White Paper

Securing the Mobile App Market

How Code Signing Can Bolster Security for Mobile Applications

Symantec™

Norton™ SECURED
powered by VeriSign

Securing the Mobile App Market

How Code Signing Can Bolster Security for Mobile Applications

CONTENTS

Introduction

The emergence of mobile applications has fundamentally changed the way that millions of people around the world work, play, and communicate. Users can now download every type of application imaginable – from games, to maps, to movie and TV show tie – ins, to apps that will turn a device into a flashlight, and more – directly to their smart phones and other mobile devices.

Though the market for mobile apps is still relatively young, it has grown exponentially over the past several years and will continue to expand rapidly. Fueled by millions of consumers and business users looking for innovative applications, this explosive growth presents a tremendous opportunity for software developers looking to create – and monetize – the next hit app to help people be more productive, or simply have fun.

But developers aren't the only ones looking to profit from the surge in apps – cybercriminals want to infect and exploit as many mobile devices as they can to steal confidential information. Infected apps are not only a threat to mobile device users, but also to network and platform providers, device manufacturers, and the reputation of the industry as a whole.

Fortunately, developers can protect their code – and their customers – with a straightforward and easy-to-manage technology: code signing certificates. This white paper will detail the rise of mobile applications and why code signing certificates are essential to protecting the entire mobile apps ecosystem.

An Industry is Born: The Dawn of the Mobile Application Market

Mobile device apps have been around for years, but some analysts have picked July 11, 2008 – the day Apple launched its iPhone App Store – to mark the birth of the market for mobile applications. Apple customers downloaded more than three billion applications in just the first 18 months of the App Store's existence, making it the largest applications store in the world[1].

Even though Apple was hailed as a mobile apps pioneer, mobile device users had already been downloading apps from online application stores for many years. Mobile device users have also been able to download apps from numerous "off-store" sources, including popular websites such as Download.com, and directly from application developers themselves. In addition, some cellular network carriers have tested the waters with their own mobile app sites.

While the Apple App Store wasn't the first to offer apps, it was the first to prove that consumers would flock to mobile applications – and integrated "on-device" storefronts – if they were easy to download, install, and use. By lowering technical and financial entry barriers, Apple's innovative storefront also succeeded in attracting hundreds of thousands of enthusiastic app developers. These changes have drastically changed the mobile apps landscape. Now, network and platform providers, as well as some device manufacturers, offer development

[1]Apple's App Store Downloads Top Three Billion", January 5, 2010.
http://www.apple.com/pr/library/2010/01/05Apples-App-Store-Downloads-Top-Three-Billion.html

kits to help software vendors create innovative applications. In turn, developers who work with storefronts get marketing help and ready access to millions of eager customers ready to pay for the next killer app.

Mobile applications have become big business, a fact that has led to more opportunities for developers, a deluge of new apps for customers, and fierce competition among device manufacturers, network providers, and platform providers racing to stake out their piece of the mobile applications market.

The Mobile Apps Business is Booming – and So Are Security Risks

Since the launch of the App Store, many other companies have joined the field and opened their own app stores, the most notable being Google's Android Market.

In addition to selling apps through storefronts, developers can work with network providers and device manufacturers, whose portals typically do not contain dedicated storefronts to create apps across a range of mobile operating systems and devices. For example, AT&T has built a strong developer program that allows app vendors to reach 80 million AT&T customers, while LG has created its own Applications Store to offer apps that are compatible with LG devices sold under a variety of brands.

Even though storefronts currently generate the most buzz, users can still download apps through a variety of different independent off-store websites. In fact, off-store downloads account for the majority of application downloads and revenue worldwide. The number of off-store downloads will decrease as storefronts become more popular, but they will likely remain an important distribution channel.

With tens of thousands of apps to choose from, customers are spending billions of dollars on applications every year. By 2014, consumer spending on apps is estimated to grow to 25.5 billion dollars[2] . To put that in perspective, that's more than the revenue generated by professional football, baseball, basketball, and hockey in the United States – combined.

For mobile device users, apps are just a quick tap or click away. Unfortunately, more apps and software downloads mean that there's a greater chance that malicious code will slip through. In fact, rogue apps are already sneaking into storefronts: In January of 2010, two credit unions discovered a "banking" app in Google's Android Market that fooled customers into sending sensitive financial information to cybercriminals. Google quickly removed the app – along with 50 others written by the same hacker[3].

Apps for Everyone

A steep rise in the number of app downloads will continue to fuel the rapid growth in the mobile apps market. How sharp will the increase be? By 2014, it is estimated that there will be 19.5 billion app downloads. That averages out to just under three apps downloaded by every person on the planet.

[2]Mobile Applications & App Stores: Business Models, Opportunities & Forecasts": Juniper Research, May 2009
[3]"Malware Sneaks Into Android Market": Wired.com, January 14, 2010

As mobile apps become more popular, malware attacks on these devices will rise exponentially. Part of what makes malicious apps so dangerous is that they can be next to impossible to spot. Malware apps can be easily assembled using parts from standard developer toolkits, and many of these apps exploit information – such as location and contact lists – to which many users will grant access when they believe an app is safe and legitimate. Even if users aren't sure if an app is safe, many don't read permissions notices closely, or may grant access out of habit. It takes just a quick click to give an application access to highly sensitive information.

Even if users don't allow an app to discover their location or other personal information, many are designed to collect this type of information anyway. In fact, the App Genome Project discovered that nearly one third of apps track a user's location, and about 10 percent try to access contact and address lists[4].

Apps that are built to gather personal information are an ideal target for hackers. If apps like these are left unsecured, hackers can alter just a few lines of code and turn them into dangerous, information-stealing malware. Instead of creating a malware program from scratch, hackers can simply hijack an existing application, a fact that makes it even harder to ferret out malicious programs.

Despite growing awareness, and the fact that end users are more careful and take more precautions to prevent infections, malware is here to stay. Given these trends, securing your mobile applications is absolutely essential to protect your customers, your products, your business reputation, and the overall mobile apps ecosystem.

Security Is Key to Successful App Development

Along with smooth game play or an appealing, easy-to-use interface, application developers also need to consider how to deliver their apps safely to customers. While most malware may seem like more of a nuisance than a true danger, a malware infection of any kind can be potentially disastrous. And if consumers are too fearful to download an app, it can not only damage the reputation of a developer or network provider, but also drive away revenue as users switch to apps, networks, and devices they believe are safe.

Many app storefronts and websites recognize this danger and have developed security protocols that require the use of digital signatures to identify the software developer. However, some stores require only self-signed digital certificates that don't validate the developer's identity, a practice that can expose storefronts – and customers – to malicious apps.

Even though most app stores and websites outline some security standards, these are often not as strong as they could be. Code signing certificates from a trusted third-party provider can help ensure secure distribution and bolster trust that your apps are safe to download.

[4]"Smartphone security put on test": BBC News, August 9, 2010

Are Self-Signed Certificates Really Safe?

While commonly used, self-signed certificates are not the best option for developers. While self-signing confirms that code comes from a particular publisher and that it hasn't been tampered with, it can't prove that the publisher is trustworthy. In other words, anyone can self-sign a certificate, including a cybercriminal. Working with a trusted third party helps ensure that your code is safe, demonstrates that your business is authentic, and keeps cybercriminals from masquerading as legitimate developers.

Code Signing Certificates Mitigate Security Risks Unique to Mobile Apps

Although driven by business objectives that are substantially different, mobile device manufacturers, network and platform providers, and app developers are closely related and depend on each other to maintain a thriving mobile apps marketplace. Given the shared risks to their revenue and reputation, each of these key players has a vested interest in ensuring the safety and integrity of the entire mobile apps environment. Code signing certificates, particularly those from a trusted third-party provider, are critical to protecting mobile apps and the technologies that support them.

For developers, the benefits of code signing certificates are obvious. Many storefronts and network providers require digital signatures to allow apps to access phone functionality, and code signing certificates not only help ensure that your code has not been altered since it was signed, but can also demonstrate to customers and business partners that you are a legitimate, trusted developer.

Network providers, on the other hand, face a different challenge. Facing declining revenue from voice services, network providers need to attract more subscribers and sell more network services. To make this new, services-focused business model a success, network providers are turning to apps, either by working with developers to create cross-device and cross-platform apps (such as AT&T), or by supporting the mobile devices that feature the latest popular apps. By helping to ensure the integrity of application code as well as providing a mechanism to control which applications are deployed on their networks, code signing certificates can help providers keep their networks malware free.

How Code Signing Works

Code signing certificates from a third-party provider can authenticate the identity of the publisher and the integrity of each piece of signed code. Here is how the process works in general:

1. A Certificate Authority (CA) validates a developer's identity and legitimacy as a software or content publisher.
2. The CA then issues the developer a specific developer ID that is used to authenticate the developer when they want to sign code.
3. The developer then uses their specific developer ID to sign the files of their application that they send to the CA.
4. The "re-signed," or authenticated, content is now ready for trusted distribution.

For device manufacturers, the challenge is also two fold: These companies need to appeal to developers while being mindful of the requirements of network providers. To attract the most buyers, mobile devices need to offer the apps that consumers want. Manufacturers also need their app-enabled devices to be accepted by network providers, a situation that may involve a patchwork of security requirements. Code signing certificates can help ensure the integrity of the apps on mobile devices regardless of which network carries it.

Platform providers also need to ensure the integrity of apps on their networks, but for slightly different reasons. Providers like these license their platforms to device manufacturers, so the more licenses they sell, the more successful the platform provider becomes. In turn, device manufacturers that use these platforms want their devices to be carried on as many networks as possible. To protect end users, as well as the reputation of every player in this chain, testing and code signing security are essential for platform providers.

From initial development to final download on an end user's mobile device, code signing certificates can be used to effectively safeguard the entire mobile apps ecosystem, protecting consumers and companies alike.

Conclusion

Although mobile apps have been around for more than a decade, innovative new mobile devices and easy-to-use storefronts have made apps mainstream and pushed demand higher than ever before. Developers, network and platform providers, and device manufacturers have teamed up to create a thriving – and highly profitable – market for mobile apps.

Unfortunately, cybercriminals are also looking to capitalize on the explosive growth of mobile apps. They are already hard at work creating malicious software designed to steal users' information and wreak havoc on the larger apps ecosystem.

However, there is a relatively simple yet highly effective solution to protect mobile apps. By using code signing certificates from a trusted third-party provider like Symantec, developers can safeguard their code and prove that their business is legitimate. By the same token, network and platform providers, as well as device manufacturers, can require code signing certificates in their security protocols to help ensure safety across the mobile apps environment. When consumers are sure that apps are safe, they will download more, boosting distribution volume and revenue for developers and the businesses that carry and market their software.

By making code signing certificates an integral part of the application development process, companies as well as their customers can continue to benefit from the unexpected and exciting rise of the marketplace for mobile apps.

More Information

Visit our website

http://go.symantec.com/code-signing

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com