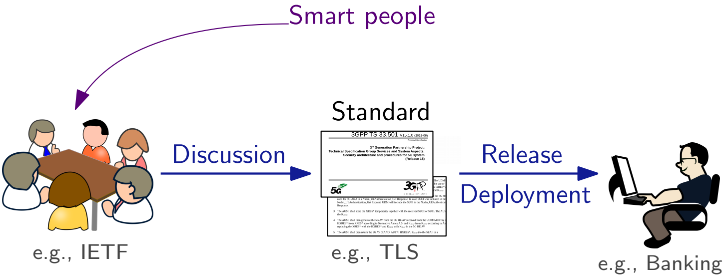
Security and Privacy of 5G vs. Formal Methods

SSL

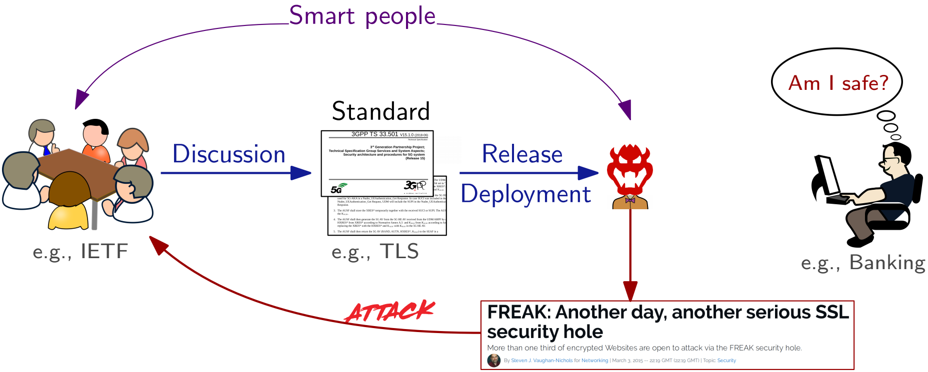
Lucca Hirschi

June 6, 2019

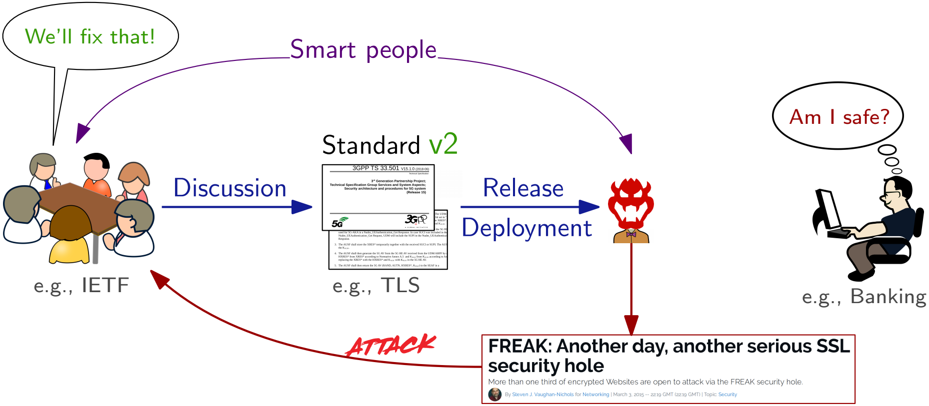
Designing Security Protocols



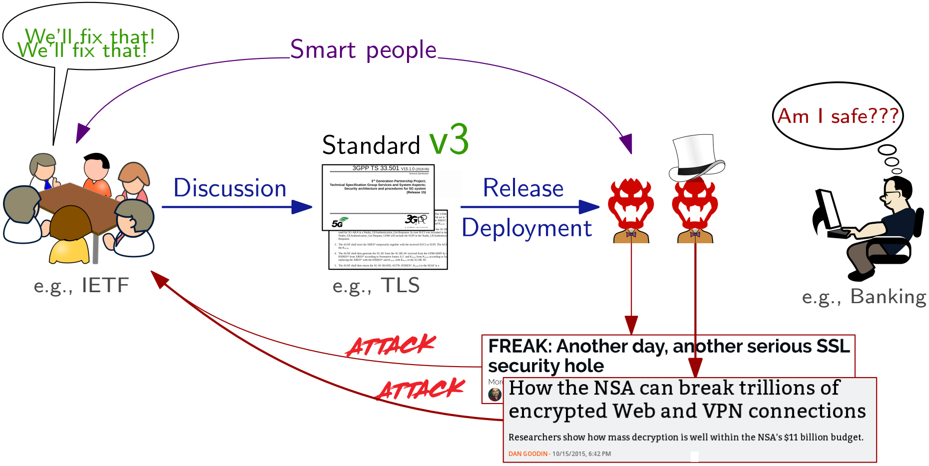
Designing Security Protocols



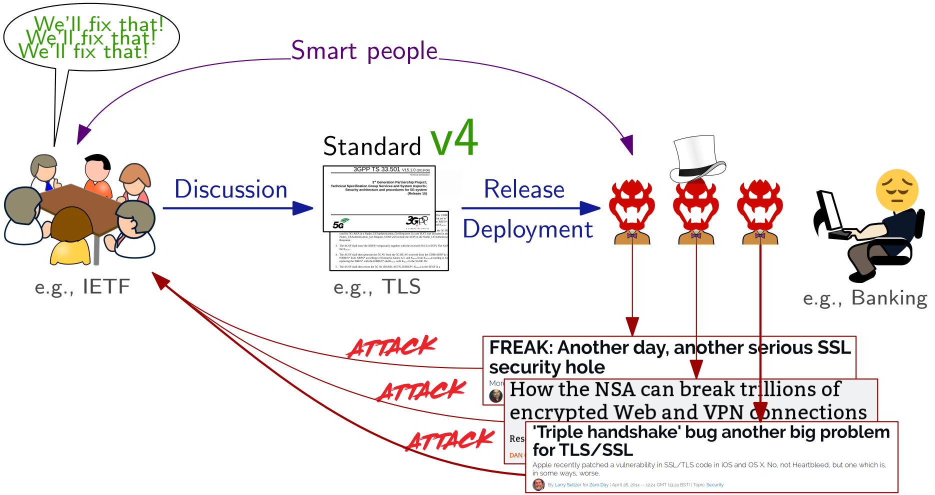
Designing Security Protocols



Designing Security Protocols



Designing Security Protocols

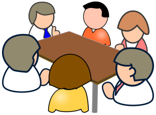


Designing Security Protocols

Both are smart people

But asymmetric fight:

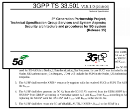
- weakest link
- active adversary exploiting insecure network
- concurrency + backward compatibility + ...



e.g., IETF

Discussion

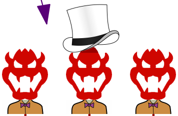
Standard v4



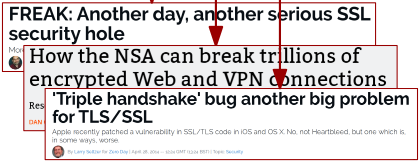
e.g., TLS

Release

Deployment



e.g., Banking


FREAK: Another day, another serious SSL security hole

How the NSA can break trillions of encrypted Web and VPN connections

'Triple handshake' bug another big problem for TLS/SSL

Apple recently patched a vulnerability in SSL/TLS code in iOS and OS X. No, not Heartbleed, but one which is, in some ways, worse.

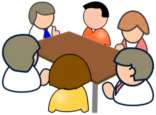
By Larry Seltzer for Zero Day | April 28, 2014 -- 12:24 GMT (13:24 BST) | Topic: Security

Designing Security Protocols

Both are smart people

But asymmetric fight:

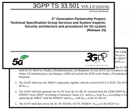
- weakest link
- active adversary exploiting insecure network
- concurrency + backward compatibility + ...



e.g., IETF

Discussion

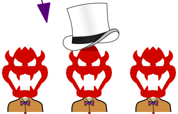
Standard v4



e.g., TLS

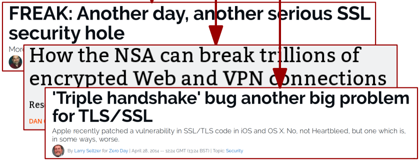
Release

Deployment



e.g., Banking

How can we help those guys?


FREAK: Another day, another serious SSL security hole

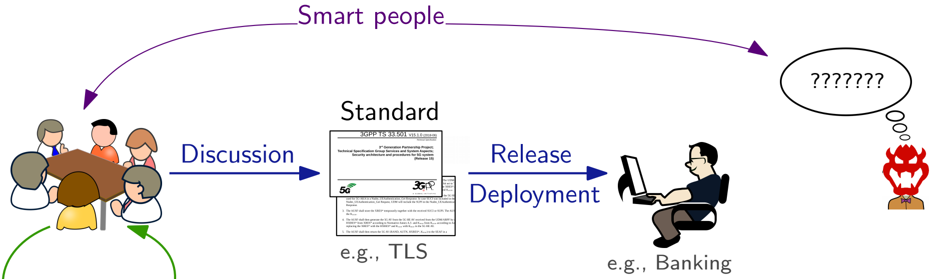
How the NSA can break trillions of encrypted Web and VPN connections

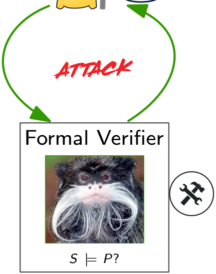
'Triple handshake' bug another big problem for TLS/SSL

Apple recently patched a vulnerability in SSL/TLS code in iOS and OS X. No, not Heartbleed, but one which is, in some ways, worse.

By Larry Seltzer for Zero Day | April 28, 2014 -- 12:24 GMT (13:24 BST) | Topic: Security

Designing Security Protocols





Formal methods come to the **rescue**!

- Find errors and attacks **early** and **quickly**
- Establish **formal security guarantees**
- One must be **explicit** about **system spec.**, **environment spec.** (threat model), and **security goals**

TLS 1.3 ISO/IEC 9798

5G Authentication

Mobile communication

- 4.8 billion unique users, 60% of world population has 4G
- next-gen 5G designed by 3GPP (as for 3G/4G); deployed in 2 phases
- Phase 1: frozen specification in 2018 and commercial service in 2020

Authentication

- Key protocol AKA: secure channel + authentication between  and 
- Different AKA protocols: 3G:AKA ⇝ 4G:EPS AKA ⇝ 5G:**5G AKA**

5G Promises

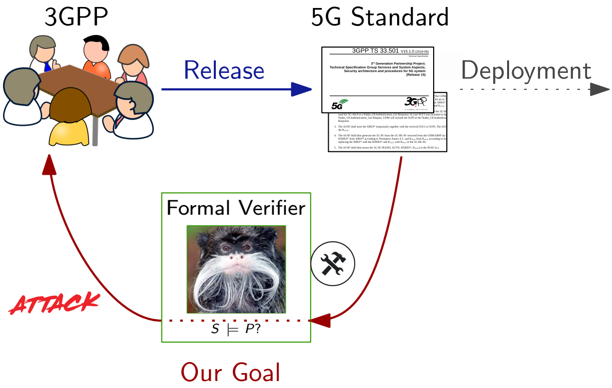
5G AKA intended to improve security and privacy but:
Which security guarantees? Under which threat model/security assumptions?

5G Promises

5G AKA intended to improve security and privacy but:

Which security guarantees? Under which threat model/security assumptions?

Let's try to formally analyze 5G AKA!



Outline

Outline

Introduction

I A Formal Analysis of 5G Authentication (CCS'18)

II New Privacy Vulnerability in 5G (+3G, 4G) (PETS'19)

III Privacy vs. Formal Methods ?

IV Conclusion

Outline

Paper

Session 7B: Formal + LangSec CCS'18, October 15-19, 2018, Toronto, ON, Canada

A Formal Analysis of 5G Authentication

David Basin
Department of Computer Science
ETH Zurich
Switzerland
basin@inf.ethz.ch

Jannik Dreier
Universite de Lorraine
CNRS, Inria, LORIA
Nancy, France
jannik.dreier@loria.fr

Lucca Hirschi
Department of Computer Science
ETH Zurich
Switzerland
lucca.hirschi@inf.ethz.ch

Saša Radomirović
School of Science and Engineering
University of Dundee
UK
s.radomirovic@dundee.ac.uk

Ralf Sasse
Department of Computer Science
ETH Zurich
Switzerland
ralf.sasse@inf.ethz.ch

Vincent Stettler
Department of Computer Science
ETH Zurich
Switzerland
svincent@student.ethz.ch

ABSTRACT

Mobile communication networks connect much of the world's population. The security of users' calls, SMSs, and mobile data depends on the guarantees provided by the Authenticated Key Exchange protocols used. For the next-generation network (5G), the 3GPP group has standardized the 5G AKA protocol for this purpose.

We provide the first comprehensive formal model of a protocol

1 INTRODUCTION

Two thirds of the world's population, roughly 5 billion people, are mobile subscribers [25]. They are connected to the mobile network via their USIM cards and are protected by security mechanisms standardized by the 3rd Generation Partnership Project (3GPP) group. Both subscribers and carriers expect security guarantees from the mechanisms used, such as the confidentiality of user data

in ACM Conference on Computer and Communications Security 2018

Formal Verification in the Symbolic Model

(also called Dolev-Yao model)

Cryptographic primitives assumed perfect

Security protocols encoded in a formal language (syntax + semantics)

Attacker = network (worst case scenario)

- eavesdrop: he learns all protocol outputs
- injections: he chooses all protocol inputs

Security properties encoded as reachability or equivalence properties

Sweet spot between precision and automation

Formal Verification in the Symbolic Model

(also called Dolev-Yao model)

Cryptographic primitives assumed perfect

Security protocols encoded in a formal language (syntax + semantics)

Attacker = network (worst case scenario)

- eavesdrop: he learns all protocol outputs
- injections: he chooses all protocol inputs

Security properties encoded as reachability or equivalence properties

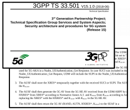
Sweet spot between precision and automation

Automated Verification (tool):

- several efficient procedures and tools (but verification is undecidable)
- our tool of choice: Tamarin (the only one with the required features)

Process

5G Standard



≈700 pages, 4 docs.

Formalization

Precise System Specification

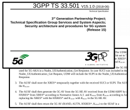
- architecture and process spec.
- system assumptions and threat model (environment)
- security goals

Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

Process

5G Standard


3GPP TS 33.501 V15.1.0 (2018-06)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 15)

≈700 pages, 4 docs.

Formalization →

Precise System Specification

- architecture and process spec.
- system assumptions and threat model (environment)
- security goals

Modeling →

System S

Property P

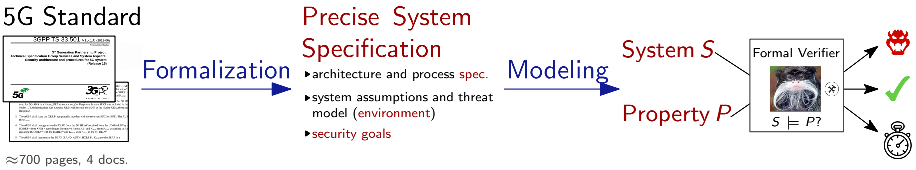
Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

Modeling

- large, complex protocol with intricate state-machine
- encode security goals under many threat models

Process



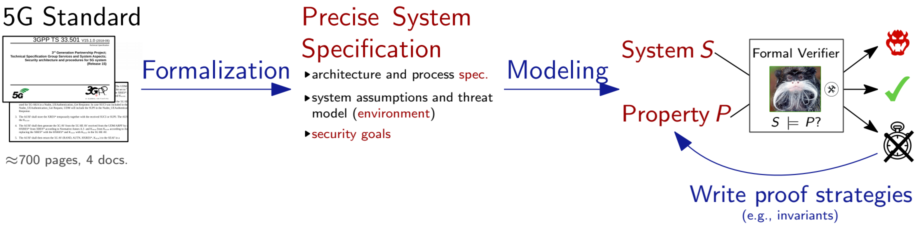
Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

Modeling

- large, complex protocol with intricate state-machine
- encode security goals under many threat models

Process



Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

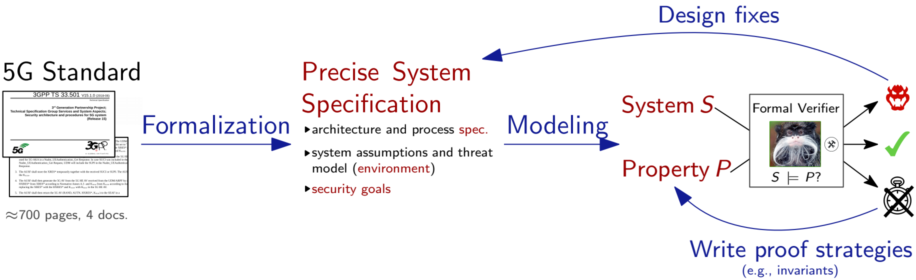
Modeling

- large, complex protocol with intricate state-machine
- encode security goals under many threat models

Proofs

- many features that make the verification ⏱
- need for proof strategies: sound by design, guide the proof search

Process



Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

Modeling

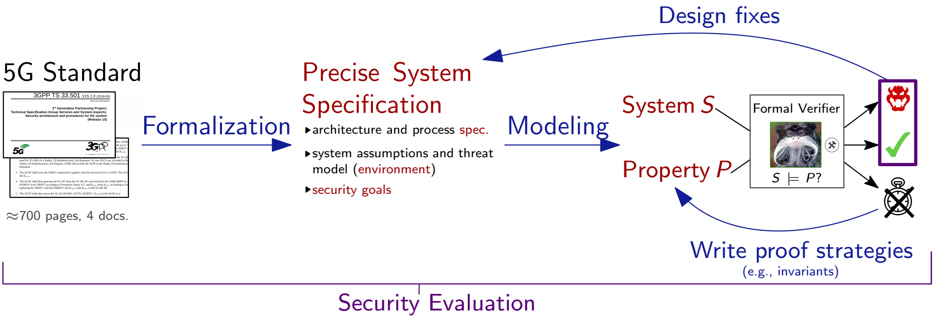
- large, complex protocol with intricate state-machine
- encode security goals under many threat models

Proofs

- many features that make the verification ⏱
- need for proof strategies: sound by design, guide the proof search

Design fixes that are provably secure

Process



Formalization

- implicit/unclear threat model and goals
- documents are often not self-contained

Modeling

- large, complex protocol with intricate state-machine
- encode security goals under many threat models

Proofs

- many features that make the verification ⏱
- need for proof strategies: sound by design, guide the proof search

Design fixes that are provably secure

Sec. Evaluation: attacks and fixes

Our Contributions (CCS'18)

Formalization of the 5G standard

- Identify key missing security goals + flaws in stated goals
- Propose fine-grained variants of goals (secrecy, authentication, privacy)
- Extract/Formally interpret security assumptions and system spec.

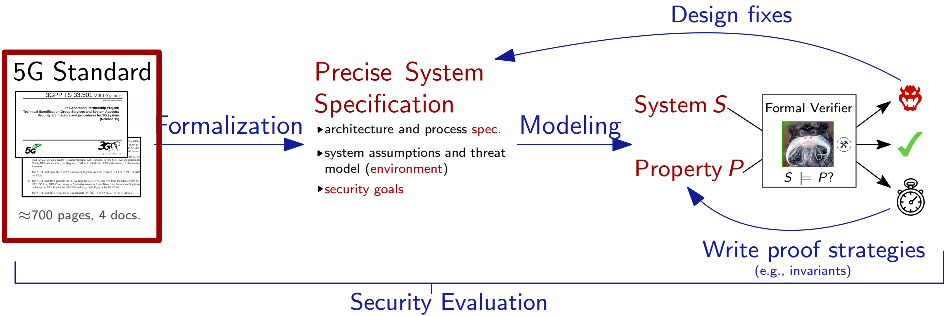
Formal model of 5G AKA amenable to automation

- First faithful model of an AKA protocol (challenges: loops, stateful, complex state-machine, scale, XOR)
- Dedicated proof strategies (in Tamarin)

Security Evaluation of 5G AKA

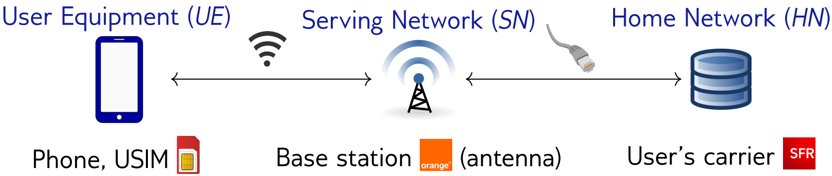
- Identify minimal assumptions required for each security goal to hold
- Highlights: critical authentication properties are violated
- Explicit recommendations and provably secure fixes (also simplify)

Process



Design fixes
5G Standard
3GPP TS 33.501 V15.1.0 (2018-06)
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
$S \models P$?
Write proof strategies
(e.g., invariants)
Security Evaluation

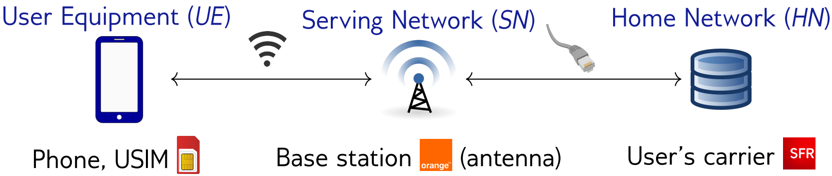
5G AKA



5G AKA designed to:

- **mutually authenticate** User Equipment with its Home Network
- **establish session keys** for User Equipment and Serving Network

5G AKA



5G AKA designed to:

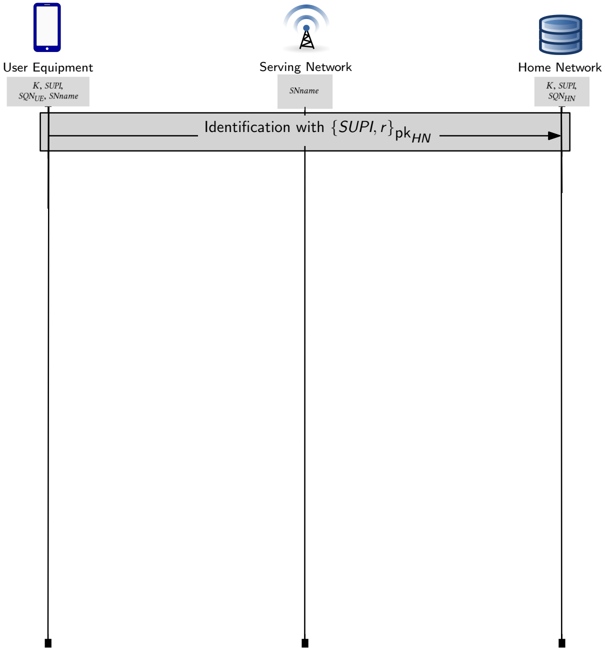
- **mutually authenticate** User Equipment with its Home Network
- **establish session keys** for User Equipment and Serving Network

User Equipment (Phone with USIM) and Home Network **share**:

- a permanent *UE*'s **identifier** *SUPI* (for identification)
- a **symmetric key** K (shared secret)
- a **sequence number** *SQN* (for replay protection for the UE)

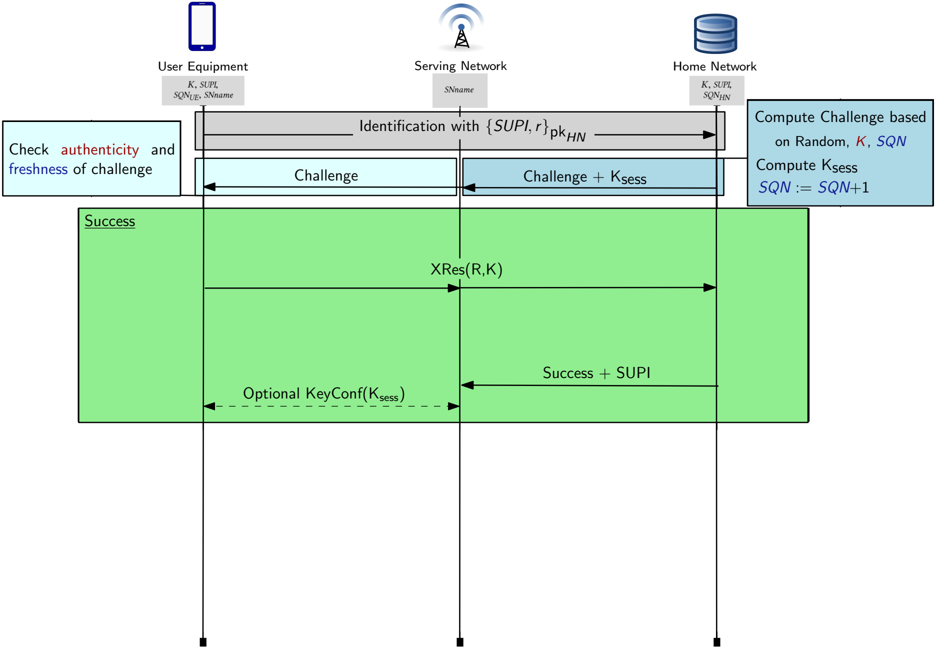
User Equipment knows the Home Network's **public key** pk_{HN}

5G AKA (cont.)



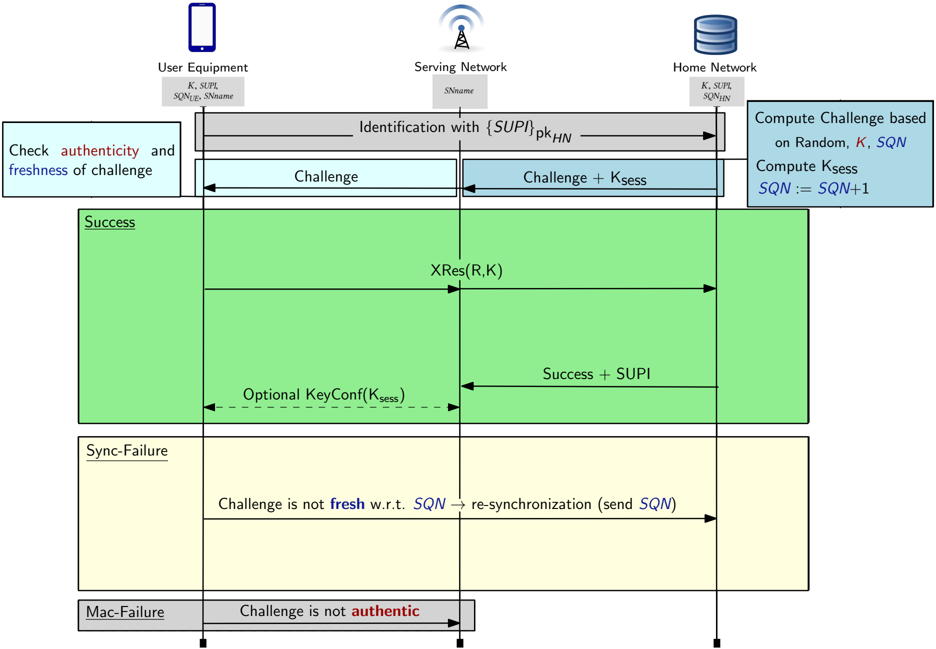
User Equipment
K, SUPI, SQN_{UE}, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_{HN}
Identification with $\{SUPI, r\}_{\mathrm{pk}_{HN}}$

5G AKA (cont.)



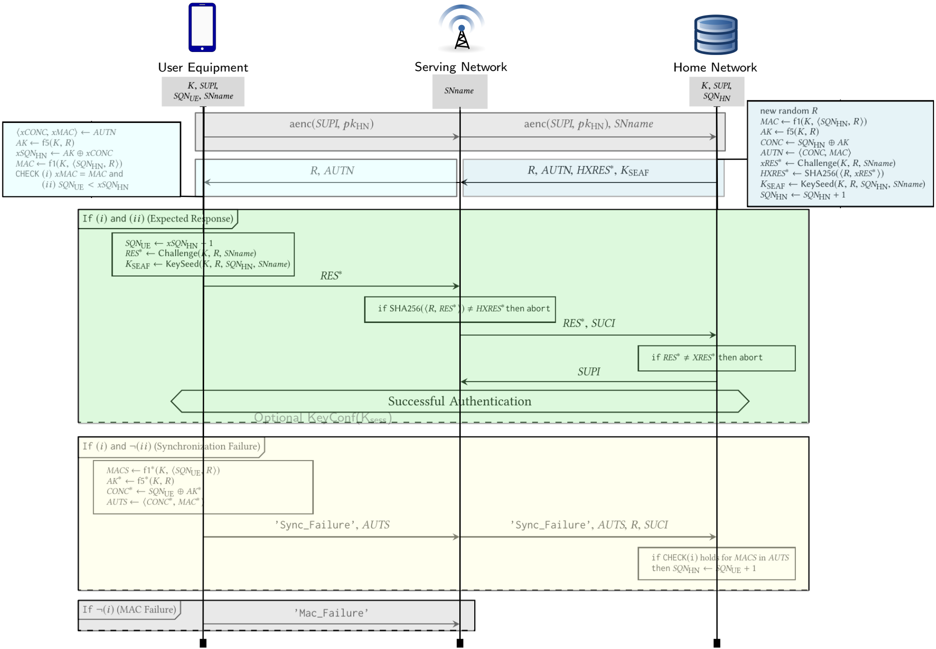
User Equipment
K, SUPI, SQN_UE, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_HN
Identification with {SUPI, r}pk_HN
Check authenticity and freshness of challenge
Challenge
Challenge + K_sess
Compute Challenge based on Random, K, SQN
Compute K_sess
SQN := SQN+1
Success
XRes(R,K)
Success + SUPI
Optional KeyConf(K_sess)

5G AKA (cont.)

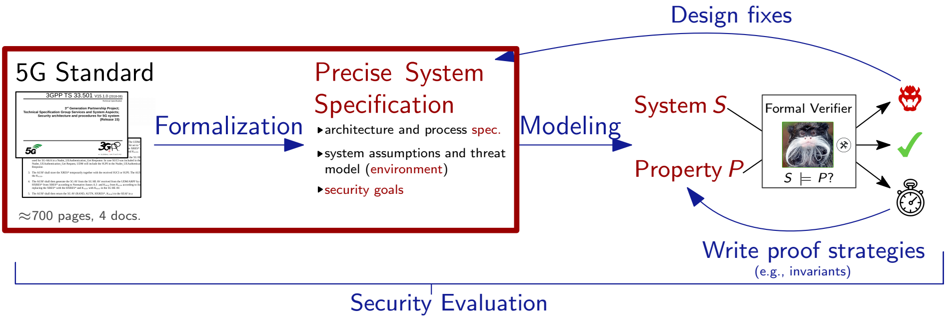


User Equipment
K, SUPI, SQN_UE, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_HN
Identification with {SUPI}pk_HN
Check authenticity and freshness of challenge
Challenge
Challenge + Ksess
Compute Challenge based on Random, K, SQN
Compute Ksess
SQN := SQN+1
Success
XRes(R,K)
Success + SUPI
Optional KeyConf(Ksess)
Sync-Failure
Challenge is not fresh w.r.t. SQN → re-synchronization (send SQN)
Mac-Failure
Challenge is not authentic

5G AKA (cont.)

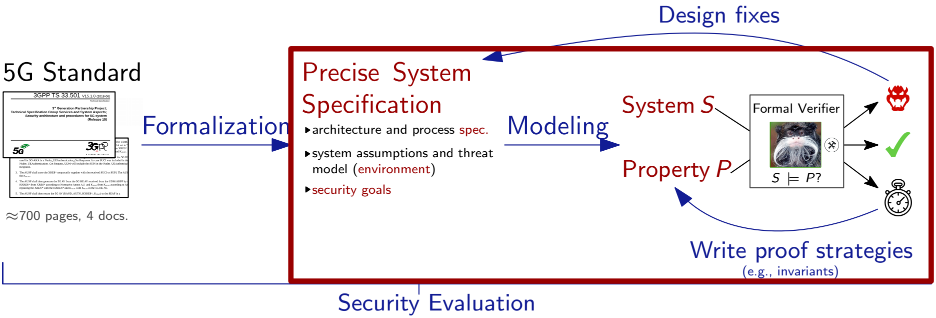

User Equipment
K, SUPI, SQN_UE, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_HN
new random R
MAC ← f1(K, ⟨SQN_HN, R⟩)
AK ← f5(K, R)
CONC ← SQN_HN ⊕ AK
AUTN ← ⟨CONC, MAC⟩
xRES* ← Challenge(K, R, SNname)
HXRES* ← SHA256(⟨R, xRES*⟩)
K_SEAF ← KeySeed(K, R, SQN_HN, SNname)
SQN_HN ← SQN_HN + 1
aenc(SUPI, pk_HN)
aenc(SUPI, pk_HN), SNname
⟨xCONC, xMAC⟩ ← AUTN
AK ← f5(K, R)
xSQN_HN ← AK ⊕ xCONC
MAC ← f1(K, ⟨SQN_HN, R⟩)
CHECK (i) xMAC = MAC and
(ii) SQN_UE < xSQN_HN
R, AUTN
R, AUTN, HXRES*, K_SEAF
If (i) and (ii) (Expected Response)
SQN_UE ← xSQN_HN + 1
RES* ← Challenge(K, R, SNname)
K_SEAF ← KeySeed(K, R, SQN_HN, SNname)
RES*
if SHA256(⟨R, RES*⟩) ≠ HXRES* then abort
RES*, SUCI
if RES* ≠ XRES* then abort
SUPI
Successful Authentication
Optional KeyConf(K_sess)
If (i) and ¬(ii) (Synchronization Failure)
MACS ← f1*(K, ⟨SQN_UE, R⟩)
AK* ← f5*(K, R)
CONC* ← SQN_UE ⊕ AK*
AUTS ← ⟨CONC*, MAC*⟩
'Sync_Failure', AUTS
'Sync_Failure', AUTS, R, SUCI
if CHECK(i) holds for MACS in AUTS
then SQN_HN ← SQN_UE + 1
If ¬(i) (MAC Failure)
'Mac_Failure'

Process



Design fixes
5G Standard
3GPP TS 33.501
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
S ⊨ P?
Write proof strategies
(e.g., invariants)
Security Evaluation

Process



5G Standard
3GPP TS 33.501 V15.1.0 (2018-06)
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
S ⊨ P?
Design fixes
Write proof strategies
(e.g., invariants)
Security Evaluation

Formal Modeling

System ~500LoC

- for unbounded number of *UEs, SNs,* and *HNs,* and unbounded sessions
- full state-maching with re-synchronization, precise modeling of XOR and counter SQN (only Tamarin can handle all that)
- + optional key-confirmation

Formal Modeling

System ~500LoC

- for unbounded number of *UEs*, *SNs*, and *HNs*, and unbounded sessions
- full state-maching with re-synchronization, precise modeling of XOR and counter SQN (only Tamarin can handle all that)
- + optional key-confirmation

Threat Model & Security Goals ~1000LoC, 124 lemmas

- wide-range of formal security goals (including secrecy, authentication, privacy)
- + many compromise scenarios in order to identify minimal assumptions

$\rightsquigarrow$ strongest possible adversary model

Formal Modeling

System ~500LoC

- for unbounded number of *UEs*, *SNs*, and *HNs*, and unbounded sessions
- full state-maching with re-synchronization, precise modeling of XOR and counter SQN (only Tamarin can handle all that)
- + optional key-confirmation

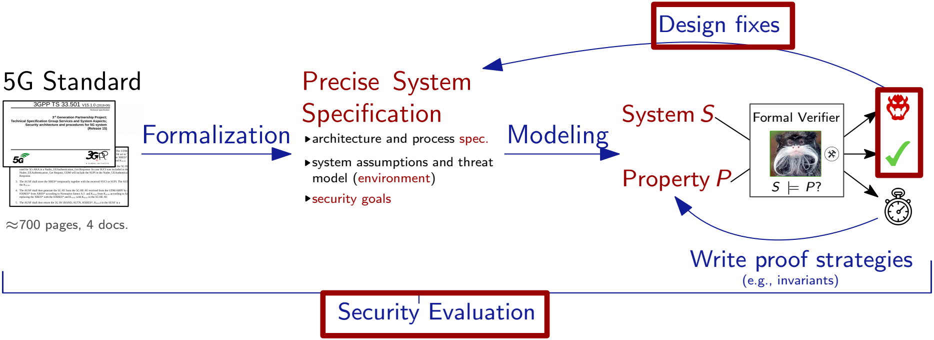
Threat Model & Security Goals ~1000LoC, 124 lemmas

- wide-range of formal security goals (including secrecy, authentication, privacy)
- + many compromise scenarios in order to identify minimal assumptions
  $\rightsquigarrow$ strongest possible adversary model

Proof Strategies ~1000LoC, ~ 5 hours computation time

- complex state-changes + loops $\rightsquigarrow$ automatic: / manual: impractical
- proof strategies: lemmas + heuristics that guide the proof search

Process


5G Standard
3GPP TS 33.501 V15.1.0 (2018-06)
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
S ⊨ P?
Design fixes
Write proof strategies
(e.g., invariants)
Security Evaluation

Results

More than just 👹/✓?

Results

More than just /?

YES! For instance for *authentication:*

- Different perspectives ... (who obtains guarantees, about whom?)

Pair of parties

Point of view	*UE*		*SN*		*HN*	
Partner	*SN*	*HN*	*UE*	*HN*	*UE*	*SN*

Results

More than just /✓?

YES! For instance for *authentication:*

- Different perspectives ... (who obtains guarantees, about whom?)
- with different kinds of agreement properties ... (identities?, data?, replay?)

Pair of parties

Point of view	*UE*		*SN*		*HN*	
Partner	*SN*	*HN*	*UE*	*HN*	*UE*	*SN*
Agreement						
on K_{sess}						
on *SUPI*						
on *SNname*						
Weak agree.						

Authentication properties

Results

More than just /✓?

YES! For instance for *authentication:*

- Different perspectives … (who obtains guarantees, about whom?)
- with different kinds of agreement properties … (identities?, data?, replay?)
- under different attacker models. (*e.g.* what can be compromised?)

Pair of parties

Point of view	*UE*				*SN*				*HN*			
Partner	*SN*		*HN*		*UE*		*HN*		*UE*		*SN*	
Agreement	NI	I	NI	I	NI	I	NI	I	NI	I	NI	I
on K_{sess}	…		…	…	…		…	…	…	…	…	…
on *SUPI*	-	-	-	-	-	-	…	-	-	-	-	-
on *SNname*	-	-	…	-	-	-	-	-	…	-	-	-
Weak agree.	…		$\neg K$		…		…		…		…	

Authentication properties

Minimal assumption

Results (cont.)

Minimal security assumptions:

- k-c: requires key-confirmation
- $\neg K$: no reveal of long-term key
- $\neg sk_{\mathrm{HN}}$: no reveal of sk_{HN}
- ¬ch: requires secure channel *SN-HN*
- ¬*SUPI*: no reveal of *SUPI*
- ¬*SQN*: no reveal of *SQN*

Pair of parties

Point of view	*UE*				*SN*				*HN*			
Partner	*SN*		*HN*		*UE*		*HN*		*UE*		*SN*	
Agreement	NI	I	NI	I	NI	I	NI	I	NI	I	NI	I
on K_{sess}	...		...	...	...		...	...	...	...	...	...
on *SUPI*	-	-	-	-	-	-	...	-	-	-	-	-
on *SNname*	-	-	...	-	-	-	-	-	...	-	-	-
Weak agree.	...		$\neg K$		...		...		...		...	

Authentication properties

Minimal assumption

Results (cont.)

Minimal security assumptions:

- k-c: requires key-confirmation
- $\neg K$: no reveal of long-term key
- $\neg sk_{\mathrm{HN}}$: no reveal of sk_{HN}
- ¬ch: requires secure channel *SN-HN*
- ¬*SUPI*: no reveal of *SUPI*
- ¬*SQN*: no reveal of *SQN*

Point of view	*UE*				*SN*				*HN*			
Partner	*SN*		*HN*		*UE*		*HN*		*UE*		*SN*	
Agreement	NI	I	NI	I	NI	I	NI	I	NI	I	NI	I
on K_{sess}	✗	✗	$\neg K \wedge$k-c	$\neg K \wedge$k-c	✗	✗	¬ch	$\neg K \wedge$¬ch	$\neg K$	$\neg K$	¬ch	¬ch
on *SUPI*	wa	×	wa	×	wa	×	[¬ch]	×	wa	×	×	×
on *SNname*	wa	×	[$\neg K \wedge$k-c]	×	wa	×	wa	×	[$\neg K$]	×	wa	×
Weak agree.	[✗]		$\neg K$		[$\neg K \wedge$¬ch]		¬ch		$\neg K$		¬ch	

wa: coincides with weak agreement. ×: undefined.

Results: Authentication: Attack 1

Attack 1

(on explicit goal given in the spec.)

makes *SN* think it is talking to another UE ($\neq$ *SUPI*)

How?

- $SN \xleftarrow{\text{Challenge}+\text{K}_{\text{sess}}} HN$ and $SN \xleftarrow{\textit{SUPI}} HN$ are not bound together!
- : interleave two sessions and swap two *SUPI*

Remark: In an earlier draft (v0.7.1), *SUPI*, K_{sess} sent together $\rightsquigarrow$ ✓

(we detected the introduced flaw when updating our models)

Results: Authentication: Attack 1

Attack 1

(on explicit goal given in the spec.)

👹 makes *SN* think it is talking to another UE ($\neq$ *SUPI*)

How?

- $SN \xleftarrow{\text{Challenge}+K_{sess}} HN$ and $SN \xleftarrow{SUPI} HN$ are not bound together!
- 👹: interleave two sessions and swap two *SUPI*

Remark: In an earlier draft (v0.7.1), *SUPI*, K_{sess} sent together $\leadsto$ ✓

(we detected the introduced flaw when updating our models)

Fix

Either:

- explicitly assume a binding channel *SN-HN* (= binding message−session)
- cryptographically bind the messages together

Results: Authentication: Attack 2

We re-verify all authentication properties when attack 1 is fixed:

Point of View	$\boxed{UE}$	SN
Partner	$\boxed{SN}$	UE
$\boxed{\text{Weak agreement}}$	$[\neg K \wedge \boxed{\text{key-conf}} \wedge \neg \text{ch}]$	$[\neg K \wedge \neg \text{ch}]$

Key-confirmation is required!

However, key-confirmation is not mandatory in the standard!

(subsequent procedures?)

Results: Authentication: Attack 2 (cont.)

Attack 2
(on explicit goal given in the spec.)

can impersonate a *SN* towards *UEs* without key-conf (not mandatory)

How?

- *SNname* is not included in the MAC sent by *HN* that comes with the challenge

Results: Authentication: Attack 2 (cont.)

Attack 2 (on explicit goal given in the spec.)

can impersonate a *SN* towards *UEs* without key-conf (not mandatory)

How?

- *SNname* is not included in the MAC sent by *HN* that comes with the challenge

Fix

Either:

- mandatory key-confirmation, required in one direction only ($UE \leftarrow SN$)
- add *SNname* to the MAC sent by *HN* (key-confirmation not required then)

Remark: our fixes reduce the number of roundtrips required to get security!

Results: Secrecy and Privacy

Secrecy($\mathsf{K}_{\mathsf{sess}}, K$) holds but not PFS($\mathsf{K}_{\mathsf{sess}}$)

Privacy: The *UE*'s identifier *SUPI* remains **secret** (with honest *SN*/*HN*)

- defeats IMSI-catchers but not necessarily passive (?)
- **insufficient** to ensure **untraceability** with an active
- we were not able to formally analyze any fix or find attacks for the full model (we'll come back to that)

Takeaways (CCS'18)

Contributions: Formalization of the 5G standard + Tamarin model with proof techniques + comprehensive security evaluation

5G AKA standard:

- definitely lacks explicit assumptions and security goals ☹
- meets core properties after easy fixes/+assumptions ☺
- improves privacy over 3G/4G, but still suffers from traceability attacks ☹

We have an ongoing discussion with 3GPP and GSMA about potential remedies. Process is slow and communication is hard.

Takeaways (CCS'18)

Contributions: Formalization of the 5G standard + Tamarin model with proof techniques + comprehensive security evaluation

5G AKA standard:

- definitely lacks explicit assumptions and security goals ☹
- meets core properties after easy fixes/+assumptions ☺
- improves privacy over 3G/4G, but still suffers from traceability attacks ☹

We have an ongoing discussion with 3GPP and GSMA about potential remedies. Process is slow and communication is hard.

Future work:

- verify and formally compare other variants of AKA (3G, 4G, EAP-AKA' in 5G)
- follow the development of 5G (*e.g.* phase 2)

Outline

Introduction

I A Formal Analysis of 5G Authentication (CCS'18)

II New Privacy Vulnerability in 5G (+3G, 4G) (PETS'19)

III Privacy vs. Formal Methods

IV Conclusion

Paper

sciendo

Proceedings on Privacy Enhancing Technologies 2019

Ravishankar Borgaonkar, Lucca Hirschi*, Shinjo Park, and Altaf Shaik

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

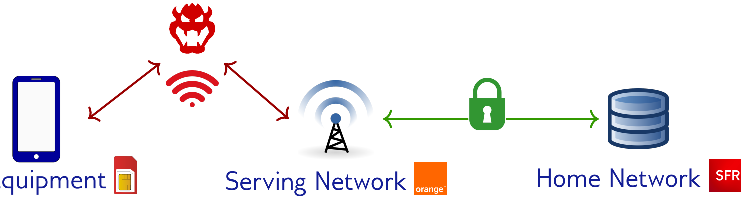
Abstract: Mobile communications are used by more than two-thirds of the world population who expect security and privacy guarantees. The *3rd Generation Partnership Project* (3GPP) responsible for the worldwide standardization of mobile communication has designed and mandated the use of the *AKA protocol* to protect the subscribers' mobile services. Even though privacy was a requirement, numerous subscriber lo-

The *3rd Generation Partnership Project* (3GPP) group, responsible for the standardization of 3G, 4G, and 5G technologies, designed the *Authentication and Key Agreement* (AKA) protocol that aims at mutually authenticating a phone equipped with a USIM card with networks, and establishing keys to protect subsequent communications. This protocol is notably implemented in all 3G and 4G USIM cards and cellular networks

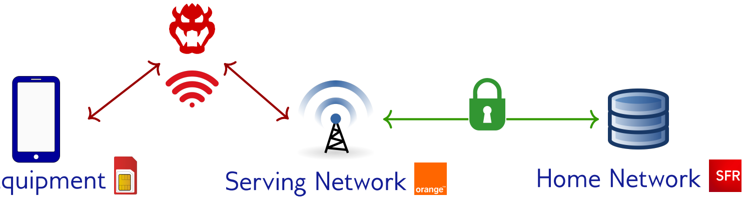
in Privacy Enhancing Technologies Symposium 2019

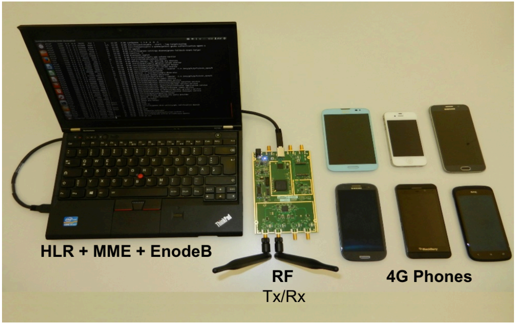
Privacy: Threat Model

Privacy: Threat Model



Privacy: Threat Model





SDR (Soft Defined Radio) hardware + open software (`srsLTE`, `OpenLTE`)

$\leadsto$ can set up fake Base Stations (BS) for $\approx$ 1200€

Background on Privacy

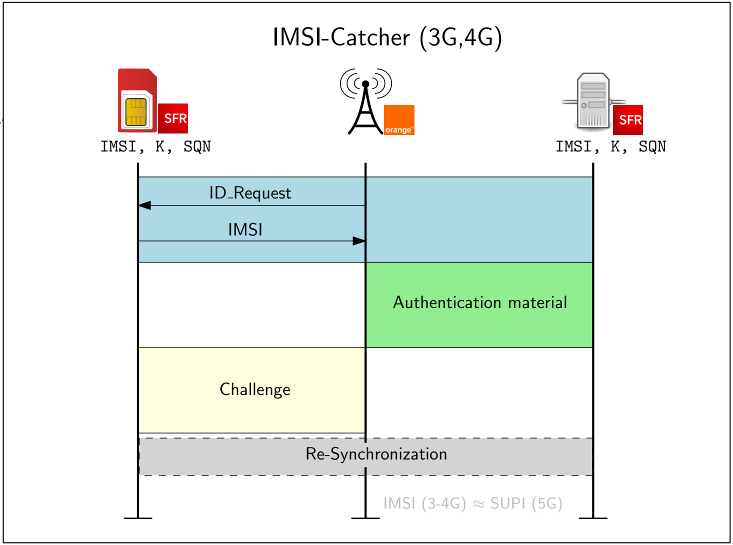
State-of-the-art

- known issues: Location Privacy
  -  can track User Equipments around his fake Base Stations
  - *e.g.* IMSI-catchers (3G,4G), failure messages (3G,4G,5G), etc..

Background on Privacy

St

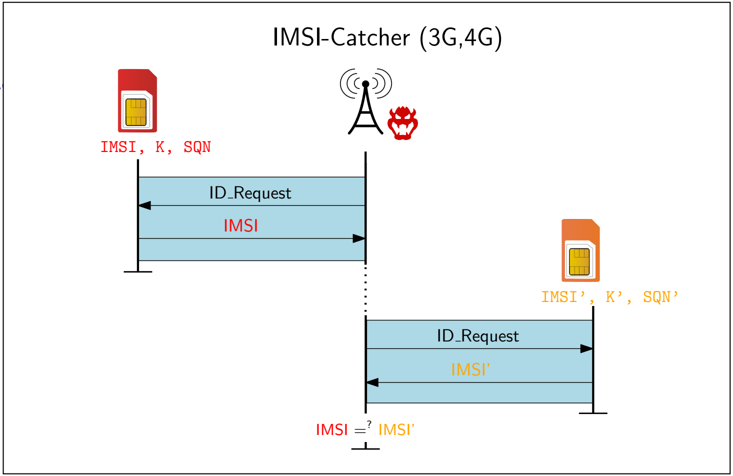
▶



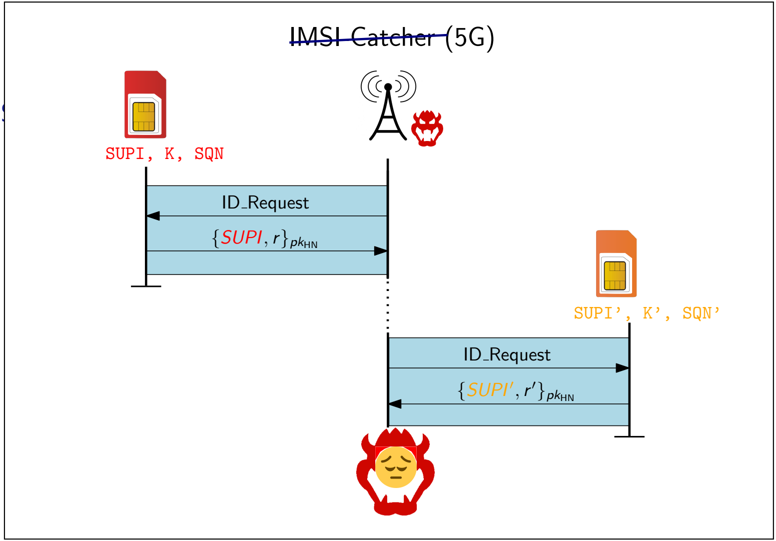
Background on Privacy

St

▶



Background on Privacy



Background on Privacy

State-of-the-art

- known issues: Location Privacy
  - can track User Equipments around his fake Base Stations
  - *e.g.* IMSI-catchers (3G,4G), failure messages (3G,4G,5G), etc..
- 4G: many proposed fixes but devices are still vulnerable
- 5G: asymmetric encryption of SUPI $\rightsquigarrow$ promise to protect privacy,
  but still vulnerable to location privacy attacks

Our attack

- Vulnerability in the protection mechanism for SQN in the specification of AKA in 3G, 4G, and 5G
- $\leadsto$ learns n least significant bits of SQN

  (Confidentiality(SQN) is an explicit goal of 5G AKA)
- $\leadsto$ leaks target's activity/consumption

  Service consumption (*e.g.* calls, SMSs) triggers AKA sessions and thus SQN$\nearrow$

Our attack

- Vulnerability in the protection mechanism for SQN in the specification of AKA in 3G, 4G, and 5G
- $\leadsto$ learns n least significant bits of SQN

  (Confidentiality(SQN) is an explicit goal of 5G AKA)
- $\leadsto$ leaks target's activity/consumption

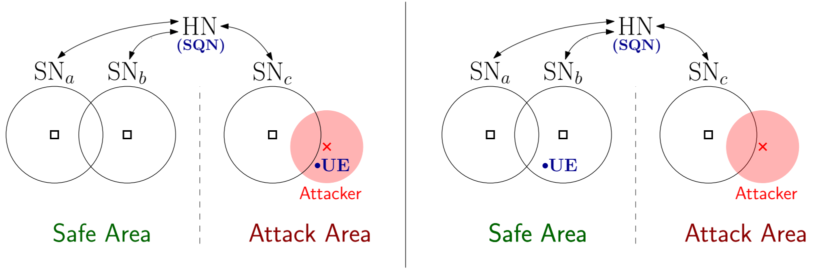
  Service consumption (*e.g.* calls, SMSs) triggers AKA sessions and thus SQN$\nearrow$
- $\leadsto$ activity monitoring attack even when is not in the target's vicinity

Our attack

- Vulnerability in the protection mechanism for SQN in the specification of AKA in 3G, 4G, and 5G
- $\rightsquigarrow$ learns n least significant bits of SQN

  (Confidentiality(SQN) is an explicit goal of 5G AKA)
- $\rightsquigarrow$ leaks target's activity/consumption

  Service consumption (*e.g.* calls, SMSs) triggers AKA sessions and thus SQN$\nearrow$
- $\rightsquigarrow$ activity monitoring attack even when is not in the target's vicinity



Attacker in the target's vicinity

known: location and monitoring

Attacker outside the target's vicinity

NEW: monitoring

Our attack

- Vulnerability in the protection mechanism for SQN in the specification of AKA in 3G, 4G, and 5G
- $\leadsto$ learns n least significant bits of SQN

  (Confidentiality(SQN) is an explicit goal of 5G AKA)
- $\leadsto$ leaks target's activity/consumption

  Service consumption (*e.g.* calls, SMSs) triggers AKA sessions and thus SQN$\nearrow$
- $\leadsto$ activity monitoring attack even when is not in the target's vicinity
- based on new attack vectors (need dedicated fixes) + new location attacks

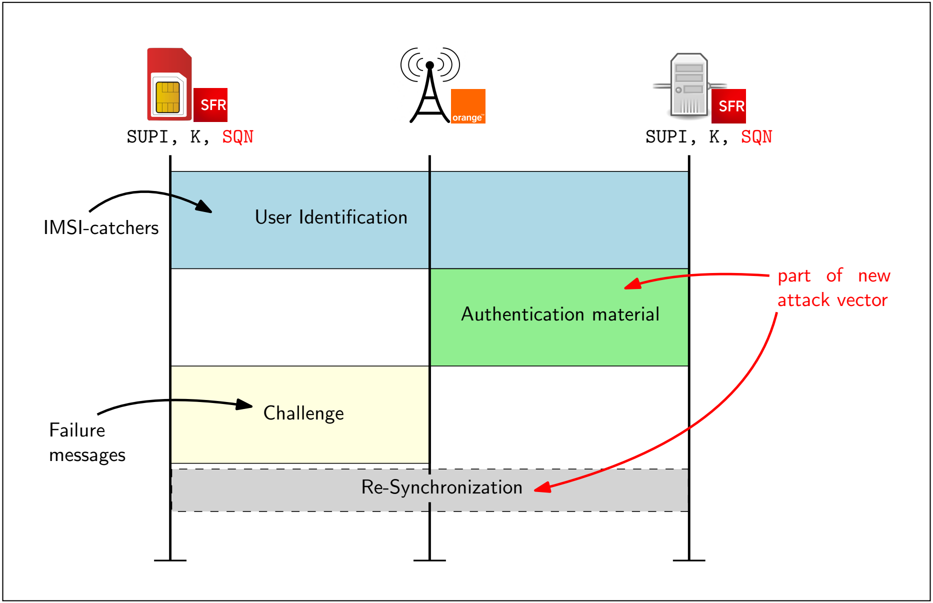
Our attack

- Vulnerability in the protection mechanism for SQN in the specification of AKA in 3G, 4G, and 5G
- $\leadsto$ learns n least significant bits of SQN
  (Confidentiality(SQN) is an explicit goal of 5G AKA)
- $\leadsto$ leaks target's activity/consumption
  Service consumption (*e.g.* calls, SMSs) triggers AKA sessions and thus SQN$\nearrow$
- $\leadsto$ activity monitoring attack even when is not in the target's vicinity
- based on new attack vectors (need dedicated fixes) + new location attacks

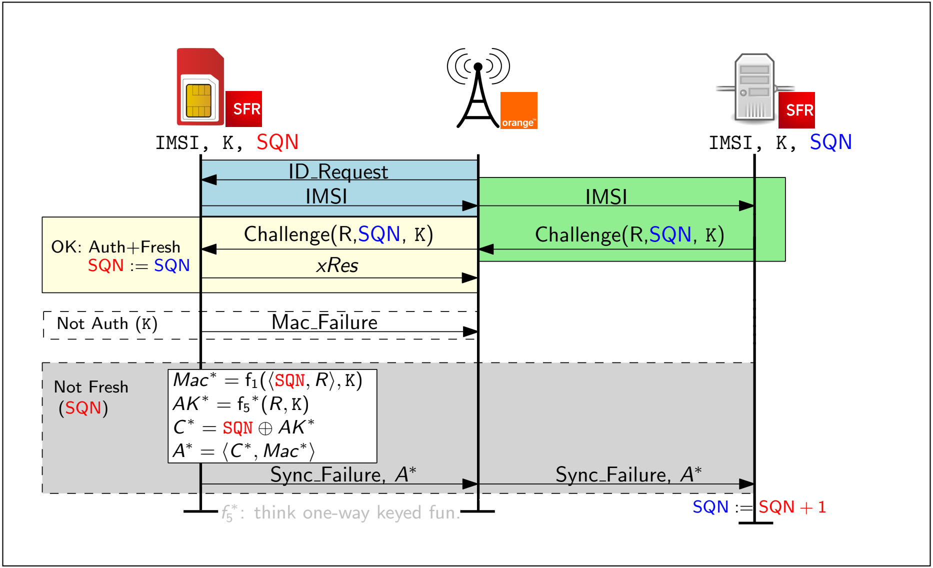
Privacy Threat? Maybe...
In practice: BSs in subway stations, shops, work places, etc. $\leadsto$ "sporadic"

- VIP targets (embassy, journalists): phone has been switched off?, detect the use of multiple SIM cards, typical usage per SIM card?
  $\leadsto$ when at home, during business trips, etc.
- work places: activity out of work, use different SIM cards?
- shop greedy about your data: mobile consumption patterns (*e.g.* Navizon)

Re-Synchronization



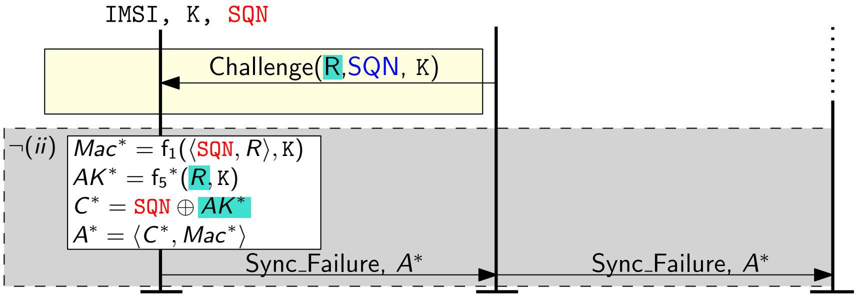
Re-Synchronization



Attack Vector

Attack vector = combination of:

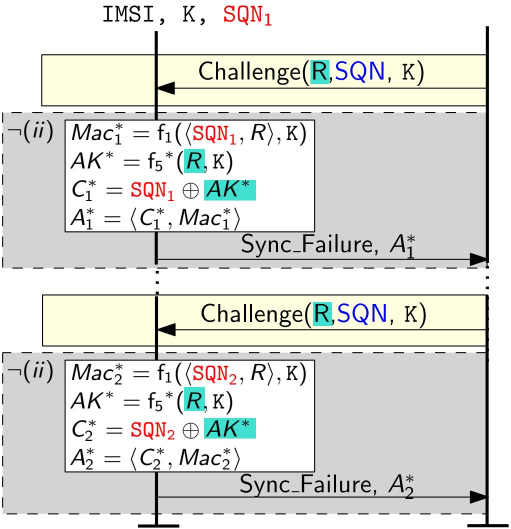
1. requests of challenges are not authenticated
2. injections of the same (unfresh) challenge $\rightsquigarrow$ same conceal factor AK^*



Attack Vector

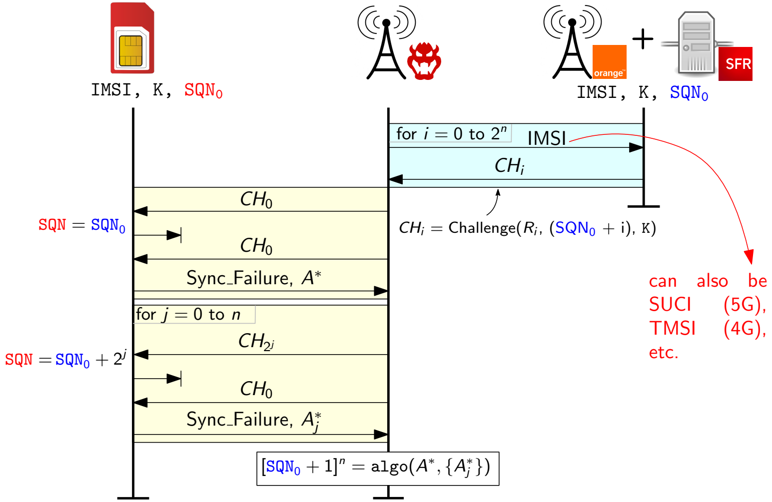
Attack vector = combination of:

1. requests of challenges are not authenticated
2. injections of the same (unfresh) challenge $\rightsquigarrow$ same conceal factor AK^*

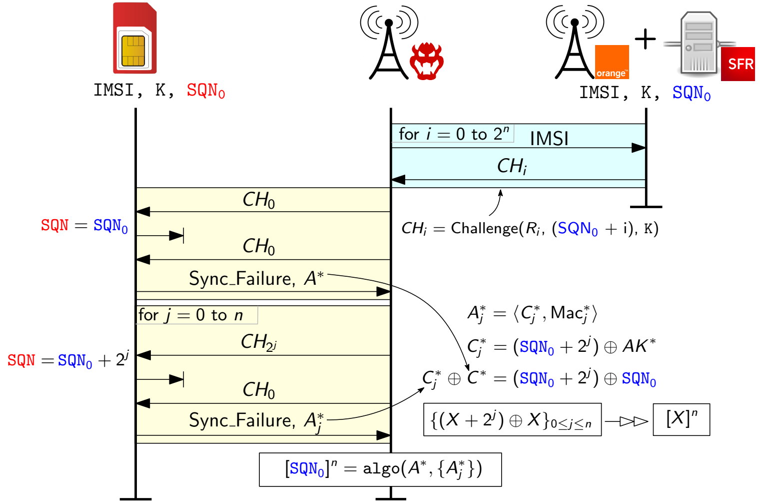


$$C_1^* \oplus C_2^* = \mathtt{SQN}_1 \oplus \mathtt{SQN}_2$$

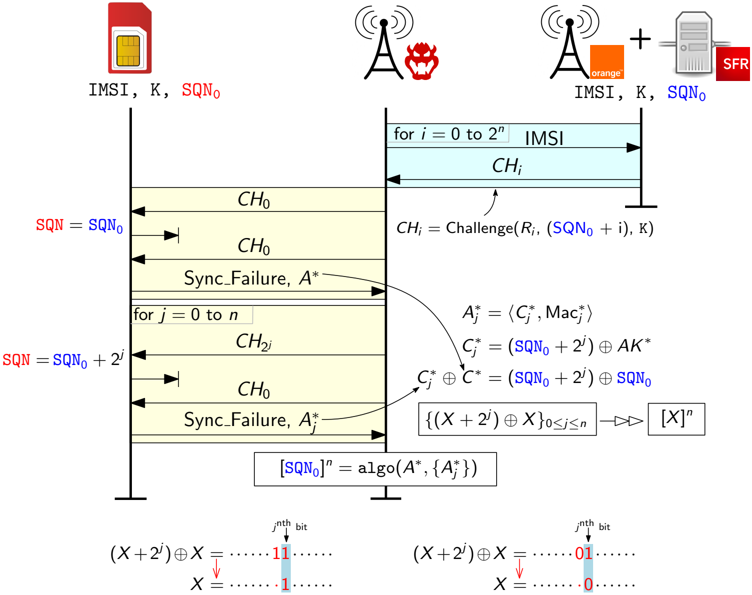
Breaking SQN Confidentiality



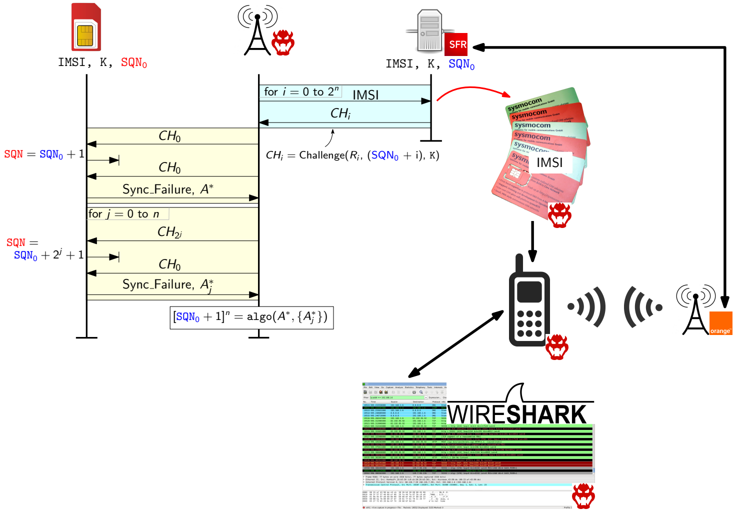
Breaking SQN Confidentiality



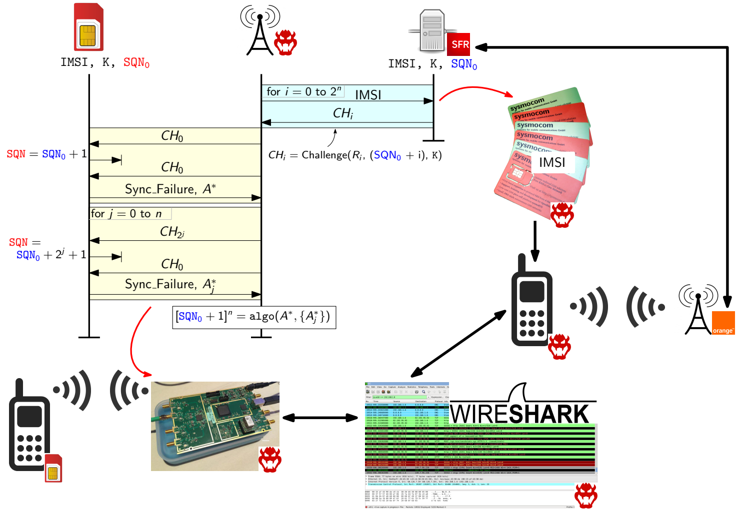
Breaking SQN Confidentiality



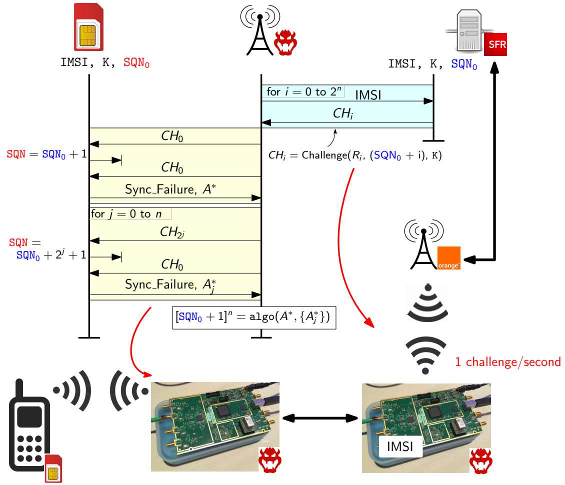
Proof of Concept: it can be exploited (done in 4G)



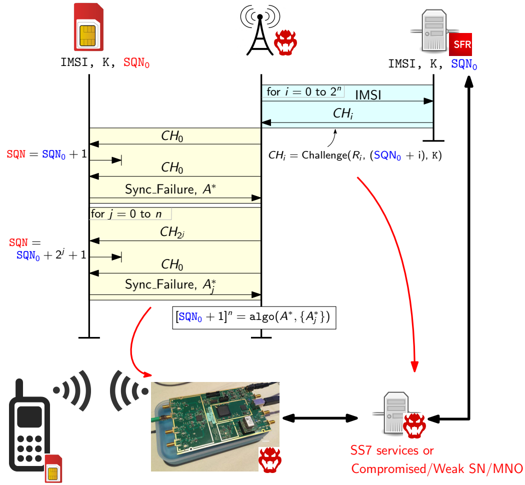
Proof of Concept: it can be exploited (done in 4G)



Proof of Concept: it can be exploited (done in 4G) (better)



Proof of Concept: it scales (?)



Practical considerations

- On the 3-5G spec $\rightsquigarrow$ impacts all 3G, 4G devices + 5G devices (if not fixed), as well as variants (*e.g.* $\{\text{EAP}, \text{EPS}\}$-AKA$^{',*}$, HTTP digest AKA)

Experiments in 4G

- Full hardware setup: 1200€ (≈100€ for PoC only), widely available
- Tested on a couple of Europeans TelCo operators
- Obtained ≈10 bits of SQN in minutes, many ways to improve
- We did not observe any rate limit at which AKA tokens can be requested

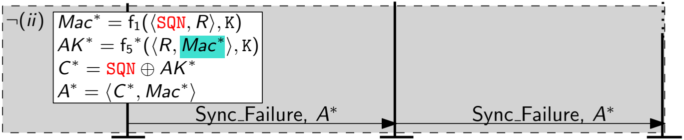
First responsible disclosure to 3GPP SA#3 and GSMA: Spring 2017.

Fixes

- Fixes based on: *asymmetric encryption* or *random* from  $\rightsquigarrow$ impractical for 3G, 4G
- We propose instead to use the cipher suite used for the transport mode to encrypt SQN instead of $\oplus$.
  Problem: encryption is outsourced to phone.

Fixes

- Fixes based on: *asymmetric encryption* or *random* from ⇝ impractical for 3G, 4G
- We propose instead to use the cipher suite used for the transport mode to encrypt SQN instead of $\oplus$.
  Problem: encryption is outsourced to phone.
- Qualcomm Inc. propose instead to use MAC* (based on SQN) in AK*.



`Change Request S3-190376` discussed during a 3GPP SA#3 meeting on February 1st, 2019: not pursued (postponed according to Qualcomm).

AT&T supported this change. Apple: we should first investigate whether it is feasible in 5G, and then evaluate the effect and make corresponding enhancement. It was left open to verify what GSMA was doing on this topic.

Lessons (PETS'19)

- Trade-offs are no longer valid - almost 25 years (*e.g.* passive attacker only, no fake BSs).
- Mobile devices are still dumb terminals in the architecture
- Unexpected components can put users' privacy at risk
- TelCo standardization is rather opaque, patent-driven, slow
  $\rightsquigarrow$ what to expect from 5G?

Outline

Main Questions

(3G,4G,5G) AKA suffer from privacy attacks: location privacy, activity monitoring attacks, etc.

There have been several prior formal analyses focusing on privacy:

- Why haven't they found all those attacks?
- Even *a posteriori*: why is it so hard to find the known attacks?
- How can we quickly evaluate fixes? (*e.g.* give Qualcomm some feedback about their CR)

Main Questions

(3G,4G,5G) AKA suffer from privacy attacks: location privacy, activity monitoring attacks, etc.

There have been several prior formal analyses focusing on privacy:

- Why haven't they found all those attacks?
- Even *a posteriori*: why is it so hard to find the known attacks?
- How can we quickly evaluate fixes? (*e.g.* give Qualcomm some feedback about their CR)

Privacy vs. classical properties:

- It worked well and "smoothly" for classical properties ☺
- Not so much for privacy ☹ notoriously harder

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* **PETS'16**. (new location attack, fix, and a computational proof)
- *Koustos* **Euro S&P'19**. (attack on the fix from PETS'16, fix, and computational proof)

$\rightsquigarrow$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* **PETS'16.** (new location attack, fix, and a computational proof)
- *Koustos* **Euro S&P'19.** (attack on the fix from PETS'16, fix, and computational proof)

$\leadsto$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* **CCS'12.** (failure messages attack and fix with `aenc`)
- *O'Hanlon, Borgaonkar, Hirschi.* **S&P Workshops'12.**
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses as benchmarks but not faithful to the original protocol

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* **PETS'16**. (new location attack, fix, and a computational proof)
- *Koustos* **Euro S&P'19**. (attack on the fix from PETS'16, fix, and computational proof)

$\leadsto$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* **CCS'12**. (failure messages attack and fix with `aenc`)
- *O'Hanlon, Borgaonkar, Hirschi.* **S&P Workshops'12**.
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses as benchmarks but not faithful to the original protocol

$\leadsto$ Only for finding an attack *a posteriori*. (+ extremely weak proofs)
$\leadsto$ Even then, none of the analyses is faithful to the original protocol (stateful and $\oplus$).

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* **PETS'16**. (new location attack, fix, and a computational proof)
- *Koustos* **Euro S&P'19**. (attack on the fix from PETS'16, fix, and computational proof)

$\leadsto$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* **CCS'12**. (failure messages attack and fix with `aenc`)
- *O'Hanlon, Borgaonkar, Hirschi.* **S&P Workshops'12**.
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses as benchmarks but not faithful to the original protocol

$\leadsto$ Only for finding an attack *a posteriori*. (+ extremely weak proofs)
$\leadsto$ Even then, none of the analyses is faithful to the original protocol (stateful and $\oplus$).

We also tried ourselves (partial results in the 2 papers) but also failed.

Open Questions

What should be analyzed and how:

- The threat models have evolved: passive, active, sporadic, notion of locality and time (PFS, PCS). $\rightsquigarrow$ How to model and verify privacy for those different attackers?
  $\rightsquigarrow$ How to evaluate trade-offs between threat models and guarantees?

Open Questions

What should be analyzed and how:

- The threat models have evolved: passive, active, sporadic, notion of locality and time (PFS, PCS). $\rightsquigarrow$ How to model and verify privacy for those different attackers?
  $\rightsquigarrow$ How to evaluate trade-offs between threat models and guarantees?
- The privacy impact of partially learning SQN was far from being obvious.
  $\rightsquigarrow$ Shift from "verifying privacy properties A,B,C modelled as X,Y,Z" to "veryfing the absence of any (symbolic) privacy leak".
  Use emulation-based proof techniques based on ideal functionality?
  α/β privacy approach? (describe what is allowed to be leaked)

Open Questions

What should be analyzed and how:

- The threat models have evolved: passive, active, sporadic, notion of locality and time (PFS, PCS). $\rightsquigarrow$ How to model and verify privacy for those different attackers?
  $\rightsquigarrow$ How to evaluate trade-offs between threat models and guarantees?
- The privacy impact of partially learning SQN was far from being obvious.
  $\rightsquigarrow$ Shift from “verifying privacy properties A,B,C modelled as X,Y,Z” to “veryfing the absence of any (symbolic) privacy leak”.
  Use emulation-based proof techniques based on ideal functionality?
  α/β privacy approach? (describe what is allowed to be leaked)

Modeling issues, even for re-finding known attacks:

- Is my equational theory rich enough? Confidentiality of SQN: requires $\oplus$ but not enough (even if strong secrecy is used). We also need some algebraic relations of $+$ with $\oplus$ (such that $(X + 1) \oplus X \not\sim Y$).

Open Questions

What should be analyzed and how:

- The threat models have evolved: passive, active, sporadic, notion of locality and time (PFS, PCS). $\rightsquigarrow$ How to model and verify privacy for those different attackers?
  $\rightsquigarrow$ How to evaluate trade-offs between threat models and guarantees?
- The privacy impact of partially learning SQN was far from being obvious.
  $\rightsquigarrow$ Shift from "verifying privacy properties A,B,C modelled as X,Y,Z" to "veryfing the absence of any (symbolic) privacy leak".
  Use emulation-based proof techniques based on ideal functionality?
  α/β privacy approach? (describe what is allowed to be leaked)

Modeling issues, even for re-finding known attacks:

- Is my equational theory rich enough? Confidentiality of SQN: requires $\oplus$ but not enough (even if strong secrecy is used). We also need some algebraic relations of $+$ with $\oplus$ (such that $(X+1) \oplus X \not\to Y$).
- AKA is stateful (SQN), uses a counter with arithmetic (SQN), uses $\oplus$, has ≥ 3 parties, is rather large and complex. How to handle all that?
  $\rightsquigarrow$ critical issues: precision (stateful, counter), scope (equational theories), scale (size and complexity).

Long-term goal

Privacy evaluation of all pre-authentication protocols (incl. AKA) in X-G.

+ Impact of optional mechanisms and sub-protocols.
+ Explore threat model trade-offs.
+ All generations together.

Outline

Conclusion

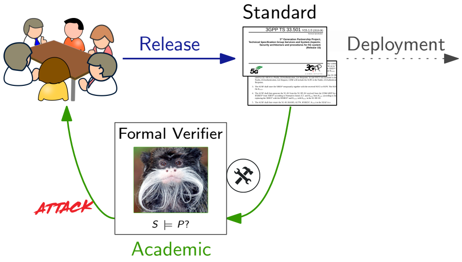
Mobile communication:

- critical area, yet it dœs not attract as much attention as it should
- experiments are hard to perform, much details in TelCo walled gardens
- huge specification with a lot of other mechanisms and protocols to analyze
- formal methods and TelCo: far away from IETF's positions (*e.g.* TLS, MLS) but still positive discussions with Ericsson, Nokia, Vodafone

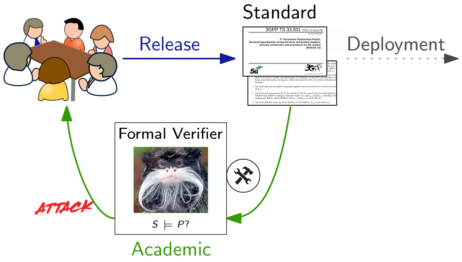
Formal methods:

- now meet expectations for classical properties: can guide and quickly evaluate design decisions. It should be used more often.
- not really industry-ready for privacy yet: many interesting challenges ahead
- importance of putting formal methods into practice: provides much insights and highlights current limitations

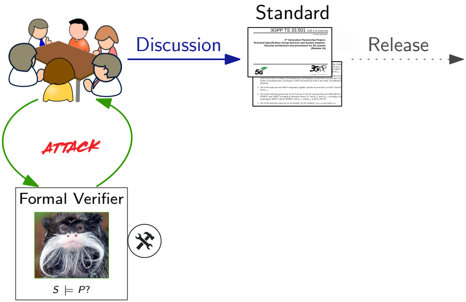
Now:


Standard
Release
Deployment
3GPP TS 33.501
Formal Verifier
$S \models P$?
ATTACK
Academic

Now:

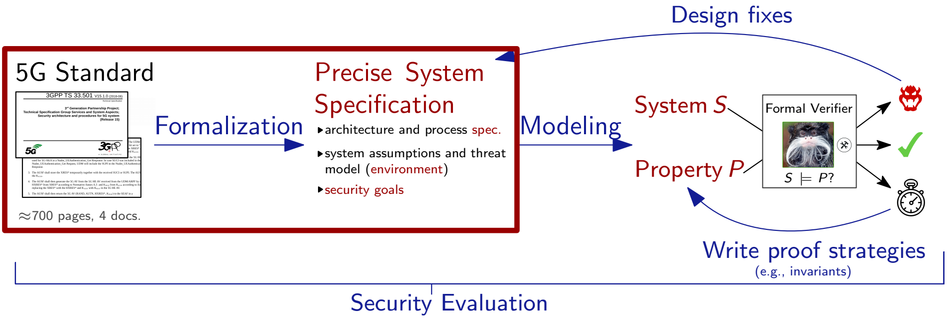

Release
Standard
3GPP TS 33.501
Deployment
Formal Verifier
$S \models P$?
ATTACK
Academic

Ideally:


Discussion
Standard
3GPP TS 33.501
Release
ATTACK
Formal Verifier
$S \models P$?

Backup Slides

Process



Design fixes
5G Standard
3GPP TS 33.501 V15.1.0 (2018-06)
3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 15)
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
S ⊨ P?
Write proof strategies
(e.g., invariants)
Security Evaluation

Formalization

Goal: build a precise specification of the system (protocol), environment (*e.g.* threat model), and security goals

Example of imprecision in the standard and our interpretation:

Assurance [that the subscriber] is connected to a serving network that is authorized by the home network.

$\rightsquigarrow$

Subscriber must obtain non-injective agreement on SNname with its Home Network.

Formalization

Goal: build a precise specification of the system (protocol), environment (*e.g.* threat model), and security goals

Example of imprecision in the standard and our interpretation:

Assurance [that the subscriber] is connected to a serving network that is authorized by the home network.

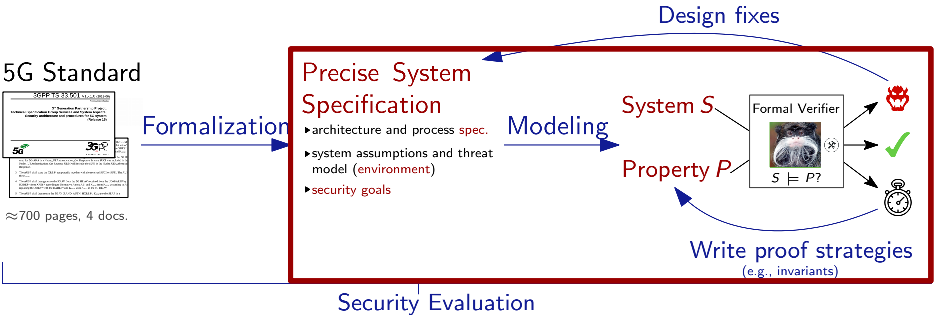
$\rightsquigarrow$

Subscriber must obtain non-injective agreement on SNname with its Home Network.

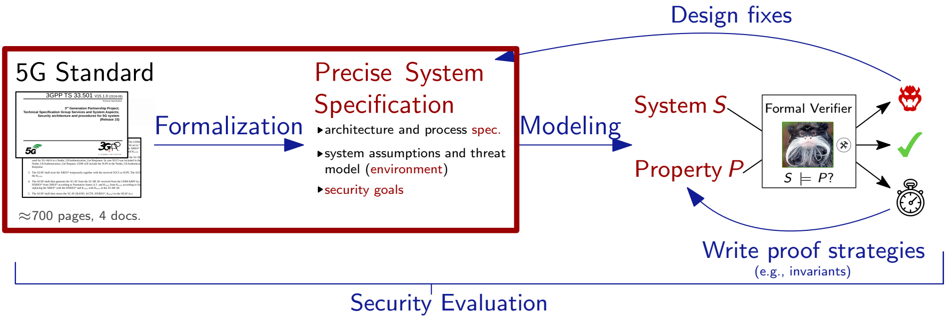
Takeaways

- critical security goals are missing (implicit?): *e.g.* injective agreement on the key seed
- some stated goals are too weak: no assurance that the authenticated party participated to the current session
- unclear system assumption (*e.g.* on channels) and threat model (notably for privacy)

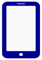
Process


Design fixes
5G Standard
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
$S \models P$?
Write proof strategies
(e.g., invariants)
Security Evaluation

Outline


Design fixes
5G Standard
3GPP TS 33.501
≈700 pages, 4 docs.
Formalization
Precise System Specification
architecture and process spec.
system assumptions and threat model (environment)
security goals
Modeling
System S
Property P
Formal Verifier
S ⊨ P?
Write proof strategies
(e.g., invariants)
Security Evaluation

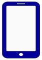
Authentication: definitions

						
Point of view	*UE*		*SN*		*HN*	
Partner	*SN*	*HN*	*UE*	*HN*	*UE*	*SN*

Authentication depends on the perspective and the expected agreement:
What guarantees dœs *UE* obtain regarding *HN*?

(*HN*'s identity, *HN*'s view on the session)

Authentication: definitions

						
Point of view	*UE*		*SN*		*HN*	
Partner	*SN*	*HN*	*UE*	*HN*	*UE*	*SN*
Weak agree.	? ?	? ?		[...]		

Authentication depends on the perspective and the expected agreement:
What guarantees dœs *UE* obtain regarding *HN*?

weak agreement	agreement on *HN*'s and *UE*'s ids (mutual auth.)

Authentication: definitions

Point of view	*UE*				*SN*		*HN*	
Partner	*SN*		*HN*		*UE*	*HN*	*UE*	*SN*
Agreement	NI	I	NI	I				
on K_{sess}	?	?	?	?		[...]		
on *SUPI*	?	?	?	?				
on *SNname*	?	?	?	?				
Weak agree.	?	?	?	?				

Authentication depends on the perspective and the expected agreement:
What guarantees dœs *UE* obtain regarding *HN*?

weak agreement	agreement on *HN*'s and *UE*'s ids (mutual auth.)
(NI) non-injective agreement on K_{sess}	agreement on *HN*'s and *UE*'s ids and K_{sess}

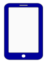
Authentication: definitions

Point of view	UE				SN		HN	
Partner	SN		HN		UE	HN	UE	SN
Agreement	NI	I	NI	I				
on K_{sess}	?	?	?	?	[...]			
on *SUPI*	?	?	?	?				
on *SNname*	?	?	?	?				
Weak agree.	?	?	?	?				

Authentication depends on the perspective and the expected agreement:
What guarantees dœs *UE* obtain regarding *HN*?

weak agreement	agreement on *HN*'s and *UE*'s ids (mutual auth.)
(NI) non-injective agreement on K_{sess}	agreement on *HN*'s and *UE*'s ids and K_{sess}
(I) injective agreement on K_{sess}	NI + uniqueness of *HN*'s session (no replay)

Authentication: definitions



Point of view	*UE*				*SN*		*HN*	
Partner	*SN*		*HN*		*UE*	*HN*	*UE*	*SN*
Agreement	NI	I	NI	I				
on K_{sess}	✗	✗	$\neg K \wedge$k-c	$\neg K \wedge$k-c	[...]			
on *SUPI*	wa	×	wa	×				
on *SNname*	wa	×	[$\neg K \wedge$k-c]	×				
Weak agree.	[✗]		$\neg K$					

Authentication depends on the perspective and the expected agreement:
What guarantees does *UE* obtain regarding *HN*?

weak agreement	agreement on *HN*'s and *UE*'s ids (mutual auth.)
(NI) non-injective agreement on K_{sess}	agreement on *HN*'s and *UE*'s ids and K_{sess}
(I) injective agreement on K_{sess}	NI + uniqueness of *HN*'s session (no replay)

Minimal security assumption:

- $\neg K$: no reveal of long-term key
- k-c: requires key-confirmation
- $\neg$ch: requires secure channel *SN-HN*
- (also compromise of sk_{HN}, *SUPI*, *SQN*)

Authentication: definitions

Point of view	UE				SN				HN			
Partner	SN		HN		UE		HN		UE		SN	
Agreement	NI	I	NI	I	NI	I	NI	I	NI	I	NI	I
on K_{sess}	✗	✗	$\neg K \wedge$k-c	$\neg K \wedge$k-c	✗	✗	¬ch	$\neg K \wedge \neg$ch	$\neg K$	$\neg K$	¬ch	¬ch
on *SUPI*	wa	×	wa	×	wa	×	[¬ch]	×	wa	×	×	×
on *SNname*	wa	×	[$\neg K \wedge$k-c]	×	wa	×	wa	×	[$\neg K$]	×	wa	×
Weak agree.	[✗]		$\neg K$		[$\neg K \wedge \neg$ch]		¬ch		$\neg K$		¬ch	

Authentication depends on the perspective and the expected agreement:
What guarantees does *UE* obtain regarding *HN*?

weak agreement	agreement on *HN*'s and *UE*'s ids (mutual auth.)
(NI) non-injective agreement on K_{sess}	agreement on *HN*'s and *UE*'s ids and K_{sess}
(I) injective agreement on K_{sess}	NI + uniqueness of *HN*'s session (no replay)

Minimal security assumption:

- $\neg K$: no reveal of long-term key
- k-c: requires key-confirmation
- ¬ch: requires secure channel *SN*-*HN*
- (also compromise of sk_{HN}, *SUPI*, *SQN*)

Authentication: all results

Point of view	*UE*				*SN*				*HN*			
Partner	*SN*		*HN*		*UE*		*HN*		*UE*		*SN*	
Agreement	NI	I	NI	I	NI	I	NI	I	NI	I	NI	I
on K_{sess}	✗	✗	$\neg K \wedge$k-c	$\neg K \wedge$k-c	✗	✗	¬ch	$\neg K \wedge$¬ch	$\neg K$	$\neg K$	¬ch	¬ch
on *SUPI*	wa	×	wa	×	wa	×	[¬ch]	×	wa	×	×	×
on *SNname*	wa	×	[$\neg K \wedge$k-c]	×	wa	×	wa	×	[$\neg K$]	×	wa	×
Weak agree.	[✗]		$\neg K$		[$\neg K \wedge$¬ch]		¬ch		$\neg K$		¬ch	

After fixing Attack 1 (binding):

Point of View	*UE*		*SN*	
Partner	*SN*		*UE*	
Agreement	NI	I	NI	I
on K_{SEAF}	$\neg K \wedge$key-conf$\wedge$¬ch	$\neg K \wedge$key-conf$\wedge$¬ch	$\neg K \wedge$¬ch	$\neg K \wedge$¬ch
Weak agreement	[$\neg K \wedge$key-conf$\wedge$¬ch]		[$\neg K \wedge$¬ch]	

Other Results

Secrecy:

Point of view	*UE*	*SN*	*HN*
K_{sess}	$\neg K \wedge \neg \mathsf{ch}$	$\neg K \wedge \neg \mathsf{ch}$	$\neg K \wedge \neg \mathsf{ch}$
$\mathsf{PFS}(K_{\mathrm{sess}})$	✗	✗	✗
SUPI	$\neg sk_{\mathrm{HN}} \wedge \neg \mathsf{ch}^{*}$	–	$\neg sk_{\mathrm{HN}} \wedge \neg \mathsf{ch}^{*}$
K	$\varnothing$	$\varnothing$	$\varnothing$

*: no dishonest SNs (violated otherwise)

Other Results

Secrecy:

Point of view	*UE*	*SN*	*HN*
K_{sess}	$\neg K \wedge \neg \mathsf{ch}$	$\neg K \wedge \neg \mathsf{ch}$	$\neg K \wedge \neg \mathsf{ch}$
PFS(K_{sess})	✗	✗	✗
SUPI	$\neg sk_{\mathrm{HN}} \wedge \neg \mathsf{ch}^*$	–	$\neg sk_{\mathrm{HN}} \wedge \neg \mathsf{ch}^*$
K	$\varnothing$	$\varnothing$	$\varnothing$

*: no dishonest SNs (violated otherwise)

Privacy:

- *SUPI* remains confidential, even against active attackers and hence also against passive attackers.
- 5G AKA thus defeats previous active IMSI-catcher attacks
- We also have modelled a weak, passive attacker and have automatically proven that he cannot trace subscribers.
- active attackers are realistic threats for most use cases. We have (automatically) found that 5G AKA suffers from a traceability attack in that setting.

Background on Privacy

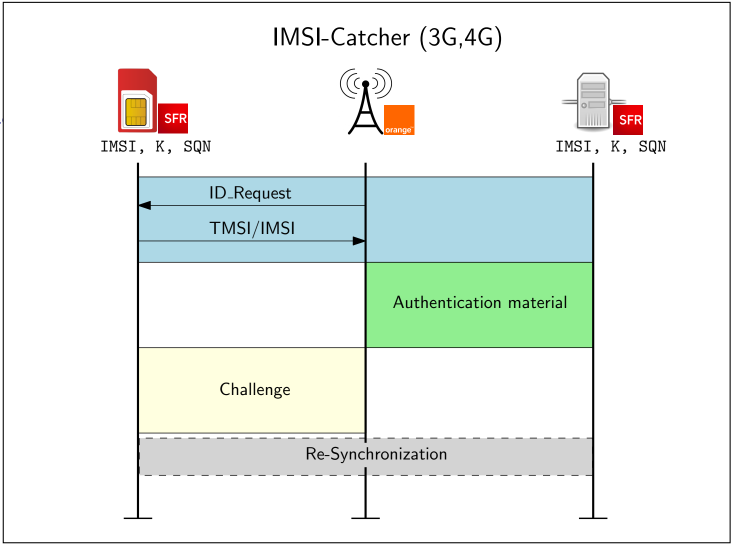
State-of-the-art

- known issues: Location Privacy
  - can track User Equipments around his fake Base Stations
  - *e.g.* IMSI leakage, failure messages, etc..

Background on Privacy

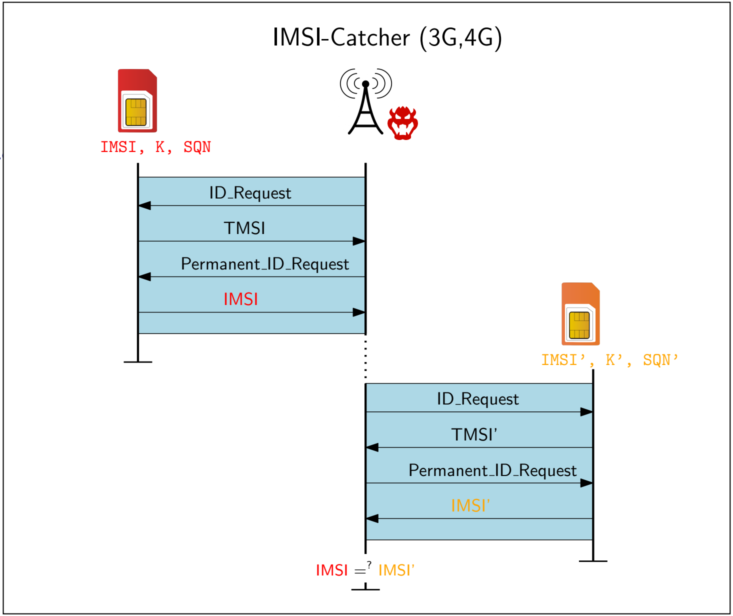
St

-

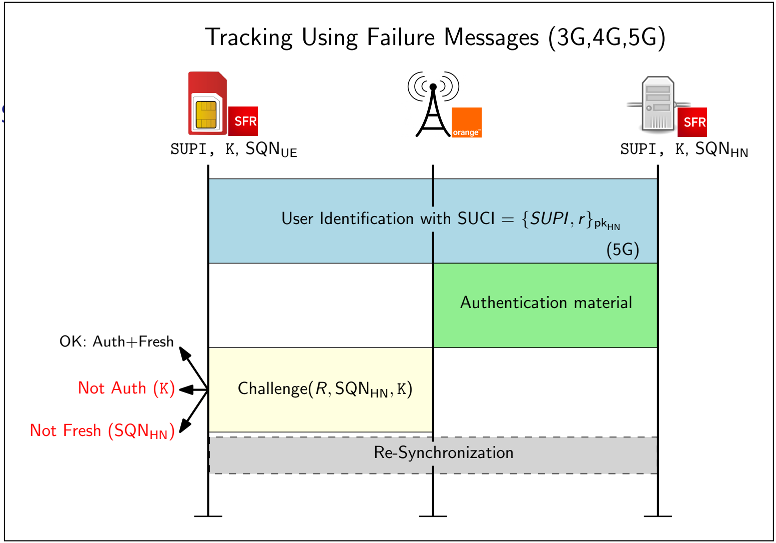


Background on Privacy

St



Background on Privacy

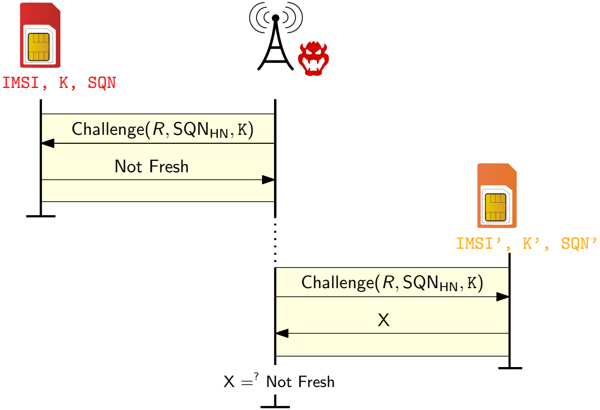


Background on Privacy

Stat

- k

Tracking Using Failure Messages (3G,4G,5G)

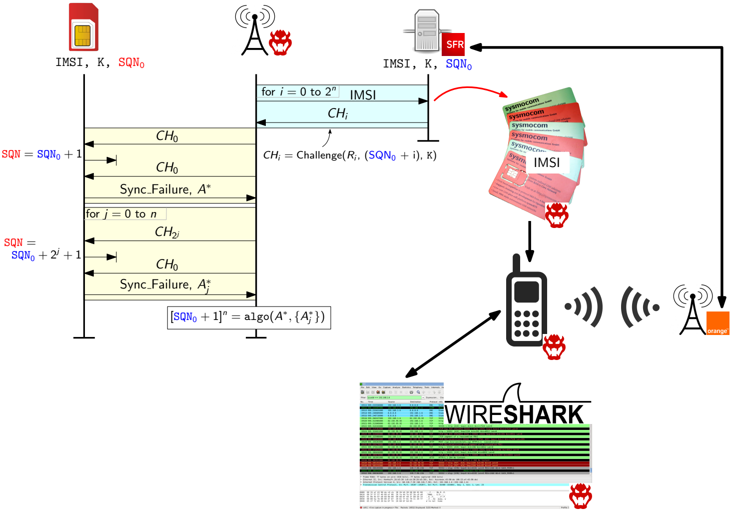


Background on Privacy

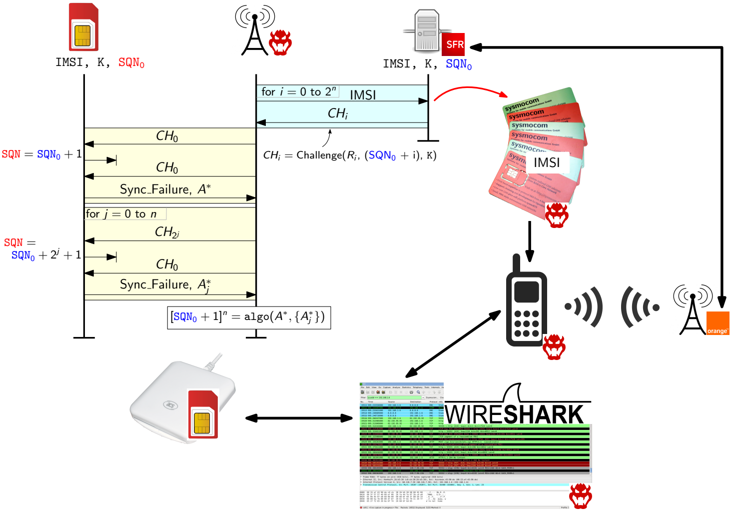
State-of-the-art

- known issues: Location Privacy
  -  can track User Equipments around his fake Base Stations
  - *e.g.* IMSI leakage, failure messages, etc..
- 4G: many proposed fixes but devices are still vulnerable
- 5G: asymmetric encryption of SUPI $\rightsquigarrow$ promise to protect privacy,
  but still vulnerable to location privacy attacks

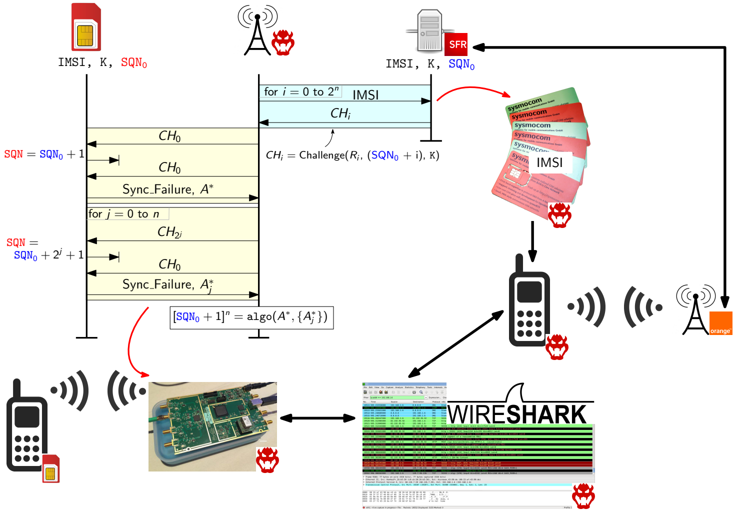
Proof of Concept: it works (done in 4G)



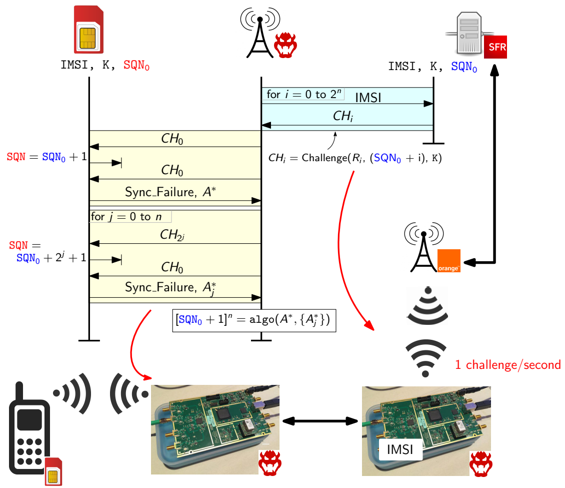
Proof of Concept: it works (done in 4G)



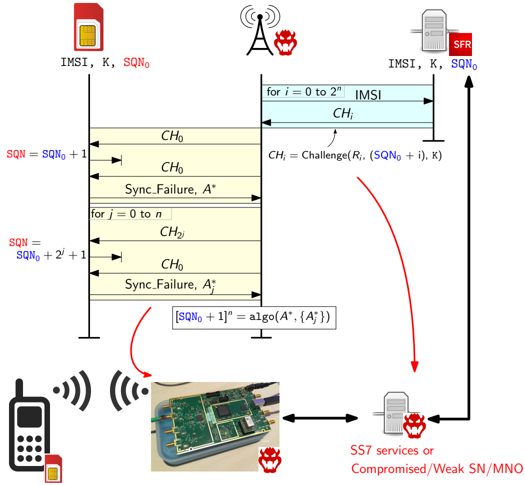
Proof of Concept: it can be exploited (done in 4G)



Proof of Concept: it can be exploited (done in 4G) (better)



Proof of Concept: it scales (?)



Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* "Achieving better privacy for the 3GPP AKA protocol." **PETS'16**.
  (new location attack, fix, and a computational proof)
- *Koustos* "The 5G-AKA Authentication Protocol Privacy" **Euro S&P'19**.
  (attack on the fix from PETS'16, fix, and computational proof)

$\leadsto$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* ”Achieving better privacy for the 3GPP AKA protocol.” **PETS’16**.
  (new location attack, fix, and a computational proof)
- *Koustos* “The 5G-AKA Authentication Protocol Privacy” **Euro S&P’19**.
  (attack on the fix from PETS’16, fix, and computational proof)

$\rightsquigarrow$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* ”New privacy issues in mobile telephony: fix and verification.” **CCS’12**. (failure messages attack and fix with `aenc`)
- *O’Hanlon, Borgaonkar, Hirschi.* “Mobile subscriber WiFi privacy.” **S&P Workshops’12**.
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses of AKA (*e.g.* with DeepSec) as benchmarks but not faithful to the original protocol

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* "Achieving better privacy for the 3GPP AKA protocol." **PETS'16**.
  (new location attack, fix, and a computational proof)
- *Koustos* "The 5G-AKA Authentication Protocol Privacy" **Euro S&P'19**.
  (attack on the fix from PETS'16, fix, and computational proof)

$\leadsto$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* "New privacy issues in mobile telephony: fix and verification." **CCS'12**. (failure messages attack and fix with $\mathtt{aenc}$)
- *O'Hanlon, Borgaonkar, Hirschi.* "Mobile subscriber WiFi privacy." **S&P Workshops'12**.
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses of AKA (*e.g.* with DeepSec) as benchmarks but not faithful to the original protocol

$\leadsto$ Only for finding an attack *a posteriori*. (+ extremely weak proofs)
$\leadsto$ Even then, none of the analyses is faithful to the original protocol (stateful and $\oplus$).

Prior Privacy Formal Analyses of AKA

Manual Analyses:

- *Fouque, Onete, Richard.* "Achieving better privacy for the 3GPP AKA protocol." **PETS'16**.
  (new location attack, fix, and a computational proof)
- *Koustos* "The 5G-AKA Authentication Protocol Privacy" **Euro S&P'19**.
  (attack on the fix from PETS'16, fix, and computational proof)

$\rightsquigarrow$ Extremely complex proofs, hard to check, hard to adapt (for more practical fix?).

Automated Analyses:

- *Arapinis, Mancini, Ritter, Ryan, Golde, Redon, Borgaonkar.* "New privacy issues in mobile telephony: fix and verification." **CCS'12**. (failure messages attack and fix with aenc)
- *O'Hanlon, Borgaonkar, Hirschi.* "Mobile subscriber WiFi privacy." **S&P Workshops'12**.
  (Wifi-based IMSI-catchers, weak model for AKA, new attack found on EAP-SIM)
- other analyses of AKA (*e.g.* with DeepSec) as benchmarks but not faithful to the original protocol

$\rightsquigarrow$ Only for finding an attack *a posteriori*. (+ extremely weak proofs)
$\rightsquigarrow$ Even then, none of the analyses is faithful to the original protocol (stateful and $\oplus$).

We also tried ourselves (partial results in the 2 papers) but we failed: we found the linkability attacks and the SQN leakage attack in 5G but only for models tailored for the attacks. No succesful analysis for the full protocol.