APCO International

Leaders in Public Safety Communications™

PSCR

Emerging Technology Forum

Public Safety Mobile Application Security Requirements Workshop

Nelson Hastings

Computer Security Division, NIST

February 26, 2014

Objectives

- Begin/continue dialog between the public safety and mobile application development communities

- Document initial security requirements for public safety mobile applications

- Document strategies for conformity assessment of the public safety mobile application security requirements

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

Six Topics Discussed

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

Battery Life

- 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)

- 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 be designed to optimize network usage
  - Limiting idle connections
  - Efficient caching
  - Adapting to network load

Mobile Application Vetting

- 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 in a useful way

- What are some of the variables – time, cost, technology

Location Information

- 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

- 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

- 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?

Next Steps

- 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

Q & A

Follow APCO at…

facebook.com/apcointernational

@apcointl