NextG and Wireless Security

Chairs: Syed Hussain (Penn State) and Brad Reaves (NCSU)
Scribe: Taqi Raza (U.of Arizona)

Societal and Intellectual Importance

Cellular Networks used by virtually every human, and increasingly for machine-to-machine communications including critical infrastructure.

Securing these systems poses unique challenges that will require close collaboration across all areas of computing, including hardware, communications, software, applications, and networking.

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

Pressing Challenges

Cellular security research has exceptionally **high barriers to entry**.

Cellular networks must coexist and interoperate with older and less secure standards. **How can we protect subscribers?**

Privacy for subscribers is an essential property with few and very limited mechanisms, especially given new sensing modalities.

5G moved away from dedicated hardware and closed-source software to open-source hardware run in elastic computing environments. **Security and privacy risks of virtualizing cellular infrastructure** are poorly understood.

How can we ensure protocols are **secure before deployment?**

Promising Directions

Privacy should be a first-class citizen in cellular networks. Bridging the privacy, cryptography, and network security communities could provide provable privacy guarantees.

Examining the impact of virtualization on network functions provides opportunities for **clever attacks and even more clever defenses.**

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.**

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.