Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security

Yu Yu
joint work with Junrong Liu, F-X Standaert, Zheng Guo, Dawu Gu, Sun Wei, Yijie Ge, Xinjun Xie
Some updates from Citizenfour

“When the NSA and GCHQ compromised the security of potentially billions of phones (3G/4G encryption relies on the shared secret resident on the SIM), they not only screwed the manufacturer, they screwed all of us, because the only way to address the security compromise is to recall and replace every SIM.”
Outline

• Background
  1) 2G/3G/4G (U)SIM Security
  2) cryptology, 2G/GSM AKA protocol

• Our work
  1) 3G/4G AKA protocol and MILENAGE algorithm
  2) Side Channel Attack / Differential Power Analysis
  3) Strategy, results and demos

• Lessons learned
Cellular networks (1-4G)

- 1G: analogue signal
- 2G: GSM vs. CDMA digital signal
- 3G/4G: UMTS/LTE high-speed data transmission
What is a (U)SIM card?

• (U)SIM = (Universal) Subscriber Identity Module
• (U)SIM is a smart card (a mini computer).
• SIM stores
  ➢ ICCID (serial number)
  ➢ IMSI (E.g. 310 150 123456789)
  ➢ Secrets
• Secret on 2G SIM: master key $K$.
• Secrets on 3G/4G USIM:
  master key $K$, and $OPc, r1, r2, ..., r5, c1, ..., c5$.
• What if secrets are stolen/compromised?
Security compromised by revealed/stolen secrets

Any cryptography in (U)SIM?
Cryptology in a nutshell

Cryptology = “Cryptography” + “Cryptanalysis”

- **Cryptography (design of crypto-systems)**
  The design of crypto-systems that help preserve various aspects of information security such as **confidentiality**, **integrity**, **authenticity** and **non-repudiation**.

- **Cryptanalysis (code-breaking).**
  1. Mathematical: break a crypto-system mathematically.
  2. Physical: break the implementation of a crypto-system.

Attacks in real life are often physical.
What cryptography is needed for (U)SIM?

- AKA (Authentication & Key Agreement)
- Authentication: a process that ensures and confirms a user's identity.
  - E.g., Bob authenticates Alice by **Challenge-and-Response**.
- Key Agreement (wrong term though!): session key derivation

Alice: $k$

- “I am Alice”
  - $R$
- $\text{RES}=\text{Enc}_k (R)$
- $K_s = \text{Enc}_k (R+1)$ (communication encrypted under $K_s$)

Bob: $k$

- Check if $\text{RES}=\text{Enc}_k (R)$
- $K_s = \text{Enc}_k (R+1)$
The 2G GSM AKA Protocol

**AKA algorithm of GSM:** COMP128-1 (A3+A8)

**Encryption algorithm:** A5

**Insecurity:**

1. COMP128-1 is fatally flawed  
   (narrow pipe attacks [BGW98])
2. Only one-way authentication  
   (spoofing base stations, DEFCON 2010)
3. Subject to side-channel attacks  
   (DPA attacks [RRST02, ZYSQ13])
Security improvement of 3G/4G over 2G

<table>
<thead>
<tr>
<th></th>
<th>2G</th>
<th>3G/4G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Algorithm</td>
<td>flawed COMP128-1</td>
<td>MILENAGE, in turn based on AES-128, which is <strong>mathematically secure</strong></td>
</tr>
<tr>
<td>Authentication mechanism</td>
<td>One-way (base station authenticates the SIM)</td>
<td><strong>Mutual authentication</strong> (preventing spoofed base stations attacks)</td>
</tr>
<tr>
<td>Secrets</td>
<td>The master key K</td>
<td>The master key K, The tweak value ( OP_c ), More operator-defined values: ( r_1, ..., r_5, c_1, ..., c_5 ) (more secrets = better security?)</td>
</tr>
</tbody>
</table>

Is 3G/4G USIM authentication **physically** secure?
3G/4G AKA Protocol

The difference between 3G and 4G is not security-relevant.
MILENAGE Algorithm

Verify MAC = XMAC
Verify that SQN is in the correct range
Secrets in USIM?

\[ K + \text{OPC} \left( r_1,c_1, r_2,c_2, r_3,c_3, r_4,c_4, r_5,c_5 \right) \]
How to recover them?

• The strategy: “Divide et impera”

Breaking into a vault is hard.
Things are different if it can be divided into independent sub problems

• Our job: recover the secrets $K$, $O Pc$, $r1,c1$, ..., $r5$, $c5$ one at a time using power analysis.
  ➢ for secret $\in \{K, O Pc, c1, c2, ..., c5 \}$
    do a Differential Power Analysis (DPA)
  ➢ for secret $\in \{r1, r2, ..., r5 \}$
    do a (non-standard) Correlation Power Analysis (CPA)
SCA (Side Channel Attack)

- EM
- Power consumption
- Time
- Heat
- Sound

Crypto System
Measurement Setup

PC
+ Software SCAnalyzer

Oscilloscope
Power Recorder
**Differential Power Analysis (DPA)**

unknown secret key

- device
- measurement
- analysis

input

<table>
<thead>
<tr>
<th>P = S^{-1}(K_G \oplus C)</th>
</tr>
</thead>
</table>

model

<table>
<thead>
<tr>
<th>E = H_{mW}(P)</th>
</tr>
</thead>
</table>

estimation

key fragments (e.g., bytes)

- AES: 128-bit secret key brute force **infeasible**
- Exhaustive search for a key byte **easy**
- 256 candidates (correct one highly correlates to traces)
- Do the above for every key byte **independently**
Differential Power Analysis cont’d

--- how to test if a key (byte) guess is correct or not?

Only the right key guess exhibits high peaks

Correlate the hypothetical intermediate values to the power traces

Correlation trace
Where to Attack

Secrets: $k$, $OPc$, $r1$~$r5$, $c1$~$c5$

Flow of $f5+f1$
Analysis Process

Step 1: Collect Power Trace

Identify the segment of interest (simple power analysis) and zoom-in for further analysis.

The first round of AES
Analysis Process

Step 2: Recover K and OPc

DPA recovers k from \( \text{RAND} \rightarrow E_k \rightarrow \)

How to adapt the attack to \( \text{RAND} \rightarrow \oplus \rightarrow E_k \) with secrets \( k \) and \( \text{OPc} \) ?

Equivalent view

Attack 1st round: (viewing \( E_{k'} \) with \( k' = k \oplus \text{OPc} \)) recover \( k \oplus \text{OPc} \)
Attack 2nd round: recover \( k_2 \) (and thus \( k \))
Analysis Process

Step3: Recover $r_1, \ldots, r_5$

- Consider $r_2$ and write $r_2 = 8i + j$
  
  right cyclic shift by $r_2$ bits

$$v_0v_1 \ldots v_{127} \quad \underbrace{\left(v_jv_{j+1} \ldots v_{j+7}\right)}_{\text{byte 0}} \ldots \underbrace{\left(v_{j+120} \ldots v_{127}v_0 \ldots v_{j-1}\right)}_{\text{byte 15}}$$

1. Recover $j$ (assume WLOG $i = 0$)

   make a guess about $j$ and do a hypothesis testing (8 possibilities)
   (correlate byte 0 to the power traces to test if which guess is correct)

2. Recover $i$. Correlate bytes 0 ~15 to the power traces, then

   $i$ is number of bytes shifted in the time axis (of the correlation trace).
## Results

<table>
<thead>
<tr>
<th>Target USIM</th>
<th>operator</th>
<th>manufacturer</th>
<th>technology</th>
<th>secrets</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>C1-1</td>
<td>C1-I</td>
<td>3G UMTS</td>
<td>K, OPc</td>
</tr>
<tr>
<td>#2</td>
<td>C1-1</td>
<td>C2-II</td>
<td>3G UMTS</td>
<td>K, OPc</td>
</tr>
<tr>
<td>#3</td>
<td>C1-1</td>
<td>C1-III</td>
<td>3G UMTS</td>
<td>K, OPc</td>
</tr>
<tr>
<td>#4</td>
<td>C1-2</td>
<td>C3-I</td>
<td>3G UMTS</td>
<td>K, OPc, r1,c1,...,r5,c5</td>
</tr>
<tr>
<td>#5</td>
<td>C2-1</td>
<td>C2-I</td>
<td>3G UMTS</td>
<td>K, OPc, r1,c1,...,r5,c5</td>
</tr>
<tr>
<td>#6</td>
<td>C1-3</td>
<td>C1-IV</td>
<td>4G LTE</td>
<td>K, OPc, r1,c1,...,r5,c5</td>
</tr>
<tr>
<td>#7</td>
<td>C1-3</td>
<td>C1-II</td>
<td>4G LTE</td>
<td>K, OPc, r1,c1,...,r5,c5</td>
</tr>
<tr>
<td>#8</td>
<td>C2-2</td>
<td>C2-II</td>
<td>4G LTE</td>
<td>K, OPc, r1,c1,...,r5,c5</td>
</tr>
</tbody>
</table>

Time needed for recovering the secrets ranges from 10 to 80 minutes, using 200 to 1000 power traces.

Note: the operators and manufacturers are anonymized.
Demo 1
Making phone calls from a USIM and its duplicate to another phone.
Demo 2

Resetting the password of Alipay app from a clone USIM.
Lessons Learned

1. Cryptography. Adding tweaks (secrets) to a block cipher in addition to the encryption key does not necessarily add more security.

2. The dilemma:
   - Low cost devices ≈ limited budget for CC/EMVCo/FIPS security evaluations.
   - Low-cost × huge volume = great impact / loss

3. Awareness of physical security for small embedded devices. Practical security requires BOTH:
   - A mathematically secure (and publicly reviewed) algorithm.
   - Sufficient countermeasures in place against physical attacks.
Thank you!

For more technical details, check out our ESORICS 2015 paper: Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards