Investigating and Improving Privacy in the 5G Authentication and Key Agreement Protocol (5G-AKA)

April 16, 2024

1 Introduction

Each User Equipment (UE) seeking connection to a 5G network must undergo stringent authentication to ensure the integrity of the network and prevent unauthorized access to fraudulent base stations. Given the inherently distributed architecture of 5G networks[1], preserving the confidentiality of authentication keys and securing traffic encryption are paramount. Consequently, the 3rd Generation Partnership Project (3GPP) has devised the 5G Authentication and Key Agreement Protocol(AKA)[2]. The 5G-AKA procedure [3] reveals potential privacy concerns during UE authentication, when the user is roaming to (international) serving networks.

This project will investigate these concerns by implementing the 5G AKA protocol in a test environment. The task then is to identify and address the potential privacy vulnerabilities, and develop and test a protocol variant with enhanced privacy."

2 Obejctives

- To explore potential privacy vulnerabilities in the 5G AKA protocol
- To analyze the effectiveness of the claimed 5G AKA privacy.
- To propose improvements or alternative solutions to mitigate identified privacy risks.
- to develop, implement, and test the suggested improvements.

3 Methodology

The main methodology will be implementations, emulations, and actual measurements of the systems and protocols. The chair already runs a 5G emulation testbed, upon which the student can build. The current privacy vulnerability is due to a fundamental misdesign in the protocol, so there is no need for formal verification or protocol fuzzing, or any other advanced vulnerability detection approach.

The empirical part will consist of three different steps

- Protocol Implementation: Implement the 5G AKA protocol within a controlled test-bed environment to simulate real-world scenarios.
- Privacy Analysis: demonstrate the protocol's privacy implications, identifying the vulnerabilities.
- Improvement Proposal: Based on the findings, propose enhancements or alternative approaches to strengthen privacy protections within the 5G AKA protocol, and demonstrate effectiveness in the testbed.

4 Expected Outcomes

- A comprehensive understanding of privacy challenges associated with 5G authentication protocols.
- Demonstration of specific privacy vulnerabilities within the 5G AKA protocol.
- Demonstration of the improvements or modifications of the protocol to enhance privacy.

5 Conclusion

The proposed project aims to shed light on privacy challenges within 5G AKA authentication protocols. By systematically analyzing privacy issue and proposing enhancements, this research will contribute to the development of more robust and privacy-respecting 5G networks.

References

[1] 3GPP, "5g; system architecture for the 5g system (5gs) (3gpp ts 23.501 version 16.6.0 release 16)," 2020.

[2] 3GPP, "Security architecture and procedures for 5g system, (3gpp ts 33.501 version 16.3.0 release 16)," 2020.

[3] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, (New York, NY, USA), p. 1383–1396, Association for Computing Machinery, 2018.