Experiences in Mobile Phone fraud

Jukka Hynninen
Helsinki University of Technology
Department of Computer Science and Engineering
Jukka.Hynninen@hut.fi

Abstract

Mobile phone services have and will be subject to fraud. This paper examines different types of fraud through examples. Reasons for fraud are explained, as are possible solutions to prevent fraud. Fraud types specific to certain analog and digital mobile phone technologies are presented, as well as broader types of fraud independent of the underlying technologies.

1 Introduction

Mobile communication has been readily available for several years, and is major business today. It provides a valuable service to its users who are willing to pay a considerable premium over a fixed line phone, to be able to walk and talk freely. Because of its usefulness and the money involved in the business, it is subject to fraud and criminal interest.

Some of the features of mobile communication make it an alluring target for criminals. It is a relatively new invention, so not all people are quite familiar with its possibilities, in good or in bad. Its newness also means intense competition among mobile phone service providers as they are attracting customers. Both of these provide an opportunity for the criminally inclined to try and make a profit out of the situation.

There are many kinds of mobile phone fraud. This paper attempts to summarise and categorise different types of fraud through different points of view on the subject matter. Practical examples are presented to gain a better understanding of the different kinds of mobile phone fraud.

The rest of the paper is organised as follows. Chapter 2 introduces the reader to the cost figures of fraud. Chapter 3 examines the different types of fraud through examples: First, reasons for fraud, answering the question of “Why?”, second, methods for fraud, answering the question of “How?”, and thirdly, fraud perpetrators, answering the question of “Who?”. Finally, chapter 4 presents conclusions about the subject.

2 Costs of fraud

Publicly available figures for the costs of fraud have many uses, so the reader should know a few things before believing them to be correct. Cost figures are published by the operators themselves, by various organizations such as the Cellular Telecommunications Industry Association, and by governmental institutions.

2.1 Hard and soft currency

Costs of mobile phone fraud can be divided into two classes, soft currency and hard currency [26].

Soft currency is a theoretical figure. It is derived from the lost revenue due to illegal use of the services. It is based on the assumption that the illegal user would have paid for the services he used without permission. This assumption does not hold always. The same assumption is usually made with the figures for music, computer software and movie piracy.

Hard currency is real money. It is money that the operator has to pay someone else. For example, when a mobile phone user of operator A roams in operator B's network, operator A pays to the operator B for the use of his network. Hard currency can also be lost on premium services, that is, services with higher than regular tariffs.

2.2 Uses of cost estimates

Cost estimates of fraud have several uses. On one hand, the operators can use high fraud figures to gain more favorable legislation from the government on the basis that the current situation is so detrimental to their business, hoping that stricter legislation will act as a deterrent to criminals. In the USA, a new strict law was amended [22], making it illegal to own a scanner or a cell phone programmer with the intent to defraud, use, own, or traffic counterfeit phones, with maximum sentences of up to 10 to 15 years in prison. Examples of fraud sentences are in [28, 5, 1, 24].

On the other hand, low fraud figures are good publicity for the operator. It gives an impression of a secure network, so customers are not afraid to use their phones. Also, low fraud means less hassle to the customers who, in the end, end up paying for fraud through the service fees.

3 Fraud types

There are different approaches to categorise fraud. In this paper, different types of frauds are presented in the following order, trying to answer the following questions:

1. Reason / Motivations for Fraud (“Why?”)
2. Method (“How?”)
3. Perpetrator (“Who?”)

We will start with the reasons for the fraud to motivate reader, and to gain a better understanding of mobile phone fraud.

3.1 Reason: Economic Gain versus Other

One reason why mobile phone services are subject to fraud is that it is a relatively expensive service.

3.1.1 Example: Roaming fraud

In this type of fraud, stolen and cloned mobile phones are used to make international calls and in roaming, possibly abroad. Once a suitable subscription has been acquired, it can be used for call selling locally (see section 3.2.3 for more detail) or it can be used to place calls in a roaming network.

In roaming a subscriber to operator A can use operator B’s network and services, provided that the operators have made a roaming agreement. Roaming, especially international roaming, and international calls in general, are usually expensive, and therefore subject to criminal interest and fraud. Roaming fraud is a hard currency problem because the roaming user’s operator has to pay to the operator of the roaming network for the roaming user’s use, whether or not the user pays his bills. Therefore, operators have taken measures to limit the costs of roaming fraud.

The main problem behind roaming fraud is the delay in the communication of billing information between the operators. The delay has been shortened [28, 19] from 72 to 24 hours. The information is transferred with EDI (Electronic Data Interchange) or by tape. An example of roaming fraud is reported in [28]. SIM cards were taken out of the phones acquired with false identities, mailed abroad where they were used in call selling operations, with call lengths averaging 10-12 hours. According to the guidelines of the GSM Memorandum of Understanding, a call report of a user exceeding 100 SDR[1] units a day must be delivered to the home network within 24 hours.

Should GSM cloning become a major problem, the importance of timely communication between the roaming operators will become critical in avoiding fraud losses. Already,

[1] Special Drawing Rights (of the International Monetary Fund), a type of international money

clearinghouses have been set up to offer billing and billing information services to roaming operators [28].

3.1.2 Example: Criminal users

Mobile communication provided by a mobile phone is a valuable tool for criminals, just as it is for ordinary people. Criminals, however, have more reason to worry about the operator knowing their location than regular users.

Mobile operators can find out the location of a mobile phone, with varying accuracy. In areas where base station density is high, for example in cities, the accuracy can be a few hundred meters, whereas in rural regions the accuracy is a few kilometers. In GSM systems, the phone has a unique identifier (IMEI, International Mobile Equipment Identity) as well as a SIM containing the subscriber information (IMSI, International Mobile Subscriber Identity).

Depending on the legislation of each country, the law enforcement can get this information from the operator, possibly in realtime. Therefore, it makes sense for a criminal to use one or more stolen or cloned phones to gain anonymity and to make it harder to track them. By constantly using the one and the same phone and SIM card, it is easy to track the criminal's movement. Using some tools (e.g. Wintesla [4]), it is possible to change the IMEI of one's phone. This will make the network think that the same SIM is used in different phones when, in reality, it is the same phone. A Radio Frequency Fingerprinting system can identify the phone as being the same one, see 3.2.1. Therefore, criminals use subscriptions that can not be connected to them (i.e. cloned or stolen subscriptions, or a subscription for a fake identity) and several different phones.

Criminals do use cloned phones. According to [22], 80 percent of the drug dealers arrested in the USA were found in possession of cloned phones. On the other hand, the hiding place of Pablo Escobar, a notorious cocaine dealer, was found by tracing his mobile phone activity [24].

This type of fraud can be prevented by offering a suitable service, such as prepaid subscriptions. In prepaid subscriptions, the customer pays up front a certain sum, for instance 100 Euros, and uses the subscription as long as there are credits left, after which he can buy more credits or take another prepaid subscription.

3.2 Method: Technical versus Social

Mobile phone fraud can be conducted by many different means. In this chapter, different technical and social methods are presented.

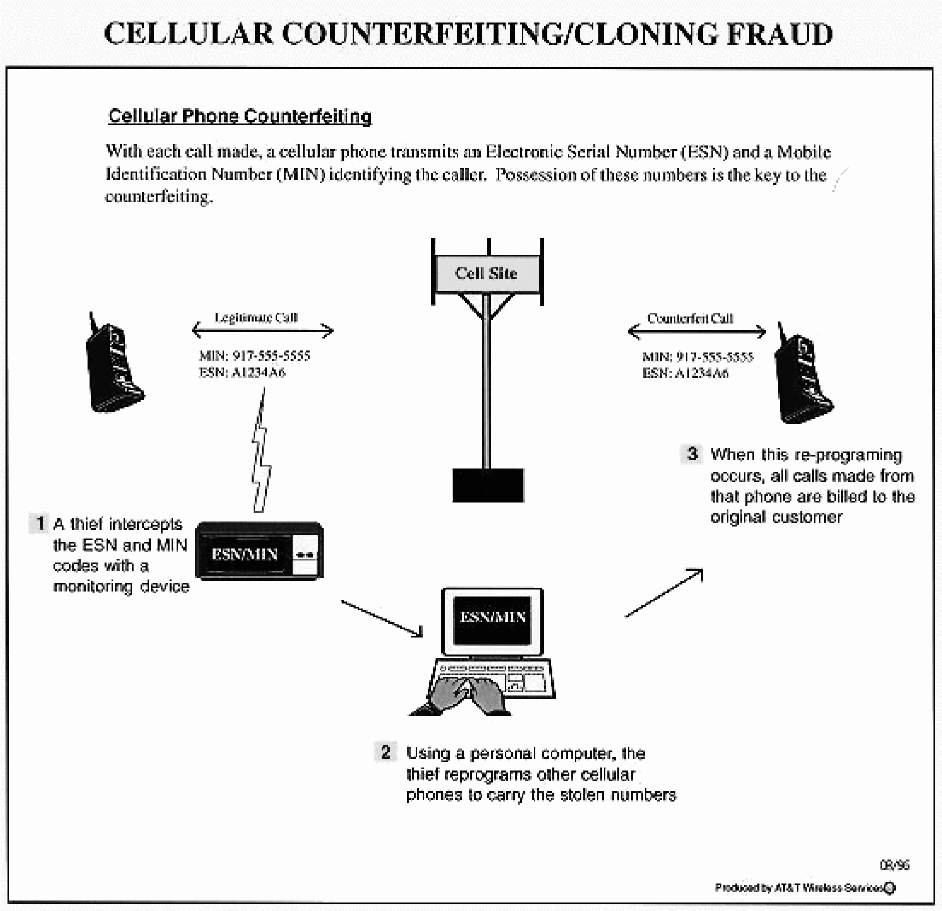
It is possible to prevent technical fraud, such as cloning, with technical methods. Likewise, social fraud is best countered with social means, for instance through better business processes, rather than technical means.

3.2.1 Example of a technical method: Cloning

Cloning of analog mobile phones was a major problem until operators and equipment manufacturers took measures to make it more difficult. Analog mobile phone systems include AMPS (Advanced Mobile Phone System) [9], used mainly in the USA, TACS [10], a version of AMPS used for instance in the UK, and NMT, used in Scandinavia. These systems had similar issues, so only one of them is presented.

AMPS, the analog mobile phone system used in the USA was in the beginning very vulnerable to cloning. Each phone has an Electronic Serial Number (ESN), identifying the phone, as well as a Mobile Identification Number (MIN), which includes the telephone number of the phone. As the acronyms indicate, these are used to identify the subscriber [24].

When placing a call, the phone transmits both the ESN and the MIN to the network. These were, however, sent in the clear, so anyone with a suitable scanner could receive them. The eavesdropped codes would then be programmed into another phone, effectively cloning the original subscription. Any calls made on this cloned phone would be charged on the original customer. See figure 1.



CELLULAR COUNTERFEITING/CLONING FRAUD

Cellular Phone Counterfeiting

With each call made, a cellular phone transmits an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN) identifying the caller. Possession of these numbers is the key to the counterfeiting.

1 A thief intercepts the ESN and MIN codes with a monitoring device

2 Using a personal computer, the thief reprograms other cellular phones to carry the stolen numbers

3 When this re-programing occurs, all calls made from that phone are billed to the original customer

08/96

Produced by AT&T Wireless Services

Figure 1. Cellular cloning [13].

Because of the relative ease of cloning these analog mobile phones, the cloning became a major problem. An example of the detailed instructions available on the Internet is [3], in which the writer describes how to modify a specific model of a scanner to receive the cellular frequencies. Also necessary software and instructions for cloning the subscriptions are provided.

Several countermeasures were taken with varying success. Here are various methods to detect cloned phones on the network:

- Duplicate detection. The network sees the same phone in several places at the same time. Reactions include shutting them all off so that the real customer will contact the operator because he lost the service he is paying for, or tearing down connections so that the clone users will switch to another clone but the real user will contact the operator.
- Velocity trap [5, 16]. The mobile phone seems to be moving at impossible, or most unlikely speeds. For example, if a call is first made in Helsinki, and five minutes later, another call is made but this time in Tampere, there must be two phones with the same identity on the network.
- RF (Radio Frequency) fingerprinting [5, 6, 23] is originally a military technology. Even nominally identical radio equipment has a distinguishing “fingerprint”, so the network software stores and compares fingerprints for all the phones that it sees. This way, it will spot the clones with the same identity but different fingerprints. Success reports of the effect of RF fingerprinting on fraud are in [2, 20].
- Usage profiling. Profiles of customers’ phone usage are kept, and when discrepancies are noticed, the customer is contacted. The same method is used by credit card companies. For example, if a customer normally makes only local network calls but is suddenly placing calls to foreign countries for hours of airtime, it indicates a possible clone.
- Call counting [22]. Both the phone and the network keep track of calls made with the phone, and should they differ more than the usually allowed one call, service is denied.
- PIN codes. Prior to placing a call, the caller unlocks the phone by entering a PIN code and then calls as usual. After the call has been completed, the user locks the phone by entering the PIN code again. Operators may share PIN information to enable safer roaming.

While these methods may detect the clone, it may be too late to prevent damages. A better solution is to add authentication to the system. Authentication has been added to the analog system, but this is problematic. Adding features to a system already in use requires upgrades to users’ and operators’ equipment before they can be used. For example, the A-Key authentication added to the AMPS phones uses a challenge-response system with a 26-digit number in the phone to answer to the challenges from network. Some operators took the easy way, and used a default key of all zeroes to ease customer service, which of course defeats the whole purpose of the authentication system [18].

3.2.2 GSM cloning

GSM (Groupe Special Mobile), the worldwide standard for digital mobile communication, has had mandatory authentication from the beginning. Yet, it is possible to clone a GSM SIM (Subscriber Identity Module) containing the subscriber information. The cloning is possible because of a flawed authentication protocol, but the GSM cloning is not considered to be a major problem yet.

The authentication algorithm used by most of the GSM operators in the world, COMP128, is the reason for making the cloning possible. Given suitable input challenges, the algorithm leaks information about the unique secret key (Ki). With a sufficient number of challenges to the SIM-card, enough information can be gathered to deduce the secret key. The required number of queries is reported to be about 150000 [14, 7] which corresponds to about 8 [14] or 11 hours [7] with a smartcard reader. This attack is reported to be feasible over-the-air to a sophisticated attacker [27]. The over-the-air attack requires more sophisticated equipment, namely a fake base station which queries the mobile phone.

Security through obscurity is viewed by some as a reason for the failures in the GSM security model. A security model design process similar to the one used to select the AES (Advanced Encryption Standard) could prove useful, and the US cellular industry is adopting such a process [27].

The risks of GSM cloning can be seen in the past of the analog cellular phones. But with the increased usefulness of GSM features such as more widespread roaming, the damages could be even greater than with the analog systems. GSM cloning has not been reported to be a problem yet, most likely because of the difficulty of cloning the subscription compared to the analog mobile systems. Some of the risks of GSM cloning are explained in [8].

Removing the possibility for cloning means fixing the authentication algorithm. This means upgrading the software of the operators network, and renewing the SIM-cards, which is not an easy or a cheap task. That is unlikely to happen until the cloning and the following fraud becomes a major problem for the operators.

For more information about the GSM cloning, see the citations above and [12]. For more information about GSM security, see [21, 17].

3.2.3 Example of a social method: Subscription fraud

Subscription fraud is currently a major form of fraud. There are several forms of subscription fraud: signing up for a mobile phone service and pretending to be a nonexistent person, or some existing person other than oneself, and just being oneself but with no intention of paying the service fees. Subscriptions can also be acquired by stealing the phones. Once the subscription has been acquired, it can be used as such or it can be used for call selling. There are several methods of acquiring the detailed information needed for the subscriptions [28].

In some countries there is heavy competition between the operators in attracting customers. Operators also pay dealers for every subscription they sell, so some unscrupulous dealers will sell subscriptions without properly authenticating the buyer.

Call selling can be done by renting the phone for a fixed sum, or by setting up a shop where customers can use it as a payphone. GSM has a few features that have been abused by fraudsters. In conference calling, more than two parties can talk to each other at the same time. Using conference calling, the fraudster acts as an operator and sets up calls for his clients by calling the client and the third party, and then dropping off the call, which leaves the client and the third party connected. After this, the fraudster may set up another call.

Call forwarding allows calls directed to a mobile phone to be automatically transferred to some other phone number. Using call forwarding the fraudster sets the forwarding to a third party, and then the client calls the fraudster's phone and is transferred to the number he wishes to call. After this call is connected, the fraudster is free to set up another call. The caller pays for the call to the fraudster and the fraudster is charged for the transferred call. There are a couple of examples of this type of fraud in [28]: In one case 110 call forwards were done in two hours, which resulted in 12.5 hours of calls on one subscription. In another case, the forwarded number changed every minute for 16 hours, with calls worth of 12000 GBP made to foreign countries.

Operators have tried to limit subscription fraud by several different means. Better screening and proper authentication of customers, and reviewing the process of acquiring new customers are ways of limiting fraudulent subscriptions. Restricting roaming and international calls, placing limits on outstanding invoices, and demanding a cash deposit before activating the subscription limit the possible damages.

One example of a quick fix is described in [19], where the operator shut down all calling to Vietnam because of the level of fraud. Only one legal customer complained about it, and he was allowed access to one specific number.

The main problem is in recognising the good customer and weeding out the bad ones. One scheme would be to give new customers only a small credit first, and when they pay their bills properly, increase the credit. Similar problems exist in the insurance, health care and financing businesses, where models and processes for dealing with fraud have already been developed. Operators could customise these to their environment to reduce the effects of fraud.

3.3 Perpetrator: End User versus Seller / Operator

The end user is not the only possible source of fraud. Even the network operators and the dealers and distributors can perpetrate fraud. The main difference is in scale. Whereas the number of end users is high, there is a substantially smaller number of operators and dealers. A dishonest operator or dealer can commit larger frauds more easily than a single end user, mainly because of the trust in them to behave appropriately.

3.3.1 Perpetrator example: Subsidy fraud

In some countries the mobile operators subsidise the cost of the mobile phones. Operators do this to lure in subscribers to their service, often requiring long subscriptions to make up for the subsidy.

The contract phones are locked to a particular subscription, making it impossible to use other subscriptions with them. Subsidies make the phone prices artificially low and, to protect the operators investment, the use of the phones is limited. However, there are instructions and software available on the Internet for removing this lock, and making the phone usable on other networks. This creates an opportunity to get phones under their street price, unlock them, and sell for profit.

The Register describes the situation in the UK in [15]. The new pay-as-you-go or pre-paid subscriptions are problematic as these subsidised phones are easier to take to another country and network, in effect wasting the operator's subsidy.

Dealers can also sell the subsidised phones directly to another dealer in the same or a foreign country. Again, the operator's subsidy does not reach its goal, the end user [22].

Operators may reduce subsidy fraud by cutting back on the subsidies but this is not always seen as a viable solution because of the intense competition in attracting new subscribers. Whatever the case, business processes can be tuned to take into account the possibility of fraud. Operators should carefully examine their interest groups, especially the dealers to which they are handing out money in the form of subscription bonuses and subsidised phones.

3.3.2 Perpetrator example 2: Billing fraud

The network operator can also defraud the customer. Most commonly this would mean overcharging the customer or, in other words, charging for services that the customer has not used.

An example of overcharging and the resulting lawsuits is described in [25]. The operator rounded up the durations of calls to full minutes, even when the call lasted only a few seconds.

In order to prevent this, customers should monitor their bills, which requires that customers keep track of their phone usage. While huge increases are easily noticed, smaller ones will pass unnoticed as few people know the exact number of calls placed and the airtime they have used.

4 Conclusion

Some of the forms of fraud presented here have been possible because of design flaws. The cloning of analog mobile phones was possible because there was no protection to the identification information and the cloning of GSM SIM-cards is possible because of a leaking authentication algorithm. These problems can be countered with technical means.

With more and more services available to mobile phone users, ranging from buying a can of soda or breakfast to a car wash, the possibilities for fraud increase with the value of the services. Possible future services include banking and stock trading services on the mobile phone, which clearly demand a good security model if they are to gain any significant use.

However, fraud in itself is a social problem. As such, it may be temporarily countered with technological means but they rarely work permanently. Mobile phones are a relatively new phenomenon and social norms to its use have not been formed. Some operators have tried the “If you can’t beat them, join them” approach and provided services that would otherwise be attained by fraud. As mobile communication matures, both socially and technologically, fraud will settle to some level. Until then, it is a race between the operators, equipment manufacturers and the fraudsters.

References

[1] Abel, Greg. Cellular theft wreaks havoc. Baltimore Business Journal, 9/30/94, Vol. 12 Issue 19.

[2] Anon. Bell Atlantic Nynex notes drop in fraud. RCR, 3/10/97, Vol. 16 Issue 10.

[3] Anon. Cloning for Dummies.
http://home.prophetnetworks.net/%7Eaiwa/clone.htm [referred Nov. 10, 2000]

[4] Anon. Wintesla Nokia service software.
http://www.gsm-cables.net/nokia/service/wintesla.html [referred Nov. 10, 2000]

[5] Brooke, Bob. Cellular phone networks fight fraud with technology. Philadelphia Business Journal, 2/24/95, Vol. 13 Issue 52.

[6] Carter, Wayne. Wireless manhunt.
http://www.internettelephony.com/archive/7.7.97/wnnews.html [referred Oct. 18, 2000]

[7] Chaos Computer Club. GSM Cloning: Technischer Hintergrund.
https://www.ccc.de/D2Pirat/index.html [referred Nov. 3, 2000]

[8] Chaos Computer Club. GSM Cloning: Eine Risikoabschätzung.
https://www.ccc.de/D2Pirat/risiko.html [referred Nov. 3, 2000]

[9] Cellular Networking Perspectives Ltd. The AMPS Wireless Standards.
http://www.cnp-wireless.com/amps.html [referred Nov. 9, 2000]

[10] Cellular Networking Perspectives Ltd. AMPS Cellular.
http://www.cnp-wireless.com/cellular.html [referred Nov. 9, 2000]

[11] Crowe, David. Authentication for small carriers. Cellular Business, Sep97, Vol. 14 Issue 9.

[12] Cryptome. Cryptome.org: GSM links.
http://cryptome.org/cryptout.htm#GSM [referred Nov. 9, 2000]

[13] DeMaria, Roseanna. How it Works: Cellular Phone Fraud.
http://www.annonline.com/interviews/961119/how.html [referred Nov. 18, 2000]

[14] Goldberg, Ian & Briceno, Marc. GSM Cloning.
http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html [referred Oct. 11, 2000]

[15] Harrison, Linda. Cheap Brit mobiles attract phone smugglers, The Register. http://www.theregister.co.uk/content/archive/11809.html 06/07/2000 [referred Oct. 26, 2000]

[16] Hollmén, Jaakko. Probabilistic Approaches to Fraud Detection. Licentiate's Thesis, Helsinki University of Technology, Department of Computer Science and Engineering, 15.12.1999.

[17] Isomäki, Markus. Security in the Traditional Telecommunications Networks and in the Internet. http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/tradsec/security_comparison.html [referred Oct. 23, 2000]

[18] Jeffrey, Stuart. False sense of security? Wireless Review, Vol 15, issue 6, 15.3.1998.

[19] Lopez, Ed. International Fraud A World Of Hurt. Wireless Week, 11/01/99, Vol. 5 Issue 44.

[20] Luna, Lynnette. Bell Atlantic's fraud decreases. RCR, 03/02/98, Vol. 17 Issue 9.

[21] Pesonen, Lauri. GSM Interception. http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/gsminterception/netsec.html [referred Oct. 23, 2000]

[22] Riezenman, Michael J. Cellular security: better, but foes still lurk. IEEE Spectrum, 37 (6), June 2000.

[23] Saunders, Renee. Outwitting cloners. http://www.internettelephony.com/archive/10.14.96/features/saunders.html [referred Oct. 18, 2000]

[24] Smith, Russell G. Preventing Mobile Telephone Crime. Paper presented to the Communications Research Forum, Melbourne, 28 and 29 October 1996. http://www.aic.gov.au/conferences/other/smith.html [referred Oct. 18, 2000]

[25] Sontakay, Arati. Cellular billing bilking? Business Journal Serving Charlotte & the Metropolitan Area, 10/20/97, Vol. 12 Issue 28.

[26] Trevisan, Paolo. Monitoring mobile fraud. Telecommunications, August 2000. http://www.telecoms-mag.com/issues/200008/tci/monitoring.html [referred Oct. 18, 2000]

[27] Wagner, David. GSM Cloning, 2.9.1999. http://www.isaac.cs.berkeley.edu/isaac/gsm.html [referred Oct. 11, 2000]

[28] Wong, Ken. Mobile Phone Fraud: Are GSM Networks Secure? February 1997. http://163.18.14.55/datapro/41035-1.htm [referred Oct. 18, 2000]