PSCR

Mobile Data & Application Isolation

Joshua Franklin – IT Security Specialist

This work is sponsored by:

FirstNet™

FirstNet
(First Responder Network Authority)

PSCR

This work is sponsored by:

National Institute of Standards and Technology

PSCR

Disclaimer

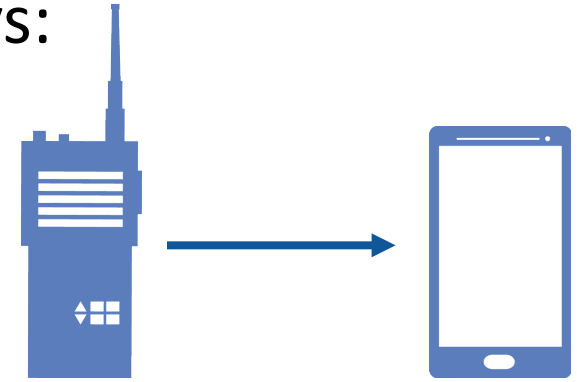
Please note, all information and data presented is preliminary/in-progress and subject to change.

Introduction

- The NPSBN enables first responder use of modern mobile devices
- Mobile devices erode traditional network boundaries and increase threat surface by adding new points of compromise
- The data and applications residing on public safety mobile devices need to be secured against modern threats
- Protection mechanisms, such as isolating commercial applications from mission critical ones, need to be identified and validated
  - This enables Bring Your Own Device scenarios for first responders

Mobile Data & Application Isolation

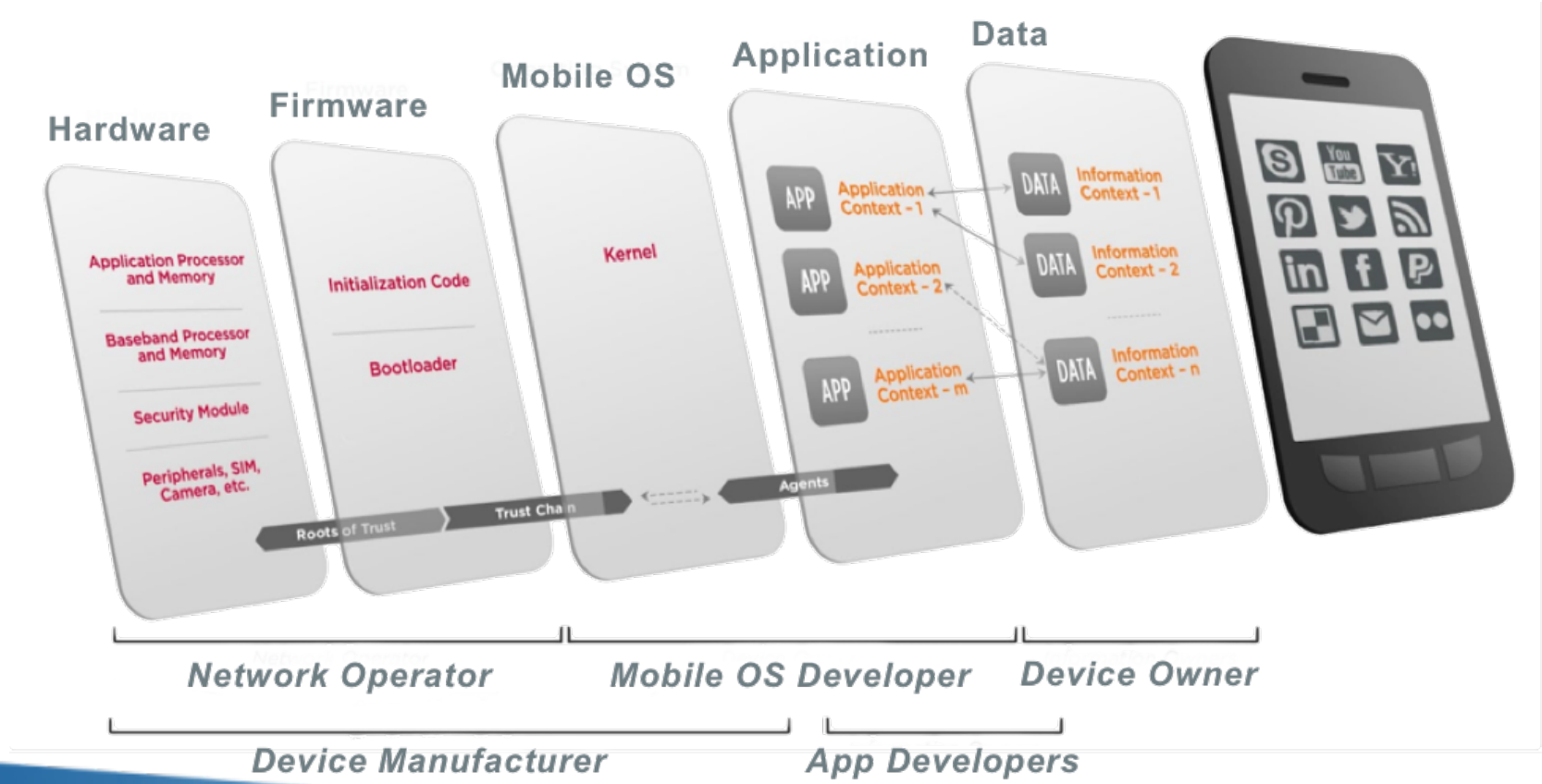
- The *Mobile Data & Application Isolation* project explores methods to manage and isolate applications/data for deployment on the NPSBN
- Devices and data can be compromised in many ways:
  - lost or stolen devices
  - network eavesdropping
  - Insecure network interfaces (e.g., WiFi, cellular)
  - device and user tracking
  - mobile malware



- This leaves sensitive public safety information at risk
- Need to protect the hardware, operating system, applications, and data to protect public safety information

Mobile Protection Mechanisms

Devices and data can be compromised
at various layers of the mobile security stack



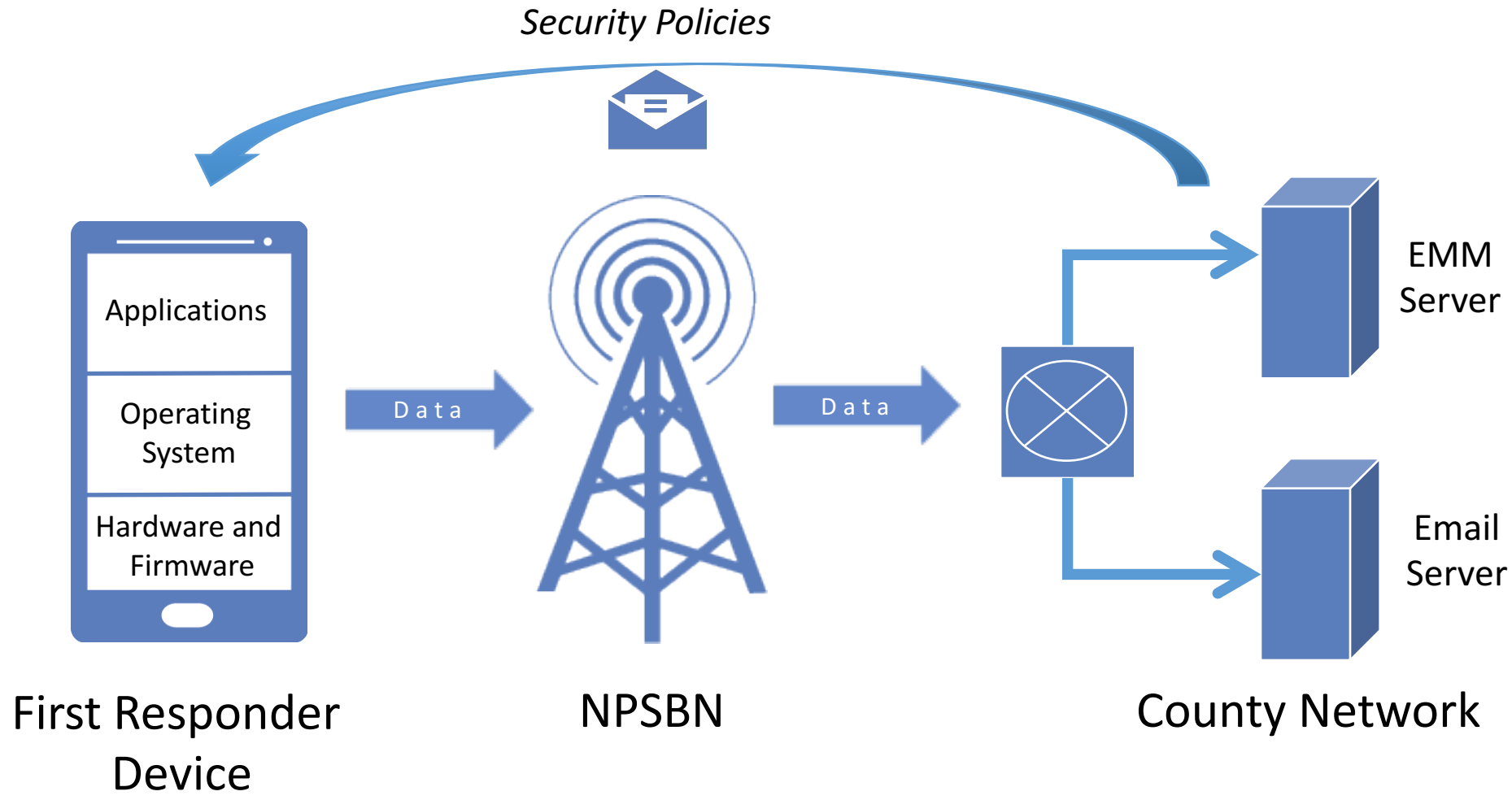
Example Use Cases

- Entering and exiting neighboring jurisdictions
- Securing evidence and other incident data on-device
- Device loss and theft
- Protecting wireless data transmissions
- Volunteers needing to access public safety services
- Bring Your Own Device scenarios
- Notifying user of malicious code on a device

Enterprise Mobility Management

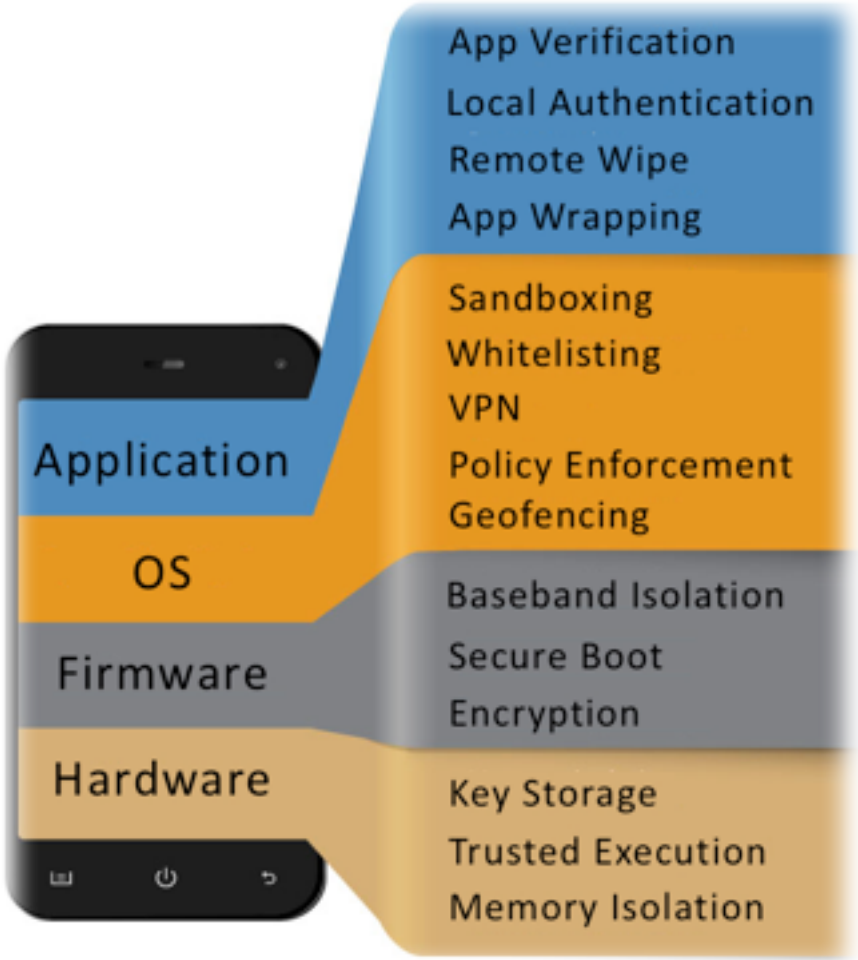
- EMM: Standard method to deploy mobile devices in an enterprise
- MDM: Defines and delivers policies to mobile devices
- EMM applications (or agents) reside on the device
  - Help to enforce policies
- Example policies:
  - Lockscreen security
  - Enable VPN
  - Device encryption
  - Root / jailbreak detection
  - Application whitelisting / blacklisting

EMMs in Action



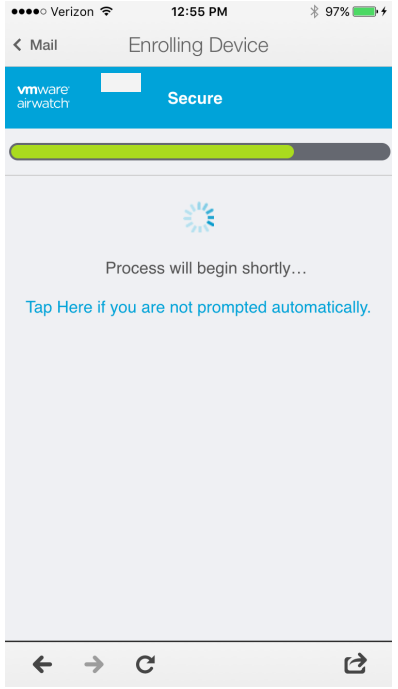
Current Research Efforts

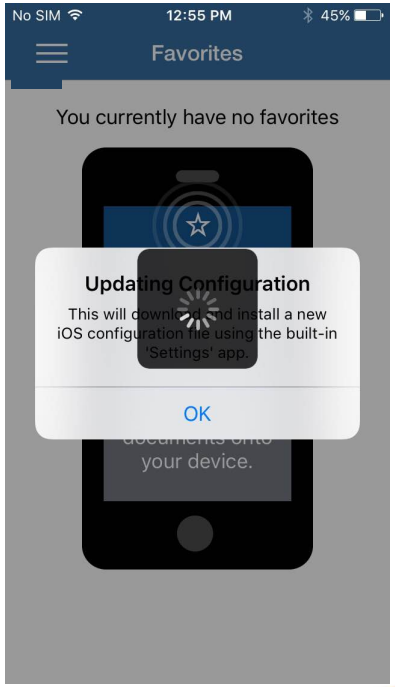
- Completed Research
  - Identified mobile security characteristics
  - Identified relevant mobile security products
  - Understand the degree to which industry products implement mobile security characteristics
- Need to understand gaps in commercially available technologies and what public safety needs
- *Testing is underway*



Preliminary Results

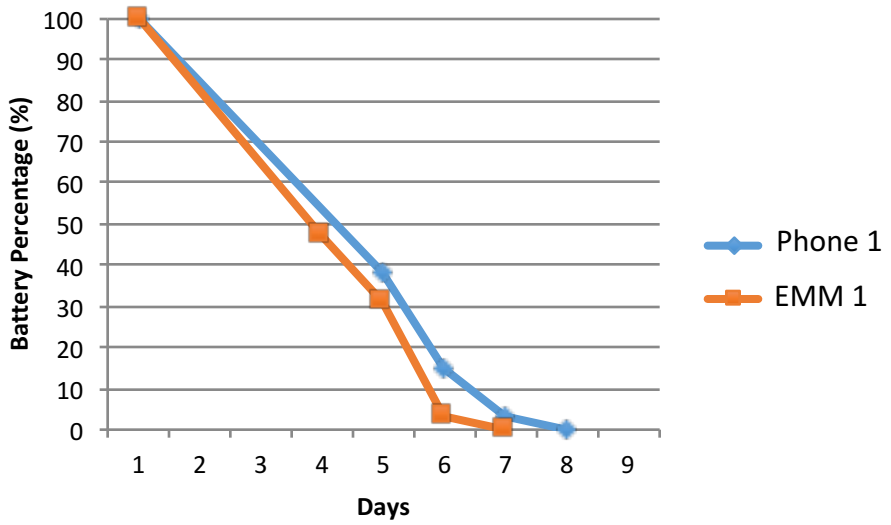
- Since testing is underway, preliminary results are arising
- Interesting results surrounding the following topics:
  - Multiple isolation technologies on a single device (Co-management)
  - Whitelisting and blacklisting
  - Encryption standards
  - Battery consumption statistics
- Capabilities vary widely from EMM to EMM

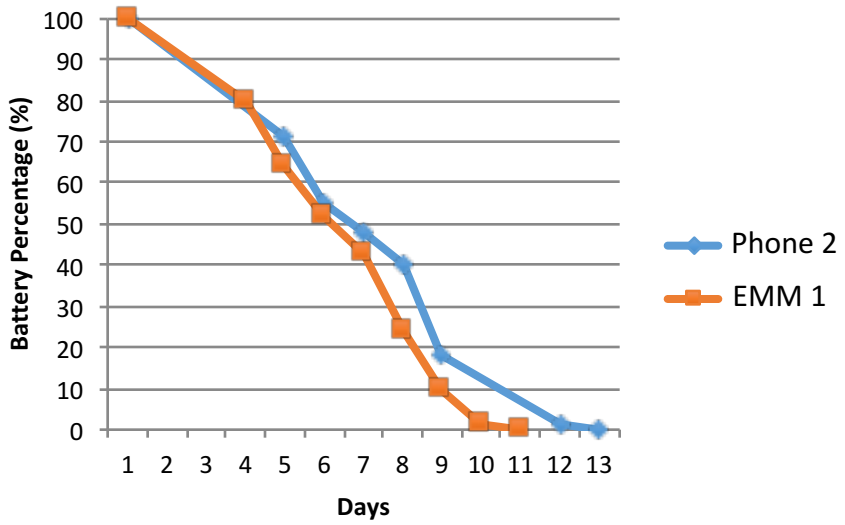




Impact on Battery Life

- EMMs may have an adverse impact on battery life
- We're collecting data to understand the degree of impact
  - Need to identify which functions consume the most power





Conclusion

- First responders need tools and support to accomplish their mission
- Compromised data and devices may allow attackers to access the cellular network infrastructure and other critical resources
- Research efforts currently underway – complete in ~ 3 months
  - Phase 2 of our research is under development
- This research will ensure public safety has the right tools in place to:
  - protect real-time communication,
  - secure access to data and services, and
  - operate in a modern threat environment.

Thank you!

Questions?

PSCR