DHS Science and Technology Directorate

Homeland Security
Science and Technology

CELL NETWORKS VULNERABLE TO ATTACK

Cellular networks like any network have exploitable vulnerabilities. The efforts of international standards bodies and vendor manufacturers to address security as networks have matured and evolved with 5G networks; however, bad actors find innovative ways to exploit zero-day vulnerabilities.

As a result, a holistic approach to securing 5G traffic to avoid threats is needed. Therefore, defining security overlays in 5G reference architectures—based upon 3rd Generation Partnership Project (3GPP) 5G Standards is needed by both the public and private sectors.

DEVELOPING END-TO-END 5G SECURITY

Through its Secure and Resilient Mobile Network Infrastructure (SRMNI) project, Commdex will develop and evaluate varying end-to-end security controls for 5G devices, 5G Radio Access Network, core, and transport network architecture. It will also determine the efficacy of the approaches in a testbed in coordination with Nokia using various real-world use-cases.

The overall objective of the appropriately titled "Fifth Generation Network Security" project is to evaluate and define the end-to-end protection of 5G network traffic, including the development of standardized, secure voice and video capabilities for unclassified communications.

The project will produce a security and privacy architecture specification that aligns with commercial 5G architectures and adheres to 3GPP standards. The initiative will propose and show how adequately developed and implemented security controls, processes, and procedures will increase the security and resiliency of 5G infrastructure to reduce the risks to government services, devices, and data.

This project will outline the research, development, testing, and piloting strategy for end-to-end security controls for a 5G device, Radio Access Network, core and transport network architecture, including Distributed Denial of Service (DDoS) mitigations, end-to-end security protections meeting requirements for public safety government communications. In addition, exploration of hardware/software and systems to mitigate supply chain threats and their applications for coexistence with other 5G priority services.

SECURE & ROBUST EMERGENCY COMMS

This end-to-end secure network architecture will help secure and enhance emergency communications to approximately 700,000 National Security/Emergency Preparedness (NS/EP) personnel subscriptions to the CISA- administered Wireless Priority Service (WPS) and Government Emergency Telecommunications Service (GETS) and the millions of public safety users, leveraging services from providers operating and deploying 5G infrastructure.

This solution specifically will address how to ensure the availability of priority services for emergency communications during congestion events on 5G infrastructure.

UPCOMING MILESTONES

- Lab-site engagement, build and install—January 2022
- Final technical report and conclusions—May 2022

SRMNI R&D PERFORMER

Commdex, LLC, Smyrna, Georgia