NISTIR 8018

Public Safety Mobile Application Security Requirements Workshop Summary

Michael Ogata
Barbara Guttman
Nelson Hastings

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8018

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

NISTIR 8018

Public Safety Mobile Application Security Requirements Workshop Summary

Michael Ogata
Barbara Guttman
Systems and Software Division
Information Technology Laboratory

Nelson Hastings
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8018

January 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

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

National Institute of Standards and Technology Internal Report 8018
56 pages (January 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8018

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8018@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

This document captures the input received from the half-day workshop titled "Public Safety Mobile Application Security Requirements" organized by the Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and the Department of Commerce and held on February 25, 2014. This first-of-its-kind workshop was attended by public safety practitioners, mobile application developers, industry experts, and government officials who contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications.

Acknowledgments

This publication was developed as part of the NTIA/NIST Public Safety Communication Research program with sponsorship from the Office for Interoperability and Compatibility (OIC) at the Department of Homeland Security (DHS). The authors would like to thank Jeff Cohen, Jay English, Mark Reddish, and Roger Wespe from Association of Public-Safety Communications Officials (APCO) International, Alex Kreilein from DHS/OEC, as well as the workshop participants for providing valuable feedback on drafts of this document. The authors would like to thank the following organizations for their public comment submissions: Intrado Inc., Secure Access Technologies, and the Mobile EAS Coalition.

Audience

This document is intended for members of the Public Safety community and mobile application developers who are interested in public safety mobile application security.

Keywords

Public safety; Mobile applications; FirstNet; First responders; Battery life; Denial of service; Application vetting; Data protection; Location information; Identity management;

Trademark Information

Table of Contents

1. INTRODUCTION 1

1.1 Workshop Organizers 1

1.2 Purpose and Scope of the Workshop 2

1.3 Summary of APCO Key Attributes 2

1.4 Workshop Description 3

1.5 Document Structure 4

2. BATTERY LIFE 5

2.1 Existing Key Attribute 5

2.2 Breakout Session Summary 5

2.3 Next Steps 6

2.4 APCO Key Attribute Refinement and Additions 6

3. UNINTENTIONAL DENIAL OF SERVICE (DOS) 7

3.1 Exiting Key Attribute 7

3.2 Breakout Session Summary 7

3.3 Next Steps 7

3.4 APCO Key Attribute Refinement and Additions 7

4. MOBILE APPLICATION VETTING 8

4.1 Existing Key Attributes 8

4.2 Breakout Session Discussion Summary 8

4.3 Next Steps 9

5. DATA PROTECTION 10

5.1 Existing Key Attributes 10

5.2 Breakout Session Discussion Summary 10

5.3 Next Steps 11

5.4 APCO Key Attribute Refinement and Additions 11

6. LOCATION INFORMATION 12

6.1 Existing Key Attributes 12

6.2 Breakout Session Discussion Summary 12

6.3 Next Steps 13

6.4 APCO Key Attribute Refinement and Additions 13

7. IDENTITY MANAGEMENT 15

7.1 Existing Key Attributes 15

7.2 BREAKOUT SESSION DISCUSSION SUMMARY 15
7.3 NEXT STEPS 16
8. RECOMMENDATIONS 17
8.1 APCO KEY ATTRIBUTE UPDATE SUMMARY 17
8.2 FURTHER RESEARCH AREAS 17

List of Appendices

APPENDIX A— ACRONYMS 19
APPENDIX B— REFERENCES 20
APPENDIX C— WORKSHOP REGISTRATION LIST 21
APPENDIX D— RELATED DOCUMENTS 23
APPENDIX E— HANDOUT MATERIAL 24
APPENDIX F— WORKSHOP PRESENTATIONS 31

1. Introduction

On February 25, 2014, the Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and the Department of Commerce held a half-day workshop titled "Public Safety Mobile Application Security Requirements" attended by public safety practitioners, mobile application developers, industry experts, and government officials. In this first-of-its-kind workshop, attendees contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications. The following document describes the workshop and captures the input that was received from the workshop attendees. A list of registered workshop attendees can be found in Appendix C.

1.1 Workshop Organizers

The Public Safety Mobile Application Security Requirements Workshop was organized and planned by representatives from APCO, FirstNet and the Department of Commerce. Each of the workshop organizers has a vested interest in ensuring that public safety mobile applications are developed to meet the functional, capability, security, and usability needs of the public safety community.

APCO is the world's oldest and largest organization of public safety communications professionals. Its members include state and local employees of law enforcement, fire, and emergency medical service departments, as well as 9-1-1 Public Safety Answering Points (PSAPs) and emergency operations centers. APCO serves public safety communications practitioners by providing professional development, technical assistance, advocacy, training, and outreach. In addition, APCO is an American National Standards Institute (ANSI) accredited standards developer.

On April 23, 2013, APCO launched the online Application Community (AppComm), a collection of mobile applications related to public safety and emergency response for use by the general public and first responders. AppComm includes a catalog of more than 180 applications sortable by category (fire, emergency medical services, police, etc.) and function (situational awareness, educational tools, disaster, etc.). The site serves as the single, trusted forum to learn about existing applications, rate and comment on applications, suggest ideas for new apps, and provide feedback on a variety of application-related issues. In addition, AppComm has resources for developers of mobile applications for public safety such as a list of Key Attributes for Public Safety and Emergency Response (Key Attributes), which is described in greater detail in Section 1.3.

FirstNet is an independent authority within the Department of Commerce's National Telecommunications and Information Administration (NTIA) charged with building, operating, and maintaining the first interoperable nationwide wireless broadband network based on Long Term Evolution (LTE) dedicated to public safety. A major benefit of an LTE based interoperable nationwide wireless broadband network is the ability to deliver multimedia data (text, video, and voice) to public safety communication devices using mobile applications. Since mobile application technology will be part of the nationwide wireless broadband network for public safety, it is important to understand the impact (including security implications) the technology may have on the network.

In addition to FirstNet, the Department of Commerce is home to a joint program run by NTIA and the National Institute of Standards and Technology (NIST) called the Public Safety Communications Research (PSCR) program. PSCR performs research, development, testing, and evaluation to foster nationwide public safety communications interoperability on behalf of their sponsors at the Department of Homeland Security (DHS) Office of Interoperability and Compatibility (OIC)/ Office of Emergency Communication (OEC) and FirstNet. Working with public safety organizations (e.g., APCO and the

National Public Safety Telecommunications Council (NPSTC)), PSCR draws on public safety communications requirements provided by public safety practitioners to ground their efforts in the needs of the public safety community. In 2013, PSCR began cyber security research efforts related to public safety communications including public safety mobile application security. The public safety mobile application security effort focuses on improving the mobile application development process, specifically the mobile application testing tools, by understanding and collecting the security requirements relevant to the public safety community.

1.2 Purpose and Scope of the Workshop

The public safety community is composed of various different disciplines, such as law enforcement, firefighters, and emergency medical technicians, with a unique public service mission implying the need for different mobile application security requirements from the general public. The purpose of the Public Safety Mobile Application Security Requirements Workshop was to identify and document an initial set of mobile application security requirements relevant to the public safety community.

Some of the public safety mobile application security requirements may be addressed using techniques after the application is deployed. The following are a few examples of these techniques: mobile device profile management, mobile application whitelisting, scanning the mobile device for installed malware, and network security. Since these techniques are highly dependent on the mobile application's operating environment and outside the control of the mobile application developer, these techniques were considered outside the scope of this workshop.

Instead, the scope of the workshop focused on how the public safety mobile application security requirements might be addressed as part of the application development process that can be influenced by mobile application developers. Using software assurance techniques to mitigate mobile application software vulnerabilities is one way public safety security requirements could be addressed as part of the mobile application development process.

1.3 Summary of APCO Key Attributes

APCO's Key Attributes of Effective Apps for Public Safety and Emergency Response describes a working set of considerations for all public safety mobile applications. The document limits its scope to mobile applications intended for use on mobile devices (such as smartphones and tablets). It identifies twelve categories that define what makes an effective mobile application. The following 10 categories were chosen as discussion topics for the workshop:

1. Operability
2. User Support
3. Security
4. Privacy/Confidentiality
5. Content
6. Location Information
7. User Experience

8. Communicating with 9-1-1

9. Sending Data to PSAPS and Public Communications Centers

10. Interface with PSAPs and Public Safety Communications Centers

A presentation of APCO's Key Attributes was provided to the workshop attendees and can be found in Appendix F.

1.4 Workshop Description

The half-day workshop was set up as an interactive event where the public safety community could describe mobile application security requirements relevant to them to the mobile application experts that attended the workshop. The workshop consisted of three sessions: a welcome and background session, two facilitated breakout discussion sessions, and a wrap-up session.

The welcome and background session provided attendees with the overall objectives, scope, and structure of the workshop. In addition, a brief overview of the mobile application topics to be discussed in the breakout sessions was provided and some initial discussions were had. The presentations provided to the workshop attendees can be found in Appendix F.

The following mobile application topics were identified before the workshop for discussion based on APCO's Key Attributes document as well as other important topics being discussed in the mobile application space:

- Battery Life
- Unintentional Denial of Service (DoS)
- Mobile Application Vetting
- Location Information
- Data Protection
- Identity Management

The overview was followed by two 75-minute breakout sessions during which the attendees were divided into two groups. Attention was made to keep each of the groups as diverse as possible by distributing developers and first responders evenly between the groups. During each session, each group was asked to discuss three of the mobile applications topics. This allowed for all attendees to weigh in on each of the six topics through the course of the workshop. Each session was framed by example first responder scenarios as well as questions to stimulate discussion. This material was provided to attendees prior to the workshop and can be found in Appendix E.

The facilitators of the breakout session encouraged participants to provide their insight on the pre-identified security requirements as well as solicited input of other possible security requirements that were important to public safety but not initially identified.

During the wrap up session, a workshop facilitator provided a brief discussion of the events and afforded attendees one last opportunity to express their insights on the various topics. In addition, the attendees

were informed of the development of a white paper (this document) to capture the results of the workshop and that meeting participants would have an opportunity to review the document before final publication.

1.5 Document Structure

The remainder of this document captures the results of the discussion and provides recommended paths forward as well as refinements and additions to APCO Key Attributes document. For each of the topics identified before the workshop, there is a section identifying the existing APCO key attribute associated with the topic, a summary of the breakout session discussion of the topic, possible next steps that could be explored related to the topic, and possible refinements and additions to the list of APCO key attributes (if any). The document concludes with suggested paths forward.

2. Battery Life

2.1 Existing Key Attribute

- Minimal strain on battery life

2.2 Breakout Session Summary

An unpowered device cannot aid a first responder in fulfilling their mission. Therefore understanding the power draw of an application on a mobile device is vital when choosing which applications are deployed for use on FirstNet. Measuring battery impact is a non-trivial exercise. An application's battery impact can be influenced by its architecture, host operating system, and host hardware. While the battery impact of applications may be mitigated as battery hardware improves or through the use of auxiliary power solutions, the issue of battery use will remain relevant. Furthermore, some organizations may rely on mobile devices that come from extra-organizational sources. Battery technology may remain an unknown factor in these Bring Your Own Device (BYOD) environments.

First responders will stress their devices in ways which differ from consumer mobile device users. Depending on their circumstances, some may be operating in areas with impaired network integrity. They may have special requirements for location awareness and GPS. Firefighters can be exposed to extreme temperatures. Others may need to stream high quality video or, in the case of an incident commander, consume multiple video streams. The availability of potentially numerous live data streams which will be made available on FirstNet will present additional challenges.

The demands on first responder mobile devices will vary with the role of the first responder and their environment. Field agents may require up to twelve or more hours of battery life, while incident responders may be tethered to a power source. Some first responders may require constant usage of their device's screen whereas others may use their devices as simple radios.

When selecting applications for use on FirstNet, first responders need the ability to both mitigate an application's battery impact and compare competing application's battery impact. Various tools, methodologies, and metrics exist for measuring application battery impact. These include analytic techniques that attempt to address application inefficiencies for remediation by developers. There are also techniques that attempt to assign quantitative consumption scores to applications. Further work needs to be done to evaluate their effectiveness and appropriateness for use in public safety.

To both prepare and adapt to the multitude of circumstances faced by first responders, public safety applications should allow for remote configuration of their power consumption. This configuration can come from two primary sources. The first comes in the form of a power management profile tailored for a first responder's specific needs. For example, a firefighter may have very different power needs from a police officer. Power management profiles for a first responder's specific needs can be applied to a device prior to it entering the field. Applications that expose themselves to this profile could adjust their behavior by changing their network interactions, processing requirements, or shutting themselves off completely.

The second method of remote power management takes the form of an on-demand control made by a centralized authority like an incident commander. It was made clear during the proceedings that this level of power consumption control is vital as device power management is likely out of scope for first responders as they carry out their respective duties. Work in this space needs to be done to evaluate the technical feasibilities of these requirements as their implications may be out of scope for this document.

2.3 Next Steps

- Evaluate the effectiveness of existing metrics for battery usage. If no suitable metric exists, the public safety community may need to establish one.
- Evaluate the effectiveness of power management profiles based on different first responder roles.
- Evaluate the feasibility of remote power management.

2.4 APCO Key Attribute Refinement and Additions

- Applications should report their battery impact using accurate battery metrics.
- Battery intensive applications should be dynamically configurable to adjust their power needs. Possible options include:
    - User control
    - Role/mission based power management profiles
    - Real time remote control to meet situational demands

3. Unintentional Denial of Service (DoS)

3.1 Exiting Key Attribute

None

3.2 Breakout Session Summary

Much like the battery life discussion, the topic of unintentional denial of service became a conversation of how to manage potentially limited resources. This topic is further complicated as the exact limitations of the FirstNet LTE deployment are still unknown and likely to change from deployment to deployment and situation to situation. This uncertainty, combined with the previous experiences of public safety with non-LTE commercial networks, has left the first responder community interested in how FirstNet will perform when stressed. Workshop participants voiced concern on the impact of multitudes of first responders saturating local cells with data such as voice, location and of most concern, video. Video upload will likely place the most strain on FirstNet and is one of the easiest network demands to conceptualize. Participants envisioned many scenarios involving multiple video streams being made available to incident commanders during an emergency.

The group consensus was a call for remote monitoring of network traffic and remote management of bandwidth consumers. This would allow incident commanders to identify and mitigate applications that consume an inappropriate amount of network resources. Furthermore, it would allow dynamically stratifying network users by the current importance of their data in order to parcel out network bandwidth.

The central question is what mechanisms, or combination thereof, will control the throttling of FirstNet devices. The Quality of Service (QoS) features built into LTE may serve to remediate some network congestion issues on FirstNet. It is unclear if they can provide the on-demand level of granular control first responders might need.

3.3 Next Steps

- Identify and explain to public safety community how to use FirstNet efficiently in terms of network throughput.
- Discover the real world network load limitations of LTE deployments.
- Evaluate the applicability/appropriateness of vendor QoS features for use in on demand first responder network control.

3.4 APCO Key Attribute Refinement and Additions

- Applications must prove they use the network in an efficient and responsible manner.

4. Mobile Application Vetting

4.1 Existing Key Attributes

- Free from malicious code
- Secure from known vulnerabilities, or fully disclose known vulnerabilities

4.2 Breakout Session Discussion Summary

The breakout session focused on the need to have apps tested by a reputable source. As with other potentially life critical software, it is vital that the software be reliable and secure. There are two primary needs in app vetting. The first is to address vetting for apps intended for use by first responders and the second is for those intended for use by the public (referred to as crowd-serving apps, to not confuse public safety and the general public).

For first responder apps, the most pressing need is to have a vetting process that focuses on attributes that are unique or especially important to the public safety community, such as those laid out in this document.

There is a potential disconnect between the stringent needs of the public safety communication system and the free-flowing development and use of apps on mobile phones. Users expect to use apps to meet specific needs. This presents both a significant management challenge and a technical/procedural challenge to vet apps that the public safety community may find useful. It has been shown to be a very effective means of bringing in new apps and ideas to "crowd source" them to the entire app development community. To be useful to the community, there needs to be a registry of apps that describes their ability to meet the public safety requirements profile. AppComm could serve this need.

Some public safety organizations may require that only apps complying with some set of public safety-relevant characteristics can be used. To be cost effective, it is generally best to develop a profile and for an organization to certify products as meeting that profile. This makes it easy for app developers to build to the profile and, therefore, meet the need of their intended users.

Some public safety organizations will use this registry to pick apps that best meet their needs at the best price and not limit themselves to a specific profile.

To meet these agencies' needs, the registry needs to list capabilities and limitations in a clear and consistent manner. This gives public safety organizations the ability to make cost benefit tradeoffs to meet their highest priority needs within budgetary constraints.

The main building blocks of an app vetting infrastructure are:

- Public safety related requirements
- Test protocols to characterize whether and to what extent an app meets the requirements
- Testing of apps and listing test results on a registry
- Public safety profiles

- Certifying organizations

There is a second concern related to apps for first responders based on general aspects of software quality. Software quality determines whether an app is likely to fail and whether its presence harms security in some way.

Like many apps used by diverse communities, public safety needs apps that do not cause security or other software quality failures. Since there are so many communities with similar needs, the marketplace has responded with numerous app vetting services. The public safety community can leverage these to meet their needs and does not need to develop a unique solution.

For crowd-serving apps, it is important for the public safety community to help educate the general public on how an app should interact with the public safety system. App developers need to be made aware of what data is appropriate to deliver to public safety systems and what mechanisms are appropriate for that delivery. This is something the public safety community understands and may not be widely known by public safety application developers.

Crowd-serving apps present a different challenge for vetting. Some requirements are universal, such as whether the app accurately describes its privacy policy. For example, does the app transmit identifying information, location information, or other demographics?

Beyond this, a critical issue is how both public safety practitioner centric and crowd-serving apps send and receive information from the public safety system. The public is likely to miss nuances between an app that communicates with a security center and one that communicates with a 9-1-1 center. There is an APCO standard in development that is focused on providing a uniform interface for apps to public safety communications systems. On March 4, 2013, APCO filed a Project Initiation Notification to develop an ANSI standard for applications that interface with public safety communications centers and public safety responders. The completion of this standard is an important step toward ensuring that these applications are efficient, interoperable, and reliable.

4.3 Next Steps

- Establishment of a testing and certification infrastructure for apps for public safety.
- Development of guidelines for how the public safety community can take advantage of software quality and security work in the general mobile app marketplace.
- Completion of a standard interface to public safety, which may include an API, providing developers with uniform interaction with public safety systems.
- Identifying and documenting methods of communicating with the public how apps actually interact with the public safety system.

5. Data Protection

5.1 Existing Key Attributes

- Sensitive information is stored and transmitted using encryption

5.2 Breakout Session Discussion Summary

First responders will access, transmit, and store various types of information using applications on their mobile devices. Data protection is divided into three categories: preventing information from unauthorized disclosure (confidentiality), guarding information from unauthorized modification (integrity), and providing access to information when it is needed (availability). In general, the information owner determines the data protection requirements for their information. These requirements may be motivated by law, such as the Health Insurance Portability and Accountability Act (HIPAA), as well as policy requirements like the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy. Understanding the data protection requirements for the information being accessed and created by a public safety mobile application is crucial for both application developers as well as first responder end users.

The law enforcement representatives at the workshop indicated that CJIS defines the standard for the protection of their data via the FBI's CJIS Security Policy. They indicated that the FBI allows for agencies to self-certify to the CJIS requirements and agencies are themselves responsible for their compliance to the requirements.

It was the consensus of the workshop that app developers should be presented with a baseline set of data protection capabilities/functionality that represents the minimum need for public safety. A baseline set of data protection would need a public safety information classification system or framework. In order to protect data consistently, developers need to know what information can/should be shared, whom can the information be shared with, and how the sharing is controlled. Some information can be shared with anyone. However, protecting the integrity and availability of public information is important. Sensitive information may only be intended for authorized recipients making the confidentiality, integrity, and availability of this data critical. Developers may stand to benefit from unified data dictionaries describing first responder-specific information types and the data protection requirements for each.

Participants also acknowledged overzealous data protection may introduce availability, performance, and cost that will interfere with or inhibit the ability of first responders to carry out their missions. Developers need a good understanding of how availability, performance, and cost relate to each other in order to balance them and create an effective, useful application.

To organize and provide a framework for how availability, performance, and cost relate to each other, participants posited the notion of having different data protection tiers based on the types of data protection provided. Mobile application developers could then choose the tier their application would be comply with. Mobile application users could select applications with the appropriate data protection for their intended use.

Another issue that needs to be discussed is the exchange of information between the public and first responders and the related data protection requirements.

With respect to implementing data protection mechanisms, the developers at the workshop expressed a strong desire for a specification of the needed functionality/capability as opposed to a software developer kit/application programming interface (SDK/API). Participants were concerned mandating specific third party SDK/APIs would stifle application developers. However, the central concern is then how can applications be vetted/verified for compliance. SDKs are good for compliance as once the SDK is reviewed it can be reused; however a specification is needed to review each application for compliance. Still there was consensus from participants that an official data protection specification is the best solution moving forward.

As many public safety mobile applications will keep sensitive data in the mobile device's memory, the question about how to protect data in memory from bad/malicious applications was raised. There are many potential solutions for addressing this concern. However, most are outside the scope of the application and the application developer's control.

5.3 Next Steps

- Develop a data protection specification for use by developers.
- Develop a data dictionary describing different first responder specific data types and their data protection requirements.
- Develop a tiered data protection hierarchy for use in determining an application's level of data protection.

5.4 APCO Key Attribute Refinement and Additions

- Applications will declare what data they handle.
- Application will declare what data protection they implement.

6. Location Information

6.1 Existing Key Attributes

- App discloses what location information is being provided, whether the GPS/location services of the device needs to be enabled, how location information is being determined (cell ID, GPS, AGPS), and whether 2D or 3D

- Adequate safeguards are in place to protect privacy, confidentiality

6.2 Breakout Session Discussion Summary

Public safety mobile applications will have access to and use location information provided by mobile devices to enhance their utility to public safety practitioners. Location information is actually a special subset of the more general topic of mobile application data protection. Location information, however, has the potential to have more immediate and severe implications to first responders.

In general, location information provided to mobile applications will either be two- or three-dimensional. There are at least three factors that will influence to what extent public safety should use the location information being provided: accuracy, integrity, and confidentiality. Location information can be derived using various sources and techniques with each providing varying levels of accuracy. The integrity of the location information may need to be protected so that false location information is not provided that interferes with a timely response. Under certain circumstances, location information being generated may need to be kept confidential so as to not endanger public safety personnel. That said; seamless, efficient, and ubiquitous location communication stands to both empower and enrich public safety as they seek to fulfill their mission. Both public safety mobile application developers and users need to understand how accurate location information is and how that data is protected (integrity and confidentiality) in order to create and use applications in the most effective and secure manner.

During the breakout discussions, various themes emerged about location information. Both breakout groups expressed concern over who should have control of location tracking services. It was suggested that both end-users and supervisors should have the ability to turn location tracking on and off. This provides end-users with the flexibility to address needs in the field while simultaneously giving supervisors the ability to better support the end-user while they may otherwise be engaged with other duties. This feature also provides for administering mobile devices by allowing the location tracking capability to be configured without touching every device.

Similar to the notion of who has control over location services, attendees discussed how to control who has access to the location information. This is of particular concern to law enforcement agencies as covert movement can be paramount to both agent safety and mission success.

With regard to both control and access, applications should, in the very least, make explicit declarations as to their capabilities and intentions.

Another theme discussed was the accuracy and freshness of location information. There was agreement that the type of use case, operation, or event being discussed would be a significant factor in determining these requirements. Discussions about what is considered “real-time” for location information was explored including increments of 1 minute, 5 minutes, or best available. Depending on the operational needs, all of these might be acceptable for a given mobile application.

Finally participants examined how location information might be exchanged and used among applications. They expressed concern that there currently is no standard for how mobile applications might transmit their location information. This complicates the ecosystem, not only in the relationship between an application developer and the PSAP, but also between varying first responder organizations that may have the need to collaborate.

Outside of the realm of mobile applications there exists a body of work relating to the digital exchange of location. Table 6-1 contains a list of existing standards that may serve as starting off points. Further work must be done to evaluate their applicability to the Public Safety space. [1]

Table 6-1 - Location Exchange Standards

Location Exchange Mechanism	Relevant Standards Documents
Emergency Incident Data Document (EIDD)	• NENA-INF-005 NENA/APCO Emergency Incident Data Document (EIDD)
HELD – HTTP Enabled Location Delivery	• RFC 5985 HTTP Enabled Location Delivery (HELD) • RFC 6155 Use of Device Identity in HTTP-Enabled Location Delivery (HELD) • RFC 6753 A Location Deference Protocol Using HTTP-Enabled Location Delivery (HELD)
PIDF-LO – Presence Information Data Format Location	• RFC 4119 A Presence-based GEOPRIV Location Object Format • RFC 5139[76] Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO) • RFC 5491 GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations
SIP – Session Initiation Protocol	• RFC 6442 Location Conveyance for the Session Initiation Protocol

6.3 Next Steps

- Evaluate and recommend standards for exchanging location information.
- Evaluate feasibility of centrally managing location information services.

6.4 APCO Key Attribute Refinement and Additions

- Application location features must be configurable either by user control, remote management, and/or location/mission-based profiles.
- Applications should be built with options for location refresh rate: best-available vs. every minute vs. every 5 minutes to suit operational need.

[1] Special thanks to Intrado Inc. for their contribution to this section

- Applications must declare who is getting the location information and make clear what kind of control users have over the location information.

- 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.

7. Identity Management

7.1 Existing Key Attributes

- Securely supports identity management

7.2 Breakout Session Discussion Summary

First responders may use mobile applications to access network resources and public safety related information such as a CJIS or record management systems (RMS). To enable access control to these resources and information, public safety mobile application developers will need to understand the identity management mechanisms available for them to leverage, and what is practical for use by the public safety practitioners.

NIST describes identity management as:

> *The process of managing the identification, authentication, and authorization associated with individuals or entities (devices, processes, etc.)*[3]

The two factors that influence the assurance of the identities include how well an identity is proofed or vetted and the type(s) of credential (something you know, something you have, or something you are) used by the system. In general, combining the types of credentials used increases assurance and is called multi-factor authentication.

Law enforcement representatives discussed how the CJIS verification worked from the user's point of view. CJIS servers authenticate stationary and mobile device terminals (MDTs) at different levels, with stationary terminals granted a higher access level than their mobile counterparts. IP addresses are used to identify and register individual terminals for access to server resources. Officers that have passed the CJIS certification class then use their fingerprint or other type of credential to access the CJIS terminal.

This discussion illustrates the need for both device (terminals) and people (users) identities. It was pointed out that having possession of the device was the best credential for access to FirstNet but additional credentials would be needed to actually use the network. Since there are authentication mechanisms (e.g., passwords, PINs, and fingerprint readers) to gain local access to the device, the question about how they might be leveraged by mobile applications was asked.

Concerns were voiced about the usability and practically of the authentication mechanisms given public safety's dynamic operating environment. Emergency responders, for example, may be hindered by requiring two-factor authentication for their applications. During a non-emergency time, it may be acceptable to require authentication before a communication transmission or information request is performed. However, during an emergency event, it might be acceptable to lower the level of authentication or eliminate it all together before a communication transmission or information request is performed. For example, a man-down call might not require any authentication before the transmission is made. In addition, a first responder may not have the time or ability to enter identity credentials (such as a password or PIN) in an emergency situation.

This led to the discussion of a hierarchy or levels of authentication based on the situation; or situational authentication. In order for something like situational authentication to occur, the different categories of situations would need to be defined and standardized as well as acceptable levels of authentication for

given operations/functions. Then a mapping between the situation categories and authentication levels for given operations/functions would need to be defined and standardized.

7.3 Next Steps

- Establish a hierarchy of authentication.

8. Recommendations

8.1 APCO Key Attribute Update Summary

The following is the list of recommendations and requirements resulting from the workshop that should be considered for inclusion in the APCO Key Attribute document:

- Applications should report their battery impact using accurate battery metrics.
- Battery intensive applications should be dynamically configurable to adjust their power needs. Possible options include:
    - User control,
    - Role/mission based power management profiles, and
    - Real time remote control to meet situational demands.
- Applications must prove they use the network in an efficient and responsible manner.
- Application location features should be configurable either by user control, remote management, or location/mission based profiles.
- Applications should be built with options for location refresh rate: best-available vs. every minute vs. every 5 minutes to suit operational need.
- Applications must declare who is getting the location information and make clear what kind of control users have over the location information.
- Applications must declare all information being gathered and whether that data is transmitted, stored, or both. When data is transmitted, the application must declare where the data is being transmitted.
- Application will declare what data protection they implement.

8.2 Further Research Areas

Several activities were identified for further research as possible next steps. The following is the list of possible activities identified from the workshop:

- Evaluate the effectiveness of existing metrics for battery usage. If no suitable metric exists, the public safety community may need to establish one.
- Evaluate the effectiveness of power management profiles based on different first responder roles.
- Evaluate the feasibility of remote power management.

- Identify and explain to the public safety community what it means to use the FirstNet network responsibly in terms of network throughput.
- Discover the real world network load limitations of LTE deployments.
- Evaluate the applicability/appropriateness of vendor QoS features for use in on demand first responder network control.
- Establish a testing and certification infrastructure for apps for public safety.
- Develop guidelines for how the public safety community can take advantage of software quality and security work in the general mobile app marketplace.
- Specify an API so that app developers can interact with the public safety system.
- Identify and document methods of communicating with the public how apps actually interact with the public safety system.
- Evaluate and recommend standards for exchanging location information.
- Evaluate feasibility of centrally managing location information services.
- Develop a data dictionary describing different first responder specific data types and their data protection requirements.
- Develop a data protection specification for use by developers.
- Develop a tiered data protection hierarchy for use in determining an application's level of data protection.
- Establish a hierarchy of authentication.

Appendix A—Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

AGPS	Assisted Global Positioning System
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
BYOD	Bring Your Own Device
CJIS	Criminal Justice Information System
DHS OIC	Department of Homeland Security Office of Interoperability and Compatibility
DHS OEC	Department of Homeland Security Office of Emergency Communication
DoS	Denial of Service
eNB	Evolved Node B
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
LTE	Long Term Evolution
MDT	Mobile Device Terminals
NIST	National Institute of Standards and Technology
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
PSAP	Public Safety Access Point
PSCR	Public Safety Communication Research
QoS	Quality of Service
SDK	Software Development Kit
VPN	Virtual Private Network

Appendix B—References

Selected acronyms and abbreviations used in this interagency report are defined below.

[1] Health Insurance Portability and Accountability Act of 1996. Public Law 104-191; http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

[2] "Key Attributes of Effective Apps for Public Safety and Emergency Response," APCO International, 18 Aug. 2013; http://appcomm.org/wp-content/themes/directorypress/thumbs/AppComm_Key_Attributes.pdf

[3] Nelson Hastings, Joshua Franklin, "Considerations for Identity Management in Public Safety Mobile Networks (DRAFT),"; http://csrc.nist.gov/publications/drafts/nistir-8014/nistir_8014_draft.pdf

[4] U.S. Department of Justice, Criminal Justice Information Services (CJIS) Security Policy, Version 5.3, 4 Aug. 2014. DOI:CJISD-ITS-DOC-08140-5.3

Appendix C—Workshop Registration List

The following are the list of workshop attendees and their affiliations.

Mark Adams, Northrop Grumman

Scott Agnew, AT&T

Rafael Bezanilla, Palm Beach County (FL) Sheriff's Office

Jeff Bratcher, FirstNet

Jeffery Carl, AT&T

Serena Chan, Institute for Defense Analyses

Jeff Cohen, APCO

Richard Coupland, General Dynamics

Ed Davey, Prince George's County (MD) Police

Donald Denning, City of Boston Office of the CIO

Crista Dexter, Lake County, FL, Sheriff's Office

Jay English, APCO

John Facella, RCC Consultants

Jeff Godin, Badge Buddy

Paul Gomez, Prince George's County (MD) Fire

Traviss Green, Lockheed-Martin

Barbara Guttman, National Institute of Standards and Technology

Terry Hall, APCO Executive Committee

Nelson Hastings, National Institute of Standards and Technology

Doug Havemann, Panasonic

Rob Jones, Lockheed-Martin

David Kahn, Covia Labs

Chris Kachigian, Lockheed-Martin

Britt Kane, Intrepid Networks

Alan Kaplan, Drakontas

Stephen Kennedy, Sumter County (FL) Fire & EMS

Alex Kreilein, Department of Homeland Security

Brent Lee, APCO Executive Committee

Michael McMenamin, 3 Birches Lane, LLC

Dick Mirgon, Public Safety Consultant

Gary Monetti, TASC

Bryan Morgan, Motorola Solutions

Michael Ogata, National Institute of Standards and Technology

Derek Poarch, APCO Executive Committee

Mark Reddish, APCO

Patrik Ringvist, Ericsson

David Rogers, Allogy Interactive

Robin Schmidt, Palm Beach County (FL) Sheriff's Office

Bill Schrier, Washington State Office of the CIO

Gigi Smith, APCO Executive Committee

Jason Stonebraker, Intrepid Networks

Andy Seybold, Andrew Seybold, Inc.

Joseph Wassel, Institute for Defense Analyses

Roger Wespe, APCO

Carl Williams, Harris Corp.

John Wright, APCO Executive Committee

Appendix D—Related Documents

J. Peterson, *A Presence-based GEOPRIV Location Object Format*, IETF RFC 4119, December 2005; http://www.ietf.org/rfc/rfc4119

J. Polk, B. Rosen and J. Peterson, *Location Conveyance for the Session Initiation Protocol*, IETF RFC 6442, December 2011; http://tools.ietf.org/html/rfc6442

J. Winterbottom, et al. *A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)*, IETF RFC 6753, October 2013; http://tools.ietf.org/html/rfc6753

J. Winterbottom, et al. *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*, IETF RFC 5491, March 2009; http://tools.ietf.org/html/rfc5491

J. Winterbottom, et al. *Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*, IETF RFC 6155, March 2011; http://tools.ietf.org/html/rfc6155

M. Barns, Ed. *HTTP-Enabled Location Delivery (HELD)*, IETF RFC 5985, September 2010; http://tools.ietf.org/rfc/rfc5985

M. Thomson, et al. *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*, IETF RFC 5139, February 2008; http://tools.ietf.org/html/rfc5139

The National Public Safety Telecommunications Council. (2014,September 30). "Defining Public Safety Grade Systems and Facilities (Final Report)" [Online]. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf

NENA, APCO, *NENA/APCO Emergency Incident Data Document (EIDD) Information Document*, NENA/APCO-INF-005, 21 Feb. 2014; https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/EIDD_INF-005_FINAL_20140221.pdf

Appendix E—Handout Material

The following was provided to the attendees before the workshop to provide some scope and context for the discussions to take place during the breakout sessions:

Expanded Description of Security Topics for Breakout Session Discussions

I. Battery life issues

- APCO Key Attribute "Minimal strain on battery life" (Operability)

The quantification of a mobile application's battery load will be paramount when choosing which applications to deploy in the first responder mobile device infrastructure.

Example Scenario: Designing the Application Ecosystem for a FEMA Response Team

> *A FEMA Urban Search and Rescue Task Force (US&R) is deployed to a building collapse scenario. Field agents are equipped with mobile devices whose suite of mobile applications has been selected to maximize the device's battery life. Location aware applications, while potentially taxing on battery performance, are allowed on the devices due to the nature of the dangers inherent in fieldwork. Other non-critical applications are designed to sense when to abdicate battery utilization if they detect extra load on the device.*

Identifying Public Safety's Needs

1. What are the phases of a response for a building collapse?
2. Who are the players, and what are their respective roles/responsibilities?
3. What is the expected time between charges for each player and scenario?
4. What scenarios require continuous or intensive location identification and tracking?
5. What data-intensive applications are most important in the field (e.g. maps, transmission of patient data, floor plans, high resolution photos, video)?
6. Should high availability applications (data or processing intensive) display adaptive behavior (dial back power needs) if they determine they are placing too much strain on a device?

Understanding the Technology Behind the Apps

1. Among the data-intensive needs of public safety, which features will place the heaviest drain on a device's battery?
2. What other types of apps drain the battery quickly?
3. How much emphasis is placed on battery efficiency during app development?
4. How much consideration is placed on battery impact when choosing apps for deployment?
5. In what ways can we quantify the battery effect of an application on a device?
    a. Verizon ranks popular apps in their store and uses a closed source method of ranking battery performance on a scale from 1 to 5.
    b. AT&T provides an open source tool: ARO for monitoring network usage, Bluetooth usage, and battery consumption for various mobile device platforms.

Potential Requirements

1. Scale-down battery-intensive functions whenever possible
    a. Allow "austere" modes
    b. Avoid duplicative tracking when devices are sure to be in close proximity
2. Provide estimates of battery life for each operational choice and create easily-consumable guidance for maximizing battery life in an app

II. Location information issues

- APCO Key Attribute "App discloses what location information is being provided…" and "Adequate safeguards are in place to protect privacy, confidentiality" (Location Information)

Mobile public safety applications will have access to location information to enhance their utility. In general, the location information provided to mobile applications is two-dimensional. However, some public safety applications may require three-dimensional location information such as conducting a search within a building or on a mountainside.

Location information provided to mobile devices originates from different sources leveraging various techniques that result in different accuracy levels for the location information.

The extent that public safety relies on the location information may vary based on the source, accuracy, and integrity (i.e. continued validity) of the information. In addition, the location information may be considered sensitive information requiring it to be confidentiality protected.

The following two scenarios describe how location information might be used by a public safety mobile application:

> *As part of a covert operation, an undercover officer is using a mobile application on his/her mobile device to provide operation information (such as video, voice, location, etc.) back to the operation's command center.*
>
> *During a response to a building fire, a firefighter uses a mobile application on his/her mobile device to navigate through the building as well as provide firefighter location to the fire incident commander.*

Identifying Public Safety's Needs

1. Under what conditions does location information need to be confidential? (also see Data Protection, below)
2. What are considered "adequate safeguards" for location information privacy/confidentiality?
3. Under what conditions does location information need to be kept private?
4. Does the source of the location information need to be verified?
5. Does the integrity of the location information need to be verified?
6. Does the source, or technique to determine, the location information suggest how the information will be used?
7. What public safety mobile apps benefit using two-dimensional location information?
8. What public safety mobile apps benefit using three-dimensional location information?
9. Understanding the Technology Behind the Apps

The following are some common techniques mobile devices use to obtain location information and their associated accuracies:

a. Global Position System (GPS) capabilities within a mobile device can provide an accuracy within about 3 meters when outdoors,
b. Location based service providers provide location information with various levels of accuracy based on techniques they choose to use, and
c. The communications network can provide location information to the mobile device using triangulation techniques with accuracy within about 1200 meters using three

towers, and in the near future LTE proximity services will improve accuracy by leveraging more of the communication infrastructure, specifically other mobile devices.

Potential Requirements

1. Apps that track first responder devices must ensure that location information is not made available to unauthorized users.
2. App users and procuring agencies should have the ability to toggle location tracking on and off based on operational and administrative needs.
3. App providers should clearly describe measures to protect users' location information.

III. Unintentional Denial of Service (DoS) Issues

- This describes a situation where access to a website or server is denied, not due to a deliberate attack, but as a result of a sudden spike in user traffic. (Candidate for a new APCO Key Attribute.)

Example Scenario:

A large earthquake has occurred in a major metropolitan area. Traffic across the cell infrastructure spikes in the following ways:

Application Layer: *911 call centers are flooded with requests from 911-communication-equipped applications (for example, texting to 9-1-1).*

The Access Network: *Due to the quake, first responders are now clustered in areas carrying out their respective duties (firemen may be working as teams engaged in rescue operations, police may be working in teams to direct traffic). Because of the increase in network traffic and the geographic proximity of first responders, local eNBs (cellular base stations) are now under increased strain.*

Identifying Public Safety's Needs

1. How must multiple 911 apps reporting the same incident be controlled or triaged?
2. What kind of information must flow from responders in the field, and from what levels (policeman, fireman, chiefs, incident commanders)?
3. What data-intensive applications are most important in the field (e.g. maps, transmission of patient data, floor plans, high resolution photos, video)?

Understanding the Technology Behind the Apps

1. How can applications equipped to communicate with 911 play well on the network to prevent 911 call center infrastructures from collapsing under the weight of heavy use?
2. How should applications that mean to send data across the network act in order to "play nice" so as not to overload and shutdown the cell network?
3. Should public safety mobile applications be stratified by their data input/output requirements in order to better judge their distribution amongst the first responder community (i.e. should instances of applications with higher data throughput requirements not be deployed on as many devices).
4. Could apps "detect" strain on the network and reduce their impact on the network (e.g. video streaming applications down-scaling their video quality)?

Potential Requirements

1. Apps that interface with public safety users should incorporate measures to minimize severe strain on communications networks.

IV. Data protection

- APCO Key Attribute "Sensitive information is stored and transmitted using encryption" (Security)

Mobile public safety application developers will need to understand the protection requirements of the data being accessed as well as for the data created by the application in order to properly protect it.

Since the mobile applications may be accessing remote databases and storing data on the mobile device, data protection may need to cover the data in transit as it travels across a communications network and at rest while stored on the mobile device.

Data protection can be broken down into the following general categories: protecting data from unauthorized disclosure (or confidentiality), protecting data from modification (or integrity), and being able to access the data when it is needed (or availability).

In general, the owner of the data being accessed and/or created determines the data protection requirements. The data owner's decision may be motivated by legal as well as policy requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA) [1] governs the data protection requirements related to health information/records. Similarly, the FBI's Criminal Justice Information Services (CJIS) Security Policy governs the data protection requirements related to Criminal Justice Information (CJI).

Example scenarios:

> *During a traffic stop, an officer determines the need to run the driver's identity through a CJIS system to determine if the driver has any current outstanding warrants or criminal history, so the officer uses a mobile application to access a CJIS system and receive the results of the query.*
>
> *During a medical emergency response, a paramedic uses a mobile application to collect a patient's information (name, age, gender, age, etc.) as well as to monitor the patient's vital signs (heart rate, blood pressure, temperature, etc.). In addition, the mobile application forwards the patient information to the hospital the patient will be taken to.*

Identifying Public Safety's Needs

1. What is considered sensitive data?
2. Is sensitive data sufficiently defined by legal/regulatory compliance requirements?
3. How is sensitive data identified and labeled?
4. How is the type of data protection needed/required determined?
5. What types of data protection are needed/required?
6. What types of data need/require privacy protection? (such as personnel information, user/agency data)

Understanding the Technology Behind the Apps

1. How do methods and levels of data protection impact app performance?

Potential Requirements

1. Privacy policy is easily accessible and contains readily understandable terms.
2. Personal information, including location information, stored on the device is not accessed or shared unless privacy policy states otherwise.
3. Any use of data extracted from the user or public safety agency through operation of the app other than for the necessary functionality of the app is fully disclosed.

4. Applications should provide confidentiality, integrity, and availability protection of data based on its sensitivity, legal, regulatory, and policy requirements.
5. Applications should protect data using standardized cryptographic techniques.

V. Mobile application vetting

- APCO Key Attribute "Free from malicious code" and "Secure from known vulnerabilities or fully disclosed known vulnerabilities" (Security)

The public safety community will want to know if apps are safe for use and if the app meets the requirements of the community. Since app testing can be expensive and time-consuming, it is important to focus on the most critical aspects that can be tested and to develop a strategy that minimizes multiple tests.

Example Scenario:

> *A public safety agency planning to procure an app seeks third party verification that the app meets public safety requirements. The third party supplies a report in a standardized format that uses common measures and terminology to allow for consistent comparisons of apps across agencies and vetting services.*

Identifying Public Safety's Needs

1. What are the best ways for public safety to be able to have confidence that an app is safe for use?
2. Should public safety rely upon a seal of approval or other certification? Should such seal or certification come from government, industry, or APCO?
3. The security and software assurance community is addressing general security for mobile apps. How can the public safety community support these efforts and use them effectively to meet public safety needs?
4. What does public safety need from testing reports to make informed choices?
5. Who should do the testing?
6. How should the reports be shared?
7. What information needs to be in reports?
8. Who should produce or be responsible for the reports?
9. How does the public safety community currently share information about product performance that could be applied to app testing?
10. Do the most trusted resources involve third-party evaluation or community-based input (open forums)?

Understanding the Technology Behind the Apps

1. Apps are just like any software and are vulnerable to commonly known risks of infection, malware, and other cyber threats.

Potential Requirements

1. While the specifics of mobile device management (MDM) services are out of scope for this workshop, we could define a set of common report features for consideration by mobile application scanners/security services to allow for quick and consistent review and comparison. Furthermore, we will seek to include references to common software weaknesses (see http://cwe.mitre.org/data/definitions/490.html). A common or interoperable reporting format stands to benefit the entire first responder application ecosystem.

VI. Identity management

- APCO Key Attribute "Securely supports identity management"

Mobile public safety application developers need to understand the identity management mechanisms available to their applications, and when and which of these mechanisms should be used to enhance the capabilities of their application. To be more specific, mobile applications will be using identity credentials issued by an identity management system to enable the application to access public safety related information systems such as a CJIS or record management system.

In general, the following steps are used by identity management systems: enrollment application/request, identity proofing, identity credential issuance, identity credential usage, identity credential revocation, credential identity expiration, and possibly identity credential re-issuance/updating.

The level of assurance provided by an identity credential is driven by the rigor of identity proofing done before the credential is issued and the type of credential issued. The following identity proofing techniques are listed by which technique provides the least to most assurance before an identity credential is issued: none, verification of some information of record (such as address), sponsor appearing before the credential issuer, and the individual/device appearing in person before the credential issuer.

Identity credentials can be categorized as something you know (passwords, PINs, one-time passwords), something you have (cryptographic based tokens such as smart cards, etc.), and something you are (biometrics such as fingerprint, retina, etc.). The assurance of an identity can be increased by combining different categories of identity credentials and is called multi-factor authentication. Finally, the way the identity credential is handled (can it be replicated) and stored (software/hardware) will also impact the level of assurance for the identity.

Example Scenarios:

> *A detective is at a restaurant and decides to use a mobile application to access criminal justice information as part of the case being investigated, so the detective needs to authenticate his/her identity to gain access to the information.*
>
> *At the beginning of their shift, firefighters authenticate their identities to mobile devices they received from firefighters on the previous shift in order to gain access to databases they are authorized to access.*

Identifying Public Safety's Needs

1. What types of applications require identity management?
2. What identity proofing mechanisms (none, in-person, sponsor based for devices and individuals, verification of some information of record, etc.) are acceptable to public safety?
3. What types of credentials/mechanisms are acceptable for use by public safety?
4. What third party identity management infrastructures are acceptable, if any?

Understanding the Technology Behind the Apps

1. What types of credentials/mechanisms are supported by mobile devices?
2. Does the application contain the identity management system or does it leverage an existing identity management system?
3. In what ways can the mobile device be used as an identity credential?
4. Can the mobile device use multiple identity credentials?
5. How does the mobile device handle revocation of an identity credential?

Potential Requirements

5. Applications should support the use of strong authentication mechanisms such as multi-factor and cryptographic techniques.
6. Applications should support the use of credentials issued by different organizations/entities.
7. Applications should verify the status of identity credentials – revoked, suspended, etc.

Appendix F—Workshop Presentations

The following presentations were given at the workshop:

Scope

- Focus on mobile application development
  - Public safety security requirements
  - Software assurance techniques and tools
- Out of Scope
  - Mobile operating system vulnerabilities
  - Mobile operating system hardening and configuration
  - Mobile device profile management
  - Mobile application whitelisting
  - Mobile application sandboxing

Structure

- Background
  - Overview of APCO's Key Attributes of Effective Apps for Public Safety and Emergency Response
  - Overview of the breakout sessions topics (and possible initial discussions)
- Breakout sessions
  - Two breakout session groups
  - Each group will discuss three topics for about 75 minutes
  - After a short break, each group will discuss three different topics for about 75 minutes
  - Everyone will get a chance to discuss all six topics and propose other topics for future discussions
- Summary of findings

Post Workshop

- Refinement of APCO's Key Attributes of Effective Apps for Public Safety and Emergency Response
- NIST whitepaper capturing:
  - The initial security requirements for public safety mobile applications and their justification for the topics discussed at the workshop
  - Additional public safety mobile application security requirement topics that need further investigation and discussion
  - Strategies for conformity assessment of security requirement for public safety mobile applications
- Possible next steps

Questions

APCO International
Leaders in Public Safety Communications™

APCO's Key Attributes of Effective Apps for Public Safety and Emergency Response

Mark Reddish – Government Relations Associate

February 25, 2014

APCO's Application Community Website - AppComm

www.AppComm.org

application community
the destination for public safety apps™

APCO International
Leaders in Public Safety Communications™

© 2013; all rights reserved

AppComm: The Destination for Public Safety Apps

- Prior to AppComm, public safety professionals largely had to learn about helpful apps by word of mouth.
- AppComm is your single, trusted site for public safety apps, meaning apps for use by first responders as well as the general public.

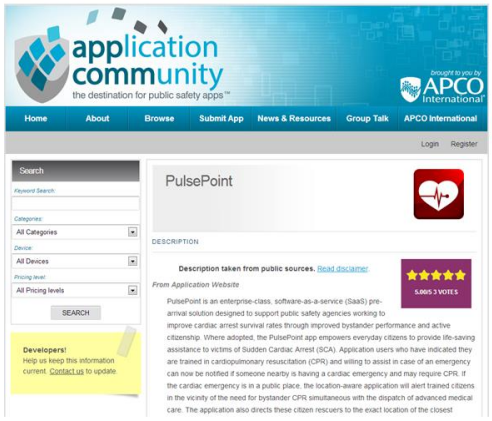
APCO International
Leaders in Public Safety Communications℠

AppComm Features

- Learn about existing apps for public safety and emergency response
  - Search by category, device, price, and function
  - Create a Favorites list
- Rate and Comment on apps
- Use the "Submit App" form if there's an app that should be included on the site
- Submit ideas for new apps
- Share your thoughts and opinions about apps on Group Talk
- Register so you can avail yourself of all of AppComm's features!

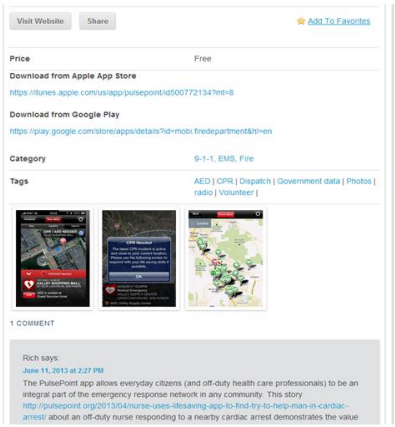
APCO International
Leaders in Public Safety Communications℠

Learn About What's Out There



APCO International
Leaders in Public Safety Communications™

Learn About What's Out There

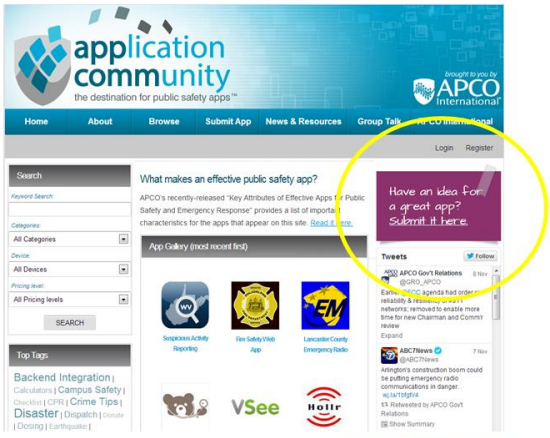


APCO International
Leaders in Public Safety Communications™


Sort by Function
Search
Keyword Search:
Categories:
All Categories
Device:
All Devices
Pricing level:
All Pricing levels
SEARCH
Tags
Calculators| Campus Safety| Checklist| CPR| Crime Tips| Disaster| Dispatch| Donate| Dosing| Earthquake| Educational Tools| Emergency Contacts| Evacuation| First Aid| Government Data| GPS| Gunshot Detection| HazMat| Help Request| Hospital| Hurricane| Incident Management| Incident Reports|
Dispatch
9 Results Found
Home / Posts tagged "Dispatch" /
save this search
view saved searches
My Favorites
Canvas Business Forms & Apps
Cliqtalk Instant Collaboration
Emergency Radio Free
Fire Hall Utility
NowForce Mobile Responder
Featured at ETF
PulsePoint
911
Response Deck - SBC
SLO EMS
APCO International
Leaders in Public Safety Communications℠
© 2013; all rights reserved


Sort by Category
Search
Keyword Search:
Categories:
All Categories
Device:
All Devices
Pricing level:
All Pricing levels
SEARCH
Tags
Calculators| Campus Safety| Checklist| CPR| Crime Tips| Disaster| Dispatch| Donate| Dosing| Earthquake| Educational Tools| Emergency Contacts| Evacuation| First Aid| Government Data| GPS| Gunshot Detection| HazMat| Help Request| Hospital| Hurricane| Incident Management| Incident Reports| Maps
9-1-1
17 Results Found
Order Results By
Home / category "9-1-1" /
save this search
view saved searches
new email alert
My Favorites
Active911
APD Tips
CityConnect San Jose, CA
CT Police Phones
EMS Field Partner
EMS Field Partner
Fire Hall Utility
American Red Cross
First Aid by American Red Cross
FLIGHT FOR LIFE CENTRAL
Flight for Life Central
APCO International
Leaders in Public Safety Communications℠
© 2013; all rights reserved

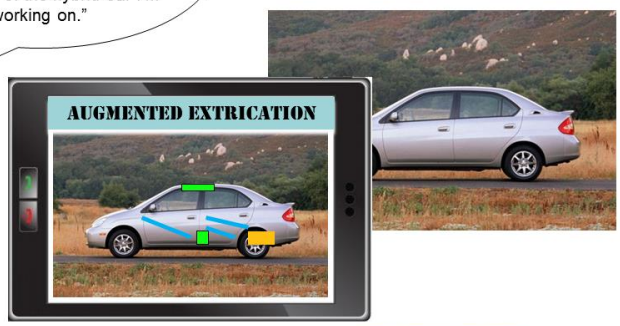
Submit Ideas



APCO International
Leaders in Public Safety Communications™

Submit Ideas

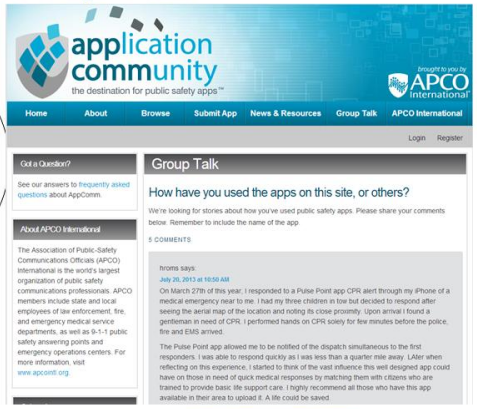
"I'd like an extrication app that overlays air bags, reinforced posts, and power supply on a live image of the hybrid car I'm working on."



APCO International
Leaders in Public Safety Communications™

Group Talk

I responded to a PulsePoint app CPR alert through my iPhone…Upon arrival I found a gentleman in need of CPR. I performed hands on CPR solely for a few minutes before the police, fire and EMS arrived…
I highly recommend all those who have this app available in their area to upload it. A life could be saved.



APCO International
Leaders in Public Safety Communications™

APCO's Key Attributes

APCO is not testing/vetting apps but has developed a list of Key Attributes of Effective Apps for Public Safety and Emergency Response to guide the selection of apps for AppComm. They address:

- Operability
- User Support
- Security
- Privacy/Confidentiality
- Content
- Location Information
- User Experience
- Communicating with 9-1-1
- Sending Data to PSAPs and Public Safety Comm Centers
- Interface with PSAPs and Public Safety Comm Centers

APCO International
Leaders in Public Safety Communications™

User Experience

- *App name and description do not present misleading information*
- *App features are clearly and accurately defined*
- What we've seen in "bad" apps:
  - Suggestions that the app is preferable to 911
  - Promises to share location information without identifying issues with accuracy in cities and indoors
  - Promises to connect users with first responders without clarifying that FRs must download the app

APCO International
Leaders in Public Safety Communications℠

Security

- Feb. 18 article: Report finds iOS apps riskier than Android apps
  - "Appthority found that 95 percent of the top 200 free apps on iOS and Android exhibit at least one risky behavior" http://www.pcworld.com/article/2098435/report-finds-ios-apps-riskier-than-android-apps.html
- Feb. 19 article:
  - "By 2013, more than 42,000 apps in Google's store contained spyware and information-stealing Trojan programs. http://www.infoworld.com/d/security/report-android-malware-and-spyware-apps-spike-in-the-google-play-store-236702

APCO International
Leaders in Public Safety Communications℠

Operability

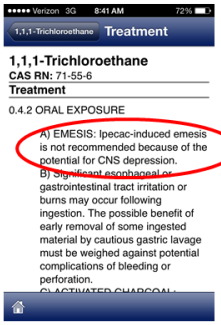
- *Efficient use of data; minimal strain on battery life*

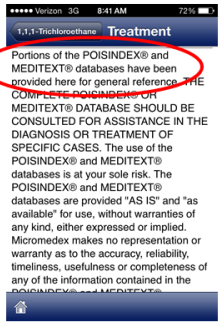
Some features that will be especially useful for public safety require particular attention for data and battery efficiency.

APCO International
Leaders in Public Safety Communications℠

Content

- *Sources of information are cited*
  - *Information, particularly for educational tools, is derived from industry-accepted sources.*

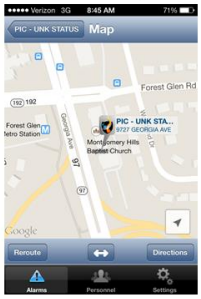


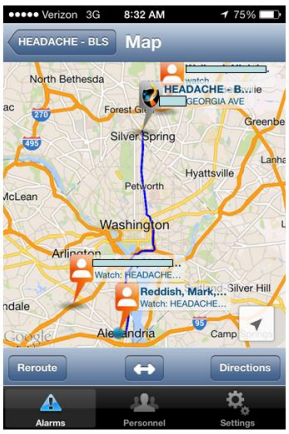


APCO International
Leaders in Public Safety Communications℠

Location Information

- *Adequate safeguards are in place to protect privacy, confidentiality.*





APCO International
Leaders in Public Safety Communications™

Interface with PSAPs and Public Safety Communications Centers

- APCO is seeking volunteers to become members of a working group that will write APCO ANS 2.104.1-201x
- Topics will include:
  - Interfaces with PSAPs, EOCs, etc.
  - Integration with legacy and NG systems
  - Security requirements
  - Voice and data networks as they relate to PS apps
- Applications due March 15; space limited

APCO International
Leaders in Public Safety Communications™

Join the Community!

- Participate & spread the word:
  - Register at www.AppComm.org
  - Your ratings, comments, submissions, and ideas will drive innovation
- Your technical expertise can benefit the public safety community
  - Refine the Key Attributes
  - Help public safety practitioners turn ideas into lifesaving tools

APCO International
Leaders in Public Safety Communications™

APCO International
Leaders in Public Safety Communications™

Contact:

Mark Reddish
reddishm@apcointl.org
@GRO_APCO

Breakout Topics Overview

The Six Topics

- Battery Life
- Unintentional Denial of Service (DoS)
- Mobile Application Vetting
- Location Information
- Data Protection
- Identity Management

Battery Life

- Facilitator: Michael Ogata
- APCO key attribute:
  - "Minimize strain on battery life"
- Battery life usage of mobile applications differ for various reasons
  - Wireless technologies (celluar, bluetooth, WiFi, etc.) usage
  - Mobile device display usage
  - CPU usage
- The development of mobile applications to efficiently use the battery would be helpful

Unintentional Denial of Service (DoS)

- Facilitator: Michael Ogata
- Denial of service not due to deliberate attack but as a result of a spike in user traffic
- Potential APCO Key Attribute
- Mobile applications should designed to optimize network usage
  - Limiting idle connections
  - Efficient caching
  - Adapting to network load

Mobile Application Vetting

- Facilitator: Barbara Guttman
- APCO key attribute
  - "Free from malicious code"
  - "Secure from known vulnerabilities or fully disclosed known vulnerabilities"
- How can these things be determined and communicated to users
- What are some of the variables – time, cost, technology

Location Information

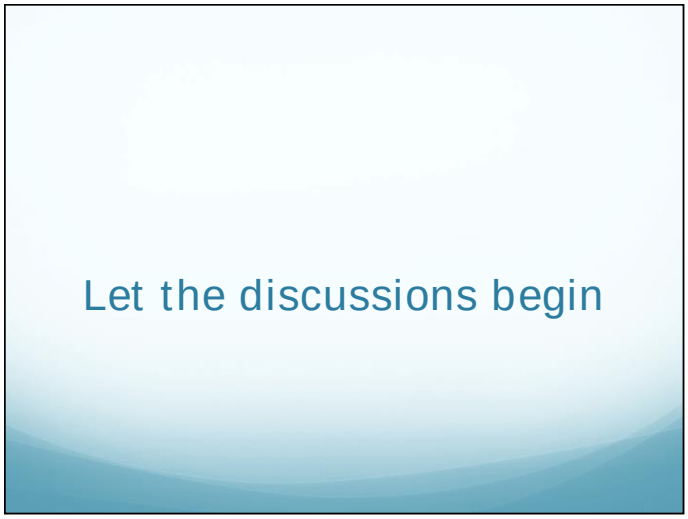
- Facilitator: Jay English
- APCO key attribute
  - "App discloses what location information is being provided…"
  - "Adequate safeguards are in place to protect privacy, confidentiality"
- Mobile applications will use location information in various ways
  - When should the integrity of the location information be verified?
  - When should the source of the location information be verified?
  - When should location information be confidential?
- The development of mobile applications to use and protect location information may be critical

Data Protection

- Facilitator: Alex Kreilein
- APCO key attribute
  - "Sensitive information is stored and transmitted using encryption"
- Mobile applications will need to be developed to protect information
  - What information needs protection?
  - When is integrity protection enough?
  - When is confidentiality protection required?
- Under what circumstances can/ should information protection be by-passed?

Identity Management

- Facilitator: Nelson Hastings
- APCO key attribute:
  - "Securely supports identity management"
- Mobile applications may need to interact with identity management systems to control access
  - Record management systems
  - Criminal justice information systems (CJIS)
- What technologies exist for the mobile environment and are acceptable for public safety use?


Let the discussions begin