# T-79.159
# Cryptography and Data Security

Kaisa Nyberg, professor

Johan Wallén, assistant

## General

- http://www.tcs.hut.fi/Studies/T-79.159/
- Course agenda (check dates!)
  - 12 lectures á 2 hours, Wed 8-10, Fri 14-16
  - 6 homework sessions, two groups: Tue or Fri
- 3 credits, requirements: Exam (max 30 pts)
- The first exam: Monday, May 16, 2005 at 13-16 in T1
- 0 - 6 pts credit from homework
- Alternative to T-110.470 Salausjärjestelmät

# Useful books

- *Network Security, Private Communication in a Public World*, by C. Kaufman, Radia Perlman, Mike Speciner. Second edition, Prentice Hall 2002, ISBN 0-13-046019-2
- *Cryptography and Network Security, Principles and Practices*, by W. Stallings. Third edition, Pearson Education 2003, ISBN 0-13-091429-0
- *UMTS Security,* by V. Niemi and K. Nyberg, Wiley 2002, ISBN 0-470-84794-8

# Contents

- Introduction to data security
- Classical cryptosystems
- Introduction to modern cryptography
- Block ciphers: DES, IDEA, AES
- Stream ciphers: RC4, 3gpp f8
- Block cipher modes of operation
- Hash-functions and MACs
- Mathematical tools: Modular arithmetic, Euclid’s algorithm, Chinese Remainder Theorem, Euler’s totient function, Euler’s theorem
- Public key cryptosystems: RSA
- Prime number generation
- Polynomial arithmetic
- Public key cryptosystems: Diffie-Hellman, El Gamal, DSS
- Authentication and Digital signatures
- Random number generation
- Authentication and key agreement protocols in practise: PGP, SSL/TLS, IPSEC, IKEv2 and EAP

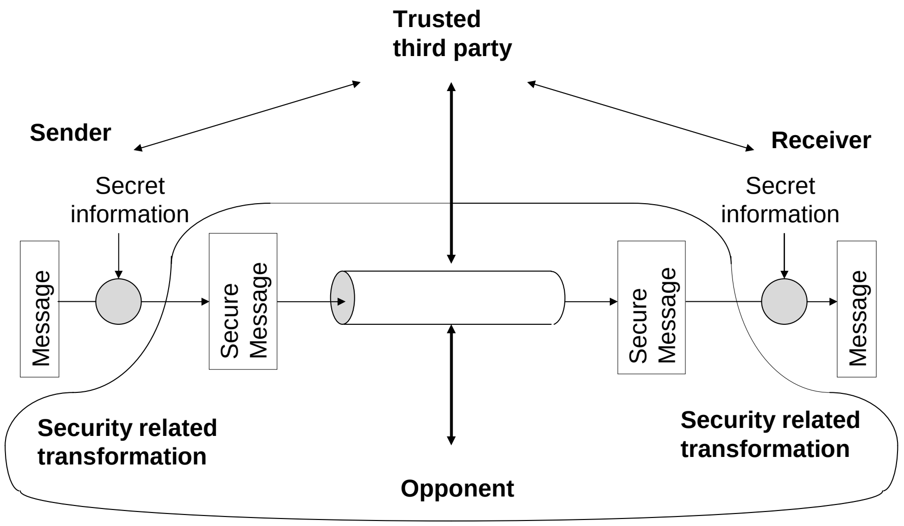
# Lecture 1:
# Introduction to data security

- General security principles
- Communication security
- Design of a secure system
- Example: GSM security

# What is Security?

- Security is an abstract concept
- Security is about protection methods against deliberate misbehaving actions
- Security in not fault-tolerance and robustness
- There is a division between physical security and information security.
- Physical security
  - locked rooms, safes and guards
  - tamper-resistance
  - proximity
  - biometric protection

# Model for network security



Trusted third party

Sender

Receiver

Secret information

Message

Secure Message

Secure Message

Secret information

Message

Security related transformation

Security related transformation

Opponent

# Threat model

- Another way of defining security
  - First perform threat analysis: cababilities of an attacker, possible attack scenarios
  - Security can then be defined in terms of combating the perceived threats
  - Not all threats are worth of combatting
- Dolev-Yao attacker model against cryptographic protocols: An attacker
  - Is a legitimate user of the network, and hence able to correspond with any other user
  - Can send messages to another user by impersonating any other user
  - Can receive messages intended to any other user

# Computer and Communication Layers Security

System level security

- "The system is as strong as its weakest link."

Application security

- e.g. banking applications over Internet use security mechanisms which are tailored to meet their specific requirements.

Protocol level security

- well-defined communication steps in certain well-defined order.

Operating system security

- the behaviour of all elements in a network depends on the correct functionality of the operating system that controls them.

Platform security

- properties of the computing platform, e.g. protected memory space.

Security primitives

- these are the basic building blocks, e.g. cryptographic algorithms.

# Design of a Secure System

Threat analysis

- What are the threats?

Risk analysis

- What is the potential damage each threat potentially can cause?

Trust model

- Whom and what can be trusted?

Requirements capture

- What kind of protection is required? What kind of protection is possible within the trust model?

Design phase

- Protection mechanism are designed in order to meet the requirements.
- Building blocks, e.g. security protocols or primitives are identified, possibly new mechanisms are created, and a security architecture is built.

Security analysis

- Evaluation of the design independently of the previous phase.

Reaction phase

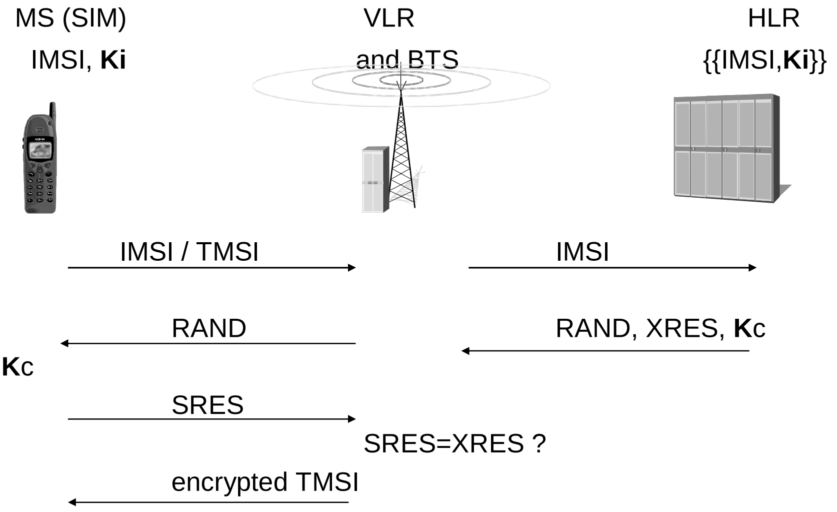
- Reaction to expected security breaches and survival plan.

# Example: GSM Security

Main features

- Authentication of the user
  - correct billing
- Encryption of communication in radio interface
  - confidentiality of user and control data
  - call integrity
- Use of temporary identities
  - user privacy
  - location privacy

# GSM Authentication



MS (SIM)
IMSI, **Ki**

VLR
and BTS

HLR
{{IMSI,**Ki**}}

IMSI / TMSI

IMSI

RAND

RAND, XRES, **K**c

**K**c

SRES

SRES=XRES ?

encrypted TMSI

# Criticism

Active attacks

- this refers to somebody who has the required equipment to masquerade as a legitimate network element and/or legitimate user terminal

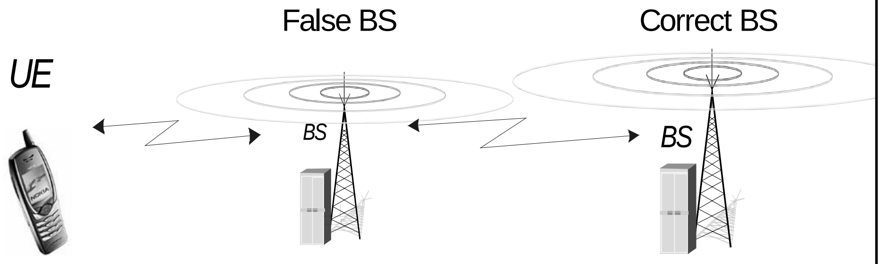
Missing or weak protection between networks

- control data, e.g. *keys* used for radio interface ciphering, are sometimes sent unprotected between different networks

Secret design

- some essential parts of the security architecture are kept secret, e.g. the cryptographic algorithms

# Active Attack



# Barkan–Biham-Keller Attack (2003)

Exploits weaknesses in cryptographic algorithms:

- A5/2 can be instantly broken

… AND other fundamental flaws in the GSM security system:

- A5/2 mandatory feature in handsets
- Call integrity based on an (weak) encryption algorithm
- The same Kc is used in different algorithms
- Attacker can force the victim MS to use the same Kc by RAND replay

Two types of attacks:

1. Decryption of encrypted call using ciphertext only
   - Catch a RAND and record the call encrypted with Kc and A5/3
   - Replay the RAND and tell the MS to use A5/2
   - Analyse Kc from the received encrypted uplink signal
2. Call hi-jacking
   - Relay RAND to victim MS and tell it to use A5/2
   - Analyse Kc from the received signal encrypted by the victim MS
   - Take Kc into use and insert your own call on the line

# Proposed Countermeasure

Amendment to the GSM security architecture: Special RANDs

- RAND is the only variable information sent from Home to MS in the authentication
- Divide the space of all 128-bit RANDs into different classes with respect to which encryption algorithm is allowed to be used with the Kc derived from this RAND.
- 32-bit flag to indicate to the MS that a special RAND is in use
- 16-bits to indicate which algorithms out of 8 GSM (and ECSD) and 8 GPRS encryption algorithms are allowed to be used with the key derived from this special RAND
- Effective RAND reduced from 128 bits to 80 bits. Remains to be judged if acceptable.
- Special RANDs trigged by the visited network identity. Requires careful configuration in the HLR/AuC.
- Solution assumes that HLR gets the correct VLR identifier.