Shaping the Research Agenda for Security in E-Commerce

Rolf Oppliger
Swiss Federal Office of Information Technology and Systems (BFI)
CH-3003 Berne, Switzerland
rolf.oppliger@mbox.bfi.admin.ch

Abstract

In this paper, we overview the current state-of-the-art and future trends in network security and argue that the security requirements of electronic commerce (e-commerce) applications generally go beyond the more traditional requirements of network security. This is particularly true for the requirements that address the complexity and availability of cryptographic applications, the anonymity of participating peers, the autonomy of mobile code, the manageability of trust, and the necessity for intellectual property protection. Based on these additional requirements, we point out some areas for further study and propose a corresponding research agenda for security in e-commerce.

1 Introduction

The low cost and wide availability of the Internet for businesses and customers has sparked a revolution in electronic commerce (e-commerce) and e-commerce applications. In short, an e-commerce application may address one or several phases of a typical business transaction, and there exist various possibilities to model these phases. For example, a possibility is to distinguish five phases of a business transaction. In phase 1, the merchant makes an offer for specific (information) goods or services. According to this offer, the customer may place an order in phase 2. In phases 3 and 4, the customer makes a payment and the merchant delivers the goods or services to the customer. The handling of the payment may involve third parties, such as banks or acquirer gateways. In either case, disputes may occur and these disputes must be addressed in phase 5. Note that this is just one model that can be used to distinguish phases of a business transaction, and that other models can be used that are partially or entirely different.

As of this writing, many organizations are exploiting the opportunities offered by Internet-based e-commerce, and many more are expected to follow. Exemplary applications include online shopping, telebanking and Internet banking, teleteaching and distance education, online gambling and virtual casinos, as well as Pay-TV and video-on-demand services. But in spite of the well-publicised success stories (e.g., `www.amazon.com`), many businesses and customers are still cautious about participating in e-commerce, and security concerns are often cited as being the single most important barrier.

The aim of this paper is to provide a thorough overview about the security issues that suround e-commerce and e-commerce applications, to point out some areas for further study, and to propose a corresponding research agenda for security in e-commerce.

More specifically, the paper is organized as follows: In Section 2, we address the security issues related to e-commerce (client-side, server-side, and transaction security issues, as well as organizational and legal security issues). In Section 3, we overview the current state-of-the-art and future trends in network security. In Section 4, we argue that the security requirements of e-commerce applications generally go beyond the more traditional requirements of network security. This is particularly true for the requirements that address the complexity and availability of cryptographic applications, the anonymity of participating peers, the autonomy of mobile code, the manageability of trust, and the necessity for intellectual property protection. Based on these additional requirements, we point out some areas for further study and propose a corresponding research agenda for security in e-commerce in Section 5. Finally, the paper concludes with some general remarks regarding the role of security for e-commerce and e-commerce applications in Section 6. Also, an analogy is used to help understand the role of security in e-commerce.

2 Security Issues related to E-Commerce

With regard to the security of e-commerce and e-commerce applications, it is useful to distinguish between client-side security issues, server-side security issues, and transaction security issues [1]. Furthermore, there are some organizational and legal security issues that should be addressed and considered with care.

2.1 Client-side Security Issues

From the user's point of view, client-side security is typically the major concern. In general, client-side security requires the use of traditional computer security technologies, such as proper user authentication and authorization, boot control, access control, and anti-virus protection. With regard to communication services, the client may additionally require server authentication and non-repudiation of receipt. In addition, some applications may require anonymity (e.g., anonymous browsing on the Web).

2.2 Server-side Security Issues

Contrary to that, server-side security is typically the major concern from the service provider's point of view. Server-side security requires proper client authentication and authorization, non-repudiation of origin, sender anonymity (e.g., anonymous publishing on the Web), audit trail and accountability, as well as reliability and availability.

2.3 Transaction Security Issues

Transaction security is equally important for both the client and the server side. Transaction security requires various security services, such as data authentication, access control, data confidentiality, data integrity, and non-repudiation services [2]. In addition, certain applications may also require transaction anonymity guarantees.

2.4 Organizational and Legal Security Issues

In addition to the technical security mechanisms to address client-side and server-side as well as transaction security, there are also some organizational and legal security issues that should be addressed and considered with care. As pointed out in [3] and [4]:

"Security continues to be and probably will always be a people problem. If you overlook that, you're in trouble."

"The real challenges are human, not technical. Old-timers will recognize a once-popular saying that the most important part of an automobile is the nut that holds the steering wheel. That's still true, even though a modern steering wheel may also contain an air bag and any number of controls and antitheft devices."

An analogy to illustrate the insufficiency of technical security mechanisms is the postal delivery service. Note that the technical security of this service is provided through the technical means of handwritten signatures (to provide data authenticity) and letter envelopes (to provide data confidentiality). Both mechanisms are relatively simple and easy to circumvent. Therefore, additional security mechanisms have been developed and deployed on the organizational and legal side. For example, letters are distributed by postmen, and the privacy of letters makes it a criminal act to illegitimately open a letter.

3 Existing Security Technologies

In the past, several network security technologies have been developed and deployed. In addition to physical security measures, such as dedicated communication links and mechanical locks, network security technologies typically address access control and communication security.

3.1 Access Control

The first and most obvious network security concern addresses access control. How can you control access to intranet resources? How can you make sure that only authorized data traffic is allowed to enter or leave a corporate intranet? There are several technologies that can be used to control access to intranet resources.

- The simplest technology is packet filtering. In addition to routing IP packets, a screening router is configured to decide for each packet, whether it should be forwarded or dropped. Normally, this decision is context-insensitive, meaning that the decision must be made for each packet individually. This poses some problems with regard to context-sensitive packet filtering, such as the one that could be used to adequately filter FTP data traffic and – more generally – data traffic for UDP-based applications.
- In addition to "normal" packet filtering, stateful inspection technologies use state information to make more intelligent decisions regarding the forwarding or dropping of IP packets.
- Furthermore, circuit-level and application-level gateways may be used to provide enhanced security. In the first case, a circuit-level gateway (e.g., a SOCKS server) takes a TCP connection, authenticates and authorizes the client, establishes a second TCP connection to the origin server, and copies data forth and back. In addition to this proxy mechanism, an application-level gateway (e.g., a HTTP proxy server) understands the application protocol being spoken and is therefore able to make more intelligent decisions.

In summary, access control technologies and corresponding security mechanisms are well understood and widely deployed for IP-based networks.

3.2 Communication Security

Communication security services can be provided by cryptographic security protocols, that may operate at different layers of the corresponding communications proto-

col stack. With regard to TCP/IP networking, exemplary protocols include:

- The Point-to-Point Tunneling Protocol (PPTP) that operates at the network access layer;
- The IPsec protocols that operate at the Internet layer;
- The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as the Secure Shell (SSH) products that operate at the transport layer;
- Several security-enhanced application protocols as well as authentication and key distribution systems (e.g., Kerberos) that operate at or above the application layer.

The various security protocols have specific advantages and disadvantages [5,6].

3.3 Current Research and Development Activities

As of this writing, network security is a hot topic, and a large number of corresponding research and development projects address the following fields of study:

- Cryptographic primitives (e.g., cryptographic algorithms, protocols, and applications);
- Electronic payment systems (e.g., electronic macropayment and micropayment systems as well as corresponding negotiation mechanisms);
- Security implications of executable content and mobile code (e.g., Java applets, and ActiveX controls);
- The use of security scanners and intrusion detection systems (IDS) to replace formal risk analysis;
- Content rating schemes (e.g., PICS) to replace content blocking strategies based on IP address or URL filtering;
- Security in multicast environments (e.g., the development of efficient encryption algorithms and scalable key distribution protocols);
- Security aspects of resource reservation and corresponding billing schemes (e.g., RSVP);
- Hardware support (e.g., smartcards and key agile ATM encryptors).

4 Additional Requirements

The security requirements of e-commerce and e-commerce applications generally go beyond the more traditional requirements of network security. This is particularly true for the requirements that address the complexity and availability of cryptographic applications, the anonymity of participating peers, the autonomy of mobile code, the manageability of trust, and the necessity for intellectual property protection.

4.1 Complexity

In e-commerce applications there are typically multiple parties and protocols involved. This complicates the design, implementation, and verification of these applications considerably. Also, attackers have many more opportunities and possibilities to attack the resulting applications. Furthermore, the cryptographic protocols must not only be complete and sound, but also efficient (or "scalable") and fair (or "multilaterally secure").

4.2 Availability

Many e-commerce applications require the permanent availability of specific parties, such as key distribution centers (KDCs) or certificate revocation components in public key infrastructures (PKIs). Consequently, there are many opportunities and possibilities to successfully launch denial-of-service and degradation-of-service attacks. More common examples include e-mail bombing and TCP SYN flooding attacks. Less common examples include resource clogging attacks against key exchange and management protocols.

4.3 Anonymity

Some parties may want to stay anonymous in specific e-commerce transactions. Examples include stock brokers querying specific quotes. Unfortunately, anonymity requirements are generally at odds with other security requirements, such as authentication and non-repudiation, and the resulting conflicts must be resolved.

4.4 Code Autonomy

A couple of years ago, many people were talking about thin clients, network computers, and similar buzzwords. Nowadays, many people are talking about mobile code and agent-based systems as being the next computing paradigm (after host-based and client/server computing). In fact, it is often argued that future e-commerce applications will require mobile code to roam autonomously through computer networks on the user's behalf. Obviously, there are many security concerns related to mobile code and agent-based systems, and these concerns are far away from being solved.

4.5 Trust Management

The success of e-commerce applications will depend on the manageability of trust. Establishing a public key infrastructure (PKI) and corresponding electronic or digital signature laws are only building blocks for the more general problem related to "trust management".

4.6 Intellectual Property Protection

A multimedia document contains digital data that may encode text, images, audio, and video. The digital representation and distribution of multimedia documents have increased the potential for misuse and theft, and have significantly intensified the problems associated with copyright protection and enforcing these rights. The problems are rooted from the intrinsic characteristics of digital data, namely that making and distributing copies is easy, inexpensive, and fast, and that each copy is identical to the original. Consequently, intellectual property protection is a prerequisite for the successful deployment of e-commerce applications that address the distribution of immaterial goods, such as MP3 music files.

5 Research Agenda

Referring to the additional requirements overviewed in the previous section, the following research agenda may be derived.

5.1 Complexity

First and foremost, a framework must be developed in which possible attacks against cryptographic primitives (algorithms, protocols, and applications) can be explored and systematically investigated. Note that the coexistance of multiple parties and multiple protocols in an e-commerce application offers new possibilities to attack the systems involved. In addition, provably secure cryptographic primitives must be developed, and it must be clarified what „provably secure“ actually means in this framework. Finally, research must address and elaborate on new security technologies, such as quantum cryptography, and study the implications of evolving technologies, such as quantum computing or DNS computing, to the cryptanalytical strength and security of existing cryptographic primitives.

5.2 Availability

With regard to the evolving Internet-based e-commerce, new security techniques must be developed that can be used to protect against denial-of-service or degradation-of-service attacks. Similarly, new security techniques must be developed that don't require (or at least minimize the existence of) online components. Furthermore, the trade-offs between the replicability of a security service and its own security is an interesting field of study. In fact, the study of these trade-offs may lead to the development of more sophisticated techniques that can be used to securely replicate security services.

5.3 Anonymity

For certain e-commerce applications, it will be necessary to develop techniques that can be used to provide

- Receiver anonymity services (e.g., anonymous browsing on the Web);
- Sender anonymity services (e.g., anonymous publishing on the Web);
- Transaction anonymity services (e.g., military applications and stock trade broker systems);

There are several techniques under investigation that can be used to provide the anonymity services mentioned above [7]. These techniques must be further refined and explored in real-world applications. Furthermore, it will be important to study the relationship between anonymity services and other security services, such as access control and peer-entity authentication services.

5.4 Code Autonomy

With regard to mobile code and agent-based systems, it will be important to study and to find solutions for the problems of (a) how to protect mobile code against potentially malicious hosts and runtime environments, and (b) how to protect hosts and runtime environments against potentially malicious mobile code. The two problems must be studied either individually or collectively. Unfortunately, the two problems are not independent, and solutions for problem (b) may severely limit the practicability of solutions for problem (a). The interdependence of the two problems and their solutions is an important field of study for the further deployment of mobile code and agent-based systems.

5.5 Trust Management

Many e-commerce applications require one (or several) PKI(s) to be existant and fully operational. Consequently, a lot of work is being done in establishing PKIs. However, it is not clear what the basis for a PKI should be. In particular, there are two competing philosophies:

- The ITU-T recommendation X.509 and the IETF Public Key Infrastructure X.509 (PKIX) WG assume the existance of a global name space;
- The proponents of the SDSI initiative and the IETF Simple Public Key Infrastructure (SPKI) WG don't assume a global name space but use linked local name spaces instead [7].

Another question relates to the authorization problem for e-commerce applications. It is not clear at the moment, what approach is best suited for e-commerce applications. Finally, the manageability of trust will also depend on the existence of appropriate user interfaces.

5.6 Intellectual Property Protection

For certain e-commerce applications, such as digital libraries and online publishing services, it will be important to have digital copyright labeling techniques (i.e., watermarking and fingerprinting techniques). These techniques can be used to secretly embed digital marks into a material to designate copyrights-related information, such as origin, owner, content, or recipient (note that digital copyright labeling is not contrary to usage control; it is rather complementary). Consequently, digital copyright labeling techniques must be developed that are efficient, robust, and secure. Eventually, it may also be necessary to develop and use asymmetric digital copyright labeling techniques (similar to the use of asymmetric cryptosystems to provide non-repudiation services).

6 Conclusions

Security is a hot topic today (this is equally true for network and e-commerce security). Consequently, a lot of research is going on and many security products are being developed and marketed.

In this situation, it is important to note that security is a system property that is not fully provable. The best we can do is to show that a specific system is resistant against a set of well-known attacks. Since we don't know all possible attacks in advance, it's impossible to say whether a system is secure (resistant against all possible attacks). Nevertheless, it is sometimes possible to make stronger arguments. For example, it is sometimes possible to prove that a cryptographic primitive is secure under certain (unproven) assumptions (e.g., that factoring a big integer or computing a discrete logarithm is hard). The opposite - to prove that a system is insecure - is much easier. It generally suffices to find a possible attack to break the system entirely or partially (e.g., finding a flaw in a pseudo-random number generator). More worrisome, even a rumour is sometimes sufficient to break the security (or at least the commercial value) of a system.

Note that security engineering is different from any other type of engineering [8]:

- Most engineering involves making things work;
- Contrary to that, security engineering involves figuring out how to make things not work or how to make them work differently and then preventing the corresponding failures.

Consequently, security engineering involves making sure things do not fail in the presence of an intelligent and malicious adversary who forces faults at precisely the wrong time and in precisely the wrong way.

Also note that security is orthogonal to functionality. This is reflected in some evaluation and certification criteria, such as the ITSEC or the Common Criteria. Just because a product functions properly does not mean that it's secure. Similarly, just because a product is secure does not mean that it's functional. Unlike functionality, security is not necesarily visible to the user and is particularly hard to market (the autombile industry has the same problem). For example, bad cryptography looks like good cryptography, and it's hard to tell the difference (even for an experienced expert).

The way we (try to) achieve security on the highway system offers another analogy that may help understand the role of security in e-commerce. We have driver license tests, car admission tests, educational programs, traffic laws, and a police to enforce these laws. All these mechanisms are currently being discussed to be used on the Internet (or any other information superhighway). For example, there are more or less serious discussions going on, whether computer systems that are connected to the Internet should be evaluated and certified in one way or another. Similar discussions are going on that address certification programs for Internet users. Finally, the discussions about the necessity of Internet laws and police organizations to enforce these laws is also being led. Stay tuned for the results of these discussions.

References

[1] L.D. Stein, *Web Security: A Step-by-Step Reference Guide*, Addison-Weseley, Reading, MA, 1998

[2] ISO/IEC 7498-2, Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, 1989

[3] R.H. Baker, *Computer Security Handbook,* McGraw-Hill, New York, NY, 1991

[4] R.H. Baker, *Network Security: How to Plan for it and Achieve it*, McGraw-Hill, New York, NY, 1995

[5] R. Oppliger, *Authentication Systems for Secure Networks.* Artech House, Norwood, MA, 1996

[6] R. Oppliger, *Internet and Intranet SecuritySecurity.* Artech House, Norwood, MA, 1998

[7] R. Oppliger, *A Security Primer for the World Wide Web.* Artech House, Norwood, MA, to be published in 1999

[8] B. Schneier, „Version 2.0 – Flaws in Cryptographic Systems", Keynote Speech at PKC ´99, April 12, 1999