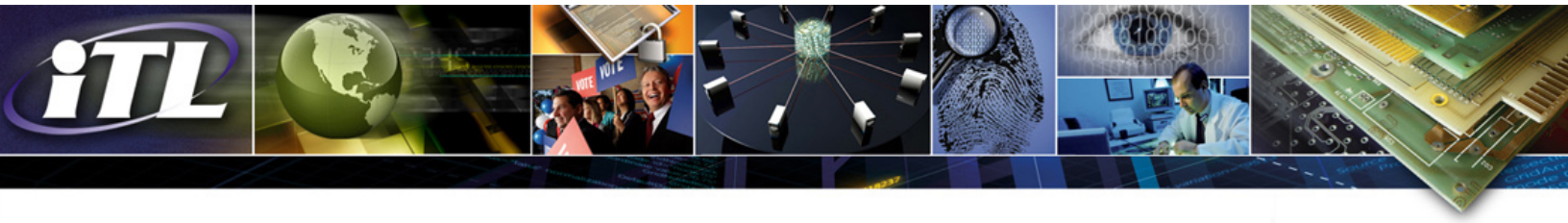


ITL BULLETIN FOR MARCH 2015

GUIDANCE FOR SECURE AUTHORIZATION OF MOBILE APPLICATIONS IN THE CORPORATE ENVIRONMENT

Tom Karygiannis, Steve Quirolgico, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

Recently, organizations have begun to deploy mobile applications (or "apps") to facilitate business processes. Such apps have increased productivity by providing an unprecedented level of connectivity among employees, vendors, and customers. As with all new technologies, new capabilities may introduce new security and privacy risks, and in this respect, mobile apps are no different. This is so because, like traditional enterprise applications, apps may contain software vulnerabilities that are susceptible to attack. Such vulnerabilities may be exploited by an attacker to gain unauthorized access to an organization's information technology resources or the user's personal data.

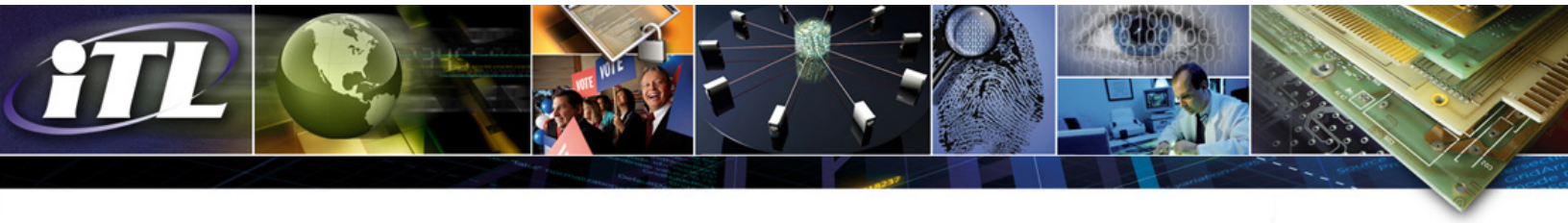
Such vulnerabilities are noteworthy for an individual, but of even more concern to an organization. Like the proverbial "weakest link" in a chain, there is a risk that a single insecure device can jeopardize the security of an organization. Because of this risk, such organizations should develop a mobile security policy and assess apps to ensure that they comply with this policy.

Introduction

ITL has released a new publication, NIST Special Publication (SP) 800-163, *Vetting the Security of Mobile Applications,* which provides guidance for organizations looking to the security of mobile applications as employees move to mobile devices such as smartphones and tablets for their work and their applications.

SP 800-163 provides guidance to help organizations to:

- Understand the process for vetting the security of mobile applications;
- Plan the implementation of an app vetting process;
- Develop app security requirements;
- Understand the types of app vulnerabilities and the testing methods used to remove those vulnerabilities; and
- Determine acceptability of apps to be deployed on the organization's mobile devices.



The publication describes the major differences between traditional and mobile application security issues.

Security Vulnerabilities in Mobile Applications

Because mobile application developers are working to reach a market of millions of users very quickly, some may not take the time to perform comprehensive software tests on their code before making it available or may not have the know-how to employ secure programming practices. This can result in the release of applications that contain functionality flaws and/or security-relevant weaknesses. On rare occasions, some developers may even introduce weaknesses intentionally for their own gain.

NIST encourages the use of new and emerging technologies, and few have more beneficial impact than the expansion of the mobile environment. It is wise to balance the benefits with the potential risks to ensure that this technology is safely introduced. Recently, the security community has observed the following needs:

- Consider the potential for abuse of login credentials provided to applications that offer widgets to access financial institutions or payment providers;
- Review the potential for release of personal information from applications such as streaming audio/video applications; and
- Ensure that applications supporting access to popular services such as social media sites do not expose users to identity theft by saving authentication keys in easily accessible, unencrypted plain text files.

Another risk is the potential issue that some mobile apps request excessive access, or access to device services that are unrelated to the app's intended function (e.g., a calculator app that seeks permission to make phone calls or access contacts). A recent *PC World* article reports that, "Many mobile apps request too many permissions and don't explain how they collect users' personal information, a study of 1211 popular apps by the Global Privacy Enforcement Network has found." [1] An application with such excessive permissions may be used for malicious purposes, such as to turn on a microphone to eavesdrop on sensitive corporate discussions.

These issues can leave an app, the user's device, and the user's network vulnerable to exploitation by attackers. Developers and users of these apps often tolerate buggy, unreliable, and insecure code in exchange for the low cost.

App Vetting Process

To help organizations ensure that an app conforms to predefined security requirements, SP 800-163 provides an app vetting process. An app vetting process is a sequence of activities that aims to determine if an app conforms to the organization's security requirements. This process is performed on an app after the app has been developed and released for distribution, but

prior to its deployment on an organization's mobile device. Thus, an app vetting process is distinguished from software assurance processes that may occur during the software development life cycle of an app. An app vetting process consists of a sequence of two main activities: *app testing* and *app approval/rejection*. The publication provides an overview of these two activities and gives recommendations for planning the implementation of an app vetting process. Figure 1 shows the major steps and actors of the process.

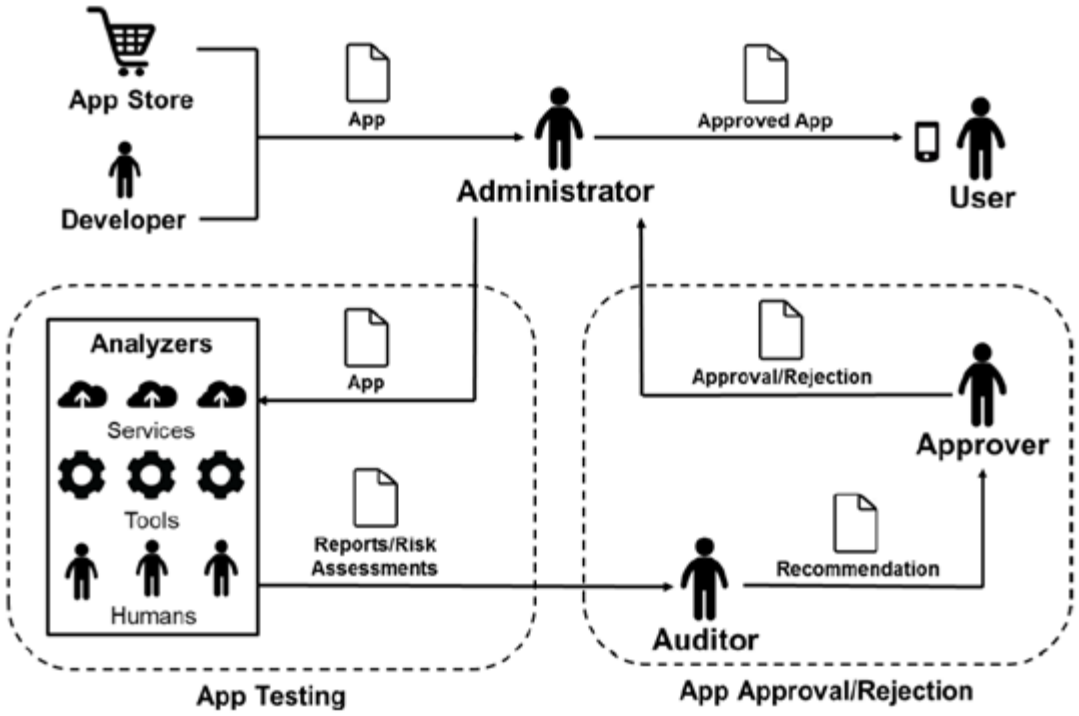
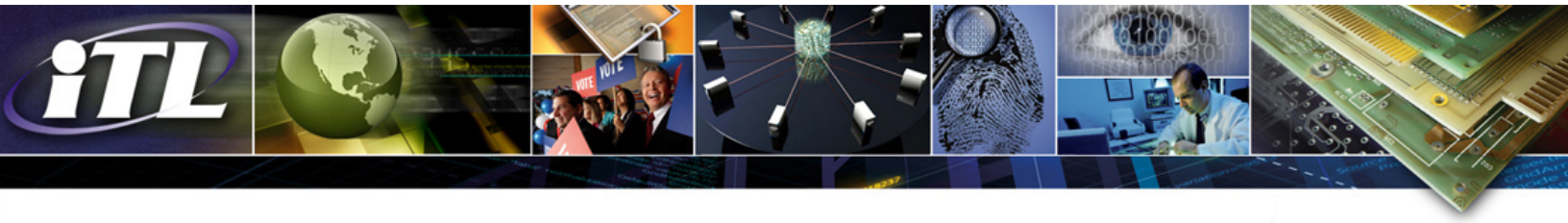


Figure 1: An app vetting process and its related actors.

Security Requirements Development

SP 800-163 describes two types of an organization's app security requirements: *general* and *context-sensitive*. A general requirement is an app security requirement that specifies a software characteristic or behavior that an app should exhibit in order to be considered secure. For an app, the satisfaction or violation of a general requirement is determined by analyzers that test the app for software vulnerabilities during the app testing activity of an app vetting process. If an analyzer detects a software vulnerability in an app, the app is considered to be in violation of a general requirement.



A context-sensitive requirement is an app security requirement that specifies how apps should be used by the organization to ensure the organization's security posture. For an app, the satisfaction or violation of a context-sensitive requirement is not based on the presence or absence of a software vulnerability and thus cannot be determined by analyzers, but instead must be determined by an auditor who uses organization-specific vetting criteria for the app during the app approval/rejection activity of an app vetting process. If an auditor determines that the organization-specific vetting criteria for an app conflicts with a context-sensitive requirement, the app is considered to be in violation of the context-sensitive requirement.

App Testing

SP 800-163 provides guidance on how to test apps against general requirements by using specific analysis tools. The publication describes the types of app vulnerabilities and the testing methods to use to detect them. In particular it provides descriptions of specific Android and iOS app vulnerabilities.

Conclusion

SP 800-163, *Vetting the Security of Mobile Applications*, encourages organizations to include mobile applications in the system authorization process, using security context and categorization to ensure that these apps do not jeopardize important business systems. It encourages testing and education to support information security. As organizations adopt the Bring-Your-Own-Device (BYOD) model, and as employees integrate mobile devices (e.g., smartphones and tablets) into their work and applications, organizations should consider these recommendations to maintain effective risk management.

[1] L. Constantin, “Privacy Lapses Riddle Majority of Mobile Apps, Data Protection Authorities Find,” *PC World* (September 12, 2014). Retrieved from http://www.pcworld.com/article/2682712

ITL Bulletin Publisher: Elizabeth B. Lennon

Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov