2022 SaTC PI Meeting
NextG and Wireless Security Breakout Report
Chairs: Syed Hussain (Penn State) and Brad Reaves (NC State)
Scribe: Taqi Raza (U.of Arizona)

This document reflects the discussions and conclusions of the NextG and Wireless Security Breakout Session at the 2022 SaTC PI Meeting after 2.5 hours of small and full-group discussions.

Societal and Intellectual Importance

Cellular networks are used by virtually every human, and increasingly for machine-to-machine communications including critical infrastructure. They are vital to the proper functioning of modern society. They are essential, but also essentially complex in order to support the high demands of availability, mobility, and performance.

5G and its successors drastically increase performance and flexibility with the aim of being more and more central to society. Securing these systems poses unique challenges that will require close collaboration across all areas of computing, including hardware, communications, software, applications, and networking.

We believe that sponsoring research to secure current and next-generation wireless systems is one of the most high-impact opportunities available to funding agencies.

Pressing Challenges

- *High barriers to entry:* Cellular security research is difficult to conduct due to a lack of educational materials, PI experience in cellular, the vast complexity of these networks, and relatively high costs for specialized equipment. Current network testbeds, such as NSF's AERPAW, are equipped for non-adversarial experimentation, making it unsuitable for security research.
- *Legacy Interoperability:* Cellular networks must coexist and interoperate with older and less secure standards. Protecting subscribers and providers from downgrade attacks or the other vulnerabilities of legacy infrastructure (e.g., SS7 signaling) is of paramount importance.
- *Privacy:* Subscribers deserve privacy from surveillance from their provider, interactive services, and active or passive eavesdroppers. The main existing mechanism, temporary subscriber identifiers, has been repeatedly shown to be inadequate to prevent third party location tracking or other privacy invasions. NextG anticipates new sensing modalities that take advantage of properties of mMWave transmission, yet little is understood of the privacy risks of such technology.
- *Implementation and deployment changes:* In contrast to prior network generations, 5G moved away from dedicated hardware and closed-source software to open-source hardware run in elastic computing environments. Security and privacy risks of of these changes are still poorly understood, Elements from the software supply chain to novel

challenges of sharing cloud infrastructure between prioviders and other tenants must be investigated for secure wireless communications.

- *Proactive Security and Privacy:* Virtually all security problems in cellular networks have been discovered by researchers after the network design was standardized and ossified. The consequence is that security vulnerabilities persist without fixes for years. A key challenge is thus developing techniques to ensure that new protocols are secure before deployment.

Promising Directions

- *Privacy:* Making privacy a first-class citizen should be a priority for next generation wireless networks. Bridging the privacy, cryptography, and network security communities could provide provable privacy guarantees, for example.
- *Cloudification:* Examining the impact of virtualization on network functions provides opportunities for clever attacks and even more clever defenses.
- *Formal and empirical methods:* Applications of formal modeling, secure protocol design, and natural language processing to cellular standards could provide secure-by-design NextG networks that offer end-to-end guarantees.
- *Building Capacity:* To address these critical problems, we need to grow the cellular security research community to meet the magnitude of the challenges we face. NSF could support workshops, curriculum development, and creation of public security testbeds or economical private platforms.

Attendees:

Hamid Bahrami
Siddharth Greg
Guofei Gu
Ting He
Hongxin Hu
Syed Hussain
Farshad Khorrami
Kevin Kornegay
Loukas Lazos
Miriam Leeser
Alan Liu
Brad Reaves
Lan Shang
Alex Sprintson
Seaver Thorn
Nghi Tran
Patrick Traynor
Selcuk Uluagac
Alvaro Velasques
Marilyn Wolf
Maxwell Young