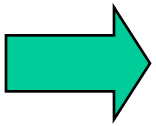
Top 8 Steps for Effective Mobile Security

Ed Skoudis and Joshua Wright
Counter Hack, LLC

Outline



Three Truths About Mobile Security

- Community Development Project
- Top 8 Mobile Security Steps
- Moving Forward
- Conclusion and Q&A

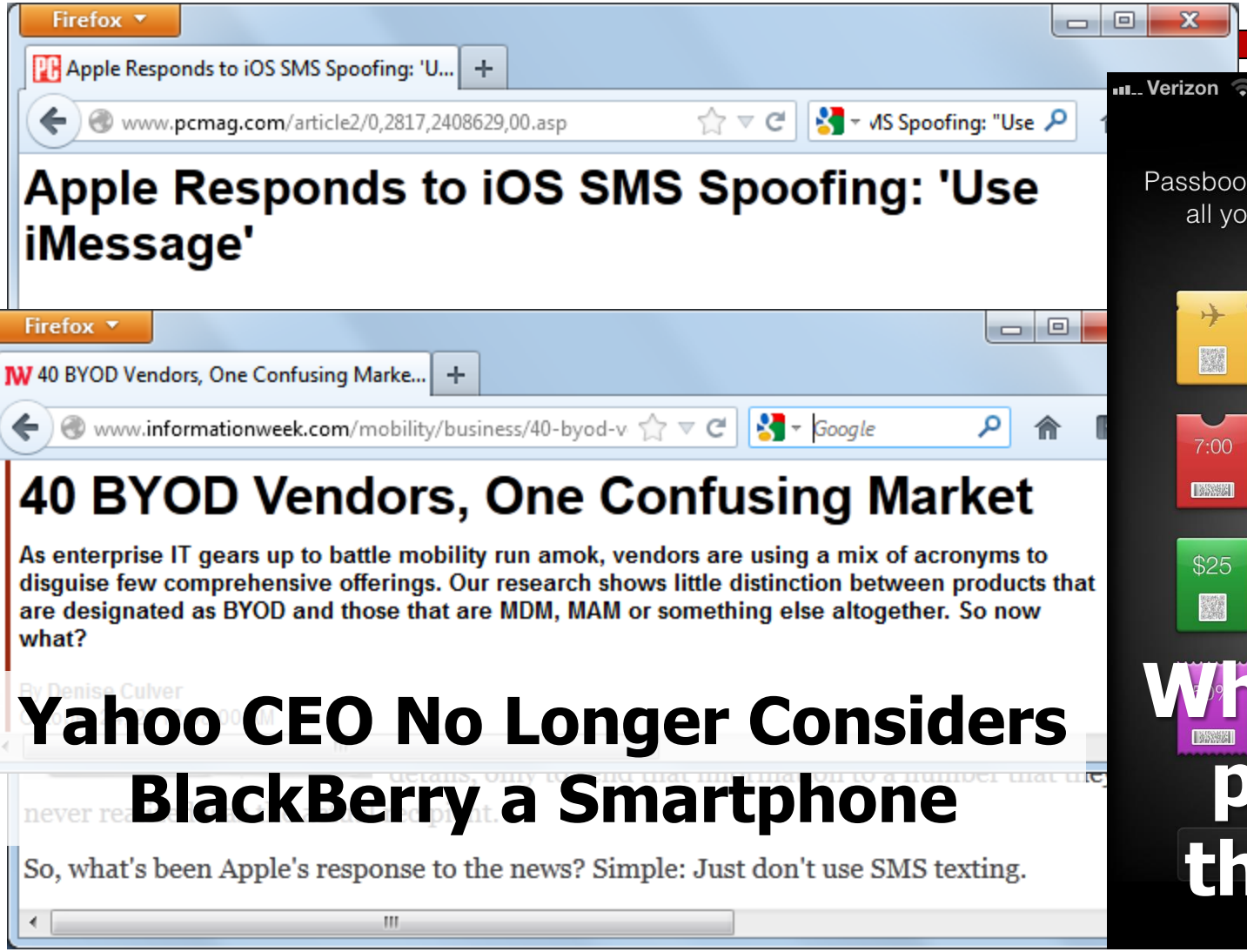
Mobile Device Security Is Hard

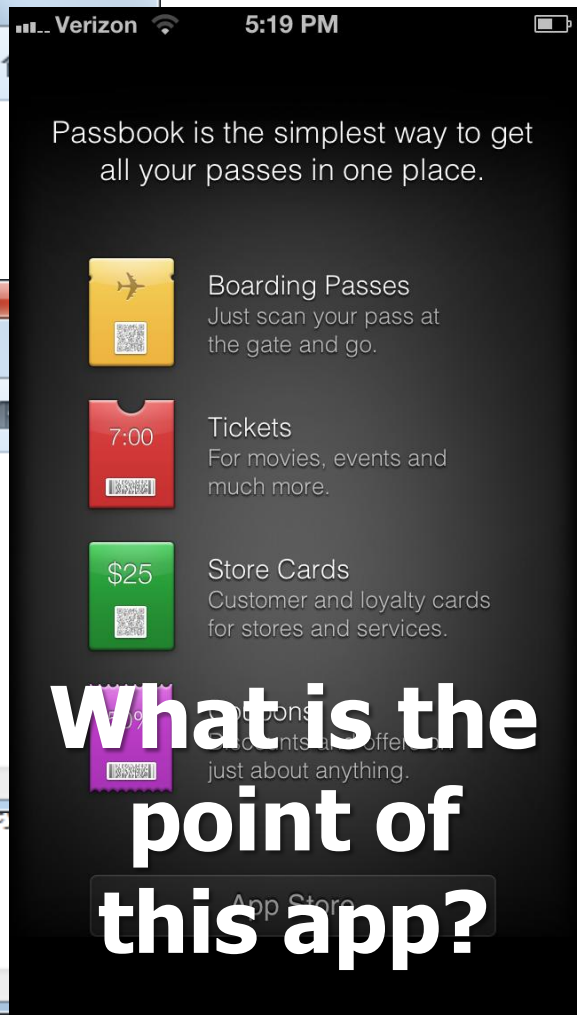
"iOS 6 Jailbroken in First 24 Hours"

"SMSZombie" Malware Infects 500,000 Android Users In China

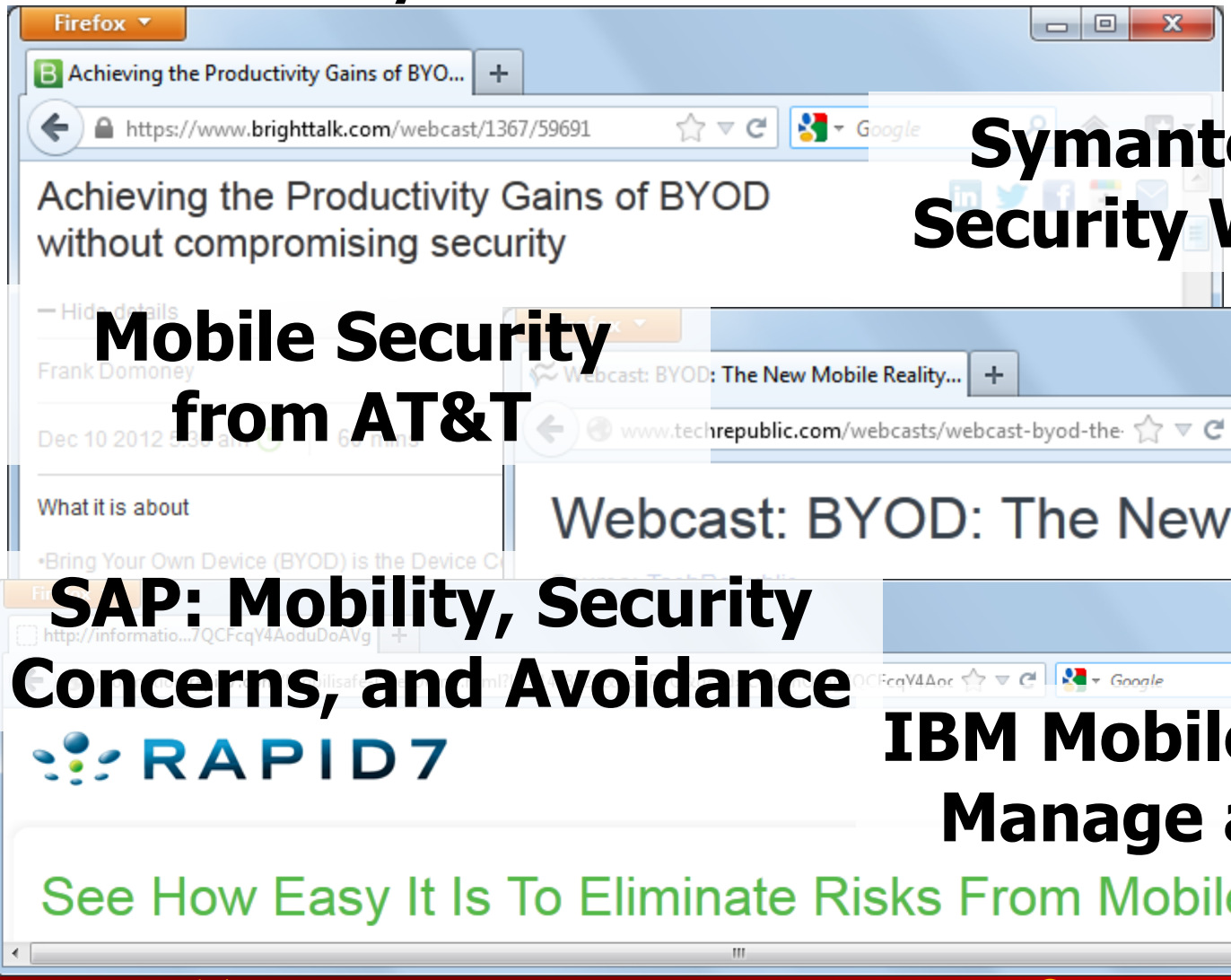
IBM bans the use of Siri on its network over data privacy fears

Mobile Security Is Confusing





Vendors All Have Something To Say About Mobile Security



Symantec Mobile Security Whitepaper

Mobile Security from AT&T

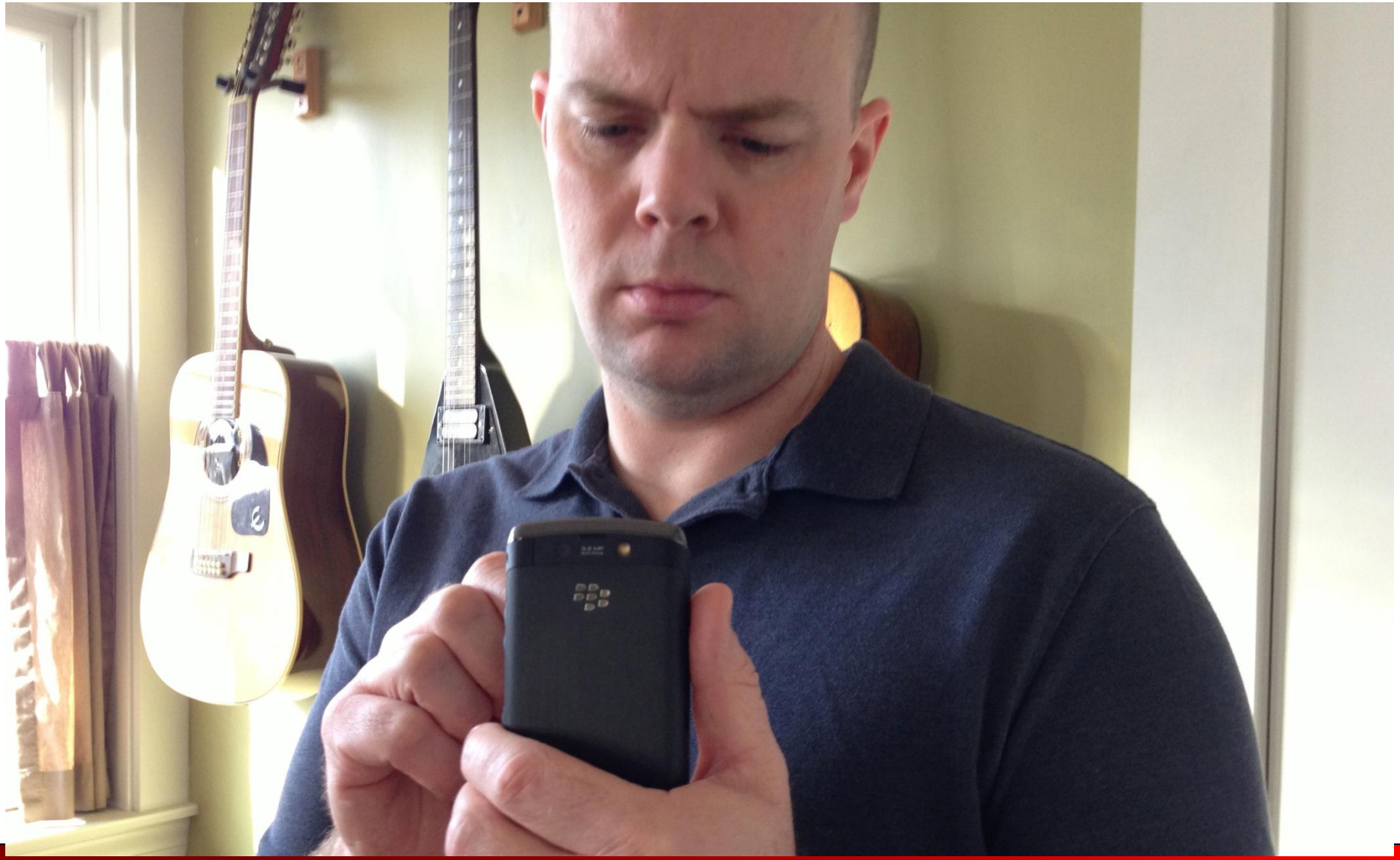
SAP: Mobility, Security Concerns, and Avoidance

RAPID7

IBM Mobile Enterprise: Manage and Secure

See How Easy It Is To Eliminate Risks From Mobile Devices

This Is Unpleasant



Outline

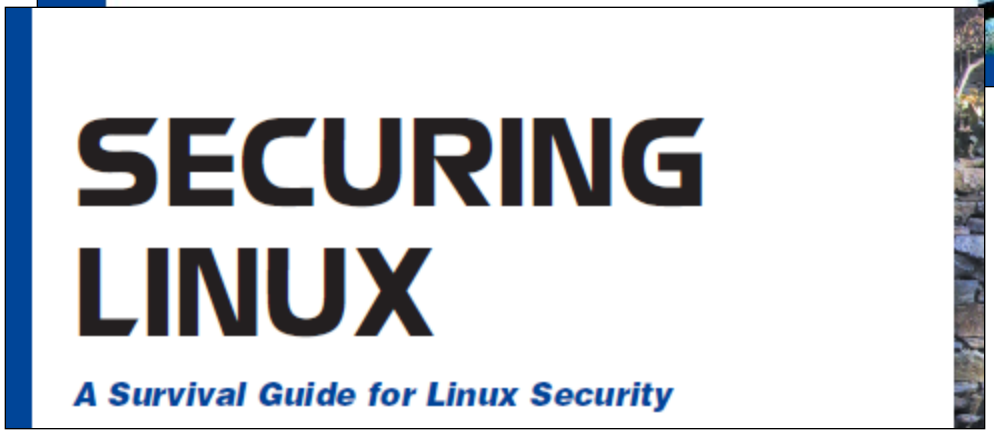
- Three Truths About Mobile Security
- Community Development Project
- Top 8 Mobile Security Steps
- Moving Forward
- Conclusion and Q&A

I Had an Idea

Develop the SANS Top Mobile Security Steps Guide

- Develop a guide to help organizations with the most important steps
- Make it practical and actionable
- Identify which steps require a lot of work, and which can be done quickly
  - Organized by the overall security benefit
- Concise language for administrators and management
- Make it free and available to everyone

Traditionally, SANS Does This Well…



…For Several Reasons

- Unbiased opinions without the aim to sell a vendor product
- Consensus steps that are the product of community involvement
  - Not one person's ideas, but based on actual successes and failures
- Designed as actionable, practical steps to actually solve a problem

History Part 1

- I started drafting the outline and content for the "Top N Mobile Security Steps"
- Solicited individual advice and comments from a small group of mobile experts
  - Representing many different organizations
- Lots of editing and content development, initial definition of 10 critical steps
- Asked for wider review from the SANS Advisory Board list
  - Forty-Four (44!) reviewers returned substantial feedback and comments
- I managed the editing process, and consensus discussion to integrate everything…

It Was…Good

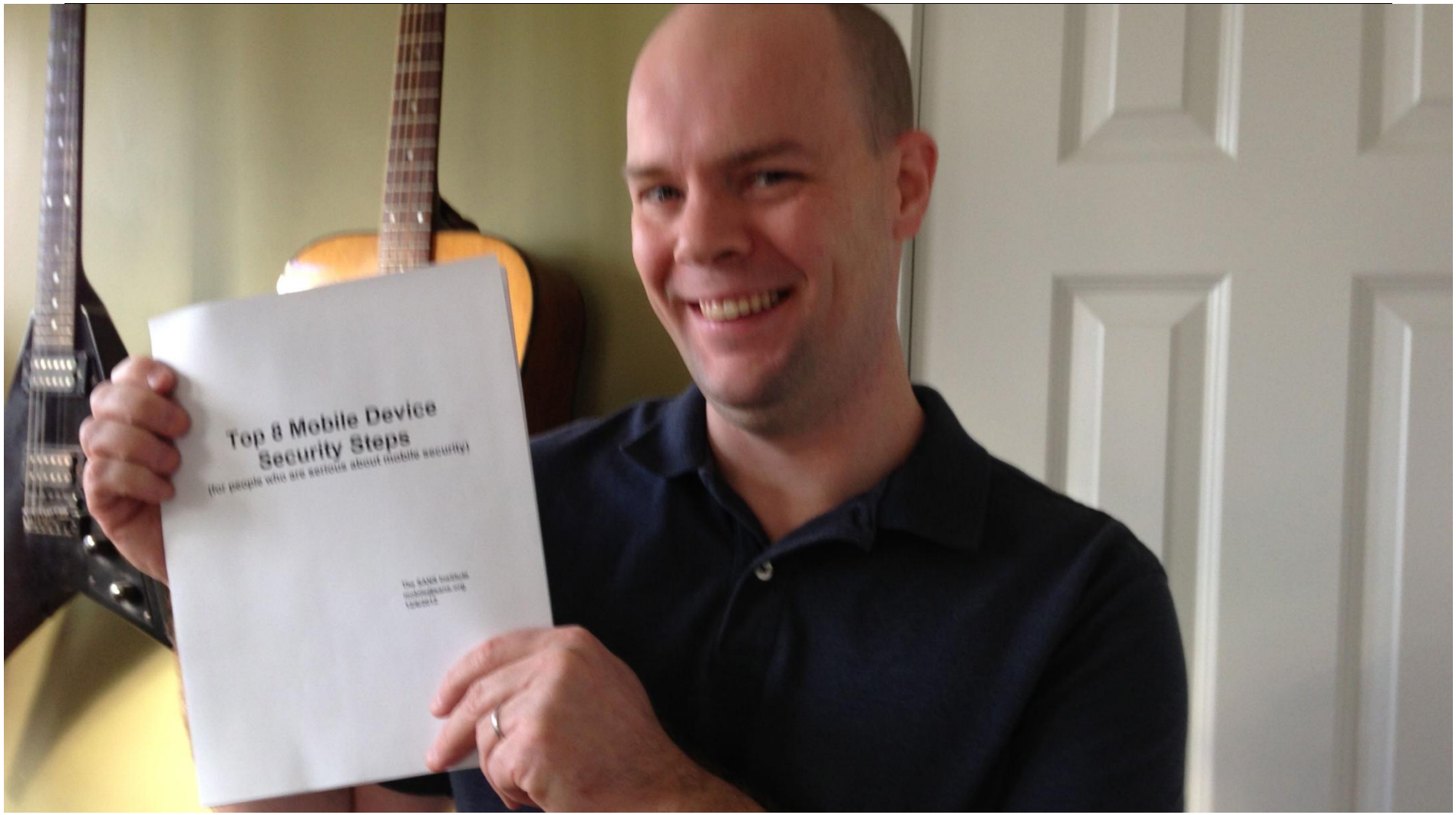
- At 25 pages, it was a good guide, but fell short of my expectations
- Advice was solid, but difficult to articulate specifically
- For example: "Develop Policies to Guide Use"
  - Great advice, but subject to interpretation, and difficult to implement

The initial guide was useful, but not great. It was another PDF to download, skim, and never read.

A Revised Plan of Action!

- Each step must be readily actionable for most organizations
- Must include detailed, illustrated examples for each step
- Identify the areas that are being exploited, and tell people how to fix them
- Consolidate steps into the most important actions for organizations

The Product


Top 8 Mobile Device
Security Steps
(for people who are serious about mobile security)

Outline

- Three Truths About Mobile Security
- Community Development Project
- Top 8 Mobile Security Steps
- Moving Forward
- Conclusion and Q&A

Top 8 Mobile Device Security Steps

(for people who are serious about mobile security)

1. Enforce Device Passcode Authentication
2. Monitoring Mobile Device Access and Use
3. Patching Mobile Devices
4. Prohibit Unapproved Third-Party Application Stores
5. Disable Developer Debug Access
6. Evaluate Application Security Compliance
7. Prepare an Incident Response Plan for Lost or Stolen Mobile Devices
8. Implement Management and Operational Support

#1: Device Passcode Use

- Regardless of enterprise owned or BYOD, all devices must use a passcode
- Selection of passcode influenced by sensitivity of data stored on the device
  - Convenient email? Minimal passcode.
  - PII? Substantial passcode.
- Must balance acceptable use requirements with security needs

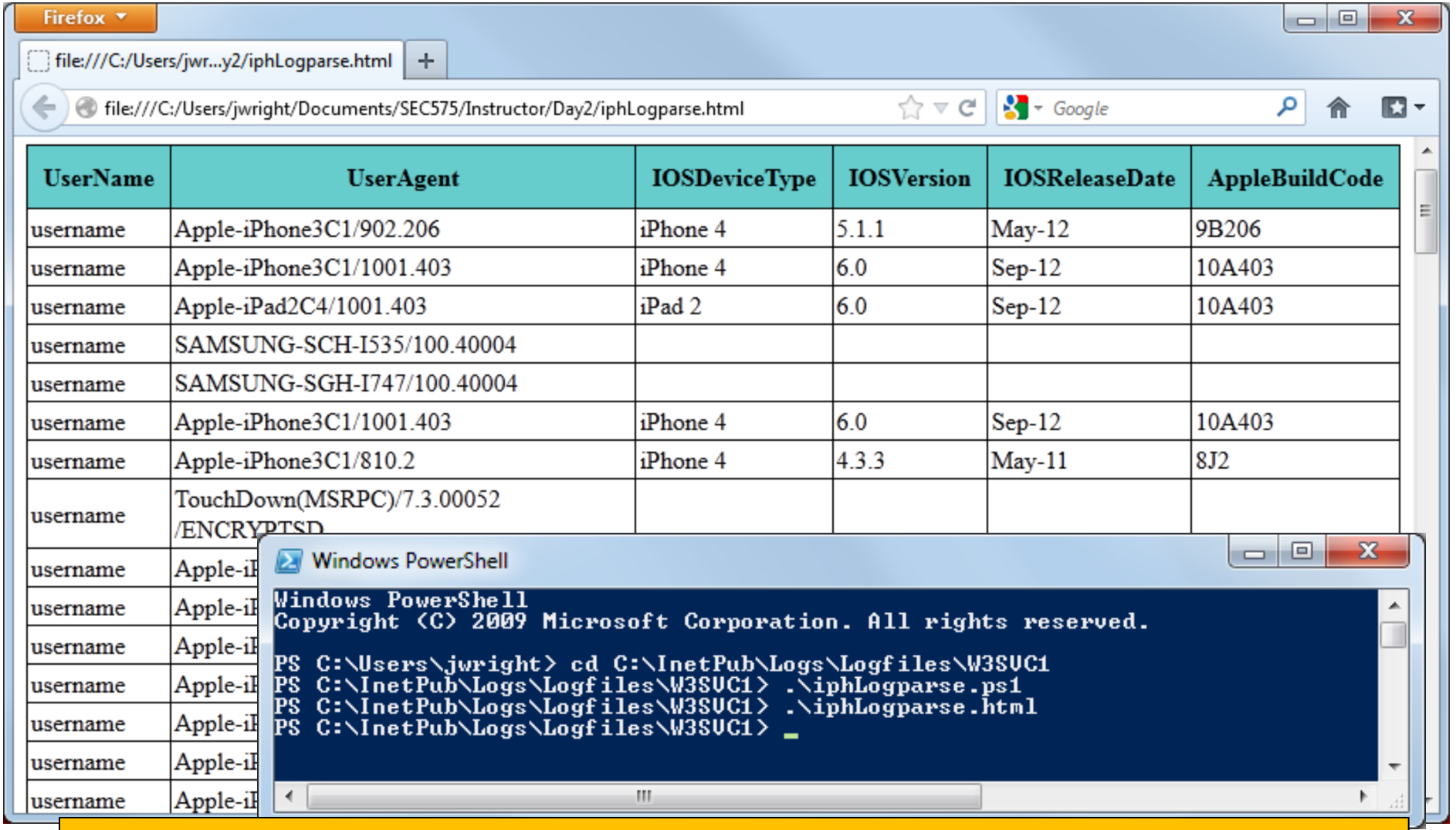
Passcode Requirements

	Minimal Security	Strong Security	Very Strong Security
Min. Length	4 characters	6 characters	8 characters
Complexity	numeric only	2 alpha, 2 numeric characters	2 alpha, 2 numeric, 2 special characters
Maximum Age	Indefinite	1 year	180 days
Passcode History	0 passcodes	4 passcodes	8 passcodes
Auto-Lock Timer	15 minutes	10 minutes	3 minutes
Maximum Failed Attempts	10 failed passcode attempts before wipe	8 failed passcode attempts before wipe	4 failed passcode attempts before wipe

#2: Monitoring Mobile Device Access and Use

- Organizations must monitor and record the types and versions of mobile devices in use
- MDM is helpful, but will not characterize unmanaged devices
- Leverage multiple data sources, including server logging

iphLogparse.ps1



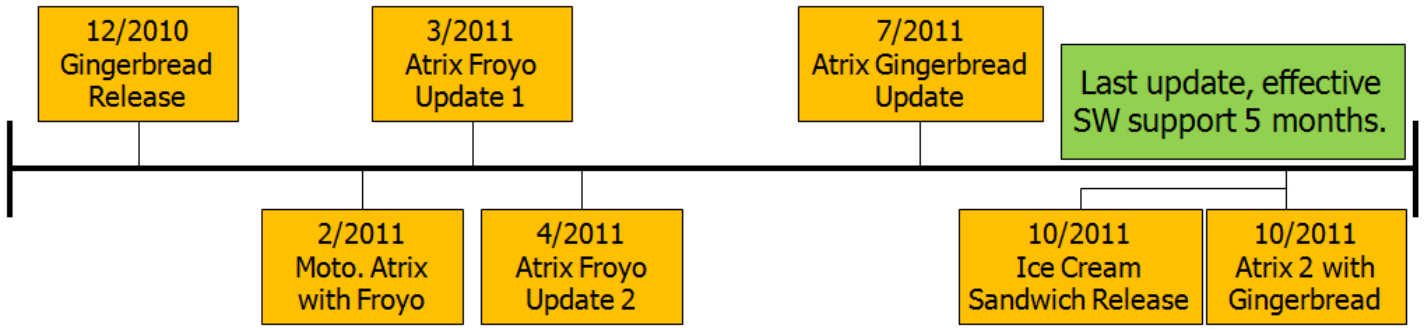
UserName	UserAgent	IOSDeviceType	IOSVersion	IOSReleaseDate	AppleBuildCode
username	Apple-iPhone3C1/902.206	iPhone 4	5.1.1	May-12	9B206
username	Apple-iPhone3C1/1001.403	iPhone 4	6.0	Sep-12	10A403
username	Apple-iPad2C4/1001.403	iPad 2	6.0	Sep-12	10A403
username	SAMSUNG-SCH-I535/100.40004				
username	SAMSUNG-SGH-I747/100.40004				
username	Apple-iPhone3C1/1001.403	iPhone 4	6.0	Sep-12	10A403
username	Apple-iPhone3C1/810.2	iPhone 4	4.3.3	May-11	8J2
username	TouchDown(MSRPC)/7.3.00052 /ENCRYPTSD				
username	Apple-i				
username	Apple-i				
username	Apple-i				
username	Apple-i				
username	Apple-i				
username	Apple-i				
username	Apple-i				

www.willhackforsushi.com/code/iphLogparse.ps1

#3: Patching Mobile Devices

- Using your device monitoring data, patch mobile devices at least quarterly
- This was a contentious issue in consensus review:
  - Not so terrible for iOS
  - Very hard for Android, Windows Phone, and BlackBerry

Typical lack of support; Android Fragmentation



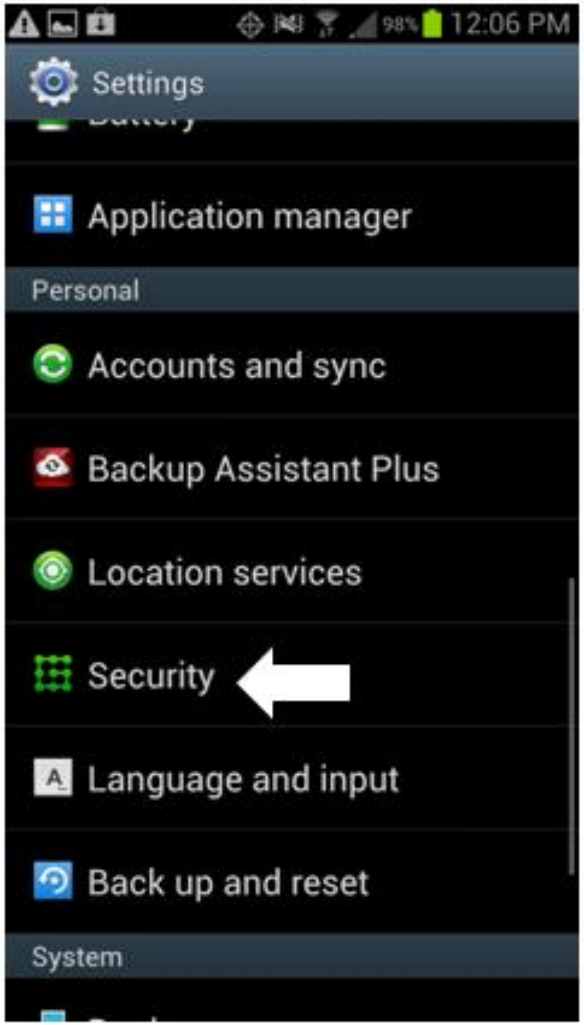
Update Monitoring

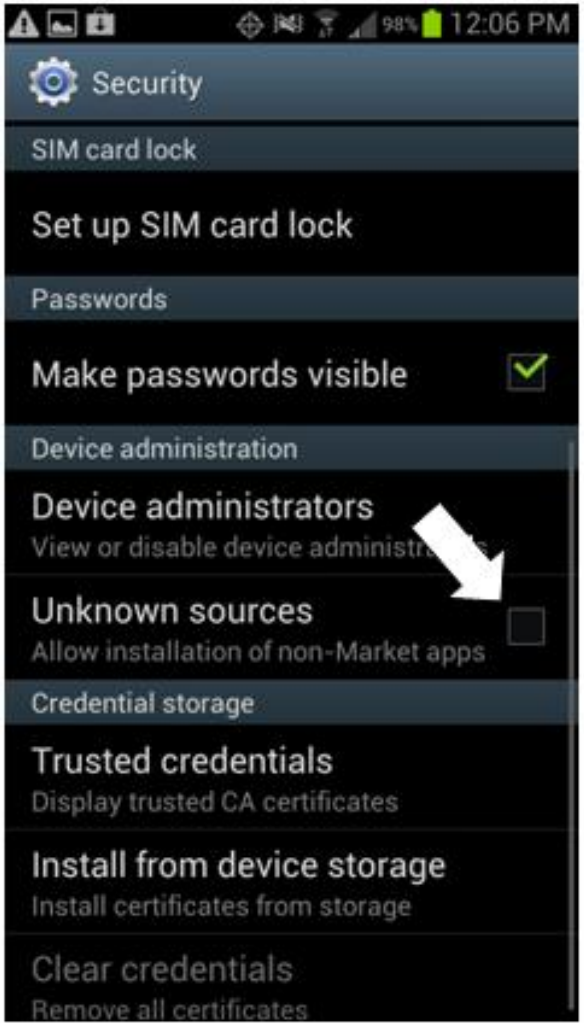
- Identify when new updates are available
  - Apple security-announce list (bit.ly/LMPOFh)
  - Android Security Discussion Group (bit.ly/VwYgOR)
- Watch for retired devices
  - Apple doesn't officially announce retired devices; Wikipedia
- Recognize that Android devices have a reduced product life with security fixes, and therefore a greater overall cost

#4: Prohibit Unapproved Third-Party App Stores

- The primary source of mobile malware is from third-party app stores
  - Android: Unofficial stores and "Unknown sources" configuration setting
  - iOS: Jailbroken devices
- Prohibit these devices from accessing company resources
  - Detect rooted/jailbroken devices with MDM, manual auditing

Android Non-Market App Control





#5: Disable Developer Debug Access

- Android USB debugging allows a local attacker to bypass security controls
  - Unlock or bypass device passcode
  - Install unauthorized applications with any permissions
  - Retrieve sensitive data
  - Execute vulnerabilities to root a device
- Cannot use an MDM to control this setting (not a feature of Android OS)
- Not on by default for most vendors
  - Commonly turned on with custom ROMs

USB Debug Universal Exploit

```
mobisec $ ./RunMe.sh
Please connect device with ADB-Debugging enabled now ...
Pushing busybox ...
Pushing su binary ...
Pushing Superuser app
Pushing ric
If all is successful i will tell you, if not this shell will run forever.
Running ...
Successful, going to reboot your device!
Waiting for device to show up again ...
Copying files to it's place ...
You can close all open command-prompts now!
After reboot all is done! Have fun!

mobisec $ adb shell
shell@android:/ $ su
shell@android:/ # grep psk /data/misc/wifi/wpa_supplicant.conf
        psk="L0NG@nd0Bscur3p455s0rd"
shell@android:/ #
```

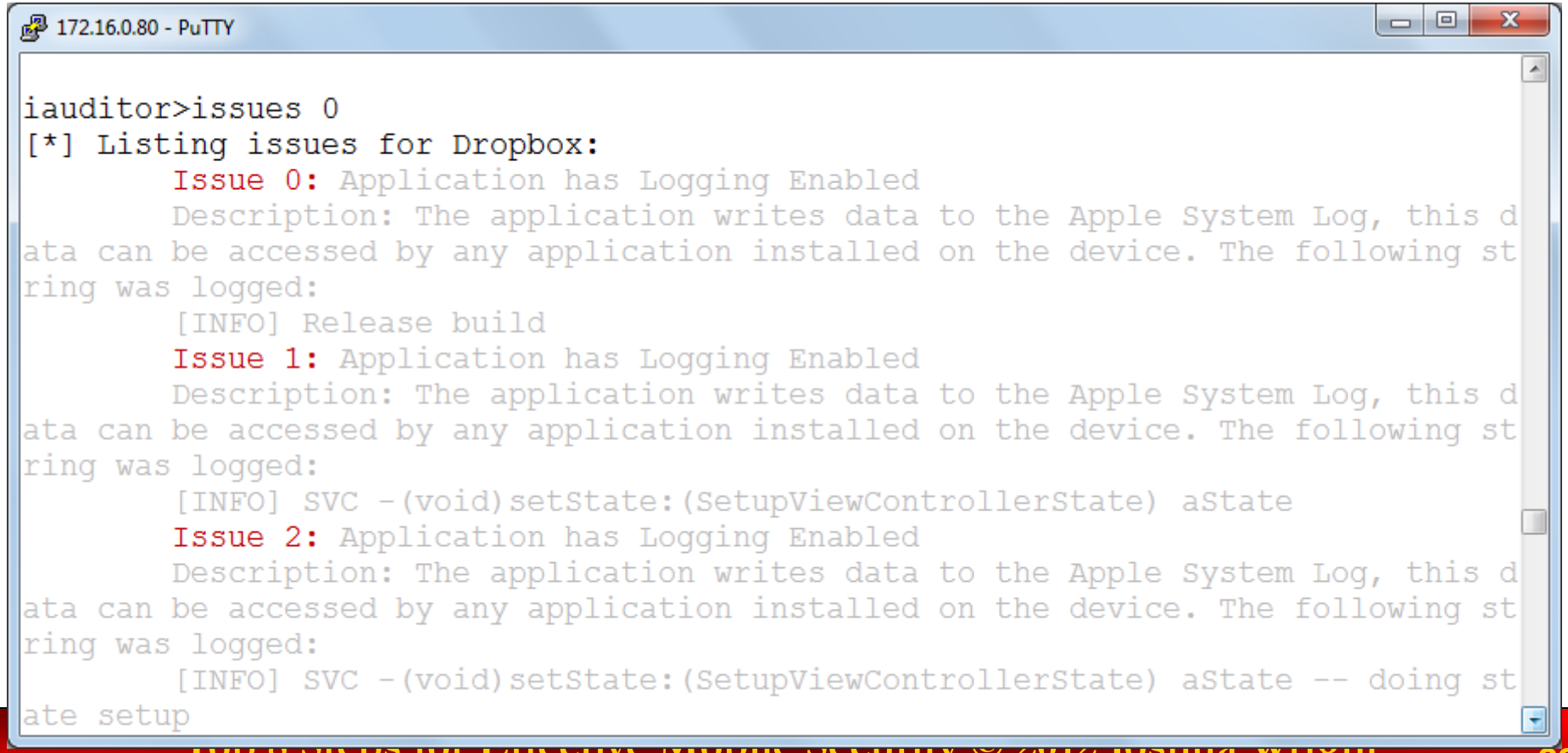
"adb restore" symlink exploit by Bin4ry, overwriting /boot/local.prop to gain root access. Relies on USB Debug privileges to exploit Android 4.1 and earlier.

#6: Evaluate App Security Compliance

- Many of the risks associated with mobile hinge on application security
- Applications on mobile devices should be evaluated to identify weaknesses, information disclosure
  - Alternative: Container-based MAM systems, which must be evaluated independently
- Manual and automated analysis systems available for app security checking

iAuditor

Command-line iOS static and dynamic analysis tool; requires jailbroken device. Still limited functionality, but promising for in-depth analysis.



#7: Prepare an Incident Response Plan

- Users will lose devices, or devices will be stolen
- Organizations must prepare for this incident to reduce the negative impact
  - Minimize local device data exposure
  - Educate users about device loss reporting
  - React with planned steps to a device loss event
  - Evaluate requirements for data breach notification
  - Review incident handling and improve process
- Step-by-Step checklist provided; must be augmented with org-specific policy steps

#8: Engage Management and Operational Support

- Non-technical step, but vitally important for thorough mobile security
  - Appoint a mobile device security evangelist
  - Adopt an MDM platform
  - Identify your supported device baseline
  - Develop mobile use policies
  - Leverage network architecture to stop misuse
  - Implement regular penetration tests

Top 8 guide details considerations and recommendations for each step

Outline

- Three Truths About Mobile Security
- Community Development Project
- Top 8 Mobile Security Steps
- Moving Forward
- Conclusion and Q&A

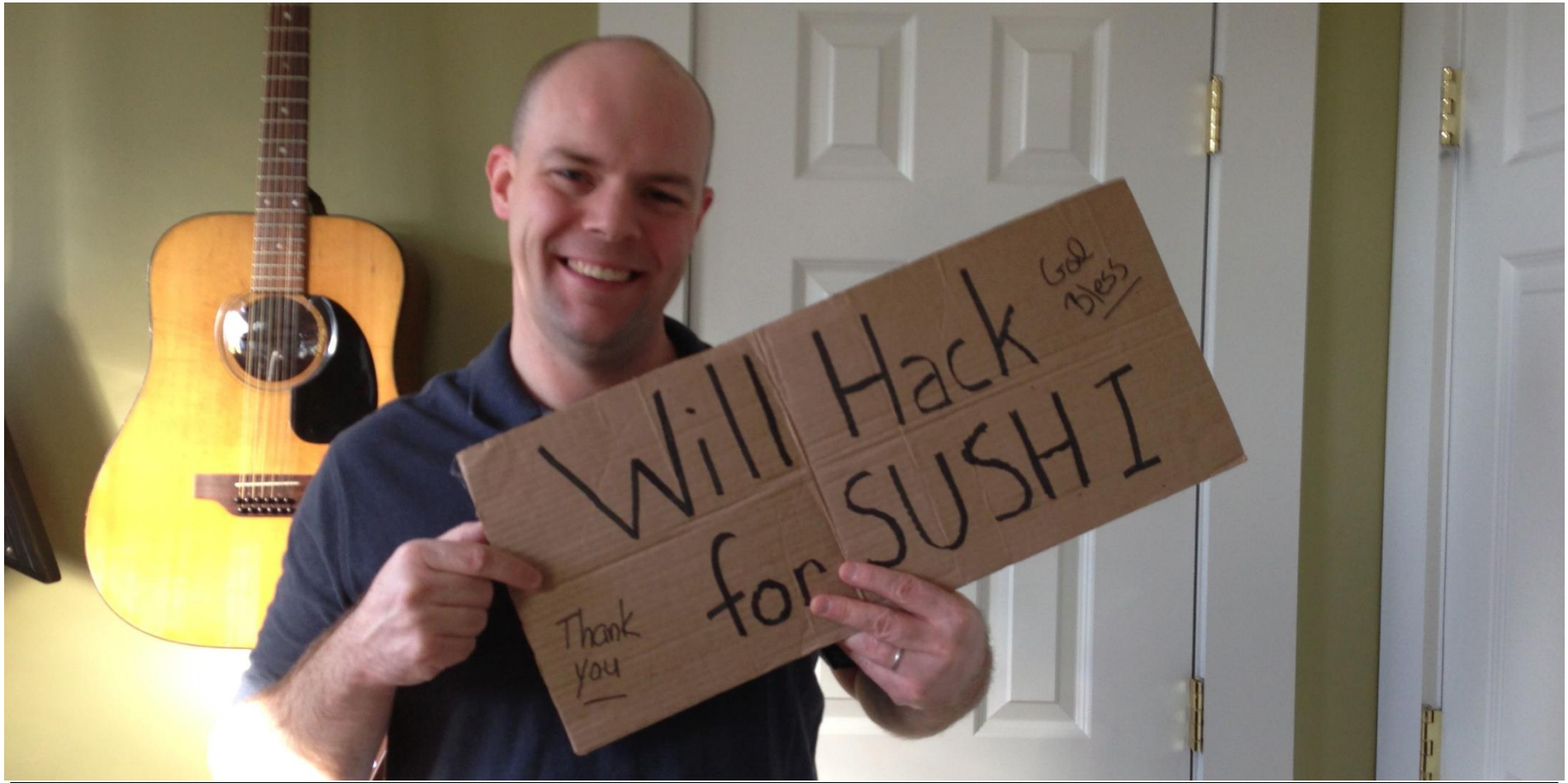
Moving Forward

- Second round of consensus feedback is currently being integrated
- Final proofing and layout design commences next week
  - Watch for announcements on SANS NewsBites, Twitter and WillHackForSushi.com

There Is Always Room For Improvement

- We can use your help!
  - We are always receptive to suggestions for improvement in the guide
- If you have some cycles to submit feedback, please contact me
- If you have stories about problems or solutions, I want to hear them!

A Big Thank You



Thank you to all the consensus reviewers who took time away from work and family to contribute to this important project!

Outline

- Three Truths About Mobile Security
- Community Development Project
- Top 8 Mobile Security Steps
- Moving Forward
- Conclusion and Q&A

Conclusion

- Implementing the Top 8 Mobile Security Steps will significantly improve mobile security
  - Based on the consensus opinions of respected experts in the field without motivation to sell you a product
- Please contact me if you want to contribute to the project for a draft copy of the guide
- Public availability to be announced shortly
- Thank you for attending!

Joshua Wright
jwright@sans.org
@joswr1ght
401-524-2911

Resources

- Apple security-announce list: bit.ly/LMPOFh
- Android Security Discussion Group: bit.ly/VwYgOR
- SANS SCORE Project: sans.org/score
- MS Exchange iOS Log Parsing: bit.ly/XuyKdG
- SANS NewsBites: sans.org/newsletters/newsbites
- iAuditor: bit.ly/OJA96S
- Android "adb restore" exploit: bit.ly/R4jxaQ
- This presentation:

Questions?