GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Practical Assignment – Version 1.2e

Digital Certificates – Are They Safe?

By Douglas Heatherly

Abstract

Digital certificates are a common method used for digital identification on the internet today. Digital crime is on the rise and both businesses and individuals require secure, reliable and trustworthy methods for ensuring the accuracy and authenticity of the information received. At the same time, methods must be developed to protect the privacy of businesses and individuals to avoid exploitation and manipulation. Digital certificate technology has evolved and matured over the past few years, but there is still significant opportunity for improvement. Digital certificate software and technologies need to be further simplified and users need to clearly understand the risks and benefits of this technology.

Introduction

In the physical world, we have fairly well established methods for verifying the identity of individuals and businesses that we interact with on a daily basis. We may meet with individuals face to face, talk with them and establish some level of confidence that they are who they claim to be. For businesses, we can visit their stores, browse and view their merchandise, ask questions. Even when we have never met a person before, we can verify their identity by collaborating with a trusted source who can vouch for their identity or we can ask to see a trusted document like a drivers license or a passport or official picture id. Merchants and banks use several common methods for verifying identity. The legal system supports identification in order to prevent fraud and impersonation. Most countries exercise some legal methods for establishing and verifying the identity of individuals and businesses. While it is certainly possible to be deceived by a person or business in the physical world, it is easier in many respects to be deceptive in the digital world. How does an individual or business validate that an electronic transmission came from a trusted, validated source? Digital certificates are one tool that can be used to effectively validate and authenticate the source of an electronic transmission. The essay will address the use of digital certificates, their level of effectiveness and present methods for safeguarding against digital certificate fraud.

What is Digital Identification and How does it Work?

Digital identification is the process of identifying an individual or business based on digital information. In order to understand digital identification you first need to understand basic cryptography. Cryptography has been around for many years. It is essentially a method for converting a plain text message into a secret message that only

© SANS Institute 2000 - 2002, Author retains full rights.

those individuals that know the method used to encrypt the text and the secret key will be able to decrypt and read the original plain text. While this is certainly a very narrow definition that doesn't encompass one way encryption algorithms, it should suffice for the purposes of this paper. There are two basic types of ciphers (encryption – de-encryption techniques). Symmetric ciphers require that the same secret be used for both encryption and decryption of the message. Symmetric ciphers are fast compared to most asymmetric ciphers and are used frequently for communication between a person and a host system. For example, to access your ATM account, you enter a password on pin. The ATM pin is the key for decrypting the information in your account. No one else's key/pin will work with your account, unless perhaps you share the same secret key. The strength of encryption or conversely the ease for breaking the cipher is proportional to the length of the key. Consequently, a symmetric key the length of one character would be easy to break whereas one with 6 or 8 characters would take much longer. Asymmetric keys differ from symmetric keys in that they are encrypted with one key and decrypted with a different key. Asymmetric encryption is slower, but it is much better suited for person to person communication, because it doesn't require the sharing of the single key among the sender and receiver and it is not subject to attack by intercepting the transmission of the key itself.

So why is all of this important? Why don't we just have the sender include a picture of himself/herself or put some identifying mark on the document that could only have come from the sender? The problem is that unlike the physical world, digital messages are very easy to copy, replicate and manipulate especially if they are sent in plain text.

For validating and authenticating an individual user/sender to a system symmetric keys work very well. As long as the user maintains the privacy of the key and does not share it with anyone else, then he/she can be relatively certain that their communication with the host system is private/secure. However, it is still important to periodically change the secret key and ensure that the length of the key is sufficient for protection.

Maintaining secure communications when corresponding with other people is a little more complex. How do you transmit the secret key to the receiver privately? How do you manage multiple keys one for each receiver? What if you decide to change your key, how do you let everyone know? What if someone intercepts your key, how do you prove to the receivers that your new key is not a clever attempt to deceive them?

The answer is to use an asymmetric cipher method. Asymmetric ciphers work by creating two keys that act as a pair. You encrypt with one key and decrypt with the other key. When you create a key pair, one key is often designated the public key and the other key is designated the private key. You share the public key with everyone that you want to communicate. In fact, most users post their public key on a public key server so that anyone that wants to communicate with them can go find their key from the server. There are many advantages to using a public key server which I will discuss later. The sender downloads the public key for the person that they want to send the message to. They encrypt the message with the public key and then send it to the receiver. Only the receiver can decrypt the encrypted message. The receiver is the only person who has the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

other key in the key pair (e.g the private key). Consequently, if the sender can trust that the public key actually belongs to the person that they want to send the message, then they can be fairly confident that only the receiver will be able to decrypt and read the message. It's important to note that once the message is encrypted by the sender that not even the sender can decrypt the message without the private key.

We now have a secure method for sending messages between people, but we still have some issues remaining. How can we be sure that the public key came from the person that we want to communicate with? Anyone can create a public key and distribute it claiming to be any identity. How does the sender prove to the receiver that they are the intended sender. If anyone can download the public key and send a message then how does the receiver know that it came from the sender? This is where digital identification, digital signatures and digital certificates come into play.

As you may recall in the earlier example, using public key encryption methods a user can distribute his public key to anyone with whom he/she wishes to communicate. The sender can then use the public key to encrypt the message so that it can only be decrypted by the owner of the private key that matches the public key in the pair. In addition to distributing the public key, the owner of the public key can include a digital signature. The digital signature is a special group of text that identifies the owner, it usually includes name at a minimum and may include other identifying information as well. The owner of the public key encrypts the digital signature with his private key. Therefore, the only way to decrypt the digital signature is with the public key which is readily available. Only a message encrypted with the private key in the pair can be used to decrypt the digital signature. Consequently, it serves as proof that the owner of the public key is the same individual as the person who created the digital signature.

But how can one be certain that the key pair was actually created by the individual named in the digital certificate? Anyone can create a symmetric key pair and put a fake name in the application form. In order to validate a digital signature, the user should check the digital signature to make sure it contains a seal of authentication from a trusted authority or certificate authority. There are several agencies that specialize in providing authentication services for digital certificates. Two well known Certificate Authorities (CA) are Verisign and Thawte. In order to obtain a stamp of authentication from a CA the user or business must submit proof that they are who they claim to be. For example, Thawte requires users to have a certain level of trust accumulated. Trust points are accumulated by having other trusted sources vouch for your identity. A user might have to provide multiple forms of physical identification to multiple trusted sources in order to establish enough points to qualify for an assigned digital certificate from the CA. Businesses may have to provide notarized documents from an officer of the company as well as provide information for follow-up contact. The authenticated digital certificate serves as proof to users that the owner of the certificate is indeed to person or business identified in the certificate.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In summary, digital identification is accomplished by having a digital certificate assigned by a trusted CA used as a digital signature to validate that the business or owner of the message is the same person/business identified in the certificate.

Are Digital Certificates used for Other Purposes?

It's important to note that digital signatures can be used independently of public key distribution and person to person communications. A digital certificate may be used by a software vendor to distribute updates to its users on the internet. The users can then be assured that the update is not malicious code that was created to destroy or compromise the data integrity of their systems. In fact, this practice is commonly used by major software vendors to thwart attempts by criminals to assume their identity and distribute viruses, backdoors and malicious code.

Have Digital Certificates assigned by a Trusted CA ever been Faked?

On January 29th 2001, Versign, a trusted CA, accidently issued two fake certificates. The fraudulent certificates were issued under the Microsoft brand name. This was a very serious failure in the system. As described in the previous section, a digital certificate assigned by a trusted CA is considered authentic and essentially "notarized". Thousands of Internet users download updates from Microsoft everyday. The recipient of these fraudulent certificates could pose as Microsoft and distribute malicious software to thousands of users. The users would see the digital certificate and assume that the software came from Microsoft.

Fortunately, Verisign discovered the mistake and quickly issued a news bulletin requesting that users check all certificates from Microsoft dated January 29th and January 30th , 2001 with the serial numbers 1B51 90F7 3724 399C 9254 or 750E 40FF 97F0 47ED F556 and reject them. Microsoft did not request any legitimate certificates on those dates so any certificates with those dates would be fakes. Obviously, this puts considerable burden on the user. Most users probably don't click and check each digital certificate to read the details.

Verisign claims that they issued over 500,000 certificates using the same process and this is the first time that they discovered they issued them to a person that submitted fraudulent information. Verisign blamed the mistake on human error. The faked certificates were considered Class 3 certificates. These certificates are the highest grade certificates available for ordering on-line. Verisign validates these certificates by calling a specified representative at the corporation requesting the certificate. It's fortunate that Verisign's audit procedures caught the mistake, however, several weeks elapsed before the information regarding the fakes were communicated.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One benefit of this event was that it forced Verisign and Microsoft to scrutinize their security processes and also made many other businesses and users aware that the digital certification process is not foolproof and there are opportunities for improvement.

Microsoft Internet Explorer (IE) software, a common internet browser, prompts the user to accept or reject software based on the digital signature. In earlier versions of the IE, the software provided a box for selecting that the user always would trust certificates from the particular company. This had the potential to greatly complicate the resolution of dealing with the fake certificates. If the user selected that they would always trust digital certificates from Microsoft, then they potentially would never see the popup screen that asks if they trust the software download. Shortly, after the discovery of the fake certificates Microsoft issued a patch that disables the automatic acceptance of certificates from Microsoft.

Verisign and other major CA's typically provide a method for checking against a database of revoked certificates. However, Microsoft browser software, at the time, did not check certificates against a revocation database. It is unclear whether current browsers validate new certificates against the revocation database. In any case, Microsoft has developed specific patches to check for the fraudulent certificates and they should no longer be a problem for anyone that has kept up with security patches and updates to their software.

Are Digital Certificates Safe?

Despite the VeriSign incident regarding the issuance of fraudulent certificates, digital certificates and methods for digital identification are well established as safe and secure for techniques for authentication and identification. Digital certificate technology is still fairly new and has some opportunities for further improvement. Procedures for the issuance of new digital certificates by CA's needs to be scrutinized and audited periodically by third party organizations to ensure that validation procedures are being followed for all certificates and that multiple checkpoints exist to prevent fraudulent claims.

Users need to be further educated on the use and purpose of digital certificates and need to understand how to read and check the certificates to ensure that they contain the proper credentials. The level of scrutiny and examination should be proportional to the level of risk that the user is willing to take that the originator of the message may not be the same as the trusted source listed in the certificate. For example, an email message that is digitally signed by a relative that does not contain any sensitive or private information may require less scrutiny than an software update that patches the primary security mechanisms of your computer operating system. And users must insist that their software providers use digital certificates and obtain proper CA authentication.

Software vendors should obtain digital certificates and use them for all distributions and updates on the internet. This helps to ensure that fraudulent applications are not

© SANS Institute 2000 - 2002, Author retains full rights.

distributed under the guise of their corporate brand. Software vendors should designate a person in charge of validating all certificate submissions and should have third party audit checks to ensure that proper procedures and checkpoints exist within the company. Browser and operating system vendors should build intelligence into the certificate validation process to make sure that certificate requests are compared against CA revocation databases. And these vendors should avoid making it too easy for users to select options for blanket trust of all certificates from a particular vendor.

As new vulnerabilities are discovered and new techniques developed to thwart attempts to falsify identification information, digital identification methods will become more robust and secure. Digital certificates, if implemented properly and validated regularly, will remain an excellent tool for conducting private, secure communications between persons and businesses.

References

1. Fonseca, Brian. "Verisign issues false Microsoft digital certificates", InfoWorld, May 2001. URL: http://www.itworld.com/Sec/4039/IW010322hnmicroversign/pfindex.html (22 Mar. 2001).

2. Fontana, John. "Verisign issues fraudulent Microsoft code-signing certificates", Network World Fusion, May 2001. URL: http://www.nwfusion.com/news/2001/0322vsign.html (22 Mar. 2001).

3. Garfinkel, Simson. Web Security & Commerce: Risks, Technologies and Strategies. O'Reilly and Associates, Inc., 1997. 99 - 243.

4. Russell, Deborah and Gangemi Sr, G. T. Computer Security Basics. O'Reilly and Associates, Inc., 1991. 163 – 197.

5. Sullivan, Bob. "Microsoft digital certificate stolen", MSNBC, May 2001. URL: http://stacks.msnbc.com/news/548228.asp (22 Mar. 2001).

© SANS Institute 2000 - 2002, Author retains full rights.