SEMPER: A Security Framework for the Global Electronic Marketplace

Gérard Lacoste, IBM France[1]
Michael Steiner, IBM Research[2]

November, 1998

Abstract

Security for electronic commerce is urgently required, but it must be built in an orderly and extendible way that provides for the security services needed today and in the future. The *SEMPER* project (Secure Electronic Marketplace for Europe), partially funded by the European Commission, aims to provide the first open and comprehensive set of security solutions for electronic commerce. This paper reviews security requirements for the global marketplace, and describes the objectives of the project, its approach to security, its field trials, and its proposal to increase certainty in electronic commerce.

Introduction

Competitive forces are pressuring the commercial community to adopt new technologies for greater efficiency. The result is the emerging Information Society. Electronic commerce is experiencing tremendous growth over the Internet. It is projected that by the year 2000, transactions worth over $25 billion will have been conducted via the new medium.

Prerequisites for such large amounts of money being exchanged over the information networks are, however, making the electronic marketplace secure as well as establishing sufficient fairness and trust. Much research is being pursued to achieve this goal. However, most of the efforts are restricted in scope, e.g. limited to payment, cryptography, intellectual property rights protection, etc. without giving enough attention to the need to integrate the various solutions in a consistent way. The *SEMPER* project proposes an open security framework that should provide for such an integrated, complete and global electronic marketplace.

The first section of this paper briefly reviews the security requirements for safely conducting electronic commerce over the Internet, the main difficulties which have arisen and the progress made so far towards their resolution. The objectives of the *SEMPER* project are outlined in this context. The second section presents the general approach of the project, its security architecture, and the basic and advanced security services that it proposes. The third section discusses the SEMPER field trials, and the results which can be drawn from these trials. The fourth section introduces work on agreements, to be signed by sellers and buyers, which are intended to encourage the use of the Internet for doing business.

1. The secure marketplace

1.1 Requirements

Electronic commerce is a transposition of traditional commerce to the context of information networks. In the traditional marketplace, every operation, apart from the exchange of physical goods and services, is based on information: offers, brokerage, negotiations, orders, contracts, payments, documents, receipts and the resolution of disputes. The model of the traditional marketplace is, therefore, perfectly suited to the electronic marketplace, provided that its characteristics and requirements are appropriately translated in electronic terms.

Like traditional commerce, the electronic marketplace should facilitate the establishment of relationships between potential sellers and buyers. Sellers and buyers should be able to negotiate the terms and conditions of transactions, such as the goods and services being offered — which may be dependent on the profile of the buyer, the applicable laws or regulations —, the price, the means of payment, the mode

---

[1] Centre d'Etudes et Recherches, BP43/Dept 3228, 06610 La Gaude, France.
Tel +33-(0)492-11-4807, Fax +33-(0)493-24-4545, Email lacoste@vnet.ibm.com
[2] IBM Research Laboratory, Säumerstrasse 4, 8803 Rüschlikon, Switzerland
Tel +41-(0)1-724-8286, Fax +41-(0)1-724-8953, Email sti@zurich.ibm.com

of delivery, guarantees, etc. The negotiation may be concluded with an explicit contract, signed electronically. The parties should be able to dispute the transaction both before and/or after its conclusion.

As a key to its acceptance and the successful development of its huge potential, electronic commerce should handle all these situations in such a way that it is open to everyone, and at least as convenient to use, reliable, secure, and legally predictable as traditional commerce. Unless these minimal properties are fulfilled, people will be cautious about the routine use of electronic commerce, or will disregard it altogether.

With the disappearance of the physical presence of the parties, trust also vanishes, especially when communication is conducted via an insecure medium like the Internet. The viability of electronic commerce requires that trust be restored. Buyers must be able to securely identify sellers and obtain assurance that they are legitimately established and accredited. Enterprises, for example, would be breaking the law if they bought from sellers that are not legally registered. Buyers might only trust sellers that are accredited by a particular payment system provider, or a particular consumer organisation. The integrity of the transaction must be preserved: buyers need to be confident that they will receive the goods, or the service that they actually ordered in return for their payment, and sellers must be sure that they will be paid for the goods, or the service delivered. Privacy is receiving more and more attention. In most cases, confidentiality will be required regarding communications, the existence of transactions, or their specific details — price, conditions, date, identity of the parties, etc. The recovery of transactions and the resolution of disputes must also be guaranteed in order to provide the parties with genuine recourse should equipment or network failures occur, or if they are confronted by dishonest practices on the part of their business partner.

1.2 Fundamental issues

The challenge to establish electronic commerce in such a way that it fulfils the requirements outlined above is formidable.

First, the techniques which are capable of meeting the trust requirements described are highly complex and the tools which support these techniques must be integrated into systems. In turn, these systems have to provide processes which allow users to act as reliably and easily in the electronic marketplace as they currently do in the context of traditional commerce. These systems need to address the complete set of issues raised by the electronic marketplace. Handling just part of the problem, such as providing payment only, is clearly insufficient and burdensome. It would only positions users half way between the physical and electronic worlds when performing a single process, the transaction, which requires that integrity be guaranteed. It goes without saying how uncomfortable this position can be.

Second, users must be able to trust that their systems are, in fact, behaving as they appear to be behaving and are protected against security attacks. Particular attention must be given to user devices, which enable users to participate in the electronic marketplace with full knowledge of the state and meaning of their transactions.

Third, these systems must be fully interoperable, and despite their heterogeneous nature, they must guarantee that no important information can be lost. For example, incompatibilities may prevent users from accessing the site of their choice, mask important transaction-related information, or prevent correct transaction recovery.

Fourth, electronic commerce needs to be backed by a legal framework which provides users with a transparent and predictable legal environment which is adapted to the medium and includes the legal acceptance of digital signatures and electronic information appropriately authenticated as evidence in case of dispute. This framework should be valid, regardless of the jurisdictions in which buyers and sellers reside. This is particularly true for cross-border commerce, where the patchwork of laws from different countries already creates significant complexity for marketing strategies and for the enforcement of contracts, liability, privacy, and security. This complexity could increase with new country-specific taxes, duties, and regulations regarding the use of new technologies and the type of information exchanged with them. This also impacts the technical means. So should registration and certification services take into account roles and liabilities, digitally signed data need clear and unambiguous semantics, legally binding actions require well-defined warning-functions, digital evidence has to be collected and finally this new form of evidence must be handled by specialised dispute protocols.

Fifth, security assumes that there is a network of registration, certification, and key distribution authorities, whether public or private. These authorities represent the cornerstone for authenticating users and, therefore, for establishing trust among users of electronic commerce.

Fifth, cryptography is subject to hot debate, in particular regarding export controls, key management and control, and the use of encryption for purposes of confidentiality. Uncertainty about future governmental regulations on these issues is having a significant effect on the expansion of electronic commerce.

Sixth, electronic commerce users must be appropriately trained to understand what electronic commerce should mean to them, its associated benefits and risks, and which security measures need to be taken in order to protect their systems and their data.

1.3 Current status

The hype of electronic commerce on the Internet has generated considerable efforts on the part of the community of manufacturers and researchers. After a first wave of products and implementations of Web sites which were designed for the narrow perspective of marketing and promoting enterprises and commercial outlets on the Internet, the second wave began to make the Web more interactive and captivating, as the technology and company know-how evolved. Digital libraries and on-line catalogues emerged. With the third wave of Internet-related technology, emerging in 1996, it has become possible to authenticate the parties, allow customers to browse through catalogues, to place orders, to pay for them, to receive the goods and to access on-line services. Progress has been made with respect to secure payment with credit cards, based on the Secure Sockets Layer (SSL) protocols from Netscape, but more importantly, based on the Secure Electronic Transaction (SET) protocol from VISA and MasterCard. Further progress has also been achieved in the area of electronic cheques, electronic cash, and micro-payment with stored-value smartcards.

In addition, the range of Internet-related products on offer has started to provide for the integration of the existing systems of the service providers. Some manufacturers are proposing architectures for building applications integrating back-office systems, and for using multiple means of payments. At the government level, several proposals are progressing on the legal aspects of electronic commerce, an example of which is the recently released proposal from the US government “A Framework for Global Electronic Commerce”.

In spite of these initiatives, apart from SEMPER in Europe and CommerceNet in the USA, all other technical projects deal only with specific aspects of secure electronic commerce. There is no generally accepted model and architecture for building the secure marketplace. As a result, security requirements are not well formulated. Due to their proprietary architecture most electronic commerce systems are closed and are, therefore, not aimed at achieving the objective of interoperability among systems. The relationship between the server and the client is often considered solely from a master-slave perspective, which disregards the applicability of the proposed protocols for the potentially large number of “any-to-any” relationships among the users of electronic commerce. The general focus is primarily on on-line payment in the context of the scenario “offer, order, payment, and delivery”. The establishment of registration, certification, and key distribution infrastructures, although essential for building trust, is progressing slowly.

Issues of primary importance with regard to trust receive insufficient attention, if any. They include a trusted user interface, fair exchanges among the parties, non-repudiation, two- and multi-party contract signing, anonymity, privacy, multi-party security, and the resolution of disputes. This, in spite of the fact that the existing variety of laws in force in different countries and the change of business practices and actors dramatically increase the complexity of resolving disputes in the electronic environment. These issues are not regarded as part of a single framework that would ensure interoperability.

1.4 SEMPER objectives

In contrast, from the standpoint of security, the *SEMPER* project aims at addressing the complete problem of electronic commerce over insecure networks, such as the Internet. Its main goal consists of developing an open and comprehensive security framework which can be regarded as a blue-print, a lingua franca, for building a global secure marketplace. Global means that the proposal should be applicable in all countries, take into account all requirements, and it should be open in allowing new components such as new payment systems to be integrated smoothly at any time. This immediately requires that the architecture has to be generic and shouldn’t restrict the set of supported business processes, networks or operating systems.

The architecture aims to support the commercial actors, buyers and sellers, in their transactions and their communications with third parties such as banks or certification authorities.

To validate the proposal the project implemented a prototype. This prototype is tested in real trials in collaboration with different types of enterprises in several european countries. Some of the service providers are members of the project; others were invited to participate in new trials.

Certain findings of the projects were already distributed at international conferences, to european standards committees, at public demonstrations of the prototype and through its public homepage http://www.semper.org. The final results including the architecture and the evaluation of the trials will be published as a book in the Springer-Verlag mid-1999.

The *SEMPER* project is part of the Advanced Communication Technologies and Services (ACTS) Research and Development programme proposed by the European Commission, Directorate General XIII. *SEMPER* was initiated in September 1995 for three years. It is financed in part by the European Commission and in part by its twenty European members: Commerzbank (D), Cryptomathic (DK), CWI Stichting Mathematisch Centrum (NL), DigiCash (NL), Eurocom Expertise (GR), Europay International (B), Fogra Forschungsgesellschaft Druck (D), France-Télécom - CNET (F), GMD Forschungsgesellschaft Informationstechnik mbH (D), IBM (CH, F), Intracom (GR), KPN Research (NL), MARIS (NL), Otto Versand (D), r3 security engineering (CH), SINTEF Telecom and Informatics (N), and the Universities of Freiburg (D), Hildesheim (D), Dortmund (D), and Saarbrücken (D). The project is managed by IBM France, and technical leadership is provided by the IBM Research Laboratory in Zurich.

2. The *SEMPER* approach

2.1 Fundamental directions

When building a security architecture for the electronic marketplace an initial requirement is to model that marketplace and identify all its players, in respect of the roles, the relationships and the interactions they have with each other. The *SEMPER* model distinguishes two classes of players: users of the marketplace and enabling third parties. Buyers and sellers form the first class, while the second is comprised of registration and certification authorities (to deliver digital certificates), network providers, directory service providers, brokers, shopping malls, payment service providers, and, to ensure fairness, notaries and arbitrators.

In this model, transactions are represented as a sequence of transfers of information such as contracts, payments, delivered goods, credentials etc. While all of these transfers have to be secured (e.g., signed) on an individual basis, they also have to be linked securely in the business process. Some transfers are even more intertwined. In *SEMPER* they are called fair exchanges. The signing of a contract or receiving a receipt for a payment or the delivery of goods are examples of such fair exchanges: the contract should be valid only if all parties have signed and the receipt should always be issued when the good is received (similar to regular certified mail). A fair exchange can be defined as the assurance that a party in an exchange will receive the other parties good if and only if it also delivers it's own promised good.

One of the foundations of the architecture reflecting current business practise is a focus on multi-party security: The required trust in other parties is limited to a reasonable minimum and responsabilities and liabilities are clearly specified. Actions of parties are made accountable with the help of signed document such as offers, orders and receipts. This will remove ambiguities and is required in such an open environment where the peer might not be known apriori and might even live on the other side of the globe in a country you have never heard of. Multi-party security applies to the buyer-seller relationship but also to third parties. Trust in financial institutions, registration authorities, notaries, network providers and software vendors should be limited and their action should be accountable. A final aspect of multi-party security is that the decision, who is trusted and to what extend, should be in the sole control of the individual parties and not mandated by the system.

In respect to the communication protocols, it is clear that security needs to be provided end-to-end, from application to application. There are two ways to achieve end-to-end security: at the transport level, or at the application level. Secure communication at the transport level means offering a secure channel for applications to communicate. The Secure Socket Layer (SSL) protocol is an example of a secure channel.

This approach ensures the confidentiality of the messages exchanged by the applications, for example the amount of a payment, a credit card number and its expiration date. It also allows the authentication of the users of these applications through an exchange of their certificates, or other means, such as passwords, or tokens. But, by definition, a secure channel is transparent to applications. It is, therefore, unable to provide document-level security, which is a key requirement for electronic commerce. For example, a secure channel cannot provide consumers with a means to sign an order, nor can it help the merchant to verify signed orders and store them securely in case of dispute. *SEMPER* proposes application-level security protocols, which co-exist during a business session with other application-level protocols. Secure information exchanges in *SEMPER* are based on the concept of a container which is a package of the different elements of information to be transferred and is associated with security attributes. Three types of elements are defined: signed documents, such as certificates, receipts or signed statements; information, such as digital goods or information to access a service; and, payment. Containers can be structured according to a template to define the semantics of the data exchanged.

Another fundamental desicion taken by *SEMPER* was to split clearly the display of critical security relevant information from other informations. For example, payments or binding signatures should be realised with security garantuees which normaly don't apply to catalogues. To prevent interference by viruses and trojan horses such critical information should be displayed in a well-defined und unifom manner and eventually be handled on a separate highly secured personal device controlling the signature function and equipped with a trusted I/O path to the user.

Finally to approach the global electronic marketplace the security architecture has to be open. The provision of proprietary protocols, not promoted to the level of open standards, is inherently unable to achieve universal interoperability between the many players in electronic commerce, not to mention the high complexity and costs incurred by maintaining this variety of different protocols, especially for financial institutions, sellers, and buyers. Until the Internet, the Web, and their suite of open standards, such as TCP/IP and HTTP emerged, electronic commerce was inhibited. With the introduction of such standards, the issues of interoperability, complexity, and cost have taken a giant step towards being resolved, and electronic commerce is now generating considerable impact on the way goods and services can be managed and sold. This path has proven itself over time. It is being followed by a number of serious standardisation candidates, such as the SET protocol for payment using credit cards, the X.509 standard for certification, or the standards on cryptography like DES, RSA, etc. Several other standards will evolve to handle payment with electronic cheques, electronic money, etc. An open security architecture must make provisions for them, by providing application programming interfaces at two levels: at the component level to include new components to support existing and future protocols; and at the application level to provide applications with a standard set of security services that abstract the variety of protocols which achieve similar goals and leave the specific methods which are used up to users' preferences and negotiation. This is the approach followed by *SEMPER*.

2.2 The SEMPER Architecture

The *SEMPER* architecture follows a layered structure comprising four layers. The upper layer offers the *SEMPER* security services to business applications. From top to bottom, this is supported by the Commerce Layer, the Exchange Layer, the Transfer Layer, and the Supporting Services Layer. Figure 1 below illustrates this structure.

Business applications use the services of the underlying layers, principally by means of the Commerce Layer. In a few cases, for reasons of efficiency, business applications can have direct access to a limited set of functions of the other layers. For example, a user registration application can directly use the certificate service located in the Transfer Layer.

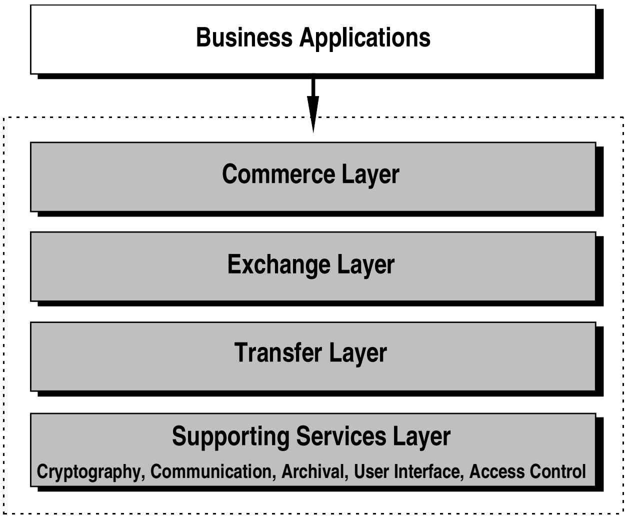

Figure 1 - *SEMPER* architecture - a layered functional structure

The Commerce Layer offers application designers a business application framework, i.e. a set of building blocks for general use, in order to reduce the effort of developing business applications. The application writer is shielded from the low level security details while she gets at the same time the assurance that the building blocks will protect her security requirements. To establish a business relationship a business context is created for a given business partner. In a first step the quality of service attributes will be negotiated with the peer. Then primitive transactions such as offer, order, payments, etc. can be executed in that context and will be stored in persistent storage. Additional services allow the suspension and recovery of transactions and support for the resolution of disputes.

The Exchange Layer is in charge of controlling fair exchanges among the parties. Here fair means that the parties agree on the terms of the exchange before hand, and that they are assured that they will receive either the information according to the agreement or nobody receives anything.

The Transfer Layer provides services for transmitting and receiving information in the form of containers. Transfer of containers depends on associated security attributes. For example, a container associated with non-repudiation of origin requires that the sending entity signs the contents of the container and that the receiving entity verifies the signature and marks the contents of the container as received with non-repudiation of origin. The Transfer Layer processes the different types of information to be sent or received through containers: signed documents, information, and payments. They are handled by the certificate, statement, and payment blocks, respectively. Containers passed by the Exchange Layer for transfer are opened, and each type of information contained in them is directed to the corresponding block for specific transfer through the appropriate protocol. The receiving entity of the Transfer Layer reassembles the various pieces received to rebuild the container and passes it back to the Exchange Layer. For example, a container with a document and a payment will be transferred through the statement and the payment blocks. If the selected payment method is the SET protocol, the payment block will perform the payment according to the SET protocol. Finally, the Transfer Layer provides management of the transfer services like wallet management, establishment or termination of connections, etc.

The bottom layer, the Supporting Services Layer, provides support to all other layers. It collectively offers cryptographic services, communication services, archiving services, preferences services, the trusted user interface, and access control services. The cryptographic services provide for encryption, hashing, digital signature, and key generation. The communication services shield users from the specific details of the underlying network. Only the quality of service parameters needs to be specified. The archiving services provide for secure storage and archiving of persistent information, such as certificates, signed documents, cryptographic keys, and transaction records. The preferences services offer a uniform view of the preference setting for each of the other services. They also maintain information regarding the installed configuration. The trusted user interface provides users with any critical data and actions that, otherwise, would be left to HTML pages supplied by third parties. In this way, the trusted user interface minimises the trust required in other parties. The trusted user interface permits users to manage their wallets, to access secure storage, to display critical information from other parties, such as authentication, quotes or certificates, and to take actions like signing orders, paying, or acknowledging receipt.

Analogous to an operating system, *SEMPER* proposes a system kernel which is in charge of ensuring system integrity. Within the kernel (the bottom three layers), access control verifies the rights of all modules (including application modules) to access, use, and modify critical resources. This protects them against potential threats from each other and from outside sources.

As already mentioned, the *SEMPER* architecture is open in that different designs and implementations may be integrated, provided they have a suitable API. This is achieved by means of the concept of a service block. A service block consists of a manager and a number of modules. The manager provides the required services using one of the modules (e.g., the payment block will use existing payment systems as modules). The manager provides a generic interface, such that several modules (possibly through an adapter) can be plugged into *SEMPER*. This is the basis for the independence of specific implementations of the modules — one of the key points of *SEMPER*.

2.3 SEMPER services

Within its architecture, *SEMPER* specifies a number of security services. The development plan of these services is structured into basic services and advanced services. Basic services meet five basic security requirements: authentication, integrity, signature, payment, and confidentiality. Advanced services address fair exchange of values, resolution of disputes and aspects of secure document processing, such as time-stamping, certification of documents, credentials, certified mail, or multi-party contract signing. They also handle anonymity issues and the integration of new payment instruments, such as electronic cheques, and stored-value smartcards.

As basic services are generally understood, they are not discussed further here. Rather, a brief overview of some aspects of the advanced services that SEMPER is currently developing is preferred. These aspects are fair exchange, credentials, and anonymity.

Fair exchange was discussed briefly in the previous section. It assumes a prior agreement among the parties before proceeding to the exchange. More precisely, a fair exchange is achieved if two conditions are met: atomicity and fairness, or transfer and contents. Atomicity means that all agreed transfers of information are performed, or none are performed. Fairness means that the parties actually receive what they agreed to receive. Fairness requires that the parties specify what they expect from the exchange. Upon receipt, each party verifies that what they received matches their specified expectation. Usually fair exchange is implemented using one or more third parties. In this case, the third parties must be specified in advance (e.g., as part of the contract which specifies the exchange), and for most security requirements at least one (or "all," or "the majority of all," etc.) must be assumed to be honest. The required trust in third parties is an additional parameter of the security attributes of the exchange. The protocols which have currently been designed are based on an optimistic approach: after a mutual agreement among the exchanging parties and a third party for recovery, the exchanging parties send their information. If a fault occurs, the exchanging parties may complain to the designated third party which will restore fairness. The restoration of fairness depends on the items exchanged, e.g., undoing a payment, or creating affidavits. Only when such an optimistic approach is not possible, will the third party be actively involved in the exchange protocols.

Credentials are electronic tokens which associate certain rights with their owner. Tickets, ski passes, membership cards, business cards, passports, diplomas, property deeds and prescriptions are examples of credentials. A credential identifies its owner and his or her associated rights, its issuer , its period of validity, and proof of its authenticity. Credentials may be dynamic if use modifies their associated rights. A one-way bus ticket is a dynamic credential: its use makes it invalid for re-use. Credentials may be anonymous in order to protect the privacy of their owner. In this case, they are delivered by means of validated pseudonyms. A pseudonym is delivered by a third party, based on certificates, or previously issued pseudonyms. Depending on how much a user trusts the issuer of the pseudonym, the credential may or may not conceal the identification of the issuer of the pseudonym. Credentials require new types of third parties: issuers of pseudonyms and issuers of credentials. In addition, a third party to provide secure time-stamps, and one to provide for the clearing of credentials among the different organisations accepting them may also be needed.

Anonymity in electronic commerce relates to two areas: services specially designed to prevent the users' identity being revealed by the information exchanged between clients and service providers; and communications to provide anonymous channels. Depending on efficiency, privileges and the choice of anonymous channels, different levels of anonymity can be obtained. Anonymity in *SEMPER* means extending the security architecture to support anonymity, both at the services and communication levels, while allowing the selection of different degrees of anonymity according to the context in which the anonymous requests are made. It also means appropriate extensions to the security services, and creating new building blocks to support anonymous credentials and anonymous channels. An in-depth study conducted on anonymity in *SEMPER* has identified both the architectural and service extensions required, as well as the new blocks needed to support it.

3. The *SEMPER* trials

3.1 Prototype

The purpose of the trials is to evaluate the applicability and the soundness of the security architecture and services proposed by *SEMPER* as well as to understand the acceptance and behaviour of the actor facing electronic transactions. The verification of the concepts proposed by *SEMPER* required the construction of a robust prototype to conduct trials in a realistic environment. The prototype is based on Java. This choice was taken in the light of the portability of the language environment to allow deployment in various environment (Windows 95/NT, MacIntosh and various UNIX systems) and to quickly adapt to the changes in this still immature field.

3.2 SEMPER trial sites

Multiple trials sites were chosen to explore the possibilities of the architecture in various different commercial contexts. The first three sites were opened with the help of the services providers who are members of the project: The Eurocom site, located in Athens (GR), offers distance learning services. Students browse through the Eurocom offering of courses, and after successful on-line registration and payment, they can gain on-line access to the selected course presentation, notes, and examinations. With the Fogra site, located in Munich (D), Fogra customers benefit from on-line ordering, payment, and on-line delivery of documents and software. Customers browse through the Fogra catalogue, select documents, place orders, and receive the documents. From Hamburg (D), the Otto Versand site offers on-line ordering, based on a catalogue of 13.000 different articles in a variety of colours and sizes. Three additional sites were opened later to investigate more specifically the requirements of SMEs: in Amsterdam, OPL and KPN offer books, maps, documents, and database access for the oil and gas industry; in Sophia Antipolis, Actimedia built in cooperation with IBM France and the Centre International de Communications Avancées a site selling CD-ROM to the french speaking communities. Also in Sophia Antipolis, Acri provides in cooperation with the Institut Eurécom and IBM France a secure database of satellite images over the experimental ATM network EuroSud 155.

To reflect the specific requirement of the trial sites special business applications were written for each site. These applications all reside on top of the same common core which handles the security requirement in a uniform manner. The certification infrastructure was provided by GMD in Darmstadt. Commerzbank, GMD and IBM Zurich built the infrastructure for SET payments. KPN integrated the smartcard based electronic purse scheme Chipper in the trial software. Further payments were possible by using traditional bank transactions and by sending securely credit card numbers. This allowed each trial site to offer multiple payment systems.

To experiment with more advanced security services the project wrote in a third phase a generic application, the *Fair Internet Trader (FIT).* This application supports enterprises in negotiations, contract signing, payments with multiple schemes including electronic checks and delivery. This is done in a highly secure manner, e.g., by clearly specifying liabilities, by guaranteeing fair receipts and most importantly by giving support for dispute resolutions with the help of collected evidence. Trials and their evaluation are currently ongoing.

Figure 2 - *SEMPER* trial sites

3.3 First results

Following experiences from building the business applications and interviewing the users, consumers as well as service providers.

On the whole, the security architecture posed no problem for implementing the trials. The fundamental directions of the architecture could be confirmed: The distinction of security relevant information from other information, the separation of generic and specific aspects of the business process, the realisation of the basic and advanced security services, the writing of the business applications on top of these services, the openness of the architecture based on the concepts of pluggable modules and the layering and structure of the architecture all proved to be appropriate. Actually, the architectural directions proposed by *SEMPER* have been confirmed by the emergence of products for electronic commerce which follow similar lines.

The writing of the business applications and the corresponding web pages unfortunately proved to be rather difficult. Some service providers would have preferred a customisable turn-key solution. This obstacle asked for more involvement of the service providers than foreseen and substantial help from the project. In the future we will hopefully see the appearance of generic but customisable applications. The above mentioned FIT is a first step towards that goal. We note nevertheless that the service providers could mature their approaches faster than with any current turn-key solution with the additional benefit of improved protection of multi-party security requirements.

Electronic payments in catalogue based commerce gives additional difficulties: while in traditional trade the billing is handled after the receipt of the delivered goods electronic payment means stipulate payments before delivery. But this also requires a reversal of the trust requirements and manifests the importance of making actions by the player accountable and disputable.

The feedback of the service providers proved to be largely positive but also acknowledged the problems intrinsic in such prototypes, notably in installations and stability, and the lack of maturity in Java itself. The trusted user interface gave them the necessary confidence; they noted though that the graphical quality could be improved. The main difficulties encountered were a lack of understanding of the inherent risks in networks, the importance of a clear authorisation of critical actions such as payments and signatures with a warning function and the technical and legal problems in realising semantically unambiguous signatures on documents. This makes it clear that in particular awareness for the real threats has to be raised with education of users of electronic commerce but also education of developers of such systems.

Banks are much more aware of the risks. They are rather prudent in the use of the Internet for payments. In some countries banks even slow down considerably the growth of electronic commerce. In Europe the national structure of the financial institutes, notebaly the credit card systems, represent unsurmountable barriers for a fast adaption of cross-border commerce as all current trials of electronic payment systems are limited to national borders. A better acceptance of standards like SET and the introduction of the Euro should overcome these obstacles in the future.

4. The SEMPER agreements

Signatures represent the cornerstone of commerce, whether traditional or electronic, because they can make the signatories liable for fulfilling terms of contracts, offers, quotes, orders, payments, receipts, etc. Therefore, for participants to be willing to participate in electronic commerce on a routine basis it is imperative that they can also rely on a recognised equivalent of paper-based signatures, i.e. digital signatures. The development of the trusted certification services which support digital signatures is of particular importance.

Substantial work on digital signatures has already been achieved. For example, the model law of the United Nations Commission on International Trade Law (UNCITRAL) provides for the acceptability of international electronic contracts and digital signatures, for legal and commercial purposes. The German Signature Act recognises the legal bindingness of digital signatures, provided they rely on tamper-resistant secure hardware. Other countries might follow the German approach, or legislate differently. If the latter occurs, uncertainty about the validity of digital signatures will increase. In either case, implementing these regulations, providing users of electronic commerce with appropriate means, and giving them sufficient confidence to use and accept digital signatures will take significant time.

In order to remove uncertainty in this area, and allow a quick and soft start of mass electronic commerce, SEMPER proposes a series of agreements that establish a set of rules for each role: buyer, seller, bank, certification authority, etc. Users playing this role can commit to abide by these rules. Signatories of the *SEMPER* agreements have a common legal basis protecting them from unforeseen risks. They can safely conduct business among themselves.

The concept of *SEMPER* agreements does not require a priori contacts among the single players making business, nor does it mandates contracts between pairs of roles. The agreement is signed on paper with a third party. It establishes in advance the liability of the parties regarding the future transactions which they might want to conduct. Buyers are bound to their own digital signature, thereby taking some liability for the damage if their signature key was compromised. Within the limits established for a buyer's overall liability, per transaction liability may also be established. Within the scope of the agreement, the third party maintains the buyer's current liability status and, according to the transactions conducted, it guarantees to the sellers, by means of certificates delivered on a per transaction basis, that the buyer has not exceeded his or her agreed current liability, and that the buyer's signature key has not been revoked. This scheme can easily be extended to ensure anonymity.

In addition, the agreements provide for explicit rules regarding the validity period of contracts, the choice of applicable law, the conditions of sale. They regulate offers, advertising, revocation of orders. They promote awareness on the business processes used to provide fair applications, and on the need to carefully handle signature keys, signing and revocation procedures, etc.

Independent of the payment method used, the agreement gives buyers the opportunity to benefit from the offers available on the Internet, and, at the same time, protects them against unacceptably high damages, in spite of the fact that they may be using insecure hardware vulnerable to trojan horse attacks (note that smartcards without trusted I/O are highly vulnerable too!)[MS1]. It gives merchants and service providers the opportunity to increase their market share on the Internet, while being assured that their customers can be held liable for their signed orders. Hence, it encourages sellers to offer their goods and services over the Internet, and buyers to implement transactions with limited financial risk, thereby enabling a practical and quick start to secure electronic commerce.

Conclusion

The emerging global electronic marketplace urgently needs a security framework that can encompass the full set of security services required today and in the future. The *SEMPER* project is working towards achieving these goals. This paper has reviewed the objectives of the project, its approach, its proposed architecture and security services, and a proposal for an agreement which aims to facilitate bringing sellers and buyers to the Internet to conduct business together.

With its comprehensive and consistent approach to the secure electronic marketplace, the *SEMPER* project is positioned to contribute substantially to making the vision of global electronic commerce a reality.

Acknowledgements

This work was partially supported by the Swiss Federal Department for Education and Science and the European Commission in the context of ACTS Project AC026, *SEMPER*, Secure Electronic Marketplace for Europe. However, it represents the view of the authors. SEMPER is part of the Advanced Communications Technologies and Services (ACTS) research programme established by the European Commission, Directorate General XIII.

This paper is based on joint work from all members of the SEMPER consortium. Many thanks to all of them for their kind support and cooperation. Further information on *SEMPER* can be found on the homepage http://www.semper.org.

References

President William J. Clinton: A Framework For Global Electronic Commerce, White House, 1997.

W. Ford, M. Baum: Secure Electronic Commerce, Prentice-Hall, 1996

M. Waidner: Development of a Secure Electronic Marketplace for Europe, ESORICS '96, LNCS 1146, Springer-Verlag, Berlin 1996, 1-14.

A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner: Trusting Mobile User Devices and Security Modules, IEEE COMPUTER 30/2 (1997) 61-68.

N. Asokan, P. Janson, M. Steiner, M. Waidner: State of the Art in Electronic Payment Systems, IEEE COMPUTER 30/9 (1997) 28-35

Page: 10
[MS1]Reference IEEE Computer paper ....