

Information and Communication Management in Business Information Systems

Pavel OCENASEK

ocenaspa@fit.vutbr.cz

Brno University of Technology, FIT, Bozotechnova 2, Brno, Czech Republic

Keywords: Information, Communication, Security, Business Information System.

Abstract. This paper outlines a security management of information exchange and communication in business information systems. It is focused primarily on business applications that include the payment protocol implementation and therefore require security properties achievement.

Introduction

The actual popularity of business applications and information systems like internet banking and electronic commerce has created both risks and opportunities. Many of risks stem from security issues, which can be ruinously expensive. One of the solutions is the use of security (a.k.a. cryptographic) protocols where information is exchanged in a way intended to provide security guarantees.

Business Information Systems

Payment Protocols

There a category of communication protocols - payment protocols [1]. These protocols are widely used in electronic commerce. The SET protocol has been proposed by a consortium of credit card companies (Mastercard, Visa) and software corporations to secure e-commerce payments. When the customer makes a purchase, the SET dual signature guarantees authenticity while keeping the customer's account details secret from the merchant and his choice of goods secret from the bank.

For a comparison of payment protocols, their specification and properties we refer to the author's publication [2] or [3].

Security Protocol Life Cycle

The lifecycle of security protocol is similar to payment protocol life cycle and is shown on Fig. 1. The designer comes with the idea of new protocol goals. The next step is the protocol design (in most cases analytic). The design process usually employs some verification techniques, which the author uses to check whether the designed protocol contains flaws or is vulnerable to cryptographic attacks.

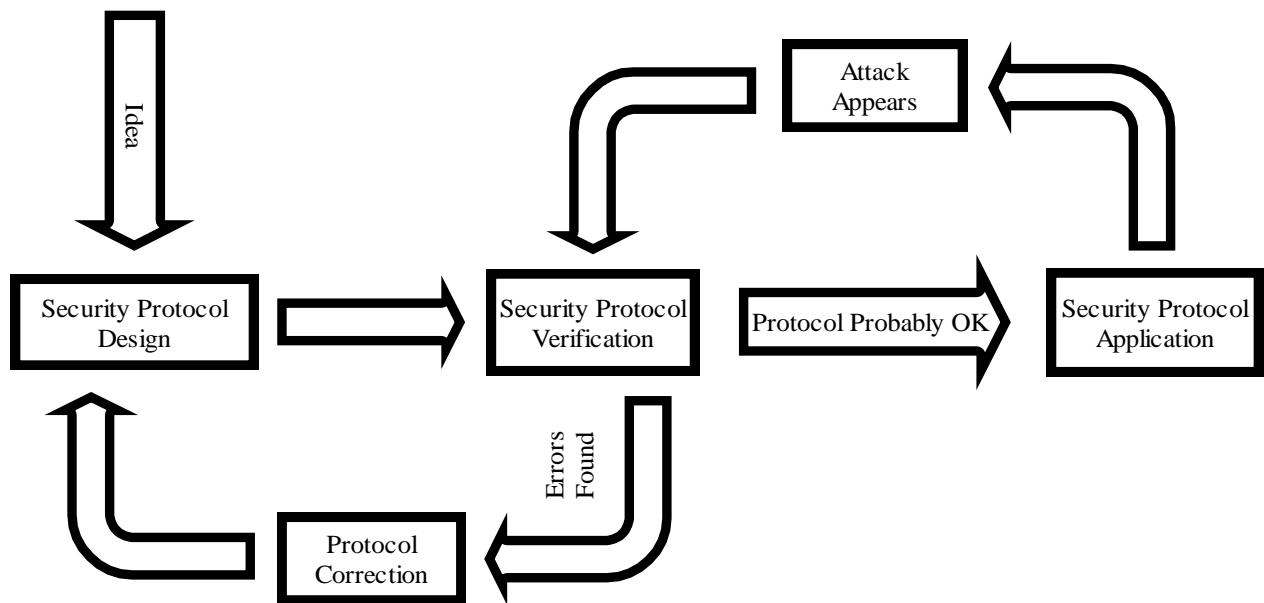


Figure 1. Security Protocol Life Cycle

After the “probably successful” verification, the protocol is being used in the real network applications. We use the quotes because not every verification method can discover all flaws and attacks, some security issues may not appear until the protocol is applied in the real conditions. When this happens, researchers go back to use the verification approaches (either analytic or automated) and try to design another (corrected) version of the protocol.

Theory of Protocols with Security Properties

Introduction

Protocols with security properties are used for secure communication of subjects over an insecure network. A crucial goal is to prevent a spy from reading the contents of messages addressed to others (secrecy). Most security protocols also guarantee an authenticity. This means that if a message appears to be from a subject A, then A sent precisely this message and it contains the indication of its integrity.

Because security protocols may contain certain security issues and flaws, finding such attacks is the purpose of formal verification. There have been written many papers and publications concerning formal verification methods. For introduction in this area, we recommend mainly the following papers: [4], [5] and [6]. There are also books about protocol verification available, such as [BM03], [7] and [8].

Dolev and Yao

Dolev and Yao [9] proposed the first algebraic model for the security protocols. Their protocols dealt more with the distribution of secrets than authentication, although the two are closely linked. The main difference is that we generally think of authentication as involving a third party authentication server, whereas the Dolev and Yao protocols dealt with only two parties.

Dolev and Yao define some classes of protocols [9]. In their paper, they reason about these classes of protocols rather than individual protocols themselves, and prove some interesting properties of these classes. For example, cascade protocols and name-stamp protocols are examined. A cascade protocol is a protocol in which a user can apply the public key encryption-decryption operations in several layers, to form messages. The authors prove that such protocols are secure if and only if the following conditions hold.

1. The message transmitted between X and Y always contains some layers of encryption functions $E_{\neg x}$ or E_y
2. In generating a reply message, each participant A ($A = X, Y$) never applies a decryption function without also applying an encryption function.

Similarly, Dolev and Yao presented a polynomial time algorithm for deciding if a given name-stamp protocol is secure. Dolev and Yao not only show how to model protocols algebraically, they consider whole classes of protocols and demonstrate how to reason about any protocol that shares certain properties.

Security Properties

The following text describes selected security properties in details. Some of the definitions come from or are inspired by [10].

Authentication

This term denotes the process of identity verification.

ENTITY AUTHENTICATION

Assuring one party identity through the presentation of evidence and/or credentials of the identity of a second party involved in a protocol, and the fact that the second party has actually participated during the execution of the current run of the protocol.

MESSAGE ORIGIN AND INTEGRITY

The protocol must provide means to ensure confidence that a received message or a piece of data has been created by a certain party at some time in the past, and that this data has not been corrupted.

REPLAY PROTECTION

Assuring one party that an authenticated message is not old. This property deals with the freshness of messages.

Key Agreement

KEY AUTHENTICATION

Mechanism where one party is assured that no other party aside from a specifically identified second party may gain access to a particular secret key.

KEY CONFIRMATION

One party is assured that a second party actually has possession of a particular secret.

FRESH KEY DERIVATION

The protocol uses dynamic key management in order to derive fresh session keys.

Confidentiality (Secrecy)

The property that a particular data item or information is not made available or disclosed to unauthorized individuals and remains unknown to the intruder.

Non-Repudiation

Non-repudiation protocols must ensure that when two subjects exchange information over a protocol, neither one nor the other can deny participation in this communication. A typical non-repudiation protocol can provide a number of different non-repudiation services [11], like non-repudiation of origin, non-repudiation of receipt and fairness, but the actual non-repudiation services provided by a protocol depend mainly on its application.

PROOF OF ORIGIN

Non-repudiation of origin provides the recipient with the evidence, which ensures that the originator will not be able to deny having sent the message. The evidence of origin is generated by the originator and held by the recipient.

PROOF OF DELIVERY

Non-repudiation of delivery is intended to provide evidence that the recipient received the message. This service also only applies when the protocol uses a third trusted party. Evidence of delivery is generated by the delivery subject, and will be held by the originator.

PROOF OF RECEIPT

Non-repudiation of receipt provides the originator with the evidence, which ensures that the recipient will not be able to deny having received the message. The evidence of receipt is generated by the recipient and held by the originator.

PROOF OF SUBMISSION

Non-repudiation of submission is intended to provide evidence that the originator submitted the message for delivery. This service only applies when the protocol uses a third trusted party. Evidence of submission is generated by the delivery subject, and will be held by the originator.

Fairness

The fairness can be defined as a function of non-repudiation of origin and of non-repudiation of receipt. If either both these properties are ensured or both are flawed for a given message, then we have fairness.

Attacks on Security Protocols

Post-design analysis of security protocols is very important because there are no guarantees that a given protocol is correct. This chapter deals with the basic attacks on security protocols that should be considered during the verification process.

Generally, attacks can be divided into two categories – active and passive attacks.

Active Attacks

These involve trying to modify data during transmission.

Passive Attacks

The goal here is not to modify the data but rather to capture the data being transmitted by eavesdropping. Passive attacks are also used for capturing information that can help attacker create a map of communication subjects, which usually forms the preamble of an active attack.

The description of particular attacks follows.

Eavesdropping

Eavesdropping attack occurs through the interception of a network communication. It just stands for a secretly listening to a communication between subjects. We can prevent eavesdropping by applying some cryptographic functions such as encryption. For example, the communication keys are usually considered secret so they are not allowed to be sent in the communication unencrypted.

Replay Attack

Replay attacks are caused by an intruder monitoring and storing network communication over a period of time, and later using it against the involved parties. An intruder can basically capture valid protocol communication, which would be authentic with the client and server. Later, when the client or the server is no longer active, the intruder can pretend to be the client or the server and initiate a session with the partner.

Man-in-the-Middle Attack

In this attack, an attacker intercepts a message exchange, and pretends to be a sender to the receiver and a receiver to the sender. These attacks essentially hijack one of the two endpoints of the communication. The attack can take place during authentication sequence, but the worse scenario is when it can occur over an already established session.

Acknowledgement

This project has been carried out with a financial support from the Czech Republic through the project no. MSM0021630528: Security-Oriented Research in Information Technology and by the project no. ED1.1.00/02.0070: The IT4Innovations Centre of Excellence; the part of the research has been also supported by the Brno University of Technology, Faculty of Information Technology through the specific research grant no. FIT-S-14-2299: Research and application of advanced methods in ICT.

References

- [1] Kailar, R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, Vol. 22, Issue 5, May 1996.
- [2] Ocenasek, P. Payment Protocols Used in Electronic Commerce, In: Management, Economics and Business Development in the New European Conditions, Brno, CZ, 2007.
- [3] Ocenasek, P., Kučerová, P. A Comparison of Czech and Foreign Payment Systems, In: Management, Economics and Business Development in the New European Conditions, Brno, CZ, CERM, 2008, ISBN 978-80-7204-582-2.
- [4] Gritzalis, S. Security protocols over open networks and distributed systems: Formal methods for their Analysis, Design and Verification, University of Aegean, Greece, Computer Communications, Vol. 22, Issue 8, 1999, p. 695-707.
- [5] Ma, L., Tsai, J. Formal Verification Techniques for Computer Communication Security Protocols. Handbook of Software Engineering and Knowledge Engineering, World Scientific Publishing Company, 2000.
- [6] Leathrum, J.F., Morsi, R., Leathrum, T.E. Formal Verification of Communication Protocols, 1996 [online] Available at: <http://www.ece.odu.edu/~leathrum>
- [7] Holzmann, G.J. Design and Validation of Computer Protocols. Prentice Hall, 1991, ISBN 0-13-539925-4.
- [8] Schneider, S.A., Ryan, P.Y.A. Modelling and Analysis of Security Protocols. Addison-Wesley, Boston, USA, 2000, ISBN 0-201-67471-8.
- [9] Dolev, D., Yao, A. On the security of public-key protocols. Communications of the ACM, Vol. 29, August 1983, p.198—208.
- [10] AVISPA: Deliverable: List of selected problems. Automated Validation of Internet Security Protocols and Applications [online] Available at: <http://www.avispa-project.org>.
- [11] Santiago, J., Vigneron, L. Study for Automatically Analysing Non-repudiation. In: Actes du 1er Colloque sur les Risques et la Sécurité d'Internet et des Systèmes, CRiSIS, Bourges, France, October 2005, p. 157-171.