Monthly Research

A Survey of Threats in OS X and iOS

FFRI, Inc.
http://www.ffri.jp

Ver 1.00.01

Overview/Background

- Recently, business use of Mac and iPhone/iPad is increasing.
  - It is possible to coexist with Windows by virtual machine or Boot Camp.
  - BYOD(Bring Your Own Device) solution for iPhone is available.
    - iPhone is popular for general users in Japan, so it is often also used to BYOD.
  - It is believed no malware exists on iPhone.

- A security researcher showed that OS X's four security mechanisms(Gatekeeper, XProtect, App Sandbox, Code Signing) were avoidable easily at RSA Conference USA 2015.
  - He said that no security software for Mac detects his attack technique.

- Therefore, we surveyed threats of OS X and iOS

Case Studies: OS X/iOS Malware

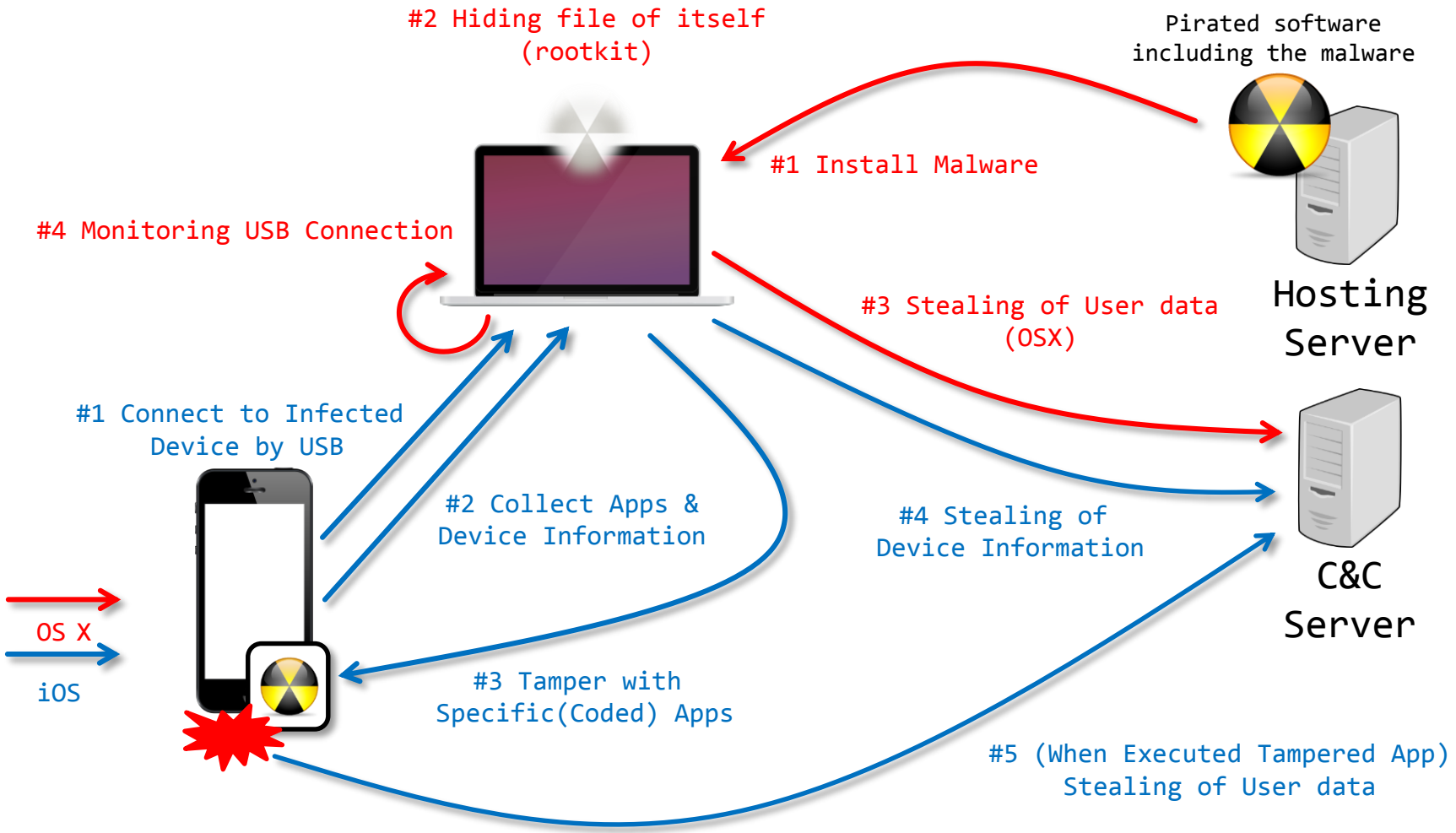
- [OS X/2014] iWorm
  - Infected via pirated software.
  - This bot gets C&C server address list which was written by the attacker on reditt.com.

- [iOS/2014] WireLurker
  - Infected to Windows and OS X via pirated software.
  - Infected iPhone App by abusing Sync function.
  - Send contacts list to C&C server.

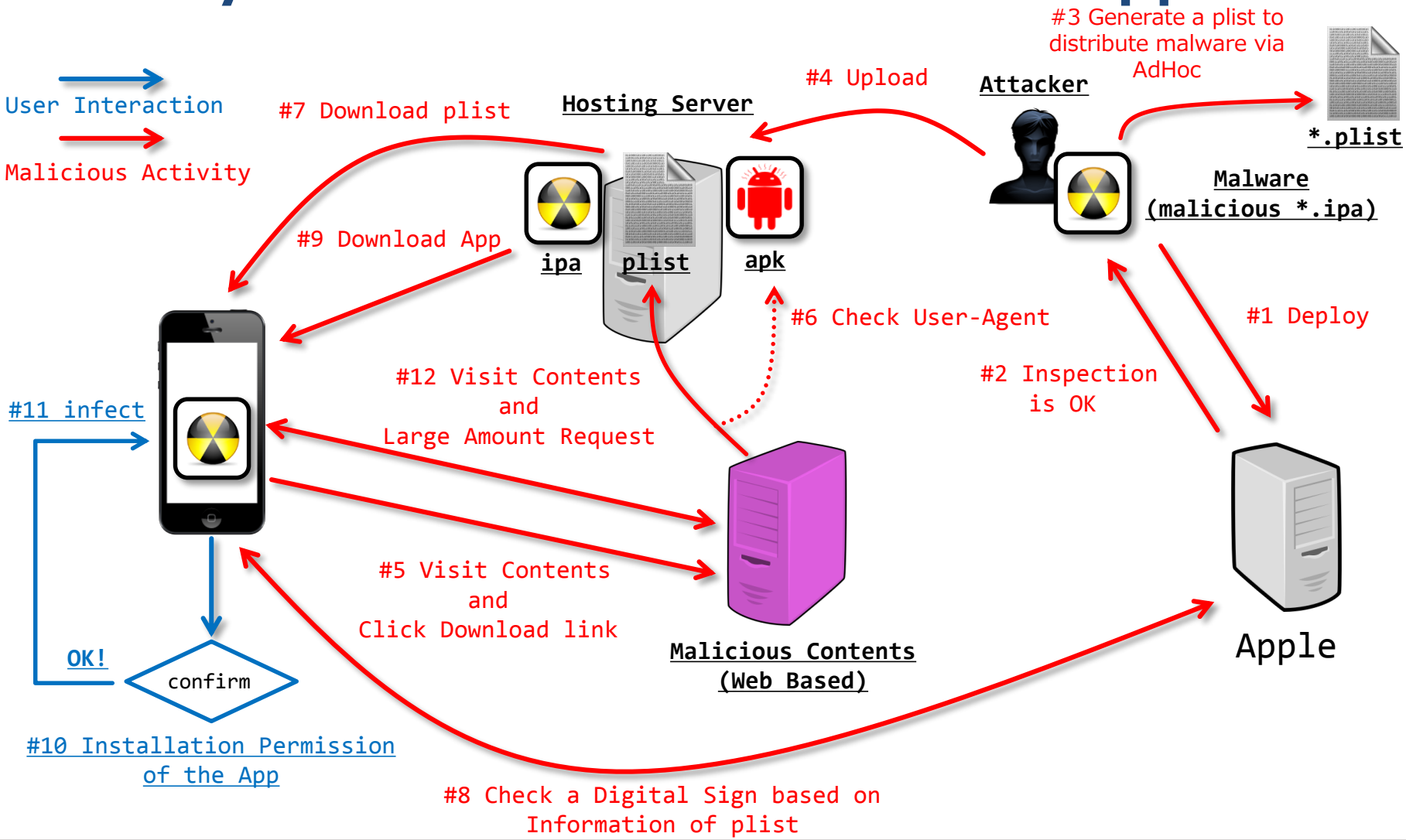
- [iOS/2015] OneClick Fraud App
  - Attacker abuses “iOS Developer Enterprise Program” and distributes malware any place other than AppStore.
  - This malware displays fraud contents on the Web server side.*

** The malware to use such a technique is generally in Android.*

Activity Overview: WireLurker



Activity Overview: OneClick Fraud App

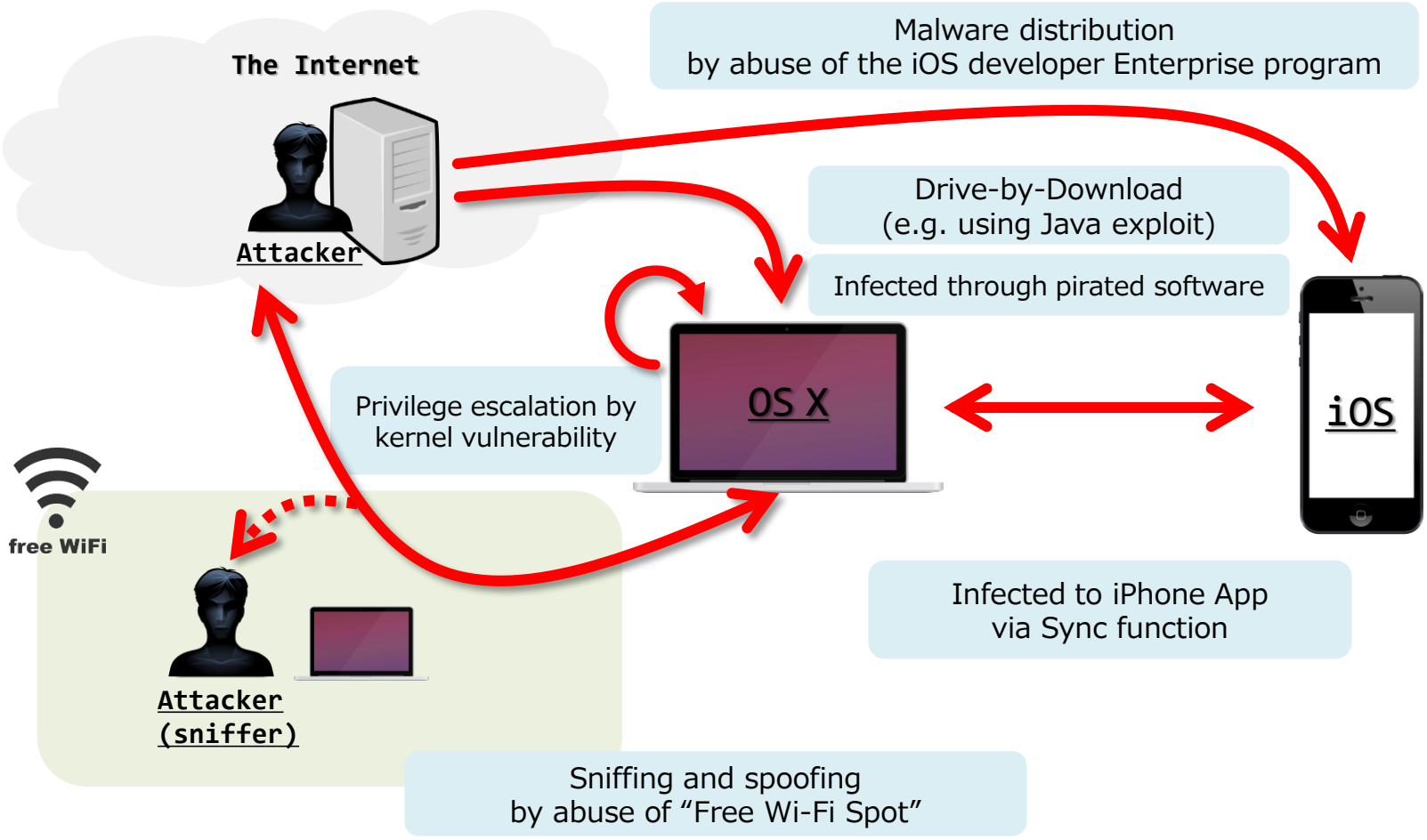


Case Studies: OS X/iOS Vulnerability

- [OS X/iOS] Denial of Service via crafted Unicode text
  - CVE-2015-1157
  - OS/app crashes or reboots when it received crafted message.
  - Reported in May 2015.
  - Fixed at iOS 8.4 and OS X 10.10.4.

- [OS X/iOS] Cross Application Resource Access (XARA)
  - Vulnerability caused by authentication between application.
  - Various passwords might be stolen if the vulnerability is exploited.
  - Reported in June 2015.
  - Apple officials released the following statement:
    "we implemented a server-side app security update that secures app data and blocks apps with sandbox configuration issues from the Mac App Store."

Routes of Infection and Cyber Attacks



Conclusion

- Recently, OS X and iOS are becoming target of cyber attacks.
  - As a result, attack technique peculiar to OS X and iOS comes up. (e.g. Abuse of sync function, malware distribution by AdHoc etc.)

- We recommend some security settings for Mac and iPhone based on current state of threats.
  - Target system is OS X 10.10.x (Yosemite) and iOS 8.x.
  - These settings are only minimal measures.
  - These are not always preventing any attacks.

Security Checkpoints in Your Mac/iPhone

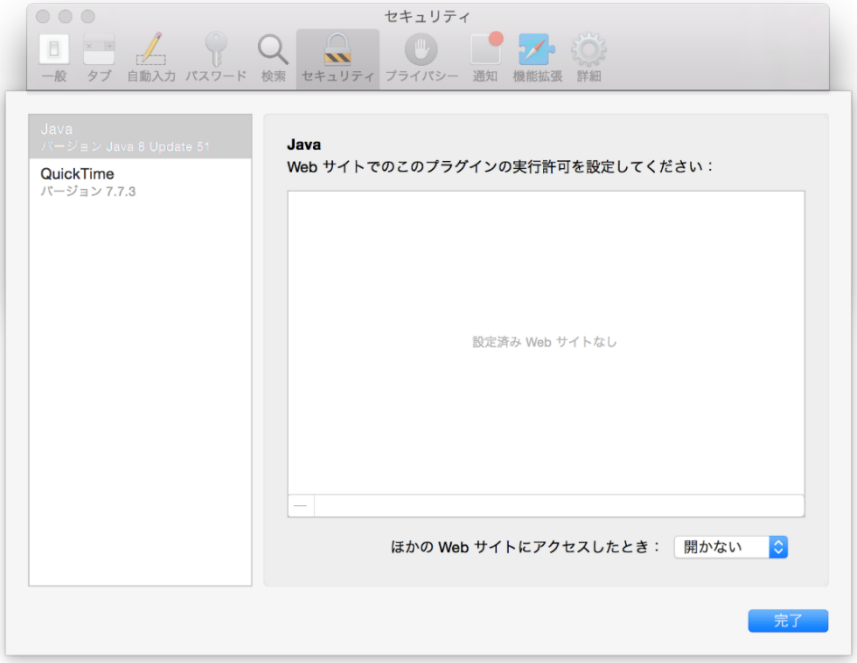
Security Checkpoints in Your Mac #1

1. Install security update automatically
   - Keep latest software version for vulnerability fix.

Security Checkpoint in Your Mac #2

2．Disable Java plug-in on browser

- Java vulnerabilities are exploited for a lot of malware infection on Mac.



Security Checkpoint in Your Mac #3

3．Enable Firewall

- Firewall is blocking untrusted inbound communication.

Security Checkpoint in Your Mac #4

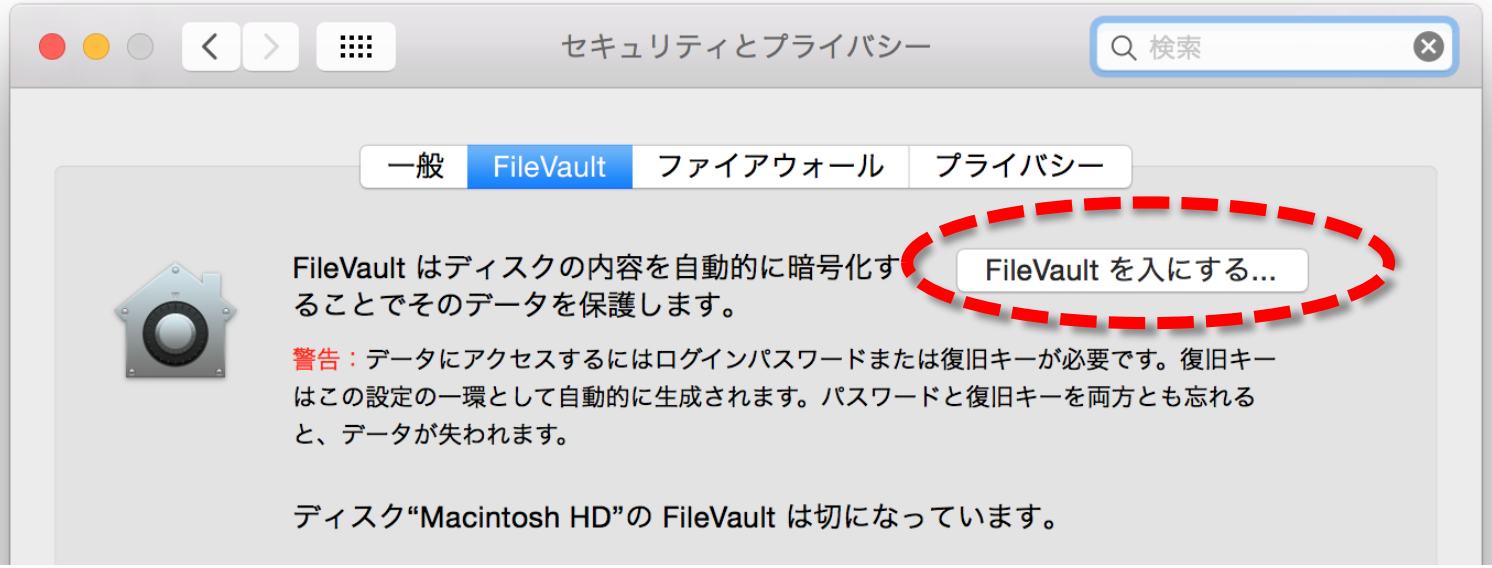
4．Finder settings

- Finder does not display file extension by default
- We recommend “Show all filename extensions” to detect malware disguised as harmless file.

Security Checkpoint in Your Mac #5

5．Encryption setting of disk (FileVault)

- It is possible to prevent info leakage when your mac was lost or stolen.



Security Checkpoint in Your Mac #6

6．Screen lock with password

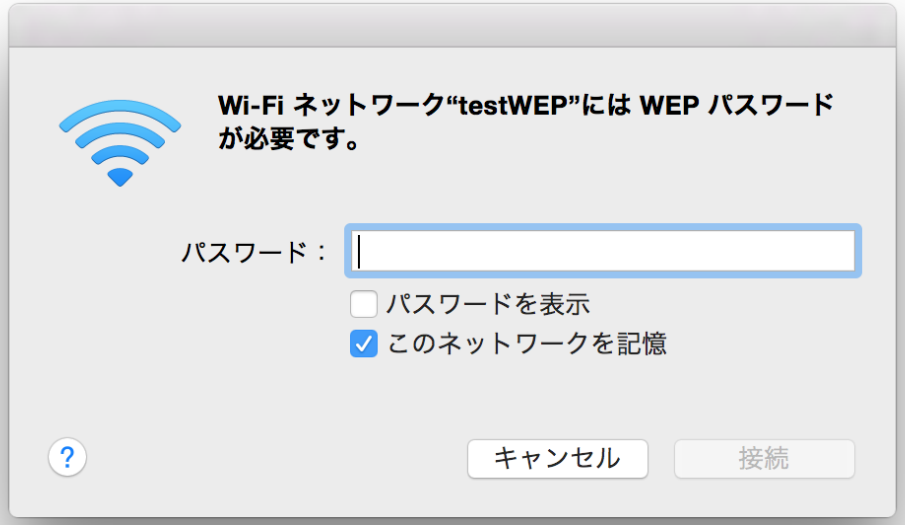
- It is possible to prevent info leakage when your mac was lost or stolen.

Security Checkpoint in Your Mac #7

7. Disable built-in guest user
   - It is possible to reduce attack surface.

Security Checkpoint in Your Mac #8

8. Use strong encryption method for Wi-Fi
   - Do not connect to non-encrypted access point
   - Do not use WEP and WPA-PSK (TKIP)
   - Use WPA2 or WPA-PSK (AES)



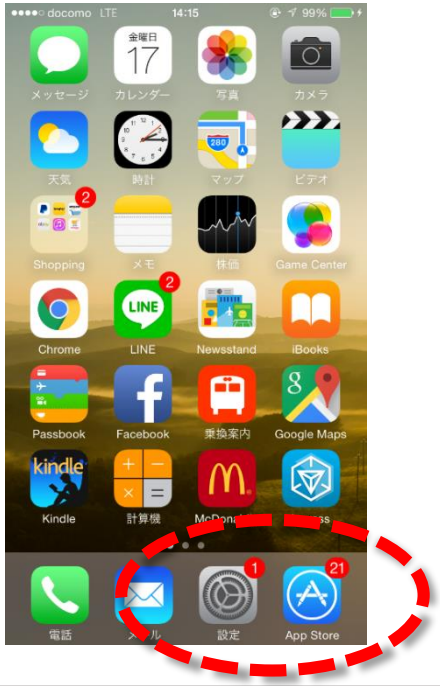
Security Checkpoint in Your Mac #9

9．Enable “Find my Mac”

- It is possible to trace location when your mac was lost or stolen

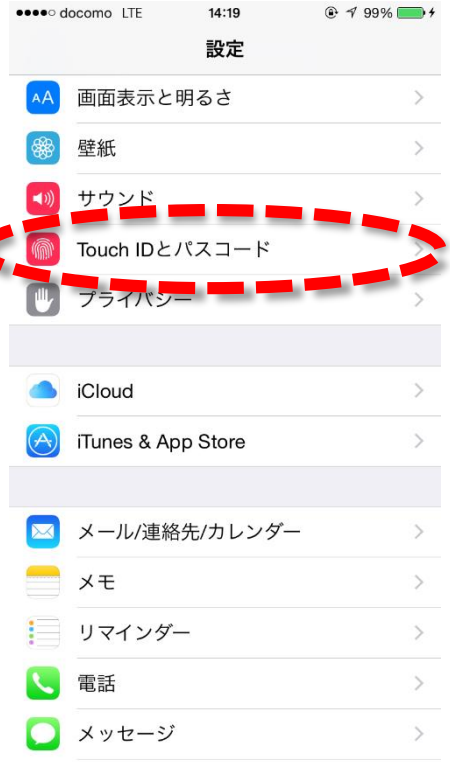
Security Checkpoint in Your iPhone #1

1. Install Software update
   - iOS update is included security updates
   - Keep latest iOS version for vulnerability fix.



Security Checkpoint in Your iPhone #2

2. Screen lock with Touch ID/Passcode
   - It is possible to prevent info leakage when lost or stolen



Security Checkpoint in Your iPhone #3

3. Use strong encryption method for Wi-Fi
   - Do not connect to non-encrypted access point
   - Do not use WEP and WPA-TKIP
   - Use WPA2 or WPA-PSK(AES)

Do not connect to non-encrypted access point

Security Checkpoint in Your iPhone #4

4-1. Do not “trust” PC unnecessarily

- WireLurker infects to iPhone via infected PC

4-2. Do not install apps provided by untrusted developer

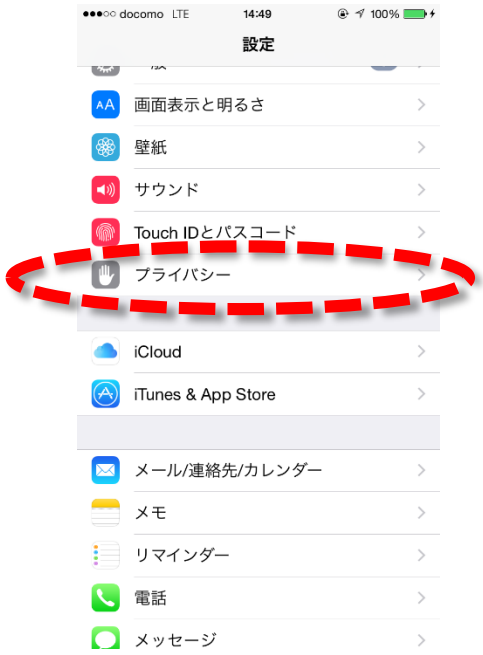
- Confirm app developer identity
  when iOS demands your permission

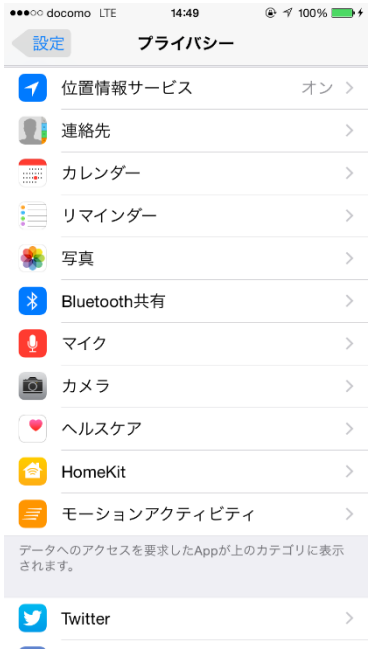
Security Checkpoint in Your iPhone #5

5. Enable “Find my iPhone” and “Backup”
   - It is possible to trace your iPhone location when lost or stolen.
   - Even if iPhone breaks down, you can restore data from backup.

Security Checkpoint in Your iPhone #6

6. Check privacy settings
   - iOS can control core functions(camera, location service, etc.) for each apps.
   - Check your needs and app permissions.





Security Checkpoint in Your iPhone #7

7. Check profile settings
   - Do not install suspicious profile
   - Delete suspicious profile
   - Malicious profile allow sniffing of your traffic by attacker

References

- Malware Persistence on OS X Yosemite
  - https://www.rsaconference.com/writable/presentations/file_upload/ht-r03-malware-persistence-on-os-x-yosemite_final.pdf
- WIRELURKER: A New Era in iOS and OS X Malware
  - https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
- Japanese one-click fraudsters target iOS users with malicious app delivered over the air
  - http://www.symantec.com/connect/blogs/japanese-one-click-fraudsters-target-ios-users-malicious-app-delivered-over-air
- Unauthorized Cross-App Resource Access on MAC OS X and iOS
  - https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view?pli=1
- Serious OS X and iOS flaws let hackers steal keychain, 1Password contents
  - http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/
- iPhone text message bug can crash Apple Watch, iPad and Mac too
  - http://www.theguardian.com/technology/2015/may/28/iphone-text-message-bug-crash-apple-watch-ipad-mac
- Malicious Profiles – The Sleeping Giant of iOS Security
  - https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/
- NETMARKETSHARE
  - http://www.netmarketshare.com/
- openclipart
  - https://openclipart.org/share

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research