5G-AKA: A Formal Verification

David Clayton and Ira Harmon

November 29, 2018

Abstract: The 5th generation of cell phone technology is scheduled to be deployed by 2021. It will connect more people around the world than any prior generation. The 5G protocol suite includes modifications of existing protocols as well as new protocols. However, the foundation of 5G security rest upon the 5G-AKA protocol. Since inception, 5G-AKA has gone through multiple revisions due to discovered vulnerabilities. In this paper the most recent version of the protocol is tested through symbolic analysis and recommendations are made that would improve its overall security.

1 Introduction

By 2019 over 5 Billion people are expected to own a mobile phone. Currently over 62 percent of the world population uses mobile phones. As cell phones become more pervasive their use touches every aspect of modern life: Facebook updates, news, and banking transactions are all increasingly done via cell. At this critical time in the evolution of cellular technology, 3GPP, the body that standardizes cell phone protocols is preparing to deploy 5G. And while 5G promises to connect more users with better service than previous generations, the unrestrained growth of the technology makes the security implications of 5G critical. 5G-AKA (Authentication and Key Agreement) is the first line of defense in securing mobile communications. The protocol authenticates the user and distributes long term keys. The most recent version of the protocol is outlined in 3GPP Publication TS 33.501 V15.2.0. In this paper we validate the most recent version of the protocol through symbolic analysis.

2 Related Work

The Tamarin-Prover is software for the symbolic analysis and verification of security protocols. It allows the user to outline the workings of a protocol and The protocol serves two purposes to distribute authenticate the user and distribute keys between the user and the serving network.

References

[1] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1383–1396. ACM, 2018.

[2] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, and Thyla van der Merwe. A comprehensive symbolic analysis of tls 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1773–1788. ACM, 2017.

[3] Martin Dehnel-Wild and Cas Cremers. Security vulnerability in 5g-aka draft (3gpp ts 33.501 draft v0.7.0). Available at https://www.cs.ox.ac.uk/5G-analysis/(2018/02/08).

[4] Roger Piqueras Jover and Vuk Marojevic. Security and protocol exploit analysis of the 5g specifications. *arXiv preprint arXiv:1809.06925*, 2018.

[5] Anand R Prasad, Sivabalan Arumugam, B Sheeba, and Alf Zugenmaier. 3gpp 5g security. *Journal of ICT Standardization*, 6(1):137–158, 2018.