Study on Mobile Device Security

Cybersecurity Act of 2015, Title IV, Section 401

Acknowledgements: DoD, DHS HQ, DHS NPPD, DHS S&T, GSA, NIST NCCoE

Homeland Security
Science and Technology

Vincent Sritapan
Program Manager
DHS S&T

Joshua M Franklin
IT Security Specialist
NIST

Act's Requirement

Consolidated Appropriations Act, 2016, Division N— Cybersecurity Act of 2015

Title IV, Section 401, Study on Mobile Device Security*

Subsection (a)

(1) Directs the DHS Secretary, in consultation with NIST, to complete a **study on threats relating to the security of the mobile devices** of the federal government

(2) Requires submission of an unclassified **report** (with a classified annex if needed) to Congress **within one year of the Act's passage**

Subsection (b)*

(1) Evolution of mobile security techniques from a desktop-centric approach, and adequacy of these techniques to meet current mobile security challenges

(2) Effect such threats may have **on the cybersecurity of the information systems and networks of the federal government**

(3) Recommendations for addressing the threats **based on industry standards and best practices**

(4) Deficiencies in the current authorities of the Secretary that may inhibit the ability of the Secretary to address mobile device security throughout the federal government

(5) Plan for accelerated adoption of secure mobile device technology by DHS

Homeland Security
Science and Technology

**Excludes National Security Systems and DoD and IC systems and networks*

Timeline

- Congress Commissioned Study

- Working Group Created Across Multiple Federal Agencies & Departments
- Additional Staffing Resources Allocated

- Initial Working Group Meetings
- Created Threat Model
- Created RFI Structure & Documents

- Issued RFI
- Held Industry Days
- Received RFI Responses
- Final Analysis of Industry RFI Submissions

- Completed Study Draft
- Finalized Study
- WG & MTTT Review
- Internal DHS ExecSec Review

- External ExecSec Review
- **Deliver Final Report**

Homeland Security
Science and Technology

Mobile Threats and Defenses RFI

- **Open 47 Days - Closed August 22**
  - https://www.fbo.gov/notices/bc457545615649b4371cedd9de371bb9
- **Divided Threats to Mobile Ecosystem into Five Categories**
  - Application-Based Threats
  - Operating System/Firmware/Lower Level Device Threats
  - Physical Device/Access-Based Threats
  - Network-Based Threats
  - Threats to the Mobile Enterprise Systems

RFI: Information Requested

Part 1: Survey Worksheet for Products, Services or Technologies

- Current and/or future technical capabilities of systems and solutions that mitigate or counter known or predicted threats to the total mobile environment related to the Government's use of mobile devices and services.
- Responses will be used for the congressionally required study and will help the Government understand the range of products and technologies available to protect the mobile ecosystem.
- This will also help the Government to identify gaps between known, emerging or anticipated threats and current solutions and capabilities.
- DHS is primarily seeking detailed technical descriptions of threats with mitigations

Part 2: Industry Standards and Best Practices

- Standards and best practices for security and interoperability
- Demarcation points on mobile communication chain that need attention

Homeland Security
Science and Technology

Breakdown of Responses

- Responses by Industry – 46 Total Including:
  - Two Largest Mobile Network Operators in U.S. (AT&T, Verizon)
  - Two Largest Mobile OS Providers in World (Apple, Google)
  - Largest Cellular Chip Maker in World (Qualcomm)
  - US Cellular Industry Association (CTIA)
  - Leading EMM/MDM Makers (AirWatch, MobileIron, IBM, Samsung)
  - Several Dozen Security Vendors
- Responses by Threat Category
  - Applications 36
  - Operating System/Firmware/Software 29
  - Device Physical Access 27
  - Network 30
  - Mobile Enterprise 21

Homeland Security
Science and Technology

RFI Responses - 46 Organizations

4K Solutions, LLC
Absolute Software
AdaptiveMobile Security
Advanced Cyber Security
AirWatch (VMWare)
Akamai
Applied Communication Sci.
Appthority
AT&T
Better Mobile Security
Blackberry
BlueRISC
Cellbusters
Check Point
Cisco Systems
CTIA
Cyber adAPT
Dexter Edward, LLC
Duo Security
Gadget Guard
Galois
Google
HRL Laboratories
IBM
Intel Security
Intelligent Automation Inc.
IPTA & Akamai
Kaprica Security Inc.
Kryptowire
Lookout
MobileIron
Optio Labs
Oracle
Procera Networks
Qualcomm Technologies
Rivetz
RML Business Consulting
RunSafe Security Inc.
Samsung
SecureLogix
Squadra Technologies
Temple University & Sentar, Inc.
Trustonic
TSI
Verizon
Waverly Labs

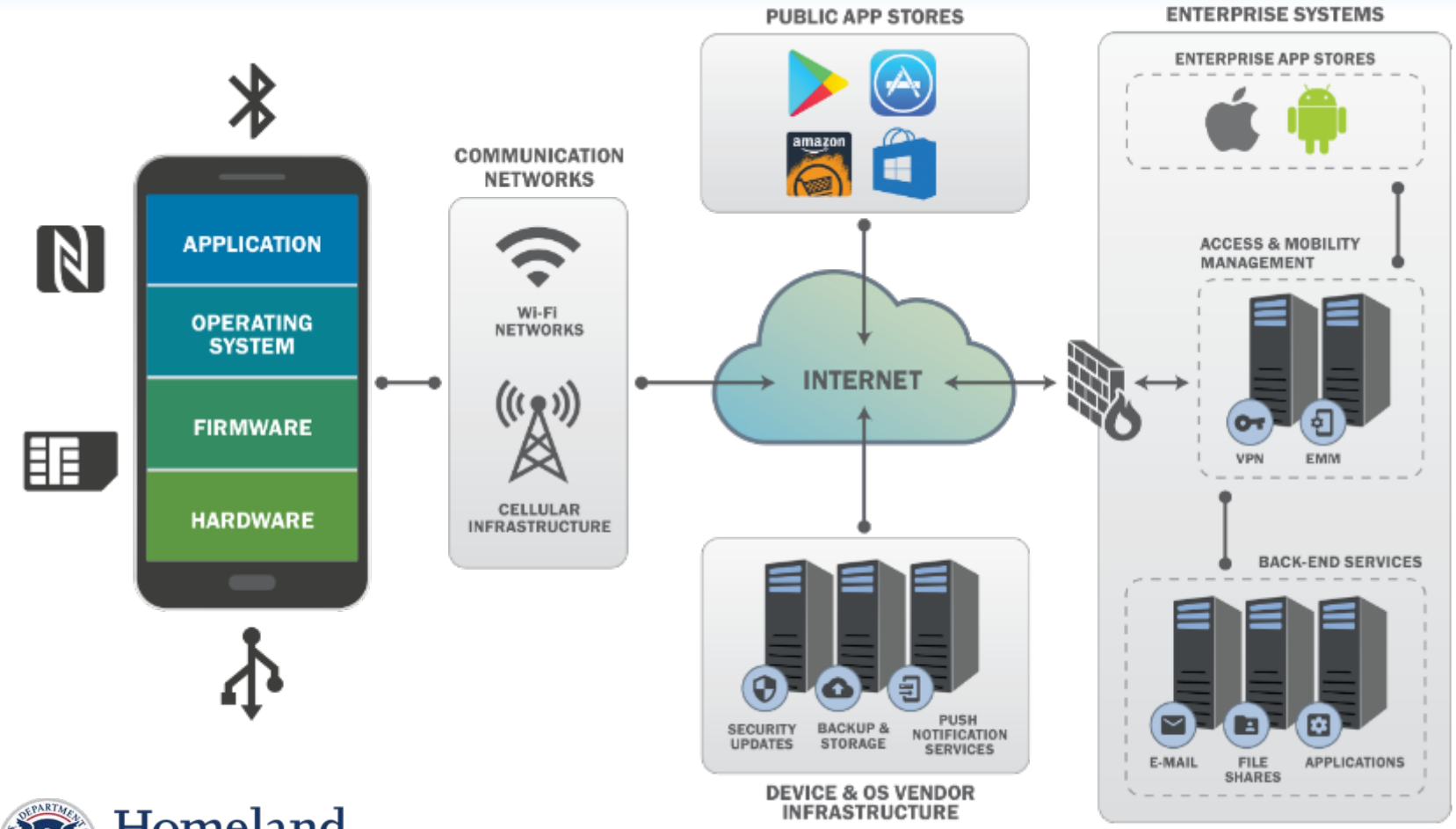
Homeland Security
Science and Technology

One-on-One Interviews

- California
  - Cyber adAPT
  - Google
  - Lookout
  - MobileIron
  - ProofPoint
  - Qualcomm
  - Samsung
- Washington, DC
  - VMWare AirWatch
  - Apple
  - AT&T
  - CTIA

Homeland Security
Science and Technology

Mobile Ecosystem



Homeland Security
Science and Technology

Primary Mobile Threat Types

Threat	Definition	Examples
Denial of Service	Deny or degrade service to users	Jamming of wireless communications, overloading networks with bogus traffic, ransomware, theft of mobile device or mobile services.
Geolocation	Unauthorized physical tracking of user	Passively or actively obtaining accurate three-dimensional coordinates of target, possibly including speed and direction.
Information Disclosure	Unauthorized access to information or services	Interception of data in transit; leakage or exfiltration of user, app, or enterprise data; tracking of user location; eavesdropping on voice or data communications; surreptitiously activating the phone's microphone or camera to spy on the user.
Spoofing	Impersonating something or someone	Email or SMS message pretending to be from boss or colleague (social engineering), fraudulent Wi-Fi access point or cellular base station mimicking a legitimate one.
Tampering	Modifying data, software, firmware, or hardware without authorization	Modifying data in transit, inserting tampered hardware or software into supply chain, repackaging legitimate app with malware, modifying network or device configuration (e.g., jailbreaking or rooting a phone).

Mobile Security Threats by Category

MOBILE DEVICE TECHNOLOGY STACK	• Delays in Security Updates • Exploitation of OS or Baseband Vulnerabilities • Deliberate Bootloader Exploitation • Jailbreak/Rooting • Supply Chain Compromise • TEE/Secure Enclave Exploitation • Compromised Cloud System Credentials
MOBILE NETWORKS	• Data/Voice Eavesdropping • Data/Voice Manipulation • Device and Identity Tracking • Denial of Service/Jamming • Rogue Base Stations & Wi-Fi Access Points • Interference with 911 Calls
DEVICE PHYSICAL SYSTEMS	• Device Loss or Theft • Physical Tampering • Malicious Charging Station • Attacks on Enterprise PCs
MOBILE APPLICATIONS	• Malicious and/or Privacy-Invasive Practices • Vulnerable Third-Party Libraries • Exploitation of Vulnerable App • Insecure App Development Practices • Exploit Public Mobile App Store • Malware, Ransomware
MOBILE ENTERPRISE	• Compromised EMM/MDM System or Admin Credentials • Man-in-the-Middle Attacks on Devices • EMM/MDM system impersonation • Compromised Enterprise Mobile App Store or Developer Credentials • Bypass App Vetting

Homeland Security
Science and Technology

Best Practices and Standards

Enterprise Mobility Program

- Mobile Computing Decision Framework (MTTT)
- Federal Mobile Computing Security Baseline (DHS, DoD, NIST)
- Mobile Security Reference Architecture (DHS, DoD, NIST)
- NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure Draft (NIST)
- Security Guidance for Critical Areas of Mobile Computing (Cloud Security Alliance)
- Privacy Policy for DHS Mobile Apps (DHS)

Mobile Device Technology Stack

- NIST SP 800-164 (Draft): Guidelines on Hardware-Rooted Security in Mobile Devices (NIST)
- NIST SP 800-88r 1: Guidelines for Media Sanitization (NIST)
- NISTIR 7981 Mobile, PIV, and Authentication (NIST)
- NIST SP 800-121r1 Guide to Bluetooth Security (NIST)
- Mobile Device Security a Comparison of Platforms (Gartner)
- NIAP Protection Profile for Mobile Device Fundamentals 3.0 (NIAP)
- Specification for Trusted Execution Environment/Specification for Secure Element Management (Global Platform)
- Specifications for Trusted Platform Module (Trusted Computing Group)

Mobile Enterprise

- NIST SP 1800-4 Practice Guide: Mobile Device Security (NIST NCCoE)
- NIST SP 800-124r1: Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST)
- Commercial Solutions for Classified Mobile Access Capability Package (NIAP)
- NIAP Protection Profile for Mobile Device Management Version 2.0 (NIAP)
- NIAP Protection Profile - Extended Package for Mobile Device Management Agents 2.0 (NIAP)

Mobile Applications

- NIST SP 800-163: Vetting the Security of Mobile Applications
- Adoption of Commercial Mobile Applications within the Federal Government (CIO Council)
- NIST SP 1800-1 Practice Guide: Securing Electronic Health Records on Mobile Devices (NIST NCCoE)
- NISTIR 8136: (Draft) Mobile Application Vetting Services for Public Safety (NIST)
- Mobile Application Single Sign-On for Public Safety and First Responders (NIST NCCoE)
- Open Web Application Security Project - Mobile Security Project (OWASP)
- Mobile Application Security Testing Initiative (Cloud Security Alliance)
- NIAP Protection Profile for Application Software (NIAP)

Mobile Networks

- NIST SP 800-187 Guide to LTE Security
- SS7 Interconnect Security Monitoring Guidelines (GSMA)

Legal Authority Gaps

- Gap 1: DHS has no legal authority to require mobile carriers to assess risks relating to the security of mobile network infrastructure as it impacts the Government's use of mobile devices.
- Gap 2: While DHS has the authority to evaluate voluntarily provided mobile carrier network information, DHS has no legal authority to compel mobile carrier network owners/operators to provide information to assess the security of these critical communications networks.

DHS Next Steps

- To address these areas of concern DHS proposes the following:
  - FISMA metrics should be enhanced to focus on securing mobile devices through the Federal CIO Council's Mobile Technology Tiger Team (MTTT). Metrics for consideration include mobile operating systems, mobile device authentication methods, and volume of mobile device user traffic not going through the agency's Trusted Internet Connection.
  - The DHS CDM program should address the security of mobile devices and applications with capabilities that are at parity with other network devices (e.g., workstations and servers), and NPPD's definition of critical infrastructure should include mobile network infrastructure
  - DHS S&T HSARPA Cyber Security Division should continue its work in Mobile Application Security to ensure the secure use of mobile applications for government use.

DHS Next Steps (cont'd)

- Potential areas for additional research or partnerships within DHS include:
  - Creating a new applied R&D program in securing mobile network infrastructure to address current and emerging challenges impeding mobile technology.
  - Establishing a new program for applied research in advanced defensive security tools and methods for addressing mobile malware and vulnerabilities, including new ways to handle CVE generation for mobile and mobile threat information sharing, e.g., Structured Threat Information eXpression (STIX™), and Trusted Automated eXchange of Indicator Information (TAXII™). DHS should coordinate this initiative with existing efforts within DoD.
  - Coordinating the adoption and advancement of mobile security technologies recommended in this report into operational programs such as Einstein and CDM to ensure future capabilities include protection and defense against mobile threats.
  - Developing cooperative arrangements and capabilities with commercial mobile network operators to detect, protect and respond to threats (e.g., rogue IMSI catchers and SS7/Diameter vulnerabilities) that impede the confidentiality, integrity and availability of Government communications; and if necessary, extend the legal authorities of NPPD to achieve these objectives.

DHS Next Steps (cont'd)

- Additional topics that require a response by the federal government are:
  - The U.S. government should continue and enhance its active participation in international standards bodies so it can represent America's national interest with the private sector in the development of consensus-based voluntary mobile security standards and best practices.
  - Continued development of the NIST draft *Mobile Threat Catalogue* with additional cooperation from industry and the inclusion of emerging threats and defenses and additional risk metrics for mobile threats.
  - Federal departments and agencies should develop policies and procedures regarding Government use of mobile devices overseas based on threat intelligence and emerging attacker tactics, techniques, and procedures.

Questions

Homeland Security

Science and Technology

DHS:

Homeland Security

Science and Technology

Homeland Security

Science and Technology