Security Bar to 4G and Beyond

Yoshihiro Ohba
(yohba@tari.toshiba.com)
Toshiba America Research, Inc.

Introduction

- High-security is one of the requirements for 4G
- Security in 4G can be divided into two
  - Access network security
  - Core network security
- Mobiles are involved in both types of security

Note: End-to-end security is not discussed here because it's not specific to 4G

Access Network Security

- A unified peer-entity authentication (PEA) mechanism across different link-layer technologies is required for roaming
- EAP (Extensible Authentication Protocol) is recognized as the unified PEA mechanism
  - Within EAP, each home operator can use an operator-specific authentication algorithm to authenticate its clients in visited networks
- What makes stagnation then?
  - Not all link-layer technologies support EAP, especially cellular technologies
  - Additional work is needed to make EAP applicable to seamless handover across different link-layer technologies
    - There is ongoing work in IETF HOKEY WG and IEEE 802.21 WG

Core Network Security

- SAs (Security Associations) need be established between a mobile and a middle box in the core network for different protocols
  - Mobile IPv4/v6, SIP, IPsec, 802.21 MIH (Media-Independent Handover) protocol
- Bootstrapping such SAs require LTCs (Long-Term Credentials)
  - Per-protocol LTCs are difficult to manage, especially in a global roaming environment
  - Network-access LTCs could address the credentials management issue
    - In 3GPP, AKA credentials are usable across different protocols
    - Non-3GPP networks may not use AKA credentials
    - Also, it is not efficient to use LTCs every time bootstrapping an SA
- A Single Sign-On mechanism based on network access LTCs may be needed to bootstrap SAs for different protocols