RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Enterprise Mobility Management

Security Without Compromising User Experience

SESSION ID: SPO2-R03

Brian Robison

Principal Technology Evangelist, XenMobile
Citrix Systems, Inc.

Divergent Concepts

Providing the freedom to access and use enterprise corporate data

While ensuring security and management of enterprise corporate assets and adhering to local regulations

Mobile: Security Issues, Past & Present

More than half of large businesses report mobile security incidents have amounted to more than $500,000 in the past year. **

One analyst firm found over 59% of Android devices had mobile malware.*

In June, Facebook disclosed an estimated 6 million Facebook users had e-mail addresses or telephone numbers shared with others due to a software bug in the “Download Your Information.”

Source:* http://www.zdnet.com/five-simple-ways-to-avoid-android-malware-7000017463
** http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf

Standards? Tablets and Smartphones aren't PCs

Security measure comparison of legacy PC's, Android, iOS and Windows* models				
Security measure	**PC**	**Android**	**iOS**	**Windows***
Device control	Add-on	Add-on	Add-on	Add-on
Local anti-malware	Add-on	Add-on	Unavailable	Native
Data encryption	Add-on	Configuration	Config/Add-on	Configuration
Data isolation/segregation	Add-on	Add-on	Native	Native
Managed operating environment	No	No	Yes	Yes
Application patching	User-managed	User-managed	Native	Native
Access to modify system files	Requires administrator	Requires rooting	Requires rooting	Requires administrator

** = Refers to Windows tablets and smartphones based on Microsoft Windows Phone, RT and Surface*

Supporting mobile platforms in the enterprise

iOS

- "Walled Garden" approach to OS and app management
- Devices can be jailbroken for modification of OS
- OS updates can impact enterprise networks
- Apple maintains tight control over MDM APIs

- Android is open to rooting and unlocking
- OS upgrades are not always available – check with carrier
- Browser-based active content security concerns
- Beware rogue app stores and overly permissive apps
- Support chain includes Google, device vendor and carrier
- Similar to a PC security model – require a security suite

CITRIX

Security is more than hardware…

Data

- Share
- Sync
- Encrypt
- Manage

Access

- Net Optimization
- Authentication
- Encryption

Devices

- Configure
- Provision
- Secure
- Support

Apps

- Contain
- Inter-app controls
- Provision-app store

Introducing EMM

What is needed is…

An enterprise-grade complete mobility solution for managing and securing apps, data, and devices-across the whole stack

- Enterprise-class MDM
- Multi-factor single-sign on
- Unified corporate app store
- Mobile app management
- Essential mobile productivity apps

Enterprise Mobility Management (EMM)

> *“is the set of people, processes and technology focused on managing the increasing array of mobile devices, wireless networks, and related services to enable broad use of mobile computing in a business context.”*

wikipedia

CITRIX

Mobile Device Management

Mobile Application Management

MDM and MAM Use Case Examples

BYOD Knowledge Worker

Native email and access to work documents

MDM: Control usage and prevent access if device is out of compliance.

MAM: Doc collaboration. Enterprise file sync and share

BYOD Board of Director

Access to corporate data with restrictions on data storage

Prevent access if device is out of compliance

Deliver virtualized apps with no on-device data storage

Remote/Field Worker

Company-issued device with controlled access to data and apps

Manage full device life cycle

Push custom apps and updates to the device

CITRIX

#RSAC

RSACONFERENCE2014

Mobile Device Management (MDM)

- Manage the device - whether corporate issued or BYO

- Manage the device throughout lifecycle

CITRIX

#RSAC

RSACONFERENCE2014

MDM - Device Level Controls

- Device password
- Remote wipe, lock
- Lock camera, WIFI
- Encrypt email, calendar, contacts
- Detect jail broken/rooted devices access
- Prevent backup to cloud

MDM Challenges

- Heavy-handed for BYOD
- All or nothing/Device wide
- Intrusive
- Privacy concerns
- Data leakage issues

Mobile Application Management (MAM)

- Manage and secure application whether off-the-shelf or internally developed
- Separate business from personal (containerization – app wrapping, SDK, virtualization, dual persona)

- Corporate app store to deliver apps to BYO or company-issued device
- Content management

MAM – Application level controls

- Application password
- Application encryption
- Prevent cut/copy/paste and open-in
- Geo-fencing
- Per app VPN
- SSO

MAM – Security Examples

Data Protection/Leakage

- App wrapping or SDK for iOS /Android/Windows
- App level policies
- Encryption
- Data containment

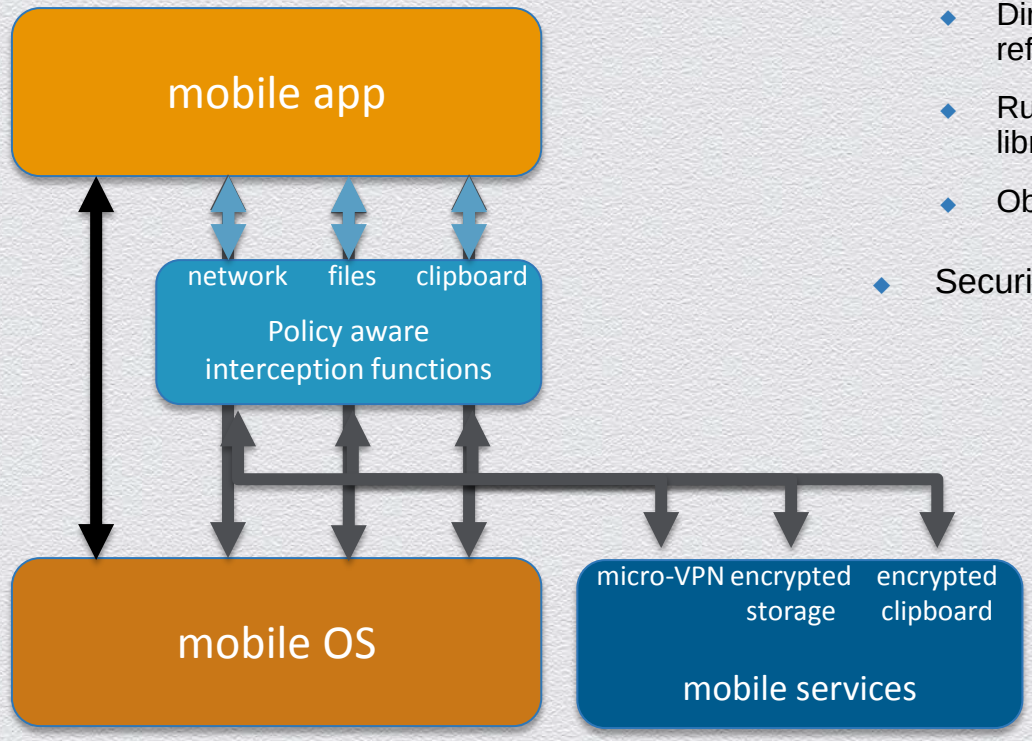
Inter App

- Intuitive app to app workflows
- Constrained Open-in
- Mailto and http intercepts

Network Access

- Secure browse with micro-vpn
- SSO & Identity federation
- Micro-vpn for all apps

Two Methods



App Wrapping

- API Interception techniques
  - Direct modification of app binary (replace symbol references)
  - Runtime hook injection for system calls & native libraries
  - Objective-C categories with method swizzling (iOS)
- Security Framework code injected via dynamic library

SDK based apps

- Symbols redirected at compile time
- Access to native services reduces need for hooks/swizzling
- Security Framework statically linked

Access Policy Examples

Authentication

- Enterprise logon only (AD + 2nd FA)
- Local logon only (pin/passcode)
- Enterprise & Local (based on connectivity)
- None
- No. of failed login attempts before lock

Time-based

- Re-authentication period
- Max offline period
- Active poll period
- App update grace period

Device status

- Block jailbroken/rooted devices
- Allow WiFi connected devices only
- Allow devices on Corp WiFi only

Information Security Policy Examples

- **Data Containment**
- **Hardware blocking**
- **Encryption**

What happens in containerized apps stays in containerized apps….

CITRIX

#RSAC

RSACONFERENCE2014

Information Security: Data Containment

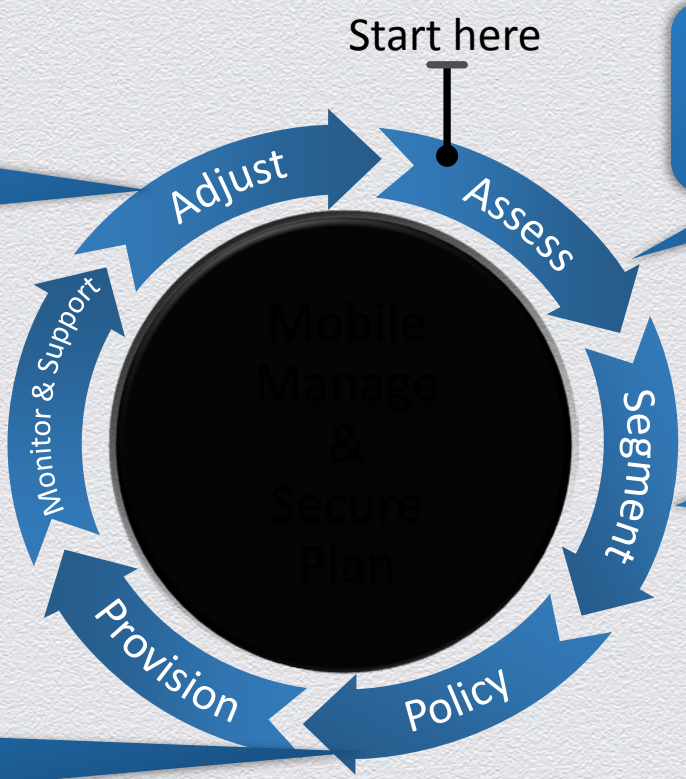
- Block cut/copy/paste
- Block/Constrain Open-in
- Define URL schemes (iOS)/Intents (Android)
- Scoping via security groups

Information Security: Encrypted App Vaults

- File vaults
  - Private by default, configurable by policy to shared within group
- Separate encryption of persistent app data
  - Online only: Vault keys held in KMS, Key TTL configurable
  - Offline: Vault keys maintained by app, user must authenticate with local password
- Potentially more secure than device level encryption

Best Practices

Create a Security & Management Plan



What's the goal of the plan? Timeline?

Not all users need to be treated equally: define needs.

Create, publish, market and support rules and guidelines.

Fine tune policy settings as needed. Nothing set in stone.

Best Practices Supporting Enterprise Mobility

- Establish formal policies: security, mobility, BYO
  - And make users aware of policies and their importance!
- Monitor and secure sensitive data-don't allow if not secured
- Two words-authentication and encryption
- Follow local regulations, in regards to privacy and data movement
- Work with users—segment security rules based on location, data, access

Work better. Live better.

Come see our XenMobile Enterprise solution at our booth!