Ch 14

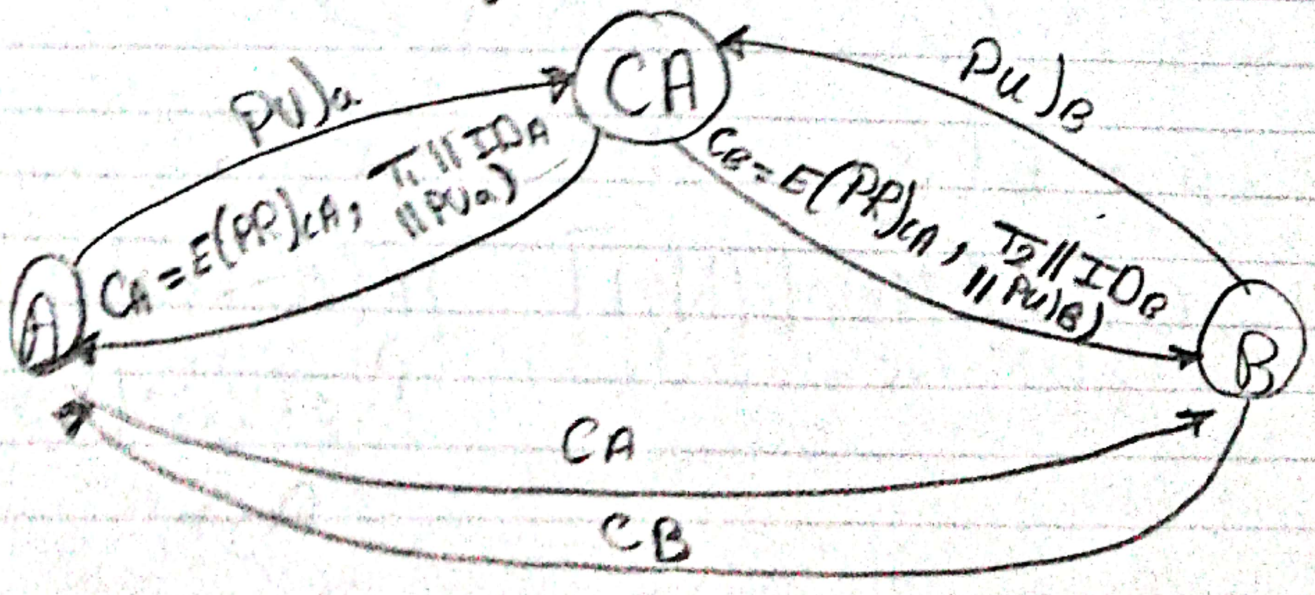
1) What are the Certificate Req? OR PU Key Certs

* Any Participant Can read it to determine the name and the PU Key of the it's owner
* Any Participant Can verify that it's originated From a Certificate Authority, not a Counterfeit
* Any Participant Can verify the Currency (T) & the Certs
* Only the Certf. Authority Can Create/update Certs

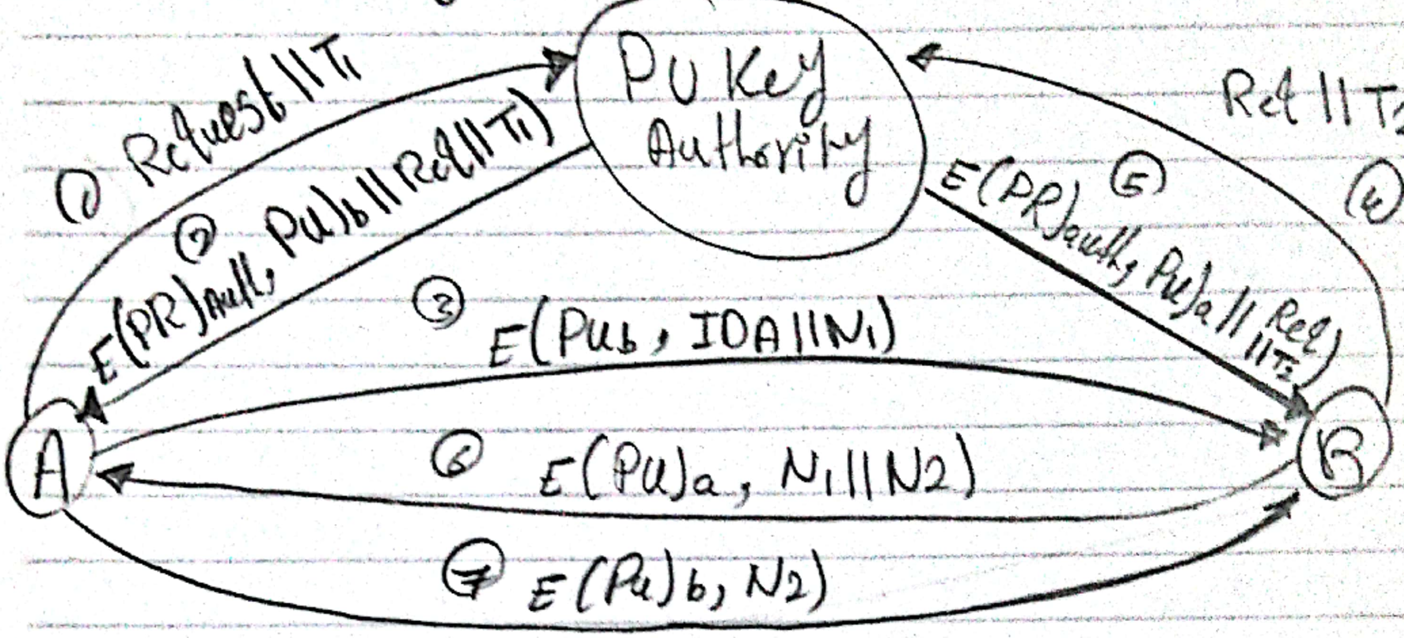
2) What's the Content & Certificate?

* Time Stamp (T) + Public Key (PU) + IDentity (ID)
* it binds an IDentity to PU key, all Signed by the $PR)_{CA}$ key.

3) PU Key Cert. diagram?



4] Draw PU Key authority diagram!



5] Share session Key without PU Key?

* Draw Needham Schroeder Protocol   بتاع ch15

6] "Needham suffers from Man in the Middle Attack" EXPLAIN!

* الـNeedham العادي معموش المشكلة ديه ، لكن ده فيـ

$A \rightarrow B : E(K_b, K_s || ID_A)$
$B \rightarrow A : E(K_s, N)$
$A \rightarrow B : E(K_s, f(N))$

* دخل D في النص بقى وسيط
* آخر ٣ خطوات من Needham

7] Share session Key using PU Key with Conf + Auth

1) $A \rightarrow B : E(PU_b, N_1 || ID_A)$
2) $B \rightarrow A : E(PU_a, N_1 || N_2)$
3) $A \rightarrow B : E(PU_b, N_2)$
4) $B \rightarrow A : E(PU_b, E(PR_A, K_S))$

without:

1) $A \rightarrow B : PU_a || ID_A$
2) $B \rightarrow A : E(PU_a, K_S)$

Ch 15

1) Describe Needham-Schroeder Protocol for distribution of a shared key bet. 2-Parties?

* it's a 3rd Party key distribution Protocol, to securly distribute a new session key bet. A & B.
* Vulnerable to a [replay] attack if an old session key has been compromised [تعرض اكسج بتاعت خطوة ٣]
* Modification to adress this → Add timestamp in step 2 & 3
  → use extra nounce
* Protocol:

1) $A \rightarrow KDC : ID_A \| ID_B \| N_1$
2) $KDC \rightarrow A : E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
3) $A \rightarrow B : E(K_b, K_s \| ID_A)$
4) $B \rightarrow A : E(K_s, N_2)$
5) $A \rightarrow B : E(K_s, F(N_2))$

لو B كان offline وقت دخول دول ↓

$E(K_b, K_s \| ID_A) \| E(K_s, M)$

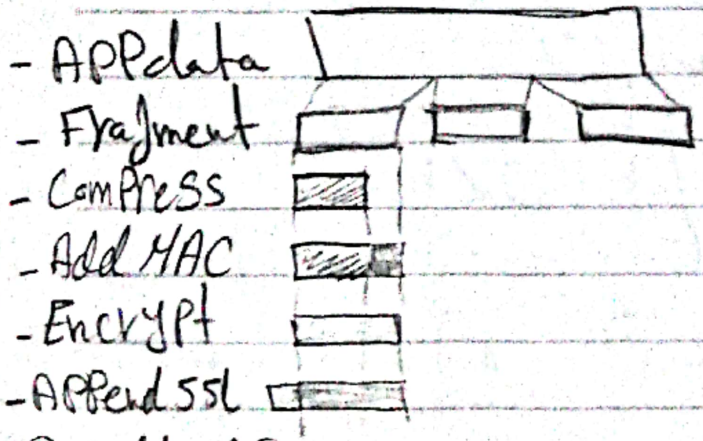
$A \rightarrow B$

Ch 16 Exam Questions

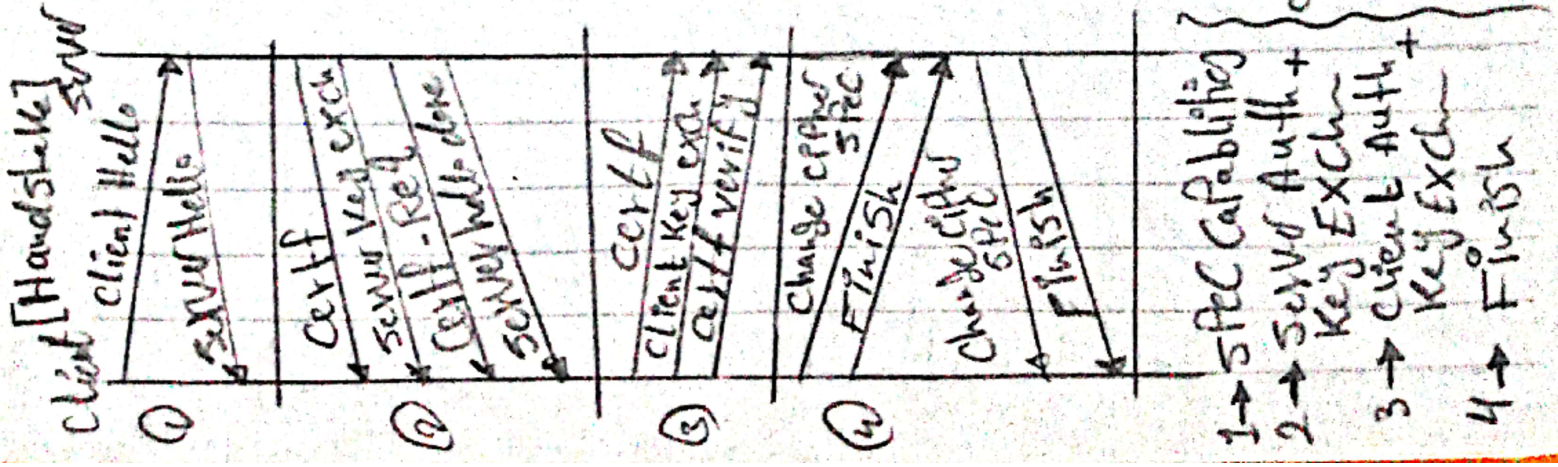
1) Draw SSL Protocol stack [Archi~]

SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol	HTTP
SSL Record Protocol			
TCP			
IP			

2) SSL Record Protocol operation and its security services



* Confidentiality: Symm Enc with a shared secret.
  - Msg Compressed before Enc
* Msg Integrity:
  - Use a MAC with shared secret key
  - Similar to HMAC but with diff Padding



SSL Arch

3) Diff. between SSL Connection & SSL Session?

* SSL Connection → Transient, P2P, Comm Link
  → Associated with [1] SSL session

* SSL session → Association bet. server & client
  → Created by the Handshake Protocol
  → Defines a set of cryptographic Params
  → May be shared by multiple SSL Connections

4] SSL Alert Protocol?

* Conveys SSL-related alerts to Peer entity
* Compressed & encrypted like all SSL data.
* Has severity level [warning & Fatal]
* Has specific Alerts → Fatal → unexpected MSG, bad record MAC, handshake failure
  → Warning → [no Bad expired revoked unknown] certificate

5] Complete: HTTPS Consist of HTTP and SSL or TLS

6] Fields in SSL record Protocol Header? [from the Ref]

* Content type
* Major version
* Minor version
* Compressed length

(From the Ref)

7] SSL features that prevents the following attacks:

* Brute force cryptoanalytic attacks → the conventional algo uses key length ranging from 40 ~ 168 bits
* Reply attack → By the use of Nonces
* Man in the middle attack → use of the PU key certificate
* Password sniffing → user data is encrypted
* IP Spoofing → the spoofers must be in possession of the [secret key] and the [forged IP address]
* IP Hijacking → by encryption
* Known Plaintext [Dictionary] → using a 128 bit key, the rest of the key is constructed from the data in the Hello msg
* SYN flooding → SSL Provides no Protection against this attack

8] Provide func of:

* SSL Alert → Conveys SSL-related alerts to Peer entity
* SSL Handshake → Allows server & client to Auth each other, negotiate encry and MAC Algos, and used cryptographic keys
* SSL Cipher change → Cause the Pending State to be Copied into the Current State, which updates the cipher suite to be used on this Connection

Ch 20 Exam Questions

① Show the types of Intruders and their description: (classes) (From Ref)

* Masquerader → Unauthorized individual that penetrates a system's access control as a legitimate user and exploit his account.
* Misfeasor → A legitimate user who misuses his privilages
* Clandestine user → Indiv. who seizes supervisory control and uses that to → evade auditing & access control
  → Suppress Audit Collection

2) what's an Audit record? Why it is used?

* it's used for Intrusion detection.
* May be → Native Audit Records
  → Already present in use, wanted info not in the desired form
  → Part of all common multi-user OS
  → Detection-specific Audit Records
  → created to collect wanted info
  → adds cost & overhead on the sys.

Ch16, Describe SSL Protocol in one sentence?

* A transport layer security service, uses TCP to provide reliable E2E service, and has 2-layers of protocols.

3) What's a honeyPot? How it's used?

* Decoy SYS to lure attackers → away from accessing critical SYS
  → Collect info of their activity
  → encourage attackers to stay on SYS so Admin can respond
* they are filled with fabricated data
* Are single or multiple networked SYS.

4] Mention 2 techniques for detecting intruders & their description?

5] Diff bet [Rule based ID] and [statistical ID]?

* Statistical Anomly Detection → Collection of data [Audit] of the behavior of Legitimate users Then apply some tests
  → threshold Dete → define thresholds for the freq of occurance of specific events
  → Profile based → A profile of the activity of each user is developed, used to detect changes in a user's behaviour.

* Rule based Detection → Attempts to define a set of Rules to decide that a given behaviour is of an intruder
  → Anomly detection → Rules to detect deviation from prev usage patterns
  → Penetration Identification → An expert SYS tech that searches for suspicious behavior

[From the Ref]

6] What's the Common Technique to Protect Pswd Files?

* Access Control → access to the Pswd file is limited to few accounts

* one-way func e.g. Hash "Irreversible" → the SYS stores only the value of the func based on the user's Pswd.
→ when user presents a Pswd, it's transformed using the func and Cmp with the stored value

7] What's the Salt in Unix Pswd mangment? Why used?

* After the Password is encrypted or Hashed, it's stored in the Password file with a plain text copy of the salt [Noise, Timestamp, ___]

* Why?
→ Prevents duplicated Pswd from being visible in the file, since they will differ in their extension i.e salt [timestamp].
→ Increases the length of the Pswd with no need to memorize the long one. Increases the Possible Pswd with a factor of 4096 [2^{12}]. Hence, Diff Pswd Guessing
→ Prevents the use of HW implem of DES. Hence, Diff brute force attacks.

Note → salt is 12-bit
→ A modification of DES is used for Encryp.

OR List 4 Techniques to avoid PSWD Guessing

Management

(9) Illustrate Pswd Selection strategies!

* USR Education
  - educate USRS about the Importance of good Pswd
  - give guidlines to follow
  - Ignored by many USRS

* Computer generated Pswd
  - strong Pswd, but not memorisable by the USRS
  - have Poor USER acceptance.

* Reactive Pswd Checking
  - reactively run Pswd guessing tools and disable cracked Pswds
  - Resource Intensive
  - Bad Pswd are Vulnearable till found

* Proactive Pswd Checking "most promising Approach"
  - USR is allowed to select his own Pswd However, at the time of selection, the SYS checks it and decide if it's allowed or not
  - Cmp against dic. of bad Pswd

Ch 21 Exam Quest

(1) what's the rule of Compression in the operation of the virus?

* So that, the infected Proj is the same length as the uninfected ones, deceive the Anti-verus Programs

(2) what are typical Phases of the operation of virus/worm?

* Dormant → Propagation → Triggering → execution

3) How Does worm Propagate?

* Search for other sys to infect, by examining host tables.
* Establish a connection with a remote server
* copy itself to the remote and cause the copy to be run

4) what's digital Immune sys?

* the sys Provides a general Purpose emulation and virus detection sys.
* Provid rapid response to capture virus es.
* when a new virus ents sys an org, the Immune sys capture it, analyze it and adds detection from it
* it Passes info about the virus to the sys running the Anti-verus, to detect it before it can run elsewhere

5] How does behavior-blocking SW works?

* It integrates with the OS of a host computer and monitors Prog behavior in real time for malicious actions
* it then blocks potentially malicious actions before they affect the sys.

6] what is DDOS?

* Distributed denial of SVC attack, makes a networked sys unavailable
* it floods with useless traffic using zombies.

7] Phases/Life cycle of worm/virus?

* Dormant → the virus is idle, needs to be activated to have effect
* Trigg → the virus is triggered by a certain event like certain date or no of virus copies
* Propagation → the virus places a copy of itself into other programs. virus often morph to evade detection. each Prog will have a copy of the virus that can propagate!
* Execution → the payload performed, may be harmless like msg on screen. OR, damaging such as destruction of data.

8) Diff bet. worm & virus?

worm → A Program that can replicate itself and send copies from computer to another through Network
[No HOST]

virus → A piece of code, that can infect other Programs by modifying them. [Needs HOST]

9) Types of Malicious sw?

* Trap doors → secret entry point into a Program

* Logic Bombs → Embedded code into some Prog, triggered when specific cond. is met.

* Trojan horses → Attractive Prog with hidden side-effects (like game or update)

* virus ——→ Piece of sw that infects Programs

* Worm ——→ A Program that usually replicate itself on a Network

* Zombie
  ↳ A Prog that takes over another internet-attached computer, and uses it to launch attacks, that are difficult to trace the zombie creator.