iOS MITM Attack
Technology and effects
Boot validation

- **CA** – Apple Certificate Authority
- **SIGN** – Signature
Files Protection

iOS File System

- Keychain db (Password, certificates)
  - ENCRYPTED
- User Files (application data, sms, calls, etc)
  - ENCRYPTED

iOS Backup

- Keychain db (Password, certificates)
  - ENCRYPTED
- User Files (application data, sms, calls, etc)
  - NOT ENCRYPTED
Classic provisioning

Apple

Developer's UDID

Signed Provision profile

Developers Certificate request

Developer

99 $

Developer's Key

Unsigned Application

Signed Application

Signed Provision profile

iOS Device
Actual provisioning

Certificate Pusher

Device UDID

10 $

Developer’s Key

Developer’s Certificate

Developer

Signed Application

Signed Provision profile

iOS Device
Why we can’t create fake signature?

Certificate Authority Storage

| Storage | Securityd built in storage (186 CA) | KeychainDB expandable storage |

Few from 186 are quite interesting:

- C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DoD CLASS 3 Root CA
- C=JP, O=Japanese Government, OU=ApplicationCA
- C=CN, O=China Internet Network Information Center, CN=China Internet Network Information Center EV Certificates Root

...
Certificate authentication

Start

for CA in STORGAE

check incoming certificate with CA

OK

FAILED
I want my CA in your iOS
Ways to install CA in iOS

- Safari
- Email attachment
- MDM
  - With configuration profile
    - Can be installed with Safari
Mobileconfig contains

✓ WiFi settings (pass, SSID) for “Gate”

✓ CA

✓ Proxy Settings, if we want victim’s traffic even it has left attack range. (Only for iOS6)

✓ iCloud backup (enable it, if not)
Mobileconfig installation
Looks bad =(
Let’s take a look on default CA list...

Certificate:

Data:

Version: 3 (0x2)
Serial Number:

4e:81:2d:8a:82:65:e0:0b:02:ee:3e:35:02:46:e5:3d

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO

Validity

Not Before: Dec 1 00:00:00 2006 GMT
Not After : Dec 31 23:59:59 2029 GMT
COMODO trial certificate

- You only need valid admin@yourdomain.com mail for confirmation
- Can be used for signing
How to sign

openssl cms -sign -in uns.mobilconfig \ 
-out s.mobilconfig -signer comodo_cert.pem \ 
-inkey comodo_cert.key -outform DER \ 
-nodetach -certfile comodo_trustchain.pem
Looks much better
SSL Defeated
But we want more
How to get files from device

Attacker

AppleID + pass (or auth token)

iCloud

AppleID + pass (or auth token)

iPhone full backup

AppleID + pass (or auth token)

iPad full backup

Victim’s iPhone

Victim’s iPad
Elcomsoft Phone Password Breaker
Once again
What’s in backup?

• SMS
• Private photo
• Emails
• Application data
• And more ...

![Example images and text from backup content]
Files done
But we want more
Apple Push Notification Service
Fake! Fake! Fake!

Wipe Tragedy (act 1/1)

Hi, I'm %UDID%. My, version, hardware, carrier, etc... AND here is my API

Hi, %UDID%. FindMyiPhone has something for you, plz check. Here is your fmips API token.

Hi, I'm %UDID%, my owner is %AppleID%. Do you have something for me?

Sure, %UDID%! I want you to die!

Okay 😊

Data Wipe

Reboot
Summary

User only have to tap ‘Install’ two times to make us able to:

- Sniff all his SSL traffic (cookies, passwords, etc)
- Steal his backup (call log, sms log, photos and application data)
- Send him funny push messages or just wipe device
sieg.in
al@sieg.in
@siegin