Establishing and Maintaining Trust in a Mobile Device

Kristopher Carver, BlueRISC
Vincent Sritapan, US Department of Homeland Security Science and Technology Directorate
Cherita Corbett, SRI International

The mobile device market has grown tremendously. Individuals, businesses, and governments rely on mobile devices to access critical infrastructure and share vital information (banking, medical data, intellectual property, and so on). This growth in adoption has also brought about a parallel surge in attacks. Malware, ransomware, and spyware are targeting mobile platforms to steal sensitive data, access private networks, track users, and do other nefarious activities. Particularly for governments using mobile technology, mobile attacks can disrupt life-saving operations, endanger personnel, and expose government systems to exploitation. Securing mobile devices is no small feat and is therefore a forefront issue to the US Department of Homeland Security Science and Technology Directorate’s (DHS S&T’s) cybersecurity R&D program.1

Roots of Trust
Mobile roots of trust (RoT) are highly trustworthy, tamper-evident components that can provide a foundation for building security and trust for mobile devices. RoT is usually provided as a specialized hardware chip (such as a trusted platform module) on desktop or laptop systems. However, mobile devices are resource-constrained and lack dedicated hardware mechanisms for providing RoT. This leaves a single solution—namely, to provide RoT in software. Unfortunately, this is challenging to realize given the sophistication of current threats and the ease with which a mobile device’s state and information can be extracted and altered. Moreover, security specifications such as the Trusted Computing Group’s Mobile Trusted Module2 don’t address how to support mobile RoT requirements in software, nor do they address dynamic verification of device and software behavior while applications are running.

BlueRISC is developing MobileRoT, a fully software-based dynamic mobile trusted module technology under support from the DHS S&T Cyber Security Division (CSD). MobileRoT measures and verifies a device’s static and runtime state (for example, boot loader, operating system, apps, and runtime memory) to enable trust and overall device security. It can be utilized to detect malicious system changes or activity and to ensure that access to critical information and software can only be performed in a trusted state. MobileRoT requires no modifications to the underlying operating system kernel, nor any manufacturer or service provider support for insertion, greatly reducing hurdles to adoption.

MobileRoT Architecture
To overcome the array of surface attacks targeting software-based systems, MobileRoT utilizes a new architecture for enabling transitive trust based on the Core Root of Trust for Measurement (CRTM).2 The CRTM is hardened code that acts as the RoT for reliable integrity measurements and is the foundation for additional trusted services. The MobileRoT architecture includes a layer of encrypted CRTM code that is tied to a cryptographic key.
generated at boot-time. With the CRTM established, the resulting system doesn’t require any sensitive information to be stored persistently in an unprotected state, closely mimicking the level of security achievable via dedicated hardware. A secure cryptographic sealing and unsealing procedure tied to the boot-time and runtime measurements performed by the solution enables application and data protection. Because all protected data and applications are sealed, they remain protected even in cases in which an attacker attempts to alter or bypass the MobileRoT technology.

Figure 1 shows an example measurement and verification flow, which illustrates the boot process of an Android mobile device and gives an example of how an RoT can be established within it. In this example, the MobileRoT sits logically between the boot loaders and the Android kernel. Here, it can establish the CRTM and perform backward verification (1), self-verification (2), and forward verification (3) of both privileged components and userland applications.

Traditional solutions focus primarily on boot-time validation, establishing the validity of each component prior to a complete boot, while providing only minimal support for runtime activities. Unfortunately, it is widely known that sophisticated attacks can target applications that are already running, and devices these days are rarely rebooted. To address the shortcomings of one-time static verification, MobileRoT provides dynamic verification and attestation by performing runtime measurements of the system state of the device (4 and 5 in Figure 1). These runtime agents harden themselves from attack and modification by creating a self-validating network, which can instantly respond to a threat to the system or the protection technology itself.

MobileRoT reliably allows all levels of software, including user applications, to have access to its trusted services through an open API. This enables the creation of secure, off-the-shelf, third-party and proprietary applications and data, and strengthens key management and policy enforcement technology, such as mobile device management (MDM). MobileRoT also provides fine-grained protection integrated directly into an application. For example, a standard Android Calendar application can be modified to support the concept of a “secure event.” This secure event is established in cooperation with the MobileRoT and persistently protected. To view a secure event, proper authorization and authentication is required, and the system state must be verified.

Although cybercrime targeting mobile devices is becoming pervasive, mobile RoT can preserve and confirm the integrity of the device while it’s at rest or in use. BlueRISC’s MobileRoT technology has overcome barriers to bring RoT to a mobile platform, providing a foundation of security features to accelerate the development of secure mobile devices.
Acknowledgments
The views and conclusions contained herein are the authors’ and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the US Department of Homeland Security (DHS) or the US government. The work by BlueRISC was sponsored by the DHS Homeland Security Advanced Research Projects Agency (HSARPA), Cyber Security Division (CSD), via the Small Business Innovation Research Program under contract number D14PC00178. The work by SRI International was funded by the DHS S&T under contract number HSHQDC-10-C-00144.

References

Kristopher Carver is the technical director at BlueRISC, and principal investigator on the MobileRoT project sponsored by the US Department of Homeland Security Science and Technology Directorate. He leads the technical direction of BlueRISC and its system assurance and cybersecurity products and technologies. Carver has more than 10 years of experience in software and hardware protection solutions. He is co-inventor of seven patents. Contact him at kris@bluerisc.com.

Vincent Sritapan is a program manager in the US Department of Homeland Security Science and Technology Directorate’s Cyber Security Division. His projects focus on mobile software-based roots of trust, mobile device protection, access control, and continuous automated assurance for mobile apps. Sritapan is also an information professional officer in the US Navy Reserves. Contact him at vincent.sritapan@hq.dhs.gov.

Cherita Corbett is a senior computer scientist at SRI International. Her research interests include mobile security, self-healing cellular networks, and cyber-physical systems security. Corbett provides subject matter expertise and project management for the US Department of Homeland Security Science and Technology Directorate’s cybersecurity R&D program. Contact her at cherita.corbett@sri.com.

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.

CALL FOR ARTICLES
IT Professional seeks original submissions on technology solutions for the enterprise. Topics include:
- emerging technologies,
- cloud computing,
- Web 2.0 and services,
- cybersecurity,
- mobile computing,
- green IT,
- RFID,
- social software,
- data management and mining,
- systems integration,
- communication networks,
- data center operations,
- IT asset management, and
- health information technology.

We welcome articles accompanied by Web-based demos. For more information, see our author guidelines at www.computer.org/itpro/author.htm.

WWW.COMPUTER.ORG/ITPRO