INTRODUCTION TO iOS SECURITY Lecture 16

COMPSCI 702 Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad Rizwan Asghar

April 20, 2021



iOS SECURITY: MAIN TOPICS



- Introduction to iOS security
- iOS device and app trust evaluation
- Address Space Layout Randomisation (ASLR)
- iOS sandboxing
- iOS encryption
- Enterprise security in iOS
- iOS jailbreaking
- Recent iOS (in)security incidents
 - If we get some time

PORTABLE DEVICES

What kind of portable devices do people carry?



Are smartphones different from other devices?

– How?

SMARTPHONES ARE DIFFERENT



Always with us

- Likely to be **lost** or stolen
- Contain all sorts of useful data
 - E.g., Passwords, personal contacts, documents and emails
- Always ON
 - Present a continuous target
- Change networks repeatedly
 - Multiple wireless and cellular networks
 - Greater chance of Man-in-the-Middle (MitM) attacks
 - Especially on FREE WiFi
- Password protection
 - Less likely to use **long** pass phrases because of keyboard limitations

STANDARD SECURITY ATTACKS

- Smartphones are subject to almost all of the standard security attacks
 - Malicious websites
 - Trojan horses
 - Buffer overflow attacks
 - Social engineering



WHAT ARE WE TRYING TO PROTECT?

- Data on the device
- Data sent or received by the device
- Our applications (apps)
- Operating System (OS)



- Making sure the device works properly
- Making sure we do not get charged for services we have not intentionally used

IDEA BEHIND iPHONE



- Steve Jobs, CEO at Apple Inc. conceived an idea of multi-touch screen
 - Essentially removing the physical keyboard and mouse
- When Jobs reviewed the prototype, he came up with a second idea of implementing the technology onto to a mobile
 - The whole effort was called **Project Purple 2**, began in 2005
- Jobs introduced iPhone as a combination of
 - A widescreen iPod with touch control
 - A revolutionary mobile phone
 - A breakthrough Internet communicator

iPHONE OS 1.0 (2007)



- A cut down version of OS X
- Very little in terms of security
 - No privilege separation
 - All processes ran as root
 - No code signing
 - No Data Execution Prevention (DEP)
 - No Address Space Layout Randomisation (ASLR)
 - No sandboxing





- There was an attempt to reduce the attack surface
- No support of flash or shell
- Limited file formats
 - MobileSafari cannot deal with all formats acceptable to Safari
 - Safari is the Apple web browser
 - PDF viewer only parses some features
 - PDF rendering has still been used in many exploits

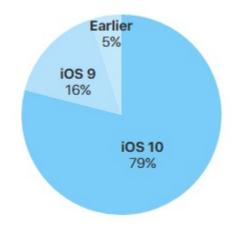
iOS 2 – 10



- iOS 2 (2008) introduced the App Store
- Security was taken much more seriously

USAGE OF iOS

- As of February 20, 2017
 - 79% devices use iOS 10
 - 16% devices use iOS 9
 - 5% devices use earlier versions



Source: <u>https://developer.apple.com/support/appstore/</u>

HOW CAN WE THE USER HELP?

Use a passcode

- Prevents easy access to others
- Used to encrypt files on the device
- Combined with auto-lock and require passcode after
 - It means that an attacker probably has to enter a passcode
 - Even if the device was unlocked when taken

••••• 2degrees 🗢 11:00 am	∦ 100% ■ •
Settings General	
Auto-Lock	5 Minutes >
Restrictions	On >
	••••• 2degrees ♀ 11:00 am ∦ 100% ■• Settings
Date & Time	Control Center
	C Do Not Disturb
Keyboard	General >
International	Wallpapers & Brightness
	Sounds
	Passcode >
iTunes Wi-Fi Sync	Privacy >
VPN Not	
	Mail, Contacts, Calendars
Reset	Notes >

PASSCODES

Use a strong passcode

Simple passcode off —

Brute-forcing

 Springboard (home and login) screen app) slows down after repeated attempts

- Users can set the device to erase data quickly after 10 attempts

iPhone is of try again in		∦ 100% ■	
	Simple Passcode	\bigcirc	
ode	A simple passcode is a 4 digit n	umber. •••••○ 2degrees 중 11:02 am	
	Voice Dial	Back Require Passcode	
	Music Voice Control is always e	Immediately	
		After 1 minute	
	ALLOW ACCESS WHEN LOCKE	After 5 minutes	
	Siri	After 15 minutes	
and login		After 1 hour	
s down	Passbook	After 4 hours	
ots	Reply with Message	Shorter times are more secure.	
levice to			
after 10	Erase Data		
	Erase all data on this iPhone aft passcode attempts.	er 10 failed	
	Data protection is enabled.		

DELAYS BETWEEN PASSCODE ATTEMPTS iPhone is disabled

try again in

Attempts	Delay Enforced
1-4	None
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

disabled 훅	11:02 am	∦ 100% ■ •
1 minute Pass	scode Lock	
Simple Passcoo	le	\bigcirc
A simple passcode	e is a 4 digit n	umber. ••••• 2degrees 중 11:02 am
Voice Dial		C Back Require Passcode
Music Voice Contro	ol is always e	Immediately
		After 1 minute
ALLOW ACCESS V	WHEN LOCKE	After 5 minutes
Siri		After 15 minutes
		After 1 hour
Passbook		After 4 hours
Reply with Mess	sage	Shorter times are more secure.
	5	
Erase Data		
Erase all data on the passcode attempts		er 10 failed
Data protection is	enabled.	

OTHER RESTRICTIONS

- To change these, you need the restrictions passcode
 - Different from device passcode

●●●●● 2degrees 11:05 am く General Restrictions	 ३ 99% ■ ●●●●● 2degrees ◆ General Restrict 	,	
Disable Restrictions	ALLOWED CONTENT:		
ALLOW:	Ratings For	New Zealand >	
💋 Safari	Music & Podcasts	Clean >	
Camera	Movies	R16 >	
FaceTime	TV Shows	PGR >	
iTunes Store	Books	Restricted >	
iBooks Store	Apps	All >	
Installing Apps	Siri	All >	
Oeleting Apps	Websites	All >	
In-App Purchases	Require Password	15 minutes >	
🕖 Siri	Require password for purchases.		
	PRIVACY:		

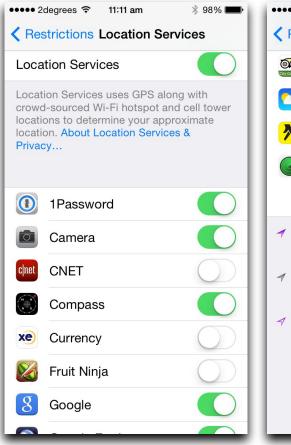
APP PRIVILEGES

- Since iOS 6, the user is asked when apps first attempt to use "private" information
- Restrictions can be applied or lifted at any time

●●●●○ 2degrees 중 11:07 am	∦ 99% ■ •
Ceneral Restrictions	
PRIVACY:	
Location Services	>
Contacts	>
Calendars	>
Reminders	>
Photos	>
Bluetooth Sharing	>
Microphone	>
Twitter	>
Facebook	
Advertising	>

E.G. LOCATION SERVICES

 Every time you leave the Restrictions screen and return to it, you are required to re-enter your restrictions passcode



•••	• 2	degrees ᅙ	11:14 am	×	97% 💻
Restrictions Location Services					
O City G	O uides	TripAdvisor			\bigcirc
[Weather		1	
7		Yellow®			
		Find My iF	Phone	1	>
		System Se	ervices		>
 A purple location services icon will appear next to an item that has recently used your location. 					
1	A gray location services icon will appear next to an item that has used your location within the last 24 hours.				
P	An outlined location services icon will appear next to an item that is using a geofence.				
	A geofence is a virtual perimeter around a location. Apps like Reminders use geofencing to notify you when you arrive at, or leave, these locations.				
1				_	_

FIND MY iPHONE

- Must be set up on the device
 - Uses the user's Apple ID
- Lock lost mode
 - If no passcode, will ask for one
 - Can put a message and phone number on the lock screen
- Tracking of the device begins
- Email sent to user's account when any event happens
- Erase contacts, email, music, and settings
 - Done very quickly by deleting the file system encryption key



STOP THIEF



- Mobile phone theft is a major problem
- Manufacturers now prevent device erasure without the correct password
- iOS 7 has "Activation Lock" turned on with "Find my iPhone"
 - Apple ID stored on Apple's activation servers
 - Cannot turn off "Find my iPhone", erase, reactivate or use without the ID and password
 - For details, see: https://support.apple.com/en-us/HT201365

REMOTE DISABLING/ DELETION OF APPS



- The infamous kill switch Apple can disable or delete an app on your device
 - Not clear that it has been used at all
 - Google used it on Android devices
 - Windows 8 app store apps also can be removed remotely

APPLE'S TERMS AND CONDITIONS



 "Notwithstanding any other provision of this Agreement, Apple and its licensors reserve the right to change, suspend, remove, or disable access to any iTunes Products, content, or other materials comprising a part of the iTunes Service at any time without notice. In no event will Apple be liable for making these changes. Apple may also impose limits on the use of or access to certain features or portions of the iTunes Service, in any case and without notice or liability."

GOOGLE'S TERMS AND CONDITIONS



"Removal or Unavailability of Products. Subject to these Terms, Products that you purchase will be available to you through Google Play for the period selected by you in the case of a purchase for a rental period, and in other cases as long as Google has the right to make such content available to you. In certain cases (for example, if Google loses the relevant rights, discontinues a service or a Product is discontinued, breaches applicable terms or the law), Google may remove the Product from your Device or cease providing you with access to certain Products that you have purchased. If we are able to do so, Google will provide you with reasonable prior notice of any such removal or cessation. If you are not able to download a copy of the Product before such removal or cessation, then Google will, offer you either (a) a replacement of the Product if possible or (b) a refund of the price of the Product."

SECURITY PROVISIONS



- iOS now has many provisions to keep devices secure
 - Mandatory code signing and code signing enforcement
 - Protects against the execution of unauthorised native code
 - Address Space Layout Randomisation (ASLR)
 - Makes Return Oriented Programming (ROP) attacks harder
 - Sandboxing of apps
 - Data encryption
 - On the device and in the backups created with iTunes
 - Vulnerabilities in the backup restore process are one of the main ways to break into a device

RESTORING BACKUP



Cannot restore backup without the password (different from device passcode)

KNOWN VULNERABILITIES

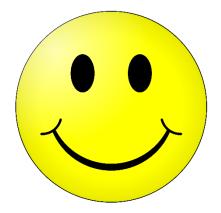


- All versions of iOS before 4.3.5 are vulnerable to an SSL MitM attack
 - Many Android devices are also susceptible to this
 - Since iPhone(1), 3G and 1st and 2nd gen iPod cannot be upgraded beyond this, they will always be susceptible
- All iOS devices before October 2009 (up to and including many iPhone 3GS devices) are vulnerable to the 24kPwn or 0x24000 segment overflow exploit
 - This allowed the bootrom signature checks on the low-level bootloader to be avoided
 - Great for jailbreaking
- Several new bugs, flaws and vulnerabilities discovered for all new versions of iOS
 - The basis for more recent jailbreaks





See the next lecture



Questions?

Thanks for your attention!