12 / 14

504112505 G. Selda UYANIK
March 19, 2012

BLG609E - Special Topics: 4G Wideband Wireless Network Architectures
(Spring 2012)

Homework-6: Security Architecture Part-I

1. What is the reason that each security key shall have a finite lifetime? POINTS 2

2

Security keys' vulnerability ~~decreases~~ increase with time and that is the reason they should have a finite lifetime. Probability of a key being physically lost/stolen or cryptographically stolen (solved) is increasing with ongoing time. (e.g. brute force search for a key whose length is known.)

2. What kind of technique is used for providing replay protection in data communications? Briefly describe how it works. POINTS 3

3

Using timestamp or random number/s is used for providing protection on replay attacks. Replay attack is the act of the attacker who resends or the captured packet's copy or delays the captured packet without any modification. This attack can be crucial on session handshake or any other important handshake like money transaction. The protection with a timestamp or a random number makes the delayed or resent copy invalid due to the fact known by the recipient that: the timestamp/random number that the sender sends has to be changed for each new packet. For delayed packet attack, timestamp is more useful.

3. Are the R4, R6, and R8 trust relationships (i.e., security associations) dynamically established or pre-established (i.e., statically established)? POINTS 1

1

R4 interface between ASNGW↔ASNGW security associations : usually pre-established
R6 interface between ASNGW↔BS security associations : usually pre-established
R8 interface between BS↔BS security associations : usually pre-established

4. Why is mutual authentication between the MS and the BS always necessary? POINTS 2

0

MS's network security related operations are dynamically established and started via R1 interface before MS starts network signaling. Mutual authentication is always necessary among these two entities because this is the starting point of the latter authentication, authorization, accounting etc. process that reaches up to the AAA server. Moreover mobile MS could need to connect to another BS and same mutual authentication has to be achieved with the new BS before getting connected to the network via new BS. Network access authentication process performs message integrity protection for control packets via AES-CMACC. Thereafter the data packets will be encrypted with AES-CCM.

Explains "auth" but not "mutual auth"

5. What NAI shall be presented by an MS whose user (Ali) is subscribed to Operator1.com and roaming to Operator2.com? POINTS 2

2

visited home

Operator1.com!Ali@Operator2.com — ASN - VCSN — HCSN

6. Why are the TEKs not derived (generated) on the MS but instead they are delivered from the BS to the MS? POINTS 2

2

Traffic encryption keys are used for MSs for their data transmissions. These data transmissions do not need to just consist of unicast messages. TEK keys are not designed as generated keys considering multicast or broadcast messages. With these kinds of messages, if the keys were designed as generated, many MSs should be synchronized and has to be managed to generate the

authenticate MS → operator needs to know who MS really is
authenticate BS → MS need to know BS is really his operator's BS.

not dependent on subscriber info

same keys. Distributing such a common key via a trusted entity (BS) to many users (MSs in message destination) is more profitable for performance and is preferred.

7. Give an example of a physical security mechanism used for protecting the networking infrastructure on the university campus. POINTS 2

2

One of the physical security mechanisms for protecting the networking infrastructure on university campus can be given from our department's network and server room. In this room, there is a high capacity switch that distributes the supplied Ethernet connection from university and provides a static IP range for the offices of the members of CE Department. It is being locked in the server room and its key is only available to the members selected for network stability duty and the head of department. Same approach is applied in Computer Networks Research Lab.'s switch that stays in a locked up rack.

ethernet cables going through walls.