ETSI Future Security Workshop:
the risks, threats and opportunities

Smart Cards

Dr. Klaus Vedder

Chairman ETSI TC Smart Card Platform (TC SCP)
Executive VP, Giesecke & Devrient
ETSI TC  

**Smart Card Platform**

- **18 Years of Dedication and Real-life Experience**
  - founded in March 2000 as the successor of SMG9, the SIM-people, which specified the SIM for GSM, the most successful smart card application with more than 1.6 billion subscribers and 4 billion SIMs deployed

- **The Mission**
  - create a series of specifications for a smart card platform, based on real-life (outside) requirements, on which other bodies can base their system specific applications to achieve compatibility between all applications resident on the smart card
The SIM

"A SIM is the physically secured module which contains the IMSI, an authentication algorithm, the authentication key and other (security related) information and functions. The basic function of the SIM is to authenticate the subscriber identity in order to prevent misuse of the MS (Mobile Station) and the network."

From the report of SIMEG#1 in January 1988
The SIM in 1988

The ID-1 card used by Deutsche Telekom in their analogue network

Option 1: "IC card"

Option 2: "Fixed"
Software SIM fully incorporated into the handset OS
Rejected due to security concerns and less flexibility

Option 3: "Removable"
24 pin DIL with 8 pins connected vs 24 pin DIL with 8 pins connected
The SIM - A Removable Security Module

GSM System Requirement:
To provide the same level of security as the fixed network

- The SIM: Providing the security
  - issuer specific algorithm for cipher key generation
  - security management specified by issuer
  - issuer specific authentication algorithm

- The SIM: Providing universal plastic roaming
  - keeping your identity when changing terminal or technology

- The SIM: Freeing the mobile of the burden of the subscription
  - terminal does not contain any subscription data
  - creating a global terminal market
  - bigger choice for the customer through more competition
GSM Authentication and Cipher Key Generation

User

Radio Interface

Network

PIN Check

IMSI/TMSI

HLR/AuC

Ki

A3/A8

RAND

A5

BSS

SRES

Ki 128 Bits

RAND 128 Bits

Kc 64 Bits

SRES 32 Bits

Ki

A3/A8

Kc

A3/A8

Kc

Match ?
SIM Security Today

- **The SIM has successfully stood the test of time**
  - as time goes by attacks become more sophisticated - so do the countermeasures
  - the mechanical check that a SIM is not removed was enhanced by an electrical/logical check in the very early days
  - verification of the PIN was made a pre-requisite to perform the authentication in 1993

- **1998: Comp 128-1 (A3/A8) successfully attacked**
  - black box attack against the GSM-MoU example algorithm
    - does not utilise any hardware or software property of the SIM
    - attack against just one card, not against the system itself
  - chosen plaintext-ciphertext attack
    - approximately 160,000 - 200,000 very specific challenges were then required to calculate the secret subscription specific key $K_i$
  - authentication counter with "automatic silencing" of the SIM is no longer a valid countermeasure
    - only 3,000 to 36,000 challenges to calculate $K_i$ needed now
copying tools for SIMs using COMP 128-1 are available on the Internet
www.chinatoysco.com package contains: smart card reader, PC SW, 10-in-1 SIM (80 $ US)

software only version for free download:
http://users.net.yu/~dejan
Module and Chip

- CPU, RAM, ROM, EEPROM, Flash on a single piece of silicon
- Structure today: ≤ 0.18 µm; metallised surface
- Sensors for Low Voltage, Frequency, Passivation Layer, Light, ….
A Smart Card Chip

Processor and Memory

1990
- 6 Bit CPU
- 7 kB ROM
- 3 kB EEPROM
- 128 Byte RAM

2006
- 32 Bit CPU
- 500 kB ROM
- 512 kB EEPROM
- 16 kB RAM
  or
- 400 kB Flash instead of ROM, EEPROM

In addition:
- 128 MB Flash
An Early Power Consumption Attack

Programming of non-volatile memory is a function of power consumption:

- Writing of the retry counter (EEPROM) can be monitored.
- Cutting off the power if the power increases during a PIN check.

![Graph showing power consumption over time with possible trigger points marked.](image-url)
Countermeasure PIN Attack

PIN Check Routine

Programming retry counter

Check PIN

PIN = PIN ref

yes

Write initial retry counter value

Process completed

no

Process aborted

PIN Check Routine

Check PIN

PIN = PIN ref

yes

no

Process aborted

Process completed

t = const

Programming retry counter

Programming dummy cell

Process completed
DFA and Timing Attacks

**DFA (Differential Fault Analysis)**
- Generating hardware faults during the execution of an algorithm
- Calculating the key by comparing correct and incorrect output data

**Countermeasures**
- A check sum over the key is calculated and checked after every execution of the cryptographic algorithm
- The results of the cryptographic algorithm is checked
  - DES: critical parts of the algorithm are calculated twice
  - RSA: check by using the correspondent public key
- Control counter to ensure the complete calculation of the algorithm

**Timing Attacks**
- Obtaining information about the secret key by measuring the execution time of a cryptographic algorithm

**Countermeasures**
- Symmetric algorithms: execution time is independent of data and key
- Asymmetric algorithms: the same execution time for squaring and multiplying or random execution time
SPA (Simple Power Analysis)

Obtaining information about the secret key by direct observation of the power consumption

Part of the key permutation (PC 2) in the DES
Differential Power Analysis (DPA)

Calculating the secret key from several hundreds of power consumption measurings using statistical methods

Straightforward Implementation

G&D Implementation with countermeasures

Correlation on output S-box with usage of the right key
From the SIM to the UICC

From a standardised application offering secure value added services to a true multi-application security platform providing the user with a wealth of opportunities.
The UICC – the Multi-application Platform

The UICC specifies generic (application independent) functions and features with a clear separation of lower layers and applications.

Specified by TC SCP

Fire walls between applications provided by smart card (USIM) supplier

USIM  SIM  (U)SAT  Phonebook  Public Transport  Electr. Purse  Ticketing  ID
The UICC

- The UICC provides a standardised security platform on which specific applications can be realised using today's interface to the outside world
  - Logical channels allow to run applications in parallel
  - Applications may share standardised security functions
  - Applications may have their own security functions and attributes (algorithms, (file) access conditions, …)

As long as an application uses only the functionality specified in the platform it will run on any terminal supporting all the platform

- A new high speed Megabit interface is about to be standardised and will allow to use the smart card for DRM, stream ciphering (Pay TV) and as a mass storage device

- A contactless interface will create a wealth of new opportunities
The Vision

To turn today's mobile phone into a multipurpose terminal, lifestyle tool, and personal security device by establishing a second, contactless communication channel

- turning the mobile phone into a "contactless card"
- using the true multi-application capabilities of the UICC
- combining applications on the card with the offerings of GSM and 3G networks
Cross-over Applications - The Contactless USIM

Mobile Phones
- High penetration
- Personal device
- Demand of new services

Contactless Cards
- Ease-of-use
- High level of convenience
- Infrastructure increasing

Phase I
Mobile phone as contactless card
- Transportation
- Corporate access
- Electronic purse
- Event tickets

Phase II
Mobile phone as contactless card reader
- Credit cards
- Electronic tickets
- ID documents

perfect match
Contactless Mobile Solutions

- Payment applications
  - Contactless payment transaction at supermarkets
  - Amount owed is deducted from purse on the UICC
  - Subscriber can access transaction history via handset

- Ticketing/Transportation applications
  - Ticket is stored electronically
  - Subscriber just holds handset up to reader
  - Additional tickets are paid for over-the-air

- Access applications
  - Contactless access to company premises
  - Subscriber just holds handset up to reader
  - Review access timestamp history via handset

The merging of contactless and mobile technology opens up a new channel of communication with a wide scope for additional applications.
What the SIM Does for the Operator

Acquire subscribers

- SIMs in time and volume
- Reliable deliveries
- Production on demand (stock management)

Increase ARPU

- Roaming assistance
- Large phonebooks
- Ringtone management
- Service + event promotions
- SMS management
- DRM for own services

Reduce OPEX

- Limit subscriber acquisition cost
- Secure authentication
- Anti fraud
- eVoucher to topup prepaid SIMs

Manage subscribers

- Service and handset tracking
- Customer relationship mgmt
- enhance customer care
- Phonebook synchronisation
- (POD for number portability)

Preserve revenues from other actors

- Mobile banking, mobile payment
- Co-branding the SIM
- DRM for other services

Profitability

ETSI Security WS
Sophia Antipolis
16-17 January 2006

# Subscribers

Standards for Business

Giesecke & Devrient
Dr. Klaus Vedder

Giesecke & Devrient GmbH
Prinzregentenstr. 159
81607 Munich
Germany

klaus.vedder@gi-de.com