

16th Annual New York State Cyber Security Conference



Mobile Security (not MDM) Understanding the Real Risk

Eric S Green
SVP, Mobile Active Defense
Program Director, SC Magazine



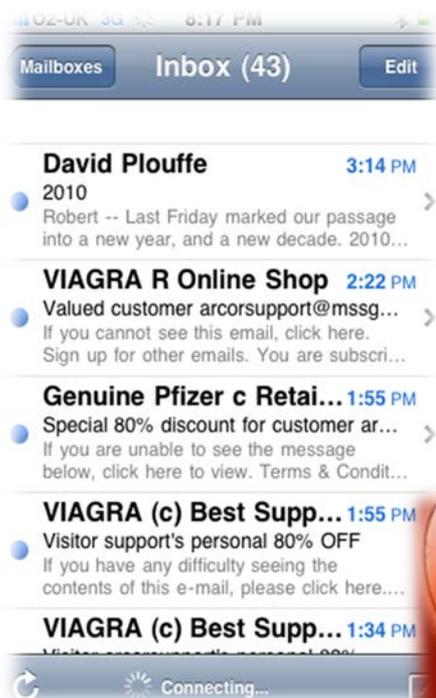
Key Points

- The real threats to mobile devices
- Apps, apps and more apps
- Personal email
- Data in motion
- BYO What??!!
- Sandboxing
- Plain old MDM
- BYOD Mobile Security Spectrum
- The Perfect Storm
- What's really happening out there?
- Summary and recommendations
- Specific things to look for



The Real Threats to Devices

Malicious content = bad apps, web sites, spam, OS hacking & security that can be turned off



JailbreakMe

by comex (et al.)

JailbreakMe
Jailbreak to get tweaks and apps
Apple won't allow in the App Store.
Free, legal, safe.
You should sync with iTunes before
using this tool.

More Info »

slide to jailbreak



The App Problem

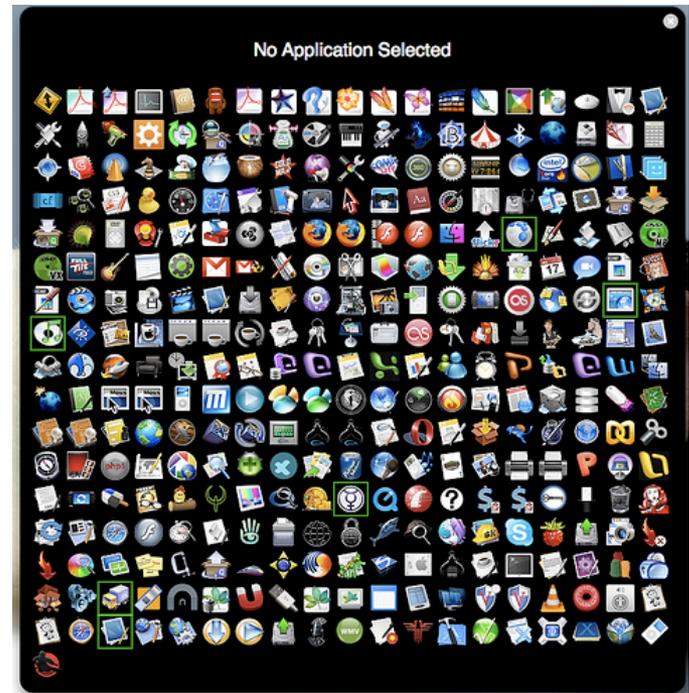
“App stores are the number one malware delivery mechanism ever created by mankind.”

- Rob Smith, CTO, Mobile Active Defense



The App Problem cont.

- No effective vetting process
 - App stores do not code review
 - Droid store is Wild West of infected apps
- Users do not know what they are downloading
- Echo enterprise policy?
 - Download no apps that are not approved
- Smart phone social engineering
 - Automated voice phishing
 - Text-based phishing





ANGRY BIRDS SPACE

AVAILABLE NOW

Available on the App Store
iOS

ANDROID APP ON Google play
ANDROID

SHOP
PC

Available on the Mac App Store
MAC



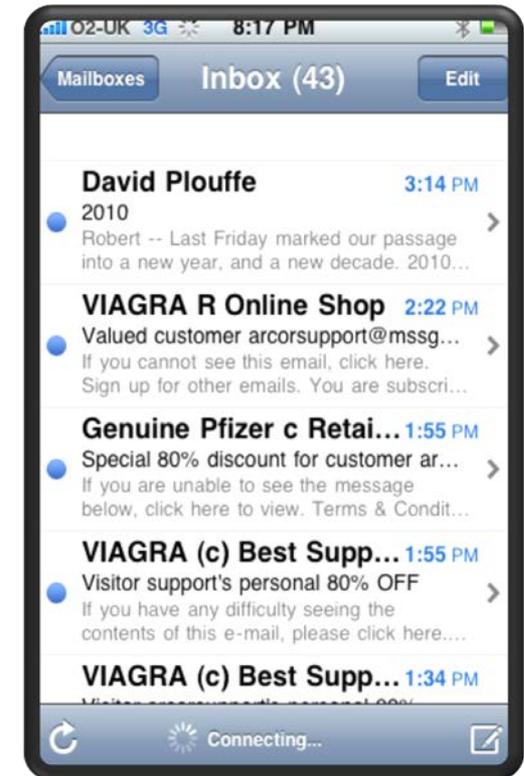
ANGRY BIRDS SPACE



Mobile Email Problems

- Mobile email security should be just as strong as internal network controls.
- Personal email bypasses enterprise security exposing the corporate network to unknown threats
- 70-95% of all mobile email is unwanted.
 - Minimal SPAM and virus protection.
 - Limited malware or phishing detection
- Emails are often too big for mobile device, consume bandwidth and can not be read.
- Can employees check personal email (i.e, Yahoo and Gmail) from their company smart phone
- Survey: 85% of Employees Under 25 Use Personal E-Mail Accounts for Work

<http://www.readwriteweb.com/enterprise/2011/02/survey-85-of-employees-under-25.php>



Data in Motion

- Industry standard is IPsec
- So why do vendors use SSL?
- Cheaper, easier, less 'complex'
- SSL spoofing is inherently one of the most potent Man-In-The-Middle attacks because it allows for exploitation of services that people assume to be secure.



The Scary Search Engine

Shodan (www.shodanhq.com) is a free, open source hacking tool for the Industrial Internet

SHODAN

Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR

FREE SIGN UP

Popular Search Queries: **default password** - Finds results with "default password" in the banner; the named defaults might work!

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.



Apples Almost iOS VPN Changes

<http://support.apple.com/kb/TS4550>

Symptoms

Due to a lawsuit by VirnetX, Apple will be changing the behavior of VPN On Demand for iOS devices using iOS 6.1 and later.

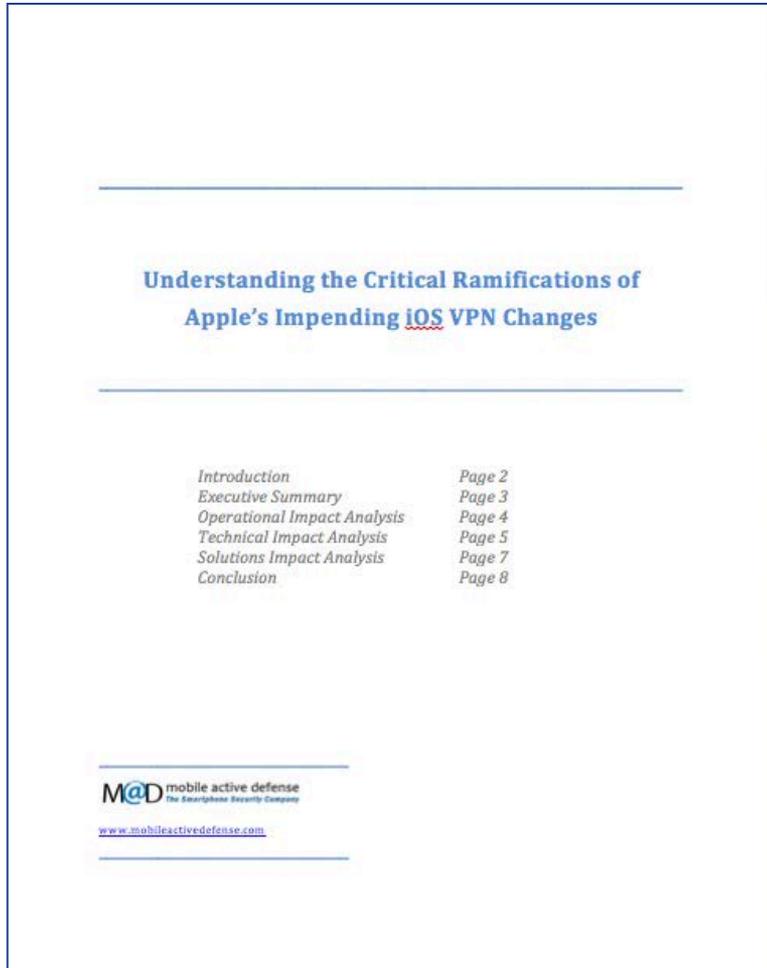
Devices using iOS 6.1 and later with VPN On Demand configured to "Always" will behave as if they were configured with the "Establish if needed" option. The device will establish a VPN On Demand connection only if it is unable to resolve the DNS name of the host it is trying to reach. This change will be distributed in an update later this month.

If the name of a host can be resolved without a VPN connection, you may see one of the following behaviors:

- If the host is a web server that presents different content to internal and external users, the VPN On Demand connection will not be established and you will see the external content.
- If the host is a web or mail server that has a name that can be resolved externally but cannot be contacted externally, the VPN On Demand connection will not be established and you will not be able to connect to the server.
- If you are using a public DNS service that provides an alternative IP address for hosts that it cannot resolve, the VPN On Demand connection will not be established and you will not be able to connect to the server.
- If you are using a VPN configuration that includes wildcard entries (such as *.com) that match top-level domains that are publicly accessible, the VPN On Demand connection will not be established when you contact hosts in those domains.



Download the White Paper



www.mobileactivedefense.com/wp-content/uploads/2013/04/ios-ondemand-vpn-WP.pdf



Apples Almost iOS VPN Changes

<http://support.apple.com/kb/TS4550>



iOS 6.1: About VPN On Demand

Products Affected

iPad, iPhone, iPod touch

Symptoms

This is an update to an article describing potential changes to the behavior of VPN On Demand due to a lawsuit by VirnetX.

Resolution

Apple no longer plans to change the behavior of the VPN On Demand feature of iOS 6.1 for devices that have already been shipped. The "Always" option will continue to work as it currently does on these devices.

Important: Information about products not manufactured by Apple is provided for information purposes only and does not constitute Apple's recommendation or endorsement. Please [contact the vendor](#) for additional information.



BYO What??!

Definition of personally owned device:

Any device capable of storing corporate data and/or connecting to an organizations network is bound by the acceptable use policy.



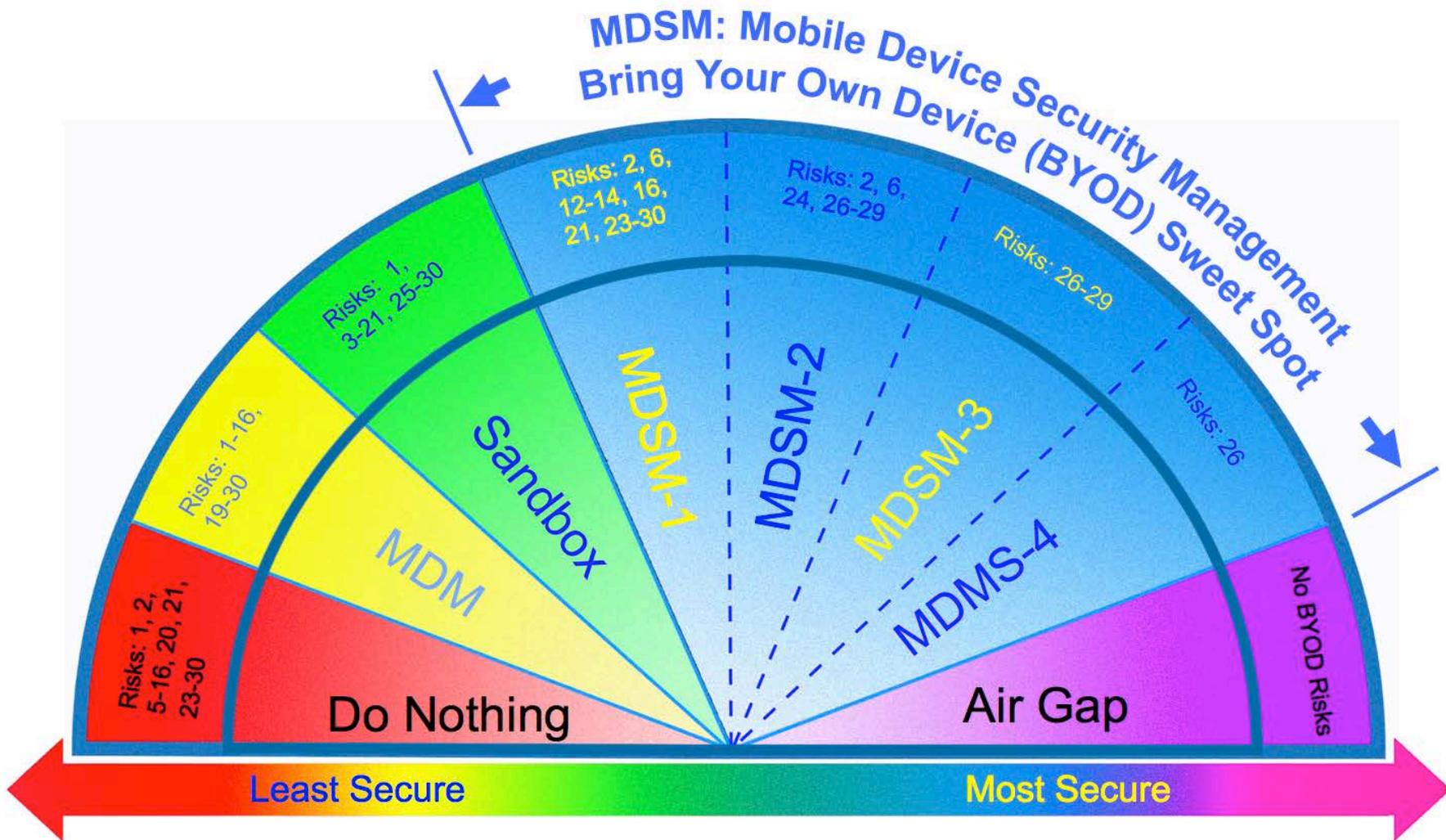
BYOD: Containers/Sandboxes

- Custom APIs & SDKs
 - Browser
 - Email
 - Apps
- Does not protect device – just a small piece
- SSL is weak crypto
- Single Point of Failure
 - No defense in depth
 - Future cracks





BYOD Mobile Security Spectrum



Key Risks

Risk ID #	Mobile BYOD Risk Description	Do Nothing	MDM	Sandbox	MDMS-1	MDSM-2	MDSM-3	MDSM-4	Air Gap
1	Risk of Password & Credentials Interception	x	x	x					
2	Risk of Comingling Personal & Company Data	x	x		x	x			
3	Risk of User Bypassing/Disabling Security Controls		x	x					
4	Risk of ID Spoofing (Unknown Devices) and Audit Control (no-CA)		x	x					
5	Risk from No Trust Model	x	x	x					
6	Risk of Company Data Breach	x	x	x	x	x			
7	Risks of WiFi Data Eavesdropping	x	x	x					
9	Risk of Carrier (3G/4G) Data Interception	x	x	x					
8	Risk of VoIP Interception	x	x	x					
10	Risk of Application Data Eavesdropping	x	x	x					
11	Risk from Lack of IDS/IPS & Remediation	x	x	x					
12	Risk from Phishing	x	x	x	x				
13	Risk of Malware Breaches	x	x	x	x				
14	Risk of Malware Download	x	x	x	x				
15	Risk of No Device Lock Down or Mobile Firewall	x	x	x					
16	Risk of Becoming Part of Mobile Botnet	x	x	x	x				
17	Risk of User Misusing Non-Native Apps			x					
18	Risk of User Error in App Configuration			x					
19	Risk of Man in the Middle Attack (for SSL VPNs)		x	x					
20	Risk of Mobile IP Address Scraping (NAT)	x	x	x					
21	Risk of Falling out of Regulatory Compliance	x	x	x	x				
22	Risk of Delayed Active Sync Response		x						
23	Risk of 3rd Party Data Exposure from Lost Device (FDE)	x	x		x	x			
24	Risk of Company Liability for Loss/Disclosure of User Data	x	x		x				
25	Risk of BYOD Breaches	x	x	x	x	x	x	x	
26	Risk From Device Policy Not Changing With Device Location	x	x	x	x	x	x		
27	Risk of Violating Policy When Travelling to Restricted Locations	x	x	x	x	x	x		
28	Risk of Exposing PII When Not on Premises (Fin., Med, Gov, etc.)	x	x	x	x	x	x		
29	Risk of Not Using DLP	x	x	x	x				
30	Risk of Inadequate audit and forensics records (SIEM)	x	x	x	x				

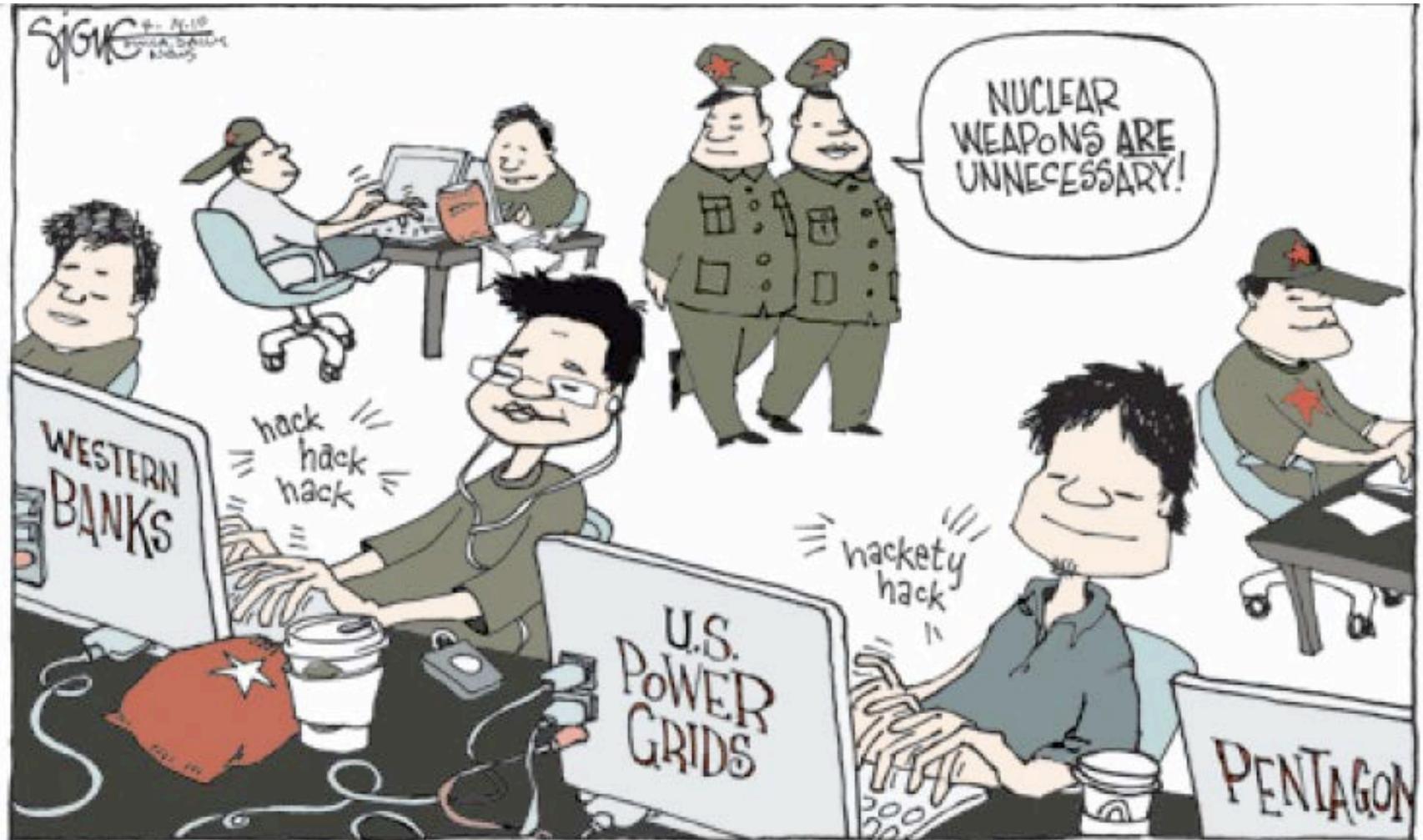


Thus, The Perfect Storm

- **Billions of intelligent mobile endpoints**
- **An inherently insecure backbone infrastructure**
- **Clueless users**
- **Smart bad guys**



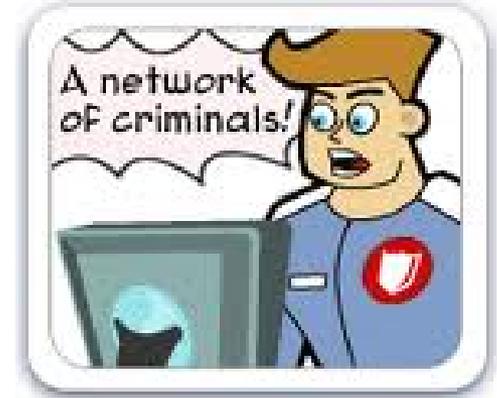
Nation-State Actors



Hactivists



Organized Crime



Online fraud

crippled customers of online...

victims

credit...



What's really happening out there?

- Was a rush to a solution a year ago
- Organizations stuck just barely managing exchange and sandboxing
- Organizations realizing that despite what vendors are saying, all devices are not created equally and simple MDM does not solve the bigger issue
- Many start by saying only corporate owned or mostly with some BYOD - end up mostly BYOD
- Many start with just wanting to 'manage' exchange - end up with senior management, etc wanting network access with even BYOD devices



What's really happening out there cont.?



- Large percentage of organizations that bought a MDM product realize it does not provide security and more is being demanded of both smartphones and tablets bringing the need to figure out how to treat them like any other device on the network.
- Requirements coming from IT and IS continue to conflict causing compromise which often increases risk but with no remediation.
- MDM providers and/or organizations are trying to cobble together multiple point solutions to meet their requirements (ie. MDM + Cisco Anywhere Connect + PKI + Content Filtering + AV, etc)
 - Makes matters highly complex which is bad for security, often breaks and no one agrees who's responsibility it is given the number of products involved, etc.
- Supply Chain Risk Management – If your vendor does any coding in China – it has backdoors!



It's a Risk Discussion



Summary and Recommendations

A smartphone security solution should

1. Carefully plan policy and procedures for mobile roll out
2. Treat desktops, laptops, smartphones and tablets the same
3. Work for both corporate and personally owned devices
4. Provide blacklisting and remediation for bad apps
5. Have the ability to either clean personal email or prevent it
6. Ensure user cannot remove or disrupt
7. Offer jail break and rogue behavior detection & remediation
8. Support multiple platforms via single console
9. Encrypt and force all traffic to VPN when required
10. Have PKI / Certificate Authentication



Specific things to look for

- Can the mobile security be turned off by the user from their device? Can user re-enroll whenever they want from a self service portal?
- Access Control: Can administrators track all devices connected to the network AND prevent non-enrolled devices from connecting? (certificate authentication / PKI)
- Are all over the air communications using true IPSec as opposed to simple SSL? (man in the middle attacks)
- Devices being used: Android, iOS and Windows Mobile are not all created equal by any means. If there is a claim a combination of these devices is being used and all have the same level of 'security' – that is not accurate.
- BYOD / Sandbox / Container: Are user groups doing any of these only granted minimal access rights to network resources (ie: mail, calendar, contacts). Are there metrics for the residual risk in allowing most of the device to be un-monitored or secured. Has someone signed off on that risk?



Specific things to look for cont

- Compliance – Are these organizations governed by certain regulatory guidelines including security and privacy, and is the mobile security stance meeting those regulations?
- Is there an incident response plan in place for mobile?
- Are all of the basic controls in place – enforced passwords, ability to wipe device, integrity checks, app store, app blacklisting, etc?
- Continuous monitoring and change management – Pretty reports and charts and seeing minutes used is all well and fine – but not security. If logging – need it real-time or near real-time with ability to monitor and act.



Thank you for your time!

Questions?

mobile active defense



The Smartphone Security Company

Eric Green

egreen@mobileactivedefense.com

914.244.1060



Man-In-The-Middle Attack (MITM)

1. Traffic between the client and web server is intercepted.
2. When an HTTPS URL is encountered the attacker replaces it with an HTTP link and keeps a mapping of the changes.
3. The attacking machine supplies certificates to the web server and impersonates the client.
4. Traffic is received back from the secure website and provided back to the client.

