

Ch 1: The Mobile Risk Ecosystem



CNIT 128: Hacking Mobile Devices

Updated 1-12-16

The Mobile Ecosystem

Popularity of Mobile Devices

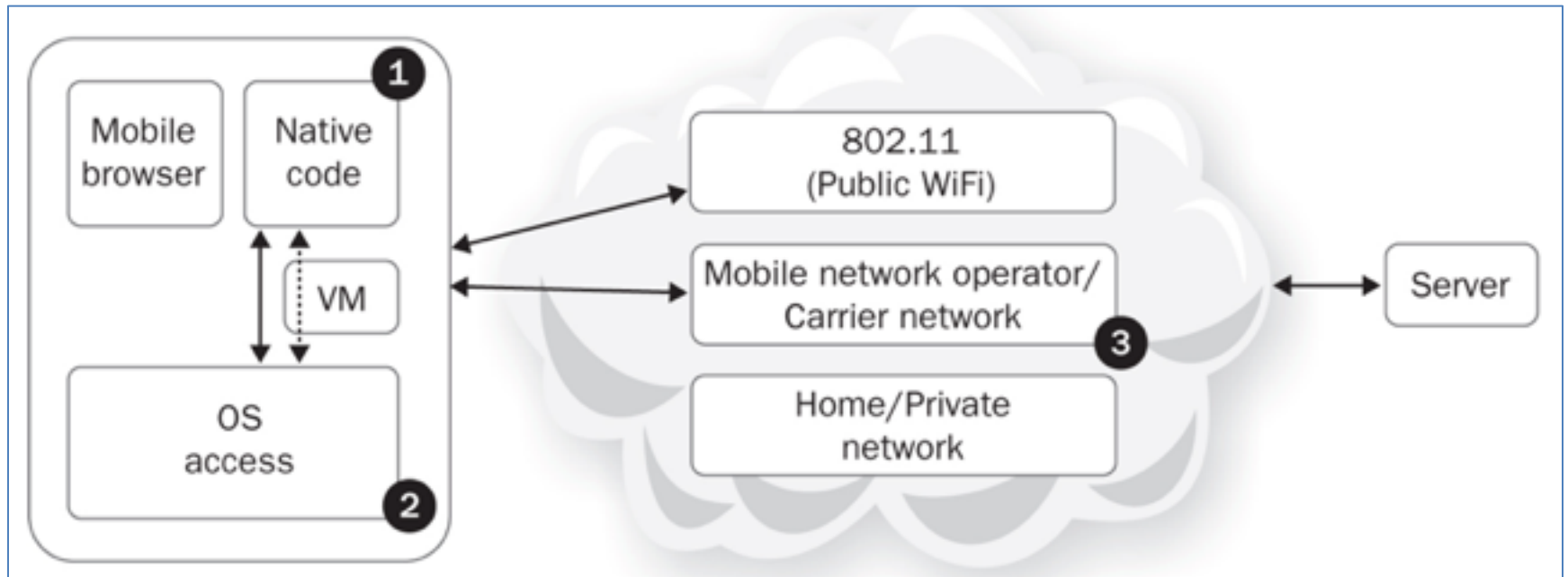
- **>300,000** Mobile apps developed in three years (2007–2010)
- **\$1 billion** Mobile startup Instagram's value within 18 months
- **1.1 billion** Mobile banking (*m-banking*) customers by 2015
- **1.2 billion** Mobile broadband users in 2011
- **1.7 billion** Devices shipped in 2012 (an increase of 1.2 percent over 2011)
- **6 billion** Mobile subscriptions worldwide (China and India account for 30 percent)
- **\$35 billion** Estimated value of app downloads in 2014
- **76.9 billion** Estimated number of app downloads in 2014
- **\$1 trillion** Mobile payments (*m-payments*) estimated in 2015
- **8 trillion** Estimated number of SMS messages sent in 2011

Insecurity of Mobile Devices

- McAfee's quarterly Threats Report indicated that mobile malware exploded 1,200 percent in the first quarter of 2012 over the last, or fourth, quarter of 2011.
- Trend Micro predicted 60 percent month-on-month malware growth on Android in 2012.
- IBM X-Force predicted that in 2011 "exploits targeting vulnerabilities that affect mobile operating systems will more than double from 2010."
- Apple's iOS had a greater than sixfold increase in "Code Execution" vulnerabilities, as tracked by CVE number, from 2011 to September 2012 (nearly 85 percent of the 2012 vulnerabilities were related to the WebKit open source web browser engine used by Apple's Safari browser).

The Mobile Risk Model

Mobile Network Architecture



1. Native Code

- Some languages like Java operate in a virtual machine
 - Run in a sandbox
 - Limited access to resources
- Other languages like Objective-C run directly on the OS
 - More access to resources
 - Less safe

2. OS Access

- Software running in a browser has limited access to the OS
 - Libraries
 - File system access
 - Interprocess communications
 - System calls

3. Internet Access

- Mobile devices commonly use the mobile carrier's network and public WiFi networks to connect to the Internet
- Increased opportunity for Man-in-the-Middle (MiTM) attacks
- Most mobile threats are variations on MiTM
 - MiTB (Man in the Browser)
 - MiTOS (Man in the OS)

Risk Model

- Identify stakeholders
- Enumerate assets
- Find relevant risks

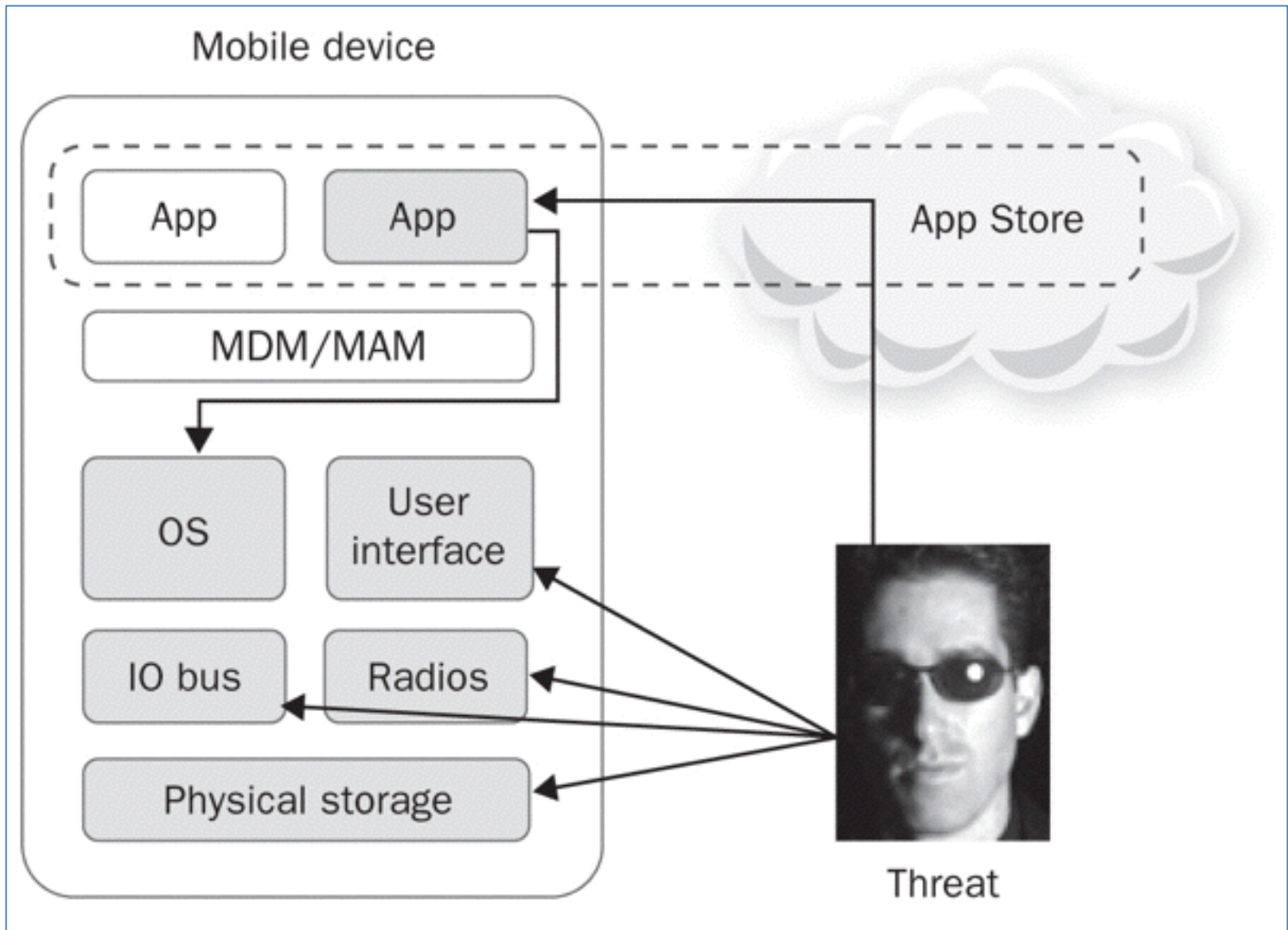
Stakeholders

- Mobile network operators (MNOs, aka carriers, telcos, and the #\$\$%&* companies who drop our calls all the time)
 - Device manufacturers (aka OEMs, hardware manufacturers, and so on)
 - Mobile operating system (OS) vendors like Apple and Google
 - Application Store curators (for example, Apple, Google, Amazon, and so on)
 - Organizational IT (for example, corporate security's mobile device management software)
 - Mobile application developers
 - End users

Assets

- OS manufacturer values phone as a source of revenue
 - Threats include
 - Apps that may crash the OS
 - Users who may jailbreak the phone
- Users value their privacy
 - Threats include
 - The OS which may send data back to the carrier for "statistical purposes"
 - Apps preloaded by the MNO which might send data out

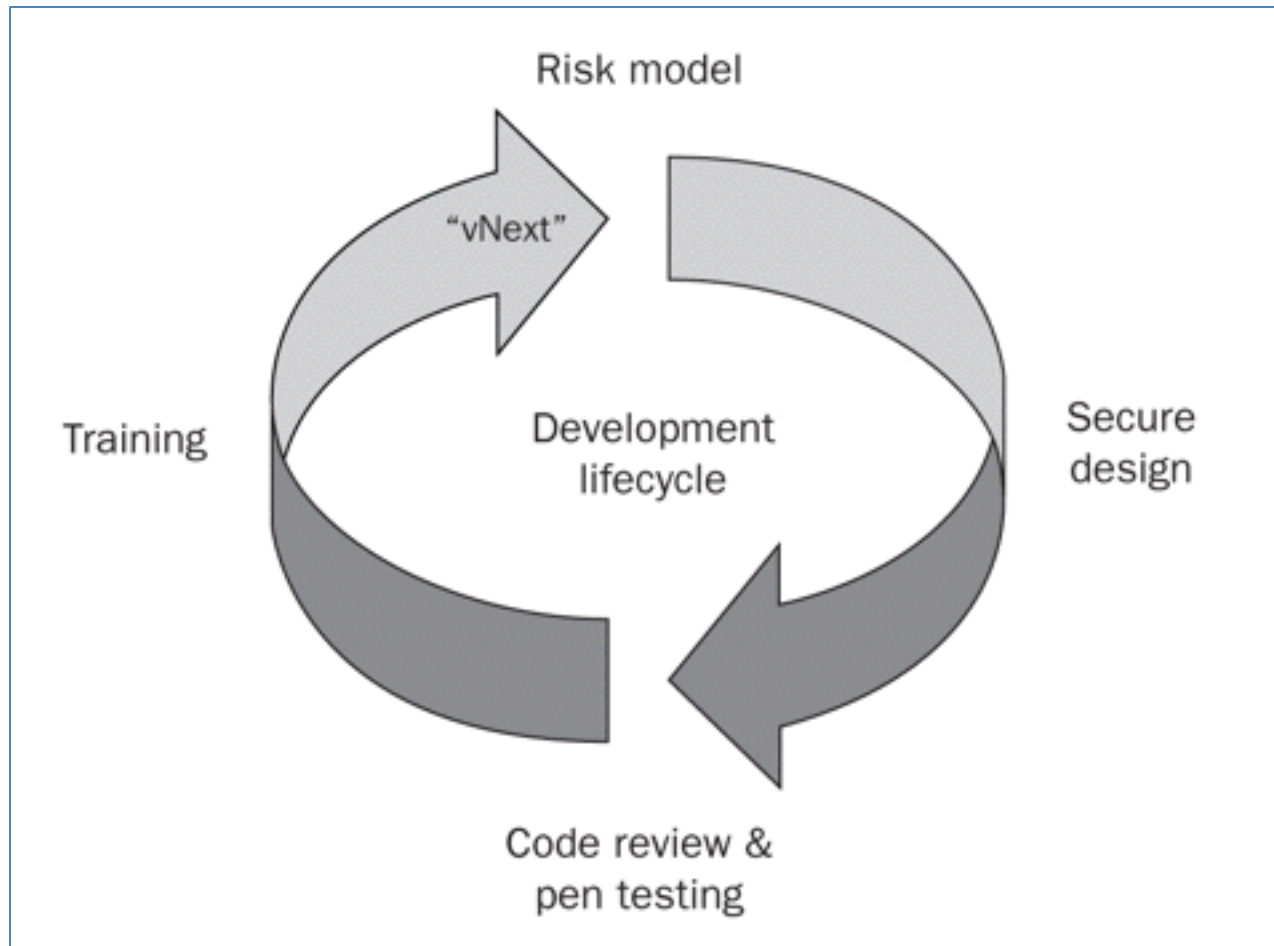
Attack Surfaces



Attack Surface

- Physical theft
 - Access to the **user interface, physical storage, IO Bus, and radios**
- App publication
 - Trojan horse or other malware
 - Access to OS resources
 - Interprocess communication
 - Phone may be jailbroken/rooted
 - App permissions may be weak
 - User may allow excessive permissions

Security in Development Lifecycle



vNext = next version

Special Risks

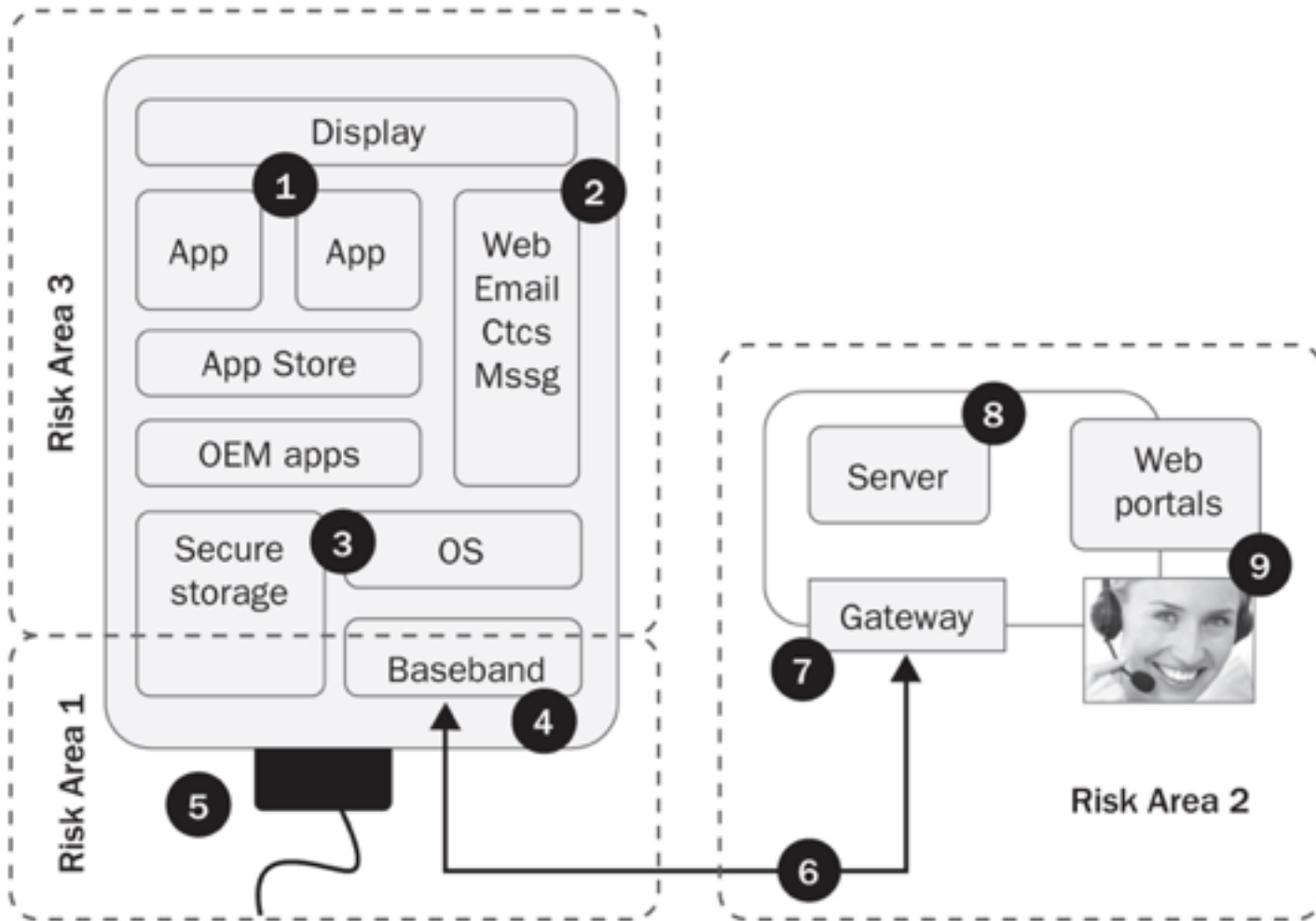
- Mobile devices are connected to many networks
 - Often insecure or unknown ones
- Mobile devices are used for personal, private purposes
 - Banking, selfies, SMS messages, phone calls

Anthony Weiner

- Member of US House of Reps.
- Destroyed his political career with sexting scandals
 - [Link Ch 1a](#)



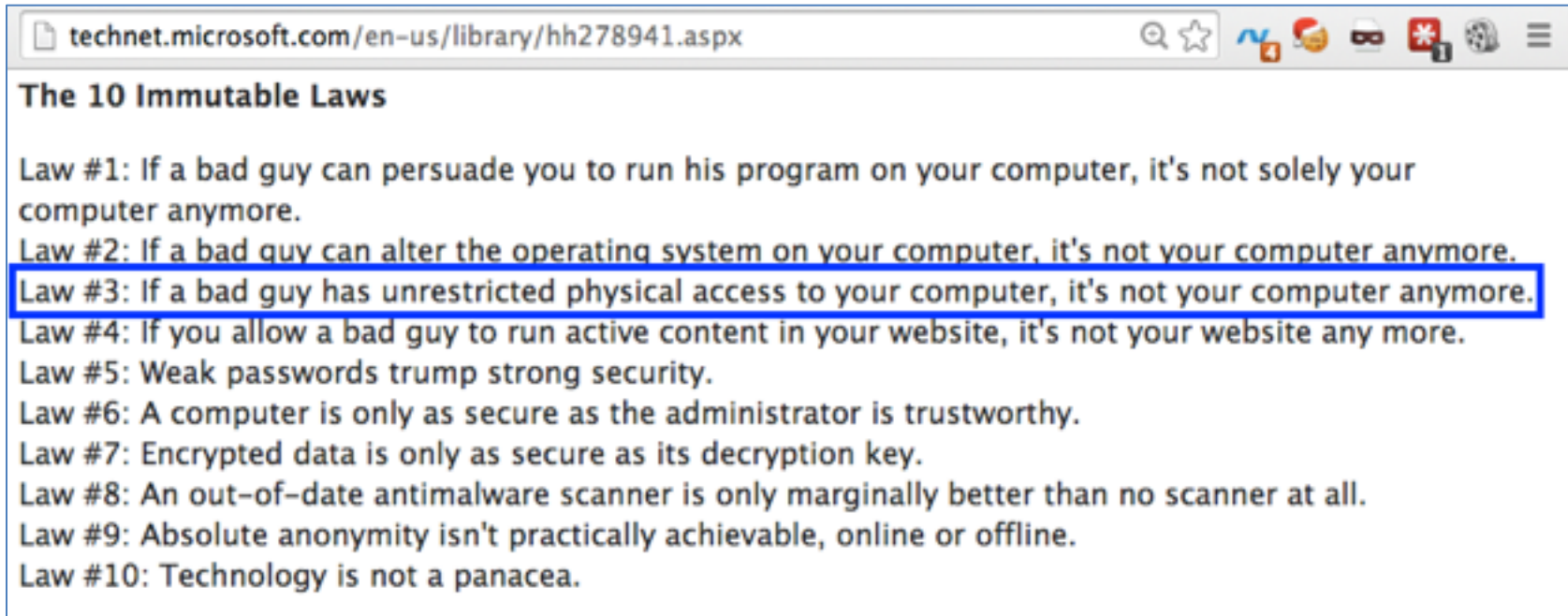
Areas of Risk



1. Physical Access

- Attacker with physical access to the device can overcome almost any security barrier
- Rooting/Jailbreaking continues to be popular
- Neither Apple nor Google can stop it
- No information stored indefinitely on a mobile device can be regarded as secure

The 10 Laws of Security



The screenshot shows a web browser window with the address bar containing the URL technet.microsoft.com/en-us/library/hh278941.aspx. The page title is "The 10 Immutable Laws". The content lists ten laws of security, with the third law highlighted by a blue border:

The 10 Immutable Laws

Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

Law #4: If you allow a bad guy to run active content in your website, it's not your website any more.

Law #5: Weak passwords trump strong security.

Law #6: A computer is only as secure as the administrator is trustworthy.

Law #7: Encrypted data is only as secure as its decryption key.

Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all.

Law #9: Absolute anonymity isn't practically achievable, online or offline.

Law #10: Technology is not a panacea.

- Link Ch 1b

5. USB Port

- USB connection gives direct access to the phone's storage, in "debug" mode
- Commonly used by law enforcement to collect all data from a phone

4. Baseband Attack

- If an attacker can get close to your phone, she can:
 - Trick your phone into connecting to a rogue cellular base station
 - Own your device almost completely, unless it's in Airplane Mode
- Baseband stack of radio chip hardware and firmware drives
 - WiFi, Bluetooth, GPS, Near Field Communication (NFC), etc.

2. Web, Email, Contacts, SMS

- 8. Most code is on the server side of apps
 - Most bugs and security errors are there too
- 9. Tech support will often give attackers access to your account or device with a phone call
 - Social engineering

Mat Honan

How Apple and Amazon Security Flaws Led to My Epic Hacking

BY MAT HONAN 08.06.12 | 8:01 PM | [PERMALINK](#)

- Hackers social-engineered Amazon and Apple for password resets
- Google account deleted
- AppleID broken into
 - Wiped iPhone, iPad, and MacBook
 - Link Ch 1c



Axway API Gateway



- Linux-based server
- Performs protocol translation
- Can block attacks
- Recommended by author
 - Links Ch 1d, 1e

App Risks

App Risks

- Apps are the primary attack surface for mobile devices
- Major security issues
 - Fragmentation
 - Sensitive information leakage
 - "Secure" on-device storage
 - Weak authentication
 - Failure to properly implement specs
 - BYOD

Open v. Closed Platforms



Figure 1-5 Closed versus open—which do you choose? Does it affect security?

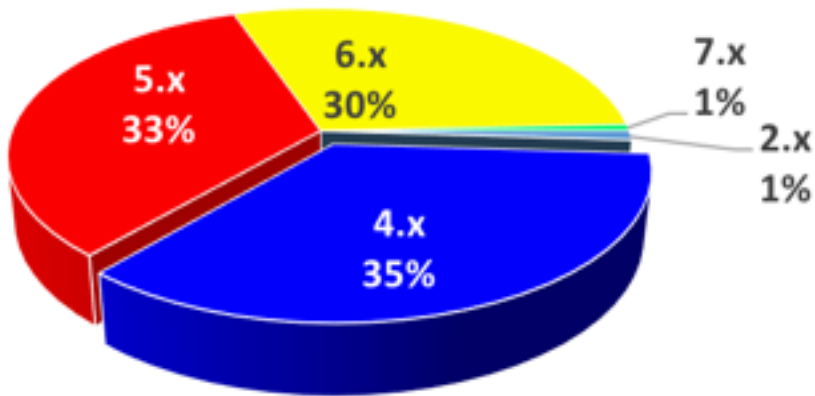
Open v. Closed Platforms

- Apple is closed and more secure
 - Code must be signed by Apple to run
 - Has Address Space Layout Randomization (ASLR)
 - Better code sandbox
 - No shell
- Android is open and less secure
 - Custom OS versions for each device manufacturer
 - Updates often blocked by MNOs

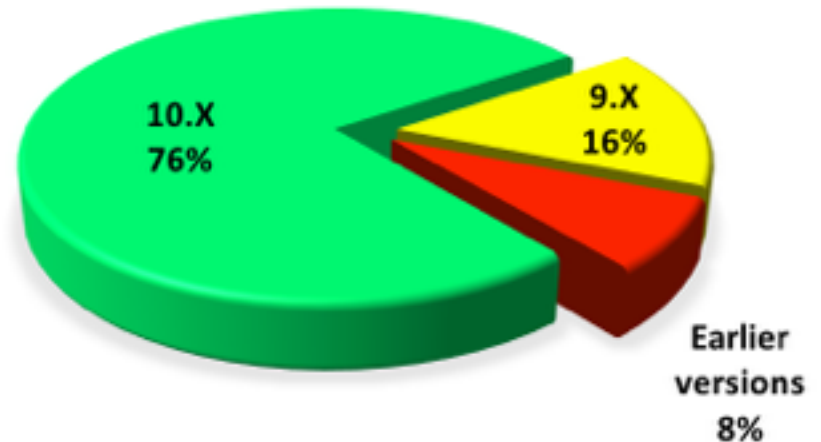
Fragmentation

- Updates are essential for security
- Very big problem for Android
 - Data from links Ch 1v, 1w

Android versions 1-9-17



iOS Versions 1-12-17



App Store Security

- Before appearing in the App Store, apps are
 - Manually reviewed by Apple for flaws and malware
 - Screened with a static analyzer
- Apps run in a sandbox
- Memory is segmented

Google Marketplace "Security"

Report: Malware-infected
Android apps spike in the
Google Play store



Zach Miners
@zachminers

Feb 19, 2014 2:03 PM

- More than 42,000 apps in Google Play contain information-stealing trojans as of 2013
 - Link Ch 1h

Installing Apps from Untrusted Sources (Side-Loading)

- Android devices can install apps posted directly to the Web by developers
- Not screened by Google at all

Xcode 7 allows anyone to download, build and 'sideload' iOS apps for free

- *Apple has changed its policy regarding permissions required to build and run apps on devices. Until now, Apple required users to pay \$99/year to become a member of Apple's Developer Program in order to run code on physical iPhone and iPads. As part of the new Developer Program, this is no longer required. Apps can be tested on devices, no purchase necessary.*
- June 10, 2015 (Link Ch 1s)

Sideloading

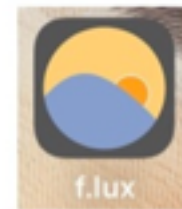
- iOS 7 and later allow "side-loading" apps directly from a computer
- Without using the App store
- Rarely used by non-developers
- Links Ch 1s, 1t

How to Sideload iOS Apps onto iPhone & iPad from Xcode

Jan 12, 2016 - 10 Comments



How to Side Load Apps to iOS Devices



osxdaily.com

Android Antivirus

14 best antivirus Android apps and anti-malware Android apps

BY JOE HINDY | JULY 16, 2014 | 173

250
SHARES



- Many options
- Pick one and use it
 - Link Ch 1i

Custom Software from Device Manufacturers

- Samsung added a TouchWiz overlay to some Android devices
- Introduced a serious vulnerability
 - Link Ch 1j

Major security vulnerability in some Samsung phones could trigger factory reset via web page

Sensitive Information Leakage

- Real issues found in mobile devices

- Authentication PINs to Google system logs in debug builds
- Session identifiers and credentials cached in WebView
- Inappropriate data stored in local SQLite databases
- iOS application snapshots recording screens with sensitive data when the app is suspended
- Sensitive credentials like application PINs being logged to the iOS keyboard cache

dmesg

- Samsung devices stored sensitive user-input data into device driver logs (the "dmesg" buffer)
- Those logs could be read by non-root users and other apps



Handsets currently deployed: **141,287,795** Raise Your IQ →

- Software that sends information about device usage back to the carrier for "quality of service monitoring"
 - Apparently including keylogging
- Concerns emerged that this data was excessive and not handled properly
 - Link Ch 1l

Input Validation

- Many attacks rely on input to one app that does unexpected things when passed on to another app
 - JavaScript injection to run code, including "eval"
 - URL query strings that execute application functions

"Secure" On-Device Storage

- All data on a mobile device is at risk
- Balance value of data with the risk
- Poor software has stored
 - Hard-coded passwords
 - AES encryption keys

Advice for Storing Sensitive Data

- Don't do it (if possible)
- Use existing storage facilities
 - Like iOS KeyChain
 - Much safer than custom code
- Use specially designed hardware to store secrets
 - SE (Secure Element) chip can be embedded in device, or on a SIM or SD card
 - Good security, if implemented correctly
 - Link Ch 1m

Weak Authentication

- Falsely assume that tokens on the mobile device are secret
 - Mobile Device Number (MDN)
 - Allowed password resets without a security question
- Popular authentication standards
 - OAuth
 - SAML
- Security will be analyzed in chapter 6

Exposed ICC-ID Numbers

Apple's Worst Security Breach: 114,000 iPad Owners Exposed



Ryan Tate

Filed to: EXCLUSIVE 6/09/10 4:50pm

1,071,665



2

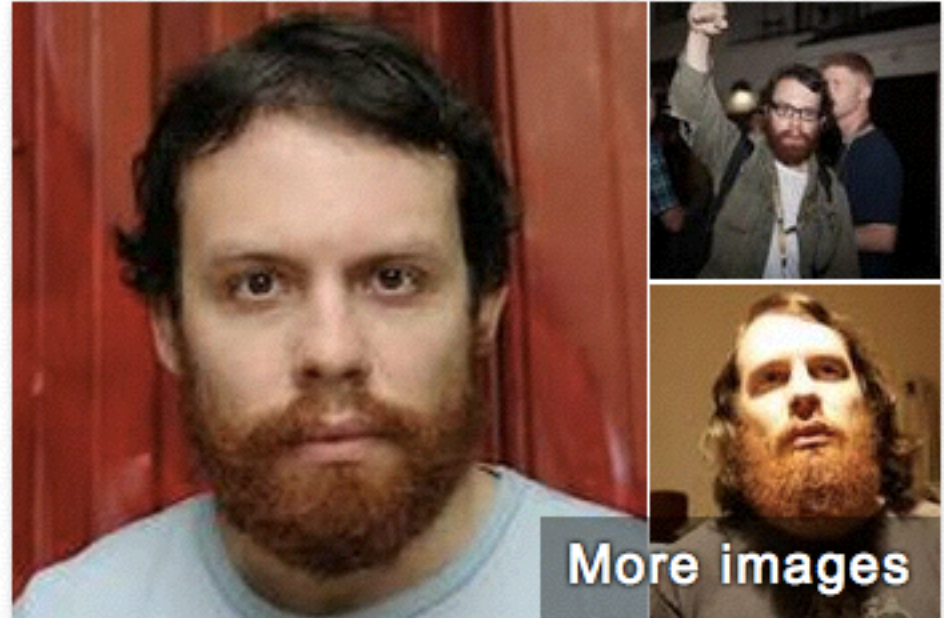


89014104243220	██████████	:	██████████@nytimes.com	←	Janet Robinson, CEO of NY Times
89014104243219	██████████	:	██████████@time.com	←	Ann Moore, CEO of Time Inc.
89014104243221	██████████	:	██████████@newscorp.com	←	Chase Carey, President/COO of News Corp.
89014104243315	██████████	:	██████████@hearst.com	←	Cathie Black, President of Hearst Magazines
89014104243315	██████████	:	██████████@dowjones.com	←	Les Hinton, CEO of Dow Jones
89014104243221	██████████	:	██████████@weinsteinco.com	←	Harvey Weinstein, Co-Founder of Weinstein Co.
89014104243315	██████████	:	██████████@bloomberg.net	←	Michael Bloomberg, Founder of Bloomberg LP

- Ch 1n

Weev

- Sentenced to 41 months in prison for the AT&T "hack"
- Released early because the venue (New Jersey) was improper
 - Link Ch 1o



weev

Andrew Alan Escher Auernheimer, also known by his pseudonym weev, is an American grey hat hacker, white supremacist, and Internet troll. [Wikipedia](#)

Failure to Properly Implement Specs

- Using cleartext username and password in a "WS-Security" header (link Ch 1p)
- Leaving debug mode on in production systems
 - SSL certificate validation disabled
- Fast development leads to insecure code
 - Speed to market is valued more highly than security

Android Tablet Vulnerabilities

Store	Device	Price	Trust Score	Trustworthiness	OS	Known Vulnerabilities	Security Backdoor	USB data theft	Security Misconfigurations
Google	HTC Nexus 9	\$399.99	10	Trustable	5	0	✓	✓	✓
Multiple Stores	Samsung Galaxy Tab 3 Lite	\$99.99	8.6	Trustable	4.2.2	0	✓	✓	✓
BestBuy	DigiLand	\$49.99	**	N/A	4.4.0	Futex	X	✓	X
Walmart	Nextbook	\$49.00	7	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	✓
Target	RCA Mercury 7"	\$39.99	6.9	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	✓
Kmart	Mach Speed Xtreme Play	\$39.99	6.5	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	X
Walmart	Pioneer 7"	\$49.99	6.4	Semi-Trustable	4.2.2	Masterkey and FakeID	✓	✓	✓
Walmart	Ematic	\$49.99	6.3	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Staples	Mach Speed Jlab Pro	\$39.99	6.1	Semi-Trustable	4.4.2	FakeID and Futex	✓	X	✓
Walmart	RCA 9"	\$69.00	5.8	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Fred's	Craig 7"	\$49.99	5.5	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Walmart	Worryfree Zeepad	\$47.32	4.4	Suspicious	4.2.2	FakeID and Futex	X	X	X
Walgreens	Polaroid	\$49.99	2.7	Suspicious	4.1.1	Masterkey, FakeID, Heartbleed, and Futex	X	✓	X
Kohl's	Zeki	\$49.99	2.1	Suspicious	4.1.1	Masterkey, FakeID, Heartbleed, and Futex	X	X	X

- Link Ch 1q

BYOD

- Bring Your Own Device to work
- Recommendation
 - Keep sensitive data on servers
 - Only put non-sensitive data on mobile devices

Mobile Device Management (MDM)

- Enterprise solutions to centrally administer mobile devices
- Important but immature field
 - Link Ch 1r



Key Countermeasures for App Developers

- Architecture and design
 - Align architecture with value of assets in play
- Input/Output validation
- Caching and logging
 - Disable or mitigate logging of confidential data
- Error handling
 - Don't just fail-open; enforce security checks

Key Countermeasures for App Developers

- Device loss or capture
 - Prepare for phone theft
 - Enable remote wipe of your data
- Server-side strength
 - Implement strong controls
 - Application-level protections
 - Strengthen self-help password reset system