How Much Negotiation and Detail Can Users Handle? Experiences with Security Negotiation and the Granularity of Access Control in Communications

Kai Rannenberg

Microsoft Research Cambridge, UK
kair@microsoft.com

Abstract. Tailor made security is being enabled by more options for specifying security policies and enhanced possibilities for negotiating security. On the other side these new options raise the complexity of transactions and systems: Users can be overwhelmed, which can lead to less security than before. This paper describes conclusions from a case study and trial of a personal reachability and security manager for telephone based communication. The device helped to negotiate and balance security requirements. The study analysed how much negotiation and detail users could handle during their day-to-day transactions and how they could be supported. Some results are strongly related to more 'classic' security techniques like access control that are becoming more and more interactive: When users learn to understand the consequences of their access control decisions and can tune their policies these mature to a satisfying level. When users see advantages for their daily activities they are willing to invest more time into understanding additional complexity.

1 Introduction: Non-expert Users and Security Technology

Security technology tends to become more powerful and to open more options for specifying individual and fine-grained security policies. Moreover enhanced communication facilities allow negotiating the security properties of transactions. As participants often have different and conflicting interests, these negotiations are important. But more options also raise the complexity of transactions and systems, users can be overwhelmed [Gong99, p. 150], which can lead to less security then before [WhiTyg99]. Therefore it is important to see how much negotiation and detail users can handle during day-to-day transactions and how to support them in this. Usability for non-expert users can even be an important factor in the decision whether or not to implement a security mechanism.

This paper describes conclusions from a case study on the negotiation of reachability and relates them to more 'classic' security techniques, especially access control. The study was part of a larger project on multilateral security (see

F. Cuppens et al. (Eds.): ESORICS 2000, LNCS 1895, pp. 37–54, 2000.

Section 2). It focussed on personal telephone reachability and security management, an approach that aims at avoiding annoying calls and securing telephone communication (Section 3 and 4): Callees (receivers of a call) can formulate general and security requirements for accepting calls. Callers can use several options to demonstrate the importance or urgency of their call. The reachability and security manager was used in a trial by more than 30 users in public healthcare (doctors, nurses etc.), most of them neither computer nor security literate (Section 5).

While the main security goals of the reachability manager (avoid annoying calls but don't force the callers to deliver all information all the time) do not exactly match 'classic' security requirements, the configuration of one's own reachability and security requirements has some striking similarities to computer and data access control. So some of the experiences of how users reacted to the complexity introduced into their 'telephone life' seem to be useful in a broader sense. Therefore Section 6 discusses some of the results from the study and puts them into relation to fundamental issues of access control, negotiation in general, and issues of security perception.

2 Multilateral Security and Negotiation

The 'Kolleg Security in Communications' [MülRan99] aimed at 'Multilateral Security' for communications: All parties in a transaction, e.g. a telephone call, should be able to formulate and enforce their security interests [RaPfMü99]. This was considered to be especially important for open communication systems, where different parties, e.g. subscribers, providers, or network operators, have different and maybe even conflicting interests. One approach was to make technology offer options and facilitate negotiations to balance one's own security requirements against those from others.

2.1 The Example: Annoying Calls and the Caller ID Conflict

One example that had strongly influenced the work was the conflict regarding Caller ID displays in telephone communication. Caller ID displays had in the early 90's led to an extensive public discussion[1].

One side argued that the security and privacy interests of callers were violated if their telephone numbers were displayed at the called persons' (callees') side. For example, other people on the callee side could get knowledge of the caller calling. Also the callees themselves could misuse the collected numbers for advertisement calls, or an unlisted telephone number 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 generally used [Caller ID].

The other side argued that Caller ID would just balance the power between caller and callee properly. 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 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.

This situation gave rise to the idea of 'Reachability Management' (Section 3): 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 Section 4 on Security Management)

3 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 allows for reachability management even in situations when no secretary could be around. Additionally some stationary reachability managers were connected to ISDN lines.

This section describes the selection and negotiation of the data being transmitted during the signalling phase of a communication request (see Section 3.1). It also shows how callers can describe their communication request adapted to their situation (3.2), and how callees are able to configure their reachability needs in various ways (3.3). More information can be found in e.g. [ReDaFR97].

3.1 Options for the Negotiation of Reachability

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

[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.

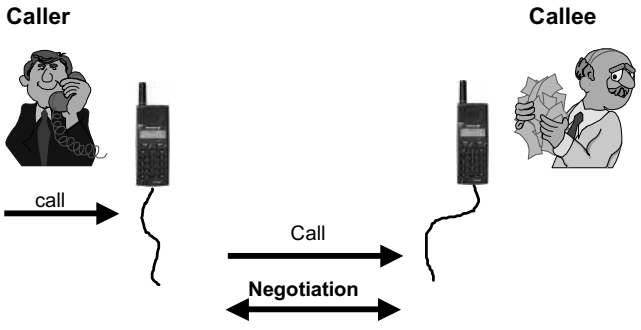

Fig. 1. Communication supported by a Reachability Management System

- How the communication partners are known to 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 Section 4).

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. 3.2).
- *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 role:* The caller can indicate that he is calling in a certain role (or with a specific qualification), for example in fulfilling a certain task. This role is contained in the 'identity cards' of the identity management subsystem. When a particular identity card is selected for personal identification the role 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 to administer 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 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 for his return call.
- *Offering a surety:* In order to emphasize the seriousness of his communication request and his statement regarding the urgency, the caller may offer a (possibly negotiated) amount of money as a surety. "Satisfaction guaranteed or this money is yours!" is the philosophy of this feature. If the callee does not agree with the caller's evaluation of the urgency, he can keep the money or, e.g. donate it to a charity. The callee may use this option, for example, if the caller did not want to disclose his identity. This option is implemented as a further inquiry (cf. Section 3.2).

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).

3.2 Performing a Call – Caller's View of Reachability Management

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

Before the callee is personally involved, the communication request is evaluated and negotiated by his reachability manager. Depending on the rules established in the configuration of the callee's reachability (cf. 3.3) 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.

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 top 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 top right): 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).

Fig. 2. Call set-up dialogue

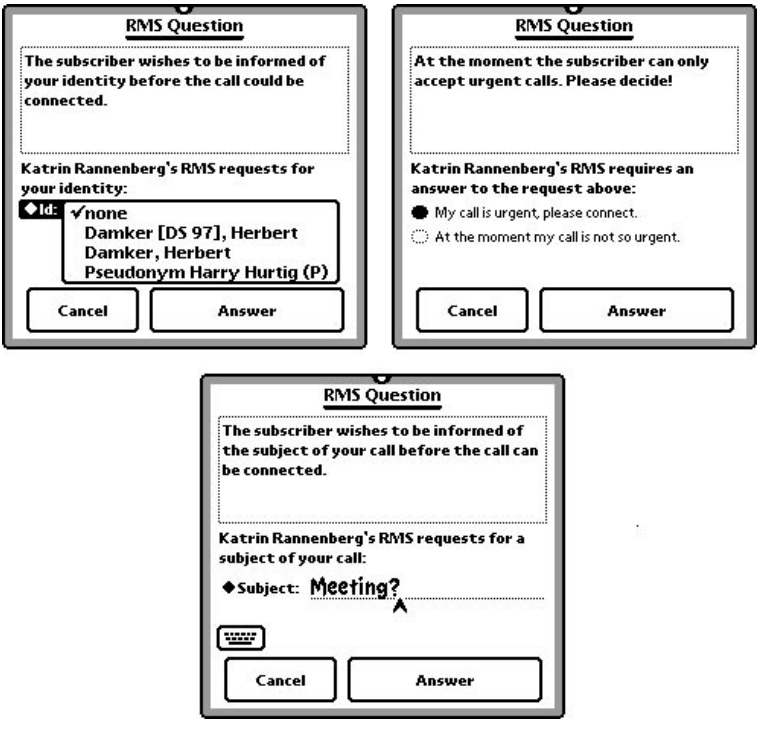

Fig. 3. Inquiry dialogues on caller's reachability manager – initiated by callee's reachability manager

- Inquiry regarding the subject (cf. Figure 3 bottom): 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 a call rejection dialogue. This informs him about the reason for the rejection and offers him 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.

3.3 Configuring Reachability – Callee's View of Reachability Management

In the personal configuration of his reachability manager the user determines the various reactions to incoming calls (communication requests). He defines, 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.

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 to be too complex in the simulation study (cf. Section 5 and Section 6).

4 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* [GaGrPS97,Pordes98]. Users can independently decide whether to use security measures or not and negotiate this

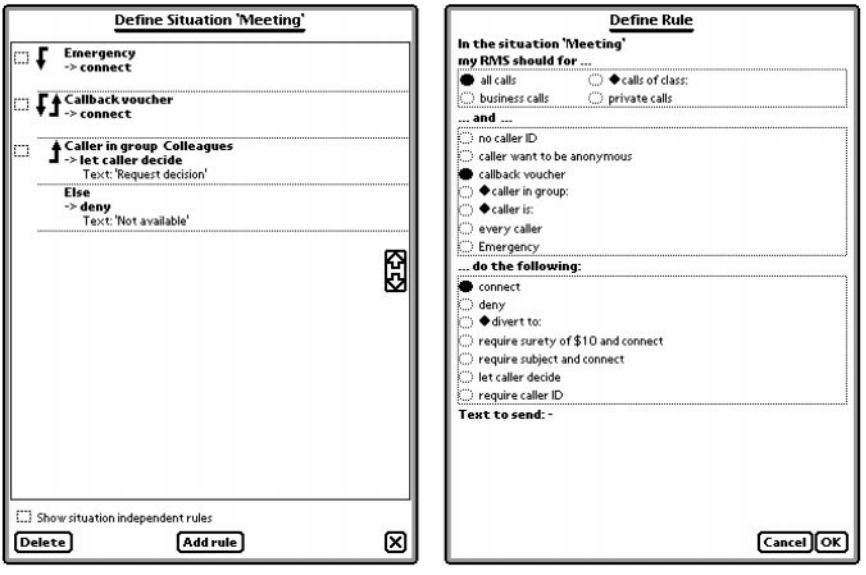

Fig. 4. Configuration of a situation and definition of a rule

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.

4.1 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 *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 contains the measures encryption and unobservability. Commitment contains

[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 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.

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').

4.2 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. The caller makes a security proposal in the call template. This proposal contains the security measures he requests and those he is prepared to take. This is transmitted to the callee's reachability management system.
2. The callee's security manager compares the proposal with his security requirements and preferences. He then produces a coordinated and modified counterproposal.
3. The caller's security manager compares the proposal and counterproposal and puts the call through if both match. Otherwise the caller is asked whether he accepts the callee's proposal.

4.3 Security Scope

To avoid repeated inquiries or frequent failures of negotiation, both parties specify additional conditions, e.g. whether to take specific security measures if requested, or if a personal security requirement can be ignored, if necessary. This is done by means of 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 scope of the security is not communicated directly. Instead, the caller (or his/her 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.

5 Testing and Trialling

The reachability and security manger was tested and trialled 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 complete according to 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 [DuENRS99].
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 paper 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 5.1) and gives an overview of the environment (5.2), the participants (5.3), the cases and set-up (5.4), and the course of the study and the methods of observation and analysis (5.5). A more detailed description of the simulation study can be found in [AmBlBR99,PoRoSc99,RoHaHe99].

5.1 Simulations 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.

5.2 The Simulation Environment

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

- The healthcare informatics had some sense for 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 when they were visiting patients at home.
- 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 drugs or special examinations to the hospital pharmacy or the radiology department. Testing of this software was part of the study.

5.3 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.

5.4 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.

5.5 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 drug, shows how near to reality the cases were: The message created so much discussion and involvement among the participants that some administrative officers 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 administered 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.

6 Reachability as an Example for Controlled Complexity and Advanced Access Control

The general positive outcome was that users accepted the extra complexity, as they saw a high personal benefit for their daily communication tasks (6.1). This could prove useful for other forms of access control (6.2). An increasing awareness of security issues could be noted (6.4), but also some limits of the concept of negotiation showed up clearly (6.3).

6.1 Making Users Migrate into Managing More Complex Controls

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 full 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. 5.2).
- 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.

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

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 aspects also encouraged users to experiment with the more sophisticated functionality:

- 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 move into this direction when offering 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.

6.2 Reachability Management as a Form of Access Control

Reachability management can be seen as a special form of access control, defining the rules for external access to internal resources, especially to the telephone bell, whose ringing usually has a strong influence on the next-minute activities of the people around and can be rather disruptive.

Therefore it is useful to look into the developments in other areas of access control. This holds especially for areas, where mandatory access control policies are not very feasible, e.g. as private or small office users don't have a security administrator at hand and also might not wish to be restricted on their own computer. They then act as their own security administrators and often have to learn by trial and error. This was already shown in the area of encryption software, even for programs that aim at easy usability like PGP 5.0. In [WhiTyg99] several cases are described where users did not understand the concepts of the

software they used. Consequently they made crucial mistakes that could have caused exactly the risk the software should have protected against[8].

An example directly from the area of access control is controlling executable web content, which aims at protecting local systems and data against possible malicious behaviour of web content from insecure areas, e.g. from the Internet. Early Java sandbox approaches were very restricted, but easy to use and configure. Recent technology, e.g. the JDK 1.2 security architecture, is much more powerful and allows a much finer granularity of access control, but its "overall complexity might appear overwhelming to the non-expert computer user" [Gong99, p. 150].

The next useful step might be an interface delivering useful standard and start-up settings but also some freedom to explore the full functionality. This especially holds as more and more access control policies are not only a question of 'granted' or 'not granted' but

- Include some negotiation with the claimer and other parties, e.g. when authorisation or payment information has to be checked before access is granted;
- Embrace accompanying measures such as extended audit in cases when access is granted[9].

Also including the dimension of time that has been tested extensively in reachability management becomes more important: e.g. accesses can be more easily allowed during office hours (as support is easier at hand) or after office hours (as the potential damage on business processes is lower).

Controlling executable web content has another set of similarities with reachability management, resulting from a certain fuzziness of the problem, at least in practice:

- In many cases it is not decidable, what would be the 'right' decision: Granting access to an applet, whose security properties are unclear, might cause damage or not; denying access can be the only way to be safe, but can also reduce the productivity of the workflow. Many users don't understand the security options of applet access control anyway, but have to allow some things to get their work done. So they are always risking that something goes wrong. Granting or denying access to caller can always be the wrong decision, as one never knows what the person on the other side is up to.
- In many cases the damage is limited: Having to reboot the computer or to reinstall some software after an aggressive applet caused problems is a

[8] For example PGP users did not understand the concept of public key infrastructures and the fact, that confidential messages had to be encrypted with the public key of the communication partner, so they failed to use this key thus sending the message unprotected.

[9] One example is the 'grey list' of identifiers of 'dubious' mobile terminals as specified in the GSM standards: subscribers registering with a terminal that is found in the grey list usually get access, but are tracked intensively, as terminals registered in the grey list are usually stolen mobile phones.

nuisance, but not catastrophic, and one can very often recover. Getting an unwanted call because the reachability management did not work as intended, can happen, but there is almost always 'a new game' to start over with.

There are also properties of reachability management that make it different from 'classical' access control:

- A 'one time wrong' might not be tolerable due to the consequences, e.g. for highly confidential data.
- Allowing users to control every successful access (i.e. the option to manually deny calls) was very popular with callees. It is probably not so popular with many administrators of large databases who have other things to do than to confirm every access. However users browsing around the WWW are quite accustomed now to windows that pop up rather unexpectedly and ask for details or extra authorisation.

Altogether the degree of the differences depends largely on the application environment, and so it can be useful in access control areas to look for a migration path along the experiences made with reachability management.

6.3 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. On the other side one can negotiate a lot of information out of the other party when one is in high demand.

The project group had envisaged this problem beforehand, but no general solution was seen[10]. Therefore the group was rather interested how things would turn out in 'real life' and how important the 'principal problem' would be in practice. It turned out that callees were most keen on the 'subject' information accompanying a call, and that callers had other things to do than to investigate the reachability settings of their counterparts.

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.

6.4 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 it. 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.

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 [WhiTyg99] on users misunderstanding terms and concepts of encryption and public key infrastructures (cf. 6.2) 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.

7 Conclusions

Usability of security mechanisms 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 in different stage of interest, understanding, and competence. The simulation study gave good evidence that the features and implementation of reachability management complied with users' requirements. Users learned to understand the consequences of their access control decisions and tuned their policies so these matured to a satisfying level. Therefore the experiences should be useful in other access control areas, especially when circumstances require that more complex

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

mechanisms are introduced. Negotiation showed to be a helpful feature, though one should not think that offering parties the flexibility to negotiate the issues could solve every problem.

Acknowledgments. Thanks go to my colleagues in the Kolleg 'Sicherheit in der Kommunikationstechnik' for their work there. I would also like to thank Dieter Gollmann for e.g. broadening my horizon regarding access control and Michael Roe, Fabien Petitcolas, and Roger Needham for helping to re-reflect and advance the Kolleg's ideas.

References

[AmBlBR99] Elske Ammenwerth, Hans-Bernd Bludau, Anke Buchauer, Alexander Roßnagel: Simulation Studies for the Evaluation of Security Technology; pp. 547 - 560 in [MülRan99]

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

[DuENRS99] Cornelius Dufft, Jürgen Espey, Hartmut Neuf, Georg Rudinger, Kurt Stapf: Usability and Security; pp. 531 - 545 in [MülRan99]

[GaGrPS97] Gunther Gattung, Rüdiger Grimm, Ulrich Pordesch, Michael J. Schneider: Persönliche Sicherheitsmanager in der virtuellen Welt. S. 181-205 in Mehrseitige Sicherheit in der Kommunikationstechnik. Günter Müller, Andreas Pfitzmann (eds), Vol. I, Bonn et al. 1997

[Gong99] Li Gong: Inside Java 2 Platform Security: Architecture, API Design and Implementation; Addison-Wesley; Reading et al 1999

[MülRan99] Günter Müller, Kai Rannenberg: Multilateral Security in Communications; Addison-Wesley-Longman; München et al. 1999; ISBN-3-8273-1360-0

[Pordes98] Ulrich Pordesch: Negotiating security among end users: concept and test in a simulation study, Computer Networks and ISDN-Systems 30/1998, 1597 - 1605.

[PoRoSc99] Ulrich Pordesch, Alexander Roßnagel, Michael J. Schneider: Simulationsstudie "Mobile und sichere Kommunikation im Gesundheitswesen", DuD 1999, p. 76

[RaPfMü99] Kai Rannenberg, Andreas Pfitzmann, Günter Müller: IT Security and Multilateral Security; pp. 21-29 in [MülRan99]

[ReDaFR97] 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

[RoHaHe99] Alexander Roßnagel, Reinhold Haux, Wolfgang Herzog (eds), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig, Vieweg, 1999

[WhiTyg99] Alma Whitten, Doug Tygar: Why Johnny Can't Encrypt: A Usability Evaluation of PGP5.0; Proceedings of the 8th USENIX Security Symposium, August 1999