Multilateral Security: Enabling Technologies and Their Evaluation*

Andreas Pfitzmann

TU Dresden, Department of Computer Science, 01062 Dresden, Germany
pfitza@inf.tu-dresden.de

Abstract. First, multilateral security and its potential are introduced. Then protection goals as well as their synergies and interferences are described. After pointing out some basic facts about security technology in general, a structured overview of technologies for multilateral security is given. An evaluation of the maturity and effectiveness of these technologies shows that some should be applied immediately, while others need quite a bit of further research and development. Finally, a vision for the future is given.

1 Introduction and Overview

Multilateral Security means providing security for all parties concerned, requiring each party to only minimally trust in the honesty of others:

- Each party has its particular *protection goals*.
- Each party can *formulate* its protection goals.
- Security conflicts are recognized and compromises *negotiated*.
- Each party can *enforce* its protection goals within the agreed compromise.

In the same way as enlightenment freed human beings from the suppression imposed by superstitious mental models and authoritarian political systems, technology for multilateral security has the potential to free users of IT systems from a lack of self-determination concerning their (in)security.

To set the tone, I begin with a rather comprehensive ensemble of protection goals, their synergies and interferences.

Thereafter, I state some basic facts about the constraints on security technology in general, and on multilateral security in particular. This helps to identify which technologies are particularly helpful, or even essential, for the construction, use, and maintenance of secure IT systems.

Some of these technologies can unilaterally be employed by various parties. To use others, bilateral cooperation is needed, e.g. the cooperation of both communication partners. For some, trilateral cooperation is required. An example are legally binding digital signatures which need not only cooperation of the at least two communicants, but additionally at least one somewhat trusted third party for the certification of public keys. For other technologies, even the

* Part of this work has been published in G. Müller, K. Rannenberg (Eds.): Multilateral Security in Communications, Addison-Wesley 1999; R. Wilhelm (Ed.): Informatics. 10 Years Back. 10 Years Ahead; LNCS 2000, pp. 50-62, 2001.

G. Müller (Ed.): ETRICS 2006, LNCS 3995, pp. 1–13, 2006.

Table 1. An ordered ensemble of protection goals

Protection of / Threats	Content	Circumstances
unauthorized access to information	Confidentiality Hiding	Anonymity Unobservability
unauthorized modification of information	Integrity	Accountability
unauthorized impairment of functionality	Availability	Reachability Legal Enforceability

multilateral cooperation of a large number of independent parties is necessary. I use this distinction to structure a short overview of what is known about technology for (multilateral) security, providing pointers to the relevant literature.

In conclusion, I give an evaluation of the maturity and effectiveness of the different described technologies for (multilateral) security. This emphasizes which technologies should be introduced immediately in order to enhance existing IT systems or as a basis for new ones. Furthermore I give my opinion which technologies need quite a lot of further research and/or development.

Finally, I give my vision for the future of the field.

2 Protection Goals, Their Synergies and Interferences

Twenty-five years ago, security was nearly equated with *confidentiality*, e.g. in the Orange Book [13]. Twenty years ago, *integrity* of information and *availability* of functionality have been added, e.g. by Voydock and Kent [24] and in the European Security Evaluation Criteria [16]. Fifteen years ago, *accountability* has been added as a fourth protection goal, e.g. in the Canadian Criteria [12].

Outside the mainstream of government dominated security research, *anonymity* and *unobservability* became a big issue fifteen years ago [7, 20], when the technical advance of storage technology made it possible to store all person-related information forever nearly for free. In the last decade, attempts of governments to control the use of cryptography and the pressure of the music and film industries to develop digital copy protection technology, gave a big boost to steganography, i.e. the art of *hiding* information within other, unsuspicious data. Mobile networks, which technically allow people to be reached irrespective of where they are and what they do, gave rise to the protection goal *reachability*, i.e. to control who is able to reach whom under what circumstances by which media. Electronic-commerce caused attention to be given to *legal enforceability*, i.e. users have to fulfill their legal responsibilities within a reasonable period of time.

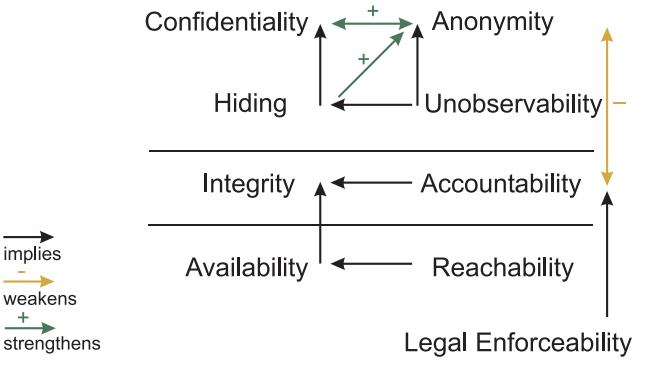

Fig. 1. Synergies and interferences between protection goals

To impose some order on this ensemble of protection goals in the context of communication over networks, it proves fruitful to discern between the content and the circumstances of communication [25], cf. Table 1.

Of course, there are quite a few synergies and interferences between these protection goals, which are explained in detail in [25] and depicted in Fig. 1.

In addition, it has to be expected that additional protection goals will be defined and will become important in the future.

3 Basic Facts

If the parties concerned, e.g. users, service providers and network operators, are unwilling or, perhaps even unable, to express the security properties they expect, it is unlikely that they will get what they require.

→ Users, service providers and network operators must be willing and able to formulate all the security properties they expect.

The security properties expected by different parties tend to be quite diverse in respect of applications and even transactions with different partners using the same application. Moreover, the security properties expected may change dramatically over time, e.g. as a result of negative personal experiences, or reports by the media.

→ Security properties have to be dynamically adaptable.

The security of a human user can only be as good as the security of the device he or she is directly interacting with.[1] (Whether the device is secure for other parties concerned, is only of secondary interest.)

[1] This is certainly true within the IT system. Outside the IT system, there may be compensation for security breaches. But this can work at best for those security properties where compensation is possible at all. Compensation is not possible for confidentiality properties – information which got public cannot be de-publicized –, but compensation is possible with regard to integrity and availability properties, e.g. accountability and legal enforceability, cf. [4].

→ Devices which are secure for their user(s) are needed.

If a user device is built to integrate more than one application, its security has to be adequate for its most demanding application. If a general purpose user device is built, its security has to be adequate for the most demanding application perceivable during its lifetime. If this is not achieved, the user device is clearly not general purpose – which applies to all Windows 98/ME/XP Home based PCs.

→ The security target of user devices is set by the most demanding application the device is intended to be used for.

If the designers are cautious, the security target will even be set by the most demanding application the device will ever be used for – and this application may not yet be known at the time the device is being designed.

→ User devices have to provide a very, very secure basis to bootstrap further security properties during their lifetime.

The erasure of data ever available in a globally networked IT system is by no reasonable means really to assure. In addition, the technical progress makes transfer, storage and usage of huge amounts of data very cheap. Therefore, wherever possible, the parties concerned have to be able to hinder even the ability to gather their data.

→ Data avoidance techniques for anonymity, unobservability, and unlinkability are needed. If accountability is required, a suitable form of pseudonymity should be used.[2]

4 Overview of Technologies for Security

Security technologies are mentioned and briefly explained in this section. It is structured according whether security technologies are uni-, bi-, tri-, or even multilateral.

4.1 Unilateral Technologies

Unilateral technologies can be decided on by each party for itself. Therefore, neither coordination nor negotiation is needed concerning their usage. Important unilateral technologies for multilateral security are:

Tools to help even inexperienced users to formulate all their protection goals, if necessary for each and every application or even each and every single action, cf. [22, 25]. Fig. 2 gives some examples.

(Portable) devices which are secure for their users in order to bootstrap security. The devices need at least minimal *physical protection* comprising direct input/output with their users [21] and, if they are multi-purpose, an *operating*

[2] A structured explanation, definitions of and interrelationships between anonymity, unobservability, unlinkability, accountability, and pseudonymity can be found in [25, 18].

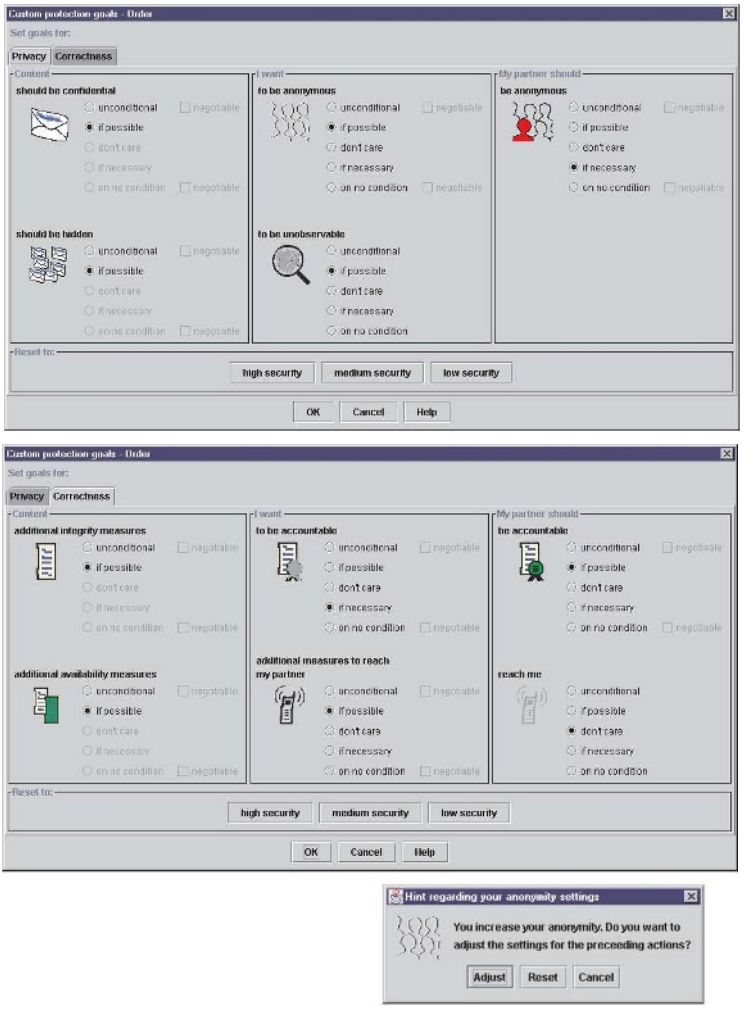

Fig. 2. User interface screen shots

system providing fine-grained access control and administration of rights for applications, adhering to the principle of least privilege, cf. Fig. 3. This is essential to limit the spread of Trojan horses, and can prevent computer viruses completely. For convenience, these devices might recognize their authorized user by biometrics.[3]

Encryption of local storage media to conceal and/or authenticate its contents.[4]

[3] Please note that this is the only place where biometrics is useful for multilateral security. And last but not least, this is the only place where biometrics does not pose unsolvable privacy and safety problems, cf. [19]

[4] Attempts to control the usage of encryption to conceal the contents of storage would be quite useless, since criminals might then employ steganography to do so.

Fig. 3. Portable devices secure for their users

Hiding of secret data in local multimedia contents or in the local file system [2] using steganographic techniques, not only to conceal the contents of the secret data, but also its very existence.[5]

Watermarking or *fingerprinting* digital data using steganographic techniques to help prove authorship or copyright infringements.

Using only *software* whose *source code is published and well checked* or the *security of which is certified* by a trustworthy third party[6] having access to the complete source code and all tools used for code generation. The best technique is to combine both approaches with regard to as much of the software as possible. It is only by using at least one of these two approaches that you can be reasonably certain that the software you use does not contain Trojan horses. More or less the same applies to hardware where all sources and tools used for design and production are needed as well to check for the absence of Trojan horses.[7]

4.2 Bilateral Technologies

Bilateral technologies can only be used if the communication partners cooperate. This means that some coordination and negotiation is needed concerning their usage.[8]

[5] Attempts to control the usage of steganography to hide the very existence of secret data in storage would be quite useless.

[6] In this case, other parties are involved than in the here presented uni-, bi-, and trilateral technologies where only the parties actively involved at the runtime of the IT system are taken into account. Of course these terms on laterality can be expanded to handle non-runtime situations as well, e.g. the preparation of communication or other circumstances like the software developing or testing process.

[7] Attempts to control thorough checking would be quite useless, since authorities need secure IT systems themselves.

[8] Note: the term "bilateral" does not necessarily mean that exactly two parties are involved, but there may be many communication partners, e.g. in a video conference,

Important bilateral technologies for multilateral security are:

Tools to negotiate bilateral protection goals and security mechanisms, cf. [22] and Fig. 4.

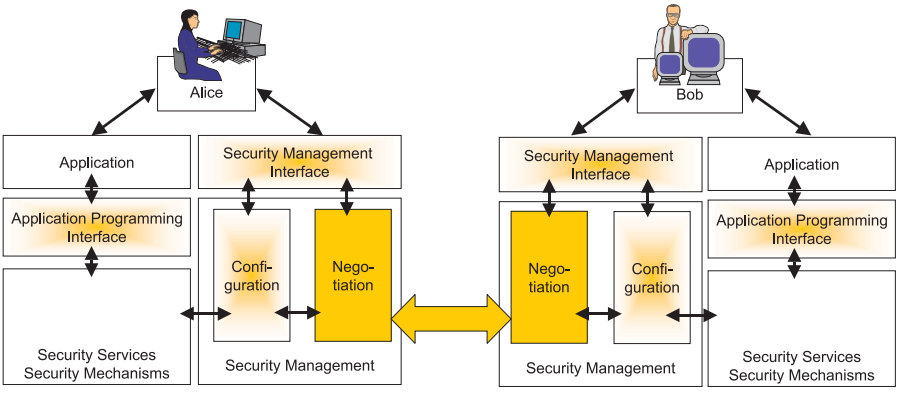

Fig. 4. Tools to negotiate

Cryptographic mechanisms[9] and *steganographic mechanisms*[10] to secure the communication content, cf. Figs. 5 and 6.

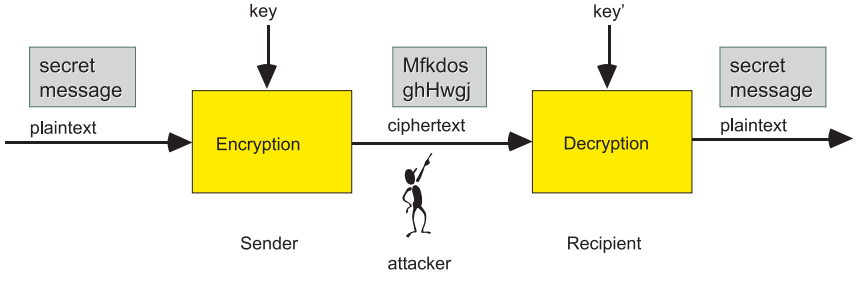

Fig. 5. Cryptography to achieve confidentiality and integrity of the communication contents

who may have differing interests. Nevertheless this is counted here as two sides (i.e. bilateral technologies): the user's side and the other side with at least one and perhaps more communication partners.

[9] Attempts to control the usage of encryption to conceal the contents of communication would be completely useless, since criminals might then employ steganography to do so.

[10] Attempts to control the usage of steganography to hide the very existence of secret data in communications would be completely useless.

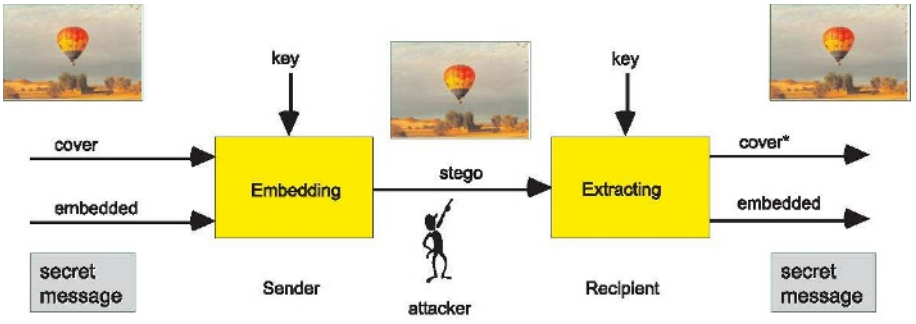

Fig. 6. Steganography to achieve hiding, i.e. secrecy of the confidentiality of the communication contents

4.3 Trilateral Technologies

Trilateral technologies can only be used if a third party is involved to fulfill a specific task for the other participating parties. This means that more coordination and negotiation is needed concerning their usage compared to unilateral - and in most cases as well bilateral - technologies. Important trilateral technologies for multilateral security are:

Tools to negotiate trilateral security mechanisms, e.g. for accountability.[11]

A *public-key infrastructure* (PKI) to provide users with certified public keys of other users to test their digital signatures and to give users the ability to revoke their own public key if the corresponding private key has been compromised.

Security gateways to bridge incompatibilities with regard to security mechanisms or their details, cf. Fig. 7. Security gateways work well concerning integrity and accountability mechanisms, but are of questionable value concerning confidentiality and anonymity mechanisms. Of course, security gateways cannot bridge incompatibilities concerning protection goals.

4.4 Multilateral Technologies

Multilateral technologies can only be used if a large number of independent parties cooperate. This means that coordination and negotiation are needed on a large scale. Important multilateral technologies for multilateral security are:

Tools to negotiate multilateral protection goals and security mechanisms, e.g. for anonymity, unobservability, unlinkability, and pseudonymity.[12]

[11] The negotiation process itself between the communication partners belongs to bilateral technologies, but as far as the negotiation is extended to include third parties in order to achieve accountability, it is a trilateral technology.

[12] The negotiation process itself between the communication partners belongs to bilateral technologies, but as far as the negotiation is extended to the necessary parties in order to achieve multilateral security goals, it is a multilateral technology.

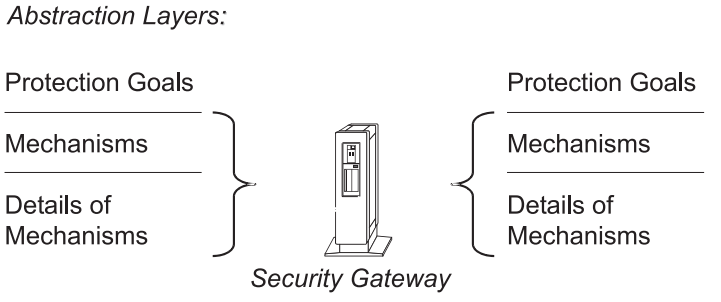

Fig. 7. Security gateways

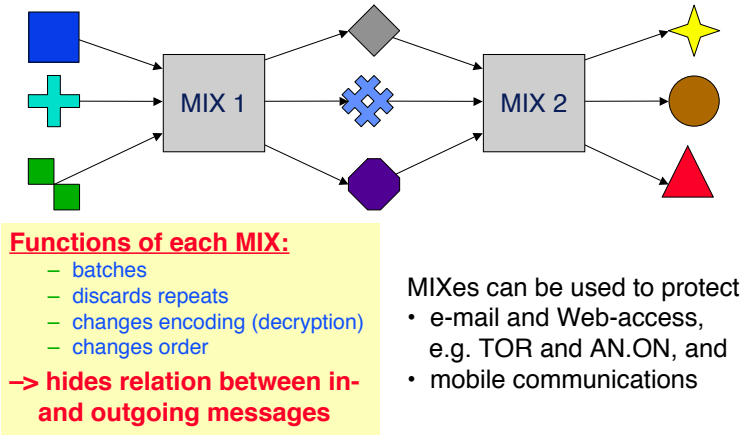

Fig. 8. Anonymity, unobservability, and unlinkability for communication

Mechanisms to provide for *anonymity*, *unobservability*, and *unlinkability* with regard to

- communications,[13] i.e. protect who communicates when to whom from where to where [6, 7, 20, 11, 14, 17, 23, 15], cf. Fig. 8,
- payments, i.e. protect who pays what amount to whom and when [8, 1], and
- value exchange, i.e. protect electronic shopping from observation [5, 3], cf. Fig. 9,

without compromising integrity, availability, or accountability.

Mechanisms to provide for *digital pseudonyms*[14], i.e. a suitable combination of anonymity and accountability [6]. In particular, there are mechanisms to securely

[13] Data retention is quite useless, since criminals might employ e.g. public phones, prepaid mobiles bought by others, unprotected WLANs, or unprotected-bluetooth mobiles of others to avoid leaving traces.

[14] If we only consider the accountability aspect, digital pseudonyms are a trilateral technology. But taking into account anonymity as well, digital pseudonyms are clearly a multilateral technology.

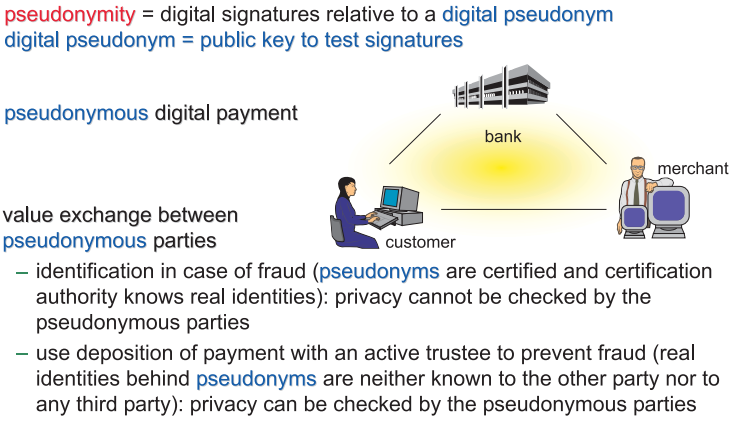

Fig. 9. Pseudonymous digital payment and value exchange between pseudonymous parties

transfer signatures (expressing authorizations, called credentials) between different pseudonyms of the same party [7, 9, 10]. This is called *transferring signatures between pseudonyms*.

5 Evaluation of Maturity and Effectiveness

Table 2 gives my evaluation of the maturity and effectiveness of the technologies for security mentioned in the last sections. Their sequence in the table is mainly bottom-up, i.e. a technology for security placed in a particular row is required before a technology listed below can be effective. In some places, examples are given following a semicolon.

As can be seen, the weakest link of the security chain today is the user device, in particular its physical protection and operating system. Much has to be done to improve both.

Obviously, security evaluation of software as well as IT and integration of security technologies are those challenges for research that have the most impact on IT security.

6 A Vision

Without multilateral security, e-commerce will be severely hindered and there will be definitely no e-democracy. Therefore, I expect that portable devices secure for their users will finally be developed and find their way into the mass market. The diverse projects to introduce secure and legally binding digital signatures are important first steps. Building on devices secure for their users, cryptography will prove as a very powerful enabling technology for all kinds of security services.

Of course, we will experience broad discussions (and at least some attempts of various secret services to achieve facts without any public discussion at all)

Table 2. Maturity and effectiveness of security technologies

	state of public research	**demonstrators and prototypes**	**available products**	**products fielded on a large scale**
physical protection	hardly any respectable publications	hard to assess	hard to assess; Me-chip	very poor; chipcards
security evaluation of software and IT	acceptable	hard to assess	hard to assess	hard to assess
security in operating systems	very good	good	poor; Windows NT, 2000, XP Professional, Linux, MacOS X	very poor; Windows ME, CE, Mobile, XP Home, MacOS 9, Symbian, PalmOS
cryptography	very good	good	good; PGP 2.6.x	acceptable; PGP 5.x, PGP 6.x
steganography	good	acceptable	very poor	very poor
public-key infrastructure	very good	good	hard to assess	hard to assess
security gateways	good	acceptable	-	-
mechanisms for anonymity, unobservability, and unlinkability	very good	good	acceptable; TOR, AN.ON	poor; proxies
digital pseudonyms	very good	good	good; PGP 2.6.x	acceptable; PGP 5.x, PGP 6.x
transferring signatures between pseudonyms	good	acceptable	-	-
tools to help even inexperienced users to formulate and negotiate	good	acceptable	-	-
integration of these technologies	acceptable	poor	poor	very poor

what the balance between electronic surveillance and digital privacy should be. In my opinion, we have to overcome 2001 to avoid 1984.

It is well known and agreed for at least three decades that nearly complete surveillance is possible by IT systems. I am happy that public research has shown in the last two decades that strong digital privacy is possible as well. So society is free to decide how we shall live in cyberspace – and beyond.

I am sure that multilateral security and privacy enhancing technologies are prerequisites for the long term acceptance of IT systems in general and for ubiquitous computing in particular in a democratic society as we know it.

Acknowledgements

Many thanx to my colleagues in general and Marit Hansen in particular for suggestions to improve this paper. In addition, Stefan Köpsell gave lots of technical support.

References

1. N. Asokan, Phillipe A. Janson, Michael Steiner, Michael Waidner: The State of the Art in Electronic Payment Systems; Computer 30/9 (1997) 28–35.
2. Ross Anderson, Roger Needham, Adi Shamir: The Steganographic File System; Information Hiding, 2nd Workshop, Portland, Oregon, LNCS 1525, Springer, Heidelberg 1998, 73–82.
3. N. Asokan, Matthias Schunter, Michael Waidner: Optimistic Protocols for Fair Exchange; 4th ACM Conference on Computer and Communications Security, Zürich, April 1997, 6-17.
4. Birgit Baum-Waidner: Ein Service zur Haftungsverteilung für kompromittierte digitale Signaturen; Verläßliche IT-Systeme, GI-Fachtagung VIS '99, DuD Fachbeiträge, Vieweg, Braunschweig 1999, 203–223.
5. Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715–721.
6. David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84–88.
7. David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030–1044.
8. David Chaum: Privacy Protected Payments - Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conference; Laxenburg (Austria), 1987, North-Holland, Amsterdam 1989, 69–93.
9. David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, LNCS 453, Springer, Berlin 1990, 246–264.
10. David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96–101.
11. David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26–38.

12. Canadian System Security Centre; Communications Security Establishment; Government of Canada: The Canadian Trusted Computer Product Evaluation Criteria; April 1992, Version 3.0e.
13. Department of Defense Standard: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711.
14. Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy; Information Hiding, 1st Workshop, Cambridge, UK, LNCS 1174, Springer, Heidelberg 1996, 121–135.
15. David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections; Communications of the ACM 42/2 (1999) 39–41.
16. European Communities - Commission: ITSEC: Information Technology Security Evaluation Criteria; (Provisional Harmonised Criteria, Version 1.2, 28 June 1991) Office for Official Publications of the European Communities, Luxembourg 1991 (ISBN 92-826-3004-8).
17. Anja Jerichow, Jan Müller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol; IEEE Journal on Selected Areas in Communications 16/4 (May 1998) 495–509.
18. Andreas Pfitzmann, Marit Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology; `http://dud.inf.tu-dresden.de/Anon_Terminology.shtml`.
19. Andreas Pfitzmann: Biometrie – wie einsetzen und wie nicht? Zum Umgang mit Sicherheitsproblemen von Biometrie und Sicherheits- und Datenschutzproblemen durch Biometrie; digma, Zeitschrift für Datenrecht und Informationssicherheit, Schulthess 5/4 (Dec. 2005) 154–157.
20. Andreas Pfitzmann, Michael Waidner: Networks without user observability; Computers & Security 6/2 (1987) 158–166.
21. Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trustworthy User Devices; in: G. Müller, K. Rannenberg (Eds.): Multilateral Security in Communications, Addison-Wesley 1999, 137–156.
22. Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Guntram Wicke, Gritta Wolf, Jan Zöllner: A Java-based distributed platform for multilateral security; IFIP/GI Working Conference "Trends in Electronic Commerce", Hamburg, LNCS 1402, Springer, Heidelberg 1998, 52–64.
23. Michael K. Reiter, Aviel D. Rubin: Anonymous Web Transactions with Crowds; Communications of the ACM 42/2 (1999) 32–38.
24. Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM Computing Surveys 15/2 (1983) 135–171.
25. Gritta Wolf, Andreas Pfitzmann: Properties of protection goals and their integration into a user interface; Computer Networks 32 (2000) 685–699.