Information Security and Network Security

Chapter – 5

Network Security

Fundamental Network Security

For the first few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions' security did not get a lot of attention. But now in corporate network is used connect all the computers to share the server data and run the enterprise on line applications. Also, millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is becoming potentially massive problem.

Network security is concerned with making sure that nosy (having curiosity about other people's affairs) people cannot read, worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. It also deals with problems of legitimate (Confirming to law) messages being captured and replayed, and with people trying to deny that they sent certain messages.

Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. A few of most common perpetrators (Person who carries out harmful, illegal or immoral act) are as follows

Adversary	Goal
Student	To have fun snooping (trying to find something especially information about someone's private affairs) on people's e-mail
Cracker	To test out someone's security system; steal data
Businessman	To discover a competitor's strategic marketing plan
Ex-employees	To get revenge for being fired
Accountant	To embezzle (steal or misappropriate) money from company
Stockbroker	To deny a promise made to customer by e-mail
Con Man (Cheater)	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

It should be clear from above list that making a network secure involves lot more than just keeping it free of programming errors. It involves outsmarting often intelligent, dedicated and sometimes well-funded adversaries (conflict).

Network security problems can be divided into four closely intertwined (twist) areas:

- Secrecy – Also called Confidentiality, hast to do with usually keeping information out of hands of unauthorized users. This is what comes to mind when people think about network security.

- Authentication – deals with determining whom we are talking before revealing (significant information known) sensitive information or entering into a business deal.
- Non-repudiation – deals with signatures: Deny of message sent or message received. e.g. How do you prove that your customer really placed an electronic order for ten laptops at Rs 35,000/- each he later claims that price was 25,000/? Or maybe claims he never placed any order. Finally, how we can sure that the message we received was really the on sent and not something malicious adversary modified in transit or concocted (Combining other information)?
- Integrity control – Control of unauthorized writing while transmitting message.

Integrity and secrecy are achieved by using registered mail and locking documents up. In the data link layer, packets on a point-to-point line can be encrypted as they leave one machine and decrypted as they enter another. All details can be handled in the data link layer, with higher layers oblivious (not concern about) to what is going on. This solution breaks down when packets have to traverse multiple routers, however, because packets have to be decrypted at each router, leavening them vulnerable to attacks from within router. Also, it does not allow some sessions to be protected and others not. This method is called **link encryption** can be added to any network easily and is often useful.

In the network layer, firewalls can be installed to keep good packets and bad packets out. IP security also functions in this layer.

In transport layer, entire connections can be encrypted, end to end, that is process to process. For maximum security end-to-end security is required. Finally, issues such as user authentication and nonrepudiation can be handled in the application layer.

It is well documented that most security failures at banks, for example, are due to incompetent employees, lax (not sufficiently strict) security procedures, or insider's fraud, rather than clever criminals tapping phone lines and then decoding encrypted messages. E-commerce becomes more widespread, companies will eventually debug their operational procedures, eliminating this loophole and bringing the technical aspects of security to center stage again.

Except for physical layer security, nearly all security is based on cryptographic principles.

Communication Security

Communication security, that is, how to get the bits secretly and without modification from source to destination and how to keep unwanted bits outside door.

Transport Level/Layer Security

The basic function of the transport layer is to accept data, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were

sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is true end-to-end layer, all the way from the source to destination. In other words, a program on the destination machine, using the message headers and control messages. The layer is above internet layer in TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversion, just as in the OSI (Open Systems Interconnection) transport layer. Two end-to-end transport protocols have been defined. The first one, TCP (Transmission Control Protocol), is reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do

not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

Transport-level security is a well-known and often used mechanism to secure HTTP (Hyper Text Transport Protocol) Internet and intranet communications. Transport level security can be used to secure web services messages. Transport-level security functionality is independent from functionality that is provided by message-level security (Web Socket WS-Security) or HTTP basic authentication.

We can use either message-level security (WS-Security) or transport-level security, or a combination of both. The following examples are common usage scenarios, but are not an exhaustive list of all possible scenarios:

- Use message-level security when security is essential to the Web service application. HTTP basic authentication uses a user name and password to authenticate a service client to a secure endpoint. The basic authentication is encoded in the HTTP request that carries the SOAP (Simple Object Access Protocol) message. When the application server receives the HTTP request, the user name and password are retrieved and verified using the authentication mechanism specific to the server.

  Important: With message-level security, if you are not using the default outbound secure sockets layer (SSL) port of 443, ensure that the dynamic outbound endpoint for SSL is configured properly for your configuration.

- Use transport-level security to enable basic authentication. Transport-level security can be enabled or disabled independently from message-level security. Transport-level security provides minimal security. You can use this configuration when a web service is a client to another web service.

- Use SSL for confidentiality and integrity and HTTP Basic Authentication for authentication.
- Use SSL for confidentiality and integrity and WS-Security for authentication. For example, a Username token or LTPA (Lightweight Third-Party Authentication) token can be used for authentication.
- Use WS-Security for both confidentiality and integrity, and authentication.

Transport-level security is based on Secure Sockets Layer (SSL) or Transport Layer Security (TLS) that runs beneath HTTP. HTTP, the most used Internet communication protocol, is currently also the most popular protocol for web services. HTTP is an inherently insecure protocol because all information is sent in clear text between unauthenticated peers over an insecure network. To secure HTTP, transport-level security can be applied.

Transport level security can be used to secure web services messages. However, transport-level security functionality is independent from functionality that is provided by WS-Security or HTTP Basic Authentication.

SSL and TLS provide security features including authentication, data protection, and cryptographic token support for secure HTTP connections. To run with HTTPS (S for Secure), the service port address must be in the form https://. The integrity and confidentiality of transport data, including SOAP messages and HTTP basic authentication, is confirmed when you use SSL and TLS.

Web services applications can also use Federal Information Processing Standard (FIPS) approved ciphers for more secure TLS connections. WebSphere Application Server uses the Java™ Secure Sockets Extension (JSSE) package to support SSL and TLS.

This task is one of several ways that you can configure the HTTP outbound transport level security for a web service acting as a client to another Web service server. You can also configure the HTTP outbound transport level security with an assembly tool or by using the Java properties. If you do not configure the HTTP outbound transport level security, the web services runtime defers to the Java Platform, Enterprise Edition (Java EE) security runtime in the WebSphere product for an effective Secure Sockets Layer (SSL) configuration. If there is no SSL configuration with the Java EE security runtime in the WebSphere product, the Java Secure Socket Extension (JSSE) system properties are used.

You can define additional HTTP transport properties for web services applications. Use the additional properties to manage the connection pool for HTTP outbound connections, configure the content encoding of the HTTP message, enable HTTP persistent connection, and resend the HTTP request when a timeout occurs.

Procedure

1. Develop and assemble a web services application.
    a. You can configure and assemble the HTTP outbound transport level security for the application with an assembly tool.
2. Deploy the application.
    a. For more information about deploying web services applications, read about deploying Web services.
3. Configure transport level security for the application.
    a. Use one of the following methods to configure HTTP outbound transport level security:
        - Configure HTTP outbound transport level security using the administrative console.
        - Configure HTTP outbound transport-level security using Java properties.
4. Define additional HTTP transport properties for the Web services application.
    a. Use one of the following methods to define additional HTTP transport properties:
        - Configure additional HTTP transport properties using the JVM custom property panel in the administrative console.
        - Configure additional HTTP transport properties using an assembly tool.

By completing these steps, you have secured web services applications at the transport level.

Wireless Network Security

Digital wireless communication is not new idea. As early as 1901, the Italian physicist Guglielmo Marconi demonstrated a ship-to-shore wireless telegraph, using Morse Code (dots and dashes are binary after all). Modern digital wireless systems have better performance, but the basic idea is the same.

The wireless networks can be divided three main categories:

1. **System interconnections**
   System interconnections is all about interconnecting the components of computer using short-range radio. Almost every computer has monitor, keyboard, mouse, and printer connected to main unit by cables. Some companies got their deign a short-range wireless network called **Bluetooth** to connect these components without wires. Bluetooth also allows digital cameras, headsets, scanners, and other devices to connect to a computer by merely being brought within range. The system unit is normally the master, talking to the mouse, keyboard etc as salves.
2. **Wireless LANs**
   These are systems in which every computer has radio modem and antenna with which it can communicate with other systems. Often there is an antenna on the ceiling that the machines talk. However, if the systems are close enough, they can communicate directly with one another in a peer-to-peer configuration. Wireless LANs are becoming increasingly common in small offices and homes, where installing Ethernet is considered too much trouble, as well as in older office building, company cafeterias, conference rooms, and other places. There is standard for wireless LANs called IEEE (Institute of

Electrical and Electronics Engineers) 802.11, which most systems implement and which is becoming very widespread.

3. Wireless WANS

Third kind of wireless network is used in wide area systems. The radio network used for cellular telephone is an example of low-bandwidth wireless system. In addition to these low-speed networks, high-bandwidth wide area wireless networks are also being developed. The initial focus is high-speed wireless Internet access from homes and business, bypassing the telephone system. This service is often called local multipoint distribution service. Almost all wireless network hooks up to wired network at some point to provide access to files, databases, and the Internet.

Wireless Security

It is surprisingly easy to design a system that is logically completely secure by using VPNs (Virtual Private Network) and firewalls, but that, in practice, leaks like sieve (mesh). This situation can occur if some of machines are wireless and use radio communication, which passes right over that firewall in both directions.

Much of security problems can be traced to the manufacturers of wireless base stations (access points) trying to make their products user friendly. Usually, if the user takes a device out of the box and plugs it into the electrical power socket, it begins operating immediately – nearly always with no security at all, blurting secrets to everyone within radio range. If it is then plugged into the Ethernet, all the traffic suddenly appears in the parking lot as well. Wireless is snooper's dream come true: free data without having to do any work. It therefore goes without saying that security is even more important for wireless systems than for wired ones.

802.11 Security

The 802.11 standard prescribes a data link-level security protocol called WEP (Wired Equivalent Privacy), which is designed to make the security of a wireless LAN as good as that of wired LAN.

When 802.11 security is enabled, each station has secret has secret key shared with the bas station. They could be preloaded by manufacturer. They could exchange in advance over the wired network. Finally, either the base station or user machine could pick a random key and send it to other one over the air encrypted with other one's public key. Once established, keys generally remain stable for months or years.

WEP encryption uses a stream cipher based on the RC4 algorithm. RC4 was designed by Ronald Rivest and kept secret until it leaked out and was posted to the internet in 1994. As we have pointed out before, it is nearly impossible to keep algorithms secret, even when the goal is guarding intellectual property rather than security by obscurity (unknown).

But even if each user has a distinct key, WEP can still be attacked. Since keys are generally stable for long period of time, the WEP standard recommends (but does not mandate) that IV be changed on every packet to avoid the key stream reuse attack. Unfortunately, many 802.11 cards for notebook computers reset IV to 0 when the card is inserted into the computer, and increment it by one on each packet sent.

Bluetooth Security

Bluetooth has a considerably, shorter range than 802.11 so it cannot be attacked from the parking lot, but security is still an issue here. Bluetooth has three security modes on/off. Bluetooth provides security in multiple layers.

Physical layers, frequency hopping provides tiny bits of security, but since any Bluetooth device that moves into a piconet (is an ad hoc network that links a wireless user group of devices using Bluetooth technology) has to be told the frequency hopping (jumping) sequence, this sequence is obviously not secret. The real security starts when newly-arrived slave asks for channel with the master. The two devices are assumed to share a secret key set up in advance. These shared keys are called as **passkeys.**

To establish a channel, the slave and master each check to see if other on known the passkey. If so, they negotiate whether that channel will be encrypted, integrity controlled, or both Then they select a random 128-bit session key, some of whose bits may be public. The point allowing this key weakening is to comply with government restrictions in various countries designed to prevent the export or use of keys longer than the government can break.

It sometimes amazes people that then perennial (exiting for long time) cat-and-mouse-game between cryptographers and cryptanalysts, the cryptanalyst is so often on the winning side. Another issue in that Bluetooth authenticates only devices, not users, so theft of a Bluetooth device may give the thief access to the user's financial and other accounts. However, Bluetooth also implements security in the upper layers, so even in the event of breach of link-level security, some security may remain, especially for applications that require a PIN code to the entered manually from some kind of keyboard to complete the transaction.

IP Security (IPsec)

IETF (Internet Engineering Task Force) known for years that security was lacking in the internet. The result of this comment was design called IP security (IPsec) which is described in RFCs (Request for Comments is formal standards-track document developed in working groups within the IETF) 2401, 2402 and 2406 among others. Not all users want to encryption (because it is computationally expensive). Rather than make it optional, it was decided to require encryption all the time but permit the use of a null algorithm. The null algorithm is described ad praised for its simplicity, ease of implementation, and great speed in RFC 2410.

The complete IPsec design is a framework for multiple services, algorithms and granularities (define who can have access to each part of a system, as well as what they can do with that access). The reason for multiple services is that not everyone wants to pay the price for having all the services all the time, the major services are secrecy, data integrity, and protection from replay attacks (intruder replays a conversation).

The reason for having multiple algorithms is that an algorithm that is now thought to be secure may be broken in the future. By making IPsec algorithm-independent, the framework can survive even if some particular algorithm is later broken.

The reason for having multiple granularities is to make it possible to protect a single TCP connection, all traffic between a pair of hosts, or all traffic between a pair of secure routers, among other possibilities.

One slightly surprising aspect of IPsec is that even though it is IP layer, it is connection oriented. To have any security, a key must be established and used for some period of time – in essence a kind of connection. A "connection" in IPsec is called a SA (Security Association). A SA is simplex connection between two end points and has a security identifier associated with

it. If security traffic is needed in both directions, two security associations are required. Security identifiers are carried in packets travelling on these secure connections and are used to look up keys and other relevant information when a secure packet arrives.

IPsec has two principal parts. The first part describes two new headers that can be added to packets to carry the security identifier, integrity control data, and other information. The other part, ISAKMP (Internet Security Association and Key Management Protocol) deals with establishing keys.

IPsec can be used in either of two modes. In **transport mode**, the IPsec header is inserted just after the IP header. The *protocol* field in the IP header is changed to indicate that an IPsec header follows the normal IP header (before the TCP header). The IPsec header contains security information, primarily the SA identifier, a new sequence number, and possibly an integrity check of the payload.

In **tunnel mode** the entire IP packet, header an all, is encapsulated in the body of new IP packet with a completely new IP header. Tunnel mode is useful when the tunnel ends at a location other than the final destination. In some cases, the end of the tunnel is security gateway machine, for example company firewall. In this mode, the firewall encapsulates ad decapsulates packets as they pass though the firewall. Tunnel mode is also useful when a bundle of TCP connections is aggregated and handled as one encrypted stream because it prevents an intruder from seeing who is sending how many packets to whom. Sometimes just knowing how much traffic is going where is valuable information. Studying the flow patterns of packets, even if they are encrypted is called **traffic analysis**. Tunnel mode provides a way to foil it to some extent. The disadvantage of tunnel mode is that it adds an extra IP header, thus increasing packet size as much.

The first new header is AH (Authentication Header). It provides integrity checking and antireplay security, but not secrecy (i.e. no data encryption). The use of AH is in transport mode.

Finally, we come to the *Authentication data*, which is a variable length field that contains the payload's digital signature. When is SA is established, the two sides negotiate which signature algorithm they are going to use. IPsec is based on symmetric-key cryptography and the sender and receiver negotiate a shared key before setting up a SA, the shared key is used in the signature computation. One simple way to compute the hash over the packet plus the shared key. The shared key is not transmitted of course. A Scheme like this is called HMAC (Hashed Message Authentication Code).

Network Endpoint Security.

Endpoint security or endpoint protection is an approach to the protection of computer networks that are remotely bridged to client devices. The connection of endpoint devices such as laptops, tablets, mobile phones, internet-of-things devices, and other wireless devices to corporate networks creates attack paths for security threats. Endpoint security attempts to ensure that such devices follow a definite level of compliance to standards.

The endpoint security space has evolved during the 2010s away from limited antivirus software and into a more advanced, comprehensive defence. This includes next-generation antivirus, threat detection investigation, and response, device management, data leak protection (DLP), and other considerations to face evolving threats.

Endpoints are target of many cyberattacks, and with shifts in corporate IT infrastructure, are becoming more vulnerable to attack. Increased support for remote work moves corporate endpoints outside of enterprise network and its protection Bring your own device (BYOD)

policies allow employee-owned devices to connect to the enterprise network and access sensitive corporate data.

The Endpoint protection always been important for defence in depth, but the blurring (less clear) of the enterprise network perimeter due to the remote work and BYOD policies has made it even more important. Endpoints are companies first line of defence against cyber threats and major source of cyber risk.

How Does It Work?

Endpoint protection work via a combination of network and device-level Défense. At network level, the organization may restrict access to the enterprise network based on a device's compliance with corporate security policies and least privilege. By Blocking insecure devices from accessing the corporate network and sensitive resources, the organization restricts its attack surface and enforces its security policies.

Organization may also install software directly on and endpoint to monitor and protect it. This includes both standalone solutions and ones that use an agent installed on the device to allow it to be centrally monitored, controlled, and protected. This allows an organization to monitor and protect devices that may not always be connected directly to the enterprise network.

Types of Endpoint Protection

The modern enterprise has a variety of different endpoints that face a wide range of potential cyber threats. Endpoint protection solutions comes in several different forms, including:

- Endpoint Detection and Response (EDR)
- Endpoint Protection Platform (EDP)
- Mobile Threat Defence (MTD)
- Advanced Threat Protection (ATP)

The right choice of an endpoint security solution depends on the endpoint in question and company's unique needs. For example, as remote work and BYOD become more common, mobile devices are greater focus of cybercriminals, and MTD is more vital endpoint protection solution.

Endpoint Protection Features (Components)

An endpoint protection solution should offer comprehensive protection to the endpoint and corporate network. Some essential features of endpoint security solution include the following:

- Anti-Malware: Endpoint protection solutions should detect and prevent infections by viruses, worms and other malware.
- Behavioural Analytics: Ransomware and other malware variants have unique behaviours that make them detectable without the use of signatures. By monitoring these behaviours, endpoint protection solutions can detect and respond to zero-day attacks.
- Compliance: The ability to enforce compliance with enterprise security policies is increasingly important with growth of remote work and BYOD endpoint solutions should evaluate devices and only allow connections to the corporate network if they are compliant with corporate policy.

- Data Encryption: Encryption is the most effective way to protect data against unauthorized access and potential breach. Endpoint security solutions should offer full disk encryption (FDE) and support encryption of removable media.
- Firewall and Application Control: Network segmentation is essential for managing access and cybersecurity risk. Firewall and application control functionality enable network segmentation and blocking of traffic based on security policy and application-specific rules.
- Sandbox Inspection: Endpoints can be infected with malware via various means such as phishing, vulnerability exploitation and more. Endpoint security solutions should extract and inspect files in a sandboxed environment to identify and block malicious content from reaching an endpoint.
- Secure Remote Access: Secure remote access is essential for employees working under a remote or hybrid model. Endpoint security solutions should incorporate a Virtual Private Network (VPN) client or other secure remote access solution.
- URL Filtering: Malicious links are a commonly-used technique in phishing attacks, and inappropriate web usage on corporate devices impedes productivity and puts the company at risk. URL filtering helps prevent these threats by blocking malicious and inappropriate websites.