NON-INTRUSIVE SECURITY ARRANGEMENTS TO SUPPORT TERMINAL AND PERSONAL MOBILITY

Steven M.Furnell[†], Mark Green[‡], Stephen Hope[‡], Joseph P.Morrissey[§] and Paul L.Reynolds[†]

[†]School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, United Kingdom.
[‡]Orange Personal Communications Services Ltd., 15-16 Eagleswood Business Park, Bradley Stoke, Bristol, United Kingdom.
[§]Aldiscon Ltd., Hambleden House, Lower Pembroke Street, Dublin 2, Ireland.

KEYWORDS

Security, Telecommunications, Terminal Mobility, Personal Mobility.

ABSTRACT

This paper examines the requirements for subscriber security and authentication mechanisms to support modern telecommunications services involving terminal and personal mobility. In both cases, transparent and non-intrusive techniques are desirable so as to minimise inconvenience. However, appropriate approaches vary depending upon the type of mobility involved. It is suggested that terminal mobility devices may lend themselves to a variety of handset-specific approaches. This discussion is supported by an examination of how the issue has been addressed by Orange, a leading player in the UK cellular communications market. By contrast, personal mobility calls for a highly generic software-based approach which is suitable to many types of terminal. The paper proposes the concept of keystroke analysis to authenticate users by the way that they key in their personal identifiers. This aspect is supported by summarised results from two keystroke analysis studies that have been conducted by members of the research team.

AN INTRODUCTION TO MOBILITY

In recent years, the area of mobile communications has witnessed massive growth in terms of both the number of subscribers and overall traffic. Today, third-generation wireless networks are being designed to carry multimedia traffic (including voice, video, images, textual data or a combination of these) and to enable communication among persons at any time, in any location (Padgett et al. 1995). The enabling concepts for providing such capabilities include terminal mobility and personal mobility, as described below.

- Terminal mobility is a basic feature of a mobile network and refers to the "ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal" (Pandya 1995). It has already been implemented in many analogue and digital cellular systems such as NMT, TACS, AMPS and GSM (Mehrotra 1994).

- Personal mobility has been introduced as a new capability in telecommunication networks. It refers to the "ability of a user to access telecommunication services at any terminal on the basis of a personal telecommunication identifier, and the capability of the network to provide those services according to the service profile of the user. Personal mobility involves the network capability to locate the terminal associated with the user for the purpose of addressing, routing and charging of the user's calls" (Zaid 1994).

Currently, the second-generation networks such as GSM and PCS are under intensive study by world-wide and European standardisation bodies, such as the International Telecommunication Union (ITU) and ETSI, as well as the Commission of the European Communities (Asatani and Nogami 1995). As far as terminal mobility is concerned, ITU-R SG8 and ITU-T SG1, SG2, SG4, SG11, SG13, SG15 in particular are working on standards defining the Future Public Land Mobile Telecommunication Systems (FPLMTS). FPLMTS is a third-generation mobile system that will enable a user in around the year 2000 to access services anytime and anywhere with one mobile terminal. A similar specification is also being developed in Europe under the ETSI standards for the Universal Mobile Telecommunication System (UMTS). Personal mobility is being studied by ITU-T SG1, SG2, SG3, SG11, SG13. These study groups are currently defining the Universal Personal Telecommunication (UPT) service.

The Commission of the European Communities has addressed mobility issues since the start of the RACE (Research and development in Advanced Communications technologies in Europe) programme. The most notable projects in this area have included the following :

- Mobilise (RACE 2003);
- MONET (RACE 2066);
- PERCOM (RACE 2104).

The Mobilise project (Mobilise 1994) was intended to be a link between mobile features and network intelligence aimed at controlling network functionality. Mobilise had the objective of defining the Personal Service Communication Space (PSCS) concept, specifying a PSCS architecture, building components for PSCS and demonstrating different PSCS applications. The PERCOM project (PERCOM 1994) was also working on PSCS issues. It focused on the validation of some concepts through the development of a demonstrator in a broadband ATM environment. Both projects worked in parallel with the MONET project (MONET 1995) which dealt with network architecture and protocol issues arising in the design of the third-generation UMTS system. The work done in MONET suggested network management and control research questions that still have to be addressed in handling multimedia traffic over future mobile networks. More recently the research has been extended by projects under the ACTS (Advanced Communications Technologies and Services) programme, which are conducting a number of technological trials. One such case is the DOLMEN project (DOLMEN 1996), in which distributed processing techniques are being introduced into mixed fixed and mobile environments to enable the establishment of a generic telecommunications service machine. It is also within this project that an investigation into the area of non-intrusive security arrangements is being undertaken as part of the ongoing experimentation.

SECURITY AND AUTHENTICATION REQUIREMENTS FOR MOBILE COMMUNICATIONS

Numerous events in recent years have shown that the telecommunications medium is already a prime target for fraudulent

and / or malicious misuse (Shimomura and Markoff 1996). In North America alone mobile telecommunications fraud costs providers one million dollars a day (Shapiro 1995). Some of the problems that plague service providers are subscription fraud, international roaming fraud, and handset rechipping. Law enforcement agencies have discovered that the element of society that conducts illegal business, such as drug smuggling, has been very quick to pick up on the advantages of mobile phones for the co-ordination of their activities. Criminals utilising mobile communications do not wish to use a subscription that can be traced back to themselves and, as a consequence, an industry has grown to provide illegal mobile equipment that has been stolen or cloned using legitimate subscriber identities. Such considerations dictate a need to guard against masquerade attacks in both mobility scenarios (i.e. preventing the use of either a terminal or a personal identifier by an impostor). As such, some method of subscriber authentication must be incorporated.

The establishment of a personal mobility session will typically involve three stages, as described below :

- *Identification*

This procedure is traditionally carried out by the user in order to identify himself to the service operator. In order to be identified the user usually needs to insert his Identification Number. Because the devices used to access the personal mobility services may be different realisations depending upon the networks, terminals and services used, the introduction of this identity can be performed in different ways. One way is to type it in, whilst another is to introduce card reader technology. This procedure may be seen as being analogous to the entry of a username in a traditional computer system.

- *Authentication*

This procedure is used by the service operator to verify and validate the identity of the calling or answering party after the initial identification has been performed. During the authentication the user is currently required to provide some additional form of information that will be checked out by the service provider against that stored in the *user profile*. Potential approaches vary and may be based upon the use of a device which accepts a user identity token (e.g. a magnetic strip card or a smart card) or upon the possession of “secret” knowledge (e.g. entering a PIN code or a password). The strongest option using current technologies is the combination of both approaches (i.e. authentication via a card and a PIN).

- *Registration*

Registration procedures inform a service provider of the terminal from which a user wants to receive or activate services. De-registration procedures are subsequently used to break the association between user and terminal when the session is terminated. These procedures require access, identification and authentication procedures to be carried out before or in conjunction with them.

It can be seen that these stages represent the means by which a secure, authenticated session can be established.

In the terminal mobility scenario, explicit identification and authentication of the user are not usually a mandatory requirement when initiating a call session (the reason being that a permanent physical association is assumed to exist between the terminal and its legitimate owner). Some terminals will allow the owner to specify that a password / PIN is required to gain access, but this is an optional feature. As such, there is no guarantee that authentication will be performed unless the safeguard has specifically been enabled by the legitimate user.

It can be seen that, in both scenarios, the authentication phase currently requires some positive action on the part of the subscriber. As such, the provision of security can be broadly considered to be impacting upon the usability and friendliness of the service. The sections that follow will attempt to consider how this aspect may be made more transparent.

SECURITY MECHANISMS FOR TERMINAL MOBILITY

There are a number of approaches by which protection may be non-intrusively integrated into the terminal mobility scenario. Much of the following discussion is specifically focused upon the approach that is taken by Orange, a leading cellular communications provider in the UK.

A central element of the terminal security is the Subscriber Identification Module (SIM). This is an ISO standard smartcard containing several types of data. The primary purpose for having a smartcard in the terminal is one of security, since smart card technology is considered to be inherently secure.

The SIM Operating System (OS) stands between a user and the data stored on the card. Because the entire device is on one chip (processor, program and memory), there is no access to data other than through the OS controlled I/O. Therefore, for each datafield on the card, an access condition has to be satisfied before read, update, etc., can be achieved. Various levels of access can be defined for each instruction when the data is created, from "Always" (instruction can always be performed on data), through PIN1 (PIN has to be verified before instruction can be performed) to "Never" (instruction can never be performed). In between there are a number of administrative levels of access, where special sets of procedures have to be satisfied before the instruction can be performed. This allows the card issuer to define the condition "Read Never" for data such as Keys. The OS can access the data for algorithm execution, but the data can never be divulged across the interface.

The SIM uses EEPROM technology for secure storage of the data, with the manufacturers of the smart card chips having designed them to ensure that data is not available to direct probing. Measures such as vertical bus architecture and oxide layers within the silicon are used to achieve this.

The main security task of the SIM is that of authenticating the phone as a valid subscription on the network. This authentication uses an algorithm which is stored in the SIM and network, together with a random number provided by the network and a secret key stored in the SIM and the network Authentication Centre (AuC). The SIM, therefore, securely stores the Algorithm and the Secret Key (Ki). The algorithm can be part of the SIM ROM code since is identical on all SIMs, this makes the algorithm unalterable on a particular SIM design. By contrast, the Ki is different for each card and can be loaded at personalisation, providing the personalisation lock mechanism is satisfied. However, the operating system does not allow this data to be read across the interface.

The SIM also has a method of updating certain data on the card remotely, using the Short Message Service (SMS) as a transport mechanism. This allows the network to personalise data on the card to the individual user, without the user having to either send in their SIM back or go into a service centre. The mechanism includes a number of security measures, whereby the network has to send a specific code that is SIM dependant before the SIM will accept any update information. The SIM will also only accept update information for a given field if that field has been enabled for remote updating at personalisation time. Therefore, the network can control at card issue time what data is changeable by this system.

Further facilities offered by the SIM toolkit are an area in which new services and features can be based. Some ongoing work within Orange will take advantage of these facilities, together with other proprietary mechanisms, to deliver new, innovative and secure SIM-based services.

Various other approaches for achieving security within terminal mobility can also be employed. For example, the GSM standard attempts to provide subscriber identity confidentiality, subscriber identity authentication and data confidentiality, through the application of cryptographic techniques (GSM 1994). GSM providers also use

Equipment registers to hold the authorisation status of International Mobile Equipment Identity (IMEI) numbers belonging to their current subscribers. Recently a Central Equipment Identity Register (CEIR) for Europe has been set up in Dublin to provide a co-ordinated database for the 130 GSM providers currently operating (Acland 1996). Although most operator's EIRs are not capable of electronic information transfer with those of another, or with the CEIR, the MoU Association plans for this to change.

A technique for combating mobile fraud that is very applicable within a Terminal Mobility scenario is that of Radio Frequency (RF) fingerprinting. Although it has been applied within very few networks it has a great potential. RF fingerprinting works on the premise that a transmitted RF signal will exhibit unique characteristics dependent upon the transmission equipment. If the characteristics can be measured and classified accurately enough it should be possible to identify transmitters, in the case of mobility - mobile stations, from their RF fingerprint. This approach currently suffers from certain drawbacks :

1. the need for hardware at each cell site, render it a costly approach;
2. there is no standard for the characteristics chosen in RF fingerprinting, therefore cross vendor application is limited;
3. the accuracy of fingerprinting is not 100%.

However, its innate advantage is that it is non-intrusive, requiring no additional effort from the user.

SECURITY MECHANISMS FOR PERSONAL MOBILITY

As previously indicated, the concept of personal mobility allows users to initiate and receive calls at any terminal, irrespective of geographical location, on the basis of a unique personal identifier. A key aspect of this is that before any service access is granted, the user needs to identify him/herself at the terminal. However, the sheer range of potential access points and terminal types demands that a highly generic mechanism must be employed.

Whilst it is possible to achieve this via a number of traditional methods (as described earlier), these generally necessitate some aspect of inconvenience to the legitimate user (e.g. having to remember a password or carry a card). In addition, the methods have weaknesses in that passwords may be forgotten or guessed, whilst cards may be lost or stolen (cards also have another disadvantage in the sense that associated readers are then required on each terminal that wishes to support personal mobility features. Wide-scale introduction, therefore, represents a significant consideration in financial terms).

However, current technology permits the use of a rather more subtle non-intrusive scheme, based upon a biometric technique known as keystroke analysis. This relates to the verification of user identity from an analysis of their typing characteristics when accessing data services. In the personal mobility scenario, keystroke data would become part of the standard profile entry for registered users and authentication would be achieved when a personal identifier is input (by not only looking at what was entered, but also the way in which it was typed). The approach is based upon the assumption that the difference in style between the legitimate user typing his identifier and an impostor doing so is likely to be very marked. This is illustrated in figure 1, which shows the difference between legitimate users and average impostor performance when typing the same sample text. The results are based upon a test population of 13 subjects and measure the level of departure between the subject and a stored reference profile (whilst legitimate users are by no means perfectly compatible with their profile, the departure is not as marked as for impostors).

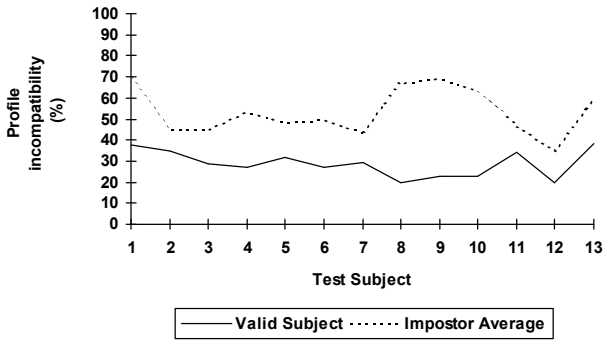

Fig. 1 : Performance differences between impostors and legitimate users

Keystroke analysis should enable the authentication procedure to become totally transparent to the legitimate user (as it physically merges with the identification phase), whilst at the same time offering more in terms of security, as the biometric characteristic could not be compromised in any of the ways previously identified.

Keystroke profiles may be based upon a variety of potentially characteristic factors, including inter-keystroke times, keystroke duration times and typing error frequency. Legitimate users will be expected to be consistent with this profile, although certain circumstances (such as hand injury, fatigue and keyboard variations) may affect performance. Incompatibilities between the keystroke profile and the current users performance would be used as the trigger for some further action such as additional authentication (e.g. issue of a random challenge) or denial of service. In general terms, the technique can be implemented in two ways - referred to as static and dynamic verification strategies.

- *Static verification*
  Authentication is based upon entry of a static text string such as the personal identifier. The information would be entered as usual, but the system would also analyse the way in which it was typed, providing authentication as well as identification. Previous studies in this area have been conducted by Joyce and Gupta (1990) and Bleha et al. (1990)

- *Dynamic verification*
  Authentication is based upon any arbitrary keyboard input, allowing greater scope for continuous, real-time session supervision. Authentication no longer relies upon a single judgement, which should guard against impostors attempting to use unattended logged-in terminals, as well as compensating for potential false acceptances from the static stage. An example of previous work in this area comes from Leggett et al. (1991).

In both cases, the effectiveness of the authenticator is judged on the basis of False Acceptance Rate (FAR) and False Rejection Rate (FRR) measures. The FAR relates to errors where impostors are falsely believed to be legitimate users, whilst the FRR refers to errors where the legitimate user is identified as an impostor. It is generally not possible to attain optimum levels for both measures and, therefore, a decision is required as to which should receive priority. This will be influenced by whether static or dynamic authentication is used. In the static scenario, minimising false acceptances is the chief requirement, as any impostor passing authentication could then potentially go unchecked for the remainder of the session. By contrast, the dynamic scenario provides a greater window for impostor detection and so minimising the FRR becomes the more important consideration (as rejections *during* a session would significantly negate any transparency benefits). The speed of identity assessment is also important in this scenario.

Practical experiences using keystroke analysis

This section presents details of experimental keystroke analysis studies that have been performed within the University of Plymouth. It should be noted that for the purposes of this discussion only a brief overview of each of these will be presented, along with the principal results obtained (as this is sufficient to illustrate the inherent potential of the approach).

Practical evaluations of both the static and dynamic approaches have been conducted on PC-based prototype systems, using inter-keystroke timing rhythms as the basis for profiling. The technical implementations differed in that the static analyser compared typing samples against the profiles using neural network-based pattern recognition, whilst the dynamic system (which was actually the earlier implementation) incorporated statistical tests based upon the mean and standard deviation of timings. Whilst the static analysis is more immediately appropriate to personal mobility subscriber authentication, the results from both studies will be considered because the dynamic approach could conceivably find a role in both mobility scenarios as a means of continuous session authentication.

A variety of test subjects were involved in both cases, with experience ranging from professional typists to relative novices. A summary of the overall characteristics of each experimental study is given in table 1.

	Static Analyser	Dynamic Analyser
Test subjects involved	15	30
Profile length (chars)	560†	4400
Avg. test sample length (chars)	16	482
Legitimate user attempts	150	60
Impostor attempts	2100	1740
FAR (%)	8	15
FRR (%)	7	0

† based upon 35 samples at average string length of 16 characters

Table 1 : Comparison of the keystroke analysis studies

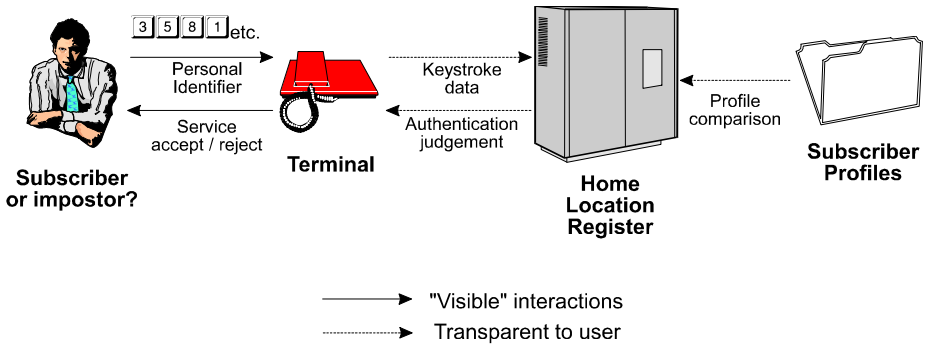

Fig. 2 : Keystroke analysis for Personal Mobility

In the dynamic scenario, the results for speed of impostor detection indicated that 85% of them would be challenged in under 160 keystrokes. Moreover, in 26% of cases, detection would occur in under 40 keystrokes.

The overall FAR and FRR results indicate that it is possible to differentiate between legitimate users and impostors at traditional computer keyboards with a significant degree of accuracy. It is anticipated that with a certain amount of further development, the technique could be utilised by Telecommunications Operators to assist in providing for non-intrusive authentication to support personal mobility. Full details of the existing implementations and their associated results can be found in Furnell et al (1996).

Implementation considerations

A basic implementation scenario, highlighting the transparent aspects of the protection, is shown in figure 2.

Further experimental studies will focus on assessing the effectiveness of the technique when applied to the entry of example "personal identifiers" (as opposed to general text passages, as used in the previous studies). This should theoretically have the potential to yield better performance, because :

- keystroke profiles can be based upon the entry of the specific identifier that applies to each user (as opposed to having to cater for any arbitrary input);
- users are likely to become familiar with typing their personal identifier and should, therefore, be more consistent than with other keyboard input.

However, the studies will also need to assess the entry of the same personal number on the various different terminal types that might be encountered (e.g. computer keyboard versus mobile handset). Problems could be expected in this respect, due to variations in the same users performance between different "keyboards".

Ensuring the transparency of the protection mechanism is particularly important with regard to personal mobility because subscriber sessions / associations are frequently likely to be quite short. This point tends to refute the conventional wisdom regarding acceptable FRRs in static analysis systems. As previously indicated, it is normally considered reasonable for some level of false rejection when using static keystroke analysis on a traditional computer system. In these cases the login period is typically very short in comparison to the overall session length (and, in any case, many users frequently mistype passwords anyway and are used to being prompted for re-entry). Such analogies are considered to be less valid in the personal mobility context because :

- personal identifiers are likely to be longer than most conventional passwords (and will, therefore, require more effort to re-enter);
- the forced repetition of the identification stage is very likely to be considered intrusive if the user only wants to make a short call.

Another potential problem in the wider sense is that the use of the technique would introduce a generic requirement for appropriate keystroke timing data to be obtainable. In the case of intelligent terminals it will probably be possible for this information to be obtained locally. However, other scenarios such as voice access terminals may be more problematic. Nevertheless, the idea would still be potentially feasible if the data collection responsibility was to migrate from the terminal to a distributed “service machine”. For example, using tone dialling systems, inter-keystroke timings could be determined by measuring the interval between the end of one dialled digit tone and the start of the next. In cases where the required data truly cannot be obtained, the security risk could be addressed by including links to service portability in the subscriber profile (e.g.

specifying that certain services should only be available if the user can be keystroke authenticated at the terminal).

It is considered that the technique could also be usefully applied in the terminal mobility scenario, allowing the legitimate user to verify his / her identity to the handset.

A further technique that is already used by some providers is *subscriber profiling*, which exploits the habits that users exhibit in their everyday use of mobile services. Intelligent analysis enables typical usage patterns to be established and, therefore, allows departures to be identified as anomalous and potentially worthy of further examination. This represents another transparent safeguard that is appropriate to both mobility scenarios. The technique is already widely used in the credit card industry and tools such as the Aldiscon Signal Monitor are making this type of anti-fraud defence available to mobile providers. The disadvantage of the approach is that misuse can only be identified once some level of unauthorised activity has already occurred.

CONCLUSIONS

In conclusion, the provision of adequate security will be essential in future telecommunications scenarios if advanced services are to be used with confidence.

A variety of handset-based methods already ensure that some degree of security can be achieved in the terminal mobility scenario and the range of possibilities is likely to increase as the handset technology advances.

In terms of improved software-based methods, the keystroke analysis concept is considered to hold some interesting potential (particularly within the personal mobility scenario) and the experimental results are encouraging. However, whether the technique can afford totally transparent protection is obviously questionable in view of the degree of false rejection observed. However, some level of error may be justifiable to subscribers based upon the additional safeguard that is provided for the use of their identifier.

Overall, both mobility scenarios will be best protected if a range of countermeasures are employed. The transparency of these mechanisms will be an important factor in determining their acceptability and, in turn, the user-friendliness of the resulting services.

REFERENCES

Acland, A. 1996. “An interface to cut GSM fraud”, *Mobile Europe* (Jan.) 1996: 24-26.

Asatani, K. and S.Nogami. 1995. “Standardization of Network Technologies and Services”, *IEEE Communications Magazine* (Aug.)

Bleha S.; C.Slivinsky; and B.Hussien. 1990. “Computer-Access Security Systems Using Keystroke Dynamics”. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 12, no.12, 1217-1222.

DOLMEN. 1996. ACTS project A036, Deliverable APD1, AC036/FUB/AP-DEL01, *Mobility Functions and Open Service Architecture Requirements*.

Furnell, S.M.; J.P.Morrissey; P.W.Sanders; and C.T.Stockel. 1996. “Applications of keystroke analysis for improved login security and continuous user authentication”. In *Information Systems Security - Facing the information society of the 21st century*. S.K.Katsikas and D.Gritzalis (Eds.). Chapman and Hall, London, UK.

GSM. 1994. "European digital cellular telecommunications system(phase 2); security related network functions", GSM 03.20 prETS 300 534.

Joyce, R. and G.Gupta. 1990. Identity Authentication Based on Keystroke Latencies. *Communications of the ACM* 33, no.2, 168-176.

Leggett, J; G.Williams; M.Usnick; and M.Longnecker. 1991. "Dynamic identity verification via keystroke characteristics", *International Journal of Man-Machine Studies* 35, no.6: 859-70.

Mehrotra, A. 1994. *Cellular Radio - Analog and Digital Systems*, Archtech House Publishers.

Mobilise. 1994. RACE project R2003, Deliverable D20, R2003/ETM/CT2/DS/P020/b1, *PSCS Specification and CFS-Final Version*.

MONET. 1995. RACE project R2066, Deliverable R2066/BT/PM2/DS/P/113/a4, *UMTS System Structure Document (Revised)*.

Padgett, J.E.; C.G.Gunther; and T.Hattori. 1995. “Overview of Wireless Personal Communications”, *IEEE Communications Magazine* 33, no. 1.

Pandya, R. 1995. “Emerging Mobile and Personal Communication Systems”, *IEEE Communications Magazine* (June).

PERCOM. 1994. RACE project R2104, Deliverable D05, R2104/SESA/WP3/DS/P/005/ed1, “Specification of the Services provided by the PERCOM Service Node at its External Interfaces”.

Shapiro, S.M. 1995. “Real-world fraud busting”, *Telephony*, August 1995: 30-32.

Shimomura, T. and J.Markoff. 1996. *Takedown*. Secker and Warburg Limited, London, UK. ISBN 0 436 20287 5.

Zaid, M. 1994. “Personal Mobility in PCS”, *IEEE Personal Communication* 1, no. 4, 4Q.