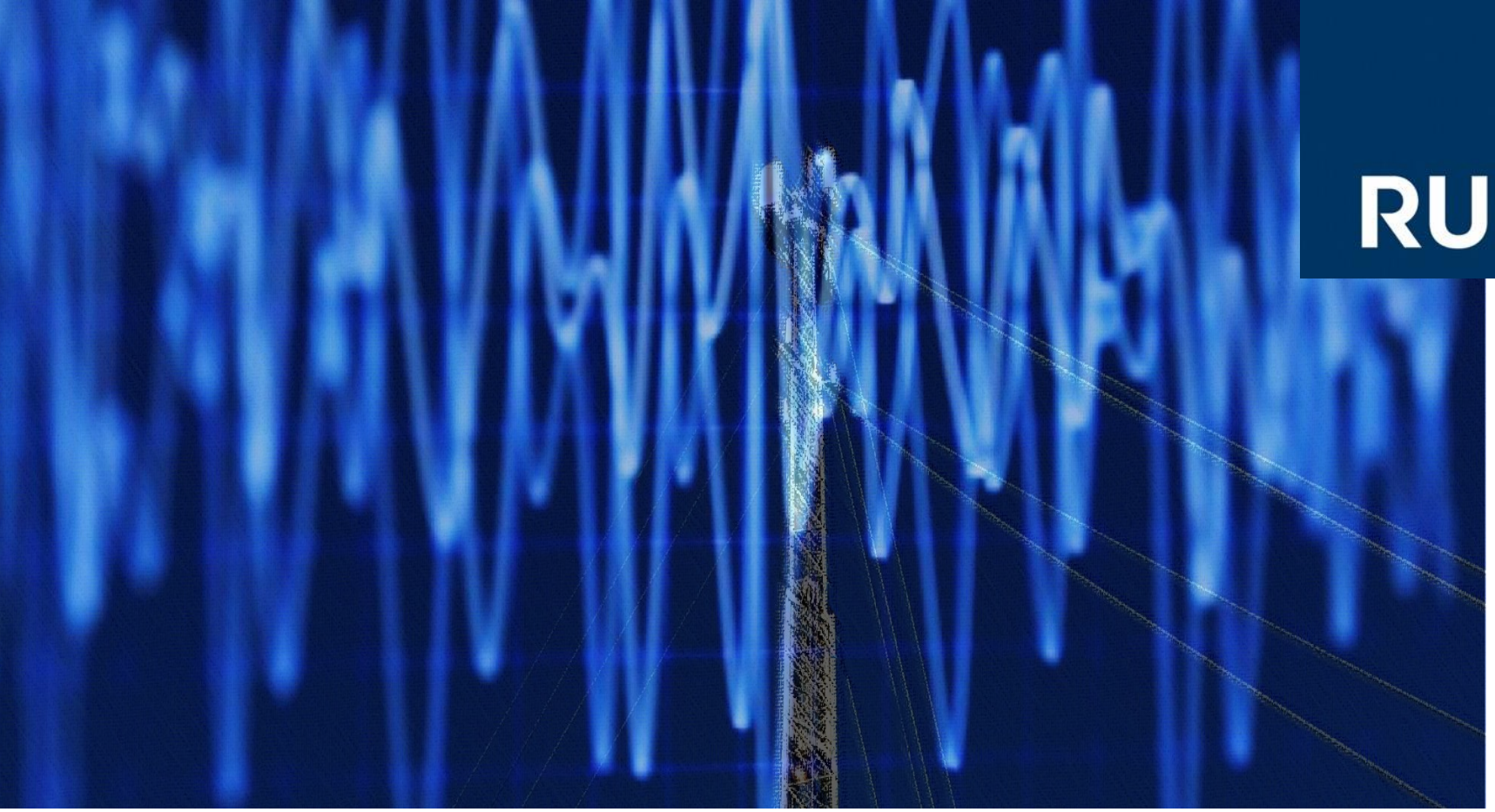


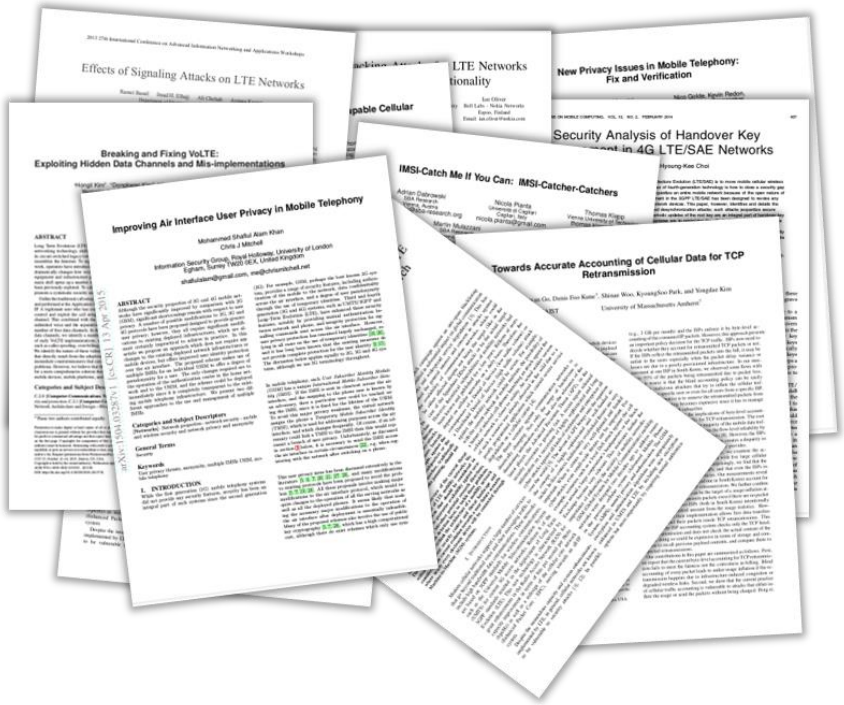
Learning from the Past: Systematization for Attacks and Countermeasures on Mobile Networks

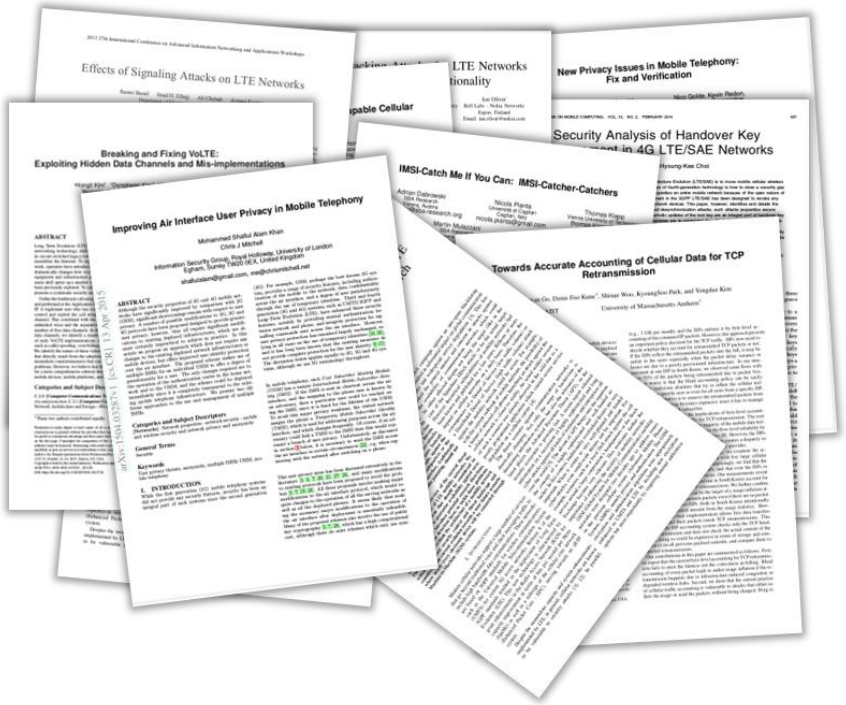
Workshop on 5G Security, 19 March, ITU HQ, Geneva

David Rupprecht

david.rupprecht@rub.de

What is the future of mobile network and 5G security **research**?


Effects of Signaling Attacks on LTE Networks
New Privacy Issues in Mobile Telephony: Fix and Verification
Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations
Security Analysis of Handover Key
IMSI-Catch Me If You Can: IMSI-Catcher-Catchers
Improving Air Interface User Privacy in Mobile Telephony
Towards Accurate Accounting of Cellular Data for TCP Retransmission



3GPP™

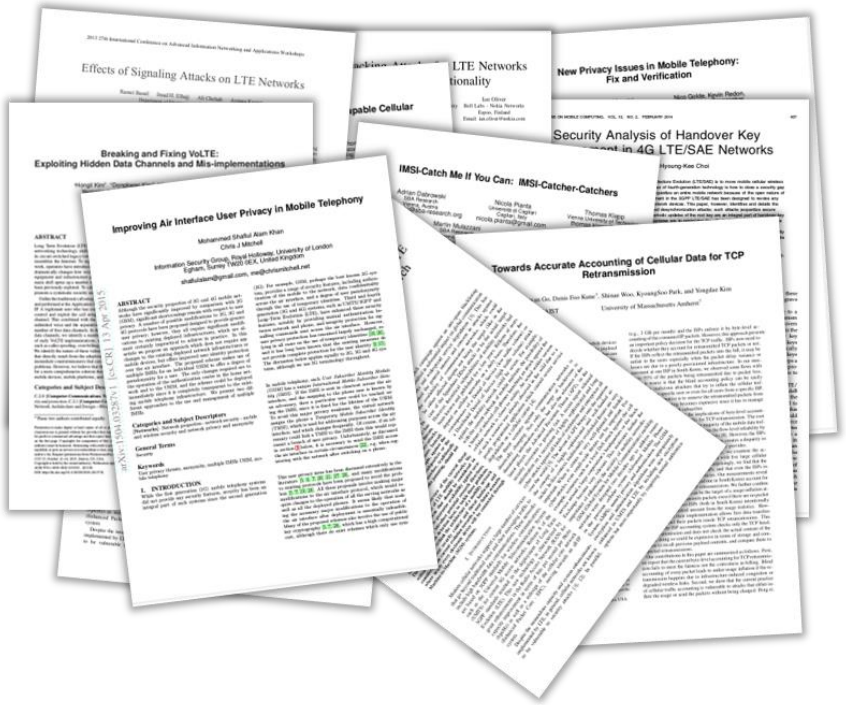
A GLOBAL INITIATIVE™

HUAWEI

GSMA

Nokia Siemens Networks

ETSI



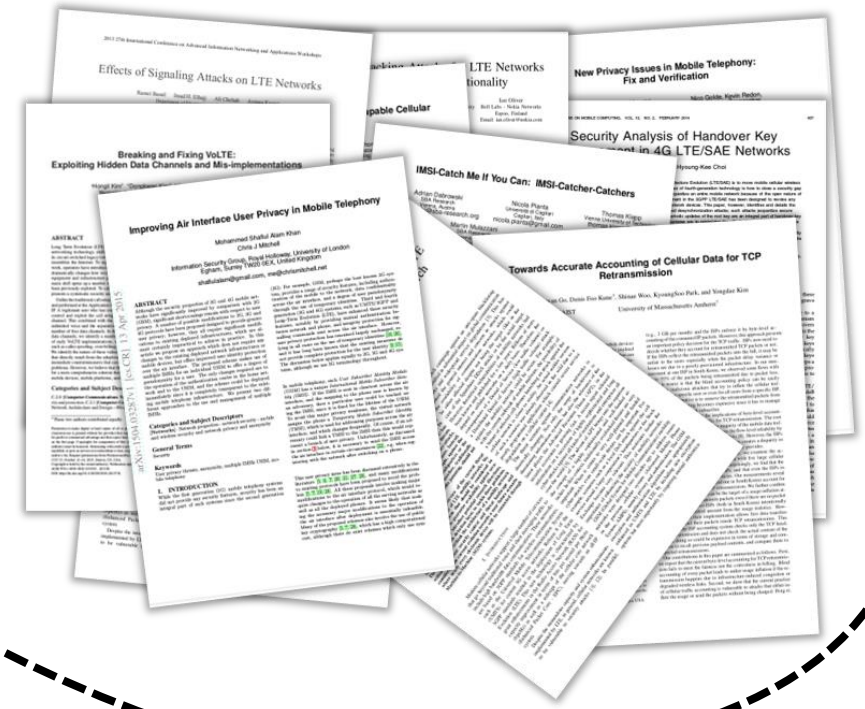
3GPP™ A GLOBAL INITIATIVE™ HUAWEI GSMA

Nokia Siemens Networks ETSI

black hat®

DEFCON

EICE a new dawn



3GPP™

A GLOBAL INITIATIVE™

HUAWEI

GSMA

Nokia Siemens Networks

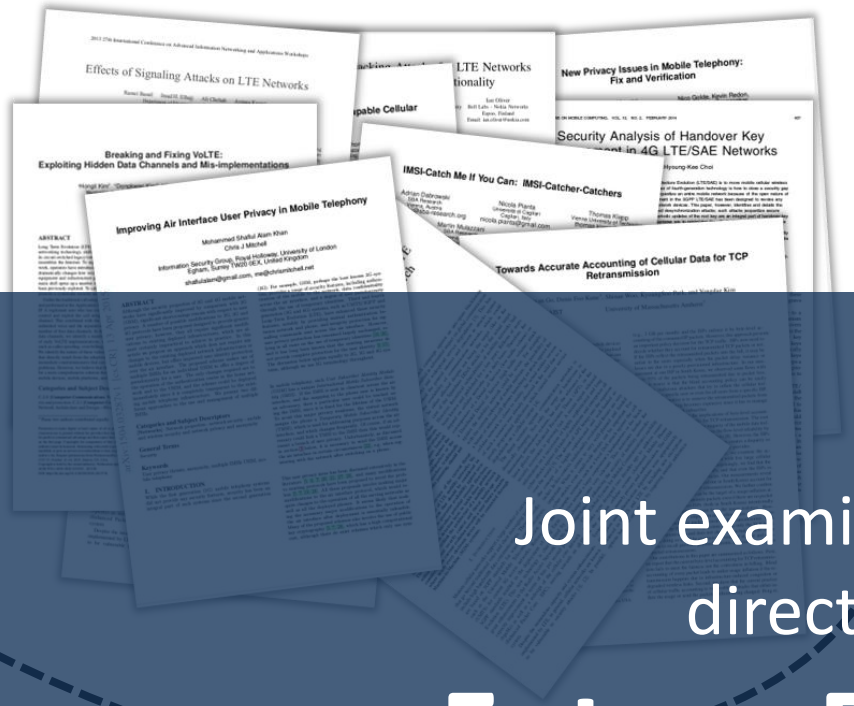
ETSI

black hat®

DEFCON

EICE

a new dawn



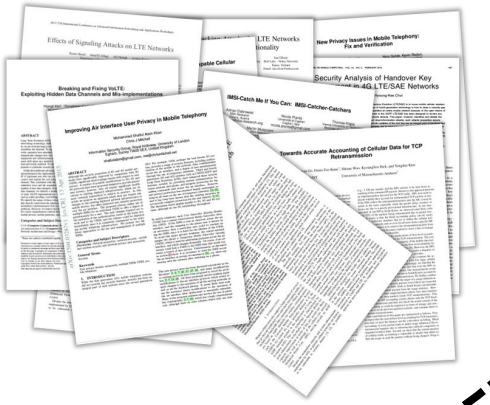
3GPP™ A GLOBAL INITIATIVE™ HUAWEI GSMA Nokia Siemens Networks ETSI

Joint examination carves directions for

Future Research!

black hat® DEFCON

ɘICɘ a new dawn



“On Security Research Towards Future Mobile Network Generations”

IEEE Communications Surveys and Tutorials 2018

Root Causes

Root Causes for Attacks

Specification Issue

Implementation Issue

Wireless Channel

Protocol Context Discrepancy

Root Causes for Attacks

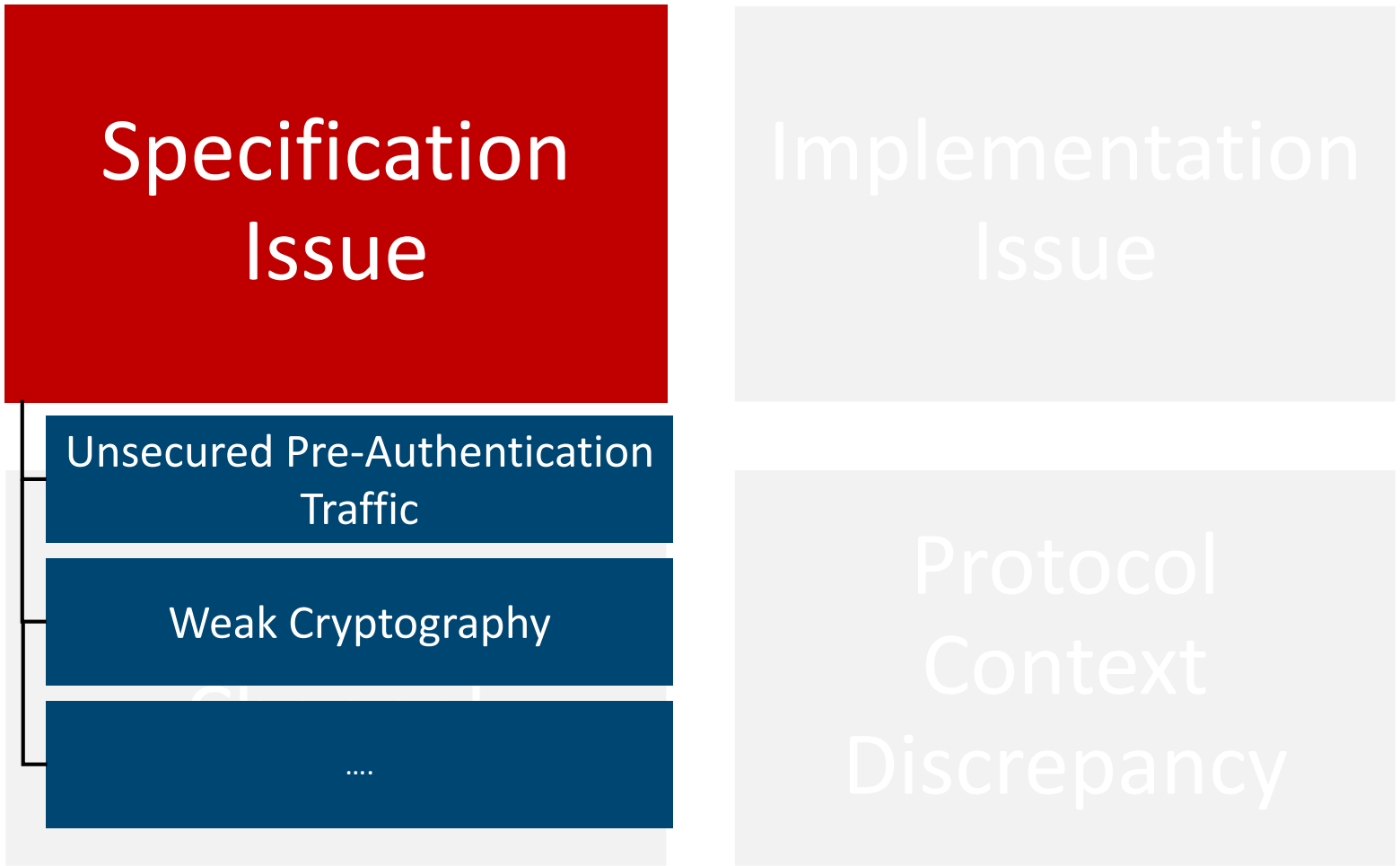
Specification Issue

Implementation Issue

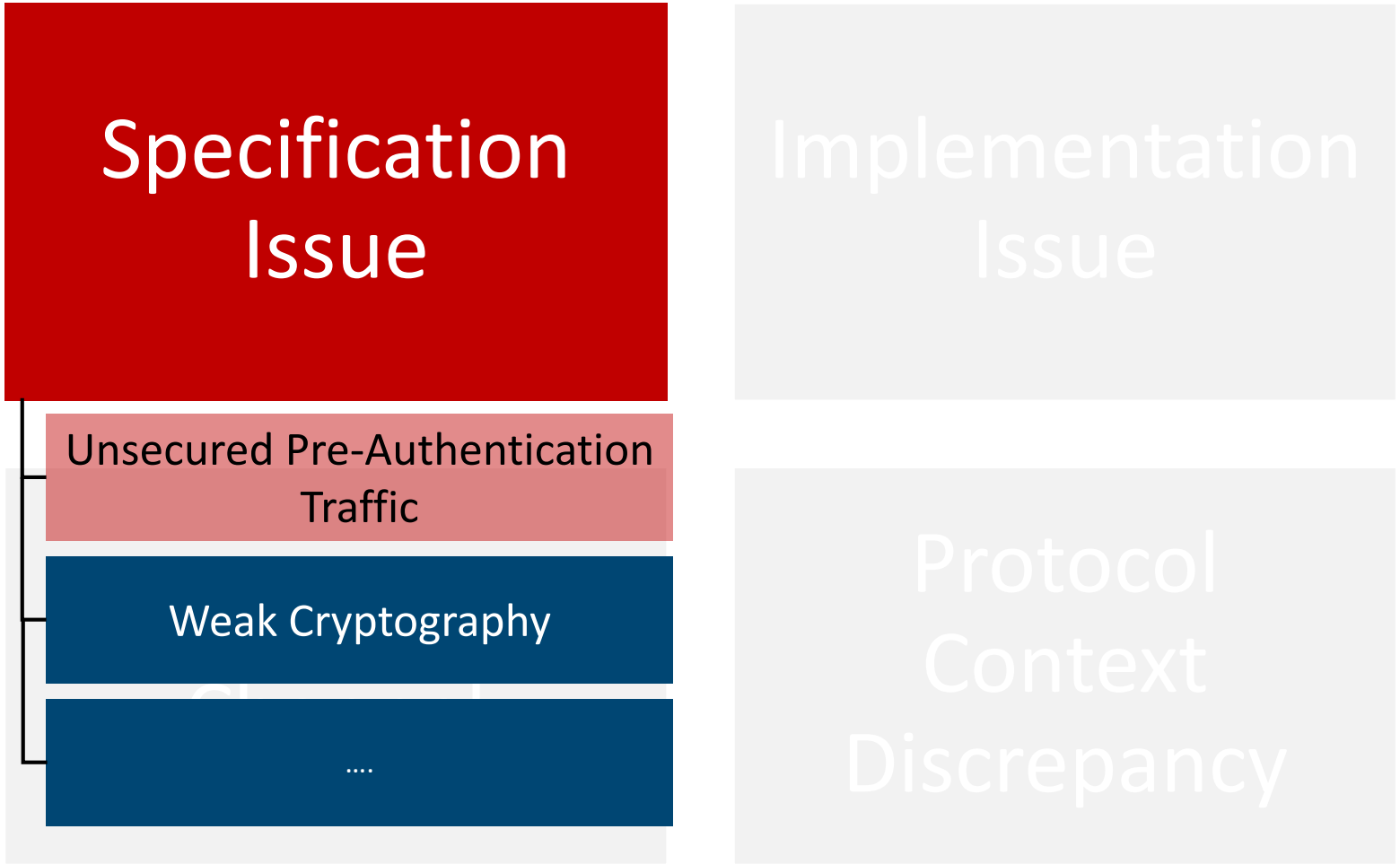
Wireless Channel

Protocol Context Discrepancy

Root Causes for Attacks

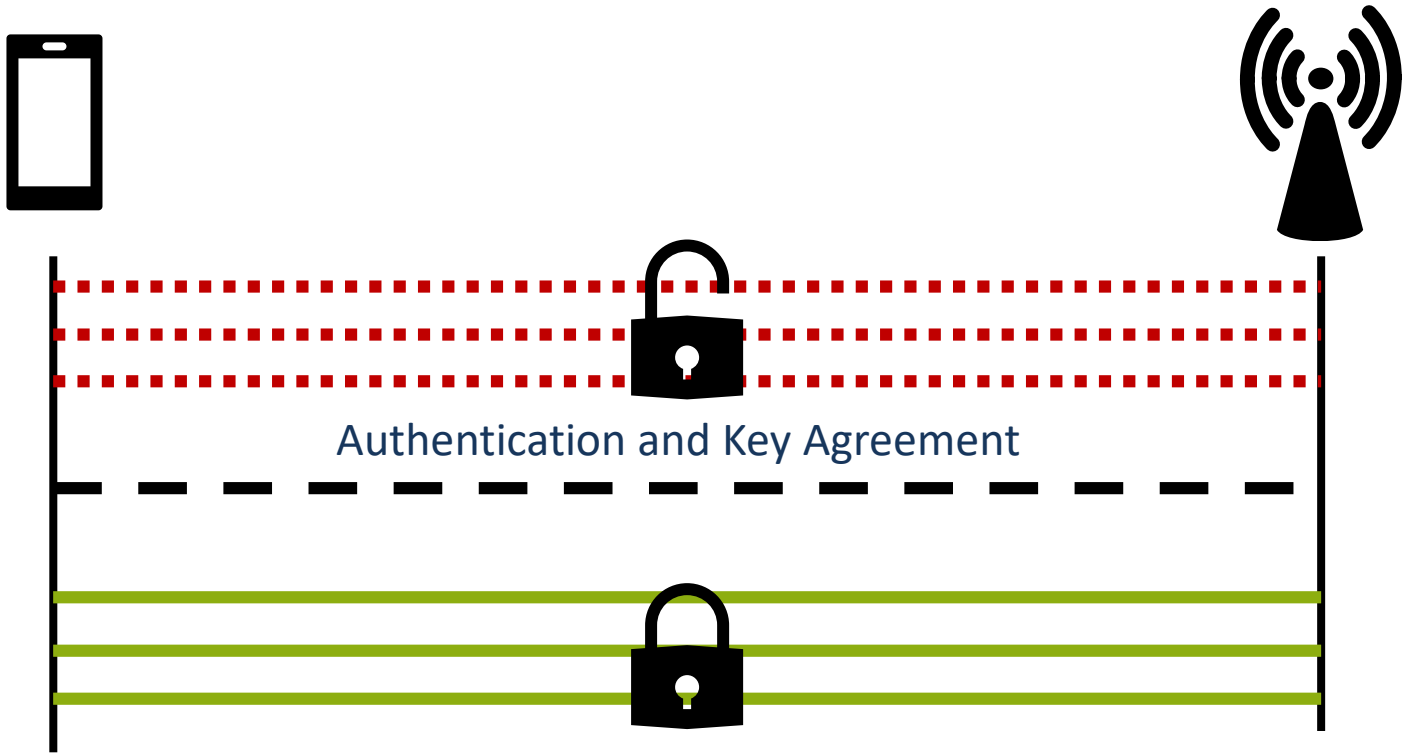


Root Causes for Attacks



Unsecured Pre-authentication Traffic

- The phone cannot verify the network **before** authentication and key agreement



Unsecured Pre-authentication Traffic

- Possible Attacks:
  - Downgrade Attacks
  - IMSI/TMSI Request Attack
  - Paging Attack
  - IMSI Paging Attack
  - Measurement Report Attack

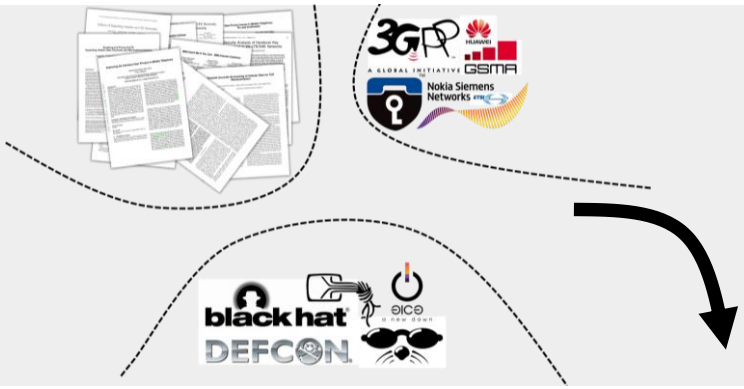
Unsecured Pre-authentication Traffic

- Possible Attacks:
  - Downgrade Attacks
  - IMSI/TMSI Request Attack
  - Paging Attack
  - IMSI Paging Attack
  - Measurement Report Attack

Loss of Privacy and Confidentiality

Take Home Messages

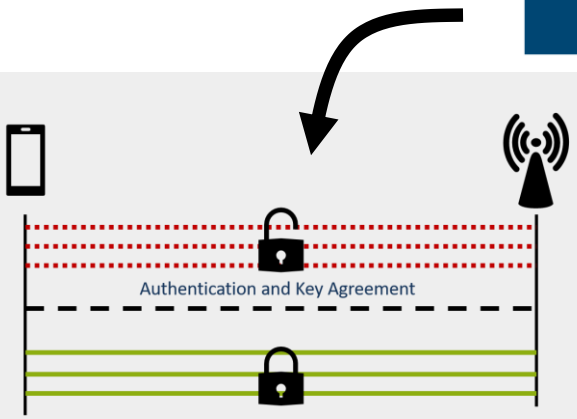
Different kind research areas in mobile network security



Specification Issues harm the security of a mobile generation

Specification Issue	Implementation Issue
Wireless Channel	Protocol Context Discrepancy

Attacks help to secure future generations



hgi Horst Görtz Institute for IT-Security

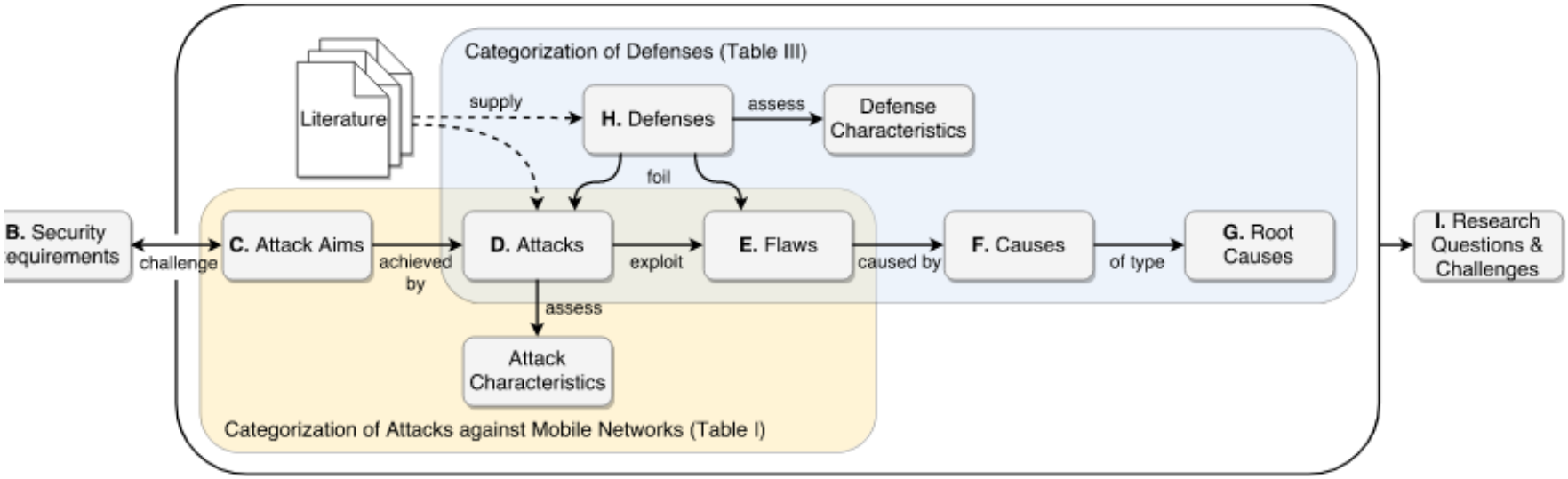
RUHR UNIVERSITÄT BOCHUM

RUB

Conclusion

On Security Research Towards Future Mobile Network Generations

David Rupprecht*, Adrian Dabrowski*, Thorsten Holz, Edgar Weippl, and Christina Pöpper



https://arxiv.org/abs/1710.08932