Mobile Security

Stephen M Dye

2 March 2015

The Need for Security

- Both BYOD and GFE devices will be used
- Both manage sensitive respondent data e.g. Title 13
- Citizens need to be confident their privacy is secure
- Auditors, oversight bodies and Congress confidence
- Protect investment in GFE and BYOD

Mobile Device Security Challenges

- Becoming FISMA Compliant
- No mandated policy for mobility standards in Federal Government
- Applying current standards
- Further developing standards for statistical agency use

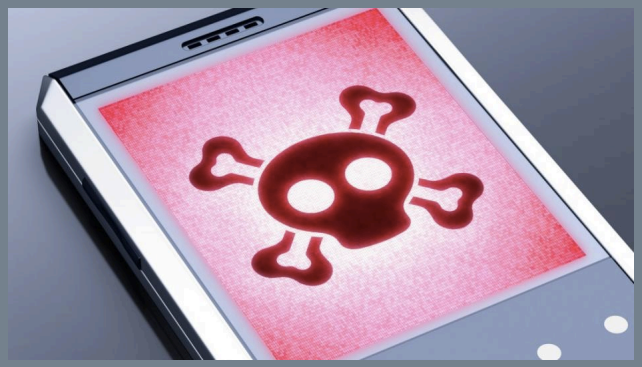
Mobile Device Security Challenges

- **Protecting data on phones**
  Data spill, exfiltration, device theft
- **Secure network access**
  Wi-Fi vulnerabilities, attacks
- Controlling a phone and apps
  Open to multiple attack vectors
- User authentication
  Secure access, illicit lockout
- **Malicious apps**
  Threats and risks to device & data

Mobile Device Security Challenges

- What Malicious apps can do
- Compromise the phone
- Run up Bills
- Read stored data
- Copy private information

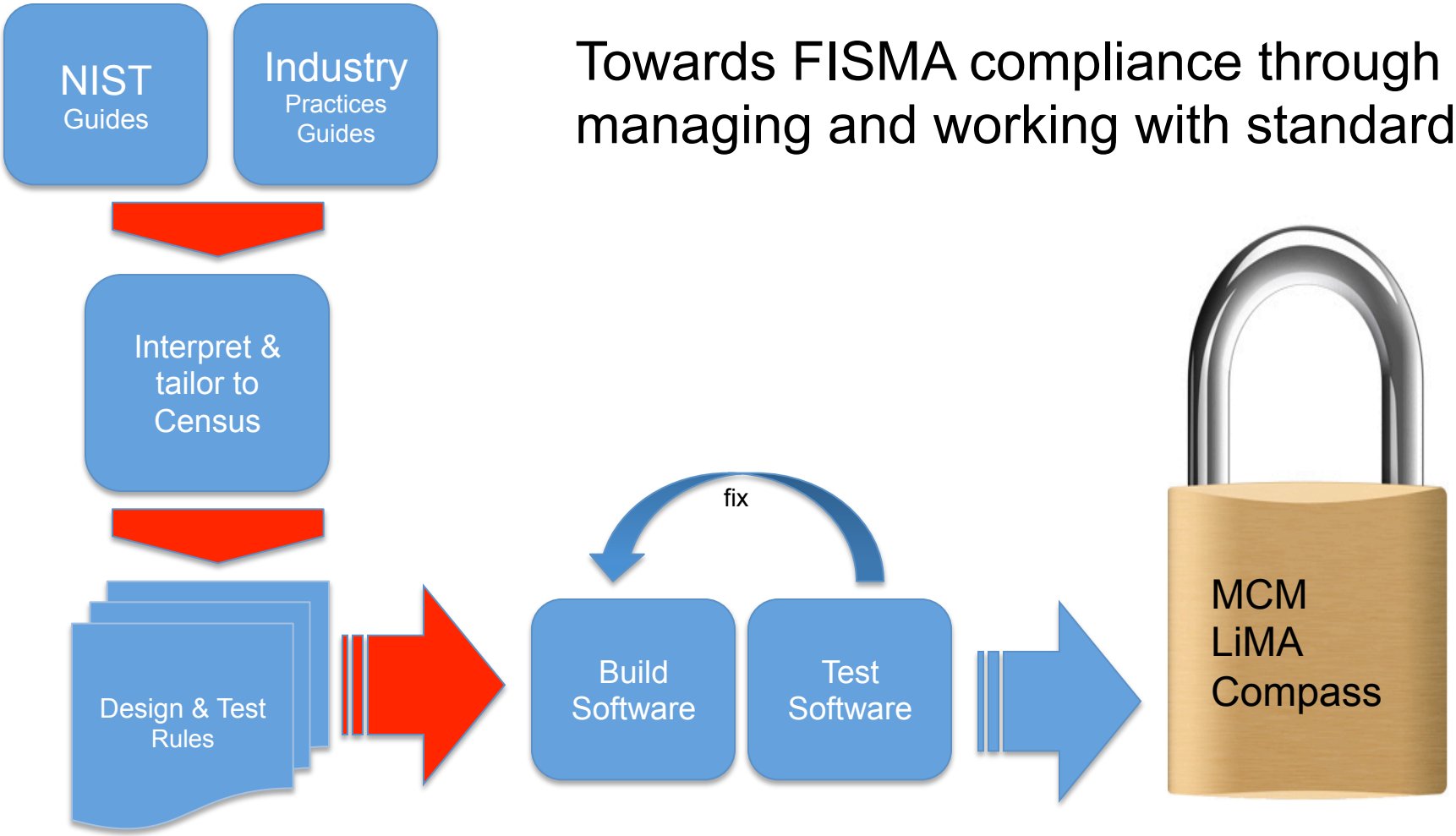
- Most Malicious apps are Android
- Exhaust battery, slow device down
- Subscribe user to premium services
- Modify or send to other locations
- Third party keyboards



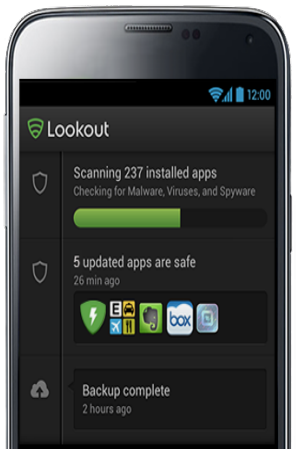
Implementing Security- innovations in the market

- Mobile Security Frameworks
- Real-time threat monitoring services
- Mobile security products used by Finance and Healthcare
- App usage, reliability & general operational health monitoring

Innovation- securing Census Apps at creation



Real-time mobile threat monitoring

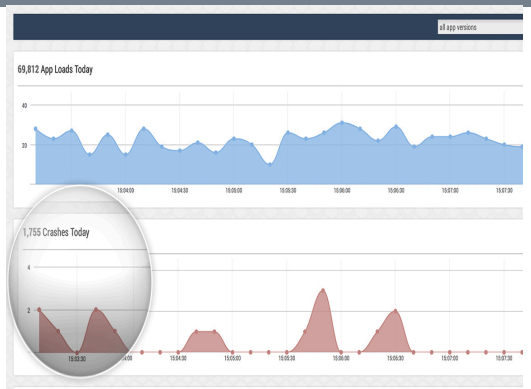


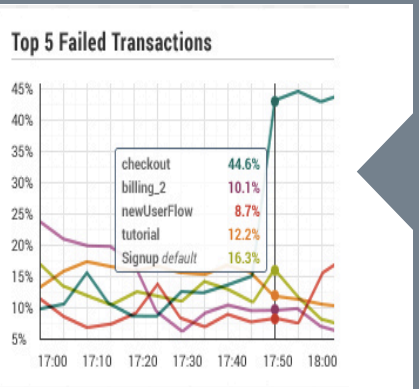
- Manage BYOD Risk & Vulnerability
- Automate Enterprise App Approval
- Vet every app on all devices
- Research Threats in Real-Time
- Discover anomalous mobile threats
- See apps accessing private data

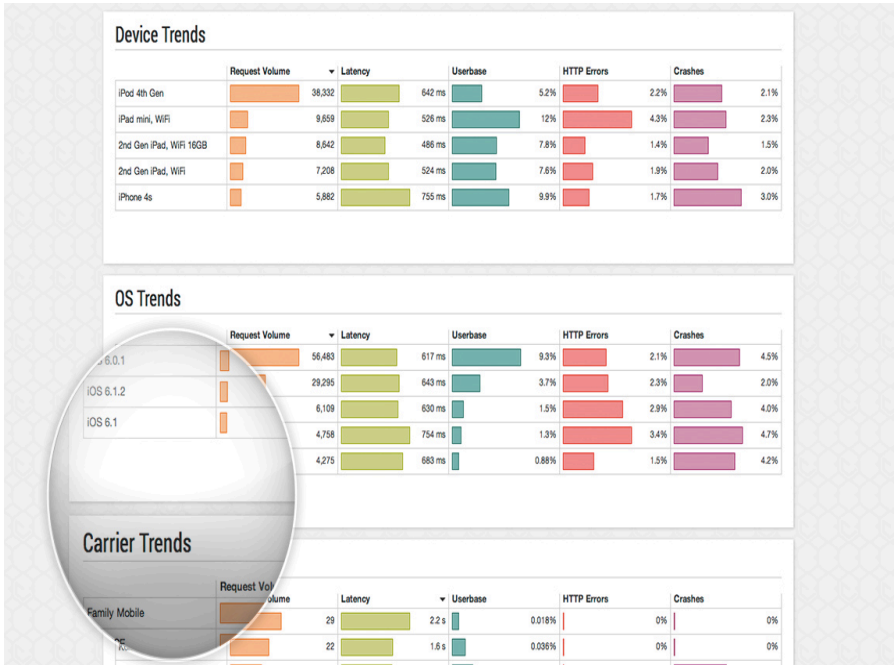
Mobile Device and Mobile Application Management

- MDMs manage devices:
  - Control entire phone
  - Set policies across entire phone
  - Black and white list apps, app stores
  - Entire phone can be wiped
- MAMs literally manage apps:
  - Corporate / enterprise apps
  - Secures data created by apps
  - Remote wipe: enterprise data only
  - Leave personal items alone
  - If authentication is required
  - whether data is stored on device
  - Control GPS, Cutting & Pasting etc.

App usage, reliability & monitoring







- Dashboards & Reports Notifications
- Availability, Performance Monitoring
- User action scrutiny
- Transaction execution monitoring
- Crash and Error reporting

In summary

- Security is paramount for mobile operations
- Security is also mission assurance; not just data
- Many challenges in implementing mobile security
- Innovation in the market place addresses concerns

Stephen M Dye
email: stephen.dye@agilex.com
703-585-9399