DHS Science and Technology Directorate

Homeland Security
Science and Technology

CHALLENGES TO MOBILE SECURITY

There are many challenges to providing mobile network security on a nationwide, network or device basis. For instance, threat protection must be deployed to encompass emerging technologies such as 5G, which will see telecom protocols converge with internet and IT protocols but also support legacy network technologies from 2G through 4G. However, with each generation of mobile technology the complexity of threat detection increases as attack surfaces broaden.

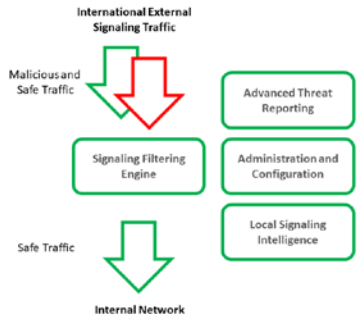
Given that communications infrastructure has been deemed critical infrastructure by the federal government, it is critical for federal-government and private-sector entities to be able to detect, analyze and respond to attacks on mobile network infrastructure—whether next-generation or legacy systems.

CREATING AN INNOVATIVE SOLUTION

The AdaptiveMobile Security Secure and Resilient Mobile Network Infrastructure (SRMNI) R&D project will develop an innovative threat-detection solution that will help increase the security posture of mobile networks and devices. Specifically, the performer will develop a solution that uses stateful communication protocols with security-focused advanced analytics algorithms and a global-threat intelligence service to ensure mobile networks are continually secured and threats to US subscribers' data, communications and safety detected.

The project's approach will address three main areas that organizations face when securing mobile infrastructure: detection, analysis, and response planning. The project will research requirements for a managed, secure defense and the processes required to update protection against the latest threats. The research will then detail the platform, skills, and processes that will be required to manage and implement a threat-intelligence platform with the capabilities to prioritize and plan responses to mobile network infrastructure threats.

It will demonstrate the ability of mobile network signaling threat-detection and intelligence technologies to identify security threats in current (3G and 4G) and future (5G) mobile networks. The approach has three unique prongs to defend against cross-/multi-protocol threats: a signaling firewall, security-focused advanced analytics algorithms, and a global threat intelligence service to ensure that network borders are continually secured against the most sophisticated attacks and attackers.



AdaptiveMobile's Security Signaling Protection Platform Architecture

PROTECTING MOBILE INFRASTRUCTURE

The performer's research will provide a comprehensive approach for designing practical solutions to the challenges of protecting national mobile infrastructure. The project will not only enable a defensive solution for current mobile technologies but also will demonstrate how the architecture can be extended to secure networks into the future.

A nation with the ability to secure its mobile communications infrastructure from external attacks or misuse will maintain a critical advantage in the battle against cybercrime and espionage. Preventing access to sensitive intelligence, unsecured conversation, locations, and other attack vectors commonly associated with insecure mobile network infrastructure is an essential defensive capability.

Knowledge gained from analysis and correlation of information will provide insight into the techniques, tactics, infrastructure, and procedures used to deploy attacks against mobile networks. This project will provide a blueprint for how and to what extent these capabilities can be delivered and deployed.

UPCOMING MILESTONES

- Demonstration and evaluation of the initial design.

SRMNI R&D PERFORMER

AdaptiveMobile Security Inc., Frisco, Texas