Chapter 9

A Novel Technique for Securing E–Commerce Transaction

Arnab K. Maji
North Eastern Hill University, India

ABSTRACT

The emergence of online businesses along with the use of the Internet as its basic network has brought new concerns and risks to the e-commerce environment. It is essential for the online companies to gain customers’ trust to retain their existing e-commerce market share and provide for growth, because e-commerce transactions take place in an open environment that cannot be trusted since the network is highly vulnerable to outside security threats. The main problem of e-commerce transaction is anonymity. One may steal another’s identity and get access of his confidential information such as banking password, credit card details, etc. very easily. The most convenient way to prevent such kind of identity theft is digital certificate. But that is very expensive. In this chapter, a novel attempt is made to prevent identity theft using Visual Cryptography and Steganography during e-commerce transaction, in a very cost-effective manner.

1. INTRODUCTION

Electronic Commerce is a commercial transactions conducted electronically using computers over a large network like Internet. It involves exchange of business information using EDI (Electronic Data Interchange), email, electronic bulletin boards, online transactions etc. During Online transactions of E-commerce, Identity Theft is identified as a major security threat, as the major problem of internet is anonymity. If we briefly classify the different security issues of E-Commerce they can be classified as:

- **Network Security:** This is probably the most obvious issue for e-commerce applications, since the amount and severity of hack attacks are increasing. Fortunately, significant progress has been made in this area through firewall security products that protect against basic network-level attacks. A proper security strategy should not end here, though.

- **Identity:** Since e-commerce implies trading with potentially unknown and untrusted partners, identification of trading partners can be crucial. Once again, work has
been done to provide standardized methods to identify users by using certificates based on the X.509 standard. Unfortunately the deployment of these certificates for general e-commerce applications has been slow.

- **Authorization:** In order to automate trading processes, it is often required to verify more than identity. Various emerging standards such as certificates, authorization servers and the use of a database with registered users and privileges inside the application, all contribute to address the authorization issue of who may do what.

- **Host and Application Security:** The protection offered by most operating systems falls short in a global networked environment. Efforts such as signed applets and signed executables are commendable, but will most probably not solve the problem of virus and Trojan attacks. In addition to these obvious flaws, more subtle problems such as buffer overflow attacks on certain networked applications can also lead to security compromises.

- **Transaction Security:** The protocols used for electronic transactions range from the primitive to the very sophisticated. Older secure protocols, for example those used in Point of Sale terminals, rely on the DES algorithm, and typically require some form of secure storage for the cryptographic keys. Many newer protocols (e.g. SET) are based on public key mechanisms, but have not yet achieved widespread adoption.

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. The virtual market is facing a continuously growing threat in terms of identity theft (Vasistha, 2005) that is causing short-term losses and long-term economic damage. Among several identity thefts, phishing and its various variants are most common and deterrent to e-commerce. The scams and frauds on internet like identity theft leads to the problem of computer theft and massive penetration and espionage. Phishing is an outcome of unsolicited bulk email and unsolicited commercial e-mail also referred to as spam. Unfortunately some companies realized that not only could they communicate by e-mail with staff and existing business partners, but also they could also reach out to millions of potential new customers on web, introducing themselves and their services for minimum cost and required only a tiny response and service uptake to make it all worthwhile. Email spam has become a fact of life. A variety of new message threats now combine to attack individuals, organizations and businesses and thus prove to be a great threat of e-commerce, they include email born viruses, spyware, adware, Trojan horses, directory harvesting attacks(DHA), denial of services (DOS) attacks and more importantly phishing attacks(Banday, 2007).

So here introduces a new method which can be used as a safe way against online identity theft. In this approach website cross verifies its own identity and proves that it is a genuine website, during E-commerce Transaction before the end users and make the both the sides of the system secure as well as an authenticated one.

The concept of image processing and an improved Visual Cryptography and Steganography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/ or characteristics of the input image. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message.