Public Safety & 9-1-1 Mobile Apps

Mark Reddish
Senior Counsel & Manager of Government Relations
APCO International
www.AppComm.org
Different Types of “9-1-1” Apps
Misleading Claims

• The app can “pinpoint” user locations.
• The app is certified.
• Let’s you communicate directly with first responders.
• It’s better than 9-1-1.

• (Often contradicted by the Terms of Service)
  • “not a replacement for 9-1-1”
  • “do not rely on the [app]”
Upgraded required
Because you recently upgraded to iOS9, you must update this app.
Update App

Application crash
Your last session closed unexpectedly. Send a crash report?
No, thanks  Send report

Location Services
To continue you must enable location services
Go to Settings

Not Available In App Store
This app is not currently available in the store. Contact the app developer for more information.
OK
Claim: “The app can find you, but 9-1-1 can’t.”
APCO’s Vision for a 9-1-1 App

- Comply with industry standards
- Work anywhere in the country
- Be as reliable as the existing 9-1-1 system
- Preserve the familiar simplicity of 9-1-1
- Connect users to the appropriate PSAP
- Comply with FCC rules, state/local regs, and industry best practices
- Work without delay, regardless of device or app software updates
- Be free to the public and not impose unreasonable costs on PSAPs
- Be device and OS agnostic
- Meet public safety’s cybersecurity needs
- Efficiently use/monitor device battery and throttle-down if necessary
Mobile App Security Testing
App Security Testing

• Partnership with DHS OIC

• Explored whether app testing platforms can detect security vulnerabilities such as:
  • Excessive Permissions
  • Sensitive Data Exposure

• Adapted a program used by federal agencies for public safety and considered broader issues such as:
  • Data interoperability between agencies
  • Meeting security requirements
  • Compliance with federal, state, & local laws, regulations, & policies
Mobile App Analysis

**Android and iOS application analysis**

- No source code needed
- Submitted to Kryptowire directly from AppComm
- Automated analysis
- Combination of Dynamic and Static Analysis
- Confidential results
Security Evaluation Categories

Security

- The Kryptowire platform scans for various security issues that can be present in applications causing them to be vulnerable to exploitation. These types of issues can lead to sensitive data that is handled by the application to be compromised by malicious parties. Each of these issues should be considered carefully by the reviewing party and developers to ensure that applications are as secure as possible before they are distributed to users.

Privacy & Information Access

- Mobile applications can potentially have access to a wealth of sensitive information about the user and or device. These findings can range from applications integration with ad networks to proper handling of a user’s password. Each piece of information that is accessed by the application should be able to be justified by core functionality which is needed for operation.

Device Access

- The platform performs analyses to identify which sensitive functionality of the device that the application might access. The analysis will be able to identify the usage of these functionalities as well as the context to better understand the nature of the access. As with the privacy and information access, it should be evaluated whether the application requires these functionalities for its intended task.
Participants and Scan findings

- 20 app developers
- 10 dropped out during the pilot
- 33 apps tested total (15 Android & 18 iOS)
- Findings in two categories: red and orange
  - Red findings are more critical and should be corrected by developers unless sufficient evidence is provided to justify the behavior.
  - Orange findings correspond to behavior that is often necessary for operation, but requires that the developer explain the need for the functionality. These findings can often identify unnecessary code that is included in the application which can be safely removed.
Sample Report

**Required Developer Action**

Uses hard coded credentials for secure operations

Scans were performed on the application's byte code and any packaged SDKs to search for hard-coded credentials used in cryptographic functions. These codes are declared as constant values within the application's code.

The application contains a hard coded credential to perform secure operations such as encryption or web authentication. This allows anyone who has access to the application to retrieve the credentials and perform the same operations compromising security and privacy. Proper functionality provided by the native platform should be used to properly create and store credentials. More information can be found [here](#) and [here](#) (Android, iOS).

**Required Developer Explanation**

Integrates with an ad network

This application integrates with one or more ad networks which can potentially expose sensitive user information to 3rd parties.

We identify through Dynamic Analysis if the application integrates with an ad network during execution. Please explain the ad networks your application integrates with and what data is given to them.

Developer explanation:
Android apps

• All apps had at least one issue that was found
• 5 apps had red flags
  • 6 red flags total
  • Example findings:
    • Uses hard coded credentials for secure operations
    • Contains code to accept all SSL certificates
• 15 apps had orange flags
• 52 orange flags total
• Example findings:
  • Accesses device’s microphone
  • Accesses device’s camera
iOS apps

- 17 apps had at least one issue, 1 app had no issues
- 13 apps had red flags
  - 14 red flags total
  - Example findings:
    - iOS Application Transport Security feature disabled
    - Exposes sensitive user/device information
- 17 apps had orange flags
  - 57 orange flags total
  - Example findings:
    - Accesses the device’s contacts
    - Accesses the device’s microphone
Red & Orange Flags for 33 Apps

- Android Red Flags: 6
- Android Orange Flags: 52
- iOS Red Flags: 14
- iOS Orange Flags: 57
Addressing the Red & Orange Flags

- 20 red flag issues that were found:
  - 5 addressed/corrected by developers
  - 2 explained to be necessary for application’s operation
  - 1 flag determined to be a non-issue
  - 12 flags unaddressed

- 109 orange flag issues that were found:
  - 39 flags explained as necessary for the application’s operation
  - 4 flags determined to be non-issues
  - 2 flags addressed/corrected by developers
  - 64 flags unaddressed
Pilot Testing Takeaways

• Many false positives
  • In part, due to the nature of app testing.
  • Occasionally there was a finding which was found statically in code, but never used in the execution of the application. Typically we report this as a risk, but for this effort it became apparent that these findings were of little value. This is due mainly to the fact that each version of the application will be scanned and any previously unused code that is now invoked will be identified.

• Even “automated” testing requires a judgement call
  • Reasonable minds can differ on what constitutes a “critical” flaw.
  • Someone has to decide if a potential issue is an actual issue.
What is a “secure” app?
AppComm: www.appcomm.org

