Security Issues in Mobile Communication Systems

N. Asokan

Nokia Research Center

IAB workshop on wireless internetworking

February 29 - March 2, 2000

What is different about wireless networks?

- Low bandwidth
  - minimize message sizes, number of messages
- Increased risk of eavesdropping
  - use link-level encryption ("wired equivalency")
- Also wireless networks typically imply **user/device mobility**
  - Security issues related to mobility
    - authentication
    - charging
    - privacy
  - Focus of this presentation

Overview

- Brief overview of how GSM and 3GPP/UMTS address these issues
- Potential additional security concerns in the "wireless Internet"
- Ways to address these concerns, and their implications

GSM/GPRS security

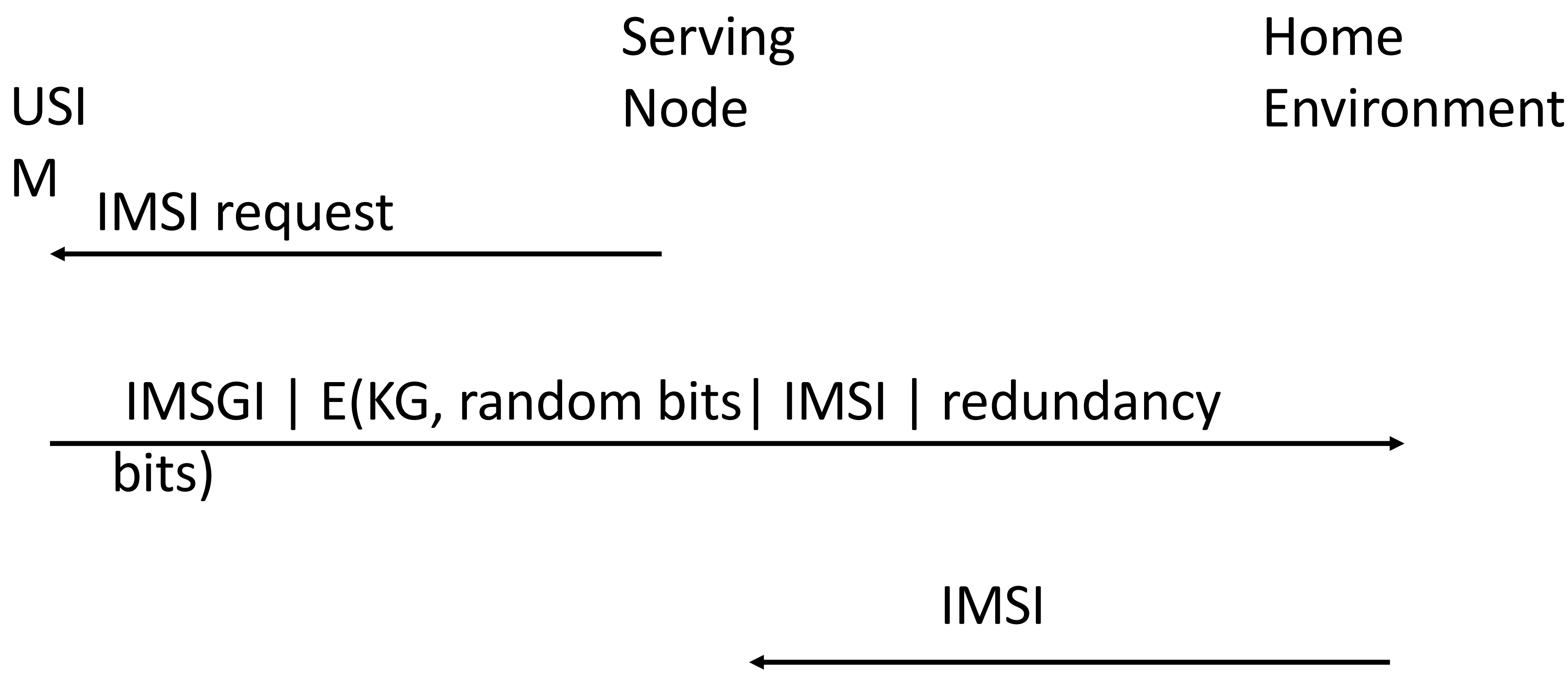
- Authentication
  - one-way authentication based on long-term shared key between user's SIM card and the home network
- Charging
  - network operator is trusted to charge correctly; based on user authentication
- Privacy
  - data
    - link-level encryption over the air; no protection in the core network
  - identity/location/movements, unlinkability
    - use of temporary identifiers (TMSI) reduce the ability of an eavedropper to track movements within a PLMN
    - but network can ask the mobile to send its real identity (IMSI): on synchronization failure, on database failure, or on entering a new PLMN
    - network can also page for mobiles using IMSI

3GPP/UMTS enhancements (current status)

- Authentication
  - support for mutual authentication
- Charging
  - same as in GSM
- Privacy
  - data
    - some support for securing core network signaling data
    - increased key sizes
  - identity/location/movements, unlinkability
    - enhanced user identity confidentiality using "group keys"
    - a group key is shared by a group of users
- Other improvements
  - integrity of signaling, cryptographic algorithms made public

Enhanced user identity confidentiality

- IMSI is not sent in clear. Instead, it is encrypted by a static group key KG and the group identity IMSGI is sent in clear.

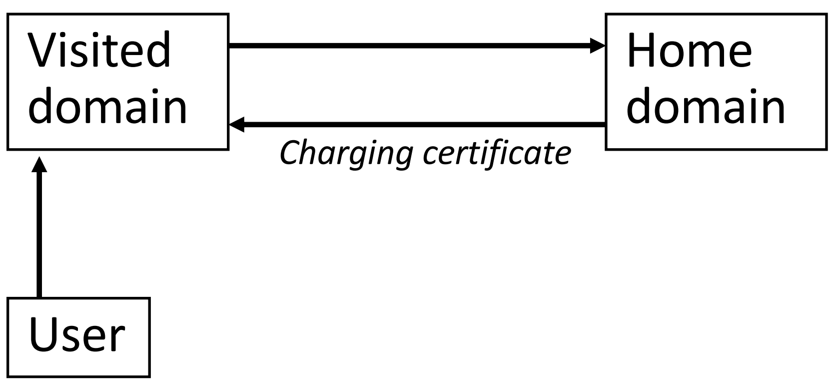


What is different in the wireless Internet?

- Potentially low cost of entry for ISPs supporting mobile access
- Consequently, old trust assumptions as in cellular networks may not hold here
  - between user and home ISP
  - between user and visited ISP
  - between ISPs
- Implications: potential need for
  - incontestable charging
  - increased level of privacy
- Relevant even in cellular networks?

Incontestable charging

- Required security service: unforgeability
- Cannot be provided if symmetric key cryptography is used exclusively
  - hybrid methods may be used (e.g., based on hash chains)
- Authorization protocol must support some notion of a "charging certificate"
  - used for local verification of subsequent authorization messages



Enhanced privacy

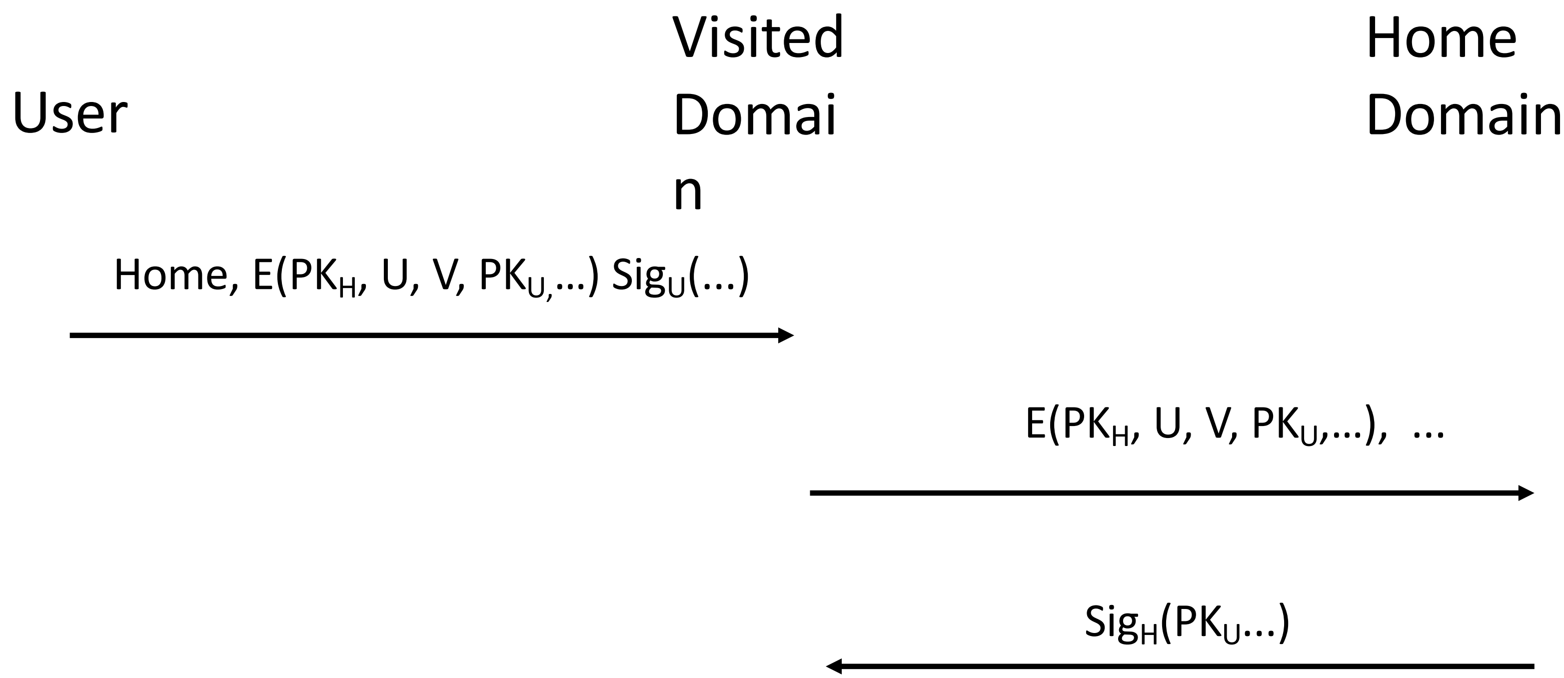
- Stronger levels or privacy
  - temporary id = home-domain, E(K, random bits| real-id)
  - using public key encryption
    - K is the public encryption key of the home-domain
  - using opaque tokens
    - K is a symmetric encryption key known only to the home-domain
    - tokens are opaque to the mobile user
    - user requires means of obtaining new tokens
  - no danger of loss of synchronization
- Identity privacy without unlinkability is often not useful
  - static identities allow profiles to be built up over time
  - encryption of identity using a shared key is unsatisfactory: trades off performance vs. level of unlinkability

NOKIA

Enhanced privacy (contd.)

- Release information on a need-to-know basis: e.g., does the visited domain need to know the real identity?
  - typically, the visited domain cares about being paid
  - *ground rule:* stress authorization not authentication
  - require authentication only where necessary (e.g., home agent forwarding service in Mobile IP)

An example protocol template



- unforgeable registration request
- real identity not revealed to the visited domain

NOKIA

Implications

- Public-key cryptography can provide effective solutions
  - increased message sizes: use of elliptic curve cryptography can help
  - lack of PKI: enhanced privacy solution does not require a full-fledged PKI, some sort of infrastructure is required for charging anyway
- Are these problems serious enough?
  - trust assumption may not change so drastically
  - providing true privacy is hard: hiding identity information is irrelevant as long as some other linkable information is associated with the messages
  - try not to preclude future solution
    - e.g., don’t insist on authentication when it is not essential
  - provide hooks for future use
    - e.g., 16-bit length fields to ensure sufficient room in message formats

Summary

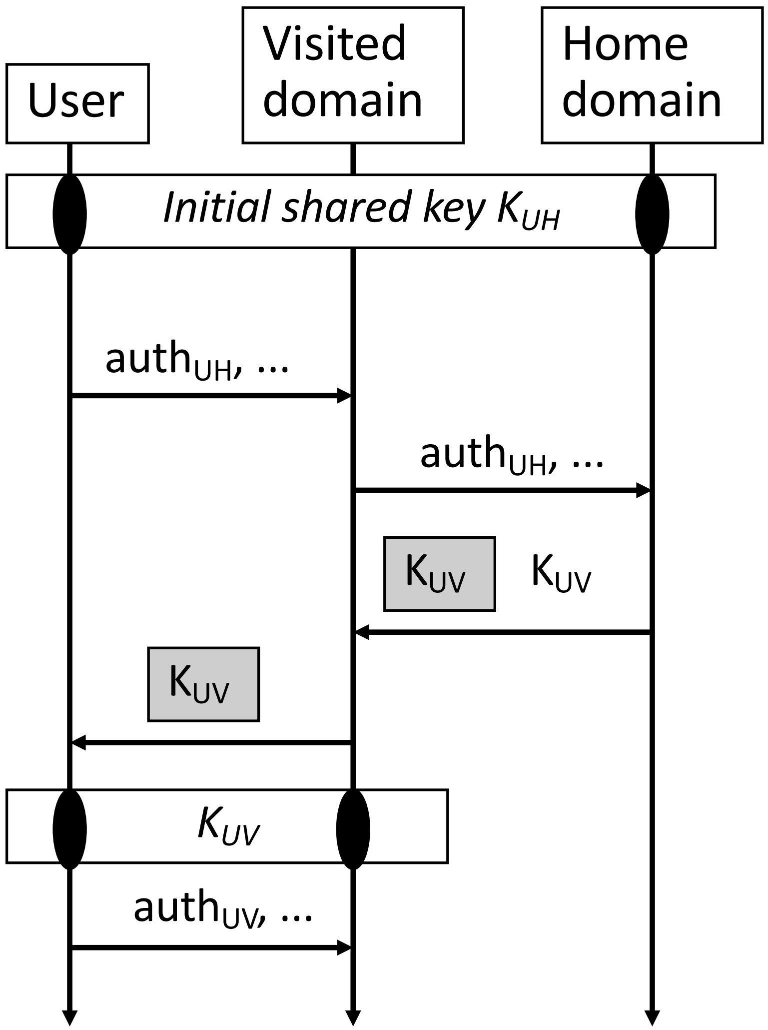
- Trust assumptions are different in the Internet
- Enhanced levels of security services may be necessary
- Public-key cryptography can provide effective solutions
- Try not to preclude future provision of improved security services

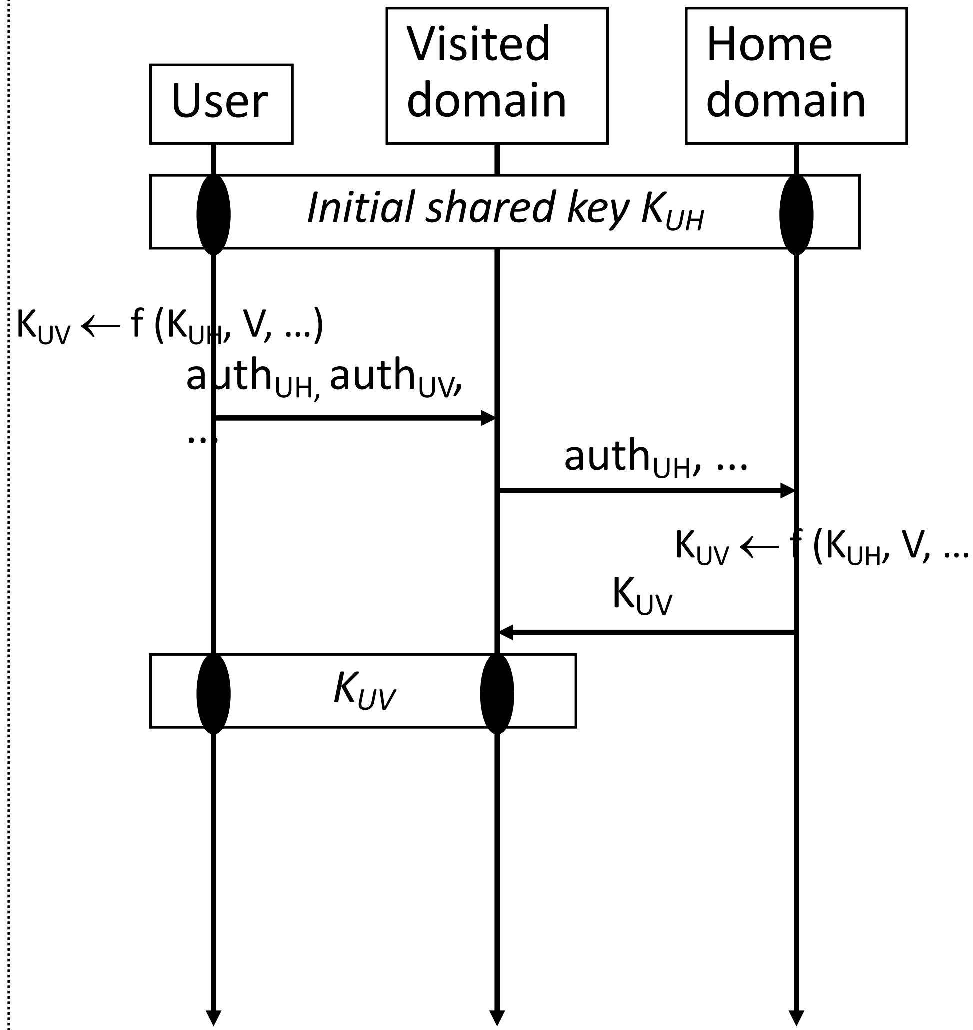
NOKIA

End of presentation

- Additional slides follow

Reducing number of messages





Elliptic curve cryptosystems

- Comparison between discrete log based systems of equivalent strength in different groups
  - DSA: system parameters = 2208 bits, public key = 1024 bits, private key = 160 bits, signature size = 320 bits
  - ECDSA: system parameters = 481 bits, public key = 161 bits, private key = 160 bits, signature size = 160 bits
- Comparison between EC and RSA of "equivalent strength"
  - RSA: public key = 1088 bits, private key = 2048 bits, signature size = 1024 bits
- (taken from Certicom's white papers)

NOKIA