Institution: Royal Holloway, University of London

Unit of Assessment: B10 Mathematical Sciences

Title of case study: Design of Authentication Algorithms for GSM Phones

1. Summary of the impact (indicative maximum 100 words)

Mobile telecommunication networks serve nearly 7 billion users; over 90% of the world's population. The flexibility and pervasive nature of mobile networks underpin an enormous range of business and personal activities. Many systems are based on GSM (Global System for Mobile Communications) standards for digital cellular networks that were created by the European Telecommunications Standards Institute (ETSI) in the 1990s to replace analogue network standards. A key factor in the success of GSM has been the ability to authenticate legitimate users and to provide privacy for wireless transmissions. A strong authentication mechanism is critical for the economic operation of mobile telephony.

The security of GSM is based on a secret key, known only to the network operator and the Subscriber Identity Module (SIM), and an authentication algorithm implemented by the SIM and the network operator. A network operator may implement its own authentication algorithm, but many adopted the example implementation (known as COMP128, or COMP128-1) suggested by the GSM Association (GSMA). COMP128-1 was later found to be flawed. Cryptographers at Royal Holloway, at the request of GSMA, designed a replacement algorithm (COMP128-2), the example implementation offered by the GSM Association (GSMA) to over 800 Mobile Network Operators (MNO) in over 200 countries. The algorithm is still regarded as robust and it and derivative algorithms are relied upon by enormous numbers of users every day.

2. Underpinning research (indicative maximum 500 words)

An authentication protocol enables one entity (the verifier) to confirm the identity of a second entity (the claimant). In the case of GSM networks, the verifier is the network operator and the claimant is the SIM. The claimant and the verifier share a secret key and the claimant proves its identity to the verifier by applying a cryptographic algorithm to a message chosen by the verifier (a "challenge"). The generation of an appropriate response to the challenge demonstrates knowledge of the shared secret (assuming that only the network and the SIM know the secret key).

The underpinning research is the specification for the authentication algorithm COMP128-2 that is used in GSM phones. Three Royal Holloway academics, Sean Murphy (then Reader, now Professor), Fred Piper (then Professor, retired 2004) and Peter Wild (then Professor, retired 2010), designed the original algorithm in the late 90's [2]. The specification for the GSM authentication algorithm is confidential, and is distributed under a suitable Non-Disclosure Agreement to GSM Operators as required. The algorithm was reviewed by ICO Services Ltd (a small UK-based telecommunications operator) and then by ETSI, before being adopted by ETSI as their recommended authentication algorithm COMP128-2. Later the variant of this algorithm known as COMP128-3 was introduced; this algorithm is identical to COMP128-2 except that an artificial limitation on the effective key length (originally imposed due to export restrictions for cryptographic algorithms) is removed.

Quality: Chairman of the GSM Association Security Group [2], after confirming that the design originated at Royal Holloway in the late 90's, writes:

> The design of COMP128-2 by the group at Royal Holloway is a good example of the impact academic study can have outside academia: the design of a robust and novel cryptographic algorithm such as this is a delicate business, requiring a great deal of technical proficiency. All the evidence that I have seen indicates that COMP128-2 remains secure after years of use in high-profile applications, and this is a significant achievement.

The specification for COMP128-2 has been subject to a more rigorous peer review process than is usual for academic publication. The President of the IACR (the main international organisation concerned with cryptographic research), a consultant for industry, and a member of ISO standards committees for security technologies. He writes [1]:

> I would like to make two points: first, that good cipher specification is regarded as a significant research contribution in my field; second, that the review process for a key industrial cipher can be more demanding than the refereeing process for a top cryptography conference. […] For the GSM […] ciphers above, the design will be reviewed by several teams (certainly more than 3), each team looking at the cipher for (as an absolute minimum) 2 days. The review procedure is therefore typically much longer than for a submission for an academic conference. Moreover, high-profile academics and highly-regarded industrial consultants are often the same people. This leads me to believe that the industrial review process is often more rigorous than for a top academic conference. I should mention a second, unofficial, 'reviewing' process of an industrial cipher takes place when the deployed cryptographic system is attacked by third parties. If the system remains resistant to real-world attacks, this gives further evidence of the quality of the cipher.
> All of this context points to the two ciphers that Royal Holloway are putting forward as being clearly of 2 star or higher research quality, as defined above.

In his letter of support, President of the IACR gives more detailed evidence of the high esteem the community gives to research of this type.

Context: This design of COMP128-2 forms part of a strong tradition of the study of cryptology in the School that continues to the present day. Royal Holloway is designated as an Academic Centre of Excellence in Cyber Security Research (2012-) and hosts a Centre for Doctoral Training in Cyber Security (2013-); and our expertise in cryptography (as part of an interdisciplinary group spanning mathematics and computer science) contributes significantly to this. Highlights of work completed over the history of the group include the invention of key distribution schemes (Mitchell-Piper), the cryptanalysis of FEAL (the first use of differential cryptanalysis; Murphy), the algebraic framework for the cryptanalysis of AES (Cid-Murphy-Robshaw), pairing-based cryptography (Galbraith-McKee), ID-based cryptography (Paterson), key predistribution for Wireless Sensor Networks (Blackburn-Martin-Ng), codes for copyright protection (Blackburn-Ng) and group-based cryptography (Blackburn-Cid). Consultancy in the field of information security is regularly carried out, including the design and cryptanalysis of ciphers and work with new digital mobile telephony standards. Blackburn, Cid, Martin, McKee, Murphy, Ng and Paterson are current academic staff who have published cryptography papers and/or undertaken cryptographic consultancy within the current REF period.

3. References to the research (indicative maximum of six references)

S.P. Murphy, F. Piper, P.R. Wild, Functional description of COMP128-2, GSM Association, 2002. Available under an appropriate NDA.

4. Details of the impact (indicative maximum 750 words)

What is the link between the research and the benefit? There is a clear and direct link between the specification produced as underpinning research and the impact, due to the specification being recommended by the GSMA as an authentication algorithm for GSM networks and subsequently adopted by over half of all GSM operators.[2]

Who benefits? Phones based on the GSM standards were first commercially released in 1992; the GSM Association (GSMA) of network operators announced in 2010 that more than 5 billion phones have been manufactured under this standard to date. There are billions of GSM subscribers and hundreds of GSM networks and a significant proportion will be using the COMP128-2 and COMP128-3 algorithms for authentication. Then there are all the businesses and services that rely on these networks as a trusted infrastructure. The Chair of ETSI Security Algorithms Group of Experts, states [2]:

> COMP128-2 and COMP128-3 have been a huge success. Although we do not have precise figures, we estimate that more than half of the world's network operators, representing a number of subscribers in the billions, use one of these algorithm variants.

How do they benefit? As an individual, the COMP128-2/3 algorithm safeguards you in a number of ways. It protects against cloning, which stops criminals making costly calls charged to your account; when a clone is detected by the network you will be blocked from the network, whereas the criminal will pick a new identity. Furthermore, the clone is linked to your telephone number, so when the criminal makes a call it appears to be you in a friends/family phone book. Phone numbers are also used in business systems and form parts of security processes such as text message warnings when changing bank instructions, as well as alerts that may leak other personal information and location; cloning compromises these processes. The algorithm prevents your secret key from becoming known to a criminal to safeguard the authentication process, but also stops a criminal from regenerating the current cipher key in order to decipher radio transmission to obtain private or sensitive call data.

Cloning is a real threat to mobile networks. The introduction of GSM, replacing analogue systems, led to a sharp reduction in phone cloning, a practice that was close to making analogue mobile telephony uneconomic towards the end of its operating life (with 1% of all phones in the UK found to be cloned in 1994/5 [6]).

The GSMA originally distributed an algorithm known as COMP128 (or COMP128-1) to its members, as an example of an authentication algorithm that complied with the GSM standard. Though a specific authentication algorithm was not mandated by the GSM standard, in practice many operators used COMP128 rather than developing their own algorithm. The specification of COMP128 was not made public, but COMP128 was reverse engineered in 1998 by Briceno, Goldberg and Wagner, and in 2002 Rao, Rohatgi, Scherzer and Tinguely were the first to publicly demonstrate that a GSM phone using COMP128 could be cloned after access to the SIM card for only one minute. Thus cloning was possible on networks still using COMP128. Indeed, by mid-2002 shrink-wrapped cloning kits for COMP128-based SIM cards were being sold in some countries; blank cards and cards with multiple identities became available [4].

In order to prevent cloning attacks on their networks, several mobile operators commissioned the group at Royal Holloway to design an algorithm to replace COMP128. Recognising a common need, the GSM Association commissioned the group at Royal Holloway to design the algorithm that became known as COMP128-2, and this algorithm and its variant COMP128-3 became the example authentication algorithms provided by the GSMA to its members. No successful cryptanalysis has been demonstrated to date, and there is no evidence that SIM Card cloning has returned on networks using these algorithms [2]. Ten years on, the algorithm is still recommended by ETSI, and authorisation to use this algorithm is regarded as a significant benefit of a network operator's membership of the GSMA.

> One single fraudulent SIM card on a network can lose an operator in excess $3000 (£1,885) a month and these operations usually use hundreds or even thousands of cards. This illegal activity often goes on to fund other criminal activity.

says Andy Gent, CEO of Revector (a company detecting fraud on mobile networks) in a 2012 BBC Technology interview [5]. The research effort to design COMP128-2/3 has led to the elimination of SIM card cloning for over ten years on networks using this technology [3], resulting in significant financial benefits for operators and users alike throughout the REF period.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[1] Supporting statement from a Professor at KU Leuven and President of the International

Association of Cryptologic Research, 11 May 2013. Copy available on request. [To corroborate quality.]
[2] Supporting statement from the Custodian of GSM Algorithms, 25 March 2013. Copy available on request. [To corroborate quality and authorship, and the reach of impact.]
[3] Supporting statement from the Chair of ETSI SAGE (European Telecommunications Standards Institute Security Algorithms Group of Experts), 28 March 2012. Copy available on request. [To corroborate quality and authorship of the underpinning research; the reach and significance of impact.]
[4] Charles Brookson, 'Can you clone a GSM Smartcard (SIM)?' July 2002. Available from: www.brookson.com/**gsm**/**clone**.pdf. [To corroborate the reach and significance of impact.]
[5] BBC Technology News Report, 'Mobile firms bleed billions to fraud and bill errors', 29 March 2012, http://www.bbc.co.uk/news/technology-17551858. [To corroborate the significance of impact.]
[6] 'Mobile Telephone Crime', Parliamentary Office of Science and Technology Note 64, June 1995. [To corroborate the significance of impact.]