Vulnerabilities of the usage of digital signature

The efforts made concerning the use of the digital signature represent a significant step in the information technology. These efforts do not or just to a small extent concern the issues of security. Unfortunately, there are many devices whose use for digital signatures raises serious problems concerning security.

When we sign a document on paper we rely on our eyes and it depends on our mental ability whether we can make sense of what we can 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 our eyes and we must make sense of it. Also, we must believe that the information displayed on the screen (or on any other output device) corresponds to a raw of bits stored in the memory or the mass storage, which has exactly the same sense as we interpret it. We must believe that the unit constructing the signature (e.g. an outer card reader connected on a serial port) provides only that raw of bits with the electronic signature whose correspondence is displayed on the screen.

From what I have said above we can claim that when we use a multipurpose 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, for a potential attacker there are two opportunities:

- affect the presentation,
- manipulate the signing procedure.

This paper highlights that there are a lot of security problems of the digital signature usage. It will be demonstrated using some samples.

Introduction

The tram drivers in Budapest often warn the passengers: “Attention! There are pickpockets in the tram, take care of your properties!” Who would question the rightfulness of the driver’s warning? Every public message warning of attacks has two effects: on the one hand the people hold their bags tighter and put their papers in their inner pockets—it is just natural for law-abiding people. On the other hand, the message heels the attention of the potential pickpockets for the good opportunity that should be exploited now or other times. 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 and they should do their best to limit the number of these gaps. If somebody gets on the tram, they too would like to be aware of the dangers.

The aim of this paper is to examine the security of the computers relating to the digital signature and to explore the potential points of attack. These issues are closely related to the general security problems of the computers. The first part of the article covers the theoretical background of the operation of the electronic signature. The following chapters deal with the security problems of using a personal computer for providing and checking digital signatures and the analysis of the security issues of forwarding digital signatures.

1. Theoretical bases

To understand the security problems it is essential to overview the mathematical theoretical bases, which are to provide the security of the digital signatures.

1.1. Public Key algorithms

The basic idea of the public key methods *(Ralph Merkle, 1974)* is that the keys used for encoding (enciphering) and decoding (deciphering) need not necessarily be the same.

The public key algorithms are similar to a padlock that has two keys—one for opening it and another for closing it. The two keys are closely linked together and they are called a *'keypair'*. The key that closes the padlock (encodes the message) is called *'public key'*, and the one that opens the padlock (deciphers the message) is called *'cipher key'*. If the public key is made known then anybody can send us a ciphered message. Of course, to prevent the unauthorised parties from having access to the ciphered message the cipher key must be kept in secret. Formally, the encoding and the decoding can be expressed as

$$M=C_e(m) \text{ and}$$

$$m=D_d(M)$$

where m is the original message, M is the encoded message, C_e is the encoding algorithm using the public key e, and D_d is the decoding algorithm using the cipher key d.

- - - - - - - - - - - - - - - - -

Insert Figure 1 here

- - - - - - - - - - - - - - - -

If the roles of the keys can be swapped over, that is

$$M=C_d(m) \text{ and}$$

$$m=D_e(M),$$

then message M can be decoded with public key e, therefore message M carries the information the cipher key of which public key was used for ciphering i.e. validating it.

- - - - - - - - - - - - - - - - -

Insert Figure 2 here

- - - - - - - - - - - - - - - - -

The encoding procedure can be applied two times: for validating with our own cipher key and for ciphering with the public key of the receiver. Formally:

$$M=C_{e2}(C_{d1}(m)) \text{ and}$$

$$m=D_{e1}(D_{d2}(M)),$$

where *d1* and *d2* are the cipher keys of the two parties and *e1* and *e2* are the public keys of the two parties. Thus the public key algorithms provide solution to the problems of both validation and ciphering.

1.2. Digital signatures

The algorithm of the digital signature uses the algorithm of the public key encoding described in 1.1. This method is described in Figure 3. The first step is that the document to be signed appears on the computer of the sender; from the binary code series of the document the fingerprint peculiar to the document is prepared. This can be carried out with the help of the Hash algorithms. This fingerprint is then ciphered with the cipher part of the keys 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 and the digital signature rendered to it. The receiver receives the document and the digital signature and does the following: with the help of the same Hash algorithm he prepares the fingerprint rendered to the document. Also, from the digital signature, he prepares the fingerprint rendered to the digital signature by using the sender's public key. 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.

- - - - - - - - - - - - - - - - - -

Insert Figure 3 here

- - - - - - - - - - - - - - - - -

2. Traditional signature – electronic signature

When we sign a document on paper we rely on our eyes and it depends on our mental ability whether we can make sense of what we can see. Our eyes will give evidence to the fact that the signature is put only onto the document that we intend to sign (Figure 4.).

- - - - - - - - - - - - - - - -

Insert Figure 4 here

- - - - - - - - - - - - - - - -

When we prepare an electronic signature we must believe our eyes and we must make sense of it. Also, we must believe that the information displayed on the screen corresponds to a bit series stored in the memory or the mass storage, which has exactly the same sense as we interpret it. We must believe that the unit constructing the signature (e.g. an outer card reader connected on a serial line) provides only that bit series with the electronic signature whose correspondence is displayed on the screen. (Figure 5.)

- - - - - - - - - - - - - - - -

Insert Figure 5 here

- - - - - - - - - - - - - - - -

From what I have said above we can claim that when we use a multipurpose 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, for a potential attacker there are two opportunities:

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

2.1. Affecting the presentation

We ought to expect the document to be signed to contain all the information to interpret and present it. If, for the interpretation, information from another source is required then the presented image of the document can be affected. Such typical information is the image of the characters. Word and certain PDF documents do not contain the fonts required to present the image of a document. Thus, by changing the fonts the image of the document will be different in a new environment. Unfortunately, the ASCII text files are not different either. Despite the fact that there are no fonts here we must know the image of the characters for the presentation. And 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 NOT relating to the operation system. Under the terminals of Linux and UNIX systems exists the notion of fonts too and a StarOffice document does not contain the images of the letters either. To ensure the correspondence between the document and its presented image it is indispensable that the document **in itself** contains the binary images of the characters.

The question is what possibilities an attacker has to exploit the gap in the security system:

1. If the attacker can have access to another computer he can change the image of the letters in any of the fonts. These applications are freely accessible on the Internet.
2. He can change the letters with a small program of his own too.
3. He can send this program even in e-mail. For this there are tremendous amounts of viruses sent by e-mail today.

We can claim now that a malicious attacker can easily—especially if his partner does not know much about security in information technology—enter a program into his lay partner's computer, which then ensures that the signer will see something different from what he intends to sign. He can also eradicate himself entirely from the layman's computer following the signing, e.g. at a definite time. After that the lay user would try to prove his truthfulness in vain; the electronic signature is an approved evidence in the courts of many countries…

2.2. Manipulating the signing procedure

If we are fully aware of what we intend to sign — or at least we believe so — we can provide the document with our electronic signature. In order to do this we need a *signature-making device*. This device contains software as well as hardware elements. When we make up our minds to sign a document this device ensures that every condition is fulfilled 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.

A typical possibility for attack could be the following method: a small program, which is entered into the computer this way or the other watches an interactive activity that the user must carry out after satisfying every condition for the signature—e.g. he has entered the chip-card into the reader. The program senses what information the user program sends to sign for the card reader. The program sends this to the reader and waits for the response but it does not forward it to the user program but sends another bit series for the reader to sign. When this has happened, the program then sends back the signed answer to the user program. All this happens so quickly that the user does not notice anything. This 'small program'—like the majority of e-mail viruses—can even send the signed bit series back to the attacker with its own SMTP routine.

3. Using documents with digital signature

The advantage of the digital signature is that the two signers of a common declaration (e.g. a contract) need not meet. It is enough to exchange the electronically signed declarations (electronic documents) through messages. 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 this by ciphering the messages.

3.1. Forwarding on the Internet

The electronically signed document must be sent to the receiving party. We can do this through data media or by mail. In any of the cases the solution is not less comfortable than in the case of the traditionally signed paper document. The only significant difference is that forwarding through data media we can send or carry the information ciphered. With paper documents this cannot be done.

A natural way of forwarding a document is sending it through the Internet. Sending a message on the Internet is just as safe as sending information on a postcard, therefore it is essential to cipher the document.

- - - - - - - - - - - - - - - -

Insert Figure 6 here

- - - - - - - - - - - - - - - -

3.2. Forwarding through firewall

Today every business or institute has internal information infrastructure or inner network. It is also inevitable to build a firewall at the meeting point of the internal network and the Internet. The firewall must watch the traffic between the inner network and the Internet and by influencing it tries to protect the internal network from the dangers coming from the Internet. A well-configured firewall system must have packet filtering devices and a content filtering possibilities (e.g. virus protection) too.

Let us assume that the two managers intend to exchange their electronically written documents on the Internet. The most natural way to do it is to send the signed message through e-mail. It is essential for both of them to keep the contents of the document in secret even in the internal network. Therefore they cipher their messages, which can be easily made with the PKI technology (Figure 7.).

- - - - - - - - - - - - - - - - -

Insert Figure 7 here

- - - - - - - - - - - - - - - - -

But 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 the documents through the contents of which they cannot check. But in this way the ciphered and signed documents will never get through to the other party.
2. The firewall is set to let through the ciphered messages without supervision. Then the two managers can exchange the signed and ciphered messages. But this ‘security relief’ is just enough for an attacker to enter through the firewall an attacking program, which is ciphered with the manager’s public key (Figure 8.).

- - - - - - - - - - - - - - - - -

Insert Figure 8 here

- - - - - - - - - - - - - - - - -

4. Suggestions

Knowing the above described security problems we can claim that the use of the digital signature is not perfectly safe. If a single or limited purpose target machine—a bank ATM or mobile phone—is at our disposal then we can use the achievement of the digital era entirely safely. If we assume that the signature is made on a computer that is used for other purposes as well, 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 basic shortages of the legal regulations in many countries is that they do not formulate unambiguously the circle of data that can be signed electronically. The regulation ought to define 'text' and 'letter'. Which are the electronic forms that can be regarded as 'text communicated with letters'? Is a scanned A/4 page saved in a binary picture form 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.

A further demand is that regulations should be disposed about the forwarding of the documents 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 a lot more easily carry out both authentications than separately.

If possible, I find it necessary to inform the users about the potential sources of danger. This could be one by the providers of authentication because they know the devices used for digital signatures thus they ought to provide the guidelines about the secure use. Also, the users ought to be trained about the security precautions and the protection.

The users—private individuals, business enterprises or public institutions—are interested in the secure operation of their systems. The security of the machines used as computers as well as signature-making devices is closely related to the overall security of the computer. Making the computer more secure—with a firewall or virus protection or security regulations—the making of the digital signature becomes more secure too. There is no solution to the security of the digital signature that could be detached from the overall security of the computer.

5. Summary

The fact that four times as much money is being spent on the security of the computers as three years ago proves that we are facing more and more sources of danger, which ought to be handled by the computer users with greater care.

The electronic signature—rendering it to the document—raises a number of security problems when we use a computer for making signatures. The reason is that there is no operation system,—probably there cannot be any—which could provide sufficient security for making digital signatures at the moment. The users must obtain a **security culture**, which can help to prevent the potential problems and, if there has been trouble, to reconstruct the system.

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
Official Journal of the European Communities, 19.1.2000
http://www.ict.etsi.org/

[2] Community framework for electronic signatures
http://europa.eu.int/scadplus/leg/en/lvb/l24118.htm

[3] Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 1999
http://www.ietf.org/html.charters/pkix-charter.html

[4] Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 1999
http://www.ietf.org/html.charters/pkix-charter.html

[5] Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
RFC, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 1999
http://www.ietf.org/html.charters/pkix-charter.html

[6] Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)
Internet Draft, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 2000
http://www.ietf.org/html.charters/pkix-charter.html

[7] Simple Certificate Validation Protocol (SCVP)
Internet Draft, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 2000
http://www.ietf.org/html.charters/pkix-charter.html

[8] Alternative Certificate Formats for PKIX-CMP
Internet Draft, Internet Engineering Task Force (IETF) Public-Key Infrastructure (X.509) (pkix) Working Group, 2000
http://www.ietf.org/html.charters/pkix-charter.html

[9] Public-Key Cryptography Standards
RSA Laboratories
http://www.rsasecurity.com/

[10] Recommendation X.509 (03/00) - Information technology - Open Systems Interconnection
The directory: Public-key and attribute certificate frameworks
ITU Telecommunication Standardization Sectuion (ITU-T)
http://www.itu.int/itudoc/itu-t/rec/x/x500up/x509.html

[11] Information and Communications Technologies Standards Board (ICTSB)
http://www.ict.etsi.org/

[12] European Electronic Signature Standardization Initiative (EESSI)
http://www.ict.etsi.org/eessi/EESSI-homepage.htm

Figure 1

Encoding and decoding with public key algorithm

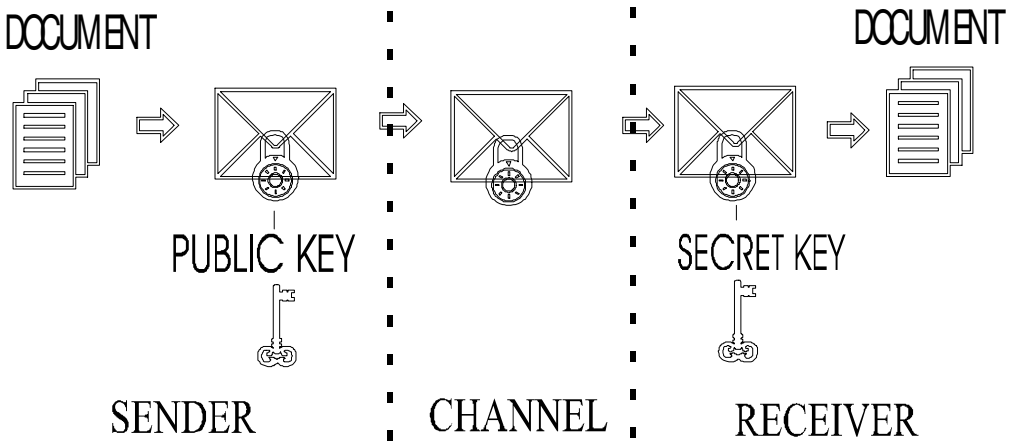

Figure 2

Validation with public key algorithm

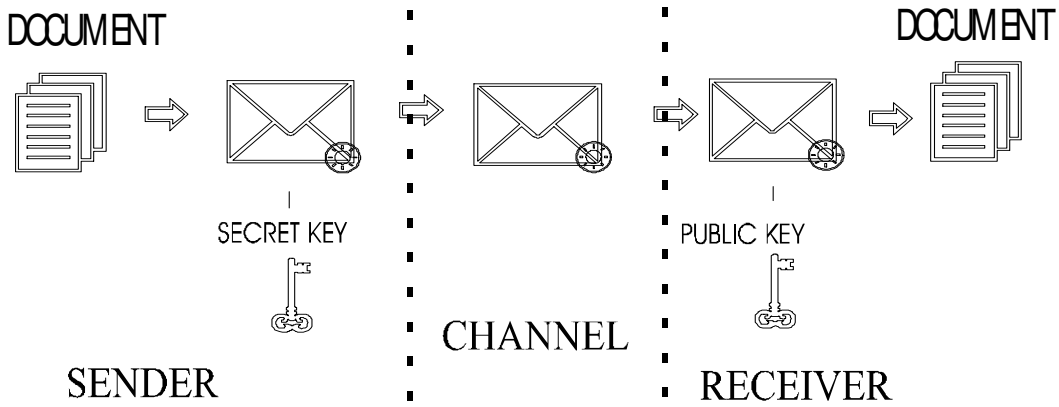

Figure 3

The operation of the digital signature

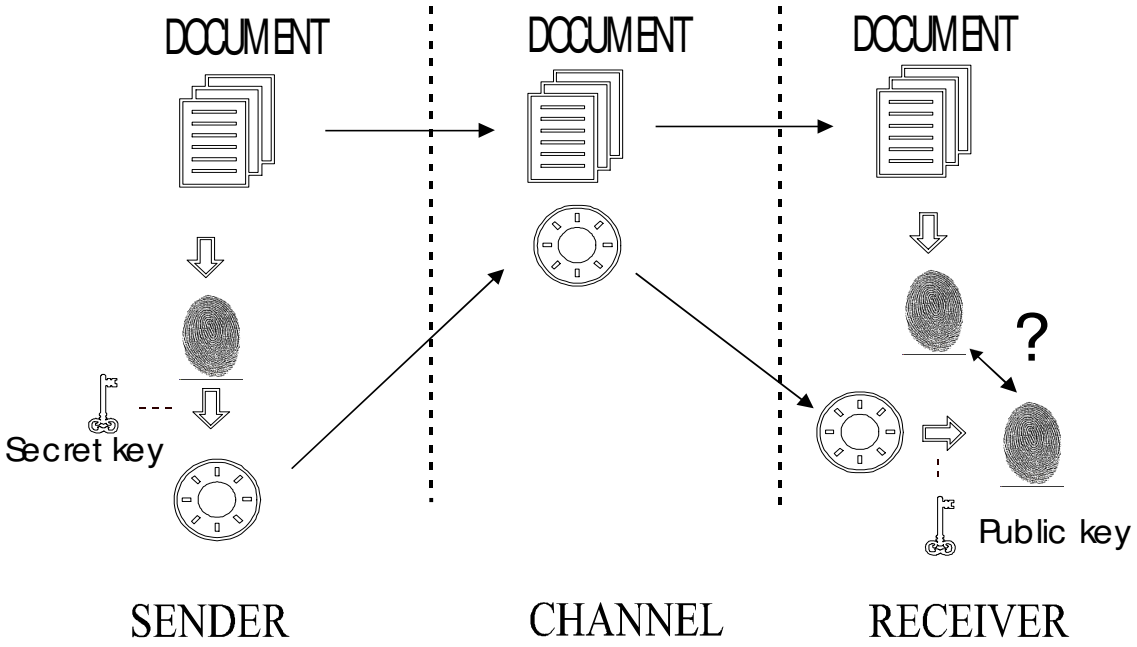

Figure 4

Traditional signature

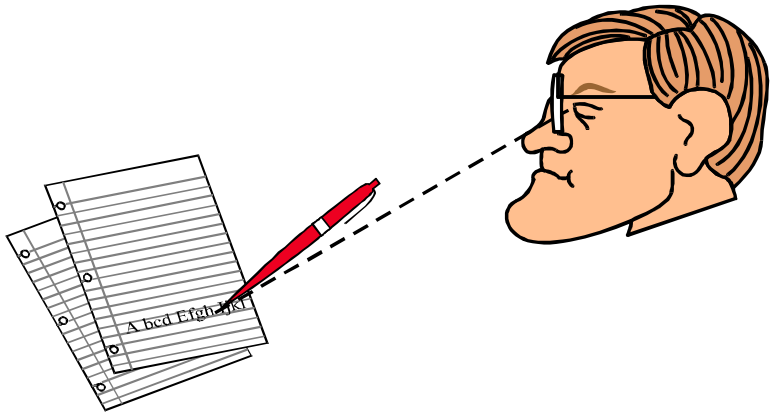

Figure 5

Electronic signature

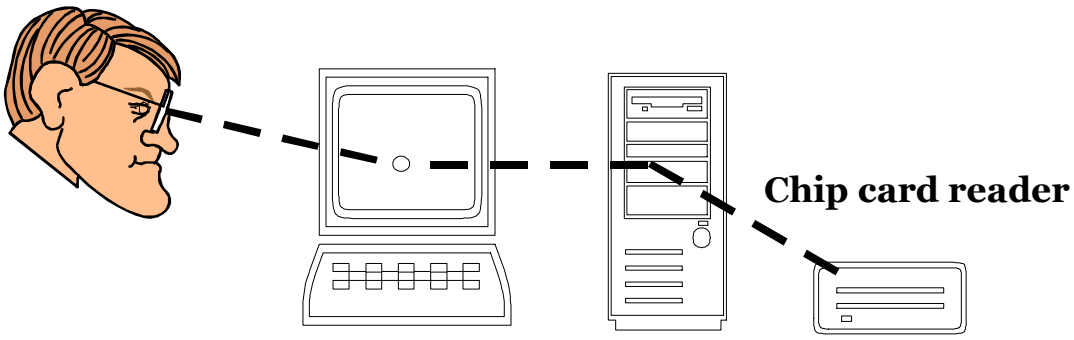

Figure 6

Forwarding on the Internet

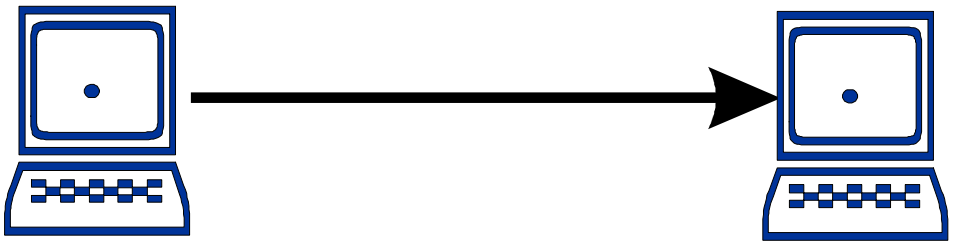

Figure 7

Forwarding through firewall

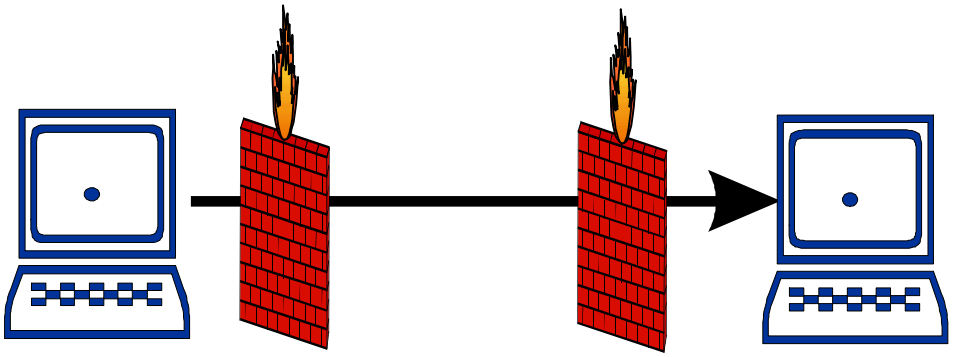

Figure 8

Opportunity to attack through the firewall