Abstract

Code signing allows consumers to better trust developers by allowing developers to ensure their product is protected from unwanted tampering by a third-party. Through methods including TLS encryption and Xcode implementation, code signing protects end-users from unwanted criminal and malicious intent from outside parties.

1 Code Signing Introduction

Security and protection are very important to consumers as it allows people to feel safer when using their computer. Consumers can ensure their applications are safe typically when developers undergo the process of code signing. Code signing allows developers to digitally sign their applications as to ensure that the code written is valid and not harmful. This process is very important as it is the base form of protection against unwanted tampering of code. Certification authorities (also known as CAs) sign each person's program with a public key linked with their identity to create their certificate. The process of obtaining a certificate is not complex but is very integral for the developer's software to be determined as safe for the public. The certification authorities help combat against malicious developers which are becoming more of a threat.

2 Authentication and Integrity

The two keywords to proper code signing, *Authentication* allows the consumer to verify the author of the application and *Integrity* which allows the verification that the application's code has not been modified since signed. Authentication not only lets the user know where the application is from and who developed it, but rather the knowledge that the application is reputable enough to not question the validity. Integrity ensures all participants are willing to understand that their application is proper, and any malicious code is directed to the signed applicants.

3 Code Signing Process for Application

Receiving a certificate for an application is straightforward but requires payment and information from the user. Services including DigiCert allow for the certificate to be signed towards the application. Signing an application ensures the end-user the program in question is safe to use.

4 SSL Encryption

SSL (Secure Sockets Layer) encryption allows companies to receive authorization that their website is safe for the public and contain no malicious content. Creating an authorized environment involves a similar process as one obtains a certificate from CAs. SSL allows the encryption of important data from the end-user to not be tampered with during the delivery.

5 TLS Encryption

TLS (Transport Layer Security) encryption is the overall security protocol used by websites to protect against unwanted tampering of website data. TLS is now widely used as the proper encryption for website and requires a valid certificate from CAs. TLS evolved from SSL which improved on security and is less vulnerable.

6 Code Signing Process for Domain

The retrieval process for a certificate is miniscule however the underlying steps are 100% unique to each party and require unique info from the first party.

6.1 Generating Certificate Signing Request (CSR)

Using a proper operating system such as most Linux-distributions:

1. `openssl req -new -key domain.com.key -out /path/to/www_server_com.csr` will generate the requires *certificate signing request* (CSR) file needed to send to a proper CA. `domain.com` needs to be altered to where the user's website address is located.
2. Following will prompt several instructions to input:
    a. Common Name: `domain.com`
    b. Organization Name: `Example Inc.`
    c. Organization Unit: `Marketing`
    d. City/locality: `Silicon Valley`
    e. State/province: `California`
    f. Country/Region: `US`
3. When instructed, do not input challenge password. Each instruction should be modified to the developer's discretion.

6.2 Obtaining certificate with CSR

The CSR generated allows the user to obtain a certificate from a trusted CA. There are many examples of CAs across the internet including but not limited to, DigiCert, Let's Encrypt, Google Trusted Services, etc. Options including Let's Encrypt are nonprofit solutions that do not require payment and are trusted the same as other CAs. Understanding where the certificate is being retrieved from is important.

6.3 Usage of certificate

The certificate obtained from the authorized CA allows the securing of a website and securing of applications written from the developer.

7 Apple's Implementation

The modern multi-billion-dollar corporation Apple has implemented a form of code signing for use on Apple hardware. Code signing is required to submit and upload their application to the App Store which requires their Apple Developer ID. This process is important in securing the App Store from unwanted malicious applications but also disallows independent developers from publishing their application without requiring monetary compensation.

8 Conclusion

Protection from outsiders is important for the stability of the digital world. While code signing does not 100% guarantee protection, it is a good step to dismantle unwanted tampering of websites or products as well as understanding the product the end-user decides to endure.

https://casecurity.org/wp-content/uploads/2013/10/CASC-Code-Signing.pdf
https://www.digicert.com/ssl/
https://www.sslshopper.com/what-is-code-signing.html
https://www.ssl.com/how-to/manually-generate-a-certificate-signing-request-csr-using-openssl/
https://mkaz.blog/code/code-signing-a-windows-application/
https://linux.die.net/man/1/openssl