Standardization of Cryptographic Techniques – The Influence of the Security Agencies

Gunnar Klein

Standardization of Cryptographic Techniques –The Influence of the Security Agencies

Gunnar Klein

Informatics/eHealth division, Business School

Örebro University, Örebro, Sweden

gunnar.klein@oru.se

Abstract. This paper is inspired by the global debate emerging after the release by Edward Snowden in 2013 of many documents describing the policy and practice of the US National Security Agency (NSA) and some of its collaborating partners in other countries, GCHQ in the UK and FRA in Sweden. This paper gives five examples from 1989-1995 on how security experts from Norway, Denmark and Sweden were put under pressure by actions from NATO and various security agencies during their work for the European standardization bodies, CEN and ETSI. Even after the cold war essentially ended by the fall of the Berlin Wall in 1989, the use of cryptographic techniques, today completely legal and an essential part of the information society, was highly sensitive at least through 1996. The security experts were put under strong pressure to favour weak encryption algorithms that would facilitate eavesdropping by the national security agencies.

Keywords: Cryptography, Standardization, Security Agencies

1 Introduction

1.1 Cryptographic Techniques were considered Military Technology

For hundreds of years the techniques to conceal messages by cryptographic techniques were mainly developed for the benefit of governments but were also used by the opposition. With the invention of machines for serious encryption, costs were until around 1980 such that only military and some other government organizations could afford it and used it. While there was an open scientific literature on cryptographic algorithms and their possible flaws, leading for instance to the publication of the still most widely used public key algorithm (RSA) by Rivest, Shamir and Adleman [1] in 1977, hardware to perform sophisticated algorithms was restricted for use in many

countries, and certainly export was regulated.

1.2 Personal Computers and Microprocessor Chips

With the development of integrated circuits and general purpose personal computers from early 1980s, tools for advanced cryptography became affordable and the increased use of data communication in all aspects of society from personal communication to health and business dramatically changed the requirement for cryptographic services. Also, the development of digital mobile communication - with GSM from Europe as the star example that has conquered the world with now some 5 billion subscribers - introduced the need for cryptographic techniques for the masses. Smart cards with on card cryptographic capabilities started to be used in the mid 1980s and since the 1990s they are part of every mobile phone and most banking cards as well as many other security applications. The early history of these involved several clashes between the security agencies in western Europe and US and various civil human rights interests as well as growing business interests where many new services depend on the ”dangerous” techniques.

It is my opinion that the security agencies in a number of ”democratic” countries, including Scandinavia, for a number of years acted against this sound development often without appropriate support from legislators. This paper includes five examples.

2 The Author's Background

This paper is mainly based on the personal experience of the author, now a professor of eHealth/Health Informatics at both Örebro University in Sweden and at NTNU in Trondheim, Norway. The author has had the privilege of not only observing, but also actively participating, in some of the events described herein. He has also personally met three of the named informants to this paper. The GSM cryptographic story comes from recent literature.

1987-93 the author was leading a small company, Infocard Nordiska AB that developed systems for smart cards, including the first personalization systems for GSM SIM cards used by the telecom operators in Sweden, Finland, Denmark and Norway. 1994-99 Klein was working for the Swedish Institute for Health Services Development (Spri) with the leadership of three EU projects, Trusted Health Information Systems 1994, TrustHealth I and TrustHealth II 1995-98. Klein was chairing the Swedish standardization group for identification cards Ag 17, 1992-2002 and represented Sweden in the European CEN/TC 224 and international ISO/IEC JTC1/SC 17 committees. Klein was also the convenor of the security working group CEN/TC 251/WG 6 within medical informatics. In Sweden Klein was leading the development of the technical specification for an electronic ID card for SEIS (Secure Electronic Identification in Society) an organization with members from government, telecom, banking, healthcare and industry. In this context he was interacting closely with the leading cryptography and security experts of Sweden. 1996–2004 Klein was the chairman of CEN/TC 251 Health Informatics and in this capacity interacted with the European Commission.

3 General Information Security Standardization

For many years there was a sound international sharing of knowledge by academics on basic mathematical analysis and cryptographic applications, while at the same time some of the basic science was kept highly classified and still is. But already from the 1970s a lot of powerful techniques was in the public international domain, but all attempts to formalize this into practical standards for the growing different forms of civilian digital communication were stopped by various means, as the information security committee of ISO/IEC learned in the 1980s. Crypto-Algorithms should not be part of the work.

3.1 When NATO entered CEN

In 1989-90 there were preliminary attempts from several European countries to start formal standardization of important security techniques within CEN – the European federation of national standards bodies. Mr Vangelis Vardakas (Secretary General of CEN 1984-1990) has personally in 1997 (when he was a director at the European Commission DG III for Regulatory Policy, Standardization, New Approach Legislation) told me, how he one day in 1990 received an unannounced visit to his office in Brussels.

Three NATO generals in full uniform from different countries stepped into his office. The Italian general had the largest collection of colourful medals.

- We have heard that you in CEN are drafting standards on cryptographic techniques, said the English General.
- We do not think it is your business to do this, said the Dutch General.

The Italian general stomped the floor to emphasize the next message.

- You have to stop doing this!

The poor CEN boss, Mr Vardakas, who had some 250 technical committees working on more than 10 000 ± standards had no idea what they were talking about, but rapidly agreed to comply, and the proposal for a new security standardization group was buried for 20 years.

4 ETSI and GSM Encryption

During the 1980s ETSI – one of the three official standards bodies of Europe for telecommunications - was busy defining the new digital mobile telephony system GSM. Cryptographic techniques are used to authenticate the mobile subscriber having a specific SIM card in the mobile phone. But GSM, the first large scale digital radio telephony system was designed also to encrypt the data stream sent over the air to the

base station to make it difficult for any eavesdropper to listen to private voice communication. During the last years of the 1980s an expert group was working on this, and from a technical point of view an RSA algorithm A5/1 was proposed with 128 bits key length, which was considered to be very secure for at least 15 years. However, powerful pressure was made on delegates from especially UK and France, and a weakened algorithm with only 56 bits was finally selected and used until today. An even weaker version was defined later by ETSI A5/2 as a version to export to certain countries not trusted by European governments.

The history of how this happened was recently revealed by the Norwegian daily Aftenposten [2] and echoed to various other daily newspapers in January 2014. Two Norwegian experts, professor Jan Arild Audestad who participated in the security work, and Thomas Haug who was one of the leading persons for the whole GSM standardization effort over decades, were interviewed.

In the standardization process which started in 1982, a key length of 128 bits was originally proposed. At that time, 128 bits was projected to be secure for at least 15 years. It is now estimated that 128 bits would in fact also still be secure as of 2014. Audestad, Haug and also Peter van der Arend, a Dutch participant of the group, said that the British insisted on weaker encryption, allowing the British secret services to eavesdrop more easily. A number of attacks on A5/1 by Ross Andersson and others have been published since 1994, including the fact that the American National Security Agency is able to routinely decrypt A5/1 messages according [3-10].

It is noteworthy that law enforcing agencies have had every possibility to apply wiretapping in unencrypted form also of GSM communication from a specific number, since the communication from the Base station and to the general switched network is not encrypted. What would be difficult with a stronger encryption algorithm is, for the security agencies, to pursue illegal listening to mobile phone conversations from persons that are locally followed.

5 ETSI and the general Telephony Card

In addition to GSM, that was starting operations in 1991 but remained quite small for a number of years, ETSI was working on standards for other applications using wired communication where smart cards were going to be used to increase security. The intended applications were for the authentication of a subscriber to pay for the network use and but also other security services such as signatures on financial transactions or protection of confidentiality using encryption.

The chairman of the group ETSI STC TE9 was Ove Bardenfleth Nielsen, who at the time worked for KTAS, the Danish public telephone operator. He told me the following story a few years later, verified in 2014.

- The specification was for a multi-application smart card based on the EN 726 series of basic standards aligned with the international ISO/IEC 7816 standards. However, the European operators also wanted to define some security provisions that were not included in the international work. We discussed since 1990-91 various suitable algorithms, but quite independently from the

GSM discussion above.

- One day I received an invitation, which I could not reject for a meeting with the security services in Denmark. I had to come to their offices for a meeting.
- They said: «We understand that you in ETSI are considering to adopt this xxx-algorithm. But we urge you not to select such a strong algorithm which would compromise National security.»
- OK, I said, I hear you, but it is not for me to decide alone. I have to listen to
- the group. It later turned out that pressure was coming from various sources to the group on this issue, and we received directions from the ETSI group SAGE to adopt a weaker algorithm.

It is noteworthy that this specification with the weaker algorithm never became implemented at large. Partly because of the special and weak crypto algorithm other potential co-operating partners such as banks did not want to be part of this, and other smart card products became available that were equipped with RSA and other well- known symmetric algorithms.

6 INFOSEC and Cryptographic Services in Health

The author was the project coordinator of the Trusted Health Information Systems 1994-95 [11-13]. This was a requirements analysis project including representatives of nine European national health authorities, assigned to write about the need for cryptographic services by the EC program ”Electronic Signatures – Key to Mobility”. Our expert group was in very good agreement, and we recommended the broad introduction of public key encryption and a corresponding PKI infrastructure to issue certificates, first to all personnel and units in health care services to ensure the three basic services: Authentication of users, Confidentiality encryption of all messages over open networks and finally Digital signatures on important documents such as health records or electronic prescriptions.

However, the manager of the Infosec programme at the European Commission, David Herson, was very unhappy with this. He had spent 20 years in the British security agency GCHQ, ten years as a liaison with CIA in Washington. He tried various ways to persuade us to change our minds alternating between being nice and threatening. He once invited me to a private dinner where he was tried to win me over by stating that Sweden and the UK had co-operated already during the Second World War to crack the German Enigma crypto device. Although most of the work was done at Bletchley Park with Alan Turing in the lead it was true that a Swedish mathematician had a role in this. Mr Herson asked me ”did I really want to have on my conscience that with our scheme the evil terrorists and Chinese agents would hide in primary care centers and send their dangerous messages to each other, and the good guys of the security services had no chance of eavesdropping.” When I and the other experts of the group decided to ignore the advice, Mr Herson changed tone and said the CEC would not pay our contracted expenses. Later he had to give in, because there was no political mandate in EU to act in this way.

Four years later after the 1996 policy change from the US, Mr Herson and I met at a conference, and he actually sincerely apologized and said I had been right all

along. In 1996 through CEN/TC 251, where I was chairing the security working group, we made RSA mandated in the European pre-standard ENV 12388 " Medical Informatics - Algorithm for Digital Signature Services in Health Care».

7 The Battle over Electronic Signatures in the EU

In 1996 there was an attempt to form a EU policy on encryption in one area, namely the algorithm for digital signature services. RSA was an obvious choice promoted by most crypto experts at the time, and with 20 years of knowledge it was well established, and products were available from several companies to manage it in smart cards, e.g. Philips and Siemens. However, the US government was afraid of its potential use for confidentiality encryption and not just signatures. The NSA had developed DSA, which in the Digital Signature Standard from NIST was an alternative. Some of the European governments were recommending the adoption of this in Europe opposing RSA, e.g. UK, France and Netherlands. Other governments like the Danish were strongly for RSA and against DSA. In Sweden, various experts gathered from banks, police, defense, telecom and healthcare actually all agreed to recommend RSA. Other countries were struggling with forming an opinion for a scheduled decision by the council of ministers.

Yet the Swedish government representative went to Brussels and voted for DSA in this preliminary poll. I later learned what happened from the now late Mats Ohlin, who worked for the Swedish defense as an information security expert and an important contributor to the international information security standardization of ISO/IEC JTC1/SC 27. The US state department sent a high official on a tour to various European governments some weeks prior to the Brussels meeting. The message was clear and easy to follow for a Swedish government: If you do not vote as we like on the issue of algorithm, your country can no longer receive privileged military technology. Sweden with its development of an advanced military aircraft JAS Gripen would face having wasted lots of money and missing possible lucrative export contracts. That was why Swedish government officials made the strange change of opinion in Brussels. In the end it did not help, because there were too many countries of diverging opinions so no unanimous agreement could be made.

8 Discussion

These stories are just some evidence of the very strong influence that national security agencies in Europe and the US has had on the standardization of cryptographic techniques. For us who experienced this often quite frightening behaviour with the sudden appearance of men in uniform using violent language, the revelations by Snowden on co-operation between NSA come as no surprise. It is a fact that NSA and some other security agencies have had a very strong mandates from their governments to eavesdrop on not only traditional and mobile telephones but also data communication. Many citizens like me and politicians such as those of the European Parliament who started an action in 2001 on the Echelon system [14] are

concerned that the goal of fighting terrorism does not justify the risks of privacy infringement and basic human rights related to freedom of speech.

In this paper I present five examples, where pressure was exerted by security agencies, not only but most strongly from the US and UK, but also from the Scandinavian countries, against the efforts at a European level to create a good protection of privacy in the modern information society. It is noteworthy that in all cases the fact that such pressure was put on technical experts from various countries was never revealed at the time. In many cases the security agencies managed to influence the selected standard, which we all still suffer from. In some other cases the technical experts succeeded to pursue security standards including encryption against the wish of security agencies. This is fine but over time the capabilities of some agencies like NSA has increased a lot, and we generally do not know what measure of privacy protection is safe against such attacks, probably very little, even if we manage to secure transmission against lesser resourced hackers.

References

1. Rivest, R., Shamir, A., Adleman, L.: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM 21 (2): 120–126. (1978).
2. Færaas, A.: *We were forced to weaken the mobile security*. Aftenposten. Retrieved from the Internet 2014-01-14: http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html (2014).
3. Anderson, R.: *Hacking digital phones*. Retrieved from the Internet 2014-01-14: https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ (1994).
4. Jones, S.: *NSA Able To Crack A5/1 Cellphone Crypto*. Retrieved from the Internet 2014-01-14 http://yro.slashdot.org/story/13/12/14/0148251/nsa-able-to-crack-a51-cellphone-crypto
5. Biryukov, A., Shamir,A., Wagner., D.: *Real Time Cryptanalysis of A5/1 on a PC.* Fast Software Encryption—FSE. 1–18. (2000).
6. Golic, J.D.: *Cryptanalysis of Alleged A5 Stream* Cipher. Eurocrypt 239–55. (1997).
7. Biham, E., Dunkelman, O.: *Cryptanalysis of the A5/1 GSM Stream Cipher*. Indocrypt. 43–51. (2000).
8. Ekdahl, P., Johansson, T.: *Another attack on A5/1*. IEEE Transactions on Information Theory 49 (1): 284–89. doi:10.1109/TIT.2002.806129. (2003).
9. Barkan, E., Biham, E.: *Conditional Estimators: An Effective Attack on A5/1*. Selected Areas in Cryptography 1–19. (2005).
10. Barkan, E., Birham, E., Keller, N.*: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*. Crypto 600–16. (2003).
11. Klein, G.O.: *Trusted Health Information Systems*. A project within the DGXIII INFOSEC programme on Electronic signatures and trusted third party services. Final deliverable. Part 1. Requirements on electronic signature services. 1-87 (1995).
12. Klein, G.O.: *Trusted Health Information Systems*. Final deliverable. Part 2. Trusted Third Party Services. Version 2 January: 1-54 (1995).
13. Klein, G.O. *Trusted Health Information Systems - Management Summary*. December: 1-16 (1994).
14. Schmid, G.: *On the existence of a global system for the interception of private and commercial communications* (ECHELON interception system), (2001/2098(INI))" (pdf – 194 pages). European Parliament: Temporary Committee on the ECHELON Interception System. (2001).