Chapter 29
An Electronic Contract Signing Protocol Using Fingerprint Biometrics

Harkeerat Bedi
University of Tennessee at Chattanooga, USA

Li Yang
University of Tennessee at Chattanooga, USA

Joseph M. Kizza
University of Tennessee at Chattanooga, USA

ABSTRACT

Fair exchange between a pair of parties can be defined as the fundamental concept of trade where none of the parties involved in the exchange have an unfair advantage over the other once the transaction completes. Fair exchange protocols are a group of protocols that provide means for accomplishing such fair exchanges. In this chapter we analyze one such protocol which offers means for fair contract signing, where two parties exchange their commitments over a pre-negotiated contract. We show that this protocol is not entirely fair and illustrate the possibilities of one party cheating by obtaining the other's commitment and not providing theirs. We also analyze a revised version of this protocol which offers better fairness by handling many of the weaknesses. Both these protocols however fail to handle the possibilities of replay attacks where an intruder replays messages sent earlier from one party to the other. Our proposed protocol improves upon these protocols by addressing to the weaknesses which leads to such replay attacks. We implement a complete working system which provides fair contract signing along with properties like user authentication and efficient password management achieved by using a fingerprint based authentication system and features like confidentiality, data-integrity and non-repudiation accomplished through implementation of cryptographic algorithms based on elliptic curves.

DOI: 10.4018/978-1-4666-2919-6.ch029

INTRODUCTION

Commerce has come a long way since the beginning of our civilization. The ability to exchange goods and services for items of equivalent value has been widely exercised. Based on the kind of items exchanged between two parties, it can either be classified as a barter system where goods and services are exchanged for other goods and services, or the act of selling and buying where goods and services are sold or bought between parties in exchange for money.

The notion of *fair exchange* can be expressed as the ability to exchange goods or services for other goods or services in a fair manner where both the parties obtain what they expected. Being a fundamental concept, this can be implemented in various scenarios that may include exchanges based on barter system or buying and selling of goods.

With the advent of computers and the Internet, new means of performing commerce have been invented. E-commerce is one such solution where good and services are bought and sold between interested parties using computers over a network. With the rapid growth of the Internet, the magnitude of commerce performed online has also increased significantly. This increase is primarily because commerce conducted online is convenient and fast when compared to the traditional methods of trade. Even though commerce of this type offers benefits like speed and convenience, without properties like fairness and security, such services become less useful as they significantly increase the risk of failure. E-commerce cannot flourish or even sustain if it is not able to provide fairness and security. Therefore the concept of fair exchange plays a vital role in shaping such forms of commerce. When carried out online using computers and the Internet, such fair exchange is known as *fair electronic exchange*.

FAIR ELECTRONIC EXCHANGE

Fair electronic exchange can be demonstrated as e-commerce that takes place between two parties who are online and where exchange of goods and services is performed such that both parties either obtain what they expected or they obtain nothing at all. After an exchange is performed or aborted prematurely, none of the parties should have an unfair advantage over the other. If cheating takes place, where one party refuses to present their part of the exchange, other means for providing fairness should be available. These may include use of additional entities like a human judge or electronic ones that can comprehend the situation and act accordingly to provide fairness. Protocols that provide such facilities are known as *fair exchange protocols*. Such protocols can be used for the following purposes:

a. **Certified E-Mail (CEM):** where a user named Alice sends a message to a user named Bob and gets a receipt from him in return. Providing the quality of fairness would include Alice getting the receipt only when Bob gets the message or Bob getting the message only when Alice gets the receipt.
b. **Electronic Contract Signing (ECS):** where both Alice and Bob wish to sign a contract that has already been negotiated. This would involve Alice sending her commitment (digital signature) on the contract to Bob and him sending his commitment on the same in return. Providing fairness would involve Alice receiving Bob's commitment only when her commitment is received by Bob and vice versa. This example demonstrates contract signing between two parties. However, various multi-party contract signing protocols also exist and have also been proposed in (Baum-Waidner, 2001; Ferrer-Gomila, Payeras-Capella, Huguet-Rotger, 2001; Garay & MacKenzie, 1999).

Related Content

Developing Secure Software Using UML Patterns
Holger Schmidt, Denis Hateburand Maritta Heisel (2015). *Standards and Standardization: Concepts, Methodologies, Tools, and Applications (pp. 228-264).*
www.irma-international.org/chapter/developing-secure-software-using-uml-patterns/125296

Information and Communication Technology Security Network: A Sure Solution to E-Governance Security Problems
Ogochukwu Thaddaeus Emiriand Chukwunweike Gracious Omede (2011). *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements (pp. 421-433).*
www.irma-international.org/chapter/information-communication-technology-security-network/45398

Framework Design and Case Study for Privacy-Preserving Medical Data Publishing
Yu Niu, Ji-Jiang Yangand Qing Wang (2015). *Standards and Standardization: Concepts, Methodologies, Tools, and Applications (pp. 1115-1130).*
www.irma-international.org/chapter/framework-design-and-case-study-for-privacy-preserving-medical-data-publishing/125338

The Role of Technology Standardization in RFID Adoption: The Pharmaceutical Context
May Tajima (2012). *International Journal of IT Standards and Standardization Research (pp. 48-67).*
www.irma-international.org/article/role-technology-standardization-rfid-adoption/64322

The Effect of Pre-Existing Standards and Regulations on the Development and Diffusion of Radically New Innovations
J. Roland Orttand Tineke M. Egyedi (2014). *International Journal of IT Standards and Standardization Research (pp. 17-37).*
www.irma-international.org/article/the-effect-of-pre-existing-standards-and-regulations-on-the-development-and-diffusion-of-radically-new-innovations/111333