

Chapter 1. Introduction to Mobile Security

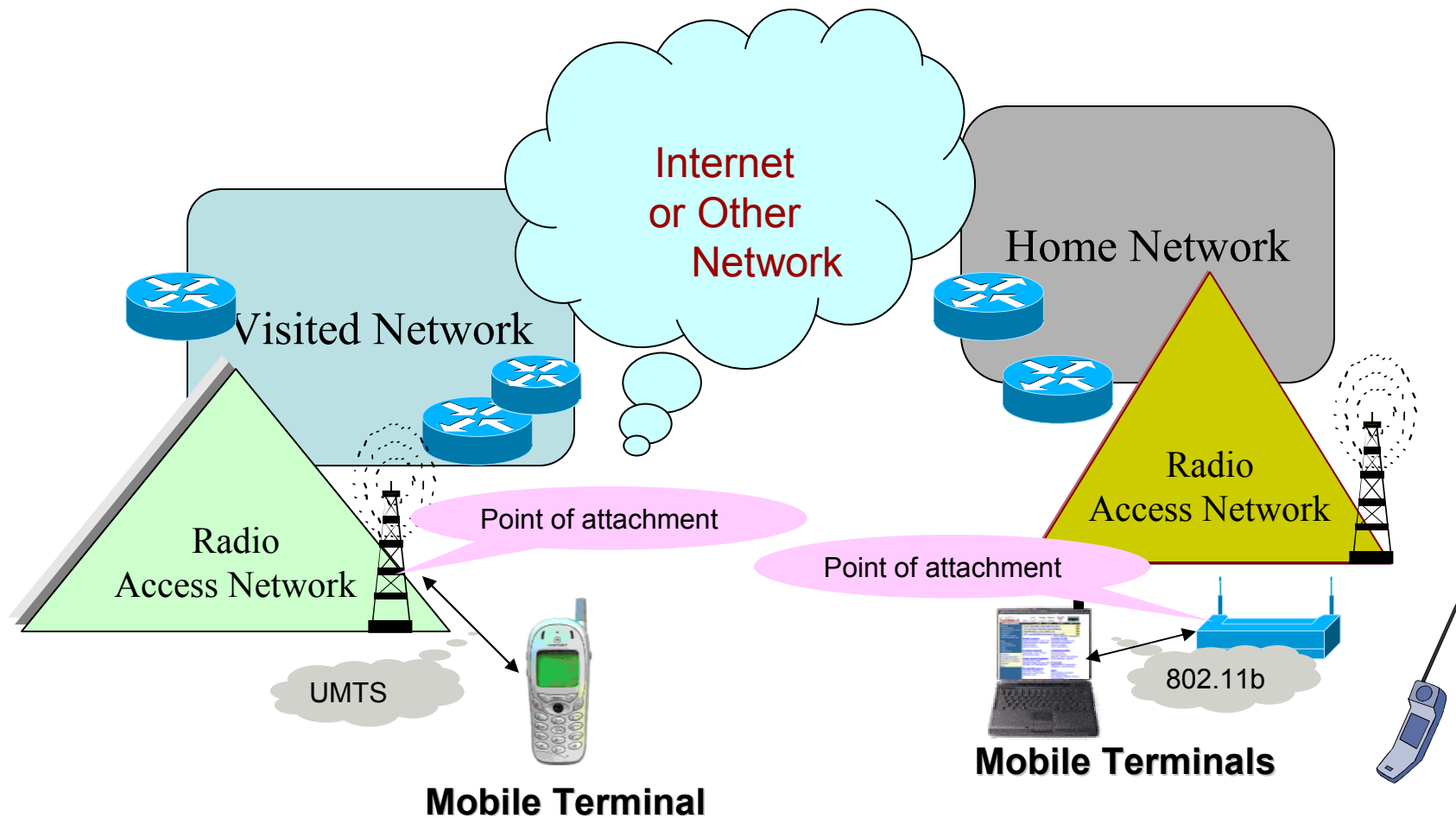
1. Evolution of Mobile Communications Systems
2. Model of Mobile Security
3. Security Objectives and Principles
4. Security Architecture
5. Security Objectives, Threats, Architecture, and Issues in 3G
6. Security in 4/5 G

1. Evolution of Mobile Communications Systems

Generation	1G	2G	2.5G	3G	4/5G
Time Frame	1980s	1990s	Late 1990s	2000s (2010 full deployment)	2010s
Signal Type	Analog	Digital	Digital	Digital	Digital
Multiple Access	FDMA/FDD	TDMA/FDD CDMA/FDD	EDGE, GPRS	CDMA, W-CDMA, TD-SCDMA	MC-CDMA, OFDM
Frequency spectrum		824-894 MHz 890-960 MHz 1850-1990 MHz (PCS)		1800-2400 MHz (varies country to country)	Higher-frequency bands 2-8 GHz
Bandwidth				5-20 MHz	≥ 100 MHz
Antenna				Optimized antenna, multiband adapter	Smarter antenna, Multiband and wide-band support
FEC				Convolutional rate, 1/2, 1/3	Concatenated coding scheme
Media type	Voice	Mostly voice Low-speed data services via modem (10-70 kbps)	Mostly voice Higher-speed data (10-384 kbps)	Voice High-speed data (144kbps-2Mbps)	Converged voice/data/multimedia over IP; Ultra-high-speed data (2-100 Mbps)

Generation	1G	2G	2.5G	3G	4/5G
Network type	Celluar	Celluar	Celluar	WWAN Cell based	Integrated WWAN, WMAN, WLAN (Wi-Fi, Bluetooth) and WPAN (Bluetooth)
Structure	Infrastructure based	Infrastructure based	Infrastru cture based	Infrastructure based network	Hybrid of Infrastructure based and ad hoc network
Switching	Circuit switched	Circuit switched	Circuit switche d	Circuit switched And packet switched	Packet switched
IP support	N/A	N/A	N/A	Use several air link protocols, including IP5.0	All IP based (IP6.0)
New applications				Emails, maps/directions, News, shopping, e-commerce, interactive gaming, etc.	Ubiquitous computing with location intelligence
Ex system	AMPS, NMT, TACS	GSM, DCS1900, IS-95,CdmaOne	GPRS, EDGE	UMTS, IMT200, CDMA2000, WCDMA	
Security	M-sequences for voice enc	A5, m-sequences in CDMA, authentication symmetric crypto	A5, m-seq. auth.	Stream cipher, block cipher, symmetric key auth	Public key crypto

2. Model for Mobile Security – A Big Picture



Model for Mobile Security – Characters

- Mobile terminal can be a laptop computer, a mobile phone, or any smart device with radio (wireless) or without radio interface (wired).
- When a mobile terminal is connected via radio link, the radio links could be licensed radio bandwidth (e.g. cellular) or unlicensed radio bandwidth (e.g. 802.11).
- A mobile terminal may or may not have a home network (service provider).
- A mobile terminal can access a network entity via any layer of connections, e.g. transport layer connection for an application server.

3. Objectives

- Controlled network access – To bar unauthorized access.
 - ✓ Protect service provider's revenue;
 - ✓ Protect network properties;
 - ✓ Guarantee quality of service.
- Trusted platform – To guarantee the mobile platform will behavior as it is assumed.
 - ✓ Protected storage;
 - ✓ Trusted execute environments;
 - ✓ Validated system software;
 - ✓ Authenticated applications;
 - ✓ Authorized user transactions
- Protected communications – To protect the information flow from and to a wireless terminal and protect the information flow from any one network entity to another network entity.
 - ✓ Layered protection protocol;
 - ✓ Link to link or end to end protection.

Security Principles

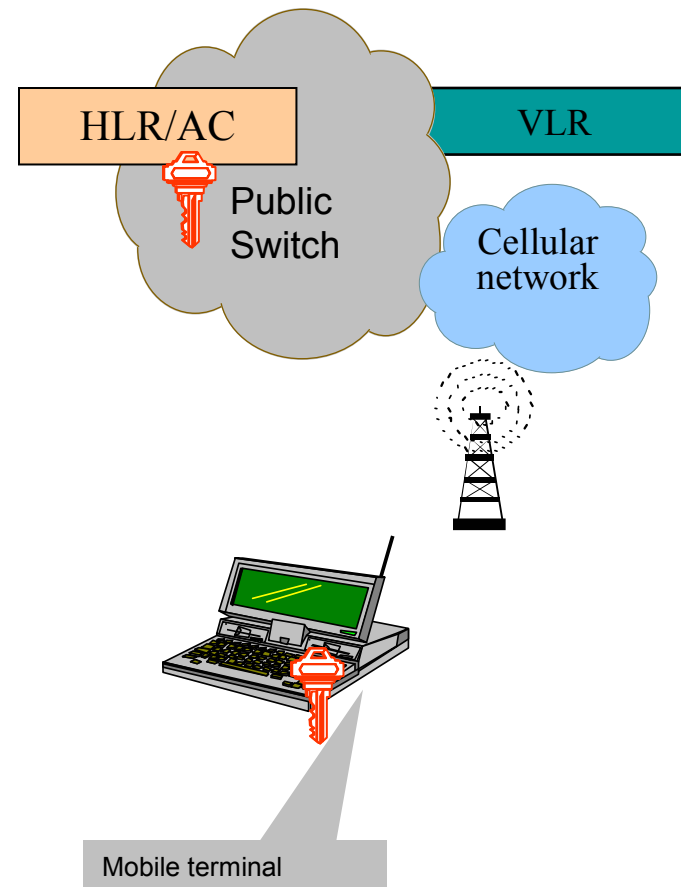
A mobile terminal, access from any point of attachment via either wireless or wired connections, shall be able to authenticate itself to a network entity and establish protected communications.

4. Security Architecture – Access Authentication and Session Key Agreements

- When a mobile terminal accesses a subscription based network, then the service home network shall provide subscriber authentication.
 - The home network will run an authentication center, e.g. in cellular situation, it may co-located with its Home Location Register, in Mobile IP situation, home AAA server.
 - The visited network will conduct authentication and session key agreement with the authentication data provided by home network, assuming that the visited network and the home network have some kind of business relationship, e.g. roaming agreement.
- Usually the lower layer access authentication for radio or media access is very much depending on access technologies, e.g.
 - UMTS – AKA (see 3GPP 33.102);
 - IEEE 802.11 – IEEE 802.1X (See IEEE 802.1X).
- The higher layer access authentication may use more common protocols, e.g.
 - IP network – Radius and Diameter (see IETF RFC 2865);
 - Applications – Extensible Authentication Protocol (see IETF RFC2716).

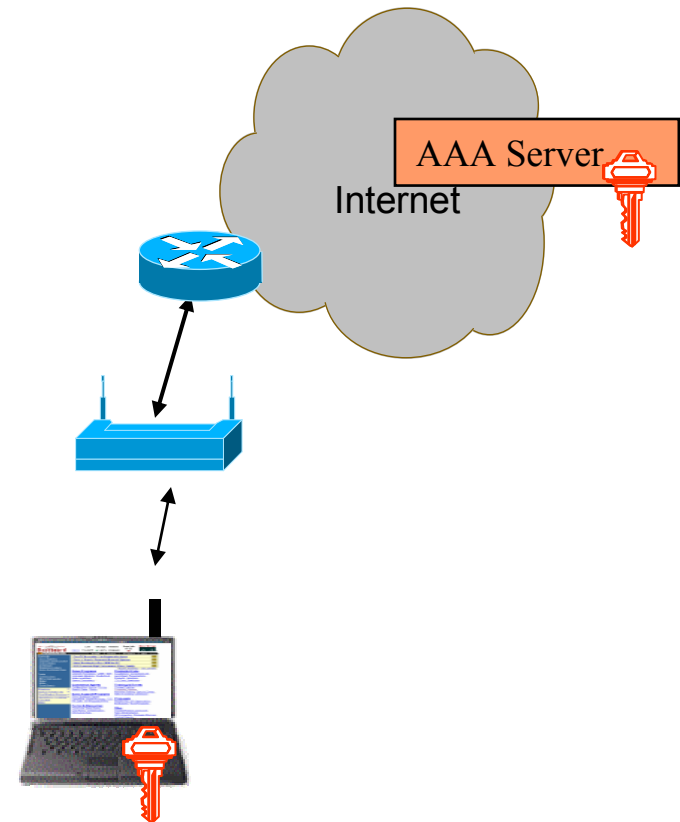
Security Architecture – Cellular Access

- When a mobile terminal requests for access, the visited network, usually, an entity called Visiting Location Register (VLR) will ask HLR for authentication data.
- The VLR will use the data received from HLR to authenticate the subscriber and establish session key.
- The VLR will deliver the session keys to the point of attachment, a base station possibly.
- The protected communication will be established between the terminal and the point of the attachment.



Security Architecture – WLAN Access

- A mobile terminal accesses network via WLAN.
- WLAN may not be subscriber based. However, an AAA server is employed by the WLAN service providers to authenticate the access.
- AAA is a centralized data base and can conduct protocols with a point of attachment, e.g. access point (AP).
- Upon a success authentication, the session keys are delivered to AP for the over the air link protection.



5. 3G Security Principles

- Build on the security of 2G systems (GSM)
 - Security elements which have proved to be needed and robust shall be adopted
- Improve on the security of 2G systems
 - Correct real and perceived weakness in second generation systems
- Offer new security features
 - Secure new services offered by 3G

Security Elements from GSM

- Authentication of subscribers
- Radio interface encryption
- Subscriber identity confidentiality
- Subscriber identity module (SIM)
 - Removable hardware security module

3G Security Objectives

- Ensure that information is adequately protected
- Ensure that resources and services by networks are adequately protected
- Ensure that security features are world-wide available
- Ensure that the level of protection is better than that of contemporary fixed and mobile networks
- Ensure that the implementation of 3GPP security features can be enhanced as required by new threats and services

Security Threats and Requirements

Security Threats

- Unauthorized access to data
 - Violation of confidentiality
 - Eavesdropping traffic or control data
 - Masquerading
 - Traffic analysis
 - Browsing, Inference, etc.
- Threats to integrity
 - Violation of integrity
 - Manipulation of user traffic or control data

Security Threats (Cont.)

- Denial of services
 - Intervention: jamming or protocol failures
 - Resource exhaustion
 - Abuse of services
- Repudiation
- Unauthorized access to services

Points of Attacks

- Radio Interface
 - Between the terminal equipment and the serving network
- Other parts of the system
 - Other wireless or wired interfaces
- Terminals and USIM
 - Use of stolen terminals and USIM

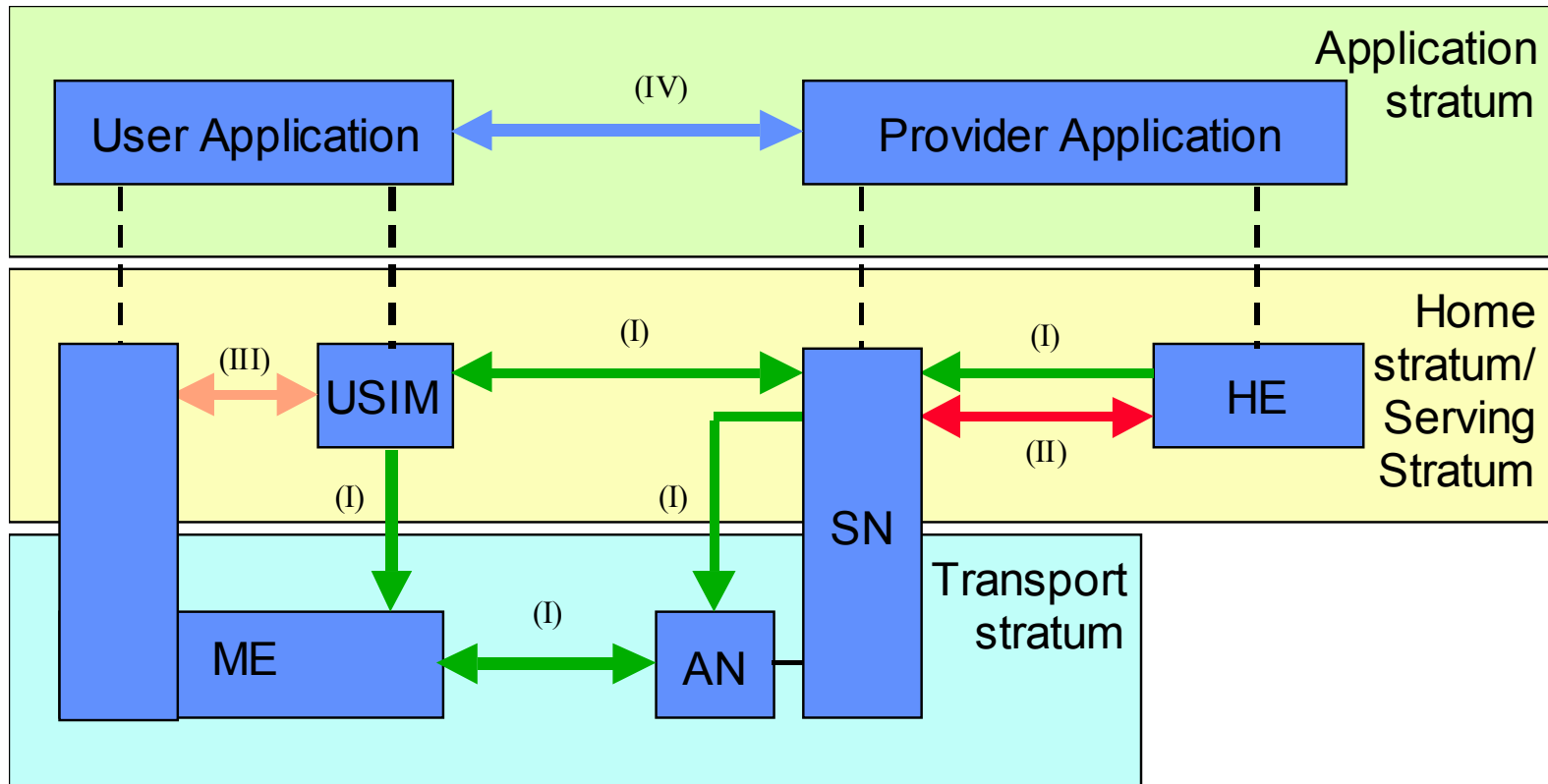
Security Requirements

- Authentication of serving networks by users at the start of and during service delivery
- Authentication of users by service providers at the start of and during service delivery
- Secure infrastructure between network operators
- Protection against unauthorized modification of traffic, signaling or control data
- Integrity and freshness of authentication data including cipher key
- Confidentiality of traffic, signaling, identity, and location data

Infrastructure

- Home Environment (HE)
 - Provide a set of services to users associated with subscription
 - Negotiation with network operators for network capabilities
 - HLR/AuC
- Serving Network (SN)
 - Provide and manage radio resources and fixed resources
 - Interact with HE to identify, authenticate, authorize and locate users
 - VLR/SGSN

Overview of Security Architecture



User Services Identity Module (USIM)

- Identifies a user and his association with a HE in 3G services
- Contains functions and data needed to identify and authenticate users
- Contains a copy of user's service profile and any security parameters

Security Feature Layers

- Network Access Security (I): Set of security features that provide users with secure access to 3G services:
 - User identity confidentiality
 - Entity authentication: Authentication and key establishment
 - Confidentiality
 - Data integrity
- Network Domain Security (II)
- User Domain Security (III)
- Application Domain Security (IV)

Security Issues in 3G Systems

Terminal Security: Smart Card with PIN number has been used to protect terminal security.

<u>Abbreviation</u>	<u>Full Name</u>	<u>Defining Standard</u>
SIM	Subscriber Identity Module	GSM
UIM	User Identity Module	IS-95
USIM	Universal SIM	UMTS
R-UIM	Removable UIM	CDMA2000
WIM	Wireless Identity Module	WAP

Security Issues in 3G Systems (Cont.)

Lawful Interception

The UMTS and GSM, like all telecom systems, allow lawful interception for authorized law and enforcement agencies. This is required by national laws and EU directives, and is used for crime investigation and national security. The Internet users have traditionally very negative attitudes towards monitoring of their communications, and lawful interception can become at least an image problem for the new IP-services of the telecom systems.

Security Trends in 3G Systems

- Offer complete security solutions-not just provide protection over the radio link
- Offer negotiation
- Offer mutual authentication
- Offer data confidentiality and data/signaling authentication
- Prevent replay attack on the signaling
- Provide period data authentication
- Use SIM card
- Universal roaming
- Continuously migrate to 4G systems in terms of enhanced security, services, access media, data rate, capabilities

6. Security in 4/5G Systems

- Use public-key algorithms for key agreement, privacy and authentication
- Provide non-repudiation services
- Provide key recovery (escrow)
- Universal access to any type of media and devices
- Integrate services, including payment and charging

References:

- IEEE 802.1X “ Port-based network access control”.
- “Wireless security”, http://www.compaq.ch/ins_wpwirelesssecurity.pdf
- ETSI 3GPP Technical Specifications 33.102 v5.1.0.
- 3G TS 33.120, v4.0.0, 3G security; Security objectives and principles (Release 4).
- 3G TS 21.133, v4.1.0, 3G security; Security threats and requirements (Release 4).
- 3G TS 33.102, v4.5.0, 3G security; Security architecture (Release 4).