UNIT-III

Security issues on Web:

E-commerce systems are based upon internet use, which provides open and easy communications on a global basis. However, because the internet is unregulated, unmanaged and uncontrolled, it poses a wide range of risks and threats to the systems operating on it.

The use of the internet means that your internal IT and e-commerce systems are potentially accessible by anyone, irrespective of their location.

Threats from hackers and the risks to business

Some of the more common threats that hackers pose to e-commerce systems include:

- carrying out denial-of-service (DoS) attacks that stop access to authorized users of a website, so that the site is forced to offer a reduced level of service or, in some cases, ceases operation completely
- gaining access to sensitive data such as price lists, catalogues and valuable intellectual property, and altering, destroying or copying it
- altering your website, thereby damaging your image or directing your customers to another site
- gaining access to financial information about your business or your customers, with a view to perpetrating fraud
- using viruses to corrupt your business data

Impact of a security incident on the business

If your website is hacked into, it can have a significant impact upon a business running an e-commerce service. The potential business implications of a security incident include the following:

- direct financial loss as a consequence of fraud or litigation
- subsequent loss as a result of unwelcome publicity
- criminal charges if you are found to be in breach of the Data Protection or Computer Misuse acts, or other regulation on e-commerce
- loss of market share if customer confidence is affected by a DoS attack

The images presented by your business, together with the brands under which you trade, are valuable assets. It is important to recognize that the use of e-commerce creates new ways for both image and brands to be attacked.

Importance of firewall:

Firewall is a software or hardware device that protects your computer from being attacked over the internet by hackers, viruses, and worms. This may occur either at a large corporate network, or simply at a small home network; both have the same security issues.
Having a firewall in each company's internet connection allows the business to setup online rules for the users. For example, with the firewall the company can control the access to certain websites,

giving it the control of how employees use the network. These are the different ways of how a firewall controls the online activities:

- **Packet filtering:** small amount of data is analyzed and distributed according to the filter's standards. .
- **Proxy service:** online Information is saved by the firewall and then sent to the requesting system.
- **Stateful** inspection: matches specific details of a data packet to a database of reliable information.

Firewalls allow you to either add or remove filters based on certain circumstances such as:

IP addresses: If a certain IP address, not belonging to the company's network is accessing too many files from the server, this IP can get blocked by the firewall.
Domain names: with the firewall, a company is able to block or allow access to certain domains.
Specific words and phrases: The firewall will scan each packet of information to match the filter content. You may select any word or sentence to be blocked.

Protect your home computer at home by turning on a firewall, or if you have more than one, use a hardware firewall (such as a router) to protect your network. If you use a "public" computer, you should follow the network administrator's policy.

Even though some firewalls offer virus protection, it is recommended to install anti-virus software on each computer. Depending on the layers of security you use, you will determine how many threats can be blocked by your firewall, and prevent any outside user to login into your private network.

In cases when you need to allow remote access from others to your network, you may create a DMZ (Demilitarized Zone). This is an option provided by most of the software firewalls; they will designate a directory on the gateway computer as a DMZ.

Firewall components:

A firewall is a collection of hardware and software that, when used together, prevent unauthorized access to a portion of a network.

A firewall consists of the following components:

- **Hardware**. Firewall hardware usually consists of a separate computer dedicated to running the firewall software functions.
- **Software**. Firewall software can consist of some or all of these applications:
    - Packet filters
    - Proxy servers
    - SOCKS servers
    - Network address translation (NAT) services
    - Logging and monitoring software

- Virtual private network (VPN) services

Transaction Security:

Electronic commerce lets companies integrate internal and external business processes through information and communication technologies. Companies conduct these business processes over intranets, extranets, and the Internet. E-commerce lets businesses reduce costs, attain greater market reach, and develop closer partner relationships. However, using the Internet as the underlying backbone network has led to new risks and concerns. Often, industry analysts cite trust and security as the main hurdles in growing e-commerce. A number of factors have hampered the growth of e-commerce in developing countries. Yet, the main perceived obstacle to increased Internet usage is very similar in companies from both developed and developing countries. Firms already using the Internet consider the lack of network security to be the primary problem, followed by slow and unstable connections. This litany of evolutionary phases masks a number of growing technical challenges, including following.

- Security and authentication
- Content management and publication
- Reliable systems, messaging, and data
- Complex interactions and transactions
- Business model implementation and business process enactment
- Distributed processing and distributed data

E-commerce applications are categories into different types

- B2B – Business to Business E-commerce
- B2C – Business to Consumer
- C2C-Consumer to Consumer
- B2E – Business to Employee
- C2B-Consumer to Business
- G2G- Government to Government

The online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce. This paper is organized as follows. Section I is introduction which gives brief ides about E-commerce applications. Section II focused on security challenges in the E-commerce Applications. Section III discusses security-oriented transaction privacy design model for e-commerce

Emerging Client Server:

E-Commerce involves doing transactions on the Internet be it online shopping, online banking, business to business commerce, EDI - Electronic Data Interchange, and a whole bunch of other stuff that can be handled over remote sites automatically without any human intervention.

E-Commerce Applications need not necessarily only have Web-based front-ends. They can also be an Application running on your Command Prompt that talks to server components elsewhere or it can be a typical Windows Application with a GUI front-end which may once again talk to server components elsewhere on a network.

E-Commerce Applications with Browser front-ends are called **Thin-Client** applications. E-Commerce Applications which have an Application based front-end (or more specifically native Applications that run on an OS instead of a browser) with all the native Windows-like GUI -- buttons, list-boxes, edit-controls, etc. are called **Fat-Client** E-Commerce Applications.

Creating E-Commerce Applications generally involves building and interacting with Components that are distributed all over the network. Each E-Commerce Application can be divided into multiple Tiers. These Tiers are classified depending on what tasks they perform. These are generally broadly classified into

1. **Presentation Services** or **User Interface Tier (Client Tier)**
2. **Business Logic** or **Middleware Tier**
3. **Database Services** or **Data Source Tier**

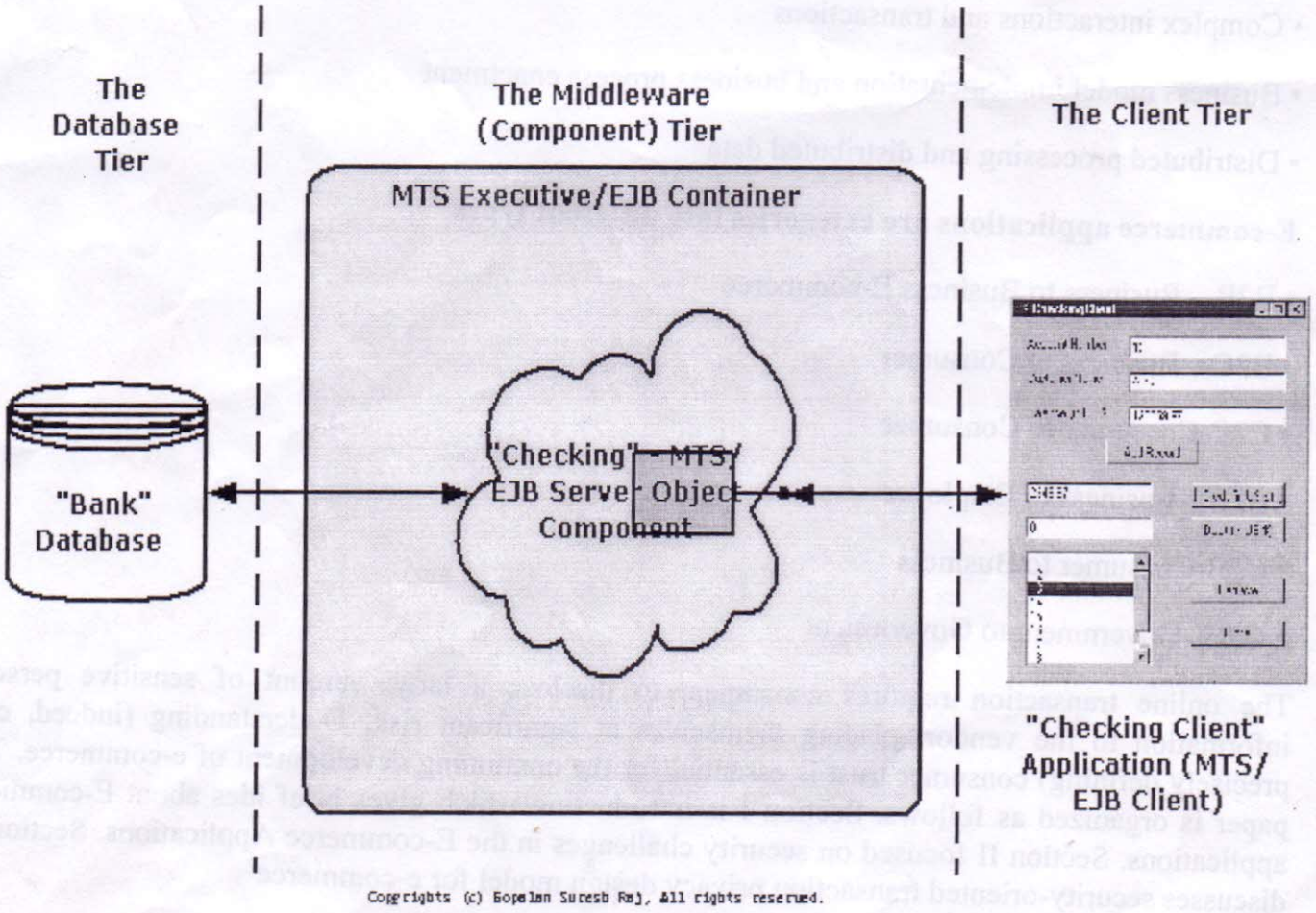


Figure: A Typical 3-tier E-Commerce Application - A Banking Application (Fat-Client)

Once again when building an E-Commerce Application you have to decide which technology you want to go with.

1. Microsoft has COM+/Windows DNA, and the .NET Framework,
2. Sun has Java/J2EE,
3. OMG has CCM/CORBA 3.0

Security Threats:

Most businesses that have made the move towards an online presence have experienced some kind of security threat to their business. Since the Internet is a public system in which every transaction can be tracked, logged, monitored and stored in many locations, it is important for businesses to understand possible security threats to their business.

There are many threats to e-commerce that may come from sources within an organization or through some external channel. The following are the top corporate security threats categorized by internal and external threats.

1. Unauthorized internal users who accesses confidential information by using a stolen passwords for the purpose of committing fraud or theft.

2. Former employees of an organization that maintain access to information resources directly by creating alternative passwords, "back doors into the computer system, or indirectly through former co-workers.

3. Weak access points in information infrastructure and security that can expose company information and trade secrets.

4. Management that undermines security is maybe the greatest risk to e-commerce as there are continuously new ˜electronic' threats to be aware of and fight.

5. Employee error or malicious act that causes data to be destroyed or corrupted.

6. Employees who receive or download inappropriate content from the Internet exposing the organization to cyber problems such as viruses

7. Contractors, partners, consultants, and temps who take advantage of even limited access to important systems.

8. Mistaken disclosure of confidential data

9. Hackers who break into networks through an Internet connection and steal confidential information.

10. These security threats are the most common as they can spread across corporate networks through file sharing and can be sent automatically to all listings in a system's address book.

Network Security:

What is network security? How does it protect you? How does network security work? What are the bus network security?

You may think you know the answers to basic questions like, What is network security. Still, it's a good your trusted IT partner. Why? Because small and medium-sized businesses (SMBs) often lack the IT res companies. That means your network security may not be sufficient to protect your business from today' Internet threats.

In answering the question What is network security?, your IT partner should explain that network securit activities designed to protect your network. Specifically, these activities protect the usability, reliability, of your network and data. Effective network security targets a variety of threats and stops them from ent your network.

What Is Network Security and How Does It Protect You?

After asking What is network security?, you should ask, What are the threats to my network?

Many network security threats today are spread over the Internet. The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

How Does Network Security Work?

To understand What is network security?, it helps to understand that no single solution protects you from You need multiple layers of security. If one fails, others still stand.

Network security is accomplished through hardware and software. The software must be constantly upda protect you from emerging threats.

A network security system usually consists of many components. Ideally, all components work together, maintenance and improves security.

Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-ho
- Virtual Private Networks (VPNs), to provide secure remote access

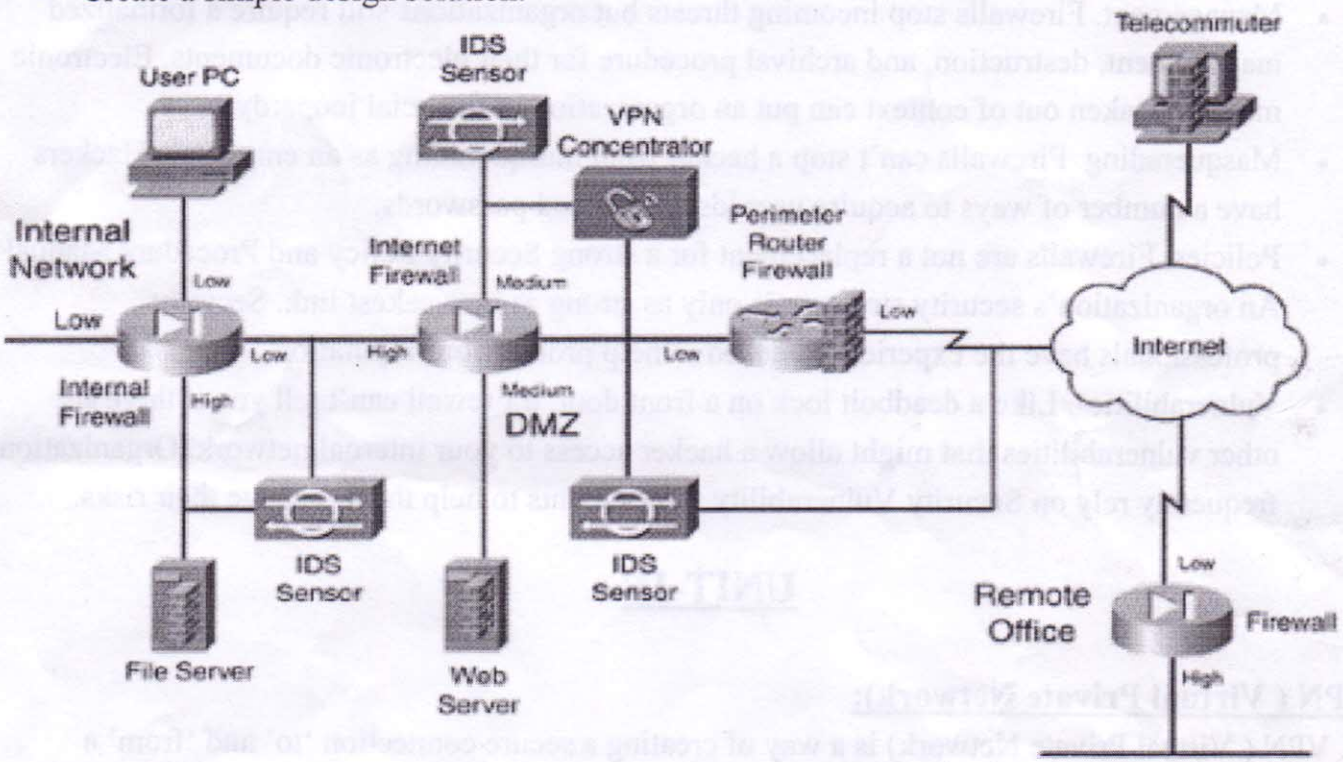
What are the Business Benefits of Network Security?

With network security in place, your company will experience many business benefits. Your company is business disruption, which helps keep employees productive. Network security helps your company mee regulatory compliance. Because network security helps protect your customers' data, it reduces the risk c data theft.

Ultimately, network security helps protect a business's reputation, which is one of its most important ass Assets.

Factors to consider in Firewall design:

- Develop a security policy.
- Create a simple design solution.



- Use devices as they were intended.
- Implement a layered defense to provide extra protection.
- Consider solutions to internal threats that should be included in your design.

Limitations of Firewalls:

Firewalls are a good first step in protecting your organization from hackers. But they do have their limitations. The top 10 firewall limitations include:

- Viruses. Not all firewalls offer full protection against computer viruses as there are many ways to encode files and transfer them over the Internet.
- Attacks. Firewalls can't protect against attacks that don't go through the firewall. For example, your firewall may restrict access from the Internet, but may not protect your equipment from dial in access to your computer systems.
- Architecture. Consistent overall organization security architecture: Firewalls reflect the overall level of security in the network. An architecture that depends upon one method of

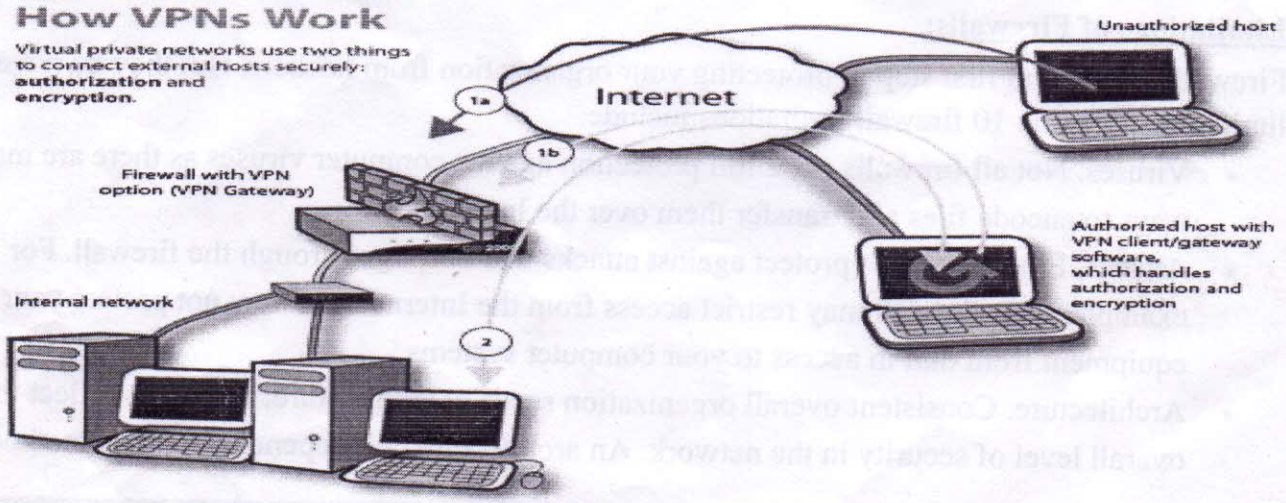
security or one security mechanism has a single point of failure. A failure in its entirety, or through a software application bug, may open the company to intruders.

- Configuration. A firewall can't tell you if it has been incorrectly configured. Trained professionals have the talent and experience to properly configure firewalls.
- Monitoring. Some firewalls can notify you if a perceived threat occurs, however, they can't notify you if someone has hacked into your network. Many organizations find they need additional hardware, software and network monitoring tools.
- Encryption. While firewalls and Virtual Private Networks (VPNs) are helpful, they don't encrypt confidential documents and E-mail messages sent within your organization or to outside business contacts. Formalized procedures and tools are needed to provide protection of your confidential documents and electronic communications.
- Management. Firewalls stop incoming threats but organizations still require a formalized management, destruction, and archival procedure for their electronic documents. Electronic messages taken out of context can put an organization in financial jeopardy.
- Masquerading. Firewalls can't stop a hacker from masquerading as an employee. Hackers have a number of ways to acquire user ids and related passwords.
- Policies. Firewalls are not a replacement for a strong Security Policy and Procedure Manual. An organization's security structure is only as strong as its weakest link. Security professionals have the experience needed to help protect your reputation.
- Vulnerabilities. Like a deadbolt lock on a front door, a firewall can't tell you if there are other vulnerabilities that might allow a hacker access to your internal network. Organizations frequently rely on Security Vulnerability Assessments to help them manage their risks.

UNIT-IV

VPN (Virtual Private Network):

A VPN (Virtual Private Network) is a way of creating a secure connection 'to' and 'from' a network or a computer. The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users of the underlying network which could often be a public network like the Internet. VPNs have been used for years, but they have become more robust .They are more affordable & also much faster.



Types of VPN

There are many different types of VPNs available. Let's take a look at most common types.

1. PPTP VPN

This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don't need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for Point-to-Point Tunneling Protocol. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

2. Site-to-Site VPN

Site-to-site is much the same thing as PPTP except there is no "dedicated" line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

3. L2TP VPN

L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn't provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

4. IPsec

Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it's designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

5. SSL

SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you're accessing. The major advantage of SSL is that it doesn't need any software installed because it uses the web browser as the client application.

6. MPLS VPN

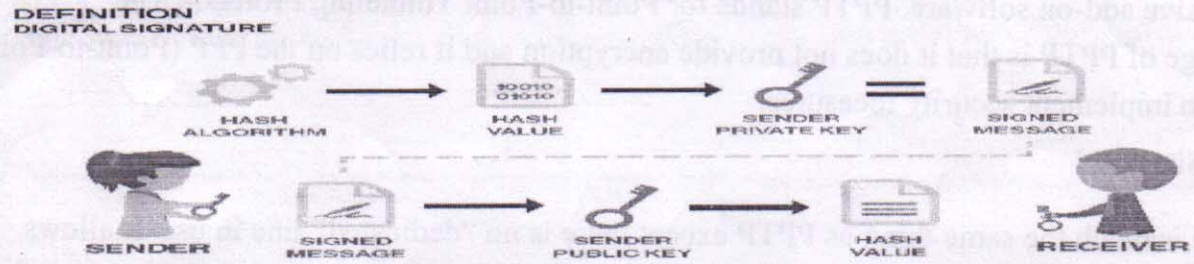
MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they're the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn't as easy to set up or add to as the others, and hence bound to be more expensive.

7. Hybrid VPN

A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both client and server levels and bound to be expensive.

Digital Signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.



The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

How digital Signatures work: Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing. A digital signature can be used with any kind of message whether it is encrypted or not simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) assuming their private key has not been compromised as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person.