



BYOD - Bring Your Own Devastation Taking On the Mobile Threat

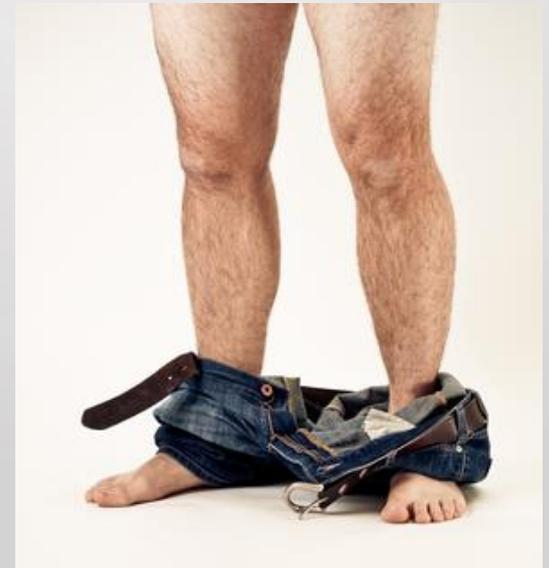
“Vulnerabilities Exposed” Webcast Series - Part 3

Paul Asadoorian and Jack Daniel

“Vulnerabilities Exposed” Series

- Part 3 of a 4-part series
 - Part 1: “Reducing Your Patch Cycle to Less Than 5 Days”
 - Part 2: “Addressing the Security Challenges of Virtualization”
- Archives & slides:
www.tenable.com/vulns-exposed

Strategies & solutions for today’s
common security challenges



Today's Webcast Roadmap

- **Mobile evolution** – How we got here
- **Mobile challenges** – The problems we face
- **Solutions** – Procedural & tactical

Technology Evolves...



PC in 1981/1982



Approximate Cost: \$3,000.00

Cell Phones Circa 1991/1992



\$300.00 for the phone, likely plans were pay-per-minute

Today

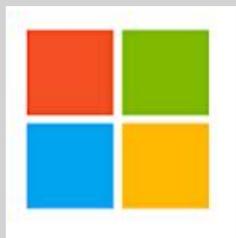
- iPhone 5c: \$99.00
- Google - Nexus 7" tablet with 16GB memory (2nd generation): \$229.00
- Dell - refurbished - 14.1" Latitude notebook - 2GB memory - 60GB hard drive: \$203.63 (free shipping)



Reality

- For 1/6th the cost of 1st generation PC, you can own a smartphone, tablet, & laptop

- >900,000 apps for  &  respectively



Windows pre-installed on your laptop

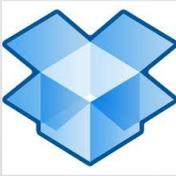
If Your Phone Is Not Up to Date...



Features Rule Upgrades

- “According to statistics from Fiksu, a mobile analysts firm, more than 50% of all iOS devices have upgraded to iOS 7.”
 - <http://www.latimes.com/business/technology/la-fi-tn-users-are-upgrading-to-ios-7-at-record-pace-20130923,0,5439783.story>
- OTA (Over-the-Air) upgrades help, apps are still problematic

Usefulness

- Email
- Corporate Communications
 - Twitter  Facebook  LinkedIn 
- Cloud Apps
 - Salesforce  Dropbox 
- Custom applications
- Retail
 - Payment processors, menus, in-flight

But it just can't be!

“American became the first major commercial airline company to fully utilize tablets in all cockpits during all phases of flight, allowing it to eliminate 24 million pages of paper documents, save an estimated 400,000 gallons of jet fuel each year, worth \$1.2 million, and help prevent back injuries among pilots who will no longer have to carry heavy bags full of paper flight manuals.”



iPhone holds 62.5% share of U.S. commercial market based on latest quarterly data published by IDC

- <http://appleinsider.com/articles/13/07/23/apples-iphone-cements-its-position-as-the-smartphone-of-choice-for-business>

More Reality: BYOD Extends Beyond “Mobile”



BYOD Destruction

- **Control** – IT no longer has control of device configuration & patch management
- **Data Security** – Physical device security is up to the user & devices access and/or contain data
- **Connectivity** – Devices have multiple paths
 - 3G/4G, WiFi, Bluetooth, NFC

More BYOD Destruction

- Software (Apps) – Too easy to install new apps, all of which could contain vulnerabilities
- Malware
- Phishing Attack Vectors – SMS phishing

Audit Mobile Devices



System Configuration



General Settings



Feed Settings



Mobile Settings



Results Settings



Advanced Settings

Mobile Settings

Setting Type

ActiveSync (Exchange)

ActiveSync (Exchange)

Nessus can use ActiveSync to gather information about all the mobile devices that used this protocol to fetch their email (via Exchange). If you have an Exchange deployment, please enter the following information regarding your Domain Controller below

Domain Controller

Domain

Domain Username

Domain Password

Update

Cancel

Review Vulnerabilities & "Inventory"

The screenshot displays the Nessus web interface. At the top, the 'Nessus' logo and 'vulnerability scanner' text are visible. A navigation bar includes 'Results', 'Scans' (with a red '0' badge), 'Templates', 'Policies', 'Users', and 'Configuration'. The user 'paula' is logged in, with links for 'Help & Support' and 'Sign Out'.

The main content area is titled 'Mobile Devices Audit Vulnerability Summary'. It features a 'Filter Options' button (with a blue '0' badge) and a 'Delete All Results' button. On the left sidebar, there are sections for 'Hosts' (1130), 'Vulnerabilities' (9), and 'Export Results'.

The central 'Vulnerability Summary' table lists various findings:

Severity	Vulnerability Description	Category	Count
critical	Apple iOS < 5.1.1 Multiple Vulnerabilities	Mobile Devices	585
high	Apple iOS < 6.0.1 Multiple Vulnerabilities	Mobile Devices	645
high	Apple iOS < 6.0 Multiple Vulnerabilities	Mobile Devices	615
high	Apple iOS < 5.1 Multiple Vulnerabilities	Mobile Devices	555
high	Apple iOS < 5.0.1 Multiple Vulnerabilities	Mobile Devices	510
high	Apple iOS < 5.0 Multiple Vulnerabilities	Mobile Devices	480
medium	Windows Phone7 < 7.0.7392 Out-of-Date SSL Blacklist	Mobile Devices	15
medium	Windows Phone7 < 7.10.8107 Out-of-Date SSL Certificate	Mobile Devices	15
info	MDM Mobile Device Reporting	Mobile Devices	1130

Mobile Devices Audit Hosts Summary

Filter Options ⁰ Delete All Results

- Hosts 1130
- Vulnerabilities 9
- Export Results

Hosts Summary

Sort Options Filter Hosts

iPhone/A10991 100%	iPhone/A10981 100%
1 5 1	1 5 1
iPhone/A10971 100%	iPhone/A10961 100%
1 5 1	1 5 1
iPhone/A10951 100%	iPhone/A10941 100%
1 5 1	1 5 1
iPhone/A10931 100%	iPhone/A10921 100%
1 5 1	1 5 1
iPhone/A10911 100%	iPhone/A1091 100%
1 5 1	1 5 1
iPhone/A10901 100%	iPhone/A10891 100%
1 5 1	1 5 1
iPhone/A10881 100%	iPhone/A10871 100%
1 5 1	1 5 1

Apple Profile Manager

Nessus can use Apple's Profile Manager to gather information about the iOS devices managed in your company. If you do have a Profile Manager deployment, please enter the information below (note that it is recommended that Nessus sends an 'update' request to every device and wait for their answer to get the newest data about them)

Apple Profile Manager server

Apple Profile Manager port

443

Apple Profile Manager username

Apple Profile Manager password

SSL

Verify SSL Certificate

Force Device Updates

Device Update Timeout (Minutes)

5

Solutions: SecurityCenter

cody [cody]

SecurityCenter

Dashboard

Analysis

Scanning

Reporting

Assets

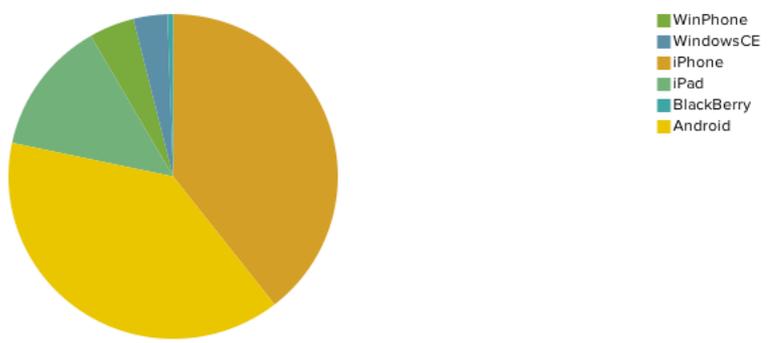
Workflow



Mobile Summary ?

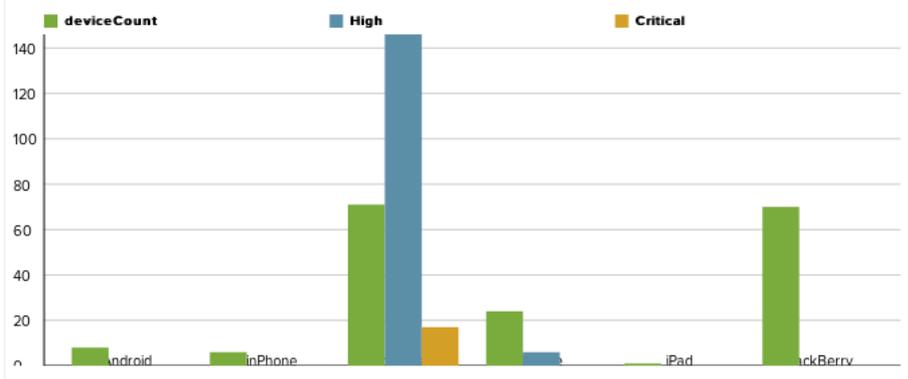
Add Component

Mobile Summary - Device Type Summary Pie Chart



Last Updated: 8 minutes ago

Mobile Summary - Mobile Device Count, Critical and High Severity Summa...



Last Updated: 8 minutes ago

Mobile Summary - Top 50 Mobile Users

User	Low	Medium	High	Critical	Total
SOMECORP.COM/Jane36 Doe36	0	0	7	1	10
SOMECORP.COM/Jane50 Doe50	0	0	3	0	5
SOMECORP.COM/Jane14 Doe14	0	0	2	0	4
SOMECORP.COM/Jane25 Doe25	0	0	2	0	4
SOMECORP.COM/Jane28 Doe28	0	0	2	0	4
SOMECORP.COM/Jane38 Doe38	0	0	2	0	4
SOMECORP.COM/Jane48 Doe48	0	0	2	0	4
SOMECORP.COM/Jane51 Doe51	0	0	2	0	4
SOMECORP.COM/Jane1 Doe1	0	0	0	0	2
SOMECORP.COM/Jane10 Doe10	0	0	0	0	2
SOMECORP.COM/Jane11 Doe11	0	0	0	0	2

Last Updated: 8 minutes ago

Mobile Summary - Vulnerable Mobile Devices

	Device Count	Critical	High	Medium
iPad	24	None	2	None
iPhone	71	17	27	None
WindowsCE	6	None	None	None
WinPhone	8	None	None	7
Android	70	None	None	None
HTC	3	None	None	None
Samsung	0	None	None	None
LG	1	None	None	None

Last Updated: 8 minutes ago

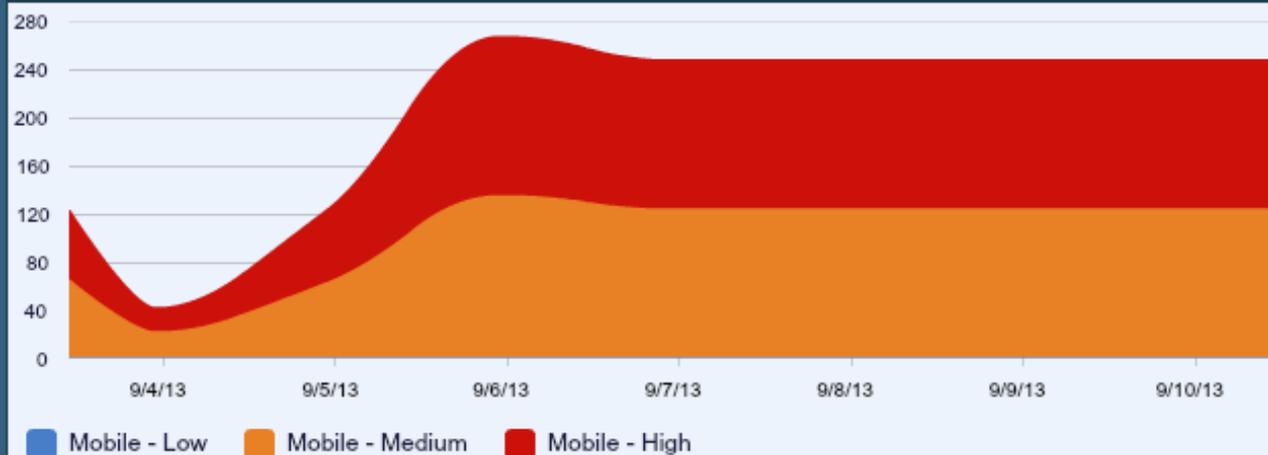
Solutions: Passive Vulnerability Scanner

Mobile Vulns (Passive)

Plugin ID	Name	Severity	Total
5737	Android < 2.3 Multiple Vulnerabilities	High	96
6041	Apple iOS 3.0 through 4.3.5 Multiple Vulnerabilities	High	5
5337	Apple iPhone OS < 3.1.3 Multiple Vulnerabilities	High	4
5578	Apple iPhone/iPad OS < 4.0 Multiple Vulnerabilities	High	3
5715	Apple iPhone/iPad iOS < 4.2 Multiple Vulnerabilities	High	3
5814	Apple iPhone/iPad OS < 4.3 Multiple Vulnerabilities	High	3
5888	Apple iPhone/iPad OS < 4.3.2 Multiple Vulnerabilities	High	3
5986	Apple iPhone/iPad iOS < 4.3.4 and iOS 4.2.5 through 4.2.9 Multiple Vul...	High	3
5110	Apple iPhone < 3.0.1 Overflow	High	2
5160	Apple iPhone < 3.1 Multiple Vulnerabilities	High	2

Last Updated: 2 minutes ago

Mobile Trend (Passive)



Last Updated: 2 minutes ago

Tenable Resources



Blog:

<http://blog.tenable.com>



Podcast:

<http://www.tenable.com/podcast>



Videos:

<http://www.youtube.com/tenablesecurity>



Discussions Forum:

<https://discussions.nessus.org>



Buy Nessus, PVS, Perimeter Service, Training, & Bundles:

<https://store.tenable.com>



Find a Channel Partner:

<http://www.tenable.com/partners/find-a-subscription-partner>

For More Info or to Evaluate

Nessus:

<http://www.tenable.com/products/nessus>

PVS:

<http://www.tenable.com/products/passive-vulnerability-scanner>

SecurityCenter Continuous View:

<http://www.tenable.com/products/securitycenter-continuous-view>

Questions?



Thank You!

Contact us:

Paul Asadoorian – paul@nessus.org

Jack Daniel – jdaniel@tenable.com

“Vulnerabilities Exposed” webcast #4:

November 12th at 2 pm EST

Reporting & Communicating Results