Security Issues in the 5G Standard and How Formal Methods Come to the Rescue

Lucca Hirschi, Ralf Sasse, Jannik Dreier

Security Issues in the 5G Standard and How Formal Methods Come to the Rescue

by Lucca Hirschi (Inria & LORIA), Ralf Sasse (ETH Zurich) and Jannik Dreier (Université de Lorraine & LORIA)

Our recent academic research has identified several serious security and privacy issues in the 5G standard. These issues were discovered with the help of security protocol verification tools based on formal methods, which are now mature enough to meet industry-level standards. We thus advocate for their systematic use in critical standardisation processes, such as mobile communication and e-voting.

Our intensive daily use of cell phones and other mobile devices relies on the capacity of our devices to connect to carriers which serve us internet data, calls, and SMSs. When sending/ receiving calls/texts or browsing the web, phones and corresponding networks need authentication (whom to bill?) and confidentiality (privacy) mechanisms for securely exchanging user data over-the-air. Since the advent of 3G, this has been achieved worldwide through a protocol called Authentication and Key Agreement (AKA), standardised by 3GPP. 3GPP claims that the 5G version of AKA (5G AKA) provides better security and privacy guarantees than previous iterations, but there exists very little evidence to support this claim. Two of our recent works [1, 2] have identified critical security and privacy shortcomings in 5G AKA and indicate that use of formal methods and verification tools could have avoided this situation and should be used early in the design process in the future. This effort is the outcome of past and ongoing collaborations [L2, L5, L6] with different research teams.

5G AKA does not meet its Security Goals

A comprehensive, formal security evaluation of the 5G AKA protocol [1], reveals that 5G AKA does not meet two critical security goals: an attacker can either impersonate a serving network towards a mobile, or a mobile towards a network.

Our methodology is as follows [L1] (see Figure 1):

- We extract precise requirements from the 3GPP standards defining 5G and we identify key missing security goals as well as flaws in the stated goals.
- Using the security protocol verification tool Tamarin, we conduct a full, systematic, security evaluation of the protocol with respect to the 5G security goals.
- Our evaluation automatically identifies the minimal security assumptions required for each security goal and we automatically find that the aforementioned security goals are not met, except under additional assumptions missing from the standard.
- Finally, we make explicit recommendations with provably secure fixes for the attacks and weaknesses we found.

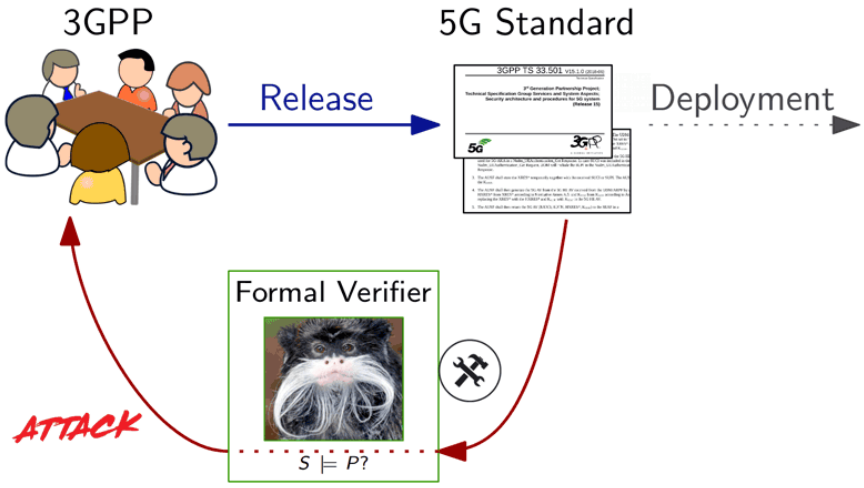

Figure 1: Formal verification workflow. The Tamarin picture refers to a state-of-the-art verifier.

A new vulnerability has been identified in all generations of AKA, including 5G AKA,; in fact, 5G AKA can be leveraged to breach subscriber privacy more severely than known location privacy attacks, e.g., IMSI catchers [2]. Namely, [2] shows for the first time how an attacker can learn 3G, 4G, and 5G subscribers' typical activity patterns including number of calls and SMSs sent in a timeframe. We stress that these activity patterns can be monitored long-time and remotely even if subscribers are outside attacked areas most of the time. Moreover, IMSI-catcher attacks have been mitigated in 5G through the use of randomised encryption for protecting subscribers' identities. [2] shows that other attack vectors will be at the disposal of attackers to locate and monitor subscribers.

Impact

Our research reveals that the specification, serving as deployment basis, of 5G networks does not meet critical security goals. This can lead to a flawed deployment of 5G networks that may suffer from attacks. It is very likely that all 5G subscribers will be subject to the aforementioned attacks, a situation that has already drawn the attention of news media [L3, L4]. It turns out that it is also possible for a poor standard-conform implementation to result in users being charged for the mobile phone usage of a third party, due to a lack of authentication. We proposed an improvement that removes this flaw. It is now advisable for 3GPP to integrate our recommendations in order to reduce the risk of flawed deployments and to mitigate the privacy threats for future generations. We have communicated our findings to 3GPP and GSM Association (GSMA) (see the acknowledgments [L1]), and we are in communication regarding possible fixes and improvements.

We stress that potential remedies must be standardised. Having them only deployed by some network providers does not meet our expectations of a global standard.

Mandating the Use of Formal Methods and Verifiers

Our security evaluation is made possible by improvements in automated tools based on mathematical principles, such as the Tamarin or ProVerif verifiers for security protocol analysis. Our resulting security guarantees are machine-checked and based on a solid mathematical foundation. From different lines of research in the area numerous verification tools are now capable of analysing various security properties. This has led to numerous large-scale formal analyses of standard properties on real-life protocols recently, e.g., TLS 1.3 and the Signal instant messaging protocol. Some of those analyses have led designers and standardisation bodies to correct flawed protocols. It is safe to say that existing techniques for automated security verification have now reached maturity to guide design, analysis, and standardisation. We have the encouraging example

of the TLS Working Group adopting an “analysis-prior-to-deployment” paradigm for drafting TLS 1.3 with notable efforts from the academic community, and the example of the Swiss government mandating the use of such techniques for e-voting systems [L7].

We intend to continue to bring mathematical reasoning to the security protocol design process. We hope that 3GPP and other standardisation bodies also plan to bring verification tools to their decision process. Possible future targets are the new wireless standard WPA3, as well as e-voting schemes being prepared in different countries.

[1] is a joint work with: David Basin (ETH Zurich), Jannik Dreier (Université de Lorraine & LORIA), Lucca Hirschi (Inria & LORIA), Saša Radomirović (University of Dundee), Ralf Sasse (ETH Zurich), Vincent Stettler (ETH Zurich).
[2] is a joint work with: Ravishankar Borgaonkar (SINTEF Digital), Lucca Hirschi (Inria & LORIA), Shinjo Park (TU Berlin), and Altaf Shaik (TU Berlin).

References:

[1] D. Basin, et al.: “A Formal Analysis of 5G Authentication. ACM CCS, 2018.
[2] R. Borgaonkar, et al.: New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. PETS, 2019.

Please contact:

Lucca Hirschi
Inria & LORIA, France
lucca.hirschi@inria.fr