Vetting the Security of Mobile Applications

Steve Quirolgico
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

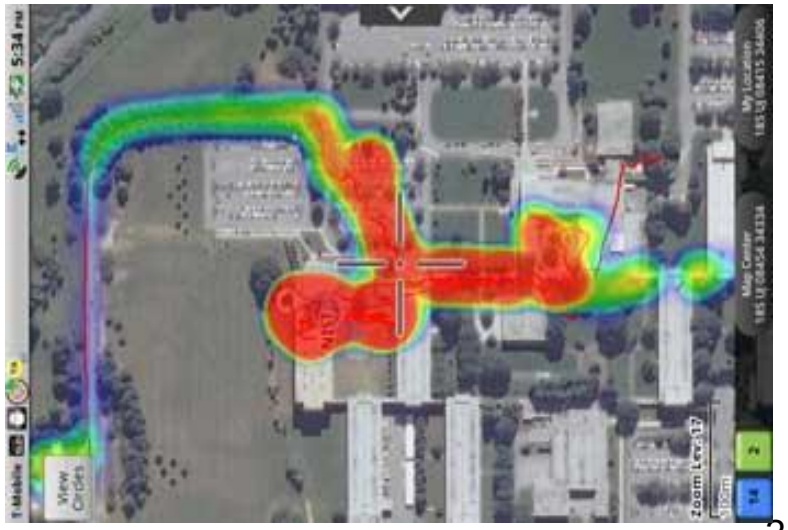
FCSM 2015
Gaithersburg, MD
August 26, 2015

DARPA Transformative Applications (TransApps)

DARPA TransApps focused on the use of smartphone applications (apps) for tactical use.

TA Apps:

- Provided mission-critical, leading-edge capabilities:
  - Weaponry
  - Medical/First-Aid
  - Cultural/Language
  - Mapping/Recon/Logistics
  - Tactical Information Sharing
- Deployed on latest smartphone devices
- Significantly improved combat operations
- Saved the lives of U.S. soldiers

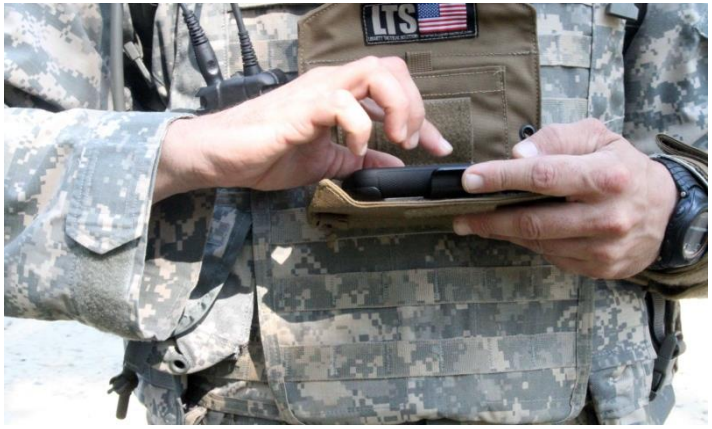


TransApps Security

Security of smartphone technologies was crucial for protecting sensitive information and ensuring proper operation.

Security Needed to Prevent:

- Unauthorized access to PII, geo-location, or other sensitive information
- Unauthorized network communication
- Unauthorized audio/video recording
- Unintended app or device behavior
- Resource (memory, CPU, *etc*.) exhaustion
- Shortened battery life
- **Mission failure**



App Vulnerabilities

- **Thousands of vulnerabilities exist for Android and Apple iOS apps**
- **On average, an app contains 14 vulnerabilities***
- **Types of vulnerabilities include:**
  - Exposed Communication
  - Incorrect Permissions
  - Dangerous or Hidden Functionality
  - Traditional Software Vulnerabilities
- **TA Apps include:**
  - Commercial/COTS (no source code)
  - Government-Developed/GOTS
  - Open-Source

***Cenzic, *Application Security Trends Report*, 2014.**

Hardware/OS Security

Focused on the development of hardened COTS Android devices (referred to as PANTHR devices).

- **Modified Android OS**
- **Hardware Security Stack**
  - CVE Patched Linux Kernel
  - Data At Rest Protections
  - Data In Transit Protections
  - Device Integrity Checks
  - Device Authentication

Application Security

Focused on securing software applications

- **App Functional Testing:** Ensure that apps provided the intended functionality
- **App Vetting (NIST/CSD):**
  - Investigate apps for vulnerabilities and malware
  - Determine if apps are in accordance with organizational security policies and requirements
- **App Acquisition:** Develop an app store for deploying *only vetted* apps onto PANTHR devices.

NIST App Vetting Contributions

1. Formulated the *App Vetting Process*
2. Developed and deployed a system called the *App Testing Portal* (ATP) for managing and automating the TransApps app vetting process
   - Afghanistan (2011-Present)
   - Presidential Inauguration (2013)
   - Boston Marathon (2013-2014)
   - Other USG operations (2011-Present)
3. Published NIST SP800-163, *Vetting the Security of Mobile Applications*, that described the app vetting process as well as issues, recommendations and lessons-learned during the development and deployment of ATP

NIST SP800-163, Vetting the Security of Mobile Applications

SP800-163 is intended to help organizations:

- understand the process for vetting the security of mobile applications
- plan for the implementation of an app vetting process
- develop app security policies and requirements
- understand the types of app vulnerabilities and the testing methods used to detect those vulnerabilities
- determine if an app is acceptable for deployment on the organization's mobile devices

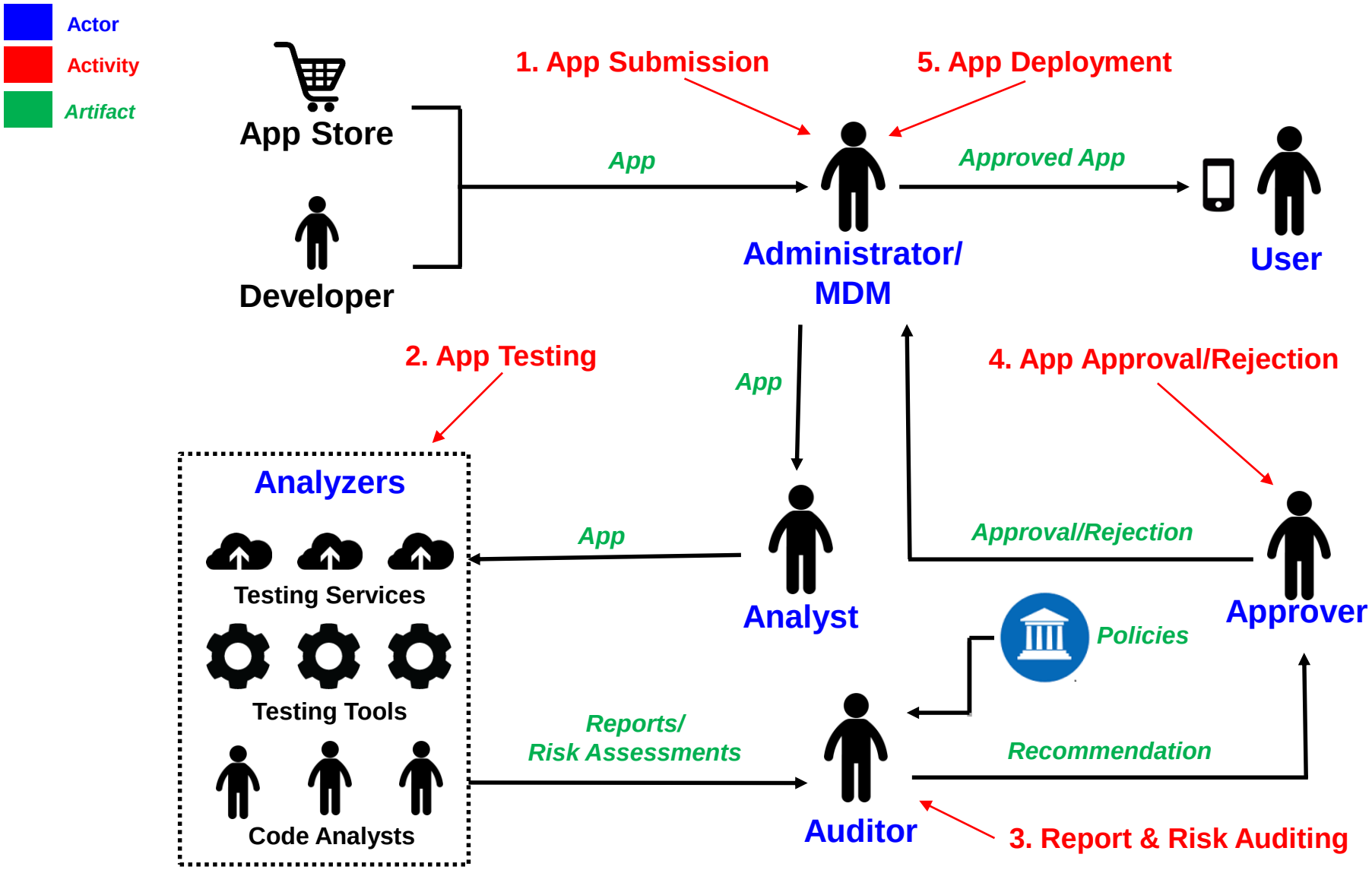
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf

App Vetting Process

The app vetting process is a sequence of activities:

- for investigating the security, reliability, and efficiency of apps (i.e., testing for vulnerabilities and malware)
- for determining if apps are in accordance with organizational security policies and requirements (usually regarding usage)
- that is performed after apps have been developed and released for distribution but prior to deployment

Workflow


Actor
Activity
Artifact
App Store
Developer
1. App Submission
5. App Deployment
App
Approved App
Administrator/
MDM
User
2. App Testing
App
4. App Approval/Rejection
Analyzers
Testing Services
Testing Tools
Code Analysts
App
Analyst
Approval/Rejection
Approver
Policies
Reports/
Risk Assessments
Recommendation
Auditor
3. Report & Risk Auditing

Benefits

App vetting process benefits include:

- **Adaptable:** Can be modified to fit organizational needs
- **Implementation-Agnostic:** Can be implemented as a manual or automatic system (e.g., ATP)
- **Simple but Powerful:** Simple and intuitive process provides framework for uncovering a host of issues (e.g., aggregation of disparate tool reports)
- **Monitoring:** Sequence of activities can be monitored for performance, efficiency, etc.

Planning an App Vetting Process Implementation

Planning involves:

- specifying the organization's app security policies and requirements:
  - General requirements (vulnerabilities and malware)
  - Context-Sensitive (usage)
- procuring an appropriate budget and staff
- understanding the limitations of app vetting

Specifying General (Vulnerability/Malware) Requirements

- Specify software characteristics or behavior that an app should or should not (e.g., specific vulnerabilities) exhibit
- Examples:
  - Apps must not leak personally identifiable information (PII)
  - Apps should include only those permissions required to perform their intended functionality
- The satisfaction or violation of a general requirement must be determined by an Analyzer (e.g., test tool). If an Analyzer detects a software behavior or characteristics that the app should not exhibit (e.g., vulnerability), the app is considered to be in violation of a general requirement of the organization.

Specifying Context-Sensitive (Usage) Requirements

- Specify how an app should be used by the organization to ensure the organization's security posture
- Examples:
  - Apps that access a network must not be used in a sensitive compartmented information facility (SCIF)
  - Apps that record audio or video must only be used by classified personnel
- The satisfaction or violation of a context-sensitive requirement must be determined by an Auditor using organization-specific vetting criteria
- Examples of organization-specific vetting criteria:
  - The app's intended set of users
  - The app's intended deployment environment

Procuring Budget and Staff

- Ensure Auditors are properly trained in software assurance, analyzer reports/risk assessments, and the organization's security policies and requirements
- Budget:
  - Equipment, licensing (Analyzer Tools and Services)
  - Salaries (Auditors, Administrators, etc.)
- Review the organization's mobile hardware and OS for security controls that might already address security/privacy requirements (e.g., encrypted file system)

Limitations of App Vetting

- May be difficult to ascertain the degree to which app vetting improves the organization's security posture
- Results will vary depending on the quality of the Analyzers, Auditors, *etc*.

App Testing

- Involves the testing of apps for software vulnerabilities by Analyzers that may be internal or external to the organization
- Involves generating reports and risk assessments
- Risk assessments:
  - estimate the likelihood that a detected vulnerability will be exploited by an attacker
  - estimate the impact that a detected vulnerability may have on the app or its related device or network
  - are often represented as ordinal values indicating the severity of the risk (e.g., low-, moderate-, and high-risk)

Testing Approaches

- Correctness Testing
- Source Code vs. Binary Code
- Static vs. Dynamic Analysis
- Automated Tools
  - Disclaimer: NIST is prohibited from recommending or endorsing commercial testing entities, products, equipment, or materials
- Sharing Results/Leveraging Existing Reports
  - Significantly reduces cost and effort
  - Reference vulnerability repositories including the National Vulnerability Database (NVD)

Recommendations

- Ensure that Analyzers detect vulnerabilities that satisfy or violate the organization's general app security requirements
- Leverage existing test results if possible
- Leverage multiple analyzers to increase vulnerability detection coverage
- Understand security implications (integrity, IP, and licensing issues) of sending app file to third-party analyzers

Auditing/Approval

- Involves Auditors that examine reports and risk assessments from Analyzers, as well as organization-specific vetting criteria against context-sensitive requirements to generate recommendations
- Organization-specific vetting criteria includes:
  - Target set of users
  - Target deployment environment
  - Provenance (Identity of developer, developer's organization/reputation, app store consumer reviews, *etc*.)
- An Approver assesses recommendations from Auditors and considers other non security-related issues to determine the official approval or rejection of an app

Recommendations

- Identify organization-specific vetting criteria
- Ensure that organization-specific vetting criteria can be used to determine the satisfaction or violation of context-specific requirements
- Ensure sufficient training of auditors on organizational security requirements and interpretation of analyzers' results
- Monitor vulnerability repositories to keep abreast of new developments

Questions