Privacy Enhancing Techniques: A Survey and Classification

Peter Langendörfer, Michael Maaser, Krzysztof Piotrowski, Steffen Peter
IHP, Im Technologiepark 25, D-15236 Frankfurt (Oder), Germany
{langendoerfer|maaser|piotrowski|peter}@ihp-microelectronics.com

Abstract: This chapter provides a survey of privacy enhancing techniques and discusses their effect using a scenario in which a charged location based service is used. We introduce four protection levels and discuss an assessment of privacy enhancing techniques according to these protection levels.

Keywords: privacy enhancing techniques, mix networks, pseudonyms, anonymous e-cash, GeoPriv, P3P, APPEL

I. Introduction

Privacy is a very complex topic that touches legal, social and technical issues. In this chapter we are focussing on the technical aspect of how to preserve privacy in the Internet. Throughout this chapter we define privacy as users' capability to determine who may know, store and compute their data.

Privacy is one of the major concerns of Internet users [Cranor00]. The combination of wireless technology and Internet provides a means to combine real world and cyber world behaviour. Thus, extending Internet use to mobile devices is going to aggravate privacy concerns. But, privacy concerns influence also the revenue of companies which are offering their service via the Internet [FTC99]. So there is an interest in proper preserving of privacy on both sides. Especially big enterprises may suffer a lot from loss of trust in case they cannot protect the privacy relevant data or do not adhere to their own privacy policies [Barbaro06, Anton04].

Privacy enhancing technologies (PET) are a hot research topic in the last years leading to a plethora of approaches that intend to protect privacy. This chapter provides an overview of privacy enhancing technologies, and discusses their effect on information disclosed while using a location based service from a mobile device. In addition, an assessment of the protection level that can be achieved by applying the introduced means is provided. Thus, this chapter helps scientists to understand what is going on in the privacy research area so they probably can identify new research topics more easily. In addition, it enables practitioners to find approaches that allow them to build a privacy preserving system.

The rest of this chapter is structured as follows. We first discuss privacy protection goals and provide an example that outlines which information can be gathered while using a charged service. In section III we explain privacy enhancing technologies. A discussion of the protection level achieved by individual means is given in section IV. The chapter concludes with an investigation of the currently reached deployment of privacy enhancing techniques and a discussion of new research challenges.

II. Privacy Protection Goals

While browsing the Web or doing e- or m-commerce every user exposes information about her interests, personal data etc. to one or several of the following service providers: network service provider, e.g. telco company, internet service provider, e.g. online book store, context service provider, e.g. location handling system, and payment service provider, e.g. her bank. Perfect privacy can be achieved if and only if the user reveals no information at all. Since this excludes the user from all benefits online services provide it is not a reasonable choice. The most valuable alternative is to disclose as few information as possible and only to the service provider who essentially needs this information.

In order to achieve a reasonable good separation of information personal data and communication habits have to be protected at network as well as at application level. The former is an essential prerequisite of the latter, i.e. protection at the application level does not make any sense as long as no protection at the network level is used. Protection at application level is much more difficult to achieve than protection at the network level. Here some information has to be revealed in order to get a useful service, i.e. data has to be given away and therefore it has be protected somehow. At the application level two dimensions have to be considered to prevent detailed profiling: time and location (in the sense of data gathering entity). The time dimension hinders service providers to construct a relationship between different service uses executed by the same individual but at different points in time. The location dimension provides separation of information between several service providers so that each one of them knows only data of a specific type.

In the following subsection we discuss a service scenario in which the current position of the user is requested by the service provider, who is also charging for the service. We use this scenario to show which data is known by which party of the whole system. We will also refer to this scenario later on to illustrate the effect of the privacy enhancing techniques discussed in the following section.

A. Example

In this section we present a charged location based service scenario that shows privacy issues in detail. It shows the information flow between the involved parties and the resulting dependencies that may cause privacy flaws.
The service provides its mobile user with information that is dependent on the location of the user. Additionally, the user pays for the information using a payment protocol. As shown in Figure 1 there are five parties, besides the user, involved in this scenario.

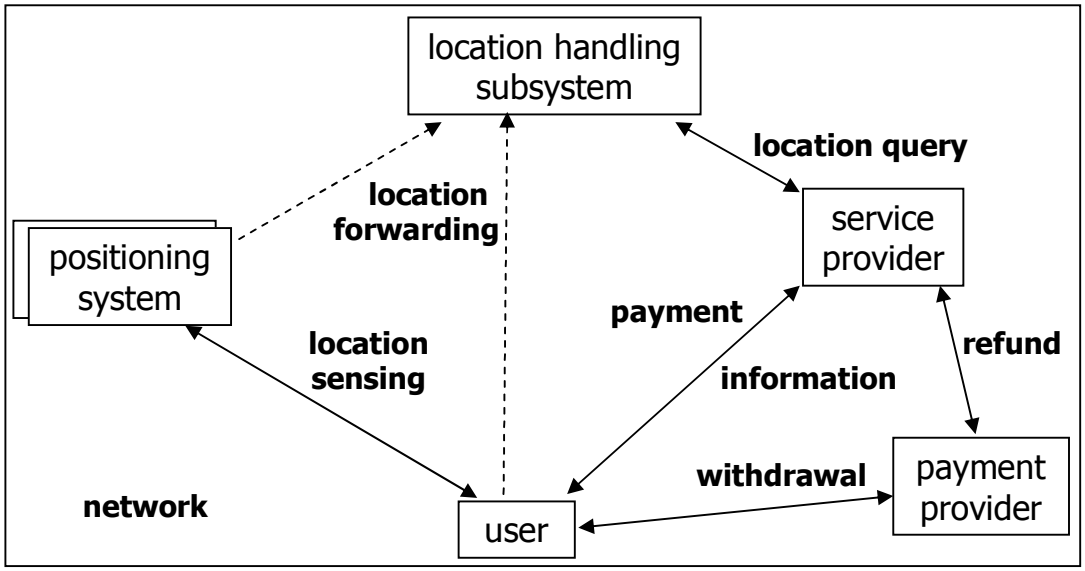

Figure 1: The data exchange in the charged location based service scenario

1. Positioning system is used to sense the current location of the user. Depending on the kind of the system the location information is sent to the location handling subsystem either direct from the positioning system or is forwarded by the user. In the first case the role of the user in location information forwarding is passive in the latter active.
2. The location handling subsystem combines the location information together with the user identity. This subsystem may be a part of the service, or it may be a part of the positioning system with passive user role. Of course, it may also be a standalone infrastructure part that manages the location information for multiple users and provides it to multiple services.
3. The payment provider transfers money in order to allow the user to pay the service for the information.
4. The service provides the user with information based on the current location of the user received from the location handling subsystem.
5. An additional, but virtual party is the network. It may be a local network or the Internet. It may introduce parties that, generally, can be considered as eavesdroppers.

Each party of the scenario has some of the user data. In other words they have a kind of knowledge. Table 1 shows the distribution of knowledge between these parties. Additionally, if not protected by means of cryptography the user data is available to eavesdroppers.

Table 1.: Distribution of the knowledge about the user in the scenario. Information in brackets can also be available to the corresponding parties depending on the setup.

Party	Knowledge about the user
user	- Identity - Purchased information - Location
positioning system	- (Location) - (Identity)
location handling subsystem	- Location - Identity - Kind of purchased information
service	- Identity - Purchased information - Location
payment provider	- Identity - Kind of purchased information
network	- (Kind of purchased information) - (Identity) - (Purchased information) - (Location)

The habits of the user are reflected in her location and purchase history. Even if the content of the purchased information is not known, the fact that the user communicated with or paid a specific service provider causes privacy flaws. Table 1 shows that in this scenario a detailed profiling of the user is possible if she provides always the same identifier to the individual service providers. So, almost every party in the scenario can create a kind of profile. The situation becomes even worse if the service providers are collaborating to get a more detailed profile of the user.

III. Discussion of Privacy Enhancing Techniques

In this section we provide an overview on privacy Enhancing techniques but do not discuss basic technologies such as cipher means. Throughout this section we assume that all messages are encrypted in order to avoid eavesdropping and easy observation of user activities by third parties. We start with the discussion of network level protection means, before we describe application level approaches.

A. Network level privacy protection

An often used approach intended to increase the security is the application of a proxy chain, which provides better security than use of a single proxy. By this means the messages are forwarded from one proxy to another and eventually to the destination. Without additional security mechanisms this approach cannot be recommended since every proxy has access to data and at least the destination address, so that no protection improvement is achieved. An improvement of the proxy chain idea is the crowds approach [Reiter98]. Each user runs a program called Jondo. This program is the local access of the user to the proxy network and also a proxy for other users in the network. If a Jondo proxy receives a packet it randomly decides whether to forward the packet to another Jondo or to send it to its destination. The receiver and also an external eavesdropper cannot decide whether the packet was originally sent by the direct peer or by another computer in the crowd, because the encrypted packets will be re-encrypted on every proxy. However, since every proxy still has access to content and destination address, the crowds approach still has security and privacy flaws.

In 1981 Chaum proposed in [Chaum81] mix networks as solution that solves the open issues. Mix networks are a combination of proxy chains and asymmetric cryptography. Instead of forwarding the plain message, every packet is encrypted using pubic-key cryptography (PKC). PKC allows every sender to encrypt the message with the publicly known public key of the proxy. Only the specific proxy is able to decrypt the message with the corresponding private key. The idea of mix networks is to encrypt the actual message with the public keys of a set of proxy servers (also called stages or mixes). Encryption is performed cascaded in reverse order of the mixes that will receive the packet. Additionally to the message, each encryption layer contains the address of the next mix in the chain or the final receiver. That is, first the sender encrypts the message together with the address of the receiver using the public key of the last mix in the chain, while this cipher text is encrypted together with the address of the last mix using the key of the second last mix, and so on. Every mix only knows the previous and the next computer in the chain. No mix but the first knows the sender, and no mix but the last has information about the receiver. A single proxy is not able to disclose sender or receiver. Only with the private keys of every mix in the network it is possible to reconstruct the path from the sender to the receiver. Such alliance is unlikely if individuals or organizations with different interests administrate the mixes on the route. As long as one mix on the route does not cooperate in order to reconstruct the route the anonymity is preserved. Indeed, it is required that many users use the mix network. In order to strengthen the privacy every mix can delay and reorder messages. Due to the successive decryption on every mix recognition of forwarded packets is prevented.

Though mix networks have been matured, are available and very safe, they also have some problems. First, the effective transfer speed is limited. While for mail applications it is not a problem and for the web mostly acceptable, for example real-time video streams are hardly possible. A survey on mix networks available in [Sampiget06] provides insight into both, the design and weaknesses of existing solutions.

Similar approaches such as Onion Routing [Reed98], Crowds [Reiter98] and Web Mixes [Berthold00] have been reported in the past. The first two are in contrast to the original mix approach vulnerable to traffic analysis attacks, but they are more efficient. The Web Mixes provide the same level of privacy as mix networks, but are optimized for real time traffic such as browsing the web. The comparison of these approaches discussed in [Berthold00] clearly shows that better protection of user privacy comes at the cost of less efficiency.

Several projects have realized implementations of mix networks. The Tor-network [TOR] is a freely available open peer-to-peer solution of a mix network. Every Internet-user may open a mix server that can be part of randomly selected routes through the network. Before transmitting a packet the sender selects a route and encrypts the message with the public keys of the corresponding mixes. Both input and output mix change from connection to connection. In contrast the Java Anon Proxy (JAP) [ANON] uses fixed routes, termed mix cascades. The mixes are administrated by independent well reputed partners. Though JAP is more reliable and more trustworthy than a P2P network, it shows a weakness with respect to privacy for the user. If the last mix detects illegal content, all mixes in the cascade work together and log the incident together with the subjects.

Mix networks are probably the best way to protect privacy on network level. On this level they are a means that provides provable perfect security. However, the gain of privacy can turn useless if privacy is not additionally protected on application layer.

B. Application layer privacy protection

a) Location protection

In [Gruteser03] an approach is presented that reduces the accuracy of location information in order to prevent re-identification of objects using location based services. Two dimensions, i.e. space and time can be modified by the system. So, instead of a single position a region is reported to the location based service, or instead of a single point in time an interval in which the user was at a certain position is reported. The fuzzification of the data is done at a trusted server which also extracts the user identity and network address. The communication between the user and the trusted server is protected by cryptographic means and use of mix networks. The major drawback of this approach is that the trusted server knows almost everything about the user, i.e. her identity, network address, when she was where as well as which services she used.

Another approach, which was not actually designed for privacy on the first hand, releases position information only in case they may be actually needed [Treu05]. For proximity detection of two objects that actively report their location, location updates are not

necessary as long as either of them remains in a certain circular surrounding. Consider two moving objects A and B that report their location to the infrastructure. There is a registration for a proximity event between A and B of equal or less than 1 km. Their current positions are at 101 km distance. Both objects are notified about a logical circular region with 50 km radius around their current position. These circles do not intersect and have a minimum distance of 1 km. That is, while either objects moves only within the given circle there is no chance that the objects are closer than 1 km. Hence neither of them needs to report its actual location to the infrastructure, so the location server only knows a certain region within the user is moving and thus no detailed location tracking is possible. Since the system was not designed originally for privacy protection purposes, no means to withhold the user's identity from the server or protection of the communication between the location server and the user are investigated.

b) Use of pseudonyms

The idea of pseudonyms is to hide the real identity of a user by using a bogus identity. Nicknames used in chat rooms are widely known pseudonyms. Pseudonyms prevent service providers from linking isolated transaction to a certain user. There are several approaches that propose the use of pseudonyms in order to protect user privacy [Jendricke00, Koch01, Berthold00, Jia04]. The fundamental difference between those approaches is that [Jendricke00, Berthold00] manage the different user pseudonyms at the user's own device, whereas [Koch01, Jia04] propose the use of a centralized pseudonym service. The major drawback of systems relying on a centralized pseudonym management is that they still know the user's real identity, which services the user required etc., i.e. they have a detailed user profile. Thus, such solutions provide only limited privacy to their users. The positive aspect of these systems is that information such as network addresses cannot be used by third parties to link pseudonyms, if the system acts as a proxy for its users as described in [Jia04]. In case of systems that still require direct interaction between their users and potential service provides such as [Koch01] this benefit is no longer there. On the other hand centralized systems provide means to identify individual users if necessary, i.e. after incorrect behaviour was detected. This may help to increased acceptance of such systems on the service provider site. Decentralized approaches such as [Jendricke00] allow each user to define pseudonyms herself, so that there is no other entity, which has complete knowledge of real identity, and cyber world behaviour. The open issue that network addresses can be used to link pseudonyms together can be solved by additionally using mix networks.

Pseudonyms are also used to realize anonymous e-cash systems, which are explained in the next paragraph.

c) Anonymous payment systems

In an electronic payment scheme there are at least three parties. Let us describe the minimum setup. The shop or service provider delivers goods or services to the user in return of a monetary equivalent by means of payment provider. Figure 2 shows the flow of the virtual money in this setup. The payment provider issues some kind of electronic money the user uses to pay the service provider for its services. There can be multiple instances of above mentioned parties, but to simplify the description only the presented flow of virtual money is assumed.

Figure 2. The flow of the virtual money in an electronic payment scheme

But besides the flow of the money there is also flow of information about the user. If the payment provider can recognize the electronic money tokens it issued for the user it can create a history of the service providers the user prefers. On the other hand, if the service provider can recognize the user each time the user uses the service then the history of user purchases can be created. By combining the knowledge of these two parties a complete profile of the user can be created. To avoid the possibility of profiling the user, i.e., to improve her privacy, there is a need for mechanisms that remove the link between the payments and the user identity. Thus, payment providers that use credit card like approaches, where the link to the user identity is strong, are to be avoided in privacy protecting systems.

The protection against profiling done on the payment provider side is especially important because usually during the token creation process the payment provider has access to the identity of the user. The remedy is to create the electronic money tokens in such a way that the payment provider cannot recognize them as they are returned by the service provider. The basic mechanisms that can be used for that purpose are blind signatures and anonymity as they were introduced in [Chaum85]. However, complete anonymity causes several problems, e.g., the user can try to use one token twice without any consequences in case of success. To avoid this problem, improvements to the basic scheme were introduced. Revocable anonymity introduced in [Brands93] allows linking the user identity with the token if the user used a single token twice. Generally, there is a

trade-off between the security of the electronic payment scheme and the privacy level it provides to the user. As already stated, completely anonymous schemes usually suffer from security flaws. On the other hand, completely secure ones provide less privacy. Anyway, for security reasons there is a need for the inclusion of the identity users in their tokens. This is usually done in an encrypted form that allows to reveal the user identity only in case of user misbehaviour.
To avoid the user profiling by the service provider, there is a need to remove link between any two transactions or sets of transactions, depending on the desired granularity. To allow this, the electronic payment scheme tokens shall not contain any clue that might lead to linking any two tokens or sets of tokens that belong to the same user. Additionally, if any identification is needed, the user shall use pseudonyms while talking to the service provider. Changing the pseudonym frequent enough helps to remove the links between transactions.

d) Descriptive approaches

There exist a number of technologies which do not actually protect privacy in a technical manner but rather in a descriptive way. That is, the parties involved in a data exchange agree on certain statements about the content and use of the data to be gathered, stored and /or processed. Most prominent representatives for such descriptive approaches are P3P [Cranor07] and GEOPRIV [Peterson05].

(1) P3P/APPEL

The goal of P3P is to increase user trust and confidence in the Web. P3P provides a technical mechanism to inform users about the intended privacy policies of service providers and web sites. The P3P specification defines the following:

- A standard schema for data a Web site may wish to collect, known as the "P3P base data schema".
- A standard set of uses, recipients, data categories, and other privacy disclosures.
- An XML format for expressing a privacy policy.
- A means of associating privacy policies with Web pages or sites, and cookies.

The P3P policy further states consequences in case of privacy breach. P3P complements legislature and self-regulatory programs in helping to enforce web site policies.

APPEL [APPEL] can be used to express what a user expects to find in a privacy policy. P3P and APPEL merely provide a mechanism to describe the intentions of both sides than means to protect user data after agreeing to use the service.

There are several privacy related tools that are based on P3P and APPEL specifications. AT&T's Privacy Bird [PrivacyBird] is a free plug-in for Microsoft® Internet Explorer. It allows users to specify privacy preferences regarding how a website stores and collects data about them. If the user visits a website, the Privacy Bird analyzes the policy provided and indicates whether or not the policies fits to the users preferences. The

Microsoft® Internet Explorer 6 [IE6] and Netscape® 7 [NS7] embed a similar behaviour. They allow the user to set some options regarding cookies and are capable of displaying the privacy policy in human readable format. All these tools are a valuable step into the right direction, but they still lack means to personalize privacy policies. Steps towards personalized privacy policies are discussed by [Maaser05] and [Preibusch05]. In [Preibusch05] a fine-grained choice from a set of offered policies is proposed whereas a form of a bargaining in which neither party fully publishes all its options is proposed in [Maaser05].

Privacy policies allow for "opting-out" of or "opting-in" to certain data or data uses. But they do not provide a technical protection means. The user has no control on the actual abidance of the policy but still has to trust that her personal data is processed in accordance to the stated P3P policy only. Enforcement of the policy abidance could be done by Hippocratic databases or other means.

(2) IETFs GeoPriv

GEOPRIV is a framework [Cuellar04] that defines four primary network entities: a Location Generator, a Location Server, a Location Recipient, and a Rule Holder. For appropriate interaction between those three interfaces are defined, including a publication interface and a notification interface.

GEOPRIV specifies that a 'using protocol' is employed to transport location objects from one place to another. Location Recipients may request a Location Server to retrieve GEOPRIV location information concerning a particular Target. The Location Generator publishes Location Information to a Location Server. Such information can then be distributed to Location Recipients in coordination with policies set by the Rule Maker, e.g. the user whose position is stored.

A 'using protocol' must provide some mechanism allowing Location Recipients to subscribe persistently in order to receive regular notification of the geographical location of the Target as its location changes over time. Location Generators must be enabled to publish location information to a Location Server that applies further policies for distribution.

One of the benefits of this architecture is that the privacy rules are stored as part of the location object [Cuellar04]. Thus, nobody can claim that she did not know that access to the location information was restricted. But misuse is still possible and it is still not hindered by technical means.

C. Server side means

In order to ensure privacy after agreeing to a certain privacy policy or privacy contract suitable means on the data gathering side are needed. Such could be Hippocratic databases [Agrawal02], HP Select Access [Casassa05], Carnival [Arnesen04], PrivGuard [Lategan02]. All these systems check whether an agreed individual privacy policy allows access to a certain data for the stated purpose and by the requiring entity.

There are several approaches that try to protect privacy in location aware middleware platforms [Gruteser03, Langend02, Bennicke03, Wagealla03, Synnes03]. In [Langend02, Bennicke03, Wagealla03] means are discussed that enable the user to declare how much information she is willing to reveal. In [Synnes03] the authors discuss a middleware that uses user defined rules which describe who may access the user's position information and under which circumstances. The approach investigated in [Gruteser03] intentionally reduces the accuracy of the position information in order to protect privacy. All these approaches lack means to enforce access to user data according to the access policy defined by users. A combination of the location aware middleware platforms with protection means sketched above would clearly improve user privacy. A first step in this direction was reported in [Langend06] where users are enabled to generate Kerberos tokens at their own device and where the platform checks these tokens before granting access to user data.

IV. Assessment of Privacy Enhancing Techniques

In this section we discuss the protection level that can be achieved by applying privacy enhancing techniques. In order to clarify how different classes of approaches effect user privacy we resume our example from section II and show which data is protected by which means. Thereafter we identify the protection level achieved by each class of protection means.

A. Evaluation of presented techniques

For the evaluation of the privacy enhancing techniques we resume our example. Table 2 shows that each class of privacy enhancing techniques has its own merit and is applicable for specific type of information. The fact that all techniques have been designed to protect specific information allows easy combination of several approaches to improve user privacy. In the case of e-cash with revocable anonymity the use of different pseudonyms is essential in order to prevent service providers from linking individual transactions by using un-altered pseudonyms. Along these lines, use of identity management systems becomes essential in order to ensure that all pseudonyms are used correctly, when interacting with service providers. In addition, support for the generation

of pseudonyms can be of help in order to guarantee a minimal level of pseudonym quality.

Table 2: The sets of user data each party can link per transaction. The positing system can get information only if the user role is passive i.e. the system tracks the user.

Party	**unprotected**	**pseudonyms**	**anonymous e-cash**
User	1. Identity 2. Location 3. Service provider 4. Purchase details	1. Identity 1.1 Location system user pseudonym 1.2 Service user pseudonym 1.3 E-cash user pseudonym 2. Location 3. Service provider 4. Purchase details	1. Identity 1.1 Location system user pseudonym 1.2 Service user pseudonym 2. Location 3. Service provider 4. Purchase details
positioning system	(1); (2)	(1.1); (2)	(1.1), (2)
location handling subsystem	1; 2; 3	1.1; 2; 3	1.1; 2; 3
Service provider	1; 2; 3; 4	1.1; 1.2; 1.3; 2; 3; 4	1.1; 1.2; 2; 3; 4
payment provider	1; 3	3	3
Network unencrypted *Network encrypted* *Network with MIX*	1; 2; 3; 4 3 -	1.1; 1.2; 1.3; 2; 3; 4 3 -	1.1; 1.2; 2; 3; 4 3 -

In Table 2 we have not included descriptive and server side approaches. With the former data gathered depends on user preferences and the latter provides protection against misuse only after the fact, i.e. it has no influence on the data accumulated in a certain service provider's database.

B. Protection level

In order to asses the protection a certain PET can provide we use a classification with four protection levels:

- ***High***: technical means are given to ensure that the amount of data that can be gathered by a service provider is restricted to a minimum or matches the user's requirements. So, no detailed information can be deduced from gathered data. The downside is that no value added services can be provided or a service may not be provided at all.
- ***Medium***: the data that are gathered can not only be determined by the user, but she keeps somewhat control over them. This control might be either an active data control, i.e. an obeyed request for deletion, or passive control that specifies certain rules on how these data shall be dealt with in the future or for certain purposes.
- ***Low***: the user can determine which of her data is gathered. Especially if there is no proven technical means to protect the data it is the task of service provider to ensure the security of the gathered data. The drawbacks for service providers could be that users are hesitant to use their service if they cannot prove the security/privacy of the data.
- ***None***: the user, respectively, the owner of the data has no influence on the kind of data that is gathered, which information gets inferred or derived. In addition, the service provider or data collector respectively applies no appropriate means to protect the information or privacy. In this case we cannot speak of privacy at all. Such environment enables service providers or other to gather as much and almost any data they want. Besides the drawback for service users having no privacy at all it most likely diminishes the trust of the users or potential customers respectively into such services.

In the classification of the PET according to protection levels we are focussing on the strength of the classes of mechanism and neglect side effects. We are aware of the fact that real system properties such as the number of participants have significant impact on the protection level. For example anonymous e-cash schemes provide a high level of protection since they prevent the user's bank from learning about the users online purchase habits as well as the service provider from revealing the users identity. But if the anonymous e-cash scheme is used by a single customer of the bank only, the protection provided by the anonymous e-cash scheme collapses to the protection against the service provider, since the bank can easily link the e-coins to the user's identity.

Table 3 shows the protection level of all presented classes of privacy enhancing techniques such as mix networks etc. Here we did not consider individual differences in a class since weighting individual the drawbacks of similar approaches depends much on personal preferences and technical differences are already discussed in section III.

Table 3: Protection level of the individual privacy enhancing techniques at network and application level.

	Mix networks	Pseudonyms	Anonymous e-cash	Descriptive approaches (DA)	DA + server side technologies	Location protection
Application level	none	medium	high	low	medium	low - medium
Network level	high	none	none	none	none	none

V. Conclusions

In this chapter we have presented privacy enhancing techniques that have evolved during the last decades. If all these techniques are combined and used in the correct way, user privacy is reasonably good protected. The sad point here is that despite some of these approaches are quite well understood, they are still not in place. So despite privacy protection is theoretically possible in the real world it is hard to get. Only different versions of Chaum's mix network approach and P3P/APPEL are currently in place to protect user privacy and experienced Internet users are using different pseudonyms while browsing the Web or doing e- or m-commerce.

From our perspective, most of the privacy enhancing techniques still suffer from acceptance issues. Anonymous e-cash lacks support from banks. Service providers might also be reluctant to accept fully anonymous e-cash due the challenging fraud protection mechanisms involved. Even using mix networks is problematic nowadays. Many service providers block their access if they recognize usage of mix networks. Officially it is mostly justified with crime prevention, though it can be assumed that they do not want to lose valuable additional user information.

The paradigm shift in Internet use from wired to wireless also leads to new challenges. Resource consuming privacy enhancing techniques cannot be applied by mobile service users. This holds especially true for use of mix networks.

New technologies such as Web 2.0 allow completely new kinds of attacks. In [Rao00] and [Novak04] the individual way of writing was described as a means to link pseudonyms together. As long as service users are only entering a pseudonym and an email address into Web forms they are still safe, but writing exhaustive comments in news groups or blogs provides sufficient material to link pseudonyms.

Pervasive computing is going to become a real challenge for privacy enhancing techniques. A lot of information can be gathered by the environment and up to now it is still an open issue how such an environment can be adjusted to individual privacy preferences.

VI. Additional Reading

Additional reading can be found on the web pages of the EU-projects FIDIS, PRIME and SWAMI. The first two projects are focusing on identity management issues whereas SWAMI deals with privacy issues in pervasive environments. The research agenda of FIDIS (The Future of Identity in the Information Society, http://www.fidis.net) includes virtual identities, embodying concepts such as pseudonymity and anonymity. PRIME (Privacy and Identity Management for Europe, https://www.prime-project.eu) aims to develop a working prototype of a privacy-enhancing identity management system. In contrast to other research projects PRIME also aims at fostering market adoption of privacy enhancing technologies. Privacy issues in pervasive environments have not been intensively investigated by the research community in recent years. A first attempt is made by the SWAMI project (Safeguards in a World of AMbient Intelligence, http://swami.jrc.es) which focused on AMI projects, legal aspects, scenarios and available PET.

The workshop series "Privacy Enhancing Technologies" published in Springer's LNCS series (2482, 2760, 3856, 3424, 4258) provides a great variety of publications dealing with technological, social and legal aspects of privacy.

VII. References

[Barbaro06] Barbaro, M., Zeller Jr., T., "A Face Is Exposed for AOL Searcher No. 4417749", New York Times, 9th August 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1167454800&en=f448108fbc40931e&ei=5070

[Anton04] Anton, A. I., He, Q., Baumer, D. L., "Inside JetBlue's Privacy Policy Violations", IEEE Security & Privacy, Nov./Dec. 2004

[Reiter98] Reiter, M., Rubin, A., "Crowds: Anonymity for Web Transactions", ACM Transactions on Information and System Security Vol. 1, No. 1, November 1998, pp. 66-92

[Treu05] Treu, G., Küpper, A., "Efficient Proximity Detection for Location Based Services" In Proceedings of the 2nd Workshop on Positioning, Navigation and Communication 2005 (WPNC05), vol. 2005, SHAKER-Publishing, Hannover Germany, March, 2005

[Agrawal02] Agrawal, R., Kiernan, J., Srikant, R., Xu, Y., "Hippocratic Databases", 28th International Conference on Very Large Data Bases, August 20-23, 2002, Hong Kong, China

[Peterson05] Peterson, J., "A Presence Architecture for the Distribution of GEOPRIV Location Objects", Request for Comments: 4079, July 2005, http://www.ietf.org/rfc/rfc4079.txt

[Cuellar04] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "GEOPRIV requirements", Request for Comments: 3693, February 2004, http://www.rfc-archive.org/getrfc.php?rfc=3693

[Cranor00] Cranor L. F, 1999: Beyond Concern: Under-standing Net Users' Attitudes About Online Privacy. In Ingo Vogelsang and Benjamin M. Compaine, eds. The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy. Cambridge, Massachusetts: The MIT Press, p. 47-70, 2000

[Maaser05] Maaser, M., Langendoerfer, P. "Automated negotiation of privacy contracts", Computer Software and Applications Conference, 26-28 July 2005, Edinburgh, GB

[Preibusch05] Preibusch S., "Implementing Privacy Negotiation Techniques in E-Commerce", 7th IEEE International Conference on ECommerce Technology, IEEE CEC 2005, July 19-22, 2005, Technische Universität München, Germany

[PrivacyBird] AT&T Privacy Bird, AT&T Corporation, http://privacybird.com; last visited: 12.01.2007

[IE6] "Microsoft Announces Privacy Enhancements for Windows, Internet Explorer", Microsoft® Corp. http://www.microsoft.com/presspass/press/2000/Jun00/P3Ppr.asp, 12.01.2007

[NS7] Netscape 7.0 – 7.2 Release notes, Netscape® http://wp.netscape.com/eng/mozilla/ns7/relnotes/7.html#psm, 12.01.2007

[Gruteser03] Gruteser, M., Grunwald, D., "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys), 2003

[APPEL] W3C: A P3P Preference Exchange Language 1.0 (APPEL1.0), W3C Working Draft 15 April 2002, http://www.w3.org/TR/P3P-preferences/, 12.01.2007

[Jendricke00] Jendricke, U., Gerd tom Markotten, D., "Usability meets security - the Identity-Manager as your personal security assistant for the Internet" Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference Volume , Issue , Dec 2000 Page(s):344 – 353

[Chaum85] Chaum, D., "Security without identification: transaction systems to make big brother obsolete", in Communications of the ACM, Volume 28, Issue 10 (October 1985), pp. 1030-1044, ACM Press 1985.

[Brands93] Brands, S., "Untraceable Off-line Cash in Wallets with Observers", Proc. Of Crypto '93, Lecture Notes in Computer Science 773, Springer-Verlag, 302-318.

[Koch01] Koch, M., Wörndl, W., "Community Support and Identity Management", Proc. European Conf. on Computer Supported Cooperative Work (ECSCW 2001), Bonn, Germany, Sept. 2001

[Berthold00] Berthold, O., Köhntopp, M., "Identity Management Based On P3P", Workshop on Design Issues in Anonymity and Unobservability; July 25-26, 2000, Berkeley, CA;

[Langend06] Langendörfer, P., Piotrowski, K., Maaser, M., "A Distributed Privacy Enforcement Architecture based on Kerberos", WSEAS Transactions on Communications, Vol. 5 (2), 231-238, 2006

[Rao00] Rao, J. R., Rohatgi, P.,"Can Pseudonymity Really Guarantee Privacy?" Proceedings of the Ninth USENIX Security Symposium, 2000

[Novak04] Novak, J., Raghavan, P., Tomkins, A., "AntiAliasing on the Web", Proceedings of the 13th international conference on World Wide Web New York, NY, USA, 2004

[Chaum81] Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, vol. 24 no. 2, February, 1981.

[Arnesen04] Arnesen, R. R., Danielsson, J., Nordlund, B., "Carnival: An Application Framework for Enforcement of Privacy Policies", 9th Nordic Workshop on Secure IT-systems , 2004

[Lategan02] Lategan, F. A., Olivier, M. S., "PrivGuard: a model to protect private information based on its usage", South African Computer Journal, Volume 29, p. 58-68, 2002

[Casassa05] Casassa Mont, M., Thyne, R., Chan, K., Bramhall, P., "Extending HP Identity Management Solutions to Enforce Privacy Policies and Obligations for Regulatory Compliance by Enterprises", HPL-2005-110, 2005 http://www.hpl.hp.com/techreports/2005/HPL-2005-110.html, 12.01.2007

[Jia04] Jia, G., Brebner, G., D'Uriage, M., "Privacy Protection System And Method", US Patent: US 2004/0181683 A1

[TOR] Tor: anonymity online, http://tor.eff.org/overview.html, 12.01.2007

[ANON] JavaAnonProxy at AN.ON, http://anon.inf.tu-dresden.de/index_en.html, 12.01.2007

[Langend02] Langendörfer, P., Kraemer, R. "Towards User Defined Privacy in location-aware Platforms", Proceeding of the 3rd international Conference on Internet computing, USA. CSREA Press, 2002.

[Bennicke03] Bennicke, M., Langendörfer, P, "Towards Automatic Negotiation of Privacy Contracts for Internet Services", Proceeding of the 11th IEEE Conference on Networks (ICON 2003),. IEEE Society Press, 2003.

[Wagealla03] Wagealla, W., Terzis, S., English, C., "Trust-based Model for Privacy Control in Context-aware Systems", 2nd Workshop on Security in Ubiquitous Computing, Ubicomp, 2003

[Synnes03] Synnes, K., Nord, J., Parnes, P., “Location Privacy in the Alipes platform”, In Proceedings of the Hawai'i International Conference on System Sciences (HICSS-36), Big Island, Hawai´i, USA, January 2003.

[Cranor07] Cranor, L., Langheinrich, M., Marchiori; M., Presler-Marshall, M., Reagle, J., http://www.w3.org/TR/P3P/, 12.01.2007

[FTC99] Federal Trade Commission 1999: The FTC’s First Five Years: Protecting Consumers Online, available at: http://www.ftc.org, 1999

[Reed98] Reed, M., Syverson, P., Goldschlag, D., „Anonymous connections and onion routing“, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, 1998

[Sampiget06] Sampigethaya, K., Poovendran, R., “A Survey on Mix Networks and Their Secure Applications**”,** Proceedings of the IEEE, Volume 94, Issue 12, Dec. 2006