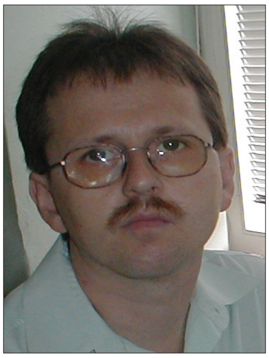
FEATURE 1

DIGITAL SIGN: THE NEXT TARGET?

Dr Ferenc Leitold
Veszprém University, Hungary



The tram drivers in Budapest often warn the passengers: 'Beware! There are pickpockets on the tram – look after your property!' Public messages like this one have two effects: the passengers hold their bags tighter, and any potential pickpockets are alerted to a good opportunity that could be exploited now or in the future. This article attempts to present the possible points of attack relating to the use of the digital signature. Of course, this warning may also have two effects. Nevertheless, it is in the interest of everyone using or accepting digital signatures to be aware of the dangers when they are using the system.

The security problems which are being made public day by day and the continual appearance of new types of virus are undermining the security of the electronic signature. In the hardware and software (including operating systems) environment there is potential for the digital signature to become the target of virus attacks. A computer virus or worm can take control of the victim's computer, where it can create a new signature or, by manipulating the signing process, counterfeit an approved signature.

A further problem is the forwarding of confidential documents or messages. For this PKI tools provide an excellent solution. But the forwarding of an encoded message – especially through a firewall with virus protection – raises several security issues.

DIGITAL SIGNATURE

The algorithm of the digital signature uses the algorithm of the public key encoding (e.g. RSA). The digital signature works as follows. Using the binary code series of the document to be signed, a fingerprint peculiar to that document is prepared. This process can be carried out with the help of the Hash algorithms. The fingerprint is then ciphered with the cipher part of the public key algorithm. The code series prepared this way is the *digital signature* rendered to the document. Afterwards the sender forwards the document together with the digital signature rendered to it. The recipient receives the document and the digital signature and, with the help of the same Hash algorithm, he prepares the fingerprint rendered to the document. Using the sender's public key, he also prepares the fingerprint rendered to the digital signature. If the two fingerprints are identical, he can make sure that the digital signature was made with the cipher pair of the public key used for the supervision. The mathematical theory of the method does NOT ensure that the digital signature has been rendered to the person signing the document or that the digital signature has been made with the knowledge of the owner of the cipher key.

TRADITIONAL SIGNATURE – ELECTRONIC SIGNATURE

When we sign a document on paper we rely on our eyes and our mental ability to make sense of what we see. Our eyes will give evidence to the fact that the signature is put only onto the document that we intend to sign.

When we prepare an electronic signature we must believe that the information displayed on the screen corresponds to a bit series stored in the memory or the mass storage. We must believe that the unit constructing the signature (e.g. an external card reader connected on a serial port or USB) provides only that bit series with the electronic signature whose correspondence is displayed on the screen.

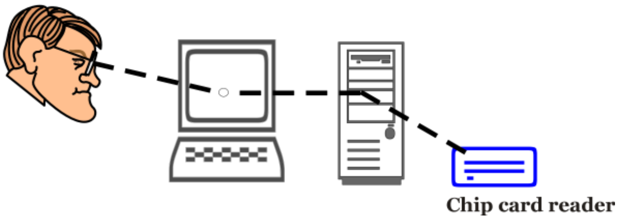


Figure 1. Electronic signature.

When we use a multi-purpose computer to prepare electronic signatures then we must completely trust its hardware and software installation and the proper operation of the software. Of course, we cannot check this in any visible objective way. Thus, there are two opportunities for a potential attacker:

- to affect the presentation
- to manipulate the signing procedure.

AFFECTING THE PRESENTATION

We ought to expect the document that is to be signed to contain all the information required to interpret and present it. If information from another source is required then the image presented of the document may be affected. For example, *Word* and certain PDF documents do not contain all the fonts required to present the image of a document. Thus, in a different environment from that in which the document was created the fonts may be substituted and the image of the document will be different in the new environment. Unfortunately, ASCII text files are no different. Despite the fact that there are no fonts here we must know the image of the characters for the presentation. This is information outside the document (the bit series of the text), which is fixed by the ASCII standard, but the presentations are made by the hardware and software of the computers. In the case of a VGA card the image of the characters can be overwritten! The problem is unrelated to operating system. The notion of fonts exists under *Linux* and UNIX systems too and a *StarOffice* document does not contain the images of the letters either. To ensure the image presented is an accurate representation of the document it is vital that the document itself contains the binary images of the characters.

What opportunities are available to an attacker to exploit the gap in the security system?

1. If the attacker has access to another computer he can change the image of the letters in any of the fonts. Applications that do this are freely available on the Internet (see Figure 2).
2. An attacker may create his own program to change the letters.
3. The attacker can send this program via email. A tremendous number of viruses are sent by email today.

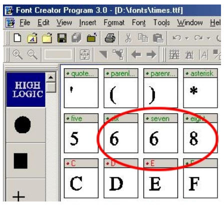


Figure 2. Easy font modification.

A malicious attacker could easily load a program onto a victim's computer, which ensures that the signer will see something different from what he intends to sign. He can also eradicate himself entirely from the victim's computer following the signing, e.g. at a definite time. After that the user would try to prove his honesty in vain; the electronic signature is an approved evidence in the courts of some countries.

MANIPULATING THE SIGNING PROCEDURE

If we are fully aware of what we intend to sign – or at least we believe that we are – we can provide the document with our electronic signature. In order to do this we need a signature-making device.

The signature-making device contains software as well as hardware elements, and ensures that all conditions are fulfilled in order to carry out the signing procedure without any further interaction. If we use some kind of a chip-card, after inserting the card every condition is given for the signature. We cannot check manually whether we render our signature to that particular bit series and we cannot make sure that there is no signature rendered to other bit series.

The following method could be used for an attack: a malicious program, which is loaded onto the computer in one way or another watches the interactive activity the user must carry out after satisfying every condition for the signature (e.g., he has entered the chip-card into the reader). The malicious program senses what information the user program sends to sign for the card reader. The malicious program sends this information to the reader and waits for the response. It does not forward it to the user program but sends another bit series for the reader to sign. When this has happened, the malicious program sends back the signed answer to the user program. All this happens so quickly that the user does not notice anything. Like the majority of email viruses the malicious program may even send the signed bit series back to the attacker using its own SMTP routine.

USING DOCUMENTS WITH A DIGITAL SIGNATURE

The advantage of the digital signature is that the two signatories of a common declaration (e.g. a contract) need not meet in person. It is sufficient to exchange the electronically signed declarations. Nevertheless, everybody prefers to handle their contracts discreetly and would not like any unauthorised party to have access to them. PKI offers an excellent opportunity to avoid such unauthorised access by ciphering the messages.

The electronically signed document must be sent to the receiving party. We can do this through data media or by mail. Either way the solution is not less comfortable than in the case of the traditionally signed paper document. The only significant difference is that when forwarding through data media we can send or carry the information in ciphered format.

A natural way of forwarding a document is sending it through the Internet. Sending a message on the Internet is about as safe as sending information on a postcard – pretty much anyone can read it – therefore it is essential to cipher the document.

Today, every business or institute has an internal information infrastructure or inner network. It is very common for there to be a firewall in place at the meeting point of the internal network and the Internet. The firewall watches the traffic between the inner network and the Internet and tries to protect the internal network from the dangers coming from the Internet. A well-configured firewall system must have packet-filtering devices and content-filtering abilities (e.g. virus protection) too.

Let us assume that two managers intend to exchange their electronically written documents on the Internet. The easiest way to do this is to send the signed message through email. It is essential for both of them to keep the content of the document secret, even within the internal network. Therefore they cipher their messages, which can be done easily with PKI technology.

The real security gap occurs at the firewall. The system managers maintaining the firewalls have two options:

1. They configure the firewall so that it does not allow documents through if their contents cannot be checked. But, in this way, ciphered and signed documents will never get through to the other party.
2. The firewall is set to let through ciphered messages without supervision. Then the two managers can exchange the signed and ciphered messages. But this lapse in security is sufficient for an attacker to send a malicious program through the firewall – if it is ciphered with the manager's public key (see Figure 3).

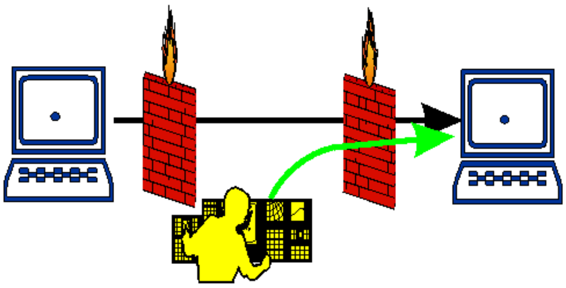


Figure 3. Opportunity to attack through the firewall.

SUGGESTIONS

Being aware of the security problems described above we cannot claim that the use of the digital signature is perfectly safe. If we assume that the digital signature is made on a computer that is used for multiple purposes, we must face serious security problems.

It does make a difference what we sign, or rather, what we sign can be interpreted only in the way we mean it. It does make a difference what system and what device we are using for the signature. And, finally, it does make a difference for what purpose we intend to use the signed document and how we intend to forward it.

One of the shortcomings of the legal regulations in many countries is that they do not specify unambiguously the types of data that can be signed electronically. The legislation ought to define 'text' and 'letter'. Which are the electronic forms that can be regarded as 'text communicated with letters'? Is a scanned A4 page saved in a binary picture format acceptable if it contains letters only?

It is also a basic expectation that the regulated forms and standards should be made public and accessible for all, otherwise how could we supervise a document based on a ciphered form? The supervision could be assisted with supervising software with an open source code.

Regulations should be brought into effect regarding the forwarding of documents that have been signed digitally. At the moment a few of the regulations about the digital signature excludes the use of the keys for other (i.e. ciphering) purposes. The ciphering keys could be classified similarly to the keys used for the signatures. With a common regulation the providers of the authentication could carry out both authentications a lot more easily than doing so separately.

I believe users should be made aware of the potential sources of danger. This could be done by the providers of authentication because they have knowledge of the devices used for digital signatures, and ought to provide a set of guidelines for their secure use.

Users – whether private individuals, business enterprises or public institutions – are interested in the secure operation of their systems. The security of the signature-making devices is closely related to the overall security of the computer. Making the computer more secure by installing a firewall and/or virus protection or a set of security guidelines will make the process of creating the digital signature more secure too.

There is no solution to the security of the digital signature that can be detached from the overall security of the computer.

CONCLUSION

The rendering of an electronic signature to a document raises a number of security problems when we use a computer for making the signatures. The reason is that there is no operating system (probably there cannot be any) which could provide sufficient security for making digital signatures at the moment. Users must maintain an overall security culture, which can help to prevent the potential problems.