Högskolan i Halmstad
Nätverksdesign och datordrift
VT 2008
Lärare:Kristina Kunert

Digital signatures and certification

Patrik Bertilsson. 198812115957. patte_was_here@hotmail.com
Martin Jönsson. 197909163955 deffan@gmail.com

Introduction

What if you have a very important text document that contains very important information like your billing information or your personal information and you have to send it to a trusted source, what if some one else could read it? To bad is there ways to get hold of the information that you did send without know the receivers' login information. One way to do this is packet sniffing witch means grabbing packets that are send thorough your network and put them together and read the information. But do not worry there is a way to protect your self by using Digital signatures and certification.

Digital signatures and certification is a way to communicate in a secure way by encrypting and decrypting messages.
By giving each other a public key and give each other a trust level you can encrypt your message and you know that when your friend receive the message it hasn't been altered in any way and only your friend can read what the message says. There is still ways to bypass this but if you use Encryption you can sort out a lot of the hobby hackers out there whose only intention is to harass and sabotage your interests.

What it is

Digital Signature
When you sign an paper then every body knows it's your handwriting, but what if you want to do this on an email. There is a way and the way is Digital Signature witch is an so called asymmetric cryptography that uses 2 algorithms, signing(private key) and verifying(public key) and the outcome is called "Digital Signature". Digital Signatures offers an authentication to the message and are used to create public key databases that binds public keys together to users with help of a Digital certificate.

Digital certificates
Digital certificates is an message that is attached to the email so the sender and receiver has an safety of that the packet that is send comes from the one he/she claims to be. In the message it is also included the information to use to generate a reply. Digital certificates are used where there is a bigger network where more computers that can sniff or alter packets you send. When it is a bigger network like the internet or a big company then digital certificates are used because you can use 3 party users to authorize mails you send/receive this way u don't have to trust the sender but can trust some one else that trust the sender.

Digital certificates and Digital Signature
Digital certificates is not the same as an Digital Signature witch many people often confuse it with, the difference is that certificates is used to sign an example email so the receiver have an guaranty that it's the right sender and Signatures is the whole process of the encryption/decryption and this offers that the email hasn't been altered or changed in any way.

Standards and Algorithms
The Digital Signature Standard (DSS) is an algorithm that was created bye the US national security agency also called NSA to ensure the authentication of the message. The standard was put in use 1994 and became the standard shortly after. Here are some digital signature algorithms:
Full Domain Hash, DSA, ECDSA, ElGamal signature scheme, Undeniable signature, SHA, Rabin signature algorithm, Pointcheval-Stern signature algorithm and Schnorr signature.

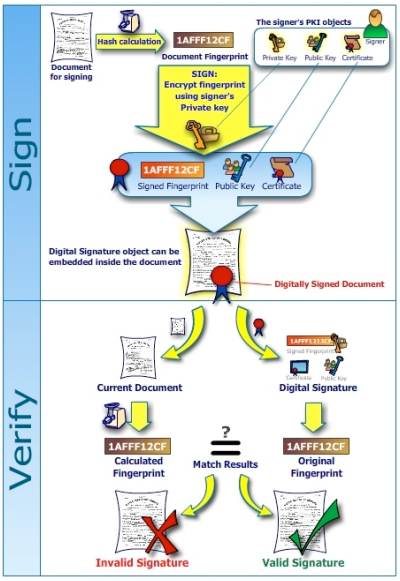
How it works

First you need text message or a document that you want to send. When you sign the message it will go through a hash calculation and make a fingerprint for your message, then you will encrypt the fingerprint with your private key. Then you take the encrypted fingerprint and private key put it together with the public key and the certificate and you will have a digital signature. That digital signature will be embedded in the document or text message you want to send.

Now you will send this to the person that it was meant for and he/she will start to decrypt the message. With your public key that you signed he can open your decrypted message and he knows it's from you and that the text hasn't been altered in any way. For a person who is trying to get hold on the document and want to see or alter it will have problem to do so but there is always a way to open it but its hard.

For the signing you need the certificate. The certificate is a way to show who you are and the certificate can verify it.

You will create a public key and send it to the person you want to have this key and will be able to receive and decrypt your message. He will get the key and will sign it, send it back to you and you can set a trust level on him how much you trust this person. By getting your key signed by different people you can see who trust you and who don't but also you can see what the others trust level is between them. This way you don’t have to sign your key by all people you want to trust but if you trust your friend who have sett a trust level on some one you want to send an email to you can use your friends knowledge about this person to set an trust level on him and send an secure email to this person.



Discussion

The digital signatures and certification is very fuzzy subject since many pages and articles mix both the signing and the certification together. It's hard to really get to know what is what but after a lot of research and a lot of discussion we think we know the different between the signing and the certification.
To sign and encrypt documents is a very important factor in the whole internet because of the Eve's droppers and so called packet sniffers. It's not so hard to encrypt a document but it's kind of hard to understand how it works and all of its belonging parts. We discussed the topic very much and did not come up with any thing because the topic was very confusing but at the end we asked a teacher who could confirm our theories.

Conclusion

Its easy to use digital signing and certificates whene you encrypt you document and its easy for the person you send the document to, to decrypt but to hijack and alter the document is very hard. Encrypting the document is a perfect and very secure way to be secure that the information you send is for the receivers' eyes.

Reference

http://www.windowsecurity.com/articles/Digital_Signatures.html
http://computer.howstuffworks.com/question571.htm
http://help.sap.com/saphelp_nw70/helpdata/en/18/ecb69017ad4765855425b97f666470/content.htm

Picture

http://upload.wikimedia.org/wikipedia/commons/b/b5/Digital_Signature_-_How_it_works.jpg