Open encryption technology and social movements

2013 Cryptologic History Symposium
17-18 October

Niels Jørgensen
Roskilde University, Denmark

nielsj@ruc.dk
Research questions

1) How did the Chaos Computer Club break the user authentication method in GSM 2\textsuperscript{nd} Gen.?

2) What would be a good conceptual framework for describing social movements that were part of the 1990s' crypto controversies?

Conceptual framework
• eg. Dennings' activism / hacktivism / cyberterrorism

Social movements
• hackers, privacy rights activists, if organized

Crypto controversies
• should (can) strong encryption be restricted by government?
Plan of talk

1) Case

The cloning in 1998 of a GSM 2\textsuperscript{nd} Generation SIM-card by the Chaos Computer Club, Germany

2) Analysis

Existing conceptual frameworks
- hackers; social movements
- useful, but insufficient

Jamison's *The Making of Green Knowledge*, 2001
- conceptual framework should include technology
  *how did the CCC-hackers use + create technology, in the process of struggling over technology*
Crypto controversies

Started early 90s: phone/internet encryption a possibility

Ended ~2000: Strong, open encryption became dominant
• perhaps social movements influenced this?

US
• Standardization of AES (2001)
• Key escrow initiatives discontinued (~2000)
• Export restrictions lifted (2000, 2004)

Europe
• GSM 3rd Gen.: strong, open encryption (UMTS, 1999)
• Encryption restrictions lifted (France)
• Encrypt. regulation initiatives discontinued (UK, 2000-2005)
Studies of the crypto controversies

Include accounts by participants in the 1990s' debates:

Politics, activism
• “Privacy advocates convinced the government”
  NSA Director McConnell (The New Yorker, 2008)

Economics
• “Businesses demanded strong encryption”
  Diffie & Landau: “Privacy on the line” (2007)

Technical
• “Key escrow was technically infeasible”
  Matt Blaze: “Encrypting history at the NSA” (2008)
Case: SIM-car cloning by the Chaos Computer Club

CCC is a German hacker group

• 1981-present

Members of CCC cloned a GSM 2\textsuperscript{nd} Generation SIM-card from operator D2

Used clone to make calls..

.. masquerading as the subscriber that holds the original card

Published in “Der Spiegel”, april 1998
The SIM-card in GSM security

User/subscriber authentication is by a “two-factor” method:
#1) user must *know* PIN-code
   to uncover unique IMSI# from SIM-card
#2) user must *possess* SIM-card,
   with its unique 128 bit *secret* key $K (K_i)$

OBS: $K$ is secret to prevent cloning

Members of the CC were able to uncover $K$
• by probing the card's standard interface
• not tampering
• then make phone calls without the SIM-card
Factor #2

GSM 2\textsuperscript{nd} G. authentication uses a function called “comp128”
- in a challenge-response protocol
- response proves SIM-card has correct key K
comp128

.. is a hash (compression) function
• input 256 bits (K + challenge)
• output 128 bits (of which 32 bits form the response)
• 8 rounds of: add K + compress in 5 steps + permute

.. implements “A3” in G2 spec.
• a “reference” implementation used by most operators
• specified ~1988, leaked 1997-98, reverse engineered

.. cryptanalyzed in 1998
• Goldberg, Wagner (UC Berkeley), Briceno (Smartcard D.A.)
• collision attack: recover two bytes of K at a time
• violation of “strong collision resistance”
• “not a novel attack”
  • black-box cryptanalysis (Schnorr & Vaudenay, 1993)
What the Chaos Computer Club did

Made the Goldberg, Wagner & Briceno attack practical

recovered key K in 11 hours
  • using self-engineered card reader
  • cryptanalysis implemented on ordinary PC

then made actual phone calls
  • using self-engineered interface to mobile phone
  • SIM-card emulator on PC
  • calls worked
  • except simultaneous calls blocked by network
    (original SIM-card + clone)
Avoid “Unsicherheit bei Geheimniskrämerei”. (Müller-Maguhn, CCC)

Customers need not worry. Cloning requires theft of SIM-card + PIN-code. (Kuczkowski, D2)

Vendors can clone SIM-cards.
Analysis: concepts from analyses of hackers

Dennings, 2001
- activism, hacktivism, cyberterrorism
- hacktivism = “marriage of hacking and activism”
- “disrupting normal operations but not causing serious damage”
- resembles white hat / grey hat / black hat distinction

<table>
<thead>
<tr>
<th>Concept</th>
<th>Chaos Computer Club, the GSM hack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful damage</td>
<td>• GSM cloning legal</td>
</tr>
<tr>
<td></td>
<td>• jail sentence, phone stealing</td>
</tr>
<tr>
<td></td>
<td>• jail sentence, espionage</td>
</tr>
</tbody>
</table>
Concepts from social movements studies

McAdams et al. (1996)
• mobilizing structure / opportunity structure / framing struct.
• typical case: civil rights movement

<table>
<thead>
<tr>
<th></th>
<th>Chaos Computer Club, the GSM hack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concept</strong></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Formal&lt;br&gt;• board, membership, journal, conferences&lt;br&gt;Informal&lt;br&gt;• network, non-members, Erfa-Kreise</td>
</tr>
<tr>
<td>Alliances</td>
<td>Concerns in Germany about surveillance</td>
</tr>
</tbody>
</table>
The Making of Green Knowledge
(Jamison, 2001)

Social movements as cognitive praxis, with
• world view (ecology; sustainability; ..)
• technical issues knowledge

Environmental movement in Denmark
• built windmills (1890s, 1950s, 1970s)
• Danish “windmill adventure”
  • 20% of electrical energy (today)
  • ~ 50% of world market for windmills (1990s)

New technology was created in the movement
• windmills built as “proof of concept”
## Extended set of concepts

<table>
<thead>
<tr>
<th>Concept</th>
<th>Chaos Computer Club, the GSM hack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Alliances</strong></td>
<td></td>
</tr>
<tr>
<td><strong>..</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Technology** | *made a theoretical attack practical*  
* demonstration (not use)*  
* perhaps one small step towards GMS 3G*  
**..** |
Discussion

Novelty: *made a theoretical attack practical*
- compare DES-cracker by EFF (1998)
- the theory/practice gap can be large
- there are $2^{76.7}$ keys that protect against the attack (Wray 2003)

Purpose: *demonstration (not use)*
- cryptanalysis can play a constructive role
  - GSM 3rd G. had stronger hash functions
- other products were made for use, during the controversy
  - PGPmail, PGphone by Phil Zimmermann
The comp128 collision attack (Wray, 2003)

For \( j = 0, \ldots, 7 \) do:

1) Probe SIM-card to find two pairs of bytes \((b_{j+16}, b_{j+24}), (b'_{j+16}, b'_{j+24})\) that collide.

2) Use comp128 to find a pair \((b_j, b_{j+8})\) that collides with both pairs from step 1.

Search space: \( 2^{2*8} \)
The comp128 collision attack (Wray, 2003)

For $j=0,..7$ do:

1) Probe SIM-card to find two pairs of bytes $(b_{j+16}, b_{j+24}), (b'_{j+16}, b'_{j+24})$ that collide

2) Use comp128 to find a pair $(b_j, b_{j+8})$ that collides with both pairs from step 1

Search space: $2^{2*8}$
Collision space: $2^{4*7}$