



**Roskilde
University**

Contentious expertise

Hacking mobile phones, changing mobile technology

Jørgensen, Niels

Published in:
First Monday

DOI:
[10.5210/fm.v27i3.11512](https://doi.org/10.5210/fm.v27i3.11512)

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Jørgensen, N. (2022). Contentious expertise: Hacking mobile phones, changing mobile technology. *First Monday*, 27(3). <https://doi.org/10.5210/fm.v27i3.11512>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain.
- You may freely distribute the URL identifying the publication in the public portal.

Take down policy

If you believe that this document breaches copyright please contact rucforsk@kb.dk providing details, and we will remove access to the work immediately and investigate your claim.

Contentious expertise: Hacking mobile phones, changing mobile technology

by Niels Jørgensen

Abstract

The concept ‘contentious expertise’ is proposed to account for technological expertise applied in technological controversies. Activists from the Chaos Computer Club, a German hacker group, adapted contentious expertise when they built a so-called clone of a mobile phone SIM card in 1998, and used the clone to publicly make a phone call — free of charge. The activists blamed the secret design of SIM cards, and subsequently, the design was changed and made fully public. The activists’ technical knowledge was crucial for the success of the hack. The paper ask how novel was the knowledge used in the hack, how did the activists acquire their knowledge in the first place, and were the hackers right in believing that their hack would always work?

Contents

[Introduction](#)

[Research method and organization of the paper](#)

[The Chaos Computer Club](#)

[The activists’ belief in design openness](#)

[The GSM Association](#)

[The GSM Association’s secrecy](#)

[How does a SIM card identify a user?](#)

[The German hack and its Californian precursor](#)

[Impact on mobile design](#)

[In what areas of engineering did the activists have technical expertise?](#)

[Question 1: How novel was the SIM card hack?](#)

[Question 2: How did the activists acquire contentious expertise?](#)

[Question 3: In what ways may we see the activists’ knowledge as uncertain and incomplete?](#)

[Discussion of contentious expertise](#)

[Conclusion](#)

Introduction

The SIM card hack by the Chaos Computer Club in 1998 was devastating to GSM (Global Systems for Mobile Telecommunications). It demonstrated that customers could not trust billing records. This was because the call made using the clone was billed to the owner of the original SIM (Subscriber Identity Module) card. In 1998, GSM completely dominated the European mobile phone market, and had approximately 100 million subscribers worldwide (Hillebrand, 2002).

The hackers' demonstration that there was a fault in the 'secret' SIM card design was one factor — out of several, to be discussed later in this paper — that led to a redesign of the card. The Universal Mobile Telecommunication System (UMTS) was launched in 2001 as the successor of GSM. It had a fully public SIM card design. UMTS was the first mobile system available worldwide which provided now familiar Internet services to users, such as e-mail accessibility and Web browsing. By abandoning GSM's approach of secrecy, UMTS supported these services with technology that was more trustworthy, because the public design could be scrutinized by independent experts.

This paper proposes the concept 'contentious expertise' to account for technological expertise applied in technological controversies.

The adjective 'contentious' may be defined as "causing, involving, or likely to cause disagreement and argument" (Cambridge Dictionary, 2020).

Contentious expertise is technological expertise that is

- involved in publicly criticizing or making demands about a technology, such as when the activists claimed that the GSM must abandon its secrecy;
- held by participants in a sustained campaign or social movement, such as the Chaos Computer Club, as opposed to an isolated event; and
- where the campaign or movement employs disruptive, political action, such as conducting a hack, as opposed to working merely inside established institutions.

This definition is inspired by the concept of contentious social movements suggested by Tilly [1]. Consider a contentious social movement in Tilly's sense, and assume that it is concerned with technology, and that technical experts participate collectively in the movement; then their expertise is 'contentious expertise'.

The paper's first contribution is the concept of contentious expertise. The concept suggests that an analysis of the SIM card hack should account for the activists' contention — their critique of GSM's secrecy and their disruptive hack — as well as their technical expertise.

The idea that activists have expert knowledge may be controversial both in practical and academic contexts. In practice, the Club's criticisms were at times discarded as unqualified. For instance, the Deutsche Bundespost (German Post Office) rejected the activists' critique of the Bundespost's so-called BTX system as "nonsense" or "Unfug" (Schönherr, 1999). Eventually the activists hacked the BTX system, as discussed below.

Even in academia, some theories of technology and social movements assume that those opposing a technology are inherently non-experts. This includes Feenberg's (1999) critical theory of technology. Feenberg examines conflicts where a dominant technology (which he terms a 'program'), is challenged by a movement ('anti-program'). I find Feenberg's approach very inspiring. It applies well to the program side of this controversy in 1998, as GSM dominated mobile telephony in Europe.

However, the account in Feenberg's theory of the social movement side may be insufficient, because it assumes one side is always 'lay' or 'non-expert'. If expertise is used in a movement, it is supplied from outside the ranks of the movement's participants. Feenberg provides an example of software engineers helping newspaper workers in Sweden develop alternative ways of computerizing newspaper production [2].

The paper's second contribution is a characterization of activists' technical knowledge. This knowledge enabled them to carry out the hack, as opposed to merely criticizing mobile technology. The analysis uses concepts from Vincenti (1990) and attempts to answer three questions:

Question 1: How novel was the Club's SIM card hack? Specifically, may we characterize it using Vincenti's concept of 'radical design'? This paper finds that the hack was more akin to 'normal design' [3].

Question 2: How did the activists acquire contentious expertise? This analysis suggests that a substantial part of the activists' technical knowledge was generated by participation in the Club's activities. This is related to Vincenti's finding that engineering knowledge originates mainly from within engineering, as opposed to applying knowledge from physics or other disciplines [4].

Question 3: In what ways may we see the activists' knowledge as uncertain and incomplete? Vincenti notes that engineering decisions are frequently made "on the basis of incomplete or uncertain knowledge" [5]. Analysis subsequent to the hack has shown that there was a defense which the activists were unaware of and which could have made the attack fail.



Research method and organization of the paper

This paper's historical account of the SIM card controversy focuses on two actors: the Club and the GSM Association. This is as in social constructivist approaches to technology studies. Social constructivism, as represented by Bijker (1997), emphasizes that technological development is not pre-determined. To understand why one design has come to prevail over another, the approach

emphasizes concrete, historical studies of the social groups involved in a controversy. The paper's historical study of the two actors is mainly literature-based.

Empirical data about the SIM card hack is from a personal interview with a Club spokesperson who took part in the hack, and an archive of the Club's Web site in 1998. The archive contains computer programs and photos of artifacts used in the hack. Data was obtained also from e-mail interviews with three Californian security experts; they had designed and published the SIM card attack that the Club implemented.

The paper is organized in two parts. The first part asks: what was the SIM card conflict about — what was the contention about? This comprises an analysis of how the two actors came to believe in design openness and secrecy, respectively. This part also contains a description of the actual hack and a discussion of the impact on future mobile technology.

The second part discusses the three research questions about the activists' technical knowledge. The activists were the weaker side in the controversy with the powerful GSM Association — what did the hackers learn that gave them the upper hand, and how did they learn it?



The Chaos Computer Club

The origin of the Chaos Computer Club was a series of meetings held in West Berlin in 1981. They were held at the offices of the leftist newspaper *Die Tageszeitung* and organized by Wau Holland.

This section's sketch of the Club's history emphasizes how Holland and the other activists came to see hacking as a means of demonstrating their technical expertise. The SIM card hack demonstrated that they were right in claiming that its secret design was insecure.

A manifesto-style article entitled "The Chaos Computer Club introduces itself" was published in 1984 in the first issue of the Club's journal, *Die Datenschleuder (Data Slingshot)*. The article expressed political or ethical values in support of unrestricted, decentralized computer-based communication. The manifesto used a radical language, promising to stand up against the fear, stupidity and censoring by "international corporations, postal monopolies and governments" (Holland, 1985a).

In comparison, the activists used a moderate language in their media campaign over the SIM card hack 14 years later. The activists emphasized the need for consumer protection ("Aussichten eines Klons," 1998). This referred to protecting users against having their SIM cards cloned and so having to pay for clone-based calls.

The shift from anti-capitalism in the early 1980s to consumer protection in the 1990s might indicate that the Club's beliefs had changed fundamentally. In turn this may question whether the Club was a contentious social movement in Tilly's sense, because this requires elements of continuity and coherent focus.

The remainder of the section argues that the Club did indeed have a coherent focus on hacking, provocation and telephony. The three elements are discussed using an anecdote about Holland as a starting point. At a memorial event after the death of Holland in August 2001, Tim Pritlove recalled that:

[Holland] always had a screwdriver with him [...] If you asked him why he had a screwdriver, he said, ‘Well, I might have to make a phone call.’ (Kettmann, 2001).

The anecdote indicates, firstly, that hacking was essential to the Club. Holland would use a screwdriver constructively, to build, or destructively, to tamper with something. A similar duality holds for other tools used in hacking. The Club always presented itself as a group for hackers. For instance, the first issue of *Die Datenschleuder* contained an article entitled “Hardware für Hacker”.

Holland demonstratively used a screwdriver in a public presentation at a data protection conference in 1984. He used it to open a so-called connection box used with the Bildschirmtext (BTX) video system marketed by Deutsche Bundespost. The Club had criticized the security of BTX, and the Bundespost had rejected the criticism as “nonsense” (Schönherr, 1999).

Holland made his point by opening the box, that is, bypassing its sealing. Then he showed how he could replace a device for user identification. Holland’s critique of BTX’s security was reported on national television. The report included video recording of the point in Holland’s speech where he physically hacked (opened) the box (*Heute Journal*, 1984). This indicated to activists that if their opponents were fending them off as amateurs talking nonsense, a public hack could demonstrate their expertise.

The Club’s hacks were public in the sense that the activists consistently published technical details. This included computer programs used in the SIM card hack and in the ‘bank robbery’ hack, discussed below. In terms of Alexandra Samuel’s taxonomy of hacking, the public approach suggests that the Club’s hacking was ‘transgressive hacking’ rather than ‘outlaw hacking’ (Samuel, 2004). Transgressive hacking operates in what Samuel calls a legally ambiguous zone, similar to civil disobedience as in civil rights movements. Transgressive hacking is conducted with a political end and does not cause direct harm. Finally, the Club’s activists used their real names, also a characteristic of transgressive hacking.

The Club’s approach to hacking was, however, challenged in the late 1980s. In two cases, people affiliated with the Club hacked in secrecy and for financial gain, rather than political goals. In one of them, two individuals were eventually convicted (with suspended sentences) in 1990 by a court in West Germany, for breaking into U.S. military computer systems and selling material to the KGB (Stoll, 1989, 1988).

In the ensuing crisis in the Club, Holland condemned the hacks [6]. Today, the Club’s ethic can be described simply as “Mülle nicht in den Daten anderer Leute” or “Do not mess with other people’s data” (Chaos Computer Club, 2021).

Pritlove’s anecdote indicates, secondly, an element of humorous provocation. A screwdriver is usually not needed for making phone calls, of course. Even the manifesto from 1984 was humorous. It included a list of 11 so-called immediate goals. The last was: “Everything that’s fun and cheap”.

The term ‘Chaos’ is itself provocative. It is used in the Club’s conference, The Chaos Communication Congress (held annually since 1984 with the 2020 and 2021 events occurring online), and the Club’s radio program, *Chaosradio* (<https://chaosradio.de>). The German nouns *Chaot* and *Chaotin* connote individuals (masculine or feminine) who may participate, say, in public marches — and possibly aim a slingshot at you, or hack you.

Thirdly, the memorial anecdote indicates that the Club was interested in telephony. SIM cards are used for telephony; even in the early 1980s the activists were preoccupied with telephony.

Club activists in 1984 conducted a “virtual robbery” of a bank connected to the BTX system mentioned earlier. The system used telephone cables for data transmission. Online banking was one of the two most popular service types in BTX, according to Gröndahl (2000), the other being pornography. The “robbery” was of Hamburger Sparkasse, the biggest savings bank in Western Germany at that time. The amount stolen was 134,635 Deutsche Marks or approximately \$US50,000 in 1984. The activists swiftly re-transferred the sum to the bank, blaming weak security allowing the robbery possible.

The manifesto quoted earlier mentioned “postal monopolies”. In Western Germany, Deutsche Bundespost (or the Post) was a state-run monopoly of both postal and telephone services. Telephony in the early 1980s used land-line cables, as opposed to mobile technology. The Post controlled all aspects of the BTX system.

The Post also controlled an individual’s access to the Internet in the 1980s. An individual needed a Post-endorsed modem to connect a computer via the telephone network. The Club’s *Hacker Bible* (*Hackerbibel*) contained instructions for building an alternative modem [7], so again the activists challenged the monopoly of the Post.

Gröndahl (2000) called the Deutsche Bundespost the major enemy (*Hauptfeind*) of the Club. Jokingly, Kargl (2002) wrote that the Post was the Club’s declared class enemy (*Erklärter Klassenfeind*).

Public estimates of the Club’s membership range from 3.000 to 4.500 (Dobusch, 2014; Kubitschko, 2015). Dobusch noted that the Club possessed limited economic resources and no professional staff, in contrast to the sometimes huge organizations supporting environmental movements. The activists’ apparent lack of resources underpinned one question: How were the activists able to influence mobile technology?



The activists’ belief in design openness

The activists claimed that GSM’s SIM card design was based on ‘insecurity by obscurity’ (*Unsicherheit bei Geheimnismäkeri*) (Bach and Riger, 1998). The phrase was a polemical, or contentious, negation of what is known as Kerckhoffs’ principle. This section describes Kerckhoffs’ principle and discusses how it became an important part of the activists’ beliefs.

Kerckhoffs (1883) formulated six principles pertaining to cryptographic systems. He stated the particular principle that now carries his name as follows:

The system must not require secrecy, and can be stolen by
the enemy without causing trouble. (Petitcolas, 2019)

The argument underlying Kerckhoffs' principle is: For a system to withstand analysis by an enemy, the proposed design should be made public, to increase the likelihood that weaknesses are found by independent experts and others before the system is deployed, so that the weaknesses can be removed; rather than be exploited by an attacker after deployment. A contemporary textbook reformulation of the principle is "the secrecy must rely entirely in the key" [8].

Kerckhoffs' principle is consistent with the Club's early values as expressed in the Club's manifesto. Yet, those values were expressed rather abstractly, for instance as "Freedom for data" [9]. By contrast, Kerckhoffs' principle is a specific design principle. The Club's adaptation of Kerckhoffs' principle is suggested to be related to the following two developments in digital technology in the 1990s.

The first development is the crypto controversy fought out mainly in the United States. The government position was that strong encryption would be (ab)used by criminals. Therefore intelligence and law enforcement agencies, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), needed a way to bypass strong encryption. Strong encryption refers to encrypting a message in a way that makes it practically impossible to decrypt the message. That is, impossible even for a big-budget agency, and even if it knows the encryption method — but of course not the encryption key.

The other side of the crypto controversy argued for an individual's right to privacy and its protection by strong encryption. This side included civil rights organizations, such as the Electronic Frontier Foundation (EFF), established in 1990 by Michell Kapor and others (Kapor, 1991), and more loosely organized initiatives, such as the community of cypherpunks (Hughes, 1993).

The privacy side saw the controversy as related to Kerckhoffs' principle. There was a widely held suspicion that the then dominant encryption algorithm, DES, had a so-called 'backdoor' that allowed the NSA to access encrypted data (Callas, 2006). The suspicion was based on the fact that the NSA had insisted on a change to an internal mechanism of DES (its so-called S-boxes). The agency refused to say why it insisted on the change.

In other words, while DES's design *per se* was public, the agency's design motivation was kept secret. Eventually it turned out that NSA's S-box changes had strengthened the security of DES (Coppersmith, 1994). But the general suspicion of secret designs and design motivations remained.

Moreover, the outcome of the crypto controversy also supported beliefs in Kerckhoffs' principle. The controversy ended in 1997–2001 when the U.S. government leaned toward privacy. This was when the Advanced Encryption System (AES) was standardized by the National Institute of Standards and Technology (NIST).

The AES algorithm is completely public. Prior to selecting the algorithm, NIST supported public discussions of its pros and cons, as well as those of a set of alternative algorithms (Dworkin, 1999).

NIST provided both a public design and a public design motivation — in accordance with Kerckhoffs’ principle.

Club activists were aware of the crypto controversy. A *Datenschleuder* article from 1994 explained the risk associated with a government-installed backdoor:

A system with a backdoor is like a bank with an open toilet window. Once you have found it, you can do anything.
[\[10\]](#)

The second development which may be related to the Club’s adaptation of Kerckhoffs’ principle is the emergence of the open source movement. Open source permits users to use, modify and redistribute software (Feller, *et al.*, 2005).

In the 1990s, the open source movement gathered momentum. The first version of the operating system Linux was released in 1991. In 1998, the first version of KDE (Kool Desktop Environment) was released. KDE was a full package of open source desktop software, including a graphical user interface, Web browser, text processor and more, with Linux underneath.

In the later half of the 1990s, RedHat and other commercial distributors of open source software emerged. Robert Young of RedHat phrased the difference between open and proprietary source as a question of user control when he asked rhetorically:

Would you buy a car with the hood welded shut?
(McHugh, 1998)

Similarly the activists were asking: how can you trust GSM’s mechanism for authenticating a user, if the mechanism is not public? That is, if you can’t “unscrew” the technology?



The GSM Association

The other side of the SIM card conflict in 1998 was the GSM Association (GSMA). SIM cards were standardized as part of the overall GSM standard, which was controlled by the GSMA. The organization’s members were mobile service providers and manufacturers of mobiles and network equipment. Moreover, the GSMA was backed by the European Commission. Thus, the GSMA was a very powerful organization — and confronting it seemed as asking for an unequal battle.

The first commercial GSM network was launched in 1992. Throughout the 1990s, GSM was based in Europe. As a trans-European standard, GSM was convenient for users, because standardization would allow the same phone be used in any country covered by a GSM service provider.

European state-run, national service providers drove the initial development of GSM. This included the Club’s acquaintance, Deutsche Bundespost. GSM was also termed a second generation mobile

system. This referred to the previous analog or first generation mobile systems. Significantly, there had been no cross-European standard for first generation systems. Also, the state-run service providers had failed to agree on a standard for online video. Instead they had developed national systems such as BTX (in Germany, as discussed earlier) and Minitel (in France, run by France Télécom).

In 1987, a memorandum was signed by 14 national service providers. The memo stated that GSM was to be an open, non-proprietary standard (Groupe Spéciale Mobile, 1987). Based on the memorandum and the national service providers, a decision making body was formed, the GSM MoU Group. MoU referred to a “memorandum of understanding”.

The GSM Association was formed in 1995, replacing the MoU Group. For simplicity, in the remainder of the paper, the name GSMA is used to refer also to the MoU Group that existed 1987–1995.

Manufacturers of mobiles and network equipment were invited in 1987 to participate in the development of the GSM standard on an equal basis with the providers. The GSMA membership also included private service providers. Among them was D2, one of three German GSM providers in 1998. The SIM card that the Club hacked was issued by D2.

Finally, the European Commission played a key role in supporting GSMA and establishing GSM as a European standard. A central concern of the Commission was lowering consumer prices. Another was demonstrating that pan-European standards and competition would lead to lower costs (Pelkmans, 2001). The Commission’s promotion of GSM included supporting the allocation of radio frequencies, a scarce resource, to the new mobile standard.



The GSM Association’s secrecy

The overall GSM standard was public. A public design was crucial for inter-operation of equipment made by different manufacturers and managed by different service providers. Inter-operation, in turn, was crucial for user convenience and for attaining competition and lowering of consumer prices.

Why was the design of the SIM card’s mechanism for user authentication kept secret? This was the more remarkable since the mechanism was the cards’ most significant part. Recall that SIM is an acronym for subscriber identity module.

In practical terms, the GSM standard for SIM cards (European Telecommunications Standards Institute [ETSI], 1996) simply did not specify the details about user authentication. In the document, the mechanism for user authentication is termed A3 and is described merely at a general level — amounting to a requirements specification.

GSM service providers were free to choose their own algorithm to implement the A3 requirements. However, the GSMA recommended an algorithm named COMP128. It was provided only to

operators and manufacturers, and only on the basis of a non-disclosure agreement. According to Briceno, *et al.* (1998), COMP128 was used by nearly all GSM operators.

The GSMA never provided a public motivation for keeping COMP128 secret. One possible, partial explanation of GSMA's resistance to open design is pressure from European law enforcement agencies.

Participants in ETSI's standardization work in the 1980s have reported such pressure on their work on encryption in GSM. Encryption covered traffic between a mobile phone and a nearby radio station that picks up signals from a mobile. The original proposal suggested a 128 bit encryption key. Following intervention from several security agencies, the standard eventually mandated a key with only 64 bits (Klein, 2014).

Yet, from the point of view of an agency, poor user authentication is of limited value. Consider an agency wiretapping an encrypted conversation related to child pornography or war crimes investigation. Suppose the agency is able to break the encryption (because the encryption key is too short). This is of limited value if the identity of the users can not be trusted (because of poor user authentication). Therefore, a benign or malign agency, seeking surveillance in an unrestricted way, may want to promote weak encryption; but promoting weak authentication is not purposeful.

However, authentication and encryption were intermingled on SIM cards. Authentication was coupled to a mechanism for generating the 64 bit key for encryption. When COMP128 was eventually published (Briceno, *et al.*, 1998), it turned out that 10 of the bits generated for the key were always zero. Keeping COMP128 secret served to conceal that the encryption algorithm had been weakened to 54 from 64 bits (already down from 128 bits).

At the time of the SIM card hack in 1998, the secrecy extended to the identity of the organization that had designed COMP128. Actually, the algorithm had been developed by Deutsche Telecom (Walker and Wright, 2001). Deutsche Telecom had been formed by separation (in 1989) and privatization (in 1995) of the telecommunications part of the Club's old adversary — Deutsche Bundespost.



How does a SIM card identify a user?

Any user of GSM has held a SIM card in his or her hand, and inserted it into a mobile. In the standard scheme, a user receives a SIM card upon entering a subscription agreement. A SIM card identifies a given user. Activists claimed that the public had a right to know the details of the mechanism, not merely the requirements laid down in a standard (European Telecommunications Standards Institute [ETSI], 1996). The requirements are recapitulated in this section. A basic understanding of these requirements is needed to understand the activists' SIM card hack.

The requirements amount to what is known in cryptology as a message authentication code [11]. To employ this type of mechanism was uncontroversial.

SIM cards were part of GSM from the launch of the technology. The card contains a processor and storage. The surface has metallic contact points for transferring data between the card and the phone, and supplying power to the card. Originally, SIM cards were credit card-sized. In the late 1990s, a 25 by 15 millimeter format was introduced, featuring the familiar cut-away in one corner to guide users to insert the card correctly. In years following the hack, micro and nano cards were introduced. The smaller cards were introduced for convenience, not security. See [Figure 1](#).

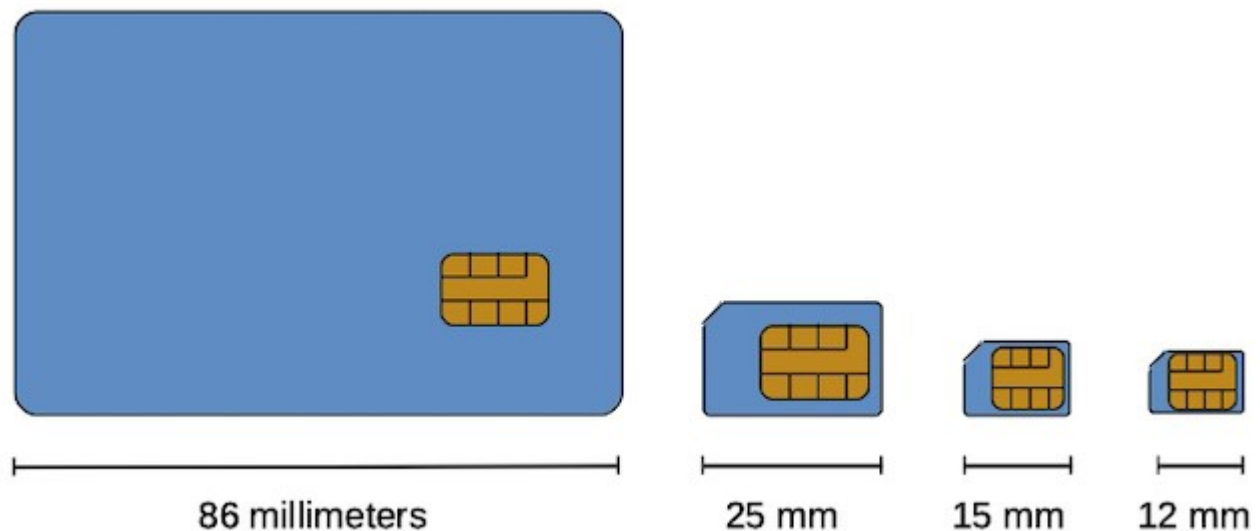


Figure 1: Ever smaller. SIM cards in credit card size and mini, micro and nano sizes.

Secure user-authentication was among the advantages ascribed to GSM (Pelkmans, 2001). By contrast, the landline telephone network and the first generation analog mobile systems had well-known security holes. Phone phreaking (an intentional misspelling of ‘phone freaking’) refers to a hacking practice, mainly in the 1960s in the U.S. Approaches included creating a 2,600-Hz tone to play into a telephone microphone in a public phone booth. John Draper, alias Cap’n Crunch (a toy whistle once included as a toy in a cereal by the same name in the U.S. generated this specific noise), claimed this sound enabled him to conduct long-distance calls for free (Rosenbaum, 1971).

Whistling a tone was an “analog” hacking approach that worked with the analog technology of the landline network. By contrast, SIM cards use digital technology and should protect against phone phreaking.

A SIM card operates similarly to a user logging into a computer, presenting a user name and a password.

The “user name” of the SIM card is a so-called IMSI (international mobile subscriber identity) number. The IMSI number identifies the subscriber and is stored on the card. It is public, and may

even be printed on the surface of the card. A convenient feature is that a user may change a phone number while retaining a specific IMSI number, keeping the SIM card.

The “password” of the SIM card is a secret key called K_i in the standard. The key is 128 bits. The subscript i suggests that each SIM card has a unique key. The key is so secret that a user is not allowed to access his or her own key. Keeping K_i secret is a matter of course and not controversial.

More specifically, the SIM card’s handling of its “username” and “password” elements is implemented as a so-called challenge-response protocol:

Challenge: The GSM network sends a challenge to the mobile phone. The challenge is called *RAND* and consists of 128 bits. The name indicates that it is chosen randomly. The mobile passes *RAND* on to the SIM card.

Response: The SIM card must send a 32-bit response back to the phone. The response is called *SRES*. The name should be read as “signed response”. Signing means that the SIM card must “sign” the response with the secret key K_i . The mobile phone then passes on *SRES* to the network. This process is described in [Figure 2](#).

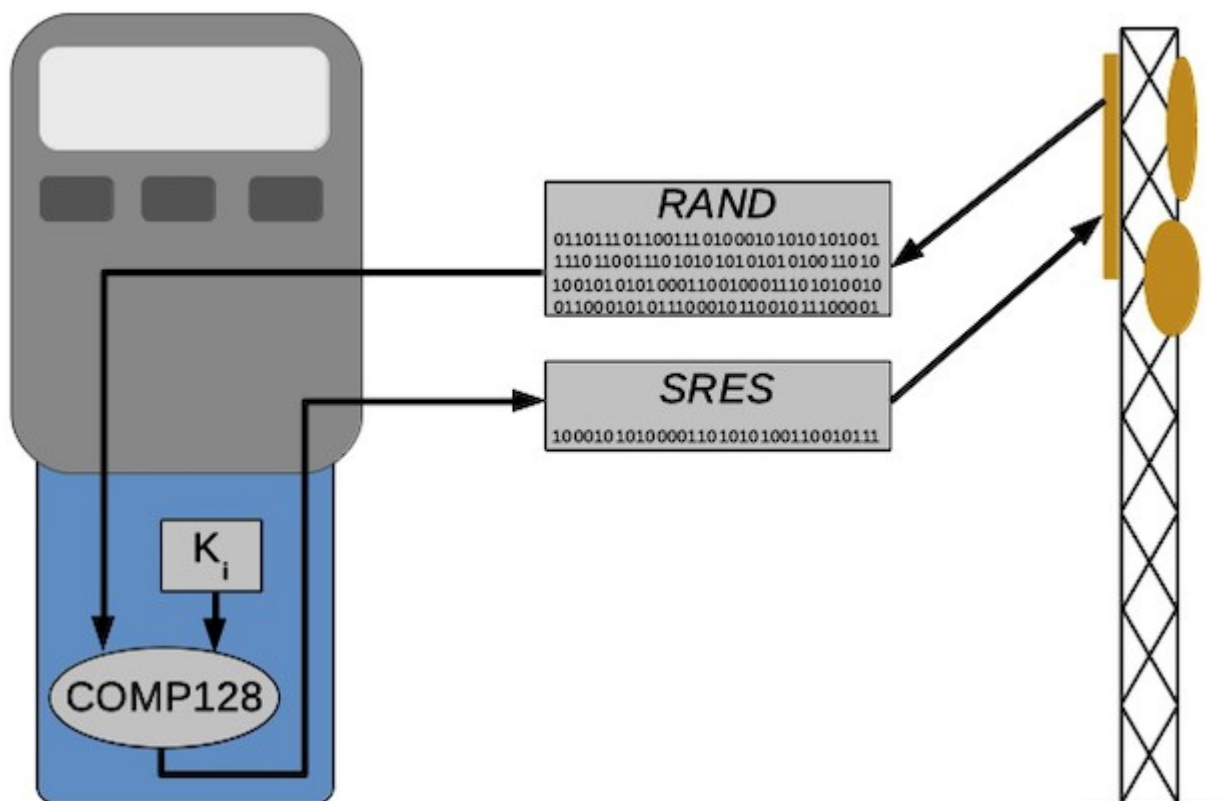


Figure 2: SIM card based user authentication by means of *RAND* and *SRES*.

Thus the SIM card employs A3 to compute *SRES* using two inputs: the challenge and secret key:

$$(*) SRES = A3(K_i, RAND)$$

The public requirements that pertain to A3 are that it must sign *RAND* in the following sense: Firstly, a party already in possession of K_i can confirm that K_i has been used in the computation of *SRES*. Specifically, the network confirms this by computing (*) and comparing the result with the *SRES* received from the mobile. The network has its own copy of K_i . Secondly, the response *SRES* must not reveal K_i to a party not in possession of it already.

While these general requirements were uncontroversial, the COMP128 algorithm that the GSMA had chosen for their implementation of A3 was not only secret — it was flawed.



The German hack and its Californian precursor

The Club's SIM card hack was published on 27 April 1998. This section describes the publication of the hack and how the hack depended on a Californian attack, by members of the Smartcard Developer Association. The subsequent section describes the effects of the hack on mobile design.

On 13 April 1998, three Californian security experts published the COMP128 algorithm used for SIM card-based user authentication. They said they “pieced together information on [the algorithm's] internal details from public documents, leaked information, and several SIMs [they] had access to” (Briceno, *et al.*, 1998). The publication was in the form of a program that implemented the COMP128 algorithm. The program was written in C, a widely used programming language (Kernighan and Ritchie, 1988).

Moreover, the Californians also published an attack to find the secret key K_i stored on a SIM card, exploiting a weakness in COMP128. They stated that their description of the attack, containing about 500 words, would enable security experts to implement an attack (Briceno, *et al.*, 1998).

Thus, the Californians, not the German activists, devised the SIM card attack. Similarly to the Club, the Californians took a stand in the design controversy, blaming GSM's secrecy:

As shown so many times in the past, a design process conducted in secret and without public review will invariably lead to an insecure system [...] (Briceno, *et al.*, 1998).

The Californians did not publicly demonstrate that their attack worked. Eric Hughes, author of “A cypherpunk’s manifesto,” had planned a public cloning to take place 18 April at a hacker club in San Francisco. Eventually he decided against conducting it, following threats of legal action from telecom companies (Savage, 1998). In a response to the press release, the U.S. mobile industry consortium, Cellular Telecommunications Association Industry [CTAI] (1998), described cloning as “illegal under federal law”.

The Californian attack was reported on the Web site of the Chaos Computer Club on 15 April, two days after the Californian press release.

The German activists went on to implement their own attack. The Club reported in a press release on 24 April that they had confirmed that an attack had worked.

The German activists went even further by publicly cloning a SIM card. They published all of the technical details about their attack on the Club’s Web site. The card that was cloned belonged to a *Spiegel* journalist who subsequently wrote about the hack (“Aussichten eines Klons,” 1998). The public cloning had not been planned, a Club spokesperson told me. A journalist, after reading the Club’s press release, contacted the Club and suggested they attempted to clone the SIM card of the journalist’s phone.

Der Spiegel in 1998 had a circulation of approximately one million, the largest in Europe for a weekly news magazine. The article explained the attack and interviewed representatives of the two parties. Jürgen von Kuczkowski, CEO of D2, acknowledged the hack, yet downplayed the risk, saying that for someone to produce a clone, “You would have to give away to someone you card and your PIN-code”.

Andy Maguhn-Müller from the Club insisted in the *Spiegel* article that customers were at risk when buying a mobile in a shop: “[...] the vendor has the card, and the PIN-code”. In other words: A mischievous vendor could theoretically produce a clone of a customer’s SIM card, selling the clone to a third party whose calls would be billed to a given customer.

The activists had demonstrated their criticism — and expertise — to a large European audience.



Impact on mobile design

The Universal Mobile Telecommunications System (UMTS), successor of GSM, embraced open design of SIM cards. In a sense, the SIM card controversy ended with a concession to the activists. This section discusses why. Frankly, I wish that I could argue that the main factor driving UMTS to embrace open design was the Californian and German hacks; this would underscore the significance of the activists’ contentious expertise. But as we shall see, there were other factors as well.

The GSM Association’s reaction to the hack indicated that the association was committed to keeping the SIM card design secret. The Association provided two new, secret algorithms, COMP128/2 and COMP128/3 (University of London, 2014). Those were alternative

implementations of A3. On the one hand, the releases indirectly acknowledged the weaknesses of COMP128. On the other hand, they maintained the principle of not making the design public.

As mentioned earlier, a partial explanation of GSMA's secrecy may have been pressure from intelligence agencies to promote and conceal that the GSM would use weak encryption. Eventually the replacements COMP128/2 and COMP128/3 were leaked, similarly to the original COMP128 (Munaut and Jos, 2015). The leak revealed that COMP128/2 would also only produce 54 significant bits. This damaged the reputation of the Association even more.

All three COMP128 variants remain available today from the Association (GSM Association, 2014). Somewhat stubbornly, GSMA persists in requiring non-disclosure agreements.

UMTS was intended to supersede GSM and become a global standard. The first commercial UMTS call was made in 2001.

In UMTS, similarly to GSM, user authentication was based on a smartcard and a challenge-response mechanism. The recommended algorithm, MILENAGE, had a public design (Pütz, *et al.*, 2001). It was in this sense that the changes pursued by the Californian security experts and German activists were actually made.

The Third Generation Partnership Project (3GPP), an industry consortium, oversaw development of UMTS. The 3GPP had a significant portion of non-European operators and manufacturers. Yet development of the standard covering user authentication (and other standards) was placed with the European Telecommunications Standards Institute (Rosenbrock and Andersen, 2002).

Other factors — beyond the hack of the COMP128 algorithm — may have influenced 3GPP to adopt an open design of the new cards.

The first factor is that 3GPP considered using an open design before the COMP128 hack. The risk of cloning was highlighted in a document accepted by a 3GPP security committee in 1997:

It is necessary to be able to deter, detect and prevent the use of cloned mobile terminal equipment. [12]

This advice appeared a year before the SIM card hack. Among the possible countermeasures, the document listed a criteria called “Algorithm maturity and exposure”. The criteria was explained as “Long-term existence of a (non-discredited) algorithm in the public domain may be an advantage since it will necessarily have resisted cryptanalytic attack” [13] — precisely the argument that underscoring Kerckhoffs’ principle.

A second event that may have influenced the adaptation of open design was the standardization of AES in 1997–2001. As mentioned in the context of Kerckhoffs’ principle, this standardization meant that an American agency was officially recommending an open design of an encryption algorithm.

3GPP was aware of NIST’s standardization of AES. MILENAGE, the new authentication method in UMTS, made direct use of AES. While user authentication and encryption, as noted earlier, are

independent tasks, one (user authentication) may use the other (encryption) in a subtask, as in UMTS' publicly defined MILENAGE.

Thus, there were at least two other factors that may have contributed to UMTS electing an open design, in addition to the Californian and German hacks.



In what areas of engineering did the activists have technical expertise?

Finally let's analyze the activists' technical knowledge and the role it played in the German hack.

The activists faced two main obstacles. The first was to obtain the secret key from the SIM card. This was similar to the Californian attack. As indicated earlier, the Californians provided only a high-level description of their approach, with no programming details. In an interview, the Californians said that they were not in contact with the Club activists and were not providing feedback on their implementation of the attack.

The Californian attack worked by "repeatedly asking the SIM to identify itself" (Briceno, *et al.*, 1998). The SIM card was removed from the phone, with a card reader connecting the card to a computer. SIM card readers were available for purchase, and would allow the computer to communicate with the SIM card like a phone. The Californian attack is outlined in [Figure 3](#).

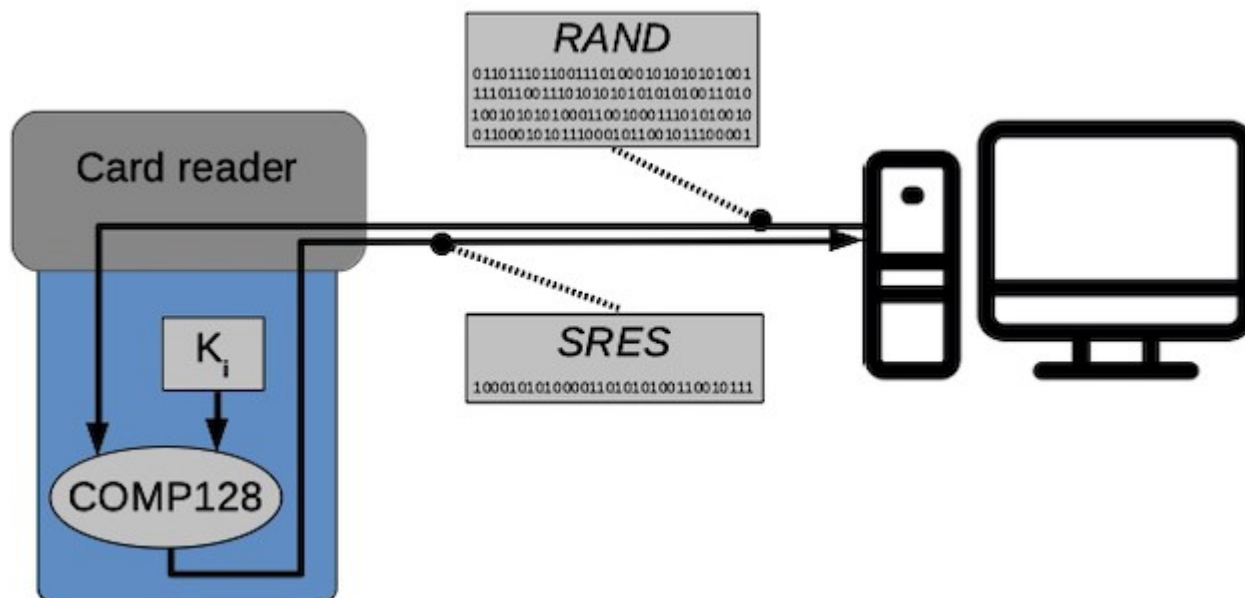


Figure 3: A graphic description of the Californian attack. The attack guesses K_i using approximately 150,000 queries. In each query, a *RAND* challenge is sent from a computer to the SIM card via a card reader. A *SRES* response is returned. Taken together, the card reader and the computer emulate a mobile phone asking the SIM card to authenticate.

In the attack, the computer sends queries to the card, as if the computer was a mobile network requiring identity information. The responses are stored on the computer, which makes a final analysis, guessing the secret key K_i .

The crucial property of the attack is that only 150,000 queries are needed. If the COMP128 algorithm had been designed properly, guessing the secret key would have to resort to a so-called brute force attack. An example brute force attack is the following approach in two phases. The first phase is to query the card once, using a particular value of *RAND*, say the value 0, so that the SIM card produces:

$$\text{COMP128}(K_i, 0)$$

The second phase is to run COMP128 on the computer, independently of the SIM card, with $K_i = 0, 1, 2, \dots$ to produce:

$$\text{COMP128}(0, 0), \text{COMP128}(1, 0), \text{COMP128}(2, 0), \dots$$

Each value produced by the computer is compared with the single value produced by the SIM card. Suppose that a computer-produced value is equal to the SIM card-produced value, say $\text{COMP128}(117, 0) = \text{COMP128}(K_i, 0)$. Then the particular value of K_i used by the computer (117) may be the secret key on the SIM card. A simple further check is required to establish that it is in fact the key.

However, the brute force approach requires trying all the 2^{128} possible values of the key. Given that a SIM card of the time would produce only three to four responses per second, the brute force approach requires approximately 10^{30} years. On average, the key will be found after trying only half the keys, but that's equally astronomical.

The idea underlying the Californian attack is to guess the secret key 16 bits at a time. The key's 128 bits are equal to 8 times 16 bits. The press release for the Californian approach explained that the stepwise approach worked because COMP128 exhibited a "lack of diffusion". This is the undesirable property that changing one bit of the input would effect only neighboring bits, and not bits further away from the changed bit.

In summary, for the activists to overcome the first obstacle required knowledge of programming and mobile security.

The second obstacle was to use the secret key K_i to create a clone. A clone of a SIM card is a card which appears to the GSM network to be the original SIM card, but is in fact a different card.

An obvious approach would be to write the secret key onto an existing SIM card, using the card reader employed in the first step. However, there is no straightforward way of doing so. GSM's standard (European Telecommunications Standards Institute [ETSI], 1996) does not define a command for writing a secret key to a card. Indeed, as an owner of a SIM card, you do not want your secret key to be overwritten.

The Californians, only days before they published the attack, purchased five SIM cards intended for testing, as they informed me in an interview. Unlike ordinary SIM cards, these special cards actually allowed for writing a new secret key to them. However, the Californians received the cards only after publication. Such cards were also not available to the German activists at the time of their hack.

Instead the Germans (and the Californians) used what may be termed a SIM card emulator. This consists of a self-made, physical card connected to a computer.

The self-made card is inserted into the mobile phone in the same way you would insert a regular card. The self-made card has the same contact points as a SIM card, so that it can communicate with the mobile. The activists used a credit card sized card (recall [Figure 1](#)). The size of the card made it easier to attach wires in order to connect it to the computer. See [Figure 4](#). For photos of the activists' self-made card, see the archive on the Club's Web site (Chaos Computer Club, 1998).

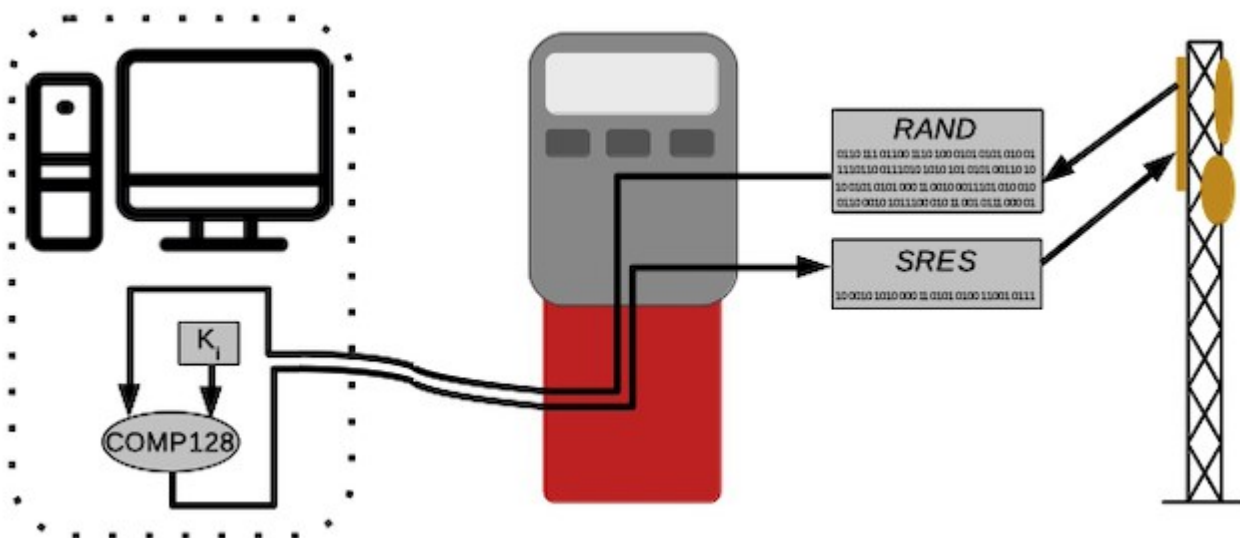


Figure 4: The clone built by the activists of the Chaos Computer Club is a self-made card (shown as red) connected to a computer.

The self-made card lacks the processing and storage capabilities of a regular SIM card. Instead, the computer stores the secret key K_i of the original SIM card. The computer, when provided with a

challenge *RAND* from the card, computes the value $\text{COMP128}(K_i, \text{RAND})$ and sends it back to the card. Then the card passes on the value to the mobile and network.

The use of a SIM card emulator restricts the mobility of the clone, since a wired connection to a computer is required. Still, one could make phone calls with the clone, such as expensive long distance calls billed to the owner of the original card.

In summary, to carry out the hack, the activists needed to overcome several obstacles, requiring technological expertise in the areas of programming, mobile network security and computer hardware.



Question 1: How novel was the SIM card hack?

This and the following sections answer three research questions. They aim at characterizing the activists' technical knowledge in terms of novelty (question 1), origin (question 2) and uncertainty (question 3). Taken together, these issues may help understand the overall role played in the hack by the activists' technical knowledge.

All three questions use concepts from Vincenti (1990) on engineering knowledge. Vincenti studied the historical evolution of aircraft wings and propellers as well as three other design cases from aeronautics. Vincenti defined engineering knowledge as concerned with design. More specifically, he defined engineering knowledge as:

[...] the practice of organizing the design, construction and operation of any artifice which transforms the physical world around us to meet some recognized need. [14]

So how novel was the Club's SIM card hack? Vincenti's definition of normal design includes:

The engineer engaged in such design knows at the outset how the device in question works, what are its customary features, and that, if properly designed along such lines, it has good likelihood of accomplishing the desired task.

Vincenti contrasts normal design with radical design, such as that involved in the development of the turbojet. Vincenti notes that "[...] normal design makes up by far the bulk of day-to-day engineering enterprise" [15].

As we have seen, the activists' work was based on a description published by Californian security experts, already known to work.

Indeed, it appears that even the Californians' work on designing the attack was normal rather than radical design. They wrote: "Within a day, Wagner and Goldberg had found a fatal cryptographic

flaw in COMP128”. They had realized that the COMP128 algorithm could be attacked using a technique from differential cryptanalysis (Briceno, *et al.*, 1998). That is, using a known technique.

A common characterization of hackers in the academic literature is in terms of a competence hierarchy. Top competency involves devising so-called zero day exploits. Zero day exploits are previously undiscovered vulnerabilities, and may be considered radical designs if the exploits are truly novel. At the bottom, the notion of script kiddies refers to copying the work of others. The competence hierarchy may reflect patterns of recognition in some hacker communities, as discussed in Jordan (2009).

In popular literature about hackers, talented hackers may even be described as geniuses (Dunlop, 2015). Perhaps Vincenti’s notion of normal design is welcome as a basis for a less hyped, and more chilly or cynical observation: yes, the activists were experts, but their technical work was of a normal, day-to-day engineering nature.



Question 2: How did the activists acquire contentious expertise?

A central idea in Vincenti’s work is that engineering is not “applied science”. Engineers do not acquire knowledge mainly by transferring notions from physics or other sciences. Instead, “knowledge used in normal design originates and develops mainly within engineering”, based on engineering practices that range from invention to production [16].

Parts of the activists’ knowledge was acquired inside the Club by reverse engineering. Reverse engineering is to observe the external behavior of a piece of equipment to determine its internal design, hidden from an observer.

The main person in the Club’s work on the SIM card emulator (recall [Figure 4](#)) had worked on telephony smartcards for several years. In 1995, the hacker received an eight-month suspended sentence. He was convicted of attempting to steal a card-based pay phone from a public phone booth (Schröder, 1999). Parts of the design of the Deutsche Bundespost’s public phones was secret, similarly to parts of the design of GSM’s SIM cards. So he needed to reversely engineer how the phone interacted with a user’s telephony smartcard. (Because he was building a card himself.)

Another instance of knowledge generated inside the Chaos Computer Club is described in Wagenknecht and Korn (2016). Wagenknecht and Korn studied the Club’s development of a local GSM network. That network serviced the Club’s annual congress from 2009 onwards. It included a radio station at the premises of the congress and a switch. A switch is software that connects callers and receivers. Club activists self-operated the somewhat unstable network, independently of a commercial service provider.

The development effort, termed ‘transgressive infrastructuring’ by Wagenknecht and Korn, included reverse engineering of software, because all GSM equipment available used proprietary software with secret source codes.

Question 3: In what ways may we see the activists' knowledge as uncertain and incomplete?

Vincenti notes that engineering decisions are sometimes made “on the basis of incomplete or uncertain knowledge” [17]. This is related to the precautionary principle. The discussion of this principle in “Late lessons from early warnings” contains 12 lessons, the first of which reads: “Acknowledge [...] uncertainty and risk [...]” [18].

The Californian description of the attack mentions the birthday paradox. The paradox predicts that certain events, such as finding the secret key, happens with a high probability, yet not full certainty [19]. Both the Californian and German activists appeared to be convinced that the probability of not finding the secret key was neglectable. For instance, in an article in *Die Datenschleuder*, the attack was summed up quite confidently: “By repeating this process [...] we can reconstruct the full key” [*Durch Wiederholen dieses Prozesses [...] können wir den gesamten Key rekonstruieren.*] (Bach and Riger, 1998).

Wray (2003) discovered a way of using the COMP128 algorithm that was not vulnerable to the Californian attack. Wray identified a set of “safe keys”. For instance, any key where the first eight bits are 00000000, and bits 64–71 are 00001010, is a safe key. If a SIM card contains a safe key, the key cannot be guessed using the attack designed by the Californian team.

Wray identified approximately 2^{76} different safe keys. He rightly asserted that the number of safe keys was “reasonable”, *i.e.*, that there were enough of them.

Rather than acquitting the COMP128 algorithm, Wray suggested an improved attack that required more time than the Californian attack.

Thus the hack could have failed. The mobile service operator D2 used COMP128 in the standard manner, so the hack succeeded. No GSM service providers have announced that they were using a defense based on Wray's safe keys.

Discussion of contentious expertise

This section argues that the concept of contentious expertise is robust in the sense of consistent with significant related work. Also this section argues that the paper's analysis of the Club's contentious expertise adds insights to this work.

The first piece of related work is Jamison's (2001) work on ‘green knowledge’. Green knowledge is knowledge of environmental issues held by participants in environmental movements. It comprises technical, cosmological (world view, ethical) and organizational elements [20]. Thus, similarly to

contentious expertise, green knowledge contains both technical and non-technical knowledge elements and is related to a social movement.

Green knowledge is acquired in what Jamison calls a ‘cognitive praxis’. This refers broadly to participation in movement activities. Jamison likens movements to schools [21]. Consistently the present paper found that movement participation was a source of knowledge (see question 2 earlier).

Jamison’s case studies focus entirely on non-technical knowledge elements. They include accounts of the political differences between ‘militant’, ‘community’ and ‘professional’ environmentalism. This paper supplements Jamison’s work by focusing not only on activists’ contentions, but also on their technical expertise.

The second piece is Vincenti’s work on engineering epistemology. We may ask if Vincenti’s epistemology is consistent with Feenberg and other assumptions that technological design, such as that of SIM cards, may be socially shaped?

Indeed, Vincenti was worried over “the current enthusiasm for the social shaping of technology”. In his study of the historical evolution of airplane landing gear he made the striking statement that:

... social considerations had little or nothing to do with shaping the form of the solution to the landing-gear problem. [22]

Vincenti notes that airplanes in the 1930s had different landing gear designs. These including fixed landing gears as well as gears that would, after take-off, retract into the body of the airplane. Subsequently, the retractable design became dominant. Vincenti claims that the prevalence of the retractable design is due merely to technical considerations. They include that even though the retractable design is heavier and more complex, it reduces drag, and so enables higher air speed than a fixed landing gear design.


Even though Vincenti holds that some designs are based entirely on technical considerations, his also notes that, in general, design is bound up with “social, personal, and environmental needs and constraints”. He terms these ‘contextual factors’. They may even have a “determining influence” [23]. Thus the idea that the design of SIM cards is socially shaped is consistent with Vincenti’s theory of engineering knowledge. We may see the activists’ belief in Kerckhoffs’ principle as a contextual factor in Vincenti’s sense.



Conclusion

This paper’s analysis of the SIM card hack in 1998 has suggested that the basis for the activists’ contention — their opposition to GSM’s design — was their belief in Kerckhoffs’ principle. In turn, this belief was rooted in the Club’s early ethical and political values, and formed also by the 1990s’ crypto controversy and open source movement.

Supplementing the analysis of the activists' contention, this paper analyzed their technical expertise, and suggested a threefold characterization that provides further insights into the hack: They were doing normal design in Vincenti's sense (question 1). They had acquired expertise by participating in previous hacks (question 2). Their knowledge was incomplete, so the attack could have failed (question 3).

There is a positive message in the story of the SIM card hack: Even when one side in a controversy related to Internet technology appears to be weaker — being a social movement, lacking financial resources, and opposing a dominant technology — then nevertheless it may acquire technical expertise, and successfully employ the expertise in disruptive hacks, in support of the movement's ends. The concept of contentious expertise may contribute to our understanding of such social movements. 

About the author

Niels Jørgensen is associate professor at the Department of People and Technology at Roskilde University. At the time of the SIM card hack in 1998, he worked for Nokia, a mobile phone and equipment manufacturer.

E-mail: nielsj [at] ruc [dot] dk

Notes

- [1.](#) Tilly, 2005, p. 308.
- [2.](#) Feenberg, 1999, p. 125.
- [3.](#) Vincenti, 1990, pp. 7–8.
- [4.](#) Vincenti, 1990, pp. 225–229.
- [5.](#) Vincenti, 1990, p. 7.
- [6.](#) Gröndahl, 2000, p. 75.
- [7.](#) Holland, 1985b, pp. 95–113.
- [8.](#) Schneier, 2015, p. 5.
- [9.](#) Holland, 1985a, p. 2.
- [10.](#) Chaos Computer Club, 1994, p. 18.
- [11.](#) Schneier, 2015, p. 31.

- [12.](#) European Telecommunications Standards Institute (ETSI), 1997, p. 24.
- [13.](#) European Telecommunications Standards Institute (ETSI), 1997, p. 33.
- [14.](#) Vincenti, 1990, p. 6.
- [15.](#) Vincenti, 1990, pp. 7–8.
- [16.](#) Vincenti, 1990, pp. 225–229.
- [17.](#) Vincenti, 1990, p. 7.
- [18.](#) Harremoës, *et al.*, 2001, p. 168.
- [19.](#) Schneier, 2015, p. 166.
- [20.](#) Jamison, 2001, p. 69.
- [21.](#) Jamison, 2001, p. 45.
- [22.](#) Vincenti, 1994, pp. 28, 31.
- [23.](#) Vincenti, 1990, pp. 11–12.

References

- “Aussichten eines Klons,” 1998. *Der Spiegel* (27 April), pp. 98–99, and at <http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/7870350>, accessed 26 May 2021.
- Andreas Bach and Frank Riger, 1998. “GSM security by obscurity,” *Die Datenschleuder*, number 63, at <https://ds.ccc.de/pdfs/ds063.pdf>, accessed 26 May 2021.
- Wiebe Bijker, 1997. *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge, Mass.: MIT Press.
- Marc Briceno, Ian Goldberg and David Wagner, 1998. “Smartcard Developer Association Clones Digital GSM Cellphone,” press release, 13 April, at <http://www.isaac.cs.berkeley.edu/isaac/gsm-press.html>, accessed 26 May 2021.
- Jon Callas, 2006. “An introduction to cryptography,” *PGP Corporation*, at <http://cisweb.bristolcc.edu/~ik/Download/CIT18/IntroToCrypto.pdf>, accessed 14 May 2021.
- Cambridge Dictionary, 2021. “Contentious,” at <https://dictionary.cambridge.org/us/dictionary/english/contentious>, accessed 26 May 2021.

Cellular Telecommunications Association Industry (CTAI), 1998. "Cryptographers announce break in authentication encryption for GSM phones" (press announcement, 13 April), at <http://www.isaac.cs.berkeley.edu/isaac/wow.html#1358>, accessed 26 May 2021.

Chaos Computer Club, 2021. "Hackerethik," at <https://www.ccc.de/de/hackerethik>, accessed 26 May 2021.

Chaos Computer Club, 1998. "GSM cloning: Technischer Hintergrund," at <https://web.archive.org/web/19980505104007/http://www.ccc.de/D2Pirat/clone.jpeg>, accessed 26 May 2021.

Chaos Computer Club, 1994. "The Clipper Chip War," *Die Datenschleuder*, number 47, at <https://ds.ccc.de/pdfs/ds047.pdf>, accessed 26 May 2021

Don Coppersmith, 1994. "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, volume 38, number 3, pp. 243–250. doi: <https://doi.org/10.1147/rd.383.0243>, accessed 22 February 2022.

Leonhard Dobusch, 2014. "Digitale Zivilgesellschaft in Deutschland: Stand und Perspektiven 2014," at https://www.bewegungsstiftung.de/fileadmin/user_upload/bws/bridge/Anlage_1_-_Dobusch_2014_Analyse-Digitale-Bu_rgerrechtsbewegung.pdf, accessed 26 May 2021.

Steven Dunlop, 2015. *Hacking: Secrets to becoming a genius hacker*. North Charleston, S.C.: CreateSpace Independent Publishing Platform.

Morris J. Dworkin, 1999. "Second Advanced Encryption Standard Candidate Conference," *Journal of Research of the National Institute of Standards and Technology*, volume 104, number 4, at <https://nvlpubs.nist.gov/nistpubs/jres/104/4/html/j44ce-dwo.htm>, accessed 22 February 2022.

European Telecommunications Standards Institute (ETSI), 1997. "Security principle for UMTS. UMTS 33.20," version 3.0.1, at https://www.3gpp.org/ftp/Specs/archive/33_series/33.20U/3320U-301.zip, accessed 26 May 2021.

European Telecommunications Standards Institute (ETSI), 1996. "GSM 11.11. Specification of the subscriber identity module. Version 5.3.0," https://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsm1111v050300p.pdf, accessed 26 May 2021.

Andrew Feenberg, 1999. *Questioning technology*. London: Routledge. doi: <https://doi.org/10.4324/9780203022313>, accessed 22 February 2022.

Joseph Feller, Brian Fitzgerald, Scott A. Hissam and Karim R. Lakhani (editors), 2005. *Perspectives on free and open source software*. Cambridge, Mass.: MIT Press.

Boris Gröndahl, 2000. *Hacker*. Hamburg: Rotbuch.

Groupe Spéciale Mobile, 1987. "Memorandum of understanding on the implementation of a pan European 900 MHz digital cellular mobile telecommunications service by 1991" (7 September), at

https://www.engagingwithcommunications.com/Technology/Mobiles/GSM/GSM_MOU_1987.pdf, accessed 26 May 2021.

GSM Association, 2014. “Rules for the management and distribution of the COMP128 family of example A3 and A8 algorithms,” version 3.6 (16 December), at <https://www.gsma.com/newsroom/wp-content/uploads/SG.03-v3.61.pdf>, accessed 26 May 2021.

Poul Harremoës, David Gee, Malcolm MacGarvin, Andy Stirling, Jane Keys, Brian Wynne and Sofia Guedes Vaz, 2001. “Late lessons from early warnings: The precautionary principle 1896–2000,” *European Environment Agency*, at https://www.eea.europa.eu/publications/environmental_issue_report_2001_22, accessed 22 February 2022.

Heute Journal, 1984. “Zweites Deutsches Fernsehen” at <https://www.youtube.com/watch?v=xPkYRho9VGc>, accessed 28 April 2021.

Friedhelm Hillebrand (editor), 2002. *GSM and UMTS: The creation of global mobile communications*. Chichester: Wiley.

Wau Holland, 1985a. “Der Chaos Computer Club stellt sich vor,” *Die Hackerbibel*, Teil 1, Hamburg: Lörbach, p. 137.

Wau Holland, 1985b. *Die Hackerbibel*. Hamburg: Lörbach.

Eric Hughes, 1993. “A cypherpunk’s manifesto,” at <http://www.activism.net/cypherpunk/manifesto.html>, accessed 26 May 2021.

Andrew Jamison, 2001. *The making of green knowledge: Environmental politics and cultural transformation*. Cambridge: Cambridge University Press.
doi: <https://doi.org/10.1017/CBO9780511489143>, accessed 22 February 2022.

Tim Jordan, 2009. “Hacking and power: Social and technological determinism in the digital age,” *First Monday*, volume 14, number 7, at <https://firstmonday.org/article/view/2417/2240>, accessed 26 May 2021.
doi: <https://doi.org/10.5210/fm.v14i7.2417>, accessed 22 February 2022.

Michell Kapur, 1991. “Civil liberties in cyberspace,” *Scientific American*, volume 265, number 3, pp. 158–160, 162, 164.
doi: <http://dx.doi.org/10.1038/scientificamerican0991-158>, accessed 22 February 2022.

Frank Kargl, 2002. “Hacker,” slides from a public CCC meeting in Ulm, Germany, at <https://docplayer.org/18941055-Hacker-frank-kargl-chaos-computer-club-ulm-frank-kargl-ulm-ccc-de.html>, accessed 26 May 2021.

Auguste Kerckhoffs, 1883. “La cryptographie militaire,” *Journal des sciences militaires*, volume 9, number 5, pp. 5—38; version at https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf, accessed 22 February 2022.

Brian W. Kernighan and Dennis M. Ritchie, 1988. *The C programming language*. Second edition. Englewood Cliffs, N.J.: Prentice Hall.

Steve Kettmann, 2001. “Remembering a hacker’s hacker,” *Wired* (18 August), at <https://www.wired.com/2001/08/remembering-a-hackers-hacker>, accessed 26 May 2021.

Gunnar O. Klein, 2014. “Standardization of cryptographic techniques - The influence of the security agencies,” In: C. Gram, P. Rasmussen and S.D. Østergaard (editors). *History of Nordic computing 4*. Cham, Switzerland: Springer, pp. 321–327.
doi: https://doi.org/10.1007/978-3-319-17145-6_33, accessed 22 February 2022.

Sebastian Kubitschko, 2015. “Hackers’ media practices: Demonstrating and articulating expertise as interlocking arrangements,” *Convergence*, volume 21, number 3, pp. 388–402.
doi: <https://doi.org/10.1177/1354856515579847>, accessed 22 February 2022.

Josh McHugh, 1998. “For the love of hacking,” *Forbes* (10 August), at <https://www.forbes.com/forbes/1998/0810/6203094a.html#265c3d9279bc>, accessed 26 May 2021.

Sylvain Munaut and Tamas Jos, 2015. “comp128.c,” at https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/src/modules/rlm_eap/libeap/comp128.c, accessed 26 May 2021.

Jacques Pelkmans, 2001. “The GSM standard: Explaining a success story,” *Journal of European Public Policy*, volume 8, number 3, pp. 432–453.
doi: <https://doi.org/10.1080/13501760110056059>, accessed 22 February 2022.

Fabien Petitcolas, 2019. “The information hiding homepage,” at <https://www.petitcolas.net/kerckhoffs/index.html>, accessed 26 May 2021.

Stefan Pütz, Roland Schmitz and Tobias Martin, 2001. “Security mechanisms in UMTS,” *Datenschutz und Datensicherheit*, volume 25, number 6, pp. 1–10.

Ron Rosenbaum, 1971. “Secrets of the little blue box,” *Esquire*, volume 76 (1 October), pp. 117–125, and at <https://classic.esquire.com/article/1971/10/1/secrets-of-the-blue-box>, accessed 26 May 2021.

Karl Heinz Rosenbrock and Niels Peter Skov Andersen, 2002. “The Third Generation Partnership Project (3GPP),” In: Friedhelm Hillebrand (editor). *GSM and UMTS: The creation of global mobile communications*. Chichester: Wiley, pp. 221–246.
doi: <https://doi.org/10.1002/0470845546.ch9>, accessed 22 February 2022.

Alexandra Whitney Samuel, 2004. “Hackivism and the future of political participation,” Ph.D. dissertation, Harvard University, at <https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hackivism-entire.pdf>, accessed 26 May 2021.

Annaliza Savage, 1998. “Cell-phone security far from airtight,” *Wired* (13 April), at <https://www.wired.com/1998/04/cell-phone-security-far-from-airtight>, accessed 26 May 2021.

Maximilian Schönherr, 1999. “Friendly Hack. Wau Holland erinnert sich an den Btx-Hack vor 15 Jahren.” *c’t — Magazin für Computer Technik* (5 November), at <https://www.heise.de/ct/artikel/Friendly-Hack-287340.html>, accessed 26 May 2021.

Bruce Schneier, 2015. *Applied cryptography*. Second edition. New York: Wiley.
doi: <https://doi.org/10.1002/9781119183471>, accessed 22 February 2022.

Burkhard Schröder, 1999. *Tron: Tod eines Hackers*. Hamburg: Sachbuch.

Clifford Stoll, 1989. *The cuckoo’s egg: Tracking a spy through the maze of computer espionage*. New York: Doubleday.

Clifford Stoll, 1988. “Stalking the wily hacker,” *Communications of the ACM*, volume 31, number 5, pp 484–497; version at <http://pdf.textfiles.com/academics/wilyhacker.pdf>, accessed 26 May 2021.
doi: <https://doi.org/10.1145/42411.42412>, accessed 22 February 2022.

Charles Tilly, 2005. “Introduction to Part II: Invention, diffusion, and transformation of the social movement repertoire,” *European Review of History*, volume 12, number 2, pp. 307–320.
doi: <https://doi.org/10.1080/13507480500269134>, accessed 22 February 2022.

University of London, 2014. “Design of authentication algorithms for GSM phones,” at <https://impact.ref.ac.uk/casestudies/CaseStudy.aspx?Id=30194>, accessed 22 February 2022.

Walter G. Vincenti, 1994. “The retractable airplane landing gear and the Northrop ‘anomaly’: Variation-selection and the shaping of technology,” *Technology and Culture*, volume 35, number 1, pp. 1–33.
doi: <https://doi.org/10.2307/3106747>, accessed 22 February 2022.

Walter G. Vincenti, 1990. *What engineers know and how they know it: Analytical studies from aeronautical history*. Baltimore, Md.: Johns Hopkins University Press.

Susann Wagenknecht and Matthias Korn, 2016. “Hacking as transgressive infrastructuring: Mobile phone networks and the German Chaos Computer Club,” *CSCW ’16: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pp. 1,104–1,117.
doi: <https://doi.org/10.1145/2818048.2820027>, accessed 26 May 2021.

Kim Walker and Tim Wright, 2001. “Security,” In: Friedhelm Hillebrand (editor). *GSM and UMTS: The creation of global mobile communication*. West Sussex: Wiley, pp. 385–406.

Stuart Wray, 2003. “COMP128: A birthday surprise” (11 May), at <http://www.stuartwray.net/comp128-a-birthday-surprise-rev.pdf>, accessed 26 May 2021.

Received 3 February 2021; revised 14 June 2021; accepted 2 August 2021.

Copyright © 2022, Niels Jørgensen. All Rights Reserved.

Contentious expertise: Hacking mobile phones, changing mobile technology
by Niels Jørgensen.

First Monday, Volume 27, Number 3 - 7 March 2022

<https://journals.uic.edu/ojs/index.php/fm/article/download/11512/10611>

doi: <https://dx.doi.org/10.5210/fm.v27i3.11512>