DHS Science and Technology Directorate

Homeland Security
Science and Technology

SECURITY GAPS IN TELEPHONY SYSTEMS

Telephony systems are the most ubiquitous and trusted communications infrastructure in the world. In both the developed and developing worlds, these networks offer reliable audio connections that allow their subscribers to chat with distant family members, perform business transactions, and even exchange sensitive information.

Many sectors of the global economy—especially finance and infrastructure—rely on telephony systems as a critical fallback to ensure high-value transactions or significant changes to operations originate from an authorized party.

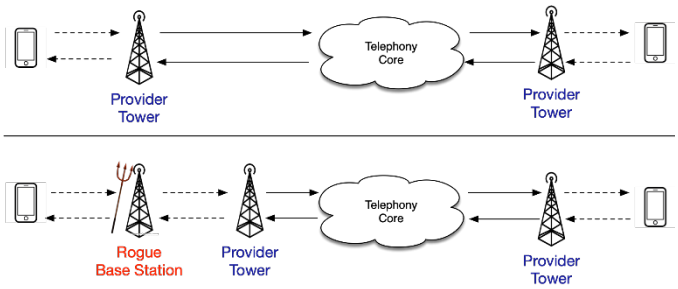
Historically, trusted service provider management issues essential mobility features to users. Broad access to core functions and equipment such as microcells invalidate such assumptions. Because of this security gap, solutions to detect and mitigate interception and user tracking by hostile third parties are critical to protect users of vulnerable infrastructure.

Securing this infrastructure—legacy, and next-generation—therefore represents a significant challenge. This effort aims to substantially improve the security of legacy and future cellular systems, specifically with regards to the interception of messages and tracking of users by hostile third parties.

DETECT/MITIGATE CALL INTERCEPTION

During its Secure and Resilient Mobile Network Infrastructure (SRMNI) project, the University of Florida R&D project is developing solutions for legacy and future cellular systems that will detect and mitigate voice call and message interception and user tracking by hostile third parties.

Tools and techniques are being develop as a mechanism to identify redirection or man-in-the-middle attacks. Additionally, the university's researchers will develop techniques for quarantining compromised devices and protect communications with encryption.



Illicit call interception depicted via a rogue base station.

IMPROVING MOBILE COMMS SECURITY

Calls and messages are not encrypted end-to-end over current or 5G cellular networks. The techniques developed through this project will assist in alerting users and operators of unsanctioned eavesdropping by hostile third parties.

The impact of these new techniques will not only improve the security of voice communications but also will help prevent attacks on two-factor authentication systems that rely on the Short Messaging Service.

The solutions developed also provide a broad range of tools to providers and end-users, allowing both groups of stakeholders to improve their security footing independently. Moreover, the techniques will improve security across both current and future network generations.

UPCOMING MILESTONES

- Preliminary Demonstration—June 2021
- Updated design document—August 2021

SRMNI R&D PERFORMER

University of Florida, Gainesville, Florida.