SIM Card Security

Sheng He

Chair for Communication Security
Ruhr-University Bochum

Contents

- What is a SIM Card?
- Logical Model of the SIM
- Threats to SIM Data
- Security features
- The Future - USIM
- Conclusion

What is a SIM Card?

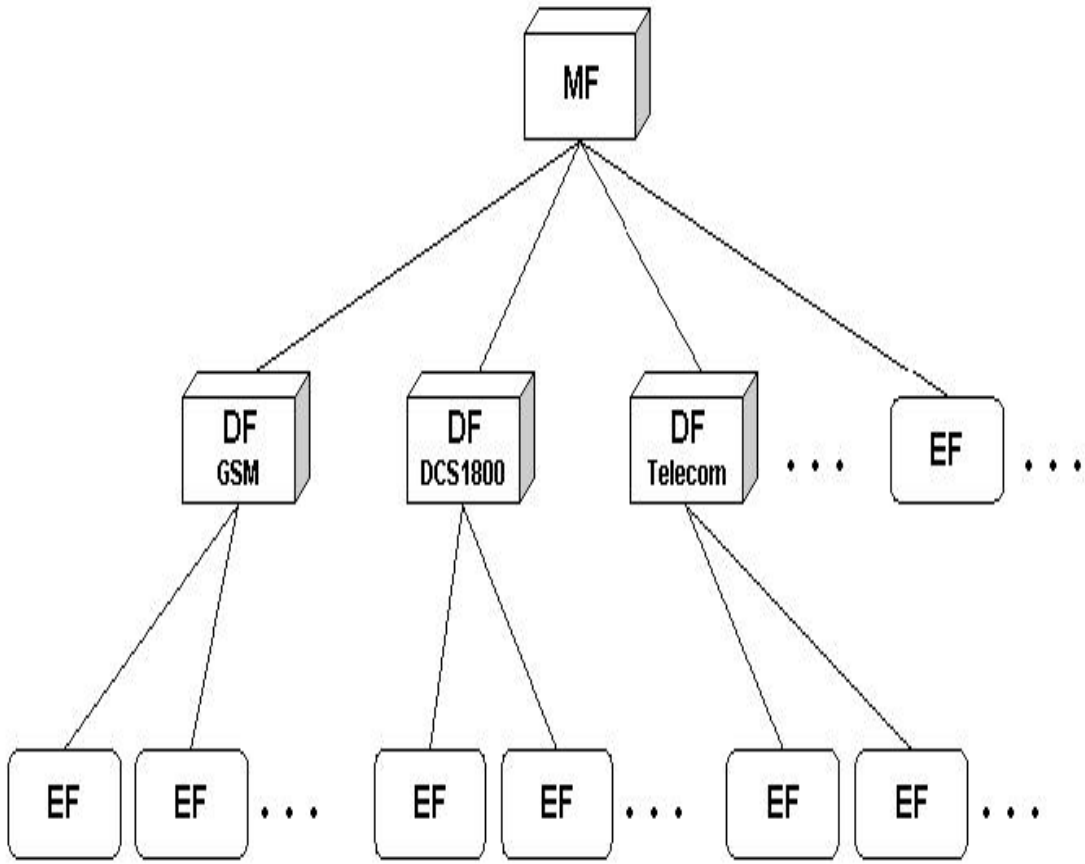
- *A portable memory chip*
- *A smart card used for identifying the cellphone*
  - *--- CPU*
  - *--- Program memory (ROM)*
  - *--- Working memory (RAM)*
  - *--- Data memory (EPROM or E2PROM)*
  - *--- Serial communication module*
- *Width of 25 mm, height of 15 mm, thickness of .76 mm*

What is a SIM Card?

- *Protected by:*
  - *–A PIN (Personal Identification Number) and*
  - *–A PUK (Personal Unblocking Code)*
- *Also includes other parameters of the user such as it's IMSI (International Mobile Subscriber Identity).*
  - *–Allows the cellphone to operate on the network.*

Logical Model of the SIM

- *Three Types of Files*
  - *–Master File*
  - *–Dedicated File*
  - *–Elementary File*



File ID

- *File ID is used to address/identify each specific file:*
  - *3F = Master File*
  - *7F = Dedicated File*
  - *2F = Elementary File under Master File*
  - *6F = Elementary File under Dedicated File*
- *File ID shall be assigned at the time of creation of the file*
- *No two files under the same parent shall have the same ID*
- *A child and any parent, anywhere in the hierarchy, shall never have the same File ID*

The files on the SIM card

Phase	*Phase ID*	*1 byte*
ICCID	*Serial Number*	*10 bytes*
SPN	*Service Provider name*	*17 bytes*
MSISDN	*Subscriber phone number*	*variable*
AND	*Short Dial Number*	*variable*
LND	*Last Dialled numbers*	*variable*
FPLMN	*Forbidden PLMNs*	*12 bytes*
CCP	*Capability configuration parameter*	*14 bytes*
IMSI	*IMSI*	*9 bytes*
LOCI	*Location information*	*11 bytes*
BCCH	*Broadcast control channels*	*16 bytes*
Kc	*Ciphering key*	

Serial Number & IMSI

- *The serial number and IMSI all provide a unique identification of the customer. The serial number, which is possible to obtain without providing PIN, identifies the SIM itself.*

Threats to SIM Data

- *Knowledgeable criminals are aware of SIM properties*
  - *Know how to manipulate them*
- *Cloning SIM data for illicit use*
  - *Two key pieces of data*
    - *IMSI*
    - *Data Encryption Key (Ki)*

Threats to SIM Data

- *IMSI can be obtained:*
  - *–From SIM using scanning software*
  - *–Eaves-dropping on networks for unencrypted transmission of the IMSI*
- *Ki can not normally be obtained directly as it is derived from encryption algorithm stored on SIM*

Threats to SIM Data

- *GSM SIMs can be cloned because authentication protocol has flaw*
  - *–COMP128 is popular algorithm and a published standard*
    - *Leaks information at every connect attempt.*
- *Chosen-plaintext attack*
  - *–Approximately 150,000 queries required takes about 8-11 hours with a suitable smart card reader*

Security features

- *authentication algorithm (A3)*
- *subscriber authentication key (Ki)*
- *cipher key generation algorithm (A8)*
- *cipher key (Kc)*

Authentication

- *Authentication involves two functional entities:*
  - *the SIM Card in mobile device*
  - *the Authentication Center (AC)*
- *Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AC.*

Authentication

- *During authentication, AC generates a random number that it sends to the mobile.*
- *Both mobile and AC use the random number, in conjunction with subscriber's secret key and a ciphering algorithm called A3, to generate a number that is sent back to the AC.*
- *If number sent by mobile matches number calculated by AC, then subscriber is authenticated.*

Encryption

- *A stream cipher known as the A5 algorithm.*
  - *A5/0: no encryption.*
  - *A5/1: original A5 algorithm used in Europe.*
  - *A5/2: weaker encryption algorithm created for export, in removal.*
  - *A5/3: strong encryption algorithm created as part of the 3rd Generation Partnership Project (3GPP).*

Encryption

- *Stream cipher is initialised with the Session Key (Kc) and the number of each frame.*
  - *The same Kc is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique key stream for every frame.*
- *The same Session Key (Kc) is used as long as the Mobile Services Switching Center (MSC) does not authenticate the Mobile Station again.*
  - *The same Session Key (Kc) may be in use for days.*

Key Generation

- *A8 algorithm generates 64-bit Session Key (Kc)*
- *One Session Key (Kc) is used until the Mobile Services Switching Center (MSC) decides to authenticate the MS again*
  - *This might take days.*
- *A8 actually generates 128 bits of output.*

Key Generation

- *The last 54 bits of those 128 bits form the Session Key (Kc).*
- *Ten zero-bits are appended to this key before it is given as input to the A5 algorithm.*
- *The A8 algorithm is implemented in the Subscriber Identity Module (SIM).*

Encryption Detailed

- *PIN –Personal Identification Number*
  - *locks the SIM card until correct code is entered*
  - *entered incorrectly 3 times → SIM blocked → PUK*
- *PUK –Personal Unblocking Code*
  - *resets PIN and the attempt counter*
- *Caution: if PUK entered 10 times incorrectly, SIM is permanently disabled and the SIM must be exchanged.*

The Future - USIM

- *The logical extension of the SIM card into the 3G environment, an evolution of the SIM card.*
- *384Kb ROM*
- *8Kb Static RAM*
- *16-bit CalmRISC CPU*
- *Triple DES*
  - *the standard symmetrical key encryption*

The Future - USIM

- *Compare with the SIM card:*

  Simply put, this is the world standard.

	Data Rates	Multi-Subscription	Java-Based USAT	Backwards Compatibility
SIM card	low	-	-	lack
USIM card	high	×	×	full

Comparison of SIM and USIM

Conclusion

- *SIM Card definition*
- *Attacks to the SIM*
- *Security features*
- *The Future - USIM*

The End

Thank You
for Your Attention

Wikipedia

- *http://en.wikipedia.org/wiki/User:Sheng.He*