Authentication and Transaction Security in E-business

Lorenz Müller

AXSionics AG, BFH Spin-off Park
c/o Hochschule für Technik und Informatik
Seevorstadt 103b, CH - 2501 Biel

Abstract. E-business is one of the driving factors for the growth of the worldwide economy. But in parallel to the upsurge of the digital trade the cyberspace became also a main attraction for criminals. Today main parts of the Internet are still outside of traditional national legislation and law enforcement. Security is therefore a task that can not be delegated to the government only. Each party in an E-business operation has to care about the threats and the effective countermeasures. This paper introduces in the theme of online security and presents at the end a technical system that helps to defeat many of the actually most dangerous threats to a trusted E-business world.

1 Introduction

Neither the bursting of the Internet bubble nor the recent boost of online criminality stopped the ascension of electronic business in the last few years. Almost all industries have developed business models which rely on so called E-business processes that use the communication facilities of the Internet. The growth rates of this new economic sector are impressive. The corresponding economic indicators show that online retail sales in 2006 (B2C) reached a value of $148 billion in North America and $102 billion in Europe with an expected CAGR of 20 % or more [1,2]. The already much larger ICT-based business to business (B2B) market (projected $2.3 trillion in US and €1.6 trillion in Europe in 2006) still continues to rise substantially above the total market growth (CAGR of 13.9 % in US [1] and 19 % in Europe) and represents already today a substantial fraction of the total worldwide economy.

E-business is now an important opportunity to extend the range and the productivity of existing and new companies. Customers appreciate the convenience and the expanded offering of the Internet shopping. Companies need the improved possibilities for their supply chain management to cut cost and to move rapidly in the global market. However this new Eldorado also attracts criminals and the Web technologies, originally designed for maximum availability and connectivity, offer numerous possibilities for abuse and attacks on the digital economy. Investigations showed that the fraud rate in online transactions is at the level of 2.1% (2004) rising to 3.7% (2005) [3] of the total transaction volume. This value is more than an order of magnitude higher than in conventional transactions and already now leads to

Please use the following format when citing this chapter:

Müller, L., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 175–197.

substantial losses especially in the financial industry [4]. Identity theft, which is a preferred way to commit online fraud, caused over $2 billion damage to the US financial industry in 2006 [3]. These facts have also changed our view on security.

1.1 The Changing Landscape of Security

A big building with a vitreous facade and a prestigious lobby with secured entry doors still represents our classic picture of a secured enterprise. However this is an idea of the past. Within the digital economy, corporations have become increasingly virtual organizations distributed over many countries and interacting with a rapidly growing community of collaborators, clients and partners. In parallel to this evolution the classical concept of secured zones inside clearly defined borderlines has been replaced by new strategies to cope with fraud and crime.

1.1.1 Security is on the radar of all industries

Such new security needs have triggered a whole security industry in the IT sector. Although the classical security market is still dominant, the newer market for logical access control grows much faster and will reach US$ 9.3 billion this year with CAGR of 20% [5]. The growing importance of security is also reflected in the spending behavior of the IT departments of F1000 companies. In 2006 about 88 % of these departments allocated constant or growing budgets for IT security compared to the budgets in previous years. Some of them intend to spend as much as 25 % more on security [6].

1.1.2 Security in the physical and the digital world

Improved security concepts now not only include physical security (buildings, labs, rooms) but increasingly have to include logical security: protecting the knowledge and information space of an enterprise and the digital transaction processes with their clients. In the traditional approach, we defined a borderline with inside and outside infrastructure and well guarded gates between the two zones, using armed doors, firewalls, virus scanners, VPNs and other protective measures.

1.1.3 Three lines of defense: the new paradigm

This borderline security approach was well adapted for classical organizations but is not sufficient in a world of virtual and widely distributed organizations. To protect a complex network organization we have to introduce an in-depth defense at staggered perimeter lines. Border security, authentication and authorization build together three layers of defenses that allow secure user access and robust security.

1.2 Security requests in online transactions

We may represent an E-commerce transaction between a person and an operator of a value service schematically by a triangular relationship. On one side we have the physical person that intends to take advantage of the operators offer. To get in contact with the operator the person needs a certain digital identity, which in some way

defines the social situation of the person and its business relation with the operator e.g. a proof of the capability to pay for a service. The operator administers the access rights to his value services and allocates these rights through his identity and service management system to the authorized users or customers. A person intending to use the operator's service must present some identity credentials to show that she really has the claimed identity with the corresponding social rights (e.g. possession of a personal credit card). On the backward step the operator then grants access or allowance to the person after having checked the presented identity credentials.

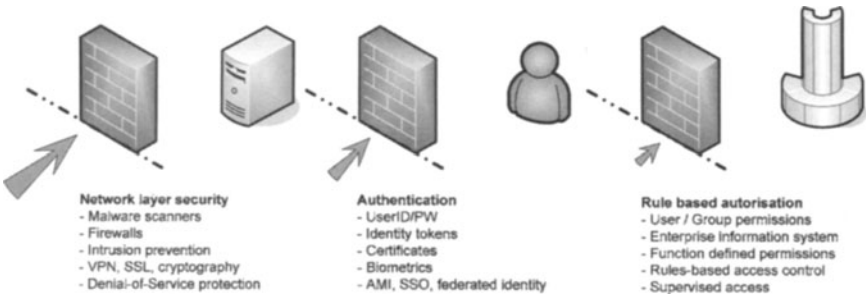

Fig. 1. Authentication is a central keystone in a layered defense system. Its strength has to match the strength of the typical border line security measures. The lines represent the three steps in an in depth security system.

2 Threats to e-business

The threats to the digital economy can be roughly put in three categories:

- Threats originating from criminals who intend to harm the welfare of others to gain financial, competitive or political advantages.
- Threats originating from reckless promoters of their online offering using unwished marketing means.
- Threats originating from software or product pirates that offer their fraudulent copies over the Internet.

All these threats target the digital economy and, in the same time, use the technological means of the digital economy. Typical methods to execute an attack within one of the above threat categories include the application of malware that is introduced to the users Internet access device, the operation of malicious Web sites or the infection of innocent Web sites with malicious codes, the pushing of unwanted information content to the user (spam, adware etc) and the distribution of illegal copies of digital content or values [12]. We will concentrate here on the threats of the first category in which the identity theft in all its forms is a major vector for the execution of an attack.

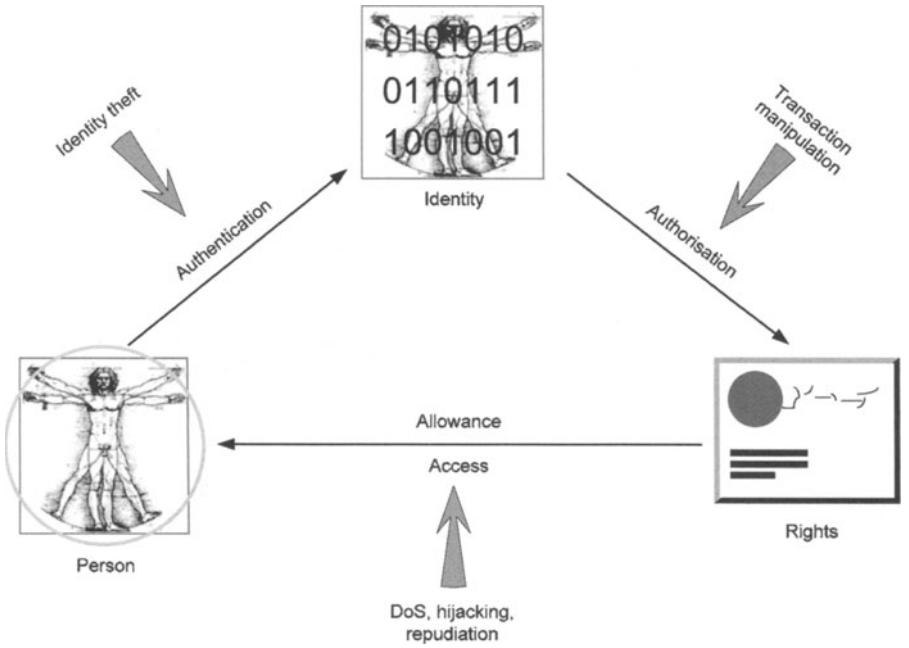

Fig. 2. The processing steps to conclude an E-commerce transaction are schematically represented by the above triangular relation between the physical person, its social identity and its rights that are administered by an operator. Each processing step is endangered by some specific threats, namely identity theft compromises the authentication, transaction manipulation jeopardizes the authorization step and any kind of threats to the use of the rights endangers the exercise of the rights through the authorized person.

2.1 What is new in online criminality

In reality the cyberspace is not so much different from the real world. Behind the entire complex infrastructure are human beings with more or less the same ethic behaviour as in the physical world. They interact with each other, make business and form social networks or build even common new living spaces. At the end we find similar threats in the cyberworld and in the physical world. Criminals still intend to rob or cheat others with the goal to enrich themselves or virtual violence can often end in real physical violence or sexual abuse. So the basic threats are not new in the cyberworld. There are however important differences that change the balance between threats and risks in the cyberspace [13].

2.1.1 Automation

Automation enabled by the digital technology overcomes the limits of single unit production of traditional attacks. A classical bank robbery needs a very high success rate to be profitable for the bank robber. He has neither the time nor the resources to rob thousands of banks with the same method. This is different for a cyberspace attacker. He simultaneously can attack thousands or millions of victims and he needs

only a tiny success rate to make the attack profitable. Typical phishing attacks have at best a few percent responding victim candidates but the absolute number of victims may be in the thousands or even more [14].

2.1.2 Remote action

A second difference comes from the very nature of the cyberspace. A personal and therefore risky presence on site of the crime is no more necessary. A cyberspace criminal may rob a bank in Norway easily from his home computer somewhere in Korea or elsewhere. The risk to get caught on the spot is quite high for a classical bank robber. For a cyberspace criminal the risk to be dismantled and caught however is at the per mille level [15].

2.1.3 Access to crime supporting technology

A further difference comes from the openness of the Internet. It leads to a rapid spread of new knowledge on security breaches and to a wide distribution of instruments to take advantage of such security holes. This is a further advantage for the cyber criminal over the classical criminal. Digital 'arms' are easy to procure and there is no real dissemination control. The attacker community has undergone a fundamental change in the last years. Highly skilled professionals produce the attacking tools and offer them on the Internet for moderate fees [16]. Organized crime but also so called script kiddies can use such tools to perform efficient attacks on persons and institutions. But such technology can also support the cheating of thousands of individual customers which may jeopardize even big companies or whole industries. The cracking of pay TV decoders or the distribution of illegal software copies are typical examples of such low level fraud at large scales.

2.2 The weak spots in online transactions

For a better understanding of the threats to online business transactions we need a closer look on the different weak spots of the end-to-end communication channel between user and operator and the way the transaction can be attacked. With 'user' and 'operator' we use the typical notation for an E-commerce transaction which is naturally the most exposed type of E-business transactions. But the same discussion holds for other forms of E-business relations e.g. for partners in internal business processes or in enterprise communication acts.

2.2.1 Attacks against the operator

A typical communication channel starts within a secure zone at the operator's site where the value services, the access rights and the user identities are administered. Such secured zones have in general a high level of logical and physical protection against intruders or malware. Their security is often assessed and defined through some sort of certification procedure. The entry threshold for an attacker into the heart of the IT infrastructure of a value service operator is rather high but can never be completely excluded [17].

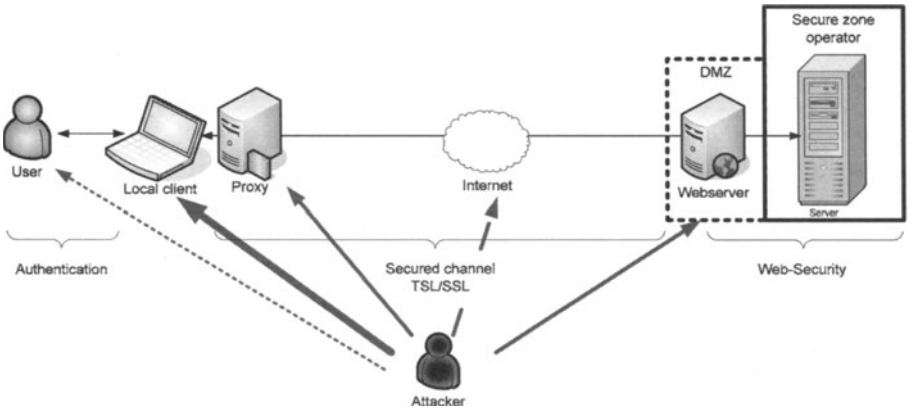

Fig. 3. There are multiple points of attacks on a user-operator communication channel in an e-business transaction scenario. The scheme is strongly simplified. In reality the communication channel is a complex technical system that bears many known and still unknown points of attacks.

The Web, mail and DNS servers of organisations are directly accessible from the outside. They reside normally in the so called DMZ (Demilitarized) zone of the internal perimeter security arrangement. Therefore they are less secure and often a target for malware attacks e.g. with the aim to infect visiting browsers. The main threats for the Web infrastructure come from attacks against the availability of the service. In so called DoS (Denial of Service) or even DDos (Distributed Denial of Service) attacks the attacker sends a huge amount of phoney service requests to the Web portal of an organisation. The resulting overload of the Web infrastructure may lead to a breakdown of the service.

2.2.2 Attacks against the connecting channel

Another potential weak point is the infrastructure of the Internet itself. Any gateway, router or data bridge can be used to eavesdrop on the passing data traffic. If the communication between the webserver and the Internet access device is secured by a SSL/TLS connection this kind of attack is marginally important. But there is the possibility that an attacker can manipulate the configuration of the local infrastructure to accept a self created SSL certificate and to connect to his webserver whenever a specific IP address is called. In this case the attacker becomes an impostor. He deviates the whole traffic to run through his machine and acts as a so called Man-in-the-Middle (see below).

2.2.3 Attacks against the user Internet access device

The most vulnerable zone in the channel is the user Internet access device and the local infrastructure of the user. Personal computers are often insufficiently protected against new types of malware. In addition local users are subject to social engineering attacks that may support the installation of malware at different levels of the local operating system, the Internet applications or even in HW device drivers. Identity theft, MITM (Man-in-the-Middle) and session hijacking attacks most often happen at

this level. There is a last but very important weak point in the end-to-end communication which is the authentication of the user itself. A simple UserID/PW authentication is highly insecure. New 2- or 3- factor authentication should be in place to protect from impostor attacks.

2.2.4 Insider attack

An insidious attack is the so called insider attack. A legitimate user for instance may run an E-commerce process and later he may deny that he had done so. This kind of cheating undermines the trust in E-business relations and it is very harmful for a proper functioning of E-business relations. It only works if the user can create reasonable doubt that he was not the author of a certain transaction. If the transactions are secured through provable and auditable mechanisms such attacks become ineffective.

2.2.5 Identity theft

The above briefly discussed attacks are only a strongly reduced summary of the threats to the end-to-end communication channel. But they already illustrate the huge task to provide real security in E-business and especially in E-commerce relations. There is an almost unforeseeable zoo of known and still to be discovered attacks on the complex IT communication infrastructure. The most dangerous ones for the further E-business development are the identity theft attacks. Today these kinds of attacks are already predominant and cause high damage to individuals and the economy [15]. Therefore we concentrate our further discussion on identity theft related attacks. Other threats like online extortion or protection code cracking are not covered in the further discussion.

3 Security requests for e-business

Security means that all the threats have to be disabled up to a certain level of remaining and acceptable risks. To improve the security situation of E-business transactions a set of security requests have to be fulfilled and the corresponding protective measures must be integrated in the ICT infrastructure [7].

3.1 Authentication

Probably the most important security problem to solve in the digital economy is the authentication of the business partners. Authentication in a transaction setting means that both partners can prove to each other that they have the identity under which they have addressed each other. Very often the authentication process is a mutual authentication between two Internet access devices with the assumption that the physical or legal persons using the corresponding computers have been authenticated beforehand locally (e.g. SSO solutions). In a typical E-commerce setting however the machine authentication is not sufficient. The value service requesting person has to deliver some additional identity credential to authenticate her at some point in the

transaction process. There are three basic concepts called authentication factors that can be used for the identity verification of a person

- Proof that the person knows a secret
- Proof that the person has a personal token
- Proof that a person has a certain biometrics

The three concepts are used alone or in combination to construct an identity credential that can be delivered by the person. The factors also serve to qualify the strength of identity verification. 1-factor systems based on the knowledge of a password or PIN-Code are still the most common but the least secure authentication method. Many institutions now move to 2- or 3-factors systems that are considered to be sufficiently secure by the extranet access management community. The drawback of such multifactor or multimodal[1] authentication schemes is that they are more expensive and complex to deploy and often costly to operate. 3-factors systems all incorporate biometrics. They have the advantage that a negative proof becomes possible e.g. the proof that a certain person is not the one she claims to be.

Fig. 4. The verification of the correct assignment of a digital (partial) identity to the physical (or legal) person is a weak point in all security systems. There are three different concepts (called factors) to establish a link between a physical person and its digital identity.

Closely related to the authentication problem of person is the authentication of machines and messages. One needs the guarantee that only the assumed sender has created a certain message. This can be achieved through a digital signing of messages with a secret key that can only be used by the authorized person or network entity.

3.2 Privacy and anonymity

The complementary request to authentication is the need for privacy and anonymity. Nobody wants to be completely transparent for any alien persons or organizations. Therefore persons tend to disclose as little as possible about their identity when they enter in a simple business relationship. This need for privacy is naturally transaction dependent. Nobody cares that the neighboring bakery knows what kind of bread he or she is consuming. But people certainly like to remain anonymous if they access an adult service. On the other side there may be a substantial commercial interest to

[1] A multimodal authentication credential includes several proofs of the same concept type e.g. different biometric qualities.

break the anonymity of consumers and to profile their habitudes for marketing or even criminal purposes. There are methods available that allow anonymity without losing trust in the existence of a correct identity of the business partner [8]. The below presented personal identity management assistant from AXSionics also provides mechanisms to protect the card holder from profiling attacks. The AXS-Authentication System delivers to each business partner unique trusted credentials for its identity which can not be linked one to the other by a third party without additional information.

3.3 Integrity and freshness

To know the origin of a message is not sufficient. It is equally important that the message was not altered afterwards by any attacker. The validity and the actuality of the exchanged messages within a transaction context is a further security request. This requirement leads to the notion of data integrity. The assurance of data integrity is an important part of an E-commerce transaction as it is the basis of the trust both parties will have in the transaction contract. Data integrity is threatened in various forms. Intentionally or unintentionally a message or a document may be changed on the way from the sender to the receiver. This is especially true if the communication channel includes a communication over a larger time gap with an intermediate storage of the data. Especially with non symbolic data (pictures, sound tracks etc) the question if data is unaltered may often be difficult to answer. Data integrity can be protected by checksums or hash codes which are mathematical or cryptographic transformations of the original data. Such codes accompany the original data as so called digital fingerprints.

A special quality of a message is the freshness. A message is often linked to some context and it could mean something completely different if the same message is exchanged in an other context. Freshness means that there is some guarantee that a message has been generated and received in a special actual context. This can be achieved by a time stamp, if the messages are exchanged over a permanent channel, or by a unique identifier that is added to the digital fingerprint of the message.

3.4 Confidentiality

The basic information security goals are confidentiality, integrity and availability. Often information security is identified with confidentiality alone although this is just one of the security goals that can be achieved by protective measures like cryptography. Confidentiality is always necessary when valuable data are implied. This can be a credit card number but also data on a persons health condition or a trade secret of a company. Almost in all business relations there are numerous information that have to remain confidential in between a restricted group. Today in any research project with some commercial interest the partners have to sign a so called non disclosure agreement. The purpose is to protect know-how or intellectual property from disclosure to third parties and urges the partner to protect the confidentiality of

the common data. The protection of secrets is the classic origin of cryptographic technologies. It is vital for military forces, governments, competing corporation but it may also be important for individuals. Confidentiality is a key issue to protect the privacy of a person. The usual way to achieve confidentiality of critical data is to encrypt such data. This reduces the need for physical protective measures for the whole data library to the need for the protection of the encryption key which in general is much smaller and easier to lock. But the breaking of the key is still a security risk that can never be completely eliminated. There are other methods to keep confidentiality of data like steganography [9] or scrambling [10]. But these methods do not allow a mathematical estimation of the remaining disclosure risk and are therefore seldom used in business applications.

3.5 Non repudiation, accountability and auditing

In E-business relations with high value transactions it is important that some additional security request have to be integrated in the underlying security scheme. It is certainly a need that neither party can deny to have agreed on the contract after the conclusion of a transaction. Therefore it must be possible to prove that the mutual transaction confirmations have really been intentionally submitted by both parties and no party had the possibility to alter the content afterwards. For this the exchanged messages need a non reputable proof that the sending party really meant what has been agreed and the receiving party accepted the message content. Such a prove may be delivered through a so called digital signature of a document. Such a signature can be provided by a business partner that has a private signature key and a certificate for the corresponding public key. The authenticity of the certificate has to be guaranteed by a trusted third party [11]. The digital signature consist of a footprint of the document encrypted with the private key of the contract signing party and the corresponding certificate contains the public key for the signature verification and the certified link to an registered identity. This non repudiation quality of a transaction system relies on two underlying security concepts. Persons are accountable for their acts. This means that the system can resolve the true identity of the transaction partners and it must be possible to proof that the system worked correctly in the specific case. This means that the correct working of a system can be verified at a later moment (auditability).

3.6 Availability

The last but not least security request is the availability of a service and the necessary communication channel to execute a transaction in the context of this service. To secure the availability always a combination of logical and physical actions are necessary. Attacks against the availability of a system undermine the trust of the transaction partners in the reliability of the system and can cause huge damage to the operator of the system.

4 The business case for cybercrimes

If we speak about criminals that move in the business of Internet fraud we have to understand their motivation. The basic explanation is given by the Willie Sutton's law [18]. The Internet today is a place where people can win and loose a lot of real money. For organized crime the cyberspace is therefore attractive. The winning perspectives are now as high as in the narcotic trade scene [19,20] and the risks to get shot are much lower. The times of the romantic hacker are definitely gone. Today's attackers intend identity theft, fraud, scam, money laundering, extortion, intellectual property and brand theft, political damage, inflicting a loss to a concurrent or ambush marketing.

4.1 Figures and facts about online fraud and phishing

There are overall statistics on the number of phishing attacks [21] and numerous compilations for losses due to Internet fraud and identity theft [3,4,22]. Typically there are 20-30 thousand phishing attacks per month all over the world and the success rate varies from less than one per mille to a few percent in the case of very sophisticated attacks. The targets of such attacks are now predominant in the financial industry. Identity theft is the most prominent form of fraud in the Internet [30]. In the US identity theft touches up to 7 % of the online banking users with an average reported loss of 1200$ [20]. For Europe similar numbers are reported [23].

4.2 How phishing works

Phishing is a method to conduct an identity theft. Let's have a closer look on a phishing attack on a banking institution.

4.2.1 Money Mules

In a first step the attacker has to prepare the environment for the collection of the stolen money. For this he needs so called money mules. These are legitimate holders of a bank account at the targeted institution or in the vicinity of it. The attacker sends out hiring e-mails offering an easy auxiliary income for people that have a bank account and are willing to make occasionally some transactions. Individuals that believe this offer get a phony contract with some offshore financial institution with the duty to transfer received money within a short time to a foreign place using a money transfer institution like Western Union.

4.2.2 Fake Web site

In a further preparation step the attacker creates a web page that looks like a legitimate web page of the targeted institution. He then sends e-mails that look like an e-mail coming from the targeted company to a large amount of Internet users. In the e-mail the attacker asks the receiver to update his identity credentials of the targeted institution for some security reason and provides a wrong link to his fake web page.

Some of the addressed users have indeed an account at the targeted institutions and connect bona fide to the fake site. There the attacker asks for the actual credentials for the original bank account contract. With the stolen credentials the attacker has access to the user's bank account and is able to make transactions in his name. Such a phishing attack was made recently on the Scandinavian Nordea bank and caused a loss of € 1 million within a week [4]. A variant of such an attack with an online use of the stolen credentials was tried against the US Citibank fooling even their 2-factor authentication system [24]. Not all phishing attacks are so successful but even with a much lower return on investment they are still profitable (see below).

4.2.3 Channel breaking MITM

In a more sophisticated scenario the attacker just attracts the legitimate users on a web site and installs a trapdoor Trojan (drive-by-infection) that allows the attacker to redirect all future sessions of the user with the bank institution's home page to a server that is under the attacker's control. He then installs a botnet and redirects the infected users to different nodes of his botnet. For the bank such a scenario looks like different independent normal E-banking users logging in from many different sites. Defensive traffic profiling programs of the bank will not register an unusual situation. The advantage of such an online channel breaking MITM attack is evident. The attacker does not need to steal the credentials the user will submit the real credentials at the begin of the session. He just modifies the transaction content in the background when the user tries to make his own online banking. Few such attacks have already been observed in the wild [25]. They can not be defeated by any of the traditional authentication or transaction security systems. The sole countermeasure is to confirm the transactions over a secure and trusted communication channel (see below).

4.2.4 Getting the money out from the financial system

Making a fake money transaction is not beneficial yet. If detected in time the transfer may be cancelled by the bank. Therefore the attacker needs the money mules that provide their ordinary bank account to receive the fraudulent transaction money. Once the money is on the account the naive helper has to go to the bank institution and take the money out. The money mule then takes his commission and sends the rest to the attacker who generally resides in a foreign country with an inefficient law enforcement system. The money mule will not be happy with his commission for a long time. As soon as the fake transmission is detected the bank will withdraw the full transferred amount from his account. In addition the money mule risks charges for money laundering. In the whole system the money mule is the person that suffers real losses. The hiring of new money mules is today's bottleneck for the attacker community. If the attackers find new ways to get the money out of the system the losses from identity theft online fraud may escalate.

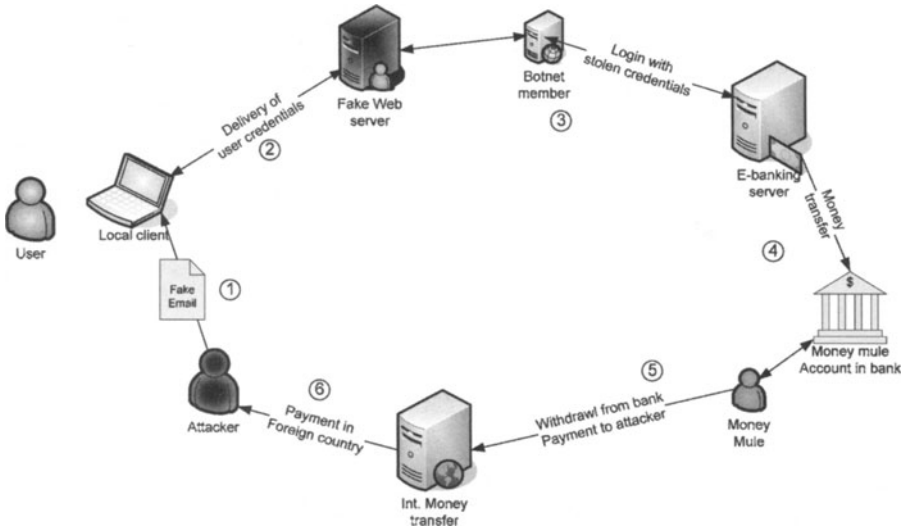

Fig. 5. Running of a phishing attack: 1. The attacker starts the process with the distribution of a phishing Email that draws the user to the fake webserver. 2. The fake webserver simulates a credible scenario of the targeted bank and extracts the authentication credentials from the user. 3 The credentials are used to access the user's bank account, most often from distributed nodes within a botnet. 4. The attacker transfers money to one of the money mule's account. 5. The money mule withdraws the transferred money and sends it via international money transfer (e.g. Western Union) to the attacking organisation (often in a country with inefficient law enforcement). 6 The attacker gets the stolen cash at his place.

4.3 Limitations and countermeasures

Classical offline phishing attacks can be averted by challenge response protocols for the user authentication or time dependent credentials that are only valid for a short time. The online MITM attacks can't be defeated with the sole authentication of user. The attacker just forwards the true authentication messages between user and bank operator without any intervention. He interferes only later with the exchanged messages and changes some transaction parameters. To get in such a MITM position the attacker has to insert himself in the encrypted communication channel (usually communications between a user and an operator run over an SSL/TLS connection). For this he has two possibilities. He may simultaneously establish a SSL/TLS connection to the bank and to the user simulating against both sides to be the expected communication partner or he can install a Trojan program on the local terminal of the user that acts as a MITM after the end of the SSL/TLS encrypted channel. The first attack can be avoided by the installation of a VPN connection between operator and user based on mutual and trusted certificates (e.g. on a smart card). The second attack is more difficult to counter. The user can't trust his local machine and needs an independent communication with the operator to discover such an attack or he must be capable to create a transaction dependent TAN number that can not be influenced

by the attacker. This needs to be done in a physical independent device with an own secure processing capability.

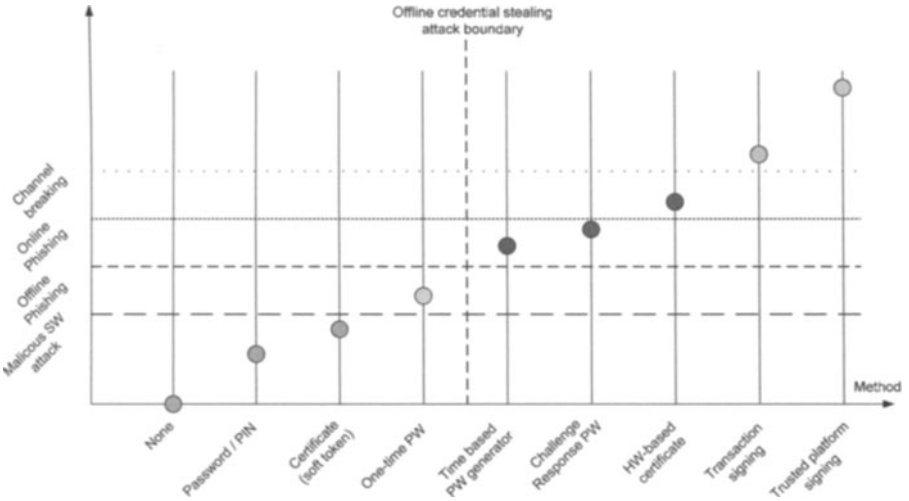

Fig. 6. Internet authentication and transaction security methods qualitatively ordered according their security level. The dashed horizontal lines show the minimum level of security to defeat a certain attack method. The dashed vertical line separates the methods which are vulnerable to classical offline phishing (left side) from the ones which can not be defeated by classical phishing (scheme adapted from [26]).

4.4 The business case

To better understand the attackers we need a closer look at the financial outcome of an average successful phishing attack. As explained above the market of malware production and distribution has reached a certain level of maturity. There is an established task sharing between developers of crimeware, programmers of fake web sites, collectors of valid e-mail addresses, managers of botnets, money mule hiring agencies and the organized crime as attack coordinator and investor.

An attacker can purchase almost all necessary tools and support service for his attack over the Internet at moderate prices. The main problem of the whole attack scenario is the question how to get hold of the money of the deviated transactions. For this the attacker has to find and hire money mules that provide their bank account for the reception of the fake fund transfer and that are willing to pick up the money in cash from the bank and forward it to the foreign receiver. In general a commission of 10 – 30 % is offered to money mules, which makes this part the most cost intensive item for the attacker. The revenue comes from the successful deviated transactions. On the average the single amount of such a transaction is in the range of a few hundred to a few thousand dollars. Higher values are unlikely to pass the banks fraud monitoring system. A phishing attack targets a few 10k to 100k Internet users. Only a small fraction of them have a business contact with the targeted bank and within this

group only a few will fall In on the phishing attack. The attacker may end up with a few dozens to a few hundred successful deviated transactions which gives him total revenue in the range of $50 to $100 thousand dollars. After paying all furnishers and the money mules he remains still with a net benefice which is a multiple of the investment. This interesting business case combined with the very low risk to get caught by the police makes phishing a very lucrative business.

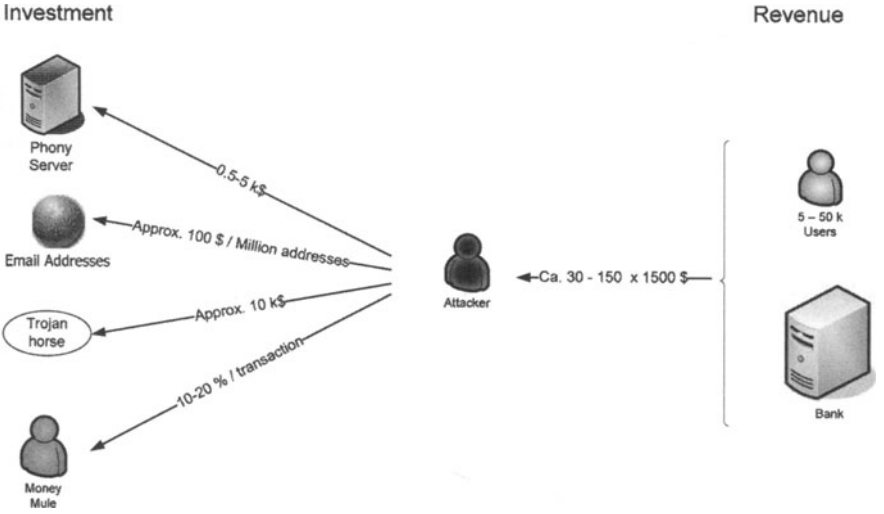

Fig. 7. An attacker has to invest for the crimeware and the customisation of the fake web site approx. $10 to $20 thousand depending on the quality of the tools. In addition he needs e-mail addresses with a good coverage of the targeted user population. All these components for an attack are available on specialised sites of the Internet. The most difficult part is the hiring of the money mules. It is a lengthy and costly process to hire persons with the wished bank connection who believe in the suspicious offer.

5 The secure channel approach

The effective loss and damage caused by cyber criminals is only one side of the medal. On the other side are the investments and costs for the security technology and their operation and the loss of confidence and trust in the E-business market. Operators have to add to the lost money of fake transactions the security bill and the loss of not realized business cases due to a growing lack of trust of the consumers or merchants. Actually the total worldwide cost for extranet access security technology is estimated to exceed $500 million per year and the rate of refused transactions due to security considerations is in the US between 6 % (domestic) and 13 % (foreign) [20,22]. The attackers in general have a leading edge on the defenders as long as the defenders just try to repair the detected weakest spots in the communication channels and the E-business protocols. Continuing in this way the arms race in the cyberspace

will continue and the related costs will rise the confidence of the users will decline with a serious risk to damage the whole E-economy.

5.1 Dedicated trusted platform

There is however a quite radical concept that defeats most of the actual attacking tools and bans the dominating threats to the Internet access device of the user. The idea is to bridge the most insecure components of the communication infrastructure and install a direct uninterrupted communication channel from the secure zone of the operator directly in a dedicated secure data terminal of the user.

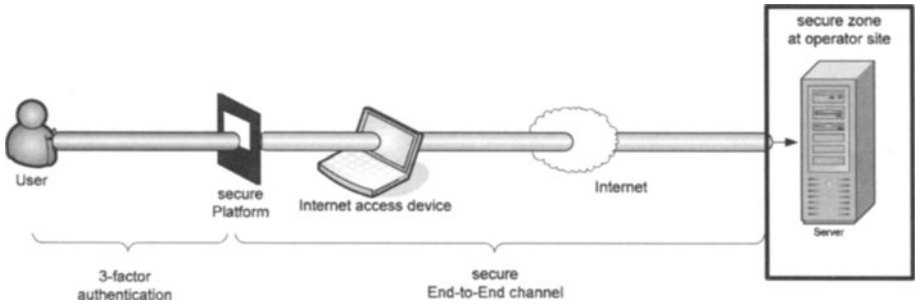

Fig. 8. The AXS-Authentication System provides a secure and tamper resistant communication channel between the operator and the personal AXS-Card of the user. The AXS- Card also verifies the identity of the owner of the token with a strong authentication protocol.

Any real secure digital system has to build up its security onto a tamper resistant hardware platform. Pure software solutions will never guarantee a strong anchor for the security measures. One approach for the realization of this idea is the so called Trusted Computing (TC) technology which is propagated by the Trusted Computing Group [27]. It is a concept that allows a certain degree of control of the hardware and software running in a computer. Although this technology is probably efficient against most of the malware attacks it is strongly disputed by privacy defending organizations. Another drawback of this technology is its limited flexibility for configuration changes that are approved by the authorized user. For real world applications it turns out that a PC system is often too complex to be controlled efficiently. TC is therefore not (yet) adapted for the home computing domain. We propose a different approach that combines the advantage of the TC technology with the requests for an easy accessible and privacy respecting computing for everybody. In fact secure transactions are needed only within a tiny fraction of our Internet activities. We therefore propose to create a secure end-to-end channel between the user and the service operator introducing a dedicated simple device that is linked but not integrated in the insecure local computing system. This personal trusted transaction assistant runs on every computer without any local installation whenever a secure communication is necessary. It assures secure transactions even over completely corrupted systems and tampered Internet connections. An attacker has no chance to enter in the strongly protected private end-to-end channel. The fact that the

user needs an additional device for the security operation is even beneficial. It underlines the special situation of a secure and trusted transaction and makes the user more alert and vigilante.

5.2 The AXS-Authentication System

The AXS Authentication System™ (AXS-AS) [28] provides a secure channel between the protected zone of the operator and a dedicated tamper resistant personal device in form of a thick smart card.

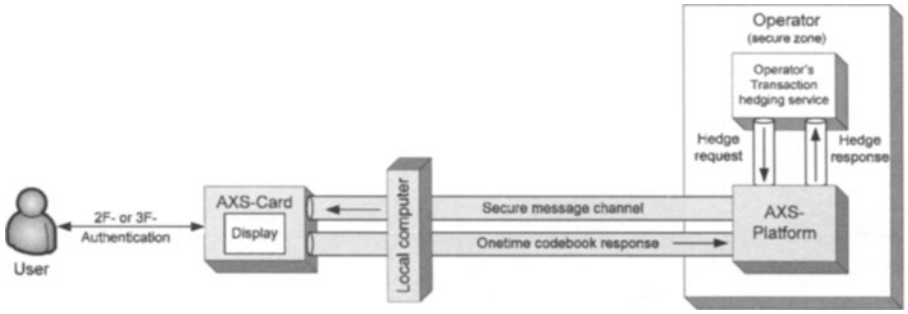

Fig. 9. The AXS-AS establish a secure ad hoc communication channel from the secure zone of the operator with the AXS-Platform into the personal AXS-Card. The message together with the possible response codes is only visible to the user on the integrated display of the AXS-Card. The local computer serves only as a transmission relay for the encrypted messages. The AXS-Card authenticates its user before it shows the message to him.

The device, called AXS-Card, is personalized to its owner and remains always in his possession. The AXS-Card contains numerous digital identity credentials that can be used to establish independent connections to different operators that run an AXS-AS. The AXS-Card controls the access to the credentials through a 2- or 3-factor authentication of the user.

The security level of the authentication protocol that verifies the identity of the card owner may be adapted according the transaction type on request of the operator. The biometric authentication factor is realised by an on-board fingerprint recognition system. On the highest security level the AXS-Card asks for a combination of biometrics and secret knowledge. For a normal authentication the user has just to present one of the enrolled fingerprint biometrics. There are two main differences relative to other token based authentication or transaction hedging systems.

5.2.1 Optical interface

The first and often surprising novelty is the way the token receives messages from the operator. The AXS-Platform, installed at the operators place, sends an encrypted message over any IT infrastructure to the screen display of the local computer. On the display appears a window with flickering fields in form of a stripe, a trapeze or a diamond. The user holds the activated AXS-Card directly on the display with the flickering window and the card reads the message over its optical interface. Only the authentic AXS-Card that was addressed by the operator can read and decrypt the

displayed flickering code. This one way communication channel is sufficient to transmit a one-time password, a transaction receipt, a voting list or any other kind of short document that is needed to hedge a transaction. The AXS-Card shows the user the message content on the internal display together with some one-time codes for the possible responses. The user returns the chosen one-time code over the keyboard to the operator. A potential attacker has no chance to interfere with this communication protocol as he will not know anything about the semantic meaning of the message or the return codes. This communication scheme needs no electrical or radio connection between the AXS-Card and the local computer and no local SW or HW infrastructure has to be installed. This makes the AXS-AS mobile, flexible and simple to roll out. Any computer that is connected to the Internet can be used to establish a secure channel between the operator and the user.

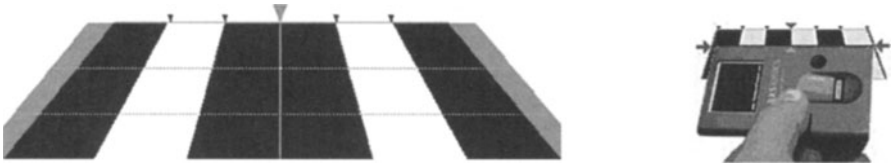

Fig. 10. The optical interface of the AXS-AS consist of a window that opens in the browser of the local computer. It shows flickering fields in the form of a trapeze. The user holds the AXS-Card directly on the flickering pattern on the computer display and receives the encrypted message from the operator. The local computer only serves as a transmission device and has no clue about the encrypted message.

5.2.2 User side identity federation

The second unique selling proposition is the identity credential management within the AXS-AS. Each AXS-Card contains a practically arbitrary number of secured channels that can be activated whenever necessary. The user decides which operators get access to the identity credentials in his AXS-Card. For this he submits a unique identifier (AXS-Card number) to the operator. The AXS-AS of the new operator and the AXS-Card of the user then allocate automatically a channel using predefined credentials for the new connection. The operator can modify the cryptographic parameters of the allocated channel in the AXS-Card already at the first message exchange. After this first registration step the allocated channel is controlled by the operator but the user decides to whom he wants to allocate the pre-initialized channels in his AXS-Card. This shared control of the communication channels allows a very flexible realization of identity federation. The trust is established and shared only between user and operator. No additional agreements between different operators or the sharing of identity information are necessary.

The advantage of such a personal identity management assistant is evident. Today a typical user of computer systems and Internet services has to memorize and manage over 50 UserIDs, passwords and PIN-codes. It is a well-known fact that users don't handle such identity credentials as valuable secrets. Users choose either simple passwords or simple rules to memorize passwords. Dictionary attacks can break most of such alleged password secrets within seconds [29]. To augment the authentication security operators move now to 2-factor authentication and distribute passive or active

tokens (cards, OTP-lists, time dependant pass code generators, digital certificates etc). The handling of all these physical and virtual identity credentials makes life not easier for their owner. Many Internet services are just not used any more because users forgot how to access the site. Users restrict their business relations to fewer operators which naturally reduces the business opportunities for E-commerce. While many systems offer identity management functions for operators the problem of the user side identity management remains unsolved. Operator arranged federated identity management (FIM) and single-sign-on (SSO) systems are ineffective to solve this problem. Both actions are taken on the wrong side of the user-operator relation. Only a user side identity management can handle the proliferation of identity credentials for the user. The AXS-Card assumes the administration of the multiple identity based relations of the typical E-business user.

5.2.3 Encapsulated biometrics

A further innovation of the AXS-AS is the way biometrics is implemented. The storage of the biometric reference template, the measurement and the comparison process are completely integrated in the AXS-Card. The card keeps the biometric data encapsulated under the full control of the owner. All the fears about irreversible corruption of biometric data become obsolete. The privacy of these data in the AXS-token is fully protected which differentiate the AXS-AS solution from most other biometric identification or verification systems. The operator only knows what kind of biometric processing is performed in the card.

First attempts in such a direction have been done with biometric reference templates on smart cards carried by the user or even cards with match-on-card functions. But a real secure and privacy protecting implementation of a biometric authentication puts all biometric data handling, including the measurement process, into the user's hand.

The shared control, biometric data controlled by the user and biometric processing controlled by the operator, allows mutual trust in the biometric identity verification and guarantees the necessary privacy and protection for the non revocable biometric data of the user. This type of shared control implementation of biometrics is recommended by the privacy protection community [30].

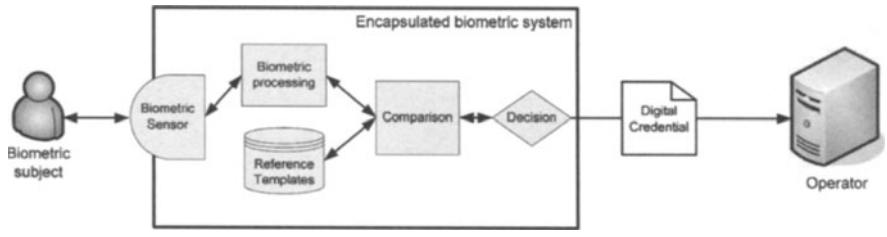

Fig. 11. In the AXS-AS all biometric processing and data are enclosed in the tamper resistant AXS-Card that remains in the possession of the user. The biometric data are encapsulated and protected in the secure processor memory of the device. Any outside instance gets only digital identity credentials with no information about the biometrics of the user. The biometric data are

controlled by the user and the way biometrics are processed and evaluated is defined and controlled by the operator.

5.3 End-to-end transaction security

The key element of the AXS-Authentication System is the AXS-Card. It is the platform over which a secured end-to-end communication can be established. Each message that is sent from the operator to the AXS-Card runs over a separate channel allocated to the specific operator – user relationship. The communication content is enveloped in a cryptographically secure message container. Its security mechanisms assure confidentiality, mutual authentication of the operator and the user, the freshness of the message and the correct display of the message on the internal screen of the card. The message also contains parameters that define the one-time response codes that the user may send back to the operator. There are protocols for different applications like onetime PW login, financial transaction hedging, voting, transaction signing, license checks, recovery of a previously stored secret and many more.

An important part of the security of such a mutual trusted communication platform is the initialization and roll out step. Special protocols make sure that only the authorized user can enroll his biometrics in the dedicated card and that only the authorized operator can take possession of one of the secured communication channels in the card. The AXS-Card can therefore be regarded as a secure container and reader of an almost arbitrary number of virtual smart cards that each operator has distributed in a secure way to the user. The advantage of the concept is the very high level of security achieved and the sharing of the infrastructure between operators without the need to establish connections and trust mechanisms between the different identity management systems.

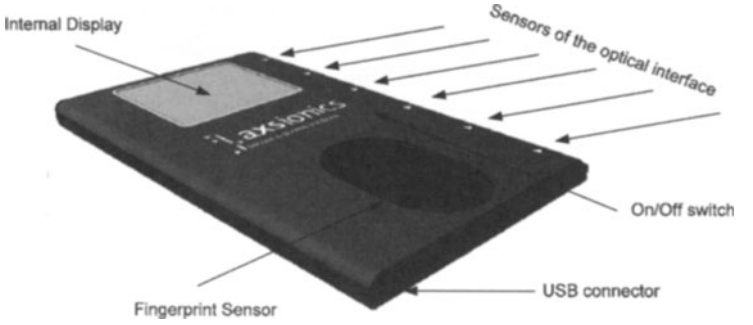

Fig. 12. The AXS-Card is the mutual controlled and mutual trusted device that allows a secure communication link between the operator and the user. All the typical security requests are realized and attackers have no possibility to make remote or automated attacks on such a system.

6 Conclusion

The E-business sector is forced to find a solution against the growing importance of Internet related crimes. The need to secure the communication between operators and users of a value service has been recognised on a broad scale [31]. However there is not yet a consensus about the way how to face this challenge. More or less all agree that the necessary secure channel needs some kind of additional infrastructure. There are communities which see the mobile phone and the SIM-Card as a carrier of this infrastructure [32], others see a solution in the Trusted Computing approach or in an extensive use of smart cards as identity credential [33]. On a longer time scale the community expects a convergence of the personal mobile communicator with an identity assistant. But independent of all the possible strategic technologies that the industry may develop and roll out on a large scale in the future, immediate efficient solutions are requested now. The presented AXS-Authentication System has the potential to defeat most of the actual MITM and identity theft attacks on financial services. It could become the requested secure platform that runs already on the present IT-infrastructure.

References

1. The Digital Economy Fact Book, 8.ed, The Progress ¬ Freedom Foundation, 2006;
2. Europe's eCommerce Forecast:2006 to 2011, Jaap Favier, Forester Research, 2006
3. Identity theft: A new frontier for hackers and cybercrime, Claudio Cilli, Information Systems Control Journal, 6, 2005Online fraud costs $2.6 billion this year, B. Sullivan, 2007 MSNBC.com, http://www.msnbc.msn.com
4. The Scandinavian bank Nordea equipped with a two-factor authentication system was victim of a malware MITM attack: http://www.nytimes.com/2007/01/25 /technology/25hack.html?ex=1327381200&en=58990497ce27b2b2&ei=5088&partner=rss nyt&emc=rss (visible 18.07.2007). A similar attack on the Nederlands ABN Amro bank was also successful: http://www.theregister.co.uk/2007/04/19/phishing_evades_ two-.factor_authentication/ (visible 18.07.2007)
5. Access Control Technologies and Market, Forecast 2007, RNCOS online Business research; http:/www-the-infoshop.com (visible 4.11.07)
6. Thursday's security tip 2/2/06, The Infopro Corp; www.theinfopro.net
7. An Introduction to Information, Network and Internet Security, The security practioner; http://security.practionier.com/introduction/infosec_2.htm
8. PRIME – Privacy and Identity Management for Europe; https:www.prime-project.eu FIDIS – Future of Identity in the Information Society; http://www.fidis.net

9. Hede and Seek: An Introduction to Steganography; N.Provos and P.Honeyman; IEEE Security and Privacy, May/june 2003; http://computer.org/security/
10. Data Scrambling Issues; White Paper; Net 2000 Ltd. http://www.datamasker.com/datascramblingissues.pdf
11. Introduction to Public Key Technology and the Federal PKI Infrastructure; NIST pub. SP800-32; 26.2.2001. See also on wikipedia: http://en.wikipedia.org/wiki/Public_key _infrastructure
12. Melani report, Informationssicherung, Lage in der Schweiz und international, 2007/1; ISB, Schweiz. Eidgenossenschaft
13. Secrets & Lies; B. Schneier; Wiley Computer Publishing, J. Wiley ¬ Sons, Inc., ISBN 0-471-25311-1
14. Identity Fraud Trends and Patterns; G.Gordon et al.; Center for Identity Management and Information Protection, Utica College- cimip US Dept. of Homeland Security
15. ID-Theft: Fraudster Techniques for Personal Data collection, the related digital evidence and investigation issues; Th. Tryfonas et al.; Onlinejournal, ISACA, 2006
16. Web server exploit Mpack: http://reviews .cnet.com/4520-3513 7-6745285-.html
17. At least 45.7 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the TJX Cos. at its headquarters in Framingham and in the United Kingdom (discounter that operates the T.J. Maxx and Marshalls chains) over a period of several years, making it the biggest breach of personal data ever reported; see also:http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/ (visible 8.11.07)
18. Willie Sutton's law: The law is named after the bank robber Willie Sutton, who supposedly answered a reporter inquiring why he robbed banks by saying "because that's where the money is".
19. Organized Crime and Cyber-Crime, P. Williams, CERT Coordination Center, preprint (visible 10.11.07):http://www.crime-research.org/library/Cybercrime.htm
20. McAfee North America Criminology Report: Organized Crime and the Internet 2007, McAfee Inc.
21. Phising Activity Trends, monthly report, 5/07; Anti Phishing Working group – APWG: http://www.antphising.org
22. Consumer Fraud and Identity theft, complaint data, FTC-report, Jan 2006, http://www.ftc.gov
23. Security report online Identity theft, Feb 2006; http://www.btplc.com/onlineidtheft/onlineidtheft.pdf
24. Washington Post Online (visible 10.11.07): http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html
25. Private communication, Security officer of a international bank (source remains confidential)
26. Secure Internet Banking Authentication, A. Hiltgen, Th. Kramp, Th. Weigold; IEEE Security & Privacy, March/April 2006
27. Trusted Computing Group; http://www.trustedcomputinggroup.org/home
28. AXSionics homepage: http://www.axsionics.ch
29. MySpace Passwords aren't so dumb, Bruce Schneier, in Wired, 14.12.06 http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300
30. Biometrics in identity management, FIDIS EU-NoE FP6; D3.10; (to be published), http://www.fidis.net
31. Information Security is falling short, it is time to change the game; A. Coviello, Keynote speech at the RSA Conference Europe 2007, London

32. The smart and secure world in 2020, J. Seneca, Eurosmart Conference, 2007
33. Establishing a uniform identity credential on a national scale; Bearing Point White Paper and Protecting future large polymorphic networked infrastructure; D. Purdy, US solution for a national governemental electronic ID-Card; presented at the World e-ID conference in Sophia Antipolis, Sep. 2007