Wireless Cellular Network Security: Part 5

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi, "*LTE Security*", John Wiley and sons, 2nd edition, 2013.

EPS Security Architecture

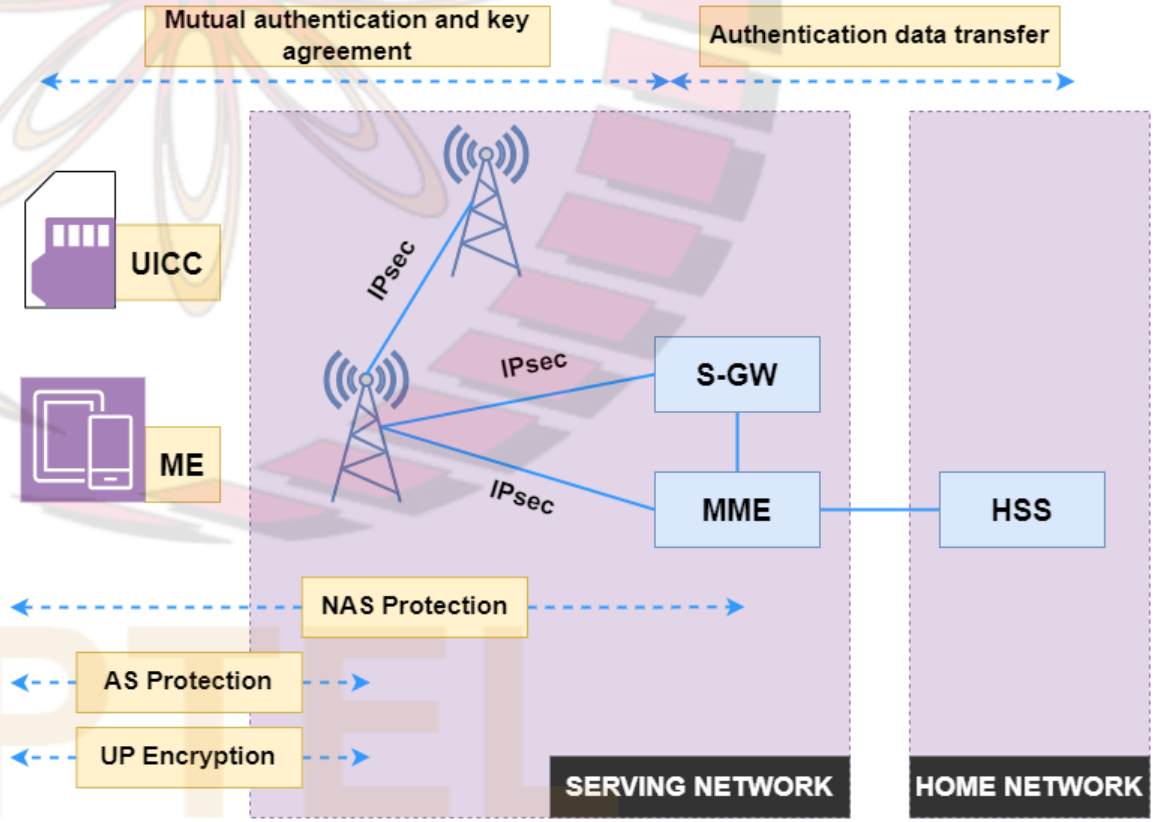
Overview

- Recall: EPS brings two new major ingredients, which were not there in 2G and 3G networks:
  - the radio network Evolved Universal Terrestrial Radio Access Network (E-UTRAN) with a new radio interface, and
  - the Internet Protocol (IP)-based core network Evolved Packet Core (EPC)
- GSM and 3G security mechanisms offer a good basis for the EPS security architecture
- But due to the significant difference in architecture of EPS relative to GSM and 3G systems:
  - each GSM or 3G mechanism, if reused, needs to be adapted from original context and embedded to the EPS architecture
- EPS must also be able to interwork with legacy systems; so these adaptations have to be done in a backward-compatible manner
- In addition to adaptations from security functionalities already existing in legacy systems:
  - many new extensions and enhancements have been introduced in the EPS security architecture

EPS Security Architecture

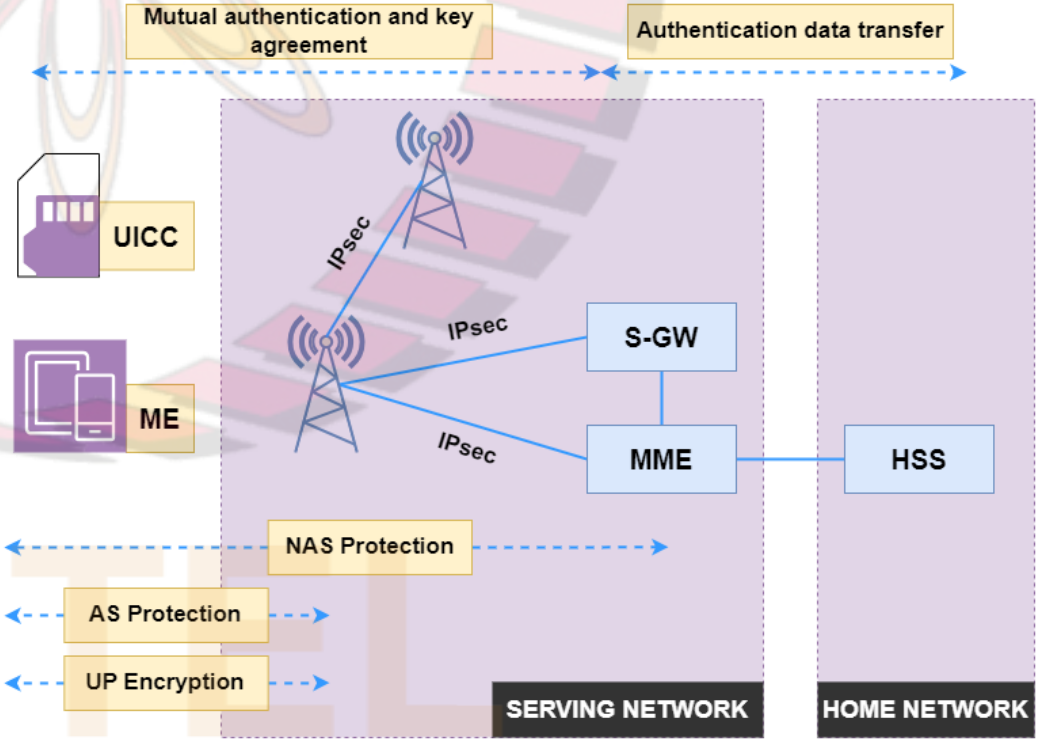
- EPS security architecture illustrated in fig.
- After the User Equipment (UE) has been identified, the Mobility Management Entity (MME) in the serving network fetches authentication data from the home network
- Next the MME triggers the authentication and key agreement (AKA) protocol with the UE
- After this protocol has been successfully completed, the MME and the UE share a secret key, K_{ASME},
  - ❑ where ASME stands for “Access Security Management Entity”

- In the EPS, the MME takes the role of the ASME
- Now the MME and the UE are able to derive further keys from the K_{ASME}
- Two derived keys are used for confidentiality and integrity protection of the signalling data between MME and UE
  - ❑ represented in fig. by arrow with ‘Non-Access Stratum (NAS) protection’



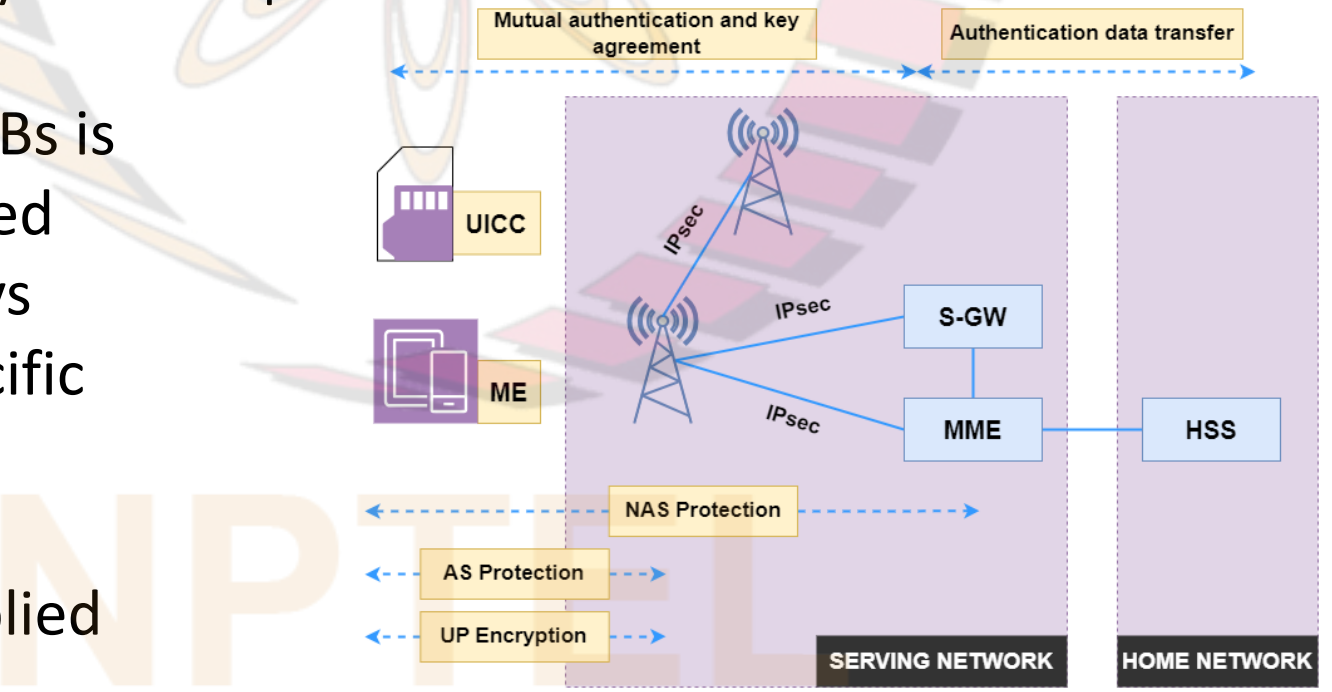
EPS Security Architecture (contd.)

- Another derived key is transported to the eNB
- Three more keys are subsequently derived both in the eNB and in the UE
  - ❑ Two of these keys are used for confidentiality and integrity protection of the signalling data between the eNB and the UE– see arrow with ‘AS protection’ (Access Stratum)
  - ❑ The third key is used for confidentiality protection of the user plane (UP) data between the eNB and the UE– see arrow with ‘UP encryption’



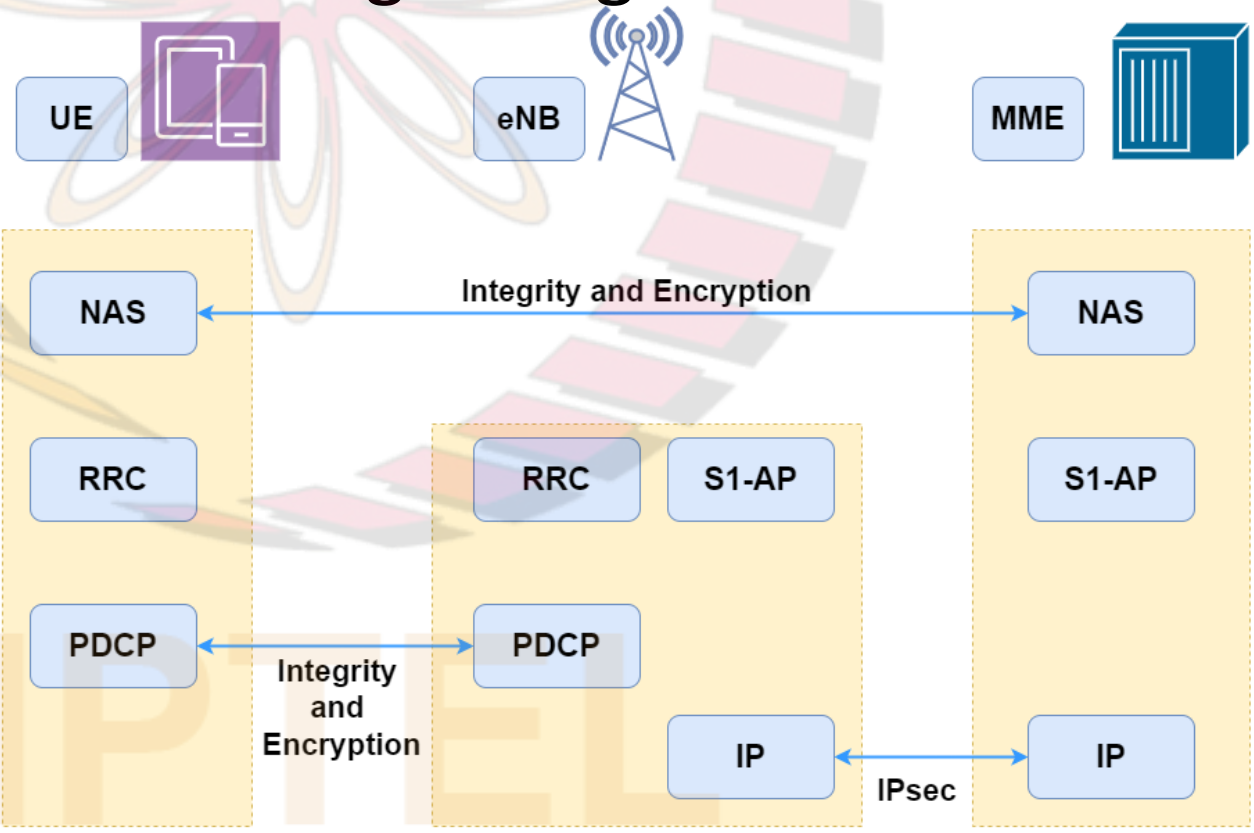
EPS Security Architecture (contd.)

- There is also confidentiality and integrity protection for the signalling and user data carried over the interface between eNB and core network (EPC)
- Signalling data transferred between the UE and the MME over the S1-MME interface, while user data transferred between the UE and the Serving Gateway (S-GW) over S1-U interface
- If cryptographic protection is applied to the S1-interfaces, the protection mechanism used is IPsec
  - ❑ The needed keys are not specific to the UE
- The X2-interface between two eNBs is similarly protected by IPsec with keys that are not specific to the UE in case cryptographic protection is applied



EPS Security Architecture (contd.)

- Fig. shows how confidentiality and integrity protection mechanisms are embedded in signalling plane protocols
- Integrity protection and ciphering is provided for NAS signalling and for AS signalling
- IPsec protection is provided on the interfaces S1 and X2



EPS Security Architecture (contd.)

- Fig. illustrates how user plane protection is provided
- For user data, confidentiality protection is optionally provided between UE and eNB
- Integrity protection is not applied on user data between UE and eNB
- For X2 and S1 interfaces, cryptographic protection for user data is provided in a way similar to that for the corresponding control plane interfaces, by means of the IPsec protocol