Hardening iOS by selectively disabling *lockdown* services

Luis Gómez-Miralles, Joan Arnedo-Moreno
pope@uoc.edu, jarnedo@uoc.edu

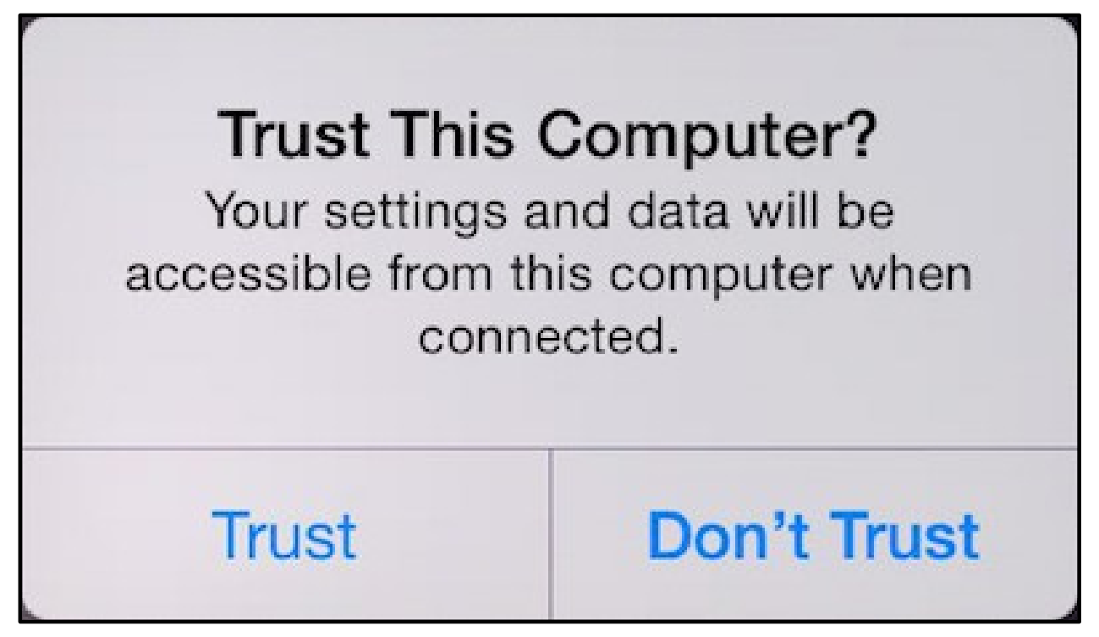
Introduction

Facts:

The U.S.A. N.S.A. has extensive surveillance capabilities over iOS devices [Rosenbach].

Targets include innocent citizens such as sysadmins working for companies where N.S.A. wants to infiltrate [Gallagher].

Surveillance likely happens through default iOS system services and abuse of pairing certificates [Zdziarski].


Trust This Computer?
Your settings and data will be accessible from this computer when connected.

Proposed solution

Many possible mitigations:

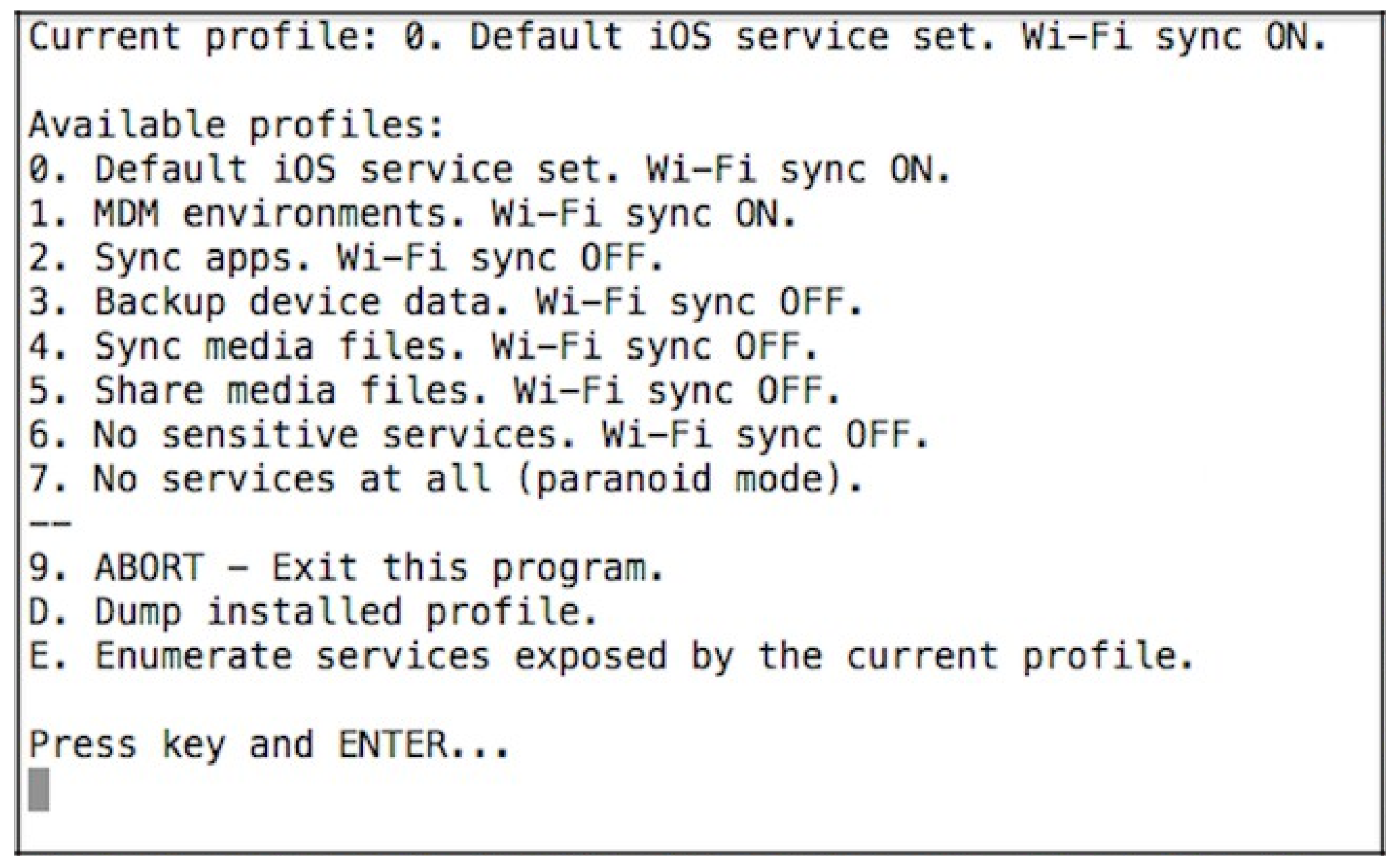
- Disable unwanted services (e.g. sniffer)
- Restrict other sensitive services to *USBOnly*.
- For the rest of services: define a number of *profiles* for typical device uses, such as: remote management through MDM; allow app installation through iTunes; media sync... And choose the desired profile at any moment.
- Periodically delete pairing records (trust certs).

Software implementation

Lockup is an implementation of the proposed mitigations for jailbroken devices running iOS 7.

With one command (*lockup-profile*) the user sets the profile in use at any given time based on the tasks he wants to perform. This disables unnecessary services.

Another command (*lockup-interval*) lets the user define the period at which pairing records are deleted. This sets the maximum lifetime of trust relationships.



```
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...
```

Fig 2: A screenshot of *lockup-profile*.

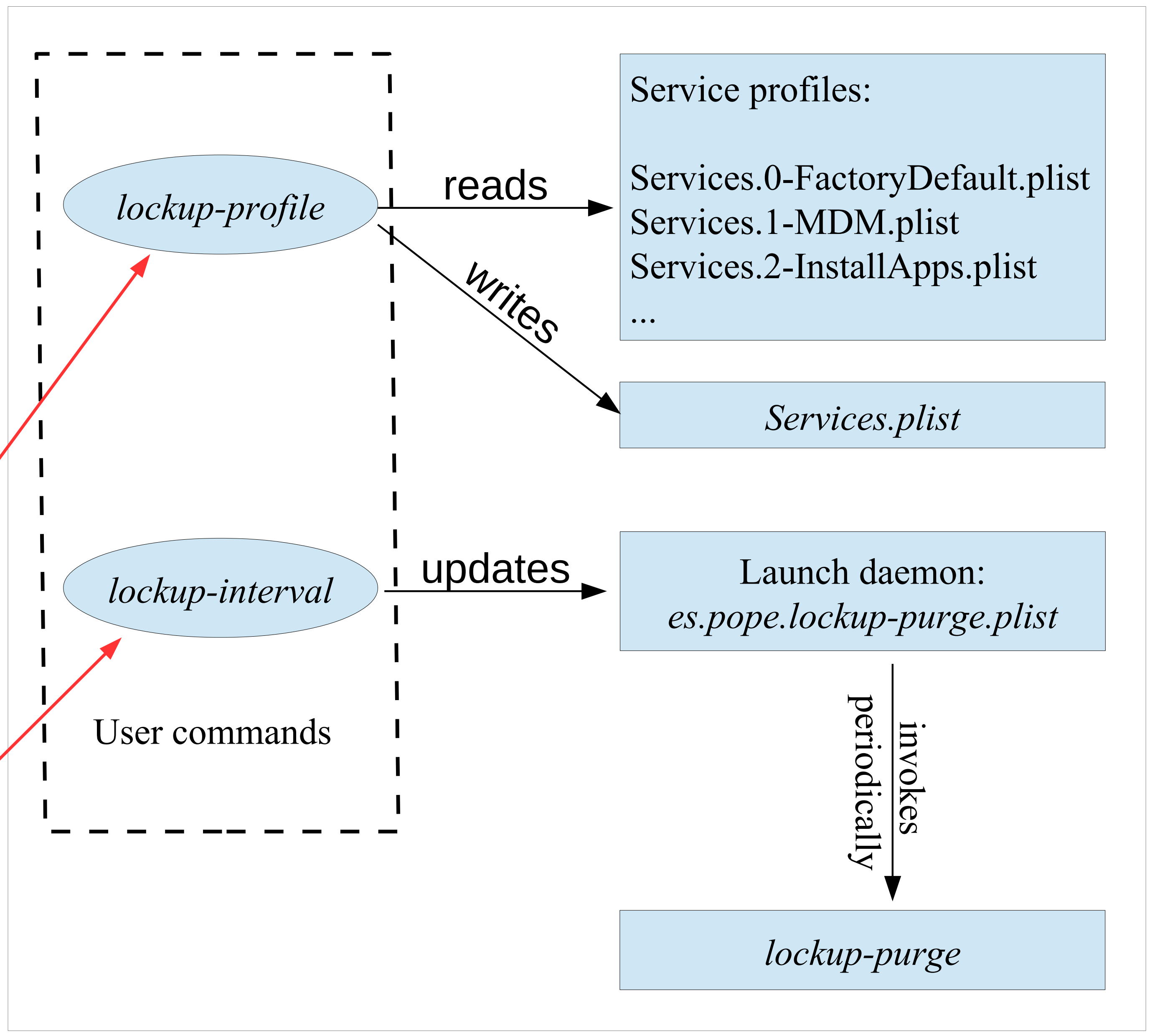


Fig. 1: The different software components of *Lockup*.

Considerations:

- In order to simplify the implementation we defined our profiles as incraesingly restrictive, meaning that if a service is available in profile *n* it will also be available in the lower profiles *n-1*, *n-2*...
- Although the overall security posture is improved, the use of jailbreak disables a number of security protections opening the door to new weaknesses.
- Consequently, users should not install any additional software via Cydia.

Work in progress:

- Port to iOS 8.
- Add a GUI.

Conclusions

This proof of concept has shown that is technically possible to restrict the number of exposed services based on the tasks the user wants to perform in the device at any given time.

Lockup will be released as free software so that other researchers and developers can adapt it as they find convenient.

We intend to continue working in the tool, maintaining it and adding new features such as: monitor the list of available services and detect if new services are installed; log service connection attempts; and offer the user real-time notifications.

The use of jailbreak was unavoidable due to the restrictions inherent to the iOS environment, but it would be trivial for Apple to implement this kind of changes in stock iOS versions. This, however, does not seem likely to happen in any near future.

Using techniques similar to those of *redsn0w* and other jailbreaks, it should be possible to perform only the first steps of the process, modify core system files to disable unwanted services, and return the device to a non-jailbroken state without installing the untethered exploit [Miller]. This would put together the best of both worlds, and is a very promising line of research for the future.

...all your iPhone are belong to us

References and related literature

M. Rosenbach, L. Poitras, H. Stark, iSpy: How the NSA accesses smartphone data, Der Spiegel 37/2013 (2013).

R. Gallagher, P. Maass, Inside the NSA's secret efforts to hunt and hack system administrators, The Intercept (2014).

J. Zdziarski., Identifying back doors, attack points, and surveillance mechanisms in iOS devices, Digital Investigation 11 (2014) 3–19.

C. Miller, D. Blazakis, D. D. Zovi, S. Esser, V. Iozzo, R. Weinmann, iOS hacker's handbook, Wiley (2012).

Acknowledgments

This work was partly funded by the Spanish Government through project TIN2011-27076-C03-02 CO-PRIVACY.

Universitat Oberta de Catalunya

Further information

For related research and additional information, please refer to the authors' website at:
www.pope.es

… or just look for this guy →