Carlos Enriquez
Dr. Philip Lunsford
ICTN4040
04/15/17

The Importance of Digital Certificates

The internet is now very common thing for most people to have within their households in America. People use it without truly knowing what keeps them safe from viruses or malware when they visit a website and decide to purchase an item from that certain website. People just see something they like and enter their credit card or debit card and make the purchase. This can be dangerous in some cases when websites do not offer digital certificates or even HTTPS to signify that the websites comply with safety features to ensure that the consumers credit cards are safe from being stolen. Most people assume that having anti-virus software, such as Symantec, will keep them safe from everything. Digital certificates offer another layer of security when people go to websites whether that be to purchase clothing or something type of item or to just log in into their email. People need to understand the importance of digital certificates and how making sure a website has it can protect them. The following paragraphs will how show someone can make sure that a website has a digital certificate, what is a digital certificate and what are the available types, why they should not purchase something that doesn't have a digital certificate and about a hacker group called Suckfly using digital certificates to exploit them for their benefits.

Digital certificates can be viewed as an ID card such as licenses issued by states. "It is a digitally signed binding between a public key and one or more attributes of its owner. Those attributes can be the owner's identity such as a name, e-mail address, URL (Uniform Address Locator), or authorizations that can be used to gran permissions or capabilities. (Levi, Caglayan,

& Koc, 2004)" This means that a certificate must be issued by a company who as the authority to issue one. They are known as the CA or certificate authority. When the CA sees, the public key coming from the party that wants the certificate they verify all the information and then hands the certificate so it can be used. The CA also digitally signs the certificate to make sure that it was reviewed. Within private networks it is not necessary to have the CA authorize the digital certificate because someone who creates that certificate and authorize it because it is within a private network (Thompson, Essiari, & Mudumbai, 2003).

Companies such as digi-sign and digicert can offer three types of digital certificates and depending on what you need you must choose between one of them. The most common is SSL certificates which means secure sockets layer but companies now a day have changed it to TLS which means transport layer security. People still use both terms interchangeably and you can say either and most people will understand both. Most consumers are protected by SSL certificates but do not know it. It appears as a green https bar on the URL and sometimes it is specified by a lock icon that is also green. It usually appears when a consumer is at a protected website and safe one. This lets the customer know that this company, such as https://www.digicert.com, is protected because they have the https instead of the regular http. Web browsers such as google chrome will usually let the person know that the website is not secure and should be looked at with caution especially if it comes to signing into something or purchasing an item. Almost all retail companies will have the green logo on the URL because they want to make sure their customers are protected and do not want their servers breached for the credit card information and this will cause them to lose consumers and be down to fix the breach.

The second type available to companies is Software signing. This means that programs such as adobe pdf reader, when downloaded, will show that their software is safe and secure. All computers will usually tell you if that software you're downloading is valid because they check the certificate for you automatically (Microsoft, n.d.). The user however can check the certificate manually to make sure the program they download is the actual program they wanted. All software that is downloaded will usually bring a code signing certificate to prove that it isn't a fake one or something malicious. Therefore, people who click on links that say "your java is out of date, update now" are fake all the time and will usually cause your machine to get a malicious program and then ruin it. The everyday user will usually have a hard time not believing that their machine is fine and doesn't need that update or program, a lot of people click it because they lack the knowledge to believe that is a false statement. People must learn to go to the actual website and download it from a verify company and see that it will not cause any problems and those websites will have the SSL certificate as well so that makes sure that it is safe.

The last one available is called client certification. This one is a little more confusing and but "they are used by specific individual people, or organizations, that went to streamline paper base process and/or replace them with more efficient digital equivalent. (https://www.digicert.com/ssl, n.d.)" So these are like stamps that people get when printing out information, a lot of companies do this for lease types of contracts like for apartment complexes. This one is the easier one for users to understand because they typically are highlighted and are pointed out that it is safe to sign the contract online. If anyone ever tried to change the information the pdf or document would show that it has been tampered by an unknown party.

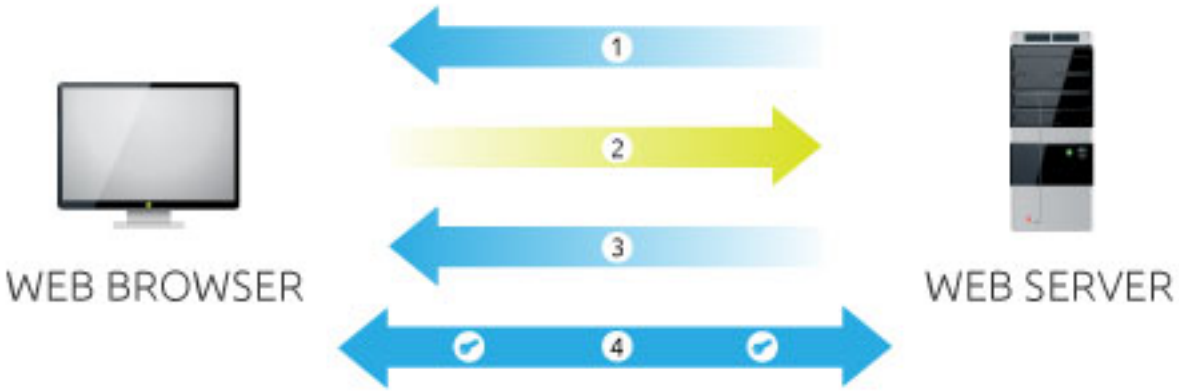
Since SSL certificate is the most common type that the average computer uses or deals with on a regular basis, the following paragraph will discuss the type of encryption that it uses

and how it is used to protect the consumers. As discussed before SSL is an encrypted link between a sever and a client and this also includes emails such as outlook. SSL uses two forms of encryption depending on the company that is using it or what type of information is being sent across the server, the first one is Asymmetric Encryption or otherwise known as public-key cryptography (IBM Integration Bus, 2017). The form of encryption that it uses is RSA because it is the most common form to use. It uses two sets of keys to send information and then decrypt it. Basically, the first key is encrypted with the information and the second key is uses to decrypt but the second key is the private key (https://www.digicert.com/ssl, n.d.). Unless the receiver has the private key, the information can be accessed and tampering with the information during transmission will not work and both parties will be notified of the occurrence.

They use 2048 bits of information to generate the keys and anything smaller such as 1024 is not recommended and anything more than 2048 is also not recommended because it's too much of a computational burden (DigiCert, 2017). This video link shows how long it would take for someone to break an encryption of 2048, https://www.digicert.com/TimeTravel/ .

The second type of encryption that SSL uses is Symmetric encryption. "Symmetric encryption (or pre-shared key encryption) uses a single key to both encrypt and decrypt data (DigiCert, 2017)". So therefore, both parties must have the same key to access the information or neither party will be able to do anything once they receive the information. Symmetric encryption uses a smaller form of AES such as 128 or 256 but it also is a less of a burden on the computer. This does not mean it is any less safe than Asymmetric encryption, it just has a disadvantage when it comes to data transfer of information, otherwise it is safe as well. SSL systems have become so secure now a day that SSL certificates can use both encryption methods.

"Public Key Infrastructure (PKI) is the set of hardware, software, people, policies, and procedures that are needed to create, manage, distribute, use, store, and revoke digital certificates (DigiCert, 2017)." PKI is also what holds together and binds keys with user identities by using the CA. "PKI uses a hybrid cryptosystem and benefits from using both types of encryption" (DigiCert, 2017).



This diagram best displays the session of a PKI. The number one is when the web server sends the asymmetric public key and then two is when the web browser creates a symmetric key for the session and encrypts it with the severs asymmetric public key and when it all finally comes together it send it back to the sever. The line three is when the sever uses the asymmetric key to decrypt the session and to get the symmetric session key. Once this is all done line four is when all the information is being shared back and forth so both parties can read everything. However, each key that is created is a one-time deal so when the user connects again, a new key would have to be generated (DigiCert, 2017).

During the year and month of March 2016, Suckly an advanced cyberespionage group, made a serious of attacks towards companies in India. The way they did this, was through the method of stealing digital certificates (DigiCert, 2017). Symantec was the company that discovered these flaws but it took them two years to find out what was going on. They used a

custom malware that they created to steal the digital certificates and the name of this malware was called Backdoor.Nidiran. The type of certificate was a code signing certificate, this means that someone within the company approved the use of a program or email and clicked on something and that is how Suckfly infected the computer of a single user and then worked their ways into other parts of the company or companies. The reason the person clicked the download or upload was because of the stolen digital certificate so Suckfly falsely used that to make it seem like their program was a valid type of program. This just proves that even CA must be checked to confirm that they are doing their jobs well enough and prevent further incidents from happening.

People must be informed on whether a website is safe to use or just to learn what https stands for. By knowing this, a lot less consumer data will be stolen and people can be sure that they are buying from a valid website that provides a safe environment for the consumer. A lot of people aren't tech savvy so just being a little informed about SSL and how it is looking green can mean to them "safe" is enough to show a little knowledge or just the basic knowledge of a lock.

REFERENCES

Works Cited

DigiCert. (2017). *DigiCert*. Retrieved from DigiCert: https://www.digicert.com/ssl-cryptography.htm

DiMaggio, J. (2016, May 17). *Indian Organizations Targeted in Suckfly Attacks*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks

https://www.digicert.com/ssl. (n.d.). *digicert*. Retrieved from digicert: https://www.digicert.com/ssl-cryptography.htm

IBM Integration Bus. (2017, February 7). *IBM*. Retrieved from IBM: https://www.ibm.com/support/knowledgecenter/en/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55140_.htm

Levi, A., Caglayan, U. M., & Koc, C. K. (2004, February 2004). *ACM*. Retrieved April 12, 2006, from www.acm.org: * http://dl.acm.org.jproxy.lib.ecu.edu/citation.cfm?id=984336&CFID=751753696&CFTOKEN=89612744

Microsoft. (n.d.). *Digital Certificates*. Retrieved from Microsoft: https://technet.microsoft.com/en-us/library/cc962029.aspx

Symantec. (n.d.). *What is an SSL certificate?* Retrieved from Symantec: https://www.symantec.com/page.jsp?id=ssl-information-center#

Thompson, M. R., Essiari, A., & Mudumbai, S. (2003, November 4). *ACM*. Retrieved from www.acm.org: * http://dl.acm.org.jproxy.lib.ecu.edu/citation.cfm?id=950196&CFID=751753696&CFTOKEN=89612744