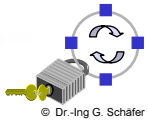
Mobile Communications Security

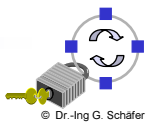
Dr.-Ing. Günter Schäfer
Telecommunications Network Group
Technische Universität Berlin, Germany

- Introduction: Threats & Countermeasures
- GSM, GPRS & UMTS
- Mobile Internet Based on IETF Protocols
- Conclusions



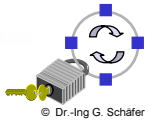
What is a Threat in a Communication Network?

- Abstract Definition:
  - A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
  - The actual realization of a threat is called an *attack*
- Examples:
  - A hacker breaking into a corporate computer
  - Disclosure of emails in transit
  - Someone changing financial accounting data
  - A hacker temporarily shutting down a website
  - Someone using services or ordering goods in the name of others
  - ...
- What are security goals?
  - Security goals can be defined:
    - depending on the application environment, or
    - in a more general, technical way



Security Goals Technically Defined

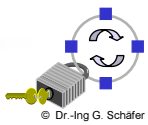
- *Confidentiality:*
  - Data transmitted or stored should only be revealed to an intended audience
  - Confidentiality of entities is also referred to as *anonymity*
- *Data Integrity:*
  - It should be possible to detect any modification of data
  - This requires to be able to identify the creator of some data
- *Accountability:*
  - It should be possible to identify the entity responsible for any communication event
- *Availability:*
  - Services should be available and function correctly
- *Controlled Access:*
  - Only authorized entities should be able to access certain services or information



Threats and Technical Security Goals

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

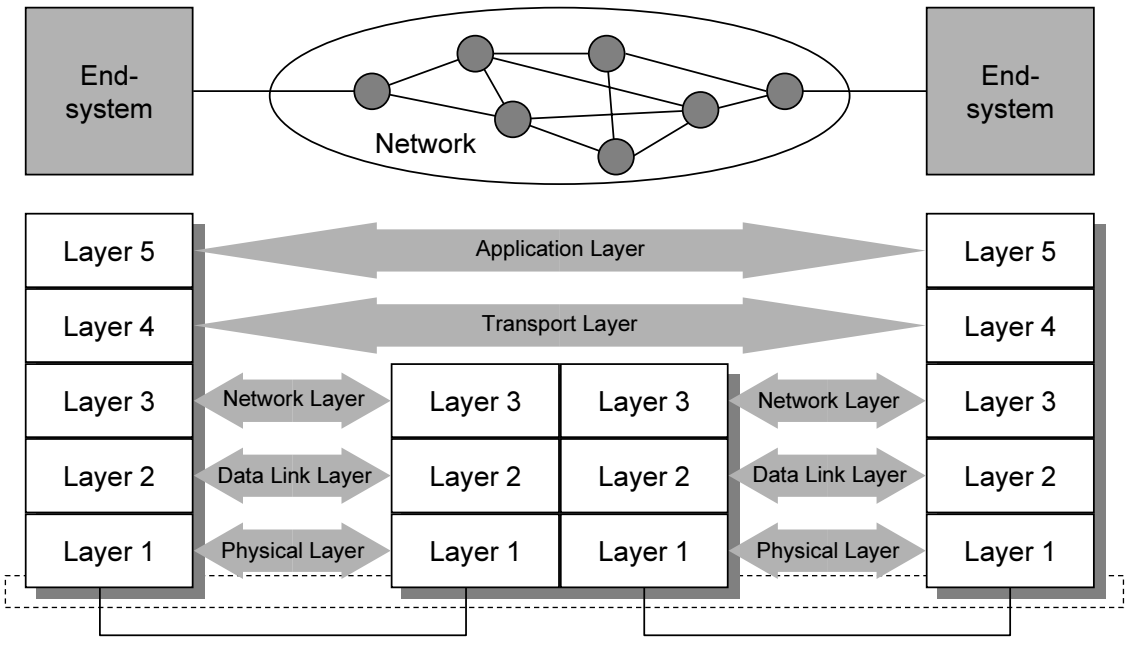
These threats are often combined in order to perform an attack!



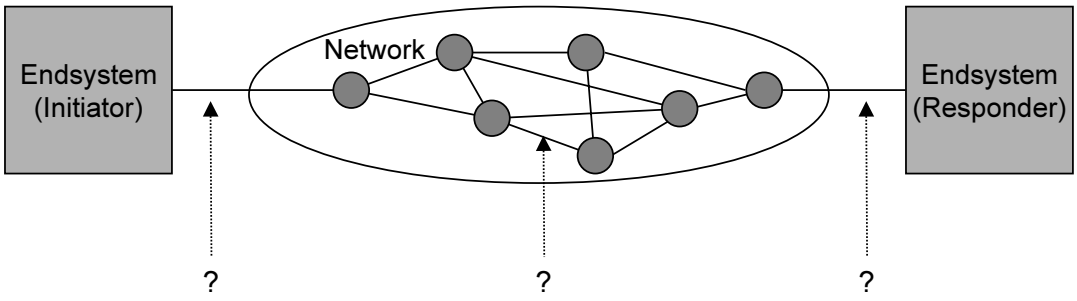
Attacking Communications on the Message Level

- Passive attacks:
  - Eavesdropping
- Active attacks:
  - Delay of PDUs (Protocol Data Units)
  - Replay of PDUs
  - Deletion of PDUs
  - Modification of PDUs
  - Insertion of PDUs
- Successful launch of one of the above attacks requires:
  - There are no detectable side effects to other communications (connections / connectionless transmissions)
  - There are no side effects to other PDUs of the same connection / connectionless data transmission between the same entities
- A security analysis of a protocol architecture has to analyse these attacks according to the architecture's layers

Communication in Layered Protocol Architectures

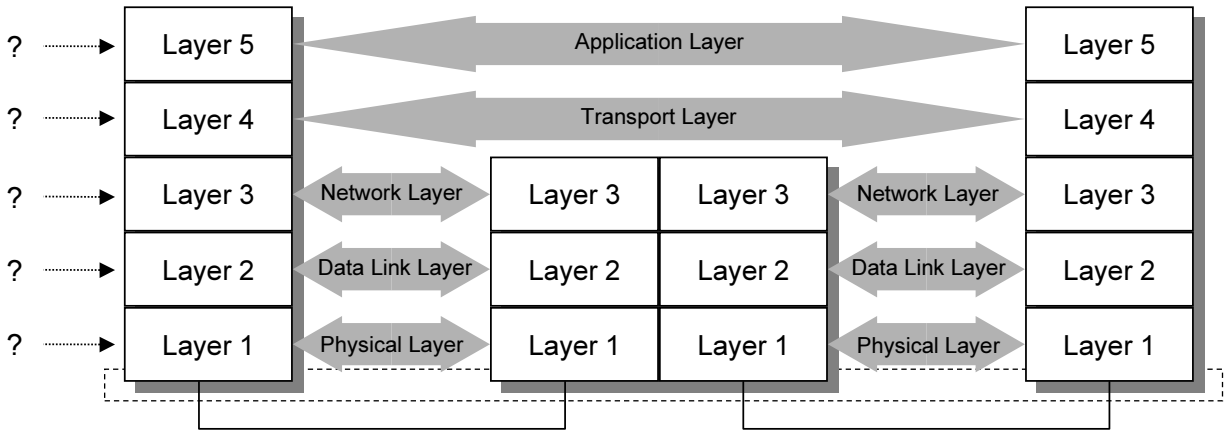


Security Analysis of Layered Protocol Architectures 1



Dimension 1: At which interface does the attack take place?

Security Analysis of Layered Protocol Architectures 2



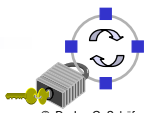
Dimension 2: In which layer does the attack take place?

Communications Security: Some Terminology

- Security Service:
  - An abstract service that seeks to ensure a specific security property
  - A security service can be realised with the help of cryptographic algorithms and protocols as well as with conventional means:
    - One can keep an electronic document on a floppy disk confidential by storing it on the disk in an encrypted format as well as locking away the disk in a safe
    - Usually a combination of cryptographic and other means is most effective
- Cryptographic Algorithm:
  - A mathematical transformation of input data (e.g. data, key) to output data
  - Cryptographic algorithms are used in cryptographic protocols
- Cryptographic Protocol:
  - A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

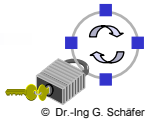
Security Services – Overview

- *Authentication*
  - The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- *Integrity*
  - In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- *Confidentiality*
  - The most popular security service, ensuring the secrecy of protected data
- *Access Control*
  - Controls that each identity accesses only those services and information it is entitled to
- *Non Repudiation*
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred



Cryptographic Algorithms: Overview

- For network security two main applications of cryptographic algorithms are of principal interest:
  - *Encryption* of data: transforms plaintext data into ciphertext in order to conceal its' meaning
  - *Signing* of data: computes a *check value* or *digital signature* to a given plain- or ciphertext, that can be verified by some or all entities being able to access the signed data
- Some cryptographic algorithms can be used for both purposes, some are only secure and / or efficient for one of them.
- Principal categories of cryptographic algorithms:
  - *Symmetric cryptography* using 1 key for en-/decryption or signing/checking
  - *Asymmetric cryptography* using 2 different keys for en-/decryption or signing/checking
  - *Cryptographic hash functions* using 0 keys (the "key" is not a separate input but "appended" to or "mixed" with the data).



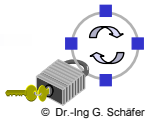
Cryptographic Protocols

Definition:

A *cryptographic protocol* is defined as a series of steps and message exchanges between multiple entities in order to achieve a specific security objective

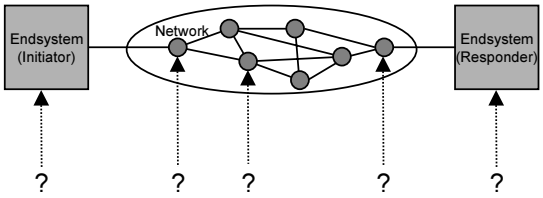
Applications of cryptographic protocols:

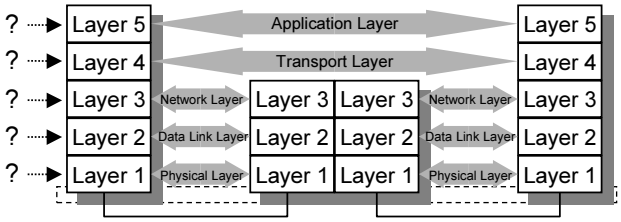
- Key exchange
- Authentication
  - Data origin authentication: the security service, that enables a receiver to verify by whom a message was created and that it has not been modified
  - Entity authentication: the security service, that enables communication partners to verify the identity of their peer entities
- Combined authentication and key exchange
- plus many others...



Integrating Security into Networks: What to do where?

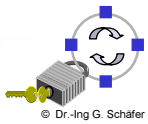
- Analogous to the methodology of security analysis, there are *two dimensions* guiding the integration of security services into communications architectures:



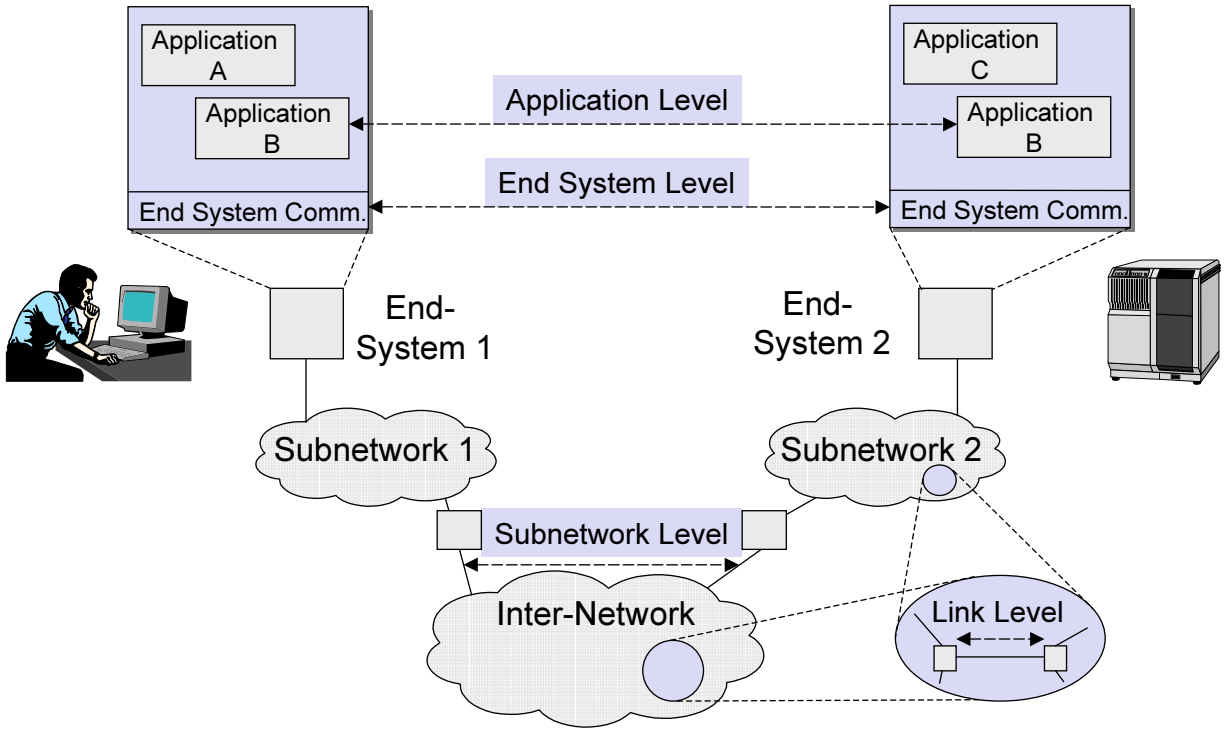


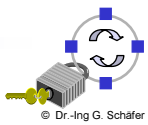
Dimension 1:
Which security service should be realized in which node?

Dimension 2:
Which security service should be realized in which layer?



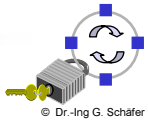
A Pragmatic Model for Secured & Networked Computing





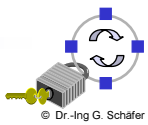
Security Aspects of Mobile Communication

- Mobile communication faces all threats that does its' fixed counterpart:
  - Masquerade, eavesdropping, authorization violation, loss or modification of transmitted information, repudiation of communication acts, forgery of information, sabotage
  - Thus, similar measures like in fixed networks have to be taken
- However, there are some specific issues arising out of mobility of users and / or devices:
  - Some already existing threats get more dangerous:
    - Wireless communications is more accessible for eavesdropping
    - The lack of a physical connection makes it easier to access services
  - Some new difficulties for realizing security services:
    - Authentication has to be re-established when the mobile device moves
    - Key management gets harder as peer identities can not be pre-determined
  - One completely new threat:
    - The location of a device / user becomes a more important information that is worthwhile to eavesdrop on and thus to protect



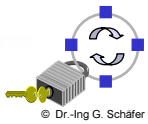
Location Privacy in Mobile Networks (1)

- There is no appropriate location privacy in today's mobile networks:
  - GSM / UMTS:
    - Active attackers can collect IMSIs on the air interface
    - Visited network's operators can partially track the location of users
    - Home network operators can fully track the location of users
    - However, at least communicating end systems can not learn about the location of a mobile device
  - Wireless LAN:
    - No location privacy, as the (world-wide unique) MAC address is always included in the clear in every MAC frame
  - Mobile IP:
    - Standard Mobile IP: HA can fully / FA can partially track MNs
    - Mobile IP with AAA: no location privacy on air interface, foreign AAA infrastructure can partially / home AAA server can fully track MNs
    - Mobile IP with route optimization: even CNs can track an MN from everywhere around the world if the MN wishes to use the optimization



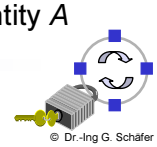
Location Privacy in Mobile Networks (2)

- The basic location privacy design problem:
  - A mobile device should be reachable
  - No (single) entity in the network should be able to track the location of a mobile device
- Some fundamental approaches to this problem [Müller99a]:
  - *Broadcast of messages:*
    - Every message is sent to every possible receiver
    - If confidentiality is needed, the message is encrypted asymmetrically
    - This approach does not scale well for large networks / high load
  - *Temporary pseudonyms:*
    - Mobile devices use pseudonyms which are changed regularly
    - However, to be able to reach the mobile device this needs a mapping entity which can track the mobile's history of pseudonyms
  - *Mix networks:*
    - Messages are routed via various entities (mixes) and every entity can only learn a part of the message route (see below)



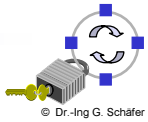
Location Privacy in Mobile Networks (3)

- Addressing schemes for location privacy with broadcast:
  - *Explicit addresses:*
    - Every entity that "sees" an explicit address is able to determine the addressed entity
  - *Implicit addresses:*
    - An implicit address does not identify a specific device or location, it just names an entity without any further meaning attached to the name
    - *Visible implicit addresses:*
      - Entities that see multiple occurrences of an address can check for equality
    - *Invisible implicit addresses:*
      - Only the addressed entity can check for equality of the address
      - This requires public key operations: $ImplAddr_A = \{r_B, r_A\}_{+K_A}$ where r_A is chosen by the addressed entity and r_B is a random value created by an entity *B* which wants to invisibly make reference to entity *A*



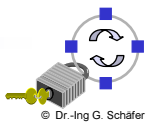
Location Privacy in Mobile Networks (4)

- *Temporary Pseudonyms:*
  - The location of a device A is no longer stored with its' identification ID_A but with a changing pseudonym $P_A(t)$
    - Example: VLRs in GSM might just know and store the TMSI (which is kind of a temporary pseudonym)
  - The mapping of an ID_A to the current pseudonym $P_A(t)$ is stored in a trustworthy device
    - Example: GSM HLRs might be realized as trustworthy devices
  - When an incoming call has to be routed to the current location of device A:
    - The network provider of device A asks the trustworthy device for the current pseudonym $P_A(t)$
    - The network then routes the call to the current location of A by looking up the temporary pseudonym in a location database
    - It is important, that the entities that route a call can not learn about the original address of the call setup message ($\rightarrow$ implicit addresses)
    - The use of mixes (see below) can provide additional protection against attacks from colluding network entities



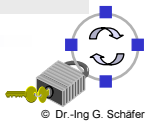
Location Privacy in Mobile Networks (5)

- *Communication mixes:*
  - The concept was invented in 1981 by D. Chaum for untraceable email communication
  - A *mix* hides the communication relations between senders and receivers:
    - It buffers incoming messages which are asymmetrically encrypted so that only the mix can decrypt them
    - It changes the "appearance" of messages by decrypting them
    - It changes the order of messages and relays them in batches
    - However, if the mix is compromised an attacker can learn "everything"
  - Security can be increased by cascading mixes
  - Example: A sends a message m to B via two mixes M1 and M2
    - A $\rightarrow$ M1: $\{r_1,\{r_2, \{r_3, m\}_{+K_B}\}_{+K_{M2}}\}_{+K_{M1}}$
    - M1 $\rightarrow$ M2: $\{r_2, \{r_3, m\}_{+K_B}\}_{+K_{M2}}$
    - M2 $\rightarrow$ B: $\{r_3, m\}_{+K_B}$
    - It is important, that the mixes process "enough" messages
  - This concept can be applied to mobile communications [Müller99a]



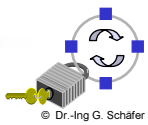
GSM Security Overview (1)

- GSM provides the following security features [ETSI93a, ETSI94a]:
  - *Subscriber identity confidentiality:*
    - Protection against an intruder trying to identify which subscriber is using a given resource on the radio path (e.g. traffic channel or signaling resources) by listening to the signaling exchanges on the radio path
    - Confidentiality for signaling and user data
    - Protection against the tracing of a user's location
  - *Subscriber identity authentication:*
    - Protection of the network against unauthorized use
  - *Signaling information element confidentiality:*
    - Non-disclosure of signaling data on the radio link
  - *User data confidentiality:*
    - Non-disclosure of user data on the radio link
- However, only eavesdropping attacks on the radio link between the mobile and the base stations are taken into account!

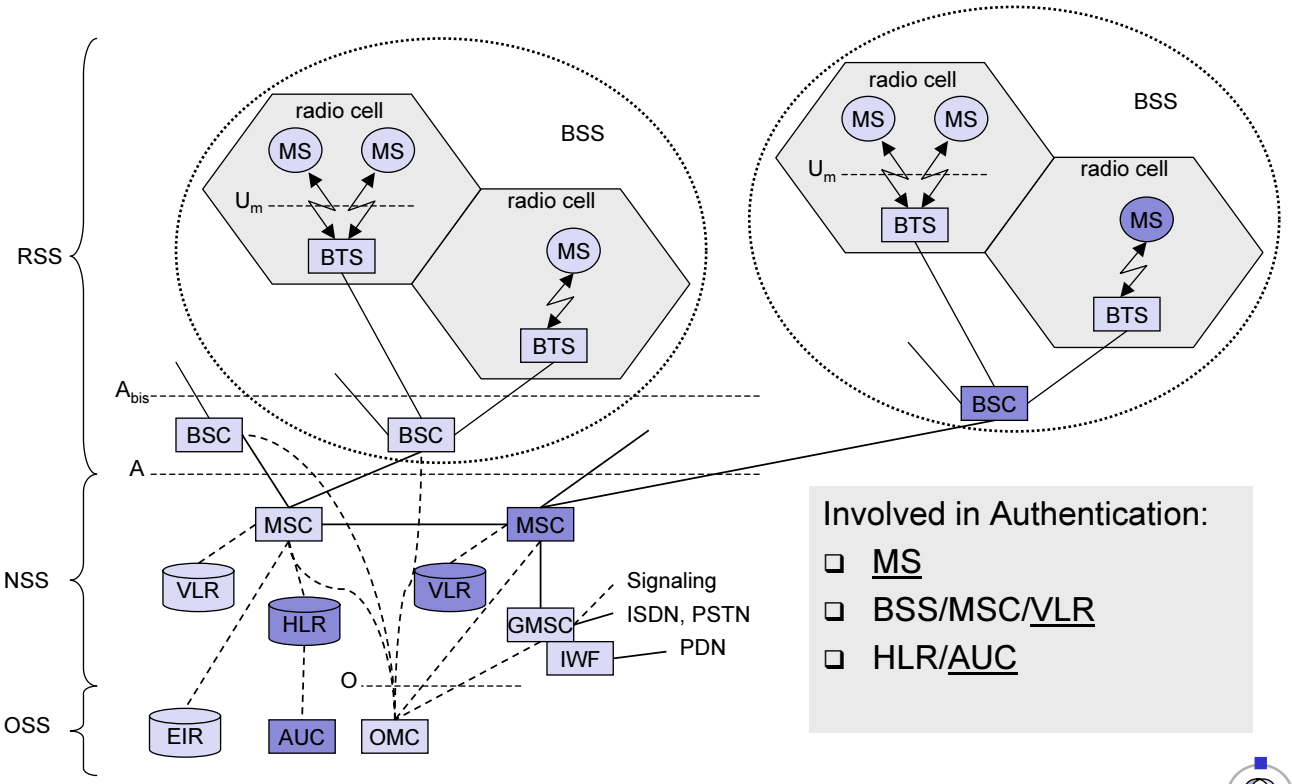


GSM Security Overview (2)

Some GSM Abbreviations	
AUC	Authentication center
BSC	Base station controller
BTS	Base transceiver station
IMSI	International mobile subscriber identity
HLR	Home location register
LAI	Location area identifier
MS	Mobile station (e.g. a mobile phone)
MSC	Mobile switching center
MSISDN	Mobile subscriber international ISDN number
TMSI	Temporary mobile subscriber identity
VLR	Visitor location register



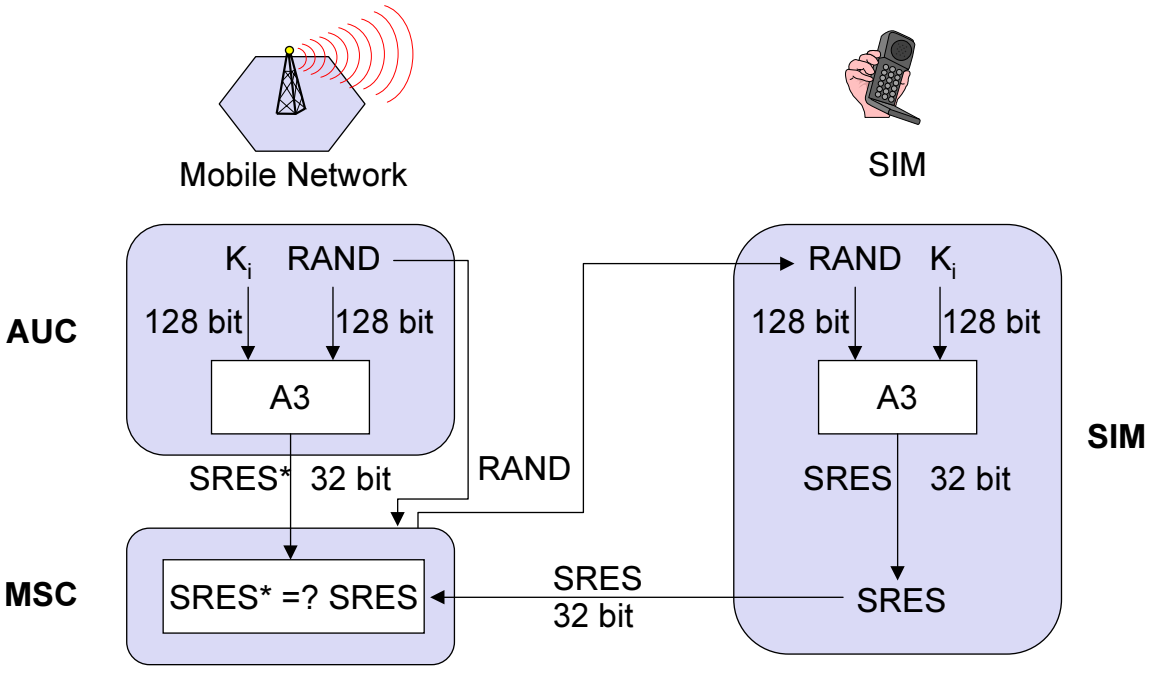
Authentication in GSM (1)



Involved in Authentication:

- MS
- BSS/MSC/VLR
- HLR/AUC

Authentication in GSM (2)

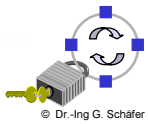


K_i: Individual Subscriber Authentication Key

SRES: Signed Response

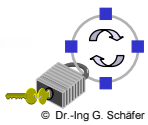
Authentication in GSM (3)

- The basic (initial) authentication dialogue:
  1.) MS → VLR: ($IMSI_{MS}$)
  2.) VLR → AUC: ($IMSI_{MS}$)
  3.) AUC → VLR: ($IMSI_{MS}$, $K_{BSC,MS}$, R_{AUC}, $SRES_{AUC}$)
  4.) VLR → MS: ($R_{AUC:1}$)
  5.) MS → VLR: ($SRES_{AUC:1}$)
  6.) VLR → MS: (LAI_1, $TMSI_{MS:1}$)
- Remarks:
  - $SRES_{AUC}$ = A3($K_{AUC,MS}$, R_{AUC}); A3 is an algorithm
  - $K_{BSC,MS}$ = A8($K_{AUC,MS}$, R_{AUC}); A8 is an algorithm
  - R_{AUC}, $SRES_{AUC}$ are arrays of multiple values



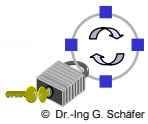
Authentication in GSM (4)

- Re-authentication dialogue with the same VLR:
  1.) MS → VLR: (LAI_1, $TMSI_{MS:n}$)
  2.) VLR → MS: ($R_{AUC:i}$)
  3.) MSC → VLR: ($SRES_{AUC:i}$)
  4.) VLR → MS: (LAI_1, $TMSI_{MS:n+1}$)
- Remarks:
  - The *location area identification* LAI_1 allows to detect an MS "coming in" from another area
  - After successful authentication a new temporary mobile subscriber identity $TMSI_{MS:n+1}$ is assigned



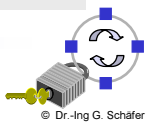
Authentication in GSM (5)

- Re-authentication dialogue with handover to new VLR_2:
  1.) MS → VLR_2: (LAI_1, $TMSI_{MS:n}$)
  2.) VLR_2 → VLR_1: (LAI_1, $TMSI_{MS:n}$)
  3.) VLR_1 → VLR_2: ($TMSI_{MS:n}$, $IMSI_{MS}$, $K_{BSC,MS}$, R_{AUC}, $SRES_{AUC}$)
  4.) VLR_2 → MS: ($R_{AUC:i}$)
  5.) MS → VLR_2: ($SRES_{AUC:i}$)
  6.) VLR_2 → MS: (LAI_2, $TMSI_{MS:n+1}$)
- Remarks:
  - Only unused R_{AUC}, ... are transmitted to VLR_2
  - This scheme can not be used and an initial dialogue is needed:
    - If $TMSI_{MS:n}$ is unavailable at VLR_1, or
    - If VLR_2 is not able to contact VLR_1
  - If VLR_1 and VLR_2 belong to different network operators the handover can not be performed and the call is disconnected



Conclusion on Authentication in GSM (6)

- Only the mobile authenticates itself to the network
- Authentication is based on challenge-response:
  - The AUC in the home network generates challenge-response pairs
  - The MSC/VLR in the visited network checks them
  - Challenge-response vectors are transmitted unprotected in the signaling network
- The permanent identification of the mobile (IMSI) is just sent over the radio link when this is unavoidable:
  - This allows for partial location privacy
  - As the IMSI is sometimes sent in clear, it is nevertheless possible to learn about the location of some entities
    - An attacker may impersonate a base station and explicitly demand mobiles to send their IMSIs!
- Basically, there is trust between all operators!



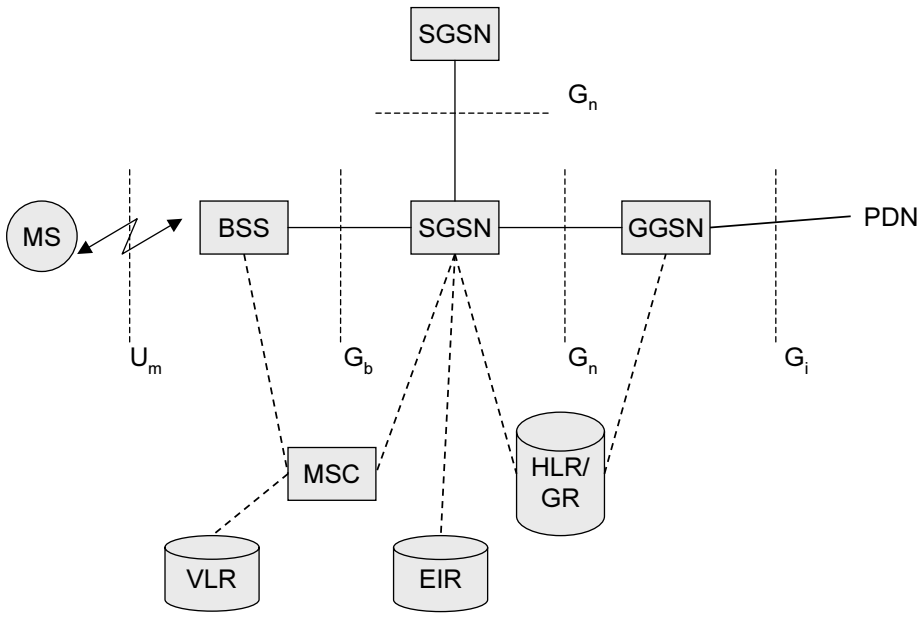
General Packet Radio Service (GPRS)

- GPRS (General Packet Radio Service):
  - Data transmission in GSM networks based on packet switching
  - Using free slots of the radio channels only if data packets ready to send (e.g., 115 kbit/s using 8 slots temporarily)

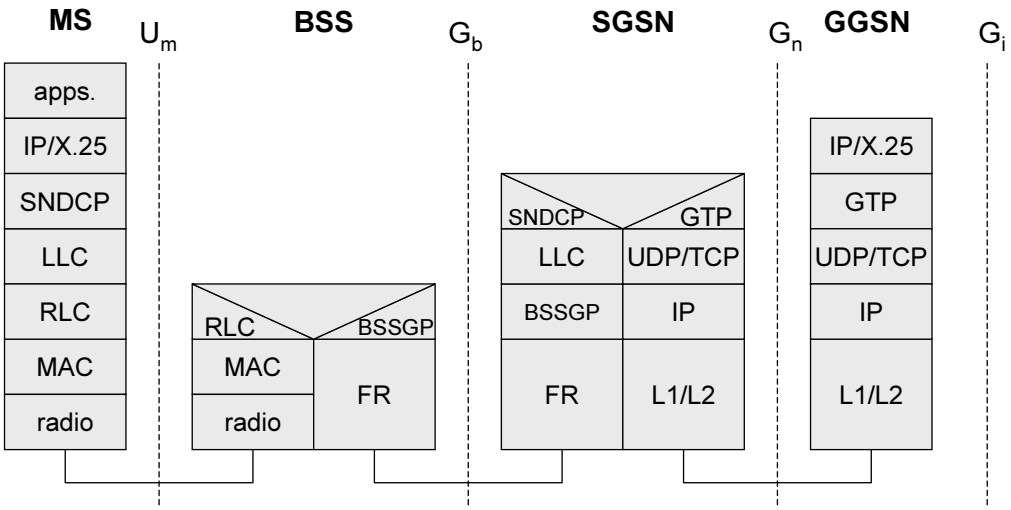
- GPRS network elements:
  - GGSN (Gateway GPRS Support Node)
    - Interworking unit between GPRS and PDN (Packet Data Network)
  - SGSN (Serving GPRS Support Node)
    - Supports the MS (location, billing, security, basically equivalent to MSC)
  - GR (GPRS Register)
    - Handles user addresses (equivalent to HLR)

(general GPRS description taken from [Sch02a])

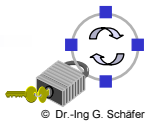
GPRS Logical Architecture



GPRS Protocol Architecture (Transmission Plane)

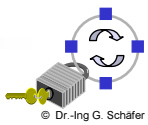


SNDCP: Subnetwork Dependent Convergence Protocol
GTP: GPRS Tunnelling Protocol

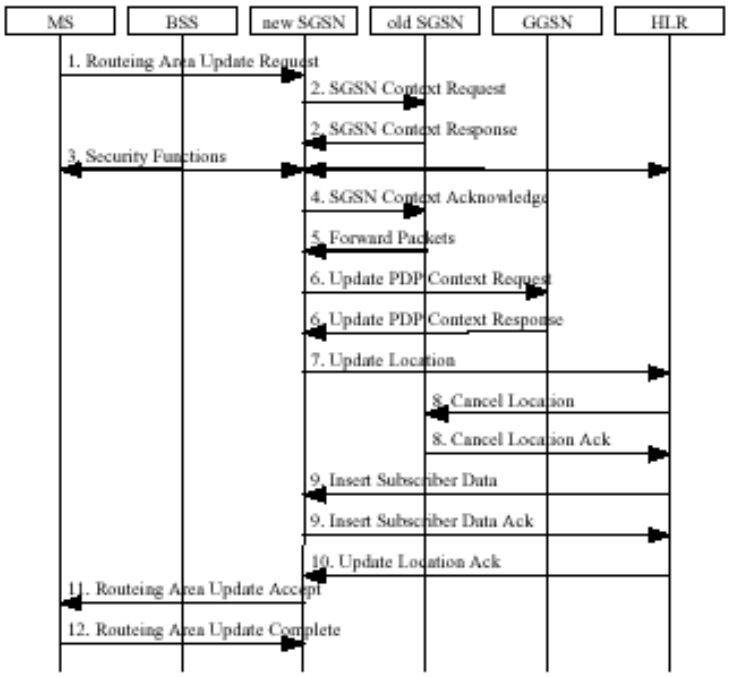


GPRS Security

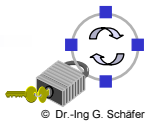
- Security objectives:
  - Guard against unauthorised GPRS service usage (authentication)
  - Provide user identity confidentiality (temporary identification and ciphering)
  - Provide user data confidentiality (ciphering)
- Realization of security services:
  - Authentication is basically identical to GSM authentication:
    - SGSN is the peer entity
    - Two separate temporary identities are used for GSM/GPRS
    - After successful authentication, ciphering is turned on
  - User identity confidentiality is similar to GSM:
    - Most of the time, only the Packet TMSI (P-TMSI) is send over the air
    - Optionally, P-TMSI “signatures” may be used between MS and SGSN to speed up re-authentication
  - User Data Confidentiality is realized between MS and SGSN:
    - Difference to GSM which just ciphered between MS and BTS
    - Ciphering is realized in the LLC protocol layer



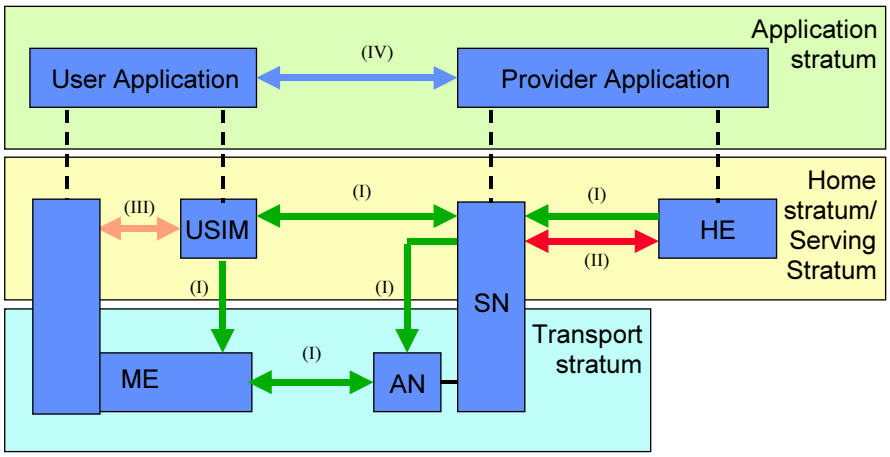
GPRS Handover Execution



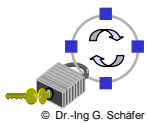
GPRS supports an “optimized handover” including re-authentication (however, this might inhibit a weakness → P-TMSI “signature”)



Overview over the UMTS Security Architecture



(I) *Network access security:* protect against attacks on the radio interface
(II) *Network domain security:* protect against attacks on the wireline network
(III) *User domain security:* secure access to mobile stations
(IV) *Application domain security:* secure message exchange for applications
(V) *Visibility and configurability of security:* inform user of secure operation



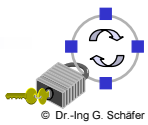
Current State of the UMTS Security Architecture

- Network Access Security:
  - Currently the most developed part of UMTS security (see below)
- Network Domain Security:
  - This part is mainly to be done (in specifications up to Release 5)
- User Domain Security:
  - Basically requires that the user authenticates himself to his user services identity module (USIM), e.g. by entering a PIN
  - Optionally, a terminal can require authentication of the USIM
- Application Domain Security:
  - Defines a security protocol to be used between applications running in the terminal / USIM and some system in the network (3GPP TS 23.048)
  - Somewhat out of the scope of mobile communications security
- Visibility and configurability of security:
  - Defines requirements so that the user will be in control of security features

→ In the following, we will concentrate on network access security

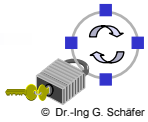
UMTS Network Access Security Services (1)

- User identity confidentiality:
  - *User identity confidentiality:* the property that the permanent user identity (IMSI) of a user to whom a service is delivered cannot be eavesdropped on the radio access link
  - *User location confidentiality:* the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link
  - *User untraceability:* the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link
- Entity authentication:
  - *User authentication:* the property that the serving network corroborates the user identity of the user
  - *Network authentication:* the property that the user corroborates that he is connected to a serving network that is authorized by the user's HE to provide him services; this includes the guarantee that this authorization is recent.



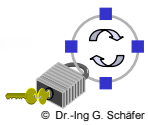
UMTS Network Access Security Services (2)

- Confidentiality:
  - *Cipher algorithm agreement:* the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently
  - *Cipher key agreement:* the property that the MS and the SN agree on a cipher key that they may use subsequently
  - *Confidentiality of user data:* the property that user data cannot be eavesdropped on the radio access interface
  - *Confidentiality of signaling data:* the property that signaling data cannot be eavesdropped on the radio access interface
- Data Integrity:
  - *Integrity algorithm agreement*
  - *Integrity key agreement*
  - *Data integrity and origin authentication of signaling data:* the property that the receiving entity (MS or SN) is able to verify that signaling data has not been modified in an unauthorized way since it was sent by the sending entity (SN or MS) and that the data origin of the signaling data received is indeed the one claimed

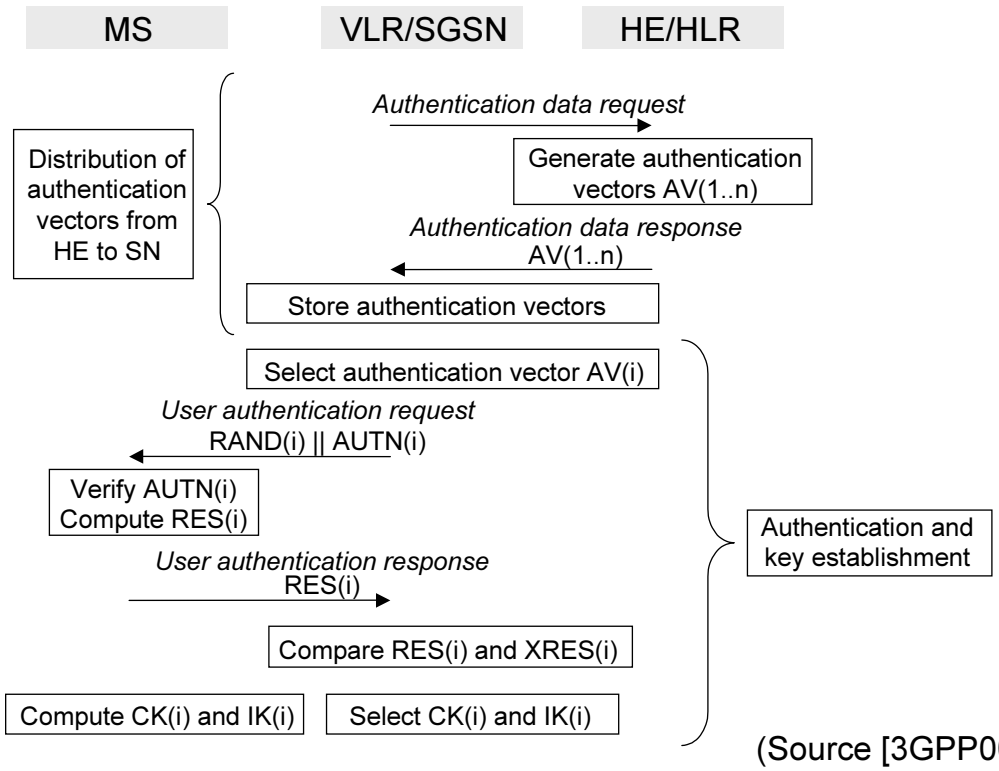


Overview of the UMTS Authentication Mechanism (1)

Some UMTS Authentication Abbreviations	
AK	Anonymity Key
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
HE	Home Environment
IK	Integrity Key
RAND	Random challenge
SQN	Sequence number
SN	Serving Network
USIM	User Services Identity Module
XRES	Expected Response

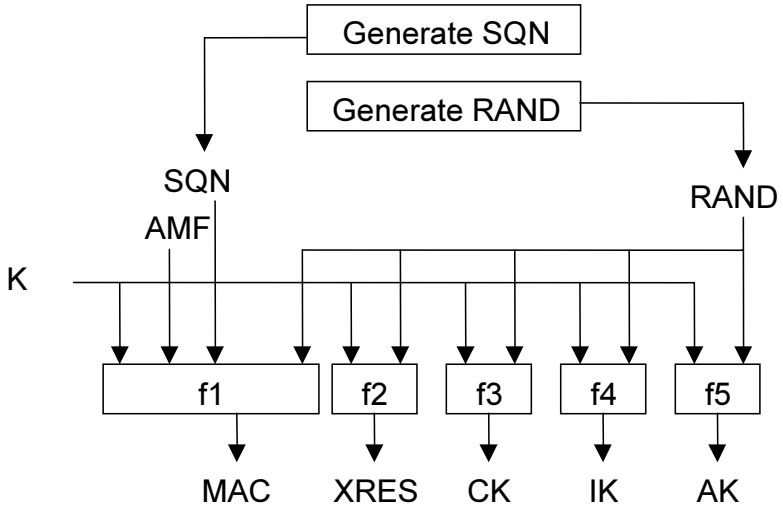


Overview of the UMTS Authentication Mechanism (2)



(Source [3GPP00a])

Generation of UMTS Authentication Vectors (1)



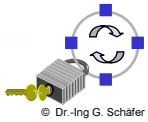
AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

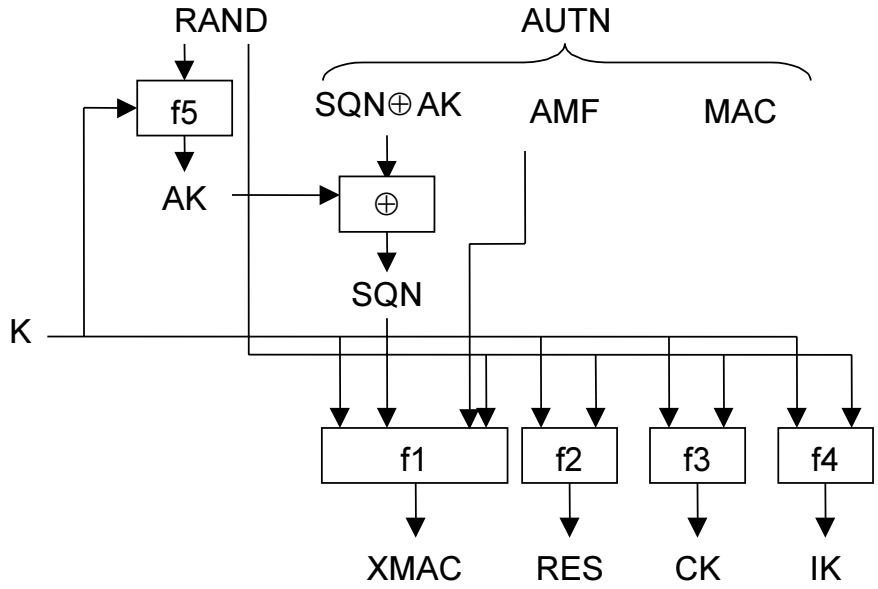
(Source [3GPP00a])

Generation of UMTS Authentication Vectors (2)

- The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND
  - For each user the HE/AuC keeps track of a counter SQN_{HE}
- An authentication and key management field AMF is included in the authentication token of each authentication vector
- Subsequently the following values are computed:
  - a message authentication code MAC = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function
  - an expected response XRES = $f2_K$(RAND) where f2 is a (possibly truncated) message authentication function
  - a cipher key CK = $f3_K$(RAND) where f3 is a key generating function
  - an integrity key IK = $f4_K$(RAND) where f4 is a key generating function;
  - an anonymity key AK = $f5_K$(RAND) where f5 is a key generating function
- Finally the authentication token AUTN = SQN ⊕ AK || AMF || MAC is constructed.



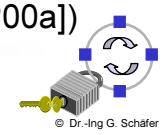
UMTS User Authentication Function in the USIM (1)



Verify MAC = XMAC

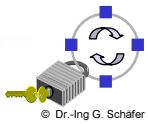
Verify that SQN is in the correct range

(Source [3GPP00a])



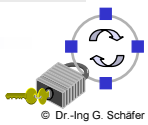
UMTS User Authentication Function in the USIM (2)

- Upon receipt of RAND and AUTN the USIM:
  - computes the anonymity key AK = $f5_K$ (RAND)
  - retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK
  - computes XMAC = $f1_K$ (SQN || RAND || AMF) and
  - compares this with MAC which is included in AUTN.
  - If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure.
  - If the MAC is correct, the USIM verifies that the received sequence number SQN is in the correct range:
    - If the sequence number is not in the correct range, the USIM sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure
  - If the sequence number is in the correct range, the USIM computes:
    - the authentication response RES = $f2_K$(RAND)
    - the cipher key CK = $f3_K$(RAND) and the integrity key IK = $f4_K$(RAND).



Conclusions on Network Access Security in UMTS

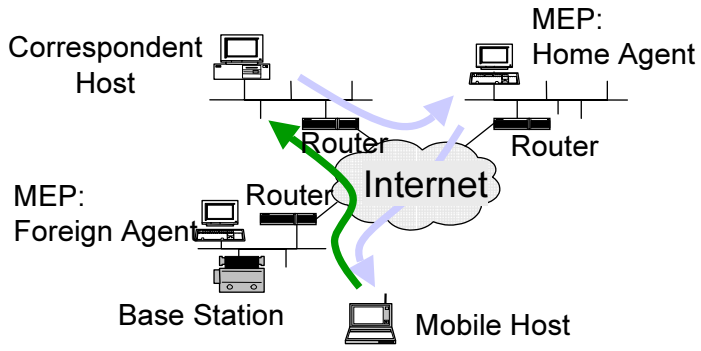
- UMTS network access security is quite similar to GSM security:
  - The home AUC generates challenge-response vectors
  - The challenge-response vectors are transmitted unprotected via the signaling network to a visited network that needs to check the authenticity of a mobile
  - Unlike in GSM, the network also authenticates itself to the mobile
  - The IMSI which uniquely identifies a user:
    - is still revealed to the visited network
    - can still be demanded by an attacker which impersonates a base station, as there is no network authentication in this case!
  - The security model still assumes trust between all network operators
  - Confidentiality is only provided on the radio link
- Concluding, without the currently lacking network domain security UMTS is designed to be just as secure as an *insecure* fixed network



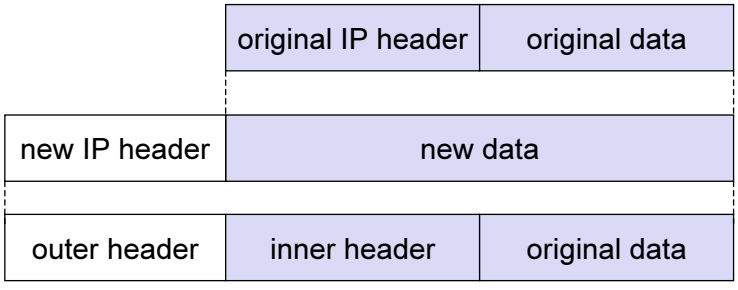
Mobile Internet Communications

- General IP mobility problem:
  - Classical IP-based protocols assume stationary hosts
  - IP address reflects identity and location
  - When hosts become mobile: active network sessions are disrupted
- No „user mobility“-concept in Internet as it is common in e.g. GSM

Mobile IP:
Indirect routing
and tunneling



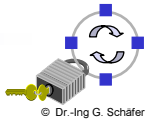
Mobile IP: Encapsulation



- Encapsulation of one packet into another as payload:
  - E.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
  - For Mobile IP: IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Routing Encapsulation)
  - Mostly used: IP-in-IP tunnel between HA and COA

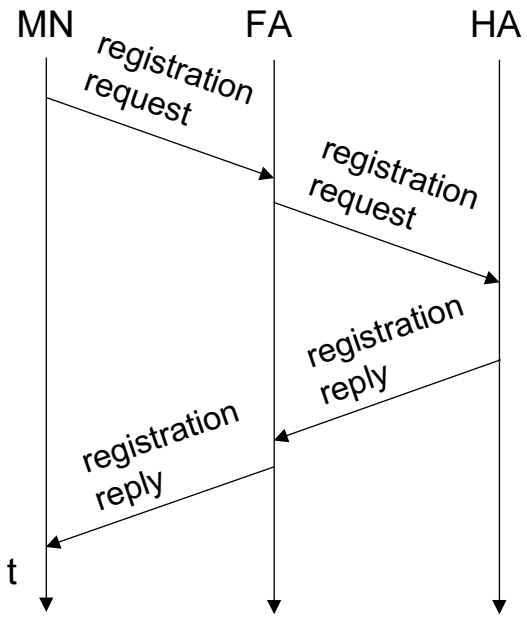
Network Integration of a Mobile Node

- Agent Advertisement:
  - HA and FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
  - MN reads a COA from the FA advertisement messages
- Registration (always limited lifetime!):
  - MN signals COA to the HA via the FA, HA acknowledges via FA to MN
  - This procedure has to be secured by authentication
- Advertisement:
  - HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
  - Routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - Packets to the MN are sent to the HA,
  - Independent of changes in COA/FA

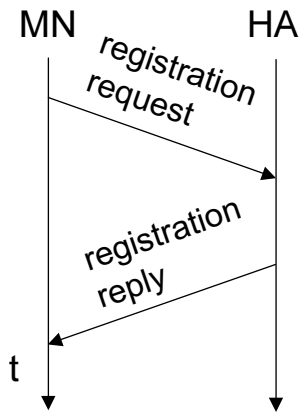


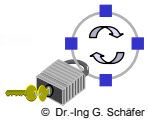
Mobile IP Registration

Registration in a Foreign Network



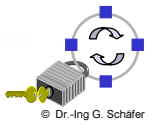
Registration in the Home Network



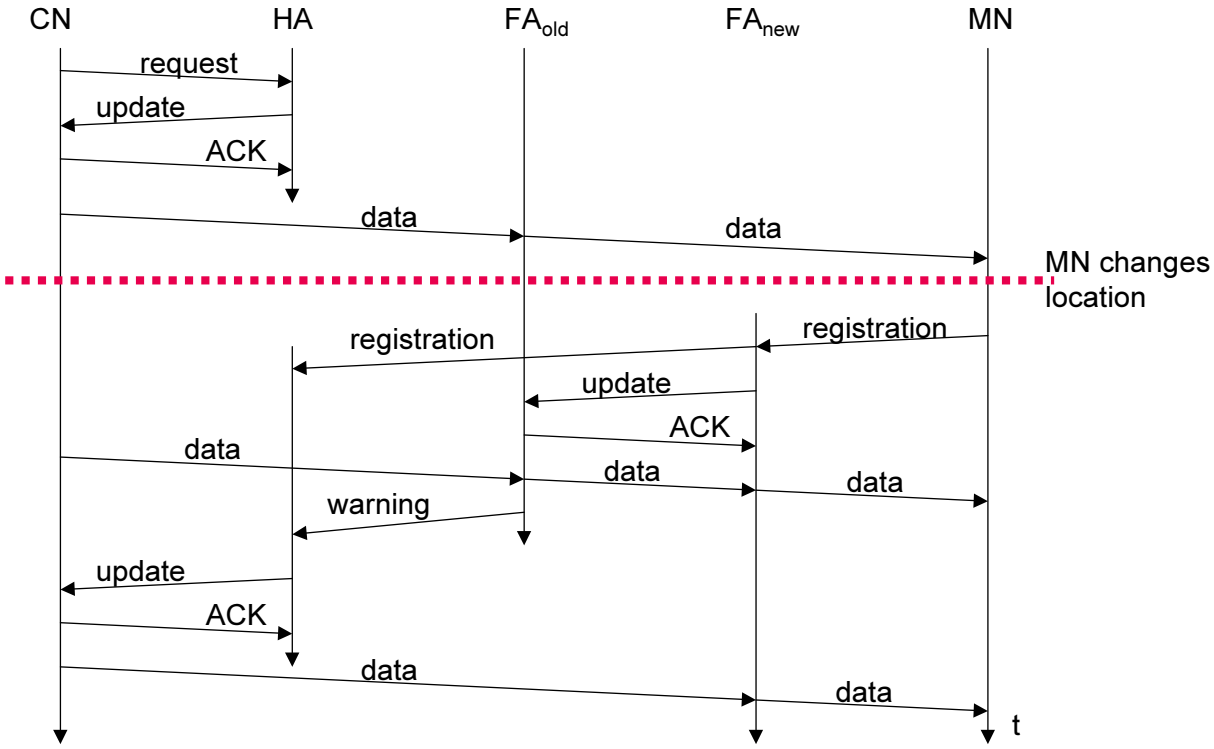


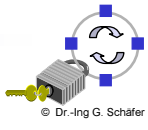
Optimization of Packet Forwarding

- Triangular routing of standard Mobile IP:
  - Sender sends all packets via HA to MN
  - Higher latency and network load
- One proposed solution, *route optimization for Mobile IP* [Perkins00a]:
  - Sender learns the current location of MN from HA *(binding update)*
  - Direct tunneling to this location
- Change of FA:
  - Packets on-the-fly during the change can be lost
  - New FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  - This information also enables the old FA to release resources for the MN
- Security problems:
  - Tunnel hijacking: binding updates to CNs are not authenticated
  - Location privacy: route optimization reveals the MN's current location
    - However, it can be configured to which CNs the COA is revealed



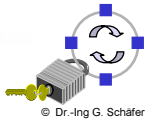
Route Optimization: Change of Foreign Agent





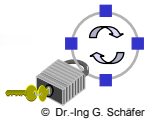
Mobile IP with Reverse Tunneling

- Routers accept often only “topological correct“ addresses (e.g. firewalls):
  - Standard Mobile IP lets MNs send their packets with their home address
- Furthermore, there exist some multicast and TTL problems (TTL in the home network correct, but MN is to far away from the receiver)
- *Reverse tunneling for Mobile IP* [RFC3024] addresses these problems:
  - 1. MN sends to FA
    2. FA tunnels packets to HA by encapsulation
    3. HA forwards the packet to the receiver (standard case)
  - This extension can be implemented easily and co-operates with current implementations without reverse tunneling
- However, reverse tunneling does not solve:
  - Further problems with *firewalls:* the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  - Optimization of data paths: this gets even worse, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

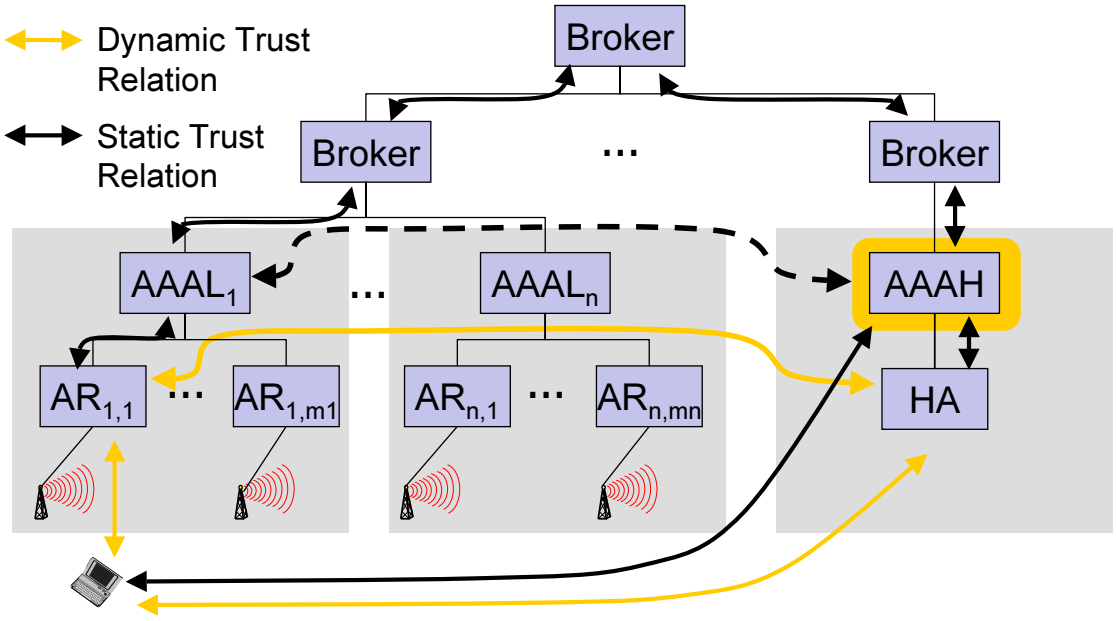


Authentication for Mobile IP Access (1)

- Motivations for different authentication relations:
  - Authentication between MN and home network:
    - Basically serves to counter hijacking attacks
  - Authentication between MN and visited network:
    - Control access to network resources
    - Secure accounting of resource usage
  - Authentication between visited network and home network:
    - Control which MN may use network resources
    - Secure accounting of resource usage
    - Control which networks may be accessed by an MN
- Standard Mobile IP does not include sufficient means to provide authentication and key management for truly mobile Internet access:
  - IETF is currently defining interaction with an *authentication, authorization & accounting (AAA)* infrastructure [RFC2977]

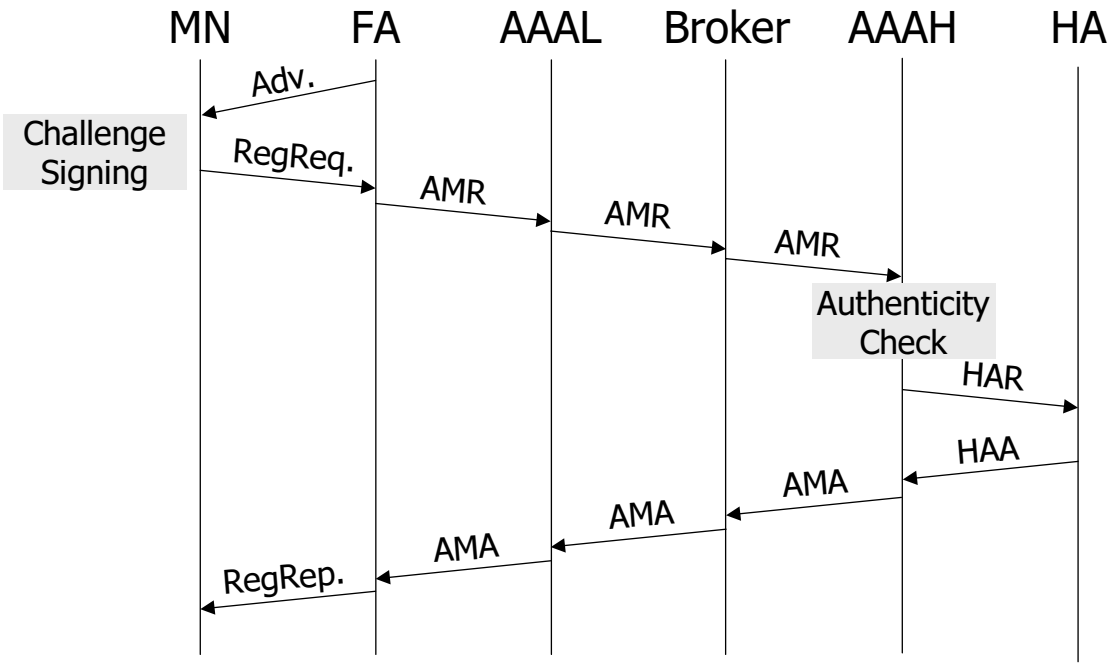


Authentication With Help of an AAA Infrastructure



The AAA-server in the home network (AAAH) generates the keys for dynamic trust relationships

Authentication with AAA Infrastructure (1)



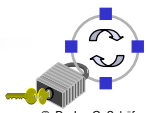
Signaling Security and Protection on Wireless Link

- Two main security needs have to be distinguished:
  - Security of the signaling procedures upon handover
  - Security of data exchanged over wireless link (including user data)
- Available “standard solutions”:
  - Layer 2: WEP (insecure), L2TP, PPTP
  - Layer 3: IPSec with Internet Key Exchange (IKE)
  - Layer 4:Transport Layer Security (at least for signaling security)
- Problems of standard solutions:
  - Overhead of additional tunneling (Layer 2 & 3 solutions)
  - Re-establishment time for context between the mobile node and a new access router
  - “Sequential process” (handover, security negotiation, QoS establishment) does not allow to make handover dependent on QoS-availability

→ The idea of building an optimized handover procedure with the existing standard protocols for fixed networks is as realistic as going into an ironmongery shop to buy the parts for constructing a new racing car

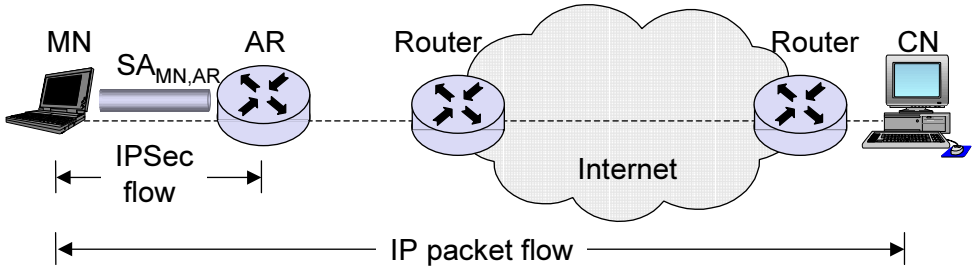
Security for the Wireless Link Example: IPSec (1)

- Confidentiality, data integrity and replay protection is required for data transmitted over the wireless link
- Two alternatives:
  - Technology-specific security protocol in data link layer
  - IP Security Architecture IPSec
- Base concepts for IPSec deployment:
  - Unidirectional security associations (SA)
  - Tunneling (e.g. in Encapsulating Security Payload, ESP)
  - Local security policy database (SPD) to decide which traffic should be protected in which manner
  - Security association database (SADB) for storing active SAs
  - However, use of standardized key management protocol IKE (with many options requiring expensive processing) would result in poor performance



Security for the Wireless Link Example: IPSec (2)

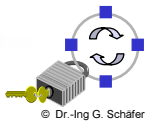
- Tunnel Mode is generally used when at least one cryptographic end-point is not a communication end-point:



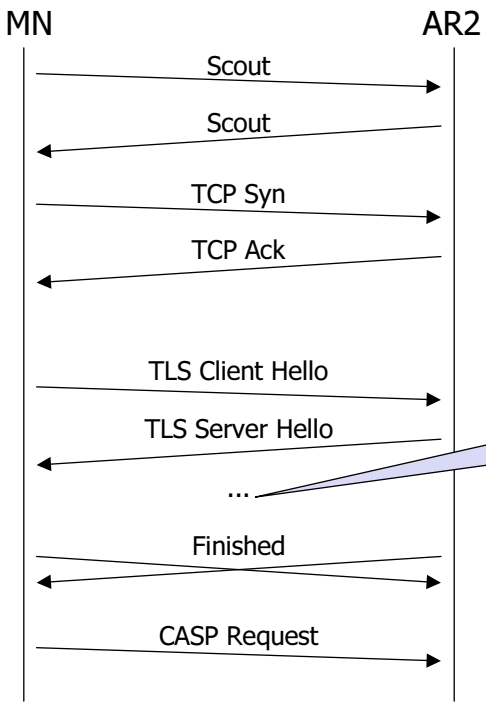
IPSec packet structure

- Example: Deployment of ESP-Tunnels between MN and AR

IP header	IPSec header	IP header	protected data
Src = MN Dst = AR		Src = MN Dst = CN	



Security for HO Signaling Example: CASP QoS Client

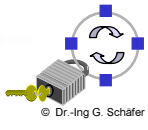


- CASP is a standard "Cross Application Signaling Protocol"
- Message flow with detection of next CASP node via "Scout"
- Establishment of TCP connections
- TLS connection establishment with 4-6 message exchanges

Two more TLS messages may be required, if TLS session can not be resumed

→ Requires 8 or 10 messages to be exchanged before CASP Request can be send

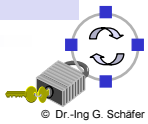
→ Does not allow to make handover dependent on QoS



Summary: Challenges of Mobile Internet Communications

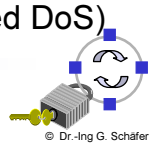
- Fast handover with efficient:
  - Authentication,
  - Authorization, and
  - QoS re-establishment (allowing to make HO dependent on QoS-availability)
- Efficient technical solution that reconciles:
  - Authentication requirements for billing purposes
  - Privacy requirements that demand for:
    - privacy preserving registration and handover handling
    - privacy preserving routing of data packets
  - Law enforcement requirements (political discussion put aside)
  - Effective wireless link security (i.e. no IEEE 802.11 WEP!)
- Coordinating performance enhancing proxies with e2e-security

→ Current approaches like HMIP, HMIPv6, AAA, RSVP, CASP, IPSec, TLS, etc. do not fulfill these requirements



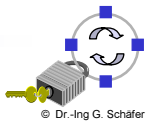
Challenges of Convergence: Denial of Service (1)

- Denial of Service (DoS) attacks aim at denying or degrading legitimate users' access to a service or network resource, or at bringing down the servers offering such services itself
- Attacking Techniques:
  - Disabling services:
    - Hacking into systems
    - Making use of implementation weaknesses as buffer overrun
    - Deviation from proper protocol execution
  - Resource depletion by causing:
    - Expensive computations ("expensive cryptography"!)
    - Storage of (useless) state information
    - High traffic load (requires high overall bandwidth from attacker)
    - Resource reservations that are never used (e.g. bandwidth)
  - Origin of malicious traffic:
    - Single source with single / multiple (forged) source addresses
    - Multiple sources with forged / valid source addresses (Distributed DoS)



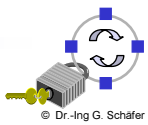
Challenges of Convergence : Denial of Service (2)

- New Risks:
  - The introduction of Internet protocols in classical and mobile telecommunication networks also introduces the Internet's DoS vulnerabilities to these networks
  - Programmable end-devices (PDAs, smart phones) may constitute a large base of possible slave nodes for DDoS attacks on mobile networks
  - Software defined radio implementation may even allow new attacking techniques:
    - Hacked smart phones answer to arbitrary paging requests
    - Unfair / malicious MAC protocol behavior
  - The ongoing integration of communications and automation may enable completely new DoS threats
- Protocol engineering needs to address DoS-resistance:
  - Network protocol functions and architecture will have to be (re-)designed with the general risk of DoS in mind
  - Base techniques: stateless protocol design, cryptographic measures like authentication, cookies, client puzzles, etc.



Conclusions

- Mobile communication faces the same threats as fixed network communications with some increased risks, new difficulties and a new threat (location tracking)
- GSM / GPRS / UMTS networks up to now address only security threats of the air interface, and are, therefore, just designed to be as secure as an insecure fixed networks (in fact there are also some problems as active IMSI catching, etc.)
- Mobile Internet communications still poses many engineering challenges (not only but also in the area of security)
  - Pure combination of "standard" solutions (for fixed networks) is not likely to produce adequate results
- With the introduction of Internet protocols to mobile communication networks and increased terminal intelligence DoS attacks are emerging as a major challenge for mobile communications protocols



Additional References (1)

[Amo94] E. G. Amorosi. *Fundamentals of Computer Security Technology.* Prentice Hall. 1994.

[For94b] Warwick Ford. *Computer Communications Security - Principles, Standard Protocols and Techniques.* Prentice Hall. 1994.

[Gar96] Simson Garfinkel and Gene Spafford. *Practical Internet & Unix Security.* O'Reilly, 1996.

[Men97a] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and Its Applications, Hardcover, 816 pages, CRC Press, 1997.

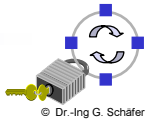
[Müller99a] G. Müller, K. Rannenberg (Ed.). *Multilateral Security in Communications.* Addison-Wesley-Longman, 1999.

[Sch96] B. Schneier. *Applied Cryptography Second Edition: Protocols, Algorithms and Source Code in C.* John Wiley & Sons, 1996.

[Sch02a] J. Schiller. *Mobile Communications - The Course.* http://www.inf.fu-berlin.de/inst/ag-tech/resources/mobile_communications.htm

[Sch03a] G. Schäfer. *Netzsicherheit - Algorithmische Grundlagen und Protokolle.* dpunkt.verlag, 2003.

[Sta98a] W. Stallings. *Cryptography and Network Security: Principles and Practice.* Hardcover, 569 pages, Prentice Hall, 2nd ed, 1998.



Additional References (2)

[3GPP00a] 3GPP. *3G Security: Security Architecture (Release 1999).* 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3GPP TS 33.102, V3.6.0, October 2000.

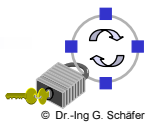
[3GPP02a] 3GPP. *3G Security: Security Architecture (Release 5).* 3GPP TS 33.102, V5.0.0, June 2002.

[3GPP02b] 3GPP. *Security Mechanisms for the (U)SIM application toolkit; Stage 2.* 3GPP TS 23.048, V5.5.0, December 2002.

[ETSI93a] ETSI TC-GSM. *GSM Security Aspects (GSM 02.09).* Recommendation GSM 02.09, Version 3.1.0, European Telecommunications Standards Institute (ETSI), June 1993.

[ETSI94a] ETSI TC-SMG. *European Digital Cellular Telecommunications System (Phase 2): Security Related Network Functions (GSM 03.20).* ETS 300 534, European Telecommunications Standards Institute (ETSI), September 1994.

[Les02a] Lescuyer, P. *UMTS – Grundlagen, Architektur und Standard.* dpunkt.verlag, 2002.



Additional References (3)

[Perkins00a] C. Perkins, D. B. Johnson. *Route Optimization in Mobile IP.* Internet Draft draft-ietf-mobileip-optim-10.txt (work in progress), 2000.

[RFC2002] C. Perkins. *IP Mobility Support.* Internet RFC 2002, obsoleted by RFC 3220, 1996.

[RFC2977] S. Glass, T. Hiller, S. Jacobs, C. Perkins. *Mobile IP Authentication, Authorization, and Accounting Requirements.* Internet RFC 2977, 2000.

[RFC3024] G. Montenegro. *Reverse Tunneling for Mobile IP, revised.* RFC 3024, 2001.

[RFC3220] C. Perkins. *IP Mobility Support, revised.* Internet RFC 3220, 2002.