Mobile Application Security for Public Safety

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.

Introduction

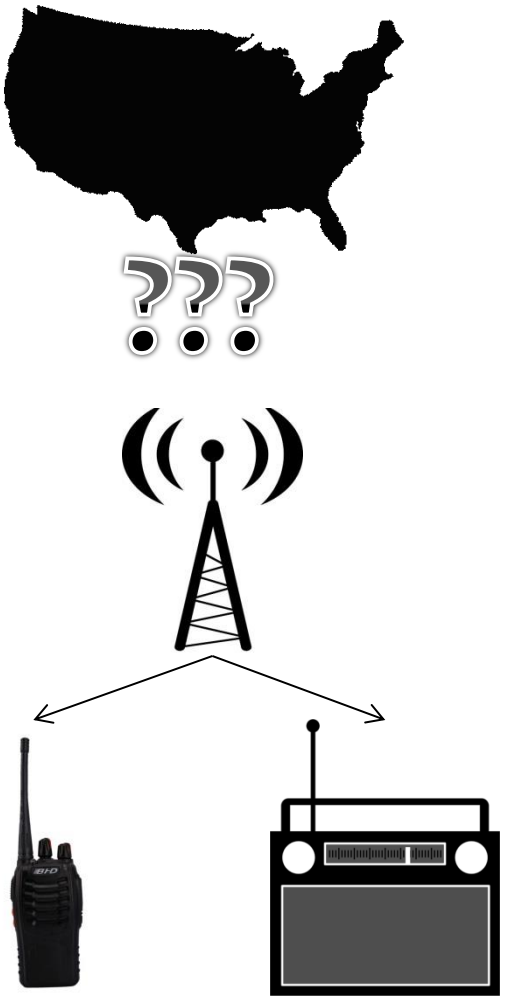
- What are we going to discuss?
  - NIST's efforts in defining and understanding mobile application security as it relates to public safety
- Who is involved?
  - Public Safety Communications Research (PSCR)
    - National Institute of Standards and Technology (NIST)
    - The National Telecommunications and Information Administration (NTIA)
  - First Responder Network Authority (FirstNet)
  - Federal, state, and local public safety organizations

Introduction –Why Mobile App Security?

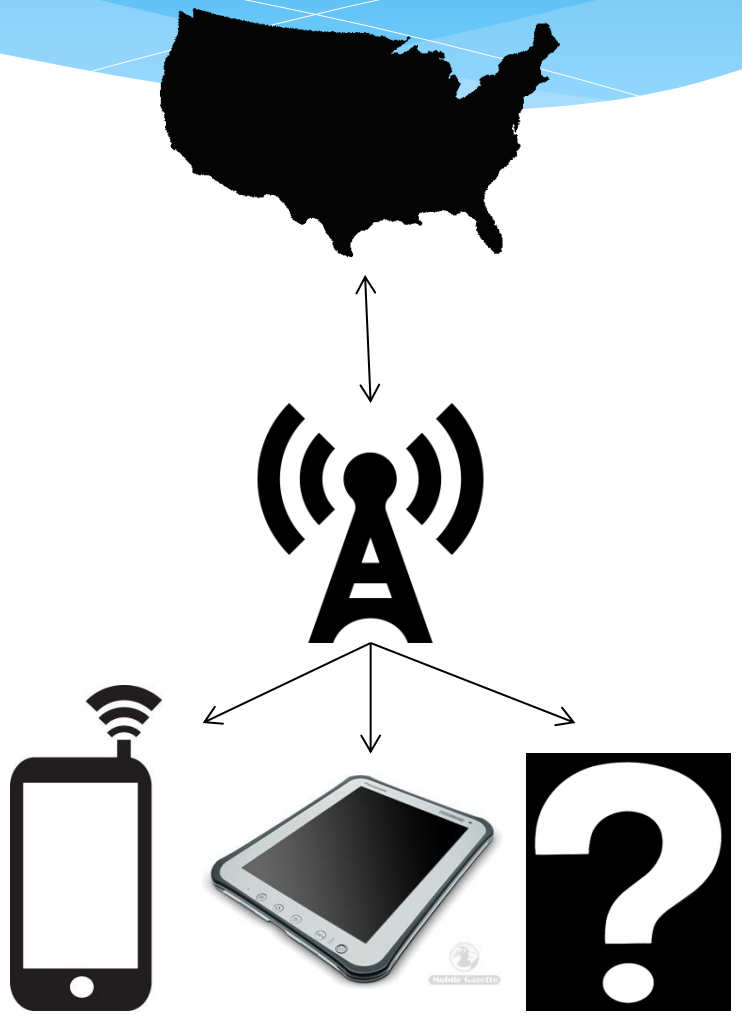
- Middle Class Tax Relief and Job Creation Act of 2012
  - Nation's first interoperable Public Safety Broad Band Network (PSBN)
  - Long Term Evolution LTE network
- Many public safety organization already use apps on commercial networks
- Public safety has specific domain needs and requirements

The Changing Landscape

LMR



PSBN



Discussion Topics

- Engaging public safety professionals
  - Workshop I: Public Safety Mobile Application Security Requirements Workshop
  - Workshop II: Identifying and Categorizing Data Types for Public Safety Mobile Applications
- Mobile Application Vetting Services
- Future Work

Common Themes

- Allocation of finite resources
- Local control and fine grain configuration
- Defining role based needs/profiles

Workshop I

Identifying Public Safety's Security Requirements for Mobile Apps

Public Safety Mobile App Security Requirements

- Held February 2014
- NISTIR 8018 published January 2015
- Identify security concerns specific to public safety
- 50 public safety community members
  - Law enforcement
  - Emergency Response
  - Application Developers

Impetus

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

Workshop Goals

- Identify mobile application security requirements for public safety
- Identify areas of required further research

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 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

Workshop Discussion Topics

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

Battery Life

Battery Life

Domain Specific Considerations

- Impaired/varying network availability
- Requirements for location services
- High bandwidth media streams
- Extensive field time
- Extreme temperatures

Battery Life

Domain Specific Considerations

- Different Roles have different needs
- Different Situations have different needs

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

Battery Life
Recommendations

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

Battery Life – Next Steps

Next Steps

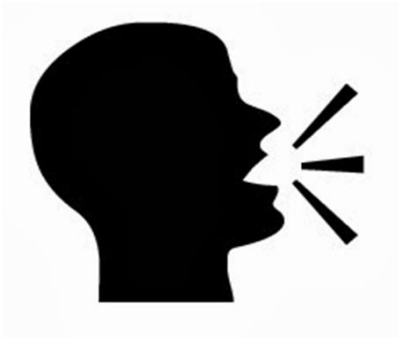
- Evaluate existing battery usage metrics
- Evaluate effectiveness of power management profiles
- Evaluate feasibility of remote power management

Unintentional Denial of Service

Unintentional Denial of Service (DoS)

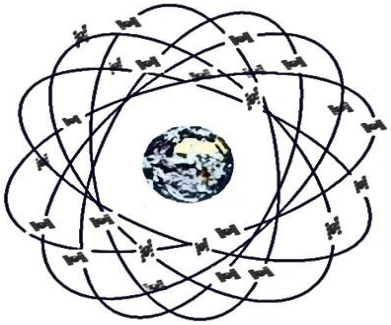
- A situation where access to a website, server, or service is denied, not due to a deliberate attack, but as a result of a sudden or sustained spike in user traffic

Unintentional DoS



Voice

Video



Location

W Lexington St
W Fayette St
W Baltimore St
W Lombard St
Pratt St
W Pratt St
Martin Luther King Jr Blvd
Lexington Market (Metro) S/B
Shot Tower Station (Metro) N/B
Renaissance Baltimore Harborplace Hotel
E Lombard St
S President St
Ostend St
Bush St
Lot O

Unintentional DoS

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

Unintentional DoS

Next Steps

- PSCR PSBN research work: identifying the limitations of the network
  - Modeling and measuring throughput
  - Extending the range of LTE deployments
  - Researching models for network congest
  - Evaluating QoS features for on demand network control

http://www.pscr.gov/projects/broadband/700mhz_demo_net/meetings/stakeholder_mtg_062015/index.htm

Unintentional DoS

Recommendations

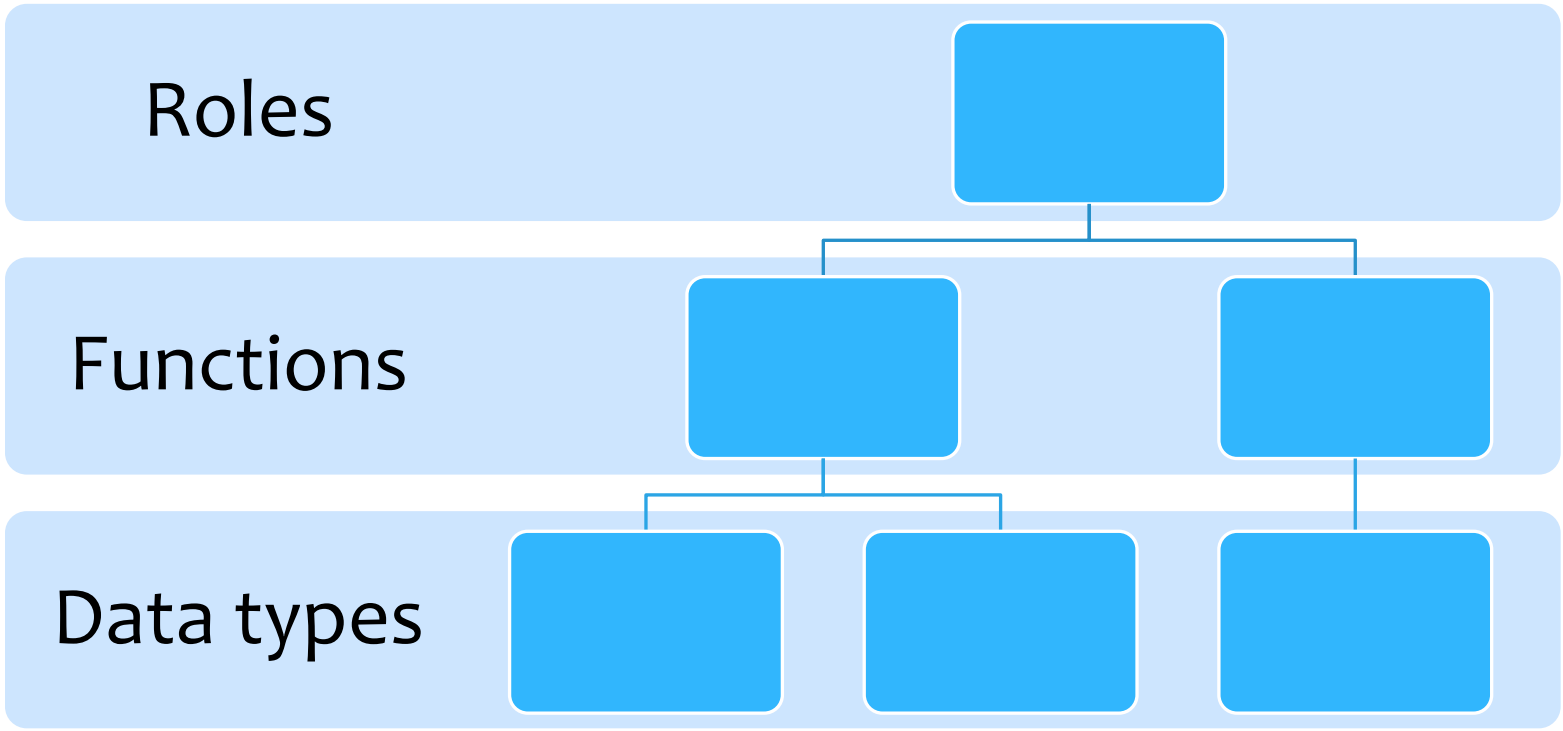
- Applications must prove they use the network in an efficient and responsible manner.
  - Actionable metric when selecting apps
  - Target for app developers
  - Aides profile based management strategies

Data Protection

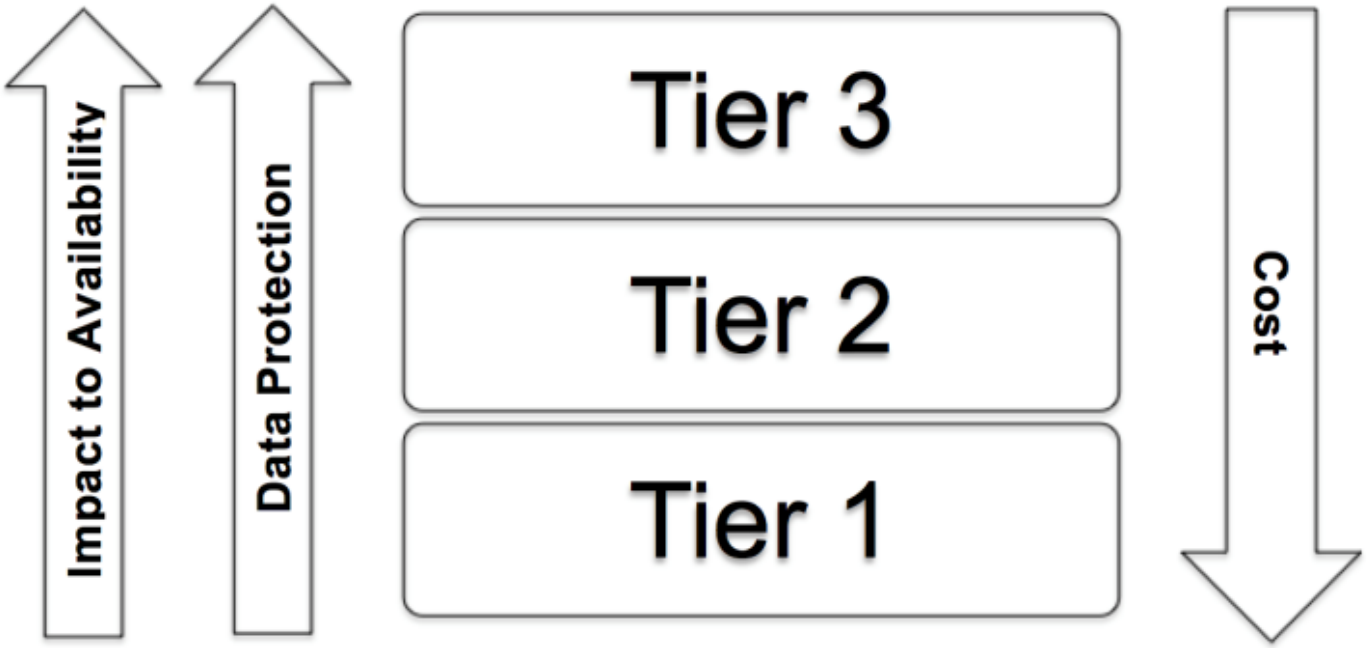
Data Protection

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

Data Protection - Baseline



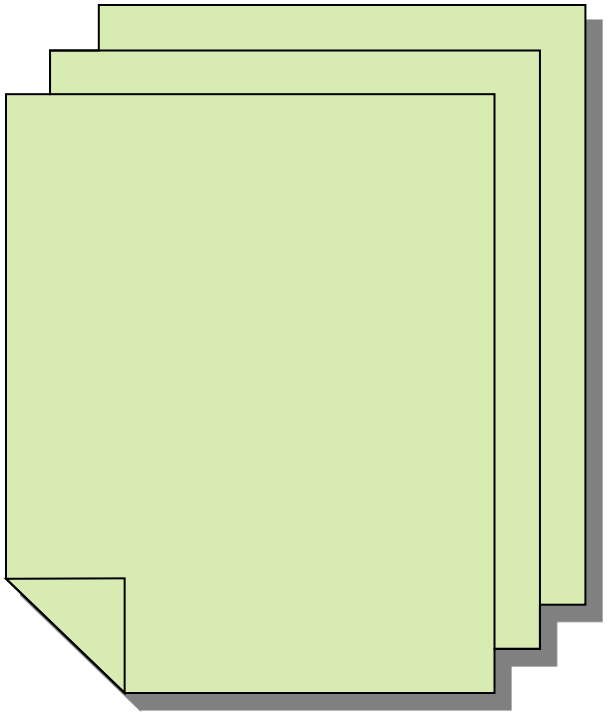
Data Protection – Tiered Approach



Data Protection

Implementation Strategy

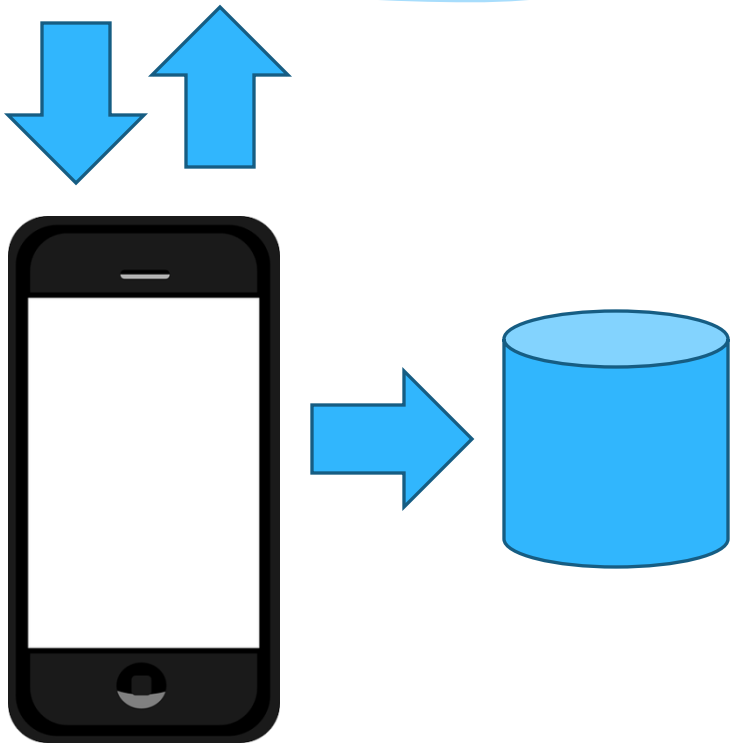
- Data protection specification
- Pros:
  - Evaluate SDKs for compliance
  - Evaluate apps for compliance
- Cons:
  - Apps must be tested



Data Protection

Recommendations

- Develop a data dictionary
- Applications should declare
  - Data consumed
  - Data stored
  - Data transmitted



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

Next Steps

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

Location Information

Recommendations

- Location features should be configurable
  - By user
  - Remotely
- Location refresh should rate be configurable
- Application must make declaration
  - What location data is being collected
  - Where location data is being transmitted

Identity Management

Identity Management

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

Identity Management

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

Identity Management

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

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

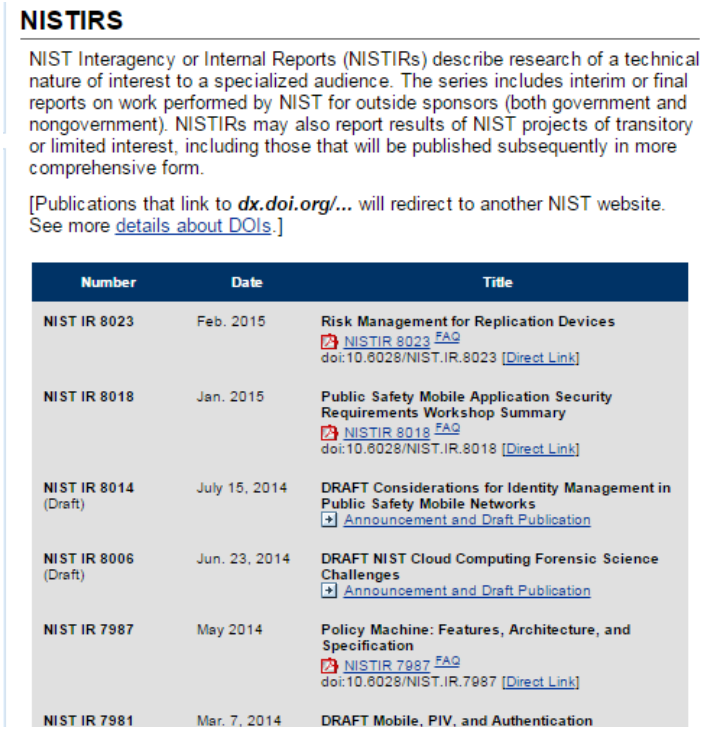
Recommendations

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

Mobile Application Vetting

NIST Interagency Report 8018

- 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.]

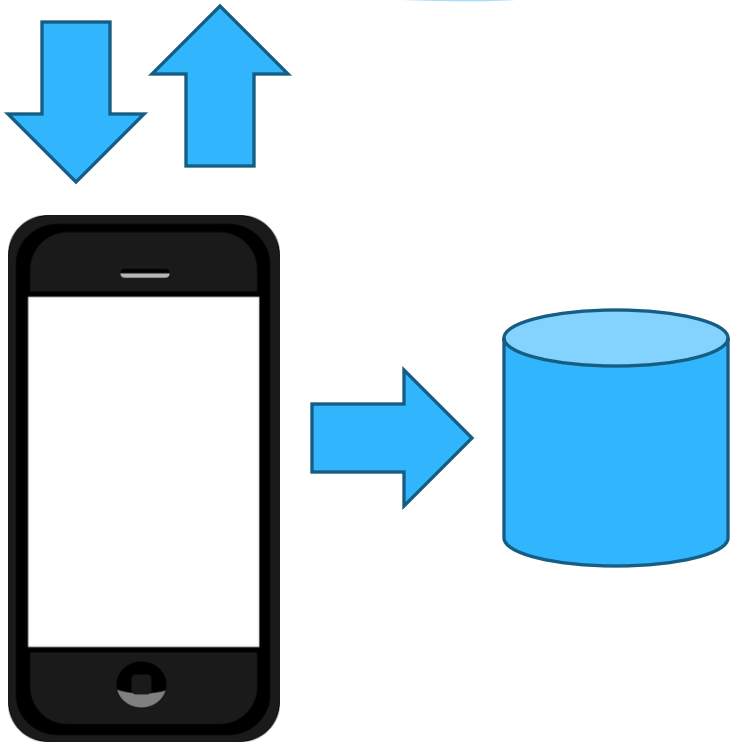
Number	Date	Title
NIST IR 8023	Feb. 2015	Risk Management for Replication Devices NISTIR 8023 FAQ doi:10.6028/NIST.IR.8023 [Direct Link]
NIST IR 8018	Jan. 2015	Public Safety Mobile Application Security Requirements Workshop Summary NISTIR 8018 FAQ doi:10.6028/NIST.IR.8018 [Direct Link]
NIST IR 8014 (Draft)	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

Workshop II

Identifying and Categorizing Data Types for Public Safety Mobile Applications

Workshop II: Data Types for Public Safety

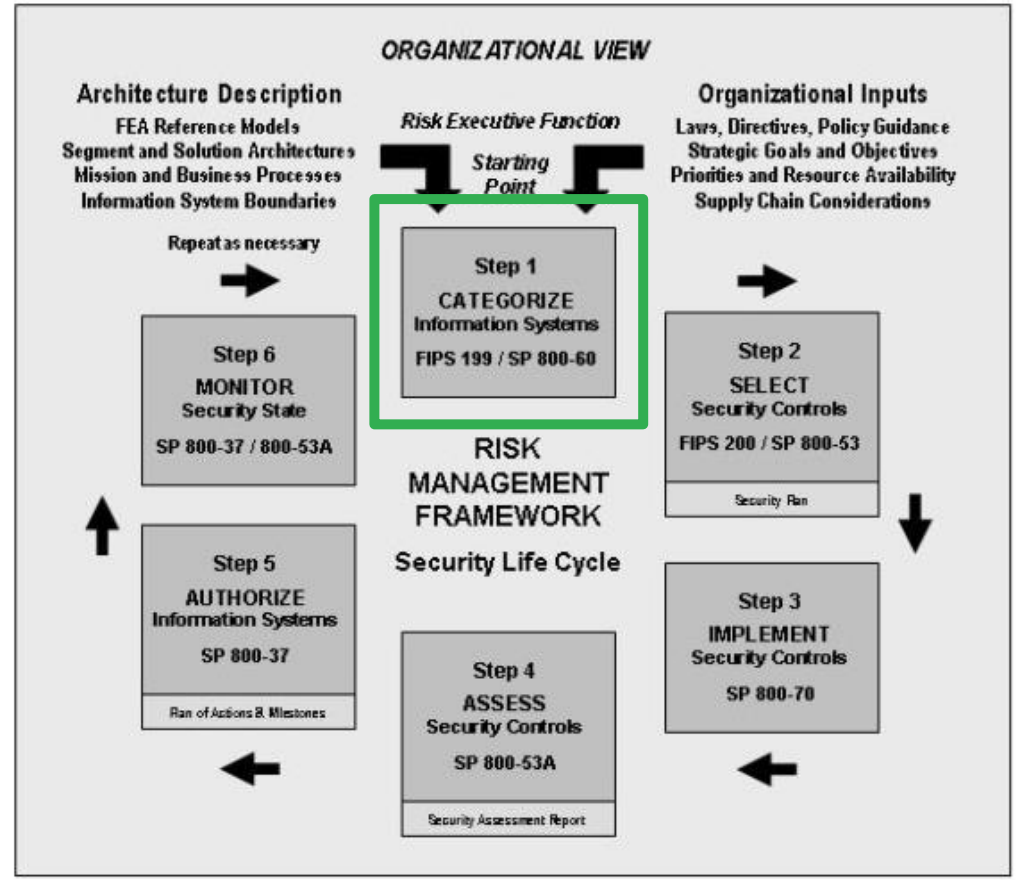
- Goals
  - Identify Data Types
  - Security categorization
  - Explore desired app functionality



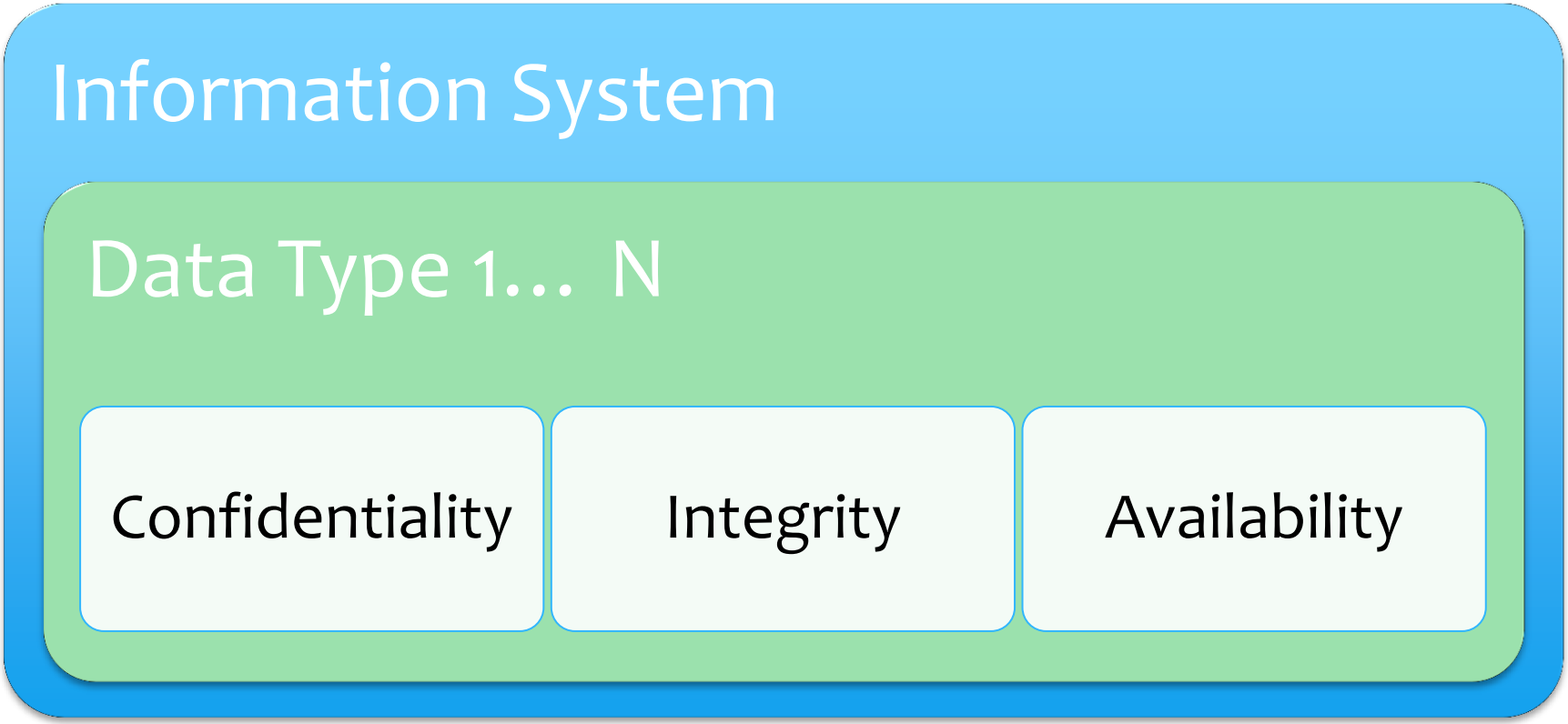
Benefits of a Data Dictionary

- Familiarizes developers with public safety's mission
- Provides common language when describing, comparing, and requesting mobile apps
- Aides in information sharing
- Promotes interoperability
- Aids in contingency and disaster recovery planning
- Enables other recommendations NISIR 8018

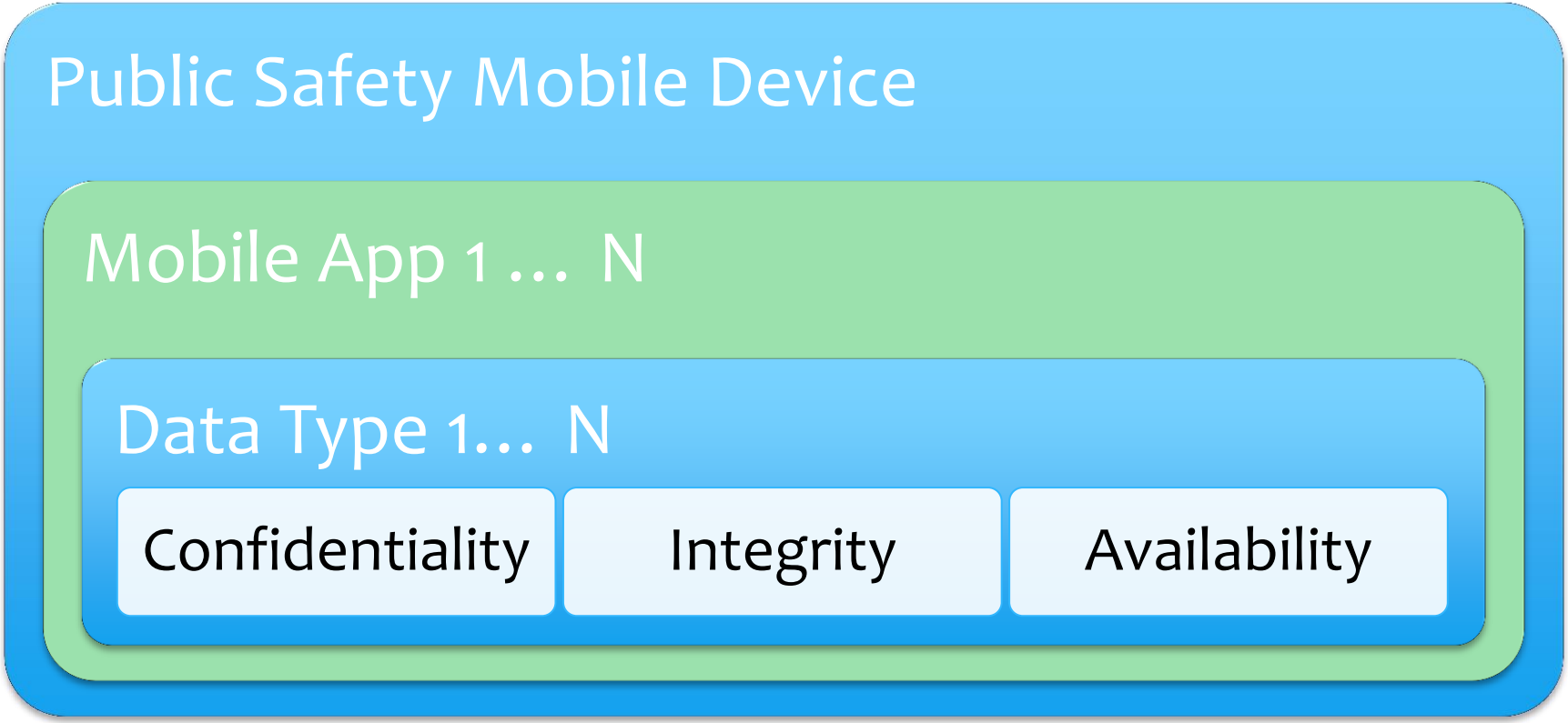
NIST Risk Management Framework: Security Categorization



Security Categorization



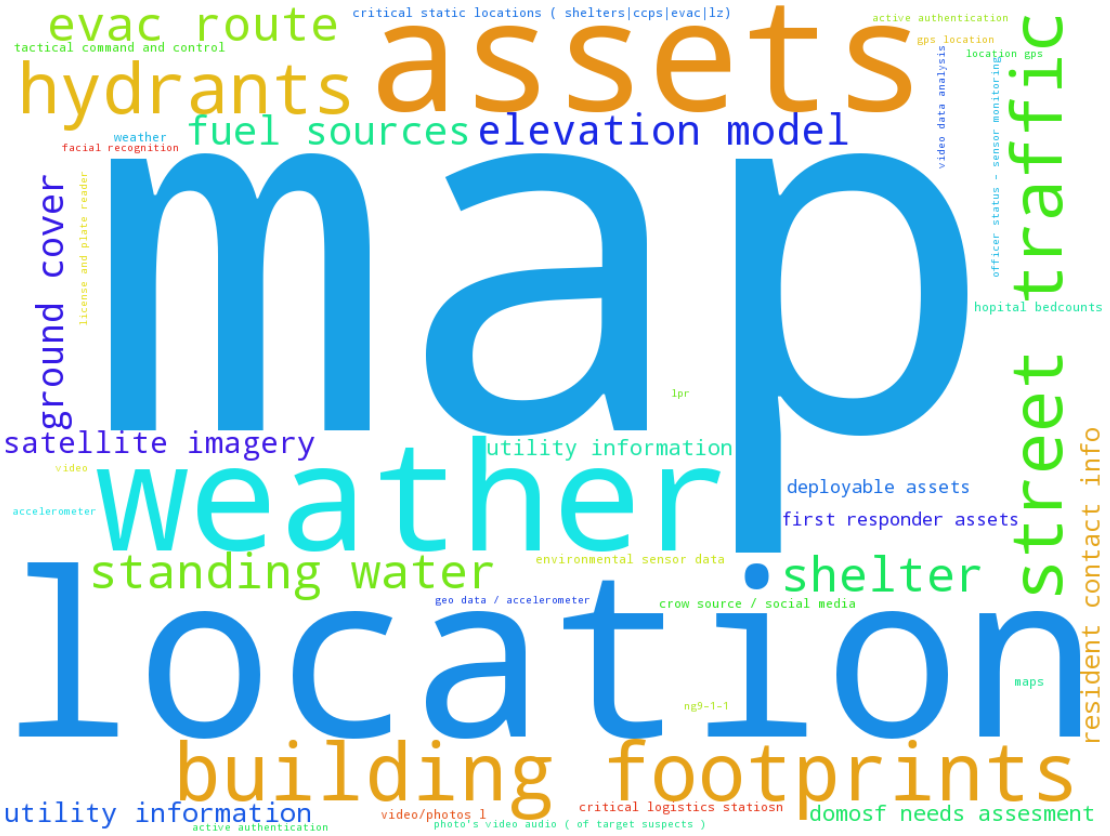
Security Categorization



Workshop Format

- Broke workshop into small working groups
  - Tried to make each group as heterogeneous as possible
- Provided sample scenarios to each group
- Asked groups to imagine
  - they had the “perfect app” on the “perfect device”
  - List data types their devices would handle
  - Categorized those by their impact to security

Data Types for Public Safety



Data Type Groups

- Operations
- Situational Awareness
- Sensor Data

Operations Data

High	• **Confidentiality**
High	• **Integrity**
High	• **Availability**

Operations Data

- Tactical Command and Control
- Incident action plans
- Deployable Assets
- GIS Intel Location
- White boarding

Situational Awareness Data

- **Confidentiality**
- **Integrity**
- **Availability**

Situational Awareness

- Building blueprints
- Weather
- Map data
- Hospital capacity
- DoT information

Sensor Data

Medium	• **Confidentiality**
High	• **Integrity**
High	• **Availability**

Sensor Data

- Environmental sensor data
- Location GPS
- Officer Status monitoring

Temporal Nature Data

- During vs after an incident
- Incidents escalate and change

Crowd Sourced Data






Mobile Application Vetting

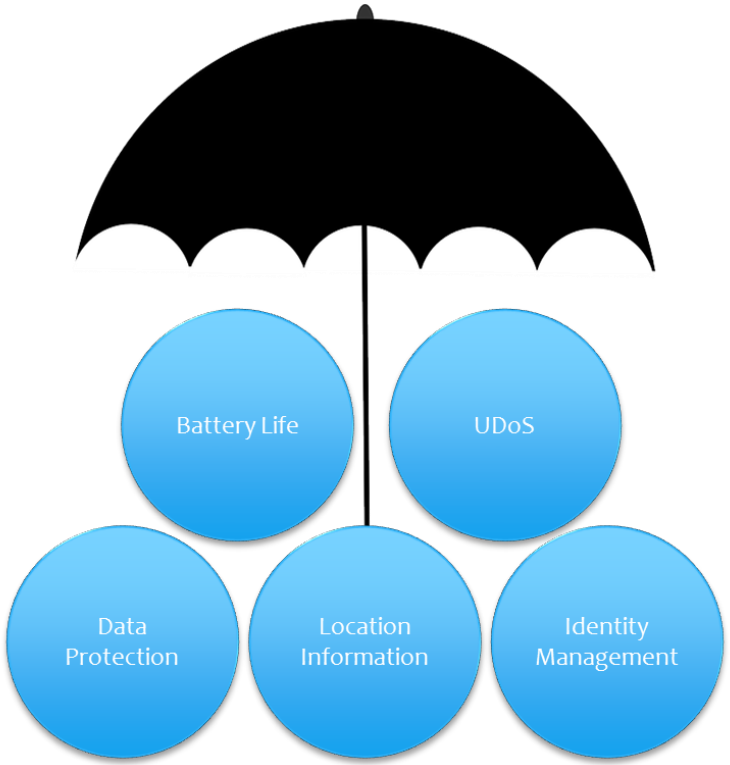
Mobile Application Vetting

- Mobile app vetting is crucial
  - Domain specific requirements
  - General software quality
- App Vetting will have two audiences
  - Public safety community member apps
  - Crowd-serving apps

Mobile Application Vetting

Considerations

- Problems
  - Vetting is expensive
  - Time consuming
  - Resource Intensive
  - Difficult to manage
- Solution
  - Leverage existing solutions



Vetting Service Comparison

No.	FEATURES	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Distributed vs. Centralized	D	D	C	C	D	D/C	D	D/C	D	D	D	C	D
2	Static vs. Dynamic	S/D	S/D	S/D	S/D	S/D	S/D	S	S/D	S/D	S	S	S	S/D
3	Pricing Models	$	$	$	$	$	$	$	$	$	$	$	Free	$
4	On Demand Scans	✘	✓	✓	✓	✓	✘	✘	✓	✓	✘	✘	✓	✓
5	Personal vs. Enterprise	E	E	E	E	E	E	E	P/E	E	E	E	P	P/E
6	Mobile Devices	Android, Apple, Windows, BB		Android, Apple, Windows	Android, Apple			Android, Apple, BB,	Android, Apple		Android, Apple, BB, Windows	Android, Apple, BB, Windows, Nokia	Android	Android, Apple
7	Public Safety Analytics	✓	✘	✘	✓	✓	✓	✘	✘	✘	✓	✘	✓	✘
8	Repository	✘	✘	✘	✓	✘	✘	✘	✓	✘	✘	✘	✓	✓
9	Report Review	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Report Distribution													
11	Mobile App Dataset	✘	✘	✘	✓	✘	✘	✘	✓	✘	✘	✘	✓	✓
12	Country of Service Provider	U.S., Mexico	U.S., U.K.	Israel	U.S., The Netherlands	U.S., U.K., India	U.S., Asia Pacific	U.K., South Africa, Latin America	U.S., U.K., Japan, Canada, Australia, Singapore	U.K.	U.S.	U.S., U.K., India, Thailand, Malaysia, Indonesia	U.S.	U.S., U.K.
13	General Testing	✘	✘	✘	✘	✓	✓	✘	✘	✘	✘	✘	✘	✘

App Vetting Features

- Origin country of service provider
- Supported mobile platforms (Android, iOS, etc…)
- Analysis methodologies
- Application Corpus
- Contract Models
- Reporting

Analysis Methodologies

- Static vs. dynamic
- Distributed vs. centralized
- Domain restriction
- App version regression
- Platform Enumeration

Application Corpus

- Automated app store scrapping
- On Demand Scanning

Contract Models

- Pricing Models
- Personal vs. Enterprise

Reporting

- Report format
- Report redistribution

Future Work

Feature Work

- Finish Report on Workshop II
- Finalize draft of mobile application vetting services
- Engage with FirstNet Application Team
- Explore Federal Mobile Application Security Efforts

Michael Ogata
michael.ogata@nist.gov

Questions?

Both 219 on the expo floor!