



# Securely Equipping a Mobile Workforce

Trends & Considerations

**InformationWeek**  
::analytics

## About *InformationWeek Analytics*

- New each year: 50 research reports and 150 strategy, best practices, how-to reports, vendor rankings, product assessments and more
- For IT, by IT – reports are written by current and past IT professionals
- Plus: InformationWeek current and past issues in digital format
- \$399 per year – you'll never see an ad and we'll never sell your name!

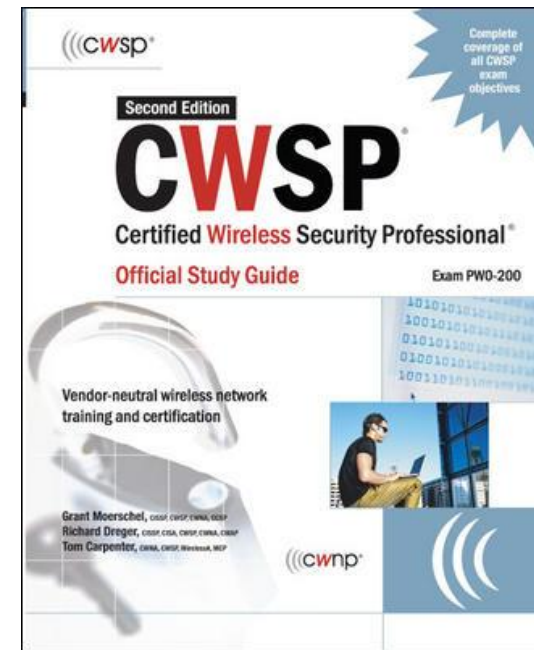
Visit us soon at [\*analytics.informationweek.com\*](http://analytics.informationweek.com)

**InformationWeek**  
:: analytics

---

# Who we are?

- Grant P. Moerschel
  - VP, WaveGard
    - IT Security Consulting
    - Risk Assessments/Auditing
    - Network & Systems Design
    - Security Remediation
  - Specialties include secure perimeter design, next gen firewall technologies, 802.11 design & security
  - CiscoPress & McGraw-Hill Books
  - InformationWeek Contributor



## InformationWeek Contributors



For our articles, go to [www.informationweek.com](http://www.informationweek.com)

Search on: **wavegard** OR **savid**

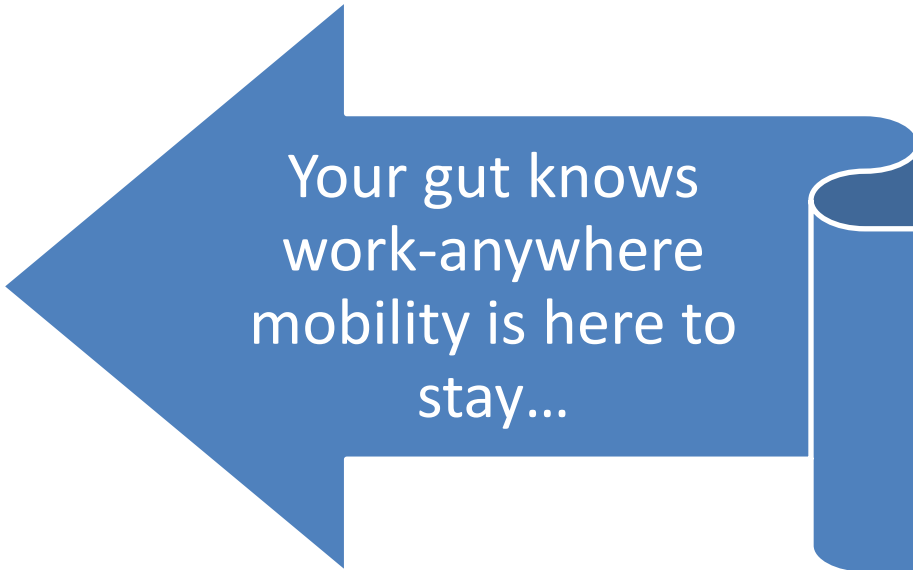
**InformationWeek**  
::analytics

  
**UBM**  
TechWeb

# Agenda

- Trends in platform growth
- Struggles / Risk
- Vulnerabilities
- Strategies & Tactics
- Vendor approaches
- Questions

# Mobility Trends



Your gut knows  
work-anywhere  
mobility is here to  
stay...

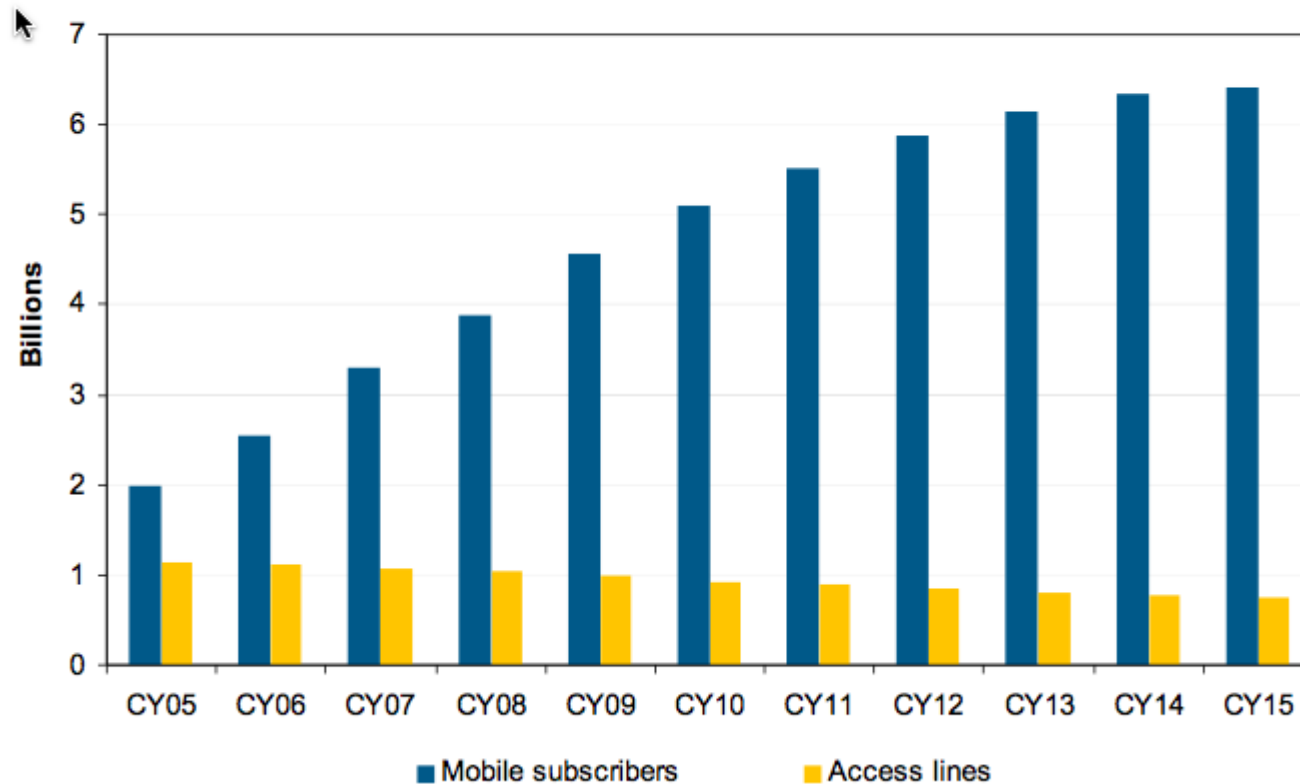


But to what extent??

# Mobility Trends

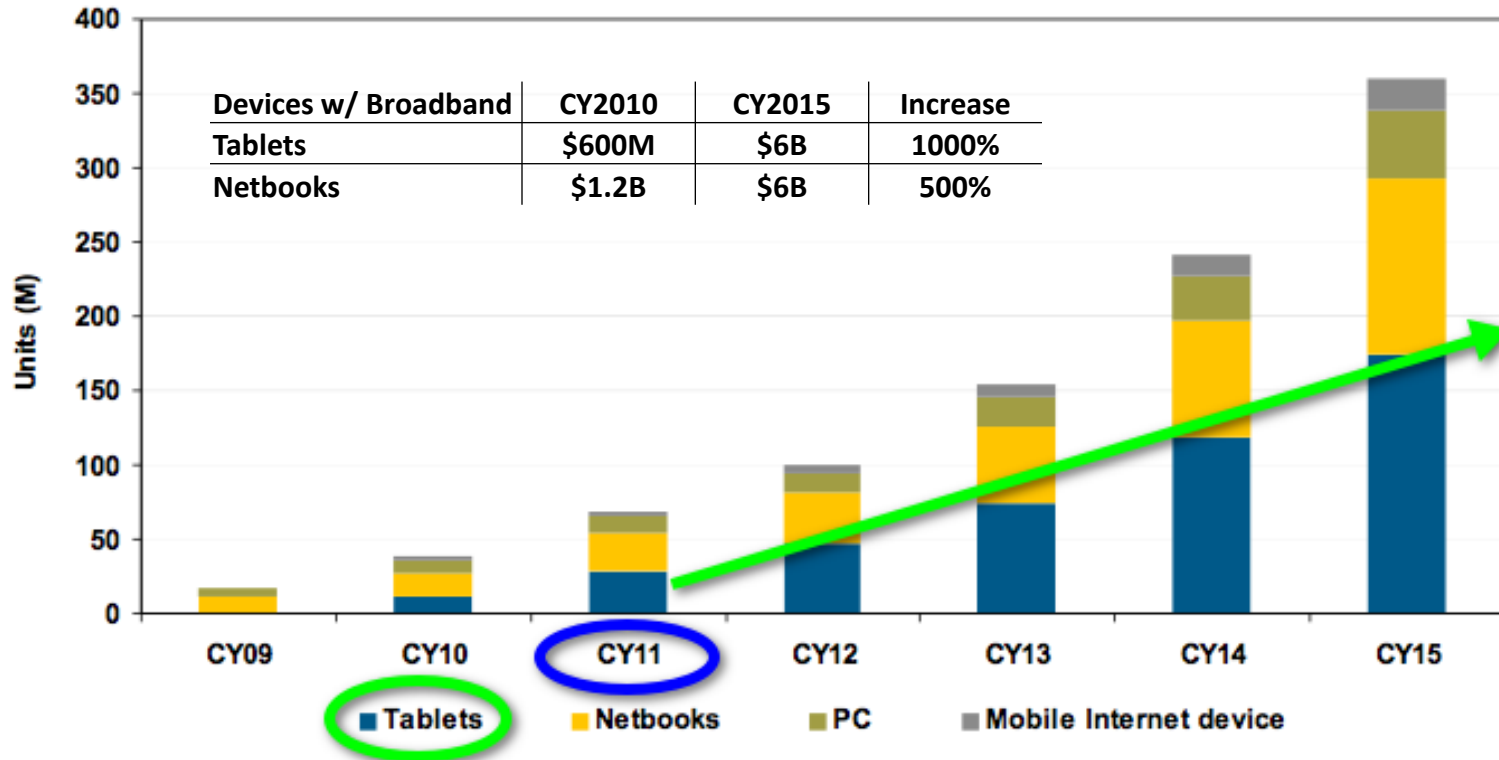
Exhibit 1

Worldwide Mobile Subscribers vs Access Lines



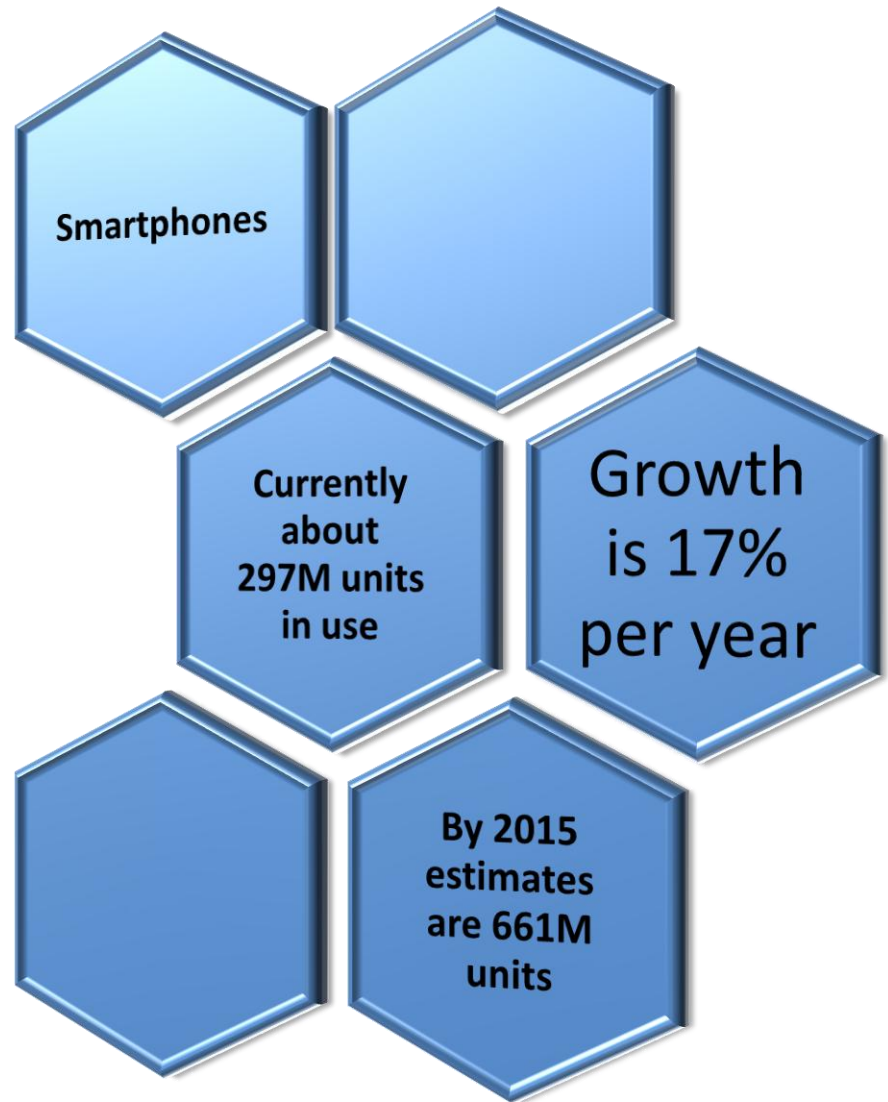
# Mobility Trends

**Exhibit 3 Worldwide Embedded Mobile Broadband Device Units**



# Smart Device Growth

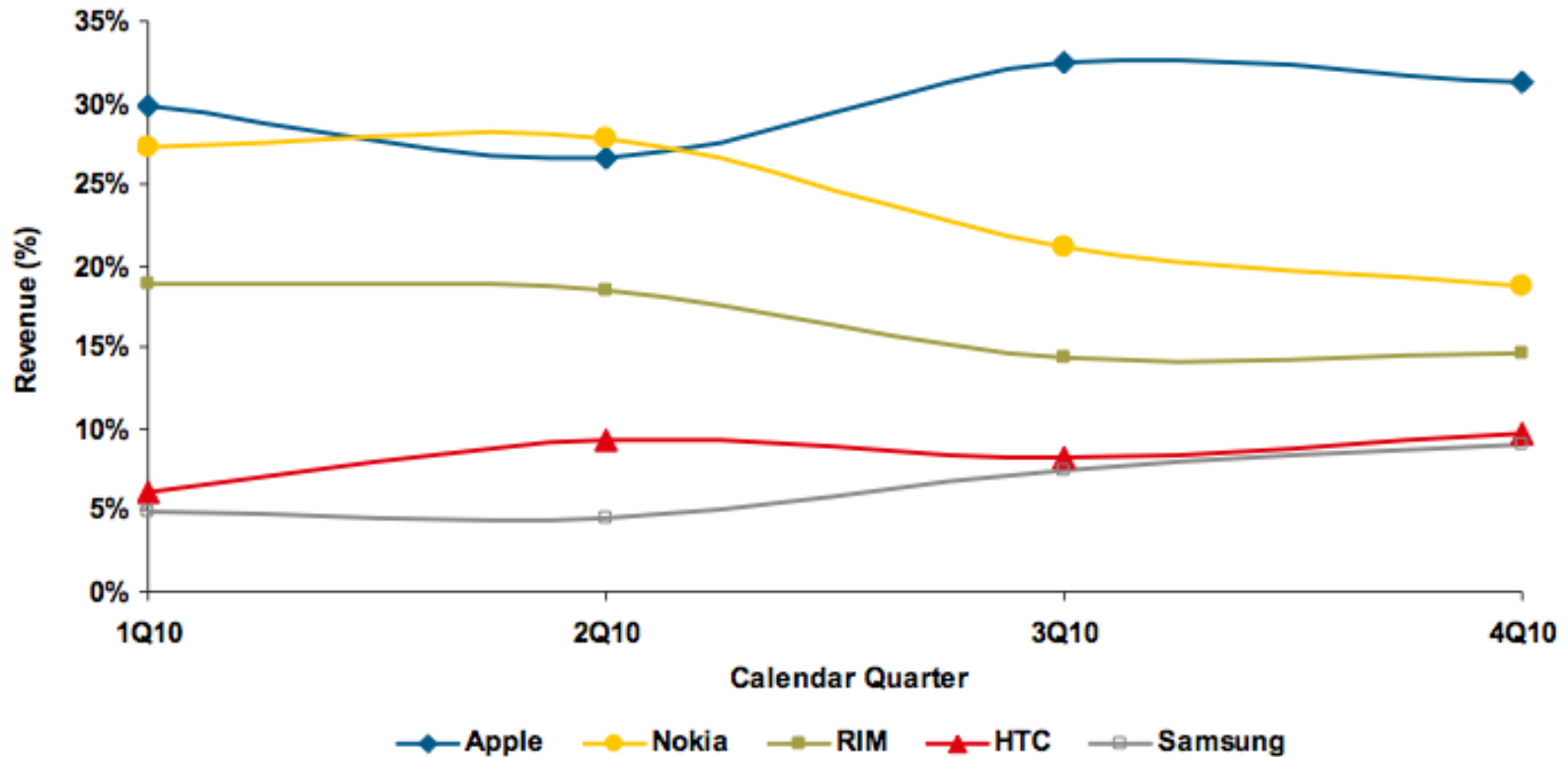
- Google Android flavors
- RIM BlackBerry
- Apple iPhone
- Microsoft Phone
- Nokia Symbian
- HP webOS
  
- Don't forget tablets!



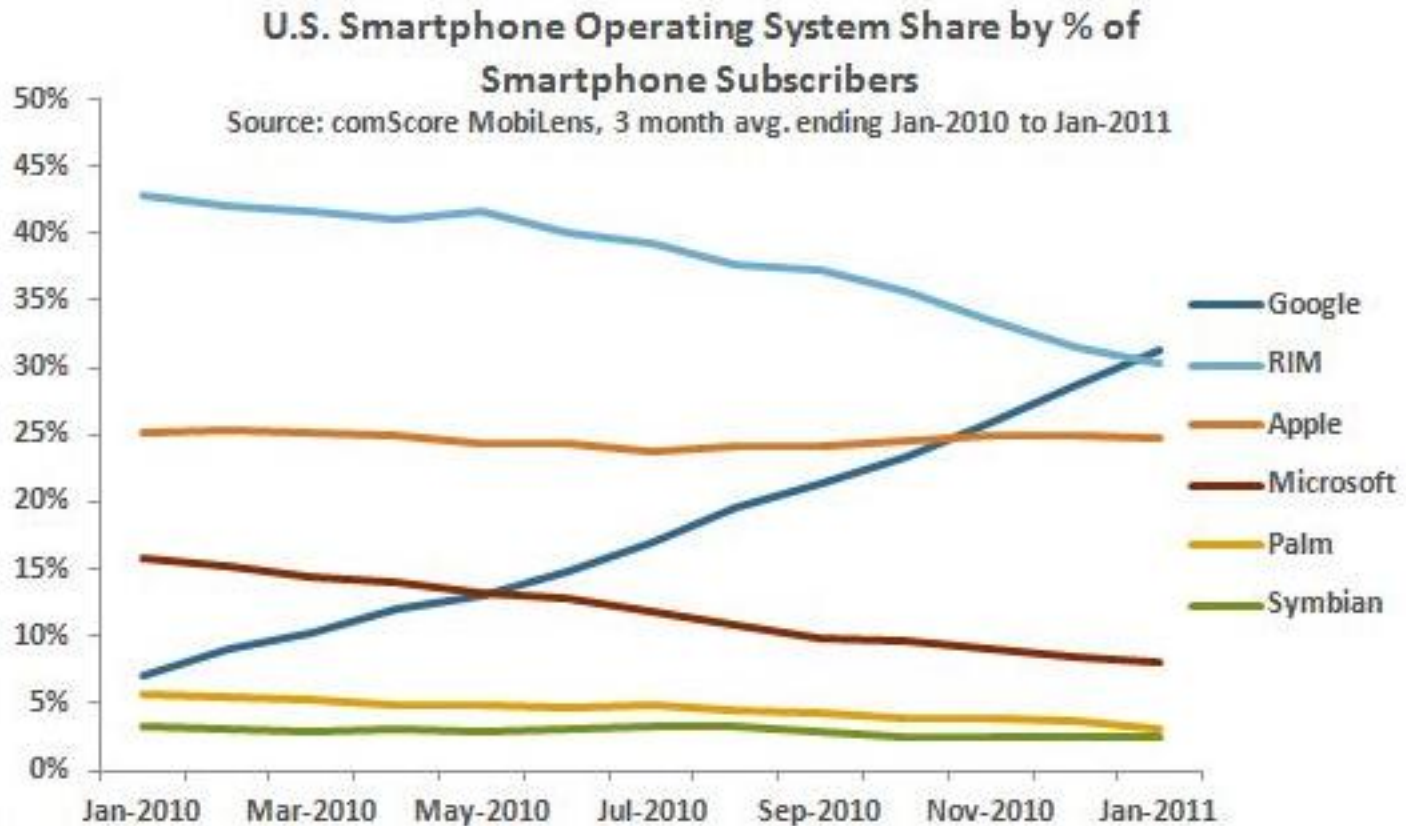
# Worldwide Platform Trends

Exhibit 19

Smartphone Worldwide Revenue Market Share



# U.S. Platform Trends



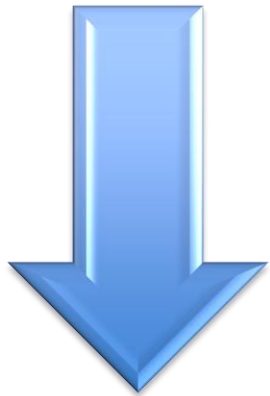
Source: [www.comscoredatamine.com](http://www.comscoredatamine.com)

# Mobility Trends



Mobile

By 2012, enterprise workers who want to use a personal mobile device for work-related activities are expected to account for 25 percent of all workers. (Forrester Research) **Number is Low**



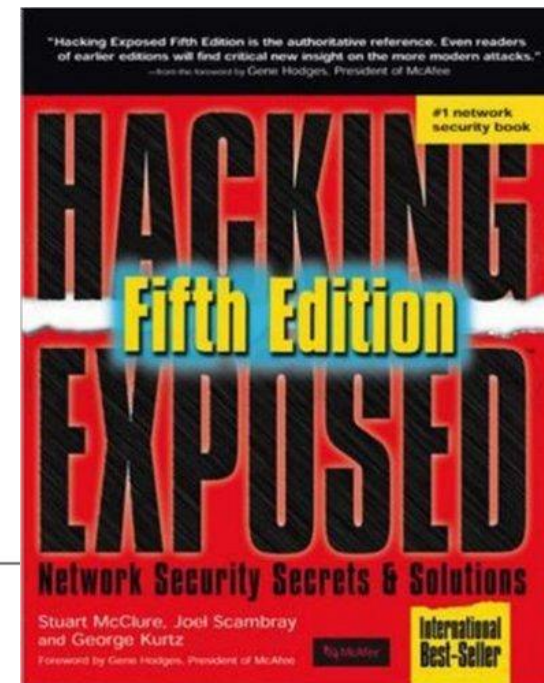
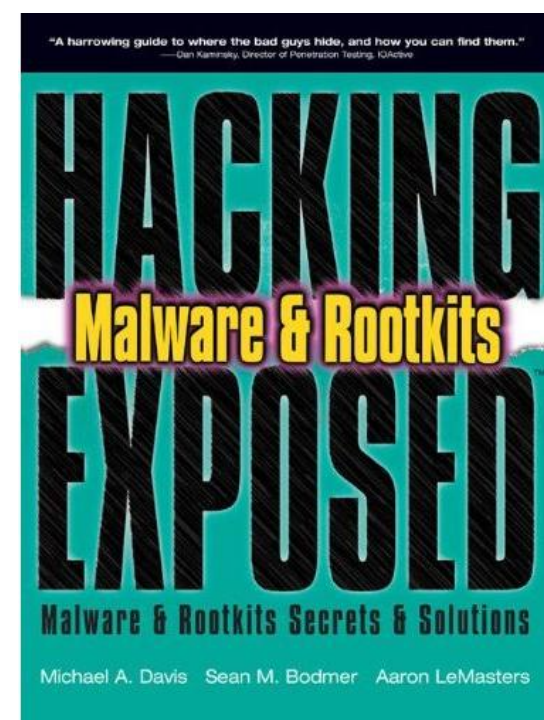
Stationary

- Smartphone sales are up
- Tablet sales are up
- Platform innovation is off the chart

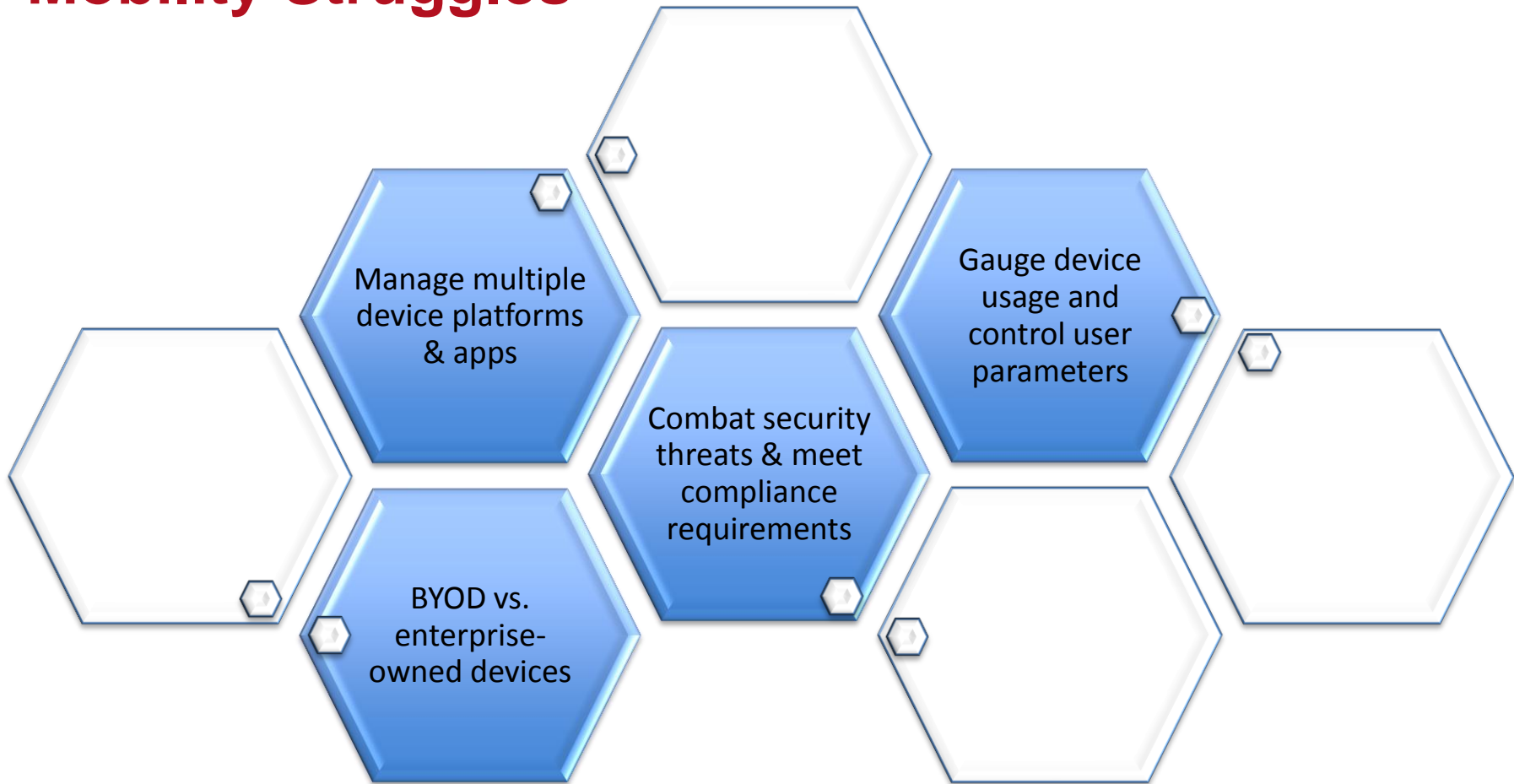
Unlike days of old, consumers are driving platform adoption (BYOD)

# Who we are?

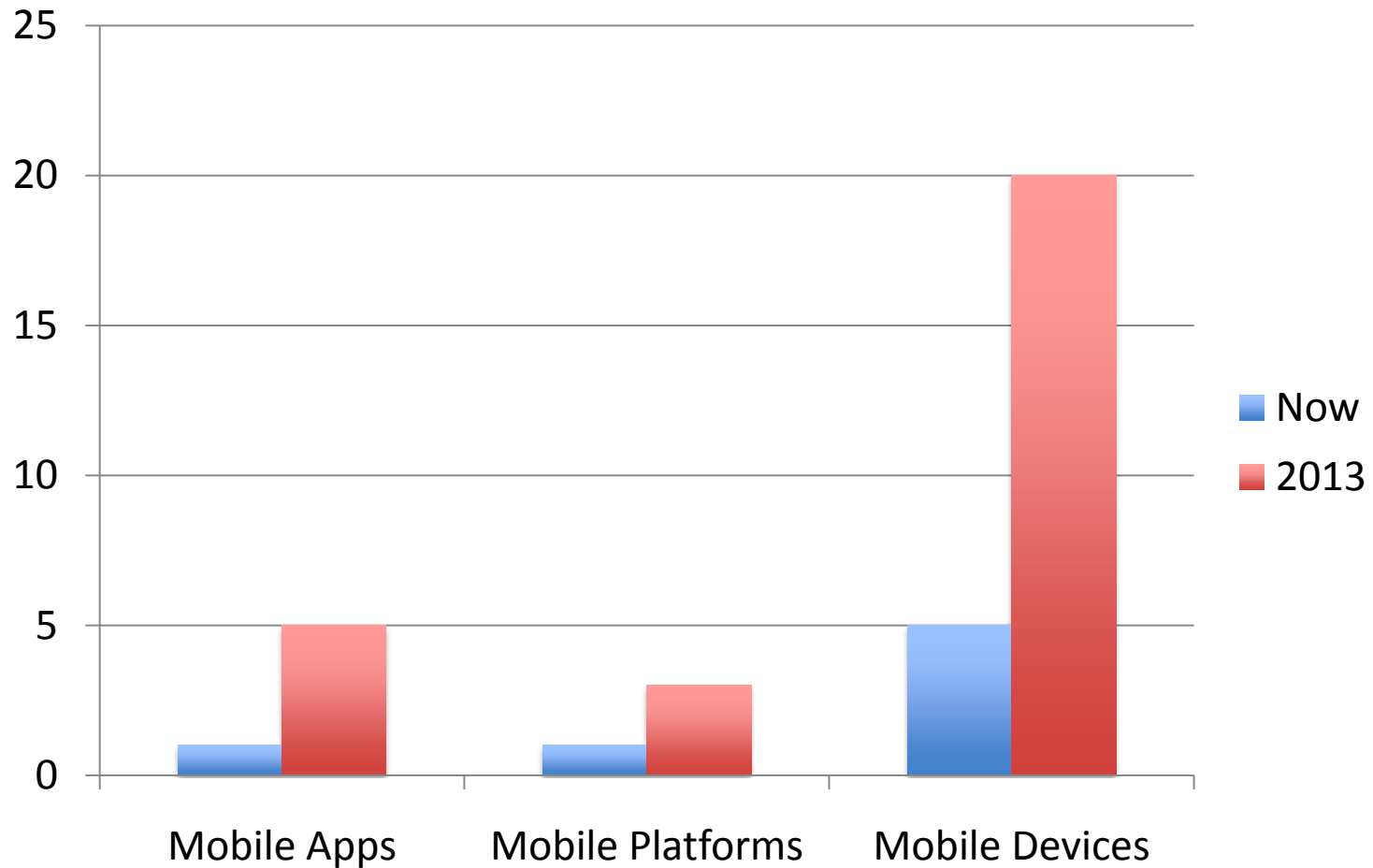
- Michael A. Davis
  - CEO, Savid Technologies
    - IT Security Consulting
    - Risk Assessments/Auditing
    - Security Remediation
  - Speaker at Major Security Conferences
    - Defcon, CanSecWest, Toorcon, Hack In The Box
  - Open Source Software Developer: Snort, Nmap, Dsniff
  - Hacking Exposed Author
  - InformationWeek Contributor



# Mobility Struggles

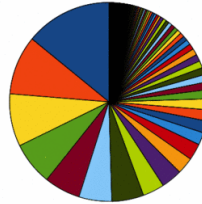


# Mobile Struggles



# But...

Android TweetDeck Beta Users by Phone



- HTC Dream
- GT-9000
- SD-01B
- HTC Legend
- OPR0C2
- T-Mobile G1
- HTC Dream
- L201
- Q01
- GT-9000M
- SHW-M1010
- htc1004a8
- MSM
- SCH-I890
- Hera
- Devour
- Sis-100
- genaro
- GT-15000
- GT-P1000
- GT-9000
- HTC Vision
- HTC Dream SparkleMod
- CamelPhone
- HTC Desire
- GD02-09
- HTC Desire
- android
- MSA
- Motrola XT720
- midfire
- Google Ion
- HTC Dream :: Destiny ::
- HTC Desire
- Hero
- Neepco'sNerdzStar-Port
- AndroidLamborghini-Evolution
- LUK000
- Desire
- ROMLabs
- soft stone
- htc1003
- Desi-Hi-Pulse-Mini-with-MG-From
- CyanogenMod-Port-by-Neepco
- Super-Dior
- Nexus-NX-A890
- M700
- Droid
- Android
- Milestone
- X10
- SPH-D700
- T-Mobile-myTouch-3G
- X10a
- HTC Tattoo
- GT740
- SHW-M1005
- Evo
- SKY-BA-AD005
- GT-KV8000
- HTC-9000B
- Milestone-XT720
- Orange-San-Francisco
- Plain-Bit-Dream
- htc1004a800
- chromatic Dream
- Fu990
- U8100
- Tattoo
- Nokia N900
- EvoS
- Droid Incredible
- Android-for-Telechip-TC08900-Evaluation-Board
- HTC Magic SparkleMod
- htc
- HTC Magic SparkleMod
- HTC Magic SparkleMod
- google\_asp
- SPH-A800(AndroidMobileSupport.com)
- T-Mobile-myTouch-3G
- htc1004a-SuperBad-G1
- DevilWan
- Evo-G1
- TESTTEL-Mot1.1
- Hero
- Neepco'sNerdzStar-Port
- AndroidLamborghini-Evolution
- salgany
- android-mr-in
- Cyano-Taz2-froyo
- Garmin-Asus-A10
- GT-15000L
- Cyanogen-Taz2-2.0-vanilla
- GT-720
- SXA-Magic-GlassRider-Port
- Android2
- Droid-2-Global
- M700
- Supra
- HTC Hero
- A863
- HTC Wildfire
- SAHMSUNG-SGH-887
- SCH-I500
- T-Mobile-G2
- XOLO-T
- E10
- FroyoEvo
- SPH-BA-6500
- SHW-M130L
- ASMA
- Incredible
- GT-15000
- U7500
- Behold-II
- MSB01
- U8110
- Acer-Liquid
- Android-Dev-Phone-1
- Chromatic-Magic
- p901a
- Botan
- Imobile-856
- Ultimate-Droid
- htc1004a-SuperFly-3G
- htc
- htc
- Android-for-Telechip-TC08902-Tablet-PC
- htc1004a-SuperFly-3G
- HTC Hero
- Full-Android-on-Vogue
- Aras-Nexus-One
- M501
- LG-P900
- U8500
- BTX's-GammaFly-3G
- HT860
- Motrola-KT502
- Garmin-Asus-A10
- GT-15000L
- SmartGT7
- KT800C
- GSman-G1-300
- MSB20
- HT8580
- HTC Hero
- HERC2000
- Evo
- KT720
- L2200
- Aly
- Dial-Break
- Luigi
- Orange-HT-G0A
- P999400
- GT-6000
- Moto-Droid
- KT800W
- Desire-HD
- Galaxy
- Vodafone-845
- UR20
- MSB02
- MSB02
- Froyo-Mini
- GT-8700R
- Froyo-Taz2
- SP-Photo-on-HTC-Tattoo
- HTC-Ara-A8380
- M8511
- BA-99008
- GT-8800
- CTE-RACEER
- htc
- htc1004a-SuperBad-3G
- SHW-M185S
- SK-5100
- HTC Dream G1
- SC-FC
- HTC Brain-Magic
- PandoraDroid-Tab-by-JesterDroid
- iPhoneD3
- Cyano-Taz2-3.0
- HTC-Bit-Dream
- CyanogenMod-Port-by-Neepco
- Atatched-pdx
- My-Phone-Bitch
- my-Shellz
- MB800
- HTC-G1
- UD-PoolBoy-BLACK
- DIRC0X
- SGH-T999
- HTC Magic
- GT-6100
- T-Mobile-myTouch-3G-Slide
- SPH-A890
- MSB20
- HTC HD2
- Orange-HT-G0A
- P999400
- GT-6000
- Moto-Droid
- KT800W
- Desire-HD
- Galaxy
- Vodafone-845
- UR20
- MSB02
- MSB02
- Froyo-Mini
- GT-8700R
- Froyo-Taz2
- SP-Photo-on-HTC-Tattoo
- HTC-Ara-A8380
- M8511
- BA-99008
- GT-8800
- CTE-RACEER
- htc
- htc1004a-SuperBad-3G
- SHW-M185S
- SK-5100
- HTC Dream G1
- SC-FC
- HTC Brain-Magic
- PandoraDroid-Tab-by-JesterDroid
- iPhoneD3
- Cyano-Taz2-3.0
- HTC-Bit-Dream
- CyanogenMod-Port-by-Neepco
- Atatched-pdx
- My-Phone-Bitch
- my-Shellz
- MB800
- HTC-G1
- UD-PoolBoy-BLACK
- PC9100
- HTC Hero
- A863
- HTC Wildfire
- SAHMSUNG-SGH-887
- SCH-I500
- T-Mobile-G2
- XOLO-T
- E10
- FroyoEvo
- SPH-BA-6500
- SHW-M130L
- ASMA
- Incredible
- GT-15000
- U7500
- Behold-II
- MSB01
- U8110
- Acer-Liquid
- Android-Dev-Phone-1
- Chromatic-Magic
- p901a
- Botan
- Imobile-856
- Ultimate-Droid
- htc1004a-SuperFly-3G
- htc
- htc
- Android-for-Telechip-TC08902-Tablet-PC
- htc1004a-SuperFly-3G
- HTC Hero
- Full-Android-on-Vogue
- Aras-Nexus-One
- M501
- LG-P900
- U8500
- BTX's-GammaFly-3G
- HT860
- Motrola-KT502
- Garmin-Asus-A10
- GT-15000L
- SmartGT7
- KT800C
- GSman-G1-300
- MSB20
- HT8580
- HTC Hero
- HERC2000
- Evo
- KT720
- L2200
- Aly
- Dial-Break
- Luigi
- Orange-HT-G0A
- P999400
- GT-6000
- Moto-Droid
- KT800W
- Desire-HD
- Galaxy
- Vodafone-845
- UR20
- MSB02
- MSB02
- Froyo-Mini
- GT-8700R
- Froyo-Taz2
- SP-Photo-on-HTC-Tattoo
- HTC-Ara-A8380
- M8511
- BA-99008
- GT-8800
- CTE-RACEER
- htc
- htc1004a-SuperBad-3G
- SHW-M185S
- SK-5100
- HTC Dream G1
- SC-FC
- HTC Brain-Magic
- PandoraDroid-Tab-by-JesterDroid
- iPhoneD3
- Cyano-Taz2-3.0
- HTC-Bit-Dream
- CyanogenMod-Port-by-Neepco
- Atatched-pdx
- My-Phone-Bitch
- my-Shellz
- MB800
- HTC-G1
- UD-PoolBoy-BLACK
- PC9100
- HTC Hero
- A863
- HTC Wildfire
- SAHMSUNG-SGH-887
- SCH-I500
- T-Mobile-G2
- XOLO-T
- E10
- FroyoEvo
- SPH-BA-6500
- SHW-M130L
- ASMA
- Incredible
- GT-15000
- U7500
- Behold-II
- MSB01
- U8110
- Acer-Liquid
- Android-Dev-Phone-1
- Chromatic-Magic
- p901a
- Botan
- Imobile-856
- Ultimate-Droid
- htc1004a-SuperFly-3G
- htc
- htc
- Android-for-Telechip-TC08902-Tablet-PC
- htc1004a-SuperFly-3G
- HTC Hero
- Full-Android-on-Vogue
- Aras-Nexus-One
- M501
- LG-P900
- U8500
- BTX's-GammaFly-3G
- HT860
- Motrola-KT502
- Garmin-Asus-A10
- GT-15000L
- SmartGT7
- KT800C
- GSman-G1-300
- MSB20
- HT8580
- HTC Hero
- HERC2000
- Evo
- KT720
- L2200
- Aly
- Dial-Break
- Luigi
- Orange-HT-G0A
- P999400
- GT-6000
- Moto-Droid
- KT800W
- Desire-HD
- Galaxy
- Vodafone-845
- UR20
- MSB02
- MSB02
- Froyo-Mini
- GT-8700R
- Froyo-Taz2
- SP-Photo-on-HTC-Tattoo
- HTC-Ara-A8380
- M8511
- BA-99008
- GT-8800
- CTE-RACEER
- htc
- htc1004a-SuperBad-3G
- SHW-M185S
- SK-5100
- HTC Dream G1
- SC-FC
- HTC Brain-Magic
- PandoraDroid-Tab-by-JesterDroid
- iPhoneD3
- Cyano-Taz2-3.0
- HTC-Bit-Dream
- CyanogenMod-Port-by-Neepco
- Atatched-pdx
- My-Phone-Bitch
- my-Shellz
- MB800
- HTC-G1
- UD-PoolBoy-BLACK

Platform fragmentation makes effective risk reduction and management just about impossible without a heterogeneous device management platform

## Determine Your Risk

- Always think sensitive data protection & compliance
- Develop & enforce mobile policy from the get go!!
- Your risk is unique depending on use of mobile apps
- Priority e-mail → calendar → contacts → device
- Use DLP to prevent sensitive data from reaching email in the first place
- Tablets should use RDP/Citrix to access “rich” applications

# Mobile Device Risks at Every Layer

## NETWORK

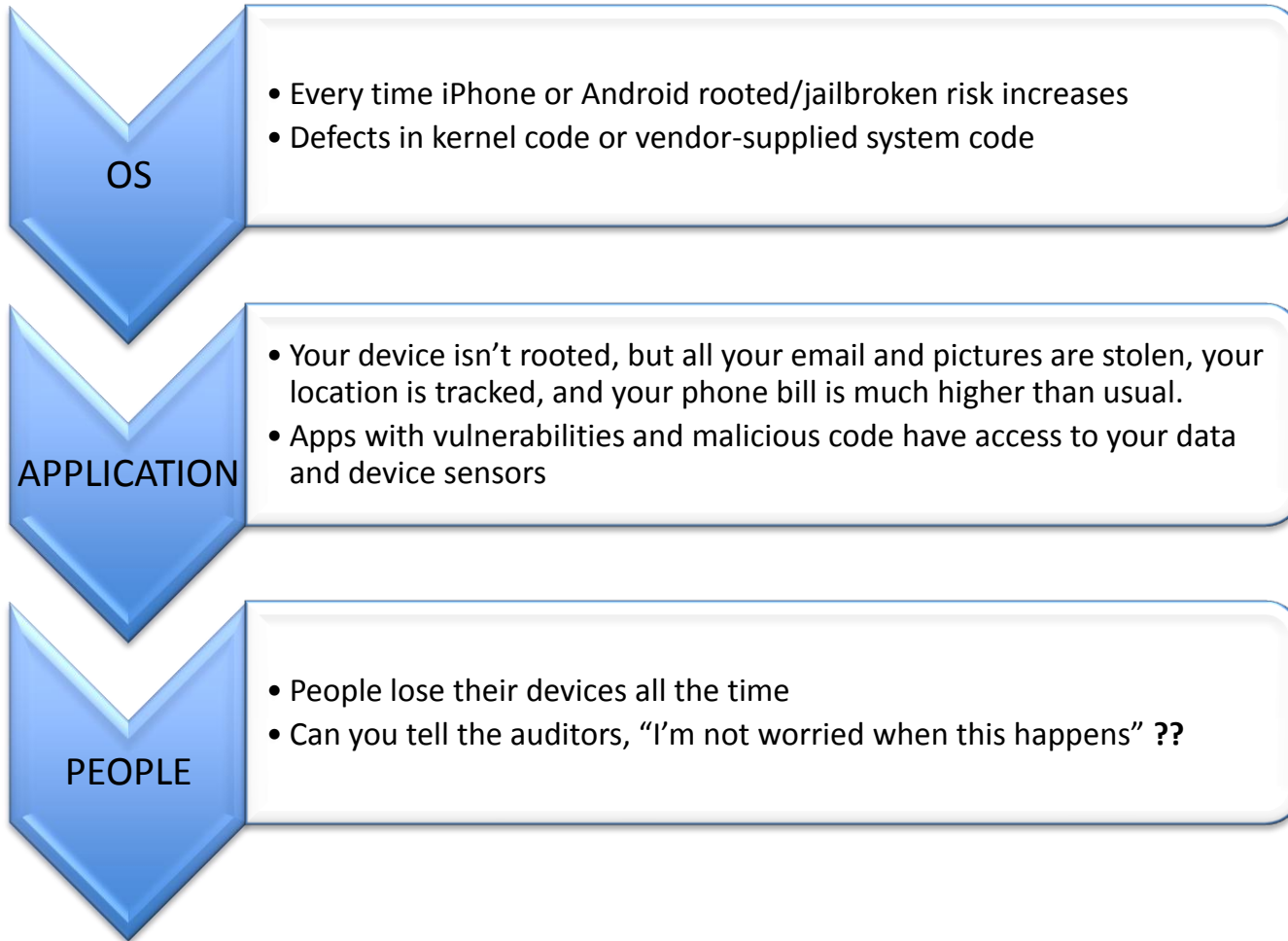
- Data interception
- WiFi has all the same problems as laptops
- GSM has shown some cracks. Chris Paget demo DEFCON 2010

## HARDWARE

- Baseband layer attacks
- Memory corruption defects in firmware used to root your device
- Demonstrated at Black Hat DC 2011 by Ralf-Philipp Weinmann



# Mobile Device Risks at Every Layer



# Mobile App Ecosystem

Mobile platform providers have different levels of controls over their respective ecosystems

Platform	Signing	Revocation	Approval
Android	Anonymous, self-signed	Yes	No
iOS	Signed by vendor	Yes	Policy & quality
Blackberry	Signed with vendor issued key	Yes	No
Windows Phone	Signed by vendor	Yes	Policy, quality & security
Symbian	Signed by vendor	Yes	Quality

# Why a Top 10 Mobile App Risks?

- Mobile Apps need their own list.
  - Modern mobile applications run on mobile devices that have the functionality of a laptop running a general-purpose operating system.
  - *But* mobile devices are not just small computers. Mobile devices are designed around personal and communication functionality, which makes the top mobile applications risks different from the top traditional computing risks.
- Risks can be maliciously designed or inadvertent.
- Designed to educate developers and security professionals about the mobile application behavior that puts users at risk.
- Use Top 10 to determine the coverage of a mobile security solution
  - Development of an app
  - Acceptance testing of an app
  - App store vetting process
  - Security software running on a mobile device.

# The Top 10 List....

## Malicious Functionality

1. Activity monitoring and data retrieval
2. Unauthorized dialing, SMS, and payments
3. Unauthorized network connectivity (exfiltration or command & control)
4. UI Impersonation
5. System modification (rootkit, APN proxy config)
6. Logic or time bomb

## Vulnerabilities

7. Sensitive data leakage (inadvertent or side channel)
8. Unsafe sensitive data storage
9. Unsafe sensitive data transmission
10. Hardcoded password/keys



# Activity monitoring and data retrieval

- Risks:
  - Sending each email sent on the device to a hidden third-party address
  - Listening in on phone calls or simply open microphone recording
  - Stored data, contact list or saved email messages retrieved
- The following are examples of mobile data that attackers can monitor and intercept:
  - Messaging (SMS and Email)
  - Audio (calls and open microphone recording)
  - Video (still and full-motion)
  - Location
  - Contact list
  - Call history
  - Browsing history
  - Input
  - Data files



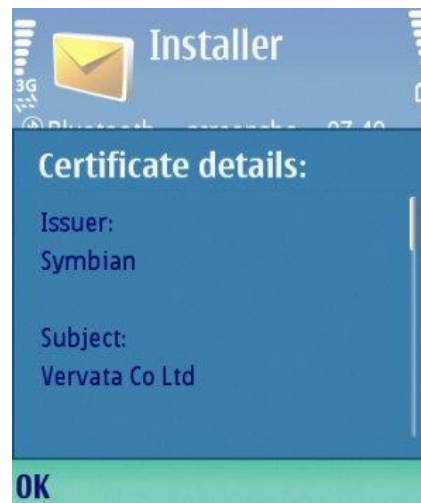
# Activity monitoring and data retrieval

Secret SMS Replicator for Android

<http://www.switched.com/2010/10/28/sms-replicator-forwards-texts-banned-android/>

RBackupPRO for Symbian

[http://www.theregister.co.uk/2007/05/23/symbian\\_signed\\_spyware/](http://www.theregister.co.uk/2007/05/23/symbian_signed_spyware/)



# Unauthorized dialing, SMS, and payments

- Directly monetize a compromised device
- Premium rate phone calls, premium rate SMS texts, mobile payments
- SMS text message as a spreading vector for worms.

Premium rate SMS – Trojan-SMS.AndroidOS.FakePlayer.  
[https://www.computerworld.com/s/article/9180561/N\\_texts\\_premium\\_rate\\_numbers](https://www.computerworld.com/s/article/9180561/N_texts_premium_rate_numbers)



Premium rate phone call –Windows Mobile Troj/Terdial-A  
<http://nakedsecurity.sophos.com/2010/04/10/windows-mobile-terdial-trojan-expensive-phone-calls/>

# Exfiltration or command & control

- Spyware or other malicious functionality typically requires exfiltration to be of benefit to the attacker.
- Mobile devices are designed for communication. Many potential vectors that a malicious app can use to send data to the attacker.
- The following are examples of communication channels attackers can use for exfiltration and command and control:
  - Email
  - SMS
  - HTTP get/post
  - TCP socket
  - UDP socket
  - DNS exfiltration
  - Bluetooth
  - Blackberry Messenger

# UI impersonation

- Similar to phishing attacks that impersonate website of user's bank or online service.
- Web view applications on the mobile device can proxy to legitimate website.
- Malicious app creates UI that impersonates that of the phone's native UI or the UI of a legitimate application.
- Victim is asked to authenticate and ends up sending credentials to an attacker.

Proxy/MITM 09Droid Banking apps

<http://www.theinquirer.net/inquirer/news/1585716/fraud-hits-android-apps-market>

# System modification (rootkit, APN proxy)

- Malicious applications will often attempt to modify the system configuration to hide their presence. This is often called rootkit behavior.
- Configuration changes also make certain attacks possible. An example is modifying the device proxy configuration or APN (Access Point Name).

Android “DroidDream” Trojans Rootkit Phone

<http://www.androidpolice.com/2011/03/01/the-mother-of-all-android-malware-has-arrived-stolen-apps-released-to-the-market-that-root-your-phone-steal-your-data-and-open-backdoor>

## Logic or Time Bomb [CWE-511]

Logic or time bombs are classic backdoor techniques that trigger malicious activity based on a specific event, device usage or time.



# Sensitive data leakage [CWE-200]

- Sensitive data leakage can be either inadvertent or side channel.
- A legitimate app's usage of device information and authentication credentials can be poorly implemented, thereby exposing this sensitive data to third-parties.
  - Location
  - Owner ID info: name, number, device ID
  - Authentication credentials
  - Authorization tokens

Sensitive data leakage -Storm8 Phone Number Farming

<http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html>

Android "DroidDream" Trojans steal data

<http://www.androidpolice.com/2011/03/01/the-mother-of-all-android-malware-has-arrived-stolen-apps-released-to-the-market-that-root-your-phone-steal-your-data-and-open-backdoor>

# Unsafe sensitive data storage [CWE-312]

- Mobile apps often store sensitive data, such as banking and payment system PIN numbers, credit card numbers, or online service passwords.
- Sensitive data should always be stored encrypted so that attackers cannot simply retrieve this data off of the file system.
- It should be noted that storing sensitive data without encryption on removable media such as a micro SD card is especially risky.

Citibank insecure storage of sensitive data

[http://www.pcworld.com/businesscenter/article/201994/citi\\_iphone\\_app\\_flaw\\_raises\\_questions\\_of\\_mobile\\_security.html](http://www.pcworld.com/businesscenter/article/201994/citi_iphone_app_flaw_raises_questions_of_mobile_security.html)

Wells Fargo Mobile application 1.1 for Android stores a username and password, along with account balances, in clear text.

<http://osvdb.org/show/osvdb/69217>

# Unsafe sensitive data transmission [CWE-319]

- It is important that sensitive data is encrypted in transmission lest it be eavesdropped by attackers.
- Mobile devices are especially susceptible because they use wireless communications exclusively and often public Wi-Fi, which is known to be insecure.
- SSL is one of the best ways to secure sensitive data in transit.
  - Beware of downgrade attack if it allows degrading HTTPS to HTTP.
  - Beware of not failing on invalid certificates. This would enable a man-in-the-middle attack.



# Hardcoded password/keys [CWE-798]

- The use of hardcoded passwords or keys is a shortcut sometimes employed by developers to make the app easier to implement, support or debug.
- Once this hardcoded password is discovered through reverse engineering it renders the security of the application or the systems it authenticates to with this password ineffective.

Mastercard sample code:

<http://jack-mannino.blogspot.com/2011/02/scary-scary-mobile-banking.html>

```
final String companyId = "your-company-id-here";  
final String companyPassword = "your-company-  
password-here";
```

# Strategy

- Form a cross-functional mobility council. Engage end users – “consumerization.”
- Prioritize goals & establish mobility plan.
- Determine applications that can be used.
- Make the plan part of approved policy.
  - Define policy
  - Document end user license agreement
  - Define who pays for the device (all/none/partial subsidy)
  - Establish data security & management controls
  - Deployment with proper tools

# Strategy

- Think outside the box. At minimum, entertain cutting-edge MDM vendors with new ideas.
- MDM software can lessen the blow of multi-platform madness. Ultimately makes multi-platform management cheaper and more effective!



# Tactics

- Enroll devices in a controlled fashion vs. free-for-all.
- Control device access to corporate network.
  - ActiveSync, Wi-Fi, VPN
- Enforce user-to-device authentication with pin code
- Set full or partial “lock/wipe” policies depending on who owns the device.
- Be leery of platforms without embedded crypto. Encrypt devices and data cards, when possible.
- Deliver firewall and antivirus capabilities, if possible.
- Whitelist mobile applications.

## The Basics – ActiveSync

- Since most back-end email systems are based on MS Exchange, it's a convenient place to push policies.
- ActiveSync provides the basics of device mgmt
  - Windows Mobile/Phone
  - Apple
  - Nokia
  - Android
  - Palm
- BlackBerry is done via Blackberry Enterprise Server

# The Basics – ActiveSync

- ActiveSync features vary by phone platform and the version of Exchange you use
- Users can be enrolled in ActiveSync ... meaning it's off for everyone until turned on for individuals.
- Email / calendar / contacts / tasks pushing and sync
- Full device wipe
- Device passwords
- Encrypted storage cards
- Bandwidth reductions
- Disable Wi-Fi / Bluetooth

And more...

# I Want My MDM

- Maybe ActiveSync does not offer enough control?
- Mobile device management platforms from a wide array of vendors offer all sorts of control
- Before buying:
  - Do your research well.
  - MDM must support the major platforms *not* just 1 or 2.
  - Don't always take the first offer. Look at three minimum.
  - **Attempt to identify the visionaries**
  - Determine your business requirements and how they fit
  - Verify vendor financial viability
- This space is moving fast

# MDM Approach Examples

- Talked with some recent Gartner leaders to get a feel for what they offer
- This is not an advertisement
- No particular order

## MDM Approach Example: Boxtone

- Multi-platform mobile *service* management (MSM)
- Focused on 1) device control 2) device support 3) ops mgmt leveraging its own gateway, BES, ActiveSync
- Technology is (mostly) agent-less. Infrastructure traffic collectors near VPN and firewall use sniffing and analyses to determine mobile device activities. Apple, BB, and Windows native MDM hooks are licensed.
- Boxtone Speaks:
  - “The current industry obsession is device management, but app management and app security is where it’s going.”
  - “Independent app security with policies per app container.”

## MDM Approach Example: AirWatch

- Multi-platform MDM that uses agent software
- Comprehensive control & features across all major platforms.
- Company excels at massive automated rollouts
- Architecture permits for large scale control across customer divisions that can all rollup to one screen
- SDK framework for adding “mini sandbox” for apps
- AirWatch speaks:
  - “It used to be all about device management but now it’s about that *and* application security.”

# MDM Approach Example: MobileIron

- Multi-platform MDM that uses agent software
- Multiple policies can be employed to monitor for situations that exceed permitted bounds. Ex: “If you jailbreak your device, you can’t VPN to Corp.”
- Comprehensive control & features across all major platforms. User self-servicing.
- MobileIron speaks:
  - “Prepare to support three mobile OS platforms!”
  - “IT should not be surprised that lines of business are building apps. IT can turn from being a blocker to an enabler.”

## MDM Approach Example: GOOD

- Multi-platform MDM that uses agent software
- Creates an encrypted “sandbox” environment through which users interact with their corporate data via the GOOD infrastructure:
  - Email
  - Contacts
  - Calendaring
  - Secure web browsing
- Container can be wiped remotely if needed.

## MDM Approach Example: Zenprise

- Multi-platform MDM that uses an agent software
- Views competition as security “configurators” but says they have that plus app-centric services
- Developed app tunnel security architecture similar to BB. No VPN client needed.
- Interesting features:
  - Disable camera if within 500 feet of certain coordinates
  - App communication compression
  - Private apps stores for all major platforms

# Thank You for Attending

Watch for our research report on Mobile Device Management this fall in *InformationWeek* and on our site, at [analytics.informationweek.com](http://analytics.informationweek.com)

# Thank You!



Grant P. Moerschel  
WaveGard, Inc.  
[gm@wavegard.com](mailto:gm@wavegard.com)  
(703) 568-5077

Michael A. Davis  
Savid Technologies  
[mdavis@savidtech.com](mailto:mdavis@savidtech.com)  
(708) 243-2850



**InformationWeek**  
::analytics

