Mastering the Mobile Security Landscape

Scott Behrens

June 19th, 2013

NEOHAPSIS

Security consulting since 1997

Strong focus on application and mobile security

Headquartered in Chicago

Scott Behrens

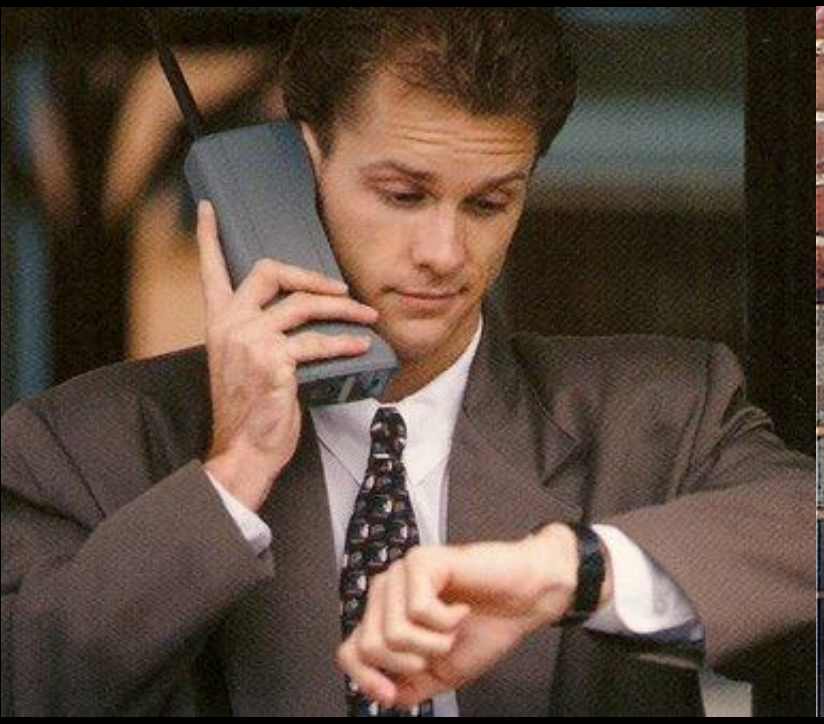
Senior Security Consultant

Adjunct Professor at DePaul University

Application and Security Research

1. The History and Significance of Mobile
2. What is a Mobile Device?
3. Using Mobile Devices Securely in the Enterprise
4. What is a Mobile App?
5. Mobile App Security
6. Conclusions

mobile devices are everywhere



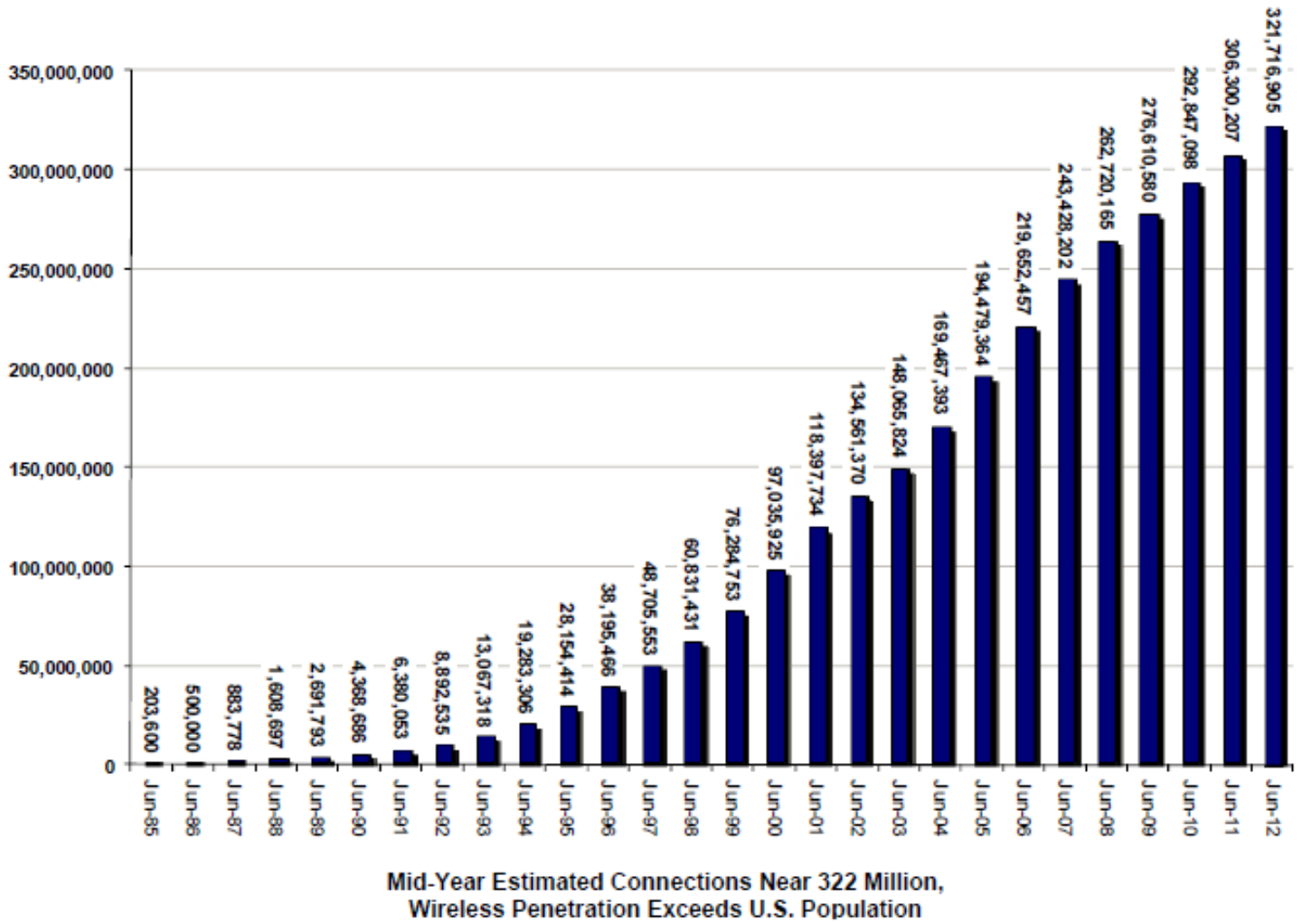
In the beginning was the feature phone

- Limited functionality
- Risks based around device misuse, not data security

Today's modern smartphone

- Always-on broadband connection
- High-resolution cameras
- Operating systems built for flexibility and extensibility
- Tech savvy users with a pathological attachment to their devices

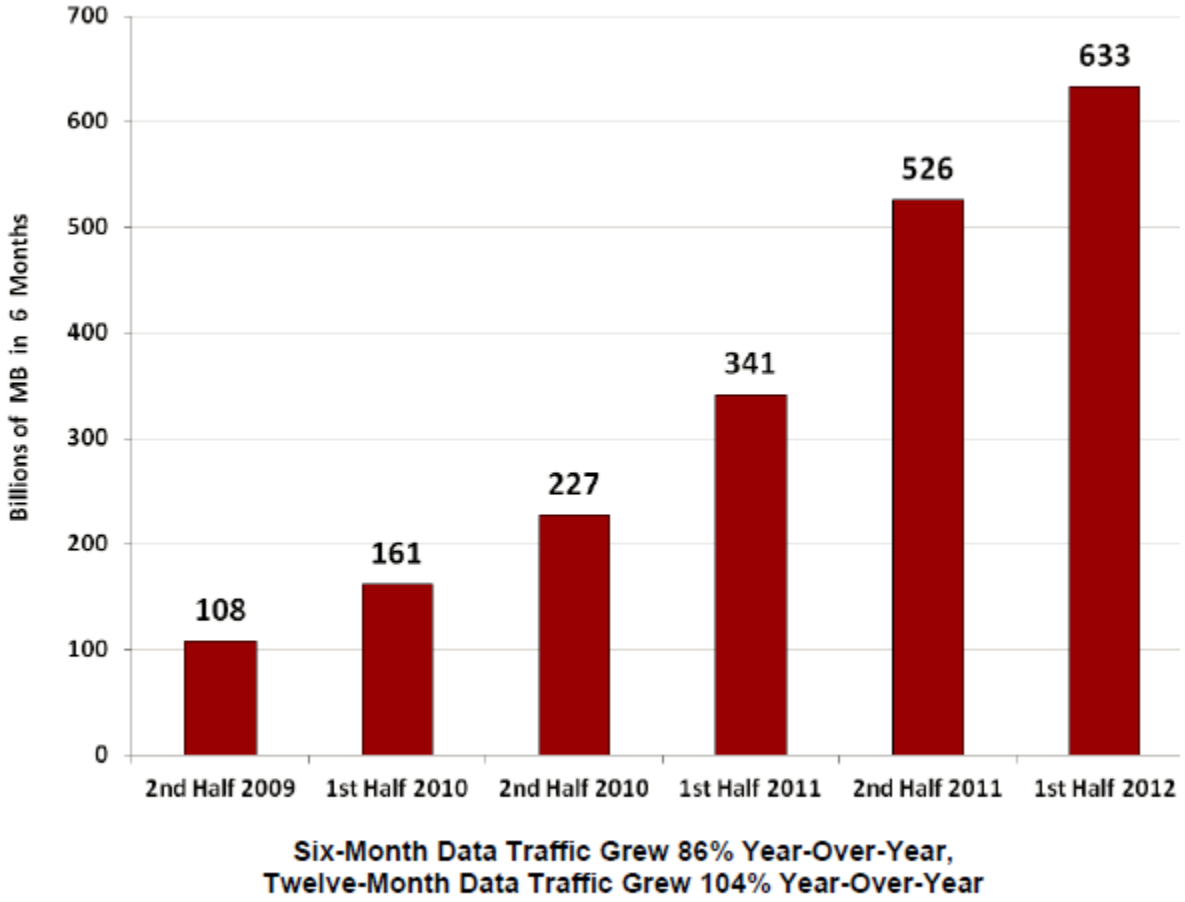
Total US Mobile Subscribers



Mid-Year Estimated Connections Near 322 Million, Wireless Penetration Exceeds U.S. Population

Used with the permission of CTIA-The Wireless Association

Total US Mobile Data Traffic



Mobile devices provide a great advantage to businesses.

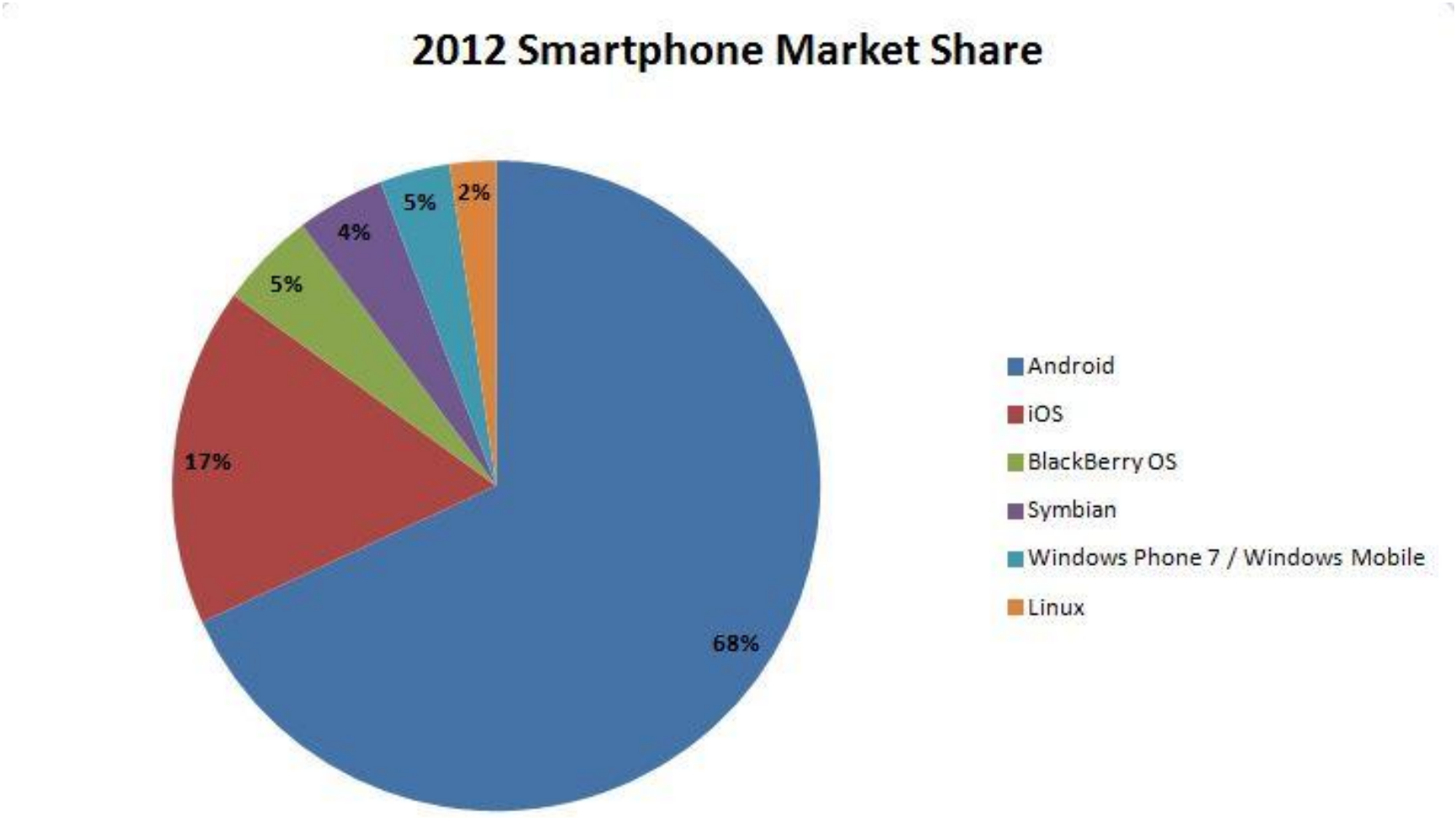
Mobile also represents an opportunity for engaging with customers.

People expect to use their mobile devices for everything they can use their PC's for.

Mobile Device Platforms

- Android
- iOS
- Windows 8
- Blackberry
- Symbian

Platform Breakdown



- Introduced in 2007 by Apple
- Derived from Apple's flagship OS X operating system
- Highly customized UNIX variant
- Applications written with Cocoa framework in Objective-C

- First device released in 2008
- Running custom Linux kernel
- Android software written in Java using the Android SDK

Security is a Concern

- 2012 Webroot Survey found:
  - 83% - believe that mobile devices create a high security risk
  - 73% - have a mix of company and employee-owned devices.
  - 47% - have implemented mobile security solutions

- Rate of mobile adoption is causing security challenges that businesses are just catching up with

http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf

Mobile Enterprise Security

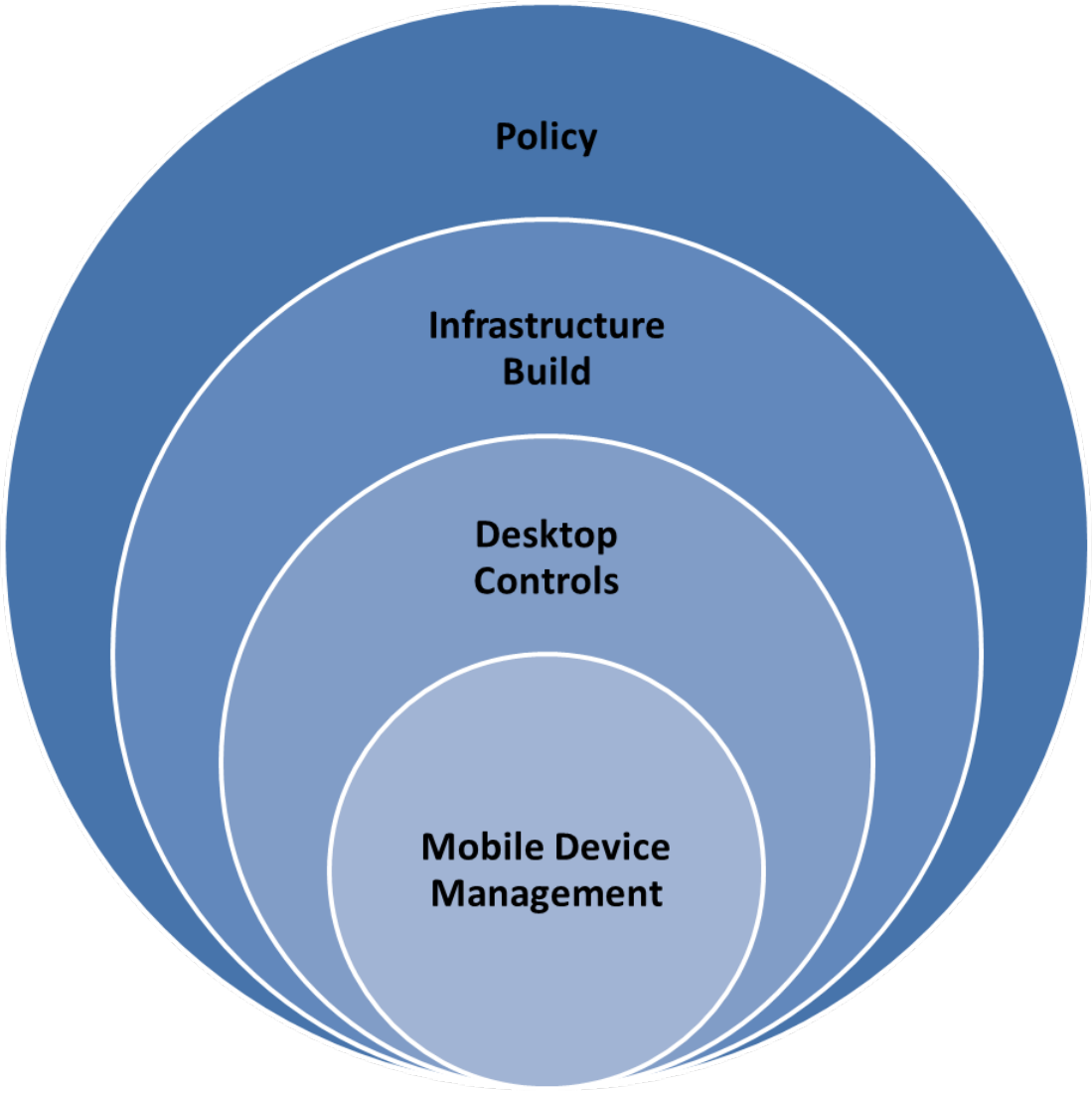
Mobile Threat Landscape - Enterprise

- Mobile data loss and leakage
- Intellectual property loss
- Employee privacy
- Mobile phone theft
- Mobile usage fraud
- Malicious applications
- Operating system vulnerabilities
- Wireless technology vulnerabilities
- Device rooting

Approaching Mobile Security in the Enterprise

- Secure your infrastructure from mobile devices
- Secure the mobile devices themselves

Layering Enterprise Security Controls



Mobile Security Policies

- Clearly articulate acceptable usage of mobile devices
- Employee training & reminders
- Emphasize to employees that mobile devices are for business purposes

Infrastructure and Connectivity

- Wireless LAN
  - Use best practices for WLAN security
  - Segment networks for employee mobile devices only
  - Consider what you want mobile devices accessing
  - Separate guest networks from employee networks
- Mobile Data Networks
  - Ultimately, you must treat them like an ISP

Mobile Devices and Desktops

- Mobile devices function as portable hard drives
- Users can also access underlying mobile device file systems with their desktops
- Enable best practices for iTunes Security (iOS)
- DLP
- Disable usage of USB drives if possible

Mobile anti-virus is not the solution

- Anti-virus vendors are trying to get into the mobile device market
- Has been a subject of debate in the mobile community
- None are enterprise-focused and are of questionable effectiveness

A Better Solution – Mobile Device Management

- Allows administrators remote management and provisioning of mobile devices
- Range from relatively basic controls to very comprehensive
- Both on-site and cloud-based deployment solutions

Mobile Device Management - Platforms

- iOS, Android, Blackberry, and Windows all have MDM features built-in

- Apple is pulling ahead of Android in feature availability
  - Has the advantage of stricter OS control
  - Is winning the tablet market

- Blackberry is still the leader in features - but losing market share rapidly

Basic MDM - Microsoft Exchange

Devices provisioned to Exchange can have some security settings enforced:

- Screen lock
- Mobile device encryption
- Restriction of mobile phone features
- Remote data wipe

Mobile Device Management – Key Operational Features

- Detailed reporting on users and devices
- Restrict and monitor phone usage
- Detection of rooted/jail-broken devices
- Remote wipe of lost devices
- Concept of "personal space" and "work space" on user's phones

Mobile Device Management – Key Security Features

- Enforced password/PIN complexity
- Application management
  - White-Listing/Black-listing applications
  - Block specific application permissions
  - Remotely remove applications and data
- Encrypt data storage on phone
- Restrict phone usage

Future of Mobile Device Management

- Increasing focus on tablets
- Expansion into desktop management
- Document management/file sharing
- Private application stores

Mobile Device Management - Major Vendors

- Airwatch
- Blackberry
- Fiberlink
- Good Technologies
- Symantec
- MobileIron
- Zenprise

MDM Shortcomings

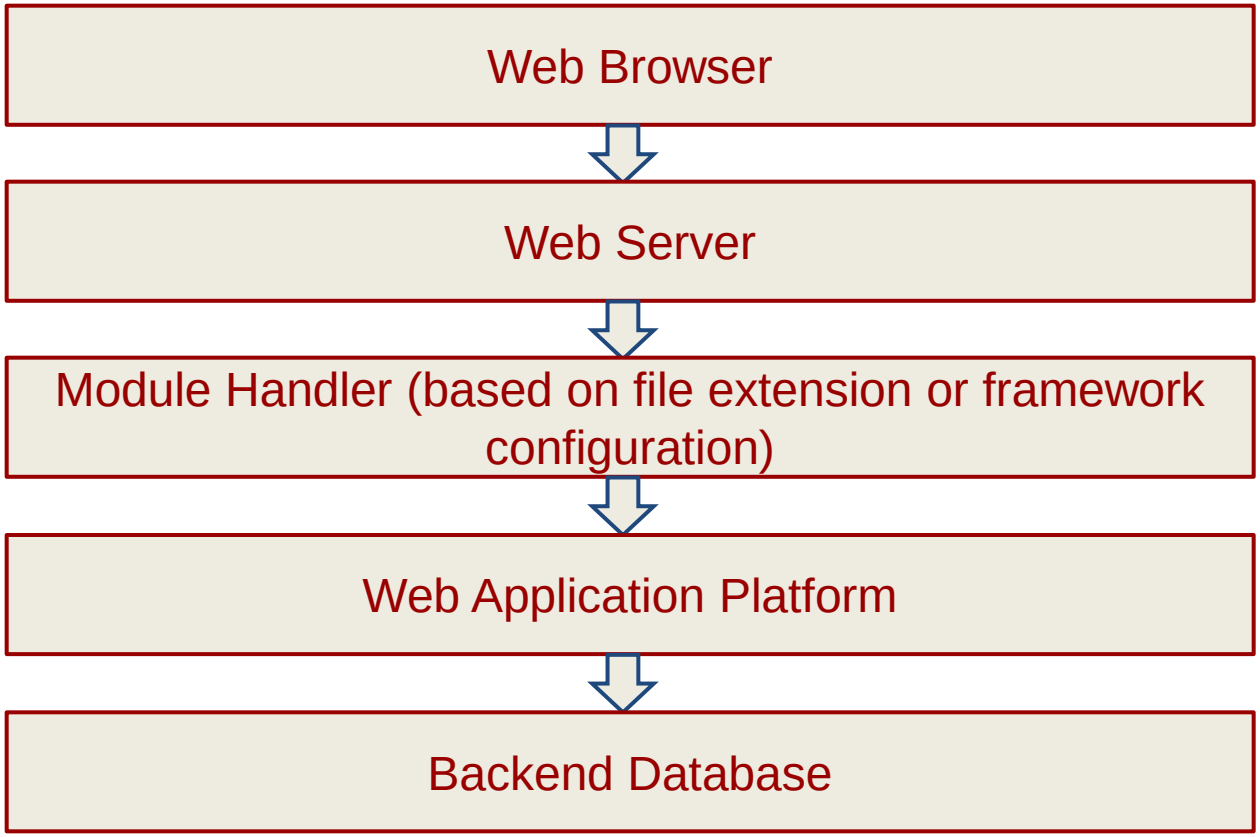
- Users can simply remove the MDM solution from their device
- Users can work within the restrictions of the MDM
- A policy and enforcement issue
- Provides little protection against malicious applications

Mobile Application Security

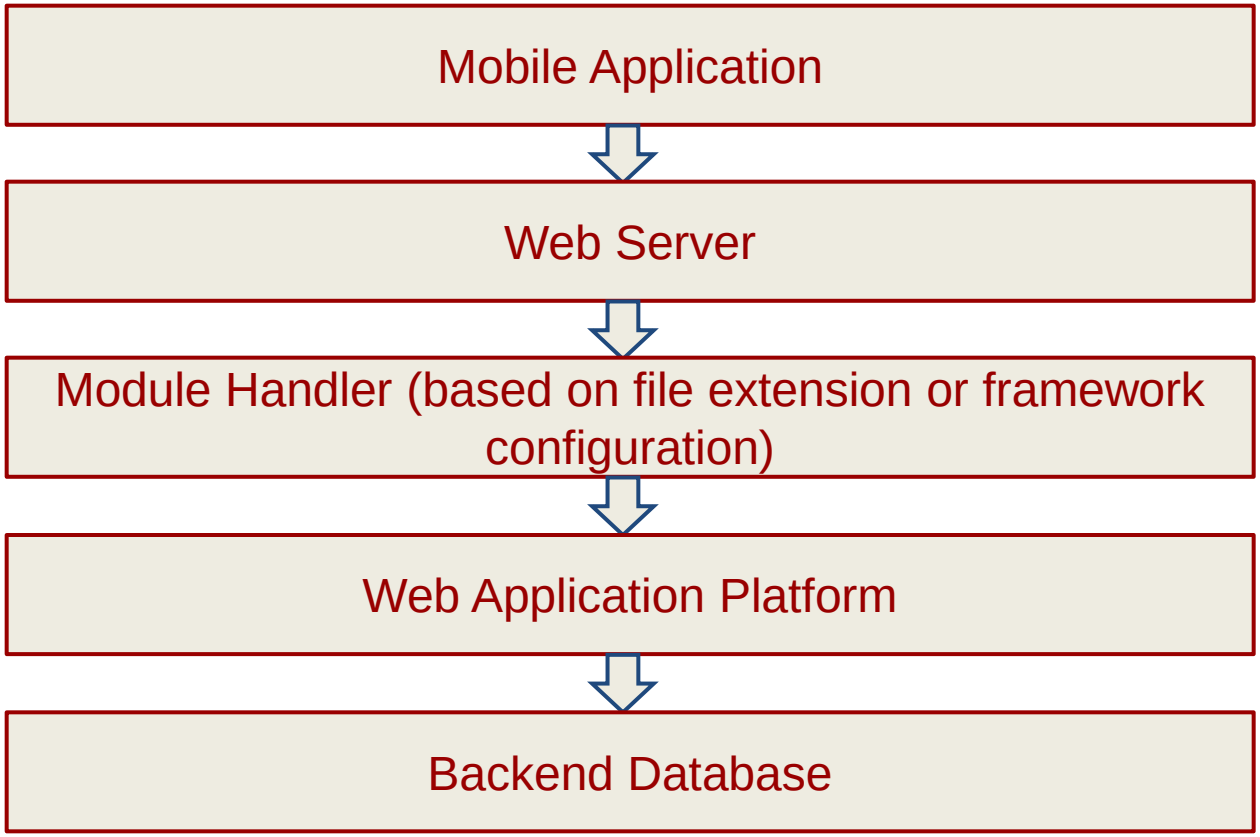
What is a mobile application?

- An application that runs on a mobile device
- Have some local data store or cache
- Act as a frontend that interacts with backend service

Traditional Web Application



Client/Server Mobile Applications



Mobile Threat Landscape - Applications

- Business reputation
- Customer satisfaction
- Financial loss
- Liability
- Compliance and regulation requirements
- Sensitive information disclosure
- Key management

Mobile Application Security Features: Android

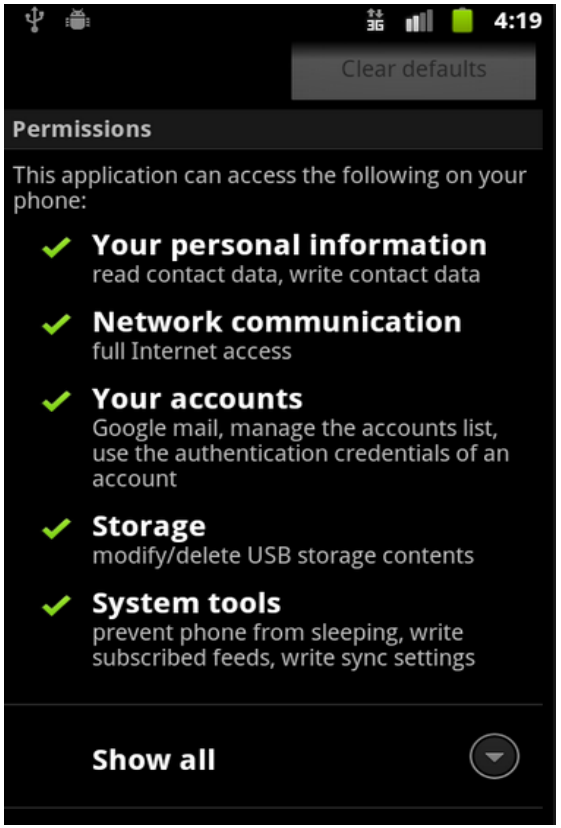
- Sandboxing
- SDK includes common security features:
  - Cryptography
  - Secure inter-process communication (IPC)
- Memory management protections:
  - ASLR, NX, ProPolice, safe_iop, mmap_min_addr
- User and application level permissions

Mobile Application Security Features: Android

- Applications must explicitly share resources and data
- Applications run in sandbox with own unique UID
- Sandbox runs on native OS level

Application Permissions: Android

Applications must explicitly request permissions to access data and services and data



Application Permissions: Android

Specifically includes permissions that restrict access to sensitive phone-related user information

- Permissions are pretty granular and specific
- Can be problematic as some permissions are grouped together
- Users may get desensitized to the permission check and just click accept

Android: Rooting

- Without rooting the device, users cannot access areas in the /system directory
- Rooting allows users to fully access filesystem and make changes to help attack applications

Application Permission Model: iOS

Sandboxing

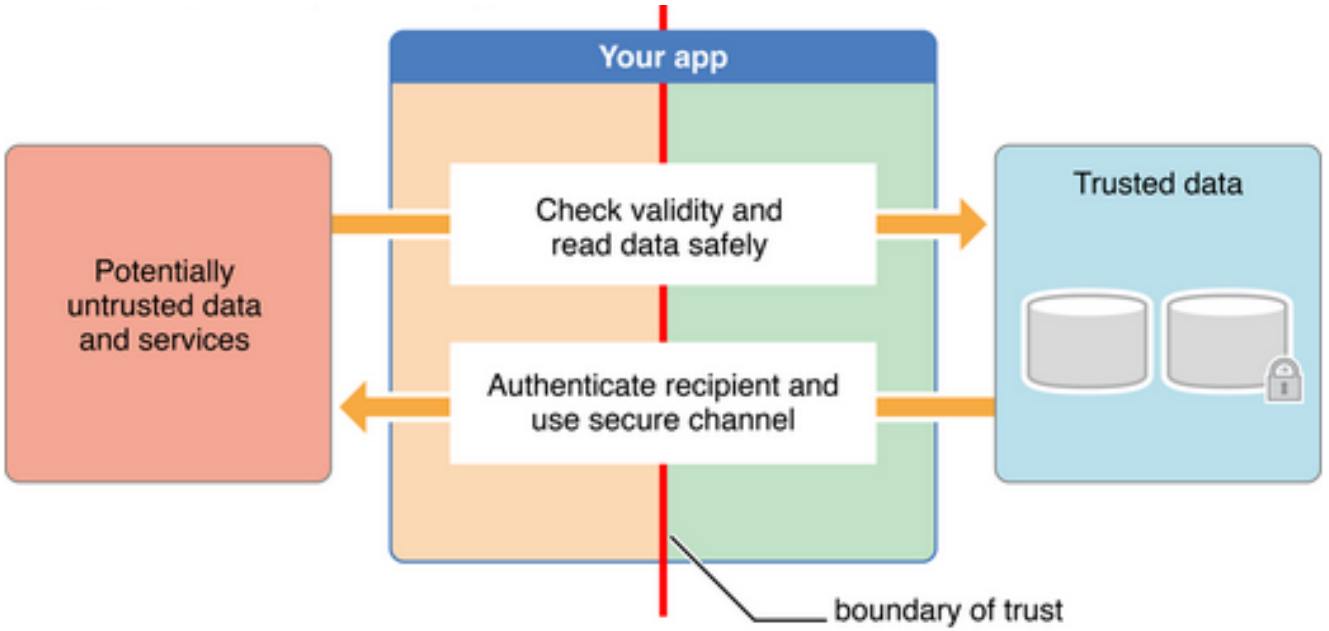
- iOS5: No concept of explicit permissions
  - All applications have equal access to all of iOS device resources
- iOS6: More granular permissions system
- Security is assumed on application review process by Apple for their application store

Mobile Application Security Features: iOS

- Keychain services
- Cryptographic functions for application developers
- Secure file storage using FileVault or iOS File Protection
- Code signing

Mobile Application Attacks

Mobile Application Boundaries



Mobile Application Common Attacks

- Root device
- Attack application backend services
  - Intercept SSL traffic (SSL MITM)
- Attack local file storage (database)
- Attack XML Processors
- Look for debugging log information
  - May contain debug statements that contain PII, passwords, etc.
- Examine Plist files (iOS) for sensitive information and permissions

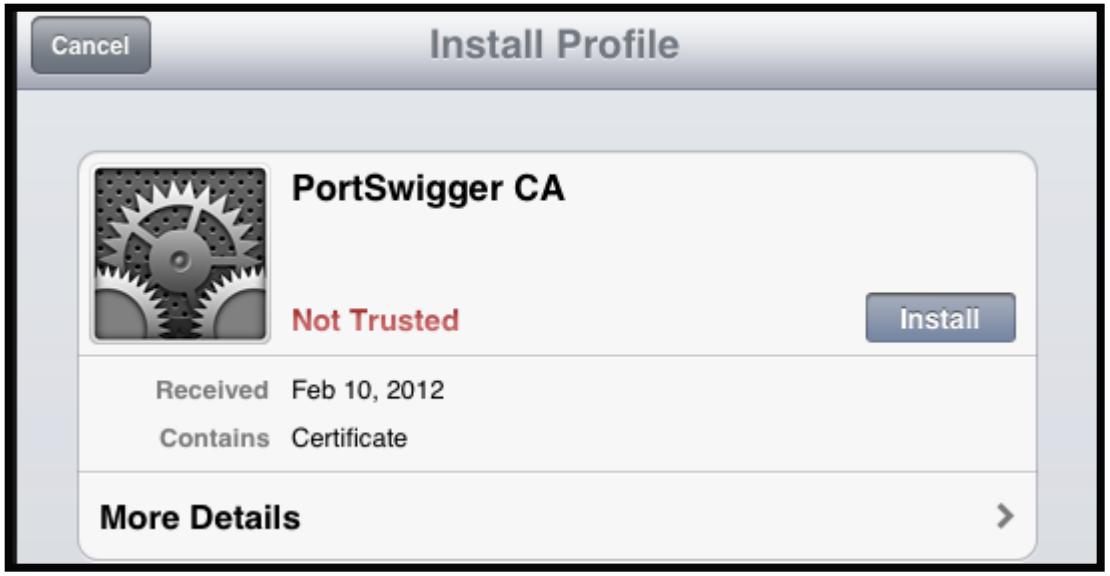
Mobile Application Common Attacks

- Attack IPC endpoints (Android)
  - Activities, Broadcast Receivers, Content Providers, Services
- Disassemble or decompile application to look for security vulnerabilities or sensitive information in the application source code
- Look for low level memory application vulnerabilities
  - Buffer overflows, integer bugs, etc.
- Look for snapshot files

Application Attack Demo

Using a web application proxy, generate root level certificate and install on iPhone.

Typically attacker copies the cert to phone via hosting it on a web site.



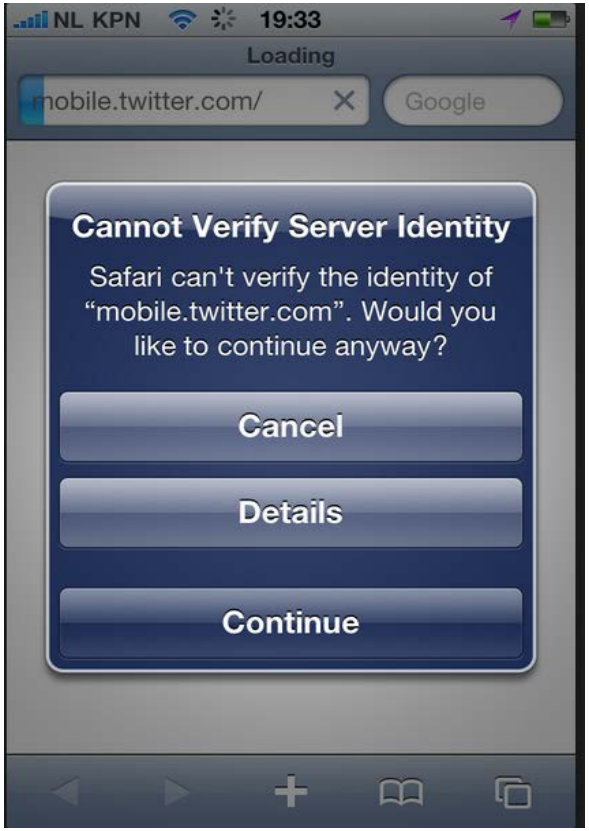
Application Attacks

- Many built in security features and even MDM do not address all of these attacks
- Attackers take advantage of insecure coding practices and backend services which operate in different trust models

Application Attack Demo

Once Root certificate is installed, proxy automatically generates self signed certs for each web server or service requested.

Prevents the following error:

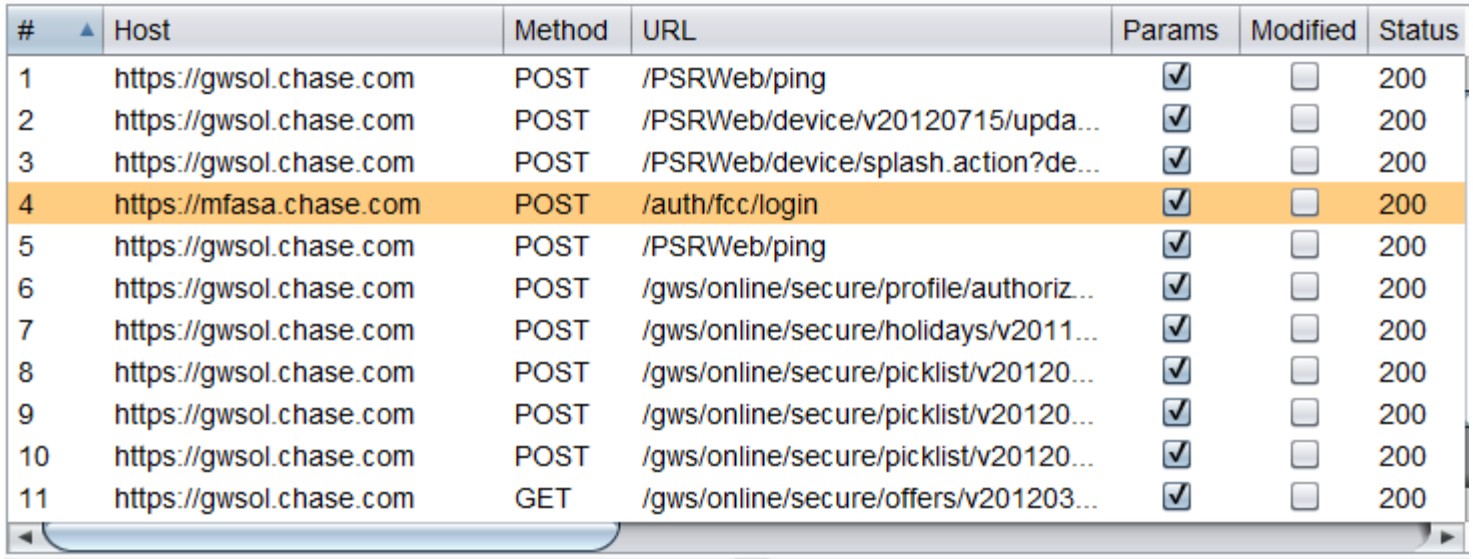


Application Attack Demo

- Since our Proxy certificate is trusted, the application will think every SSL certificate presented for each domain is valid
- Attacker now configures phone's network to proxy internet traffic through the web application proxy
  - This is simply done in the Network tab on iOS
  - On Android ICS 4 it's a bit more complicated
- Attacker now launches application and begins to perform functions

Meanwhile...

All that encrypted SSL traffic to and from the mobile application to backend web service can be now be intercepted and modified.



#	Host	Method	URL	Params	Modified	Status
1	https://gwsol.chase.com	POST	/PSRWeb/ping	☑	☐	200
2	https://gwsol.chase.com	POST	/PSRWeb/device/v20120715/upda...	☑	☐	200
3	https://gwsol.chase.com	POST	/PSRWeb/device/splash.action?de...	☑	☐	200
4	https://mfasa.chase.com	POST	/auth/fcc/login	☑	☐	200
5	https://gwsol.chase.com	POST	/PSRWeb/ping	☑	☐	200
6	https://gwsol.chase.com	POST	/gws/online/secure/profile/authoriz...	☑	☐	200
7	https://gwsol.chase.com	POST	/gws/online/secure/holidays/v2011...	☑	☐	200
8	https://gwsol.chase.com	POST	/gws/online/secure/picklist/v20120...	☑	☐	200
9	https://gwsol.chase.com	POST	/gws/online/secure/picklist/v20120...	☑	☐	200
10	https://gwsol.chase.com	POST	/gws/online/secure/picklist/v20120...	☑	☐	200
11	https://gwsol.chase.com	GET	/gws/online/secure/offers/v201203...	☑	☐	200

Request | Response

Raw | Params | Headers | Hex

```
POST /auth/fcc/login HTTP/1.1
Host: mfasa.chase.com
User-Agent: iPhone-Version 2.230:UDID-255bd6783415aaaa9c8f8bc00a092c28d82753b7
:OriginalInstallDate-2012-04-30 17:44:46.7120
Content-Length: 598
Accept: */*
channel-id: MON
Accept-Language: en-us
Cache-Control: no-cache
Cookie:
adtoken.chase.com=IDSS3VZKP8KNAFZGIOSCRJAKGLTTNRTWOIB5Q84X01XPCLFHS6XZIDQ4JR9ZWXNB
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: keep-alive
Proxy-Connection: keep-alive

auth_passwd=[redacted]&Referer=https%3A%2F%2Fwww.chase.com&auth_otpprefix=&auth_userId
=[redacted]auth_otp=&type=json&auth_deviceCookie=adtoken&auth_deviceSignature=&auth_exte
rnalData%3E=LOB%3DRBGLogon&auth_passwd_org=[redacted]&LOB=RBGLogon&auth_mobile_mis=DEV
MAKE%3DApple%26DEVID%3D255bd6783415[redacted]7%26DEVOS%3DiPhone%2520OS%2
6DEVMODELVER%3DiPhone4%2C1%26DEVOSVE&auth_otpreason=&auth_siteId=MON&auth_deviceId=IDSS3V
ZKP8KNAFZGIOSCRJAKGLTTNRT[redacted]&auth_contextId=login
```

Application Attack Demo

- Has ability to read and modify communication
- Attacker can target the backend web service as well as client side vulnerabilities triggered by interaction with web services

Building Secure Mobile Applications

Building Secure Mobile Applications

- Encrypt local datastores
  - Store sensitive information in keychain (iOS specific)
- Don't store secrets, passwords, private keys if possible
  - Assume attacker can see your code
- Request and use minimal permissions
- Examine your applications IPC calls and make sure they are securely implemented
  - AKA. don't allow me to reset passwords from another application

Building Secure Mobile Applications

- Ensure your application is "Production" ready
  - Disable logging, developer backdoors, developer IPCs, unencrypted storage, etc.
- Implement encrypted connections for everything
- Assume that someone will do a security assessment of it
- Perform security assessments of your mobile applications and backend web-services

Summary

Summary

- Mobile devices present a unique set of security concerns
  - BYOD challenges, control circumvention, data loss, etc.
- Mobile Applications have many of the same risks of traditional applications
- A hybrid approach to mobile security
  - Policy, infrastructure, endpoint hardening, secure coding, conducting assessments

References

- http://developer.android.com/guide/topics/security/permissions.html
- http://source.android.com/tech/security/index.html
- http://developer.android.com/training/articles/security-tips.html
- http://technet.microsoft.com/en-us/library/bb123484(v=exchg.141).aspx
- http://developer.android.com/guide/topics/admin/device-admin.html
- http://www.idc.com/getdoc.jsp?containerId=prUS23818212#.UTI39TB0NgO
- http://www.internetretailer.com/trends/sales/
- http://blog.nielsen.com/nielsenwire/online_mobile/young-adults-and-teens-lead-growth-among-smartphone-owners/
- https://developer.apple.com/library/mac/#documentation/Security/Conceptual/Security_Overview/Introduction/Introduction.html#//apple_ref/doc/uid/TP30000976
- https://developer.apple.com/library/mac/navigation/#section=Topics&topic=Security
- http://www.ctia.org/advocacy/research/index.cfm/AID/10316
- http://images.apple.com/ipad/business/docs/iOS_6_MDM_Sep12.pdf
- http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf

Thank You!

Scott.Behrens@neohapsis.com