Lockup: A software tool to harden iOS by disabling default *Lockdown* services

Gómez-Miralles, Luis & Arnedo-Moreno, Joan
pope@uoc.edu jarnedo@uoc.edu
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya

Workshop on Security and Privacy in Systems and Communication Networks (SecureSysComm 2015)

November 2015

Kraków, Poland

Index

Intro

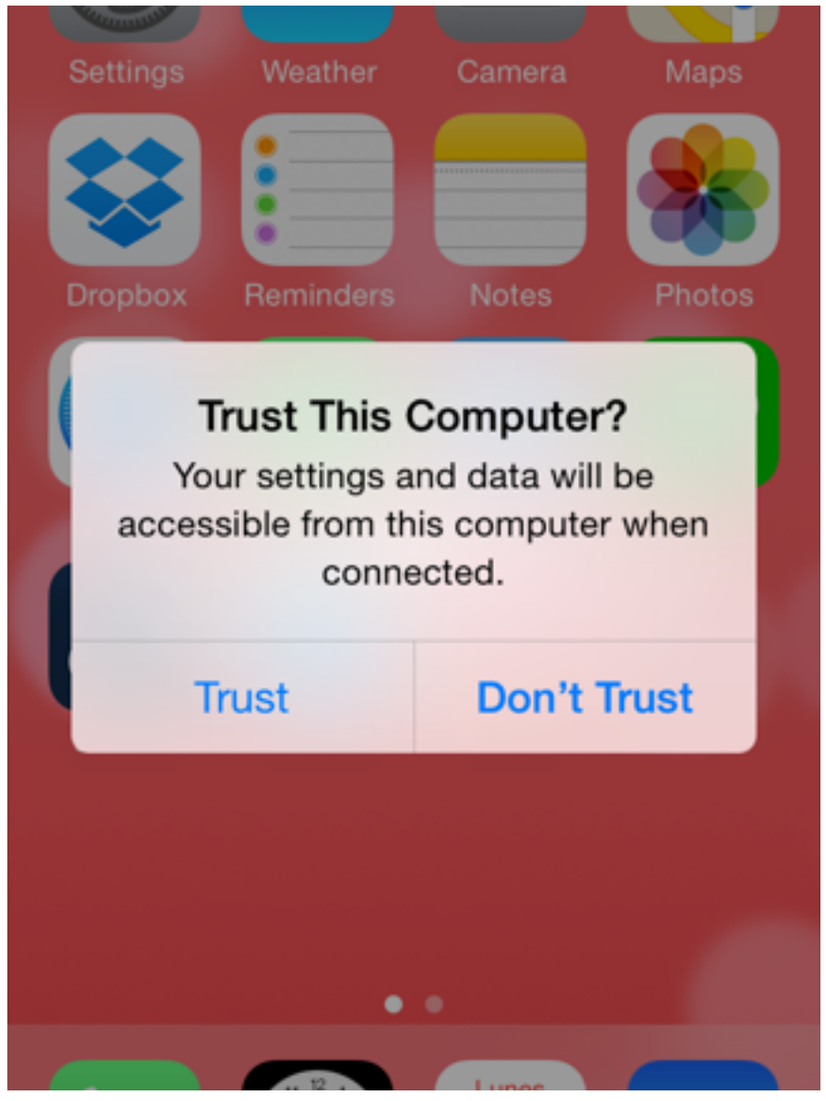
- 2007: iPhone. Multi-touch, no stylus.
- 2010: iPad. *iPhone O.S.* goes *iOS*.
- Smartphones and tablets hold vast amounts of personal information: e-mail and IM messages, contacts, calendars, to-do lists, history of visited places, photographs…

- iOS market share (Q2 2015) over 10%.
  - Over 60% in corporate environments.

Background

The problem: iOS trust relationships.

- User prompt presented when connected to a new computer/device (stereo, alarm clock...)
- Upon consent, trust certificates are created and interchanged. These are used to access a number of services: audio, data transfer… through the *Lockdown* daemon.
- A malicious device (or an attacker with a copy of the trust certificate) can access all the device data, install applications remotely, sniff network traffic, modify settings… All of this wirelessly and without the device alerting the user.



📚→J. Zdziarski, "Identifying back doors, attack points, and surveillance mechanisms in iOS devices". Digital Investigation 11 (2014).

Background

Sensitive iOS services offered through *Lockdown*:

- **`com.apple.file_relay`** - Extract data, bypass backup encryption password, no known purpose.
- **`com.apple.pcapd`** - Network sniffer, no known purpose.
- **`com.apple.mobile.MCInstall`** - Install config profiles, MDM.
- **`com.apple.mobile.installation_proxy`** - Install / remove apps.
- **`com.apple.mobile.house_arrest`** - Transfer files in / out of apps.
- **`com.apple.mobilebackup2`** - Backup device data (respects backup encryption pw).
- **`com.apple.mobilesync`** - Sync bookmarks, notes, etc.
- **`com.apple.afc`** - Access to media library: pictures, videos and music.

Mitigation strategies

- Delete existing pairing records.
- Disable sensitive services over-the-air.
- Remove dangerous/unneeded services.
- Lock pairing with new devices.

Lockup

Proof of concept software tool.

1. Disables unwanted services (e.g. sniffer).

2. Limits other services to *USBonly* (no over-the-air).

3. For the rest of services, defines a number of profiles based on typical use cases (MDM; sync to iTunes; standalone…).

4. Periodically revokes trust certificates.

Lockup

Screenshot showing the main menu and different profiles

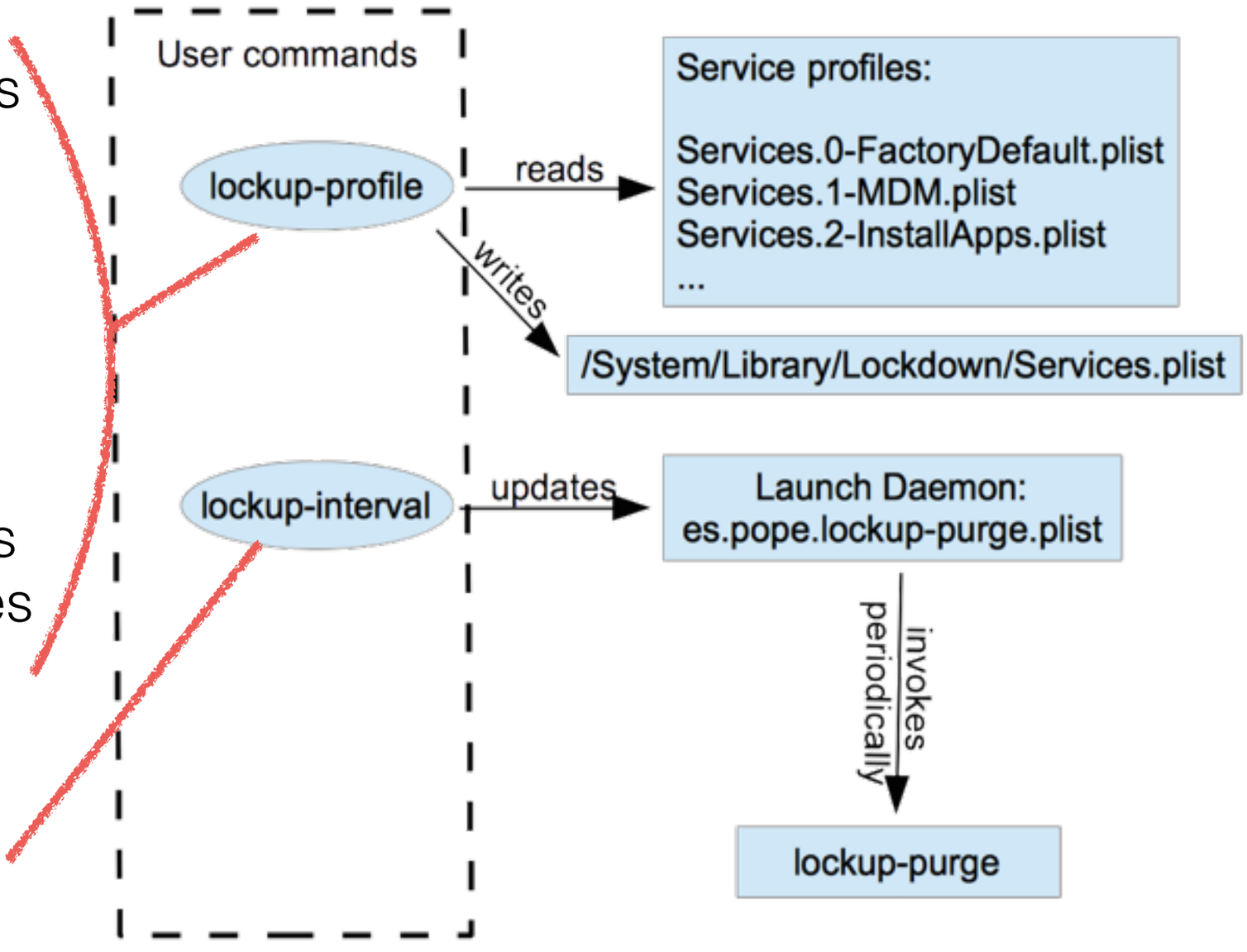
```
Current profile: 0. Default iOS service set. Wi-Fi sync ON.

Available profiles:
0. Default iOS service set. Wi-Fi sync ON.
1. MDM environments. Wi-Fi sync ON.
2. Sync apps. Wi-Fi sync OFF.
3. Backup device data. Wi-Fi sync OFF.
4. Sync media files. Wi-Fi sync OFF.
5. Share media files. Wi-Fi sync OFF.
6. No sensitive services. Wi-Fi sync OFF.
7. No services at all (paranoid mode).
--
9. ABORT - Exit this program.
D. Dump installed profile.
E. Enumerate services exposed by the current profile.

Press key and ENTER...
```

Lockup: components

1. Disable unwanted services (e.g. sniffer).
2. Limit other services to *USBonly* (no over-the-air).
3. For the rest of services, define a number of profiles based on typical use cases (MDM; sync to iTunes; standalone…).
4. Periodically delete pairing records.



Lockup: iOS 8 & 9

- Starting with iOS 8, the list of *Lockdown* services is not stored in a separate file, but at the end of the *Lockdown* binary itself.

- We have succeeded at enabling/disabling services by altering that section of the binary.

- Work in progress: automatically detect the right position within the *Lockdown* binary to overwrite the service list, instead of relying on pre-calculated offsets, in order to automatically support future iOS releases.

Conclusions

- iOS trust model — a door to back doors.
- In our proof of concept implementation, the need for a jailbreak introduces additional weaknesses & threats.
- However it would be trivial for Apple to offer this kind of protection in stock iOS versions, although this is unlikely compatible with their love for simplicity.

Questions?

Thanks for your assistance

Get *Lockup* at `http://pope.es/lockup`