Distribution of Risks in Implementations of Digital Signatures

Arnd Weber[1]

Secure Orders over the Internet using Digital Signatures

Currently, an increase in electronic commerce over open systems can be observed. For this purpose personal computers which are connected to the Internet are used to transmit orders to sellers, or banks (see BHKL_96, Horn_96). Broad-based discussion is taking place as to whether these contracts should be digitally signed by the person placing the order. This would achieve multi-party security to the extent that the recipient of the order could only demand payment from the person placing the order if he could prove that neither he nor deceitful employees of his company had placed the order in question. In the following there will be a discussion of how the signature procedure can be implemented in such a way that the signatory can trust his device, or be certain that it cannot be manipulated by other persons. In this respect it is irrelevant whether the signature is to be added to an offer, an order, or a contract which has been signed by both parties. In order to simplify things, in the following only the case of a buyer signing an order to a seller will be treated.

Assignment of Liability for Signature Systems Without Secure Devices

The suggestion that the signature procedure should be implemented on the software of the user's PC is widespread. There is the possible alternative of storing the signature key, or signature procedure itself, on a chip card which is inserted in a chip card reader in the personal computer. A further variant is that a chip is put between the PC, the keyboard and another interface so that this chip can check whether the keyboard input is consistent with the content of the document to be signed (Bugo_96). With all these procedures there is a danger that Trojan horses may lead to forged signatures. Software which is installed in the PC may contain a Trojan horse which manipulates the signature software. In the case of

---

[1] This paper is based, together with other material, on expert interviews made for the EU-project SEMPER (Secure Electronic Marketplace for Europe), but it is the author's interpretation of the findings (see ACTS-project AC 026 of the European Union <www.semper.org>). The author wishes to express his thanks to interviewees and to the colleagues in the project and at Institut für Informatik und Gesellschaft of Albert-Ludwigs-Universität Freiburg im Breisgau who contributed valuable input to this paper, in particular Herbert Damker and Michael Waidner. An overview over project SEMPER is given by Waidner (Waid_96). A similar, but larger text will be published as „Zur Notwendigkeit sicherer Implementation digitaler Signaturen in offenen Systemen“ in: Müller, Günter; Pfitzmann, Andreas (eds.): Mehrseitige Sicherheit in der Kommunikationstechnik. Vertrauen in Technik durch Technik. Bonn 1997. SEMPER identifier: 111FR023.DOC (7.10.1997)

implementation by means of a chip card this Trojan horse can only have an effect as long as the chip card is inserted in the computer. In this case the risk is reduced, but not eliminated. With chips which call up information via the keyboard there is the risk that the Trojan horse manipulates the output on the computer screen. With all of these implementation procedures there is the risk that an incorrectly displayed text of the contract sent by the seller is accepted by the buyer. If the use of a secure chip has been neglected it is possible for completely falsified security software to be distributed or for the interface of the security software to be feigned in the browser window during automated sales on the World Wide Web.

The German digital signature law, being in force since August 1, 1997, requires:

> "For the creation and storage of signature keys, as well as the creation and verification of digital signatures technical components with security precautions are necessary which make forgeries of digital signatures and the falsification of signed data reliably visible and provide protection against the unauthorised use of private signature keys." (German Law for Digital Signatures, § 14, Section 1.)

Therefore, secure implementation is required.[2] Other actors have considered making a cost-benefit analysis of measures for the prevention of forged digital signatures. The American Bar Association, for example, distinguishes between various degrees of system security and, indirectly, takes a position which is opposed to the very secure implementation of all signature processes. Trustworthy systems should only be "reasonably secure from intrusion and misuse" (ABAs_96, p. 54).

> „The determination whether a particular system is 'reasonably secure,' should be based on the following considerations:
>
> - whether more secure or reliable systems and practices are available and feasible, and
> - if such systems and practices are feasible and available, the cost of providing the higher level of assurance balanced against the seriousness of the risk incurred by forgoing the higher level of assurance" (ABAs_96, p. 56)[3]

In a different section the American Bar Association writes that digital signatures will be enforceable, just as traditional signatures are:

> „A message bearing a digital signature verified by the public key listed in a valid certificate is as valid, effective, and enforceable as if the message had been written on paper." (ABAs_96, p. 82)

As a result there is a risk that one will be held liable, even if only a moderately secure implementation has been used. In the following the risks of implementation without secure input and output will be discussed and consequences suggested. Various experts were interviewed within the framework of the project SEMPER.[4] These interviews confirmed that there is a risk of systems being threatened by

[2] The draft of a regulation, however, states that such secure components shall only be used „as required" („nach Bedarf", see § 16 of SigV). Also extensions of PC operating systems are being discussed for providing secure output.

[3] The American Bar Association is referring here to Ford (Ford_94). Ford assumes that future chip cards will have a keyboard (Ford_94, S. 127). Judging from personal experience such keyboards cannot be used in practice because they are too small, and also, according to expert opinion, such cards with a thickness of .76 mms (banking standard) are not robust enough. In addition, Ford does not to take into account that without a display you do not see what you are authorising.

[4] The expert interviews have already been evaluated partially for Baert et al. (BHKL_96). For this paper additional expert interviews with security experts from Germany, Switzerland and the USA were conducted.

Trojan horses. As early as 1994 Roßnagel et al. (Roßn_94) illustrated that simple signature systems employing chip cards could be manipulated by third parties at the operating system level, e.g. that other data could be signed than the data which is displayed. More complex systems make this type of attack more difficult, but according to experts in the field, they do not make it impossible. As a result, it can be assumed that the users of these types of systems will have a duty to keep their systems free of untrustworthy software. According to one expert interviewed:

> "The customer himself will be responsible for ensuring that his means of access is kept secure."

A similar reaction is found in the VeriSign Certification Practice Statement of 1996:

> „each ... subscriber (is) responsible for protecting his, her or its private key(s) from compromise, loss, disclosure, modification, or unauthorized use" (Veri_96, p. 34)

One could advise the user to refrain from installing software which might, among other things, contain a Trojan horse, or even make this a requirement of the general conditions of sale. For users of the Internet, however, this would appear to be divorced from reality and would place considerable limitations on the use of a personal computer. First of all, users frequently download data from the net. Secondly, users frequently have to obtain updates of various programs. A large number of programmers are involved in producing these updates, which creates a potential security weakness. Thirdly, the reality of the matter is that users also install a variety of software from diskettes or CDs of which they cannot practically be convinced of the security. It is also too much to ask of the user to forego the use of updates or new software, as this is part of normal usage of a personal computer nowadays. The danger becomes even greater if users regularly obtain small programs from the Web which implement tasks independently, such as Java applets, or ActiveX-components (see also <www.iks-jena.de/mitarb/lutz/security/ activex.html>). In such cases digital signatures under the programs can only offer limited assistance, as it is impossible to be convinced of the integrity of the numerous programmers throughout the world who are involved in their development.

The degree of effort required for such attacks depends on the implementation and, thus, no general estimation can be made regarding the costs of such efforts. One of the security experts interviewed maintained that only a few days effort would be required to manipulate a chipcard-based homebanking system if the computer is connected to the Internet. Another maintained that "the threats have not yet been convincingly and comprehensively analysed". Yet another expert pointed out that Trojan horses are particularly easy for insiders to distribute, by software distributors, or installation and maintenance personnel. A white paper from the US American APSON (Advanced Payment Systems for Open networks) group came to a similar conclusion in 1995, i.e. that "protected devices" are required:

> "Protected devices encompass more than the card/token but include reader/keyboard (I/O) as well. This is to prevent Trojan horse attacks for input and interfacing the protected device." (APSO_95, p. 7)

A distinction should be made between the various opportunities for manipulation, i.e. between those aimed at profit and those only intended to disturb or to damage someone's reputation. It is relatively easy for a deceiver to entice any number of previously unknown users to install damaging software (by offering information to download, or distributing CDs or diskettes). In individual cases the damages may be easy to remedy, e.g. the distributor may agree to take back orders which have been deceptively placed, or a bank may cancel a money transfer. With the delivery of information, however, the supplier will seldom be prepared to accept a "returned" delivery and neither will the banks necessarily be prepared to cancel money transfers as the recipient may already have spent the money. In addition, it is unclear whether or not the creditor will actually be prepared to annul the transaction where, apparently, an order exists and the creditor can scarcely distinguish between a security attack and simple reluctance to pay.

According to experts it will be more difficult to damage *particular* individuals. However, should this become possible it is conceivable that individual users could be specifically deceived at different times and in different places so that the user would have considerable difficulty in making the damages believable.

Some types of attacks can be made more difficult if at the end of a session all of the signed transactions are displayed once again before they are sent. It can be assumed that a display of this type would make manipulation more difficult, but would not completely eliminate the possibility.

There are further conditions for the secure implementation of signature procedures, such as the generation of keys by the signatory and unambiguous registration of the signatory. Basically, it is sensible for the signatory himself to generate his signature key in order to eliminate from the onset the possibility of another party having the key. The exact way in which registration should be carried out is the subject of various discussions in the literature and is, to a certain extent, dependent on the extent to which the resident registration office, or existing bank connections, or a telephone call-back can be used. These debates will not be treated here, due to the fact that there is apparently consensus regarding the fact that liability can only be an issue if identity has been verified beyond a doubt (see BHKL_96).

Suggestion for the Assignment of Liability

The seller has the primary advantage of a legally binding signature. For this reason it is also the sellers, or banks which are promoting digital signature procedures. For reasons of fairness, therefore, the seller should not impose the risk of being made the victim of forged signatures on the buyer. Signature laws, or certification practice statements could be the place to establish that:

- secure implementation (secure creation of signatures with secure input and output) = liability
- lack of secure implementation = no liability

Consequently, the signatory should also be liable for his signature (non-repudiation) if he has complete control over all of the devices required for implementing it and has good reason to trust these. At least for private users it will be attractive to limit the risk to some monthly amount in order to deal with the possibility that they may lose control over their device or passphrase.

An alternative might be that the seller assumes the risk of Trojan horses, as long as the damages cost less than equipping his customers with secure hardware. This solution, however, appears to be unsuitable, due to the fact that either the seller has to give every customer who maintains he has been the victim of a Trojan horse the benefit of the doubt, or leave the decision as to whether the contract will be annulled or treated as valid up to the discretion of the employee handling the case. The latter is unfair to the customer who is generally the economically weaker partner is such a transaction. A question which arises is whether or not the risk could be insured against. In this case the question arises as to how the insurer should decide whether the case involves deception on the part of a third party, or if the customer is simply unwilling to pay. In other words, the problem is only passed on. Yet another possibility is limiting the risk to a maximum monthly turnover which can be freely selected. This requires the management of appropriate limits. If such a limit, however, were set at for a considerable sum, e.g. several thousand ECU per month, but no secure implementation is used, the risks would be large.

How Could the Distribution of Secure Devices Take Place?

Pfitzmann and others (PPSW_97) have discussed how such devices should be designed. It is, for example, sensible that the design of such devices should be varifiable and, in principle, they shouldn't be manufactured by parties which are to take part in a contract which will be concluded using the devices.

How could the diffusion of such devices take place? It can be assumed that such devices would either be fully new, or adapted from existing devices. For this reason it would be advisable to develop security software which can be used on a variety of devices.

- It is possible to use a special computer keyboard with display.
- If there is no requirement for the input of alphabetical characters and if a small display is sufficient, e.g. a GSM telephone, PCMCIA card or something similar could be used or adapted.
- Devices similar to palmtop computers could be used to securely input text, for example to create electronic cheques, or money transfers.[5]

It is essentially desirable for these types of devices to be small, so that the user can transport them easily, use them with different computers (at home, in the office, or when travelling) and that they are easy to lock up (for further information see PPSW_97). In addition, devices of this type could be used for storing the keys used to decode texts. Beyond this, it is advisable that they be equipped to manage various types of signatures, for example, for private use and business use. Devices which could be used in various combinations would be even more useful. An "electronic wallet" of this type could be equipped to handle the offline use of digital money and various currencies, e.g. display the currency of one's country of residence and ECUs (see the results of the project CAFE[6], BBCM_94, WCPS_95). In this case the device would contain a chip from the bank and transfer the money via the contactless interface. The device can also be used to check if payments being made with electronic money are, in fact, being conducted anonymously (Chau_89). Further, the device could also be used to secure credit card transactions and, thereby, reduce the current level of credit card fraud. Last, but not least, such a device is better suited for the storage of information than the chips in a customary card which are subject to extreme mechanical demands in purses and chip card reading devices. Surveys carried out in the CAFE project indicated that virtually nobody would sit on such a device. This raises the question of how men could carry it with them. It would be attractive if the device were thin enough for to be put in a traditional wallet or in a shirt pocket (see <www.uni-freiburg.de/<www.iig.uni-freiburg.de/~aweber/>). A device which is thin enough for this purpose could provide a number of functions if, in place of the

[5] Professional users who trust the security software and the operating system could perhaps reserve a normal computer for conducting business on the Web and could, therefore, keep it free of Trojan horses. This solution is less secure, but can be used in the short run.

[6] ESPRIT-Project No. 7023 CAFE (Conditional Access for Europe) of the European Union, 1992-1996

customary chip cards, it accepted smaller modules, such as those use for GSM telephones which are 15 x 25 mm. As it is desirable for the device to be placed in a normal wallet, it shouldn't, in fact, be called an "electronic wallet".[7]

Electronic wallet: particularly critical information, such as amounts to be paid, account numbers, will be shown on a secure display. Secure input of PINs and amounts is possible. The device contains a variety of chips from the bank, railway, telephone company and the personal signature key. Design by Nilgün Özalp, Fachhochschule Hildesheim/Holzminden (Özal_96).

Further consideration should be given to the fact that exclusive use of the device for the entry of a secret number would result in the number being relatively easy to guess due to the wear on the keys. This can be prevented if the device is used to enter other data, e.g. amounts to be paid, or account numbers. A touch screen combined with multi-functionality, or permutation of the numbers is also a means of reducing the danger of guessing the secret number. Yet another solution would be the use of a variety of secret numbers for more risky or less risky transactions (see PPSW_97 for further information). As an alternative, future devices could utilise biometric recognition of the owner (analyse the pores of the fingers, iris scan, see MiRS_95).

A question which has not been resolved is how the energy source for devices of this type should be supplied. The simplest solution would be to use the energy supply of the PC, or the terminal (telephone, cash dispenser, etc.). Batteries have also been considered, as well as solar cells. In addition to the

[7] It is expected that in the future personal computers will be standardly eqipped with a chip card reader. This would not have any secure channels available. It might make sense to have a second chip card reader available. This would make it possible for one chip card to give access to the software and another one to manage the signature key. The use of two chip cards would also make it possible for one to be a bank card, which occasionally is given out of hand, and the other to contain the signature key. Otherwise, a criminal who has possession of the bank card with a signature key could attempt to abuse it by testing PINs.

interfaces which have already been mentioned (contact, infra red, radio), it is also possible to conduct data inductively. A particularly attractive option is an infra red connection, as such an interface is already available on some palmtop computers and laptops.

Costs

Small devices similar to a pocket calculators, which are used only to secure the signature procedures, are particularly inexpensive to manufacture. The cost for devices of this type runs at less than ECU 50 per unit for a batch size of 10,000 (expert interviews). This refers to a device with a small display, a ten key keyboard and an interface such as an infra red module, or an electrical interface. For larger batches the costs could fall to as little as 15-25 ECU. The costs for the complete system are, of course, higher than the costs for the hardware. Any additional costs would be similar to those for signature systems without secure devices and are, therefore, not discussed here.

Willingness to Pay

In general, the seller, who has the main benefit of a digital signature, should bear the largest portion of the costs. It is conceivable that the seller might offer lower prices for digitally signed orders. The buyer could then use the reduction to finance his secure hardware. For commercial use it can be expected that the costs of the device would be covered after only a few express courier deliveries had been saved.

There may also be a willingness to pay on the part of the signatory who, for example, wants unambiguous proof of what he has ordered, or wishes to protect himself against a Trojan horse. He will only be able to find certain offers in the Internet when there is a legally binding method of ordering. This will make comparing prices on a global basis, as well as lower transaction costs possible. The willingness to pay may also exist for multi-functional devices. Respondents in the CAFE projects indicated such a readiness (see WCPS_95).

Dealing with the Remaining Risk

In principle, secure devices can also contain Trojan horses. In this case, however, only a few persons would come under suspicion. In addition, it is conceivable that an attacker might forge secure devices and bring them into circulation. If the manufacture of a secure device cost, for example, ECU 500,000, the attacker would have to aim at earning more with his deception. This would result in the deception becoming noticeable, either due to the fact that deceptions involved large sums, or a large number of individuals had been cheated. This would protect signatories from the accusation that they were simply reluctant to pay. In addition, forged devices would be recognisable and could be used as evidence.

Alternatives to the Use of Securely Implemented Signatures

Electronic commerce can also be implemented fairly without the secure implementation of signature procedures,

- if the seller is prepared to take back the goods
- if business partners identify identify each other, but do not require *legally binding* documents to be created (see BHKL_96)
- if the buyer pays in advance, in particular if fair exchange procedures are used (AsSW_97). In this case even anonymity is, in principle, possible (keeping the connection data secret and using anonymous ecash; see Chau_81, Chau_83).
- if the of insecure implementation procedures are used in order to prevent large numbers of false orders being placed. A non-binding registration of the signatory is sufficient for this purpose. Due to the fact that, in the case of each online registration, a sender to whom a reply can be sent is required, it would be possible for a deceiver to use a host which is under his control. All of the addresses would then come from the same host, which could be discovered by routine checks. The deceiver could also obtain access to a variety of hosts and generate new addresses from these. This, however, would become apparent to the system administrators. He could also use existing addresses on unrelated hosts, but the users of these hosts could turn in bewilderment to the certification authority. As a result, it is difficult to create large numbers of false registrations.

Summary

The following questions will be discussed: Is secure commerce using personal computers via the Internet possible without the implementation of signature procedures on secure devices with trustworthy input and output? Can security systems for electronic commerce which lack secure devices with secure input and output, that is software only systems, or systems using chip cards, be manipulated with relatively little effort, in such a way that financial damage arises for the seller or buyer? How should the liability for signature systems with and without secure devices be assigned?

A general expectation of a signature system is that a signatory cannot dispute a signature (non-repudiation). This contribution provides arguments in support of the necessity for secure devices and unambiguous registration of the user as prerequisites for the achievement of non-repudiation. In addition, the question of how the diffusion of secure devices could take place is discussed. This includes the form, size and additional functions of such devices. Finally, a sketch is provided of how electronic commerce without the secure implementation of signature procedures could be implemented fairly.

Literature

ABAs_96 American Bar Association: *Digital Signature Guidelines.* Chicago 1996

APSO_95 APSON-Gruppe (Advanced Payment Systems for Open Networks), *White Paper*, (1995)

AsSW_97 Asokan, N., Schunter, M., Waidner, M.: *Optimistic Protocols for Fair Exchange.* 4th ACM Conference on Computer and Communications Security. Zurich, 1997

BHKL_96 Baert, Christoph; Hecht, Thomas; Kuron, Ralf; Lacoste, Gérard; Livas, Dimitris; Petersen, Christian; Schunter, Matthias; Weber, Arnd; Wildhaber, Bruno; Whinnett, Dale: *Survey Findings, Trial Requirements, and Legal Framework.* 1996. Available at <www.semper.org/deliver/#D05>

BBCM_94 Boly, Jean-Paul; Bosselaers, Antoon; Cramer, Ronald; Michelsen, Rolf; Mjølsnes, Stig; Muller, Frank; Pedersen, Torben; Pfitzmann, Birgit; de Rooij, Peter; Schoenmakers, Berry; Schunter, Matthias; Vallée, Luc; Waidner, Michael: *The ESPRIT Project CAFE. High Security Digital Payment Systems.* Paper, ESORICS' 94

Bugo_96 Bugovics, Jozsef: *Sicherheit in Homebankinganwendungen: Sind Softwarelösungen geeignet?* Paper, Sicherheit in Netzwerken, Bad Homburg, 28.-29. März 1996

Chau_81 Chaum, David: *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* In: Communications of the ACM 1981, p. 84-88

Chau_83 Chaum, David: *Blind Signatures for Untraceable Payments.* In: Advances in Cryptology: Proceedings of CRYPTO '82. New York 1983, p. 199-203

Chau_89 Chaum, David: *Card-Computer Moderated Systems.* International Application Published under the Patent Cooperation Treaty (Classification H04K 1/00 No. WO 89/11762 of 30. November 1989)

DiHe_76 Diffie, Whitfield; Hellman, Martin: *New Directions in Cryptography.* In: IEEE Transactions on Information Theory, 1976, p. 644-654

Ford_94 Ford, Warwick: *Computer Communications Security. Principles, Standard Protocols and Techniques.* Englewood Cliffs 1994

Horn_96 Horning, Richard: *Has Hal Signed a Contract: The Statute of Frauds in Cyberspace.* 1996 <www.iway.fr/groupecx/uae/Horning.html>

MiRS_95 Miller, Bejamin; Richards, Donald, Sweet, William: *Who's Really on the Other End: Identification Technologies and Nonrepudiation.* Paper presented at Worldwide Electronic Commerce Conference in Bethesda, 1995

Özal_96 Özalp, Nilgün: *Entwurf von Benutzerendgeräten für elektronische Zahlungssysteme.* Paper 1996, Fachhochschule Hildesheim/Holzminden

PPSW_97 Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael: *Trusting Mobile User Devices and Security Modules*, IEEE Computer 30/2 (1997), p. 61-68

RiSA_78 Rivest, Ronald; Shamir, Adi; Adleman, Leonard: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. In: Communications of the ACM. February 1978, p. 120-126

Roßn_94 Roßnagel, Alexander et al.: *Die Simulationsstudie Rechtspflege. Eine neue Methode zur Technikgestaltung für Telekooperation.* Berlin 1994

Veri_96 Verisign, *Certification Practice Statement,* August 1996, avalalble at <www.verisign.com>

Waid_96 Waidner, Michael (1996): *Development of a Secure Electronic Marketplace for Europe*. Proceedings of Esorics '96, Rome, September 1996, also available at <www.semper.org/>

WCPS_95 Weber, Arnd, Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael: *Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet.* Frankfurt 1995 (Project CAFE)

Webe_97 Weber, Arnd: *Soziale Alternativen in Zahlungsnetzen*. Frankfurt, New York 1997