SECURING BYOD: MITIGATING RISK, NOT FORCING CONTROL!

Giri Sreenivas (@giri_sreenivas)
RAPID7
Overview

► Cred
► Data
► Top Threats and Examples
► Designing for Security
► A Risk Management Approach
Cred

- 1st mobile app stores, mobile JVMs, OHA + Android
- Security projects for US government orgs
- Software engineer to startup founder/CEO
- Now VP/GM Mobile @ Rapid7
Data - Q2 Global Mobile OS Share

1. Android 79%
2. iOS 13%
3. Other 8%
Data - Blind About BYOD

- 64% Allow BYOD
- 50% Do Not Know Extent Of Mobile Device Usage
- 40% Do Not Secure BYOD
Data - Policy Insecurity

- No Security: 38
- No Password: 54
- No Patching: 66
WHY NOW?
Instinctive When Overwhelmed

- BYOD has happened fast and most orgs are reeling
- Instinctive response is to replicate IT asset management and security practices for BYOD
- Blackberry-like approach to personal mobile devices and containers creates UX challenges and user rejection
- May not make your organization any more secure as users will attempt to work around your controls
TOP 7 MOBILE THREATS
Lost/Stolen Phones / Terminations
Lost/Stolen Phones / Terminations

- 35% of phones are lost or stolen
- Phones are replaced ~18 months
- More than 50% of employees kept confidential data upon termination, 40% will use it at their new job
- Improper termination is an overlooked vulnerability

- Mitigate with PIN/remote wipe policies and patching
Jailbroken and Rooted Devices
Jailbroken and Rooted Devices

► 5% of iOS devices are jailbroken
► Similar percentage of Android devices are rooted
► Typically intentionally compromised by end users
  ► Tethering / SIM Unlocking
  ► Customization / Removing Bloatware / Upgrade OS
  ► Evading security policies like PINs

► Mitigate with jailbreak detection and patching
Trojans and Malware
Trojans and Malware

- Well controlled in iOS App Store
- Room for improvement in Google Play
- FDA vs. CDC models
- 3rd party app stores remain high risk
  - Chinese 1+M phone botnets
- AV solutions limited to awareness, unable to protect

- Mitigate with app risk management and patching
User Behavior

Critical System Error

User competence level does not meet the required specification.
User Behavior

➤ BYOA – Bring Your Own Apps
➤ BYOD devices average ~50 ad hoc applications
➤ Evernote, Dropbox, Mailbox, etc.
➤ Unintentional leakage of data

➤ Mitigate with app risk management and user training
Promiscuous Apps

Application info
Permissions
This application can access the following on your phone:

- **Your messages**
  Send and receive Google Talk instant messages

- **Network communication**
  Full Internet access

- **Your accounts**
  Android services, Google Checkout accounts, Google Checkout Sandbox accounts, manage the accounts, Google Checkout accounts, manage the accounts, use the authentication credentials of an account

- **Phone calls**
Promiscuous Apps

- Apps accessing corporate data, frequently unbeknownst to the user
- Recent versions of LinkedIn, Path, Evernote
- Pending legislation may drive better awareness through disclosure requirements

- Mitigate with app risk management
Phishing
Phishing

► Personal email address and mobile number are new vectors
► Limited screen sizes inhibit browser security
► More than 4000 sites are dedicated to mobile phishing

► Mitigate with user education
Man In The Middle Attacks
Man In The Middle Attacks

- Mobile data costs and wifi-only tablets drive insecure access
- Difficult to determine compromised communications

- Mitigate with per app VPN connections
THREAT AND VULNERABILITY EXAMPLES
It All Started With A Dream

- Malware exploiting vulnerabilities
  - DroidDream (2009)
    - Embedded in 60+ apps/games in Google Play
    - Arbitrary privilege escalation, ad hoc C&C payload download
  - Obad (2013)
    - SMS Phishing, embedded in Google Play fake apps
    - Leveraged 0-day to keep DeviceAdministrator privileges
Browser and File-based Attacks

► Webkit attack (2007-10) – [http://jailbreakme.com](http://jailbreakme.com) and AppSnapp
  ► Jailbreak an iOS device simply by visiting a website

► PDF attack (2011) – Click-to-pwn scenario
  ► Jailbreak an iOS device by opening a malformed PDF
Android OEM Customizations

- HTC
  - Unauthorized permissions
- LG
  - Sprite Backup
- Samsung
  - TouchWiz / Dialer
- Motorola
  - TrustZone vulnerability unlock
Platform Weaknesses

► Android Master Key Vulnerability (2013)
  ► Modify legitimate APKs with trojans and bypass crypto signature check

► iOS Lockscreen Bypasses (2007 – present)
  ► Varying levels of access to the entire device, contacts, photos, dialer without entering policy-mandated PIN
Intermediate Recap

- BYOD is pervasive
- Many orgs just getting started on securing BYOD
- Most IT/security teams fly blind
- Top 7 threats are real and growing
- Challenges with control-based approaches to secure against threats
WHAT NOW?
Inheriting Control-based Approaches

► Instinctively treat personally-owned devices like company assets

► Control is at odds with UX for most end users
  ▶ Users abandoned Blackberry for UX
  ▶ Leverage UX focus and make it easy for users to be secure
Clean Slate Approach

► Design it (Don’t inherit it)
  ► BYOD is not for every organization
  ► Involve your employees
  ► Make it too hard for the end user and they will work around you, exposing your organization to even more risks
  ► There may not be an alternative given Blackberry’s troubles
MANAGE THE RISK
A Risk Management Approach

► Define tolerable risk and acceptable use
► Get real visibility and balance with employee privacy
► Assess the risks and prioritize remediation / mitigation
► Act
► Rinse and repeat
Tolerable Risk and Acceptable Use

► Differentiate between corporate issue and personally owned if appropriate
► Define what data can be wiped in specific situations
► Engage and communicate with employees
  ▶ Their acceptance is equally important
► At a minimum, implement basic native security policies
  ▶ Passwords, encryption, VPN configuration
Getting Visibility

► 50% of organizations know about BYOD, but not the extent of it
► Classic example: financial services organization
  ► Estimated: 15% BYOD penetration, minimal Android usage
  ► Actual: 85% BYOD penetration, 20x more Android devices
► Realtime visibility into all mobile usage is essential
Assess Risks / Prioritize Action

► Analyze devices for vulnerability exposure, risky behaviors
► Review high severity vulns for business risk
► Identify unpatched devices whose vulnerability exposure can be reduced or eliminated with an update
Act

► Inform users, reiterate policies
  ► Provide a window for patching, along with specific details
  ► Suggest recommended applications over riskier alternatives
  ► Aggressive: block user access
  ► Balanced: hand hold users through upgrade process
Importance of Mobile Patching

- 75% iOS devices outdated
- > 60% Devices with a high severity vulnerability
- 94% Devices with high severity vulnerabilities that can be mitigated with a patch
Recap

► BYOD is pervasive, but not for every org
► Most organizations are in the dark about BYOD and risks
► Top 7 threats are real and growing
► Design for risk management, don’t inherit approaches to control
► Patching is central to managing risk
Thank you!

Giri Sreenivas
VP/GM Mobile, Rapid7
@giri_sreenivas
Giri_Sreenivas@rapid7.com
http://rapid7.com