Daniel Bender

VERACODE

Solution Architect

Application Centric Mobile Application Security Model

Mobile Application Program Constraints:

1) Enabling the program within budget realities

2) Limitations of current counter-measures (including configuration/device management)

3) Best solutions often involve multiple services/processes (complementary)

    a) Defense in depth principles apply (independence & layering)

    b) Deep analysis (forensic approach)

4) Analysis time & limited information sharing

Definition of Malicious:

1) Varies depending on perspective:

    a) Software with malicious intent

    b) Software as a form of barter (privacy traded for functionality)?

2) Classifications and taxonomies (e.g., MAEC)

3) Complexity is evolving beyond a single file

    a) multi-stage (dynamically loaded) malware

    b) application collusion

BYOD and BYOA situations present risk to an organization

1) Difficult to quantify

    a) Mobile application inventory (easy to compile)

    b) Fit for use, valid business apps

    c) Impact of BYOA (personal apps)

2) Difficult to mitigate

    a) "Thought Police” – who determines, what is the criteria, how to enforce, etc.

    b) Technical limitations (prevent install, delete, warn, restrict access, or wipe)

Mitigation Options (aside from accept the risk)

1) Evolving threats require different approaches to analyze and mitigate risk

    a) Multi-solution approach required *(*sta*tic, dynamic, behavioral, etc.)*

    b) Multiple solutions require strong analytics (e.g., machine learning)

    c) Determine fit for use, privacy impact, vulnerability assessment, etc.

2) Application wrapping, sandboxing, and code level remediation

    a) But should we? (reject application, analyze further, or accept risk)

    b) Scalability, volatility, and impact to application

Before we go any further…

- Mobile Security Policy
  - Applications
  - Device Configuration
  - Mobile Device Management
- Acceptable use policy
  - Does it address mobile devices and applications?
- Consult with Legal and Human Resources
  - Emerging case law and opinions that could influence decisions
- User training and awareness
  - Transparency
  - Access to same resources and information that organization has
  - Loss of personal data impact

References (partial list of Federal):

1) NIAP Protection Profile (App on OS; in development)

2) NIST SP 800-124, SP 800-163 (Draft), & NIST App Vetting Workflow

3) DISA Mobile SRG

4) DISA STIG (APPSEC)

5) DHS CarWash

6) NSA Center for Assured Software (CAS) & CyberCom

7) Software & Supply Chain Assurance Forum (https://buildsecurityin.us-cert.gov/swa/)

References (partial list of Academic):

1) Advanced Mobility Academic Research Center (AMARC)

a) Academic community is an untapped research resource

b) Developing better prepared graduates for hire

2) Automatic Malware Analysis, an Emulator Based Approach
(Yin & Song, 2013)

3) Data Mining and Machine Learning in Cybersecurity (Dua & Du, 2011)

The Mobile Mindset/Moment

- Defined in Schadler, Bernoff, & Ask's (Forrester Research) book: The Mobile Mind Shift
- "...expectation that I can get what I want in my immediate context and moment of need"
- Mobile Moment is characterized by:
  - Point in time and space when someone pulls out a mobile device to get what he/she wants immediately, in context and location
  - These moments can be built, borrowed, or shared
- Capture the mobile moment:
  - Re-engineering platforms and business process
  - New engagement technologies, cloud-based integration & delivery, data delivery, and comprehensive analytics
  - Heavy use of APIs to piece together social networks, collaboration, maps, and other services

Mobile Mindset/Moment Applied

- Evident in mobile applications emphasizing convenience
  - Can the mobile application predict what you need by what it knows about you and where you are?
  - Users have to trust the organization/entity with their data
  - Privacy Policy
  - Transparency

- Part of business transformation
  - Businesses recognizing that mobile apps are a better fit for “mobile” or active employees
  - Break down business processes to determine whether the employees have mobile moments
  - Simplify transactions and anticipate what employees need based on context and location (discrete tasks)
  - Also characterized by heavy data collection and analysis
  - What works? What is being used?, etc.
  - Eliminate keystrokes and non-value add activities

The Mobile Mindset/Moment vs. Security/Privacy

- Security & Privacy gets mentioned in a paragraph (“bugaboo of mobile interactions”)
- Convenience of mobile apps and trust regarding an individual’s data
- Difficult equilibrium to achieve:
  - Numerous case studies in the book support massive data collection and analysis
  - How, when, why, & where people use the application and data
  - Predictive analysis of what the user wants or may be interested in at the mobile moment
  - Trade-offs: privacy, trust, and benefits
  - Reconciling data collection to privacy policy
  - Do the developers know what data is being collected or how it is used?
- Mindset/Moment is about selling and capturing dollars on the table
  - If you do not, your competitors will (think Uber & Lyft vs. taxis)

Approaches Observed for App Stores & MDM (BYOD/A):

1) Do nothing or implement ad hoc blacklist

2) Implement a risk based approach based on a mobile app reputation service[1,2]

3) Develop & implement mobile application centric security policy (MDM enforce)[1]

4) Deep application vetting (e.g., forensic approach)[1]

[1] MDM typically selected first, then realization that approach does not scale (well)
[2] Default option selected when no mandate for stricter security

Case Study - Government Agency (mobile app reputation service)

1) MDM selected and mobile security program in place

2) iOS device count 5,000-10,000; Android device count 5,000 - 10,000

3) Initial application counts:

    a) Android: 9,000 - 11,000

    b) iOS: 7,000 - 10,000

4) 63,891 applications analyzed (malicious: 1,503; suspicious: 224)

5) Noted approximately 4-5% of applications categorized as malicious

Case Study – Commercial Manufacturing Client (mobile app reputation service)

1) MDM selected and mobile security program in place

2) iOS device count 10,000; Android device count 5,000

3) Initial application counts:

    a) iOS: 35,000

    b) Android: 3,600

4) Selected ~3,000 Android applications for testing; ~36,000 apps/versions tested

5) 3-4% of tested applications considered malicious

Shift to Mobile Application Attribute Based Security Policy

1) Leverage automation to assess applications

    - Process for handling exceptions or additional analysis

2) Integrate results into MDM and GRC (Reporting) systems

    - Metrics: Mobile device restores, device audit statistics, etc.

3) This approach can be applied to application store models

    a) Accelerate application vetting process

    b) Demonstrate compliance with STIG/SRG/Guide

Feature Vectors Available for Analysis

ESTABLISH FINE-GRAINED POLICIES TO PROTECT SENSITIVE DATA

Meta Data

- Application File Name
- Application Version
- Application Minimum SDK
- Application Target SDK
- Date Analyzed
- Account Name
- Source IP Address
- Package Name
- Request ID
- Request Date and Time
- APK MD5
- Application Size
- Package File Contents

File Activity

- Files Modified
- Files Deleted
- File Created

GUI

- Screenshots of application activities
- UI Elements Including Labels
- Number of Activities
- Name of Activities

Network Traffic

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- TCP / UDP
- Internet Connection By Country (Geolocation)
- Bytes Sent
- Bytes Received
- Packets Sent
- Packets Received
- Network Throughput
- HTTP URL Data
- Resolved DNS of Source / Destination Address
- Results of SNORT IDS Scans
- Custom SNORT Rules

Binary Analysis Data

- Basic Block Data
- Intent Data
- Full List of Classes
- String Constants

Risk Ratings

- Results of over 40 AV Scanners
- Veracode Machine Learning Risk Rating

Additional Logs

- System Event Logs
- Activity Event Logs
- GUI Logs
- Operating System Call Logs by Time

Behavioral Data (Red Flags)

- Privacy Impacting Behaviors
- Saftey Impacting Behaviors
- Network Impacting Behaviors
- Identity Impacting Behaviors
- File Impacting Behaviors
- Dangerous Behaviors
- Location Impacting Behaviors
- Total Activiated Behavior Count

Services and Permissions

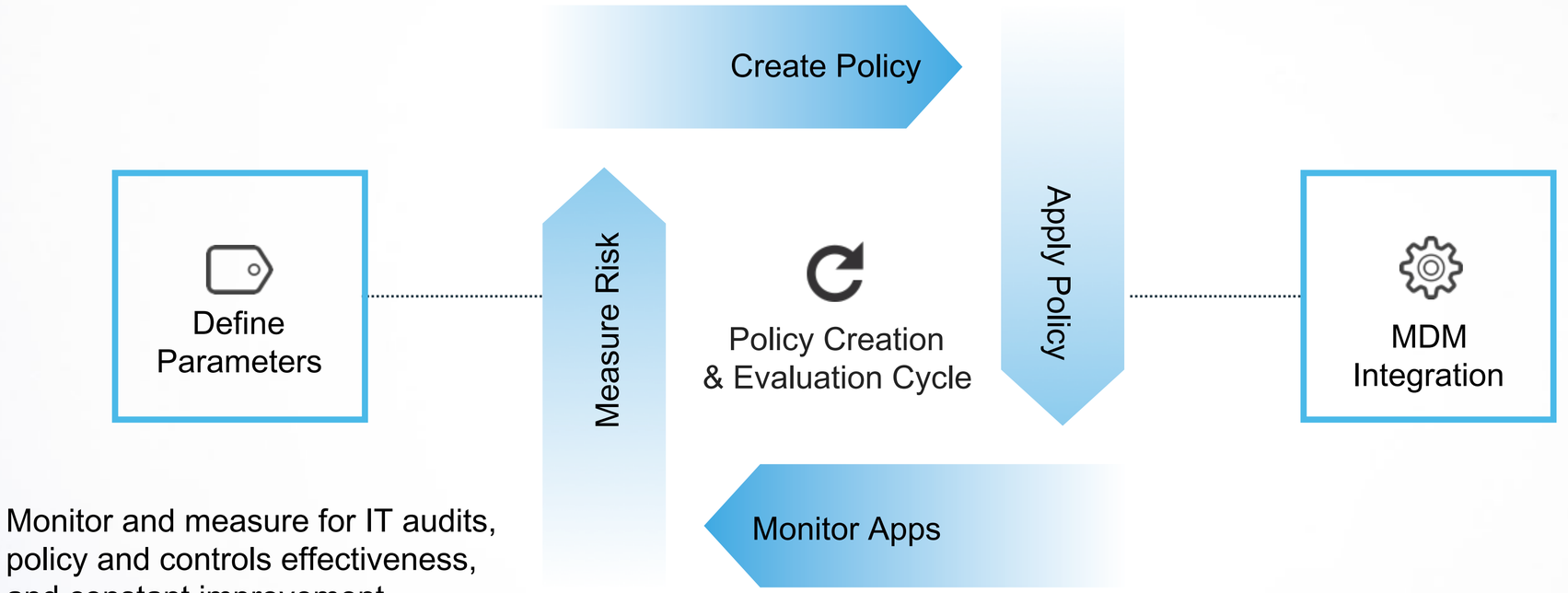
- Services and Listeners Enabled
- Application Manifest
- Application Required Permissions

System Resources

- Physical Memory Impact
- Virtual Memory Impact
- CPU Utilization

CUSTOM MOBILE APP SECURITY POLICIES

Strategic, Comprehensive, and Policy-Driven Approach



Monitor and measure for IT audits, policy and controls effectiveness, and constant improvement.

Processes complement each other to create a mobile app security lifecycle that can adapt business, IT and security requirements change.

CUSTOM MOBILE APP SECURITY POLICIES

Sample Business Policy to Prohibit Apps that Access Sensitive Data

Sensitive unencrypted network data

Sensitive unencrypted SQLite data

Sensitive unencrypted filesystem data

APPLY POLICY TO PROHIBIT APPS

- ☑ Direct HTTP Access
- ☑ Direct Socket Access
- ☑ Uses SQLITE
- ☑ Examine Filesystem
- ☑ Read Files

Define Security Policy

1) Define acceptable/unacceptable behaviors

    a) code inspection elements (e.g., privacy impacting)
    b) permissions
    c) network connections

2) Evaluate policy against mobile application population

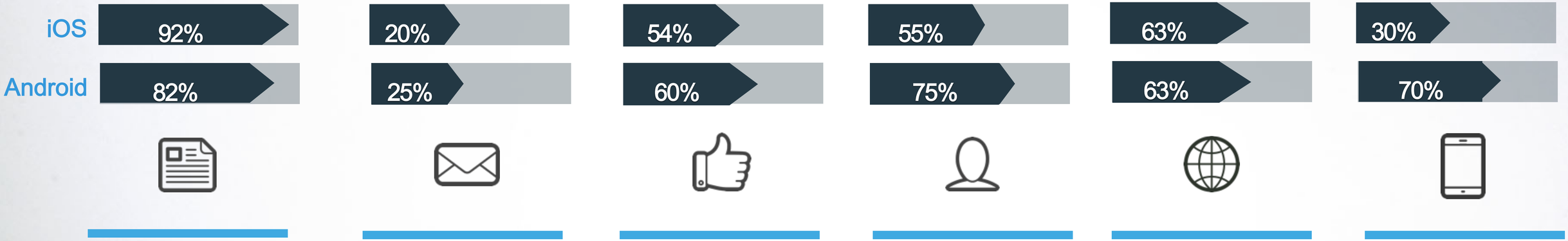
3) Develop exception process

4) Automate assessment and policy enforcement (MDM)

5) Revise and repeat

CUSTOM MOBILE APP SECURITY POLICIES

Sensitive Data by Organization or Role



FILES

- ☑ Read Files
- ☑ Access Cloud Resources
- ☑ USB Usage
- ☑ Examine File System
- ☑ Retrieve Browser History
- ☑ Access Cookies
- ☑ Access to Bookmarks

CORRESPONDENCE

- ☑ Read SMS Messages
- ☑ Send, Receive, Prepare SMS
- ☑ Consume SMS Messages
- ☑ Access Call Log
- ☑ Record Phone Calls
- ☑ Monitor Phone Calls

CONTACTS

- ☑ Read Contacts
- ☑ Write Contacts
- ☑ Edit Contacts
- ☑ Track Address Book
- ☑ Bulk Access Contacts
- ☑ Access Facebook Audience

IDENTITY

- ☑ Examine Android Account
- ☑ Access Unique Device ID
- ☑ Retrieve SIM Card Info
- ☑ Access Social Networks
- ☑ Access Facebook
- ☑ Access Twitter
- ☑ Access Accounts

LOCATION

- ☑ Monitor Location
- ☑ Uses Geocoding

DEVICE

- ☑ Root Device
- ☑ Listen for Key Presses
- ☑ Monitor Phone Activity
- ☑ Monitor Camera Interface
- ☑ Capable of Recording Audio
- ☑ Access System Logs
- ☑ Retrieve List of Running Apps
- ☑ Access to Shared Library
- ☑ Access to Default Preferences

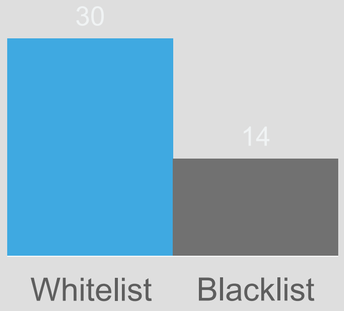
CUSTOM MOBILE APP SECURITY POLICIES

Access to Sensitive Data with use of Unencrypted Network Data

ANDROID

- ☑ HTTP Download
- ☑ HTTP Upload

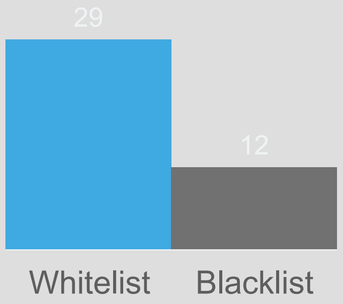
- ☑ Read SMS
- ☑ Install Applications
- ☑ Record Phone Calls
- ☑ Check if Device is Rooted
- ☑ USB Usage
- ☑ Access System Logs
- ☑ Retrieve Browser History
- ☑ Retrieve List of Services



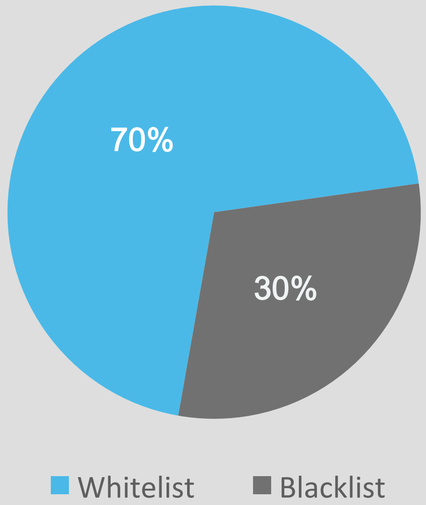
iOS

- ☑ Direct HTTP Access
- ☑ Direct Socket Access

- ☑ Access Cloud Resources
- ☑ Read Clipboard
- ☑ Access Global Clipboard
- ☑ Monitor Phone Calls
- ☑ Monitor Device Location
- ☑ Uses Geocoding
- ☑ Access Accounts
- ☑ Runs Other Programs
- ☑ Access to Bookmarks



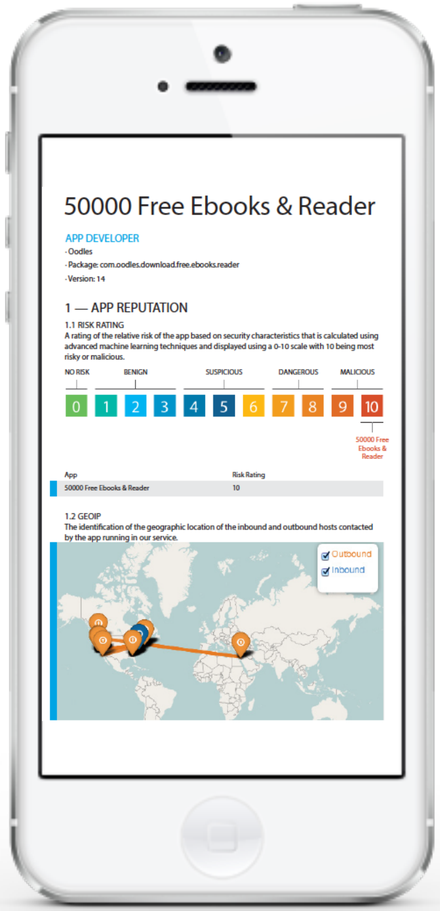
APPS

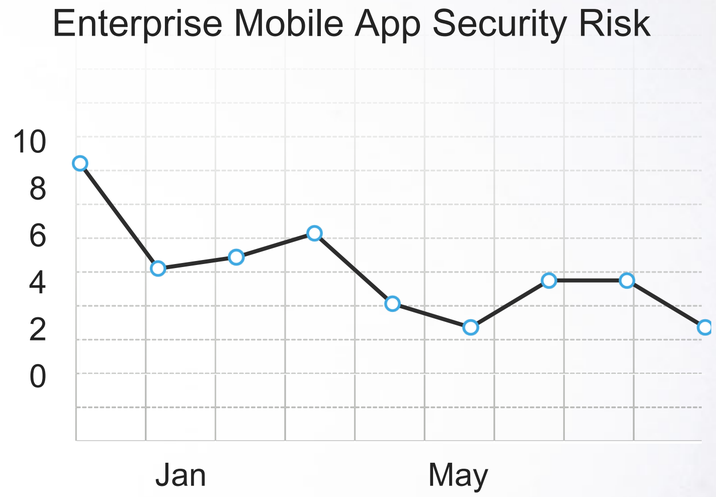


CUSTOM MOBILE APP SECURITY POLICIES

Protect Sensitive Data

- **Files:** Prohibit apps that access sensitive files
- **Correspondence:** Prohibit apps that access correspondence
- **Contacts:** Prohibit apps that access contacts
- **Location:** Prohibit apps that access location
- **Identity:** Prohibit apps that access identity
- **Ad Tracking:** Prohibit apps that perform ad tracking





Apps Prohibited	Apps Allowed
22%	78%

Future Direction?

Integrate security findings based on richer data set:

- RISK FACTOR-ENABLING AND OR LOADING JAVASCRIPT ON WEBVIEWS
- RISK FACTOR-INTERACTING WITH JAVASCRIPT WEBVIEWS
- RISK FACTOR-PERIPHERAL SIDE LOADING INJECTION OF JAVA CLASSES ROOTSTRAPING
- RISK FACTOR-POSSIBILITY OF PERIPHERAL SIDE LOADING OF JAVA CLASSES
- RISK FACTOR-RELYING ON SOMEWHAT DENSE USE OF STRINGS
- RISK FACTOR-RELY ON TIME DELAY STRUCTURE POSSIBLY ASSOCIATED WITH NETWORK SMS INTERACTION
- RISK FACTOR-RETRIEVE SENSITIVE INFORMATION ABOUT YOUR NETWORK PROVIDER
- SAFETY FACTOR-FINE GRAINED MANAGEMENT OF LIFECYCLE OF ITS
- YOUR FILES-EXFILTRATE VIA DELETION ON FILESYSTEM
- YOUR FILES-ACCESS TO YOUR SD CARD
- YOUR FILES-INQUISITIVE ABOUT DOWNLOAD CACHE DIRECTORY CONTENTS
- YOUR FILES-INQUISITIVE ABOUT SD CARD DIRECTORY CONTENTS
- YOUR IDENTITY-RETRIEVE INFORMATION ABOUT YOUR DEVICE TYPE
- PRIVACY-ACCESS AD SERVICE ADMOB COM
- YOUR PRIVACY-ACCESS AD SERVICE MDOTM COM
- YOUR SMS-RECEIVE SMS MESSAGES

Questions?

Contact me at: dbender@veracode.com