Identifying Public Safety's Security Requirements for Mobile Apps

Michael Ogata
Computer Scientist, NIST
michael.ogata@nist.gov

Disclaimer / Disclosure

Trade names and company products may be mentioned during this presentation. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for their stated purpose.

Workshop Description

- Half day workshop, February 25th, 2014
- Titled: “Public Safety Mobile Application Security Requirements Workshop”
- Joint effort between
  - APCO
  - FirstNet
  - Department of Commerce
    - DHS/OIC (Funding Partner)
- Attended by approx. 50 community members

Workshop Impetuous

- FirstNet will empower first responders
- FirstNet can benefit from mobile application ecosystem
- FirstNet will have domain specific security requirements
- Developers must be empowered to these needs

Workshop Impetuous

APCO Key Attributes for Public Safety and Emergency Response

- Operability
- User Support
- Security
- Privacy/Confidentiality
- Content
- Location Information
- User Experience
- Communicating with 9-1-1
- Sending Data to PSAPS
- Interfacing with PSAPS

http://appcomm.org/wp-content/themes/directorypress/thumbs/AppComm_Key_Attributes.pdf

Workshop Goals

- Identify mobile application security requirements for public safety
- Identify areas of required further research
- Augment and refine APCO's Key Attributes of Effective Apps for Public Safety and Emergency Response
- Publish findings in a NIST Interagency Report

Workshop Discussion Topics

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

Workshop Scope

- In scope
  - Mobile application development practices
  - Mobile application functional requirements
- Out of scope
  - Device management
  - Application whitelisting
  - Device level anti-malware/anti-virus techniques
  - Network security requirements

Battery Life

Battery Life – Stressors

- Impaired network integrity
- Special requirements for location services
- Utilization of multiple high quality media streams
- Extensive field time
- Extreme temperatures

Battery Life

- Maximizing battery life is essential for public safety
- Improving battery technology will help
- Measuring application battery impact is non-trivial
  - Application’s construction
  - Resident hardware
  - Host operating system

APCO Key Attribute

- Minimal strain on battery life

Battery Life – Workshop Feedback

- High power consuming applications highly desired
  - Location services
  - Video
- Techniques for improving / measuring battery life
  - Throttling network poll frequency
  - AT&T Application Resource Optimizer (ARO)
  - Verizon battery usage rating

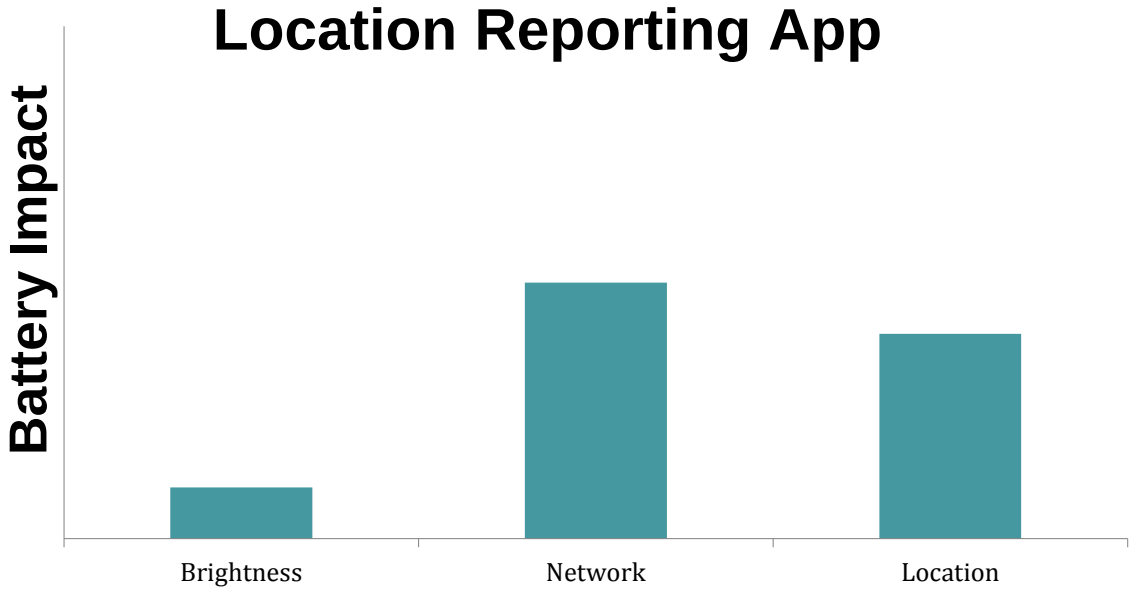
Battery Life – Workshop Feedback

- Application Resource Optimizer (ARO)
  - Measures Wifi, Cellular, Bluetooth efficiency
- Verizon background battery usage metric
  - 1-5 rating system

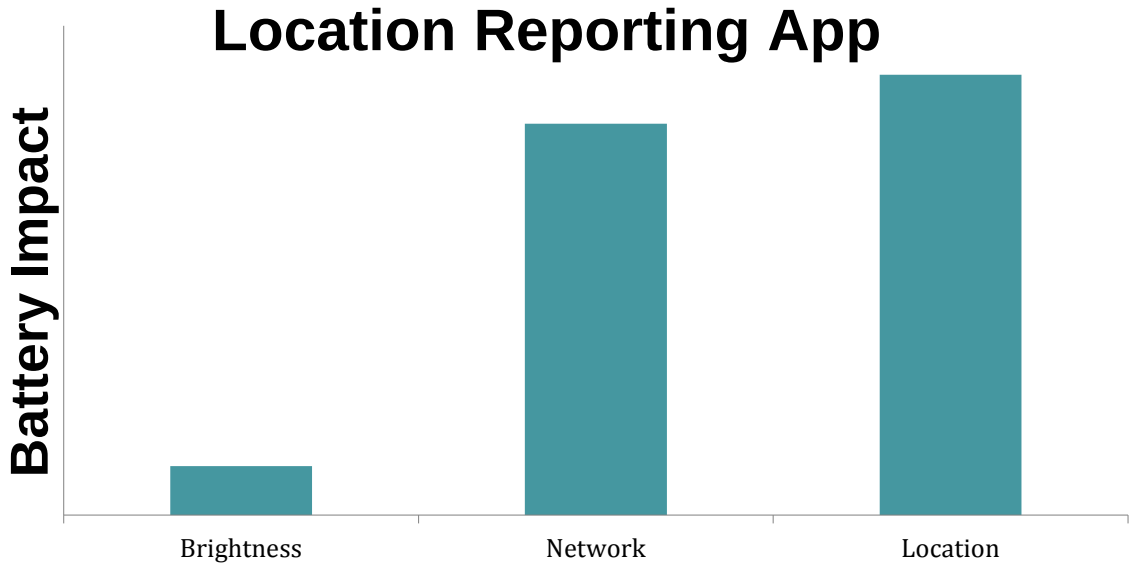
Battery Life – Workshop Feedback

- Different Roles have different needs
- Applications should be configurable
  - Role / mission based power management profiles
  - Remote on demand control
  - On demand by the user

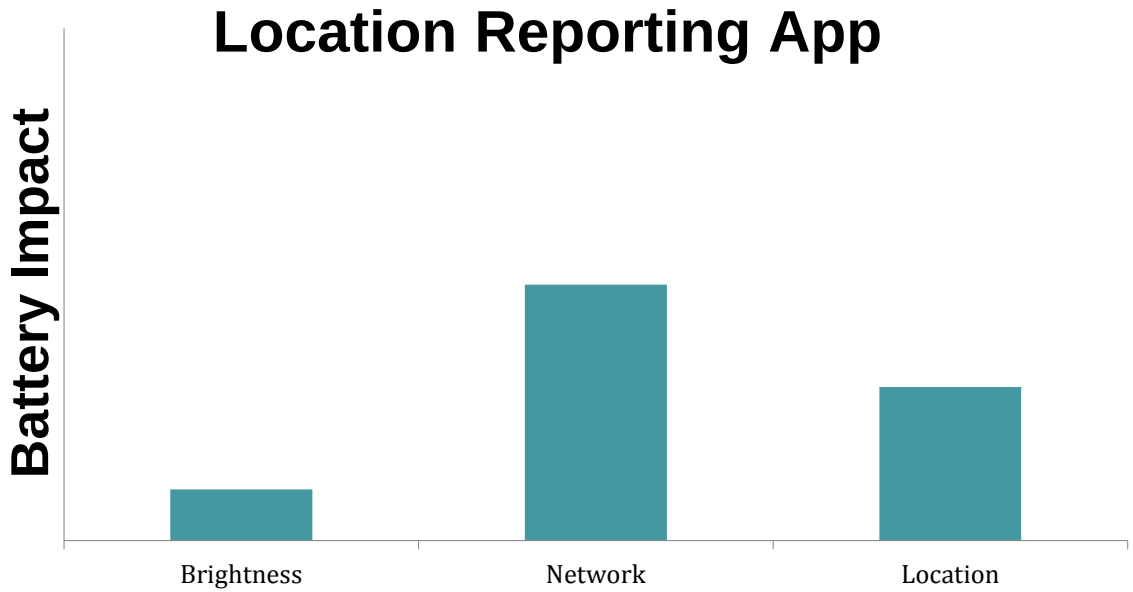
Battery Life – Workshop Feedback



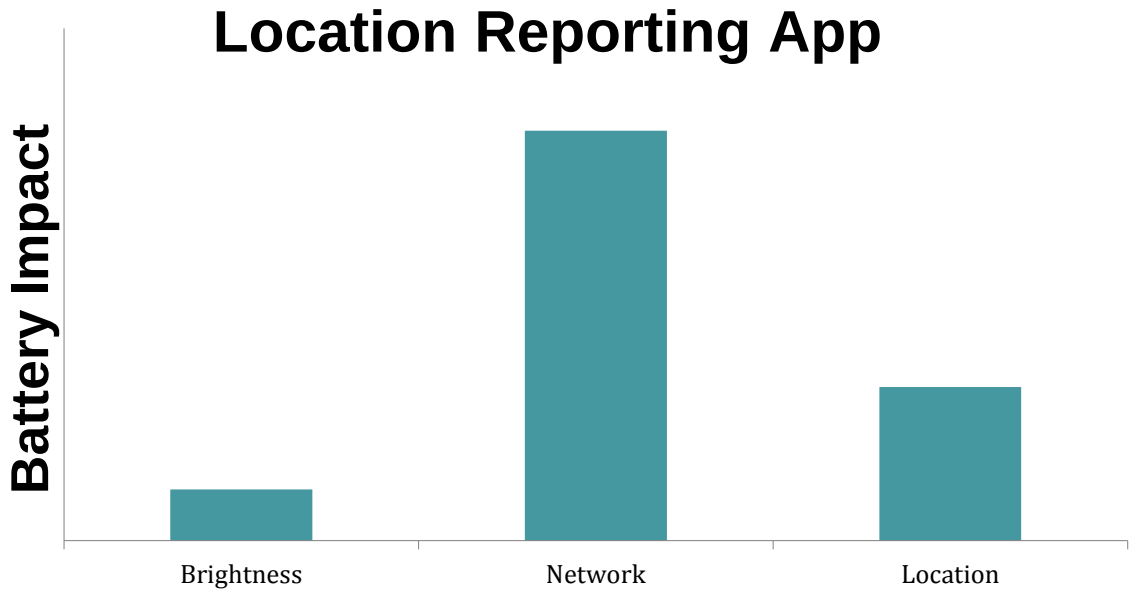
Battery Life – Workshop Feedback



Battery Life – Workshop Feedback



Battery Life – Workshop Feedback



Battery Life – Next Steps

- Evaluate existing battery usage metrics
- Evaluate effectiveness of power management profiles
- Evaluate feasibility of remote power management

Battery Life – New Key Attributes

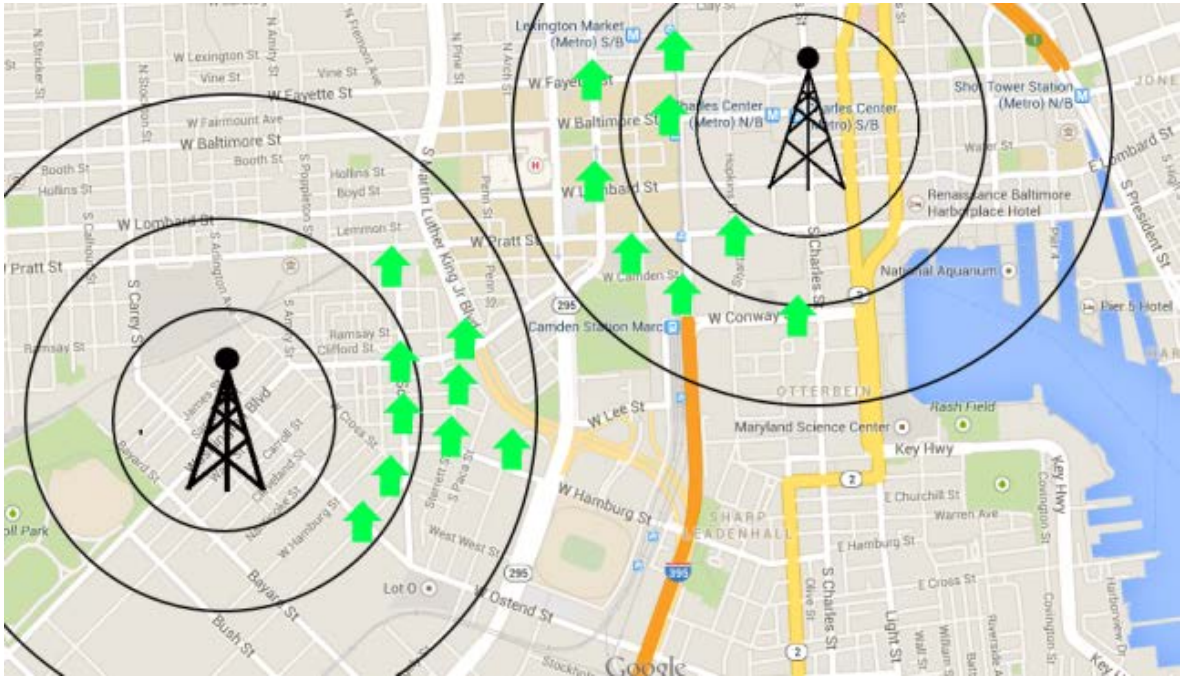
- Applications should report usage using battery metrics
- Battery intensive applications should be configurable
  - Power management profiles
  - Remotely
  - On demand by user

Unintentional Denial of Service

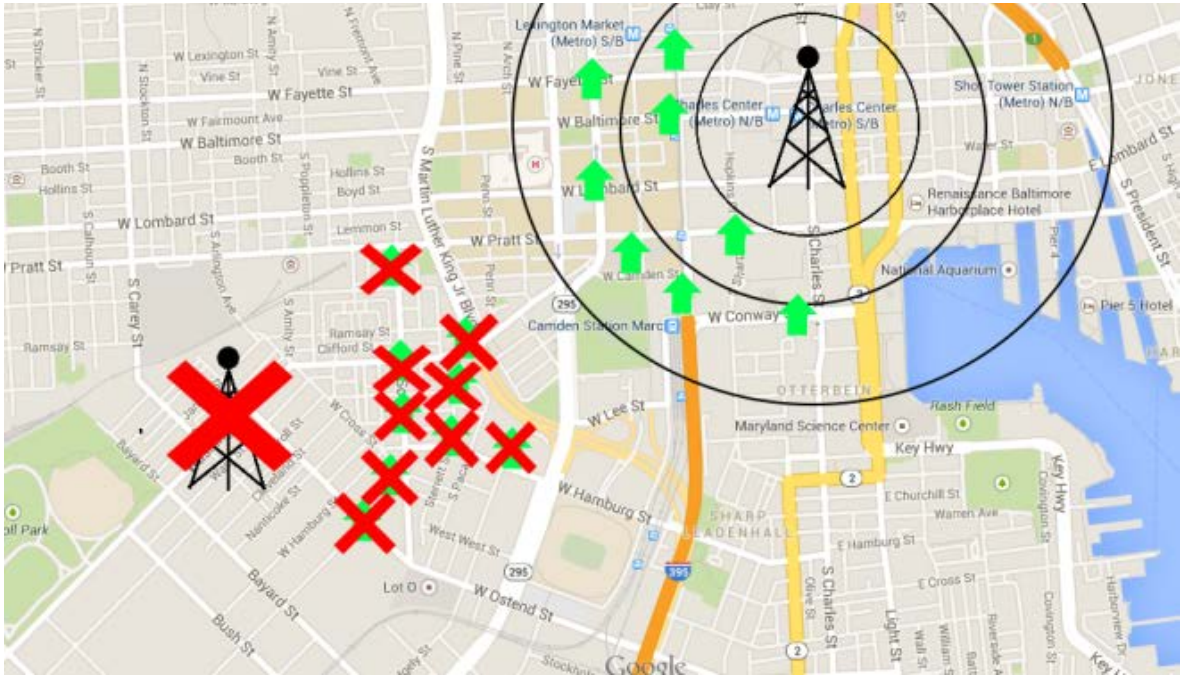
Unintentional Denial of Service (DoS)

A situation where access to a website, server, or service is denied, not due to a deliberate attack, but as a result of a sudden or sustained spike in user traffic

Unintentional DoS – Workshop



Unintentional DoS – Workshop



Unintentional DoS – Workshop Feedback

- Allocating limited resources
- Concern over FirstNet performance
- Limitations of FirstNet Unknown
  - Will change as FirstNet rolls out
  - Will differ from jurisdiction to jurisdiction
- No mission critical voice or data

Unintentional DoS – Workshop Feedback

- Remote monitoring and management
  - Throttle individual applications
  - Stratify users by current need
- LTE Quality of Service features

Unintentional DoS – Recommended Next Steps

- Discover real world load limitations of FirstNet
- Evaluate QoS features for on demand network control
- Identify and explain to public safety community how to use FirstNet most responsibly in terms of network throughput.

Unintentional DoS – New Key Attribute

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

DATA PROTECTION

Data Protection

- Divided into three categories
  - Confidentiality
  - Integrity
  - Availability
- Requirements defined by data owner
- Requirements motivated by law and policy
  - Health Insurance Portability and Accountability Act (HIPAA),
  - Criminal Justice Information Services (CJIS) Security Policy

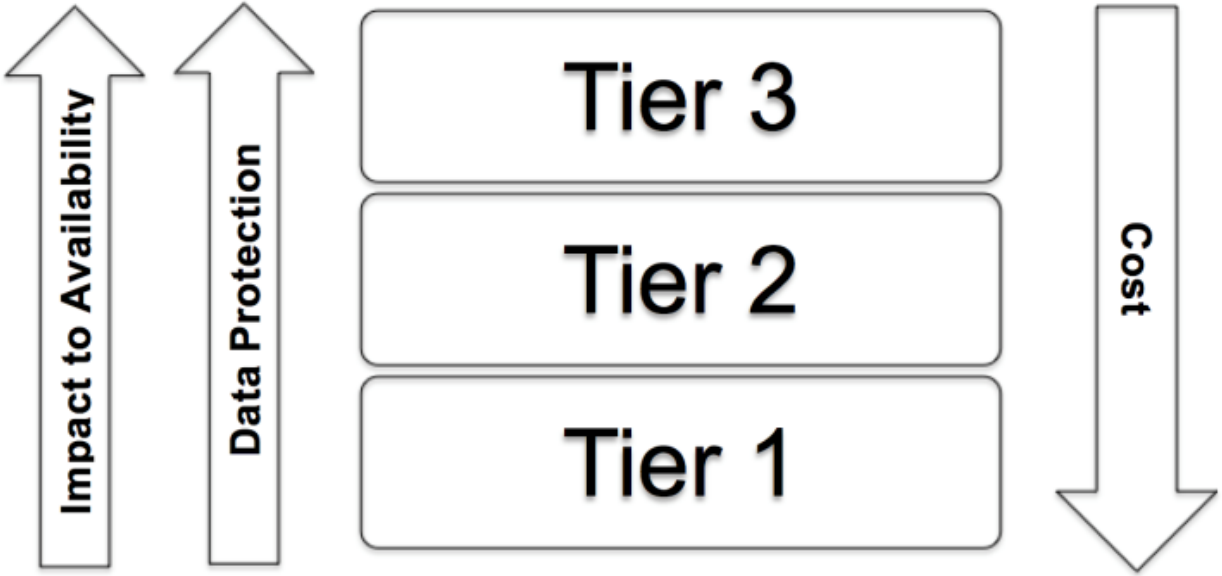
APCO Key Attribute

- Sensitive information is stored and transmitted using encryption

Data Protection – Workshop Feedback

- Two Approaches for data protection
  - Define baseline capabilities and functionality
  - Let developers define their own
- Capability and functionality baseline
  - Enumerate Public Safety data types
  - Define data protection for each type

Data Protection – Tiered Approach



Data Protection – Workshop Feedback

Software Development Kits (SDK)

- Libraries and API implementations
- Pros:
  - Reviewed
  - Reused
- Cons:
  - Rigid
  - Lock developers into 3rd party tools

Specification

- Needed functionality and requirements
- Pros:
  - Flexible
  - Evaluate SDKs for compliance
  - Evaluate apps for compliance
- Cons:
  - Apps must be tested

Data Protection – Recommended Next Steps

- Develop a public safety data dictionary
- Develop baseline data protection specification
- Develop a tiered data protection hierarchy

Data Protection - Recommendations

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

Location Information

Location Information

- Any data collected, stored or transmitted concerning the physical location of a device
- Special subset of Data Protection
- More immediate and severe implications

Location Information

- Factors governing location information use
  - Accuracy
  - Integrity
  - Confidentiality

APCO 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

Location Information – Workshop Feedback

- Control of location services
- Accuracy and freshness
- Lifetime of local logging
- Transfer format of location information

Location Information – Next Steps

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

Location Information - Recommendations

- Location features must be configurable
  - By user
  - Remotely
- Location refresh rate be configurable

Identity Management

Identity Management

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

http://csrc.nist.gov/publications/drafts/nistir-8014/nistir_8014_draft.pdf

APCO Key Attribute

- Securely supports identity management

Identity Management – Workshop Feedback

- Identity management and authentication issues
  - Interfacing with existing Identify Management Systems
    - Federal
    - State
    - Local
  - How apps authenticate users
- Complicated

Identity Management – Workshop Feedback

- Authentication directly impact usability
- Authentication occurs at different levels
  - Device Boot
  - Device unlock
  - App level

Identity Management – Workshop Feedback

Authentication Mechanisms

Something you know

- Passwords
- Pin numbers

Something you have

- RSA tokens
- ID Badges
- Mobile Device

Something you are (Biometrics)

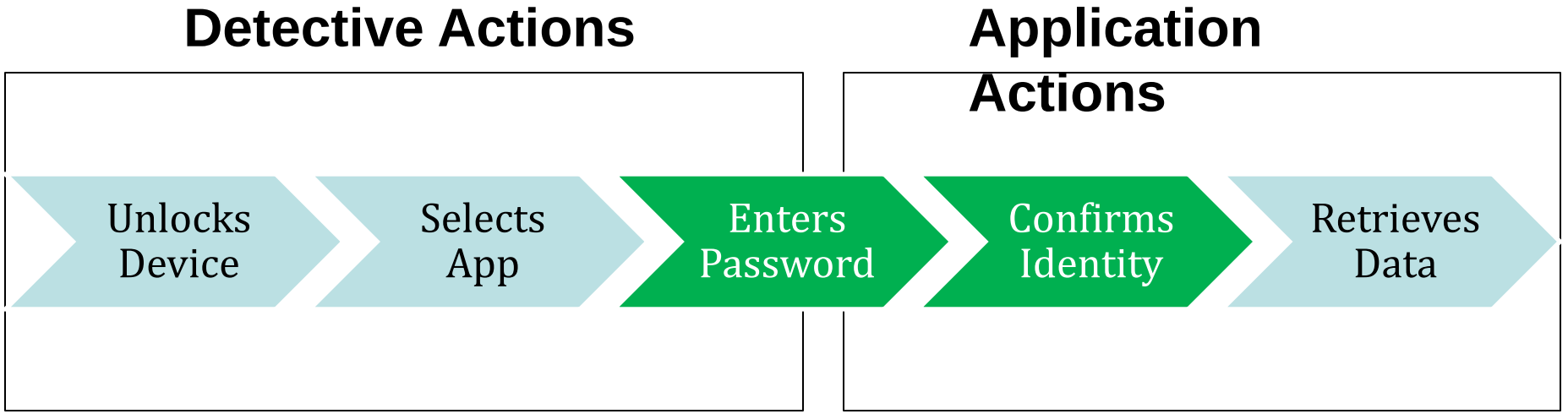
- Fingerprints
- Retinal Scans
- Facial recognition

Identity Management – Workshop Feedback

- Authentication must match operation
- Impractical is certain situations
- Availability may be more important than Authentication
  - Authentication takes time
  - Authentication takes attention

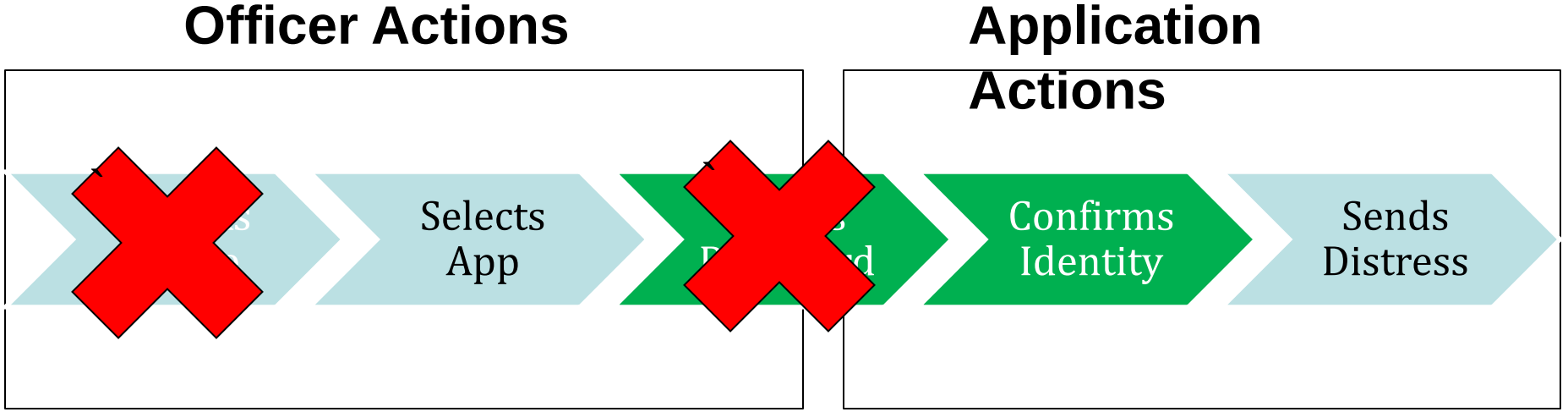
Identity Management – Example Scenarios

Retrieving Sensitive Information



Identity Management – Example Scenarios

Man Down



Identity Management – Next Steps

- Enumerate Identity management systems
- Establish parameters for acceptable authentication levels
  - Matching scenarios/roles to mechanisms
  - Identifying zero-authentication scenarios

MOBILE APPLICATION VETTING

Mobile Application Vetting

- Mobile app vetting is crucial
- Vetting can be addressed by
  - First party (App Vendor)
  - Second party (Purchaser)
  - Third party (impartial authority)
- App Vetting will have two audiences
  - Public safety community member apps
  - Crowd-serving apps

Mobile Application Vetting
Infrastructure Building Blocks

- Public safety related requirements
- Test protocols
- Application Testers
- Certifying Organizations

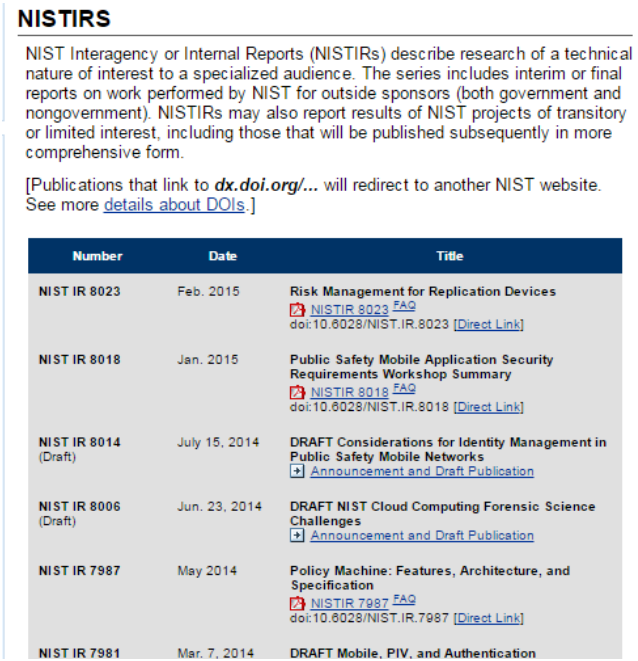
Mobile Application Vetting-Next Steps

Considerations

- Problems
  - Testing is expensive and slow
  - Forcing certification can be detrimental
- Solutions
  - Leverage existing services
  - Public Safety Profiles

NIST Interagency Report

- Available at NIST's Computer Security Resource Center(CSRC)
- http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf



NISTIRS

NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

[Publications that link to ***dx.doi.org/...*** will redirect to another NIST website. See more details about DOIs.]

Number	Date	Title
NIST IR 8023	Feb. 2015	Risk Management for Replication Devices NISTIR 8023 FAQ doi:10.6028/NIST.IR.8023 [Direct Link]
NIST IR 8018	Jan. 2015	Public Safety Mobile Application Security Requirements Workshop Summary NISTIR 8018 FAQ doi:10.6028/NIST.IR.8018 [Direct Link]
NIST IR 8014 (Draft)	July 15, 2014	DRAFT Considerations for Identity Management in Public Safety Mobile Networks Announcement and Draft Publication
NIST IR 8006 (Draft)	Jun. 23, 2014	DRAFT NIST Cloud Computing Forensic Science Challenges Announcement and Draft Publication
NIST IR 7987	May 2014	Policy Machine: Features, Architecture, and Specification NISTIR 7987 FAQ doi:10.6028/NIST.IR.7987 [Direct Link]
NIST IR 7981	Mar. 7, 2014	DRAFT Mobile, PIV, and Authentication

Next Steps: Vetting Service Survey

- Identify existing commercial services
- Enumerate vetting features

Upcoming Workshop

- Focusing on data protection
  - Compiling mobile application data types
  - Examining implications of losing
    - Integrity
    - Availability
    - Confidentiality
- Location and date: TBD
- Contact me if you are interested in attending

Identifying Public Safety's Security Requirements for Mobile Apps

Michael Ogata
Computer Scientist, NIST
michael.ogata@nist.gov