Nirbhay Sharma (B19CSE114)

CyberSecurity Lab - Protocols

---

1. **IPSec**

- **working:-** IpSec is a protocol which is used to setup encrypted and secure connection between devices, IP stands for Internet protocol and Sec stands for security so IPSec stands for Internet protocol security and it helps to keep data secure over public channels. So basically it uses key exchange techniques for encryption purposes apart from that it uses authentication, encryption etc to make the network secure.
- **application:-** it is used to setup VPN connection and it works by encrypting IP packets along with authentication. it can also encrypt encryption layer data. Ipsec protocol works in network layer.
- **strength and weaknesses:-** the strength of ipsec is that it can provide network layer security, confidentiality, it has zero dependency on application. but apart from that it has some weaknesses as well which includes, compatibility issues, cpu overhead (since it encrypt and decrypt so it demands CPU and hence it has some overhead on CPU)

2. **VPNs**

- **working:-** VPN refers to (Virtual Private Network) It is an encryption connection between two or more computers, the VPN connection is done over public channel but the data exchange is still private and secure due to encryption that it uses. so we can say that it gives online privacy and anonimity by creating a private network from a public internet connection,
- **application:-** vpn has found various application in accessing region-restricted websites and also it provides security so it has application in ethical hacking as well, while using public wifi VPN is recommended. the vpn also works in network layer.
- **strength and weaknesses:-** vpn has various strengths such as it provides safety, secure remote connection, cost effective, can bypass firewalls. Apart from that it has various weaknesses such as vpn may decrease the internet speed, it is not legal in all countries since it can also take us to restricted websites, compatibility issues.

3. **SSL**

- **working:-** SSL stands for Secure Socket Layer, it is an encryption based internet security protocol, it is basically for securing communication that take place on internet, so it is for securing communication between client and server. the basic working is SSL encrypt data and transmit it and so SSL initiates an authentication process called handshake between server and client, ssl also provides data integrity by verifying the data change.
- **application:-** SSL is used in secure credit card transactions, data transfer between client and server and also in login systems. SSL sits between application layer and transport layer
- **strength and weaknesses:-** the strength of ssl are authentication, security, relaibility, data integrity the weakness includes performance, cost issues etc.

4. **TLS**

- **working:-** TLS stands for Transport layer security, TLS also uses encryption techniques to secure the communication between client and server and also TLS can protect web applications from data breaches and other attacks. The working of TLS is as follows so TLS ensures three components i.e.

encryption, authentication, integrity, TLS also uses TLS handshake to establish secure connection between client and server.

- **application:-** TLS finds application in web browser and websites etc, and it operates between application and transport layer.
- **strength and weaknesses:-** the advantages of TLS are integrity, trust, security and also it can prevent malware prevention but it has some weakness as well as it is vulnerable to MiM attack and it has high implementation cost, it fails as network complexity increases.

it looks like that TLS and SSL are more or less same so here are some of the points of difference

- ssl uses message digest to create master secret while tls uses pseudo-random function to create master secret
- ssl uses MAC (message authentication code) while tsl used Hashed Message authentication code protocol
- ssl is more complex to implement while tls is simple
- ssl is less secured while tls is more secured as it uses secure cryptographic hash functions.

5. **PGP**

- **working:-** PGP stands for pretty good privacy and it was designed to provide privacy, integrity, authentication, non repudiation in the sending of email, so basically PGP uses a digital signature (hashing and public key encryption) to provide integrity, authenticity, non-repudiation and PGP uses public and secret key for encryption and hence provides privacy. Exact working is as follows that the e-mail is hashed using a hash function and then it is encrypted and this all being encrypted with one time secret key and the message is send together. It uses Diffie hellman digital singature.
- **application:-** the working area of PGP is application layer.
- **strength and weaknesses:-** strengths of PGP are - it allows us to securely share information over mails and also it provides all the security features like privacy, integrity, authentication, non-repudiation, but it has some disadvantages as well like it may face compatibility issues, it is more complex architecture.

6. **HTTPS/SHTTP**

- **working:-** HTTPS stands for Hyper Text Transfer protocol Secure, it is basically a secure version of HTTP protocol and HTTP is used to send data between a web-browser and website, so Basically apart from HTTP functionality, HTTPS also encrypts the messages that are transferred and hence making it more secure than HTTP. so in short HTTPS uses encryption protocol to encrypt communcations and the encrypted protocol is TLS / SSL which are used for same purposes.
- **application:-** simple real life application can be to use HTTPS in websites where login and signup functionality is required. HTTPS protocol work at application layer of TCP/IP protocol stack
- **strength and weaknesses:-** strength includes protection, verification, encryption, relaibility and weakness includes performance, cost, accessiblity, encryption decryption overhead is there in the communication etc.

7. **SET**

- **working:-** SET stands for Secure Electronic Transaction, this is basically responsible for the security and integrity of e-commerce websites / some electronic transactions by some credit card and so on. It basically uses different encryption and hashing techniques to secure electronic transactions over internet, the encryption protocol it uses is SSL.

- **application:-**
- **strength and weaknesses:-** strength includes authentication, confidentiality, integrity those are the obvious strengths since the protocol uses encryption and hash functions for securing the network. weaknesses includes computation overhead for encryption and hashing, not cost-effective, complexity.

8. **PEM**

- **working:-** PEM stands for Privacy enchanced Mail and it is an email security standard just to provide secure electronic mail communication. PEM provides the following services such as confidentiality, integrity and it uses various encryptioin algorithms like DES and hash function like MD5 etc to encrypt the data and also to generate digest. It has basically 4 main steps, canonical conversion (conversion of message into standard format i.e Generate message digest), Digital signature (generated by encrypting the message), encryption (encryption of message digest + digital signature together), Encoding (binary output transformed to character output)
- **application:-** This is a mail secure protocol and finds its applications in securing electronic mail transfers. It may operate on application layer.
- **strength and weaknesses:-** its strength includes privacy, integrity etc, its weakness includes cost of computation of RSA/ DES etc i.e. computation overhead, complex system.

9. **Kerberos**

- **working:-** Kerberos provides centralized authentication server whose function is to provide an authentication mechanism between server and client and vice versa. Kerberos runs as a third-party trusted server knows as key Distribution Center (KDC). Its main components includes, Authentication server, Database, Ticket Granting server (TGS). In kerberos authentication of client side is done using authentication server and database.
- **application:-** Kerberos operates at session layer.
- **strength and weaknesses:-** its strength includes Faster and mutual authentication, encryption, compatible for various OS, weakness includes vulnerable to weak or repeated passwords, only provides authentication for server and client. it also requires an always-on kerberos server to do the task.

10. **S/MIME**

- **working:-** It stands for Secure/ Multipurpose Internet Mail Extensions, it is used for secure exchange of email and attached documents with it. and it used RSA security intitially. S/MIME adds security to the email based on Simple mail transfer protocol (SMTP) and also provides support fro encryption to SMTP and also support authentication its working is simple it uses RSA public key cryptography scheme along with Data encryption scheme (DES) for encryption purposes. It uses Elgamal digital signature.
- **application:-** it operates on 6th layer of OSI model
- **strength and weaknesses:-** its strength includes authentication, non-repudiation, and data integrity, it is good for industiral use and it is efficient as well, weakness includes costly/expensive , computation overhead, only used in mail-services.

protocol	Vulnerability in the protocol
IPSec	it may allow authenticated remote attacker to affect the system, the vulnerability lies in improper parsing of malformed IPsec packets

protocol	Vulnerability in the protocol
VPNs	vpn's are vulnerable as they are exposed to public internet and might work as entry point for any attacker
SSL	heartbleed bug is a vulnerabiliy in open ssl, this vulnerability allows the attacker to steal private keys attached to ssl certificates
TLS	it can be vulnerable to attack like poodle due to outdated cyrptographic method used which is CBC (Cipher Block Chaining)
PGP	vulnerability is that modern e-mail programs allow for embedded html objects so an attacker can interrupt and modify a message intransit
HTTPS/SHTTP	attacker can use DDos attack to create a denial of service from server side since http is a client server protocol
SET	vulnerability lies in the fact that it indirectly uses SSL and hence the vulnerabilities of SSL are applicable here
PEM	Since it has 4 steps where encryption occures, the attacker can find vulnerabilities with respect to those algorithms and exploit this condition to break the system
Kerberos	vulnerability lies in the fact that any unauthenticated remote attacker can impersonate the kerberos key distribution center (KDC) and bypass authentication
S/MIME	attacker can modify the message intransit and sends updated message