Thank you iOS 6

BYOD Party Crashers: How to Protect Against Unauthorized Access

Topics

- Definitions
- Statistics
- Risks
- How smartphones can be used against you
  - Dangerous apps
    - Data Exfiltration
    - Web Filter Bypass
- How to protect your assets
  - Policy, Tools, Awareness, Monitor
- Summary

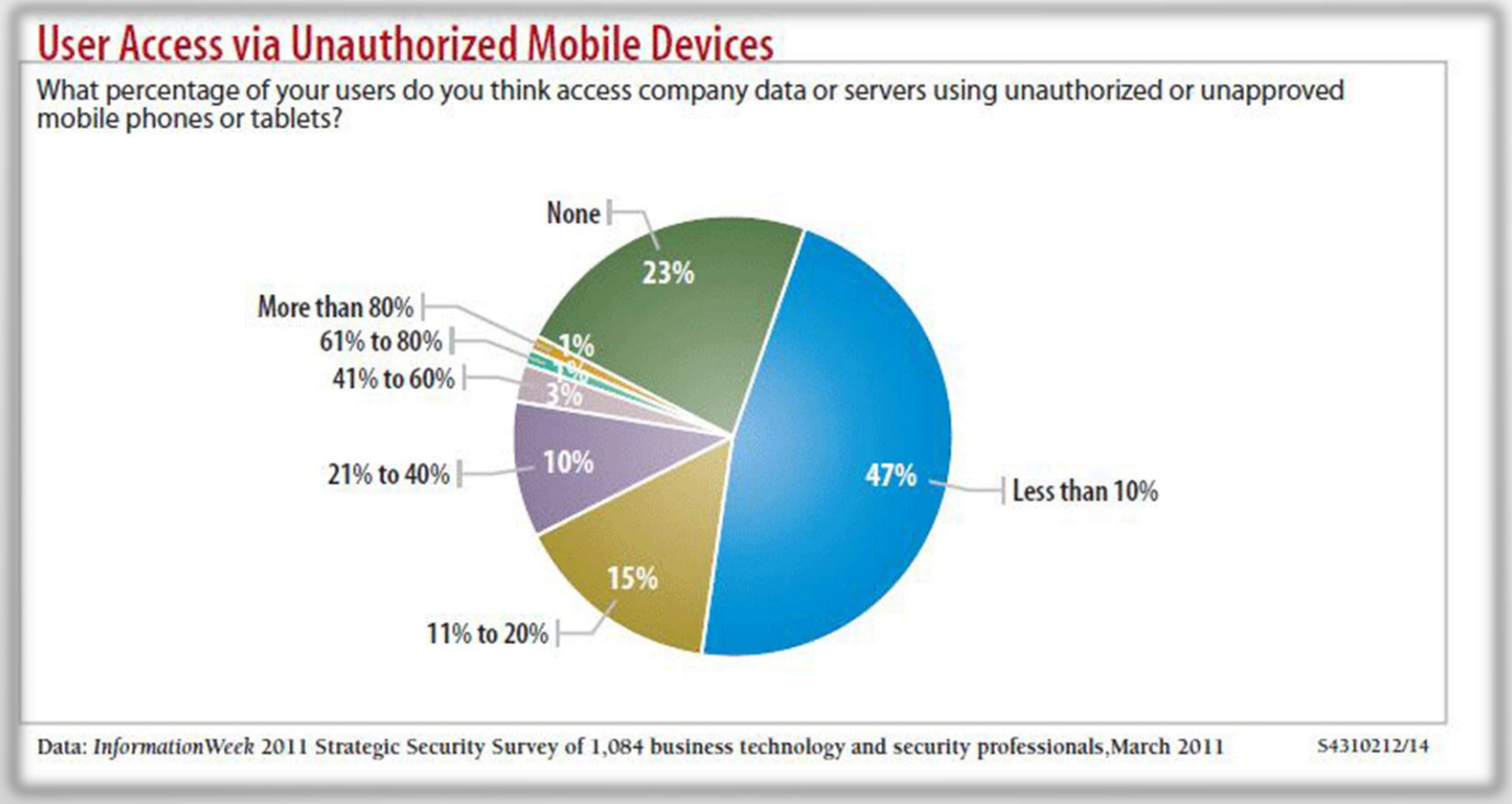
Definitions

- HYOD
  - Here's your own device
    - Most secure of the three
      - Tighter device and app controls
      - Lock down usage, restrict apps
- BYOD
  - Bring your own device
    - More secure
      - Approved Apps
- Unauthorized
  - No policy or a policy that says don't bring/use your own device
    - Unsecure

iphone:# whoami

- Brent Morris
  - Certifications: MCSE, MCSA, CCNA, CCA, APS, A+, ITILv3, CISSP, GCIH, GWAPT, GCIA
  - Work at VyStar Credit Union
    - Information Security Analyst
  - Love to take long walks on the beach . . .

Perception


User Access via Unauthorized Mobile Devices
What percentage of your users do you think access company data or servers using unauthorized or unapproved mobile phones or tablets?
None
23%
More than 80%
1%
61% to 80%
41% to 60%
3%
21% to 40%
10%
47%
Less than 10%
15%
11% to 20%
Data: InformationWeek 2011 Strategic Security Survey of 1,084 business technology and security professionals,March 2011
S4310212/14

Reality

Check Point's global survey of 786 IT Professionals conducted in the US, Canada, UK, Germany and Japan.

- Extensive use of mobile devices connected to corporate networks
  - **89% have mobile devices** connected to corporate networks
  - **Apple iOS** most common devices vs. 2 years ago

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Reality

Check Point's global survey of 786 IT Professionals conducted in the US, Canada, UK, Germany and Japan.

- Extensive use of mobile devices connected to corporate networks
  - **89% have mobile devices** connected to corporate networks
  - **Apple iOS** most common devices vs. 2 years ago
- Personal mobile devices that connect to corporate networks are growing
  - **65% allow personal devices** to connect to corporate networks
  - 78% have more than twice as many personal devices on corporate networks vs.2 years ago

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Reality

Check Point's global survey of 786 IT Professionals conducted in the US, Canada, UK, Germany and Japan.

- Extensive use of mobile devices connected to corporate networks
  - **89% have mobile devices** connected to corporate networks
  - **Apple iOS** most common devices vs. 2 years ago
- Personal mobile devices that connect to corporate networks are growing
  - **65% allow personal devices** to connect to corporate networks
  - 78% have more than twice as many personal devices on corporate networks vs.2 years ago
- Security risks are on the rise because of Mobile Devices
  - **71% say mobile devices** have contributed to **increase security incidents**
  - The **Android** platform is considered to introduce the greatest security risks

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Reality

Check Point's global survey of 786 IT Professionals conducted in the US, Canada, UK, Germany and Japan.

- Extensive use of mobile devices connected to corporate networks
  - **89% have mobile devices** connected to corporate networks
  - **Apple iOS** most common devices vs. 2 years ago
- Personal mobile devices that connect to corporate networks are growing
  - **65% allow personal devices** to connect to corporate networks
  - 78% have more than twice as many personal devices on corporate networks vs.2 years ago
- Security risks are on the rise because of Mobile Devices
  - **71% say mobile devices** have contributed to **increase security incidents**
  - The **Android** platform is considered to introduce the greatest security risks
- Employee behavior impacts security of mobile data
  - 47% report **customer data** is stored on mobile devices
  - **Lack of employee awareness** ranked as greatest impact
  - **72% say careless employees are a greater threat than hackers**

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Reality

Check Point's global survey of 786 IT Professionals conducted in the US, Canada, UK, Germany and Japan.

- Extensive use of mobile devices connected to corporate networks
  - **89% have mobile devices** connected to corporate networks
  - **Apple iOS** most common devices vs. 2 years ago
- Personal mobile devices that connect to corporate networks are growing
  - **65% allow personal devices** to connect to corporate networks
  - 78% have more than twice as many personal devices on corporate networks vs.2 years ago
- Security risks are on the rise because of Mobile Devices
  - **71% say mobile devices** have contributed to **increase security incidents**
  - The **Android** platform is considered to introduce the greatest security risks
- Employee behavior impacts security of mobile data
  - 47% report **customer data** is stored on mobile devices
  - **Lack of employee awareness** ranked as greatest impact
  - **72% say careless employees are a greater threat than hackers**

75% of users have personal devices but only 10% are managed by a mobile security strategy

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

What's the risk

Attack Vector	Impact	Sophistication/Level of Effort Required	Mitigation
Malicious App	Total compromise of device	Low - but difficult to target	Enterprise-controlled App Store
Cellular Network	Varies; up to total compromies	High - but falling	Applying software patches
Physical Access: Lost/Stolen Device	Loss of data stored outside encrypted storage areas	Low - but increasing	Store data only inside apps or partitions that provide encryption
Physical Access: Reuse After Loss of Control	Total compromise of device	High	User training
Malicious Email/Web Page	Total compromise of device	Medium to High - depends on device	Applying software patches

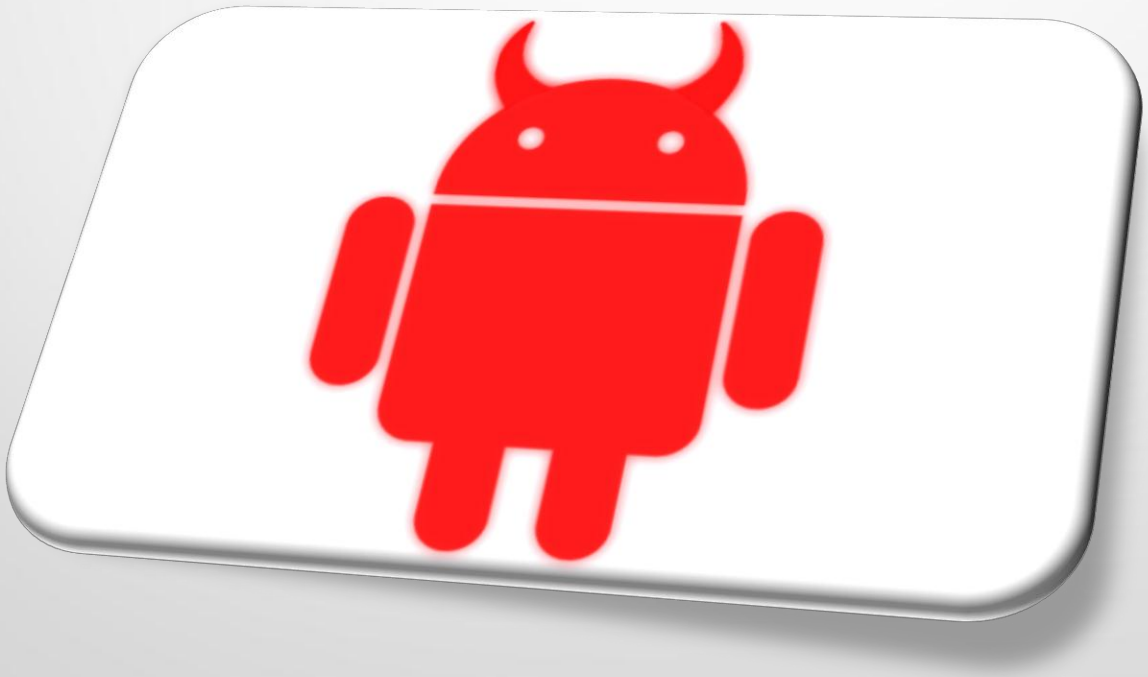
Source: http://www.nsa.gov/ia/_files/factsheets/mobilerisks.pdf

What's the risk

Attack Vector	Impact	Sophistication/Level of Effort Required	Mitigation
Malicious App	Total compromise of device	Low - but difficult to target	Enterprise-controlled App Store
Cellular Network	Varies; up to total compromies	High - but falling	Applying software patches
Physical Access: Lost/Stolen Device	Loss of data stored outside encrypted storage areas	Low - but increasing	Store data only inside apps or partitions that provide encryption
Physical Access: Reuse After Loss of Control	Total compromise of device	High	User training
Malicious Email/Web Page	Total compromise of device	Medium to High - depends on device	Applying software patches
Physical Access: Malicious/Ignorant Users	**Total compromise of device**	**Low**	**Don't implement BYOD!!!**

Source: http://www.nsa.gov/ia/_files/factsheets/mobilerisks.pdf

Smartphones can and will be used against you.



You need a plan

What about these people?

- They still have phones

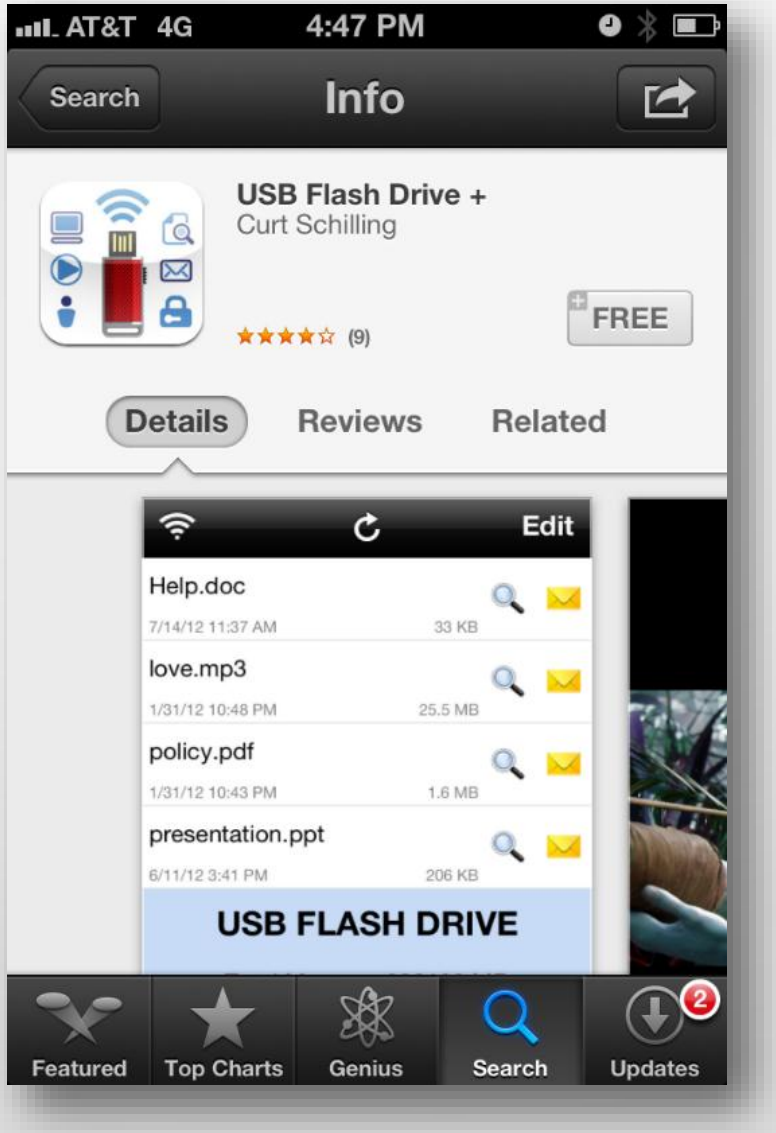
How someone can bypass your security

- Dangerous Apps
  - Data Exfiltration
  - URL Filter bypass

Data Exfiltration using iPhone as an external drive via USB

App Store:

USB Flash Drive +



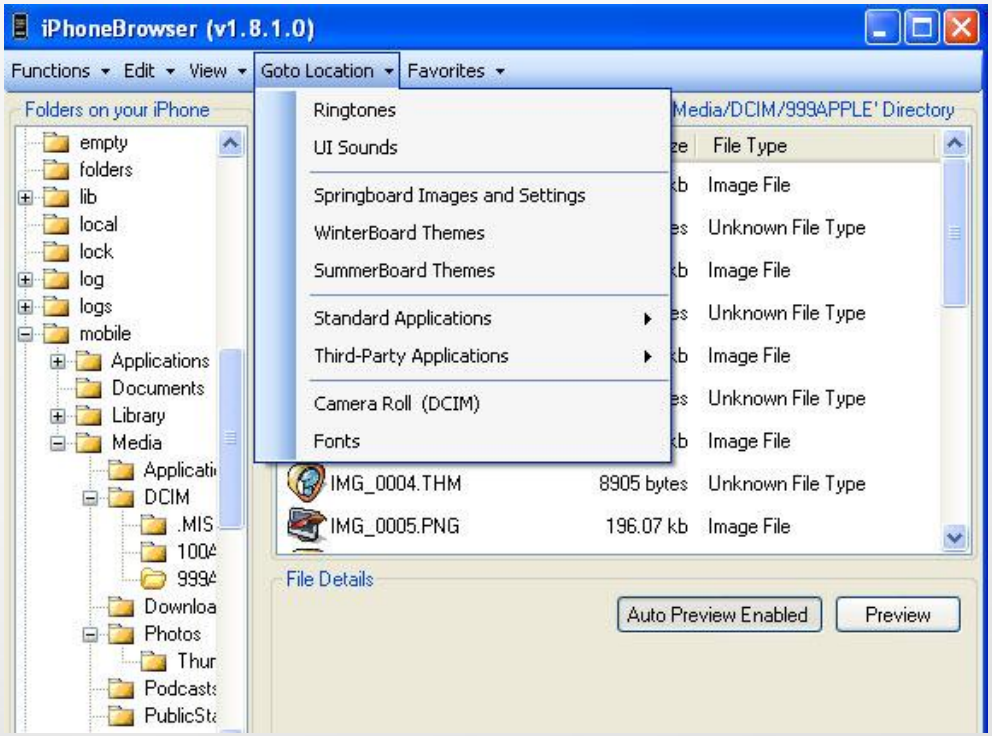
Data Exfiltration: iPhone as an external drive via WiFi

App Store:

Airdrive – Wireless Flash Disk

Cydia: iPhoneBrowser

Data Exfiltration using iPhone as an external drive with USB



But we don't allow Jailbroken devices

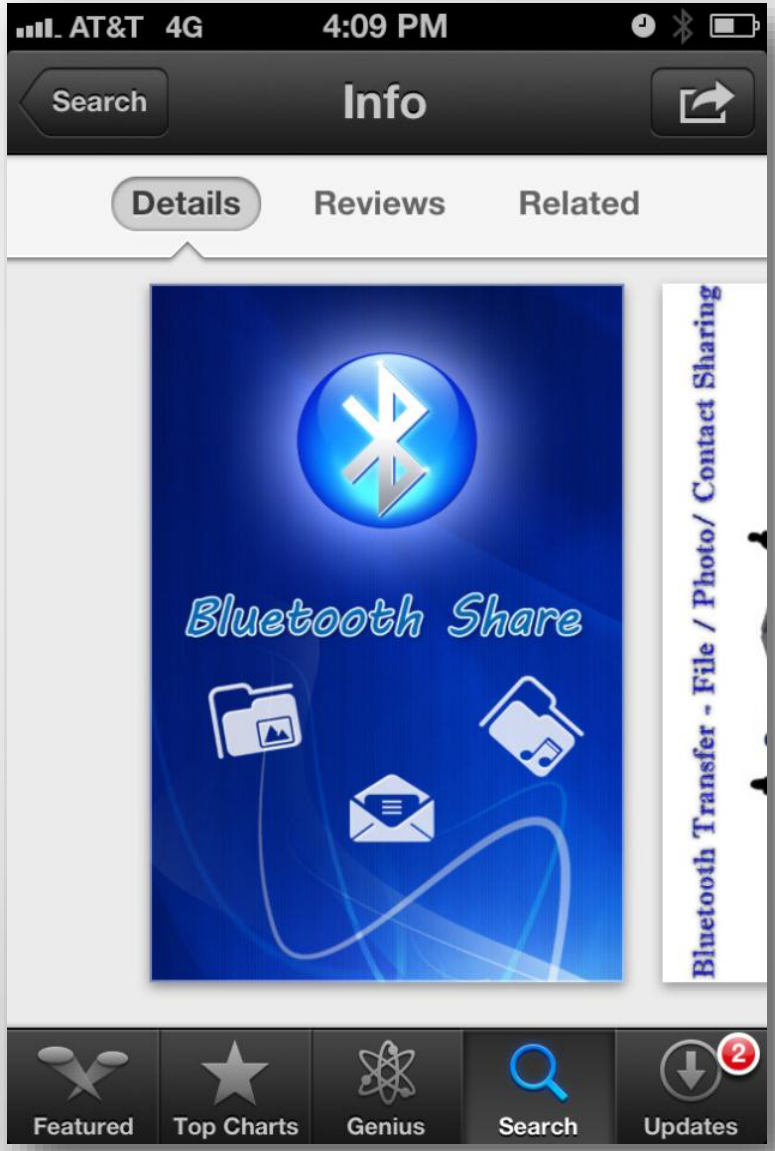
Cydia:

xCon Unblocks iPhone Apps with Jailbreak Detection

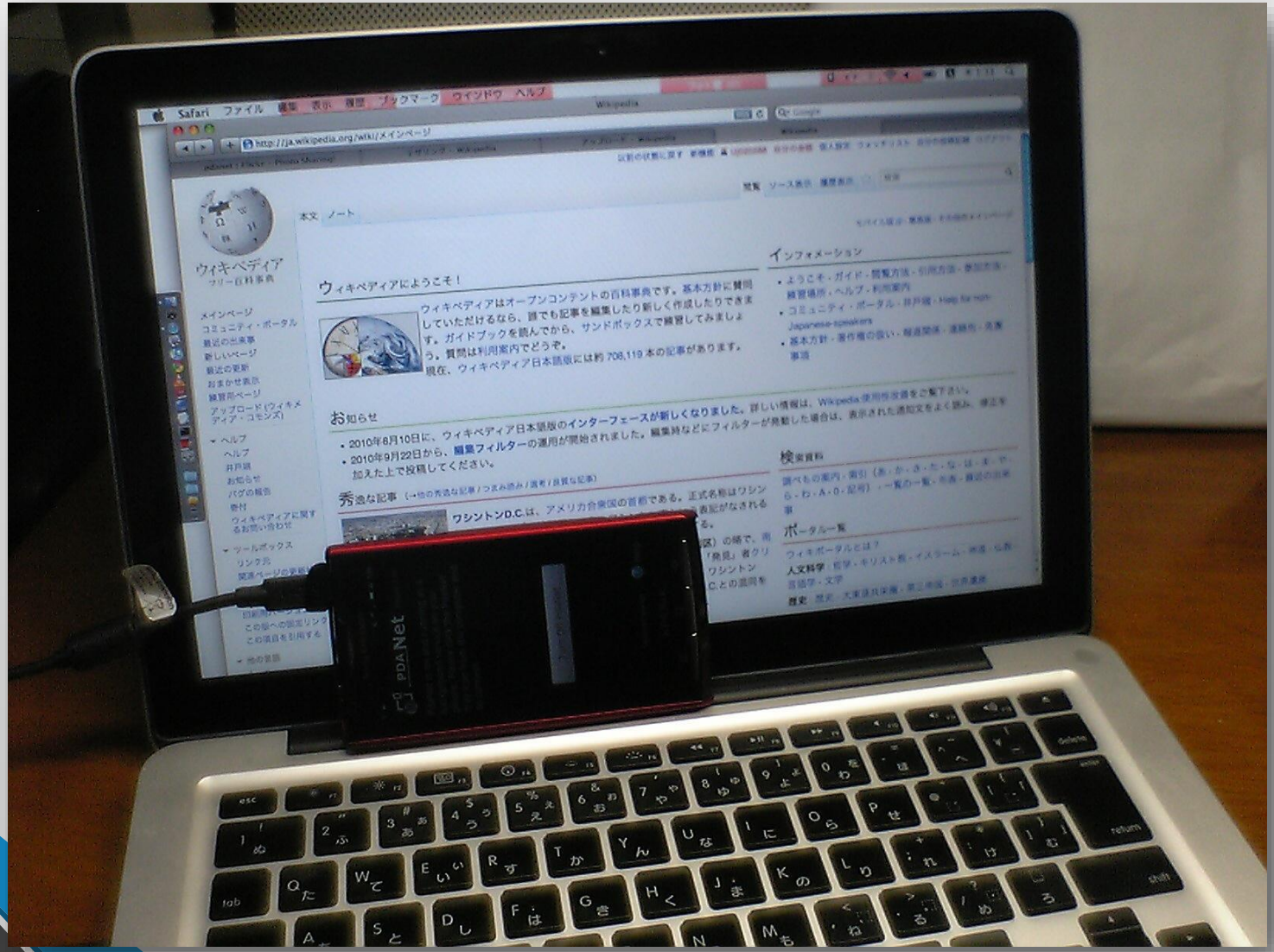
Data Exfiltration: iPhone as an external drive via Bluetooth

App Store:

Bluetooth Share



Tethering


Safari ファイル 編集 表示 履歴 ブックマーク ウィンドウ ヘルプ
ウィキペディア
ウィキペディアにようこそ！
お知らせ
PDANet

Tethering: iOS Personal Hotspot

Built into iOS, just an additional carrier cost

Tether to bypass URL Filters via USB

App Store:

iPhone app FlashArmyKnife lets you tether for free (until Apple finds out)

Tethering via USB cont'd

App Store:

DiscRecorder

Tethering via USB cont'd

Cydia:

- USB tethering with Jailbroken Apps
  - PDANet
  - TetherMe

Tethering via WiFi or Bluetooth

Cydia:
MiWi

Bluetooth tethering for super fast download speed and megaburst!!!


FOTOSEARCH

So how do we protect against these apps

- Policy (Effective and working policy)
- Tools (Keep it Basic, KISS approach)
  - Enterprise MDM
  - Active Directory Group Policy
  - Wireless Intrusion Detection
- User Awareness Training
  - Create custom alerts/scripts to catch mistakes
    - Custom error message, “Don’t plug in that USB drive! Call helpdesk”
- Monitor
  - 24/7, 365
    - 3rd party
  - Continuous

Policy

- Required to define how mobile devices will be used
- Must be practical
- Cover many components of an organization, political and technical
- Get Buy-in
    - Senior management
    - HR
    - Legal
    - Don't be stuck shouldering that burden
- No Quick Fix
    - No template where you can insert *Company Name*
    - http://www.sans.org/security-resources/policies/mobile.php

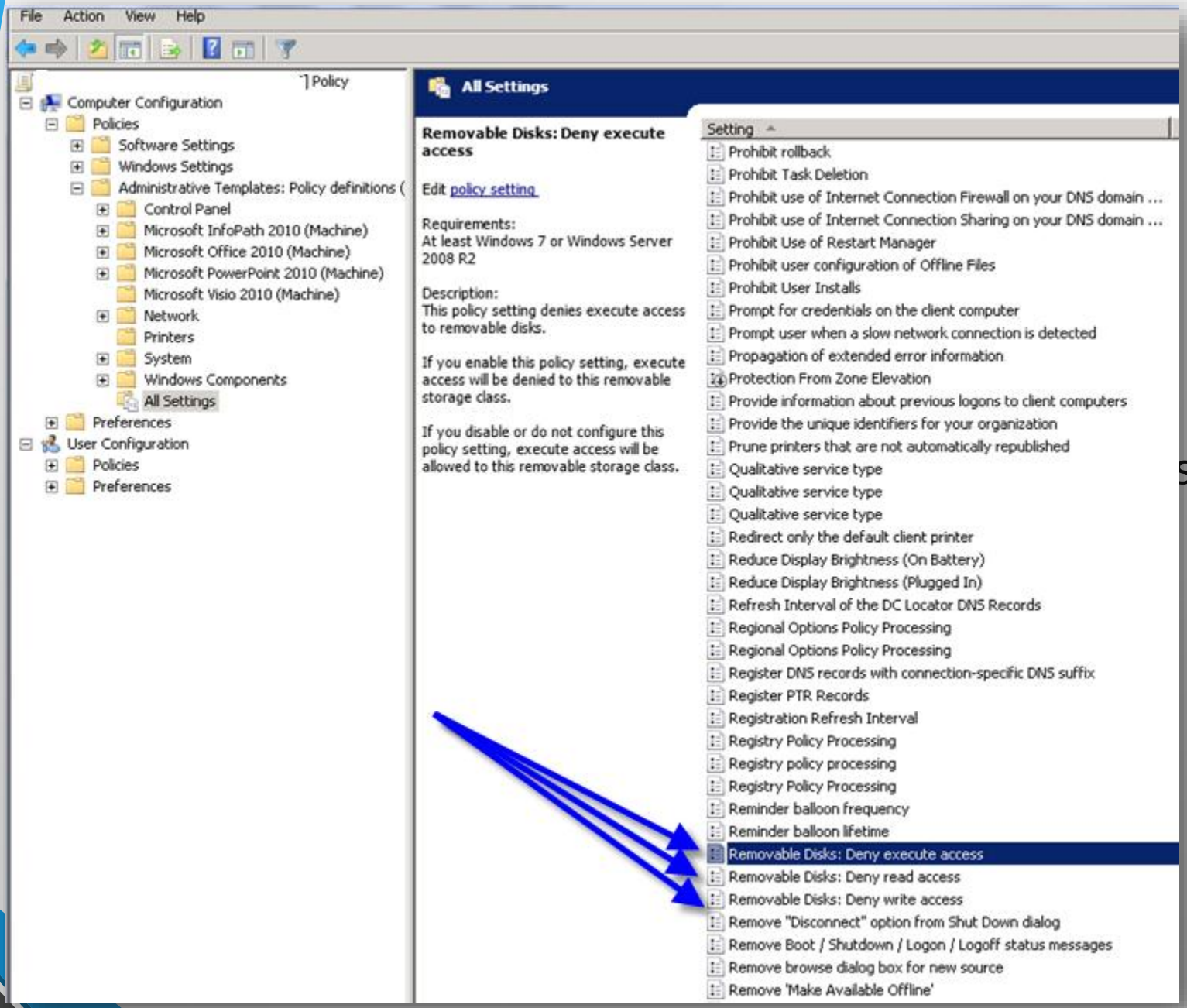
MDM

CIO says block USBs!

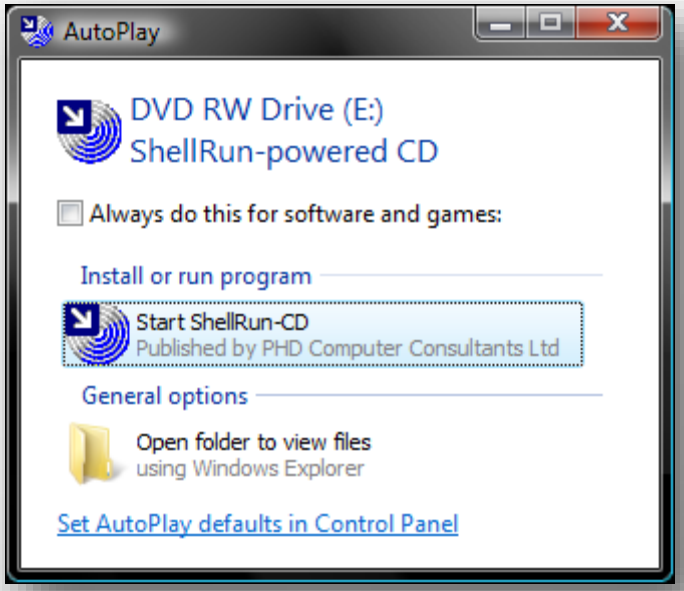
- Blocking USB everything?
  - Mice
  - Printers
  - Cameras
  - etc.

Tools: Microsoft

- Restrict Access
  - Group Policy
  - No local Admins
    - Remove/block users from Local Admin group
- Turn off Autorun
- Block external drives
  - Block USB's
- Monitor for alerts

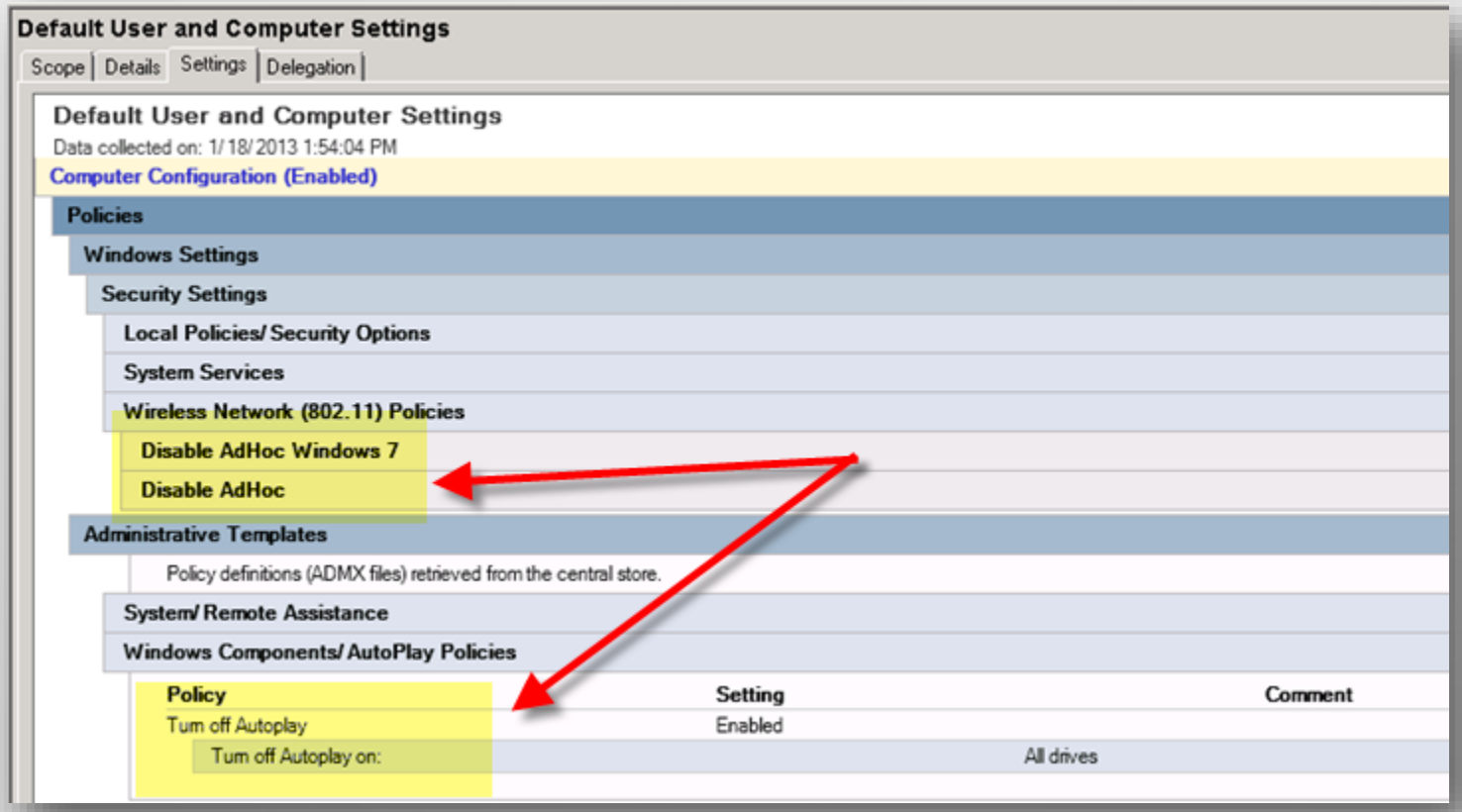

File Action View Help
Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (
Control Panel
Microsoft InfoPath 2010 (Machine)
Microsoft Office 2010 (Machine)
Microsoft PowerPoint 2010 (Machine)
Microsoft Visio 2010 (Machine)
Network
Printers
System
Windows Components
All Settings
Preferences
User Configuration
Policies
Preferences
All Settings
Removable Disks: Deny execute access
Edit policy setting
Requirements:
At least Windows 7 or Windows Server 2008 R2
Description:
This policy setting denies execute access to removable disks.
If you enable this policy setting, execute access will be denied to this removable storage class.
If you disable or do not configure this policy setting, execute access will be allowed to this removable storage class.
Setting
Prohibit rollback
Prohibit Task Deletion
Prohibit use of Internet Connection Firewall on your DNS domain ...
Prohibit use of Internet Connection Sharing on your DNS domain ...
Prohibit Use of Restart Manager
Prohibit user configuration of Offline Files
Prohibit User Installs
Prompt for credentials on the client computer
Prompt user when a slow network connection is detected
Propagation of extended error information
Protection From Zone Elevation
Provide information about previous logons to client computers
Provide the unique identifiers for your organization
Prune printers that are not automatically republished
Qualitative service type
Qualitative service type
Qualitative service type
Redirect only the default client printer
Reduce Display Brightness (On Battery)
Reduce Display Brightness (Plugged In)
Refresh Interval of the DC Locator DNS Records
Regional Options Policy Processing
Regional Options Policy Processing
Register DNS records with connection-specific DNS suffix
Register PTR Records
Registration Refresh Interval
Registry Policy Processing
Registry policy processing
Registry Policy Processing
Reminder balloon frequency
Reminder balloon lifetime
Removable Disks: Deny execute access
Removable Disks: Deny read access
Removable Disks: Deny write access
Remove "Disconnect" option from Shut Down dialog
Remove Boot / Shutdown / Logon / Logoff status messages
Remove browse dialog box for new source
Remove 'Make Available Offline'

Tools: Turn off Autorun



http://support.microsoft.com/kb/967715

Tools: Microsoft



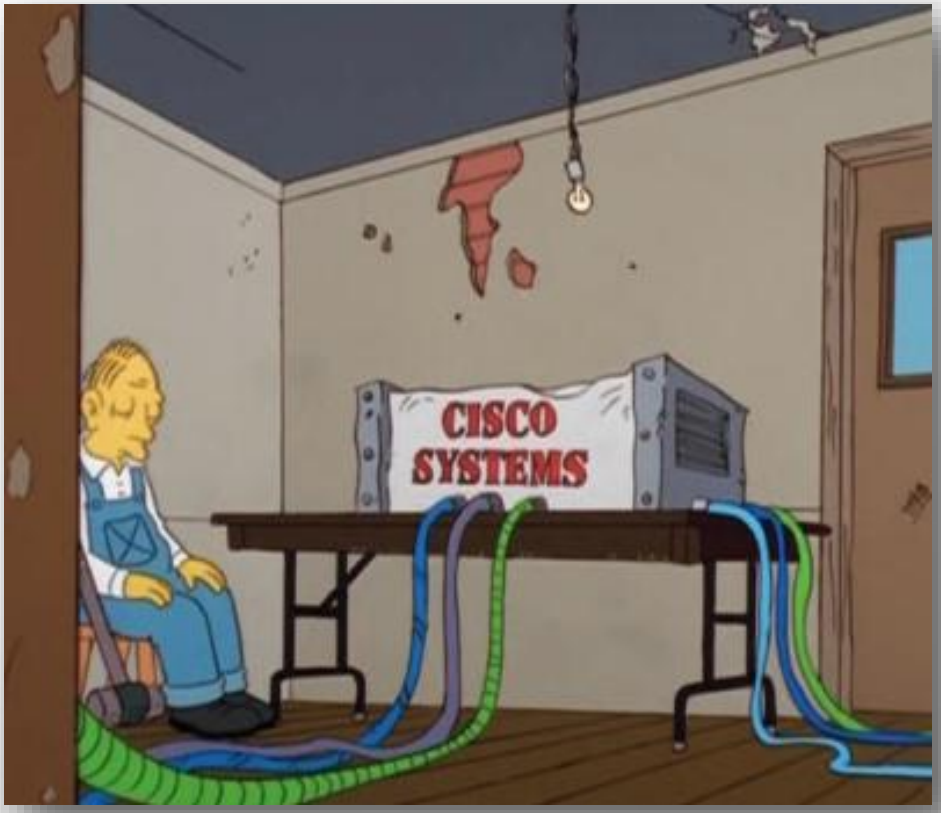
Tools: Microsoft

- Monitor for EventID 134 Source: Removable Disk
- Log to SIEM
  - **Use a Eventlog to Syslog Utility**
    - Evt2Sys
      - https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys
    - Adiscon
      - http://www.adiscon.com/en/
  - **Email alerts**

Tools: Wireless Intrusion Detection

Get a wireless intrusion detection system

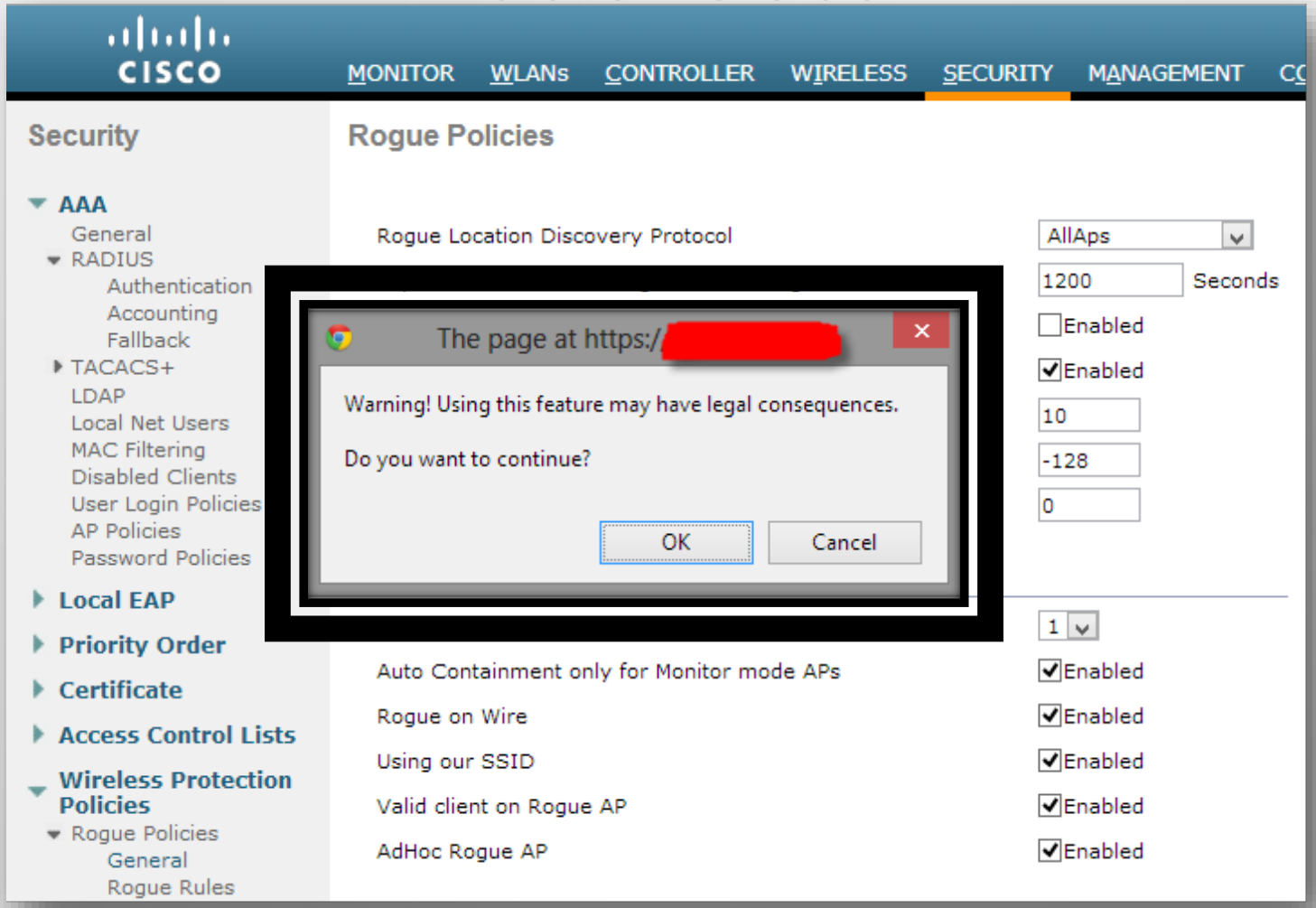
- Block rogue access points
  - Cisco WCS
  - Kismet with OpenWRT
  - http://sagan.quadrantsec.com/papers/wireless-ids/
  - http://www.sans.org/reading_room/whitepapers/detection/inexpensive-wireless-ids-kismet-openwrt_33103



Tools: Cisco Block WiFi

- Cisco Wireless Access Controller
- Stops wired access points
- Stops spoofed SSIDS
- Stops rogue SSIDS
  - Alerts to your SEIM
    - Sagan
      - www.quadrantsec.com

Tools: Cisco


CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
Security
Rogue Policies
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Rogue Policies
General
Rogue Rules
Rogue Location Discovery Protocol
AllAps
1200
Seconds
Enabled
Enabled
10
-128
0
1
Auto Containment only for Monitor mode APs
Enabled
Rogue on Wire
Enabled
Using our SSID
Enabled
Valid client on Rogue AP
Enabled
AdHoc Rogue AP
Enabled
The page at https://
Warning! Using this feature may have legal consequences.
Do you want to continue?
OK
Cancel

Block Bluetooth

http://social.technet.microsoft.com/Forums/en-US/winserverGP/thread/ad0b44c2-437c-449e-8a4b-5db55254108f

Awareness

- Have a Security Awareness Program
  - Train your users
    - Cover topics like stuxnet
    - Do phishing exercises
      - Email campaigns
      - USB drops
    - Provide security related news
      - OUCH Newsletter
      - http://www.securingthehuman.org/resources/newsletters/ouch/2013

Summary

- Smartphones bring in a lot of risk
- Have a good policy
- Use tools to help mitigate the risk
- Have alerts that monitor for irregularities
- Train employees
  - Sans Sec575 for deeper dive
    - http://www.sans.org/event/sans-2013/course/mobile-device-security-ethical-hacking
    - www.sourceforge.net/p/mobisec

Questions?

Contact:
inkrypto@gmail.com