Check Point
SOFTWARE TECHNOLOGIES LTD.

WE
SECURE
THE
FUTURE

Enterprise Apps: Bypassing the Gatekeeper

By Avi Bashan and Ohad Bobrov

Executive Summary

The Apple App Store® is a major part of the iOS security paradigm, offering a central distribution process that allows verification of nearly all code executed on iPhones and iPads. However, there are a number of architectural flaws in this ecosystem. This report covers one such flaw that exposes iOS users in the enterprise to cyberattacks.

The Check Point research team has successfully exploited a security flaw in Apple's iOS 9 that allows cybercriminals to install malicious apps on enterprise employees' iPhones and iPads. The flaw hinges on cybercriminals staging a Man-in-the-Middle attack that hijacks communications between managed iOS devices and Mobile Device Management (MDM) solutions. This exploit could give cybercriminals control of devices and the data that resides on them, potentially impacting millions of iOS users worldwide whose devices are managed by an MDM.

The research team's findings and a video demonstrating an attack were submitted to Apple's security team in October 2015. Apple responded in November 2015 that the behavior the team demonstrated was expected.

Developing Apps for iOS

A substantial part of the iOS value proposition hinges on providing superior security and privacy for users and their sensitive data. Apple uses several distinct approaches to achieve this, including:

- **Sandboxing:** Each app is embedded within a sandbox that limits its privileges and capabilities to access or operate within protected parts of the OS.
- **Permissions:** Apps that require certain access to resources in order to function must request specific permissions from the user.
- **Signed code:** Unless a device is jailbroken, only signed code can run on a device. This is done to ensure all code running on a device has received final approval from Apple and is safe to use.

iOS apps are strictly controlled by Apple. As part of Apple's app strategy, a single App Store lets users download apps to devices. Developers must be registered in order to publish apps on the App Store. This enables Apple to control who's developing apps for its ecosystem, and to banish developers who fail to meet its standards. iOS developers can't develop apps anonymously if they want their apps on the App Store.

App Review Process

Each time a developer publishes a new version of an app, it must undergo a rigorous security review. This review process may take several weeks and is conducted according to a basic set of rules outlined in the App Store Review Guidelines[1]. These rules filter out apps that contain improper content, that are low quality, or that have a malicious intent.

During the review, the app's content, functionality, behavior, APIs, and many other aspects are scrutinized to prevent malicious or dangerous apps from being published in the App

[1] https://developer.apple.com/app-store/review/guidelines/

Store. Although this process is thorough, Apple's approval process can sometimes allow dangerous apps into the App Store[2].

Apple Developer Enterprise Program

Apple created the Apple Developer Enterprise program to offer businesses a way to develop and distribute apps for internal use. These apps can be distributed quickly and directly to devices, enabling enterprises to develop apps that meet their own business requirements without publishing them on the App Store. In this way, enterprise can avoid a lengthy review process and, more importantly, keep these apps out of the hands of non-employees.

> *"In-house apps are not submitted to the App Store and are not reviewed, approved, or hosted by Apple. You can distribute in-house apps either by hosting your app on a simple internal web server or by using a third-party MDM or app management solution." - iOS Deployment Overview for Enterprise*

What *is a developer certificate?*

> *A certificate, signed by Apple, that developers can use for signing apps they create in XCode. Apps signed with this certificate can be installed on iOS devices without having to be vetted through the traditional App Store process. This is done not only for testing purposes, but for enterprises who may want to develop apps themselves then distribute them to their employees without requiring that these employees install the app through the App Store.*

[2] https://en.wikipedia.org/wiki/XcodeGhost

Enterprise App Capabilities

Malicious enterprise apps can cause significant harm. Cyber criminals can use various methods to achieve malicious goals like:

- **Abuse public APIs:** Apple makes APIs available for developer use. During the review process, Apple makes sure that apps use APIs only for their expressed purpose. An enterprise app can abuse public APIs to gain extended capabilities, such as the VOIP API which can be abused in order to run an app in the background silently and constantly.
- **Abuse private APIs:** These APIs are internal Apple API. Apple forbids developers from using these in order to protect users' sensitive data. However, since enterprise apps do not pass through Apple's review, developers can abuse them freely. Using these APIs, enterprise apps can access installed apps and sensitive information Apple tries to protect.
- **Exploit:** Enterprise apps can exploit the iOS by jailbreaking it. In this scenario, apps can do virtually anything their creator wants, like controlling both the device and the user's information.

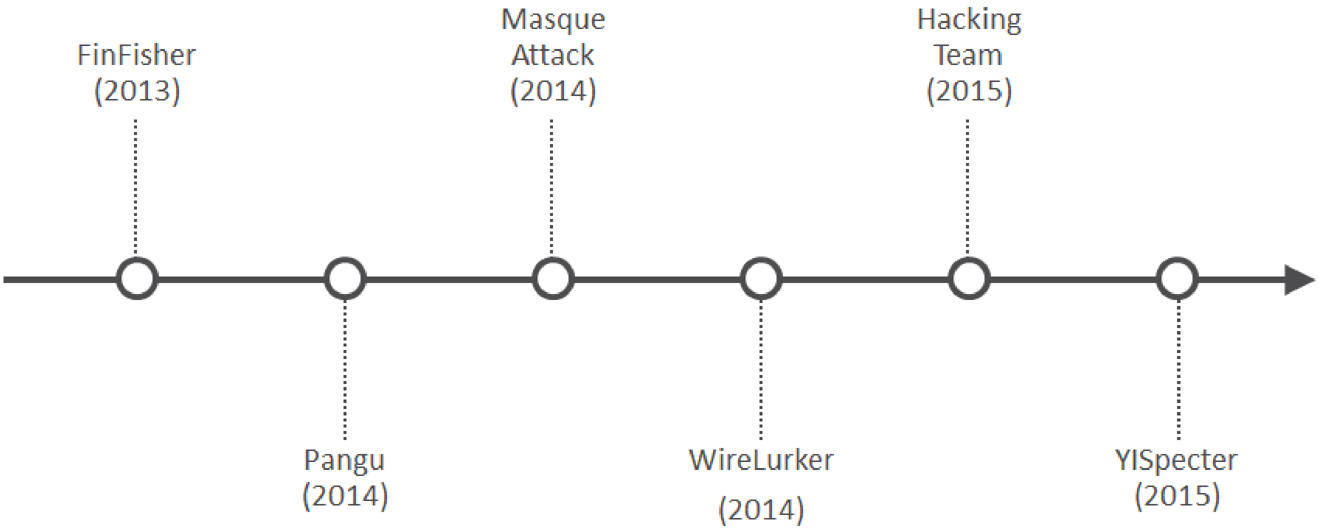
There is very little that limits enterprise app developers from using these methods in a malicious way.

The second line of defense is the iOS user's trust. A user must explicitly approve an enterprise app for it to be installed. This is supposedly an effective way to prevent malicious enterprise apps from being installed. However, most users will still go through the extra steps to install an app, as can be seen from our field research, allowing enterprise apps to be installed regardless of their origin. Although developers of enterprise apps must sign an agreement not to abuse APIs or exploit the operating system, user trust alone cannot be considered a valid form of protection.

From Theory to Practice: Enterprise App Abuse

Enterprise app certificates are abused on a regular basis. Third-party app stores like vShare, 25PP, Kuaiyong, 7659 and others abuse certificates as a distribution method. These third-party app stores register as an enterprise with Apple to enter the program and obtain an enterprise certificate. They use the certificate to install apps on their customers' devices, claiming they are "staff" members.

Unfortunately, many examples of malicious abuse of enterprise apps can be found:



Test case: Hacking Team

One example of an attack that abused enterprise developer certificates is the case of the Hacking Team's iOS malware, which in 2015 targeted iOS versions 8.1.3 and earlier.

The malware leveraged a vulnerability dubbed Masque Attack, which allows enterprise apps to replace existing apps on a device, including system apps. The newly-installed app keeps the original app's directory and can steal any local cache that existed. In order to create an app with a matching bundle identifier, an attacker must use an enterprise certificate, as bundle id verification is done when submitting an app to the App Store.

Hacking Team used this attack method and abused an enterprise certificate they owned. Using this certificate, they created a malicious app disguised as the Newsstand app which was native to iOS until iOS 9. The malware accessed the user's location, photos and address book and sent their data to a server. In addition, the malware installs a keyboard which records all keystrokes and sends them to the server.

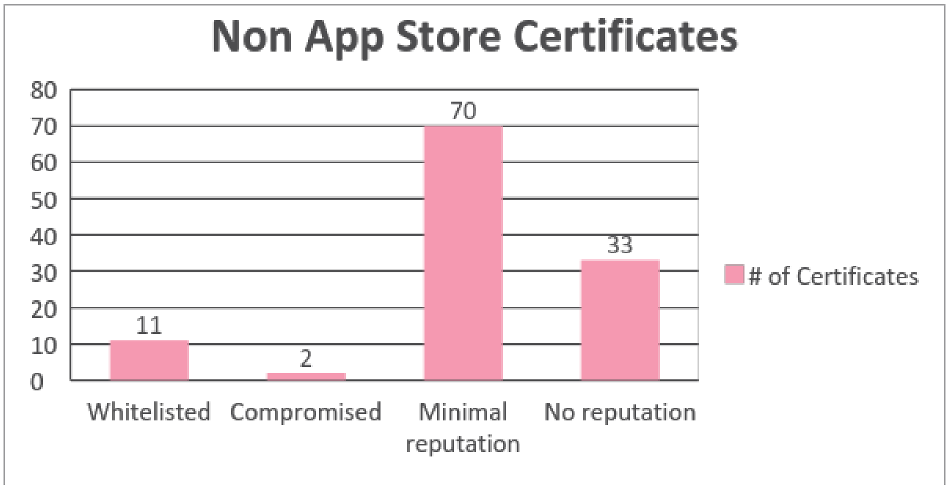
The only reason Hacking Team could have leveraged the Masque Attack is because they used an enterprise certificate to bypass the App Store bundle identifier check.

Case Study: Fortune 100 Company

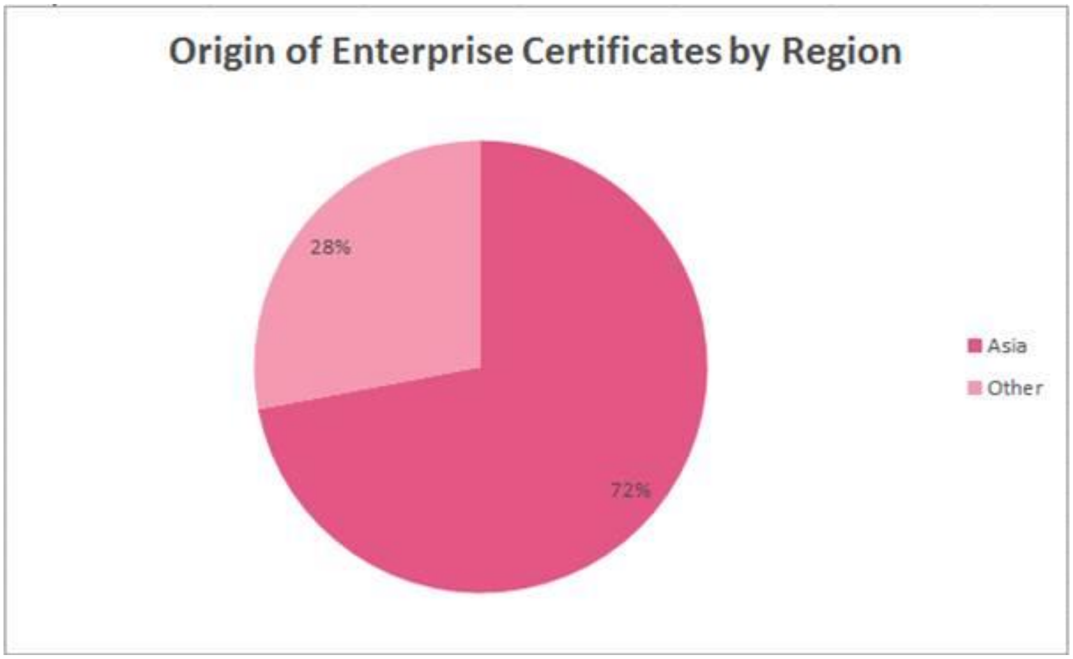
Check Point researchers studied the use of enterprise apps in a Fortune 100 company, analyzing approximately 5,000 devices. The results were intriguing:

- 318 unique enterprise apps were installed
- 116 unique enterprise certificates were used

Of the 116 unique enterprise certificates, only 11 belonged to whitelisted developers with positive reputations and a record of having previously developed apps. Most of the certificates belonged to developers with little or no information about their reputation.



More than 70 percent of the enterprise apps originated in China and other Asian countries. Because the App Store in China is not as widely adopted as in other parts of the world, developers distribute apps to other app marketplaces.



A Hard Problem to Solve

Following the attacks on the timeline above, Apple understood the problem with enterprise apps. Enterprise apps cannot be eliminated since many organizations are already heavily invested in this this solution. However, Apple did take certain steps to mitigate the threat.

In response to what amounted to a significant vulnerability to their ecosystem, Apple introduced a new security measure for enterprise apps that will increase the complexity of executing enterprise apps. When the enterprise app is initially downloaded, the user must go through a maze of settings screens in order to verify the app’s developer. Only after this verification process may the app be executed. This process differs from previous versions of iOS, in which the user was merely shown a message the first time they opened an app that stated it was from an unknown developer.

Apple did leave a loophole, however. Enterprises use apps in myriad ways, and many users can’t handle the new workflow of actively trusting apps. So iOS natively trusts any app installed by a Mobile Device Management (MDM) solution, which is exclusively used by businesses. In fact, an app installed by an MDM, will not show any indication of its origin.

Mobile Device Management (MDM)

MDM solutions are used often by enterprises to support BYOD (Bring Your Own Device) programs, in which the business allows personal devices to be used to access email and other corporate services. MDM is a central management tool that enables enterprises to manage policies on the devices used by their employees. Actions they can take include deploying security policies, remote wiping lost or stolen devices, installing applications and more.

However, MDMs can be exposed to Man-in-the-Middle (MiTM) attacks which can be used to install enterprise apps. Combine this with Apple’s policy of giving apps installed via MDM a free pass and you get a dangerous combination."

Bypassing the Gatekeeper

MDM-distributed apps can be abused by using the following process:

- Installing an iOS configuration profile: A native way to distribute a set of configuration settings such as networking, security settings, root CAs and more. An attacker can craft a configuration profile which will install a root CA and route traffic through a VPN or a proxy to a malicious server and initiate a MiTM attack. This configuration could be deployed through a phishing attack easily.
- Setting up a remote enterprise app server which serves the malicious app.
- Using a MiTM attack, an attacker can wait for a command sent by the MDM server. Once intercepted, the attacker can replace the command with an app install request. The iOS device will fetch and install the malicious enterprise app.
- The malicious enterprise app can now execute without explicit user trust. The user will not be able to distinguish between legitimate enterprise, App Store apps, or a bogus app installed by an attacker.

Conclusion

1. Apple’s iOS ecosystem allows unverified code to be introduced to the iOS ecosystem through enterprise apps.
2. Non-jailbroken devices are exposed to attacks by a malicious actor using bogus enterprise apps.
3. Enterprises cannot trust the end user judgment in BYOD environments as Apple suggests since they will remain exposed, as we have demonstrated.
4. The additional security mechanisms that Apple has added to the enterprise apps execution may not be enough to mitigate the issue.
5. Enterprises should have a clear way to view and assess the enterprise Apps in their organizations.