Lecture 3

Computer Security Technology

Computer Security Technology - Encryption

- Encryption is the process of converting a plaintext message into a secure-coded form of text, called ciphertext.
- The ciphertext cannot be understood without converting back, via decryption–the reverse process–to plaintext.
- This is done via a mathematical function and a special encryption/decryption password called the key. In many countries, encryption is subject to governmental laws and regulations that limit the key size or define what may not be encrypted.
- Encryption is part of a broader science of secret languages called cryptography, which is generally used to:
    - Protect information stored on computers from unauthorized viewing and manipulation
    - Protect data in transit over networks from unauthorized interception and manipulation
    - Deter and detect accidental or intentional alterations of data
    - Verify authenticity of a transaction or document

Key Elements of Cryptographic Systems

- Key elements of cryptographic systems include:
  - Encryption algorithm–Mathematically based function or calculation that encrypts or decrypts data.
  - Encryption key–Piece of information similar to a password that makes the encryption or decryption process unique. A user needs the correct key to access or decipher a message, as the wrong key converts the message into an unreadable form.
  - Key length–Predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute force attack where all possible key combinations are tried.

Key Elements of Cryptographic Systems

- Effective cryptographic systems depend upon a variety of factors including:
  - Algorithm strength
  - Secrecy and difficulty of compromising a key
  - Nonexistence of back doors by which an encrypted file can be decrypted without knowing the key
  - Inability to decrypt parts of a ciphertext message and prevent known plaintext attacks
  - Properties of the plaintext known by a perpetrator

Key Systems

- There are two types of cryptographic systems:
  - Symmetric Key Systems—These use single, secret, bidirectional keys that encrypt and decrypt.
  - Asymmetric Key Systems—These use pairs of unidirectional, complementary keys that only encrypt or decrypt. Typically, one of these keys is secret, and the other is publicly known.
- Public key systems are asymmetric cryptographic systems.
  - Most encrypted transactions over the Internet use a combination of private/public keys, secret keys, hash functions (fixed values derived mathematically from a text message) and digital certificates (that prove ownership of a public encryption key).
- Essentially, keys and hash values are used to transform a string of characters into a shorter or fixed-length value or key that represents the original string.
- This encryption process allows data to be stored and transported with reduced exposure so data remains secure as it moves across the Internet or other networks.

Encryption Techniques

- Symmetric (Private) Key Encryption
  - Symmetric key cryptographic systems are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext.
  - In this case, the key is said to be symmetric because the encryption key is the same as the decryption key.
  - The most common symmetric key cryptographic system is the Data Encryption Standard (DES).
  - DES is based on a public algorithm that operates on plaintext in blocks (strings or groups) of bits. This type of algorithm is known as a block cipher. DES uses blocks of 64 bits.
  - DES is no longer considered a strong cryptographic solution because its entire key space can be forced when every key is tried by large computer systems within a relatively short period of time.
  - DES is being replaced with AES, a public algorithm that supports keys from 128 bits to 256 bits.

Encryption Techniques

- Symmetric (Private) Key Encryption
  - There are two main advantages to symmetric key cryptosystems such as DES or AES:
    - The user only has to remember/know one key for both encryption and decryption.
    - Symmetric key cryptosystems are generally less complicated and, therefore, use up less processing power than asymmetric techniques. They are ideally suited for bulk data encryption.
  - The disadvantages of this approach include:
    - Difficulty distributing keys–Getting the keys into the hands of those with whom you want to exchange data can be a challenge, particularly in e-commerce environments where customers are unknown, untrusted entities.
    - Limitations of shared secret–A symmetric key cannot be used to sign electronic documents or messages due to the fact that the mechanism is based on a shared secret.

Encryption Techniques

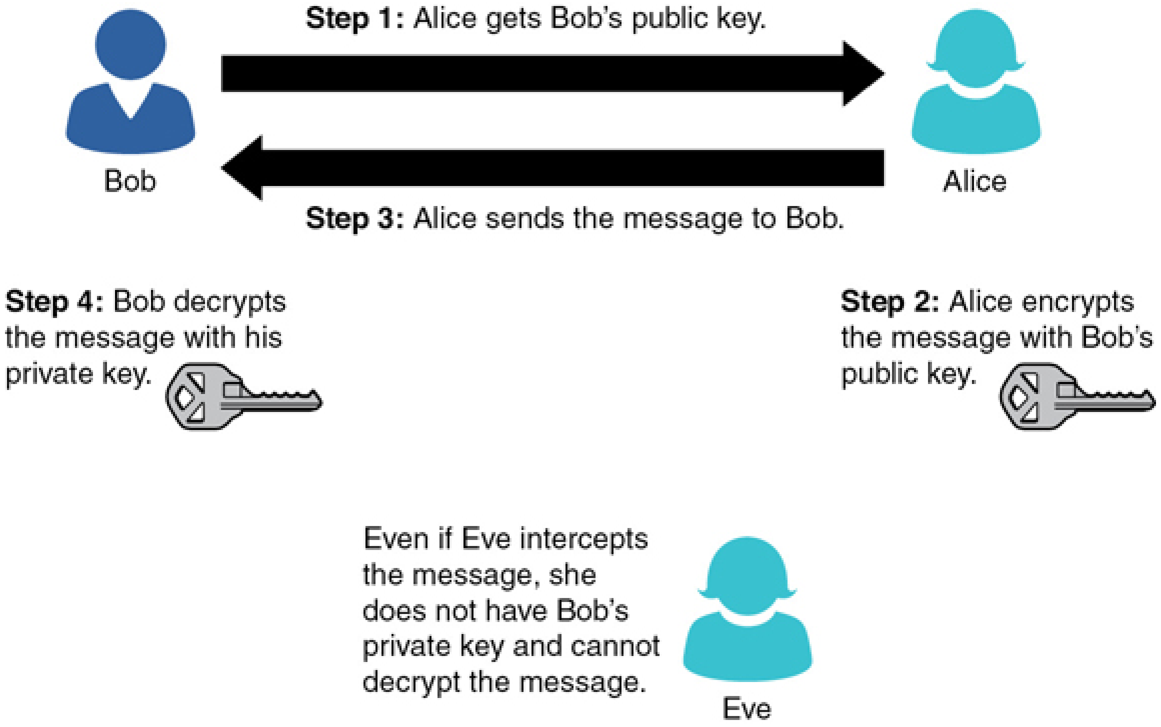
- Asymmetric (Public) Key Encryption
  - Public key cryptographic systems developed for key distribution solve the problem of getting single symmetric keys into the hands of two people who do not know each other but who want to exchange information securely.
  - Based on an asymmetric encryption process, two keys work together as a pair. One key is used to encrypt data; the other is used to decrypt data.
  - Either key can be used to encrypt or decrypt, but once the key has been used to encrypt data, only its partner can be used to decrypt the data.
  - The key that was used to encrypt the data cannot be used to decrypt it. Thus, the keys are asymmetric in that they are inversely related to each other.

Encryption Techniques

- Asymmetric (Public) Key Encryption
  - Based on mathematical integer factorization, asymmetric keys generate a single product from two large prime numbers, making it impractical to factor the number and recover the two factors.
  - This integer factorization process forms the basis for public key cryptography, a function that is easy to compute in one direction but very difficult or impractical in the other.
  - The system involves modular arithmetic, exponentiation and large prime numbers thousands of bits long.
  - Asymmetric keys are often used for short messages such as encrypting DES symmetric keys or creating digital signatures.
  - If asymmetric keys were used to encrypt bulk data (long messages), the process would be very slow; this is the reason they are used to encrypt short messages such as digests or signatures.

Encryption Techniques

- Asymmetric (Public) Key Encryption



Step 1: Alice gets Bob's public key.

Step 3: Alice sends the message to Bob.

Step 4: Bob decrypts the message with his private key.

Step 2: Alice encrypts the message with Bob's public key.

Even if Eve intercepts the message, she does not have Bob's private key and cannot decrypt the message.

Encryption Techniques

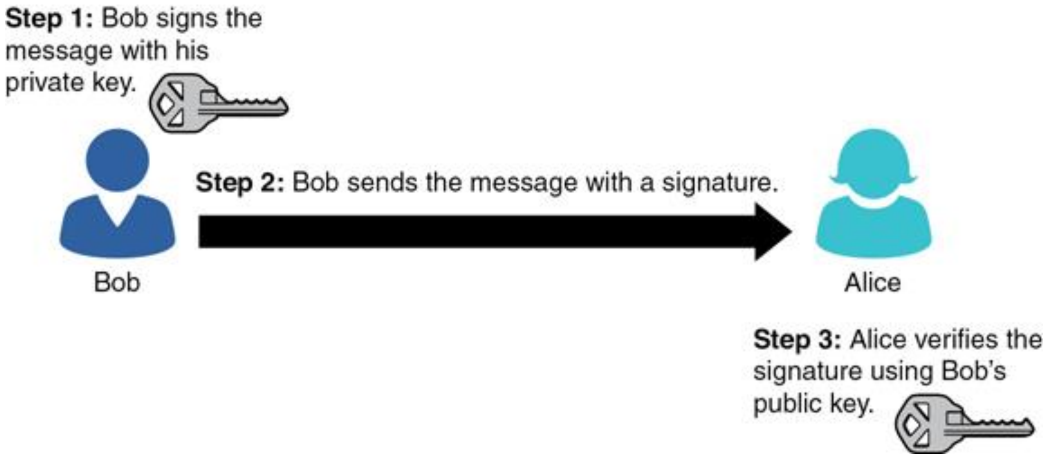
- Elliptical Curve Cryptography
  - Although public key cryptography ensures message security, the long keys and mathematical problems it uses tend to be inefficient.
  - A variant and more efficient form of public key cryptography is elliptical curve cryptography (ECC), which is gaining prominence as a method for increasing security while using minimum resources.
  - It is believed that ECC demands less computational power and therefore offers more security per bit.
  - For example, an ECC with a 160-bit key offers the same security as an RSA-based system with a 1,024-bit key.
  - ECC works well on networked computers requiring strong cryptography. However, it has some limitations such as bandwidth and processing power.

Advanced Encryption Standard

- AES has replaced the DES as the cryptographic algorithm standard. It originated in 1997, when NIST announced the initiation of the AES development effort and made a formal call for algorithms.
- For AES the block length was fixed to 128 bits, and three different key sizes (128, 192 and 256 bits) were specified. Therefore, AES-128, AES-192 and AES-256 are three different versions of AES.
- The cipher is based on substitution bytes, shifting rows, mixing columns and adding round keys that are repeated for 10 rounds.
- Each round has a 128-bit round key and the result of the previous round as input. The round keys can be precomputed or generated out of the input key. Due to its regular structure, it can be implemented efficiently in hardware.
- Decryption is computed by applying inverse functions of the round operations. The sequence of operations for the round function differs from encryption, which often results in separated encryption and decryption circuits.

Digital Signature

- A digital signature is not used to ensure the confidentiality of a message but rather to guarantee who sent the message.
- This is referred to as nonrepudiation. Essentially, nonrepudiation means proving who the sender is.
- Digital signatures are actually rather simple, but they are clever. They simply reverse the asymmetric encryption process.
- With a digital signature, the sender encrypts something with his private key. If the recipient is able to decrypt that with the sender's public key, then it must have been sent by the person purported to have sent the message


Step 1: Bob signs the message with his private key.
Step 2: Bob sends the message with a signature.
Bob
Alice
Step 3: Alice verifies the signature using Bob's public key.

Hashing

- A hashing is a type of cryptographic algorithm that has some specific characteristics. First and foremost, it is one way. That means you cannot unhash something.
- Second, you get a fixed-length output no matter what input is given.
- Third, there are no collisions. A collision occurs when two different inputs to the same hashing algorithm produce the same output (called a hash or digest). Ideally we would like to have no collisions.
- Hashes are exactly how Windows stores passwords. For example, if your password is password, then Windows will first hash it and produce something like this:

  0BD181063899C9239016320B50D3E896693A96DF

- Windows will then store that in the SAM (Security Accounts Manager) file in the Windows System directory. When you log on, Windows cannot unhash your password (because, remember, it is one way). So, what Windows does is take whatever password you type in, hash it, and then compare the result with what is in the SAM file. If they match (exactly), then you can log in.

Hashing

- MD5
  - MD5 is a 128-bit hash that is specified in RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. MD5 produces a 128-bit hash or digest. It has been found to be not as collision resistant as SHA.
- SHA
  - Secure Hash Algorithm (SHA) is perhaps the most widely used hash algorithm today. There are now several versions of SHA. All versions of SHA are considered to be secure and collision free:
    - SHA-1: This is a 160-bit hash function that resembles the earlier MD5 algorithm. It was designed by the NSA to be part of the Digital Signature Algorithm (DSA).
    - SHA-2: This is actually two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-byte (256 bits) words, whereas SHA-512 uses 64-byte (512 bits) words. There are also truncated versions of each standardized, known as SHA-224 and SHA-384. These were also designed by the NSA.
    - SHA-3: This latest version of SHA was adopted in October 2012.

Steganography

- Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.
- It is a form of security through obscurity. Often the message is hidden in some other file, such as a digital picture or an audio file, to defy detection.
- The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. If someone is aware that a message is even there, she won’t try to decipher it. In many cases, messages are encrypted and hidden via steganography.
- The most common implementation of steganography utilizes the least significant bits in a file in order to store data. By altering the least significant bit, you can hide additional data without altering the original file in any noticeable way.

Cryptography on the Internet

- Secure transport
    - In general, symmetric algorithms are faster and require a shorter key length to be as secure as asymmetric algorithms.
    - However, there is the problem of how to securely exchange keys. So most e-commerce solutions use an asymmetric algorithm to exchange symmetric keys and then use the symmetric keys to encrypt the actual data.
    - When visiting websites that have an HTTPS at the beginning rather than HTTP, the S denotes Secure.
    - It means traffic between your browser and the web server is encrypted—usually with either SSL (Secure Sockets Layer) or TLS (Transport Layer Security). Both SSL and TLS are asymmetric systems.

Cryptography on the Internet

- Virtual Private Network
  - A VPN is an example of applied cryptography that typically exchanges secure data over the Internet.
  - Encryption is needed to make the connection virtually private. A popular VPN technology is IPSec, which commonly uses the DES, Triple DES or AES encryption algorithms.
- Wireless Network Protections
  - Wireless data transmission is subject to a higher risk of interception than wired traffic, in the same way that it is easier to intercept calls made from cell phones than calls from landline telephones.
  - There is no need to manually tap into the connection, but rather remote tools can be used to intercept the connection covertly. Wireless transmission of confidential information should be protected with strong encryption.

Virus Scanners

- A virus scanner is essentially software that tries to prevent a virus from infecting a system.
- In general, virus scanners work in two ways. First, a virus scanner may contain a list of all known virus definitions—that is, files that list known viruses and their file sizes, properties, and behaviors.
- Generally, one of the services that vendors of virus scanners provide is to periodically update these files.
- When you update your virus definitions, what actually occurs is that your current file is replaced by the more recent one available from the vendor.
- The antivirus program can then scan your PC, network, and incoming email for known virus files. Any file on your PC or attached to an email is compared to the virus definition file to see whether there are matches.
- With emails, this can be done by looking for specific subject lines and content. The virus definitions often also include details on the file, file size, and more. This provides a complete signature of the virus.

Virus Scanners

- The second way a virus scanner can work is to look for virus-like behavior.
- Essentially, the scanner looks to see if the file in question is doing things that viruses typically do–things like manipulating the Registry or looking through your address book.
- Obviously, this second technique is essentially a best guess.

Virus-Scanning Techniques

- In general, there are six ways a virus scanner might scan for virus infections.
  - Email and attachment scanning:
    - Since the primary propagation method for a virus is email, email and attachment scanning is the most important function of any virus scanner.
    - Some virus scanners actually examine your email on the email server before downloading it to your machine.
    - Other virus scanners work by scanning your emails and attachments on your computer before passing them to your email program.
    - In either case, email and email attachments should be scanned before a user has a chance to open them and release viruses on the system.

Virus-Scanning Techniques

- Download scanning:
  - Any time you download anything from the Internet, either via a web link or through an FTP program, there is a chance you might download an infected file.
  - Download scanning works much like email and attachment scanning but operates on files you select for downloading.
- File scanning:
  - With file scanning, files on your system are checked to see whether they match any known virus.
  - This sort of scanning is generally done on an on-demand basis instead of an ongoing basis.
  - It is a good idea to schedule your virus scanner to do a complete scan of the system periodically.

Virus-Scanning Techniques

- Heuristic scanning:
  - Heuristic scanning, briefly mentioned in the previous section, is perhaps the most advanced form of virus scanning.
  - Because it uses rules to determine whether a file or program is behaving like a virus, heuristic scanning is one of the best ways to find a virus that is not a known virus.
  - A new virus will not be on a virus definition list, so you must examine its behavior to determine whether it is a virus.
  - However, this process is not foolproof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being viruses.
- Sandbox:
  - The sandbox approach basically involves having a separate area, isolated from the operating system, in which a download or an attachment is run. Then, if it is infected, it won't infect the operating system.
- Machine learning:
  - Most antivirus vendors are now working to implement basic machine learning algorithms into their antivirus software. This allows the antivirus software to adapt to changing attacks. Machine learning is only beginning to be used and is not yet well developed.

Firewalls

- A firewall is, in essence, a barrier between two computers or computer systems.
- The most common place to encounter a firewall is between a network and the outside world.
- However, firewalls on individual computers and between network segments are also quite common.
- At a minimum, a firewall will filter incoming packets based on certain parameters, such as packet size, source IP address, protocol, and destination port.
- In an organizational setting, you will want, at a minimum, a dedicated firewall between your network and the outside world.
- This might be a router that also has built-in firewall capabilities. It might be a server that is dedicated solely to running firewall software.

Firewall Types and Components

- There are numerous types of firewalls and variations on those types. But most firewalls can be grouped into one of the following three families of firewalls:
  - Packet inspection
    - Basic packet filtering is the simplest form of firewall. It involves looking at packets and checking to see if each packet meets the firewall rules. For example, it is common for a packet filtering firewall to consider three questions:
      - Is this packet using a protocol that the firewall allows?
      - Is this packet destined for a port that the firewall allows?
      - Is the packet coming from an IP address that the firewall has not blocked?
    - These are three very basic rules. Some packet filter firewalls check additional rules. But what is not checked is the preceding packets from that same source. Essentially, each packet is treated as a singular event, without reference to the preceding conversation. This makes packet filtering firewalls quite susceptible to some DoS attacks, such as SYN floods.

Firewall Types and Components

- Stateful Packet Inspection
  - Any stateful packet inspection (SPI) firewall will examine each packet and deny or permit access based not only on the examination of the current packet but also on data derived from previous packets in the conversation.
  - The firewall is therefore aware of the context in which a specific packet was sent.
  - This makes such a firewall far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing.
  - For example, if a firewall detects that the current packet is an ICMP packet and a stream of several thousand packets have been continuously coming from the same source IP, the firewall will see that this is clearly a DoS attack, and it will block the packets.
  - A stateful packet inspection firewall can also look at the actual contents of a packet, which allows for some very advanced filtering capabilities.

Firewall Types and Components

- Application Gateways
  - An application gateway (also known as application proxy or application-level proxy) is a program that runs on a firewall.
  - When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy.
  - The client then negotiates with the proxy server in order to gain access to the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall.
  - This process actually creates two connections. There is one connection between the client and the proxy server, and there is another connection between the proxy server and the destination.
  - Once a connection is established, the application gateway makes all decisions about which packets to forward. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

Firewall Configurations

- In addition to the various types of firewalls, there are various configuration options.
- The type of firewall tells you how it will evaluate traffic and hence decide what to allow and not to allow.
- The configuration gives you an idea of how that firewall is set up in relation to the network it is protecting.
- Some of the major configurations/implementations for firewalls include the following:
  - Network host-based firewall
  - Dual-homed host
  - Router-based firewall
  - Screened host

Firewall Configurations

- Network Host-Based Firewalls
  - A network host-based firewall is a software solution installed on an existing machine with an existing operating system.
  - The most significant concern in using this type of firewall is that no matter how good the firewall solution is, it is contingent upon the underlying operating system. In such a situation, it is absolutely critical that the machine hosting the firewall have a hardened operating system.
- Dual-Homed Host
  - A dual-homed host is a firewall running on a server with at least two network interfaces.
  - The server acts as a router between the network and the interfaces to which it is attached.
  - To make this work, the automatic routing function is disabled, meaning that an IP packet from the Internet is not routed directly to the network.
  - You can choose what packets to route and how to route them. Systems inside and outside the firewall can communicate with the dual-homed host but cannot communicate directly with each other.

Firewall Configurations

- Router-Based Firewall
  - As was previously mentioned, you can implement firewall protection on a router. In larger networks with multiple layers of protection, this is commonly the first layer of protection.
  - Although you can implement various types of firewalls on a router, the most common type used is packet filtering.
  - If you use a broadband connection in your home or small office, you can get a packet-filtering firewall router to replace the basic router provided to you by the broadband company.
  - In recent years, router-based firewalls have become increasingly common and are in fact the most common type of firewall used today.
- Screened Host
  - A screened host is really a combination of firewalls. In this configuration, you use a combination of a bastion host and a screening router.
  - The screening router adds security by allowing you to deny or permit certain traffic from the bastion host. It is the first stop for traffic, which can continue only if the screening router lets it through.

Intrusion Detection System (IDS)

- IDSs have become much more widely used in the past few years. Essentially, an IDS inspects all inbound and outbound port activity on a machine/firewall/system, looking for patterns that might indicate break-in attempts.
- For example, if an IDS finds that a series of ICMP packets were sent to each port in sequence, this probably indicates that the system is being scanned by network-scanning software, such as Cerberus.
- This type of scan is often a prelude to an attempt to breach system security, and it can be very important to know that someone is performing preparatory steps to infiltrate your system.
- There are a number of ways in which IDSs can be categorized. The most common IDS categorizations are as follows:
  - Passive IDSs
  - Active IDSs (also called intrusion prevention systems, or IPSs)

Identifying an Intrusion

- There are really two ways of identifying an intrusion. The first method is signature based.
- This is similar to the signatures used by antivirus. However, IDS signatures cover issues beyond malware. For example, certain DoS attacks have specific signatures that can be recognized.
- The second method is statistical anomaly. Essentially, any activity that seems outside normal parameters and far enough outside the given parameters to be a likely attack is identified as a probable attack.
- Any number of activities can trigger this type of alert, such as a sudden increase in bandwidth utilization or user accounts accessing resources they have never accessed before.
- Most IDSs use both forms of attack identification.

Honey Pots

- Essentially, it assumes that an attacker is able to breach your network security, and it would be best to distract that attacker away from your valuable data.
- Therefore, a honey pot involves creating a server that has fake data–perhaps an SQL server or Oracle server loaded with fake data, and just a little less secure than your real servers.
- Then, since none of your actual users ever access this server, monitoring software is installed to alert you when someone does access this server.
- A honey pot achieves two goals. First, it takes the attacker's attention away from the data you wish to protect.
- Second, it provides what appears to be interesting and valuable data, thus leading the attacker to stay connected to the fake server, giving you time to try to track the attacker.

Digital Certificates

- The digital certificate contains the user's public key, along with other information.
- However, a digital certificate can provide much more. It can provide a means for authenticating that the holder of the certificate is who she claims to be.
- X.509 is an international standard for the format and information contained in a digital certificate.
- X.509 is the most common type of digital certificate in the world. It is a digital document that contains a public key signed by the trusted third party that is known as a certificate authority, or CA.

Digital Certificates

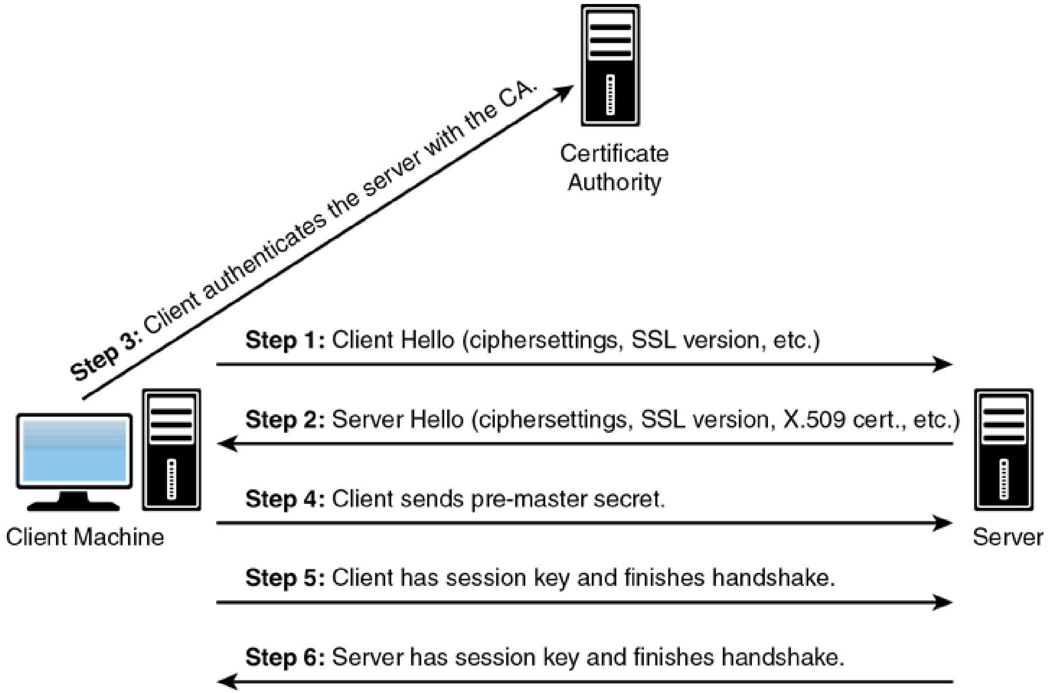
- The following are the basic items in an X.509 certificate, though there can be other optional information:
  - Version: This is the version of X.509 that this certificate complies with.
  - Certificate holder’s public key: This is the primary way of getting someone’s public key from his X.509 certificate.
  - Serial number: This is a unique identifier for this certificate.
  - Certificate holder’s distinguished name: This is often a domain name or an email address associated with a certificate.
  - Certificate’s validity period: One year is the most common validity period.
  - Unique name of certificate issuer: This is the certificate authority that issued this certificate.
  - Digital signature of issuer: This field and the next are used to verify the certificate.
  - Signature algorithm identifier: This identifies the digital signature algorithm used.

Digital Certificates

- Let us see how this works in a common scenario. Say that you visit your bank’s website. In order to get the bank’s public key, your browser will download that bank’s digital certificate.
- But there is a problem. Could someone have set up a fake site, claiming to be your bank? Could that person have also generated a fake certificate, claiming to be the bank? Yes, it’s possible.
- This is one place digital certificates help us out. Your browser will look at the certificate issuer listed on the certificate and first ask if that is a CA that your browser trusts.
- If it is, then your browser communicates with that CA to get that CA’s public key. The browser uses that CA public key to verify the CA signature on the certificate.
- If this is a fake certificate, the digital signature won’t be recognized. This means a certificate not only provides you with the certificate holder’s public key but also gives you a method of verifying that entity with a trusted third party.

SSL/TLS

- When visiting websites that have an HTTPS at the beginning, rather than HTTP, the S denotes Secure.
- It means traffic between your browser and the web server is encrypted—usually with either SSL (Secure Sockets Layer) or TLS (Transport Layer Security).
- SSL and TLS are both asymmetric systems.
- SSL, the older of the two technologies, is used to allow for transport-layer security via public key encryption.


Certificate Authority
Step 3: Client authenticates the server with the CA.
Step 1: Client Hello (ciphersettings, SSL version, etc.)
Step 2: Server Hello (ciphersettings, SSL version, X.509 cert., etc.)
Step 4: Client sends pre-master secret.
Client Machine
Server
Step 5: Client has session key and finishes handshake.
Step 6: Server has session key and finishes handshake.

Virtual Private Networks

- A VPN (or virtual private network) essentially provides a way to use the Internet to create a virtual connection between a remote user or site and a central location.
- The packets sent back and forth over this connection are encrypted, thus making it private. The VPN must emulate a direct network connection.
- Three different protocols are used to create VPNs:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPsec)

Wi-Fi Security

- Wireless networks are commonly used today, and it is important to consider wireless network security.
- There are three Wi-Fi security protocols, ranging from the oldest and least secure (WEP) to the most recent and most secure (WPA3).
- Wired Equivalent Privacy (WEP) uses the stream cipher RC4 to secure data and a CRC-32 checksum for error checking.
- Standard WEP uses a 40-bit key (known as WEP-40) with a 24-bit initialization vector (IV) to effectively form 64-bit encryption. The IV is reused, which defeats the entire purpose of an IV and leaves the protocol open to attacks.
- Wi-Fi Protected Access (WPA) was definitely an improvement over WEP. First, WPA uses AES, which is a very good encryption algorithm. In addition, WPA uses Temporal Key Integrity Protocol (TKIP), which dynamically generates a new key for each packet.