Department of Technology, Mathematics and Computer Science

DEGREE PROJECT
2004:E002

Internet banks login - a study of security solutions

Ibrahim Abdullahi
Dariusz Malolepszy

HÖGSKOLAN
TROLLHÄTTAN • UDDEVALLA

DEGREE PROJECT

Examination work

University of Trollhättan – Uddevalla
Institution of Information and Mathematics

Internet banks login – A study of security solutions

Ibrahim Abdullahi
Dariusz Malolepszy

Examiner:
Stanislav Belenki **Institution of Information and Mathematics**

Adviser:
Stanislav Belenki **Institution of Information and Mathematics**

Trollhättan, 2004

DEGREE PROJECT

Internet banks login - a study of security solutions

Ibrahim Abdullahi
Dariusz Malolepszy

Abstract

In this study we examined and studied the structures that secure the security systems such as PKI and SSL. We compared several security systems that are used to secure logons in internet banks and systems which are used for identifying through the Internet both software based and hardware based. We compared how strong or weak the security systems they offer are. An experiment was carried out showing how to compromise one of these security systems which we perceived to be weak. We mentioned as well other ways of compromising the security of these systems. Finally we gave suggestions of how to improve their security.

Keywords: PKI, SSL, Trojan, Logins, Computer Security, BankID, Electronic ID card.

Publisher:	University of Trollhättan/Uddevalla, Department of Technology, Mathematics and Computer Science, Box 957, S-461 29 Trollhättan, SWEDEN Phone: + 46 520 47 50 00 Fax: + 46 520 47 50 99 Web: www.htu.se
Examiner:	Stanislav Belenki
Advisor:	Stanislav Belenki, Samantha Jenkins
Subject:	Internet banks login - a study of security solutions
Language:	English
Number:	2004:E000
Date:	May 17, 2004
Keywords	PKI, SSL, Trojan, Logins, BankID, Electronic ID card. Computer Security

Preface

We successfully completed our work thanks to our lecturers Stanislav Belenki who guided us all along and gave us valuable advice. Thanks as well to Samantha Jenkins in supporting and helping us while writing our work. The school librarians were of great help in making available all the books we were in need of.

List of symbols

BankID is a service that offers secure electronic identification and signature on the Internet, which is now legally binding in the EU (European Union). The service has been developed by a number of large banks for use by members of the public, authorities, companies and other organisations. [28]

E-legitimation – the same as above but issued by Posten [32]

Internet bank – Service provided by banks. It make possible for customers to make bank transactions through Internet.

Key logger – programme that records or intercepts every stroke of the keyboard and can save it in a text file. It is often used by hackers to steal passwords

Virus - A computer virus is a program that replicates itself; it copies itself and infects systems. The virus can attach itself or a copy of itself to a file including e-mail files. When an infected file is opened the imbedded virus in the file is activated. The virus can increase in number on its own accord. But to infect some other computer it has to be transferred with an e-mail file, a floppy disk or some other portable medium.[4]

Worms – Is a program that can spread automatically. A worm is not a “virus” because it can reproduce itself and automatically move from one computer to another, for example through the addresses that appear in the receivers address book. One of the most well known is a worm called I LOVE YOU.[4]

Trojan Horses – These are programmes that appear to be useful or entertaining programmes such as games but in real sense is a security threat such as creating a whole in the system making it possible for a hacker to compromise the security of the system. Trojans don’t increase in number on their own accord; they are mainly spread through e-mail attachments or download from the Internet [4]

Contents

1 Introduction

The number of Internet users is increasing in number [1]. The United Nations claims that 592 million people world wide have access to the Internet in the year 2002. This will increase by 20% per annum. Banks and other service oriented companies are trying to give their customers convenient services which are comfortable and will save time for the customers and spare these banks and service providing companies any extra costs.

Services which were accomplished or carried out by the customer at the bank premises are today done in a totally different way, the customer doesn't need to leave home to transfer from one account to another or pay their bills. When using these bank services a person can confirm his or her identity through the Internet. To use all these services all you need is a computer with an Internet connection and a way to identify and authenticate oneself. The customers trust these services to be safe and secure, because they put their trust in the banks or the organisations that offer the services. Consequently as the number of Internet bank users swells and its projected by the end of the year to be 5, 2 millions. [2], so does the security risks and the trials to access confidential information illegally. According to a survey carried out by Symantec which is one of the leading Internet security companies around the world eight out of ten Internet users have experienced an unauthorised attack knowing or unknowingly. The greatest security risks come from Trojan attacks which record passwords and steal other vital personal information from the computer [3]. Trojans are actually programs which camouflage themselves to be useful while they are actually being destructive. They can appear to be screen savers, computer games or other useful programmes. They don't increase in number on their own accord and they are mostly spread through e-mails or by downloading them from the net. [4]

One might wonder if the companies that offer these services are aware of the risks that customers face. According to BankID which is an electronic based identity card produced in cooperation of some of the biggest banks within Sweden, over one hundred thousand customers have downloaded the BankID in order to make use of website services that require electronic identification and signatures.[5] We will study if these services they offer to the customers are safe.

According to the state office concerned with computer usage, about 50% of Swedish homes will be making use of the Internet to contact the authorities.[6], Its estimated within two years there will be one million software based electronic IDs in use [7] So this means there are a lot of people who believe in the security of these services that is offered by these banks. A major point of our work is to check if the security systems of logins are actually as safe as they are portrayed to be, through the study of the building blocks of these security systems and carrying out experiments which will actually check practically how safe these systems are during logins and the different security risks that a customer of some of these Internet banks can face. A greater detail of how the work will be carried out is explained in Method.

The major parts of the work will be carried out in order of:

- In section 5 we will discuss extensively Public Key Infrastructure (PKI) which is a cornerstone of electronics security. Its composed of among others among others encryption, decryption, certificates and hoe they are made and maintained.
- In section 6 we made a detailed description of Secure Socket Layer (SSL) mainly used to secure communication over the Internet
- In section 7 we mentioned IPSec which provides security at network layer, hence creating a secure communication from end to end at network layer.
- In section 8 it's about authentication and Identification and the components used for that purpose, such as Active cards, Biometrics and Password generators.
- In section 9 we mention the different logins such as Smart cards, Soft certificates and cards with one time use codes and banks such as Föreningssparbanken, Nordea, SEB and Handelsbanken.
- In section 10 we mentioned Electronic Identification, which is BankID this is an electronic ID.
- In section 11 is about the experiment, how we planned and how we carried out.
- In section 12 we mentioned other ways of compromising the system under attack other than the way we used in our experiment.
- In section 13 we discussed our work and gave some suggestions to improvement of security.
- In section 14 it's about the conclusion of our work, and we gave a suggestion in a further area of study.

2 Aim

We will analyse different security mechanisms offered by banks to secure logins to Internet banks and other applications which are put in place in order to verify the customer's identity. Through theoretical studies and experiments we will examine if they hold the security that they are suppose to offer.

3 Limitations

Since security in Internet banks is a very wide topic we will concentrate on the security mechanisms used for authentications during logins. How secure are these mechanisms and what are the systems being offered? We will be mentioning notably Handelsbanken and Föreningssparbanken but not limited to these two only. Some of the banks use advanced security systems like random key generating devices or employ the use of smart cards, there are however login systems that are simplified which use social security numbers and passwords. We will not highlight that much about the simplified login systems because this function limits the user, its possible for the customer to look and browse in its account but cannot make any changes.

4 Method

Our work is both theoretical and practical. We started by explaining and giving the reader the needed background knowledge in order to have a better understanding of what our work is all about. For that reason our literature study was a big part of our work. Later we wanted to explain the major components that make up these security systems and how they are built up. Since software based certificates introduce weak security in the login process as we will demonstrate soon in our experiment, we wrote about the risks and other alternative authentication methods available.

Further in our work we concentrated a bit more on techniques which we suspected had poor security and demonstrated the possibility of having an unauthorised access to someone's account or take over the electronic ID of a certain user. We chose to perform experiments because it is the best way to prove bad security. We have made an unauthorised access to the victim's computer by sending a Trojan to the unsuspecting customer or user by email, then copied his/her certificate which happens to be in the hard disk and at the same time accessed the password which was supposed to be protecting the certificate. We defined and described different security terms like encryption, digital signatures and PKI among others as it's demonstrated below.

5 Public key Infrastructure (PKI)

Due to the increased use of the Internet as a communication medium both by private individuals and business organisations so does the increase in the demand for a secure way of delivering sensitive information over the Internet. Banks, Hospitals, Industries and private individuals were in need of a system that could deliver their information in a way that is characterised by [8]:

- Guaranteeing the identification and the authentication of the identity of the persons involved in the transactions.
- Guaranteeing the confidentiality of the information
- Guaranteeing the integrity of the information
- Guaranteeing the non repudiation of the exchanged information.

The identification and authentication requirements makes it possible for the recipient of the information to be able to verify the sender of the information and with that make it possible to relate the information received to its sender. Guaranteeing of information's confidentiality denies any intruder to come over or disclose the information that was obtained illegally and make the information solely to be disclosed only to authorised persons. In order to guarantee the integrity of the information the recipient must be able to control the received information if it has been tampered with or not. The non repudiation characteristic makes it impossible for the sender of the information to deny its previous actions and the sending of the information and to ascertain the recipient the identity of the sender. In order to achieve all the above mentioned security an infrastructure was developed that was to fulfil them, hence the advent of PKI.[8]

PKI stands for public key infrastructure and it's made up of software, hardware, and encryption and decryption technologies in essence cryptography, certificate issuing authorities, public accessible repositories, rules and regulations that govern and manage

its overall policies. We will discuss them below and shed further light on the mentioned components that make up PKI.

The major components that play vital roles within PKI are:

- CA- Certificate Authorities
- public and private keys
- Digital signatures
- Certificate Revocation lists (CRLs)
- Encryption and decryption.
- Digital certificates [9]

We explain each of those components later because to understand their functions one must know what cryptography is and how encryption is made.

5.1 An introduction to Cryptography

Cryptography is the study of encrypting and decrypting to make data intelligible only to the intended recipient. Cryptography has therefore a long history of more than 2000 years. It's documented that the Roman emperor Caesar once used a cryptographic system which is known as the Caesar cipher.[10]For that reason the first sort of documented cryptography was based on a shift cipher. In shift cipher each letter is given a number and then the position of each letter is moved by a letter K, for example in the figure below:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 5.1

If K = 11 then A becomes L and L becomes W and Z becomes K.
The shift cipher was later replaced by a substitution cipher which is much more difficult to decrypt since it involves shift and at the same time substituting the shifted letter with another letter. Even though it's more difficult to decipher but it can still relatively easily be done so by utilising statistical cryptanalysis techniques. Cryptanalysis involves the study of deciphering encrypted information. The main element used here is statistical information which is used for the decryption of the information such as how many times a certain letter recurs within the text. With the advent of modern cryptography new ways were needed to make the decryption of information a lot harder if not impossible. The ideas of diffusion and confusion were to be used; these new methods were introduced by Claude Shannon.[10]

Diffusion – this is a technique that hardens the encrypted text's statistical composition to be used as a deduction material in order to arrive at the plain text. In other words there shall be no relation between the encrypted data and the plain text. [10]

Confusion – this is the technique that makes the encryption key to be fairly complex in relation to the statistical composition of the encrypted data. These two techniques are

hence achieved by the use of mathematically complex algorithms and with this system the birth of modern cryptography was a fact. The key size became even more important with the widespread use of Internet which makes it possible millions of computers to work together parallel in order to decipher a certain encrypted text. For example a key with 128 bits to break it will take a million super computers for almost 31,623, 153 years [10] hence the use of such long keys renders such attempts useless.

5.2 Encryption and decryption

Encryption is the alteration of data by the use of powerful mathematical algorithm into a data which is not intelligible to unauthorised persons. The level of this protection offered to the plain text is determined by the encryption algorithm used. The strength of this algorithm is decided by the key size, the bigger the size of the key used the harder and more secure is the encrypted data [11]. Decryption is the process of changing the unintelligible encrypted data back to plain text. Just as the encryption was carried out with an encryption algorithm so does the decryption process need a decryption algorithm in the form of a key. This key will hence undo the data that was previously encrypted to a plain text [12].

5.3 Symmetric and Asymmetric keys

Symmetric and Asymmetric keys - The study of encryption, decryption and authentication of data is known as cryptography. There are two major ways of encrypting data, in one of the methods it utilises symmetric cryptographic keys and the second one utilises asymmetric keys. In the symmetric cryptography which is known as symmetric-key cryptography utilises the same cryptographic key for both its encryption and decryption of data. Since it uses the same keys for its encryption and decryption this causes a major security risk. This shared private key must hence be exchanged securely over key exchange channel or use a key exchanging algorithm. This key exchanging algorithms use some shared values which the keys can be generated from. It can happen that this key exchanging secure channels and algorithms might not be available, this together with security risks involved makes another alternative to be sought.

Due to the short comings of the symmetric cryptography, asymmetric cryptography known as public-key cryptography was to be used which tackles with the insecurity related to the usage of symmetric keys. In the asymmetric cryptography the keys that are used for encryption are different from those used for decryption. The key which is used for encrypting the message before it’s sent is known as the public key and need not be kept secretly there fore freeing us the security worries attached in the exchange of symmetric keys. However the key that is to be decrypted with must be kept secretly.[9] If the two encryption systems are compared with the exception of security risks involved in the exchange of the keys, the symmetric cryptography is far faster than the public-key cryptosystems since the public key cryptography uses larger integers in its calculations.

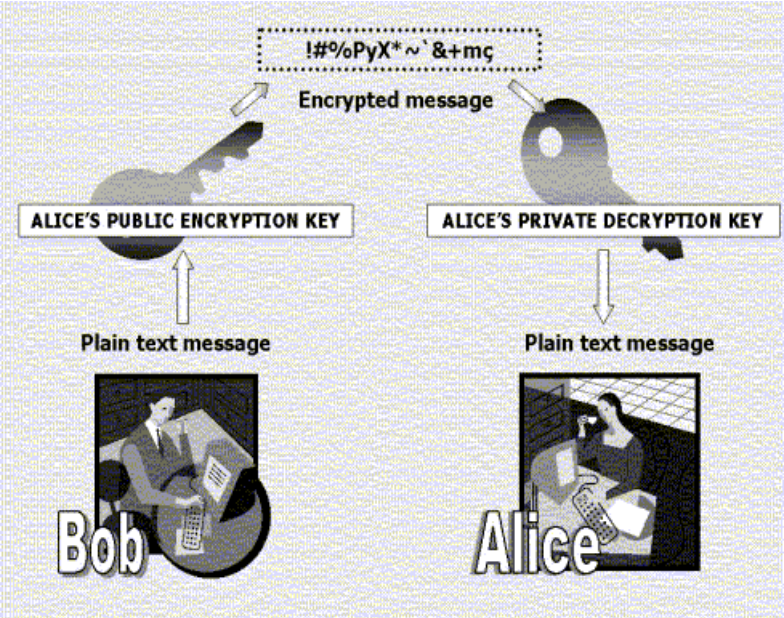


Figure 5.2

In order to keep the message sent confidential the sender must use the public key of the recipient to encrypt the plain text before sending it to the recipient. Upon receiving the message, the recipient will have to use its own private key to decrypt the encrypted message back to plain text again [9].

5.4 Qualities of good encryption

The encrypted text shall be resistant to cryptanalysis that is the possibility of taking advantage of the poorly encrypted text in order to decrypt it back to plain text.
There shall be no relation between the two that is the plain text and the encrypted text.
The size of the block to be encrypted plays a vital role, this is because the bigger the block to be encrypted the more difficult it is to decrypt it and apply cryptanalysis, since larger encrypted texts have a larger possible plaintext. [10]

5.5 CA - Certification Authority

Certification authority is a cornerstone to the PKI infrastructure. In order to oversee the development and the secure distribution of public keys a third trusted authority is needed in this case CA (certification Authority). The CA will verify and ascertain the ownership of public key to a certain entity or organisation by means of issuing a digital certificate. The CA can be recognised by its name and its public key; it fulfils four functions for the PKI infrastructure, that is:

1. It issues certificates to appropriate entities or organisations.
2. Maintains a revocation list and information about the validity of the certificates.
3. It publishes a list of the valid certificates and its up to date revocation lists.
4 keep an archive containing information about outdated certificates [8]**.**

By issuing certificates the CA is certifying that the entity or organisation named in the certificate has actually in possession of the private key that can be decrypted with what

ever information that has been encrypted with the public key. In other words that entity or organisation owns a pair of corresponding private and public key.

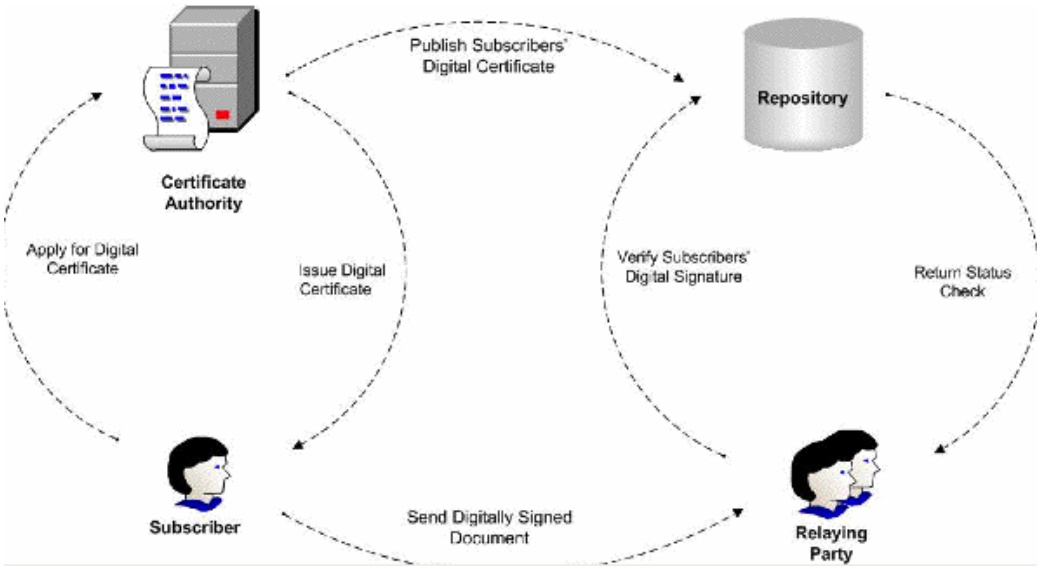


Figure 5.3 the figure above shows the central role that CA plays within the PKI infrastructure.

Any other information that might appear on the certificate is as well certified and belongs to the bearer of that particular certificate. This information might be in the form of contact information like address. The issuer of the certificate must add its name on the certificate and then sign it with its private key. A digital certificate binds a public key to an individual, organisation or an entity it validates or certifies the person or the organisation claiming to own the public key. The digital certificate has characteristics which are quite similar to those of a passport and they are almost impossible to be tampered or forged. Among other information they usually contain:

- Legality period – that is how long the digital certificate will be binding.
- The distinguished name of the owner
- The owners public key
- The distinguished name of the issuing authority
- The serial number of the certificate

The digital signature of the issuing authority in order to verify that the contents of the digital certificates are genuine [9] In order to be sure of the validity and authenticity of the digital certificate the CA must sign it digitally. So the certificate remains valid as long as it bears the valid signature of the CA, the owner's signature and that both the CA's certificate and the owner's certificate neither of them should appear in a revocation list. A revocation list is a list that contains all the non valid certificates.

5.6 Hierarchy arrangement of CA

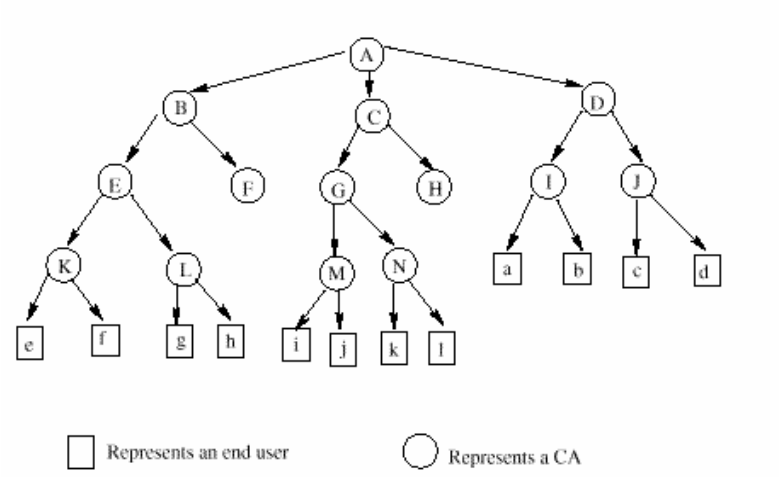


Figure 5.4

CA is arranged in hierarchy with the root hierarchy at the top, so before any other certificate is made this need be established because it will be used to certify the rest. Since its root it will have to certify itself. The security of the root CA must be taken seriously because the validity of the rest of the CA's depends on it. If the security of the root CA is compromised then the rest of the CA's plus the root CA must be revoked and a new Root CA will have to be created only then can the rest of the CA's issued afresh[10]

In the figure above the root CA, A issues CA certificates to B, C and D. Those in turn issue CA certificates to the ones below them and those in turn will finally issue to the end users. If any of the users wants to validate if its certificate is valid or not then, it should start with its own CA and then go upwards along the path of issue until the root CA. For example if g wants to validate its CA then it will have to go all the way to the root CA and see if the CA's along the root are valid too, in this case L, E and B. The system will have to go through the hierarchy step by step until the root CA in order to validate the certificate in question. [10]

If the closest CA is validated then the system will go upwards and test the next CA in line. If any of these fails then the system will fail and terminate there hence rejecting the certificate otherwise it will keep on testing until it reaches the root CA and hence accepting the certificate. In order to strengthen the security of the root CA the length of its private key must be at least 2048 bits and the hash function used for its signature generation must be at least 160 bit message digest. [10] The root CA security is strengthened because if its compromised it will have a domino effect hence forcing the rest of the CA's which happen to be under it to be as well revoked. So the higher the hierarchy the greater the security paid to it.

5.7 Format of Digital certificates

There are two main formats used that is either X.509 or PGP format. With PKI it mainly uses the X.509 format. It highlights the rules governing distribution of public keys through digital certificates which are signed by the issuing CA. This X.509 version supports as well the X.500 directory. The directory is an electronic database, the entities containing in this directory are arranged in a tree structure known as the directory information tree (DIT).[10]

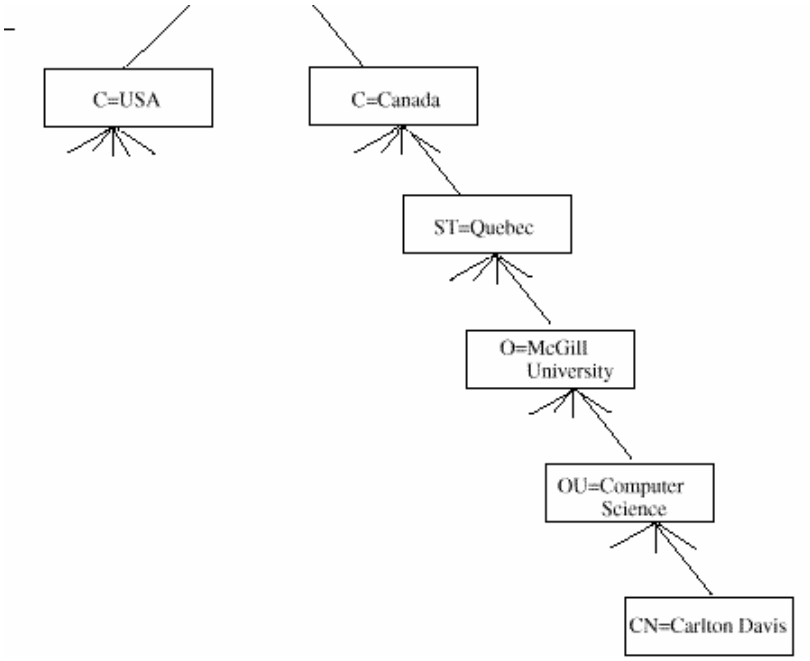


Figure 5.5

All the nodes within this hierarchical tree like structure are given a relative distinguished name (RDN). Entries made within the directory are recognised by their distinguished names (DN). The DN is globally unique and it's made by taking the RDN and attaching it with its corresponding previous entries.

For example the Dn for Carlton Davis will be [10]:

CN – Carlton Davis
OU – Computer Science
O – Mc Gill University
ST – Quebec
C – Canada

The X.509 determines the information that will finally appear on the certificate, for example the serial number, version, issuer, how long it should be valid and Extensions. The use of extensions introduces new way of associating further attributes to users or public keys. These associations can be biometric information like finger prints. It might not store the actual biometric but it might contain a URL pointing to the position where the biometric information have been stored. In short the X.509 format decides the

attributes that are to appear on a digital certificate and that in turn will help in the authentication of the entries into the electronic directory that is the X.500. [10]

5.8 Certificate revocation list (CRL)

Another vital function of CA is the issuing of revocation list; this is a list depicting the revoked digital certificates made available in a public accessible repository place. The revoked certificates are time stamped and easily recognisable by means of checking for their serial numbers, and once the serial number appears in the revoked list sent in by the issuer of the certificate then it's no longer valid and any transactions carried with that certificate will not hold. Certificates will have to be revoked in case the information contents appearing on the certificate have changed for example if the owner of the certificate changes his name.

It will have to be revoked in other cases for example the lose of private keys or if the person responsible for the private keys leaves the company then to be on the safe side that certificate will have to be revoked as well. Within the revocation list framework, the revocations of certificates are archived in such away that, any dated signature that appears on them is considered to be valid as along as that date does not extend beyond its validity period.

Certification Authorities issue these revocation lists on regular intervals depending on the policies of the CA. They might be issued on hourly, daily or weekly basis to a public repository place. But a serious breach of security can occur, for example the CA can issue the revocation list on weekly basis, let us say for example it usually issues them on Thursdays. In case it issues one on Friday then for that revocation list to be effective it will have to wait until next Thursday hence making it possible to be using in the meantime revoked certificates, thus jeopardising the legality of any transactions carried out with a revoked certificate. To counter this security breach a new mechanism was put in place that is the OCSP (Online Certificate Status Protocol). This makes it possible to determine the revocation status of the certificates on time.[10]

To use this system the certificate handling system will have to install OCSP client application. Upon the need to check the status of a certificate the application will send a request to a responder querying whether the certificate is valid or not. In the meantime the certificate will be suspended until a response is received from the responder.

The query sent contains among other:

- The distinguished name of the sender of the request[10]
- A request list in turn consisting of hash algorithms identifying the identity of the issuer of the certificate.
- Version number – specifying the protocol of the OCSP that the requestor is using.

5.9 Digital signature

A digital signature binds data with a private key in such away that it confirms the sender's identity and protects the integrity of the data and it can not be repudiated. It's much easier to forge conventional signatures that we use while digital signatures are impossible to forge unless you have the private key as well. Since digital signatures are impossible to forge so it can not be repudiated unless the owner of the private key can proof that the security of the private key was compromised. Any data from the sender is hence binding. This is so because digital signatures are signed with private keys and they are validated with public keys, there are systems like digital certificates that bind the identity of the owner to the private and public keys hence making it even harder to deny the origin of the data by the sender.[9]

Even though digital signatures are impossible to forge them but still several copies can be created from a single digital signature. For example you can create a document and sign it digitally and give your assistant to send the document, there is a risk that the assistant can make several copies of this document and it will hence be impossible to tell which was original and which is a copy, to solve this problem digital signatures will have to be time stamped this can be accomplished by using NTP, that is Network Time protocol applications. [9]

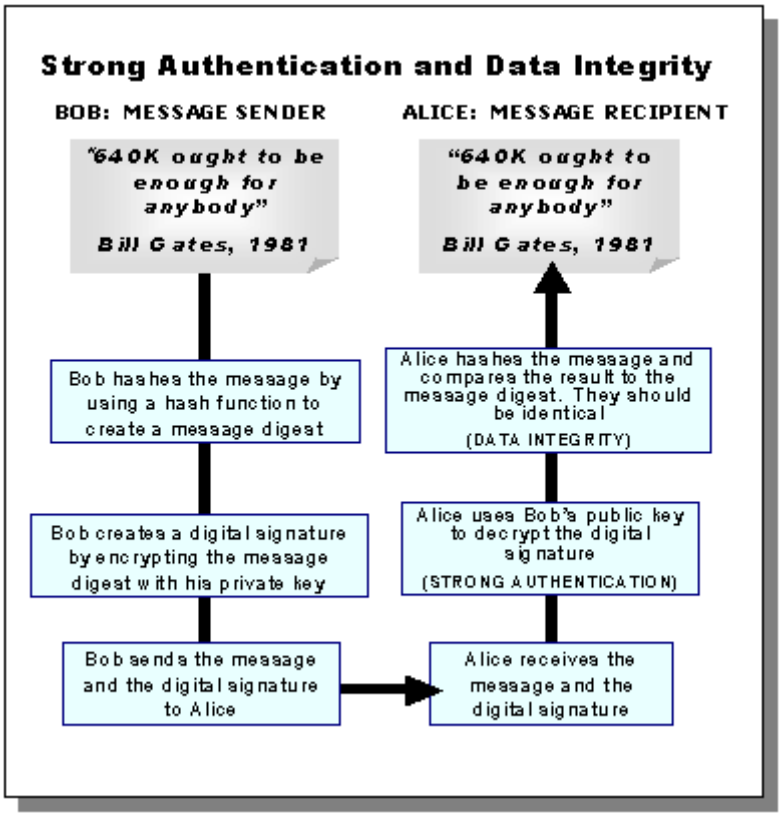


Figure 5.6

The above diagram clearly states the steps that a message goes through if it's to be digitally signed.

5.10 Digitally signing a message

This process of signing a message with an algorithm makes use of both the private and public keys. Let us say organisation A wants to communicate with organisation B in such a way that it's impossible to repudiate or tamper with that message. Organisation A will have to create a message digest or a summery of the message it intends to send. This is done by using a hash function for example SHA-1, RIPEMD-160, or Tiger, the hush function is an algorithm that creates a message digest of a fixed length from the original message. The message is initially digested with a function then the fixed digest is encrypted with the private key of organisation A, thereby producing a digitally signed message and then it's sent to organisation B.[10]

Upon receiving the digitally signed message, organisation B will decrypt the message with the public key of organisation A showing the message digest and under this decryption process it gives further information on which hash function was used in order to create the digest. Since the message could only be decrypted by the public key of organisation A then one can be sure the message originated from them. To check for the integrity of the received message organisation B runs its own hush function on the digest after it has been decrypted. If the message was not tampered with then it produces the same digest as that of organisation A and there be giving an identical answer, if it doesn't then the recipient can be sure of the message was tampered with and its integrity can not be guaranteed.[9]

Attention must be paid, unlike the widely used public encryption algorithms where the public keys are used for encryptions and the private keys for decryption, in this case its almost the other way round, the private keys are used for encryptions and the public keys for decryptions. [10] All these sophisticated computations of encrypting, decrypting and verifying are carried out smoothly beyond the scene without involving the users, but only giving them the end results, that is decrypting the message and checking its integrity.

5.11 Importance of PKI in Internet applications

Secure applications that make use of public keys or digital certificates in order to offer security need to use digital certificates. Digital certificates are used in the distribution of these keys and for authentication of their owners. Digital certificates for that matter are a fundamental part of PKI. Applications that make use of it are among others SSL and Secure Electronic Transactions (SET). Secure Electronic Transactions is an application that secures card payments, with the use of digital certificate it becomes possible to create a secure environment where the card holder, the banks and merchants can interact. [13]

Since our work is based on the security of bank logins it's paramount that we highlight SSL protocol which is a protocol that plays a vital role by securing the site as soon as you log on during and after logon. We will discuss it further below.

6 Secure Socket Layer

Security over the web has become paramount as transactions over the net have increased. The security should be extended not to securing the site itself but communication between the sites and between the servers and clients must be strengthened. That is the information of the communicating partners must not be disclosed to unauthorised person or be tampered with. The challenge is, information passes over networks which the communicating partners have little control over. For this matter in order to secure communications over these networks encryptions decryptions and authentications are needed and that is what Secure Socket Layer (SSL) offers. [13]

SSL functions between the application layer and the TCP/IP layer hence making the transfer of secured information smoothly. It's composed of two protocols that is the SSL handshake protocol and the SSL record protocol. These protocols will help in the negotiation between the communicating partners on the level of encryption, authentication and what sort of data format will be used in the course of the communication [14]. Secure socket layer is a protocol that offers security mechanisms in the form of encryptions, decryptions and authentications. It has two main functions for it to deliver this security which are:

1- Authentication – This is done in the beginning of the communication.
2- Encryption and decryption – This is done under the on going communication.

6.1 SSL connection

SSL shares many protocols as that of TCP/IP protocols and its connections are quite identical to it. The connections are always made by calling a socket interface and it's in the form of listen, accept and connect. The server's main function in the connection phase is to listen for any connections on certain address and port, if the connection is accepted once then the rest of the future request connections are done always through the same address and port. Once the clients connection has been accepted and connected a handshake is necessary at this level. If it were plain TCP/IP connection then data transfer would have followed immediately but since the data that is to flow between the communicating partners is encrypted hence the need for a handshake, what the handshake does is that it negotiates the encryption parameters. At this level a major role is played by the server and its certificate which is used for authentication purposes [15].

6.2 SSL Handshake

The main purpose of the handshake is that it negotiates the encryption algorithm and the keys to be used for the communication between the client and the server.
Data transfer within SSL is done with a symmetric key which is, the same key is used for both encryption and decryption between the client and the server. Symmetric keys are used because they are much faster than the asymmetric so this means that there will be a shared key between both communicating parties and this key must be kept secret. In order to keep it secret the handshake process itself must be encrypted as well.

In the initial stage of the handshake the server has to send its certificate to the client and in this way the client receives the public key of the server which it uses for encryption before sending the data to the server. Once the server receives the data it uses its private key to decrypt the information. The same time the server can encrypt message sent to

the client with its private key and the client decrypts with the public key of the server that it received initially together with the certificate. Through the use of the public and private keys of the server it's possible to encrypt the whole handshake process and hence keep the private key secret. The private key will be used for the encryption of bulk data thereby keeping the data secure throughout the communication period.
The client must authenticate the server and must be certain that it's getting connected to the right server if the handshake process is to be successful. It's not a must for the server to authenticate all those connecting to it, but it can be made a requirement too if that need be necessary, so that during the handshake both sides will have to authenticate and identify to each other [15].

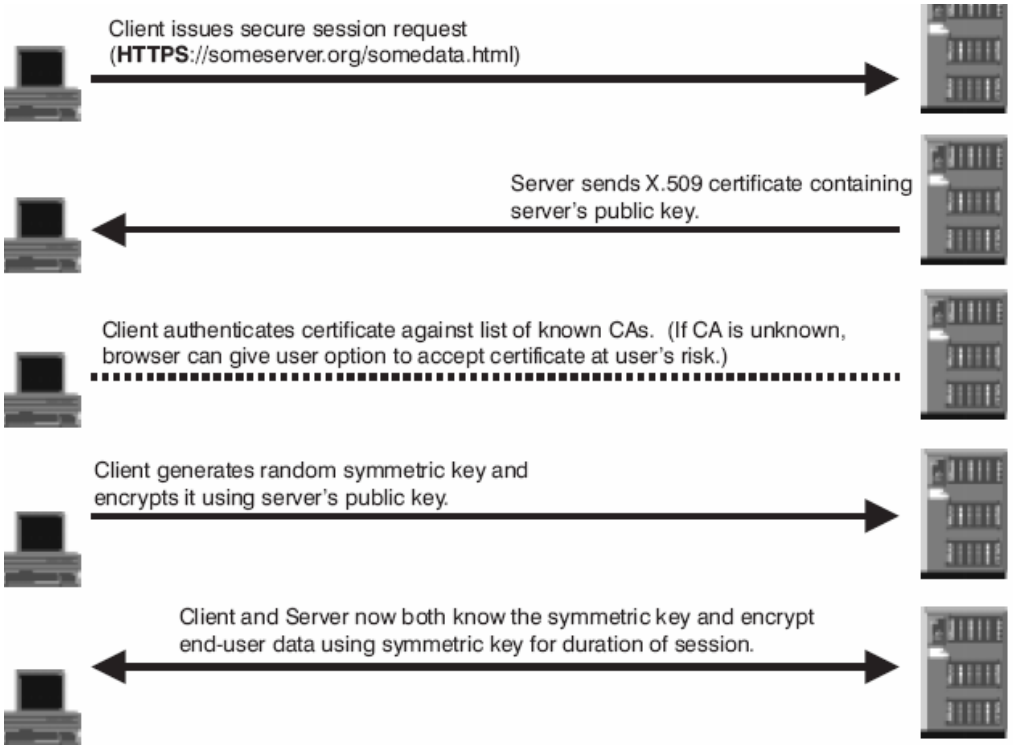


Figure 6.1 The above figure shows the process of SSL establishing a connection.

6.3 Server Authentication

During server authentication some important processes must be gone through for the client to be sure of the identity of the server. The client must be sure of the validity of the server certificate so it will check its issue and expiry date. It must verify as well if the certificate was issued by an authorised Certificate authority or by any CA which is recognised by the client. The client will finally verify if the domain name appearing on the certificate is the same as the domain name of the server [16].

6.4 Client Authentication

Even though it's not a must in the handshake procedure for the client to authenticate itself to the server, but still it might be required just so by the server to make sure it's the actual client that initiated the session which is still in contact with the server.

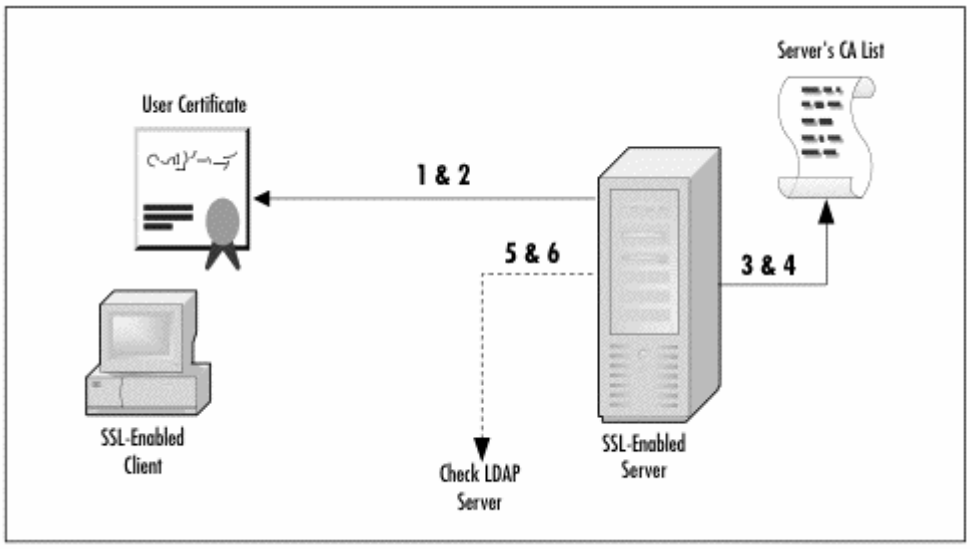


Figure 6.2 authenticating the client.

The server will verify the identity of the client by:

- The server will have to validate the digital signature of the user by using the public key that appears with the user's certificate.
- The server will have to verify if the certificate of the user is still valid by checking its issue time and expiry date.
- The server will as well a sure that the client's certificate was issued by a trusted CA that is known to the server.
- The server will have to check if the certificate of the client has a public key that can validate the user's digital signature.
- The server can further verify the user by checking for other attributes of the user in a Lightweight Directory Access Protocol (LDAP).
- The server can check if the client has enough access rights for the resources it has requested.[16]

The initial Connection is made to be so stringent in order to avoid "The man in the middle attack" so as not to intercept and impersonate to be either the client or the server. Man-in-the-Middle Attack is a way in which an intruder intercepts the message flow between the client and the server in the initial key exchange and instead substitutes the requested public key with his/her own public key, this happens without being detected by both the client and the server. The intruder will appear to the server to be the genuine client and to the client to be the genuine server.

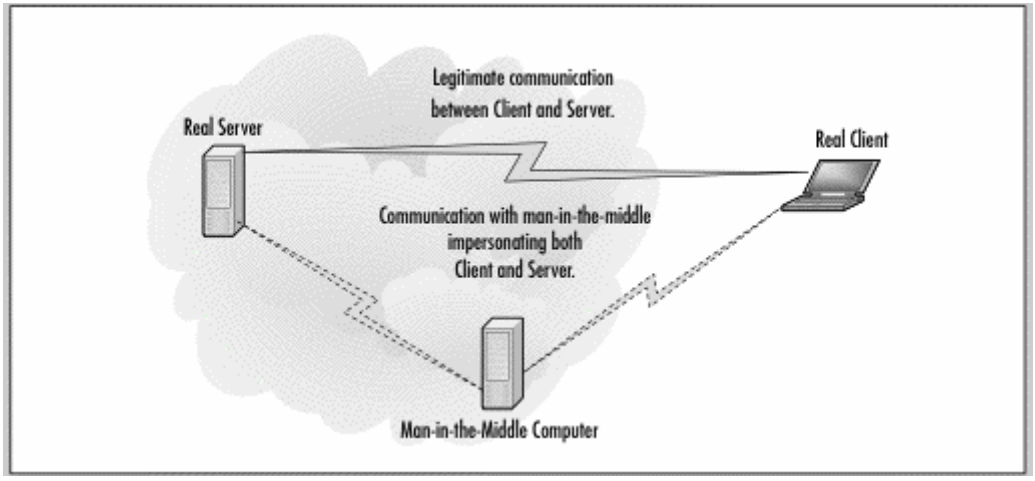


Figure 6.3

The above figure represents a typical case of man-in-the-middle attack where it acts to be an intermediary to the communicating partners of the server and the client

Through encryption, decryption and authentication and by the use of certificates between the server and the client makes it impossible for the man-in-the-middle to do its attack. The authentication process is composed of several criteria which are stated in the certificates and these criteria can only be fulfilled by the two legitimate communicating partners. These criteria can be in the form of ensuring that the name of the server and the name appearing on the certificate match or the certificate were issued by a known authorised certificate authority. If any of the criteria is not fulfilled once the client or the server makes a request and the response happens to be incorrect then the connection is terminated. [16]

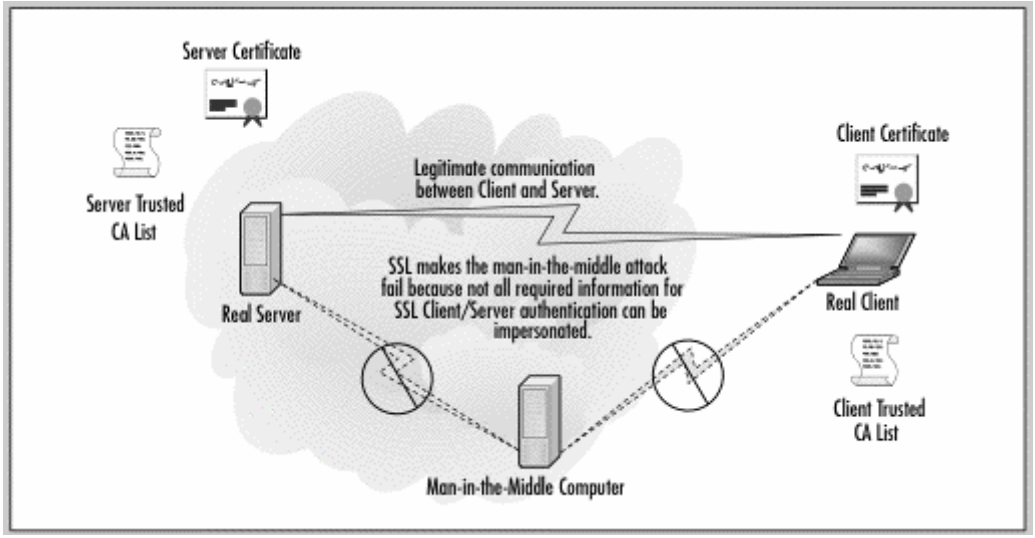


Figure 6.4

The figure above shows the man-in-the-middle attack being stopped due to lack of fulfilling all the criteria. .

SSL offers good security but its handshake requires extensive computations since it uses keys with long integers, because it uses public keys and public keys have long integers and hence the intense computations. The handshake involves too eight message

exchanges between the clients and the servers and these messages can be sent through the wide networks of internet further making the delays even worse. How often the SSL handshakes are used is dependent on the sort of transaction the customers are doing on the website. In some transactions it might happen the customer browses the net without the need of making use of the secured sites. The larger part of the transaction takes place in non secured area but once its time to pay, the customer goes to a secured site for payment and the handshake is only activated when its time to pay.[16]

There are however situations where security is intensive for example in the case of online banking. Even browsing within the site is considered to be sensitive like checking your balance so in such situations the handshake takes place only once, which is when you are logging in to the site of the online bank. Any communication between the client and the server is encrypted; hence it's this large size of data that will require a lot more resources for a lot of data need to be transferred constantly between the client and the server as the customer browses freely [17]. However there are other forms of securing information between the client and the server even though not at the application layer but at the network layer such as using IPSec.

7 IPSec

IP security protocol is a framework which creates a secure communication over the Internet. It guarantees confidentiality, Integrity and authentication of the data which is transferred across the net. IPSec provides encryption and authentication at network layer thereby securing the network from end to end. Therefore the applications as a whole are secured and there will be no need of securing each application on its own as the case would have been if SSL was used.

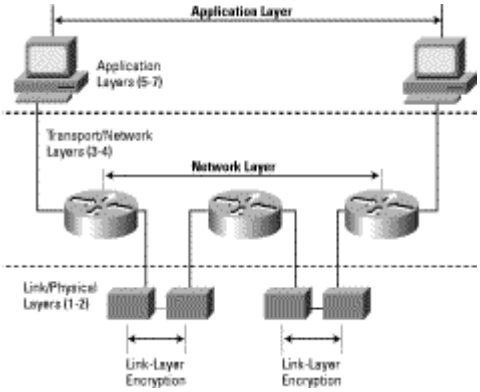


Figure 7.1 Encrypting messages at network layer by IPSec.

The encrypted packets are very much similar to the ordinary IP packets so they will be routed through the network without much change to the intermediate networks thus the implementation costs are reduced. IPSec provides security by adding new headers to the IP packets which are Authentication header (AH) and Encapsulation security payload (ESP). The authentication header provides integrity and authenticity while the ESP provides confidentiality, integrity and authenticity. These protocols can be used together or separately. The two communicating partners must establish a connection before using IPSec. This is done through the use of Internet Key Management Protocol (IKMP). During this process the communicating partners will authenticate to each other and create shared keys. It uses symmetric keys and these keys must be exchanged hence

creating some security risk. It uses too a lot of bandwidth during the set up of the initial communication and the agreeing of the algorithms and the symmetric keys to be used.[18] All these major components such as PKI, SSL and IPSec make up the structures which the security system is built upon. To make logins secure different methods are employed for authentication and identification which are essentially built upon these structures, among others smart cards, password generators or biometric based authentication systems.

8 Identification and authentication

A major part of security is to authenticate the person be it a worker or a customer if he or she is the right person or not. With authentication we mean to verify the identity of the person so that undesired people should not have access to the system. Another type of authentication is based on the authenticity of the message, which is the verification of the message if it has being tampered with since it was sent or not and if it's coming from the correct source. [19] the most used login is the traditional way of authenticating the user with a name and a password. The name is a claim to be a certain person and the password verifies that you are in fact the person you claim to be. Since the password is kept secret and it's only the user that knows it then that verifies the user. Thus a great importance is attached to the password because the whole security mechanism is built upon keeping the password secret once it's known by two or more the whole security structure that this system is built upon is jeopardised. [20] Factors used in authenticating the user are unique in order to verify and authenticate the user, because of that authentication is based on three principals [19]:

- Something you know for example a password
- Something you have for example a card
- Or something you are, for example finger prints.

In order to make it even more secure its possible to combine two or more of the above principals.

Something you know - The widely used challenge – response-system is based on this. The challenge is varied so are the responses which are returned to the system, and the response can never be reused. This system renders useless the intercepted passwords since the challenges and responses keep on changing.

Something you have principal – The idea behind this is that the user owns certain object for example an active card which is unique to him or her and it's used for authentication. A major problem with objects like this is that they can be lost or stolen and who ever finds might have access to the system. This cards can however be locked with a PIN code hence making them useless even if stolen or found by someone else.

Something you are - this is built upon a particular characteristic unique for every person for example fingerprints. It's the use of human body properties for authentication purposes. [20]

There are different technical solutions for the customers to authenticate themselves. Some of these techniques are used of Swedish banks and other companies that issue e-identity cards. These techniques are mostly based on PKI but differentiated of how they store the private keys; some store it in a file while others in a smart card. Below we

shall elaborate how these techniques function and which of these techniques are employed by the examined Banks.

8.1 Active cards

Active cards they are as well called smart cards, they resemble a credit card but with an electronic chip and memory. The chip contains RSA keys and certificates. [21] Properties of active cards are can be summarised in the following points:

- The keys never depart from the card hence a higher protection level for the keys.
- The card can not be copied which guarantees the security of the keys.
- The card can be blocked or disabled after several failed logins with a PIN code. [22]

Disadvantages of active cards are among others:

- It's costly to produce or make the cards.
- A card reading device must be installed.
- The PIN used for protecting the card is written in by using a keyboard this makes interception of the PIN code possible with programmes like Key loggers. [22]

8.2 Software based solutions

Soft ware based solutions contain the same security solutions as smart cards with the sole difference of storing the keys in a file, the card is replaced with a software programme.

Differences between smart cards and software based solutions:

- The private keys in software based systems are stored in files which give lower security than smart cards.
- The data file can be copied so it's not possible to disable access after several failed logins by the use of the PIN cards.
- Applications do not require any special devices as smart cards require card readers. This makes the software based solutions cheaper and easier to administer. [22]

8.3 Cards with one time use codes

To carry out any bank services in the Internet you issue one time use codes during log on. Some of the services offered through telephones or the Internet still need one time use codes. The one time use codes are issued in the form of paper cards. You scratch the paper cards in order to acquire the one time use codes only when necessary. Once a code is used it's not possible to reuse it again. Before you run out of cards you ought to order for a new supply and then the cards are sent through the post. To use the new codes on the card you need to activate them with a code from the old card codes. You can activate them through Internet or Telephone [23]. A major disadvantage with one time use cards are, there is nothing to protect the codes in case one loses the cards that the codes are printed on.

8.4 Password generators

There are different types of password generators, Asynchronous with or without a PIN code and synchronous with or without PIN code.

Asynchronous generators - In asynchronous generators the server generates a challenge which is fed to the generator and the generator then gives back a unique response. The generator is able to generate this response thanks to its encryption keys. The generating device can be protected with a PIN code so that it's protected in case it's stolen or gets lost. The asynchronous generators can have the possibility of reading challenge values without being fed from the keyboard, for example it can copy directly the values from the screen. The strength in this technique lies in the complexity of the algorithms being used. This system is not suitable in case where the serial numbers used can be guessed in advance like in post or bank codes [20].

Synchronous generators - In the case of synchronous generators there are no challenges rather both sides generate the same random numbers which is then compared. The generated random numbers are then sent to the authenticating unit. The randomly generated number can further be secured by including it with a PIN code. The strength in this synchronous system lies in the complexity of the algorithm that is to generate the random numbers and how long the authentication string will be valid, that is how long the whole process of authentication takes [20].

8.5 Biometrics

Biometrics is the technique of using biological properties in order to identify the person correctly. This are included for example finger prints, voice recognition and retina scan [24]. This security principal is based on using something you are, unlike passwords which are based on something you know. The most commonly used system in biometrics technology is that of sending the recorded data of a fingerprint by the client software to a database. The information sent by the client software is then compared to that already stored in the database and if they match the user is authenticated and allowed to carry transactions and if not access denied. This way of handling has though severe shortcomings, the biometric data can be stolen before it arrives to the server for authentication and reused by an unauthorised person. [25]

To use this technology more securely, instead of letting the biometric data travel through the network a system known as Match on Card (MOC) is employed. The login ID of the customer, the password and fingerprints are all stored in the chip which is attached on the smart card. To use this system the customer opens the webpage of its bank and inserts the smart card in a card reader, to complete the authentication process the user will have to place its finger on a scanner attached to the computer. The image fed in by the scanner is then compared to the image already in the card if they match then the card is unlocked setting the login process automatically with the use of the information stored in the card already. [25]

8.6 RFID – Radio Frequency Identification

This is mainly a solution for the future and it's still been studied even though limited uses are already available. Major disadvantages of smart cards are that they are expensive; it's assumed the user has a computer connected to the Internet with a card

reader. There is another solution that gives the same level of security and does not require a card reader. This solution is cards equipped with RFID.

RFID stands for Radio Frequency Identification. This is made in the form of a very small chip equipped with a small receiver. When the chip receives the right frequencies it generates enough energy which enables it to answer with pre programmed identification information. Mechanical card readers are not needed in this case. All communication goes through radio waves. The use of RFID was already standardised by year 2000 (ISO/IEC 15693-2) and it received a big boost from America's home land security act which invested in this technology greatly. The RFID technique functions on cartons, labels and on people as well.

The chip is so small it has been nicknamed the electronic dust. Hitachi has produced and it's marketing a µ- chip with area of 0, 16 mm, a width of 0, 15 mm and with a communication frequency of 2, 45 GHZ. When such a chip is equipped with an antenna it becomes a bit bigger, but still it's possible to produce an ampoule with the size that of a third of the tip of a matchstick. An ampoule like this can be inserted on user's upper arm and the frequencies from the ampoule can easily be read by a small scanner. This is not a science fiction but it's actually a service that is already applied. [26].

9 Different logins and Internet banks

We made a study of the Swedish banks which have a majority of the Internet bank customers and the type of identifications they use among the above mentioned technologies such as active cards and pass word generators. The diagram below taken from www.bankforeningen.se shows Internet bank customers in December 2003.

Figure 9.1

We choose four banks which have most Internet customers. Table below shows which technology those banks use to authenticate their users.

Logins to major Swedish banks	**Bank Name**			
	Föreningssparbanken	Nordea	SEB	Handlesbanken
Smart card		X		
Soft certificate				X
Cards with one time use codes.		X		
Digipass	X		X	

Table 1 Information obtained from their respective web sites

Initially we decided to concentrate on the biggest Swedish Internet banks such as Nordea and SEB banks, but on discovering the low security offered by software based certificates, that are certificates stored in file forms we decided as well to inform on which other banks use this technique. There are as well smaller banks that use software based certificates for logins, such as Ikanobanken, Sparbanken Finn and Sparbanken Gripen, these banks use software based BankIDs for logins in their Internet banks [27]

10 Electronic IDentification

A major modern tool employed in electronic identification is BankID. This is a software based solution which is installed in the PC as any other programme. Over hundred thousand e-Id cards have been issued to customers as a way of securing Internet services in the public sector. BankID is an infrastructure which can be utilised by any bank that is capable of guaranteeing the identity of their customers. Banks that are to use these services must as well use an Internet security solution which is according to the standards of BankID. These electronic identification cards make certain the identity of the user electronically and it was developed together by a number of large Swedish banks. In order for any bank to make use of BankID that bank must satisfy two conditions:

- The bank has to guarantee customer identity
- The bank must use a BankID approved security solution[28]

Any bank that is linked or cooperating with BankID producing companies such as Finansiell ID-Teknik BID AB can issue one to any of its customers. The bank as well can cooperate with other companies which will in turn allow those customers to utilise their services and hence use their BankIDs in identifying themselves. Some of the banks that are taking part in the formation and introduction of BankID use it as a security tool for their Internet banking services especially as an authentication tool during log ins. Finansiell ID-Teknik BID AB is one of the leading issuers of Bank-ID. It's being supported by Föreningssparbanken, Handelsbanken, Ikanobanken, Danske bank in Sweden, Länsförsäkring bank, Skandia bank, sparbankn Finn and Sparbank Gripen. These banks have a total of 2,5 million Internet bank customers. The government's prognoses are that 50% of Swedish homes will be using their PCs in contacting the authorities and a large portion of the population will be using their mobile phones hence making use of their BankIDs during authentication process.[29]

All the mentioned security systems among others smart cards, password generators and biometric systems offer security which we rely on during logins. We experiment on that.

11 Experiments

Through experiments we will try to see if the offered solutions fulfil the demands required for example authentication, confidentiality, integrity and non-repudiation. In this chapter we describe our steps through figures. It is rough description. A detailed description can be found in appendix E. The experiment is carried out according to the process that the intruder goes through from the start of the attack to its final point of withdrawing money from the victim's account. We are carrying out the experiment in the same manner. The picture below summarises the distinct steps of the experiment.

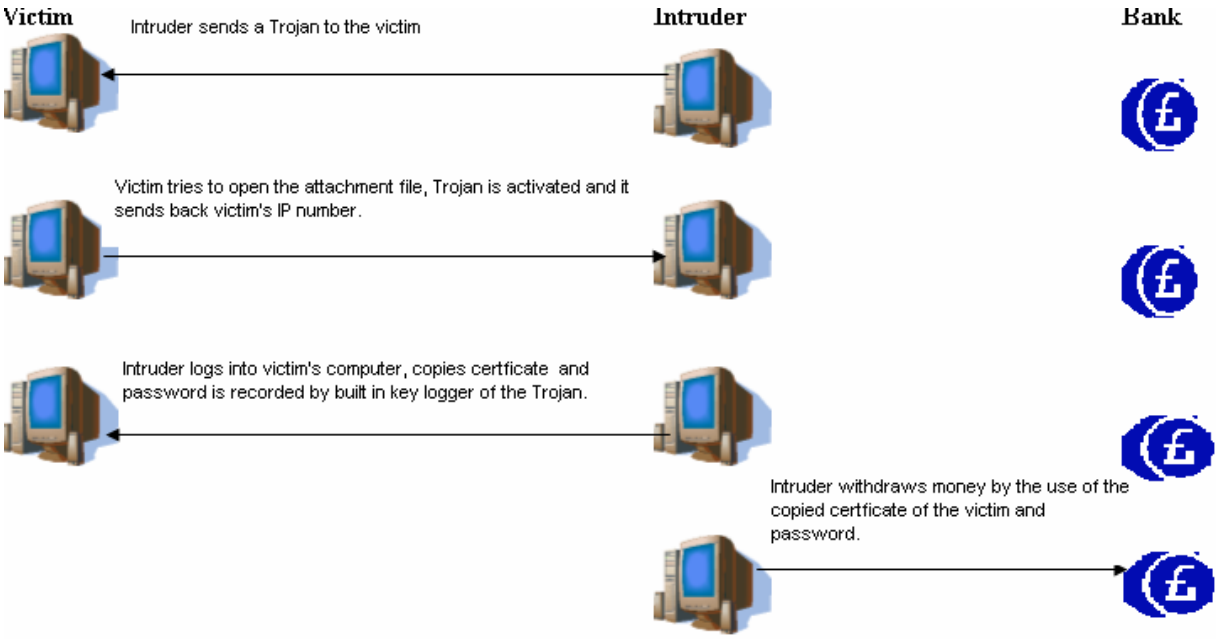


Fig 11.1 A general summary of the major steps which the Intruder will go through.

11.1 Planning the experiment

The computers we used in the experiments were all running on Windows XP Operating system (OS). We based our work on these OS because these are the most used OS today [int1], for that reason we will not write about Linux systems. The experiment that we have done was divided into two main parts, internal and external attacks.

Internal attack of software based certificates - First and foremost we looked at internal security that is when the intruder is at the same area or place as the victim for example sharing or living in the same apartment or alternatively the intruder has actual physical contact with the victim's computer or the computer which is under attack. We considered the most usual way of storing the certificate, which is storing it in the hard disk of the computer and this is the default procedure. This is the certificate which is to authenticate and verify the customers. When you are to install a copy of your certificate the installation guide from Handelsbanken says "when the certificate is made it should be stored in your computer"[30]. The same thing applies to the BankID service from Föreningssparbanken. Since it's about internal security we assumed that the intruder has physical contact to the computer where the certificate is stored. A good example of an internal attack can be a family or flatmates where several people share the same computer.

External attack of software based certificates - In the second part of the experiment we looked at external security, which is when the intruder is carrying out a remote attack and happens to be in a different physical place than the customer or the computer under attack and tries to get access to the computer through Internet. After accessing the victim's computer the intruder has to be able to copy the certificate to his own computer and must obtain the password of the certificate. Once we copy the victim's certificate and obtain it's password we shall use his/her certificate to get an unauthorised access to his/her bank account. We will try to make an unauthorised access to two bank services which use the same technique that is software based certificates which are Handelsbanken Internet login system and föreningenssparbank BankID.

We chose to study and investigate on these two banks due to their usage of software based certifications which we actually think have a low standard security. We will study on other alternatives to authenticate during logins and their level of security.
We planned to experiment with these two banks because we had access to their services, so we used our own accounts otherwise we would have been breaking the law.

11.2 Equipments

Equipments for Internal attack - The computer we experimented on was running windows XP with Norton Personal Firewall together with Symantec Antivirus and had a direct Internet broadband connection or modem based connections. The exact description of the system can be found at appendix A.

We installed a programme known as "Family key logger" on the customer's computer. A key logger is actually a free programme that records or intercepts every stroke of the keyboard in a text file. The anti virus programme never detected the programme, so it's actually not a virus and it can be put in a hidden mode where the victim never discovers if it's installed or not. We chose Family Key logger because it's quite easy to use and to

configure it. There are a lot of different versions of free Key loggers that can easily be downloaded from the Internet.

Equipment for external attack - On testing external security we used two computers both connected to the Internet. The exact descriptions of the systems are found in appendix B and C respectively. We planned to use a Trojan we chose one by the name CafeIni 1.1, because this Trojan was easy to use and to configure, it had as well all the necessary tools we needed for example Key logger and it has the ability of sending back an e-mail to the intruder with the current IP number in case the victim had a dynamic IP number. A description of all the functionalities of the programme is found in Appendix D.

11.3 Preparation for an unauthorized Intrusion

We started by downloading the necessary Trojan from the Internet in this case Caffeine. Fig 11.2 shows the steps taken. Once it's downloaded it had to be configured. We changed the name of the file to HolidayPhotos.exe so as to deceive the victim. We send an e-mail to the victim and attach it with the file HolidayPhotos.exe and send the mail finally to our victim.

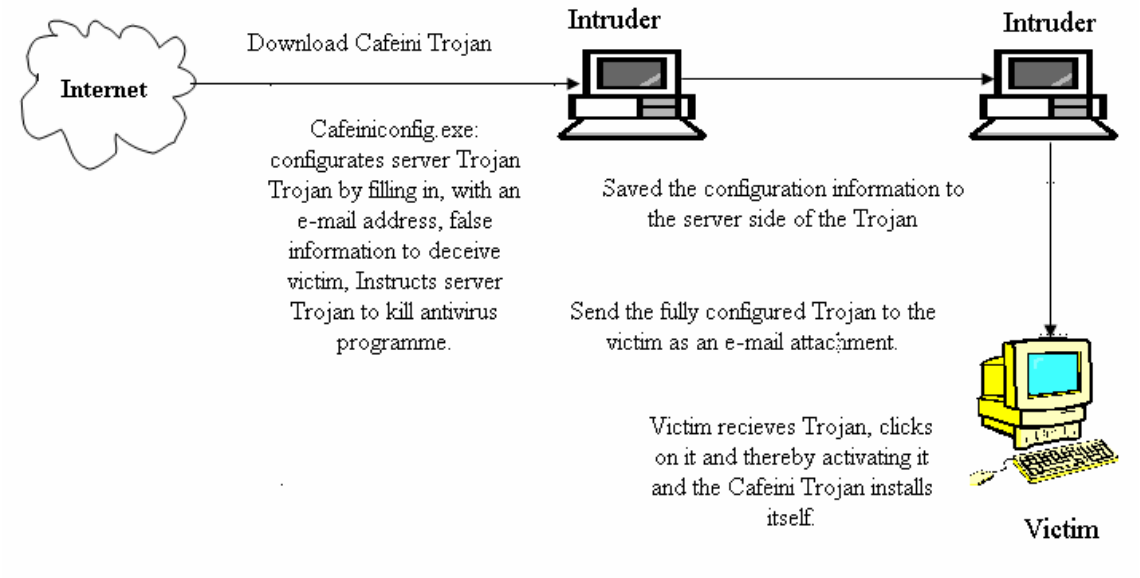


Figure 11.2 Downloading and sending Trojan**.**

Our victim opens his letter and decides to see the photos by clicking on the file expecting the self extracting file to show the photos. Instead he gets the message that "Zip file is damaged", deceiving him to believe that there is something wrong with the file. Without noticing the Caffeine server is installed in the victim's computer stealthily. Trojan sends email to address as we fed in during configuration process and tell us IP address of the victim, which we will use during our connection process. A letter like this will be sent every time the victim starts his/her computer, so that we don't lose track of the victim. We connect to our victim and can upload or download files and start programmes on his/her computer remotely. We activate key logger to get password to certificate in clear text. "Listening" for the password might take sometime depending on if the victim logs in to his bank or not. We browsed to found certificate and copied it to our computer. Figure below shows all steps and data flow.

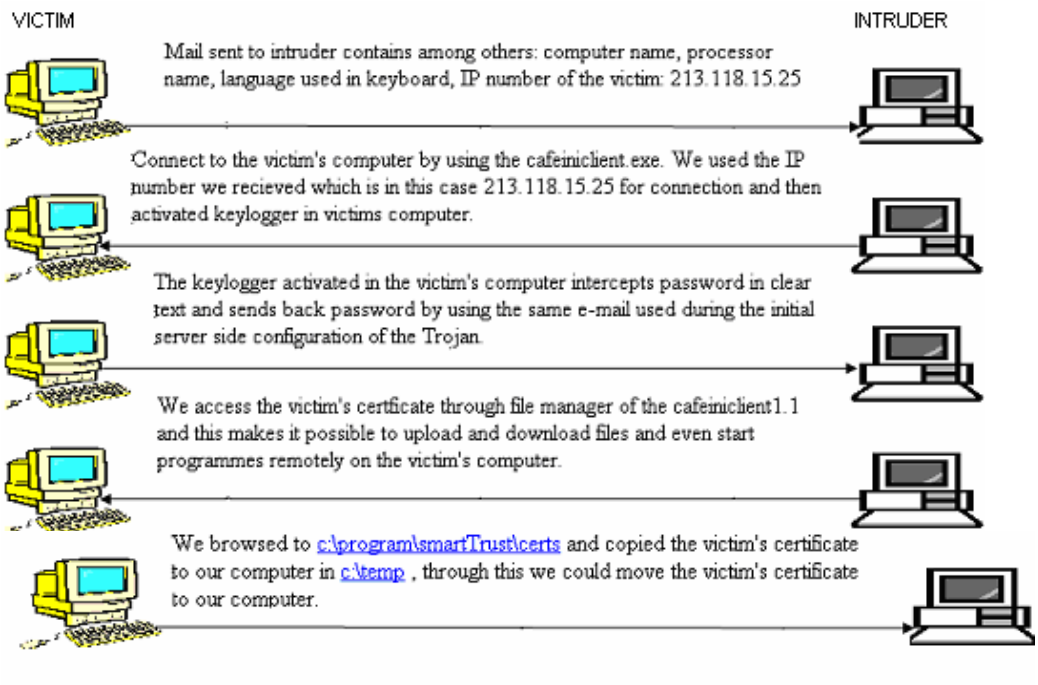


Figure 11.3

11.4 Connecting to the bank account

After succession with interception of the certificate and belonging to it password we could login to victims bank account and withdraw money from his or her account to any other account. Figure below shows taken steps.

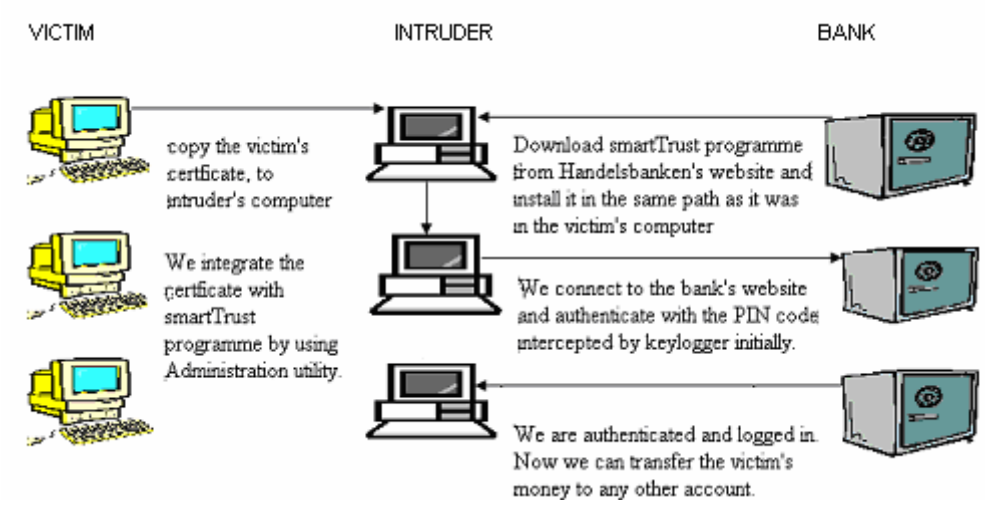


Figure 11.4

After we have succeeded in accessing the victim’s account, we decided further to check if it was possible to use the certificate without actually using any password. That is coming round the SmartTrust programme as a whole. According to SmartTrust manual if user wants to install a new certificate in SmartTrust program he must use a certificate mover tool. One of installation steps is to give password which protect certificate,

otherwise one can't continue. We managed to install certificate without using password. Figure below shows taken steps. For a detailed description go to Appendix E Part 5.

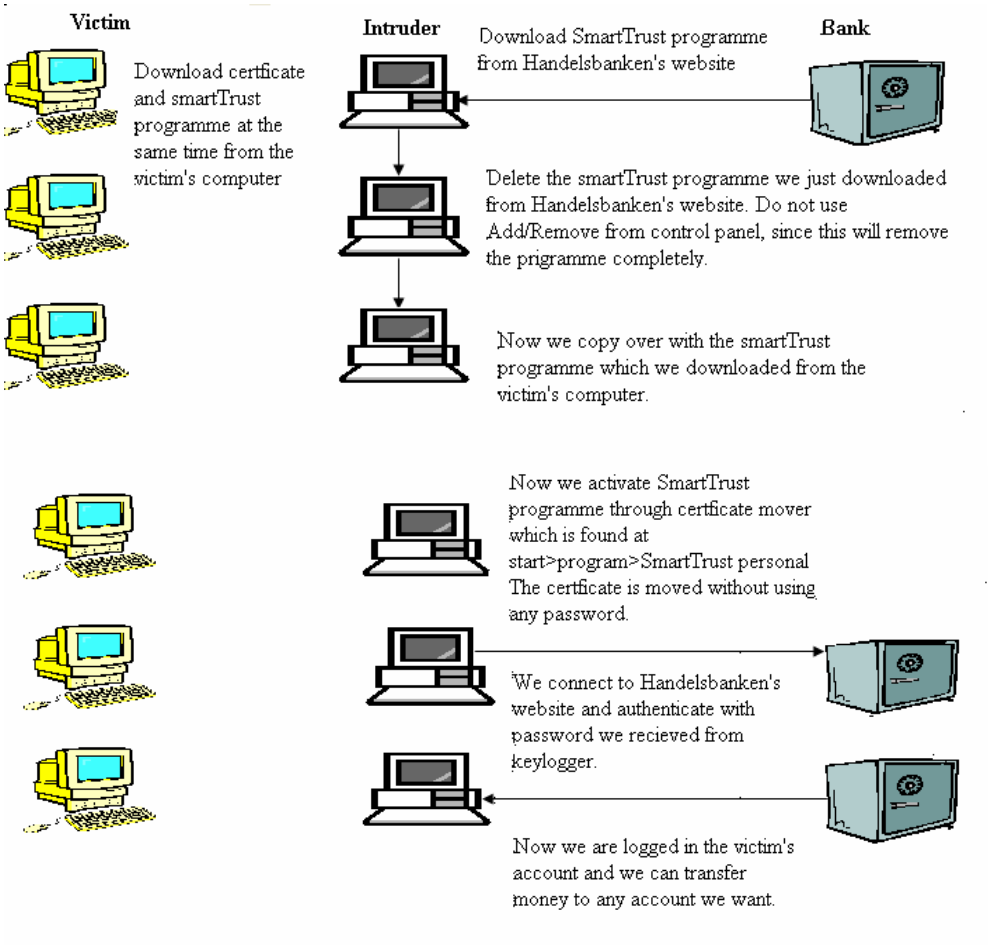


Figure 11.5

11.5 Hijacking of BankID

We have copied the BankID certificate and we have recorded its password in the same manner as the other certificate. We logged to the test site for BankID services. We test then ordering for 2 winter catalogues and 3 summers catalogues and continue by clicking OK, and then the order is approved and verified. The figure below shows the steps taken.

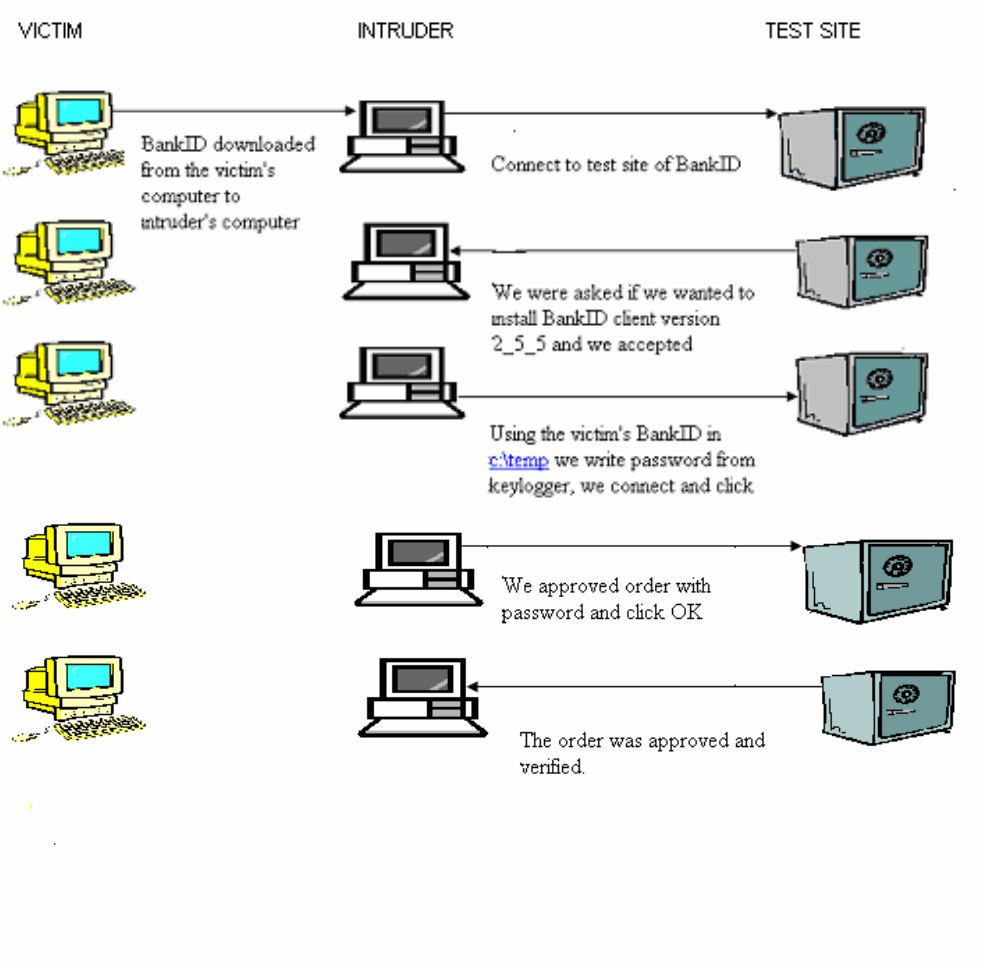


Figure 11.6

11.6 Internal attacks

Internal attack is much more easy then External attack, because intruder has direct contact with victim's computer so he doesn't need to copy certificate. Intruder must only install key logger on victim's computer and wait for password. Figure below shows taken steps.

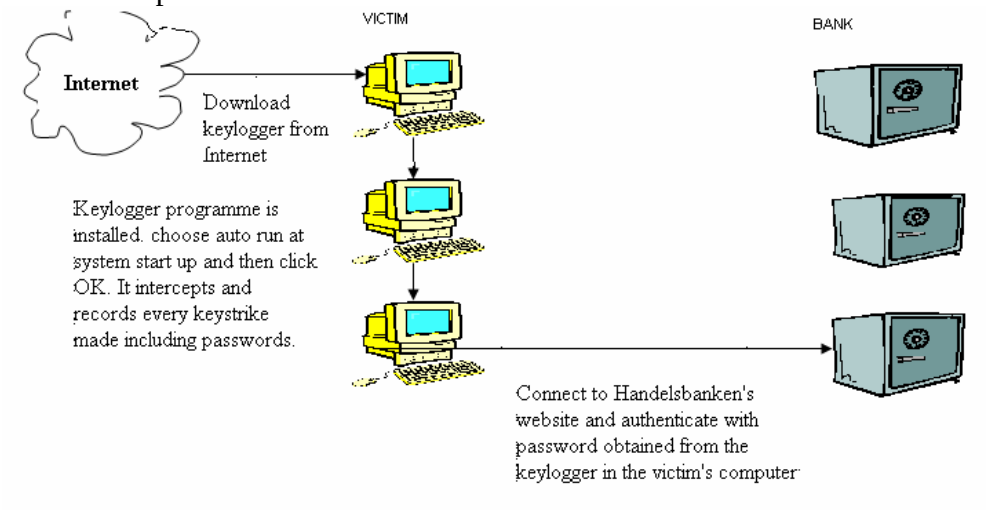


Figure 11.7

12 Alternative methods in compromising systems

The most commonly used way of compromising the security of the attacked systems is by means of attaching malicious tools such as Trojans or viruses into e-mails disguised as useful tools. There are however other ways of spreading these Trojans or other malicious codes. Some websites need only be visited and the active codes will down load themselves into your hard disk and interact with your other applications.[31]

For example the use of ActiveX controls which are in actual sense windows program that can easily be distributed from a webpage. These programmes are capable of carrying out almost anything a window programme can do, for example you can write and distribute Trojans and distribute them from a webpage while the user is completely oblivious to this. It's even possible to search for important information from the victim's hard disk and e-mail them to the owner of the malicious webpage [31]. When you visit a webpage containing an ActiveX codes, it will download itself automatically depending on the security level of your web browser.

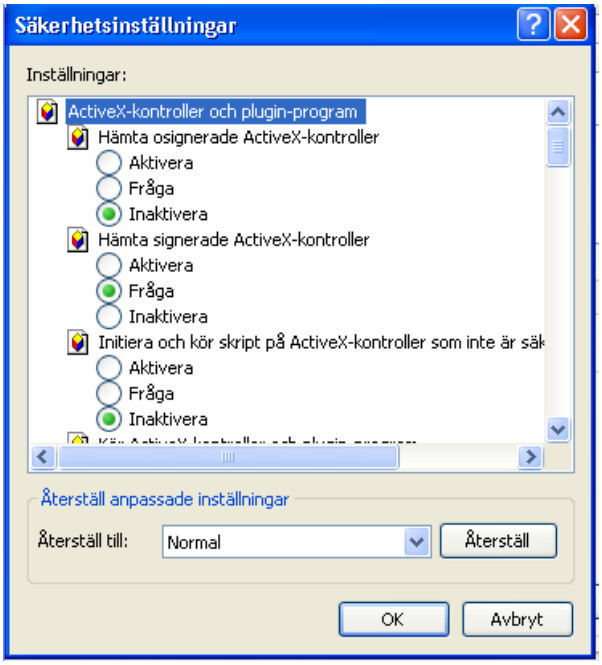


Figure 12.1 Security control for Internet Explorer.

If your security level is set to download and activate signed or unsigned ActiveX controls then the downloading will happen automatically If its set to ask, the user is asked if he/she will continue with the downloading exactly as the figure above, then a dialog box will appear with all the necessary information about that particular ActiveX control whether its verified or not or if you will continue with the downloading or not.

Figure 12.2 The above dialogue box is always shown before a download.

The verification security is built on a digital signature from VeriSign. This signature which is in the form of a certificate is incorporated with the ActiveX control before its put in the Internet. Before downloading any ActiveX programme a dialog box like the ones shown above in Fig 31 will always be displayed.

Microsoft's Authenticode which is an incorporated part of Internet Explorer will check the authenticity of the certificate with a certification authority. The major security risk in this is that the signed codes don't actually mean they are secure, since a code Signature can be obtained by anyone who needs it. The needed requirements can be falsified or stolen to obtain them, for example the requirements are name, address and credit card number among others and all these need not belong to the intruder. Once the intruder fills the form with the specified information then he/she will receive an e-mail with the necessary information for him/her to sign the ActiveX. When the intruder obtains the Digital ID then he will be able to sign any ActiveX control whether malicious or not. These signatures hence give the users some false sense of security and may even persuade the more hesitant users to download it. [31].

Another way of spreading malicious Trojans for example is simply configuring them and putting them in the shared folder of a peer to peer share programmes like Kazaa Before placing a Trojan horse in the shared folder the hacker may give it some popular name that will guarantee the highest downloads. Since most home computers are shared and they are mostly used by youngsters most of the time in downloading music files or films and for business by parents, so the target will be the youngsters hence giving the file an enticing name of a certain pop idol or film star.
After downloading, once they click on the Trojan in the hope of retrieving the music file, then the Trojan will be activated stealthily giving the hacker access to the computer.

13 Discussions

Our experiments and analysis showed that not all “secure” login systems are actually secure. One can wonder how accurate our results are. It depends if attacked system is protected by some security systems like a firewall and an antivirus program. Trojan CafeIni which we used was written year 2000 and would be probably found by new antivirus programs. However it is not a problem for sophisticated hacker to find a stealth Trojan with similar functions or write one. One might wonder how Knowledgeable the hacker has to be in order to carry out a successful attack. To successfully break in to a system one should have a good understanding of computer viruses and Trojan horses, what the key logger does, what encryption is. The intruder should have as well basic knowledge about hacked operating system, networking knowledge and security systems.

The attacks we made are categorised into Internal and External attacks. External or remote attacks are more difficult than Internal attacks where the attacker has a direct contact with the system or the computer being compromised. With internal attacks, it depends on the security system used if its software based certificates stored in the hard disk then all the attacker needs is a simple programme like Key logger which will intercept the password in clear text. Shared computers at home or among flatmates are vulnerable to internal attacks For example in the case of Handelsbanken any one who lives in the same home as the victim can download, configure and install key logger programme thereby easily accessing the victim’s account to withdraw money. The underlying security systems for example SSL for encryption is utilised when sending the message, but since the interception happens during the key strikes then any encryption no matter how strong is rendered useless.

How successful external attacks are depends on the security system used, if its software based for example Handelsbanken it’s possible to compromise the security system by moving the certificate from the victim’s computer to the attacker’s computer at the same time listening or recording the password. It’s even possible to move or copy the certificate to the attacker’s computer without the need of any password at all hence proving the SmartTrust programme that was to secure the certificate to be inadequate.

Another software based security system is the BankID. Some of the banks for example Sparbanken Finn and Sparbanken Gripen use the BankID as an authentication tool. Since BankID is software based its susceptible to the same security threats as that of the software based certificates. Its password can be listened to with the help of a key logger when it comes to internal attacks. For external or remote attacks it can be copied and installed in another computer as we have demonstrated in our experiments exactly in the same way as the certificates issued by Handelsbanken. We proved it by “kidnapping” electronic ID card issued by Föreningssparbanken which used BankID system. It is possible to attack some of the above mentioned banks which use the same system for login to bank accounts. Handelsbanken suggests storing the certificate in a floppy disk which is a bit complicated for most average users even if this is done it does not guarantee the safety of the certificate. All that the intruder has to do is to wait until the victim sets in his/her floppy disk which contains the certificate. It’s possible then to copy the certificate exactly in the same manner as we have copied it from the hard disk. The only difference will be the intruder will have to wait a bit longer than usual compared to if the certificate were stored in the hard disk.

To avoid interceptions the computer has to be kept Trojan or virus free all the time. These are expectations which most computer users can't guarantee hence the possibility of unauthorised access to the customers account becomes a reality. Our work is about Internet bank logins, the same type of authentication techniques are used however when contacting authorities such as the tax department or local authorities. If the authentications systems used in this case are compromised it will result in serious consequences for the public.

13.1 Authors thoughts and suggestions for improvement of security

As our results showed it was not at all hard to break into somebody's computer. It would have made our work much more difficult if the system was protected by some security systems. So we recommend first and foremost the use of firewall and antivirus programs.

Since our experiments clearly show the software based certificates issued to the customers such as the customers of Handelsbanken don't provide the security they claim to do, it can be remedied by making the SmartTrust programme work together in conjunction with the certificate closely. This can be achieved by issuing the programme during installation a randomly generated number, hashing it so that it's should not be tampered with and storing it in the register. By this way the programme would have been unique. Every time the programme starts it should compare its randomly generated number which is saved in the configuration file with the number already in the register. If they match then the programme is allowed to start and proceed otherwise it should terminate and give a warning. Another alternative solution would have been to bind the programme with the certificate in such away that each programme can only handle one certificate. In case you need several certificates then you will have to obtain several programmes, each for a certain certificate. This would have affected the user friendliness of the programme negatively.

Password generators are another tool used during authentication in log in process. Föreningssparbanken uses a generating device where it's fed with a challenge and in return it gives a response. This is very much secure than the software based certificate of Handelsbanken in the sense that what ever intercepted information has no use once it has been used. Since the generator is fed with a new challenge every time so is the response different every time as well. But still it's not secure as most users might perceive. It's possible to access the customers account if the attacker has access to the password generator.

Take for example; one of your friends wants to access your account; he noticed your password generator device is always near your computer and he know that you use your child's birthday as the PIN code. Then he can swiftly feed the generator with his account number as a challenge. As a response he gets a number and he writes down that number, then he feeds the generator with a certain amount of money say 10 000 SEK and he writes down the response he receives again. The reason for his actions were that just because if one needs to transfer money to an account that you never transferred to, you need to feed the receivers account number in the generator as a challenge. The amount of money to be transferred must be fed again the generator as a challenge. Let us say this friend tries to guess the number that would have been generated in order to log in to your account, in that case then it will be impossible. But since he has now all the numbers that would be generated in advance, that is the response then logging into

the customers account becomes a fact. Password generators are commonly protected by four digits PIN. Better security, is provided by using longer password with mixed letters and digits instead of a 4 digits PIN also it should be difficult to guess from accessible personal information. Password shall be always in place, so that even if lost or forgotten on the table it should not generate responses for an unauthorised person.

Active cards or smart cards are another way of authenticating oneself before logging into internet banks. The chip contains the keys and the certificate of the user. The card is protected with a PIN, but still this PIN can be intercepted by a programme like a key logger, hence making its protection vulnerable and less secure. A conceivable solution to this problem is to build in keyboard into card reader and let the card reader check if the password is correct so that data doesn't need transmitted to computer. All traffic between card reader and computer should be encrypted.

Biometrics which is a new technique of using the biological properties of the customers has been introduced newly. The use of biometrics is very safe and accurate since they are using properties which are unique to every person. The problem is that, the programme doesn't authenticate the customers itself but a biometric data that was sent to it. We revisit again the classical problem of passwords replaying them once intercepted. If passwords were to be intercepted and used illegally they can easily be changed. What about if biometrics authentication data were to be intercepted? Replacing a fingerprint if at all possible is not as easy as changing a password. So this system of sending the biometrics data in the internet is not only dangerous to the security of the system but to the user as well.

However a new system that uses biometric and never lets the biometric authentication data travel in Internet was developed. The smart card contains the login ID of the customer, password and fingerprints. Before logging in the customer will have to scan his/her finger prints, the scanned finger prints is compared to the finger print already stored in the smart card if the finger prints match then the customer is logged in automatically. Using biometrics in this way is very secure but expensive.

14 Conclusion

The banks offer strong security tools such as Secure Socket Layer (SSL) for encrypting messages sent between the client side that is the customer on one side and the server side which is the bank. Another strong infrastructure is the use of certificates issued by the banks with the support of security programme such as SmartTrust. However software based certificates such as the one used by Handelsbankens customers or BankIDs which are normally stored in the hard disk of the customers are not secure as demonstrated in our experiment. The best way to store these certificates is the use of smart cards. Some of the banks issue a password generating tool which work according to challenge response system. Password generators as the one used by Föreningssparbanken is secure as long as the password generating device is kept securely and protected with a PIN code.

The uses of smart cards equipped with a chip, together with a card reader are being used more widely. Active cards are secure but because the card is protected with a PIN code which is to be typed with a keyboard it's still possible to intercept the PIN code with a key logger. Even more sophisticated systems are making inroads into offering secure logins in internet banks such as biometrics. Biometrics are very much more secure if

used with a smart card and the authenticating biometrics data is not transferred to the Internet. Since interception of the biometrics authentication data can't be easily replaced or corrected

14.1 Further areas of study

In the course of our work we encountered some study areas that were interesting to be examined but due to lack of time and resources those projects were beyond our means.

In the book"Säkerhet med elektronisk identifiering"[22] it claims that it's impossible to copy a smart card. It's however generally known from other branches which make use of smart cards, such as digital TV it's very possible to copy their cards even though they claim it's impossible to copy them. For that reason it would have been of great interest to undertake on that and see if the systems that protect these cards are actually as secure as they claim to be.

15 References

[1] http://www.scb.se 5 April 2004

[2] http://www.svd.se/dynamiskt/naringsliv/did_7179015.asp 4 April 2004

[3] http://www.symantec.se/region/se/press/n011108_se.html 4 April 2004

[4] http://www.symantec.se/region/se/corporate/guide_to_malicious_code.html 7 April 2004

[5] http://www.bankid.com/index.jsp 4 April 2004

[6] http://www.statskontoret.se/publi/os/0401.pdf 7 April 2004

[7] http://www.statskontoret.se/pdf/2003124.pdf 7 April 2004

[8] ITRG. Public Key Infrastructure: An IT Manager's Guide. London, , Canada: ITRG, 2002

[9] http://www.cio-dpi.gc.ca 3 April 2004

[10] Davis, Carlton. IPSec: Securing VPNs RSA Press.
Blacklick, OH, USA: McGraw-Hill Professional Book Group, 2001

[11] www.ukfavourites.com/glossary.htm 10 April 2004

[12] www.oberthurusa.com/pns-sc-sc101-gloss.asp 10 April 2004

[13]http://publib.boulder.ibm.com/tividd/td/ITAME/iKeyman/en_US/PDF/ssu5emst.pdf 14 April 2004

[14] http://site.ebrary.com/lib/htubibl/Doc?id=10007029&page=489 15 April 2004

[15] http://www.erlang.org/doc/r9c/pdf/ssl-3.0.1.pdf 15 April 2004

[16] Traxler, Julie (Editor). Hack Proofing Your Web Application: Only Way to Stop a Hacker is to think like one. Rockland, MA, USA: Syngress Publishing, 2001

[17] http://kkant.ccwebhost.com/papers/ssl_paper.pdf 12 April 2004

[18] www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm 17 April 2004

[19] Gollmann, Dieter. Computer security. New York, Wiley Editorial, 1999

[20]Säkerhets arkitektur SIG Security 1998

[21] Help file from SmartTrust personal version. 3.3

[22] Statskontoret. Säkerhet med elektronisk identifiering. Stockholm, Novum Grafiska AB, 1999

[23] http://www.nordea.se/solo/safety.html 14 April 2004

[24] http://www.rsasecurity.com/rsalabs/faq/B.html 19 April 2004

[25]http://www.bankofamerica.com/newsroom/press/press.cfm?PressID=press.19990106.01.htm&LOBID=11 18 April 2004

[26] http://tinyurl.com/3x7mo 20 April 2004

[27] http://www.bankid.com/NodeServlet?command=layout&n=1064 20 April 2004

[28] http://www.bankid.com/index.jsp 11 April 2004

[29] http://www.statskontoret.se/publi/os/0401.pdf 22 April 2004

[30]http://www.handelsbanken.se/shb/INeT/IStartSv.nsf/FrameSet?OpenView&iddef=Installation&navid=Installation&sa=/shb/Inet/ICentSv.nsf/Default/qB8CF6B9D73EEACE2C1256CF300462980 6 April 2004

[31] http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm 1 April 2004

[32] http://www.posten.se/ 31 mars 2004

Figures

5.1 Shift cipher Davis, Carlton (Author). IPSec: Securing VPNs RSA Press. Blacklick, OH, USA: McGraw-Hill Professional Book Group

5.2 Encrypting messages http://www.cio-dpi.gc.ca

5.3 Certification Authorities role within PKI ITRG (Author). Public Key Infrastructure: An IT Manager's Guide. London, , Canada: ITRG

5.4 Davis, Carlton (Author). IPSec: Securing VPNs RSA Press. Blacklick, OH, USA: McGraw-Hill Professional Book Group, 2001

5.5 Davis, Carlton (Author). IPSec: Securing VPNs RSA Press. Blacklick, OH, USA: McGraw-Hill Professional Book Group, 2001

5.6 Creating a message digest http://www.cio-dpi.gc.ca

6.1 SSL with server authentication http://publib.boulder.ibm.com/tividd/td/ITAME/iKeyman/en_US/PDF/ssu5emst.pdf

6.2 Client authentication to the server. Traxler, Julie (Editor). Hack Proofing Your Web Application: Only Way to Stop a Hacker is to think like one. Rockland, MA, USA: Syngress Publishing, 2001.

6.3 Man in the middle attack - Traxler, Julie (Editor). Hack Proofing Your Web Application: Only Way to Stop a Hacker is to think like one. Rockland, MA, USA: Syngress Publishing, 2001.

6.4 Stopping man in the middle - Traxler, Julie (Editor). Hack Proofing Your Web Application: Only Way to Stop a Hacker is to think like one. Rockland, MA, USA: Syngress Publishing, 2001.

7.1 IPSec encryption layers shared keys.
www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm

9.1 A survey of Internet bank customers http://www.bankforeningen.se/downloads

11.1 Illustrates the steps taken by a hacker or an intruder - Made by authors with free Pictures from Microsoft.com

11.2 preparations for unauthorised intrusion, made by the authors with free word Pictures, paint and front page.

11.3 Connecting to victim, made by authors with free pictures, paint and front page.

11.4 connecting to bank account, picture made by authors with free pictures from Word, paint and front page.

11.5 downloading and using victim's certificate picture made by authors.

11.6 Hijacking of BankID picture made by authors

11.7 Internal attacks.

12.1 web security adjustment from Internet explorer, Microsoft windows.

12.2 Security dialog box

Tables.

Table 1 Logins to the biggest Swedish Internet Banks.

Table 2 Login systems to various Swedish Internet Banks.

Interview

[int1] Interview with the boss of computer store Electronikhuset in Trollhättan, Mikael Gustavsson. 1 April 2004

Appendix

Appendix A. A description of the system attacked in an internal attack

Operative system name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 1 build 2600
Operative system produced by	Microsoft Corporation
Computer name	TOSHIBA
Computer made by	TOSHIBA
Computer model	Satellite A10
Computer type	X86-based
Processor	x 86 Family 15 Models 2 Stepping 7 Genuine Intel ~2194 MHz
BIOS-version and date	TOSHIBA Version 1.20, 2003-05-20
SMBIOS-version	2.3
Windows-catalogue	C:\WINDOWS
Systemcatalogue	C:\WINDOWS\System32
Boot place	\Device\HarddiskVolume1
National system configuration	Sweden
HAL (Hardware Abstraction Layer)	Version = "5.1.2600.1106 (xpsp1.020828-1920)"
User name	TOSHIBA\master
Time zone	Western Europe, Normal Time.
Total memory	256, 00 MB
Available memory	34, 65 MB
Total virtual memory	825, 00 MB
Available Virtual memory	415, 02 MB
File space	586, 20 MB
Paging files C	: \page files
Antivirus program	Symantec antivirus version 8.00.9374
Virus definition files	2004.04.05 rev. 56
Firewall program	Norton Personal Firewall 2004 ver. 7.0.0.177

Appendix B. Description of attacked system in external attack

Operative system name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 1 build 2600
Operative system made by	Microsoft Corporation
Computer name	TOSHIBA
Computer made by	TOSHIBA
Computer model	Satellite A10
Computer type	X86-baserad computers
Processor	x 86 Family 15 Models 2 Stepping 7 Genuine Intel ~2194 MHz
BIOS-version and date	TOSHIBA Version 1.20, 2003-05-20
SMBIOS-version	2.3
Windows-catalogue	C:\WINDOWS
System catalogue	C:\WINDOWS\System32

Boot	\Device\HarddiskVolume1
National configurations	Sweden
HAL (Hardware Abstraction Layer)	Version = "5.1.2600.1106 (xpsp1.020828-1920)"
User name	TOSHIBA\master
Time Zone	Western Europe, normal time
Total memory	256, 00 MB
Available memory	34, 65 MB
Total virtual memory	825,00 MB
Tillgängligt virtuellt minne	415,02 MB
File space	586, 20 MB
Paging files C	: \pagefile.sys

Appendix C. Description of system in external attack

Operative system name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 1 build 2600
Operative system producer	Microsoft Corporation
Computer	STATION
Computer made by	INTEL
Computer model	AWRDACPI
Computer type	X86-baserad computer
Processor	x 86 Family 15 Models 2 Stepping 7 Genuine Intel ~2669 MHz
BIOS-version and date	Phoenix Technologies, LTD 6.00 PG, 2002-11-28
SMBIOS-version	2.2
Windows-catalogue	C:\WINDOWS
System catalogue	C:\WINDOWS\System32
Boot position	\Device\HarddiskVolume5
National configurations	Sweden
HAL (Hardware Abstraction Layer)	Version = "5.1.2600.1106 (xpsp1.020828-1920)"
User name	STATION\station
Time zone	Western European, normal time
Total memory	512, 00 MB
Available memory	331, 30 MB
Total virtual memory	1, 95 GB
Available virtual memory	1, 64 G
File space	1, 45 GB
Paging files	X:\pagefile.sys

Appendix D. CafeIni 1.1 and how to use it.

We copy this text from CafeIni read me file. We did it because it can be difficult for reader to find this Trojan on the net.

NEW GENERATION OF WIN95/98/2000/NT/ME BACKDOORS (FOR REMOTE COMPUTER CONTROL)

1. Why CafeIni is better than other backdoors (like Net Bus):

- can kill more than 30 Windows antivirus and anti backdoors from memory
- automatic update of server by http
- doesn't install itself into registry (when can or install under random name)
- written in Visual C++ (smaller and faster than Delphi)
- you can control remote computer by telnet (e.g. from Unix)
- works on Windows 95/98/ME and also Windows NT/2000
- with CafeIni client you can control multiple computers (e.g. open CD-ROM doors on 10 computers with one button click)
- full multitasking (e.g. you can upload and download files in One time from multiple computers)
- some new backdoors commands (especially with desktop)
- client is very easy to use, like old good Net bus 1.x
- includes configuration for server (edit server)

2. CafeIni is:
CafeIni consist of three programs for Windows 95/98/ME/2000/NT:
a) "CAFEiNiserver.exe" - gives client opportunity to remote control computer (host) with installed server. Server gives client control, sometimes bigger than user on computer with installed server have.
b) "CAFEiNiclient.exe" - to control remote computer (host, server). CafeIni client can be replaced with any telnet client to control Windows Computer from UNIX, Linux... But CafeIni client has much more features e.g. Port scanner and ability to control multiple computers (e.g. open CD-ROM doors on all computers (servers) with one button click).
c) "CAFEiNiconfig.exe" - to configure CafeIni server before install or sending it to Victim e.g. you may choose port or turn on e-mail notify about starting of server. Each time server will be started you should get e-mail.

3. How to try without installing server.
You can start server with "/no install" option: "CAFEiNiserver.exe /no install" and server doesn't install itself into system. Next time you start Computer there will be not CafeIni server installed. You can also start Server and client in one computer (enter "127.0.0.1" in client), but Some command may not work or work not well.

4. How to install server.
It's very simple; you have to run "CAFEiNiserver.exe" on victim's computer. If you haven't physical access to victims computer send server to victim by FTP, IRC, ICQ... You can rename "CAFEiNiserver.exe" to other name e.g. "update.exe".
When victim runs this program you will have remote access to victim's computer. Programs "CAFEiNiclient.exe" and "CAFEiNiconfig.exe" are only for your usage. You can use CafeIni configuration for setting servers starting parameters before installing or sending sever.

5. How to connect (get remote control).
a) From CafeIni client ("CAFEiNiclient.exe" works on Windows 95/98/ME/2000/NT) enter victims host name or IP, default port is 51966 (0xCAFE),

Click "Connect" and if server is installed and computer connected
to Internet (or your network) you'll be connected,
b) From any telnet client (all kind of computers) enter command "telnet <victim> 51966", where <victim> is victims host name or IP (e.g. from Windows click "Start", click "Run" and enter something like that: "telnet 107.3.45.11 51966")

6. How to remove server.
Connect to server with telnet client (see point number 5). Eventually enter password, if password is set. Later enter command "UNINSTALL" and press "Enter" on keyboard. Program should be completely removed from system. You can check it by restart system. From now server shouldn't answer (inability to get access to server).
WARNING! In some cases there can be more than one CafeIni server installed. Then you must Uninstall server more than one times (one UNINSTALL for one server)

7. Killing of antivirus and anti backdoors.
CafeIni server can kill (remove from memory) many antivirus and anti backdoors.
CafeIni server kills this antivirus from memory:
Antiviral Toolkit Pro
Antivirus expert
Anywhere Antivirus
Avast32
AVK SCAN
ESafe Protect
F-Secure Antivirus
F/WIN32
FIBER Anti Virus
Integrity Master
Intel LANDesk Virus Protect
McAfee Virus Scan
MkS_Vir
Norton Anti-virus
Panda Anti-virus
PC-cillin
Quick Heal
Romanian Antivirus Pro
Sophos Anti-Virus Sweep
Thunder BYTE Antivirus
Virus Safe Web

CafeIni server kills these anti backdoors from memory:
Anti Trojan
Back Work
Hook Protect
Lockdown
Protector2K
Tauscan
The Cleaner
Trojan Defence Suite
Trojan B' Gone

8. If you want help (bug reporting).

If you detected some bugs in server please send bug report to authors.
If you can, please also include log file created in this way:
Start server with option "/debug=<drive>\<log filename>"
(e.g. "CAFEiNiserver.exe /debug=c:\cafeini.log")

9. Program system requirements.
-computer with Windows 95/98/ME/2000/NT
-installed TCP/IP

10. Licence.
By using this CafeIni You agree that:
a) CafeIni is FREEWARE and no charge should be made to get it
b) CafeIni is provided 'as-is', without any warranty
c) Authors take no responsibility on damages and illegal actions caused by this program
d) you can't use this program to purposes which aren't agree with law in your country
e) CafeIni must be spread with this license

11. Contact with authors:
E-mail: cafeini@viper.pl
cafeini@kki.net.pl
WWW: http://viper.pl/~cafeini
http://kki.net.pl/~cafeini

Appendix E: detailed information of the experiment.

Part 1 - Preparation for an unauthorised Intrusion

1. We started by downloading the necessary Trojan from the Internet in this case Caffeine.
2. Then we configured the Trojan, that is the Cafeiniconfig.exe
3. Then we fill in during the configuration process with a password which we will use during our connection to the victim’s computer.
4. We fill in as well with an e-mail address which we will receive information from the computer of the victim, for example his/her IP address which is very much useful in case the victim has a dynamic IP address.
5. We instructed the Trojan to kill antivirus programmes so that it shall not be detected.
6. We instructed the Trojan to show the victim some false information once the Trojan is activated something in the style of “File damaged sorry it can’t be opened” we do this to minimise the suspicion of the victim.

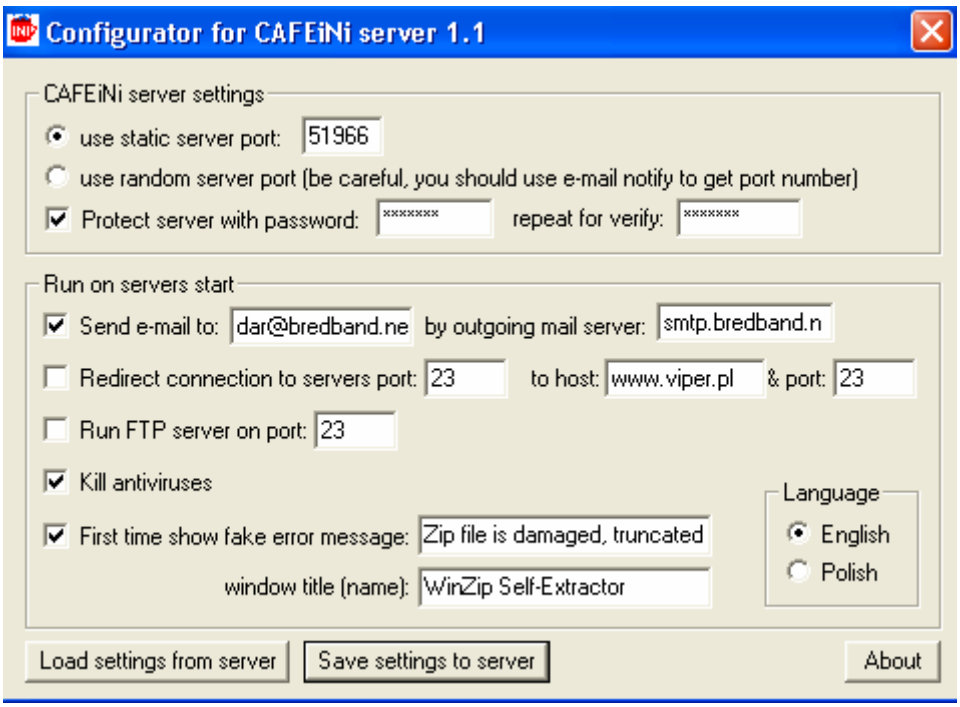


Figure 15.1

7. We saved the settings to the server part of the Trojan to store our configurations before sending it to the victim. We changed the name of the file to HolidayPhotos.exe So as to deceive the victim.

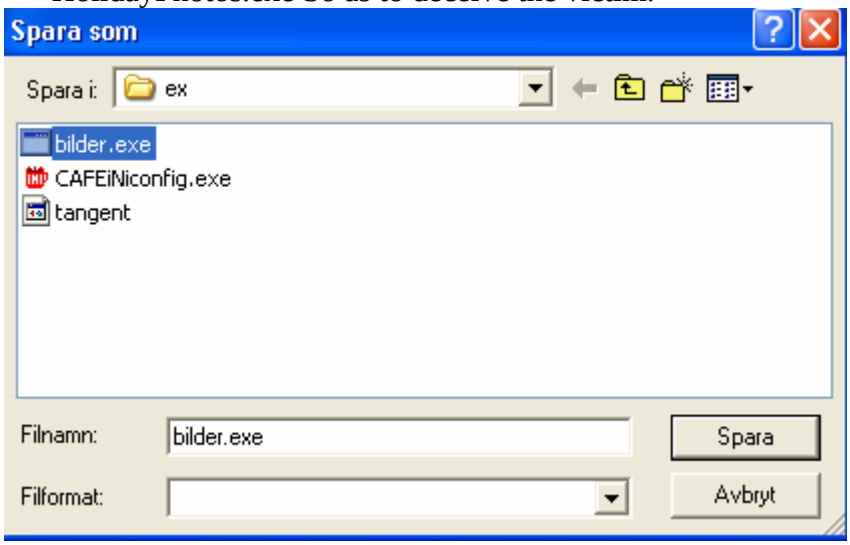


Figure 15.2

8. We send an e-mail to the victim and attach it with the file HolidayPhotos.exe

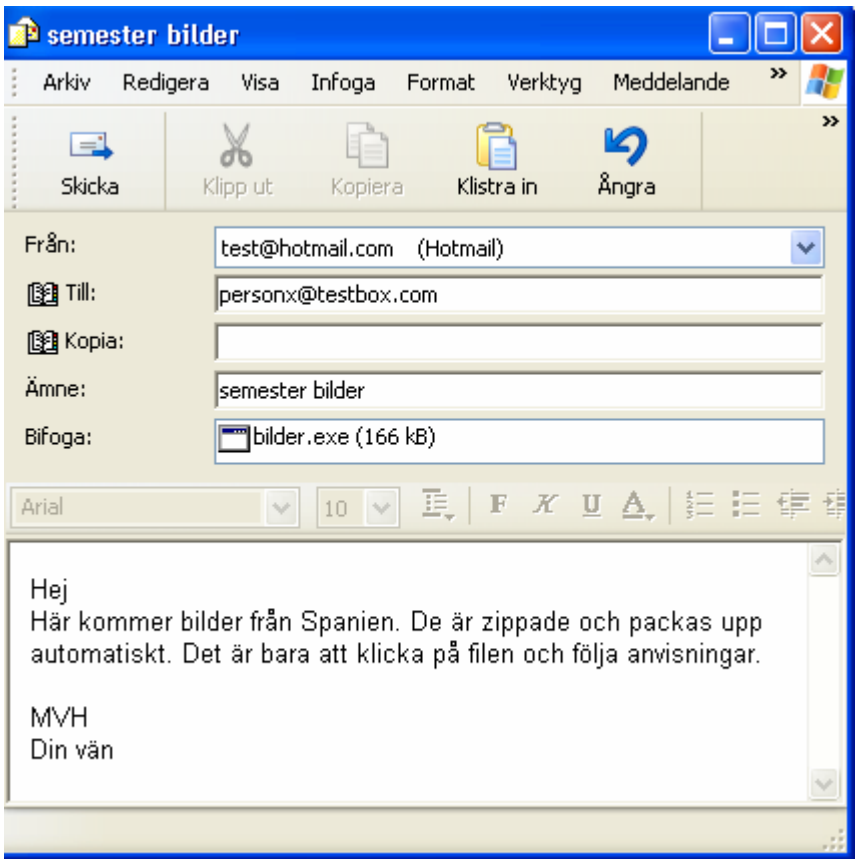


Figure 15.3

9. We send the mail finally to our victim.

Part 2 - Victim receives mail with Trojan horse

1. Our victim finally opens his letter and decides to see the photos by clicking on the file. Expecting the self extracting file to show the photos. Instead he gets the message below, deceiving him to believe that there is something wrong with the file.

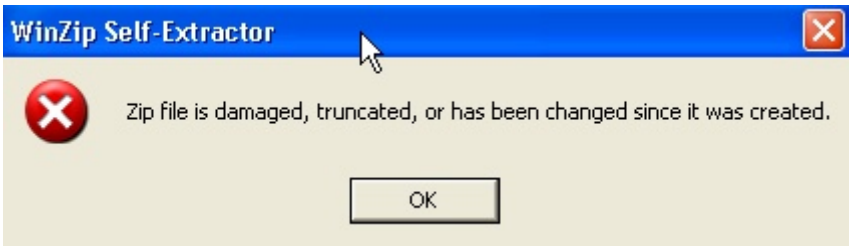


Figure 15.4

2. Without noticing the Caffeine server is installed in the victims computer stealthily

Part 3 - The Hacker connects to the Victim's Computer

Now we are to connect to the victim's computer and record his/her keyboard strikes and at the same time get his/her Certificate.

1. We received our mail in the same address as we fed in during configuration process. We received a mail from our victim with IP address, which we will use during our connection process. We will receive a letter like this every time the victim starts his/her computer, so that we don't lose track of our victim.

Figure 15.5

2. We started our Cafeiniclient.exe to connect to our victim; we filled in with the IP number of the victim which we received through mail and a password, which is the same password we used during our initial configuration process of the server side of the Trojan.

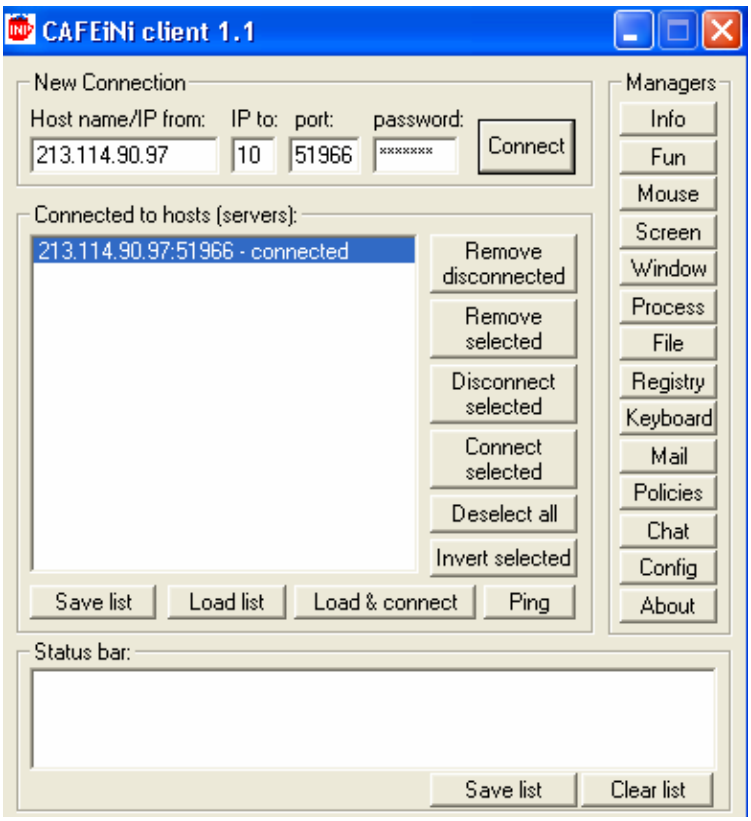


Figure 15.6

3. Now we are connected to the computer of our victim we can upload, download files and even start programmes on his/her computer remotely.

4. We click on ”Keyboard” on client side of the Trojan to initiate keyboard recording, this process records every key strike the victim makes including the passwords in clear text. The keyboard recorder records the names of the programmes used. So we check for the line “Autentisera - SmartTrust Personal” under this programme we will be able to retrieve the password in clear text: 1234567890 “Listening” for the password might take sometime depending on if the victim logs in to his bank or not.

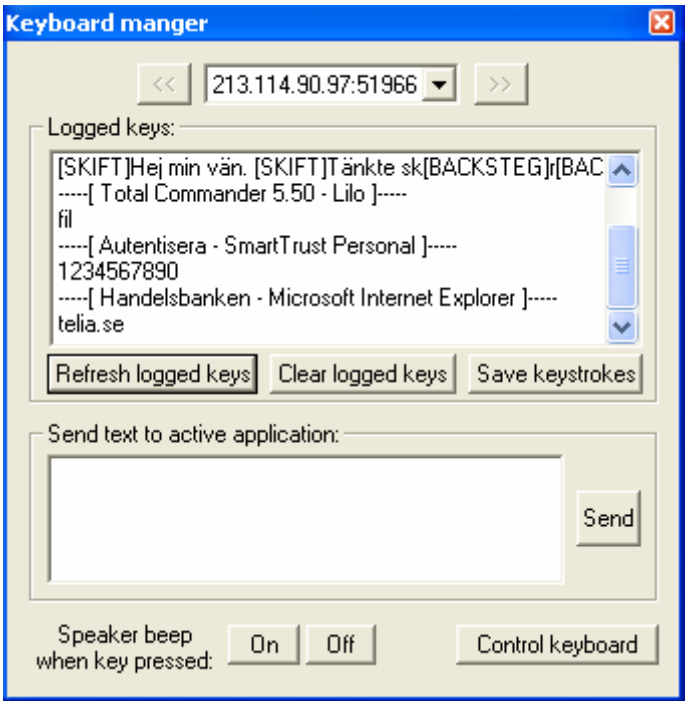


Figure 15.7

4. We clicked on “File” on the client side of the Trojan in order to access the certificate which is on the victim’s computer
5. On the left side of the window below we can see the disk contents of the victim’s computer and on the right hand side the intruder’s disk is shown. It’s possible now to download or upload files from the victim’s computer to our computer. We browsed to c:\program\SmartTrust\certs and copied the victim’s certificate to our computer in c:\temp

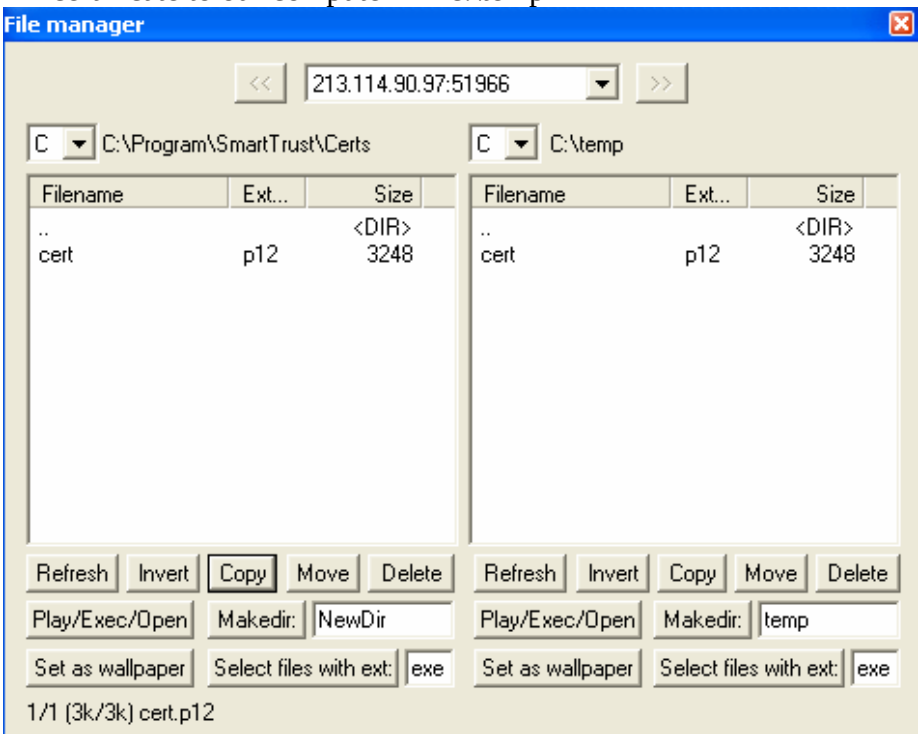


Figure 15.8

Part 4 - Copying of Certificate and password

1. Repeat step 1 to 5 from Part 3, to copy BankID.
2. We browse in the disk of the victim to C:\Document and settings\master\Mina document\cbt and then copy it to our disk at C:\temp

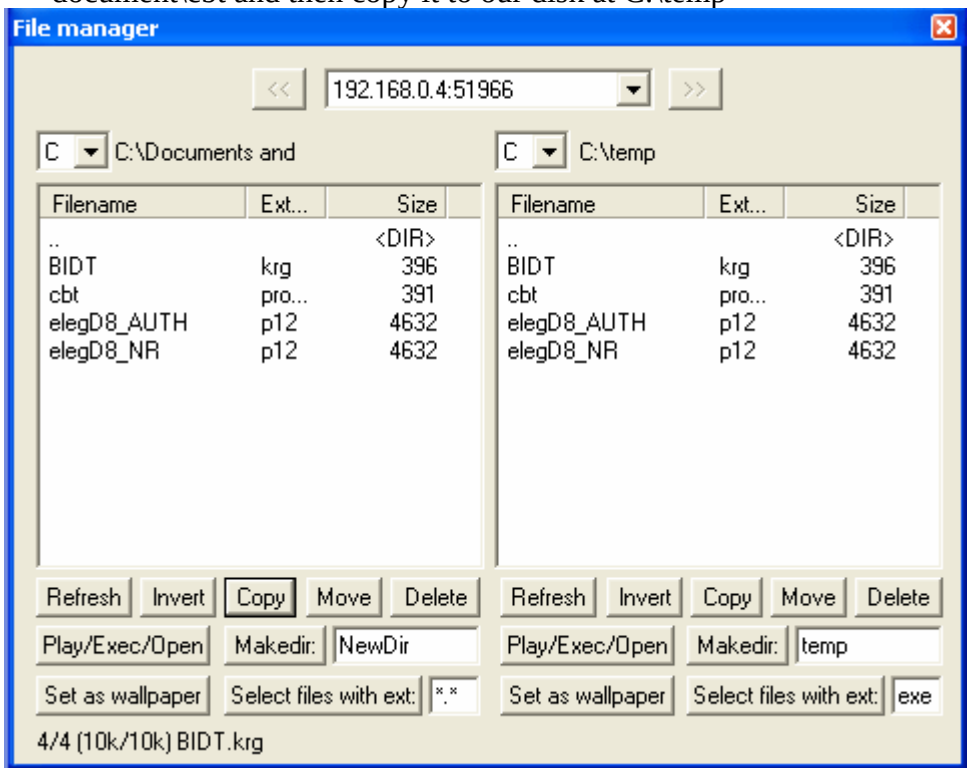


Figure 15.9

We assumed that the installations of the security certificate and corresponding programme were done according to the installation guide.

This is what we have done once we were in the victim's computer:

1. We copied the certificate from the victim's computer which we have found in C:\program\smartTrust\certs to a temporary directory C:\temp to our computer
2. We downloaded the SmartTrust programme from Handelsbank's website at https://www.handelsbanken.se/shb/inet/icentsv.nsf/vlookuppics/installation_smarttrust_personal_3.3.1swe.exe/$file/smarttrustpersonal3.3.1swe.exe and install it in our computer in the same path as it was in the victim's computer that is: c:\program\smartTrust

3. To use the certificate of the victim we have to use it together with SmartTrust programme. To do that we use the Administration Utility this is a tool for managing the certificate. It's found at Start>program>SmartTrust personal>

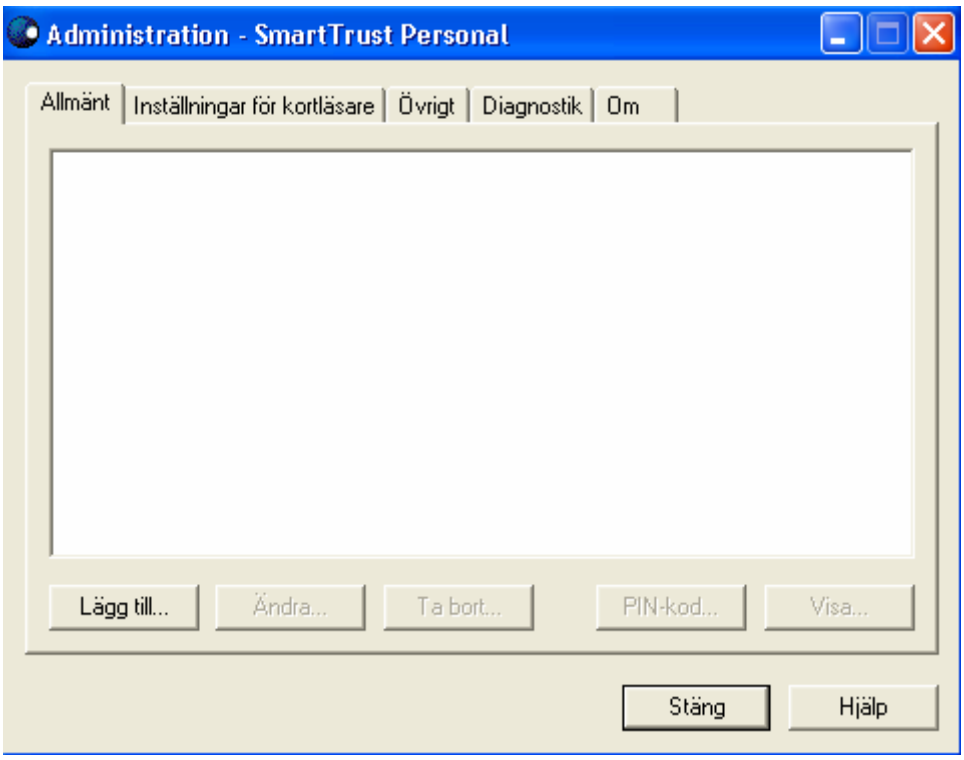


Figure 15.10

4. We click on"Lägg till" as indicated above.
5. We fill in the path C:\temp where the victim's certificate is stored and then click OK

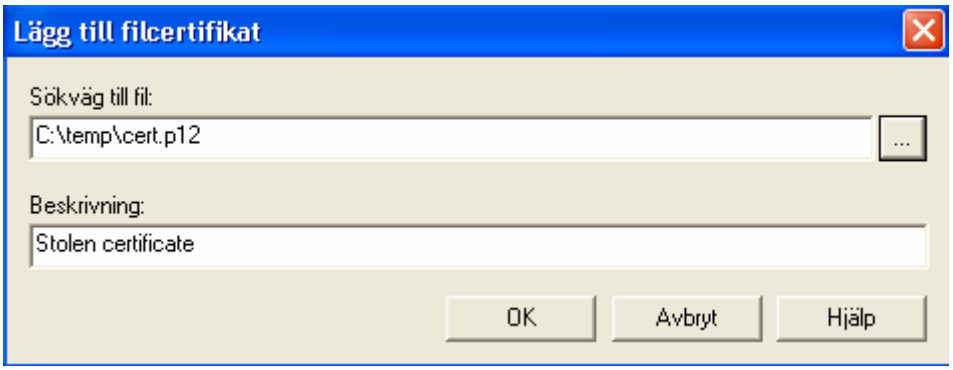


Figure 15.11

6. We fill with the PIN code that was recorded by the key logger and click OK

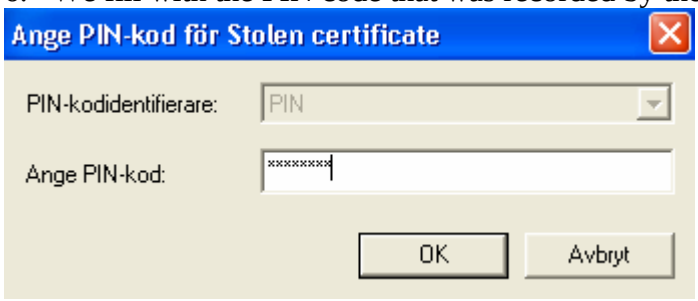


Figure 15.12

7. The programme answers with this message as shown below.

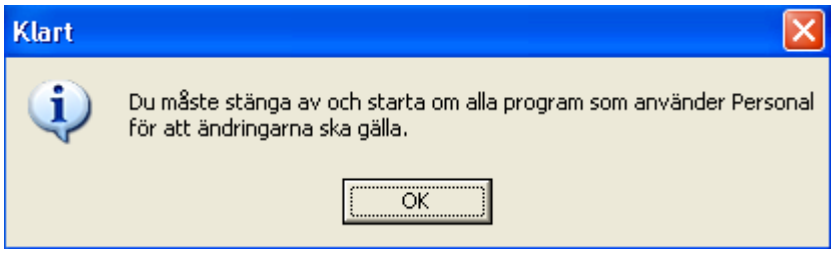


Figure 15.13

8. We click OK

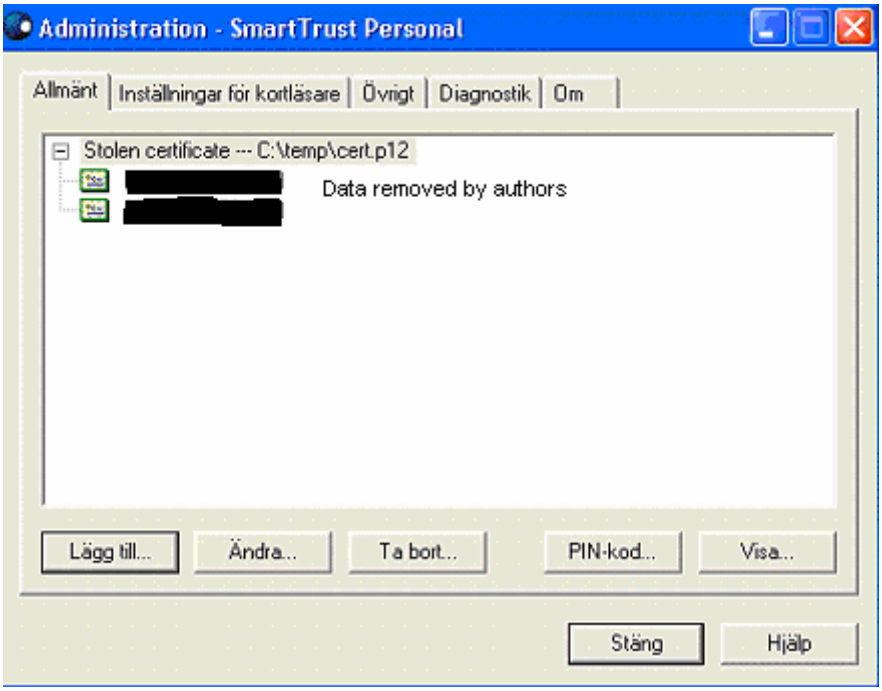


Figure 15.14

9. We click on close
10. We go to www.handelsbanken.se and click on log in.

Figure 15.15

11. In return a new window is opened, of which we have to authenticate with a PIN code.

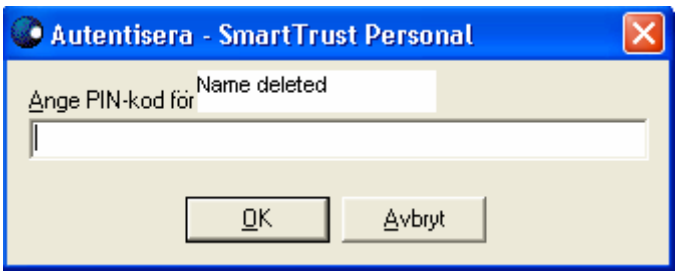


Figure 15.16

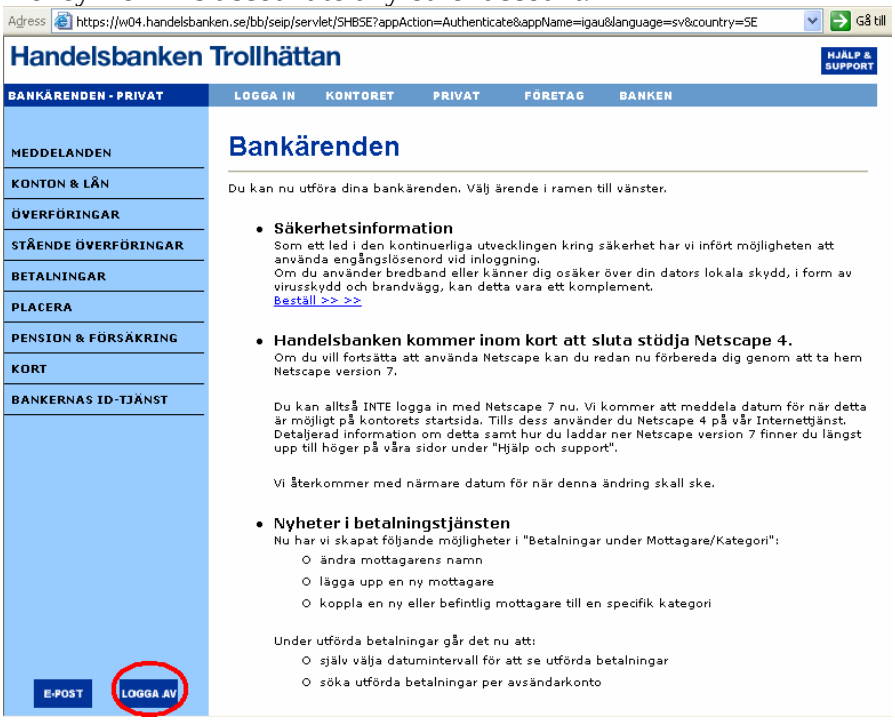
12. We fill in with the PIN code we received from the Key logger and click OK
13. Now we are actually logged in to the victim's account and we can withdraw money from his account to any other account.
14. 

Figure 15.17

Part 5 coping certificate to SmartTrust programme without password

Once we have succeeded in accessing the victim's account, we decided further to check if it was possible to use the certificate without actually using any password. That is coming round the SmartTrust programme as a whole and cutting on the time wasted for waiting the victim to use the password as we did in our earlier experiment.

1. We copy the SmartTrust programme including the certificate from the victim's computer which we have found in C:\program\SmartTrust to a temporary directory in C:\temp in our computer.
2. We download SmartTrust from Handelsbank's website: https://www.handelsbanken.se/shb/inet/icentsv.nsf/vlookuppics/installation_smarttrust_personal_3.3.1swe.exe/$file/smarttrustpersonal3.3.1swe.exe and install it in our computer in the same path as it was in the victim's computer that is C:\program\SmartTrust.

3. We close the SmartTrust programme which is activated after the installation. We do that in order to carry out step 4.
4. We delete the SmartTrust we just installed from its storage place; we will not use the Add/Remove programme in the control panel as that will remove it totally.
5. Now we copy over SmartTrust that we copied from victim's computer from C:\temp to C:\program\SmartTrust
6. Now we activate SmartTrust through Certificate Mover which is found at Start>program>SmartTrust Personal
7. In this way we were able to move the whole certificate from one computer to another without the need of using a password. If we were to use "Administration Utility" which is a tool that is used for managing the certificate which comes with SmartTrust programme then we would have been forced to use a password in order to move the certificate from one computer to another. This means we are making use of a security defect within the programme.
8. We go to www.handelsbanken.se and click on log in.
9. A window is opened indicating that the certificate has been found and we need to authenticate ourselves with a PIN code.

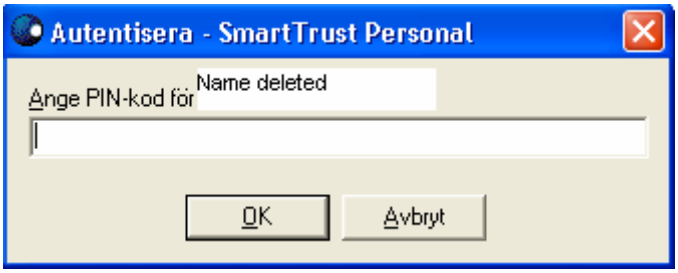


Figure 15.18

10. We write in the password we received from Key logger and click OK
11. Now we are logged in, in the victim's account and we can transfer money to any account we wish.

Figure 15.19

Part 6 - Hijacking of BankID

1. According to step 1-5 from part 3 we have copied the BankID certificate and we have recorded its password in the same manner as the other certificate. We logged on to the following site: http://bankid.cypoint.se/index.html.jsp which is the test site for BankID services.

2. Click on Test BankID

Figure 15.20

3. Click on Continue

Figure 15.21

4. Now we asked if we will install BankID client ver.2_5_5. We click YES.

Figure 15.22

5. We browse to C:\temp, its there we copied the BankID certificate from the victim, we write in the password we listened from the victim earlier and we click OK.

Figure 15.23

6. We then place an order for 2 winter catalogues and 3 summers catalogues. And we click continue.

Figure 15.24

7. Now we approve the order by writing in the password and clicking OK

Figure 15.25

8. The order was approved and verified.

Figure 15.26

Part 7 - Internal Attacks

1. Download the programme ”Family key logger” from the web at: http://www.spyarsenal.com/familykeylogger/familykeylogger.zip, this is a trial version with 21 days permission after that one has to buy, however there are many other free Key loggers in the Internet.
2. Click on Save

Figure 15.27

3. Install the programme and start the FamilyKeyLogger-setup.exe
4. Accept the conditions attached by clicking I agree
5. Click next

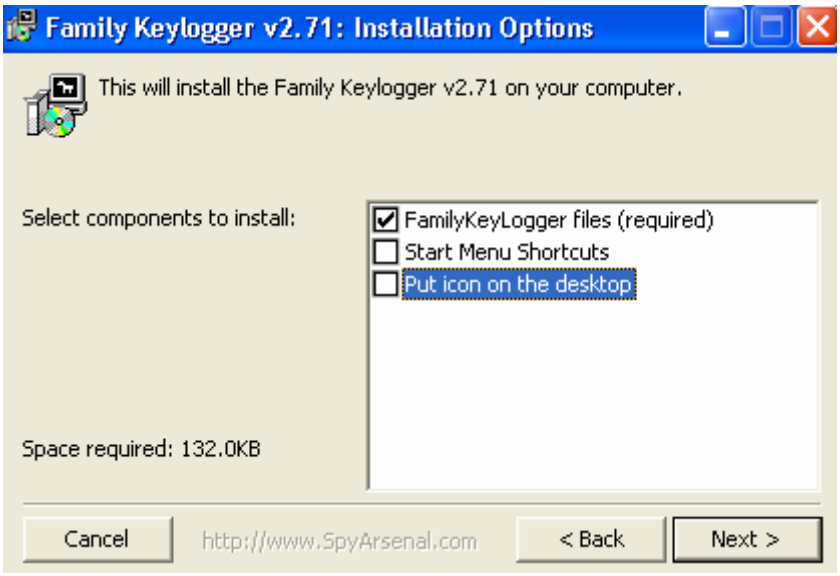


Figure 15.28

6. Install it in C:\Windows\System32\CTF

Figure 15.29

The programme during its installation was never discovered by Symantec antivirus programme, it's not a virus.

7. Now the programme is installed and must configure it. Right click on the icon of the programme.

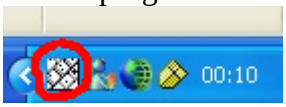


Figure 15.30

8. Choose Options
9. Choose auto run at system start up and then click on OK

Figure 15.31

10. Now it records every key strike to a file in C:\Windows\System32\CTF\ctfmon.txt
    After few days you find the password in the file in clear text and the date it was recorded which is “1234567890”

```
[07/04/2004, 00:35].   User: "master".  Window title:"Servern hittades inte - Microsoft Internet Explorer"
www.handelsbanken.se

[07/04/2004, 00:35].   User: "master".  Window title:"Autentisera - SmartTrust Personal"
1234567890
```

Figure 15.32

11. Go to www.handelsbanken.se and click on log in.
12. Authenticate with password obtained from the file and click OK

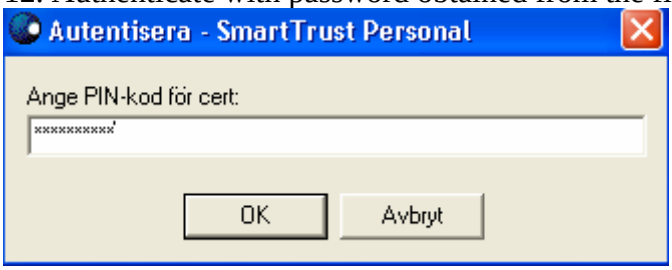


Figure 15.33

13. It’s logged in and the intruder can withdraw money from the victim’s account to any where.


Adress
https://w03.handelsbanken.se/bb/seip/servlet/SHBSE?appAction=Authenticate&appName=igau&language=sv&country=SE
Handelsbanken Trollhättan
HJÄLP & SUPPORT
BANKÄRENDEN - PRIVAT
LOGGA IN
KONTORET
PRIVAT
FÖRETAG
BANKEN
MEDDELANDEN
KONTON & LÅN
ÖVERFÖRINGAR
STÅENDE ÖVERFÖRINGAR
BETALNINGAR
PLACERA
PENSION & FÖRSÄKRING
KORT
BANKERNAS ID-TJÄNST
E-POST
LOGGA AV
Bankärenden
Du kan nu utföra dina bankärenden. Välj ärende i ramen till vänster.
Kundsupportens öppettider under påskhelgen
Långfredag Stängt
Påskafton Stängt
Påskdagen Stängt
Annandag påsk 12:00 - 22:00
Vi byter design och förbättrar privatmenyn
Inom kort kommer vi att ändra våra webbsidor. De viktigaste förändringarna kan du läsa om här: Se demo
För utskrift: Privat » » (pdf 2mb)
Vill du deklarera på nätet?
Beställ ditt BankID, så kan du identifiera dig och skriva under elektroniskt.
Beställ » »
Handelsbanken kommer inom kort att sluta stödja Netscape 4.
Om du vill fortsätta att använda Netscape kan du redan nu förbereda dig genom att ta hem Netscape version 7.
Du kan alltså INTE logga in med Netscape 7 nu. Vi kommer att meddela datum för när detta är möjligt på kontorets startsida. Tills dess använder du Netscape 4 på vår Internettjänst. Detaljerad information om detta samt hur du laddar ner Netscape version 7 finner du längst upp till höger på våra sidor under "Hjälp och support".
Vi återkommer med närmare datum för när denna ändring skall ske.

Figure 15.34