Consortium

CASSIDIAN AN EADS COMPANY | 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

Methods for Collaborative Detection and Analysis

Dennis Titze
Fraunhofer AISEC

07.05.2013

Outline

- Problem
- Solution
- Prototype
- Conclusion
- Future Work

Problem

How can a member of an Information Sharing Network (ISN) exchange messages with others,

without revealing the origin of the message?

- Member:
  - Mobile network operators
- Message:
  - Warning message containing a current incident

Problem cont‘d

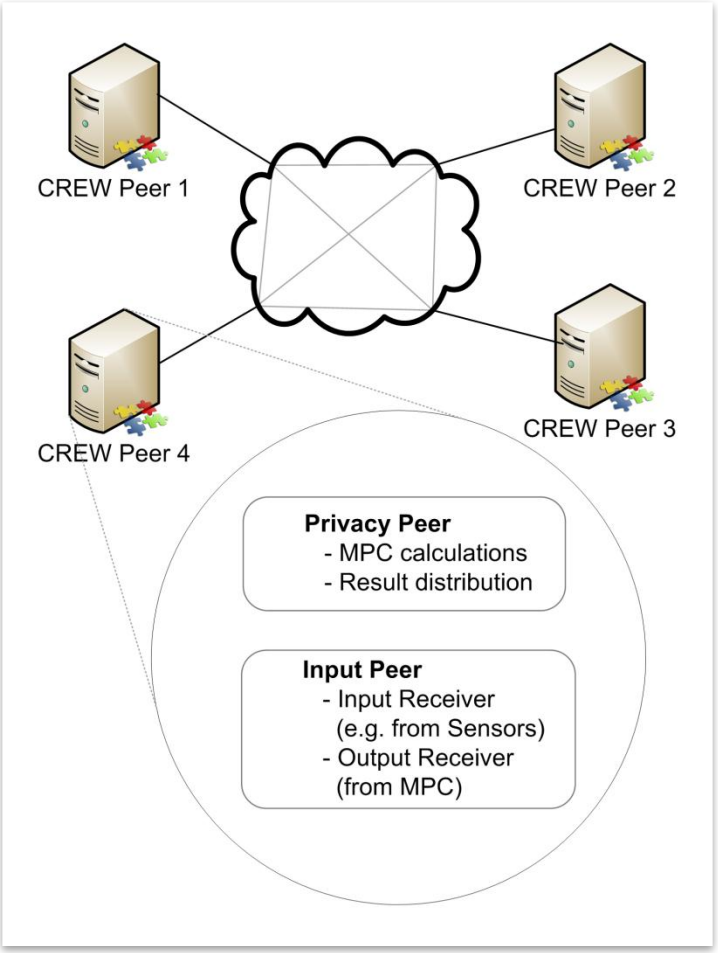
- Benefits:
  - Improving detection rate
  - Generation of overview of the global situation
  - Mitigating global threats

- Why do MNOs need a special system to share information?
  - Prevent reputation loss
  - Benefits from such a system

Solution

Collaborative **R**esilient **E**xchange of **W**arnings [4]

- Different system sizes possible for each party
  - E.g. 1 Privacy peer and 1 Input peer per MNO
- System internals:
  - MPC
  - P2P
  - Certificates (enabled for TACs)
- Disregarded technologies:
  - GNUNet Overlay network



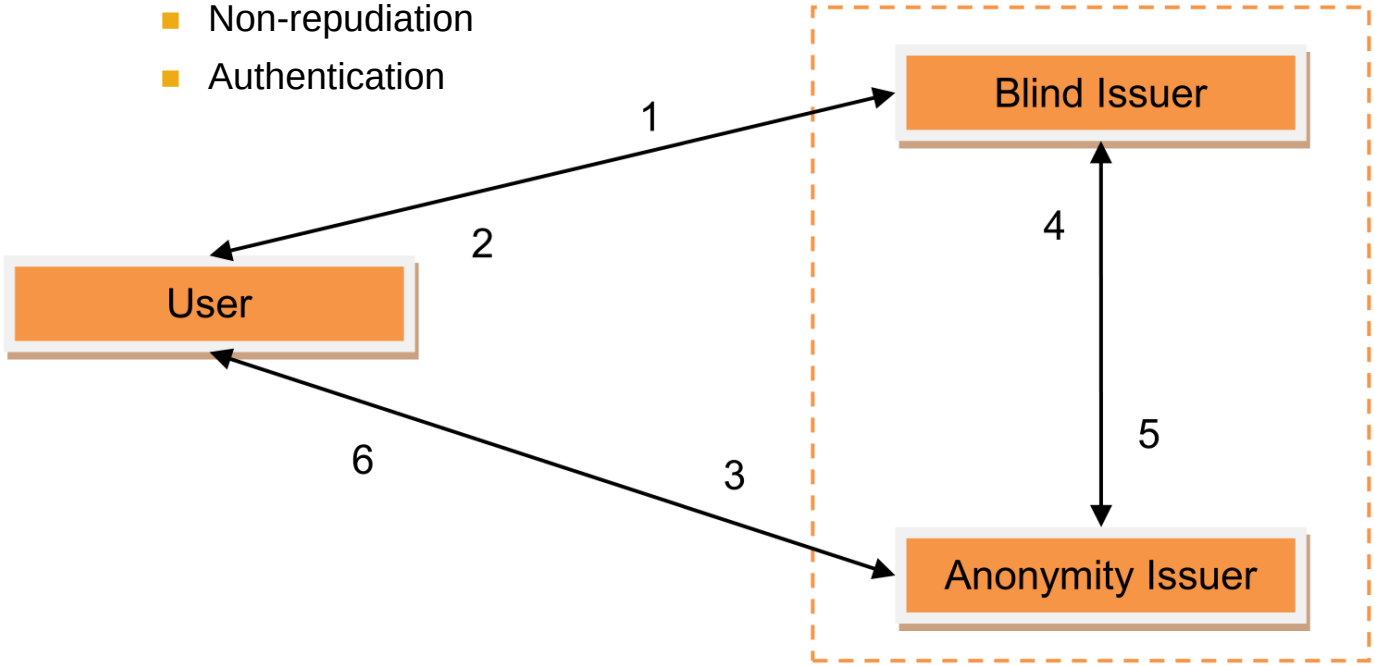
Solution: CREW

- CREW fulfills all requirements to the system
- Effort Estimation [3]
  - Organizational
  - Integration and Deployment
  - Operation, Administration and Management
- Self-Assessment of applied technology components
  - SEPIA and TAC (RFC5636) each not able to comply with the demanded objectives on their own
  - Combination satisfies the ASMONIA requirements

	CREW			
Component Requirement	TAC	P2P	MPC	Data Format
Anonymity	✓	✓		
Privacy			✓	
Non-repudiation	✓			
Interoperability				✓
Resilience		✓		
Authentication	✓			
Integrity	✓			
Confidentiality	✓			
Fairness		✓	✓	

Traceable Anonymous Certificates (TAC)

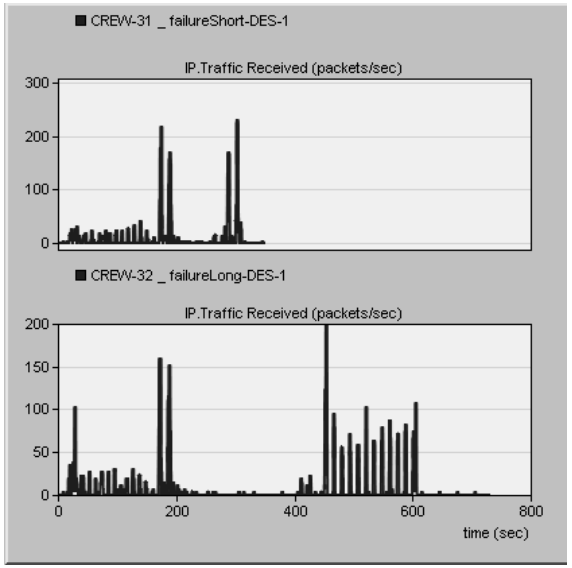
- Provide:
  - Message signing
  - Confidentiality
  - Non-repudiation
  - Authentication
- Without publication of ones identity



Prototype

- Evaluation:
  - Prototype can handle message collisions [1]
  - Prototype can handle attacks originating from the outside (e.g. DoS on one attached CREW peer) [2]

- Not considered in prototype:
  - No Service Discovery
  - No TACs
  - Only feasible for a limited number of peers/simultaneous messages

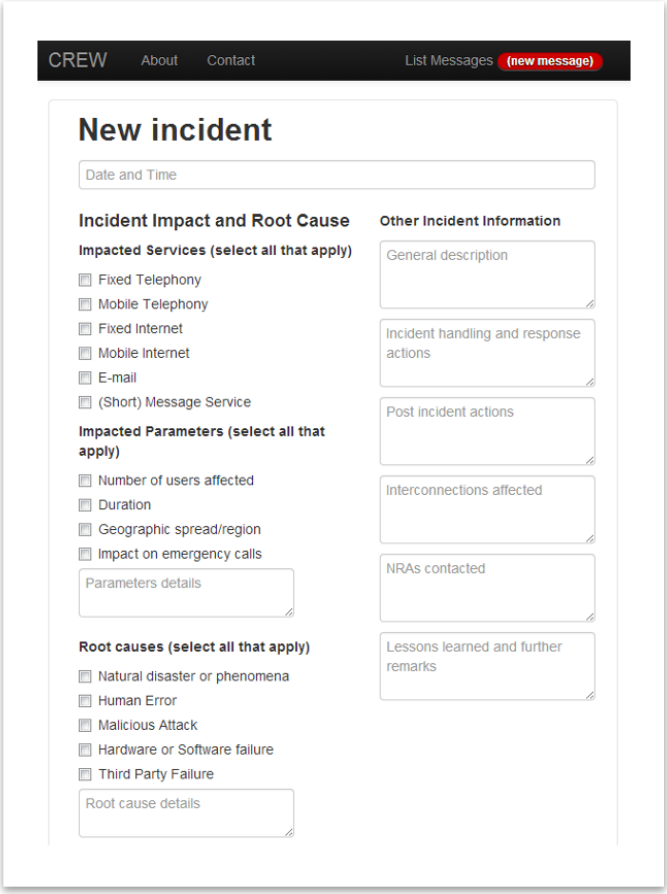


Transmitted traffic during node failure (60 and 180s)

Prototype cont'd

- Why no TACs?
  - Only organizational effort
  - Technological understanding already sufficient
  - Certificates are included in CREW. Efforts confined to creation of certs for every peer and including in the peer

- Capabilities
  - Distribution of arbitrary messages between n peers
  - Messages either automatically or manually created
  - Providing originator anonymity



Demonstrator will be shown after the talks

Conclusion

- Exchange messages with others, without revealing its origin possible

- Results:
  - Some of the functions required by ASMONIA must be completed and/or standardized before their introduction into the mobile network
  - No technology alone sufficient, but SEPIA + TAC satisfy requirements
  - Collaboration does not necessarily improve the detection rate
  - But can be crucial for
    - Generation of an overview of the global situation
    - Mitigating the threats

Questions?

References

[1] D. Titze, H. Hofinger, P. Schoo, Using Secure Multiparty Computation for Collaborative Information Exchange, accepted for publication at the 3rd IEEE International Symposium on Anonymity and Communication Systems, 2013

[2] M. Haustein, H. Sighart, D. Titze, P. Schoo, Collaboratively Exchanging Warning Messages Between Peers While Under Attack, submitted for publication, 2013

[3] ASMONIA, Deliverable D1.4, www.asmonia.de

[4] ASMONIA, Deliverable D4.3, www.asmonia.de