Publication Number: **NIST Interagency Report 8136**

Title: *An Overview of Mobile Application Vetting Services for Public Safety*

Publication Date: **January 2017**

- Final Publication: https://doi.org/10.6028/NIST.IR.8136 (which links to http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8136.pdf).
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

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

June 1, 2016

NIST IR 8136

DRAFT Mobile Application Vetting Services for Public Safety

The creation of the nation's first public safety broadband network (FirstNet) will require the vetting of mobile apps to ensure they meet public safety's cyber security requirements. It will be beneficial for the public safety community to leverage the mobile application vetting services and infrastructures that already exist. The purpose of this document is to be an informal survey of existing mobile application vetting services and the features these services provide. It also relates these features for their applicability to the public safety domain. This document is intended to aid public safety organizations when selecting mobile application vetting services for use in analyzing mobile applications.

Public comment period ends: ***June 30, 2016***.
Email comments to: MobileAppSurveyDraft @nist.gov.

Draft NISTIR 8136

Mobile Application Vetting Services for Public Safety

An Informal Survey

Gema Howell
Michael Ogata

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

Draft NISTIR 8136

Mobile Application Vetting Services for Public Safety

An Informal Survey

Gema Howell
Applied Cybersecurity Division
Information Technology Lab

Michael Ogata
Software and Systems Division
Information Technology Lab

June 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8136 (Draft)
17 pages (June 2016)

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.

Public comment period: ***June 1, 2016*** **through** ***June 30, 2016***

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

All comments are subject to release under the Freedom of Information Act (FOIA).

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 equipped with 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. The purpose of this document is to be an overview of existing mobile application vetting services, the features these services provide and how they relate to public safety's needs. This document is intended to aid public safety organizations when selecting mobile application vetting services for use in analyzing mobile applications.

Keywords

application vetting; FirstNet; mobile applications; security.

Table of Contents

List of Appendices

List of Figures

1 Introduction

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 this data. NIST Interagency Report 8018 makes the recommendation 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 app vetting process is a sequence of activities that aims to determine if an app conforms to the organization's security requirements [1]. The phrases mobile application vetting service and app vetting service are used interchangeably in this document to describe a product or service that engages in this process.

The purpose of this document is to be a high level investigation of app 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 not intended to be an evaluation of the quality or the efficacy of these services. Inclusion or omission of vetting services from this document in no way implies an endorsement or disapproval on behalf of NIST.

This document is divided into four additional sections. Section 2 lists the vetting services considered for review. Section 3 defines a set of features used to describe the services surveyed. Section 4 contains a table summarizing the results of the investigation. Finally, Section 5 concludes with overall observations and areas for further consideration.

2 List of Considered Vetting Services

Research was performed to explore today's mobile application vetting services. A web search of "mobile application security" 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. Below are the services that ranked prominently in the web search. These excerpts give a brief description of what the services claim to offer in the mobile application vetting space[1].

Aspect Security

> Aspect Security focuses exclusively on application security. We protect the applications that run your business.
>
> We can help your organization establish enterprise-wide application security strategies that are tailored to your needs. Business risk modeling, regulatory compliance, automation, developer training – Aspect understands all facets of your application security "big picture." We've worked with organizations worldwide, protecting critical applications in the government, defense, financial, healthcare, services and retail sectors. Let us bring that experience to bear on your environment.
>
> http://www.aspectsecurity.com/about (accessed 3/4/2016)

Applause App Quality

> Applause is leading the app quality revolution by enabling companies to deliver digital experiences that win - from web to mobile to wearables and beyond. By combining in-the-wild testing services, software tools, and mobile sentiment analysis, Applause helps companies achieve the 360° app quality™ they need to thrive in the modern apps economy.
>
> http://www.applause.com/about-us (accessed 3/4/2016)

AppSec Labs

> AppSec Labs is a vibrant team of professionals who love application security. Founded by Erez Metula, a world renowned application security expert and is the author of Managed Code Rootkits.
>
> Our mission is to raise awareness of the software development world to the importance of integrating software security across the development lifecycle.
>
> Our team has accumulated years of experience in penetration testing, consulting and training of secure coding and hacking at the highest level.

[1] Note, text copied from vetting service web pages may have been formatted for readability in this document.

> Our customer base is diverse, from financial, homeland security, governmental, e-commerce to hi-tech, we do our best to improve product security.
>
> Our endless curiosity drives us to continuous research of emerging technologies and platforms placing us at the top of the charts in our field.
>
> We are constantly researching and developing new professional tools to improve penetration testing for a multitude of platforms.
>
> AppSec Labs has positioned itself as a groundbreaker and leader in the field of mobile application security and is looking forward to the challenges of the new millennia.
>
> We are looking forward to helping you and your organization achieve the product security level you are seeking.
>
> https://appsec-labs.com/about_appsec_labs/ (accessed 3/4/2016)

Appthority

> Appthority was designed to provide a simple, yet scalable, way to manage mobile app risk to company data. Our mission is to identify, expose, and eliminate mobile app risk to the enterprise before it becomes a business-critical issue or crisis.
>
> https://www.appthority.com/company/ (accessed 3/4/2016)

Cigital

> Application Security Testing (AST) is a critical component of application security and the cornerstone of any software security initiative. Cigital’s testing experts combine multiple tools, custom scans and in-depth manual checks for an accurate security assessment that identifies critical risks and reduces false positives.
>
> https://www.cigital.com/services/application-security-testing/ (accessed 3/4/2016)

Foregenix

> We specialise in the following areas:
>
> - Compliance
>   - Including PCI DSS, PCI P2PE, PA-DSS and PCI PIN
> - Forensic Investigation Services
> - Security Testing
>   - (Internal and External Penetration Testing, Web Application, Mobile Application)
> - Cardholder Data Discovery Services
> - Merchant Risk Reduction Solutions
> - Security Training Courses
>
> http://www.foregenix.com/about.php (accessed 3/4/2016)

Kryptowire

> Kryptowire Enterprise integrates our cross-platform software assurance technologies with existing Enterprise Mobility Management (EMM) products, Android for Work, and Apple's iOS Device Enrollment Program (DEP) and Mobile Device Management (MDM) solutions to continuously validate the compliance and assesses the risk of all applications and devices against NIST and NIAP security standards, and enterprise-wide privacy and security policies.
>
> …Kryptowire's mobile app commercial software assurance tools can perform static and dynamic security analysis on third party iOS, Android, and Windows apps to give you valuable insight into what a mobile app actually does and identify programming practices that could put your user's privacy, data, and network resources at risk.
>
> As we collect, store, and continuously monitor mobile app data from unofficial and official marketplaces across all three major platforms, we can then begin unlocking a treasure trove of business and security intelligence using our proprietary machine learning algorithms.
>
> http://www.kryptowire.com/index.html (accessed 4/1/2016)

Lookout

> Lookout is a cybersecurity company focused on mobile. Protecting individuals and enterprises alike, Lookout fights cybercriminals by predicting and stopping mobile attacks before they do harm.
>
> https://www.lookout.com (accessed 3/4/2016)

Netcraft

> Netcraft's Mobile App Security Testing service provides a detailed security analysis of your phone or tablet based app. A key feature of this service is manual testing by experienced security professionals, which typically uncovers many more issues than automated tests alone.
>
> http://www.netcraft.com/security-testing/mobile-app-security-testing/
>
> (accessed 3/4/2016)

NetSPI

> Mobile computing, and it corresponding applications, are spreading faster than any other consumer technology in history. Gartner predicts that mobile app projects will outnumber PC projects 4-to-1 by 2015. It's not surprising that securing mobile apps, particularly around consumer privacy, is moving onto the front page. NetSPI is a highly disciplined mobile apps security expert with mature methods, a great toolbox, and experienced mobile applications testers.

https://www.netspi.com/our-solutions/application-assessment/mobile-app-pentest (accessed 3/4/2016)

Paladion

Paladion's mobile app security services is designed to bring about the right amalgamation of unrestricted innovation yet with a control over malicious attacks and threats while dealing with mobile application security. Paladion will make you strong with the defenses of not only the app itself, but also the servers it interacts with.

Understanding the risk and requirement for protection, Paladion has come up with two types of services MPT and SCR to make the application dodge bullets. We test the application for OWASP Top 10 as well as Plynt Mobile Application Certification Criteria.

http://www.paladion.net/security-testing/#mobile-security-testing (accessed 3/4/2016)

Veracode

Our behavioral analysis of mobile apps helps you determine which mobile apps violate enterprise policies for security and privacy — and why.

We provide a variety of mobile security solutions to accommodate the unique characteristics of mobile application development and deployment:

Mobile applications that you build. Our mobile security solution is a combination of automated analysis and program services that enables you to secure mobile applications during development so that security can be an innovation enabler.

Business mobile applications that you buy. Our mobile behavioral analysis engine provides intelligence and controls to help you detect which mobile apps violate your security policies.

Mobile applications your employees download under BYOD program. To help mitigate enterprise risk, our mobile security intelligence integrates with leading mobility device management (MDM) solutions.

http://www.veracode.com/solutions/by-need/mobile-security (acceded 3/4/2016)

3 Mobile App 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.

3.1 Laboratory Analysis

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

Static Analysis

Static analysis indicates applying vulnerability testing to an app that is not being run. This includes, but is not limited to, analysis of an app's source code, executable files, and design documentation.

Dynamic Analysis

Dynamic analysis describes techniques used on an app running in a testing environment. Both methods are viable forms of testing. However, depending on the requirements of the vetting service, mobile app developers may be required to expose their source code.

3.2 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. 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.

3.3 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 app. Public safety should be aware of the costs involved for mobile application vetting services.

3.4 On Demand Scanning

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

3.5 Target User Audience

Mobile application vetting services vary in their intended target audience. Understanding who app 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 (per user, per device, per app, etc.). 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) and Mobile Application Management (MAM) solutions, offered by the vetting service. Differentiating between the nuances between 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.

App 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.

3.6 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. Operating platform (e.g. iOS, Android, Windows, Blackberry, 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.

3.7 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.

3.8 Commercial Application Dataset

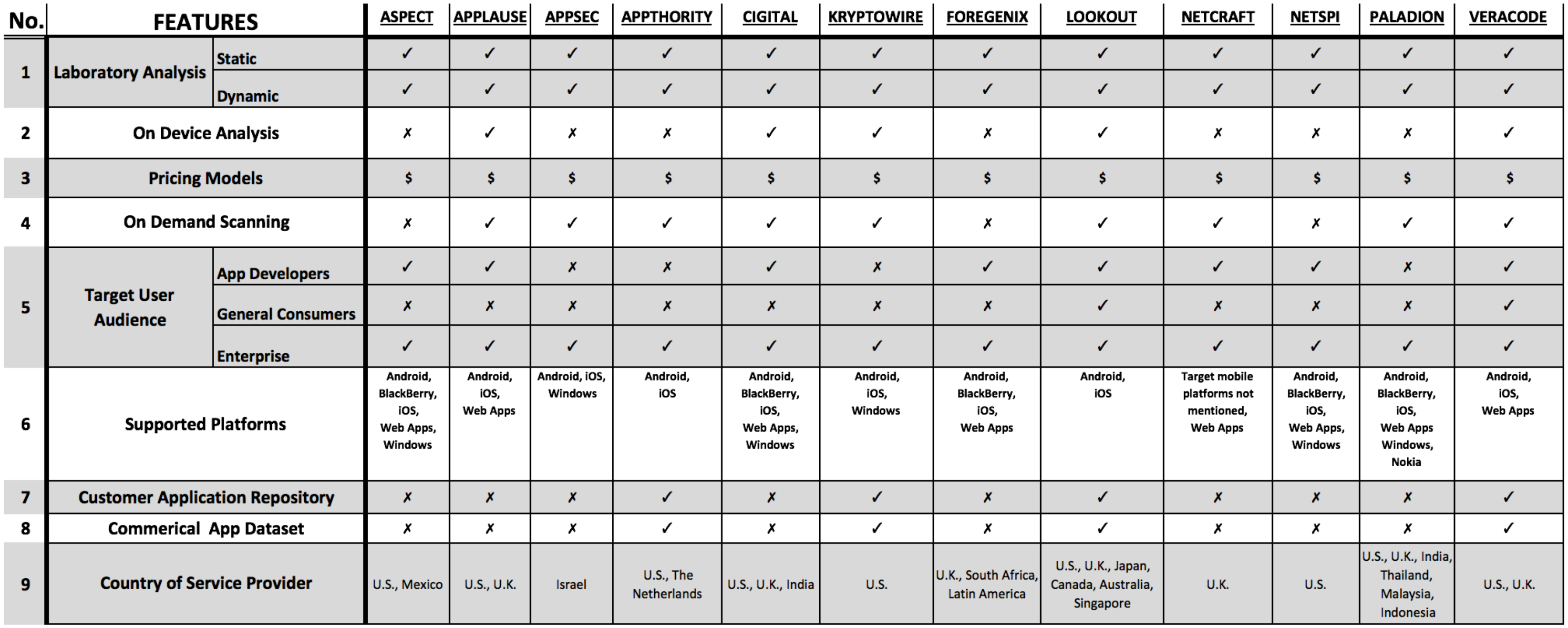
A commercial application data set is a listing of mobile applications which are currently available in the commercial app stores. These applications have been vetted by the service provider and the list is provided to the customer as part of their product. Public safety may use this data set to evaluate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

3.9 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 founded outside of the U.S.

4 Mobile App Vetting Feature Enumeration

Below is a chart (Figure 1) that is 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 do not necessarily portray definitive results in regards to whether the data collected accurately reflects the mobile application vetting services.



No.	FEATURES		ASPECT	APPLAUSE	APPSEC	APPTHORITY	CIGITAL	KRYPTOWIRE	FOREGENIX	LOOKOUT	NETCRAFT	NETSPI	PALADION	VERACODE
1	Laboratory Analysis	Static	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Dynamic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	On Device Analysis		✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓
3	Pricing Models		$	$	$	$	$	$	$	$	$	$	$	$
4	On Demand Scanning		✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓
5	Target User Audience	App Developers	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
		General Consumers	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓
		Enterprise	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	Supported Platforms		Android, BlackBerry, iOS, Web Apps, Windows	Android, iOS, Web Apps	Android, iOS, Windows	Android, iOS	Android, BlackBerry, iOS, Web Apps, Windows	Android, iOS, Windows	Android, BlackBerry, iOS, Web Apps	Android, iOS	Target mobile platforms not mentioned, Web Apps	Android, BlackBerry, iOS, Web Apps, Windows	Android, BlackBerry, iOS, Web Apps Windows, Nokia	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.K., India, Thailand, Malaysia, Indonesia	U.S., U.K.

Figure 1 - Mobile App Vetting Services Survey Data

5 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 in order 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 as follows:

- 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 surveyed.
- All of the services surveyed focused on enterprise users. Nearly all (7/11) made mention of including application developers in their processes. Only 2 services target the general consumer market.
- Android and iOS are the most common operating platform supported. Many services also target web applications.

5.1 Areas for Further Consideration

5.1.1 Public Safety Specific Analytic Features

The document Public Safety Mobile Application Security Requirements Workshop Summary identifies six areas of concern for mobile application security that are specific to public safety [2]. Three of the areas identified in that document have requirements that could be evaluated by mobile application vetting services. During the course of the survey, 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 retained for auditing purposes. To aid these requirements applications must declare all location information being gathered and whether that data is transmitted, stored, or both. When location information is transmitted, the application must declare where the location information is being transmitted.

5.1.2 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.

5.1.3 Report Redistribution

It is currently unclear who has the authority for enforcing mobile application vetting for public safety. It may be the case that multiple organizations take up the role. Information sharing is becoming more and more important in the effort to eliminate duplicated work. 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] 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