
Short Message Service	25
eNB (4G base station)	22
SAE-Gateway	21
IP Multimedia System	20
Operation and Maintenance Servers	20
GGSN (Gateway GPRS Support Node)	19
IP/MPLS Router (e.g. core site router)	19
DNS-Server	18
ePDG (evolved Packet Data Gateway)	17
PCRF (Policy and Charging Rules Function)	17

Ranking of Network Elements (less critical ones)

Asset	Risk
Location Services	15
Security Gateway	15
Web Proxy	14
Circuit-Switched Core Network Domain	14
Charging Systems	14
HSS (Home Subscriber Server)	13
MME (Mobility Management Entity)	12
SGSN (Serving GPRS Support Node)	12
HeNB-Gateway	12
EIR (Equipment Identity Register)	11
3GPP AAA-Server/Proxy	10

Summary & Conclusion

- ASMONIA has carried out a comprehensive Threat and Risk Analysis (TRA) of 4G mobile communication networks.
- ➔ Security-budgets are limited – so the TRA can give guidance on which threats and which assets to focus in order to reduce the overall risks of a deployed PLMN most efficiently.
- The TRA gives also valuable guidance for research:
  - it served as foundation and guidedance for the work in ASMONIA
  - ➔ it is used also in 3GPP's security standardization work
  - ➔ it may be used to steer efforts in future research
- The complete results of the TRA are available on www.asmonia.de (http://www.asmonia.de/deliverables/D5.1_II_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf)
- Acknowledgements to the co-authors of the TRA document: André Egners, Enno Rey, Hendrik Schmidt, Sascha Wessel

Some Abbreviations

3GPP	3. Generation Partnership Project
AAA	Authentication, Authorization, Accounting
DNS	Domain Name Service
eNB	Evolved Node B
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
GRX	GPRS Roaming Exchange Network
GW	Gateway
HeNB	Home eNB
HSS	Home Subscriber Server
IMS	IP Multimedia System
IP	Internet Protocol
LTE	Long Term Evolution
L*n*	Communication Layer *n*
MME	Mobility Management Entity
MPLS	Multi Protocol Label Switching
MSC	Mobile Switching Center
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PLMN	Public Land Mobile Network
SAE	System Architecture Evolution
SEG	Security Gateway
SeG	Security Gateway
Serv.GW	Serving Gateway
SMSC	Short Message Service Center
TRA	Threat and Risk Analysis

