NISTIR 8136

An Overview of Mobile Application Vetting Services for Public Safety

Gema Howell
Michael Ogata

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8136

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

NISTIR 8136

An Overview of Mobile Application Vetting Services for Public Safety

Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Michael Ogata
Software and Systems Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8136

January 2017

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report
17 pages (January 2017)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8136

Certain commercial entities, equipment, or materials may be identified in this document 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.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: nistir8136@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The Middle Class Tax Relief Act of 2012 mandated the creation of the Nation's first nationwide, high-speed communications network dedicated for public safety. The law instantiated a new federal entity, the Federal Responder Network Authority (FirstNet), to build, maintain, and operate a new Long Term Evolution (LTE) network. This network has the potential to equip first responders with a modern array of network devices. Mobile applications stand to be an important resource that will be utilized by this network. However, current mobile application developers may not be aware of the unique needs and requirements that must be met for operation on FirstNet's network. It would benefit the public safety community to leverage the mobile application vetting services and infrastructures that already exist. These services currently target the general public and enterprise markets. This document is intended to be an overview of existing mobile application vetting services and the features these services provide and how they relate to public safety's needs. It is also meant to aid public safety organizations when choosing which mobile application vetting services are used to evaluate relevant mobile applications.

Keywords

Application Vetting; Mobile applications; security; software assurance; software testing

Table of Contents

List of Appendices

List of Figures

1 Purpose & Scope

The creation of the Nation’s first dedicated broadband network for public safety stands to bring a boon of data and functionality directly into the hands of first responders. Mobile applications will be the delivery mechanism for much of this data. NIST Interagency Report 8018 [5] recommends that public safety organizations should evaluate mobile applications for security before allowing them access to the Nationwide Public Safety Broadband Network (NPSBN). Furthermore, the report suggests leveraging the existing mobile application vetting services. These vetting services largely target existing personal, enterprise, and federal markets but do not yet cover the specific needs of public safety.

An application vetting process is a sequence of activities that aims to determine if an application conforms to the organization’s security requirements [1]. The phrase *mobile application vetting* is used in this document to describe a product or entity that provides portions of the mobile application vetting process externally as a service. This contrasts with tools that can be used internally by an organization to evaluate mobile applications. This document focuses on services over tools because of its intended public safety audience. While mobile applications stand to become an excellent tool to aid in the fulfillment of public safety’s varied missions, the expertise required to evaluate these mobile applications is well outside of public safety’s traditional core skill set. Furthermore, requiring individual public safety organizations to acquire the technical competency to vet applications would be an extra strain on public safety’s resources.

The purpose of this document is to be a high-level investigation of application vetting services with the goal of enumerating the traits they exhibit which may be useful to public safety. Presently, there is no common language to describe mobile application vetting services. This document provides an overview of some mobile application vetting services available when this document was developed. This report is in no way intended to be an evaluation of the quality or the efficacy of these services. A quantitative study to validate the claims of these services is out of scope for this effort. Inclusion or omission of vetting services from this document in no way implies an endorsement or disapproval on behalf of NIST.

2 Document Structure

This document is divided into five additional sections. Section 3 provides a brief primer to mobile application vetting. Section 4 lists the vetting services considered for review. Section 5 defines a set of features used to describe the services researched. Section 6 contains a table summarizing the results of the investigation. Finally, Section 7 summarizes this effort’s overall observations and conclusions.

3 Mobile Application Vetting

This section provides a brief overview of the mobile application vetting process and why that process is relevant to public safety. A more complete description of the vetting process can be found in NIST Special Publication (SP) 800-163 Vetting the Security of Mobile Applications [1]. Concisely, mobile application vetting is a strategy used to inform the decision of whether a mobile application should be permitted for use within an IT infrastructure. NIST SP 800-163 defines the application vetting process as being made up of four activities:

1. **Selection** – Obtaining applications from the two general sources: public application marketplaces (Google Play, iTunes, Amazon, etc.) and custom built applications that are not made available in public marketplaces.
2. **Testing** – Applying tools, evaluation techniques, and analysis methods to determine if an application meets the usability and security requirements of the organization.
3. **Approval/Rejection** – Issuance of the go/no go decision based on the outcome of the testing activates
4. **Deployment** – Making an approved application accessible to the appropriate users within the IT infrastructure.

Consider the following scenario as a high-level example of NIST SP 800-163 in practice:

> *Jan is the IT security officer for the local fire department. Her responsibilities include ensuring the mobile devices used by the staff of the department meet the security requirements established by her organization. The firefighters at this department wish to use a new, publicly available (that is, available from a public app store), mobile application that accesses a database of hazardous materials. The firefighters wish to install this application on their department-issued mobile device for use during their mission. Using the mobile application vetting process, Jan learns the application attempts to access the GPS location of the mobile device while also making remote connections to unknown servers via the internet. Thus, Jan denies the firefighters request for use of the application.*

This document describes organizations that provide the testing activity as a service. These organizations attempt to provide assurance that the application being evaluated does not exhibit undesirable behavior.

Undesirable behavior is characterized as anything a mobile application can to do violate the confidentiality, integrity, and/or availability of data or functionality associated with the mobile application. This extends to behavior that affects the device on which the application is running as well as any other entity to which the application connects (back-end servers, other mobile devices, network infrastructure, etc.). Undesirable behavior can be introduced into a mobile application through one of two paths: malice and software weakness. Malicious undesirable behaviors include viruses, trojans, adware, and spyware. That is, behaviors designed with the intent to violate confidentiality, integrity, and/or availability. Software weaknesses introduce undesirable behavior by way of flaws of design that expose an application to a form of attack. Improper mobile device resource requests, the inclusion of flawed libraries, misconfiguration, incorrect encryption mechanisms, or poorly handled user input can all open an application to outside attack.

This document focuses on mobile application vetting services instead of providing an exhaustive analysis of mobile application vetting techniques. The skills and techniques required to analyze mobile applications are specialized and constantly evolving. The information security infrastructure currently present within the public safety community will either be required to expand its technical expertise to accommodate mobile application testing or rely on mobile application vetting services to test applications on their behalf.

4 Methodology and List of Considered Vetting Services

Research was performed to explore the features offered by mobile application vetting services. A web search of "mobile application security testing" and "mobile application testing" provided a list of companies with some variant of a mobile application vetting service; some who specialize in performing application vetting services and other companies who provide a variety of services including some mobile application testing or scanning. A quantitative study to the claims of these services is out of scope for this effort. Instead the marketing material for each service was examined and common functionality features (see Section 5) were extracted.

The following table lists the mobile application vetting services that ranked prominently in the search results. They are presented in alphabetical order along with the date they were evaluated.

Table 1 - Mobile Application Vetting Service List

Mobile Application Vetting Service	Month Accessed
Aspect Security	03/2016
Applause App Quality	03/2016
AppSec Labs	03/2016
Appthority	03/2016
Cigital	03/2016
Foregenix	03/2016
Kryptowire	04/2016
Lookout	03/2016
Netcraft	03/2016
NetSPI	03/2016
NowSecure	06/2016
Paladion	03/2016
Veracode	03/2016

5 Mobile Application Vetting Service Feature Descriptions

The goal of this exercise is to gain understanding of the features offered by services in the mobile application vetting space. The following list of features was derived from the analysis of the mobile application vetting services mentioned in the previous section. Features were established according to common characteristics found within each mobile application vetting service. This section describes each feature and provides details on how the information may be beneficial to public safety.

5.1 Laboratory Analysis

Mobile application analysis can occur within a vetting organization's testing infrastructure. This analysis can employ techniques such as decompilation, reverse engineering, penetration testing, etc. Public safety should be aware of these techniques as requiring their use may imply application developers to accede to this type of testing. There are three main methods a vetting service can use when evaluating a mobile application: static application analysis, dynamic application analysis and penetration testing. These methods are briefly described below.

Static Analysis

Static analysis applies testing techniques to an application that is not being run. This includes, but is not limited to, analysis of an application's source code, executable files, and design documentation.

Dynamic Analysis

Dynamic analysis describes techniques used on apps running in virtual testing environments or on physical devices housed within the laboratory. However, depending on the requirements of the vetting service, mobile application developers may be required to expose their source code to enable this type of testing.

Penetration Testing

Penetration testing is generally a form of manual testing where a penetration tester performs attacks on software in search of vulnerabilities. Per NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment [2], "Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network." Penetration testing has the advantage of incorporating non-technical methods of attack such as social engineering or breaching physical security controls. However, penetration testing is very labor intensive and requires targeted expertise to be effective.

5.2 On Device Analysis

Vetting organizations may choose to extract data from client mobile devices, in real time, as a means of strengthening their understanding of real-time threats to the mobile application ecosystem. Information such as the list of running/installed applications, the identities of accessed remote servers, as well as specific behaviors of running applications can help vetting organizations identify undesirable behavior. This telemetry may be transmitted back to the vetting service for storage and analysis. Public safety should be made aware of what types of data are being exfiltrated from their devices even if that data is intended for benign use by the vetting organization.

5.3 Pricing Models

The pricing model feature conveys whether the vetting service provider offers their service free of charge or requires the customer to purchase their services. Possible pricing models include: per month, per year, per user, and per application (as well as combinations thereof). Public safety should be aware of the costs involved for mobile application vetting services.

5.4 On Demand Scanning

The mobile application ecosystem is large and constantly evolving. Depending on the depth of testing, mobile application vetting can be a time-intensive operation. This makes analysis of all known mobile applications unfeasible. As such, mobile application vetting services have different models for how they choose what applications they take under consideration. Some may focus on apps that are popular in the major application stores. Others may allow their customers to make on-demand requests for applications to be investigated. The public safety application ecosystem will be smaller than the public commercial application stores, but may have a greater need for on demand application evaluation.

5.5 Target User Audience

Mobile application vetting services vary in their intended target audience. Understanding who application vetting services are targeting as their end users may benefit public safety organizations when choosing services for their own use. The categories below detail the different audience types that were observed as part of this research. This information is beneficial to public safety because it gives insight into how mobile application vetting services may support their needs. Note, these categories are not mutually exclusive as some vetting service may target multiple categories.

Enterprise

Mobile application vetting services may aim to provide services at an enterprise scale. This is to satisfy the desire of organizations that are looking to secure mobile applications used within their infrastructure. Enterprise scale solutions may have varying pricing models. They often work in conjunction with their enterprise clients to tailor their reporting and testing services to fit the specifics of the enterprise's mission. Solutions aimed at this audience may also integrate into other products, such as Mobile Device Management (MDM) / Enterprise Mobility Management (EMM) and Mobile Application Management (MAM) solutions, offered by the vetting service[1]. Differentiating between

[1] For more information concerning MDM and MAM technology, readers can consult [3] and [4] in Appendix A.

companies' solutions is out of scope for this document.

General Consumer

Vetting services may offer solutions targeted toward individual general consumers. These types of services are typically aimed at a wider audience than enterprise solutions. They tend to focus on general security issues as well as identifying malware.

Application Developers

Vetting services may work directly with mobile application developers. These services integrate their scanning and analysis techniques into a developer's software development lifecycle to provide feedback as applications are being developed.

5.6 Supported Platforms

Evaluating a mobile application may require specialized techniques and expertise depending on what platform the mobile application was intended to run on. As such, mobile application vetting services often make claims as to which mobile application platforms they support. Two subcategories were observed as common platforms supported by services.

1. Mobile Operating platform (e.g. iOS, Android, Blackberry, Windows ,etc.)

2. Web applications (i.e. applications targeted to run on a mobile device's browser)

Understanding which platforms a mobile application vetting service supports benefits public safety by allowing them to choose services that meet the needs of the devices in use.

5.7 Customer Application Repository

Customer application repositories are storage containers provided as a service for customers to submit and store information about specific mobile applications. The applications stored in such repositories may be comprised of both publicly available applications as well as custom built applications. The purpose of these repositories is to provide the user with a central location to review, update, and reanalyze specific mobile applications. This feature may be of interest to public safety because it shapes how a customer interacts with the mobile application vetting service.

5.8 Commercial Application Dataset

A commercial application dataset is a listing of mobile applications which are currently available in the commercial application stores. These applications have been vetted by the service provider and the list is provided to the customer as part of their product. Public safety may use this data set to evaluate general purpose applications which may be used on public safety devices.

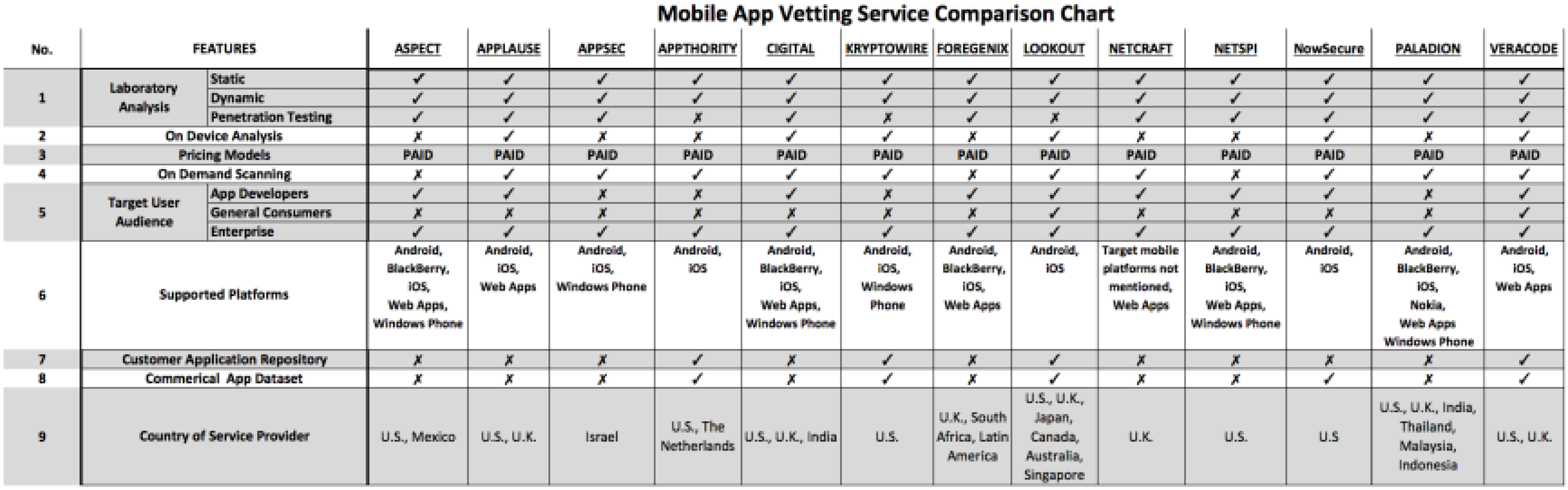
5.9 Country of Service Provider

The country of the service provider is the location at which the vetting service provider originated or has office locations. Public safety should be aware of where their information is going and where it is being stored. Some service providers may be found outside of the U.S.

6 Mobile Application Vetting Feature Enumeration

Figure 1 illustrates an enumeration of the data collected from the mobile application vetting services feature research. When looking over each vetting service's website, the list of features was used to note findings. Details within the chart reflect the vendor claims and have not been validated.

Figure 1 - Mobile Application Vetting Services Research Data



Mobile App Vetting Service Comparison Chart

No.	FEATURES		ASPECT	APPLAUSE	APPSEC	APPTHORITY	CIGITAL	KRYPTOWIRE	FOREGENIX	LOOKOUT	NETCRAFT	NETSPI	NowSecure	PALADION	VERACODE
1	Laboratory Analysis	Static	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Dynamic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Penetration Testing	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓
2	On Device Analysis		✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓
3	Pricing Models		PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID	PAID
4	On Demand Scanning		✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
5	Target User Audience	App Developers	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓
		General Consumers	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓
		Enterprise	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Supported Platforms		Android, BlackBerry, iOS, Web Apps, Windows Phone	Android, iOS, Web Apps	Android, iOS, Windows Phone	Android, iOS	Android, BlackBerry, iOS, Web Apps, Windows Phone	Android, iOS, Windows Phone	Android, BlackBerry, iOS, Web Apps	Android, iOS	Target mobile platforms not mentioned, Web Apps	Android, BlackBerry, iOS, Web Apps, Windows Phone	Android, iOS	Android, BlackBerry, iOS, Nokia, Web Apps Windows Phone	Android, iOS, Web Apps
7	Customer Application Repository		✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✓
8	Commerical App Dataset		✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓
9	Country of Service Provider		U.S., Mexico	U.S., U.K.	Israel	U.S., The Netherlands	U.S., U.K., India	U.S.	U.K., South Africa, Latin America	U.S., U.K., Japan, Canada, Australia, Singapore	U.K.	U.S.	U.S	U.S., U.K., India, Thailand, Malaysia, Indonesia	U.S., U.K.

7 Observations and Conclusions

The market of mobile application vetting services continues to grow and evolve daily. This continual expansion has led to the development of mobile application testing services focusing and specializing in different aspects of the mobile application vetting problem. It is essential for public safety to acquire knowledge of all types of analysis to narrow down which service performs the tests necessary to provide security through a public safety mobile application.

Some key conclusions found during research are:

- In general, all mobile application vetting services provide static and dynamic analysis, which are both assessments performed in-house at the service's laboratory. A more infrequently observed technique was client-side/real-time analysis.
- The on demand scanning model was the most prevalent in the services researched.
- All the services researched focused on enterprise users.
- Seven of the eleven application vetting services made mention of including application developers in their processes.
- Two services target the general consumer market.
- Android and iOS are the most common operating platforms supported. Many services also target web applications.

7.1 Areas for Further Consideration

7.1.1 Public Safety Specific Analytic Features

NISTIR 8018, Public Safety Mobile Application Security Requirements Workshop Summary, identifies six areas of concern for mobile application security that are specific to public safety [5]. Three of the areas identified in that document have requirements that could be evaluated by mobile application vetting services. During the research, no services explicitly mentioned including these features as part of their analysis. The public safety community should investigate mobile application vetting services for their ability to evaluate the following areas.

Network Usage

Mobile applications for public safety will be required to operate during a variety of network conditions. An evaluation of how much and how efficiently an application interacts with the network may be important to public safety when evaluating mobile applications. Furthermore, public safety mobile networks will need a degree of protection from either intentional or unintentional abuse of network resources.

Battery life

The analysis of a mobile application's effect on a device's battery life may be vital information for public safety. Rapid depletion of a device's battery life may quickly render a public safety responder's mobile device unusable in an emergency situation. Evaluating the battery impact of a mobile application may empower public safety to choose applications that more efficiently use a limited resource.

Location information

Public safety has special requirements for location information when compared to general purpose applications. Real-time monitoring of a device's location must be protected and controlled to protect first responders. Furthermore, location information may need to be retained for auditing purposes. To aid these requirements, public safety applications must declare all location information being gathered and whether that data is transmitted, stored, or both.

7.1.2 Report Mechanism

Typically, an application vetting service provides analysis reports of the mobile applications being investigated. The technical expertise required to understand these reports, as well as the contents of the report, will vary from service to service. A public safety organization will need to analyze the form of the report supplied by a vetting service to decide whether it meets their requirements.

7.1.3 Report Redistribution

It is currently unclear what organization(s) have the authority for enforcing mobile application vetting for public safety. It may be the case that multiple organizations perform the function. The information gathered during the mobile application vetting process will be vital to improving the quality, usability, and security of public safety mobile apps. The sharing of lessons learned and test results will be critical to further these efforts. Furthermore, this information sharing will reduce redundant reexamination of mobile apps by different public safety organizations. As such, it may be important for public safety to be conscious of what rights they have for report redistribution when they engage with a mobile application vetting service.

Appendix A—References

[1] S. Quirolgico, J. Voas, and T. Karygiannis, NIST Special Publication 800-163 Vetting the Security of Mobile Applications. National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015, 44pp. http://dx.doi.org/10.6028/NIST.SP.800-163

[2] K. Scarfone, M. Souppaya, C. Cody, A. Orebaugh, NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology, Gaithersburg, Maryland, September 2008, 80pp. http://dx.doi.org/10.6028/NIST.SP.800-115

[3] M. Souppaya, K. Scarfone, NIST Special Publication 800-124 Revision 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, http://dx.doi.org/10.6028/NIST.SP.800-124r1

[4] J. Franklin, et al., Draft NIST Special Publication 1800-4 Mobile Device Security. National Institute of Standards and Technology, Gaithersburg, Maryland, November 2015. https://nccoe.nist.gov/publication/draft/1800-4b/

[5] M. Ogata, N. Hastings, and B. Guttman, Public Safety Mobile Application Security Requirements Workshop Summary. NISTIR 8018, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015. 56pp. http://dx.doi.org/10.6028/NIST.IR.8018