RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: **SPO2-W04**

IOS TRUSTJACKING
NEW IOS VULNERABILITY

Roy Iarchy

Head of Research, Modern OS Security
Symantec
@Royiarchy

Adi Sharabani

SVP, Modern OS Security, Symantec
CEO & Co-Founder, Skycure
@AdiSharabani

Agenda

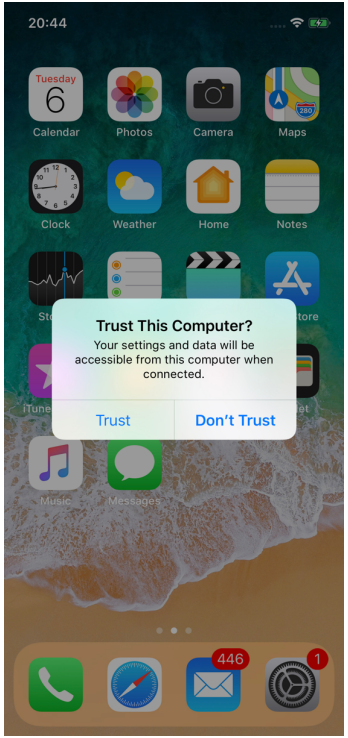
- Background
- Recap of related past attacks
- Remote Videojacking Attack + Demo
- Advanced Trustjacking attack flows + Demo
- Summary & Recommendations

A day in the office

- Working with several iOS devices
- Weird behavior

Background

- Trust This Computer?
  - Background
  - Why use it?



Background

- Behind the scenes
- Key relevant daemons:
  - usbd
  - usbmux
  - lockdown
  - authd

Juice jacking

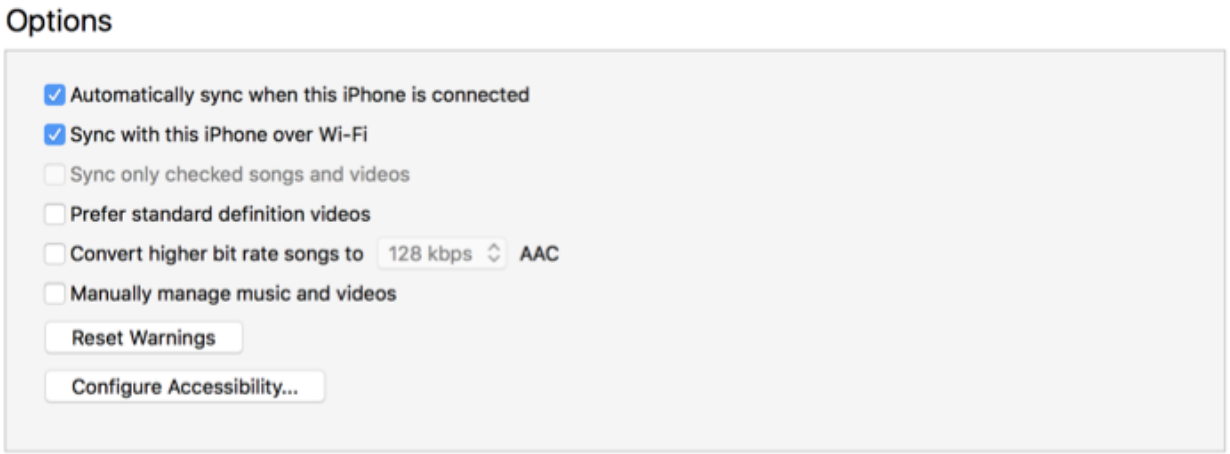
https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Videojacking (leveraging HDMI interface)

https://krebsonsecurity.com/tag/video-jacking/

But we promised you a remote (wifi?) hijacking disclosure…

iTunes Wi-Fi Sync



- Uses the trust established during initial USB connection
- Relies on implementation of usbmux over network

IOS TRUSTJACKING

iOS Trustjacking – Attack Flow

- Trust == One time mistake
- Victim side
- Attacker side
  - Accessing device information
  - Accessing device logs
  - Rebooting the device (can be used for DoS attack)
  - Leveraging the developer image

REMOTE VIDEOJACKING DEMO

Using developer image for advanced attacks

http://embed.ustudio.com/embed/DTkChBHtXcx2/UfREnMM6AY40

IOS TRUSTJACKING ADVANCED DEMO

Backup and restore

https://embed.ustudio.com/embed/DTkChBHtXcx2/UMQhu5XRecFM

Backup format

- The decision whether the backup is encrypted or not is initiated by the computer side but then enforced on the client side
- If legitimate user opted in to encrypt backup password will be required disabled that
- If user didn't choose to encrypt backup attacked to enforce encrypted backup on the user's device ☹
- Getting photos out of the device
  - Info.plist - contains information about the device and installed apps
  - Manifest.plist – contains information about the backup and installed apps
  - Status.plist - information regarding the backup
  - Manifest.db - SQLite3
  - Files paths converted to SHA1 file names

Remote Backup

- Obviously the remote backup allows us access to:
  - Messages
  - Contacts
  - App data

IOS TRUSTJACKING ADVANCED DEMO

- Installing / Deleting Apps
- Replacing Apps
- Private API Access

https://embed.ustudio.com/embed/DTkChBHtXcx2/UX50hxVoh6kp

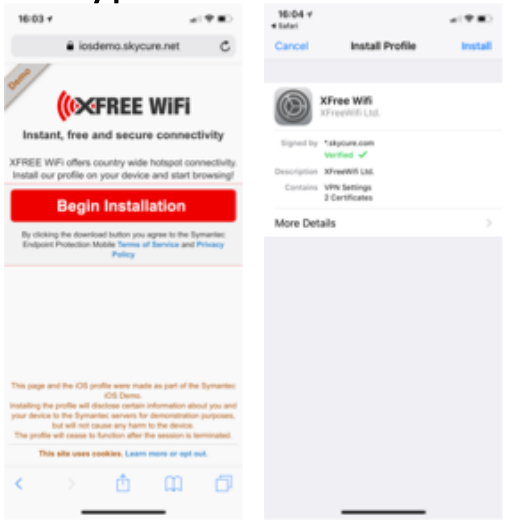
Pre-Trust vs. Post-Trust Attacks

- Trusting a malicious computer
- Attacking a trusted computer (Post-Trust Attack)
- Temporal access to a computer (Pre-Trust attacks)
  - Won’t work as Apple mitigated it by generating a unique key-pair for each connection

Is the attack confined to Wi-Fi only?

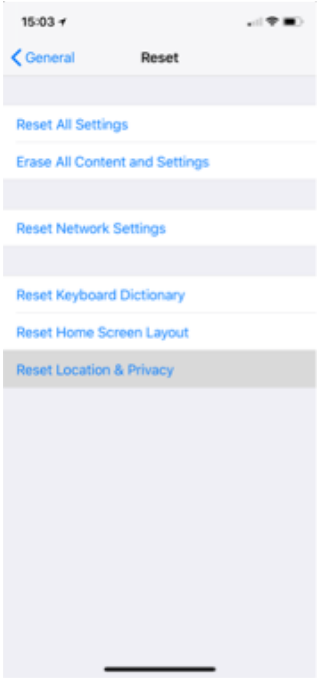
Wi-Fi Sync & Bonjour

- mDNS (Bonjour) used for device discovery
- Replicating / tunneling mDNS + Malicious Profiles attack
  - Malicious Profiles can also allow attacker to redirect and decrypt traffic
  - Allows access to the mobile phone without the need to be on the same network nor location
- More on Malicious Profiles:
  - https://www.symantec.com/connect/blogs/malicious-profiles-sleeping-giant-ios-security



Recommendations

- End Users:
  - Clear trusted computer settings
    - Settings > General > Reset > Reset Location & Privacy
  - Enable encryption on all backups
  - Trust who you really trust
- Organizations:
  - IT: Deploy Mobile Threat Defense (MTD) solutions
  - Dev: Exclude sensitive info from app backup data



Recommendations

- Work with Apple
  - As always Apple has been actively engaged to preserve and maintain the security of its users
  - Issue reported to Apple in mid July 2017
  - iOS 11 Changes
    - Trusting computers now requires passcode
  - Wi-Fi sync should be reconsidered
  - Mobile OS should be owning most of the security decisions
    - Encrypted backups

Summary

- Single point of failure / one time mistake
- Long lasting implications
- Can be used by conventional malwares
- How to avoid
- New breed of attacks jumping from traditional to modern OS

- Check out our blog for more information:
  - https://www.symantec.com/blogs/feature-stories/ios-trustjacking-dangerous-new-ios-vulnerability
- Twitter: @Royiarchy @AdiSharabani
- Birds of Feather Session: Marriot, Golden Gate A
  - Should I put security on mobile or make my whole security mobile?