Information Security –

from Small Systems

to

Management of Secure Infrastructures

Proceedings of

WG11.2

and

WG11.1

of TC11 (IFIP)

Copenhagen, Denmark, 13 May 1997

Edited by

Jan HP Eloff
Department of Computer Science
Rand Afrikaans University
Johannesburg, South Africa

Rossouw von Solms
Department of Computer Studies
Port Elizabeth Technikon
Port Elizabeth, South Africa

ISBN: 0-86970-424-9

Secure Access to *Electronic Strongboxes* in Electronic Commerce

(Extended Abstract)

Thomas Hardjono[1] *and Jennifer Seberry*

Centre for Computer Security Research
University of Wollongong
Wollongong, NSW 2522, Australia
Tel: +61-42-214327 Fax: +61-42-214329
email: t.hardjono/j.seberry@uow.edu.au

Abstract

Two protocols for access to electronic strongbox are described in the context of electronic commerce. The notion of electronic strongboxes is discussed, and the participants of the strongbox system are presented. The two protocols concern two participants of the strongbox system, namely the Customer who wishes to access a strongbox maintained by a Strongbox Provider. The security aspects of the protocols are then analysed, focusing on possible methods of cheating by the two involved participants.

Keywords

Electronic Strongboxes, Electronic Commerce, Information Security, Network Security.

1. INTRODUCTION

The development of user-friendly browsers for information deposits on the Internet, together with executable programs capable of running via these browsers, has attracted unprecedented interest in the use of the Internet as the vehicle for electronic commerce. The decrease in hardware costs and storage prices in the last few years has increased the accessibility of personal computers to the ordinary person on the street. Currently

[1]The author is also at the University of Western Sydney - Macarthur, NSW 2560, Australia.

Network Computers (NC) are speculated as being the next possible source for large consumption of PC-related technologies, bringing not only electronic commerce, but a whole range of computerized activities over the Internet.

Currently, most research efforts have been focused on providing secure payment system for customers. However, in the future, other services related to payment systems may emerge. We perceive that one such service will be that of *electronic strongboxes* (Hardjono and Seberry, 1996) as part of the larger electronic commerce infrastructure.

As currently the Internet and other networks lack the means for customers to securely store *on-line* the digital information corresponding to electronic cheques, coins or notes, the concept of electronic strongboxes represents an attractive solution to the problem.

The technology to implement secure electronic strongboxes is partly available today. Many of the required protocols can be derived from other proposed systems in electronic commerce, which so far has focused mainly on payment systems. These proposed systems range from those which require an interface to the existing financial infrastructure (such as DigiCash (Chaum, 1985; Chaum, 1992), iKP (Bellare *et al*, 1995), NetBill (Sirbu and Tygar, 1995) and SET (Visa and MasterCard, 1996)), to those which employ electronic coins/cash as a reusable payment mechanism circulating electronically (eg. NetCash/NetCheque (Neuman and Medvinsky, 1995; Medvinsky and Neuman 1993)).

In this paper we develop further the work of Hardjono and Seberry (1996) by presenting protocols for the submission and retrieval of a strongbox by a customer. The protocol employs public key (asymmetric) cryptography, as well as private key (symmetric) cryptography to ensure the security of the strongbox transfer. The customer uses a pseudonym (Chaum, 1981) when dealing with the provider of the strongbox service.

In the next section the background for electronic strongboxes is discussed. This is followed by a description of a basic system for electronic strongboxes in Section 3. Access to the strongboxes is discussed in Section 4, presenting the protocols for submission (check-in) and retrieval (check-out). Some points regarding the protocols and their security are then discussed in Section 5, with Section 6 ending the paper.

2. ELECTRONIC STRONGBOXES: BACKGROUND

The notion of *electronic strongboxes* as the counterpart of physical strongboxes or safeboxes was initially proposed in 1996 (Hardjono and Seberry, 1996). The concept was derived from the similar notion found in the physical world. In the traditional financial sector the provision of strongboxes has been in service for sometime. Customers can apply to have a private strongbox held within a bank, in which the customer can place any type

and any amount of valuables, subject only to the physical characteristics of the strongbox. The bank typically has no interest in the contents of the strongbox, and derives income from providing safe storage and access to such strongboxes. The identity of the strongbox customer and the fact itself of the customer having a strongbox are usually treated as confidential by the bank.

In the concept of the electronic strongbox the customer would access his or her strongbox over the Internet using a suitable browser that provided a secure environment for the user. Users of a "strongbox-browser" would be allowed to manipulate objects stored within the strongbox using an iconic object representation. These electronic objects or items can be certified representations of physical objects, and can include electronic coins or cash, electronic bank cheques, digital documents (eg. stocks and contracts), anonymous digital certificates of ownership of physical items, cryptographic material to access other services, and others. A customer may have multiple strongboxes, each at differing strongbox providers. Joint ownership of a strongbox can serve as an exchange medium between its two owners. Using a unified interface, customers should be able to move items between strongboxes, each under different providers.

The provision of strongboxes on a global network such as the Internet may lead to an economy which is based not only on monetary transactions, but also on *barter*, or personal trade. As the exchange of items is a normal part of daily life, electronic strongboxes can be a medium within which to carry-out non-monetary commerce with privacy, confidentiality and user anonymity. Other institutions may act as *valuers* and *converters* where legal and valuable items (eg. gold) are given a valuation and electronic certificates are generated for the items. The same institution may also provide long-term safe storage for the physical items, whilst the anonymous owner uses the electronic certificate on the Internet. Private purchases of legal items between users should be facilitated since such an event is common in everyday life.

Previous research on anonymous and verifiable databases have been conducted by Brandt *et al* (1988), and also reported by others (Hardjono and Seberry, 1995). The aim in Brandt *et al* (1988) was to allow certain institutions (eg. hospitals) to maintain data about people (eg. patients) whilst maintaining anonymity through the use of pseudonyms for privacy reasons. Persons having data in the database could verify that their information is correct and that no illegal modifications had been made. This is significantly different from the notion of electronic strongboxes. First, the items stored in the strongboxes carry real and global value as they are an electronic representation of physical goods. Secondly, the electronic items themselves can circulate within the system, moving from one strongbox to another. Thirdly, such a movement of items should be untraceable, as the ownership of an item is regarded as confidential information. Finally, although anonymity is equally required as in Brandt *et al* (1988) in electronic strongboxes it represents a more complex problem as it involves several parties – similar to electronic payment systems.

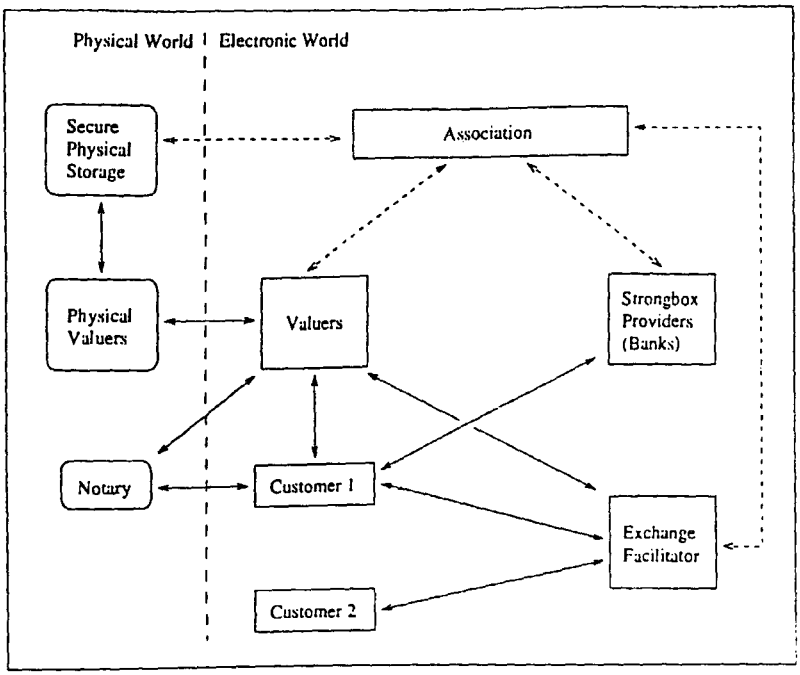

Figure 1. An Electronic Strongbox System

3. STRONGBOX SYSTEMS: BASIC COMPONENTS

Figure 1 illustrates a simple design for a strongbox system, borrowing the terminology from the area of electronic payment systems. All electronic interactions between participants are assumed to be over a secure channel, with peer authentication conducted at the commencement of communications. The proposed system of Figure 1 does not pretend to be comprehensive, and it attempts only to address the main components only. Additional components will be required to support the framework to achieve full workability.

The participants of the system are as follows:

- *Customer*: the customer or user, interacting with the Strongbox Provider (eg. Bank) for the safekeeping of electronic items.
- *Strongbox Provider*: an institution that provides the electronic strongbox service to a customer, accepting the storage and retrieval of electronic items to/from the electronic strongboxes.
- *On-Line Valuer*: the On-Line Valuer is trusted to verify that an electronic item

belonging to an owner (ie. Customer) truly exists and has not been modified by its current owner. The Valuer can also be requested to split items into several sub-items, and issue certificates for them. Several Valuers may exist on-line, and each must recognize the other's certification. In general the On-Line Valuers carry-out the tasks of the traditional Certification Authority (CA), and therefore they are equally trusted.

- *Physical Valuer*: the Physical Valuer should be distinct from the On-Line Valuer as the Physical Valuer knows what a physical item is and which pseudonym forwarded the physical item to be valued. The Physical Valuer stores the physical items at the *Secure Physical Storage*, to which the Association has access in the case of disputes. The Physical Valuer is a highly trusted entity since it has direct access to the physical goods.

- *Exchange Facilitator*: the Exchange Facilitator aids two or more Customers who wish to exchange items from their strongboxes. The Exchange Facilitator is also a trusted entity in the same way that arbiters are trusted in contract-signing protocols. They obtain income from providing the exchange service and for acting as an arbiter.

- *Association*: the Strongbox Providers and the Valuer work under the umbrella of the Association. Customers bring disputes to the Association.

In addition, there is the *Notary*. The Notary comes in on behalf of a Customer when disputes necessitates their presence.

The Customer is the owner of the contents of a strongbox and is deemed also as the owner of the strongbox. The Customer must first join the strongbox system by opening an account with the Strongbox Provider, which can be a Bank or other institutions having the necessary computer infrastructure to provide this service. The Customer obtains membership through the Association which issues the Customer with the credentials (eg. within a smartcard) and with a pseudonym to be used within the system. The Customer henceforth employs this pseudonym when using the system.

4. SECURE ACCESS TO ELECTRONIC STRONGBOXES

In the physical world, strongboxes are typically held by the provider of the service, such as a Bank. The Customer/owner of the strongbox request access to his or her strongbox to the Bank. The Bank would then provide the Customer with the physical box in a secure environment (such as a locked room or within a guarded vault). At no point does the Bank see the contents of the Customer's strongbox. The Customer returns the box to the Bank after he or she is finished with it.

Upon bringing this concept and scenario into the electronic realm, one notices similarities in the basic interaction between the Customer and the Provider (ie. Bank). However, unlike the physical strongboxes, electronic strongboxes possess features that derive directly from its electronic nature:

- Interaction between the Customer and the Provider is carried-out over the electronic communications medium (eg. Internet), and no face-to-face contact occurs. Therefore, methods of authentication must underlie the whole interaction between the Customer and the Provider.

- Customers may obtain stronger security and privacy compared to the physical strongboxes. In the case of physical strongboxes, the Bank may in fact illegally access the strongbox using a copy of the user's key. In practice it is difficult to provide a guarantee to the Customer that the Bank does not have a copy of the Customer's physical key.

  In contrast, in electronic strongboxes the Customer may simply encrypt all his or her digital items before placing them in the strongboxes. Given a secure encryption algorithm, the Bank may find it economically and computationally infeasible to break the Customer's encipherment.

- Unlike the physical environment which may be made secure (eg. a vault), an equally secure computing environment is difficult to achieve in the electronic world. Although end-to-end security can be achieved through the use of encryption technology, the security of computations and the privacy of behaviours at the Customer's end and at the Provider's end cannot so far be guaranteed.

  It is towards this end that security contributions from technologies such as Java (Dean *et al*, 1996; Felten *et al*, 1996) and CORBA (OMG, 1991; OMG, 1994; Varadharajan and Hardjono, 1996) are sorely needed.

In the following we present two basic protocols corresponding to the retrieval (or check-out) and submission (check-in) of strongboxes. We assume that a Customer (denoted as "Customer") is wishing to check-in/check-out a strongbox to/from a Strongbox Provider ("Provider" for short). We leave the form of the electronic *items* unspecified, since the items are enciphered by the Customer before entered into the strongbox, and therefore bears little relevance to the Provider.

4.1. Notation

Both public key cryptography and private key cryptography are employed. The public-key pairs are denoted as (K,k), where K is public and k is secret.

The Customer holds the public-key pair (K_c, k_c). The Customer also own a private key BK_c (ie. "Box Key") which is never revealed to anyone. This is used to encipher the digital contents of his or her strongbox before submitting it to the Provider. That is, assuming that the Customer owns the electronic items $item_1, item_2, \ldots, item_n$, the strongbox in its most simple form would consist of the encipherment of these items as a unit using the key BK_c. More precisely, $BOX = \{index, item_1, item_2, \ldots, item_n\}_{BK_c}$ where BOX is the Customer's strongbox. The Customer may choose to apply other functions – such as compression of the items – before the encipherment. The Customer may also wish to encipher each item separately, in which case an *index* (also enciphered) may be used to keep track of items in the strongbox.

The Provider holds the public-key pair (K_p, k_p). The Provider will also generate a private session-key S_{pc} and S_{cp}which is used to create a secure channel between the Provider and the Customer

The operation "$\{\}_K$" means that the contents within the braces "{}" are enciphered or deciphered using the key K. The meaning is the same in the case of public key encipherment or private key encipherment.

The operation "$[\,]_k$" denotes a signature using the private-key κ, verifiable using its matching public-key K. The string being signed is assumed to accompany the signature. Hence "$[X]_k$" really means the couple $(X, signature)$, which implies that all parties can see X and verify the *signature*. H is a secure one-way hash function, while N_i represent nonces.

All Customer employs the pseudonym PID when dealing with the Provider. The Provider is assumed to be trusted not to reveal the fact of the Customer having a strongbox, as is the custom with providers of physical strongboxes.

4.2. Strongbox Check-In

CI-1. Customer — Provider: $\{CheckInRequest, PID_c, N_1\}_{K_p}$

CI-2. Provider — Customer: $\{S_{pc}, N_1, N_2\}_{K_c}$

CI-3. Customer — Provider: $\{BOX, tstamp_c, [H(BOX||tstamp_c)]_{k_c}, N_1, N_2\}_{S_{pc}}$

Here $BOX = \{index, item_1, item_2, \ldots, item_n\}_{BK_c}$ where *index* is simply a list of items in the strongbox. The Customer keeps a copy of BOX in secure memory until the protocol is completed. At the end of a successful check-in, the Customer can discard the memory-copy of BOX. The key BK_c is a private key known only to the Customer.

Upon receiving the strongbox, the Provider re-calculates $H(BOX||tstamp_c)$ using BOX and $tstamp_c$ that it had just received, and compares the result against that

signed by the Customer. This is to ensure that the Customer is honest and does not substitute the true BOX for a bogus one.

The Provider then securely stores both the strongbox BOX and the value $tstamp_c$ denoting the check-in time.

CI-4. Provider — Customer: $\{Acknowledge, [H(BOX||tstamp_c)]_{k_p}, N_2\}_{S_{pc}}$

Here the Provider signs a hash of the BOX and $tstamp_c$ and returns it to the Customer as a receipt. The Customer can check that the hash value is indeed the same as that previously computed by the Customer. The value $tstamp_c$ is that received from the Customer in Step CI-3.

The Customer keeps a copy of the signed $[H(BOX||tstamp_c)]_{k_p}$ until the next time the Customer checks-in the strongbox. This allows the Customer to verify that no tampering occurred on the BOX whilst it was in the possession of the Provider.

In this manner, both the Customer and the Provider has a signed hash of the BOX from each other as proof should any disputes occur at a later time.

4.3. Strongbox Check-Out

CO-1. Customer — Provider: $\{CheckOutRequest, PID_c, N_3\}_{K_p}$

CO-2. Provider — Customer: $\{S_{cp}, tstamp_p, [H(BOX||tstamp_c)]_{k_p}, N_3, N_4\}_{K_c}$

The Provider retrieves the pair $(BOX, tstamp_c)$ from its secure storage, where BOX is the strongbox and $tstamp_c$ is the timestamp value from the previous check-in event.

The Provider gives the Customer a signed hash of the strongbox BOX, against which the user can compare hash values. Note that the user still has a copy of $[H(BOX||tstamp_c)]_{k_p}$ obtained from the check-in event.

The Provider also accompanies the message with the new timestamp $tstamp_p$ which the Customer can verify as being close enough to the current clock time.

CO-3. Customer — Provider: $\{[[H(BOX||tstamp_c)]_{k_p}||tstamp_p]_{k_c}, N_3, N_4\}_{S_{cp}}$

As proof for the Provider, the Customer attaches the current timestamp $tstamp_p$ to the signed-hash value $[H(BOX||tstamp_c)]_{k_p}$ received from the Provider. Next, the Customer signs the resulting concatenation and sends the result back to the Provider. In this way the Provider has some proof that the Customer has checked-out the strongbox at some time $tstamp_p$.

CO-4. Provider — Customer: $\{BOX, N_4, N_5\}_{S_{cp}}$

Upon receiving the proof from the Customer, the Provider proceeds to deliver the BOX to the Customer via the secure channel established using the symmetric key S_{cp}.

CO-5. Customer — Provider: $\{[Acknowledge]_{k_c}, N_5\}_{S_{cp}}$

The Customer then sends a signed acknowledgment message to the Provider, indicating the completion of the protocol.

5. DISCUSSION

One noticeable aspect of the two protocols for strongbox access is the unequal distribution of the burden of providing proofs (receipts). More specifically in the case of the Check-Out protocol, the Provider expects the Customer to give a receipt in advance (Step CO-3) to the Provider. Only after receiving the receipt does the Provider deliver the strongbox to the Customer (Step CO-1).

We accept this imbalance by pointing to the fact that access to a strongbox is not identical to contract-signing. The strongbox Provider must be accorded some level of trust by the Customer, similar to the situation in the physical world. In any case, the strongbox contents are assumed to be securely enciphered by the Customer, and therefore they cannot be accessed by the Provider. Furthermore, the Provider gains nothing by denying access.

Two possible scenarios with respect to cheating in the checking-in of strongbox are as follows:

- *The Customer denies checking-in the strongbox.* The Customer, therefore, claims that the strongbox is still checked-out.

  This form of cheating is self-defeating to the Customer, as only the Customer can make use of the contents of the strongbox.

  One possible motive for such a denial is where the Customer wishes to check-in the same strongbox at different Providers. This is equivalent to the Customer (illegally) duplicating items and storing these copies at the different Providers. This method of cheating cannot be detected with these protocols, but would be detected either when the Customer converts the electronic items back to physical items, or when an item is exchanged via the Exchange Facilitator and On-Line Valuer [2].

[2]Note that the issue of duplicate items circulating is not directly related to the access to strongboxes, but rather to the method of representing electronic items in the system (Hardjono and Seberry, 1996).

- *The Provider denies that the Customer has checked-in the Customer's strongbox.* That is, the Provider claims that the strongbox is still checked-out and thus not in the Provider's possession.

  To dispute this claim the Customer can reveal the receipt that he or she obtained in Step CI-4. The receipt contains the signature of the Provider, which is taken to mean that it currently holds the strongbox.

  The failure to complete the check-in protocol (particularly that of Step CI-4) can be resolved by the Customer since the Customer still holds a copy of the strongbox.

  Since the Provider will be unable to open the strongbox, this method is cheating can only be detrimental to the reputation of the Provider.

Similar to the two cheating scenarios within the check-in protocol, two possible scenarios exist for the check-out protocol:

- *Provider denies check-out has occurred.* Principally, this form of cheating is equivalent to a denial-of-service attack.

  Although the Provider can abort the protocol between Step C0-3 and Step C0-4, thereby unfairly obtaining the Customer's proof of checking-out, in practise this method of cheating can only be detrimental to the Provider. The Provider will not find any use of the strongbox since it will not be able to decipher its contents. Modifications to the protocol can be made in order to ensure that occasions of this method cheating is minimized.

- *Customer denies performing the check-out.* This method of cheating is more relevant to the Provider since in this case the Customer implicitly accuses the Provider of stealing.

  Here the Provider can protect itself by revealing the receipt it obtained in Step C0-3, which has been signed by the Customer.

  One possible solution – with undesirable effects – is to repeat Step C0-4 of the protocol in the presence of a Notary. This could lead to the Customer having duplicate copies of the strongbox (and therefore items). Such illegal duplications will later be detected by other participants of the strongbox system. In practice, the protocol should atomic in the sense that no individual steps are allowed to be repeated.

6. REMARKS AND CONCLUSION

There remains a number of issues related to the workability of the electronic strongbox system:

- *Duplicate items.*
  Similar to electronic cheques, electronic items within the strongbox system must be prevented from being duplicated. In electronic cheques, some method of numbering (serial or random) of cheques are used together with blind-signatures to provide user anonymity.

  Within any system that employs numbering of objects (electronic cheques or items) one requirement is that the "used" (old) object-numbers are stored in a database accessible to relevant parties. This would allow for the detection of duplicated numbers on items by searching through the database.

  We perceive that the nature of strongboxes are such that items are there to be stored, with far less movement of items compared to the movement of electronic cash or electronic cheques. Thus, the use of a secure database holding the identification number of items is acceptable for the strongbox system. This database solution depends, however, on the extent to which the strongbox system grows, in which case other solutions may have to be found.

- *Untraceability.*
  Ideally electronic items should be untraceable when they are moved (exchanged) between Customers. This is a natural expectation since the movement of physical items are also typically untraceable. Methods such as blind-signatures can be used in a similar manner to that used for electronic cheques. However, additional research must be conducted into methods to exchange items through the Exchange Facilitator (to ensure fairness and honesty) in such a way that the Facilitator never sees the items being exchanged between two Customers. Other methods will be needed to counter the possibility of linking electronic items to their current owners.

- *Anonymity.*
  Anonymity of Customers is particularly important in the case of the exchange of items, since exchanges typically involves the Exchange Facilitator acting as an arbiter. The use of pseudonyms within a smartcard-based system offers a potential to achieve Customer anonymity in the electronic strongbox system.

In this paper the issue of access to electronic strongboxes has been discussed, together with two protocols for the check-in and check-out of strongboxes. Although the protocols are still relatively simple, they point to the possible direction for the design and implementation of electronic strongboxes as an integrated part of the electronic commerce

infrastructure. Some security issues of the protocol have been discussed, concentrating on the possibilities and effects of cheating. The current work represents further developments in the effort to realize the electronic strongbox concept.

7. REFERENCES

Bellare, M., Garay, J. A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., and Waidner, M. (1995), "iKP – a family of secure electronic payment protocols," in *Proceedings of the First USENIX Workshop on Electronic Commerce*, (New York), pp. 89–106, Usenix, 1995.

Brandt, J., Damgard, I. B., and Landrock, P. (1988), "Anonymous and verifiable registration in databases," in *Advances in Cryptology - Proceedings EUROCRYPT '88* (Lecture Notes in Computer Science No. 330) (C. G. Gunther, ed.), pp. 167–176, Springer-Verlag, 1988.

Chaum, D. (1992), "Achieving electronic privacy," *Scientific American*, pp. 96–101, August 1992.

Chaum, D. (1985), "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

Chaum, D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

Dean, D., Felten, E. W., and Wallach, D. S. (1996), "Java security: From hotjava to netscape and beyond," in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, (Oakland, CA), IEEE Computer Society, 1996.

Felten, E. W., Balfanz, D., Dean, D., and Wallach, D. S. (1996), "Web spoofing: An internet con game," Technical Report 540-96, Department of Computer Science, Princeton University, December 1996.

Hardjono, T. and Seberry, J. (1995), "Applications of smartcards for anonymous and verifiable databases," *Computers & Security*, vol. 14, no. 5, pp. 465–472, 1995.

Hardjono, T. and Seberry, J. (1996), "Strongboxes for electronic commerce," in *Proceedings of the 1996 Usenix Workshop on Electronic Commerce*, (Oakland, CA), Usenix, pp. 135–145, November 1996.

Medvinsky, G., and Neuman, B. C. (1993), "NetCash: A design for practical electronic currency on the Internet," in *Proceedings of the First ACM Conference on Computer and Communications Security*, ACM, November 1993.

Neuman, B. C., and Medvinsky, G. (1995), "Requirements for network payment: The NetCheque perspective," in *Proceedings of IEEE Compcon'95*, (San Francisco), IEEE, 1995.

OMG (1991), "The Common Object Request Broker: Architecture and Specification," OMG Document Number 91.12.1, Object Management Group, 1991.

OMG (1994), "White Paper on Security," OMG Document Number 94.4.16, Object Management Group, 1994.

Sirbu, M. and Tygar, J. D. (1995), "NetBill: An internet commerce system optimized for network-delivered services," *IEEE Personal Communications*, pp. 34–39, August 1995.

Varadharajan, V. and Hardjono, T. (1996), "Security for the CORBA framework," in *Proceedings of IFIP SEC'96 12th International Conference on Information Security*, (Greece), Chapman-Hall, May 1996.

Visa and MasterCard (1996), "Secure Electronic Transactions," 1996. [WWW Document], URL http://www.visa.com.