A Formal Analysis of 5G Authentication

CCS'18

David Basin, Jannik Dreier, Lucca Hirschi,
Saša Radomirovic, Ralf Sasse, Vincent Stettler

October 18, 2018

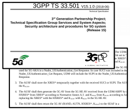
Designing Security Protocols

Smart people

e.g., IETF

Discussion

Standard



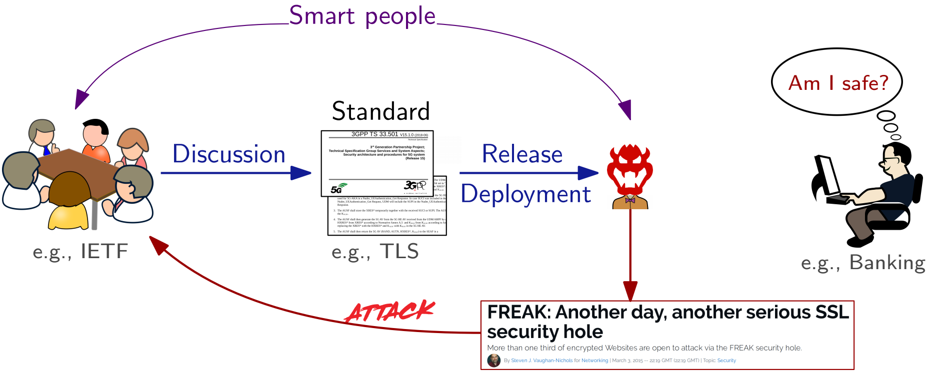
e.g., TLS

Release

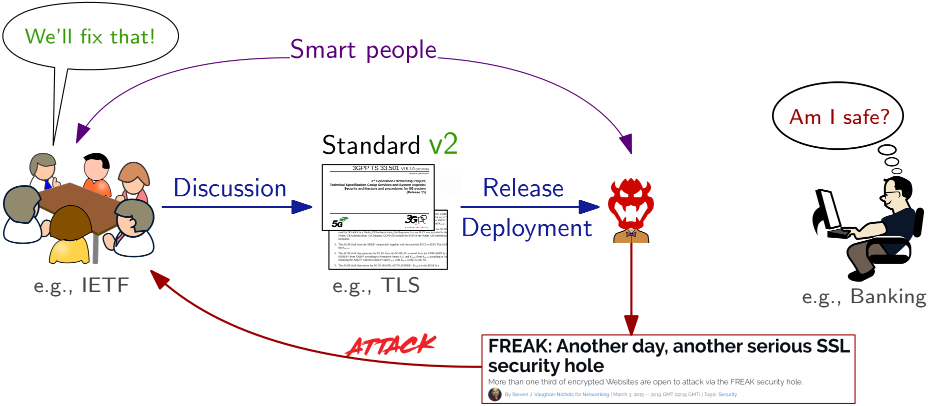
Deployment

e.g., Banking

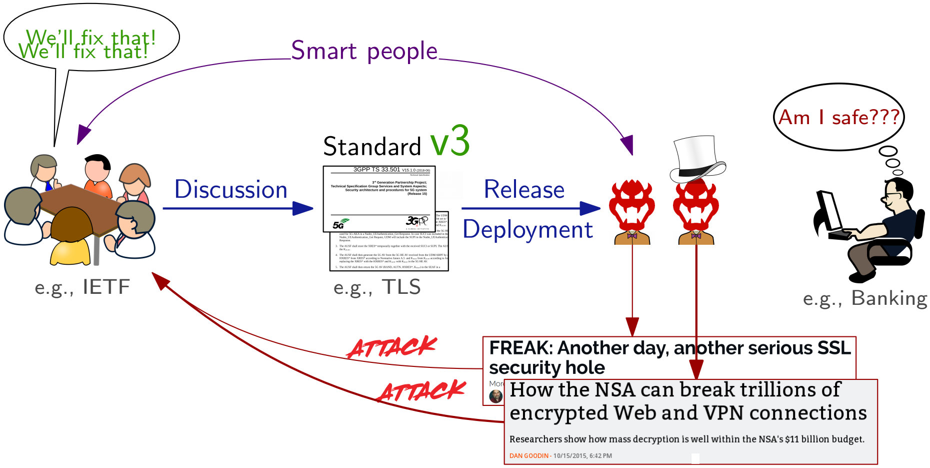
Designing Security Protocols



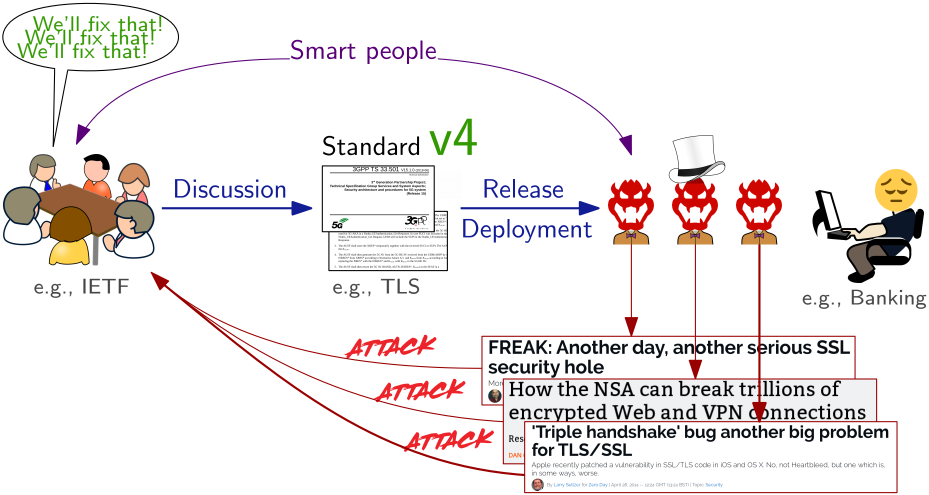
Designing Security Protocols



Designing Security Protocols



Designing Security Protocols



Designing Security Protocols

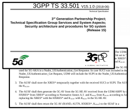
Both are smart people

But asymmetric fight:
- weakest link
- active adversary exploiting insecure network
- concurrency + backward compatibility + ...

e.g., IETF

Discussion

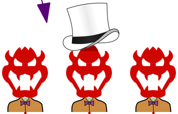
Standard v4



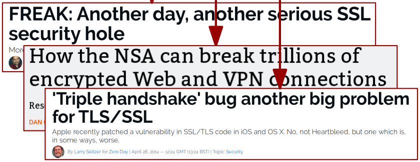
e.g., TLS

Release

Deployment



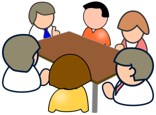
e.g., Banking



Designing Security Protocols

Both are smart people

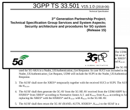
But asymmetric fight:
- weakest link
- active adversary exploiting insecure network
- concurrency + backward compatibility + . . .



e.g., IETF

Discussion

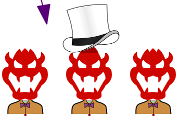
Standard v4



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

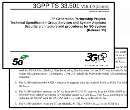
Designing Security Protocols

Smart people

???????

Discussion

Standard



e.g., TLS

Release

Deployment

e.g., Banking

ATTACK

Formal Verifier

$S \models P$?

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**

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 $\rightsquigarrow$ 4G:EPS AKA $\rightsquigarrow$ 5G:5G AKA

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 $\rightsquigarrow$ 4G:EPS AKA $\rightsquigarrow$ 5G:5G AKA

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

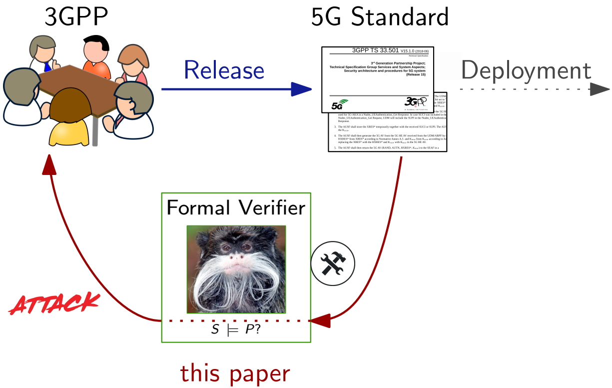
Let's formally analyze 5G AKA!

5G Authentication

5G AKA intended to improve security but:

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

Let's formally analyze 5G AKA!



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

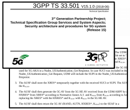
Sweet spot between precision and automation

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

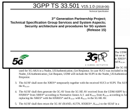
- architecture and process spec.
- system assumptions and threat model (environment)
- security goals

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

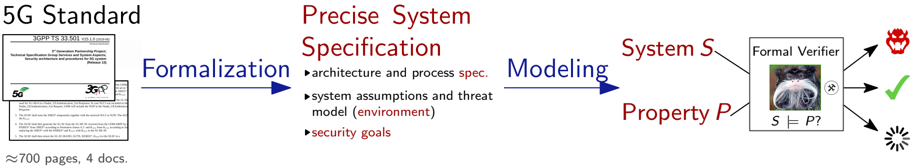
Formalization

- 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



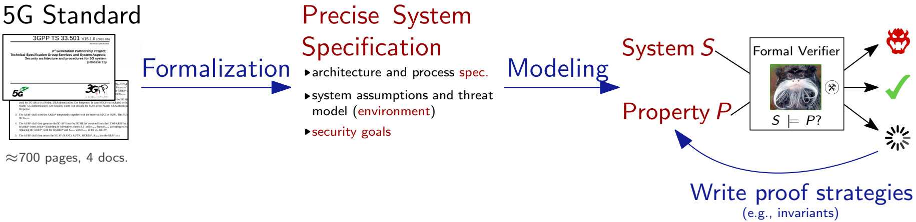
Formalization

- 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

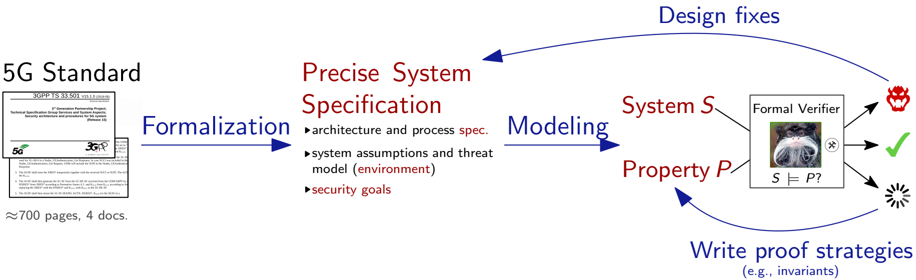
Modeling

- 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

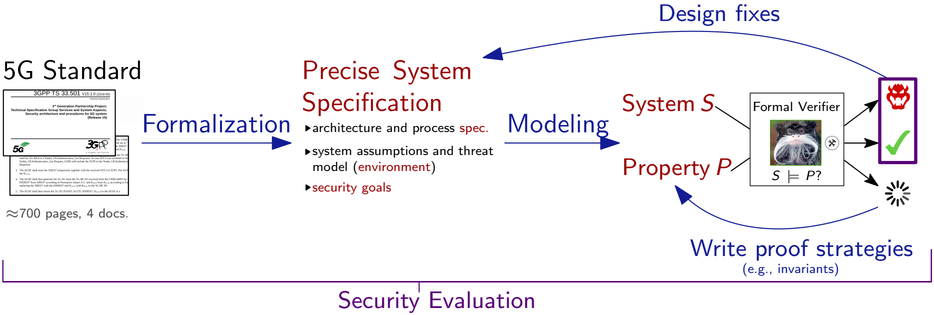
- large, complex protocol with intricate state-machine
- encode security goals under many threat models

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

Formalization of the 5G standard

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

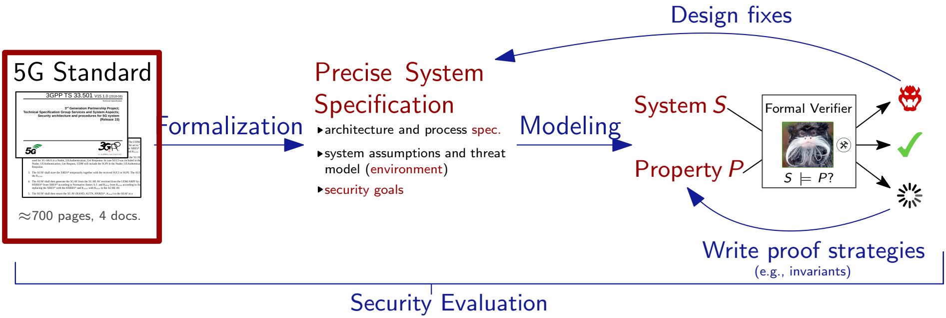
Formal model of 5G AKA amenable to automation

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

Security Evaluation of 5G AKA

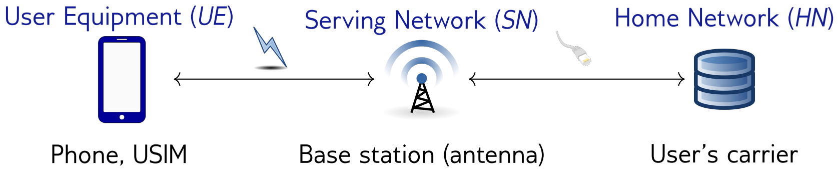
- Identify minimal assumptions required for each security goal to hold:
  - Authentication: critical properties are violated
  - Privacy: preserved for passive but broken for active
  - Secrecy: holds but not Perfect Forward Secrecy
- Explicit recommendations and provably secure fixes (also simplify)

Outline



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

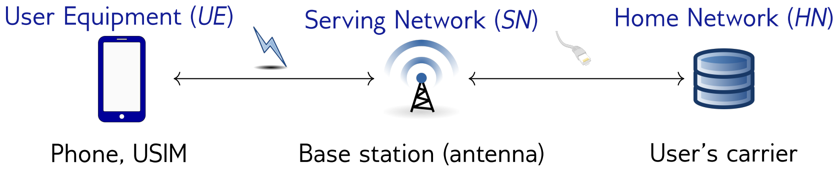
5G AKA



5G AKA designed to:

- **mutually authenticate** User Equipment with its Home Network (carrier)
- **establish session keys** btw. the User Equipment and its Serving Network

5G AKA



5G AKA designed to:

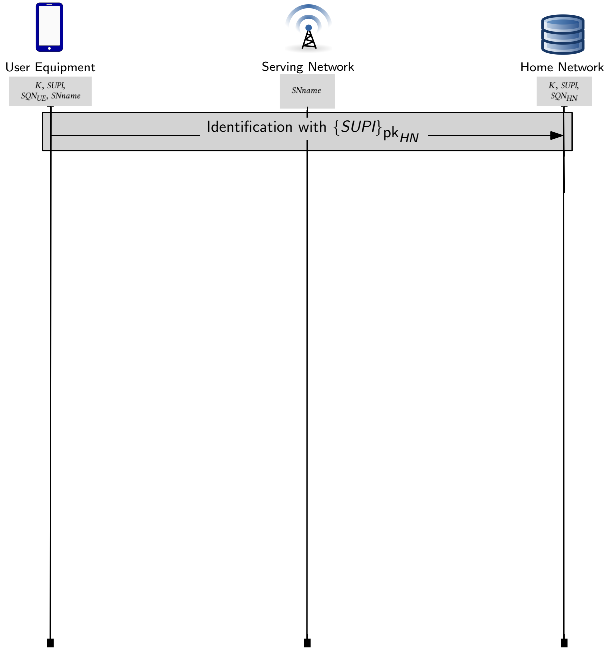
- **mutually authenticate** User Equipment with its Home Network (carrier)
- **establish session keys** btw. the User Equipment and its Serving Network

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

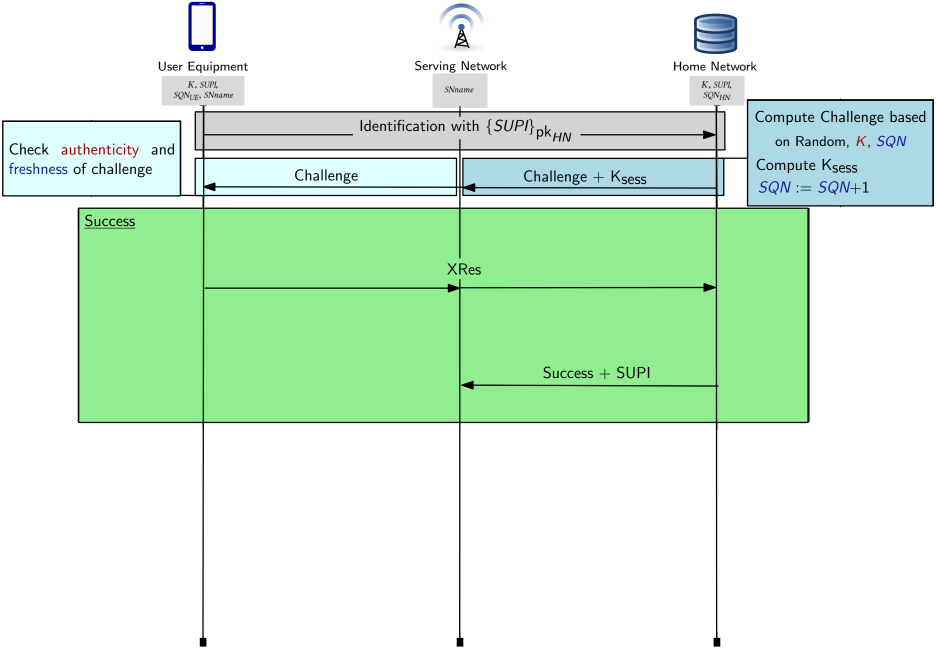
- a permanent *UE*'s **identifier** *SUPI* (for identification)
- a **symmetric key** K (shared secret)
- a **sequence number** *SQN* (for replay protection)

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

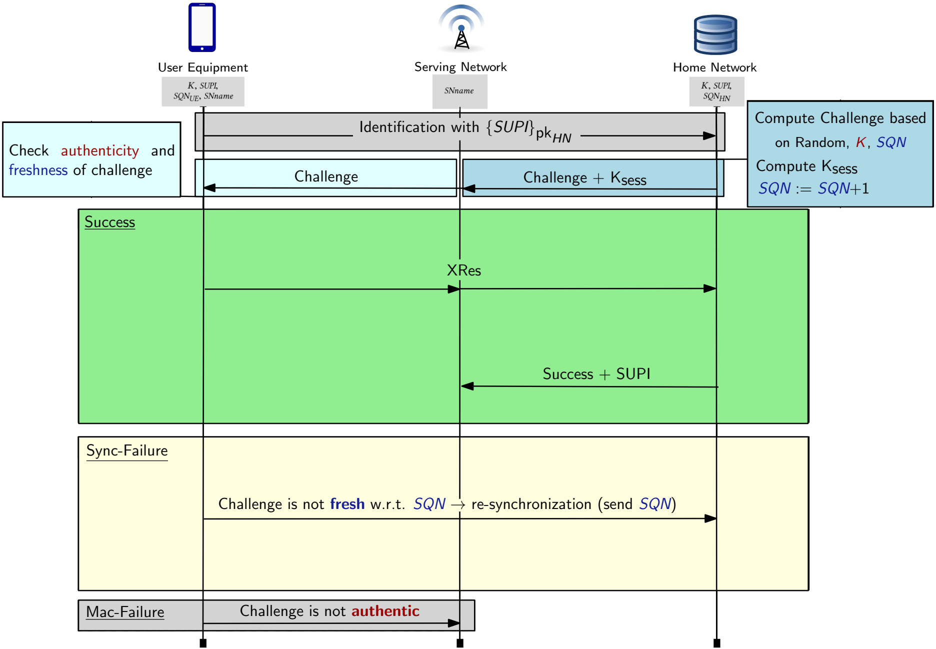
5G AKA (cont.)


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

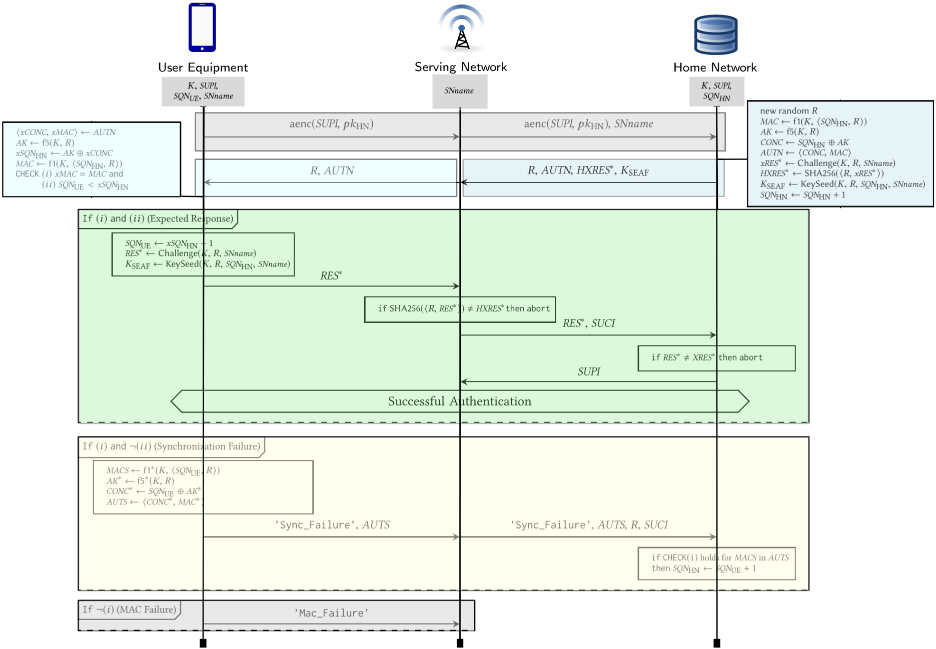
5G AKA (cont.)


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

5G AKA (cont.)

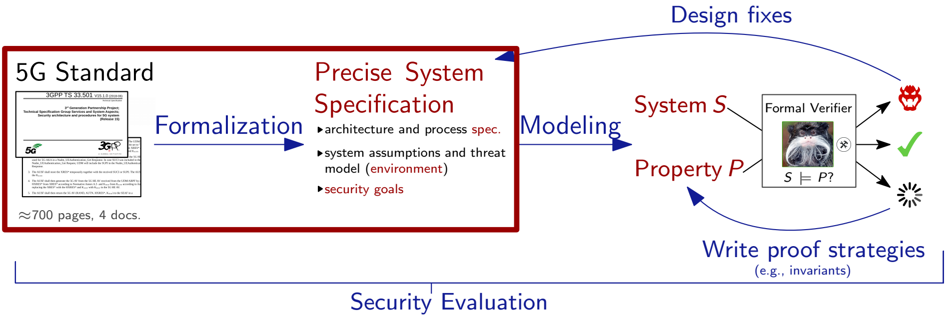

User Equipment
K, SUPI, SQN_UE, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_HN
Identification with {SUPI}pk_HN
Check authenticity and freshness of challenge
Challenge
Challenge + K_sess
Compute Challenge based on Random, K, SQN
Compute K_sess
SQN := SQN+1
Success
XRes
Success + SUPI
Sync-Failure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

5G AKA (cont.)



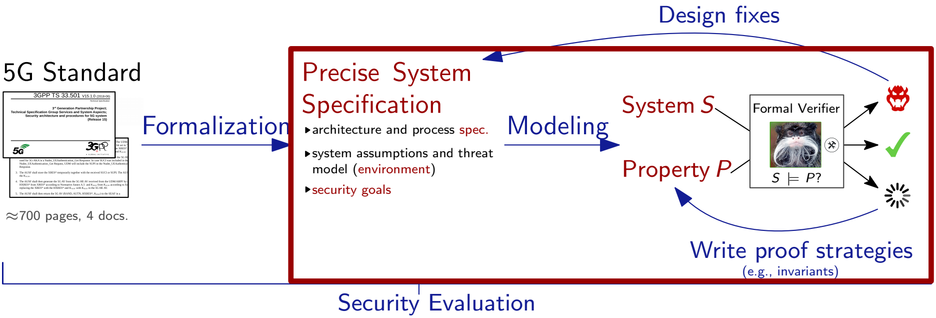
User Equipment
K, SUPI, SQN_UE, SNname
Serving Network
SNname
Home Network
K, SUPI, SQN_HN
new random R
MAC ← f1(K, ⟨SQN_HN, R⟩)
AK ← f5(K, R)
CONC ← SQN_HN ⊕ AK
AUTN ← ⟨CONC, MAC⟩
xRES* ← Challenge(K, R, SNname)
HXRES* ← SHA256(⟨R, xRES*⟩)
K_SEAF ← KeySeed(K, R, SQN_HN, SNname)
SQN_HN ← SQN_HN + 1
aenc(SUPI, pk_HN)
aenc(SUPI, pk_HN), SNname
R, AUTN
R, AUTN, HXRES*, K_SEAF
⟨xCONC, xMAC⟩ ← AUTN
AK ← f5(K, R)
xSQN_HN ← AK ⊕ xCONC
MAC ← f1(K, ⟨xSQN_HN, R⟩)
CHECK (i) xMAC = MAC and
(ii) SQN_UE < xSQN_HN
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
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'

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

Outline



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

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

Formal Modeling

System ~500LoC

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

Threat Model & Security Goals ~1000LoC, 124 lemmas

- powerful Dolev Yao: control all the network
- 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

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

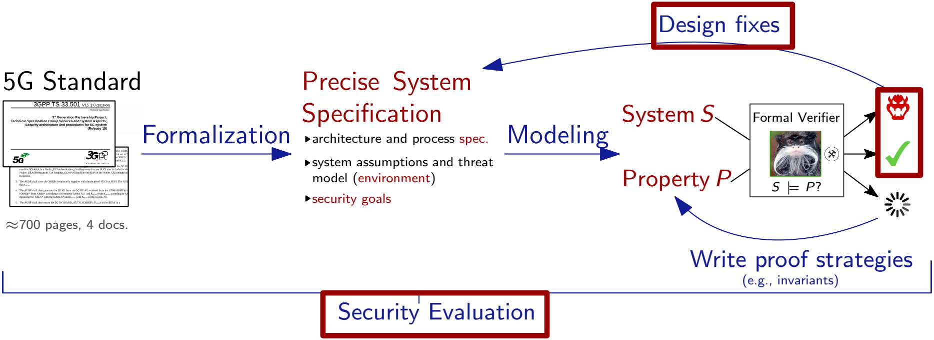
Threat Model & Security Goals ~1000LoC, 124 lemmas

- powerful Dolev Yao: control all the network
- 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

Outline


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

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: 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 $SN \xleftarrow{\mathit{SUPI}} HN$ 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?

- $SN \xleftarrow{\text{Challenge+K}_{\text{sess}}} HN$ 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 $\rightsquigarrow$ ✓

(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	UE	SN
Partner	SN	UE
Weak agreement	$[\neg K \wedge \text{key-conf} \wedge \neg \text{ch}]$	$[\neg K \wedge \neg \text{ch}]$

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(K_{sess}, K) holds but not PFS(K_{sess})

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

- defeats IMSI-catchers but
- **insufficient** to ensure **untraceability** with an active: Attack 3
- fix requires major redesign ☹

$\leadsto$ new 5G tracking device ("5G-Stingray") coming?

Conclusion

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: they will modify the standard.

Conclusion

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: they will modify the standard.

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)
- more precise/efficient verification of privacy

Conclusion

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 ☹

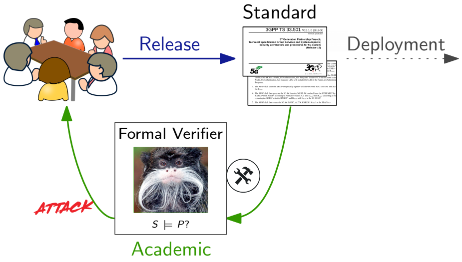
We have an ongoing discussion with 3GPP and GSMA: they will modify the standard.

Future work:

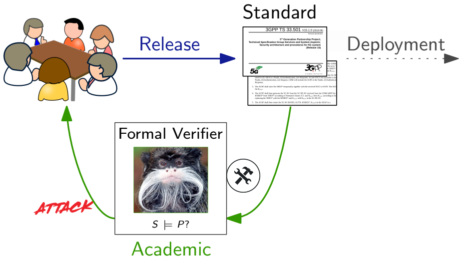
- verify and formally compare other variants of AKA (3G, 4G, EAP-AKA' in 5G)
- follow the development of 5G (*e.g.* phase 2)
- more precise/efficient verification of privacy

Others' future work: Formal Methods are a powerful tool! They are now mature enough for the real-world. ☺ Let's use them! ☺

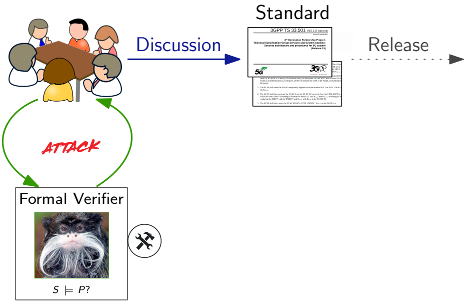
Now:


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

Now:

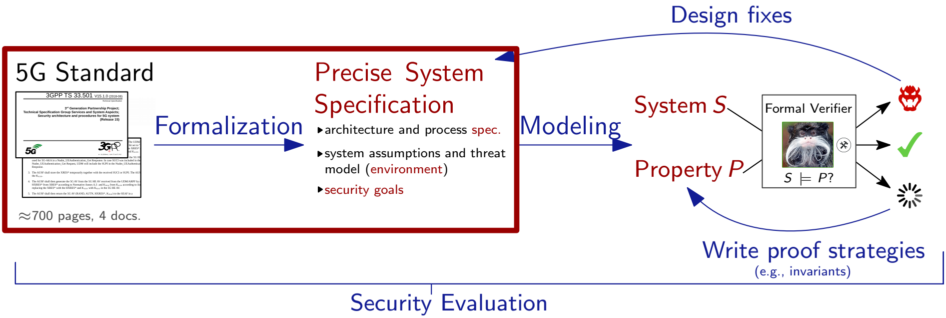

Release
Standard
3GPP TS 33.501
Deployment
Formal Verifier
$S \models P$?
ATTACK
Academic

Ideally:


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

Backup Slides

Outline



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. [...] This authorization is 'implicit' in the sense that it is implied by a successful authentication and key agreement run.

$\leadsto$

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

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. [...] This authorization is 'implicit' in the sense that it is implied by a successful authentication and key agreement run.

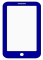
$\rightsquigarrow$

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

Takeaways

- critical security goals are missing (implicit?): *e.g.* injective agreement on the key seed
- some stated goals are two 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)

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 does *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 does *UE* obtain regarding *HN*?

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

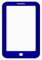
Authentication: definitions

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 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}

Authentication: definitions

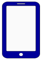


Point of view	*UE*				*SN*		*HN*	
Partner	*SN*		*HN*		*UE*	*HN*	*UE*	*SN*
Agreement	NI	I	NI	I				
on K_{sess}	?	?	?	?		[...]		
on *SUPI*	?	?	?	?				
on *SNname*	?	?	?	?				
Weak agree.	?	?	?	?				

Authentication depends on the perspective and the expected agreement:
What guarantees 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)

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	$\neg K \wedge \neg$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	

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$\wedge \neg$ch	$\neg K \wedge$key-conf$\wedge \neg$ch	$\neg K \wedge \neg$ch	$\neg K \wedge \neg$ch
Weak agreement	[$\neg K \wedge$key-conf$\wedge \neg$ch]		[$\neg K \wedge \neg$ch]	

Other Results

Secrecy:

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

*: 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.