A Formal Analysis of 5G Authentication

Presented by: Jake Ginesin

Background 1: Dolev-Yao & Symbolic Crypto-analysis

Dolev-Yao model: a *formal*, *symbolic model* for cryptographic packet exchange

Two (main) formats:

- *Passive* attacker: attacker can only read packets
- *Active* attacker: attacker can modify packets

Both formats: *computationally decidable*

original paper: On the security of public key protocols

Background 2: The Tamarin Prover

About Tamarin:

- *Symbolic* reasoning about cryptographic protocols via the Dolev-Yao Model
- TLDR; reduces to state-space exploration (but, the book describes it as a “constraint solver”)
- Allows for trace props & safety props (i.e. LTL)

Background 3: Actually using Tamarin

How to discharge proofs?

- Automated theorem proving (pretty much model checking)
- Many heuristics to choose from
- Tactics & Proof Assistance

Tamarin on Arch? Impossible. Haskell sucks. Spent 4h trying.

Arch package (linking error) -> Make (failed) -> Stack build (failed) -> Cabal build (failed) -> diff stack/cabal versions (failed) -> installed Nix -> Nix package (failed) -> GH issue -> gave up

Intro to 5G

- 5G: Concerned with *cellular* traffic
- Standard by 3GPP group, 15.1.0 released in June 2018
- (Supposedly) improved security guarantees

Motivation and Goals

Why study 5G?

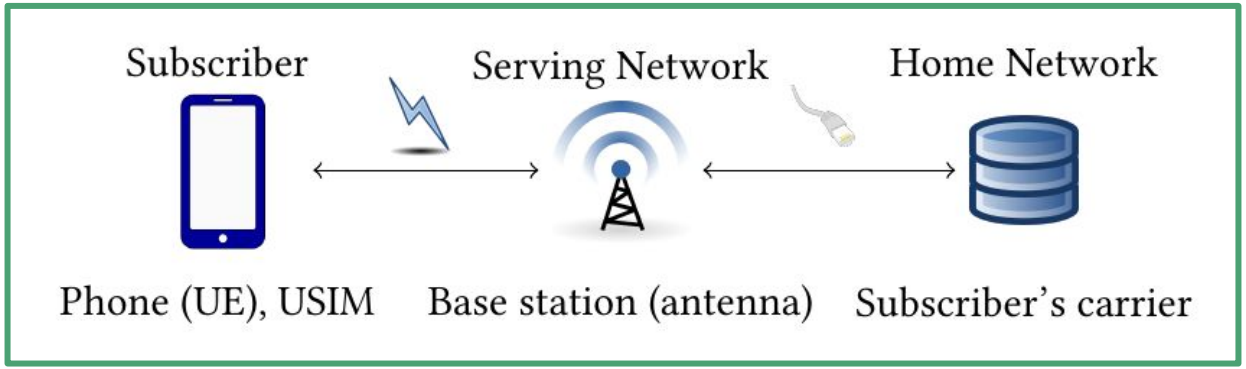
- Cellular networks have 5 billion users!?
- Authentication is extremely important (billing, etc)

But how?

- The authors assess the security guarantees of 5G under diff threat models, assumptions, etc
- A formal model of 5G, 5G AKA (auth. & key agreement)

Q1: This seems like the first 5G paper. Any other 5G papers since this one?

5G Authentication Architecture



- Serving Network <-> Home Network: perfect channel
- Subscribers have *identities*, the home network's *public key*, a long-term *symmetric key*, and a *sequence num*

Q2: Can we be sure the channel between the base station and the home network is perfect?

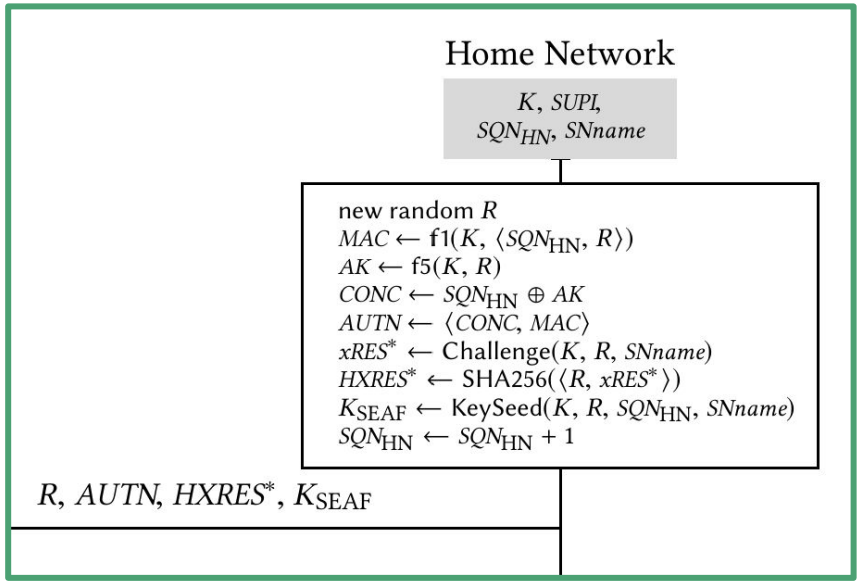
5G Authentication Architecture

For the subscriber (sub) to authenticate with the carrier...

1. The sub requests a challenge
2. The carrier generates a challenge
3. The sub verifies and responds to the challenge
4. The carrier verifies the sub’s challenge response
5. The carrier and the sub sync sequence nums

5G Authentication Architecture: The Challenge

The interesting part of the auth procedure is the challenge:



Generated and sent:

- The challenge, R
- Freshness proof of the challenge, AUTN
- (Hashed) challenge solution, HXRES*
- Key seed for the secure channel, K_{SEAF}

Q3: Why is the hashed challenge sent?

Verification Taxonomy: Assumptions :D

- Dolev-Yao model is justified because 5G is over the air
- Cryptographic primitives (hashing, key derivation) are assumed secure
- Serving Networks (the antennas) can be compromised!
- Subscriber deets are *initially* confidential

This paper uses the language ‘minimal assumptions’ etc

Verification Taxonomy: Properties (Authentication)

Props:

- Authentication can only be successful iff subs are authorized by home network
- The serving network can authenticate subs, and vice versa
- Serving networks can only authenticate subs that are authorized by their home network

Q4: What is the formal definition of authentication? Satisfying a challenge?
Q5: Can the first property be considered authentication soundness?

Verification Taxonomy: Properties (Confidentiality)

- Session keys remain confidential, even if previous session keys are compromised
- Secure channel key seeds are confidential
- No session key is established twice

Verification Taxonomy: Properties (Privacy)

- User identity and location should remain confidential, thus..
- A *passive* attacker should not be able to find the sequence number nor the subscriber's private info

But this is only required for a passive attacker!!

Unspecified security goals

Security properties that should have been included, according to the authors:

- Authentication and Agreement of the Key Seed for the constructed secure channel

Tamarin Model

- Authors created a Tamarin model of 5G AKA
- Considered compromise scenarios: secret key, sequence number, and subscriber info reveals
- Various simplifications: no message bit lengths, no sub-messages, no authentication token expiry

Q6: I didn’t check out the model super deeply. Thoughts on the simplifications?

Proof Strategies

Reasoning about 5G is hard:

- Sequence numbers use XOR, which is algebraic
- The protocol itself is large (approx. 500 LoC)

So, the verification took:

- 124 intermediate (helping) lemmas
- Complex proof strategies (approx. 1000 LoC)
- 5 hours of computation

Q7: Is reasoning about algebraic structure (e.g. XOR) decidable?

Results: Authentication

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_{SEAF}	✗	✗	$\neg K \wedge$k-c	$\neg K \wedge$k-c	✗	✗	$\neg$ch	$\neg K \wedge \neg$ch	$\neg K$	$\neg K$	$\neg$ch	$\neg$ch
on *SUPI*	wa	×	wa	×	wa	×	[$\neg$ch]	×	wa	×	×	×
on *SNname*	wa	×	[$\neg K \wedge$k-c]	×	wa	×	wa	×	[$\neg K$]	×	wa	×
Weak agreement	[✗]		$\neg K$		[$\neg K \wedge \neg$ch]		$\neg$ch		$\neg K$		$\neg$ch	

The results are in terms of *minimal assumptions* required for *authentication* properties to hold

Note: Tamarin used an active attacker

- UE: Subscribers
- SN: Serving Network
- HN: Home Network
- K: whether or not key seed is revealed
- ch: compromised channel
- k-c: key confirmation phase
- NI: Non-injective, I: Injective (key seed)
- Wa: weak agreement
- Supi: Subscriber information
- SNname: identifier for SN

Results: Secrecy

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

- Minimal assumptions required for *secrecy* properties to hold
- PFS: Perfect forward secrecy

Results: Authentication given binding channel

P.o.V.	*UE*		*SN*	
Partner	*SN*		*UE*	
Agre.	NI	I	NI	I
on K_{SEAF}	$\neg K \wedge$k-c$\wedge \neg$ch	$\neg K \wedge$k-c$\wedge \neg$ch	$\neg K \wedge \neg$ch	$\neg K \wedge \neg$ch
Weak agre.	[$\neg K \wedge$k-c$\wedge \neg$ch]		[$\neg K \wedge \neg$ch]	

Q8: What is a binding channel?

Takeaways from Results

- Missing security assumptions, namely key seed agreement, prevented lots of properties from holding
- Even with this assumption, many props don’t hold
- Many more specific recommendations (differing to the paper for this)

Any questions/Closing Thoughts?