#RSAC

RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

SESSION ID: TTA-R02

IOS TRUSTJACKING
TRUST HAS A PRICE

Roy Iarchy

Research Team Leader, Modern OS
Symantec
@Royiarchy

Yair Amit

VP & CTO, Modern OS Security
Symantec
@YairAmit

Agenda

- Background
- Recap of related past attacks
- The foundation of Trustjacking attacks
- Remote Videojacking attack + demo
- Advanced Trustjacking attack flows + demos
- Summary & Recommendations

A day in the office

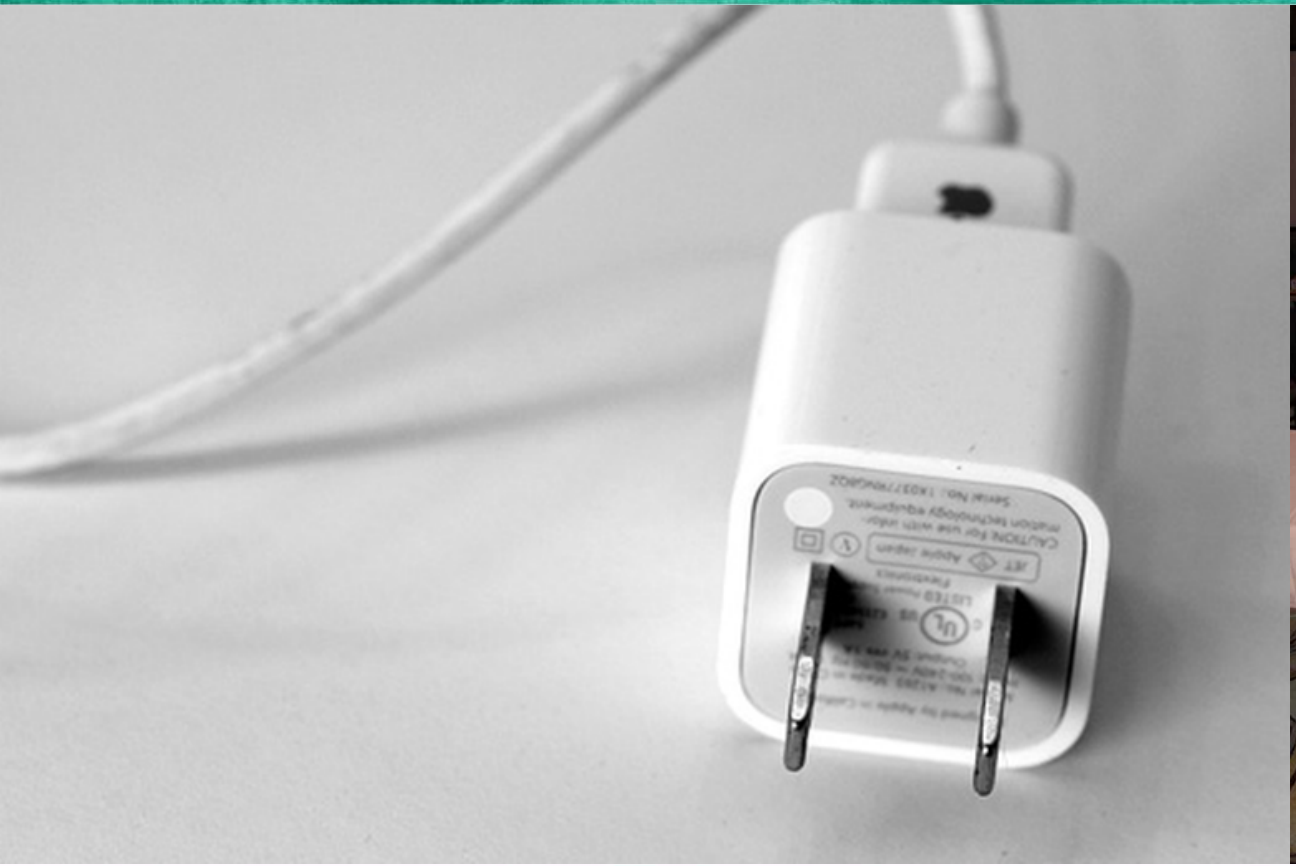
- Working with several iOS devices
- Weird behavior

Background

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

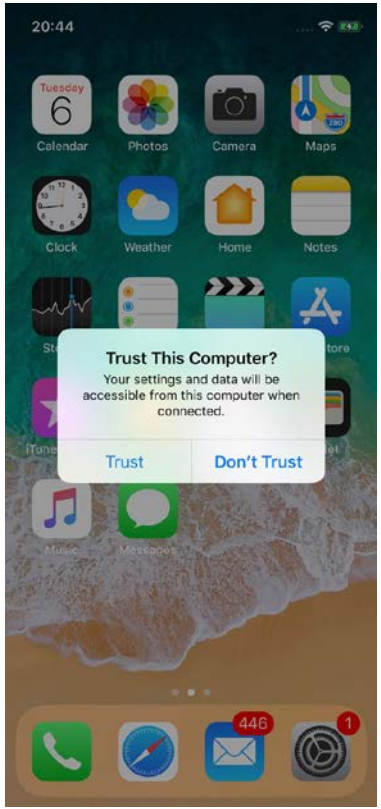
Juicejacking

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



Juicejacking mitigation

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

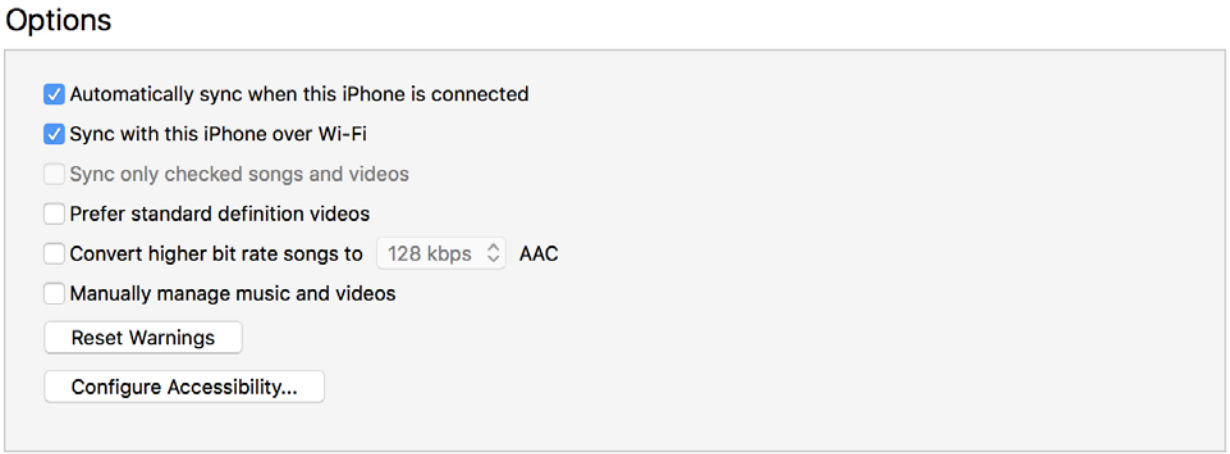


Videojacking (leveraging HDMI interface)

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 an implementation of usbmux over network

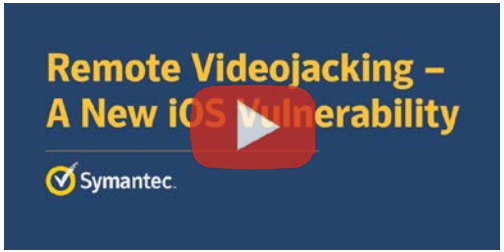
IOS TRUSTJACKING

iOS Trustjacking – attack flow

- Trust == One time mistake
- Victim side -> nothing much “seem to happen”
- Attacker side
  - Accessing device information
  - Accessing device logs
  - Rebooting the device (can be used for DoS attack)
  - Leveraging the developer image

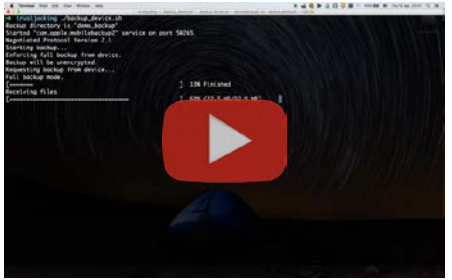
REMOTE VIDEOJACKING DEMO

Using developer image for advanced attacks



IOS TRUSTJACKING ADVANCED DEMO

Backup and restore



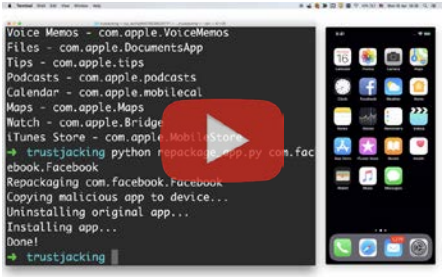
Backup format

- The decision whether the backup is encrypted or not is initiated by the computer-side but then enforced on the client side
  - An encryption policy defined at some point will take effect in future backups!
- If victim didn't choose to encrypt backups, the attacker can enforce encrypted backup on the user's device, putting the victim in a bad situation. ☹
  - This is another reason for user's to opt in to encrypt their backups; it will make attackers' life harder!
- Getting data 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

- The remote backup allows us access to:
  - Multimedia
  - Messages
  - Contacts
  - App data

IOS TRUSTJACKING ADVANCED DEMO



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

Post-Trust and Pre-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

What about USB Restricted Mode?

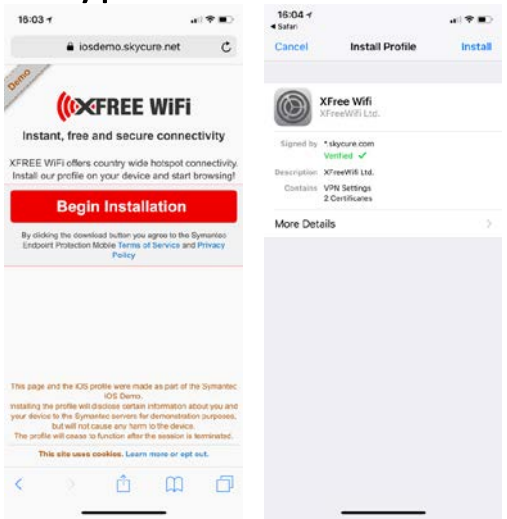
Taken via Trustjacking…
Backup and other actions are working remotely as well.

* Confirmed on iOS 12 beta 3.

Is the attack confined to Wi-Fi only?

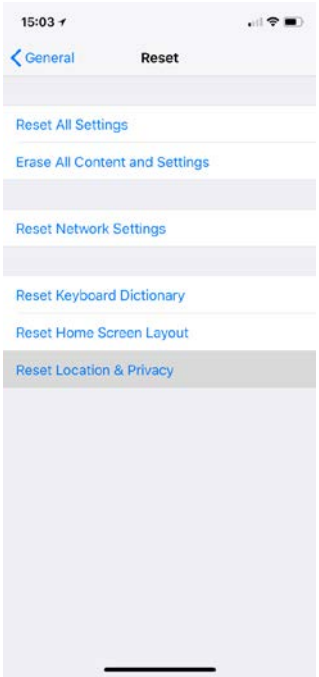
Wi-Fi Sync & Bonjour

- 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
  - Keep your OS up-to-date
- Organizations:
  - IT: Deploy Mobile Threat Defense (MTD) solutions
  - Dev: Exclude sensitive info from app backup data & logs



Recommendations

- Responsible & Coordinated disclosure process with Apple
  - As always Apple has been actively engaged to preserve and maintain the security of its users
  - iOS 11 Changes
    - Trusting computers requires entering a passcode.
    - The dialog still states that the risk of Trust is only temporal (while the computer is connected).
  - Wi-Fi sync should be reconsidered
  - Mobile OS should be responsible for most of the security decisions
    - Encrypted backups
    - Trusted hosts management

Summary

- Single point of failure / one time mistake
- Physical -> Wi-Fi -> Anywhere
- Long lasting implications
- Can be used by conventional malware
- How to mitigate

- Check out our blog for more information:
  - https://www.symantec.com/blogs/feature-stories/ios-trustjacking-dangerous-new-ios-vulnerability
- Twitter: @Royiarchy @YairAmit