DHS Science and Technology Directorate

Mobile Device Security

Concerns for Rapid Mobile Adoption

The use of mobile technology is a cornerstone of the White House's Digital Government Strategy aimed at increasing the productivity within the federal government and delivering mobile-enabled services to citizens. However, ***gaps in mobile security have been identified as major barriers to expanding the use of mobile technology***. A 2013 report indicated that 38 percent of smartphone users have been victims of cyber crime[1]. This rate is expected to grow with mobile threats on the rise. For instance, 3.5 million unique malware and high-risk apps were seen in 2014[2], 10 times more than reported in 2012[3]. Without a radical change, current and future investments in mobile technology will succumb to unmanageable risk that attenuates the benefits afforded by mobile technology.

Mobility Risks

Cybercriminal activity targeting mobile devices and data privacy can have dire consequences, including tracking users, stealing mission critical data and denying users access to their devices. The mobile device can also be used as a launching pad for more lucrative attacks aimed at enterprise systems, social networks and cloud platforms.

Mobile Security Challenges

Current mobile security techniques have evolved from a desktop-centric approach. These techniques have already fallen short in handling today's mobile malware. Compared to traditional computers, it is harder to regulate functionality on mobile devices. To exacerbate the problem, mobile devices support more complex interfaces (e.g., cellular, Wi-Fi, Bluetooth, GPS, etc.) exposing more surfaces to attack. Greater visibility into the device's behavior and interaction with the environment is needed to prevent, identify, and remediate mobility threats. This necessitates a mobile-centric approach to security that can leverage the resources and capabilities inherent on the mobile platform.

Mobile Device Security Program

The Department of Homeland Security (DHS) Science and Technology Directorate Cyber Security Division has initiated the Mobile Device Security (MDS) program to focus on innovative security technologies needed to address the challenges impeding the adoption of mobile technology. The program leverages strategic partnerships with the DHS CIO Council, federal departments and agencies and industry to identify mobile security needs, prioritize requirements to drive R&D efforts and pilot programs for transitioning R&D to practice.

Research & Development Initiatives

The MDS program is comprised of R&D in the areas of:

Software based mobile roots of trust: Developing capabilities below the operating system to provide the foundation for a "chain of trust" that ensures device integrity and enables vital security mechanisms.

Mobile malware analysis and application archiving: Developing real-time vetting techniques using static and dynamic analysis to identify malicious attributes in mobile applications. Combining big-data analytics with visualization using applications from mobile application markets to establish practices in mobile application archiving.

Mobile Technology Security: Developing secure technologies in (1) mobile device instrumentation, (2) transactional security methods, (3) mobile security management tools and (4) device layer protection to enable the rapid adoption of mobile technologies in the public and private sectors.

Impact

Mobile technologies promote lower costs, geographic flexibility and other advantages to government services such as public safety, health, education and finance. In 2013, productivity gains from mobile devices for the federal government were reported at $28 billion annually.[4] The transformational power of mobile technology hinges on the ability to secure this technology. The MDS program is aimed at accelerating the adoption of secure mobility through R&D for the Department, the Government, and the global community.

Performers

Mobile Roots of Trust R&D

- BlueRISC, Inc., Amherst, MA
- Def-Logix, San Antonio, TX
- Galois, Inc., Portland, OR

Mobile Malware Analysis / Mobile App Archiving R&D

- University of California, Santa Barbara / Vrije Universiteit Amsterdam
- George Mason University / KryptoWire LLC

Broad Agency Announcement: Mobile Tech Security

- BAA HSHQDC-14-R-B0015 to be awarded 2015

[1] 2013 Norton Report
[2] TrendLabs 3Q 2014 Security Roundup
[3] The Mobile Landscape Roundup: 1H 2014
[4] The 2013 Digital Dilemma Report – Mobile Work Exchange

Homeland Security
Science and Technology

To learn more about Cyber Security Division's Mobile Device Security Program, contact Vincent Sritapan, Program Manager, at vincent.sritapan@hq.dhs.gov.

2/06/2015