504112505 G. Selda UYANIK
March 26, 2012

8

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

Homework-7: Security Architecture Part-II

1. Describe the term "Domino Effect" and why it should be avoided. POINTS 2 (1)

   One of the optimizations performed in authentication and authorization process of a *mobile* station is called "context transfer". In such optimization, if MS moves and changes BSs, more importantly if he changes ASNGW, his security context, that is stored in the first ASNGW he registered, is transferred to the latter ASNGWs as MS moves. MS then does not need to perform re-register or pre-authentication procedures.

   Compromise of one node leads to ....

   Domino Effect comes from the fact that the security context of a MS is shared among increasing number of (i.e. n: number of different ASNGWs he traverses) network entries with such optimization approach. Security context transfer actually means that all the keys (MSK, etc.) are transferred. Domino effect should be avoided due to this point. Because the keys' vulnerability drops as the number of users who share these keys increases. Domino effect can only be discarded under the assumption that the ASNGWs will never be compromised.

   weakens security!

2. See the MIP6 Security slide #49 in March 19th lecture notes. Fill in the blanks: Authenticity of the MIP6 Binding Update is verified by the Home Agent after it receives the AAA Response message from HAAA Server. POINTS 2 (2)

   only at that point Home Agent will have keys to verify

3. Why using end-to-end security among all nodes on the Internet is not practically possible today? POINTS 2 (1)

   crypto keys to be used among them.

   End-to-end security requires ensuring the security of all of the links traversed between source and destination. This security can be in form of both physical and/or network security mechanisms. Besides, on internet, if we want to set up end to end security among all nodes, we need to think about every arbitrary node couples and the related links between them to secure. This produces a huge amount of possible paths (and also number of possible different couples) considering high number of users on internet. Therefore, end to end security is not practically possible on internet among all nodes.

   security association among all possible pairs not practicle!

4. What is the equivalent of a WiMAX device MAC address in the LTE security architecture? What is the most significant difference between the two in the context of authentication? POINTS 2 (2)

   WiMAX device MAC address equivalent in the LTE systems is: IMEI number identifying the hardware. The most significant different between them: in WiMAX, each device has a unique MAC number and a X.509 certificate. Therefore, device can be authenticated with this certificate (supplied by PKI infrastructure) whereas LTE does not support such additional information and IMSI gives only idea about device identity. Since IMSI corruption (reuse issues) is possible, it cannot be trusted solely for device authentication.

   not authenticated!

504112505 G. Selda UYANIK
March 26, 2012

5. What was the main motivation behind LTE designers not to support integrity protection on the data radio bearers? POINTS 2 (2)

For data packets, LTE uses only encryption. That is: the contents of the packets cannot be read by any tapper with traffic traces (without any key losses of communicating parties). However, the designers did not support integrity protection; therefore a tapper can manipulate the captured packet without any knowledge of its contents (e.g. a random scrambling attack). The main motivation of designers is that if an attacker does not know information about the message contents, his attack will not cause a real damage (most probably the packet will become meaningless in terms of specific fields and will be dropped). SO the designers decided not no implement data integrity protection for data packets and avoided related overhead on packet sizes.

midterm yapamadıklarım

→ What is the identity used by MME to determine UE is roaming or not?

IMSI

→ Provide one of the purposes using authenticated MAC address in WiMAX?

block stolen device
block blacklisted device
uniquely identify

⇒ In LTE describe mechanism used to protect user's permanent identity (IMSI)

STIMSI & GUTI (?)

. IMSI being compromised over air or key locked by eNB?

1. MME ---GUTI--- UE
   eNB ---CRNTI--- UE

⇒ 2 types of User Domain security in LTE. Describe one of them.

– using PIN code for lock in SIM CARD
– SIMLOCK : certain SIM CARD

midterm 46/50