The Role of the National Institute of Standards and Technology in Mobile Security

This paper will present an overview of the work of the National Institute of Standards and Technology (NIST) in security and privacy for mobile technology as well as an overview on how NIST standards and guidelines can be applied in the mobile environment.

Earlier this year the President signed a Memorandum issuing the Digital Government Strategy, which was designed to build a 21st Century digital government that delivers better services to the American people. The strategy recognizes the potential for mobile devices to be increasingly vulnerable to malicious or accidental security and privacy breaches, and the resulting need to continually review new technologies to ensure protections are sufficiently put into place.

As a part of the strategy, NIST was asked to report on its ongoing work in mobility, including the applicability of NIST's standards and guidelines to mobile devices and platforms. As a non-regulatory agency of the Department of Commerce, NIST has the responsibility to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

As a part of that mission, NIST has responsibilities under the Federal Information Security Management Act of 2002 (FISMA) to develop mandatory standards and guidelines for federal agencies information and information systems. These standards (also known as Federal Information Processing Standards or FIPS) and guidelines, which are developed collaboratively with partners in industry, government, and academia, are reviewed and updated to ensure they remain consistent with technological innovation and security practices. The documents that are created through this process can also be used voluntarily by industry and other organizations to benefit from this collaborative work.

NIST's work is conducted to ensure that industry is able to accommodate the security needs of federal agencies – and that NIST can work with industry collaboratively when gaps exist.

Overview of Mobile Security

Smart phones have become both ubiquitous and indispensable for consumers and business people alike. Although these devices are relatively small and inexpensive, they can be used not only for voice calls and simple text messages, but also for many functions once limited to laptop and desktop computers.

Smart phones and tablet devices have specialized built-in hardware, such as cameras, accelerometers, Global Positioning System (GPS) receivers, and removable media readers. Furthermore, they employ a range of wireless interfaces, including Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Communications (NFC), and one or more types of cellular interfaces that provide network connectivity across the globe. These devices

can be used for sending and receiving email, browsing the web, online banking and commerce, social networking, storing and modifying documents, remotely accessing data, recording audio and video, and as navigation aids.

Mobile devices, such as smart phones and tablets, typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats.

Like any new technology, smart phones present new capabilities, but also a number of new security challenges, including the need for secure and efficient cryptography suitable for power-constrained devices. Moreover, as the pace of the technology advancements continues to increase, our current Information Assurance standards and processes must be updated and new technologies developed to allow the continued use of Commercial Off-The-Shelf (COTS) products, allowing government users to access the latest technologies to meet their missions without sacrificing privacy and security.

Current mobile devices lack strong roots of trust that are increasingly found in laptops and other types of hosts. These roots of trust are hardware and software components that are secure by design and are trusted to perform one or more security-critical functions (including: measuring and/or verifying software; protecting cryptographic keys; performing device authentication). Roots of trust can provide greater assurance that these mechanisms are functioning properly – and shift the emphasis from configuring compliance for these devices to measuring compliance.

NIST has ongoing work to identify properties and capabilities of roots of trust needed to secure next generation mobile devices. This work is expected to examine issues relating to boot firmware protections; integrity measurement and reporting of critical firmware and software; secure storage; device authentication; and application and data isolation.

Lastly, mobile devices are designed to make it easy to find, acquire, install, and use third-party applications. This poses obvious security risks, especially for mobile device platforms that do not place security restrictions or other limitations on third-party applications. Organizations should plan their mobile device security on the assumption that unknown third-party mobile device applications downloadable by users should not be trusted.

NIST Standards and Guidance

NIST's standards and guidelines must be sufficiently robust to protect the wide range of information and information systems supporting the critical missions and business functions of the federal government—from the Department of Homeland Security, to the Federal Aviation Administration, to the Social Security Administration. As they are developed, NIST works collaboratively with Industry, often hosting workshops on specific areas, and putting the publications out for public comment to ensure industry, government, academia, and the public have the ability to engage in the process.

Given the variety of organizational sizes, devices, and uses—NIST's standards and guidelines must be sufficiently flexible to allow for a variety of deployment models. For an example in the mobility space, securing tablets with limited functionality for employees in the field for the purpose of conducting one particular task will be very different than the security considerations for devices that may be used in more typical office settings.

Below are summaries of key NIST standards and guidelines relevant to mobile security.

SP 800-53

General security recommendations for any IT technology, including mobile, are provided in ***NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.*** Earlier this year NIST published Revision 4 of 800-53 for public comment, the culmination of a year-long initiative to update the content of the security controls catalog and the guidance for selecting and specifying security controls for federal information systems and organizations. The project was conducted as part of the *Joint Task Force Transformation Initiative* in cooperation and collaboration with the Department of Defense, the Intelligence Community, the Committee on National Security Systems, and the Department of Homeland Security.

Many of the changes in SP 800-53 were driven by particular cyber security issues and challenges requiring greater attention including, but not limited to mobile technology (other examples include insider threat, cloud computing, application security, firmware integrity, supply chain risk, and the advanced persistent threat). In most instances the new controls and enhancements are not labeled specifically as "mobile computing" controls or placed in one section of the catalog. Given the diversity of these technologies, the controls and enhancements are distributed throughout the control catalog in various families and provide specific security capabilities that are needed to support those new computing technologies and computing approaches.

Agencies should first refer to ***FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems***, the mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations determine the security category of their information system in accordance with ***FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems***.

FIPS 200 and NIST Special Publication 800-53, in combination, ensure that appropriate security requirements and security controls are applied to all federal information and information systems – including those used by mobile technology. An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

As information technology advances, more powerful and diverse functionality can be found in smart phones, tablets, and other types of mobile devices. While tailored guidance may support not allocating a particular security control to a specific technology or device, any residual risk associated with the absence of that control must be managed to provide appropriate protection. The use of mobile devices might result in the need for additional security controls and control enhancements not selected in the initial baselines, but must be selected in a way that is consistent with organizational and Office of Management and Budget (OMB) policy.

FIPS 140-2

NIST runs a program with the government of Canada (the Cryptographic Module Validation Program, or CMVP) to validate hardware and software implementations of cryptography against FIPS 140-2 and NIST's cryptographic algorithm guidelines. Through this program, NIST works with private and governmental sectors and the cryptographic community to achieve security, interoperability, and assurance of correct implementation. If an organization specifies that the information or data must be cryptographically protected, then FIPS 140-2 is applicable, including for mobile devices. In essence, if cryptography is required, then it must be validated. The standard provides four increasing, qualitative levels of security, intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

Currently the same set of cryptographic algorithms validated by this testing program are used throughout the world, including in the credit card, motion picture, and health care industries. Through partnerships, other national governments also rely on this strong cryptography testing program.

CMVP allows vendors of cryptographic modules to use a set of independent and international laboratories to test their modules. NIST's role is to serve as the validation authorities for the program jointly with the government of Canada, validating the test results from the labs and issuing certificates. Given that the laboratories are independent, market forces determine the cost of validation and speed in which modules can be validated. It is important to note that only the module is tested, not the product itself. Once validated, the module can be used in a variety of products.

There are FIPS 140-2 validated cryptographic modules that can be leveraged for a variety of mobile device and mobile application requirements. The number of algorithms and modules submitted for validation continues to grow, representing significant growth in the number of validated products expected to be available in the future.

FIPS 201

On July 9th, NIST released for comment the ***Revised Draft Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification of Federal Employees and Contractors.*** The National Institute of Standards and Technology (NIST) has released the second-round draft version of its updated security standard for identity credentials in the Personal Identity Verification cards (PIV cards) that all federal

employees and contractors must use.

The document is the next step toward updating FIPS 201, which was published in February 2005. Among its requirements are that all PIV cards contain an integrated circuit chip for storing electronic information, a personal identification number and protected biometric data—a printed photograph and two electronically stored fingerprints.

FIPS 201-2 introduces the concept of a PIV-derived credential to accommodate the use of mobile devices that cannot work with contact card readers. Details on how these credentials will be derived will be specified in a Special Publication to be issued later this year (***Special Publication 800-157, Guidelines for Personal Identity Verification (PIV) Derived Credentials)***.

NIST's Publications and Additional Mobility Projects

Recently NIST has begun work on updating a series of special publications to assist organizations with challenges due to increased use of mobile devices. The first such update, ***NIST SP 800-124 Revision 1 (Draft), Guidelines for Managing and Securing Mobile Devices in the Enterprise*** was released for comment on July 10th. The purpose of this publication is to help organizations centrally manage and secure mobile devices against a variety of threats. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use. The scope of SP 800-124 Revision 1 includes securing both organization-provided and personally-owned mobile devices.

Later this year, NIST will release for comment ***NIST SP 800-114 Revision 1 (Draft), User's Guide to Telework and Bring Your Own Device (BYOD) Security***. Many federal employees telework, and they use a variety of devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. Each telework device is controlled by either the organization or an external party (such as the teleworker); the latter is known as bring your own device (BYOD). This publication provides recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks. Telework devices should be secured properly and have their security maintained regularly.

In addition, NIST is preparing ***NIST SP 800-46 Revision 2 (Draft), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*** for release. Many organizations' employees and contractors use enterprise telework and remote access technologies to perform work from external locations. All components of these technologies, including client devices and BYOD devices, should be secured against expected threats as identified through threat models. This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework and remote access technologies. It also gives advice on creating telework security policies.

Moving from devices to applications, over the last year-and-a-half, NIST has analyzed Android applications using commercial and open source static analysis tools, designed an Application Testing Portal (ATP), and implemented a proof-of-concept ATP. Based on this work, later this year NIST will release guidelines to provide a methodology for testing and vetting third-party applications that are distributed through various app stores. The methodology is based on the research and lessons learned by building the ATP. The portal allows for static code analyzers to identify software weaknesses and applications misbehavior based on their access control, resources consumptions, network usage, traffic patterns, information leakage and more.

As NIST moves forward collaboratively with industry to bridge the security gaps present on today's smart phones, tablets, and other mobile devices, it welcomes comments from all interested stakeholders to assist in this work. To learn more about NISTs computer security work in mobility and other areas, please visit the Computer Security Division's Computer Security Resource Center at csrc.nist.gov.