Consortium

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

ASMONIA

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

SPONSORED BY THE Federal Ministry of Education and Research

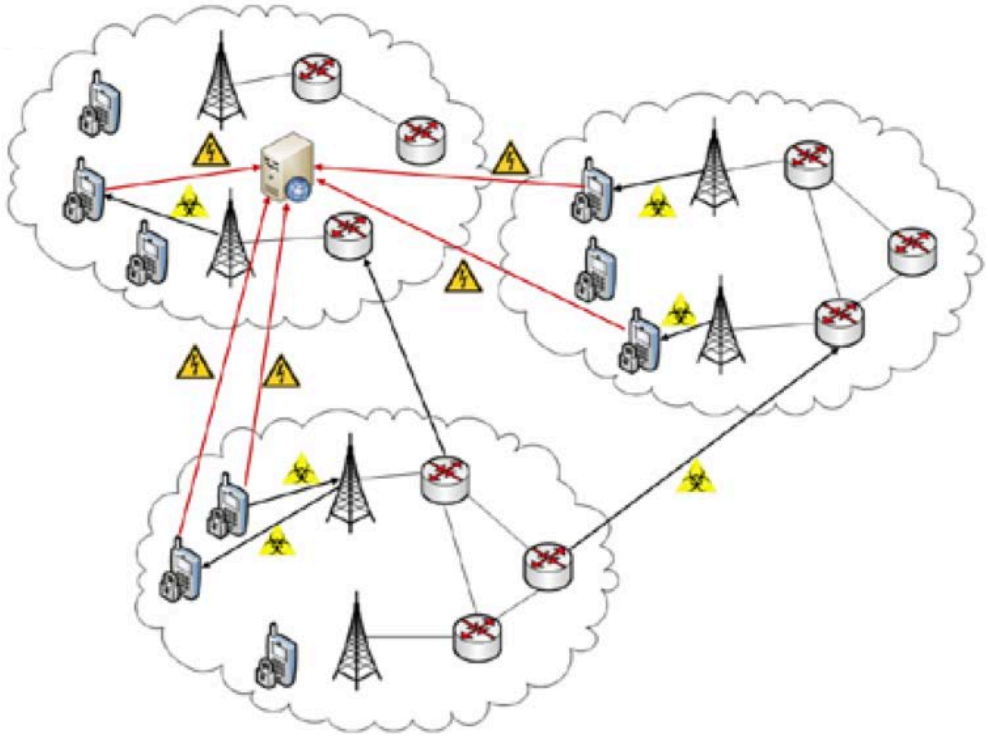
ASMONIA: Collaboration For The Exchange of Cyber Threat Information

Peter Schoo,
Fraunhofer AISEC

07.05.2013

New Threats

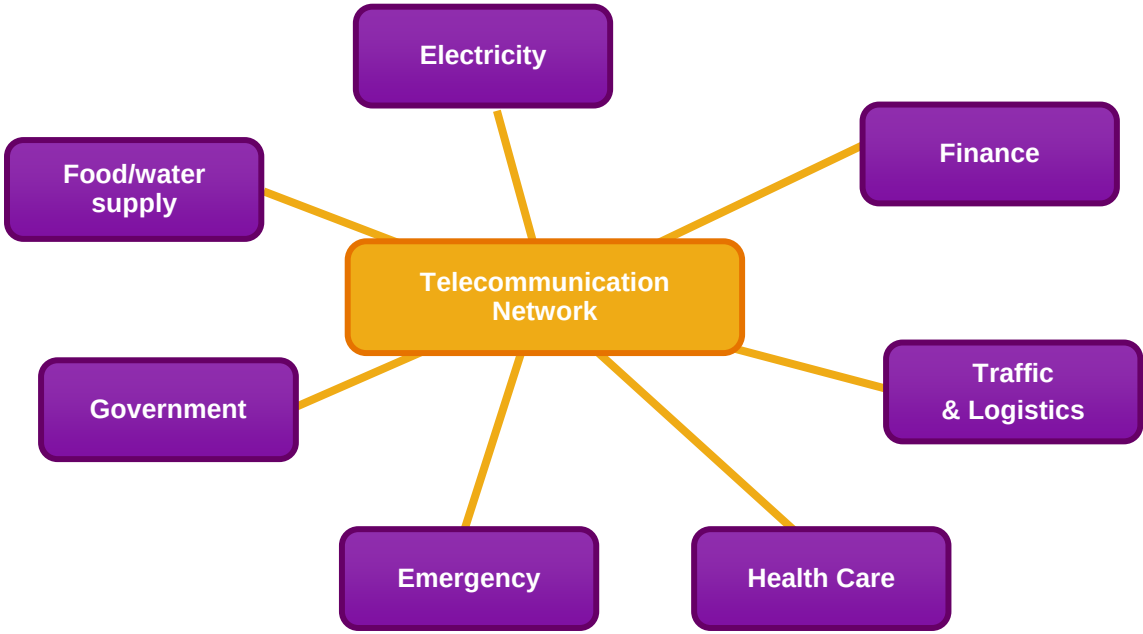
- Loss of NE Integrity
- UEs as launching pad
- Malware distribution
- Botnet installations



Project Strategic Objectives

Mobile Communication Systems are understood as part of the CII

- Improve protection
- Improve information sharing



Practice Today

So far information sharing is limited

- Project or incident based initiatives, e.g.
  - DNS Charger
  - German Anti-Botnet Initiative (ABBA)
- Group of trusted persons

- Information sharing as process or automated does not exist

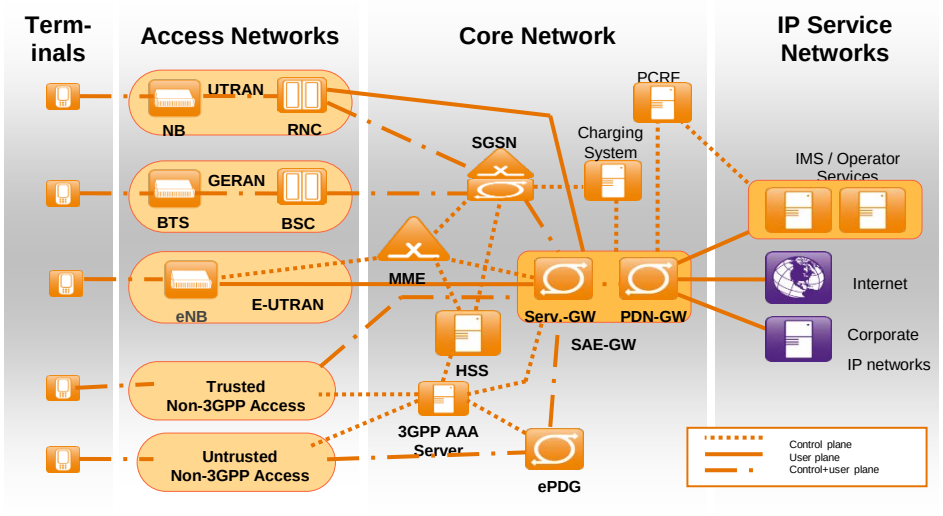
Information Sharing Obstacles

- Being attacked – feeling blamed
- No control on shared information
- Medium and long term consequences unclear
- Risk of reputation loss

You manage what you measure

Project Technical Objectives

- Understand demand and threat landscape
- Push base line to improve protection by collaboration
- Technologies applied:
  - SW Integrity Protection
  - Cloud Computing
  - UE protection
  - Malware Analysis
  - Pentesting
  - Information sharing
- Design innovative solutions
- Validate & simulate results



Results 1v3

Pentesting	■ Tools for fuzzying packet protocols, validating APN and GPRS tunnelling
SW Integrity Protection	■ Developed solution protecting SW of NE in Access Networks ■ Sensor base for shared information
UE Protection	■ HW anchored trust & visualization based solutions to improve UE protection ■ Three stakeholders – no problem holder

Results 2v3

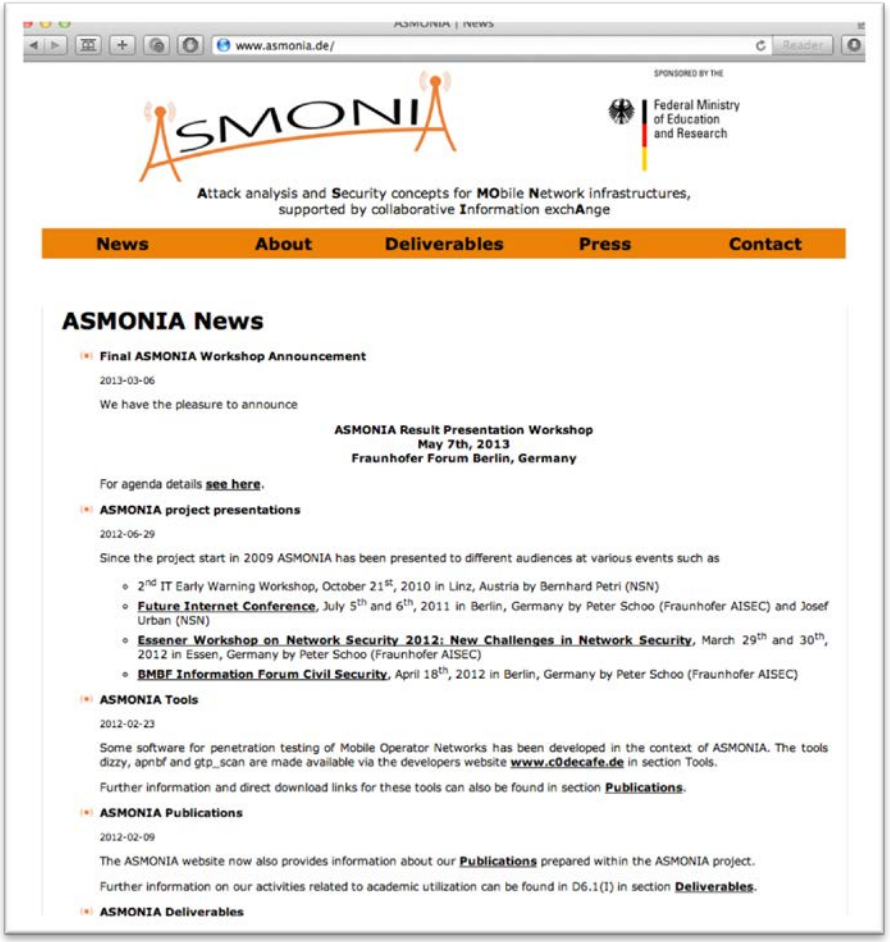
Cloud Computing	■ Use of elastic infrastructures allows improved resilience ■ More research on options and limiting factors beneficial
Malware Analysis	■ B2C: enables MNO differentiation ■ B2B: detection & reaction (promising) ■ Very relevant for vendors

Results 3v3

Continuous Risk Reduction	■ Approach starting on ROSI ■ Valid, alternative theory ■ Helpful input for further research
CREW	■ Reputation loss free information sharing solution ■ Next step: experimental deployment ■ Beyond MNO scenarios other Business Models to be developed

Summary

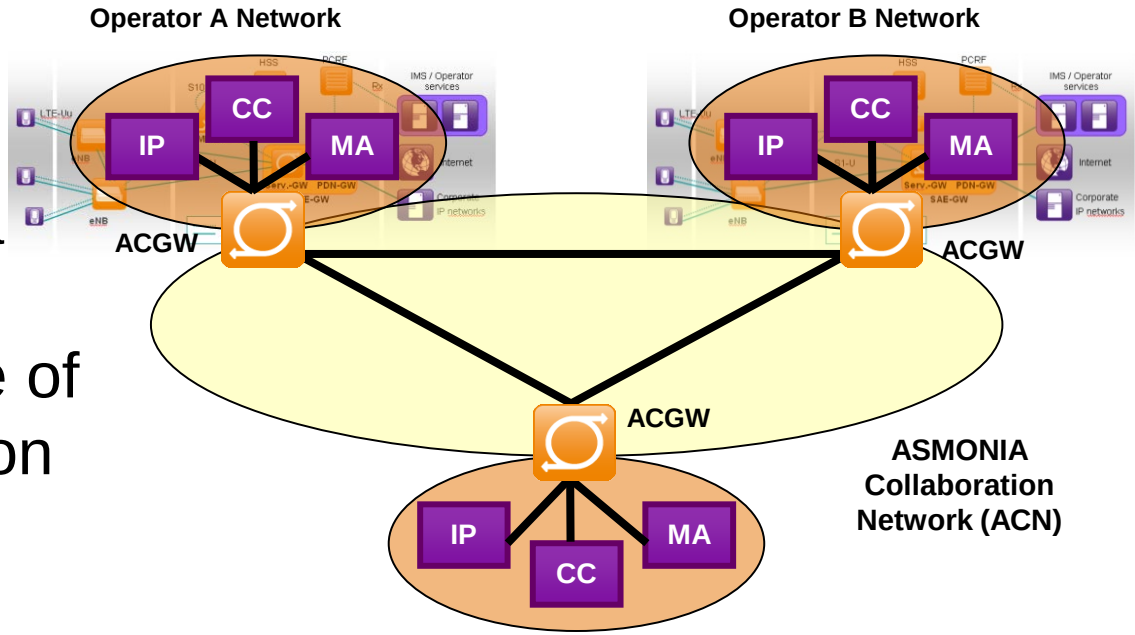
- Result documentation
  - Deliverables
    - All 12 are essentially available
    - Others follow May 2013
  - Paper
    - 11 scientific publications
  - Pentesting Tools
    - 3 available on project Website
  - Demos
    - See 8 of our 11 demos today



Conclusion

- ASMONIA identified and researched the opportunities and technical details concerning information and sensor technologies for sharing cyber threat information

- ASMONIA designed a technical solution that enables the exchange of cyber threat information



Some Abbreviations

3GPP	3. Generation Partnership Project
ACN	ASMONIA Collaboration Network
ACGW	ACN Gateway
APN	Access Point Name
B2B	Business to Business
B2C	Business to Customer
CC	Cloud Computing
CII	Critical Information Infrastructure
CREW	Collaborative Resilient Exchange of Warnings
DNS	Domain Name System
GPRS	General Packet Radio Service
GW	Gateway
HW	Hardware
IP	Integrity Protection
MA	Malware Analysis
MNO	Mobile Network Operator
NE	Network Element
ROSI	Return on Security Investments
UE	User Equipment