iOS SECURITY: THE FBI VS APPLE
Lecture 22

COMPSCI 702
Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

May 03, 2021

FBI-APPLE DISPUTE

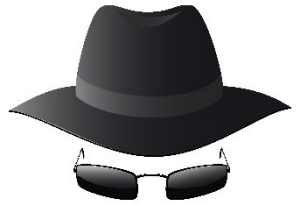
- In 2016, Apple was asked to provide software to unlock a phone
  - To assist the FBI's ongoing investigation
  - San Bernardino mass shooting in December 2015
- The phone is an iPhone 5c
  - A model sold in late 2013 and early 2014
- The model supports disk encryption
  - Meaning straightforward forensic techniques to examine the phone's storage cannot be used
- The data on disk cannot be decrypted without knowing the correct cryptographic key

WHAT WAS APPLE ASKED TO DO?

- In this case, the FBI requested **Apple to create and digitally sign** a special version of iOS which is **modified in three ways**
  - iOS can be set to erase its keys after **10 incorrect passcode** guesses, but the FBI wants software with this **feature disabled**
  - iOS imposes increasingly long delays after incorrect passcode guesses to slow down guessing, but the FBI wants **no delays**
  - the FBI wants a means to electronically enter passcodes, allowing it to **automatically try** every possible code quickly

- Apple announced its intent to oppose the order
  - Creation of a backdoor would pose security risks for customers

CAN THE FBI WRITE ONE?



- Possible, although it would be a considerable amount of work for the FBI to do reverse engineering
- However, iPhones are designed to only run software which is digitally signed by Apple
- In the case of iPhones, the signing key is known only to Apple
- So even if the FBI wrote its own software, the phone would not run it unless it were signed by Apple

SIMILAR REQUESTS IN THE PAST

- Apple has unlocked phones 70 times in the past for the authorities
- However, this was a very different proposition for older phones without disk encryption
- For older phones with no encryption, Apple already had a software version to bypass the unlock screen
  - Used, for example, to unlock phones when customers had forgotten their passcode

AFTERMATH OF THE UNLOCK

- The US government dropped the case after the FBI successfully pulled data from the iPhone
- The FBI said that the tool they used can only unlock the iPhone 5C used by the San Bernardino suspect
  - As well as older iPhone models lacking the Touch ID sensor
- The FBI also confirmed that the tool was purchased from a third party but would not reveal the source

THE FIGHT IS NOT OVER

- The U.S. said it will keep fighting to get the company's help
- This time in accessing the phone of a drug dealer in the New York borough of Brooklyn
- They argue the company should help because it provided assistance in earlier cases

UPDATE: MARCH 2017

- **Apple hired the guy** who helped it fight the FBI's order to hack the San Bernardino shooter's iPhone

- https://www.businessinsider.com.au/apple-hires-security-researcher-jonathan-zdziarski-fbi-hack-san-bernardino-iphone-2017-3?r=US&IR=T

- https://www.zdziarski.com/blog/?p=7016

RESOURCES

- **A Technical Perspective on the Apple iPhone Case**
  https://www.eff.org/deeplinks/2016/02/technical-perspective-apple-iphone-case

- **The FBI's Court Motion**
  https://www.documentcloud.org/documents/2714170-SB-Shooter-MOTION-Seeking-Asst-iPhone.html#document

- **Apple opposes judge's order to hack San Bernardino shooter's iPhone**
  http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/

RESOURCES (2)

- **San Bernardino iPhone: US ends Apple case after accessing data without assistance**
  https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone

- **San Bernardino iPhone hack won't work on newer models, says FBI**
  https://www.theguardian.com/technology/2016/apr/07/san-bernardino-iphone-hack-work-newer-models-fbi-james-comey

- **FBI fights Apple again, for another phone**
  http://m.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11619574

Questions?

Thanks for your attention!