# Multilateral Security

# A concept and examples for balanced security

*Kai Rannenberg, Microsoft Research, Cambridge, UK, kair@microsoft.com* [#]

Multilateral security considers different and possibly conflicting security requirements of different parties and strives to balance these requirements. This paper introduces the concept of multilateral security giving some example problems and solutions. It focuses on a personal reachability and security management system that was developed to overcome the caller ID conflict. The prototype and its relation to multilateral security are described. Further, some major real world assessments of the prototype and the experiences gained are discussed. The paper concludes with a collection of technical design strategies for multilateral security that were considered important for the success of the project and some remarks on further challenges.

1 From IT Security to Multilateral IT Security
2 Fields and Approaches for Multilateral Security
3 An example: Annoying Calls and the Caller ID conflict
4 Reachability Management
- *4.1 Options for the negotiation of reachability*
- *4.2 Making a call – caller's view of reachability management*
- *4.3 Configuring reachability – callee's view of reachability management*

5 Security Management
- *5.1 Security characteristics, requirements and offers*
- *5.2 Three step coordination*
- *5.3 Security scope*

6 Reachability Management and Multilateral Security
7 Reachability Management and the Real World
- *7.1 Simulation Studies*
- *7.2 The simulation environment*
- *7.3 The participants and the set-up*
- *7.4 The cases*
- *7.5 Course of the study, observation, and analysis*

8 User controlled security – An Illusion?
- *8.1 Making users manage more complex controls successfully*
- *8.2 Personal Security Assistants*
- *8.3 The limits of negotiation*
- *8.4 Security perception issues*

9 Technical design strategies for Multilateral Security and further challenges
10 Acknowledgments
11 References

---

[#] Much of this work was done when the author was at Telematics Department, IIG, Freiburg University, Germany

# 1 From IT Security to Multilateral IT Security

A lot of early security approaches are based on the assumption that it is quite clear who has to be protected against whom. E.g. the Trusted Computer Security Evaluation Criteria (TCSEC, [USA_DoD 1985]) focus very much on the protection of system owners and operators against external attackers and misbehaving internal users. Protecting users against operators is not considered to be a major issue.

Later criteria like the Information Technology Security Evaluation Criteria (ITSEC, [CEC 1991]) have expanded the scope of the TCSEC, but the following example illustrates that user protection still was not much in the focus. In an ITSEC evaluation a function for the selective logging of activities of *individual* users was classified as a non-critical mechanism that did not need evaluation. In the opinion of the evaluators, failure of this mechanism would not create weaknesses because if the function was not active, the activities of *all* users were logged [Corbett 1992]. From the operator point of view no real security risk existed, because no audit data would be lost – only perhaps more data than planned would be collected. However, from the users' point of view this is a considerable risk, because excessive logging and the resulting data can lead to substantial dangers for users.

Early security approaches, especially in the TCSEC, assume that a security policy can definitively describe which actions are authorized. Consequently to maintain a secure state the policy only has to be enforced by a secure and trusted entity.

Clean cuts like these do not really apply when several parties with different and maybe conflicting interests are involved, as it happens in networks like telephone systems or the Internet. The following list gives some examples of competing security requirements of different parties in networks:

- Subscribers need protection from others, especially from network operators or service providers monitoring their communication activities.
- Providers need protection from fraud, e.g. through unpaid and unaccountable calls, for which no subscriber takes responsibility.
- Network operators need protection from sabotage, endangering the use of their systems.
- Subscribers need protection from harassing calls, for which no one takes responsibility.

Multilateral security [Rannen 1994] therefore aims at a balance between the competing security requirements of different parties. It means taking into consideration the security requirements of all parties involved. It also means considering all involved parties as potential attackers. This is especially important for open communication systems, as one cannot expect the various parties to trust each other. The "ideal" of Multilateral Security can be described as follows:

1. Considering Conflicts:
   a. Different parties involved in a system may have different, perhaps conflicting interests and security goals.
2. Respecting Interests:
   a. Parties can define their own interests.
   b. Conflicts can be recognized and negotiated.
   c. Negotiated results can be reliably enforced.Supporting Sovereignty:Each party is only minimally required to place trust in the honesty of others.
   b. Each party is only minimally required to place trust in the technology of others.

Multilateral Security in general refers to all "classical" security goals, i.e. confidentiality, integrity, availability, or accountability can be in the interest of one party, but not necessarily in that of another.

However a typical conflict occurs between the wish for privacy and the interest in cooperation. On one hand parties wish to protect their own sphere, information, and assets, on the other hand they strive for cooperation and wish to establish trust with partners, transfer values, or enable enforcement of agreements. An example of this conflict will be discussed in more detail in Chapter 3.

# 2 Fields and Approaches for Multilateral Security

The Kolleg "Security in Communications" [MülRan 1999] investigated Multilateral Security for communications. Three technical areas were considered especially important, though this does not claim to have covered the field completely:

1. Negotiation: Where possible parties should be able to balance their own security requirements against those from others: This led to the development of a reachability and security manager as a personal device especially for mobile communication (cf. Chapter 4 and 5). A related approach though for a different technology has been followed by the Platform for Privacy Preferences (P3P) project of the Word Wide Web Consortium. P3P had been envisioned "to promote privacy and trust on the Web by enabling service providers to disclose their information practices, and enabling individuals to make informed decisions about the collection and use of their personal information. P3P user agents work on behalf of individuals to reach agreements with service providers about the collection and use of personal information" [W3C 1998].
2. Secure Infrastructures: Terminal and device based protection alone cannot fulfil all security requirements, as e.g. switching data in networks can become a risk. Projects focussed on avoiding movement profiles in mobile communication by e.g. using mixes for call set-up in GSM mobile telephone networks [Federr 1999; KeBüSp 1999] and on proper allocation of security functions in telecommunication networks in general [SaFePf 1999].
3. IT Security and Evaluation Criteria for Multilateral Security: Users cannot be expected to know exactly whether the security properties of the devices and services they use really fulfil their requirements. Therefore they need impartial and competent security assessment of the technology they use. This approach focussed on a critical analysis of evaluation criteria and certification schemes especially regarding their ability to assess communication technology that protects users [Rannen 1999].

The remainder of this paper will concentrate on reachability and security management and the experiences made during real-life tests. It is extended by some remarks on the experiences from the other projects.

# 3 An example: Annoying Calls and the Caller ID conflict

Our example deals with the conflict regarding Caller ID displays in telephone communication[1]. Caller ID displays had led to an extensive public discussion in the early 90es.

One side argued that the security and privacy interests of callers were violated, if their telephone numbers were displayed to the called persons (callees). For example, other people on the callee side could get knowledge of the caller. Also the callees themselves could misuse the collected numbers for advertisement calls, or unlisted telephone numbers could become public.

[1] Caller ID displays are connected to a telephone line, e.g. integrated into the telephone itself, and show the number of the calling telephone line when a call comes in. Modern telephones also easily allow storage and further processing of incoming Caller IDs. A more precise term would be "Calling Line Number", but Caller ID is the generally used one [Caller ID].

The other side argued that Caller ID would just balance properly the power between caller and callee. It would especially protect callees from annoying and harassing calls, as at least some information would now be given to them. Otherwise the callees would have almost no protection[2] against being woken up in the middle of the night by some malevolent or nosy caller[3].

The following examples illustrate these issues and show, which facets of security could be important in different situations:

- A nurse in a nocturnal stand-by service is not interested in every call that might arrive at night. She wants to be reachable for emergency calls and perhaps also for close relatives or friends, for whom she would get up even at night. Potentially she wants to defend herself from harassing calls. Accordingly, she would like her telephone to receive and assess information on the caller and the urgency of a call before ringing the bell (and interrupting her sleep). Protection from transmission errors and from callers pretending to be someone else requires the integrity of the call information and the accountability of the call.
- The clients of telephone help lines that handle socially sensitive topics like AIDS, alcoholism, venereal disease, or personal debts generally want to stay anonymous. Often anonymity is a prerequisite for an open and really helpful consultation. The client must therefore be able to contact the welfare centre anonymously. It must be guaranteed that, in fact, no identity information is transmitted. If the consultation can take place anonymously, but not free of charge, it must be possible to call under a pseudonym.

The introduction of options for the callers to switch off Caller ID (either per call or per default) did not solve the problem: Callees would tend to generally reject calls without Caller IDs, as they had no other selection criteria and this then was the simplest solution. So the callers would be forced to display the Caller ID anyway.

These conflicts gave rise to the idea of "Reachability Management" (Chapter 4): Computer and communication technology should be able to give callees more options to decide whether a call was welcome, and to protect themselves from unwelcome calls. It should also give callers more options to show the importance and urgency of their calls. Additional features allowed users to specify security features for their calls (see Chapter 5 on Security Management).

# 4 Reachability Management

Reachability management offers callees the possibility to specify the circumstances, under which they are willing to receive a call. This specification, together with the information callers provide during the call request, is the basis for the decision whether the callee is immediately notified of the call, e.g. whether the telephone bell rings (cf. Figure 1). Reachability management was sometimes being described as a "Secretary for those who cannot afford a real one". Most versions of the reachability management were implemented on Newton PDAs connected to GSM telephones. This facilitated reachability management even in situations when no secretary could be around. Additionally some stationary reachability managers were connected to ISDN lines.

This chapter describes the selection and negotiation of the data being transmitted during the signalling phase of a communication request (see Section 4.1). It also shows how callers can describe their

[2] Except unplugging or switching off the phone.

[3] There is also quite some marketing interest behind the introduction of caller ID, but this issue is left out here for the moment.

communication request adapted to their situation (4.2), and how callees are able to configure their reachability needs in a variety of ways (4.3). More information can be found in e.g. [ReDaFR 1997].

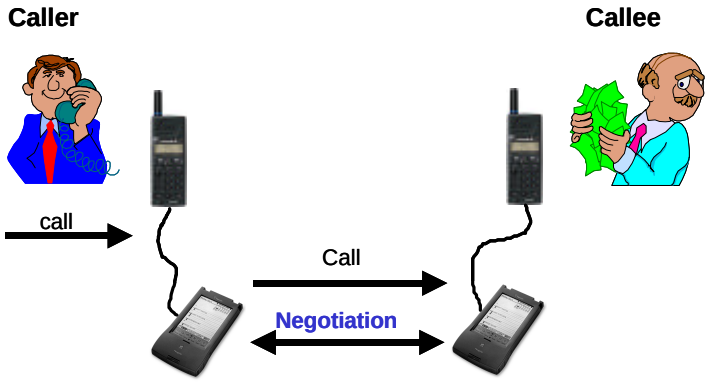


*Figure 1: Communication supported by a Reachability Management System*

## 4.1 Options for the negotiation of reachability

The prototype that was implemented facilitates negotiation of the following attributes:

- How the communication partners are acquainted with each other (anonymously, through a pseudonym, by their real identity)[4].
- The urgency or purpose of the communication request seen from each of the communication partners' point of view.
- The existing security requirements and the mechanisms used to secure the current communication (See Chapter 5).

Several options allowed specifying the urgency and importance of a communication request:

- *Statement of urgency based on self-assessment:* The caller indicates a certain degree of urgency. This assessment may be very subjective and only relevant with regard to the current situation of the callee. Therefore, this option was implemented as a further inquiry (cf. Section 4.2).
- *Specification of a subject or topic:* The topic of a desired communication can give the callee an indication of how important the communication is. The callee's reachability manager can only evaluate this specification automatically if the caller and callee have previously negotiated a list of subjects and situations.
- *Specification of a function:* Callers can indicate that they are calling in a certain function (or with a specific qualification), for example as a member of a particular project or institution. This functionality is made available by the identity cards of the identity management subsystem. When a particular identity card is selected for personal identification the function in which one is communicating is also selected. The callee may also be addressed in one of several different roles: these are essentially divided into private (private network subscriber, club member) and professional (physician in the hospital, hospital nurse) roles.

[4] An integrated "Identity Management" allowed administering real names, pseudonyms, and roles (e.g. "Member of hospital administration" or "Manager of a sports club") as well as certificates for these.

- *Presentation of a voucher:* In certain situations one may want the calls of particular persons to be given priority, e.g. when waiting for a call to be returned. A caller can issue a call voucher for this purpose. Subsequently, the callee can use this voucher in order to receive preference when she returns the call.
- *Offering a surety:* In order to emphasize the seriousness of their communication request and their statement regarding the urgency, callers may offer a (possibly negotiated) amount of money as a surety. "Satisfaction guaranteed or this money is yours!" is the philosophy of this feature. Callees who do not agree with the caller's evaluation of the urgency can keep the money or, e.g. donate it to a charity. Callees may use this option, for example, if callers did not want to disclose their identity. The option is implemented as a further inquiry (cf. 4.2).

A call only gets through if the caller's offer matches the requirements of the callee. Otherwise the callee's reachability manager can offer other options, for example to leave a message or a return call request (optionally together with a voucher).

## 4.2 Making a call – caller's view of reachability management

To set up a call, callers first have to choose their communication partner. The reachability manager supports callers with a personal subscriber directory (phone book) or an integrated "public" directory. Persons who are contacted frequently may be assigned a short code. Then the call set-up dialogue (cf. Figure 2) appears. This enables the callers to specify their identity, the reason for the call and its urgency, as well as to submit a voucher for a callback (if one is available).


*Figure 2: Call set-up dialogue*

Before the callee is personally involved, the communication request is evaluated and negotiated by her reachability manager. Depending on the rules established in the configuration of the callee's reachability (cf. 4.3) the caller's reachability manager will continue by displaying (cf. Figure 3):

- A connection set-up dialogue telling that the callee is notified;
- A message saying that the call was denied; or
- An additional inquiry.

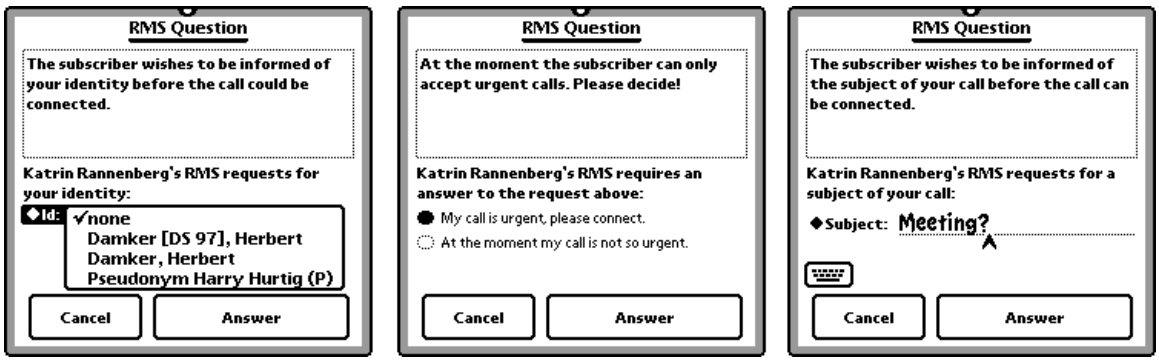


*Figure 3: Inquiry dialogues on caller's reachability manager – initiated by callee's reachability manager*

The inquiry dialogues used when establishing a connection include:

- Inquiry regarding identity: if the callee wants to be informed of the identity, a selection of the caller's own certificates appears (cf. Figure 3 left). The caller may choose not to supply identity information. In this case the callee gets the message that the caller explicitly wants to remain anonymous.
- Inquiry regarding urgency (cf. Figure 3 middle): the callee leaves the decision of whether or not to put through the call up to the caller. The caller receives a short text message and the choice of either cancelling the call (in order to avoid any disturbance in the situation described) or to insist on performing the call (because, in his opinion, it is urgent enough).
- Inquiry regarding the subject (cf. Figure 3 right): if the callee wants to be informed of the subject and the caller didn't previously give any details, a text-input field appears.
- Inquiry regarding a surety: in order to emphasize the seriousness of a communication request, the callee may ask the caller to remit an amount of money as a surety. The caller may comply (and remit the amount requested), or reject the request.

If the call is rejected, the caller sees the call rejection dialogue. This informs about the reason for the rejection and offers various opportunities to continue, e.g. the prototype offers an opportunity to leave a message or a callback request (in form of a text message with a return call voucher attached). A message editor and a simple folder system were implemented in the prototype.

## 4.3 *Configuring reachability – callee's view of reachability management*

In the personal configuration of their reachability manager the users determine the various reactions to incoming calls (communication requests). They define which information the reachability manager will request from a caller in order to evaluate the communication request. A likely example would be that the callee's reachability manager requests the identification of the caller, or a surety from an unidentified caller. Subscribers configure their reachability for different situations of daily life or the working environment by defining a set of rules for each situation. When using the reachability manager they then switch between these predefined situations.

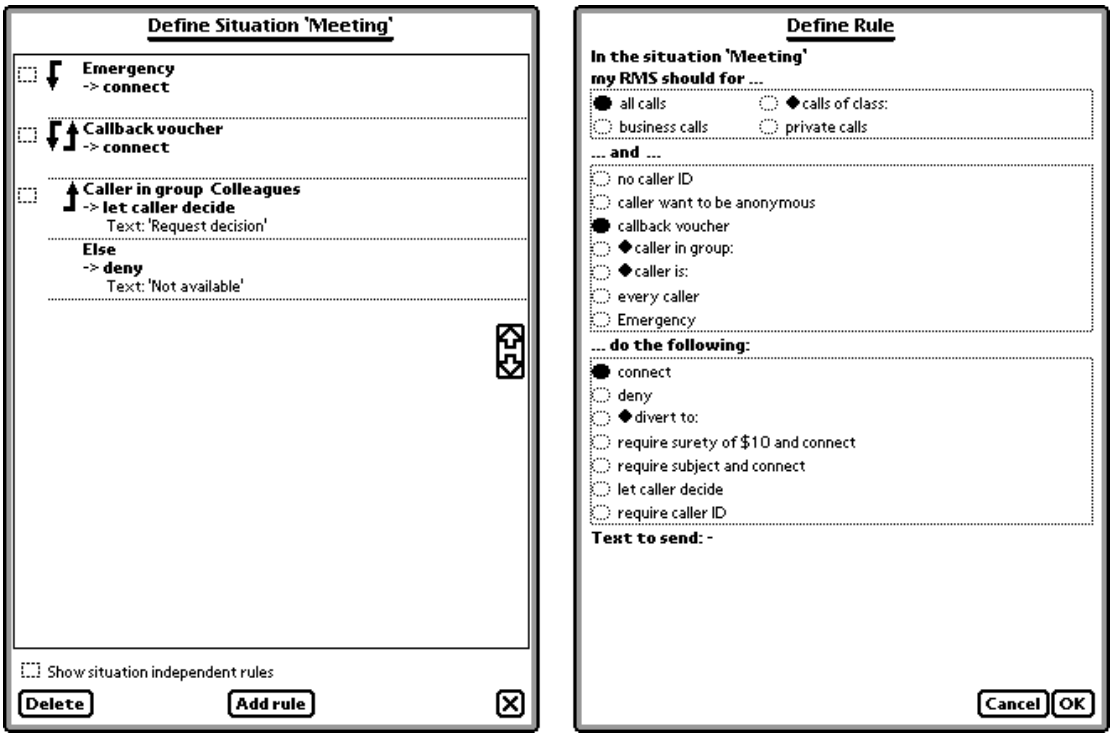


*Figure 4: Configuration of a situation and definition of a rule*

The left side of Figure 4 shows the set of rules applying to the sample situation "Meeting"; the right side shows the dialogue for defining rules. Each individual rule establishes the subscriber's role (business or private) and the conditions that have to be fulfilled (e.g. call from a particular subscriber). The reaction to incoming calls (e.g. connect, deny, divert or make further inquiry) is also defined for each case. Because the rules are evaluated top down, their order within a particular situation is important and, therefore, may be changed as required. The last rule of each situation becomes the default rule for the situation. It describes the reaction to be taken when no other rule applies. The prototype also contained other concepts, such as "situation independent rules" being evaluated with top priority in any situation, but these proved as to be too complex in the real world assessments (cf. Chapter 7 and 8).

# 5 Security Management

Which security measures are to be used in a communication is situation-dependent and the partners may view this controversially. This issue was addressed by the negotiation concept of *security management* [GaGrPS 1997, Pordes 1998]. Users can independently decide whether to use security measures or not and negotiate this with their partners. The security management is embedded in the reachability management system and aims at being easy-to-handle, even though the technical security mechanisms are fairly complex.

## 5.1 *Security characteristics, requirements and offers*

The prototype used in the simulation study did not provide all possible security measures for telephone communication, but offered examples of some particularly important measures[5]. *Encryption* and

[5] It should be noted, that some of the security functions offered were not actually implemented, as the focus of the project was on experiences on negotiation. End-to-end voice call encryption would have required special telephone

*Unobservability* provide protection of the communication connection and, therefore, affect both communication partners equally. On the other hand, a user can provide *Authentication* and *Acknowledgement* of a call without the partner doing the same.

Although only a few security measures were offered, they yield numerous possible combinations for each call. For reasons of usability the security measures were grouped into the dimensions *Confidentiality* and *Commitment*. "Confidentiality" aims at protecting the users' secrets and comprises the measures encryption and unobservability. "Commitment" aims at defining how much the users commit themselves to the call. It comprises the measures authentication and acknowledgement. Users are then able to select the requested levels of confidentiality and commitment, which the system maps to the various security measures (cf. Figure 2). However, it was also possible to set the various measures directly ("self-defined").

## 5.2 Three step coordination

In principle, the negotiation of security requirements can be carried out in any number of steps, including further inquiries from the caller or the callee. For ease of handling a simple model was implemented:

1. Callers make a security proposal in the call template. This proposal contains the security measures they request and those they are prepared to take. This is transmitted to the callee's reachability management system.
2. The callee's security manager compares the proposal with its security requirements and preferences. It then produces a coordinated and modified counterproposal.
3. The caller's security manager compares the proposal and the counterproposal and puts the call through if both match. Otherwise the caller is asked whether he accepts the callee's proposal.

## 5.3 Security scope

To avoid repeated inquiries or frequent failures of negotiation, both of the parties specify additional conditions, e.g. whether to take specific security measures if requested, or whether a personal security requirement can be ignored, if necessary. This is done by the "security scope", a three-level schema of attributes associated locally with security requirements and security offers. Security requirements can be assigned the attributes "mandatory", "if possible", "don't care" and security offers the attributes "don't care", "if necessary", "never".

To avoid the caller having to disclose requirements and offers immediately, the security scope is not communicated directly. Instead, the caller (or their security manager) "overplays" the requirements and "underplays" the offers in the first negotiation step. Only two levels of the local three-level setting are transmitted. The attribute "if possible" is transmitted as "mandatory", i.e. the requirement is described as non-negotiable. The attribute "if necessary" is transmitted as "never", making the offer non-negotiable. If the callee's counterproposal does not match the caller's proposal, the security manager can lower the original security requirements (without having to re-consult the caller) and put the call through. Only if this fails the caller is asked regarding the counterproposal.

---

hardware instead of "off-the-shelf" GSM mobile phones. Measures for unobservability would have required too substantial changes in the GSM communication infrastructure. However the prototype contained a crypto facility for signing and verifying text messages and certificates.

# 6 Reachability Management and Multilateral Security

Reachability management can be seen as an example for a technology supporting multilateral security (cf. the “ideal” of Multilateral Security in Chapter 0):

1. Reachability management considers conflicts between callers and callees and their security interests. It was actually invented to manage some of those.
2. Different interests are respected:
   a. Parties can define the circumstances under which they would like to be reached and the information they are wiling to provide.
   b. Conflicts are shown to the callers, so that they can react.
   c. Negotiated results can be enforced, e.g. sureties and deposits can be kept (this issue is not a core reachability management topic).

   The major question of course is whether the negotiation helped users to achieve the type and the degree of security they wished. To gain experience with this a number off real life assessments accompanied the development (cf. Chapter 7).
3. Sovereignty is supported:
   a. Parties are not generally required to place trust in the honesty of others, and if the choose so, they can exactly define the degree of trust they wish to place.
   b. Callers and callees have their own reachability management devices and don’t need to trust technology of others, e.g. network providers who offer reachability management as a central service. This can be very important, as the data arising in the context of personal reachability management are extremely sensitive: some of them (e.g. the programmed reaction to incoming communication requests) contain information on personal attitudes towards other people. So together with security management (which requires securing personal keys) reachability management can be seen as a starting point for a personal security assistant, which also poses new challenges (cf. 8.2)

# 7 Reachability Management and the Real World

The reachability and security manager was assessed in several ways:

1. A one-day “tele-roleplay” (“Teleplanspiel”) took place before the first implementations started: Kolleg participants all over Germany had to solve telecommunicative tasks. They had reachability managers available, which were played by colleagues, but to simulate a machine-like interface they could interact with them only via paper based forms that they had to fill out after certain rules. The aim of the tele-roleplay was to test features and the concept of stepwise negotiation.
2. Several versions of the reachability manager underwent professional usability tests by psychologists to ease their handling [DuENRS 1999].
3. The largest test was the simulation study “Reachability and Security Management in Health Care” in which more than 30 real test persons used the technology under realistic conditions.

This text concentrates on the simulation study, as this was the largest trial and brought the most advanced results. It shortly describes the concept of simulation studies (Section 7.1) and gives an overview of the environment (7.2), the participants (7.3), the cases and set-up (7.4), and the course of the study and the methods of observation and analysis (7.5). A more detailed description of the simulation study can be found in e.g. [AmBlBR 1999, PoRoSc 1999, RoHaHe 1999].

## 7.1 Simulation Studies

Simulation studies follow the principle “Highest proximity to reality without damage”: Qualified persons from the field under investigation act as “expert test persons”. They are observed over a set period of time working independently with prototype technical devices in an environment, which closely resembles reality. This means

- Real tasks, which have been devised on the basis of real problems;
- Really affected persons and cooperation partners, which are, however, played by test persons;
- Real attacks and breakdowns, the damage of which, however, is restricted to the context of the simulation;
- Real test cases, which, likewise, only produce simulated consequences.

## 7.2 The simulation environment

For several reasons the simulation took place in the Heidelberg (Germany) health care system:

- The healthcare IT professionals had some insight into security issues considering the sensitive data they were handling in their patient records;
- Reachability management was an issue in the hospital: Doctors usually carried pagers to be available when being away from their office. These pagers were seen as a constant nuisance as they only transmitted very limited information: a telephone number to be called and the signal whether the request was “urgent” or “very urgent”. So very often doctors were forced to “jump to a not so near telephone” only to find out that the call was not even half as urgent as the caller perceived. Reachability management was also an issue with general practitioners who were in the process of deploying mobile phones to use during home visits.
- The hospital already experimented with PDAs. They were used to ease mobile access to electronic patient records and other information as well as to enhance the communication, e.g. to send requests for medicine or special examinations to the hospital pharmacy or the radiology department. Testing of this software was part of the study.

## 7.3 The participants and the set-up

31 “expert test persons” from different healthcare organizations participated. A large group was physicians from eight different medical departments of Heidelberg University Hospital. Nurses from two wards, one head nurse and one administrative officer joined them. Two general practitioners, together with their assistants, also took part. Their participation was important in order to observe the use of mobile technology in outpatient care and to investigate the co-operation beyond organizational borders, e.g. between the general practitioners and the hospital physicians, when a patient was referred to the hospital or sent home again. It was also possible to investigate the co-operation between hospital staff and outpatient care at the patients’ homes as two nurses engaged in aftercare participated.

All “expert test persons” participated from their usual places of work and also during other activities including meetings, conferences, transporting of patients, and shopping. The devices were used in cafes, in corridors, in elevators, on bicycles, in cars and in trains.

Due to the fact that neither real patients, nor real patient data should be used during the evaluation of technology it was necessary to create simulation tasks for the “expert test persons” based on real tasks. These simulated tasks were prepared in advance and presented to the test users during the simulation week, together with a number of special communication tasks.

In order to offer the expert test persons a close-to-reality communication environment, 10 scientists from the research projects acted as their counter-parts. They also used the prototype technology and played the roles of friends, patients, relatives, administrative persons, and staff from the professional doctor's association and health insurance institutions (altogether 75 virtual users). Another 25 persons took part by working in the user and technical support, observing the distributed "expert test persons" and playing the patient roles. Altogether, 76 people were involved in the simulation study.

## 7.4 The cases

The "expert test persons" processed 21 medical cases during the simulation week. They were asked to add to the information available for a simulation patient by ordering specific examinations or consultation. The simulated cases were initiated by a simulation patient who appeared at the doctor's office or by an electronic referral together with a letter of admission. When examinations or consultation were ordered, the requested information (laboratory results, radiology results) was transferred to the central patient database. The physician treating the patient could access this information. For some patients additional information regarding previous stays in hospital was available. The "expert test persons" were entirely free in respect of actions or decisions. The only control the "simulation directors" exercised over the course of the simulation was that of assuming some roles (for example patient, relative, senior physicians or administrative person), or by providing specific information.

Apart from these extensive medical cases (70 examination requests, 42 examination reports), about 60 smaller communication tasks were carried out – each of them with three to ten communication contacts. These tasks were, for instance, information requests from the hospital management, requests of a health insurance company, questions from relatives, invitations from club members, or unsolicited offers from an insurance agent or an investment broker.

## 7.5 Course of the study, observation, and analysis

Altogether, roughly 2000 telephone contacts took place during the simulation week and around 1000 test messages were exchanged. Numerous changes in the configurations of the reachability and the security management system were made[6]. About 50% of the messages were encrypted and nearly 50% were digitally signed. One example, a faked warning with a faked signature certificate from a non-existing pharmacy reporting problems with a certain medicine, shows how near to reality the cases were: The message created so much discussion and involvement among the participants that some administrative officers in the hospital considered to ask for stopping the study.

In order to obtain the individual experiences of the different test users and to analyse them for future use of the technology, the following instruments were used (among others and only with agreement of the users):

- Observation of the behaviour of the test persons during processing of the simulation cases;
- Daily group discussions about experiences and specific design aspects;
- Analysis of the logged communication data;
- A questionnaire circulated after the simulation week (over 80% return);
- A post-survey in the form of two-hour intensive interviews.

[6] This includes only the documented transactions, probably more actions took place that were neither documented nor reported.

# 8 User controlled security – An Illusion?

The general positive outcome was that users happily accepted the opportunity for controlling their own security even though this introduced extra complexity. The main reason for this success was that the users saw a high personal benefit for their daily communication tasks (8.1). Users who make active use of the security functions of course pose challenges to the technical base of personal security assistants (8.2). An increasing awareness of security issues could be noted (8.4), but also some limits of the concept of negotiation showed up clearly (8.3).

## *8.1 Making users manage more complex controls successfully*

Reachability as well as security management introduces additional complexity into what used to be "a simple phone call". In general users accepted the extra complexity, as they saw a high personal benefit for their daily communication tasks.

However different users used rather different ways to cope with the complexity and to find the configurations they liked best:

- Some users never changed the pre-configured situation rule sets ("connect every call", "no calls", and "meeting").
- Many participants created some new situations or changed rules in existing situations.
- Some users created a large number of situations in advance trying to match the real-life situations they could envisage (e.g. "visiting a patient", "office work", or "stand-by") but reduced this number later after having gained more experience.

In the end most users regarded three to five different situations as a useful number, e.g. three levels of reachability similar to the phases of a traffic light (green, yellow, red) and some personal extras.

There seems to be the important lesson that the general positive reaction to the challenge of configuring one's own reachability was based on the fact that users were offered some variety: They could upgrade from simple settings but also use the whole power of the tool to find out about requirements they might have[7]. So interesting compromises between earlier extremes turned out:

- Original "normal" telephones that did not offer any options at all had been considered as too primitive. The same had been true for the pagers used in the hospital, which had too limited facilities (cf. 7.2).
- Early versions of the reachability manager included all options the developing computer scientists could think of. They failed already in the usability tests for being much too complex.
- So the version used in the simulation study aimed at a mixture of expressive power and entry-level ease to encourage as many users as possible to use as many features as they could.

Switching between telephone and email communication, e.g. for leaving a message when callees were not available, did not cause any confusion among the users. On the contrary, this feature was very popular. Callers could write and correct their messages more easily than with a normal voice mail system. Callees could more easily overview and digest incoming messages and also take advantage of the callback vouchers.

Two other issues also encouraged users to experiment with the more sophisticated functionality:

---

[7] Users could theoretically also downgrade to the "normal" situation without reachability manager, but this wasn't observed.

- A lot of the functions could easily be tested without producing any harm to the equipment or any data.
- Manual filtering was still possible and allowed users to deny a call, even when the rules would have let it through.

There was some demand for an assistance function warning users when they had specified “suspicious” combinations, e.g. illogical rule sets or more than one situation in which all calls were blocked.

However there was much more demand for improving the switching of the activated reachability situation or level. In order to avoid complicated actions, hardware buttons can be designated for quick and easy switching between reachability levels. Mobile phones now tend into this direction, when they offer buttons for switching the ringer to “silent”.

There could also be a reminder function to be activated when the user switches to a reachability level with strong filtering. This reminder function could prevent the user from forgetting to switch back to a more communicative reachability level. A more powerful step could be to let the mobile device analyse body movement patterns or other biometric data of its wearer. For example movement patterns like driving a car or riding a bicycle could restrict the reachability, while movement patterns like working at a desk could ease reachability.

It should be useful to take a look at the related effort of the Platform for Privacy Preferences (P3P) project. Unfortunately, “the P3P Specification Working Group removed significant sections from earlier drafts of the P3P1.0 specification in order to facilitate rapid implementation and deployment of a P3P first step” [W3C 2000]. So “four major components that were part of the original P3P vision” are not included in P3P 1.0:

- a mechanism to allow sites to offer a choice of P3P policies to visitors;
- a mechanism to allow visitors (through their user agents) to explicitly agree to a P3P policy;
- mechanisms to allow for non-repudiation of agreements between visitors and web sites;
- a mechanism to allow user agents to transfer user data to services.

The authors of the P3P specification envisage future versions of the P3P specification after P3P1.0 is deployed and improvements based on feedback from implementation and deployment experience. Some of the experiences with reachability and security management and how it helped users to manage more complex controls successfully might be useful, too.

## *8.2 Personal Security Assistants*

Reachability and security management show that new security functionality brings new security challenges with it. The data arising can be extremely sensitive: some of them describe callers’ and callees’ current situations; others (e.g. the programmed reaction to incoming communication requests) contain information on personal attitudes towards other people. Information like this may even be protected by the privacy regulations of some states. It must be allocated carefully and has to be protected from all potential communication partners as well as from third parties, such as service providers.

So reachability management and security management can be seen as a starting point for a “trustworthy” personal security assistant and as an example for the decentralized realisation of communication and security services. On the one hand this poses demanding challenges on the security and reliability of the personal devices, e.g. on their operating systems. Especially one issue has gained relevance in e.g. the European electronic signature directive [EU 1999]: When data are digitally signed the device must make sure, that the users see what they sign. This requires that the interoperation of a computer’s file system and display cannot be manipulated.

On the other hand personal devices are already security relevant with e.g. mobile phones allowing access to network services that can incur high expenses. So users get acquainted to the fact, that they carry important and powerful devices that bring responsibilities with them. Already during the development of the reachability manager first steps towards the integration of mobile phones and PDAs could be seen: The Nokia 9000 communicator has both functionalities in one box, though their features are not very much integrated. PCM/CIA cards that allow GSM access for PDAs are becoming a commodity.

Personal security assistants will probably be one of the major challenges for secure computing. Not only they have to be usable and trustworthy, which will include at least some security, their trustworthiness must show so that users can build trust. The prototypes were not especially guarded, as this wasn't in the focus of the project. However the reactions on the introduction of forged messages and signatures into the working process of the hospital (cf. 7.5) showed clearly how important reliability is for acceptance.

## 8.3 The limits of negotiation

Negotiation about options was generally welcomed. However there are limits to it, especially when a feature becomes very popular. The option to receive a receipt for the fact that one was calling but not being let through was particular popular with users who had a lot of outgoing communication. They saw these receipts as useful defence in case callees would complain why a time-critical decision had been taken without checking back with them. However callees tended to be less willing to hand over "non-reachability receipts" to avoid what they considered misuse.

An illustrative example was the following: Doctors, who had taken in a new patient at the reception, had to reach somebody at a ward to ask for a free bed before they could transfer the patient there. Busy wards usually did not put too much priority on answering the phone. So with reachability management the doctors tended to send a message that they required a bed and had not got through. Wards claimed that this was simply shifting problems over to them and not a cooperative way to do business and use the information they gave out. Subsequently it became harder to get "non-reachability receipts" from them.

When callees had configured their reachability managers to not issue "non-reachability receipts" callers asked for third parties to document their call attempts. While this can be solved easily (some users simply took bystanders as witnesses for not getting through) it also shows a limit of negotiation. One cannot really negotiate about proofs for being ignored.

Callees who are in high demand can negotiate a lot of information out of callers. The project group had envisaged this problem in advance, but no general solution was seen[8]. Therefore the group was rather interested how things would turn out in "real life" and how important the "fundamental problem" would be in practice. It turned out that in most cases callees were keen on the "subject" information accompanying a call and did not require much more.

There is also another non-negotiable issue: Negotiating about the unobservability of a single transaction does not make sense, when the negotiation contains the character of the transaction.

## 8.4 Security perception issues

It showed that the awareness of security issues increased over time, partially because of incidents, partially because users got a deeper understanding of the technology. However users understood "confidentiality" of a call in a far broader sense than the developers had intended. They had thought in "classic" telephone communication protection terms, meaning that "confidentiality" would apply protection against eavesdropping. Users expected that "confidentiality" would also mean that the other side had been properly authenticated and had agreed to not publish the content of the call later.

---

[8] Except turning back to the "old" telephone system with no context information being transmitted

Another observation was that many users intuitively coupled authorisation and identification issues: The concept that authorisation can make sense even without identification, e.g. when a compensation for eventual damage is prepaid, was perceived only by a few, who thought about situations where it was advisable not to come up with one's own identity.

Misunderstandings like these correspond with reports in [WhiTyg 1999] on PGP users misunderstanding terms and concepts of encryption and public key infrastructures and seem to be a rather common problem. One might like to ask for more security education, but this is only one side of the problem. There is at least one lesson for developers: To avoid confusion one should check whether technical terms like "confidential" are already reserved in the application environment. If so, it is useful to either look for other terms or to make very clear which level (e.g. technical communication or application area customs and ethics) is meant when a certain term is used.

# 9 Technical design strategies for Multilateral Security and further challenges

In conclusion there seem to be a number of technical design principles that helped the success of the project both in terms of practical acceptance and in terms of coming near to the "ideal" of multilateral security:

1. **Data Economy**: The best design strategy to fulfil confidentiality requirements of users who have no control over their own personal data is the *avoidance of data*, e.g. in communication protocols. Data that do not exist or are not transmitted need no protection from unauthorized use. Since identification data, for instance, are frequently needed for e.g. accountability purposes, complete data avoidance is often impossible. Nevertheless the strategy of *data economy* (i.e. to create as little susceptible data as possible) is worthwhile for preventing risks and also reduces the expenditure for data protection in case this is legally mandated. Examples in the project were the options offered by the reachability manager, as they allowed avoiding transferring IDs and the use of protocols for unobservable communication, e.g. mixes, implicit addresses, or limited broadcast.
2. **Careful allocation**: If the creation of some data is unavoidable (e.g. when it is indispensable for correctly providing or charging for a service) the *ownership* and *location* of such data have to be allocated carefully. Often data should be distributed among different parties of a distributed system (*decentralization*) in order to make misuse less attractive and to limit the consequences should it occur. The best strategy may even be to give the storage and the processing of data into the control of those who require the security. This approach helps customers, for example, who do not want to, or are not able to trust their service providers. It also removes the fear of all-knowing or all-powerful attackers. Examples in the project were the approach to store the reachability data in the users' PDAs and the aims to avoid central registers in communication networks, e.g. the Home Location Register in GSM mobile communication networks.
3. **User ability to control**: If users come into the situation to accept trade-offs between some of their goals, they should be able to control the situation, e.g. by easy configurations and useful status information ("Where is my data, where will it go, after I click that button?"). Examples in the project were the reachability manager options for configuration as well as for call set-up. A legal requirement promoting the use of this strategy arises with electronic signatures at least in Germany: It asks for a proper equivalent to the "warning function" of handwritten signatures, which make users realize that something relevant happens, when they have to take up a pen.
4. **Usability of security mechanisms**: Only usable mechanisms can be used. This challenge showed to be not an issue of offering *the* right solution to users, as *the* users don't exist, but to offer something for different users at different stages of interest, understanding, and competence. The simulation study of the project gave good evidence that the features and implementation of reachability management

complied with users' requirements. Users learned to understand the consequences of their decisions and tuned their policies so these matured to a satisfying level.

5. **Opportunities for individual negotiation**: Negotiation can only work if there are real options and opportunities to negotiate on. Reachability management showed that enhanced technology can open further opportunities, but it also showed that an economic and regulatory framework might be needed, e.g. to balance great differences in the power between the partners.
6. **Discernable security in products and services**: Better security can only be used and marketed if its advantages can be recognized and comprehended. Enhancing the ISO/IEC Evaluation Criteria for IT Security [ISO/IEC 1999] and their sister document, the Common Criteria [CCIB 1999], was a step of the project into this direction. This of course does not replace the need for better products fulfilling the enhanced requirements.

# 10 Acknowledgments

Thanks go to my colleagues in the Kolleg "Sicherheit in der Kommunikationstechnik" for their groundbreaking work there. I would also like to thank Dieter Gollmann, Michael Roe, Fabien Petitcolas, Roger Needham and the NSPW reviewers for helping to re-reflect the Kolleg's ideas and to transfer the results to a broader audience.

# 11 References

[AmBlBR 1999] Elske Ammenwerth, Hans-Bernd Bludau, Anke Buchauer, Alexander Roßnagel: Simulation Studies for the Evaluation of Security Technology; pp. 547-560 in [MülRan 1999]

[Caller ID] http://www.markwelch.com/callerid.htm

[CCIB 1999] Common Criteria Implementation Board: Common Criteria for IT Security Evaluation, V. 2.1, August 1999; http://csrc.nist.gov/cc

[CEC 1991] Commission of the European Communities, (Informal) EC advisory group SOG-IS: IT Security Evaluation Criteria, V. 1.2; 1991-06-28; Office for Official Publications of the EC; also www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF

[Corbett 1992] Chris Corbett: ITSEC in Operation – an Evaluation Experience, Proc. 4th Annual Canadian Computer Security Conference, May 1992, Ottawa, Canada, pp. 439-460

[DuENRS 1999] Cornelius Dufft, Jürgen Espey, Hartmut Neuf, Georg Rudinger, Kurt Stapf: Usability and Security; pp. 531 - 545 in [MülRan 1999]

[EU 1999] Directive of the European Parliament and of the Council on a Community framework for electronic signatures; http://europa.eu.int/comm/dg15/en/media/sign/elecsignen.pdf

[Federr 1999] Hannes Federrath Protection in Mobile Communications; pp. 349-364 in [MülRan 1999]

[GaGrPS 1997] Gunther Gattung, Rüdiger Grimm, Ulrich Pordesch, Michael J Schneider: Persönliche Sicherheitsmanager in der virtuellen Welt; S. 181-205 in: Günter Müller und Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn u.a. 1997

[ISO/IEC 1999] Evaluation Criteria for IT Security (ECITS), Parts 1-3; International Standard 15408; 1999-12-01; http://isotc.iso.ch/livelink/livelink/fetch/2000/2489/Ittf_Home/ITTF.htm

[KeBüSp 1999] Dogan Kesdogan, Roland Büschkes, Otto Spaniol: Stop-And-Go-MIXes Providing Probabilistic Anonymity in an Open System; pp. 365-380 in [MülRan 1999]

[MülRan 1999] Günter Müller, Kai Rannenberg (eds.): Multilateral Security in Communications; Addison-Wesley-Longman; München et al. 1999; ISBN-3-8273-1360-0

[Pordes 1998] Ulrich Pordesch: Negotiating security among end users: concept and test in a simulation study, Computer Networks and ISDN-Systems 30/1998, pp. 1597

[PoRoSc 1999] Ulrich Pordesch, Alexander Roßnagel, Michael J. Schneider: Simulationsstudie “Mobile und sichere Kommunikation im Gesundheitswesen”, DuD 1999, p. 76

[Rannen 1994] Kai Rannenberg: Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security; in Richard Sizer, Louise Yngström, Henrik Kaspersen und Simone Fischer-Hübner: Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference August 12-17, 1993, onboard M/S Ilich and ashore at St. Petersburg, Russia; North-Holland, Amsterdam 1994, pp. 113-128

[Rannen 1999] Kai Rannenberg: What can IT Security Certification do for Multilateral Security? pp. 515-530 in [MülRan 1999]

[ReDaFR 1997] Martin Reichenbach, Herbert Damker, Hannes Federrath, Kai Rannenberg: Individual Management of Personal Reachability in Mobile Communication; pp. 163-174 in Louise Yngström, Jan Carlsen: Information Security in Research and Business; Proceedings of the IFIP TC11 13th International Information Security Conference (SEC '97): 14-16 May 1997, Copenhagen, Denmark; Chapman & Hall, London; ISBN 0-412-8178-02

[RoHaHe 1999] Alexander Roßnagel, Reinhold Haux, Wolfgang Herzog (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig, Vieweg, 1999

[SaFePf 1999] Reiner Sailer, Hannes Federrath, Andreas Pfitzmann: Security Functions in Telecommunications – Placement & Achievable Security; pp. 323-348 in [MülRan 1999]

[USA_DoD 1985] Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[W3C 1998] World Wide Web Consortium: P3P Guiding Principles; W3C NOTE 21-July-1998; www.w3.org/TR/1998/NOTE-P3P10-principles

[W3C 2000] World Wide Web Consortium: The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification; W3C Working Draft 11 February 2000; www.w3.org/P3P/

[WhiTyg 1999] Alma Whitten, Doug Tygar: Why Johnny Can't Encrypt: A Usability Evaluation of PGP5.0; Proceedings of the 8th USENIX Security Symposium, August 1999