4th Cycle: D Day
(MSS)
02/01/19

Web Security :

Web Technology → server client দুইটি program এর মধ্যে communication.

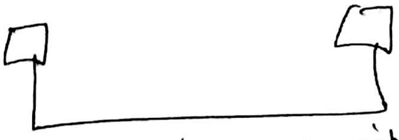
Security: 4 types

- * Computer security
- * Network security
- * Cyber security
- * System security

Computer Network:

more than two computer communicate with each other for sharing resource

system s/w er security provide করে থাকে Computer security বলে ।



communication channel এর security

Network security

অন্যজন access করছে কিনা কেউ দেখে না .

Cyber: Virtual world এ কোনো fault হলে যেমন: modification etc .

System: Particular organization এর উপর Depend করে।

Web security: ৩ ভাবে security provide হয়

~~Server client issue~~

- * server side security
- * client " "
- * channel " "

security attack এই 3 point এ হতে পারে।

** why Web security challenging ?

- two way communication
- reputation immediately hamper হতে পারে।
- Underlying (request) is very complex
  (web technology) →
- Casual user, web user দের train করার দরকার হয় না।

Web technology is actually challenging

কেননা total user & provider is untrend.

4th cycle: E Day
(MSS)

Malicios Softwar

Logic Bomb! Malware → particularly Malware ~~or~~ Malicious code হতে পারে। particular logic condition full fill হলে attack করে।

Frozen Horse! Hidely অবস্থান করে, Harmful কিছু থাকে কিন্তু আমরা বুঝতে পারি না.
↳ malicious code

Virus → একটা Malicious code.

□ S/W → User level থেকে হয়, complexity completely Hide থাকে

□ program → particular কাজ হয়, কিন্তু User level এ থাকে নাই।

S/W → একাধিক issue নিয়ে কাজ করে।

□ **Mobile Agent:-** Normal program, নিজেই move করতে পারে, ইচ্ছামত ~~network~~ particular network এ explore করে। Network Administrator এটা use করে [Positive কাজে use হয়]

→ user information automatically transfer করতে পারে।

Web security Thread/Attack

Active attack

passive attack
[traffic analysis এর মাধ্যমে information collect করে]

~~Confidentiality~~

Web security তে CIA কে Maintain ~~করব~~ হয়।

Component	Threat	Consequences	Countermeasure
Confidentiality	→ Eavs dropping → Theft	loss of information	Encryption
Integrity (source থেকে ~~po~~ accuracy দেখে)	→ Modification	loss of content property	Hash/ MAC
~~Availa~~ Authentication (sender এর accuracy দেখে.)	→		Certificated organization MAC/HMAC Use ~~[illegible]~~ করা যায়
Availability	→ Overload	Interruption হয়	technical background support এর উপর নির্ভর করে

Active n ≤ n.
↳ Interruption হয়।

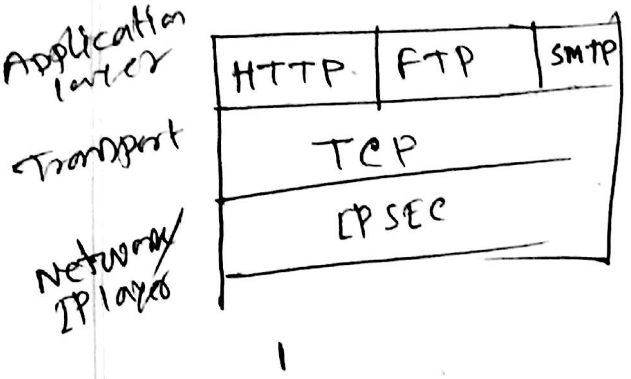
এরা Transport Layer এ কাজ করে. security

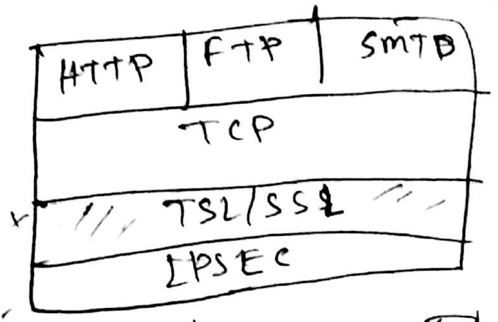
এই 2টা protocol

* SSL → secure socket ~~[illegible]~~ Layer

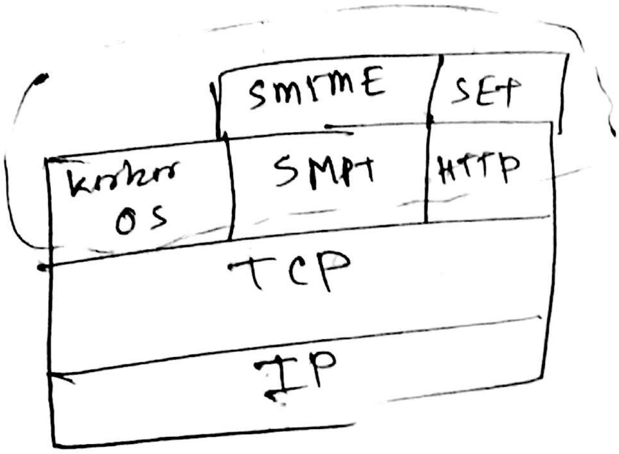
* TSL → Transport Layer security

security issue! Threat from the Internal, তখন IPSEC দিয়ে করতে পারবো না.





এটা নয় সম্ভব আমি Security provide করে সম্ভব



Application layer Security provide করতে পারি।

Uconditional: কখনো break করা যায় না

computation: break করা সম্ভব।

০ ↓ আমরা এটা বেশী use করি।

6th cycle : D Day
25/02/19
(MSS)

(Must Listen AR)

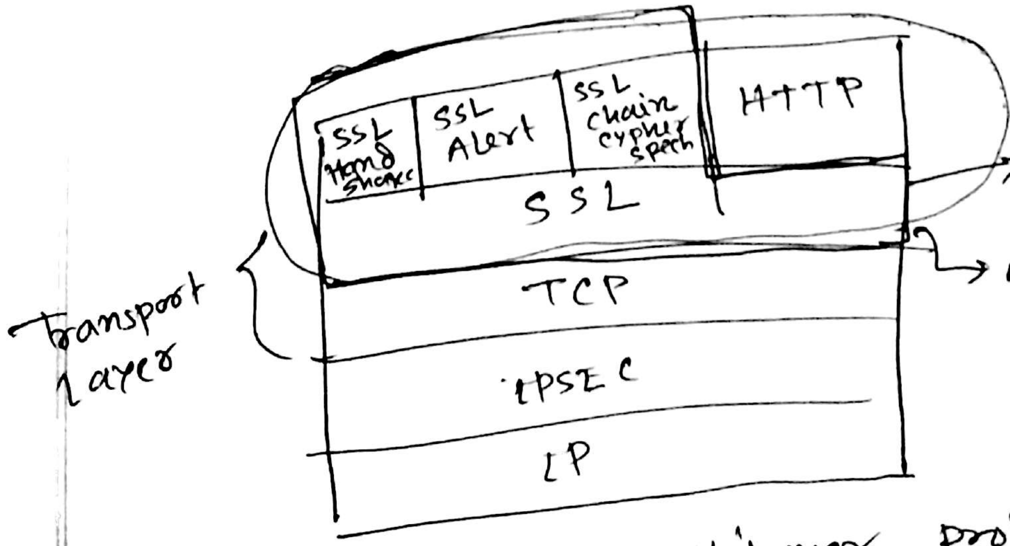
SSL/TSL

Assignment: History of Browser (Only One Page)
The History of Network Browser

SSL → একাধিক Protocol এর সমন্বয়ে অর্থাৎ একে 2 layer protocol বলে (Multilayer protocol) এর কিছু অংশ Upper Layer এ কাজ করে। অর্থাৎ Application এও কাজ করে।

IPSEC → Network Layer
HTTP → Application layer
IP → Network Layer
~~ISL~~
TCP/UDP → Network Layer

তাই SSL কে upper layer protocol বলে



~~এই~~ এই গুলো নিয়ে কাজ করে

→ Record protocol

এই জন্য SSL কে Multilayer protocol বলে, Mainly transport Layer এ কাজ করে.

Handshake → session establish এ হয়,

এ কারণে যদি হয় Two layer এ করতে হয়

why not single layer?

Logic: transport layer এর vital issue

- * connection establish
- * connection release

এখন ঠিক করতে Handshaking এর প্রয়োজন হয় যা session layer এ কাজ করে।

এখন session কেও secure করতে হবে।

Q. * one layer is enough for TCP? Do you agree? justify.

SSL Record এর ২ টি concept

- * ~~what does~~ connection
- * session

Connection: একটা আদানপ্রদানের সময় ১টি connection establish হয়। আর প্রত্যেকটা connection এ মধ্যে session থাকে logically অনেকগুলো থাকতে পারে

Session: ঐ communication এ কি ধরনের encryption use হবে?, Hand connectim & Session: collection of parameter

✓ একাধিক connection থাকতে পারে এবং একাধিক session ও থাকতে পারে,

Parammeter of session:

theorattically হতে পারে, প্রত্যেক parameter নিজ ধারণ করে, Handshake protocol এর সময় parammeter define হতে পারে।

- * Session Identifier
- * Peer Certificate
- * Compression Method
- * Cipher Spec
- * Master secret
- * Is Reusable (1 bit এর flag থাকে, session টা আবার use করা যাবে কিনা)

Master secret: দুই পক্ষের মধ্যে secret share, session টি Handshake এর মাধ্যমে করা হয়।

* Cypher spec: encryption related issue, MD5 / ~~ধ~~ SHA use করবে ?

Compression method: কোন compression use করবে ?

Peer C: প্রত্যেকের একটি certificate থাকে, unit/ organization এর certificate থাকবে।

→ প্রত্যেক session অর্থাৎ connection এ MAC আছে but, practically use হয় না কারণ complexity increase হয়

Connetion Parrameter:

* Server client Random : যে কোনো connection establish এর সময় random no generate হয়।

* server MAC secret :
↳ Hash এর মতো,
এমন key যেটা শুধু server decide করে

client MAC secret :
MAC → Message Authentication Integrity

server Write key : encrypt করে ও conventional (secret one key) use করে।

Client Write key :

Initial vector (IV) : DES এ লাগে,

sequence Number : communication এর পরে সময় হওয়া Replay Attack remove করতে লাগে

DES: Data Encryption Algorithm
↳ Random no. নিয়ে encryption হয়, Initial vector লাগে.