

NIST Mobile Efforts

Andrew Regenscheid
Computer Scientist & Mathematician
Project Lead, Roots of Trust

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce

About NIST

- **NIST's Mission Statement:**
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.
- **Information Technology Laboratory Mission Statement:**
To promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.
- **CSD Mission Statement:**
Conduct research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect our nation's information and information systems.



Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.



Overview

- NIST Computer Security Standards & Guidelines
- Mobile Security Efforts
 - Mobile Device Security
 - Mobile Device Management
 - Mobile Application Vetting
- Application Areas
 - User authentication from mobile devices
 - Public safety communications



Mobile Device Security

- NIST SP800-164, *Guidelines on Hardware-Rooted Security In Mobile Devices*
- Focus on three key capabilities:
 - **Device Integrity:** Software, firmware, and hardware configurations are in a trusted state
 - **Isolation:** Sandbox apps and separate data to control information and confine vulnerabilities
 - **Protected Storage:** Protect confidentiality and integrity of sensitive data on the device

Draft available at:

<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-164>



Mobile Device Management

- NIST SP800-124rev1, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*
 - Intended to help organizations centrally manage and secure mobile devices against a variety of threats
 - Provides recommendations for selecting, implementing, and using centralized management technologies
- Topics:
 - Security policy management and enforcement
 - Data communication and storage
 - Device and user authentication
 - Firmware and applications management and enforcement

Available at: <http://dx.doi.org/10.6028/NIST.SP.800-124r1>



Mobile Application Security

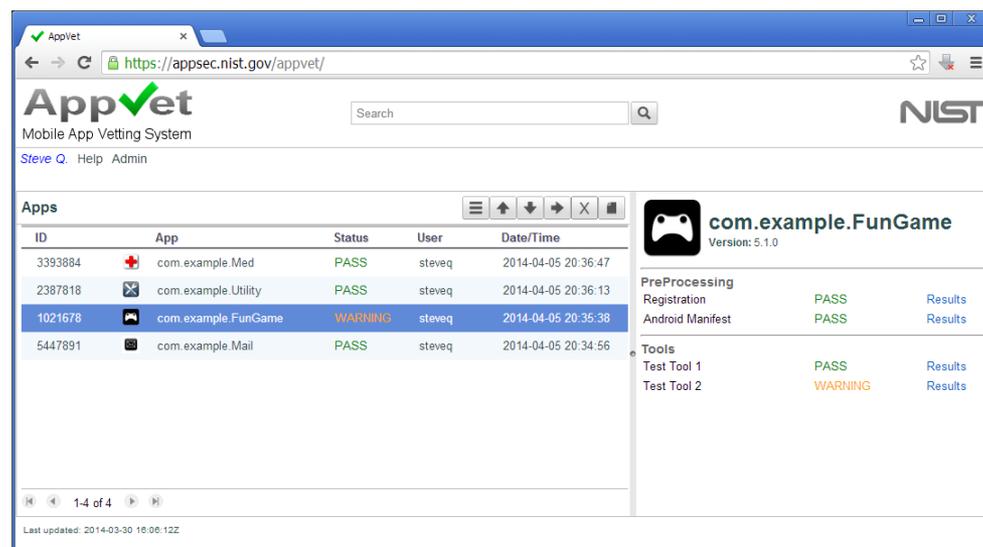
- DARPA Transformative Applications Program
 - Aimed to provide soldiers with secure mobile solutions in combat environments
 - NIST supported development of app vetting system
- Developed NIST's expertise in app vetting tools and processes
- Draft Special Publication 800-163, *Technical Considerations for Vetting 3rd Party Mobile Applications*

Draft available at: http://csrc.nist.gov/news_events/#aug19



AppVet

- Open source web service
- Facilitates app vetting workflow for submitting and testing apps, accessing reports, and assessing risk
- Designed to be integrated with 3rd party test tools



The screenshot shows the AppVet web interface. The main header includes the AppVet logo, a search bar, and the NIST logo. Below the header is a navigation menu with 'Steve Q.', 'Help', and 'Admin'. The main content area is divided into two sections. On the left is a table titled 'Apps' with columns for ID, App, Status, User, and Date/Time. On the right is a detailed view for the app 'com.example.FunGame' (Version: 5.1.0), showing 'PreProcessing' results for 'Registration' (PASS) and 'Android Manifest' (PASS), and 'Tools' results for 'Test Tool 1' (PASS) and 'Test Tool 2' (WARNING). The footer indicates 'Last updated: 2014-03-30 16:06:12Z'.

ID	App	Status	User	Date/Time
3393884	com.example.Med	PASS	steveq	2014-04-05 20:36:47
2387818	com.example.Utility	PASS	steveq	2014-04-05 20:36:13
1021678	com.example.FunGame	WARNING	steveq	2014-04-05 20:35:38
5447891	com.example.Mail	PASS	steveq	2014-04-05 20:34:56

com.example.FunGame
Version: 5.1.0

PreProcessing

Registration	PASS	Results
Android Manifest	PASS	Results

Tools

Test Tool 1	PASS	Results
Test Tool 2	WARNING	Results

1-4 of 4

Last updated: 2014-03-30 16:06:12Z

Available at: <http://csrc.nist.gov/projects/appvet/>

Authentication from Mobile Devices

Homeland Security Presidential Directive 12 was issued in 2004 to create a common identification standard for federal employees and contractors.

- A standard, interoperable, and secure credential: the PIV credential
- Consistent processes for identity vetting, proofing

But how about mobile devices?

- *Interoperability*: Leverage the same PKI infrastructure
- *Cost-savings*: Take advantage of the trust and identity-proofing performed for 5 million issued PIV cards
- **Approach**: Consider alternative methods to use PIV cards in mobile devices, and alternative form factors to store PIV credentials

Guidelines and Analysis:

- Draft NIST SP800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*
- Draft NIST IR 7981, *Mobile, PIV, and Authentication*
- **Available at:** <http://csrc.nist.gov>



Public Safety Communications

- 9/11 Commission Report recognized the need for a nationwide interoperable communications network for public safety
- Middle Class Tax Relief Act of 2013
 - Established a nationwide interoperable public safety network based on Long Term Evolution (LTE) technology with a special spectrum allocation
 - Created an independent entity within NTIA called FirstNet to deploy, operate, and maintain the nationwide interoperable public safety network
- Public Safety Communication Research (PSCR) – Joint NIST/NTIA program to conduct research, development, and testing
- NIST is conducting research into mobile apps for public safety, identity management, and participating in public safety standards development
 - Contributor in 3GPP working groups
 - Support National Public Safety Telecommunications Council's (NPSTC) efforts to develop high-level requirements



Public Safety Security Activities

- Draft NIST IR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*
 - Focus on identity credential technologies for mobile devices
 - Draft available at:
<http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8014>
- Mobile App Security Experiment
 - Seven public safety mobile apps from the Association of Public-Safety Communications Officials (APCO) AppComm website
 - Used AppVet framework with third-party test tools

More Information

Documents available at:

csrc.nist.gov

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov

