REVISITING REACHABILITY MANAGEMENT AS A MULTILATERAL SECURITY MECHANISM

Jacobus A. Ophoff and Reinhardt A. Botha

Centre for Information Security Studies,
Faculty of Engineering,
Nelson Mandela Metropolitan University,
South Africa

{jophoff,reinhard}@nmmu.ac.za, +27 (0)41 5043669, PO Box 77000,
Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa

ABSTRACT

Mobile communications are becoming ever more pervasive in our environment today. However, the decentralised nature of the technology makes achieving security and trust a considerable challenge. On the one hand, people are increasingly dependent on being reachable for communication purposes; on the other hand, they place a high value on security and personal privacy. These conflicting requirements have been discussed in reachability management literature. In essence, reachability management aims to provide users with control over their communications in such a way that their right to personal privacy and security is honoured. At the time when the concept was introduced, certain technical and usability difficulties existed. In this paper the authors, firstly, re-examine the motivation and requirements for reachability management. Secondly, they investigate the opportunities introduced by changes in technology, while also reflecting on changes in the social setting underlying the implementation of reachability management systems.

KEYWORDS

Mobile communications, Multilateral security, Reachability management, Privacy, Security, Trust

REVISITING REACHABILITY MANAGEMENT AS A MULTILATERAL SECURITY MECHANISM

1 INTRODUCTION

During the past couple of years, the popularity of mobile communications has grown tremendously. This is apparent from the fact that there are more mobile phones than traditional, wired phones in use today [1, p. 94]. Mobile phones and communication towers are commonplace in our society and we take for granted the ability to make or receive telephone calls from almost any location at any time.

Mobile communications have become ever more pervasive in our environment today. Even though the use of mobile technologies has changed and evolved, our privacy and security concerns have not. Many of the same security concerns that were present in the initial stages of adoption still prevail today. Consider, for example, the trade-off between a caller who wants to make an anonymous call and the called person who wants to avoid these harassing calls from unknown numbers.

Achieving security and trust in a mobile network is not a simple matter. Similar to networks like the Internet, there are many parties with diverse and often conflicting security requirements. To balance these different security interests, the concept of multilateral security can be applied [2]. Multilateral security proposes a framework in which each party can specify their own security requirements and discrepancies between conflicting security interests can be recognised and negotiated. In addition, no party should be required to place more than a minimal amount of trust in another [3, p. 11–17].

As a result of these aims the concept of reachability management was proposed [2]. Reachability management aims to provide a technical mechanism for enforcing multilateral security in mobile communications. By utilising reachability management the different parties involved in a communication gain greater flexibility to express and enforce their security interests before engaging in a phone call.

In this paper the authors re-introduce the concepts of multilateral security and reachability management. First, the theory behind multilateral security, and how this has led to the idea of reachability management, is reviewed. Secondly, the operation of a reachability management system and the technical and usability difficulties of an implementation are discussed. Next, we investigate the technological advances and social changes that have occurred since the initial proposal of the concept. Finally, we theorise on the possibilities and implications of these changes for a present day reachability management system.

2 MULTILATERAL SECURITY

The primary objective of multilateral security is to balance the conflicting security requirements of all parties concerned in a transaction [2]. This is especially important in networks like telecommunications and the Internet, where there are many parties with different security requirements involved. Figure 1 illustrates some of the security concerns in a typical telecommunications environment.

The basic security requirements of the parties involved (subscribers, network operators and service providers) can be summarised as follows [4]:

- Subscribers want to protect their privacy by preventing network operators and service providers from monitoring their communications. However, some measure of monitoring will always be needed to provide network services and for accounting purposes.

- Service providers need protection from fraud in the form of unpaid or unaccountable calls. Subscribers must be held accountable for their actions on the network while also protecting their privacy.

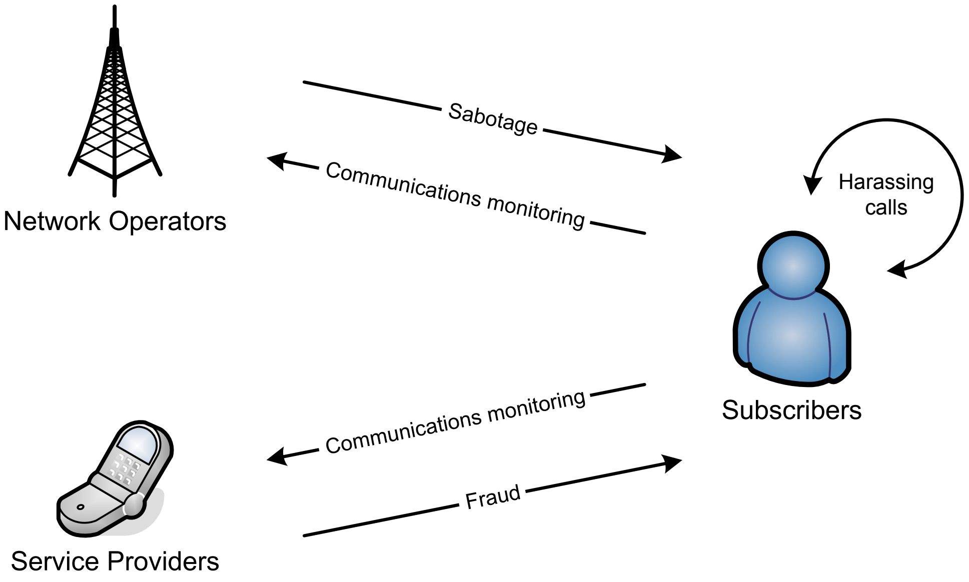


Figure 1: Conflicting security concerns

- Network operators need to protect their systems' infrastructure from vandalism and fraud by malicious persons. Protection measures to ensure the operation of the network must not violate subscriber's privacy rights.
- Subscribers need protection from invasive and harassing calls. Subscribers should be able to enforce their own privacy and security requirements.

Multilateral security endeavours to create a harmonious middle ground between these competing interests. However, all parties can be seen as potential attackers and it is thus essential that no party is forced to trust another. Therefore, in the design of a multilateral security solution the following salient principles need to be considered [4]:

1. Take conflicts into account:
   (a) Different parties involved in a transaction may have diverse and often conflicting security requirements.
2. Respect individual interests:
   (a) Parties can specify their own security requirements.
   (b) Conflicting security interests can be distinguished and negotiated.
   (c) Negotiated results must be reliably implemented.
3. Support independence:
   (a) Parties are only required to place minimal trust in another.
   (b) A party only has to place minimal trust in the technology of others.

Multilateral security infers that the classical security goals, i.e. confidentiality, integrity, availability and accountability might not be in the best interest of all the parties concerned [4]. Indeed a typical conflict occurs between the wish for privacy and anonymity and the desire for cooperation. An example of this is the so-called Caller ID conflict. On the one side it is argued that the security and privacy interests of callers are violated if their numbers are displayed to the called person (callee). This information could be misused on the callee side without the knowledge and consent of the caller. On the other hand the Caller ID will give the callee at least some protection against harassing calls by providing some information about the caller. Thus the balance of power between caller and callee is restored.

This situation led to the idea of reachability management. By utilising computing and communications technology, reachability management gives callees more protection from unwanted calls by allowing them to decide when a call is welcome. Similarly it gives callers a greater opportunity to express the importance and subject of the call. Reachability management is discussed in more detail in the following section.

3 REACHABILITY MANAGEMENT

The need for multilateral security and thus the rationale for reachability management comes from the diverse interests of callers and callees. Compared to classical security goals, reachability management aims to provide a satisfactory level of confidentiality and accountability in mobile communications. The best solution for meeting confidentiality requirements is the avoidance of data transfer. However, because data is needed for accountability purposes, this is rarely possible. Therefore, a design strategy behind reachability management is data economy, because it reduces the overhead for data protection. Another strategy, to avoid the misuse of sensitive information, is the careful allocation of data. The responsibility for storing and processing data is given to those parties who require confidentiality [2].

A reachability management system is an example of a multilateral security implementation in telecommunications on the application level [2]. The fundamental operation of a reachability management system is illustrated in Figure 2.

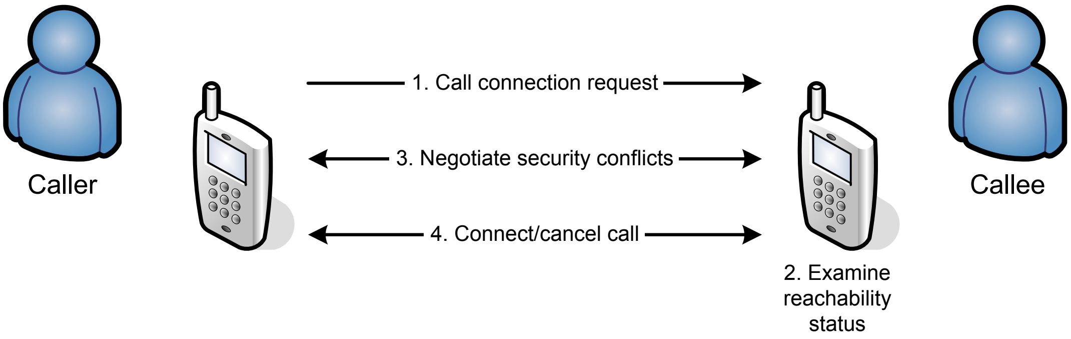

Caller
1. Call connection request
3. Negotiate security conflicts
4. Connect/cancel call
Callee
2. Examine reachability status

Figure 2: Call negotiation

Callees can specify the circumstances under which they are willing to accept an incoming phone call using their reachability management system [5]. When a data request comes in to start a conversation the reachability management system examines the current reachability status and either connects the call (i.e. sounds the ring tone) or performs additional data negotiations if any conflicts are detected. The voice call is only connected if all data conflicts are resolved successfully, otherwise the request for communication is terminated.

The reachability management system only exchanges the data that is absolutely necessary to successfully resolve a communications request. This is in accordance with the policy of data economy. Because information generated during the course of negotiations can also be extremely sensitive, it has to be carefully allocated. Thus, instead of relying on a third party for negotiations and data storage (e.g. Nokia's Presence technology project [6]), the responsibility is placed on the individual parties involved.

The negotiation of a communication can be based on various attributes. The original prototype system implemented the following possibilities [4, 5, 2]:

- The manner in which communication partners are acquainted with each other.
- The urgency or intention of the communication request.
- The security requirements and mechanisms used to secure the actual communication.

A range of options allows the urgency and importance of the communication request to be specified [4, 5, 2]. Figure 3 illustrates these options.

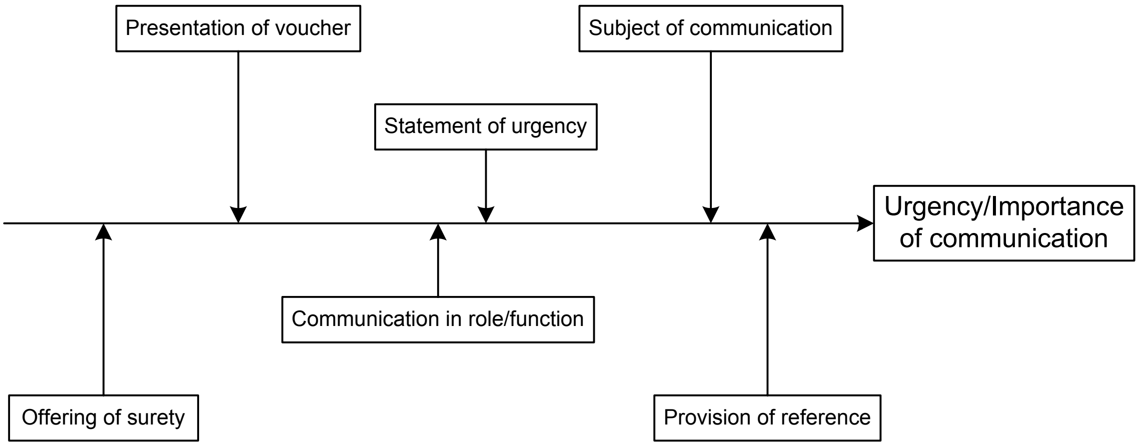


Figure 3: Specifying the urgency/importance of the communication

A statement of urgency can be given, based on the judgment of the caller. This is obviously a subjective assessment. A better indication is the specification of the subject of the communication. This can then be evaluated by the reachability management system in the case of a prearranged list of topics. The caller can indicate that he/she is communicating in a specific role or function, giving details of his/her position. The caller can also provide a reference by a trusted third party. The presentation of a voucher (issued by the callee) indicating a high priority is another option that can be used. Finally, the caller can consider offering a surety to indicate the seriousness of the communication.

In the configuration of the reachability management system the subscriber can establish the response to an incoming communications request. A call is connected only after a successful negotiation has taken place between the caller's offer and the callee's requirements. Otherwise the callee's reachability management system can offer other options, such as leaving a message or issuing a return call voucher [4].

In the following section, we will examine the technical nuances and usability issues that arise from an implementation of a reachability management system.

4 TECHNICAL AND USABILITY DIFFICULTIES

The original reachability management system consisted of an implementation using personal digital assistants (PDAs) connected to GSM (global system for mobile communications) mobile phones [5].

This enabled reachability management while allowing users to remain mobile. The configuration of security requirements and negotiation of conflicts were performed by the reachability management system running on the PDA and utilising the GSM network for communications.

A simulation study using the above configuration was performed in a health care environment [4]. While the overall opinion of a reachability management system was positive, the results of this trial indicated some problems. The following paragraphs discuss these issues.

It was noted that the current network bandwidth restrictions severely limited the features of a reachability management system. In future broadband networks these features would be easier to realise. Additionally, a problem was created by the limited capacity of the network signalling channels. This only allowed the transmission of absolutely necessary information [2].

There was a fairly lengthy delay between the initial request for communication and the actual start of the conversation. This was due to the additional negotiations which resulted when a security conflict occurred. However, as the benefits of the system were appreciated, this was tolerated.

Users now had to carry two devices (PDA and mobile phone) instead of just their mobile phone. This is obviously more cumbersome. However, because of the additional functionality the reachability management system provides, previous devices were now considered as primitive.

A demand existed for improving the switching of the active reachability level. An option to address this issue would be the use of hardware buttons on the device itself.

Finally, a feature warning the user of conflicting security settings would be useful, e.g. specifying more than one situation in which no calls are accepted.

Table 1 provides a summary of the technical and usability difficulties experienced in the original implementation of a reachability management system.

Table 1: Technical and usability issues in 1997

Type	**Issue (1997)**
Technical	Network bandwidth severely limits features
	Long delays caused by negotiation procedure
Usability	Multiple devices to carry around
	Switching difficulties due to limited hardware features
	Detecting conflicting security settings

The technological advances that have occurred since the initial prototype implementation are examined in the next section. In addition, we observe the social changes with regard to mobile communications that have occurred during the same period.

5 TECHNOLOGICAL ADVANCES AND SOCIAL CHANGES

Technological advances impacting the topic of reachability management have been made on two fronts. Firstly, communication networks have evolved from second generation (e.g. GSM) networks, with low data transmission capacity, to third generation networks which are designed for extremely high data transmission rates. Secondly, mobile devices have undergone several evolutions with the current trend to combine as much functionality as possible into one device.

The enormous growth of data communications compared to voice communications has directed the development of networks from old, circuit-switched networks to a high speed, packet-oriented architecture. The increases in data transmission bandwidth are illustrated in Figure 4.

Second generation (2G) GSM networks have a relatively low data capacity. For applications

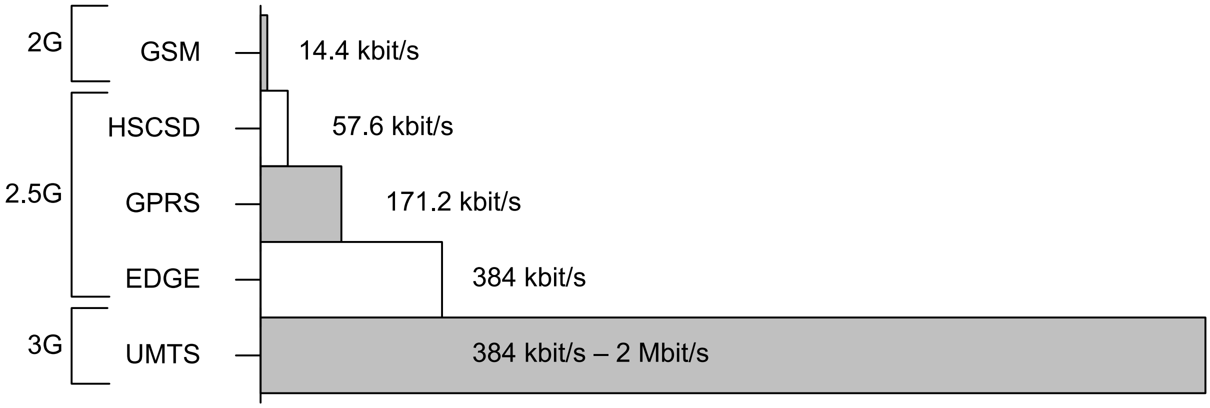


Figure 4: Theoretical maximum data transmission bandwidth

requiring high data transmission rates, such as electronic mail, web browsing and file downloads, this is not enough. An improvement of GSM's data transmission capabilities is high speed circuit switched data (HSCSD). However, HSCSD suffers from the major disadvantage that it is still connection-oriented and thus not efficient for data traffic. A more effective step to boost data capacity is through the introduction of packet switched 2.5 generation networks (2.5G). The general packet radio service (GPRS) and the enhanced data rates for global evolution (EDGE) allow data transmission speeds of up to 384 kbit/s and fall into this category. The coverage of these services is quite good, with GPRS being available in most countries worldwide. These services are ideal for data traffic as they are fully packet-oriented. Third generation (3G) networks promise to deliver true broadband wireless data transmission. The universal mobile telecommunications system (UMTS) promises data speeds of up to 2 Mbit/s, although current network coverage is limited [1, p. 93–158].

Without the restrictions of low network data capacities these advanced networks create the opportunity for innovative applications and network services to be developed. Application developers are just starting to fathom the kinds of applications they might develop to leverage the capabilities of broadband wireless-network technologies [7].

Mobile device developments have led to a convergence of technologies. The first device to combine the functionality of a mobile phone and a PDA had already been released in 1996 [8]. Today the trend is for increased functionality in mobile devices. Cameras, video recording capabilities and the ability to play digital music files are commonplace in modern mobile devices. It is predicted that over the next couple of years we will see less traditional PDAs and more PDA/phone hybrids [9].

According to Chaum [10] “advances in information technology have always been accompanied by major changes in society...” The ways in which our usage of mobile devices and technologies have evolved bear evidence of this. Today we have laws and regulations governing the use of mobile devices (e.g. driving in vehicles and during flight) as people become increasingly dependent on these devices. Even in places with well defined norms governing behaviour, such as restaurants or cinemas, people seem reluctant to switch off their mobile devices, preferring to stay reachable. For these people the benefit of being able to receive a critical (or even just trivial) message or phone call outweighs the possible disturbance/embarrassment caused to others. Ling [11, p. 123–125] reflects that “both qualitative and quantitative data suggest that the mobile telephone is seen as an invasive influence in public spaces.” He goes on to say that many people find mobile phones disturbing and there are numerous situations where the use of mobile phones are seen as inappropriate. It would clearly benefit mobile users to find some manner to maintain their normal communication customs without aggravating others.

In the following section we relate these technological advances and social changes to the concept of reachability management and look at the implications for such a reachability management system.

6 IMPACT ON REACHABILITY MANAGEMENT

From the previous section it is clear that there have been definite improvements regarding communications network bandwidth and device usability since the initial reachability management project. These advances bode well for a revisitation of reachability management.

Not only does increased bandwidth make improved reachability management systems possible, but also the conversion to packet-switched data transmissions enable data centric, economical applications. Reachability management systems, requiring fast data transmission rates for communication negotiations, will benefit from these advanced networks. High speed data transmission rates will make such a system more responsive and provide more features to users.

Today's communication networks provide an opportunity for security negotiations on multiple platform levels. Table 2 provides a summary of the available platforms and the technologies employed for both data and voice transmission.

Table 2: Communication platforms

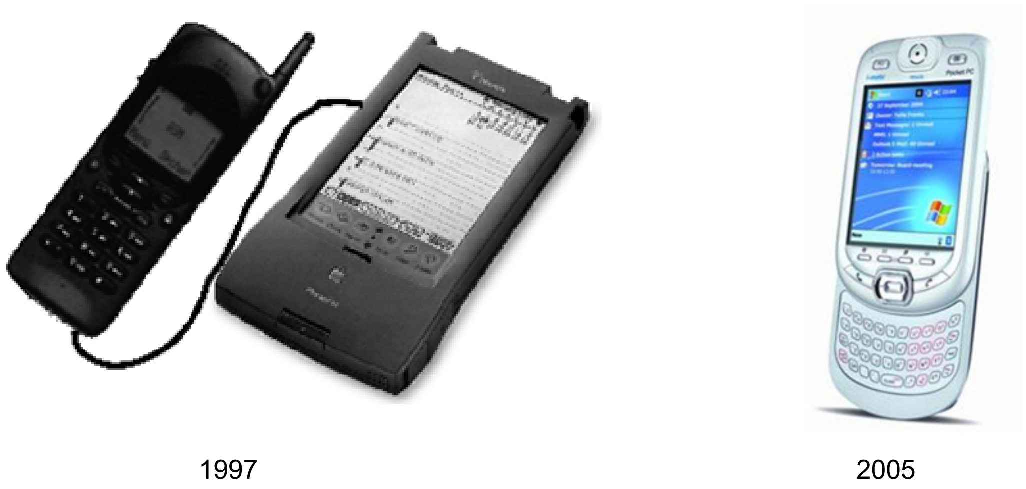
Platform	Data	Voice
GSM/HSCSD	HSCSD	GSM
GSM/GPRS	GPRS	GSM
GSM/EDGE	EDGE	GSM
UMTS	UMTS	UMTS
Internet/GSM	TCP/IP	GSM
Internet	TCP/IP	VoIP

A reachability management system could, theoretically, be implemented using any one of these platforms. However, not all platforms are ideally suited for such a data centric application. Economically it makes little sense to use HSCSD for data traffic as it uses a connection-oriented mechanism. Even a minimum amount of negotiation by the reachability management system could dramatically increase the cost of a call. GPRS and EDGE provide a better platform for data transmission. However, there are technical hardware difficulties. Current mobile devices are unable to transmit both GSM voice and GPRS data simultaneously [12]. This would make further data negotiations impossible after a call has been connected and thus limit some of the system features. In the future the UMTS platform might provide a potential solution to both the above issues. As it has a packet-oriented architecture it does not suffer from the disadvantage of HSCSD. It also utilises the same platform for both data and voice communications which could solve the problem of simultaneous data and voice transfer. Finally, using the Internet as a platform for data transfer is becoming increasingly possible today as devices are released which can access this medium.

By providing fast data transmission capabilities, modern telecommunication technologies create an efficient channel for reachability management. Increased bandwidth will enable more features to be incorporated into the system and solve the problem of delays caused by negotiations. Additionally, the use of the Internet creates interesting possibilities for future mobile applications. The effects that new communication architectures, such as VoIP (voice over Internet protocol), will have on the communications industry promises to be revolutionary.

The way in which these technologies are used is also important. Ljungstrand [13] suggests that by communicating some context information to the caller *before making a call*, the advantages of such a security negotiation can be enhanced. By placing the burden of decision on the caller the communication surplus on the callee is relieved. Also, the possibility to decide when and using what channel (e.g. phone, email, etc.) to initiate communications is given to the caller. This is a possible improvement over the methodology used in the current reachability management system.

The effects of device convergence also impact on the usability of the system. Users are no longer required to carry around multiple devices to perform the required functions, as in the original reachability management system. Input mechanism improvements, such as full sized keyboards, as well as the use of hardware features (e.g. buttons to switch from one role to another) make applications on mobile devices increasingly practical. This provides a solution to the problem of switching between different reachability settings. Figure 5 illustrates an example of device convergence.



1997

2005

Figure 5: Mobile device convergence

The equipment used in the original reachability management system in 1997 is illustrated on the left. On the right a single device combining the functionality of both the other devices is shown. For the user this means increased convenience as functionality will be combined into fewer devices. However, maintaining the usability of these devices while increasing their functionality will not be an easy task for designers and manufacturers.

It would also seem that on a social level the implementation of a reachability management system is a very logical action. With mobile usage soaring, the likelihood of social conflicts between parties is bound to increase. An application level solution to this problem can be very elegant, providing that users are willing to accept the additional complexity such a reachability management system would bring. The benefits to users would be increased privacy, by providing the ability to filter intrusive phone calls, while maintaining the security of their information and personal preferences.

In the next section we will examine other fields where the concept of reachability management is applied.

7 RELATED WORK

Fundamentally a reachability management system protects the user's privacy and prevents unwanted disturbances. Many research activities relate to this matter, albeit not necessarily in the realm of mobile communications.

In collaborative environments individuals must establish and maintain awareness (social, action and situation) of one another to complete their tasks and achieve their goals [14]. “When collaborating across distances, situation awareness is mediated by technology.” [15] Notification systems research is addressing the issue of communicating important information in an effective manner without causing unnecessary distractions [16]. This can be achieved through the constant awareness of a person’s availability. The concepts addressed in this field could also be applied to reachability management, with the similar goal of using technology to enhance communications while limiting unwanted interruptions.

Some models place the decision to initiate communication with the “caller”. A popular example of such a communication medium is instant messaging (IM). IM products contain presence awareness capabilities [17] which indicate the current status of a user using statements such as “away”, “busy”, etc. By making such context information available a user can achieve a certain amount of control over the frequency and content of his/her personal communications [18]. While the value of IM as a tool for real-time collaboration and enhanced communications is widely acknowledged [19], some users see its “interruptive nature as unfair” due to the lack of control over interruptions [17]. A reachability management system performs a similar role in mobile communications with the additional possibility of negotiating a communication in situations where a user only wants to be disturbed for important reasons, thereby limiting interruptions.

A similarity also exists with Nokia’s Presence technology. Presence is a proprietary network service which distributes your current availability status to other people in the network [6]. However, this approach has several drawbacks when compared to a reachability management system:

- As it is a third party service it does not follow the careful allocation policy of reachability management which places the user in control of negotiations and data storage.
- The service only provides an indication of the current status of a user. It does not prevent others from actually calling that person. In this respect a reachability management system provides a more complete privacy solution.
- Devices supporting the service are limited. In comparison, a reachability management system could be implemented on any device capable of running the system software and performing data negotiations.

As can be seen from the examples above, valuable lessons for reachability management can be learned from the research activities taking place in other fields.

8 CONCLUSION

Rannenberg [5] admits that “reachability as well as security management introduces additional complexity into what used to be ‘a simple phone call’.” However, the benefits of such a system are obvious, not only for the callee, but also for the caller. If the advantages of using such a system outweighs the technical complexity its adoption by mobile users is highly likely.

In this paper we outlined the fundamental concept of reachability management as well as showing how it supports the basic goal of multilateral security. The idea of balancing the security requirements of all parties involved in a transaction is particularly relevant to mobile communications. We have revealed how a reachability management system provides an example of a multilateral security implementation in telecommunications on the application level.

Table 3 provides a summarised comparison of the issues identified in Section 4 with the possibilities presented by the network and hardware technologies available today.

The technical difficulties experienced in the initial implementation of such a reachability management system were highlighted and discussed. It was noted that the main restriction to such a

Table 3: Issue comparison with current state

Type	Issue (1997)	Current state (2005)
Technical	Network bandwidth severely limits features	Broadband networks enable high speed data transmission
	Long delays caused by negotiation procedure	Shorter delays due to increased bandwidth
Usability	Multiple devices to carry around	Device convergence into a single device
	Switching difficulties due to limited hardware features	Improved hardware functionality
	Detecting conflicting security settings	Improved UI knowledge

system is communications network bandwidth (or the lack thereof). This is also a contributing factor to the delays caused by the negotiation procedure. Usability problems included the inconvenience of carrying two devices, difficulties in switching between reachability settings and the lack of a warning system to detect conflicting security settings.

We then moved on to show how technology has advanced to address these issues. Current third generation networks provide high speed data transmission rates, suitable for data applications. This should provide an effective solution to the bandwidth concerns and reduce delays caused by negotiations. Device convergence has also provided an answer to some of the usability concerns that were present. The necessary functionality for a reachability management system can now be contained in a single device, while updated hardware design and user interface (UI) knowledge provides possible solutions to switching and detection issues. Finally, we examined the social mindset prevalent in our society today and speculated on the influence this might have on the acceptance of a reachability management system.

In conclusion, we find that the topic of reachability management is not only technologically feasible, but also socially logical in our society today and thus worthy of further investigation. We have also noted similar initiatives taking place in other fields from which lessons can be learned.

9 ACKNOWLEDGEMENTS

I would like to thank Prof. Dr. Kai Rannenberg and Lothar Fritsch from the University of Frankfurt for their input and for providing access to the equipment used for the original reachability management system.

The financial assistance of the National Research Foundation (NRF) is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.

10 REFERENCES

[1] Jochen H. Schiller. *Mobile Communications*. Addison-Wesley, 2nd edition, 2003.

[2] Martin Reichenbach, Herbert Damker, Hannes Federrath, and Kai Rannenberg. Individual management of personal reachability in mobile communication. In *Proceedings of the IFIP TC11 13 international conference on Information Security (SEC '97) on Information security in research and business*, pages 164–174. Chapman & Hall, Ltd., 1997.

[3] Gunther Muller and Kai Rannenberg, editors. *Multilateral Security in Communications*.

Addison-Wesley, 1999.

[4] Kai Rannenberg. Multilateral security a concept and examples for balanced security. In *Proceedings of the 2000 workshop on New security paradigms*, pages 151–162. ACM Press, 2000.

[5] Kai Rannenberg. How Much Negotiation and Detail Can Users Handle? Experiences with Security Negotiation and the Granularity of Access Control in Communications. In *Proceedings of the 6th European Symposium on Research in Computer Security*, pages 37–54. Springer-Verlag, 2000.

[6] Nokia. Presence [online]. 2005 [cited 4 April 2005]. Available from: `http://www.nokia.com`.

[7] George V. Hulme and Rick Whiting. No Strings Attached [online]. 2005 [cited 28 February 2005]. Available from: `http://www.informationweek.com`.

[8] Richard Poynder. Converged devices market hots up [online]. 2001 [cited 4 April 2005]. Available from: `http://www.ft.com`.

[9] William Hungerford. Do PDAs have a future? [online]. 2005 [cited 4 April 2005]. Available from: `http://palmtops.about.com`.

[10] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.

[11] Richard Ling. *The mobile connection: the cell phone's impact on society*. Morgan Kaufmann, 2004.

[12] GSM World. Gprs class type [online]. 2005 [cited 28 February 2005]. Available from: `http://www.gsmworld.com`.

[13] Peter Ljungstrand. Context awareness and mobile phones. *Personal and Ubiquitous Computing*, 5(1):58–61, 2001.

[14] John M. Carroll, Dennis C. Neale, Philip L. Isenhour, Mary Beth Rosson, and D. Scott McCrickard. Notification and awareness: synchronizing task-oriented collaborative activity. *International Journal of Human-Computer Studies*, 58(5):605–632, 2003.

[15] Diane H. Sonnenwald, Kelly L. Maglaughlin, and Mary C. Whitton. Designing to support situation awareness across distances: an example from a scientific collaboratory. *Information Processing & Management*, 40(6):989–1011, 2004.

[16] D. Scott McCrickard, Richard Catrambone, C. M. Chewar, and John T. Stasko. Establishing tradeoffs that leverage attention for utility: empirically evaluating information display in notification systems. *International Journal of Human-Computer Studies*, 58(5):547–582, 2003.

[17] Ann Frances Cameron and Jane Webster. Unintended consequences of emerging communication technologies: Instant Messaging in the workplace. *Computers in Human Behavior*, 21(1):85–103, 2005.

[18] Ylva Hard Af Segerstad and Peter Ljungstrand. Instant messaging with WebWho. *International Journal of Human-Computer Studies*, 56(1):147–171, 2002.

[19] William Knight. Brace yourselves for the IM-plosion. *Infosecurity Today*, 1(6):30–31, 2004.