Hello, I am Chris, and this is my segment on Code signing, hashing implementations, and the importance of security for operating systems as well as for web servers and the various implementations used and which one is applicable for your field.

Security and protection are important to consumers as it ensures that the software you are using, the website you are visiting, as well as the developer or publisher surrounding the product are trusted. Code signing is a way of preventing unwanted malicious intent in various programs and websites. The process to sign a product isn’t entirely hard but can be expensive depending on the level. The way code signing is done is through CAs or also known as Certification authorities. These certificate authorities vary and are considered trustworthy. Some notable examples are DigiCert, Let’s Encrypt, Google Trust Services, etc. The reason this is important is because ensuring safety for consumers helps build trust in the digital presence but also builds a foundation for software and websites. The image shown showcases a piece of software that has been code signed versus one that is not. Windows will explicitly tell you the publisher the product comes from when it is signed.

There are two underlying terms when used with code signing. Authentication and Integrity. Authentication allows the consumer to verify the author of the product in line to understand and do further research when necessary. Integrity is the seal that the code has not been tampered by a 3rd party along the way due to hashing algorithms which I will explain later.

The way that code signing works is that the product is converted to hashed code through various algorithms which I will talk about later. This hash is then encrypted with a private key which is then time stamped by a third party for example DigiCert as well as given a signature which is then approved, and then the product is received. While the steps seem straight forward, there are many hurdles to overcome.

A form of code signing could be encrypting a website. There are various types of encryption but the one you will see most commonly is TLS or Transport Layer Security encryption. SSL is also a type of this however TLS has evolved from SSL. TLS encryption is a link between the server and client and is used for most trusted web servers around the world. The picture showed showcases how TLS encryption in action.

A fast way to determine whether a website is encrypted or not is just by looking at the URL at the top of the page. Most websites can be visited through its http method as well as its https method which easily showcases when websites are encrypted or not. As you see, CSUF’s website is encrypted by the organization Internet2 as of February 27th and ends in 2 years. You can see it has also been encrypted with SHA-256 which is a very common hashing algorithm used.

The process for code signing an application comes in two forms, the development and production ways. Development methods are all self-signed from the computer, are completely free, however are not meant to be shared with the public. The development method however is used for production and release to the public. The steps listed help sign the product with a specified timestamp and hashing algorithm. The websites listed help for creating a signing certificate as well as signing a package. Microsoft has detailed an explanation on how to with their resources. The picture here showcases a signed application of the Minecraft launcher with the SHA-1 hashing algorithm dated in January.

An important part of code signing is protection from tampering which is where the secure hashing algorithms come in. They are developed as a way of creating a unique signature for every application. This was started by the NSA as a way of sending documents securely but quickly evolved into a finely secured algorithm for protecting code. SHAs are used for determining whether the given software is valid.

As you can see there are many different types of hashing algorithms. The one most commonly used nowadays for websites is SHA-256 which is a great middle ground for high security and decent speed.

Now I am going to show you an example certificate generated and installed on my computer that showcases that the application is properly signed for public installation. Here is the launcher for Blizzard Battle.net used to install and launch many of Activision's products. Security is important in the scenario so ensuring secure lines and secure routes to their servers is important.

Using the program on windows certmgr, we can view the signed certificate, the hashing algorithm used, as well as the date is was signed and how much longer until it is not valid. Certmgr lets you view any certificate installed on a computer. If you look below there is also a libusbK certificate signed for intention of Code Signing. This is specifically created for use on the computer only without Server Authentication.

Apple’s implementation of code signing for their products is easy just as their products are. All you do is sign up for an Apple Developer ID. This is easy however is run by Apple and costs money. Which can help deteriorate independent developers with a high annual cost.

____

While code signing is a good way to secure a product, it isn’t perfect. Firstly, the code behind the certificate is not 100% guaranteed to be safe as there could still be bad intent inside. This process isn’t free however there are alternatives. For websites, using a website like Let’s Encrypt lets you obtain certificate for a website for free. My personal website uses Let’s Encrypt and I only had to pay for a domain name. The method took me about 30 minutes. The software in the end could also be closed source and could hide information that is malicious towards the end-user which code signing cannot protect against.

____

In conclusion, it is highly recommended to code sign website and products for public use as it helps people feel comfortable while using the software or website in question. Windows and MacOS have very high security and it is recommended to use code signing for your products in the future.