Protecting Mobile Devices

Aaron Grothe CISSP

Protecting the Organization from Mobile Devices

Michael Hoesing CIA, CISA, CISSP

IIA Regional Conference

Omaha Nebraska August 24, 2015

The Institute of Internal Auditors

Terms

- Root/Jailbreak
  - Modify your phone so you have full priveleges on it
- Unlock Bootloader
  - Allows you to load a different firmware on the phone if you choose. E.g. Cyanogenmod

Terms

Unknown Sources

Allowing your device to load files from places other than the Google Play Store, Apple App Store

Cyanogenmod

An alternative firmware for Android Phones is used by default on some phones as well

The Permissions Land Grab

- Spotify
  - Can collect the following
  - Contacts, Photos, Media Files
  - Location via GPS and Bluetooth
  - Voice Commands
  - Spotify provides additional information about how they will use this on their privacy policy page

Permissions Land Grab Continued

This is just one example

Spotify is a pretty well sorted application

They have provided some additional information about how they plan to use the data

Photo is to be used to customize your logo

Location to determine walking/running/etc

Permission Dog

App available from the Google Play Store

Provides an easy way to figure out the permissions that you are currently sharing on your device

Can be a bit scary to see how many privileges even the simplest app can require

Android Permissions

Quite simply are a mess

Apps used to ask you explicitly for every permission that the app would use

Google “simplified” this with Lollipop (5.0) to be only broken out by sections such as (location, Identity, In-app purchases, etc)

Permissions are almost Forever

Once you install an app pulling its privileges is very difficult.

There was an early build of 4.3 that allowed you to reduce privileges to an application via the sdk. Several apps were created that used that api, google then “fixed” it.

Privilege Creep

Privilege Creep is what happens when an app that you are happily using now wants additional features

An example of this is an app such as “Can Knockdown” - it begins to what to know what other applications are running and my location why (probably ads)

Fighting Back

Privacy Guard

Part of Cyanogenmod (an alternative firmware for Android)

Allows you much greater control of the permissions an app is allowed

Note: some apps don’t like being told “NO”

Fighting Back

Xprivacy is another application that allows you to control what information is sent out

It allows you to alter information

E.g. you can lie about your location, say you're in Forman North Dakota instead of Omaha, Nebraska

E.g. can also provide a random/fake DeviceID

XPrivacy

XPrivacy
- Requires a rooted phone
- Requires the xposed framework be installed
- XPrivacy App installed

Only works on some phones/setups

Phone may end up bricked during install

Fighting Back

Icognito Mode

Was planned as part of Cyanogenmod now a separate project

Allows you to run an app in an isolated environment with an empty contact list, no photos, other information to send home

Fighting Back

App Store Reviews

- Some people actually pay attention to these

Serious Sam Example

Original Version requested the following

- Ability to take screenshots of running apps
- SMS Access and a whole lot more
- Permissions fixed in next release

What about Apple

On Apple Idevices you can prevent an app from seeing your address book

Other than that you're relatively limited on permissions

There is are several apps that work on Jailbroken phones to give control similar to Xprivacy

ProtectMyPrivacy, Cydia Substrate

What about Virtualization?

Can’t we just virtualize devices into a work and personal side?

There are some products that do that

- Verizion Mobile Horizion
- Samsung Knox
- Blackberry Secure Workspace

Virtualization

Limited device support

Expensive

Still early even though VmWare did their initial Press Release about this back in 2008

Docker???

Docker is currently about the hottest thing for Servers right now

Docker is a container based system that puts an application and all its data into a container

Docker for Phones will allow you to segregate all work apps into a container which work will be able to control

Docker just started for Android so lot of work to be done

Takeaways

Give Permission Dog or something similar a look

People will got out of there way to install a popular app (such as flappy bird) - root/sideload/buy off ebay

Protecting the Organization from Mobile Devices - Agenda

- Risks MDM (mobile device management)
- Risks MAM (mobile application management)
- Controls
  - Mobile Policies/Standards
  - Software MDM
  - Software MAM
- Auditing MDM and MAM
- Example Software (Microsoft InTune)

Risks of Mobile Devices to the Organization

- Loss of Data
  - Via inappropriate connection
- Loss of the device
  - Intrinsic cost (if owned by the org, if not??)
  - First step in compromising data on the device
  - Potentially access the org's network
- Use of the device by unauthorized persons
  - Impersonation
  - Toll/data charges

Risks of Mobile Devices to the Organization

- Applications
  - Missing security software (AV)
  - Unauthorized Applications
    - Could introduce malware
    - Could enable inefficiency
    - Could generate costs
    - Could create IP/License exposure
  - Incorrect versions

Controls - Policy Considerations

- Beware: mix of corporate and personal ownership (device vs data) involve Legal, HR, Compliance
- Device Configuration Policy (Mobile Device Management {MDM})
  - Policy Type – Acknowledge, Warn, Enforce
  - Device/Screen Lock Password – Length, Complexity, Life, History, Max Attempts
  - Camera Allowed?
  - Encryption
- Approved (or required) Applications (Mobile Application Management {MAM})

Mobile Acceptable Use Policy Considerations

- Beware: mix of corporate and personal ownership (device vs data) involve Legal, HR, Compliance `
- Device Configuration Policy (Mobile Device Management {MDM})
  - Allowed equipment and operating systems
  - Policy Type – Acknowledge, Warn, Enforce
  - Screen Lock, Password – Length, Complexity, Life, History, Max Attempts
  - Camera Allowed?
  - Encryption (and many more)
- Approved (or required) Applications (Mobile Application Management {MAM})

Mobile Audit Program -General

- Obtain and evaluate all mobile policies/standards
- Collect documentation on the MDM/MAM software
- Examine configuration of MDM/MAM software alignment with your policies
- Review reports on non-compliance for blocking, or follow-up
- Review the process for acceptable policy variances
- What is the change management process for the MDM/MAM ruleset
- Is logical access to the software appropriate
- Match the user policy acceptance evidence to the device inventory

Mobile Audit Program – ISACA BYOD

- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-Computing-Security-Audit-Assurance-Program.aspx
- $45 non-member, free for members
- Things in the preceding General Program, plus:
  - **COBIT 5 soundbites - define engagement objectives, scope, stakeholders, alignment, benefits realization metrics, risk optimization, life cycle, manage security, monitoring and corrective action**

The Institute of Internal Auditors

Mobile Device Inventory

- Software will produce a listing of connecting devices
- However, many of those devices will not match the long lived assets inventory because the organization does not own the mobile device
- Try matching owners to employee HR records, non-employees should not be connecting their mobile devices

MDM/MAM Software Considerations

- Do the configuration setting align with your policy
- Can the variances be configured as detective (reported) or preventative (blocking)
- Is remediation automatic, or must be chosen
- Does the “wipe” remove non-organization apps and/or data (liability?)
- Reports available? (and data export)
- What notifications & options does the user have
- Limits on devices, OS’s, users

Example Software – Microsoft InTune

Microsoft InTune – Users & Groups

- Administrators – correct ones, trained, qualified
- Users – all have one or more authorized devices
- Groups can be a member of a group, deepest policy is applied

Microsoft InTune - Policies

- Configuration Policy – most all security settings are here
- Compliance Policy – the device must conform to this set of rules to be allowed access to connect with:
  - Exchange cloud
  - Exchange local
  - SharePoint

Microsoft InTune – Configuration Policies

- Password Security
  - Require a password to unlock device
  - Minimum password length
  - # of Sign-In failures before device is wiped (wiped = reset to factory, user installed apps and data are gone {liability} {evidence hold})
  - Screen lock at xx minutes inactivity
  - Password maximum life in days
  - Password history quantity
  - Password structure (biometric, alpha, numeric, both, special characters)

  (What is missing?)

Microsoft InTune – Configuration Policies (2)

- Encryption Security
  - Encrypt device storage
  - Encrypt additional card storage
- System Security
  - Allow screen capture
  - Allow diagnostic data submission
  - Allow factory reset {liability} {evidence hold}
- Cloud Security
  - Allow Google backup
  - Allow Google account auto sync

Microsoft InTune – Configuration Policies (3)

- Browser Security, Allow?
  - Web Browser
  - Autofill
  - Popups
  - Cookies
  - Active Scripting
- Application Security
  - Allow Google Play Store

Microsoft InTune – Configuration Policies (4)

- Hardware Security, Allow?
  - Camera
  - Removable Storage
  - Wi-Fi
  - Tethering
  - Geolocation
  - NFC (near field communication)
  - End User Power-Off
    (do not allow, this preserves the remote wipe) (keep charging)

Microsoft InTune – Configuration Policies (5)

- Cellular Security, Allow?
  - Voice Roaming
  - Data Roaming
  - SMS/MMS Messaging
- Feature Security, Allow?
  - Voice Dialing
  - Voice Assistant
  - Copy/Paste
  - Clipboard Share
  - YouTube

Microsoft InTune – Configuration Policies (6)

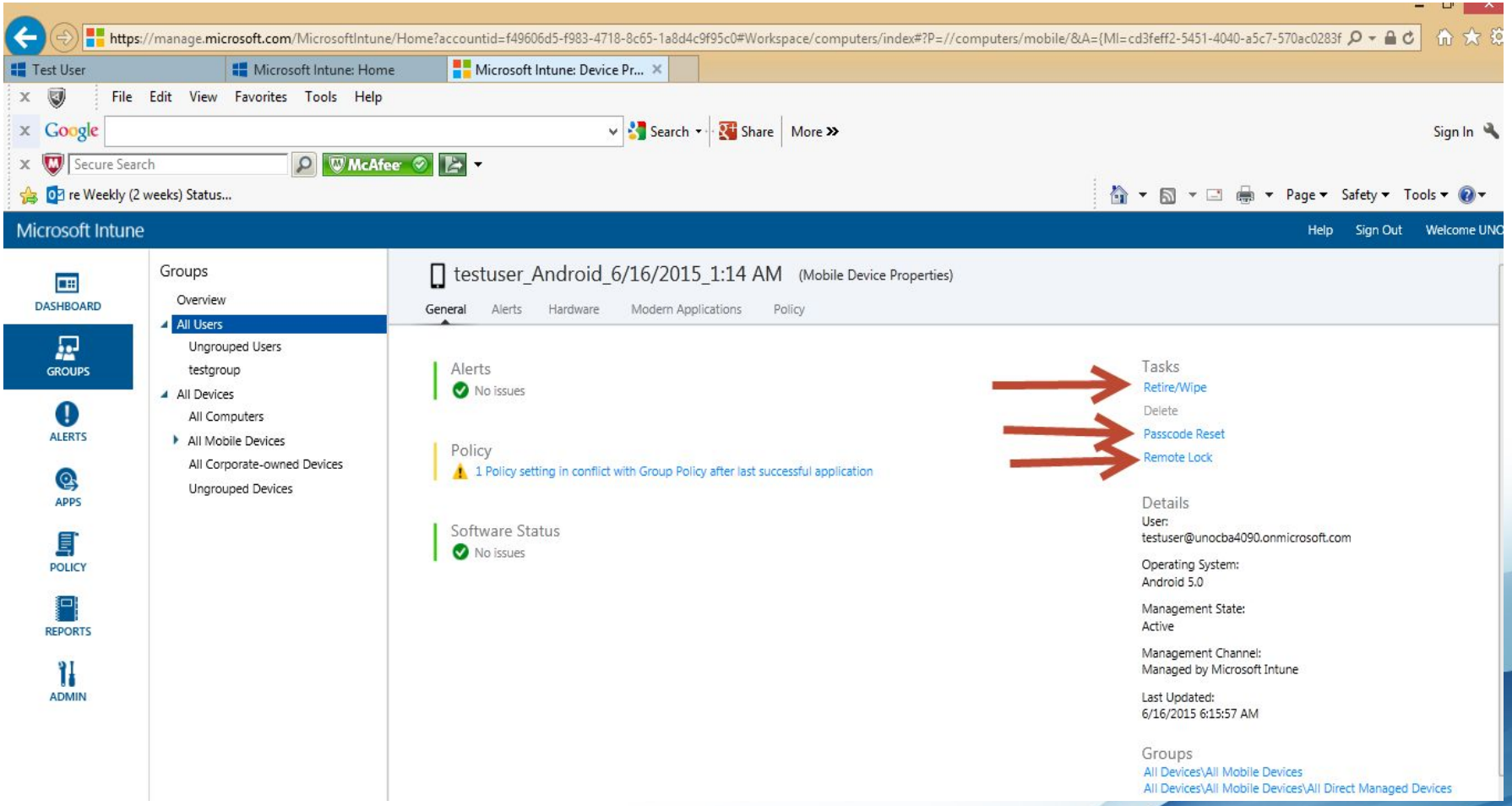
- App Security
  - Bad List
    Reports when user installs an app on this list
    Does NOT Prevent the Installation
    Does NOT check for REQUIRED Apps
    (See also the Apps tab within InTune)
  - Good List
    Reports when a user installs an app NOT on this list
    Does NOT Prevent the Installation

Microsoft InTune – Compliance Policies

Governs whether the device can access Exchange or SharePoint servers

- Password Security (same as slide 1 in Configuration Policy section)
- No Rooted or JailBroken devices allowed
- Email must be managed by InTune

Microsoft InTune – Dynamic User Control



The Institute of Internal Auditors

Microsoft InTune – I Don't See

- Application installation blocking
- Containerization, they say they have it but I have not seen how, "Selective Wipe" is on Win8.1 and W2K12, but not android
- Backup the device data
- Backup the Cloud data (policies, admin)
- Toll/Usage Cost Control
- Certificates (only for IOS)
- Phone OS Patching

Q & A (for Aaron only)

- ?????

The Institute of Internal Auditors