Rima Saliba, Gilbert Babin, and Peter Kropf. "SecAdvise : A Security Mechanism Advisor." in
Conference on Distributed Communities on the Web (DCW 2002). Sydney, Australia. April 2002. Lecture
Notes in Computer Science. No. 2468. Springer Verlag. April 2002. pp. 35-40.

SecAdvise : A Security Mechanism Advisor

Rima Saliba[1], Gilbert Babin[2], and Peter Kropf[1]

[1] University of Montreal
Computer Science and Operations Research, Montreal, Quebec, Canada
{salibar,kropf}@iro.umontreal.ca
[2] HEC – Montreal
Information technology, Montreal, Quebec, Canada
Gilbert.Babin@hec.ca

Abstract. The proliferation of incompatible e-commerce systems applying different security technologies imposes difficult choices on all the concerned parties. In this context, the purpose of this research is to provide the necessary background to develop a security advisor (SecAdvise), which will make it possible to integrate the security mechanisms and the dynamic selection of the various mechanisms between several parties wishing to conduct business transactions safely. Such an advisor aims multiple goals: overcoming compatibility and interoperability problems, evaluating and reducing technological security risks, and enhancing trust.

1 Introduction

The Internet is becoming an increasingly important channel for e-commerce where complex business interactions involve multiple parties. Clearly, the safety of the transactions using electronic means is of capital importance. Several security systems have been implemented [1, 4, 9] and are operational in many e-commerce applications. The mechanisms employed, the security services, the cryptographic algorithms, the amount of money involved in a transaction, the parties concerned, etc, distinguish these security systems. In this context, the purpose of this research project is to analyze the various types of security threats, mechanisms and services in e-commerce applications, to evaluate them, qualify them, and develop sound methods to select the most appropriate and effective mechanisms and services in a given business and technology context. The results of these investigations will provide the necessary background to develop a security advisor, which will make it possible to integrate the mechanisms and the dynamic selection of the various mechanisms between several parties wishing to conduct business transactions safely. Such an advisor aims multiple goals: overcoming compatibility and interoperability problems, reducing technological security risks, and enhancing trust. The rest of the paper is structured as follows. In Section 2, an introduction to security threats, services and mechanisms is given. This analysis should provide us with a basic understanding of the relationship between risks, services, and mechanisms. We also try to understand the link between security services, mechanisms and the layers of the OSI (Open Systems Interconnection) reference model [2]. Section 3 describes a trust management model developed in [8]. Our advisor is introduced in Section 4. Finally, Section 5 contains some conclusions and future research directions.

Rima Saliba, Gilbert Babin, and Peter Kropf. "SecAdvise : A Security Mechanism Advisor." in Conference on Distributed Communities on the Web (DCW 2002). Sydney, Australia. April 2002. Lecture Notes in Computer Science. No. 2468. Springer Verlag. April 2002. pp. 35-40.

2 Security Issues

In [5], Vesna Hassler has identified three principal issues of security: security threats, security services, and security mechanisms. Attacks on systems can be classified in several types:

- *Eavesdropping*. Intercepting and reading messages intended for other principles.
- *Masquerading*. Sending/receiving messages using another principal's identity.
- *Message tampering*. Intercepting and altering messages intended for other principals.
- *Replaying*. Using previously sent messages to gain another principal's privileges.
- *Infiltration*. Abusing a principal's authority in order to run hostile or malicious programs.
- *Traffic analysis*. Observing the traffic to/from a principal.
- *Denial-of-service*. Preventing authorized principals from accessing various resources.

This classification leads to a thorough analysis of the most probable threats and of the system's vulnerabilities to these threats. On the basis of the risk analysis results, we can define a security policy that clearly specifies what must be secured. The functions that enforce the security policy are referred to as security services.

We mention the basic security services defined by the International Organization for Standardization. Whenever possible, we also identify in which layer of the OSI reference model [2] these services may be applied. This relationship between services and OSI reference model layers has already been established in [5], on which we base this classification.

- *Authentication*. Different authentication services are available. Peer entity authentication ensures that a communicating party is really what he claims to be (network layer). Data origin authentication delivers proofs that a piece of information originates from a certain source (network layer).
- *Access control*. Access control ensures that only authorized principals can gain access to protected resources.
- *Data confidentiality*. Data confidentiality can be of different types. To ensure confidentiality between two communicating parties that establish a communication channel, a connection confidentiality service is employed (physical layer). If the communication channel is only logical, the service is referred to as connectionless confidentiality (data link layer). If only certain parts of messages to be exchanged must be protected, a selective field confidentiality service is used (application layer). Traffic flow confidentiality protects against traffic analysis (physical layer).
- *Data integrity*. Similar to data confidentiality services, data integrity services are different for connection-oriented and connectionless protocols. For connection oriented protocols they may provide message recovery (transport layer). Data integrity services can also protect selected fields of messages only.

Rima Saliba, Gilbert Babin, and Peter Kropf. "SecAdvise : A Security Mechanism Advisor." in
Conference on Distributed Communities on the Web (DCW 2002). Sydney, Australia. April 2002. Lecture
Notes in Computer Science. No. 2468. Springer Verlag. April 2002. pp. 35-40.

- *Non-repudiation*. According to the ISO, non-repudiation services can prevent denial-of-origin of data or guaranty the delivery of data. There are two additional possibilities: non-repudiation of submission and non-repudiation of receipt (application layer).

Security services are built using combinations of security mechanisms. These mechanisms are in turn realized by cryptographic algorithms and secure protocols. Here is a summary of the security mechanisms available, as described in [5].

- *Encryption*. Encryption mechanisms protect the confidentiality of data. We distinguish two types of mechanisms: symmetric mechanisms (e.g., Data Encryption Standard – DES; Advanced Encryption Standard – AES) and public key mechanisms (e.g., RSA).
- *Digital signature*. A digital signature can be generated by a special digital signature mechanism as well as by a combination of encryption mechanisms.
- *Authentication exchange*. Authentication can be based on an encryption mechanism, symmetric or public. Therefore, several mechanisms have been developed whose only purpose is authentication exchange (e.g., zero-knowledge protocols, Kerberos – a key distribution system).
- *Access control*. Access control mechanisms are closely related to authentication. They deal with controlling access of the subjects to the divers resourses.
- *Data integrity*. Data integrity mechanisms protect data from unauthorized modification. One way to protect data integrity is to use an encryption mechanism. In this way, data integrity and data confidentiality are ensured. Another way to ensure integrity is to use a digital signature mechanism. In this case, integrity and non-repudiation are ensured. If integrity is required without confidentiality or non-repudiation, message digests computed by a cryptographic hash function can be used (e.g., SHA-1, MD5). The message authentication code (MAC) can ensure authentication and data integrity.
- *Traffic padding*. Traffic padding mechanisms keep traffic approximately constant, so that no one can gain information by observing it.
- *Routing control*. Routing control mechanism makes it possible to choose a specific path for sending data through a network, hence avoiding undesirable nodes.
- *Notarization*. Notarization mechanisms are provided by a third party notary that must be trusted by all the participants.
- *Key management*. For the public key encryption, key management and certification authorities are a must.

As is the case with security services, security mechanisms may also be used at different layers of the OSI reference model. To illustrate this, we give a short list of well-known security mechanisms and the corresponding layer to which they apply.

- Application layer: S/MIME, S-HTTP, Secure TELNET.
- Presentation layer: Secure RPC, SASL, SSH.
- Transport layer: SSL, TLS.
- Network layer: IP AH, IP ESP.
- Data link layer: Link encryption, MAC address filtering.

The list of services and mechanisms above is not exhautive. In fact, specific contexts require the development of specialized security services. To illustrate this point, we present here some security services developed for electronic payment. Note that most of these services are provided at the OSI reference model application layer.

- *User anonymity and location untraceability*. These services guaranty that althought the merchant received payment for the goods sold, he cannot identify the buyer. These services may be provided, for example, by chains of mixes [3] and blind signature mechanisms. Another form of this service is the payer anonymity service provided in FV (First Virtual) [7].
- *Non-repudiation of payment transactions*. This service ensures that a payer cannot deny having made de the payment. An example of this service is found in the 3KP payment protocol, using digital signatures [9].
- *Confidentiality of payment transaction*. This service prevents eavesdropping on payment data. This type of service is provided by SET (Secure Electronic Transaction) citeSher00a.
- *Freshness of payment transaction*. This service prevents replay attacks on payment transactions. One approach to provide this service is the use of time stamps such as in the 1KP model [9].

When the payment instrument is digital money, the list of services includes protection against double spending, protection against forging of coins, and protection against steeling of coins. When electronic checks are the payment instrument, other types of services are necessary. For instance, payment authorization transfer (proxy) makes it possible to transfer a payment authorization from one authorized principal to another.

3 A Trust Management Model

Several initiatives, such as Semper [6], tried to have the various electronic payment systems converge in order to work out a common operating platform and assure interoperability between them. Robles *et al.* [8] propose a trust model for agent-oriented electronic business applications. This trust model outlines a methodology to define trust requirements and to associate safeguards with them to increase the protection and trust of electronic business frameworks. It suggests the definition of a trust problem space (TPS) as a set of all possible situations in the system, in which the e-commerce agents can have trust problems about each other or about the environment (a set of the threats and risks mentioned in Section 2). This space includes various types of attacks, and vulnerabilities due to cheating or misuse of system resources. This TPS is related to a collection of interrelated mechanisms, trust units (TU), to provide safeguards to protect systems and sub-systems, and to increase the trust in the systems or sub-systems. A TU is a trust logical unit representing a partial or complete solution or countermeasure to any of those problem subspaces presented in the definition of the trust problem space. It may involve cryptographic protocols (RSA, DSE), control mechanisms or infrastructures.

4 Secadvise Definitions

We intend to develop an optimization model, enabled by a security advisor, to

1. identify and specify the Trust Problem Space (TPS) and the Trust Units (TU) available in the context of a communication to be secured, and
2. make the optimal association between TPS and TU to actually secure that communication.

We provide here a preliminary version of the optimization model:

c transaction to secure. It is the business context/transaction that is performed and that need security.

$\mathbf{U}$ the set of all trust units (TU). A trust unit may be a security mechanism, a security protocol or a security infrastructure.

u a trust unit ($u \in \mathbf{U}$).

$\mathbf{R}$ the set of all non-decomposable security risks, such that $\forall r \in \mathbf{R}, \forall u \in \mathbf{U}$, either u covers r entirely or u does not cover r at all.

r a non-decomposable security risk ($r \in \mathbf{R}$).

$\mathbf{P}$ the set of all potential participants in secured communications.

p a participant ($p \in \mathbf{P}$).

R_u the set of security risks covered by trust unit u ($R_u \in \mathcal{P}(\mathbf{R})$).

R_c the set of security risks that need to be covered in transaction/context c ($R_c \in \mathcal{P}(\mathbf{R})$). These are the Trust Problem Spaces (TPS) defined above.

P_c the set of all participants directly communicating in transaction/context c ($P_c \in \mathcal{P}(\mathbf{P})$), e.g., host A wants to communicate with hosts B.

$A_{u,p}$ the set of participants, trusted by participant p, that can act as third party authority in conducting trust unit u ($u \in \mathbf{U}, p \in \mathbf{P}$, $A_{u,p} \in \mathcal{P}(\mathbf{P})$), e.g., the set of certification authorities trusted by a participant. If the trust unit does not require such trusted third party, $A_{u,p} = \mathbf{P}$ to simplify the matching process between trust units.

U_p the set of trust units available to a participant $p \in \mathbf{P}$ ($U_p \in \mathcal{P}(\mathbf{U})$).

$\bar{U}_P$ the set of trust units available to all participants $\forall p \in \mathbf{P}$ ($\bar{U}_P \in \mathcal{P}(\mathbf{U})$)

$$\bar{U}_P = \{u \in \bigcap_{p \in P} U_p \quad | \quad \bigcap_{p \in P} A_{u,p} \neq \emptyset\}$$

$\tilde{U}_c$ the minimal set of trust units to cover the security risks of transaction/context c ($\tilde{U}_c \in \mathcal{P}(\mathbf{U})$)

$$\tilde{U}_c = U \in \mathcal{P}(\bar{U}_{P_c}) \quad | \quad R_c \subseteq \bigcup_{u \in U} R_u \wedge ||U|| = \min_{U' \in \mathcal{P}(\bar{U}_{P_c})} ||U'||.$$

The set $\mathbf{R}$ is defined as the set of non-decomposable risks. Clearly, defining that set is not a simple task. However, we argue that $\mathbf{R}$ may be constructed. Assuming that we find a trust unit u such that risk r is partially covered by u, we can always define risks r' and r'', with $r' \cup r'' = r$ and $r' \cap r'' = \emptyset$, such that r' is covered entirely by u and r'' is not covered at all by u.

Rima Saliba, Gilbert Babin, and Peter Kropf. "SecAdvise : A Security Mechanism Advisor." in
Conference on Distributed Communities on the Web (DCW 2002). Sydney, Australia. April 2002. Lecture
Notes in Computer Science. No. 2468. Springer Verlag. April 2002. pp. 35-40.

This said, in order to avoid such *ad hoc* decompositions, we intend to provide a preliminary multidimensional classification of risks. Two of the dimensions would be the set of risks identified in Section 2 and the seven layers of the OSI reference model [2].

5 Conclusion and Future Work

The proposed model is an interoperable architecture for the various e-commerce security systems. The advisor will choose the best subspace solution for a given security context, depending on the available mechanisms. Regardless of the kind of the mechanisms, the advisor will assess minimum and acceptable security for the transactions between the various parties wishing to conduct safe business transactions. In addition, the advisor should facilitate the assessment of the trustworthiness of security mechanisms and services, providing a systematic evaluation framework based on the multidimensional risk classification. In the foreseeable future, a detailed classification of the mechanisms will be available which will conduct the trustworthiness of these mechanisms. This classification will help to demonstrate the applicability of the approach. Moreover we will choose a number of mechanisms to test the architecture/advisor. We will also define standard scenarios to implement and test the system.

References

1. W3c security. Available from http://www.w3.org/Security/.
2. Information technology – open system interconnection – basic reference model: The basic model. ISO/IEC Standard 7498-1, International Organisation for Standardization, 1994.
3. D.L. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.
4. W. Ford and M.S. Baum. *Secure Electronic Commerce — Building the Infrastructure for Digital Signatures and Encryption*. Prentice Hall PTR, second edition, 2001.
5. V. Hassler. *Security Fundamentals for E-commerce*. Computer Security Series. Artech House, 2001.
6. Gérard Lacoste, Brigit Pfitzmann, Michael Steiner, and Michael Waidner, editors. *SEMPER — Secure Electronic Marketplace for Europe*. Number 1854 in Lecture Notes in Computer Science. Springer-Verlag, 2000.
7. D. O'Mahony, M. Peirce, and H. Tewari. *Electronic Payment Systems*. Artech House, 1997.
8. S. Robles, S. Poslad, J. Borrell, and J. Bigham. A practical trust model for agent-oriented electronic business applications. In *Proc. of the 4th Int'l Conf. on Electronic Commerce Research (ICECR-4)*, volume 2, pages 397–406, Dallas, Texas, USA, November 2001.
9. M.H. Sherif and A. Serhrouchni. *La monnaie électronique — systèmes de paiement sécurisé*. Eyrolles, 2000.