Digital Business Management (DBM)

Managing E-Business

Security in E-Commerce:

eCommerce security refers to the principles which guide safe electronic transactions, allowing the buying and selling of goods and services through the Internet, but with protocols in place to provide safety for those involved.

Ecommerce security is a set of protocols that safely guide ecommerce transactions. Stringent security requirements must be in place to protect companies from threats like credit card fraud, or they risk jeopardizing revenue and customer trust, due to the inability to guarantee safe credit card processing.

Threats:

- A threat is an object, person or other entity that represents a constant danger to an asset.
- Management must be informed of the various kinds of threats facing the organization.
- By examining each threat category management and effectively protects information through policy, education, training and technology.

E-Commerce Threats:

There are various types of e-commerce threats. Some are accident, some are purposeful and some of them are due to human error. The most common threats are phishing attacks money thefts, data miss use, hacking, credit card frauds and unprotected service.

1. **In-accurate management:** One of the main reasons to e-commerce threats is poor management. When security is not up to the mark it faces a very dangerous threat to the network and systems. Also, security threats occur when there is no proper budget are allocated for purchase of anti-virus software licenses.
2. **Price manipulation:** Modern e-commerce systems often face price manipulation problems. These systems are fully automated right from the first visit to the find payment gateway stealing is the most common intention of price manipulation. It allows an intruder to side or install a lower price into the URL and get away with all the data.
3. **Snowshoe spam:** Now spam is something which is very common. Almost each one of the us deals with spam mails in our mail box. The spam messages problems have been actually solved but now it is turning out to be a not so general issue. The reason for this is the very nature of a spam message.
4. **Malicious threats:** These code threats typically involve viruses, worms, Trojan horses.
    a. **Viruses** are normally external threats and can corrupt the files on the website if they find their way in the internal network. They can be very dangerous as they destroy the computer systems completely and can damage the normal working of the computer. A virus always needs a host as they cannot spread by themselves.
    b. **Worms** are very much different and are more serious than viruses. It places itself directly through the internet. It can infect millions of computers in a matter of just few hours.
    c. A **Trojan horse** is a programming code which can perform destructive functions. They normally attack your computer when you download something. So always check the source of the downloaded file.

5. **Hacktivism:** The full form of hacktivism is hacking activism. At first it may seem like you should hardly be aware of these cyber threats. After all it is a problem not directly related to you. Why you should be bothered at all? However, that’s not the case. Firstly, hacktivists do not target directly to those associated only to politics. It can also be a socially motivated purpose. It is typically using social media platforms to bring to light social issues. It can also include flooding an email address with so much traffic that it temporarily shuts down.
6. **Wi-Fi eaves dropping:** It is also one of the easiest ways in e-commerce to steal personal data. It is like a virtual listening of information which is shares over a Wi-Fi network which is not encrypted. It can happen on public as well as on personal computers.
7. **Other threats:** Some other threats which include are data packet sniffing, IF spoofing and port scanning. Data packet sniffing is also normally called as sniffers. An intruder can use sniffer to attack a data packet. With IP spoofing it is very difficult to track the attacker. The purpose here is to change the source address and give it such a look that it should look as though it originated from another computer.

Encryption:

The process of converting information or data into a code, especially to prevent unauthorized access. In computing, encryption is the method by which plaintext or any other type of data is converted from a readable from to an encoded version that can only be decoded by another entity if they have access to a decryption key.

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.

Working:

- The encryption/decryption key is comparable with a normal password. E.g.: the one you use for your email. The key is an essential part of the process of encoding and decoding data.
- Typically, a key is a random binary or an actual passphrase. The key “tells” the algorithm what patterns it must follow in order to convert plaintext into ciphertext (and the other way around).
- It almost goes without saying, but the key is a fundamental part of the protection of the privacy of information, a message or a piece of data. The encryption and decryption process can only be initiated by using the key.
- Due to the fact that algorithms are publicly available and can be accessed by anyone, once a hacker gets a hold of the encryption key, the encrypted data can easily be decrypted to plaintext.

Uses:

Encryption is used to protect data in transit sent from all sorts of devices across all sorts of networks, not just the internet. Every time someone uses an ATM or buys something online with a smartphone, makes a mobile phone call or presses a key fob to unlock a car, encryption is used to protect the information being protected.

Advantages:

1. Encrypted data can’t be easily read.
2. Strong encryption may require years of work to decrypt without the key.

Disadvantages:

1. Encrypted files draw attention to their value.
2. If you lose the key you lose the data.
3. For large files strong encryption may take significant time to decrypt.

Cryptography:

It is an ancient art and science of writing in secret message. Cryptography comes from Greek word, CRYPTO means hiding and GRAPHY means writing. It is the art of achieving security by encoding message to make them non readable.

Technologies:

Encryption: It is the process of transforming so it unintelligible to anyone but the intended recipient.

Decryption: It is the process of transforming encrypted information so that it is intelligible again.

Plaintext: The message to be transmitted or stored

Cipher text: The disguised message or encrypted message.

Algorithm: The mathematical formula used for encryption and decryption.

Cipher: Algorithm used for encryption and decryption.

Key: Value used by algorithm to encrypt and decrypt.

Types of cryptography:

Secret-key cryptography (systematic key cryptography): It uses for both encryption and decryption.

Public key cryptography (asymmetric key cryptography): It uses one key for encryption and another for decryption.

Hash function: It uses a mathematical transformation to irreversibly “encrypt” information.

Types of encryption:

1. Secret key symmetric encryption:
   a. Relatively simple first used by Julius Caesar.
   b. Both users have a password e.g. DES.
2. Public key encryption:
   a. Two keys involved used on the internet e.g. PGP.
3. One-way function:
   a. Digital signature of certificate
   b. Unix login

Characteristics of cryptography:

- The type of operations used for transforming plaintext to cipher text.
- The number of keys used.

- The way in which the plaintext is processed.

Applications of cryptography:

- **Key recovery:** It is a technology that allows a key to be revealed under certain circumstance without the owner of the key revealing it.
- **Remote access:** Passwords gives a level of security for secure access.
- **Cell phone:** Prevent people from stealing cell phone no, access code or eavesdropping.
- **Access control:** Regulate access to satellite and cable TV.

Purpose of cryptography:

- Authentication.
- Integrity.
- Privacy confidentiality.
- Non-repudiation.

Advantages:

- It is faster.
- While transmission the chances of data being decrypted is null.
- Uses password authentication to prove the receiver's identity.

Disadvantages.

- Issue of key transportation.
- It cannot provide digital signature that cannot be repudiated.

Public Key and Private Key Cryptography:

A symmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. One key is the pair can be shared with everyone, it is called the public key the other key in the pair is kept secret, it is called private key.

The distinguishing technique used in public key cryptography is the uses of as symmetric key algorithms where a key used by one party to performance encryption is not the same as the key used by another in decryption, each user has a pair of cryptographic keys, a public encryption key and a private decryption key.

Roles of private and public key:

Private key	Public key
Private key faster compared to public key	Relatively slow to encrypt /decrypt
Private key is symmetrical. Actually, there is only one key. The another is a copy of it	Asymmetrical key.
Private key is a truly private should be available with on only the communicating parties	Public key can be made public. private key is truly secret
The two parties most have met before at least share the key	That two parties need not have met. The two may be strangers, half way around the globe

Digital Signatures:

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message.

- It is a mathematical scheme for demonstrating the authenticity of a digital message or document.
- Each signatory has their own paired public and private key.
- It consists three algorithms:
    1. A digital signature generation algorithm:
        - It consists of a (mathematical) digital signature
        - Randomly produces a key pair (public and private)
    2. A signing algorithm:
        - Produces a signature
    3. A digital signature verification algorithm:
        - It consists of verification algorithm with a method for recovering data from the message.

Advantages:

- ➢ Imposter prevention
- ➢ Message integrity
- ➢ Legal requirement

Disadvantages:

- ➢ Digital signature involves the primary avenue for any business is month.

Requirements while you apply for a digital signature certificate:

1. Submission of digital signature application form duly filled in by the applicant:
   Any individual applying for a Digital Signature Certificate is required to fill an Application Form for online submission and verification of personal details by the certifying authority.
2. Producing Photo ID proof
3. Producing Address proof

Steps to apply for a digital signature certificate:

1. Log on and select your type of entity.
2. Fill the necessary details.
3. Proof of identity and address.
4. Payment for DSC.
5. Post the documents required.

Digital Certificates:

A digital certificate is an electronic “password” that allows a person and organization to exchange data securely over the internet using the public key infrastructure (PKI). Digital certificate is also known as a public key certificate or identity certificate.

A digital certificate authenticates the web credential of the sender and lets the recipients of an encrypted message know that the data is from a trusted source or a sender who claims to be one.

Types of Digital Certificates:

1. **Secure socket layer certificate (SSL):**

Secure Socket Layer (SSL) server Certificates are installed on a server. This can be a server that hosts a website like www.digi-sign.com, a mail server, a directory or LDAP server, or any other type of server that needs to be authenticated, or that wants to send and receive encrypted data.

2. **Software signing (CODE SIGNING CERTIFICATES):**
   Code Signing Certificates are used to sign software or programmed code that is downloaded over the Internet. It is the digital equivalent of the shrink-wrap or hologram seal used in the real world to authenticate software and assure the user it is genuine and actually comes from the software publisher that it claims.
3. **Client certificates (DIGITAL ID):**
   Client Certificates or Digital IDs are used to identify one person to another, a person to a device or gateway or one device to another device. Client Certificates are issued in thousands and millions each year and would be the principle reason for purchasing a CA. Two people communicating by email will used a client certificate to authenticate or digitally sign their respective communications. This Signature will assure each person that the email is genuine and comes from the other person. A person that is given access to a secure online service like a database, an extranet or intranet will be authenticated to the gateway or entry point using a Client Certificate. This type of strong two factor authentication replaces less secure usernames and passwords currently in use on many websites.

Security Protocols over Public Networks

Network security protocols are a type network protocol that ensures the security and integrity of data in transit over a network connection.

Network security protocols define the processes and methodology to secure network data from any illegitimate attempt to review or extract the contents of data.

Types of Security:

1. **Application Security:**
   It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.
2. **Behavioral Analytics:**
   In order to detect abnormal network behavior, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.
3. **Data Loss Prevention (DLP):**
   Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures that prevent people from uploading, forwarding or even printing vital information in an unsafe manner.
4. **Email Security:**
   Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build

refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

5. **Firewalls:**
   Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections and secures all connections when you are online.
6. **Mobile Device Security:**
   Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT control which devices can access your network. It is also necessary to configure their connections in order to keep network organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to keep traffic private.
7. **Network Segmentation:**
   Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.
8. **Security Information and Event Management (SIEM):**
   SIEM products bring together all the information needed by your security staff in order to identify and respond to threats. These products are available in different forms, including virtual and physical appliances and server software.
9. **Virtual Private Network (VPN):**
   A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.
10. **Web Security:**
    A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites and blocking.
11. **Wireless Security:**
    The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

Advantages of Network Security:

1. **Protect data**:
   Network security keeps a check on unauthorized access. A network contains a lot of confidential data like the personal client data. Anybody who breaks into the network

may hamper these sensitive data. So, network security should be there in place to protect them.

2. **Prevents cyberattack**:
   Most of the attack on the network comes from internet. There are hackers who are experts in this and then there are virus attacks. If careless, they can play with a lot of information available in the network. The network security can prevent these attacks from harming the computers.
3. **Levels of access**:
   The security software gives different levels of access to different users. The authentication of the user is followed by the authorization technique where it is checked whether the user is authorized to access certain resource. You may have seen certain shared documents password protected for security. The software clearly knows which resources are accessible by whom.
4. **Centrally controlled**:
   Unlike the desktop security software, the network security software is controlled by a central user called network administrator. While the former is prone to worms and virus attacks, the latter can prevent the hackers before they damage anything. This is because the software is installed in a machine having no internet.
5. **Centralized updates**:
   It is very important that the anti-virus software is timely updated. An old version may not offer you enough security against attackers. But it is not guaranteed that every user of the network follows it religiously. A network security system which is centralized offers this advantage of timely updates without even the knowledge of the individuals.

Disadvantages of Network Security:

Network security is a real boon to the users to ensure the security of their data. While it has many advantages, it has lesser disadvantages.

1. **Costly set up**:
   The setup of a network security system can be a bit expensive. Purchasing the software, installing it etc. can become costly especially for smaller networks. It is not about a single computer, but a network of computers storing massive data. So, the security being of prime importance will definitely cost more. It cannot be ignored at any cost.
2. **Time consuming**:
   The software installed on some networks is difficult to work with. It needs authentication using two passwords to ensure double security which has to be entered every time you edit a document. It also requires the passwords to be unique with numbers, special characters and alphabets. The user may have to type a number of sample passwords before one is finalized which takes a lot of time.
3. **Requires skilled staff**:
   To manage large networks is not an easy task. It requires highly skilled technicians who can handle any security issue that arises. A network administrator needs to be employed to ensure smooth working of the network. He must be trained adequately to meet the requirement.
4. **Careless admin**:
   When the best software is installed and everything required is done, it is natural for the admin to be careless at times. It is his job to check the logs regularly to keep a check

on the malicious users. But sometimes, he just trusts the system and that is when the attack happens. So, it is very important that the admin remains vigilant always.

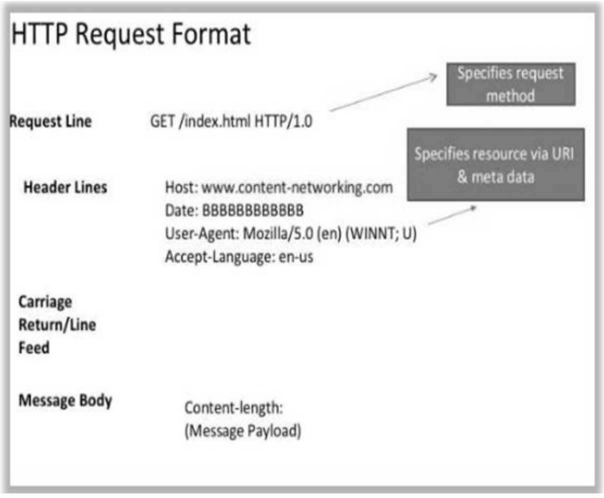
HTTP:

A Protocol is a standard procedure for defining and regulating communication. E.g. TCP, UDP, HTTP, etc. Hypertext Transfer Protocol, better known to millions of Web surfers as HTTP, was invented in 1990 by Tim Berners-Lee at the CERN Laboratories in Geneva, Switzerland. Today, it is the foundation of the World Wide Web and the Hypertext Markup Language or HTML.

Hyper Text Transfer Protocol:

1. The HTTP provides a standard for web browsers & servers to communicate.
2. HTTP is the foundation of data communication for the WWW.
3. HTTP is an application layer network protocol built on top of TCP.
4. HTTP clients & servers communicate via HTTP request & response message.
5. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text.
6. HTTP is the protocol to exchange or transfer hypertext.
7. HTTP is called a "stateless protocol" because each command is executed independently, without any knowledge of the commands that came before it.
8. E.g. When you enter a URL in your browser, this actually sends an HTTP command to the web server directing it to fetch & transmit the requested web page.

There are 2 major versions of HTTP: HTTP/1.0 HTTP/1.1



HTTP Request Format

Specifies request method

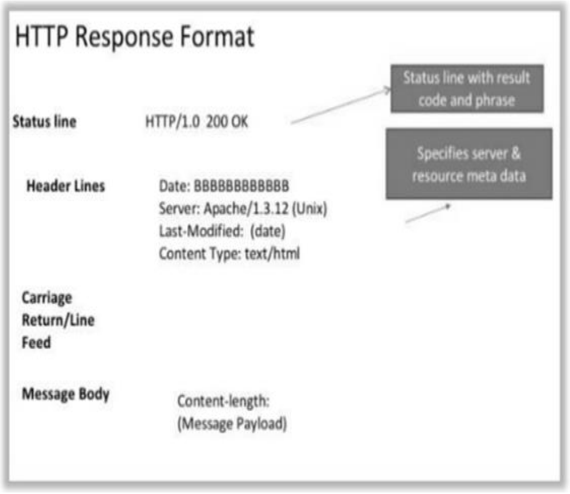
Request Line GET /index.html HTTP/1.0

Specifies resource via URI & meta data

Header Lines
Host: www.content-networking.com
Date: BBBBBBBBBBBB
User-Agent: Mozilla/5.0 (en) (WINNT; U)
Accept-Language: en-us

Carriage Return/Line Feed

Message Body
Content-length:
(Message Payload)



HTTP Response Format

Status line with result code and phrase

Status line HTTP/1.0 200 OK

Specifies server & resource meta data

Header Lines
Date: BBBBBBBBBBBB
Server: Apache/1.3.12 (Unix)
Last-Modified: (date)
Content Type: text/html

Carriage Return/Line Feed

Message Body
Content-length:
(Message Payload)

Advantages:

- Platform independent: Allows straight cross platform porting.
- No Runtime support required to run properly.
- Usable over firewalls. Global applications possible.
- Not Connection Oriented: No network overhead to create and maintain session state and information.
- Ease of programming: HTTP is coded in plain text and therefore is easier to follow and implement than protocols that make use of codes that require lookups.

- Flexibility.

Disadvantages:

- Privacy: Anyone can see content
- Integrity: Someone might alter content. HTTP is insecure since no encryption methods are used. Hence is subject to main in the middle and eavesdropping of sensitive information.
- Authentication: Not clear who you are talking with. Authentication is sent in the clear. Anyone who intercepts the request can determine the username and password being used.
- Information sent via HTTP is not encrypted and can pose a threat to your privacy.
- Packet headers are larger than other protocols as they are needed for security and quality assurance of the information being transferred.

Secure Socket Layer (SSL):

SSL (Secure Sockets Layer) is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication. The usage of SSL technology ensures that all data transmitted between the web server and browser remains encrypted.

An SSL certificate is necessary to create SSL connection. You would need to give all details about the identity of your website and your company as and when you choose to activate SSL on your web server. Following this, two cryptographic keys are created - a Private Key and a Public Key.

Use:

- The SSL protocol is used by millions of online business to protect their customers, ensuring their online transactions remain confidential.
- A web page should use encryption when it expects users to submit confidential data, including personal information, passwords, or credit card details.
- All web browsers have the ability to interact with secured sites so long as the site's certificate is issued by a trusted CA.

Firewall as Security Control:

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.

A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed.

Working:

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.

Types of firewalls:

1. **Packet filtering firewalls:**
   This, the original type of firewall, operates inline at junction points where devices such as routers and switches do their work. However, this firewall doesn't route packets, but instead compares each packet received to a set of established criteria such as the allowed IP addresses, packet type, port number, etc. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped, that is, they are not forwarded and thus, cease to exist.
2. **Circuit-level gateways**:
   Using another relatively quick way to identify malicious content, these devices monitor the TCP handshakes across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate, whether the remote system is considered trusted. However, they don't inspect the packets themselves.
3. **Stateful inspection firewalls**:
   State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This offers more security than either packet filtering or circuit monitoring alone, but exacts a greater toll on network performance. A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple layers of the OSI (Open Systems Interconnection) seven-layer model.
4. **Application-level gateways**:
   This kind of device, technically a proxy, and sometimes referred to as a proxy firewall, combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended as specified by the destination port but also by certain other characteristics, such as the HTTP request string. While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance.
5. **Next-gen firewalls**:
   This looser category is the most recent and least-well delineated of the types of firewalls. A typical next-gen product combines packet inspection with stateful inspection, but also includes some variety of deep packet inspection.

Firewall rule actions:

Firewall rules can take the following actions:

- **Allow:** Explicitly allows traffic that matches the rule to pass, and then implicitly denies everything else. It has two rules as Permit traffic that is explicitly allowed and Implicitly deny all other traffic.
- **Bypass:** Allows traffic to bypass both firewall and intrusion prevention analysis. Use this setting for media-intensive protocols or for traffic originating from trusted sources. A bypass rule can be based on IP, port, traffic direction, and protocol.
- **Deny:** Explicitly blocks traffic that matches the rule.
- **Force Allow:** Forcibly allows traffic that would otherwise be denied by other rules. Traffic permitted by a Force Allow rule will still be subject to analysis by the intrusion prevention module.
- **Log only:** Traffic will only be logged. No other action will be taken.

Advantages:

- Makes Security Transparent to End-Users.
- Easy to install.
- Packet filters make use of current network routers. Therefore, implementing a packet filter security system is typically less complicated than other network security solutions.
- High speed

Disadvantages:

- Packet filtering routers are not very secure.
- Difficulty of setting up packet filtering rules to the router.
- There isn’t any sort of user-based Authentication.
- Packet filter cannot authenticate information coming from a specific user.

Public Key Infrastructure (PKI) for Security:

A Public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption. Registration Authority (RA) is responsible for accepting requests for digital certificates and authenticating the entity making the request.

Working:

Public Key Infrastructure (PKI) is the framework of encryption and cybersecurity that protects communications between the server (your website) and the client (the users). It works by using two different cryptographic keys, a public key and a private key. The public key is available to any user that connects with the website. The private key is a unique key generated when a connection is made and kept secret. When communicating, the client uses the public key to encrypt and decrypt and the server uses the private key. This protects the user’s information from theft or tampering.

PKI security is used in many different ways. The following are a few ways that PKI security can be used.

- Securing Emails
- Securing web communications (such as retail transactions)
- Digitally signing software
- Digitally signing applications
- Encrypting files
- Decrypting files
- Smart card authentication

Components of Public Key Infrastructure (PKI):

- It starts with trust.
- Certification Authorities.
- Private and public keys.
- Certificate enrollment.
- Digital certificates.
- Usage scenarios.
- Maintaining security in a PKI environment

Benefits:

Secure access control: With a unique verifiable identity you can determine what level of access to grant to that device. In addition, you can now deny access to anyone who does not have a proper certificate - no certificate, no way. In addition, if you find out a certificate has been somehow compromised, because it is unique and identifiable, you can revoke its access privileges and that certificate will no longer be granted access.

Mutual Authentication:

In the days before IoT and autonomous networked devices, the device didn’t need to be authenticated, just the servers. You wanted to make sure that the website you were logging into was actually a bank and not some bogus phishing site. The bank authenticated your identity through your login and password. With IoT, the device needs to be authenticated and the device also needs to authenticate the server it is talking to. With digital certificates and secure elements, this is now practical.

Secure Over-the-Air (OTA) Update: The problem with many devices today is that they will accept software updates from anyone. Remember, you want a device to only accept software that is verified and comes from a trusted server. The certificates allow the device to prove it should receive an update and which one, and the cryptography in the secure element allows the device to verify the server as well as the signed code.

Advantages:

- PKI is a standards-based technology.
- It allows the choice of trust provider.
- It is highly scalable. Users maintain their own certificates and certificate authentication involves exchange of data between client and server only. This means that no third-party authentication server needs to be online. There is thus no limit to the number of users who can be supported using PKI.
- PKI allows delegated trust. That is, a user who has obtained a certificate from a recognized and trusted certificate authority can authenticate himself to a server the very first time he connects to that server, without having previously been registered with the system.
- Although PKI is not notably a single sign-on service, it can be implemented in such a way as to enable single sign-on.

Disadvantages:

- PKI has too many moving parts
- Complexity is the enemy of good computer security. The more moving parts you have, the easier it is to find weaknesses and the harder it is to implement and few computer security defenses have more moving parts than a properly set-up PKI.
- You also need two or more websites to store the CA's own certificate and CRLs (certificate revocation lists). You usually need two of these internally, on the network, and perhaps two more externally.