

# **E-Commerce: Authentication & Security on Internet**

By Jagdev Singh Kaleka

Senior Lecturer, Govt. Polytechnic for Women,  
Deptt. Of Technical Education and Industrial Training, Govt. of Punjab

---

## **Abstract:**

The core of e-business is authentication and authorization. Each of the key e-business security concerns translates into authorization and authentication solution requirements. My paper discusses briefly the various authentication techniques and security standards especially public key cryptography and biometric identification.

## **Detailed Paper**

Internet has turned business upside down. It is helping companies to lower costs dramatically across their supply and demand chains, take their customer service into a different league, enter new markets, create additional revenue streams and redefine their business relationships. Electronic Commerce can broadly be divided into two major areas: business-to-business and business-to-consumer. High business value, long-term relationships, complex business processes, inter-computer communications, security, and a multitude of transaction models dominate B2B transactions. E-commerce is buying and selling of products and services by businesses and consumers over the Internet.

## **Advantages:**

1. Lower Transaction costs
2. Larger purchases per transaction
3. Integration into the business cycle
4. Different ways to shop
5. Improved customer interactions

## **Security Requirements**

Discussion of e-commerce, risk mitigation and security focuses on five key attributes. Any system put in place to facilitate e-commerce should be designed to provide each of these needs:

- 1. Authentication:** means obtaining a level of comfort with a claimed identity. The level of comfort is likely to vary with the value of the transaction and the risk it represents.
- 2. Authorization:** means establishing entitlement based on the authentication performed. Regardless of identity, an individual may not be legally entitled to enter into the transaction.

**3. Transaction Integrity:** Transaction details match the expectations of both parties and can be verified. Neither party nor individuals with access to the transaction in progress should be able to alter the terms once the agreement has been reached.

**4. Non-repudiation:** comprises control to prevent a party from denying the transaction. Technology controls can provide mechanisms by which it is possible to prove that it is highly probable that the party entered into the agreement.

**5. Privacy:** means controls to prevent third parties from gaining access to the information within the transaction.

## **Ideal Security In E-commerce**

As the surge of online consumers continues, e-commerce security is drawing more and more attention from businesses and consumers alike. Some enterprises realize the importance to beef up their security arrangements while others display overconfidence in their traditional solutions. Of the seven security mistakes that companies make, according to the SANS Institute list, reliance on a firewall tops the list. Security supports e-business openness. Despite the threats that security managers face today they have to ensure that the security demands to the end user is low. Security focus at the expense of user interface runs the risk of rejection. Thus a delicate scale balancing the security arrangements and the demands made to the end-user has to be maintained. The main requirements of all the security systems are:

1. Preventing unauthorized insider access
2. Integrating the security infrastructure
3. Protecting decentralized data
4. Protecting assets from hacking

Putting it all together gives us the ideal authentication/ authorization solution.

### **SSL Protocol**

The Secure Sockets Layer (SSL) protocol is a set of rules governing server authentication, client authentication, and encrypted communication between servers and clients. SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers.

SSL requires a server SSL certificate, at a minimum. As part of the initial "handshake" process, the server presents its certificate to the client to authenticate the server's identity. The authentication process uses *Public-Key Encryption* and *Digital Signatures* to confirm that the server is in fact the server it claims to be. Once the server has been authenticated, the client and server use techniques of *Symmetric-Key*

*Encryption*, which is very fast, to encrypt all the information they exchange for the remainder of the session and to detect any tampering that may have occurred.

Servers may optionally be configured to require client authentication as well as server authentication. In this case, after server authentication is successfully completed, the client must also present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established.

**Public key cryptography** is the most mature technology available for this purpose. Public-key cryptography facilitates the following tasks:

1. **Encryption and decryption** allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder. Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A **cryptographic algorithm**, also called a **cipher**, is a mathematical function used for encryption or decryption. With **symmetric-key encryption**, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption. **Public-key encryption** (also called **asymmetric encryption**) involves a pair of keys--a **public key** and a **private key**--associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key.

2. **Tamper detection** allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected. Tamper detection and related authentication techniques rely on a mathematical function called a **one-way hash**. A one-way hash is a number of fixed length with unique value. Any change in the data, even deleting or altering a single character, results in a different value. The content of the hashed data cannot, for all practical purposes, be deduced from the hash--which is why it is called "one-way."

Sometimes, instead of encrypting the data itself, the signing software creates a one-way hash of the data, and then uses your private key to encrypt the hash. The encrypted hash, along with other information, such as the hashing algorithm, is known as a **digital signature**. The digital signature ensures a degree of **non-repudiation**.

3. **Authentication** allows the recipient of information to determine its origin--that is, to confirm the sender's identity. *Client authentication* refers to the confident identification of a client by a server. *Server authentication* refers to the confident identification of a server by a client. Client authentication is an essential element of network security within most intranets or extranets. The sections that follow contrast two forms of client authentication:

a) *Password-Based Authentication*: Almost all server software permits client authentication by means of a name and password. The server maintains a list of names

and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access. Passwords do not offer strong authentication. Passwords must either be memorized or written down. Easily memorized passwords tend to be weak, and any weak password can be discovered using a cracker program. If users avoid easily remembered passwords, they tend to write down their passwords or post them on their monitors. As a result, the secrecy of these passwords cannot be ensured.

*b) Certificate-Based Authentication:* Client authentication based on certificates is part of the SSL protocol. The client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. The server uses techniques of public-key cryptography to validate the signature and confirm the validity of the certificate. Certificate-based authentication is generally considered preferable to password-based authentication because it is based on what the user has (the private key) as well as what the user knows (the password that protects the private key).

The certificate authority in a **Public Key Infrastructure (PKI)** essentially serves as a trusted third party. In that capacity, the certificate authority authenticates a user according to specified criteria, and issues a certificate consisting of both public and private keys. The private key is typically generated on the user's system, and never leaves that computer. This protects the private key so that it never needs to traverse the network. The private key can also be protected by a pass phrase, so that people can't surreptitiously remove the private key. For even greater protection, the private key can be stored on a hardware security token, such as a smart card, which is portable and can be used on multiple computers.

PKI is a strong, reliable technology for securing information traveling through the Internet. PKI provides a channel of trust providing digital certificates that identify individuals or organization with unique digital IDs. The infrastructure of public key technology enables the receipt of requests for certificates, issues certificates, and revokes certificates.

Public-key cryptography can only verify that a private key used to sign some data corresponds to the public key in a certificate. It is the user's responsibility to protect a machine's physical security and to keep the private-key password secret.

***Biometric identification*** provides another mechanism for authenticating identification, and can be used in conjunction with certificates to provide added protection. Biometric techniques include fingerprint identification, retinal or iris scans, face or hand geometry, and voice verification. The most successful biometric systems for performing the positive identification have been those aimed at increasing speed and convenience, while maintaining adequate levels of security: Robustness, Distinctiveness, Accessibility, Acceptability and Availability.

a) *Iris scanning* has made the most spectacular move from development to commercialization. As an identifying body part, the human iris—the colored protein of the eye—has several advantages. It is an integral part of the body, so it is not amenable to

easy modification. Unlike fingerprints, the iris can be imaged from about 1 m away. Yet, like fingerprints, iris patterns are unique to individuals. Even identical twins don't have identical patterns, nor do one person's right and left eyes. The patterns are stable throughout life and only change in a highly predictable manner as the pupil opens and closes in reaction to light. The system uses a mathematical technique called wavelet analysis to translate the image of the iris into a 512-byte pattern called the iris code. Once an iris code is prepared, the algorithm compares a specific code against a group of codes previously stored in the computer.

b) *Finger-imaging* based on the long-established technology of fingerprinting, is the most widespread biometric technology and the one favored by most government agencies. In this approach, an individual places a finger on an optical scanner, which scans in a digitized image of the person's fingerprint.

Other biometric techniques are under development, but all of them have significantly greater error rates than either iris scanning or fingerprint imaging. *Hand dimensions* remain relatively stable but are not sufficiently unique to distinguish people in a large population. There has been considerable research on *facial recognition*, but faces vary depending on expression and are too easy to alter and disguise. *Voice identification* is desirable for remote access applications; however, a person's voice varies with emotion, age, and health, so this approach has not reached the application stage. In some systems, several identification methods are used in combination with fingerprinting.

The false rejection rate—the frequency with which a valid identification is erroneously rejected—is 1% in most systems. False acceptance rates, however, are extremely low, which makes imposture almost impossible.

## **Conclusion**

No matter what the need or solution, there is no such thing as perfect security. Moreover, security in any e-commerce scenario is only as good as the weakest link, which also extends to e-commerce partners. By classifying data and implementing proper control measures, companies can decide what information can be distributed to business partners, and what audit mechanisms should be in place to monitor the activities. Security is not easy, it takes time and perseverance to properly manage and monitor the infrastructure.

Although security needs to be kept simple in order to ensure that all users can understand and adhere to it, it also needs to be sufficiently complex and sophisticated to ensure adequate protection. If the security is difficult to execute because of too many keystrokes or passwords, users will either not use the system or will find a way to circumvent the security system.

## References

1. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition* by Bruce Schneier.
2. *Handbook of Applied Cryptography* by Alfred Menezes, Paul van Oorschot and Scott Vanstone.
3. *Cryptography and Network Security: Principles and Practice (2nd Edition)* by William Stallings.
4. *Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations* -- by Carlisle Adams.
5. *Intelligent Biometric Techniques in Fingerprint and Face Recognition* by L. C. Jain, I. Hayashi, S. B. Lee.
6. *Biometric Identification* by Eric J. Lerner in *The Industrial Physicist* Feb 2000 (Journal).
7. [www.ntsecurity.net](http://www.ntsecurity.net)
8. [www.iplanet.com](http://www.iplanet.com)

## About the Author

### Personal Details

**Jagdev Singh Kaleka**  
Senior Lecturer,  
Govt. Polytechnic for Women,  
Patiala -147003  
Punjab-INDIA  
(91)-175-208929  
Date of Birth : 11<sup>th</sup> July 1970

### Educational Qualification

<u>Degree</u>	<u>Institute</u>	<u>Percentage/CGPA</u>
Bachelor of Engineering	Thapar Institute of Engg. And Tech. Patiala	8.42 (on 10 pt scale) = 76%

### Professional Experience

<u>Title</u>	<u>Period</u>	<u>Department</u>
Lecturer	Sept.1994 to Aug 2000	Deptt. Of Technical Education and Industrial Training. Govt. of Punjab
Senior Lecturer	Sept.2000 till date	-----do-----

### Publications

<u>Title</u>	<u>Presented at</u>	<u>Year</u>
Asynchronous Transfer Mode An Overview	ATM Interact Symposium New Delhi	2001