Network Security Protocols

Background

- The rapid growth of the Internet:
  - Both individual and business communication channels
  - Growing demand for security and privacy
- Security and Privacy:
  - Essential if individual communication is to continue and
  - E-commerce is to thrive in cyberspace
  - Led to several security protocols and standards

Background

- Some of the security and privacy protocols and standards:
  - Secure Socket Layer (SSL) and Transport Layer Security (TLS)
  - Secure IP (IPSec);
  - Secure HTTP (S-HTTP),
  - Secure E-mail (PGP and S/MIME),
  - DNSSEC,
  - SSH, and others.
- We discuss these protocols and standards within the framework of the network protocol stack.

The Network Protocol Stack

- Application Layer:
  - PGP
  - S/MIME
  - S-HTTP
  - HTTPS
  - SET
  - KERBEROS
- Transport Layer: {A review !!}
  - SSL
  - TLS

The Network Protocol Stack

- Network Layer:
  - IPSec
  - VPN
- Data Link Layer:
  - PPP
  - RADIUS
  - TACACS+

PGP: Pretty Good Privacy

- The importance of sensitive communication cannot be underestimated.
- The best way, so far, to protect such information is to encrypt it.
- Encryption of e-mails and any other forms of communication is vital for the security, confidentiality, and privacy of everyone.
- This is where PGP comes in and this is why PGP is so popular today.

PGP: Pretty Good Privacy

- Pretty Good Privacy (PGP), developed by Phil Zimmermann, is a public-key cryptosystem.
- PGP works by creating a *circle of trust* among its users.
- In the circle of trust, users, starting with two, form a key ring of public key/name pairs kept by each user.
- Joining this “trust club” means trusting and using the keys on somebody’s key ring.

PGP: Pretty Good Privacy

- PGP can be used to sign messages,
- The presence of its digital signature is used to verify the authenticity of a document or file.
- This goes a long way in ensuring that an e-mail message or file just downloaded from the Internet is both secure and un-tampered with.
- However, the major weakness is that unlike the standard PKI infrastructure, the PGP circle of trust has a built-in weakness that can be penetrated by an intruder.

Secure/Multipurpose Internet Mail Extension (S/MIME)

- Extends the Multipurpose Internet Mail Extensions (MIME) protocol
  - By adding digital signatures and encryption to them.

Multipurpose Internet Mail Extension (MIME)

- A technical specification of communication protocols
- Describes the transfer of multimedia data including pictures, audio, and video.
- Messages are described in RFC 1521;
- Consult RFC 1521

Multipurpose Internet Mail Extension (MIME)

- Web contents typically consist of hyperlinks that are themselves linked onto other hyperlinks
- Any e-mail must describe this kind of inter-linkage.
- That is what a MIME server does
  - When the Web server sends the requested file to the client's browser, it adds a MIME header to the document and transmits it.
  - This means, Internet e-mail messages consist of two parts:
    - The header and the body.

Multipurpose Internet Mail Extension (MIME)

- Within the header:
  - MIME *type* and *subtype*.
- MIME type:
  - Describes the general file type of the transmitted content type such as image, text, audio, application, and others.
- The subtype:
  - Carries the specific file type such as *jpeg* or gif, tiff, and so on.
- S/MIME was then developed to add security services.
- It adds two cryptographic elements:
  - Encryption and digital signatures

Secure/Multipurpose Internet Mail Extension (S/MIME)

- Encryption
  - S/MIME supports three public key algorithms to encrypt sessions keys for transmission with the message: Diffie-Hallman, RSA, and triple DES.
- Digital signatures
  - From a hash function of either 160-bit SHA-1 or MD5 to create message digests.

Secure HTTP

- Extends the Hypertext Transfer Protocol (HTTP).
- HTTP :
  - Was developed for a simple web that:
  - Did not have dynamic graphics,
  - Did not require hard encryption for end-to-end transactions
- As the Web became popular for businesses:
  - Users realized that current HTTP protocols needed more cryptographic and graphic improvements if it were to remain the e-commerce backbone it had become

Secure HTTP

- Each S-HTTP file is either encrypted, contains a digital certificate, or both
- S-HTTP design provides for secure communications, primarily commercial transactions, between a HTTP client and a server
- It does this through a wide variety of mechanisms to provide for confidentiality, authentication, and integrity while separating policy from mechanism.

Secure HTTP

- HTTP messages contain two parts:
  - Header and body
- The header contains instructions to the recipients (browser and server) on how to process the message's body
- During the transfer transaction:
  - Both the client browser and the server, use the information contained in the HTTP header to negotiate formats they will use to transfer the requested information.

Secure HTTP

- The S-HTTP protocol extends this negotiation between the client browser and the server:
  - To include the negotiation for security matters.
  - Hence S-HTTP uses additional headers for message encryption, digital certificates and authentication in the HTTP format
  - The HTTP format also contains additional instructions on how to decrypt the message body

HTTP over SSL (HTTPS)

- Is the use of Secure Sockets Layer (SSL) as a sub-layer under the regular HTTP in the application layer.
- It is also referred to as Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).
- Was developed by Netscape
- Uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP

Secure Electronics Transaction (SET)

- A cryptographic protocol developed by a group of companies that included Visa, Microsoft, IBM, RSA, Netscape, MasterCard and others.
- A highly specialized system with complex specifications contained in three books.
  - Book one: Deals with the business description,
  - Book two: a programmer's guide,
  - Book three: Gives the formal protocol description.

Secure Electronics Transaction (SET)

- For each transaction, SET provides the following services:
  - Authentication, Confidentiality, Message integrity, and linkage
- Uses public key encryption and signed certificates to establish the identity of every one involved in the transaction and to allow every correspondence between them to be private

Kerberos

- A network authentication protocol designed to allow users, clients and servers, authenticate themselves to each other.
- This mutual authentication is done using secret-key cryptography with parties proving to each other their identity across an insecure network connection.
- Communication between the client and the server can be secure after the client and server have used Kerberos to prove their identity.
- From this point on, subsequent communication between the two can be encrypted to assure privacy and data integrity.

Kerberos

- Kerberos client/server authentication requirements are:
  - Security – that Kerberos is strong enough to stop potential eavesdroppers from finding it to be a weak link.
  - Reliability – that Kerberos is highly reliable employing a distributed server architecture where one server is able to back up another. This means that Kerberos systems is fail safe, meaning graceful degradation, if it happens.
  - Transparency – that users are not aware that authentication is taking place beyond providing passwords.
  - Scalability - that Kerberos systems accept and support new clients and servers.

Kerberos

- To meet these requirements, Kerberos designers proposed a third-party trusted authentication service to arbitrate between the client and server in their mutual authentication .

Security in the Transport Layer

- These protocols are at the level below the application layer.
- We discuss two:
  - Secure Socket Layer (SSL) and Transport Layer Security (TLS).
- Currently, SSL and TLS are no longer considered as two separate protocols but one under the name SSL/TLS, after the SSL standardization was passed over to IETF, by the Netscape consortium, and Internet Engineering Task Force (IETF) renamed it TLS.
- We have discussed these two under the “certificate based authentication mechanisms”

S-HTTP vs HTTPS

- Layer of operation:
  - S-HTTP was designed to work with only web protocols.
  - Because SSL is at a lower level in the network stack than S-HTTP, it can work in many other network protocols.
- Implementation:
  - Since SSL is at a lower level than S-HTTP, it is implemented as a replacement for the sockets API to be used by applications requiring secure communications.
  - On the other hand, S-HTTP has its data passed in named text fields in the HTTP header.

S-HTTP vs HTTPS

- Distribution and acceptance:
  - History has not been so good to S-HTTP.
  - While SSL was released in a free mass circulating browser, the Netscape Navigator, S-HTTP was released in a much smaller and restricted NCSA Mosaic.
  - This unfortunate choice doomed the fortunes of S-HTTP (See SSL protocol stack).

Security in the Network Layer

- These protocols also address Internet communication security.
- These protocols include:
  - Internet Protocol Security (IPSec) and
  - Virtual Private Network (VPN) technologies.

Internet Protocol Security (IPSec)

- A suite of authentication and encryption protocols developed by the Internet Engineering Task Force (IETF).
- Designed to address the inherent lack of security for IP-based networks.
- Has a very complex set of protocols described in a number of RFCs including RFC 2401 and 2411
- Although it was designed to run in IP Version 6 (IPv6), it has also successfully run in the older IPv4 as well

IPv4 vs IPv6 packet structures

- IPv4:
  - Version, ToS, Next Hdr, SA, DA
  - Datagram: [IP hdr][Transport {TCP;UDP}/ICMP][Payload]
- IPv6:
  - Version, Flow Label, N. Hdr, SA, DA
  - Datagram6: [IPv6 Hdr][Ext. Hdr] [Transport {TCP;UDP}/ICMP][Payload]
  - Exts: HBH, Routing Ext

Internet Protocol Security (IPSec)

- Offers protection by providing the following services at the network layer:
  - Access Control – to prevent an unauthorized access to the resource.
  - Connectionless Integrity – to give an assurance that the traffic received has not been modified in any way.
  - Confidentiality – to ensure that Internet traffic is not examined by non-authorized parties. This requires all IP datagrams to have their data field, TCP, UDP, ICMP or any other datagram data field segment, encrypted.

Internet Protocol Security (IPSec)

- Offers protection by providing the following services at the network layer:
  - Authentication – particularly source authentication so that when a destination host receives an IP datagram, with a particular IP source address, it is possible to be sure that the IP datagram was indeed generated by the host with the source IP address. This prevents spoofed IP addresses.
  - Replay protection – to guarantee that each packet exchanged between two parties is different.

Internet Protocol Security (IPSec)

- IPSec protocol achieves these objectives by dividing the protocol suite into two main protocols:
  - Authentication Header (AH) protocol and
  - Encapsulation Security Payload (ESP) protocol.

Internet Protocol Security (IPSec)

- The AH protocol:
  - Provides source authentication and data integrity but no confidentiality.
- The ESP protocol:
  - Provides authentication, data integrity, and confidentiality.
- Any datagram from a source must be secured with either AH or ESP

Internet Protocol Security (IPSec)

- IPSec Operates in two modes:
  - Transport mode and
  - Tunnel mode.

Internet Protocol Security (IPSec)

- Transport mode
  - Provides host-to-host protection to higher layer protocols in the communication between two hosts in both IPv4 and IPv6.
  - In IPv4, this area is the area beyond the IP address.
  - In IPv6, the protection includes the upper protocols, the IP address and any IPv6 header extensions

Internet Protocol Security (IPSec)

- Tunnel mode
  - Offers protection to the entire IP datagram both in AH and ESP between two IPSec gateways.
  - This is possible because of the added new IP header in both IPv4 and IPv6.
  - Between the two gateways, the datagram is secure and the original IP address is also secure.
  - However, beyond the gateways, the datagram may not be secure.

Internet Protocol Security (IPSec)

- Tunnel mode
  - Protection is created when the first IPSec gateway encapsulate the datagram including its IP address into a new shield datagram with a new IP address of the receiving IPSec gateway.
  - At the receiving gateway, the new datagram is unwrapped and brought back to the original datagram

Virtual Private Networks

- Is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, by adding security procedures over the unsecure communication channels.
- The security procedures that involve encryption are achieved through the use of a tunneling protocol.

Virtual Private Networks

- There are two types of VPNs:
  - Remote access VPNs: Let single users connect to the protected company network
  - Site-to-site VPNs: Support connections between two protected company networks.
- In either mode, VPN technology gives a company the facilities of expensive private leased lines at much lower cost by using the shared public infrastructure like the Internet.

Virtual Private Networks

- The two components of a VPN:
  - Two terminators which are either software or hardware.
    - These perform encryption, decryption and authentication services. They also encapsulate the information.
  - A tunnel – connecting the end-points.
    - The tunnel is a secure communication link between the end-points and networks such as the Internet.
    - In fact this tunnel is virtually created by the end-points

Virtual Private Networks

- VPN Activities:
  - IP encapsulation – this involves enclosing TCP/IP data packets within another packet with an IP-address of either a firewall or a server that acts as a VPN end-point. This encapsulation of host IP-address helps in hiding the host.
  - Encryption – is done on the data part of the packet. Just like in SSL, the encryption can be done either in transport mode which encrypts its data at the time of generation, or tunnel mode which encrypts and decrypts data during transmission encrypting both data and header.

Virtual Private Networks

- VPN Activities:
  - Authentication – involves creating an encryption domain which includes authenticating computers and data packets by use for public encryption.

Virtual Private Networks

- Types of VPNs (by security):
  - Trusted VPNs
  - Secure VPNs
  - Hybrid VPNs
- Trusted VPNs
  - In these VPNs a customer trusts the VPN provider to safeguard his or her privacy and security by maintaining the integrity of the circuits.
  - This security is based on trust.

Virtual Private Networks

- Secure VPNs
  - Trusted VPN actually offers only virtual security, so security concerns in VPN are still there.
  - To address these concerns, protocols that encrypt traffic at the edge of one network or at the originating computer, moved over the Internet like any other data, and then decrypt when it reaches the corporate network or a receiving computer are used.

Virtual Private Networks

- Secure VPNs
  - This way it looks like encrypted traffic has traveled through a tunnel between the two networks.
  - Between the source and the destination points, although the data is in the clear and even an attacker can see the traffic, still one cannot read it, and one cannot change the traffic without the changes being seen by the receiving party and, therefore, rejected.

Virtual Private Networks

- Secure VPNs
  - Networks that are constructed using encryption are called *secure VPNs*.
  - Secure VPNs are more secure than trusted VPNs.

Virtual Private Networks

- Hybrid VPNs
  - Hybrid VPN is the newest type of VPN technologies that substitutes the Internet for the telephone system as the underlying structure for communications.
  - The trusted VPN components of the new VPN still do not offer security but they give customers a way to easily create network segments for wide area networks (WANs). On the other hand, the secure VPN components can be controlled from a single place and often come with guaranteed quality-of-service (QoS) from the provider

Security in the Data Link Layer over LANs

- In the Data Link Layer, there are several protocols including : PPP, RADIUS and TACAS+.
  - Student to review these.