Unit VIII

Security Issues in E-Commerce

Topics Included:

- Security Issues in E-Commerce
- Risks of e-commerce, Types and sources of threats to e-commerce ;
- Protecting electronic commerce assets and intellectual property,
- Firewalls, Client server network security,
- Security Protocols – SSL, SET, S-HTTP,
- Data and message security,
- Security tools,
- Digital identity and electronic signature,
- Encryption and concept of public and private key infrastructure;
- Risk management approach to e-commerce security

Introduction

- One of the critical success factors of e-commerce is its security.

- The successful functioning of e-commerce security depends on a complex interrelationship between several components, including:
  - the applications development platforms,
  - database management systems,
  - systems software
  - and network infrastructure.

- E-Commerce systems are based upon Internet use.

- The Internet is unregulated, unmanaged and uncontrolled thus introducing a wide range of risks and threats to the systems operating on it.

Security Issues related to E-Commerce

1. Access Control: Access control ensures only those that legitimately require access to resources are given access and those without valid access cannot have access. This includes both physical access as well as logical access to resources.

2. Privacy: Privacy ensures that only authorized parties can access information in any system. Integrity ensures that only authorized parties make changes to the documents transmitted over the network.

Security Issues related to E-Commerce

3. Authentication: It ensures that the origin of an electronic message is correctly identified. This means having the capability to determine who sent the message and from where or which machine.

4. Non-repudiation: It ensures that the sender cannot deny sending a particular message and the receiver cannot deny receiving a message.

Security Issues related to E-Commerce

5. Availability: It ensures that the required systems are available when needed. Two major threats to availability problems are virus attacks and denial of service.

   Note: One complicating factor for any e-commerce venture is security for customer information, such as credit card numbers and other personal data, that most customers do not wish to have shared.

Risks to E-Commerce Systems

Some of the risks posed to e-commerce systems include:

- Corrupting or deleting data on the hard disk of your server.
- Stealing of confidential data by enabling hackers to record user keystrokes.
- Enabling hackers to hijack your system and use it for their own purposes.
- Using your computer for malicious purposes, such as carrying out a DoS attack on another website.
- Harming customer and trading partner relationships by forwarding viruses to them from your own system.

Risks involved in E-Commerce Systems

- carrying out of a denial-of-service (DoS) attack that stops 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 E-commerce risks on a Business

- The potential business implications of a security incident include the following:
  - Direct financial loss as a consequence of fraud or litigation.
  - Consequential 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 denial-of-service attack.

Risks from Viruses, Trojans and Worms

- Viruses and Worms spread across computers and networks by making copies of themselves, usually without the knowledge of the computer user.

- A Trojan horse is a program that appears to be legitimate but actually contains another program or block of undesired malicious, destructive code, disguised and hidden in a block of desirable code.

Risks from Viruses, Trojans and Worms

- Trojans can be used to infect a computer with a virus.

- A back-door Trojan is a program that allows a remote user or hacker to bypass the normal access controls of a computer and gives them unauthorized control over it.

Spyware

- Spyware is software that is placed on your computer when you visit certain websites.

- It is used to secretly gather information about your usage and send it back to advertisers or other interested parties.

- In addition to tracking your system use, it can slow down or crash your computer.

Protecting E-Commerce Systems

- As the use of the internet continues to grow, websites are assuming greater importance as the public face of a business.

- The revenue generated by e-commerce systems also mean that organizations are becoming increasingly reliant on them as core elements of their business.

- With this high level of dependency upon the services provided by e-commerce systems, it is essential that they are protected from the threats posed by hackers, viruses, fraud and denial-of-service (DoS) attacks.

Threats to E-commerce Systems

- Threats to e-commerce systems can be either malicious or accidental. The procedures and controls you put in place to protect your site should help minimize both.

Malicious threats could include:

- hackers attempting to penetrate a system to read or alter sensitive data,
- burglars stealing a server or laptop that has unprotected sensitive data on its disk,
- imposters posing as legitimate users and even creating a website similar to yours,
- authorized users downloading a webpage or receiving an email with hidden active content that attacks your systems or sends sensitive information to unauthorized people.

Intellectual Property

Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names and images.

IP is protected in law by patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create.

Intellectual Property and E-commerce

- A company’s website can be a great tool for promoting business online and for generating sales.

- However, as Web commerce increases, so does the risk that others may copy the look and feel of a website, some of its features or the content on the website.

- The risk also increases that you may be accused of unauthorized use of other people’s intellectual assets.

What elements of a website need to be protected?

Many parts of a website may be protected by different types of intellectual property (IP) rights. For example:

- E-commerce systems, search engines or other technical Internet tools may be protected by patents or utility models;
- Software, including the text-based HTML code used in websites, can be protected by copyright and/or patents, depending on the national law;
- website design is likely to be protected by copyright;

- Creative website **content**, such as written material, photographs, graphics, music and videos, may be protected by copyright;

- **Databases** can be protected by copyright or by database laws;

- Business names, logos, product names, domain names and other signs posted on your website may be protected as trademarks;

- Computer-generated **graphic symbols, screen displays, graphic user interfaces (GUIs)** and even **web pages** may be protected by industrial design law;

- **Hidden aspects** of your website (such as confidential graphics, source code, object code, algorithms, programs or other technical descriptions, data flow charts, logic flow charts, user manuals, data structures, and database contents) can be protected by trade secret law.

Who owns the IP rights in a website?

- A typical website is a collage of components often owned by different persons.

- For example, one company may own rights in the navigation software; others may own copyright in photographs, graphics and text; and yet another person may own copyright in the design of your site.

- It may not be necessary for a business to own the IP rights in all elements of their website, but they should at least find out what they own, what they have rights to use and in what way, and what they do not own or have no rights to use.

Website copyrights?

- If a website has been developed by employees who are employed for that purpose, then, in most countries, the employer would own the copyrights of the website, unless otherwise agreed with the employees.

Website copyrights?

- If creation of a website design and/or content is outsourced to an outside contractor, then the independent web developer will usually own copyright and other IP rights in the website, as well as in the design and elements contributing to that design (such as colors, gifs, jpegs, setup, hyperlinks, text coding).
- Without a valid, written agreement transferring all these rights, a business may end up owning nothing except perhaps a non-exclusive license to use their site.

TIP – It is highly advisable to enter into a clear, written agreement with the website developer that spells out who owns IP rights in each element of the site.

Firewalls

- A **firewall** is a network security system designed to prevent unauthorized access to or from a private network.
- **Firewalls** can be implemented in both hardware and software, or a combination of both.
- A **firewall** is a **network** security device that grants or rejects **network** access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate **network**).

A Firewall is defined as a system or group of systems that enforces an access control policy between two networks.

Firewalls

A firewall can take 2 forms:

- **Software Firewall**: Specialized software running on an individual computer.
- **Network Firewall**: A dedicated device designed to protect one or more computers.

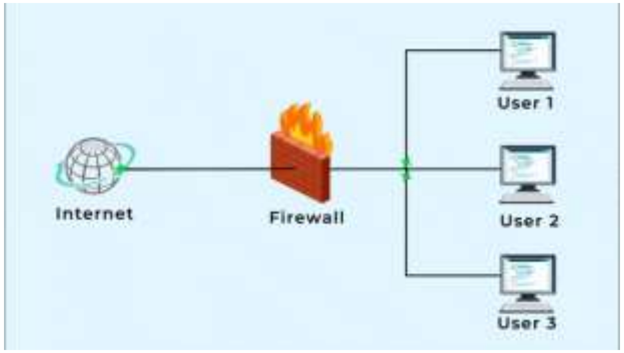
Main types of firewalls:

Packet filter firewall

-Operates at the data link and Network layers

Circuit filter firewall

-Operates at the transport layer



Application gateway firewall

- Operates at the Application layer.

Client – Server Network Security

- Network security on the internet is a major concern for commercial organizations, especially top management.

- By connecting to the Internet, a local network organization may be exposing itself to the entire population on the internet.

Client – Server network security problems manifest themselves in three ways:

- Physical security holes result when individuals gain unauthorized physical access to a computer.
- Software security holes result when badly written program or “privileged” software are “compromised” into doing things they shouldn’t.
- Inconsistent usage holes result when a system administrator enables a combination of hardware and software such that the system is seriously flawed from a security point of view.

Client – Server network security

- **Protection methods:**
- **Trust based security**: this approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files.
- **Security through obscurity**: Hiding password in binary files or in scripts with the assumption that “nobody will ever find them”, it is good in stand alone systems but not possible in Unix because users free to move around file system.
- **Password schemes**: using a mixed password or changing everyday.
- **Biometric systems:** finger prints, palm prints, retinal patterns, signature verification and voice recognization. 10-30 sec is sufficient to verify.
- **Firewall and Network Security**

Security Protocols

Secure Electronic Transaction(SET)

- SET stands for Secure Electronic Transaction (SET) protocol that was developed jointly by Microsoft and VISA International among others, **to secure electronic debit and credit card payments**. .
- This protocol involves a Digital Certificate that is issued to both the Customer and the Merchant (Seller).
- Each certificate is a guarantee that the persons involved in the transaction are who they say they are. The certificates are guaranteed by a third party who is trusted.
- Verisign is an example of such a third party.

SET

- When a transaction is initiated by the customer, the customer’s browser requests a public key from the merchant and another from the payment processor (usually a bank).

- The SET software then encrypts the transaction data using these two keys.

- The order information is sent in encrypted form to the merchant, and the payment information is sent in encrypted form to the payment processor.

- After the payment processor verifies payment, a key is sent to the merchant so that the order can be decrypted.

- With SET The merchant never sees the customer’s credit card information, and the payment processor never sees the order information.

SET

- SET blocks out all personal details on the card, preventing hackers and data thieves from accessing or stealing the cardholder's information.

- The merchant also cannot see these personal details, which are transferred directly to the credit card company for user authentication and verification.

- SET is not a payment system or gateway, but a set of security protocols.

Secure Socket Layer

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser.

Secure Socket Layer

The Secure Socket Layer, or SSL is a method of Data Encryption that operates as a layer between the TCP/IP network protocol and the HTTP applications.

Server authentication, encryption and data integrity are provided through SSL utilization.

Authentication ensures the client side that its data is sent to the correct server and the server is secured. Encryption ensures the privacy of the data transferred.

Data Integrity ensures that the data that has been transferred has not been altered.

Secure Socket Layer

SSL allows sensitive information such as credit card numbers and login credentials to be transmitted securely.

Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping.

If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

Secure Socket Layer

All browsers have the capability to interact with secured web servers using the SSL protocol.

However, the browser and the server need an SSL Certificate to be able to establish a secure connection.

To get a certificate, you must create a Certificate Signing Request (CSR) on your server. And send it to a Certificate issuer .

Once you receive the SSL Certificate, you install it on your server.

The most important part of an SSL Certificate is that it is digitally signed by a trusted CA like DigiCert.

Anyone can create a certificate, but browsers only trust certificates that come from an organization on their list of trusted CAs. Browsers come with a pre-installed list of trusted CAs,

Socket Layer

tificate issued by a CA (Certificate Authority) to an organization omain/website verifies that a trusted third party has authenticated nization’s identity.

e browser trusts the CA, the browser now trusts that organization’s oo.

vser lets the user know that the website is secure, and the user can browsing the site and even entering their confidential information.

he most important components of online business is creating a nvironment where potential customers feel confident in making s.

s give visual cues, such as a lock icon or a green bar, to help now when their connection is secured.

Secure Socket Layer

SSL secures millions of peoples’ data on the Internet every day, especially during online transactions or when transmitting confidential information.

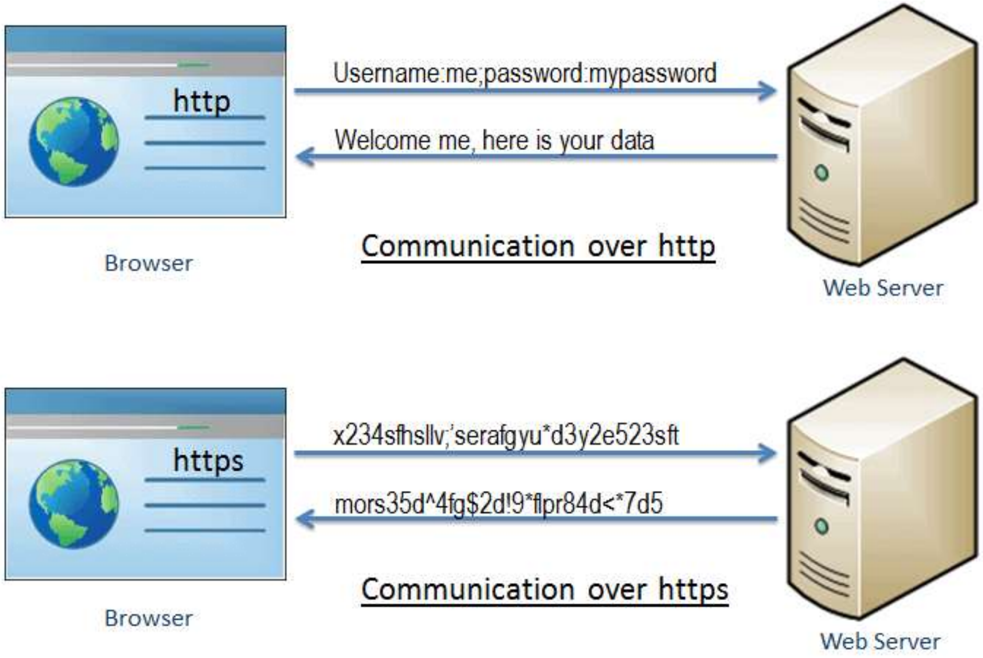
Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL- secured website.

SSL-secured websites also begin with https rather than http.

HTTPS

HTTPS (Hyper-Text Transfer Protocol Secure) is the secure version of HTTP, the system used to send information between a web browser and website.

HTTPS is HTTP with encryption. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP.


http
Username:me;password:mypassword
Welcome me, here is your data
Browser
Communication over http
Web Server
https
x234sfhsllv;'serafgyu*d3y2e523sft
mors35d^4fg$2d!9*flpr84d<*7d5
Browser
Communication over https
Web Server

HTTPS

HTTPS is able to provide multiple layers of protection to that data -

- Encryption: To anyone who somehow manages to intercept it, the data is worthless as they don’t have the key to decrypt it.

- Data integrity: with HTTPS data can’t get corrupted.

- Authentication: it prevents anyone from tricking customers into dealing with the wrong site

Advantages of using HTTPS

- Secure Communication: https makes a secure connection by establishing an encrypted link between the browser and the server or any two systems.
- Data Integrity: https provides data integrity by encrypting the data and so, even if hackers manage to trap the data, they cannot read or modify it.
- Privacy and Security: https protects the privacy and security of website users by preventing hackers to passively listen to communication between the browser and the server.
- Faster Performance: https increases the speed of data transfer compared to http by encrypting and reducing the size of the data.
- SEO: Use of https increases SEO ranking. In Google Chrome, Google shows the Not Secure label in the browser if users' data is collected over http.
- Future: https represents the future of the web by making internet safe for users and website owners.

Common E-Commerce Security Tools

1. **Authentication**: There are several techniques that can identify and verify someone seeking to access an e-commerce system. These include:

   - User name and password combination,
   - Two-factor authentication
   - Digital Certificate
   - A Biometric

Biometrics is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

2. **Access Control :** ensuring authorized access to data and services. It includes using:
   - Network restrictions
   - Application controls
   - Controlling changes to access privileges

3. **Encryption:** The technique of scrambling data held on a computer or transmitted over a network. It uses Virtual Private Network (VPNs) and Secure Socket Layers (SSLs) technologies.

2. **Firewalls:** It is a hardware or software security device that filters information passing between internal and external networks.

5. **Intrusion Detection:** The software related to intrusion detection monitor system and network activity to spot any attempt being made to gain access and if an attack is suspected, it can generate an alarm, such as an e-mail alert, based upon the type of activity it has identified.

6. **Preventing Problems from Viruses, Trojans and Worms by using:**

   - Different types of anti virus software
     - Virus scanners
     - Heuristics software
   - Installing Software Patches
   - Avoiding download of unauthorized programs and documents.
   - Virus Alerting Services

Digital Identity

- Digital identity is the network or Internet equivalent to the real identity of a person or entity (like a business or government agency) when used for identification in connections or transactions from PCs, cell phones or other personal devices.

Digital Identity

A digital identity is comprised of characteristics, or data attributes, such as the following:

- Username and password
- Online search activities, like electronic transactions
- Date of birth
- Medical history
- Purchasing history or behavior

- A digital identity is linked to one or more digital identifiers, like an email address, URL or domain name.

Digital Signature

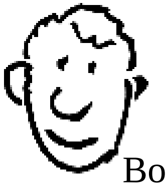
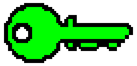
- Digital signature is a type of electronic signature that verifies the authenticity and integrity of digital messages and documents using encryption and decryption.

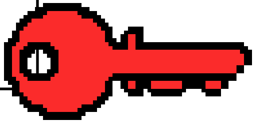
Data and Message Security

E-Commerce systems can use the following encryption techniques:

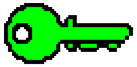
- Public Key Encryption or Asymmetric key-based algorithm,
- Symmetric key-based algorithms, or block-and-stream ciphers,
- Hashing, or creating a digital summary of a string or file.

Public/Private Key-Based Encryption (PKE)

 Bob		 **(Bob's public key)** **(Bob's private key)**



Bob has been given two keys. One of Bob's keys is called a Public Key, the other is called a Private Key.

Bob's Co-workers:				
				 Anyone can get Bob's Public Key, but Bob keeps his Private Key to himself

- In public-key cryptography, a user has a pair of keys: public and private.

- Private key is kept private and Public key is distributed to other users.

- Owner of the private key never ever shares the private key with anyone.

- Public key cryptography uses one key (the public key) to encrypt a message and a different key (the private key) to decrypt it.

Encrypt with Public Key

Decrypt with Private Key

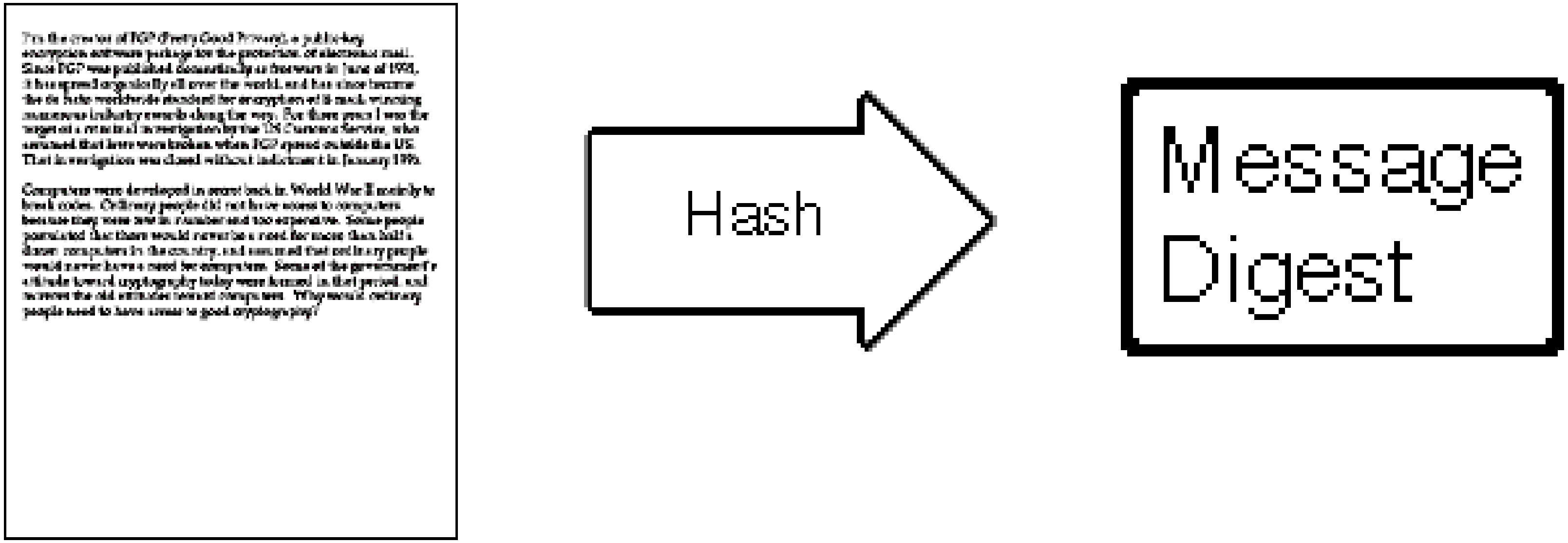
- HNFmsEm6Un
  BejhhyCGKOK
  JUxhiygSBCEiC
  0QYIh/Hn3xgiK
  BcyLK1UcYiY
  lxx2lCFHDC/A

- "Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

-

- With his private key and the right software, Bob can put digital signatures on documents and other data. A digital signature is a "stamp" Bob places on the data which is unique to Bob, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed cannot go undetected.

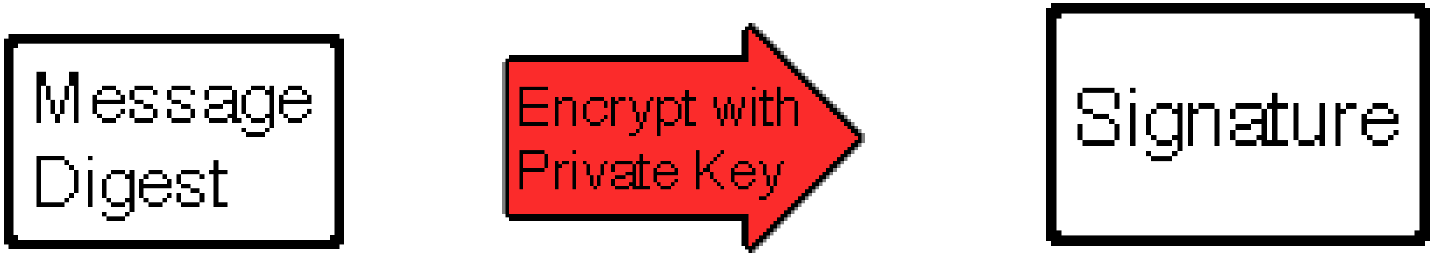
- **Digital Signature/Electronic Signature** can be defined as a computer data compilation of any symbol or series of symbols, executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.



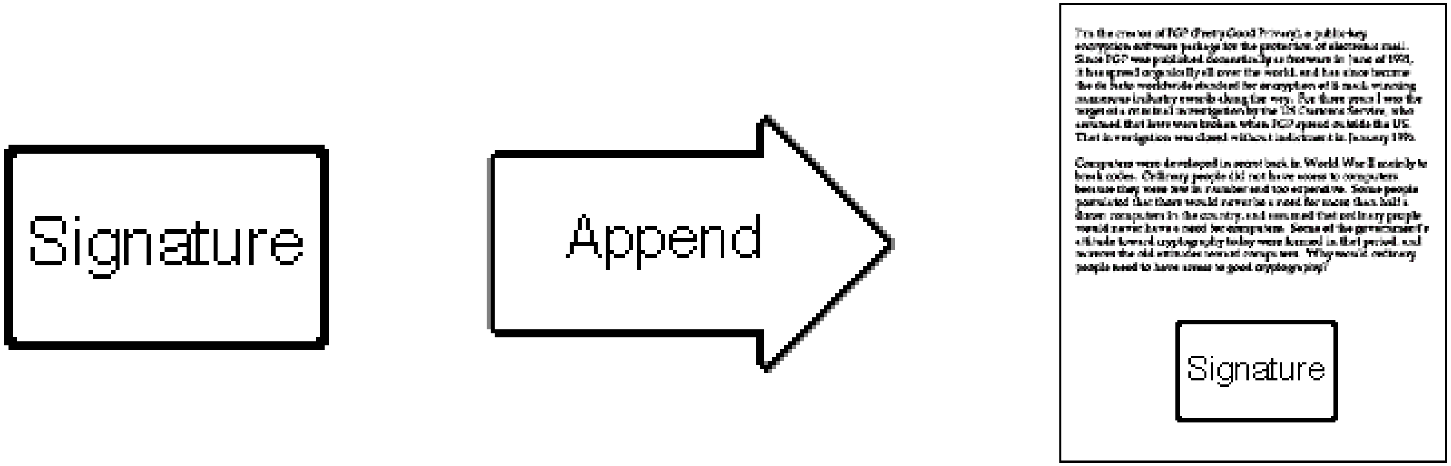
I'm the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of E-mail, winning numerous industry awards along the way. For three years I was the target of a criminal investigation by the US Customs Service, who assumed that laws were broken when PGP spread outside the US. That investigation was closed without indictment in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and mirrors the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

- To sign a document, Bob's software will crunch down the data into just a few lines by a process called "hashing". These few lines are called a message digest. (It is not possible to change a message digest back into the original data from which it was created.)



- Bob's software then encrypts the message digest with his private key. The result is the digital signature.

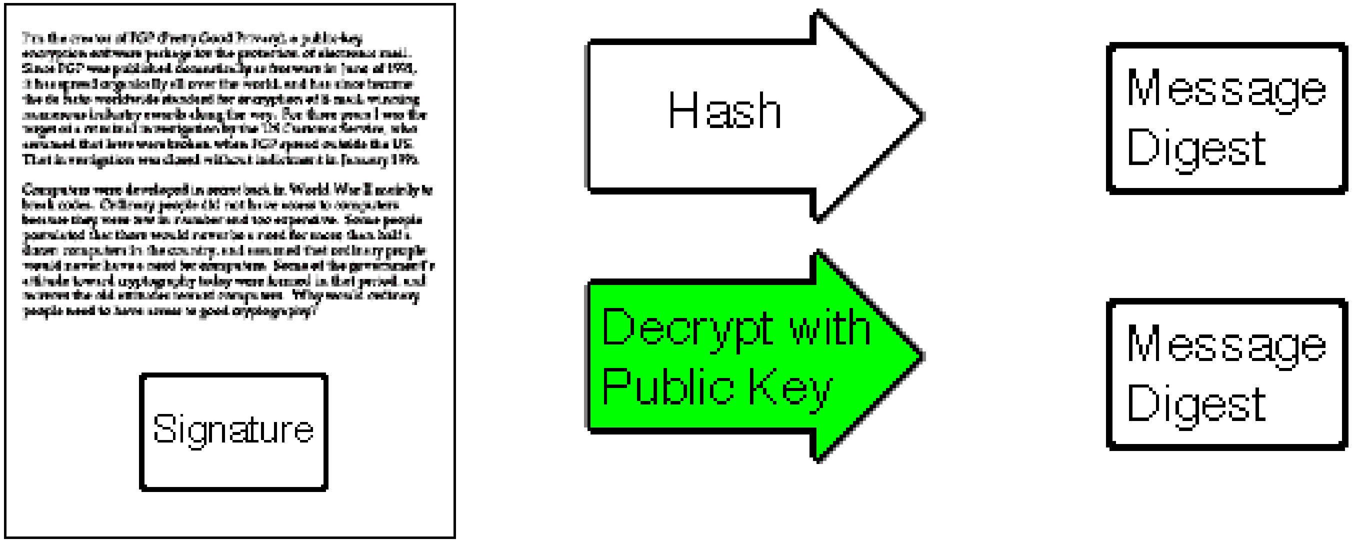


I'm the creator of PGP (Pretty Good Privacy), a public key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of E-mail, winning numerous industry awards along the way. For three years I was the target of a criminal investigation by the US Customs Service, who assumed that laws were broken when PGP spread outside the US. That investigation was closed without indictment in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers, because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and mirrors the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

- Finally, Bob's software appends the digital signature to document. All of the data that was hashed has been signed.

- Bob now passes the document on to Pat.
- First, Pat's software decrypts the signature (using Bob's public key) changing it back into a message digest. If this worked, then it proves that Bob signed the document, because only Bob has his private key. Pat's software then hashes the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Pat knows that the signed data has not been changed.



Public Key Infrastructure (PKI)

- PKI refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could “carry” certificates around that identify them in a variety of ways.

Risk Assessment

- Risk Assessment can be carried out to provide an organization with a clear understanding of the risks facing its e-commerce system and associated business processes, and the potential impact if a security incident arises.

- A key part of a risk assessment is defining the business’ information access requirements. This will cover the rules of access for different groups of users.

- For example, different rules may apply for employees, consultants, managed service providers, suppliers, customers, auditors, government agencies and so on.

- Any analysis should also take into account of how electronic transactions are verified.

Risk Management approach to E-Commerce security

- Security risk assessment and security risk management have become vital tasks for security officers and IT managers. Corporations face increased levels of risk almost daily.

- An ever-growing list of government regulations aimed to secure the confidentiality, integrity and availability of many types of financial and health-related information also is increasing IT risks and making a comprehensive security risk assessment a modern-day corporate necessity.

- The best way to avoid disasters is to establish an ongoing security risk management process that begins with quantifying the value of Web applications, as well as the data they manage, through a complete security risk assessment.

- Organizations then must continuously identify and mitigate the vulnerabilities and risks associated with those systems from the beginning and throughout their lifecycle: from development through production.

- The approach to security risk management is as follows:
  - consistently performing a security risk assessment,
  - then identifying and remedying vulnerabilities by correcting application development errors,
  - applying security patches,
  - and fixing system misconfigurations.

- This approach will lead organizations to continuous improvement of their business-technology infrastructure and a thorough reduction of risk.