Chapter 8
Applied Cryptography in Electronic Commerce

Sławomir Grzonkowski
National University of Ireland, Ireland

Brian D. Ensor
National University of Ireland, Ireland

Bill McDaniel
National University of Ireland, Ireland

ABSTRACT

Electronic commerce has grown into a vital segment of the economy of many nations. It is a global phenomenon providing markets and commercialization opportunities world-wide with a significantly reduced barrier to entry as compared to global marketing in the 20th century. Providing protocols to secure such commerce is critical and continues to be an area for both scientific and engineering study. Falsification, fraud, identity theft, and disinformation campaigns or other attacks could damage the credibility and value of electronic commerce if left unchecked. Consequently, cryptographic methods have emerged to combat any such efforts, be they the occasional random attempt at theft or highly organized criminal or political activities. This chapter covers the use of cryptographic methods and emerging standards in this area to provide the necessary protection. That protection, as is common for web-based protocols, evolves over time to deal with more and more sophisticated attacks. At the same time, the provision of security in a manner convenient enough to not deter electronic commerce has driven research efforts to find easier to use and simpler protocols to implement even as the strength of the cryptographic methods has increased. This chapter covers current standards, looking at several facets of the secure commercialization problem from authentication to intrusion detection and identity and reputation management. Vulnerabilities are discussed as well as capabilities.

DOI: 10.4018/978-1-61520-783-1.ch008

INTRODUCTION

Commerce is defined as the exchange between parties of goods and services, typically for money. While the exchange of items or services is seen in some non-human species, mating gifts or chimpanzees exchanging grooming with each other for example, the practice of commerce on a significant scale, and in the manner we understand it today, is an intrinsically human phenomenon.

Ecommerce, at its most basic, is simply commerce as usual but transacted using electronic communication methods such as telephone or internet. Primarily, however, ecommerce is coming to be understood as the transaction of business across the internet or 3G cell networks.

Ecommerce brings challenges with it that are unique in the history of commerce. The physical presence of the two parties or of an intermediary, in traditional commerce has always added a degree of security and trust in commercial activities. The use of physical currency demonstrated the ability to pay and the exchange of currency or promissory notes demonstrated the willingness to complete the transaction. While transactions could occur anonymously and untraceably, there was still a component of verification that a transaction was desired.

Ecommerce, on the other hand, is conducted remotely, without the physical presence of the parties and largely anonymously. Mediated electronically, the transaction converted into nothing more than a stream of bits, ecommerce transactions are, in the initial aspect, completely without security or trust. The necessity of other forms of trust became immediately obvious.

Security and trust in economic transactions falls into the areas of verification and authentication. Verification of the transaction and authentication of the parties is vital to the ecommerce model. However, anonymity is still a desirable trait in many transactions and authentication processes need to take this into account.

Identity theft was a cumbersome and manual process for many years, but the advent of electronic records, communications, and commerce has made identity theft far easier and far more prevalent. Governments were unprepared for the possibilities of widespread internet-based identity theft. The notion of a single, widely available, number used to identify an individual was hopelessly susceptible to attack. The ability of computing systems to correlate and mine seemingly disparate and unconnected information was demonstrated and highlights the problem of security in the near panopticon of the internet's vast databases of personal information.

An aspect of ecommerce that is not as prevalent in traditional transactions is the ability to hijack the transaction. It is far more possible for eavesdroppers to access, copy, redirect, and subvert legitimate transactions and the intents of the parties in electronically mediated transactions.

Consequently, an emerging science and industry have grown up around these security and authentication holes. New methods of encrypting transactions, of authenticating participants, and of protecting the identities of participants have been created and distributed. New understandings of the ethics and consequences of anonymous transactions have been elucidated. New discussions of the rights of privacy and of government and private enterprise scrutiny of individuals and their lives have become commonplace.

Without trustable, verifiable, and simple security processes built into the workflow of ecommerce, the current explosion of commerce onto the web could not have happened. As we move from wired connections to the web, however, new techniques and workflows are needed to ensure that wireless ecommerce transactions, which are easier to intercept and perhaps suborn, are secure and protected.

Without reliable security models which expand over time to meet the attempts to break in and subvert them, ecommerce transactions cannot continue to grow in value and convenience. In