Can you clone a GSM Smart Card (SIM)?

Charles Brookson July 2002

A History Lesson

The Algorithm Expert Group, whose first meeting was held as long ago as 1987, designed the GSM encryption algorithms. They came up with two algorithms, the one in the smart card for authenticating the subscriber and deriving the cipher key (A3/8 in the GSM Specifications) was known as COMP128. The one in the mobile, used to encrypt the information over the radio path, is known as A5.

The GSM specifications[i] allowed anyone to choose their own A3/8, and the whole system was designed to support this, even when roaming. Care was taken so that keys and algorithms were not transferred between networks. Nevertheless, many operators did not have the expertise to design their own algorithms, and so COMP128 came along as an example.

The fatal flaw

It was found within a few years that COMP128 was fatally flawed, and that it required about 50,000 or so challenges and responses to find out the sensitive key Ki of 128 bits of the user…. The key is sensitive because if you find it out then you can create a new smart card with all the information and pretend to be that user ('Clone' the smart card). Of course, for this and all the subsequent cloning I describe you need physical access to the smart card; eavesdropping the radio link still can't do it.

Ian Goldberg and Marc Bricenco first proposed this publicly [ii]. The old COMP128 algorithm now became COMP128-1, and a new version was distributed as COMP128-2, which overcame the known weaknesses. As a result of this, the GSM Association Security Group issued a warning to operators that COMP128 was an example only, and they should really consider developing their own as the specification intended.

You might like to know that there is one other version, COMP128-3 that produces a 64-bit key for A5, which is based of the 54 bit key version COMP128-2 (COMP128-1 is also has a 54 bit key for A5).

There is an even newer version COMP128-4 under development based on the 3GPP[iii] algorithm MILENAGE[iv] that uses AES[v] (RIJNDAEL).

There has been much progress made with attacks against SIM cards[vi], and with selected plain text (pre-computing the challenges) and monitoring the voltages of the smart card (Differential Power Analysis or DPA[vii]) the time to find out the key Ki has been reduced to a few minutes. IBM recently published this result.[viii]

This latest flaw was most unfortunate, as the defence used by some operators against the original COMP128-1 attack was to limit the number of challenges, so that the card would lock up before the unique key was discovered. Now this is not possible, as the few challenges required are now much less that the card would normally expect during its lifetime.

Is it possible?

So, it is possible to clone a smart card, but only if it is using the old algorithm.

Unfortunately, many operators still seem to be using the old COMP128-1 algorithm, whether by choice, ignorance, or difficulty in updating their Authentication Centres. Equipment to clone a card is available in the Far East; the kits are even shrink wrapped for consumers. Blank cards are readily available. We have even seen cards that can contain multiple identities becoming available.

Of course, this isn't the whole story. Not only do you have to use a good algorithm for A3/8, you also have to make sure you are using software and hardware to protect against other suggested attacks such as DPA, optical faults[ix] and many others!

How can you change to a new authentication algorithm?

The GSM standards have been carefully designed to allow you choose any authentication algorithm you wish, providing it meets the requirements[x].

So, an operator can change the A3/8 algorithm by changing the algorithm in the Authentication Centre (AuC) and the SIM card. Most Authentication Centres will support multiple algorithms in use in a network at the same time, and in the AuC the algorithm that the card uses is identified by the IMSI of the card. In this way an operator may gradually introduce a new algorithm to new users (or reissued cards).

References

[i] For a background on the GSM Specifications for Security see my paper on http://www.brookson.com/gsm/gsmdoc.pdf

[ii] The original paper is on http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[iii] For all the 3G and GSM Standards see www.3gpp.org

[iv] The 3GPP algorithms are on http://www.3gpp.org/TB/Other/algorithms.htm

[v] For information on AES and Rijndeal see http://csrc.nist.gov/encryption/aes/rijndael/

[vi] By software such as SIM Scan 1.21 by Dejan Kaljevic, see http://users.anytimenow.com/sid67b/GSMSIM2.htm for examples.

[vii] DPA information is on http://www.cryptography.com/resources/whitepapers/DPA.html

[viii] The IBM Press Release is on http://www.research.ibm.com/resources/news/20020507_simcard.shtml

[ix] The TAMPER pages at Cambridge University are a good start, on http://www.cl.cam.ac.uk/Research/Security/tamper/

[x] The GSM security standard is GSM 03.20 and is available from the www.3gpp.org site as 43.020.