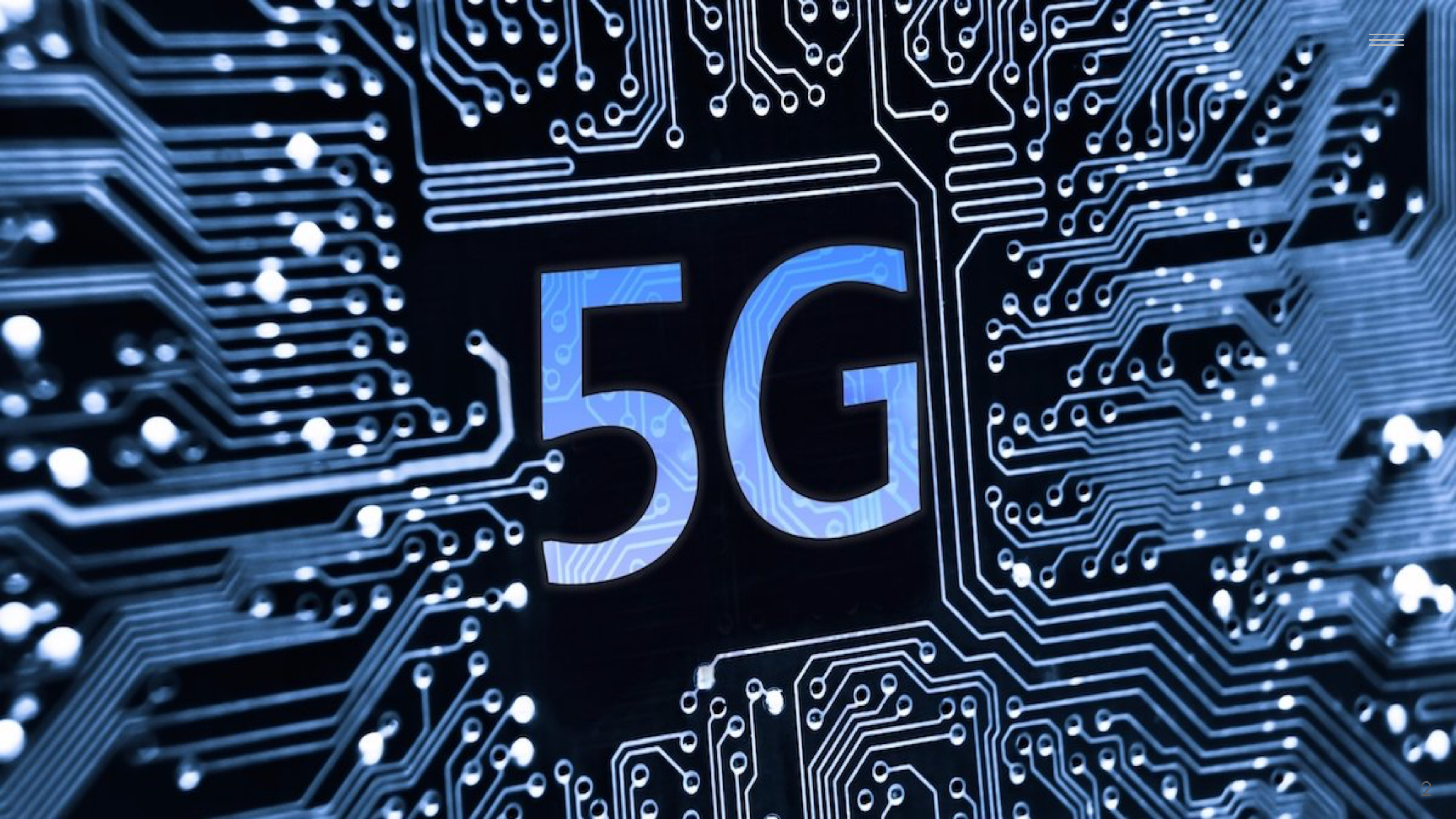
Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion

Martin Dehnel-Wild and Cas Cremers

UNIVERSITY OF OXFORD

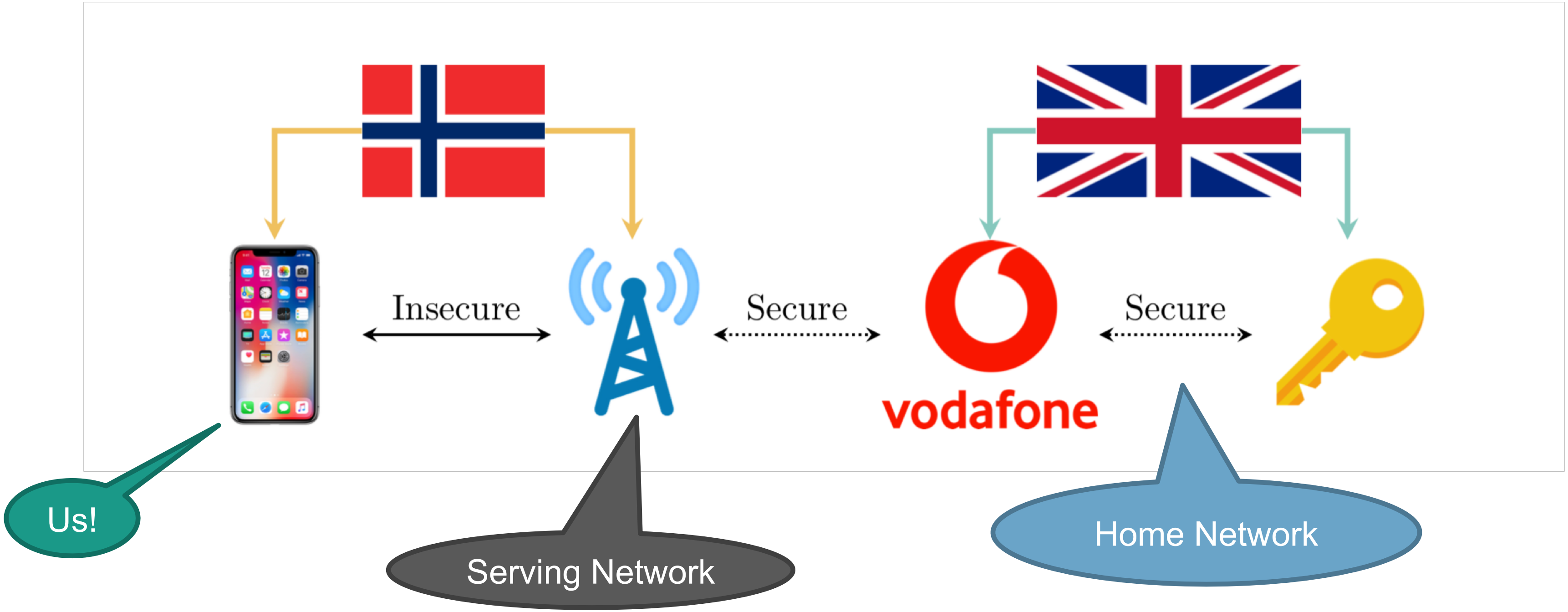
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY


5G

5G

- Fifth-Generation mobile phone standards: nearly finalised
- Advantages over 4G:
  - High Throughput: max 20 Gbit/s (1 Gbit/s on e.g. phones)
  - Low latency: target 1ms
  - High mobility: target 500km/h
  - High connection density: $10^6/km^2$
- (Slightly) Better security:
  - Stronger authentication between Phone, Home Network, and Serving Network
  - Privacy: Concealed SUCIs/IMSIs using ECIES

5G Network Setup



5G-AKA

5G-Authentication and Key Agreement: Aims

Protocol aims to provide:

- **Confidentiality** & **Integrity** for session key (and messages/data)

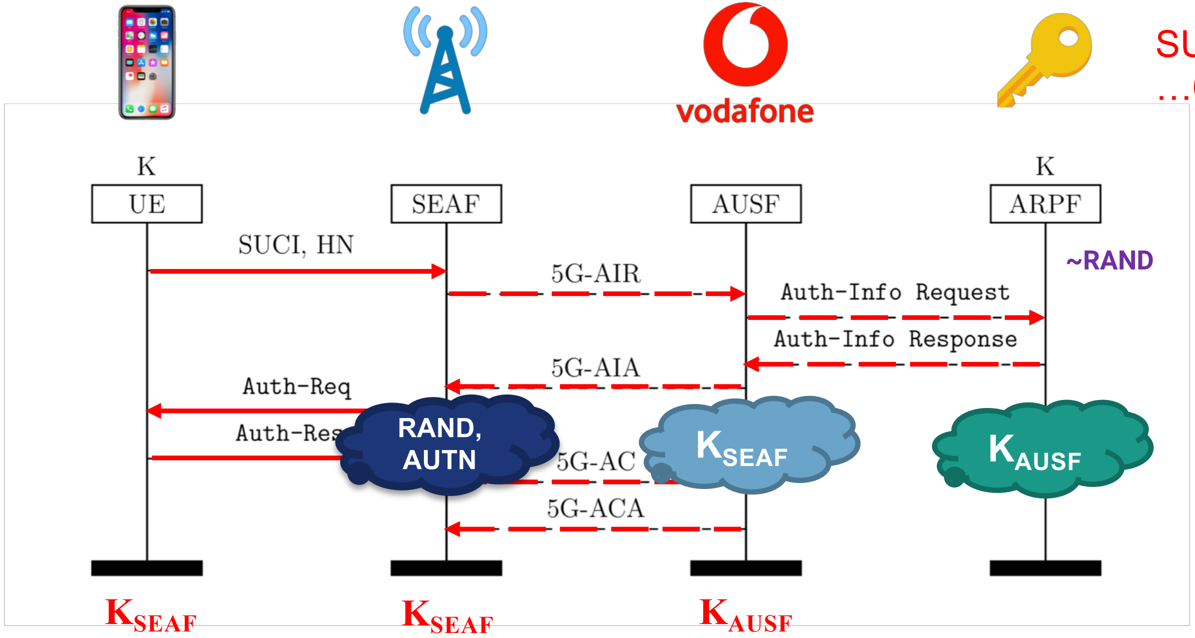
- **Authentication**: IDs and Session Key
  - Agreement on Session Key
  - Replay protection

Completely symmetric cryptography:
How hard can it be? :-)

Purpose: distribute and agree on a session key

5G-AKA Protocol

SUCI → SUPI
…699a3043 = “Alice”



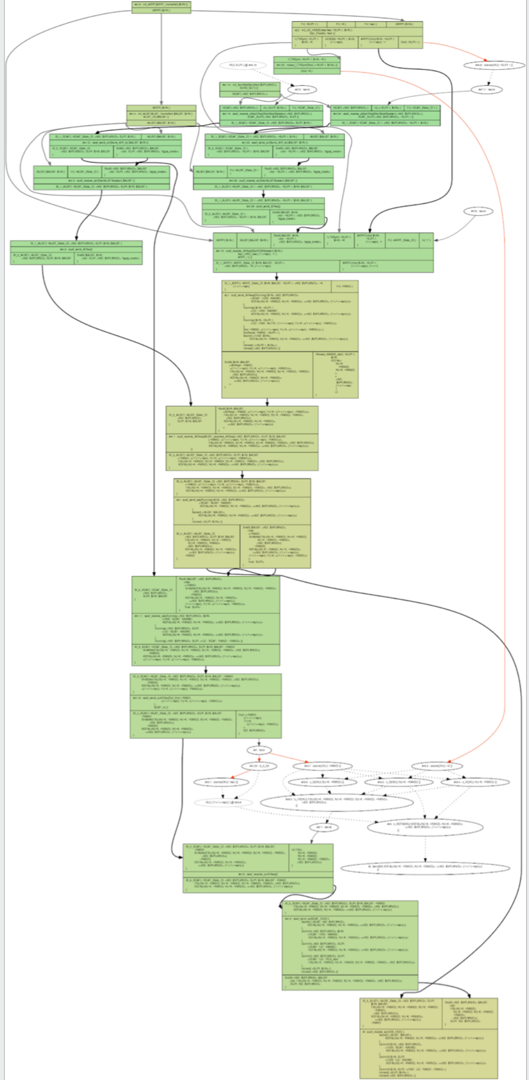
Analysis

- Know how 5G-AKA protocol operates
- Wide range of compromise models / attacker behaviours
- Know what security 5G-AKA *should* provide

Main question:

Under which threat models does 5G-AKA provide its security guarantees?

How do we answer this?



The Tamarin Prover

- Security protocol verification tool
- Symbolic: terms only
- Unbounded verification
- Protocol rules specified as multiset rewriting rules
- Ditto adversary capabilities
- Security properties specified as (temporal) first order logic statements

https://tamarin-prover.github.io

Our analysis vs. related work

- Basin et al.* focus on in-depth protocol properties:
  - Counter re-synchronisation, privacy guarantees from ECIES
  - Model **3** parties, like LTE-AKA (4G)
  - They discover other subtleties in 5G-AKA's design
- We originally considered compromise of individual components
  - Model **4** parties, as per 5G specification (TS 33.501)
  - "Home Network" split in two as per protocol specification
  - "What if we compromise some core network parties or channels?"
- Our main result holds in the specification's direct threat model

* Basin et al., *"A Formal Analysis of 5G Authentication"*, CCS'18

Selected results from Tamarin

Example: normal threat model:

Found a violation of some properties!

Main violated property:

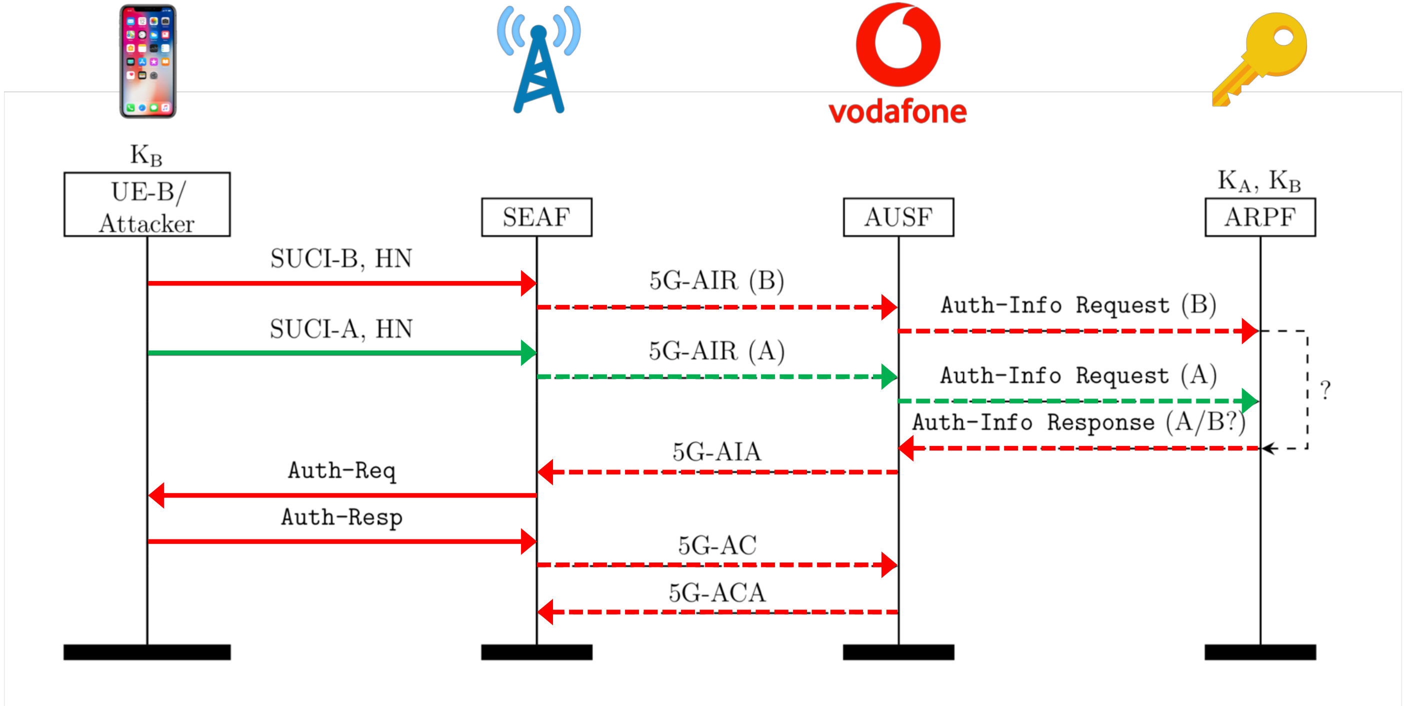
- **Secrecy of the session key, K_{SEAF}**
- ...from the point of view of the SEAF and AUSF
- Caused by insufficient authentication

So what?

- Adversary never learns a “legitimate” session key
- BUT: Adversary can trick serving network into believing their key is for someone else
- Adversary can now impersonate an honest party to serving network

A = honest, targeted identity
B = attacker owned identity

How does it work?



Implications

If allowed in reality:

- Potential for impersonation
- Billing
- Making and receiving calls


However...

Very unlikely to happen in reality:

- Requires incorrect underlying message pairing
- Lack of session-binding could cause havoc
- But! Session-binding ***not required by the specification***

Session confusion attack: proposed solution

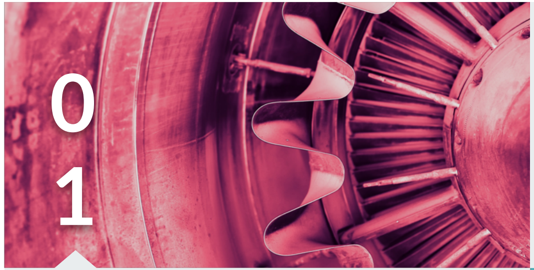
Standard must *explicitly* require correct matching of messages to responses between AUSF and ARPF.

How do we achieve session binding?

- **Include a nonce** in “Auth-Info Request” from AUSF and add same nonce in to “Auth-Info Response” from ARPF

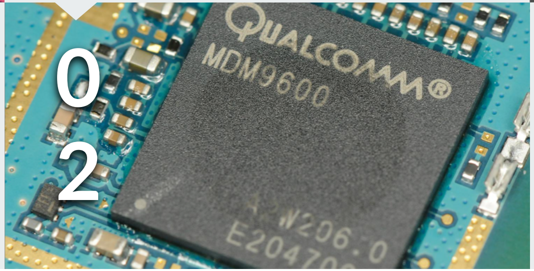
- Similar nonce and check required over SEAF ↔ AUSF interface (5G-AIR and 5G-AIA messages)

Disclosure and response



Contacted 3GPP Security Committee (SA3)

Responsible disclosure



Liaison from SA3 to 3GPP CT4: “Core Network and Terminals WG”

Security properties of any cryptographic protocol *must not depend on implicit engineering solutions.*

Martin Dehnel-Wild

@mpdehnel

cs.ox.ac.uk/5G-analysis/

- Discovered a vulnerability in 5G-AKA
- Found using the Tamarin Prover
- If unmitigated, could potentially allow identity mis-binding
- Worked with 3GPP to fix specification
- More compromise results in the paper
- Protocol security *must not depend on engineering solutions.*
- **Formal analysis continually improving!**

UNIVERSITY OF OXFORD