Design Patterns for a Systemic Privacy Protection

Kajetan Dolinar, Jan Porekar, Aleksej Jerman Blažič
Security Technology Competence Centre (SETCCE)
Tehnološki park 21, SI-1000 Ljubljana, Europe
kajetan.dolinar@setcce.si, jan.porekar@setcce.si, aljosa.jerman-blazic@setcce.si

Abstract

This paper shows that existing privacy enhancing technologies and the state-of-the-art in research on the field of privacy protection has grew to a considerable maturity up to date, yet privacy protection regulation disregards these advancements and remains in vague terms. Contemporary social situation with regards to privacy protection entails serious arguments why this disparity should rather soon be overcome. It is further shown how this disparity could be overcome by a collection of privacy protection patterns which include technical solutions as well as social models and can be combined into a systemic privacy protection framework that could be declared on the level of regulation itself in much more detailed and concrete terms than today.

1. Introduction

There have been many advancements in privacy enhancing technologies up to date. We are witnessing innovations in area of identity management solutions, trust management, privacy policy negotiation and trust negotiation, access control and many more. We know the legal and social context for privacy protection: there are known court cases and public affairs. Yet there is still a wide gap between the technologies on one edge of the gap and having them properly integrated into the legal and social paradigm of privacy protection on the other edge.

There is a lot more to privacy protection than only technologies. Technologies themselves are inefficient without a general consensus on how they should be used in a proper way. Privacy cannot be protected without a complete social support in terms of regulation, successful prosecution and business interest as well as public awareness, social studies and public education. Technology should be complemented with these expert areas to provide a systemic framework for privacy protection in society as a whole.

One of the most urgent problems is that business does not have enough incentives to invest in privacy enhancing technologies [1]. A possible reason for this may be that a formal institution of technical patterns and social models is missing where the technologies and the social structures would be combined in a congruent system with at least theoretic proof of working. Having such an institute would allow legislation on a much more concrete basis than today; it would make possible to define exact procedures for privacy protection in every data collection or processing. This in turn would force data controllers and data processors to invest into privacy enhancing technologies and thus give privacy enhancing technologies market value.[1]

This paper presents one of the possible ways how a formal institution of technical patterns and social models can be established. The approach presented here describes each of the patterns and models formally in terms of privacy protection patterns. The whole idea is referred to as *privacy protection cycle*. Section 2 elucidates the situation on field of privacy protection from the point of view of current European legislation and public privacy protection issues as witnessed up to date. In the Section 3 the current state-of-the-art in privacy enhancing technologies is presented. Section 4 gives an overview of the privacy protection patterns and Section 5 shows how they work inside the privacy protection cycle. Paper ends with conclusions in Section 6. Additional support for arguments in the following sections can be found in appendix A.

2. Legal and Social Context for Privacy Protection

This section uncovers the contemporary state in the advancements of legal frameworks and contemplates about the evolving situation in public affairs regarding privacy protection; different types of problematic situations are exposed in order to corroborate or defy the efficiency of regulation or

[1] Data controller is the party which determines the purposes and means of the processing of personal data while data processor means the party which actually processes the data on behalf of the data controller.

to provide requirements for various privacy protection patterns.

2.1. Legal Synopsis

Most of the countries in the world have their own privacy protection legal acts. This article will focus mainly on European regulation on data protection defined by European Directive 95/46/EC [2] as it summarizes all important data protection principles:

- Principle of fair and lawful processing (Article 6(1), letter a): *"Any processing of personal data should be carried out in a fair and lawful way with respect to the data subjects.*[2]*"*

- Finality principle or Limitation principle (Article 6(1), letter b): *"Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes."*

- Data minimisation principle or Proportionality principle (Article 6(1), letter c): *"Processing of personal data should be limited to data that are adequate, relevant, and not excessive."*

- Time minimization principle (Article 6(1), letter e): *"Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."*

- Notification principle (Articles 10, 11): *"Data controller or his representative has to identify himself to the data subject and notify data subject about the personal data being processed, stored or further disclosed to any third party."*

- Principle of data subject consent (Article 2, letters a, h; Article 7, letter a; Article 8): *"User consent is required for a legitimate data processing by any data controller. The user consent is defined as 'any freely given specific and informed indication by which the data subject signifies his agreement to personal data relating to him being processed.'"*

- Principle of right to access personal data (Article 12): *"Data subject has right to access (and rectify) the data collected about him and to be informed about the intended processing and the logic behind the intended processing of the data."*

- Principle of right to object processing of personal data (Article 14): *"Data subject has right to object processing of personal data (subject to certain constraints: compare articles 7, letters e and f)."*

Additional to those principles many other legal principles indirectly related to data protection can be found in other legal acts. This paper will not include an overview of those legal instruments. For the purpose of this paper the above reduced list is enough to give the exposure of the level of detail provided by the regulation: generally the regulation does not prescribe methods or technologies for data protection, it merely provides the general principles.

2.2. Problematic Social Situations

A lot of situations and affairs are known to have happened up to date with a considerable importance for privacy protection. In the following we provide a succinct[3] overview of the global state of affairs and the most critical issues with respect to privacy protection. This summary has been produced from a notably more exhaustive source provided by European FP6 SWAMI project [3]; all the footnotes in this section are reproduced from this source.

Problem Situation 1 – Working from home, monitoring of employees. What is the dividing line between working environment and private / home environment? All the privacy protection principles are related to this problem; moreover, article 8 of European Convention of Human Rights [4] protects the private home. The problem is that a workplace might be situated in a private home and that also a typical workplace is used, to a lesser extent, for private purposes.[4]

Problem Situation 2 – Digital rights management. How much it interferes with privacy of an individual? Proportionality principle obliges policy-makers to consider alternative, less infringing ways of protecting intellectual property rights, reconciling them with privacy rights.

Problem Situation 3 – ID theft. Identity thefts are reality![5] This is against Principle of fair and lawful processing, Notification principle, Principle of data subject consent, and Principle of right to object processing of personal data. Automated payments make it easy to spend money quickly. Distance contracts do not offer the same guarantees, trust and confidence as in physical commerce. It is known that

[2] Data subject is a legal or natural person to which the data refer.

[3] Succinct here means that there are nine situations complex enough to elaborate on several tenths of pages but we have to compress them to fit a few; moreover, it is in purpose of clarity that every text that would be superfluous to the exact definition of the situation, yet important to support our arguments, is placed in a footnote. Thus, the reader is asked to forgive the abundance of footnotes on this and the following pages; a reader may skip them without much harm or read them in appendix A.

victims of identity theft have great difficulties recovering from the consequences.[6]

Problem Situation 4 – Data laundering. Companies are paying a lot of money for personal and group profiles and there are market actors in position to sell them.[7] This is clearly against data protection principles. This phenomenon is known as 'data laundering'. Similar to money laundering, data laundering aims to make illegally obtained personal data look as if they were obtained legally, so that they can be used to target customers.[8]

Problem Situation 5 – Personal profiling. Personal profiling is reality. A lot of people do not realise how much personal information they are constantly giving out.[9] Also this activity is illegal with respect to data protection principles.

Problem Situation 6 – Inadequate profiling. People are victims of an inadequate profiling based on false data or processing.[10] This violates the Principle of fair and lawful processing and is a great motivator for Notification principle, Principle of data subject consent, Principle of right to access personal data, and Principle of right to object processing of personal data. However, it is far from truth that people would always be given those rights.[11]

Problem Situation 7 – Disproportional request for personal information. It is not a rare case that a data controller requires information in extent disproportional to the purposes of business. There is not much case law in which one can find out what "proportional" data processing is and what is not. However, disproportionate data collection happens and is prohibited by Principle of fair and lawful processing, Finality principle, and Proportionality principle.

Problem Situation 8 – Spyware and personal preferences. Spyware is a frequent way to steal data and intrude privacy.[12] The use of spyware programs (installing and spying) constitutes a number of criminal offences according to the Cybercrime Convention [5]: illegal access (Article 2) and illegal interception (Article 3) when there is, in the latter case, an interception, without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system.

Problem Situation 9 – Advertising and spam. Spam not only takes time and provokes irritation, but also can influence and infringe someones private world. European Directive 2000/31/EC [6] and European Directive 2002/58/EC [7] both contain provisions on (unsolicited) commercial communication, but do not really seem to have the desired effect. This situation also defies Principle of data subject consent and Principle of right to object processing of personal data.

2.3. Final Notices

Not much can be done to prevent authorities or business to know data of people. But it is relatively simple to provide an individual with a set of (potentially false) identities which can vouch for important properties of that individual such as the individual is employed, has a regular health insurance, is of appropriate age, receives such and such income, etc. The identities should provide the data along with certificate material proving the data are accurate, however the identities themselves could be completely pseudonymous. The feasibility of such a technology is not a question (cf. Section 4, Virtual Identity pattern); what is missing is that the legislation in the first place should legalize such identities and clearly define transactions where they are allowed.

Companies that process personal data acquired from third parties are bound by the rules of data protection. It might be a good safeguard to oblige those companies to check where the information they buy comes from and if it has been lawfully acquired. Similar obligations could be imposed like those on banks to control money laundering. This is important for Sticky Policies, Privacy Audit Trail, and Access Control privacy protection patterns.

Speaking of the problem of disproportionate data collection it is very difficult to define what is "proportional". On the one hand, there are too many diverse situations in which processing takes place, so that one particular situation might require more data processing for one reason or another. This motivates the idea of Privacy Policy Negotiation pattern.

3. Privacy Enhancing Technologies up to Date

Privacy enhancing technologies come in a variety of different kinds of solutions. This section will provide a quick overview through existing state-of-the-art and will try hard to be as broad as possible. This is important as there will be a need for references to the real solutions when defining patterns in Section 4. Privacy enhancing technologies can be divided into six categories:

- privacy preferences and policy languages,
- trust & reputation systems,
- trust & privacy policy negotiation,
- identity management,
- data conservation,

- control of processing,

We will briefly touch every category in the following paragraphs.

Privacy preferences and policy languages. There are systems which enable users to check how their privacy preferences relate to privacy policies of a data controller. An example is Privacy Bird [8] developed at the AT&T, a P3P user agent as a browser helper object for the Internet Explorer 5.01, 5.5, and 6.0 web browsers on Microsoft Windows 98/2000/ME/NT/XP operating systems. The Platform for Privacy Preferences (P3P) [9] enables organizations to express their privacy practices in a standard XML format that can be retrieved and interpreted automatically by user agents. P3P policies can encode contact information for the legal entity making the representation of privacy practices in a policy, enumerate the types of data or data elements collected, and explain how the data will be used. P3P Preference Exchange Language (APPEL) [10] complements P3P Specification by providing a language for specifying users preferences regarding P3P policies.

Several other policy languages have been devised for expressing privacy preferences: The Enterprise Privacy Authorization Language (EPAL) [11] is an interoperability language for exchanging privacy policy in a structured format between applications and / or enterprises, structured in XML. Another XML based language for expressing access control policies is XACML [12], which stands for eXtensible Access Control Markup Language. It complements SAML [13] which is in purpose of conveying information on authorization, authentication, and related attributes in an XML formatted assertions.

Besides encoding of simple policy rules there has been a lot of research made in knowledge representation systems enabling support for enriched semantic processing such as Description Logic [14], a family of languages on the level of the first order predicate logic with extensions for knowledge representation, some of them are well known ontology systems such as OWL - DL [15], KAON [16] and KAON2 [17]. The use of ontologies for representing important notions of privacy protection has also been researched [18][19].

The potential for machine reasoning and semantic processing over policies has been researched by PRIAM project [20][21]. The authors contemplate on theorem provers, systems that parse expressions of a (first order) logic language and process them in order to derive formulas of logical truths. There are many ways how this can be done such as method of analytic tableaux [22] or resolution with unification [23]. There are many known theorem provers such as Otter [24] or Coq [25]. One of the methods modern machine reasoners often use is superposition and term rewriting which takes a hypothesis formula, parses it and replaces subformulas by the rules of inference – either the classical formal logic rules or the rules representing facts about the actual domain of discourse referred to as *background knowledge* – as long as there is some rule possible to apply.[26][27] This method is especially suited to machine reasoning systems for evaluating ontologies such as already mentioned KAON and KAON2 systems, FaCT++ [28], Pellet [29], DIG [30] or JENA [31].

Trust & reputation systems. There are various technologies enabling trust in some way. Technologies based on PKI and cryptography have already been known for a long time; they are used to certify authorizations, identity, or other traits by means of cryptography and systems of global trust. The reference to those technologies will tacitly be assumed throughout the paper where questions about integrity or confidentiality will rise.

However, there is another branch of research and technologies which treats trust in a substantial way, tapping into the very social phenomenon of trust and reputation. There have been many attempts to formalize this important aspect of social interaction [32][33][34] and many a model studied of how trust and reputation are induced in people and society [34][35][36][37]. Some of those models are successfully used by today's leading electronic market actors such as Amazon.com or eBay for evaluating how good or bad individuals perform in transactions.

The notion of trust is most often modelled as a real number on interval from 0 to 1 inclusively, 0 meaning no trust and 1 meaning full trust. It is disputable, though, how relevant such a trust assessment is in a given situation with respect to what is to be trusted: trust should be assessed for every different kind of relation in separate. A separate number should be used for assessing how trustworthy a person is as a business partner, and a separate for how trustworthy that person is as an expert in his or her field; these two relations can each imply quite a different trust situation. One number cannot capture such a multidimensional problem. Even harder is to make a model for evaluation of trust based on individual assessments as there can always be individuals that will introduce false opinions in the system; however, recent investigations show that trust calculation models can be built which preserve high level of fidelity in communities where as much as 80% of individuals give false trust assessments [37]. Despite the weaknesses of trust management systems there are many more good reasons why such systems should be used (cf. Privacy Policy Negotiation and Trust & Reputation Evaluation System privacy protection patterns in Section 4).

Trust and privacy policy negotiation. Another way of how trust can be established between anonymous actors is by the so called *trust negotiation* whereby two negotiators exchange identifying or certifying information in order to acquire the sufficient amount of proof about the opponents trustworthiness.[38][39] Moreover, negotiation has also been investigated in scenario of a straightforward bargaining for resources and privacy protection practises, supported by rich semantics.[40][18][19][41] This type of negotiation is referred to as the *privacy policy negotiation*. Privacy policy negotiation as well as trust negotiation can be valuable tools for a fine-grained restitution of data to be disclosed and privacy protection rules before the actual data are released, thus implementing in reality Data minimisation principle and Finality principle. For a successful negotiation, taking it abstractly, there should always be a formal result in sense of an agreement, where the statements both sides agreed are evident.

Identity management. Numerous initiatives and technological standards have been created up to date for different kinds of frameworks for introducing identities into electronic transactions. YADIS [42] is an open initiative to build an interoperable lightweight discovery protocol for decentralized, user-centric digital identity and related purposes. With YADIS the capabilities of identities can be composed from an open-ended set of services, defined and/or implemented by many different parties. OpenID [43] is a distributed, decentralized network where identity is represented as a URL and can be verified by any server running the protocol. It is a part of the YADIS family of protocols. Light-Weight Identity (LID) [44] is a set of protocols and software implementations created by NetMesh Inc. for representing and using digital identities on the Internet without relying on any central authority. LID supports digital identities for humans, human organizations and non-humans (e.g. software agents, things, websites, etc.). XRI/XDI [45][46] is an international non-profit organization governing public services based on the XRI abstract identifier and XDI data interchange protocols. This new layer of infrastructure enables individuals and organizations to establish persistent Internet identities and form long-term, trusted peer-to-peer data sharing relationships. iNames are one form of an XRI, an OASIS open standard for abstract identifiers designed for sharing resources and data across domains and applications. One problem XRIs are designed to solve is persistent addressing – how to maintain an address that does not need to change no matter how often the contact data for a person or organization changes. XRIs accomplish this by adding a new layer of abstract addressing over the existing IP numbering and DNS naming layers used on the Internet today. Privacy is protected because the identity owner controls this resolution. Simple eXtensible Identity Protocol (SXIP) [47] is a protocol for automating the exchange of identity data on the Internet. It supports Single Sign-On access to different websites. User-Centric Verified Identity allows users to acquire and release verified “assertions” around their identity, enabling them to create richer profiles of their online identity. User Choice supplies added privacy by enabling users to be actively involved in the release of the data they store in their identity profile. Many of the technologies mentioned here are embraced under the Liberty Alliance initiative [48] for open standards, guidelines and best practices for federated identity management with its own identity architecture specification [49]. Another initiative for federated identity is Shibboleth [50] with architecture and open-source implementation for federated identity-based authentication and authorization infrastructure based on SAML.

CardSpace is a software which securely stores digital identities of a person, and provides a unified interface for choosing the identity for a particular transaction, such as logging in to a website. CardSpace [51] is a central part of the Microsoft effort to create an identity meta-system, or a unified, secure and interoperable identity layer for the Internet. The CardSpace software allows the users to create self-signed identities for themselves. CardSpace is built on top of Web Services Protocol Stack. Higgins trust framework [52] is a set of open source protocols and software applications that allow people to store their digital identities on their personal computers and share the stored information with commercial companies and other parties in a controlled fashion. Higgins is sponsored by IBM and Novell and is promoted as an alternative to Microsoft’s CardSpace.

Besides these efforts much research has been carried out for advanced identity management schemes in scope of some European projects. In projects PRIME and DAIDALOS the concept of multiple (virtual) identities is explored, where every person can have several identities, some of them with blurred or obfuscated data, to enhance user’s privacy.[53][41] This is one of the most powerful techniques for enforcing Data minimisation principle. The concept also makes use of pseudonymity and anonymity approaches.[54] The distinction between addressable and non-addressable pseudonyms is used to allow for the integration of identity management into the application logic. For example, non-addressable pseudonyms are used in the task assignment scenario (see [55], Section 4.5) to allow application internal processes to be supported by the identity management. In order to make a pseudonymous identity untraceable on the network level there exist models such as Onion Routing [56] and Crowds [57] which make possible routing, and thus internet communication, in an anonymous way. There are also software projects that enable this kind of protection.[58]

Data conservation. By data conservation different kinds of techniques are meant. First of all, an appropriate type of access control should be in place before access to private information is allowed to an arbitrary agent. The three most commonly refered models are Discretionary Access Control

(DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).[59] In DAC the owner of the resource decides who is allowed the access to the resource and what privileges they have. This may be achieved using access control lists or credentials, i.e. keys admitting access to the resource. In MAC agents have sensitivities assigned specifying their level of trust and resources have sensitivities assigned specifying the level of trust required for access; in order to access a resource, the subject must have a sensitivity equal to or higher than the resource. MAC can be achieved by a rule-based access control defining specific conditions for access to a resource, e.g. simple rules applying matching sensitivity labels of agents and resources; or it can be achieved applying lattice model, a mathematical structure, to infer complex decisions on relations between agents and resources. In RBAC collections of permissions that may include complex operations are the key to access a resource; agents are admitted to a resource if their roles assignments satisfy permissions. Recently, a new type of access control was introduced called Purpose Based Access Control (PBAC) with a scheme where access to a resource is allowed if the agent has a justified purpose for that.[60]

Finally, in order to protect privacy in the most general sense, data should be protected using cryptographic methods when transferring them over communication channels. More advanced protection is achieved by *steganography* [61] or other kinds of data obfuscation [62]. When privacy agreements are in question, in case they are represented in a digital form, their integrity and time of creation should be preserved by long term trusted archives [63]; failing to do so might disable a curtailed person to assert a privacy breach, since what should constitute a privacy breach in such a case is primarily measured by what the person was guaranteed by the opposite side and that should be saved for later reference in an agreement. As certificate material deteriorates over short periods of time (e.g. five years for a PKI certificate validity is already a long period), integrity and time origin of agreements or other digital documents have to be preserved using methods for long term trusted archiving.

Control of processing. When private identifying information is disclosed to data controllers and is under processing by data processors, the techniques mentioned until now can only have limited or no protection power. However, there has been a rich tradition in research of techniques for protecting privacy after disclosure, the so called *a-posteriori* privacy protection, albeit some of them may not be recognized as such in the past. One of the first attempts to protect privacy of data during processing (i.e. after their disclosure) was proposed by Rivest, Adleman, and Dertouzous [64] who introduced the idea of performing simple computations on encrypted data, the technique referred to as *privacy homomorphism*. The idea was studied in context of various cryptosystems and for different problems such as summation, multiplication, derivation, and integral of encrypted polynomials or union and intersection of encrypted sets [65]. The approach generally allows for the joint computation of a wide variety of functions, however its uses are limited by severe message expansion.

Related techniques were devised for the so called *Hippocratic databases* and privacy preserving data mining. The name “Hippocratic databases” was inspired by the concept of Hippocratic oath that has guided the conduct of physicians for centuries. The concept is a research initiative started in 2002 in IBM Almaden Research Center.[66] In the original paper the authors argue that privacy is the right of individuals to determine how and to what extend information about them will be communicated to others and suggest that the database community has opportunity to play central role in the privacy debate by re-architecting the database systems to include responsibility for the privacy of data as the fundamental tenet. The idea inspired the field of research on privacy preserving data mining.[67][68][69]

Further techniques for *a-posteriori* privacy protection were sought in direction of privacy auditing and introduced by European projects such as PRIAM [70]. The idea is that records of all the actions performed on data are stored in a trusted hardware module and authorities can perform auditing of those logs. A necessary prerequisite for this are the so called *sticky policies* [71]: to each unit of data a formal statement is attached where all the constraints about which actions are allowed on the data are defined by the owner of that data and described in a machine readable format. The sticky policy follows the data unit after it has been released to processing; the data along with the sticky policy should be cryptographically signed by the owner so that the data and the sticky policy can be proven to belong together. Data without a sticky policy should be deemed invalid. Every operation data processor commits on data is compared by the trusted hardware module to the sticky policy and if data processor has done operations to data that are not permitted by the sticky policy, then this can be signalled to the supervising agencies. This is referred to as *privacy audit trail*.[20][21]

4. Privacy Protection Patterns

We have seen that a variety of concrete techniques are available for privacy protection, which is in obvious contrast to the level of vagueness of legislation. The social situation calls for concrete solutions, but the gap between the legislation and the technologies keeps data controllers and data processors far away from using the concrete solutions in order to comply with legislation. What is missing is a collection of artifacts, which will be referred to as *privacy protection patterns*, each describing a particular technical solution or social model for privacy protection. Then legislation can be defined in terms of those artifacts.

4.1. The Structure of Patterns

A privacy protection pattern is an abstract scheme of how a particular approach to privacy protection is possible. It should include a unique name, a list of the actors included in the pattern, a list of properties the pattern provides, the context in which the pattern satisfies the properties, a succinct description of the solution and a diagram displaying the exact working of the solution. Additionally to this each pattern should include information on how it can be used in terms of controls which activate the pattern. Patterns will be laid down in the following form:

The form for specifying privacy protection patterns

Actors

A list of legal or natural persons involved in the pattern and their interests.

Properties

A list of abstract properties the pattern exhibits in relation to interests of the actors and in relation to the requirements implied by the context.

Context

A list of resources, instruments, or social and technical constraints and other factors which define the means and the possibilities how actors can achieve their ends.

Description

A succinct description of the way how the pattern operates on the context to moderate the actors' interests and achieve some aspect of privacy protection.

Controls

A list of features of that pattern allowing regulation or maintenance of the operation of the pattern described in terms of actions actors can take upon the context and the constraints for the admission of actors to commit those actions.

Definition

The activity diagram as specified in UML[72] displaying how the pattern operates on the context and how the controls influence this.

4.2. The Privacy Protection Patterns

The first pattern is about policies enabling exact specification of data protection rules and supporting machine reasoning. Principle of data subject consent, Finality principle, and Proportionality principle are impossible to enforce in an exact way without such a pattern; also what is a disproportional request in Problem Situation 7 is easier to resolve. Technical feasibility of this pattern is largely supported by policy specification languages and related research as was presented in Section 3.

Formally Provable Privacy Policies

Actors

Person – a legal or natural person.

Properties

- Deductibility: the structure of the policy supports computer aided inference of logical properties, semantic attributes and other constraints;
- Completeness: the policy is unambiguous;
- Soundness: the policy is not contradictory.

Context

- Privacy Policy: the certifying information and privacy protection rules of Person whose structure captures the first order predicate logic with extensions for knowledge representation;
- Theorem Prover: a system capable of deriving logical truths about Privacy Policy;
- Domain Model: a digital representation of the important notions from privacy protection with relations among them such as taxonomical relationships of inheritance of type or other ontological properties;
- Challenge: a request to disclose a certain personal identifying information of Person formated in the same structure as that of Privacy Policy.

Description

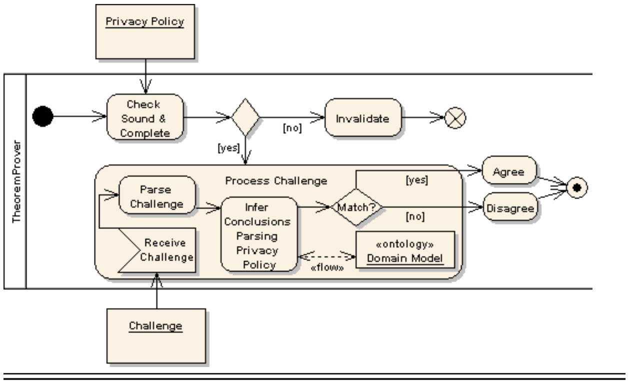
Privacy Policy captures the rules how the Person's data should be protected by data controllers and processors regarding privacy protection. The Domain Model provides the background knowledge for the Theorem Prover. The Theorem Prover makes possible a computer aided inference of facts and conditions regarding Privacy Policy against an arbitrary Challenge. Theorem Prover also makes possible checking completeness and soundness of the Privacy Policy.

Controls

For each data collected Person should be able to set in Privacy Policy at least the following:
- ENTITY identifies the Person;
- DATA describes the data which are subject to the following controls;
- PURPOSE specifies the allowed purposes for the collection or processing of DATA;[13]
- RECIPIENT identifies recipients of DATA;
- RETENTION indicates the kind of retention admissible for DATA;
- OPERATIONS defines the operations allowed on DATA;
- OBLIGATIONS states how data controllers and processors should protect DATA when handling them.

Each Challenge should define at least the following:
- REQUESTER identifies the data controller which requests a particular data;
- DATA describes the data requested;
- PURPOSE describes the purposes for data collection;
- OPERATIONS describe the operations REQUESTER wants to perform on DATA.

Definition



This pattern should be used in conjunction with

Privacy Preferences Helper Tool

Actors

Person – a legal or natural person;
Requester – a legal or natural person requesting a resource or data of Person or otherwise challenging Person's privacy.

Properties

- Maintainability: the Person is able to maintain the own set of privacy preferences;
- Friendliness: the Person is able to do so in a user friendly way.

Context

- Privacy Policy: Person's privacy preferences and other rules in a machine readable form;
- User Interface: a collection of commands and displays enabling insight into and management of Privacy Policy and related privacy preferences;
- Translator: a process which resolves user input from User Interface and relates this to the appropriate sections of Privacy Policy;
- External Application: an application through which Requester is able to challenge Person;
- Challenge: a request for a resource or data of Person or any other kind of challenge for Person regarding privacy protection.

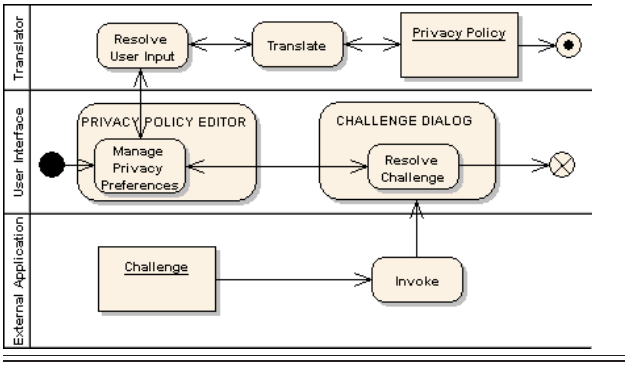
Description

User Interface enables Person to manage privacy preferences from Privacy Policy. Additionally, when Person's personal data are requested or Privacy Policy is challenged in another way by Requester, User Interface automatically informs Person of that challenge and Person is able to interactively resolve this.

Controls

User Interface should have at least two components:
- PRIVACY POLICY EDITOR is a display of Privacy Policy in a human readable way with controls which enable Person to add, update, delete, or otherwise modify privacy preferences and other rules from of Privacy Policy in a user friendly fashion;
- CHALLENGE DIALOG is a message display with appropriate controls and can be invoked by External Application when a Challenge occurs, enabling Person to interactively resolve the Challenge.

Definition



This pattern tells about a tool which makes possible a definition of privacy policy in a human friendly way so that user does not need to code the privacy policy. This is very important as policies generally are of the same complexity as programming languages and most of the people do not know how to do that. This pattern supports Principle of data subject consent and Finality principle, because the data subject can explicitly decide privacy protection preferences, it further supports Proportionality principle because it makes possible specification of which data and for what purposes and when should be disclosed. The pattern is technically possible as shown in Section 3. This pattern should be used in a combination with previous one and in combination with Privacy Policy Negotiation pattern.

The next pattern reflects upon the fact that whenever an individual or a company is about to disclose a particular information to another party it is all about trust and reputation, how much the other party will respect and protect privacy. What *respect* in the later case means can be defined as whether and how much the ways that other party handles the information are in accord with the data subject's privacy policy. Clearly, the case here is of a very specific trust domain, namely trust in how good or bad the information will be handled; accordingly, any trust representation, be it by number or category, will reflect on this. This pattern, especially in a combination with Privacy Policy Negotiation and Identity Management patterns privacy protection patterns, can be an important instrument for enforcing Principle of fair and lawful processing or Finality principle and to ward against Problem Situations 3, 4, 7 or 9; namely, market actors that indulge in such activities will get low reputation which will affect demand and consequently their market positions.

[13] This holds in either case: if Person is a data controller or processor then PURPOSE defines why DATA of data subjects need to be collected (or processed), or if Person is a data subject then PURPOSE defines for which purposes the data subject allows collection or processing of DATA.

Trust & Reputation Evaluation System

Actors

Person – a legal or natural person;
Peer – a legal or natural person requesting a resource or data of Person or otherwise challenging Person's privacy in a way so that Person has to disclose some data to Peer.

Properties

- Confidence: Person is able to deduce the degree of confidence in Peer based on rigorous trust / reputation evaluation model;
- Retribution: Person is able to reflect on the past experience with Peer in terms of trust and reputation and give Peer credit or accusation.

Context

- Trust Web: a community of persons with mutual trust relationships which also define the level of how high the whole of the community ranks each of the persons in terms of reputation;
- Trust & Reputation Manager: a tool on each person's node which makes possible assessment of trust and reputation by a rigorous trust / reputation evaluation model;
- Authority: a public body or agency moderating how persons can influence Trust Web and trust / reputation values.

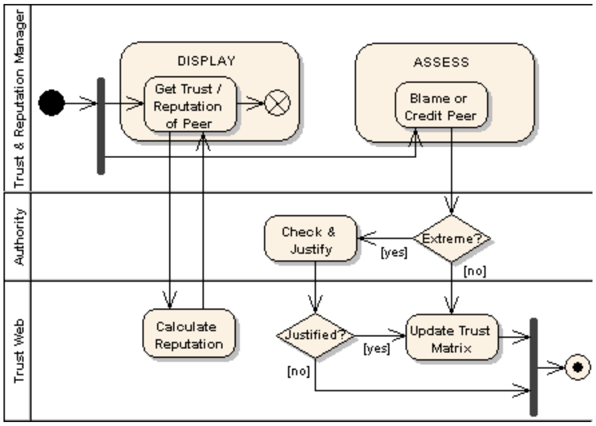
Description

(Every) Person has his own trust assessment of (Every) Peer, or at least of the close neighbours, and can adjust that using Trust & Reputation Manager. When Person wants to know reputation of Peer Trust & Reputation Manager can be used to obtain the grand total of trusts the whole Trust Web has in Peer. Trust & Reputation Manager should not allow changing Peer's reputation directly; instead, reputation should always be a cumulative of Trust Web based on trust evaluation model. In order to avoid abuse even Person's assessment of trust should not be unconditionally released into Trust Web so that possibility of unduly destroying reputation of a person is as low as possible: at least every request to gravely reduce reputation by a majority should be mediated by a special Authority.

Controls

Trust & Reputation Manager should have at least the following controls:
- DISPLAY is where trust or reputation values of peers can be read;
- ASSESS is where good or bad trust assessments can be injected into Trust Web, subject to Authority.

Definition



The next pattern identifies the need for a way to resolve privacy protection issues between two privacy policies of two parties in detail. This is required by Principle of data subject consent, Principle of right to object processing of personal data, Finality principle, and Data minimisation principle that cannot be enforced in practise without touching every issue in the two privacy policies and trying to converge them into an agreement that will display resolutions about explicit consent, opting in or out, the agreed purposes for processing, and the exact data to be disclosed. This pattern can greatly alleviate Problem Situation 7 since the agreement exactly defines the extent of data required for the transaction, subject to privacy policies and the purposes for collection. The pattern is feasible, as we have discussed in Section 3.

Privacy Policy Negotiation

Actors

Initiator – a legal or natural person which applies to Responder for some reason;[14]
Responder – a legal or natural person claiming data of Initiator or otherwise challenging Initiator's privacy with assumption to assist Initiator.

Properties

- Proportionality: the extent of data to be disclosed is proportional to the legitimate purposes for collecting the data;
- Confidentiality: the data and the privacy policy parts not directly required for the final resolution are not disclosed.

Context

- Initiator's Privacy Policy: the privacy policy of Initiator as defined in the pattern Formally Provable Privacy Policies;
- Responder's Privacy Policy: the privacy policy of Responder as defined in the pattern Formally Provable Privacy Policies;
- Agreement: an intersection of both the Privacy Policies with excerpts relating to the issues relevant for the actual situation;
- Initiator's Negotiation Agent: an agent system capable of negotiating issues of Initiator's Privacy Policy;
- Responder's Negotiation Agent: an agent system capable of negotiating issues of Responder's Privacy Policy;
- Theorem Prover: an abstract notation for a system capable of deriving logical truths about Privacy Policy;
- Domain Model: a digital representation of the important notions with ontological relations from privacy protection;
- External Application: an abstract notation for any instance of an application which allows a Negotiation Agent to invoke a dialog with the owner of the privacy policy.

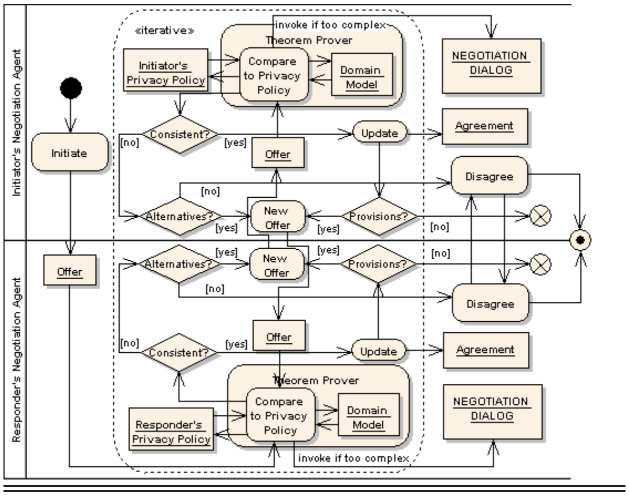
Description

The Initiator's Negotiation Agent and Responder's Negotiation Agent can automatically negotiate privacy protection issues between Initiator's and Responder's Privacy Policy. The complex reasoning for this is carried out by a Theorem Prover and associated Domain Model helps resolve the inherent semantic. The exchange of information between agents is done incrementally in packets called offers carrying only the data required to reach the final resolution and leaving the rest of the information undisclosed. In case both agree the final resolution is Agreement.

Controls

The External Application should support at least one control:
- NEGOTIATION DIALOG is a message display with appropriate controls which enable the owner of the privacy policy to interactively resolve the specific issues in negotiation that were not possible to resolve automatically.

Definition



As a follow up to the last pattern, it should be noted that Agreement should be regarded as a formal document and approved as such by legislation; it should be valid as a piece of evidence in a court case as any other formal contract is. To this end, Agreement should be archived using methods for long term trusted archiving of digital content [63].

The next pattern is about protecting identity of people in electronic transactions. It is deliberately that the very idea of digital identity on its own is not identified as a special privacy protection pattern; this is a security pattern used to identify and control what people do, whereas in privacy protection the aim is to protect the personal identifying information. Hence the following pattern proposes a special type of identity which still satisfies the security function but hides the true person behind. The Problem Situations 3, 4, 5 and 9 clearly show that the objection that such a pattern *only* supports people in illegal or illegitimate activities is far from correct. On the contrary, Problem Situation 5 shows that our personal identifying information is out there and since Problem Situations 3, 4 and 9 do happen Principle of fair and lawful processing, Finality principle and Data minimisation principle are impossible to enforce without hiding the real person behind the data disclosed in electronic transactions. The technologies required to implement this pattern range from identity federation frameworks which make possible referencing distributed personal identifying information, through protocols for data sharing and network addressing, and to anonymization models which assure unlinkability on network layer; these technologies will be referred to as the *identity infrastructure*.

This pattern isolates the personal identifiable information possible to infer out of the identity strictly to the provided information, depending on the strength of the pseudonymization. However, despite the pseudonymization such an identity can still be used for authentication and holders of such identities can still be accounted for their actions. This is possible in two ways. Either there is an authority that knows who is behind the pseudonym and can do legal interception; such a pseudonym can hide the holder and prevent Problem Situations 3 and 5 in the majority of cases with small actors in cyber crime; however, it cannot prevent Problem Situation 4 as authorities are typically involved.

Clearly, we need a way to provide people with a pseudonymous identity without possibility to trace the holder's real identity, but at the same time to prevent people to abuse them. This can be achieved through concept of *post*: a digital identity is pseudonymous to the degree whereby linking it to the true person is not possible, but in return the holder of such an identity should leave something of value (from now on referred to as *token*) at the post, but this is the only thing the holder needs to present of him/her/itself.[15] The digital identity should expire after some short amount of time; in order to get the token back or to renew the identity the holder should return to the post to do so. Meanwhile, if the digital identity in question was known to be used for illegitimate purposes, the holder can be held liable when coming to the post; if the holder does not come to the post then the token can be used to reimburse the people affected by the illegitimate uses of the identity. The token can be deposited as money, proportional to holder's income, and depending on how much money the holder has left at the post the pseudonymization can be weaker (i.e. subject to legal interception) or stronger (i.e. untraceable); for the period of time of validity of digital identity the agency running the post can make business using the money and at the revocation of the digital identity the money is returned to the holder with interest. Different agencies can compete providing better interest or better identity infrastructure.

It should also be clear that issuing a digital identity, which enables inspectors insight into parts of personal identifying information of the holder, has to be supported by appropriate access control to that information in order for the identity to be efficient: a party that was not given the identity explicitly by the holder should not have insight into the associated information. Mind also that standard measures

[14] In negotiation process also Initiator may claim data of Responder in order to aggregate enough proof for trustworthiness of Responder or to get access to Responder's resources – the process is symmetric in terms of the need for data exchange. Clearly, everything in privacy policy negotiation is about exchange of data: say one is negotiating for a service, then the service will be represented by a URI (i.e. a string of characters, thus data) so that the one can access it. Each resource in privacy policy negotiation is represented by appropriate data.

[15] That should say, one does not need to present physical appearance, real identity, bank account or any other identifying information.

for protecting integrity and confidentiality of that information are assumed to be in place using cryptography or other obfuscation techniques. These techniques do not constitute privacy protection patterns, at least they will not be identified as such in this paper; however they are important support for privacy protection and should not be neglected in realizations of privacy protection patterns. For example, before a digital identity has been issued all the data that are to be disclosed through this identity should already have been securely stored, the communications which are to be used to access these data should be protected by cryptographic protocols, and at the time the identity is defined access control should also be configured.

Virtual Identity

Actors

Person – a legal or natural person;
Inspector – a legal or natural person interested in Person;
Agency – a legal person providing Identity Infrastructure;
Authority – a legal person or other official body authorized for investigation and prosecution of cyber crime activities.

Properties

- Authenticity: demonstrates Person's credibility;
- Accountability: makes possible to hold Person liable;
- Pseudonimization: disturbs Inspector from knowing the true identity of Person;
- Unlinkability: makes hard to link the identifying information of Person outside of the directly provided data.

Context

- Person's Information: all the identifying information of Person, generally distributed on many places;
- Virtual Identity: a pseudonym of Person with references to pieces of Person's Information in function of a digital identity;
- Identity Infrastructure: a collection of technologies for federation of identity, single-sign-on, data sharing and addressing, and anonymization assuring unlinkability on network layer;
- Post: a place run by Agency where Person leaves a valuable when applying for Virtual Identity.

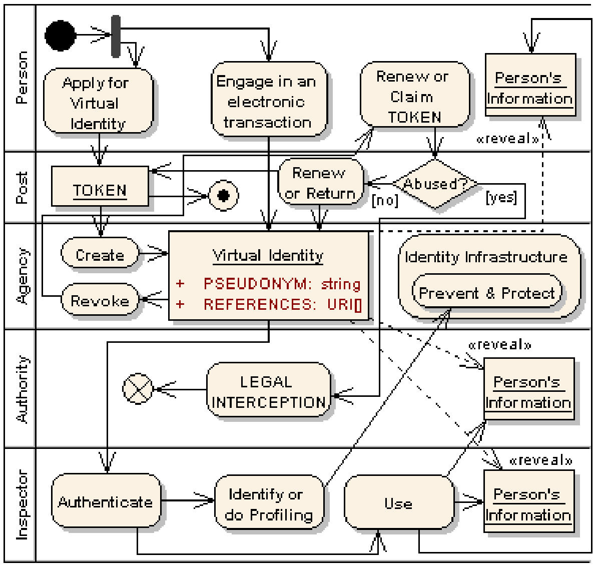
Description

Person's Information is distributed and known to public. Still, privacy protection can be achieved by using pseudonyms instead of real identities. Person can select arbitrary pseudonym and define the parts of Person's Information to be accrued to that pseudonym. This is made into a Virtual Identity and is issued by Agency after Person has left something of value at Post. Agency assures the properties of this pattern. After certain amount of time Virtual Identity expires and should be renewed by Person coming to Post. In case Person has abused Virtual Identity, Agency can withhold Person and call Authority for legal interception. When Virtual Identity is revoked, Agency has to return the valuable to Person with interest.

Controls

- PSEUDONYM is a string of characters used as the recognizing name of Virtual Identity;
- REFERENCES is a list or URIs to parts of Person's Information, packed into Virtual Identity, which represents its attributes;
- TOKEN is money deposited as valuable at Post;
- LEGAL INTERCEPTION is a procedure performed by Authority to find and prosecute the holder of Virtual Identity.

Definition



However, one of the supporting technologies for the previous pattern has for a long time been a synonym for privacy preserving internet browsing and definitelly deserves recognition as a privacy protection pattern.

Anonymizer

Actors

Person – a legal or natural person;
Inspector – a person looking for the true identity of Person.

Properties

- Anonymity: not being possible to trace the exact originator of a transaction.

Context

- Environment: a specific social or / and technical setting with infrastructure and corresponding controllers where communication between Person and Inspector is enabled;
- Anonymity Set: a collection of nodes which exhibit exactly the same traits in terms of capabilities that Environment offers Inspector for distinguishing among them;
- Anonymizer: a special technology or system which makes possible the appearance of Anonymity Set within Environment;
- Transaction: a communication between Person and Inspector carried out though use of facilities in Environment.

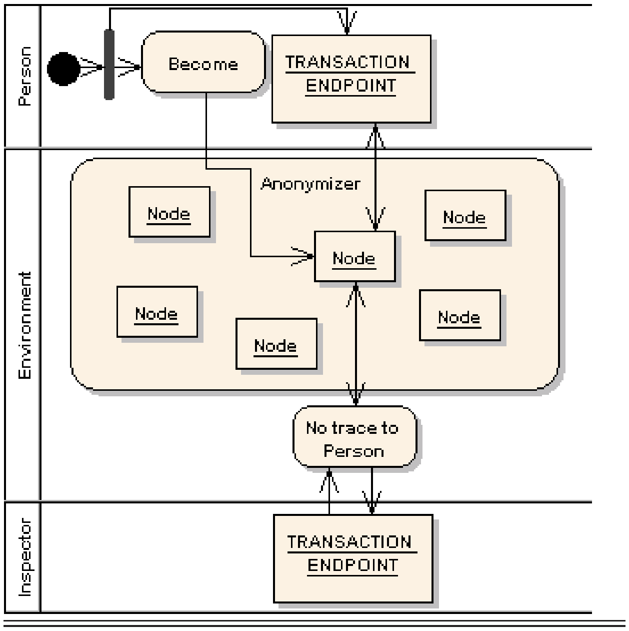
Description

In Environment Person appears as a node of Anonymity Set. Anonymizer makes impossible for Inspector to distinguish between Person and other nodes. This also implies that it is impossible for Inspector to trace, profile, or otherwise categorize objects that would make possible any kind of identification of Person inside Environment.

Controls

- TRANSACTION ENDPOINT is a system which makes possible for Person or Inspector to participate in Transaction and control it to certain extent.

Definition



Without this pattern Virtual Identity would be inefficient on the network layer since every attempt to conceal the true identity with a pseudonym could fail due to resolution of network identifiers frequently used by holder of virtual identity if they were (and normally they are) possible to trace back to the holder.

The next pattern speaks of a social model for data protection with using insurance for privacy breaches. Problematic situations, especially Problem Situation 3, have already given inspiration to some of the insurance companies[16] to think of insurance products that would "compensate for the liability arising from failure of network security protections, failure to protect or wrongful disclosure of private or confidential information, failure to protect personal identifying information from misuse or theft, or violation of any federal, state or local privacy statute alleged in connection with the failure to protect personal identifying information."[73] The products cover

- expense of third party damages and legal claims;
- fines and penalties imposed by federal, state, and local governments;
- the expense incurred in notifying customers of a breach and the cost of mitigating reputational damage done;
- expense of defense costs within policy limits;
- expense incurred repairing or cleaning up the breach; and
- expense of fines levied by banks and credit card companies due to a privacy breach.

Privacy Breach Insurance

Actors

Person – a legal or natural person;
Insurance – a legal person involved in insurance business;
Perpetrator – a person responsible for the privacy breach.

Properties

- Safety: absence of catastrophic consequences.

Context

A specific socio-technical setting which is different for every case in separate with social and technical factors such as network infrastructure, market players, technical facilities and other installations and their deficiencies which make possible the privacy breach. In all that particular Person's Data play the central role as their exploit is in the interest of Perpetrator and their protection is the aim of Insurance.

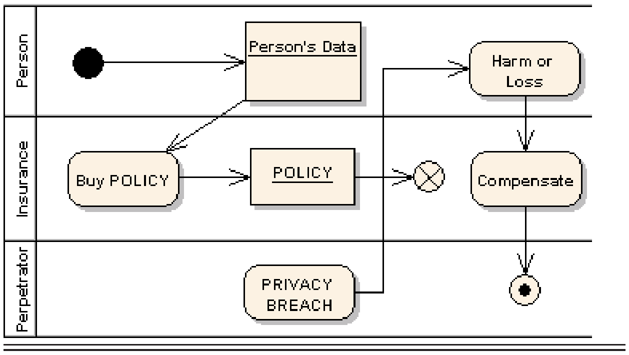
Description

At Insurance Person has bought an insurance policy for protecting Person's Data. By some device Perpetrator is able to exploit the context and gain illegitimate access or control over Person's Data. Perpetrator moreover causes harm or loss to Person by abusing Person's Data. Person can claim compensation at Insurance to cover expenses of recovering from that harm or loss.

Controls

- POLICY is a contract between Person and Insurance on the extent of protection;
- PRIVACY BREACH is an exploit of context done by Perpetrator whereby Person's Data are abused causing harm or loss to Person.

Definition



At that point it should be pointed out that all the privacy protection patterns which have been presente until now protect personal identifying information before it has been disclosed. This is referred to as *a-priori privacy protection*. As opposed to this a set of techniques is known to be able to (at least partially) protect privacy after the privacy identifying information was disclosed and are referred to as *a-posteriori privacy protection*. The remaining of the privacy

[16] cf. http://www.aig.com/Network-Security-and-Privacy-Insurance-(AIG-netAdvantage)_20_2141.html

protection patterns in this paper will focus on that last category and will close the whole cycle of privacy protection, as indicated in the introduction.

The first and probably the most important *a-posteriori* privacy protection pattern is that of a sticky policy. In this paper *sticky policy* is referred to as a fragment of Agreement as defined in pattern Privacy Policy Negotiation which pertains to an exact piece of private identifying information; such a fragment should hold only the certifying information and privacy protection rules that are somehow important for the protection of different parts of data of that piece of private identifying information. Any data without a sticky policy should be invalid and handling data without a sticky policy attached should be illegitimate.

This pattern is a prerequisite for the efficient performance of most of the following patterns of *a-posteriori* privacy protection and by this way importantly contributes to protection against some of the most problematic social situations, such as Problem Situations 4, 5 and 6. It should be clear that without such a pattern Finality principle and Time minimisation principle are impossible to enforce.

Sticky Policy

Actors

Data Subject – the person Data and Sticky Policy refer to as the subject;
Data Controller – the person which collects Data and defines purposes and ways how Data will be processed;
Data Processor – the person which actually processes Data.

Properties

- Intendment: the sense in which Data Controller should interpret Data Subject's volition about the way Data should be handled.

Context

- Data: a part of personal identifying information of Data Subject;
- Sticky Policy: a part of Agreement as defined in pattern Privacy Policy Negotiation adhering to Data;
- Data Token: the combined information made of Data and Sticky Policy and cryptographically signed by Data Subject.

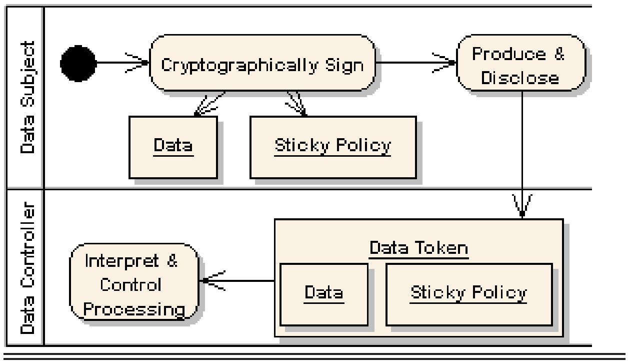
Description

Data and Sticky Policy are cryptographically signed by Data Subject and integrity of Sticky Policy adhering to Data is thus preserved in Data Token. Sticky Policy contains all the constraints and rules of how Data Processor should handle Data. Handling Data in disaccord with Sticky Policy is illegitimate.

Controls

- ENTITY identifies Data Subject;
- DATA describes Data;
- PURPOSE specifies the allowed purposes for the processing of DATA;
- RECIPIENT identifies allowed recipients of DATA;
- RETENTION indicates the kind of retention admissible for DATA;
- OPERATIONS defines the operations allowed on DATA;
- OBLIGATIONS states how Data Controller and Data Processor should protect DATA when handling them.

Definition



The next pattern can be of a great value when preserving Problem Situations 3, 4 and 5. Also Time minimisation principle or other forms of limitation of insight into data have a straightforward enforcement in this pattern. Technologies that support it have been outlined at the end of Section 3.

Privacy Preserving Data Processing

Actors

Data Subject – the person Data refer to;
Data Controller – the person which collects Data and stores them into Data Base;
Data Processor – the person which processes Data on behalf of Data Controller.

Properties

- Confidentiality: complete or selective hiding of data required for producing the final result of processing.

Context

- Data: a part of personal identifying information of Data Subject or other data owned by Data Processor;
- Data Base: the place where Data are stored at Data Controller, res. Data Processor, but under authority of Data Controller.

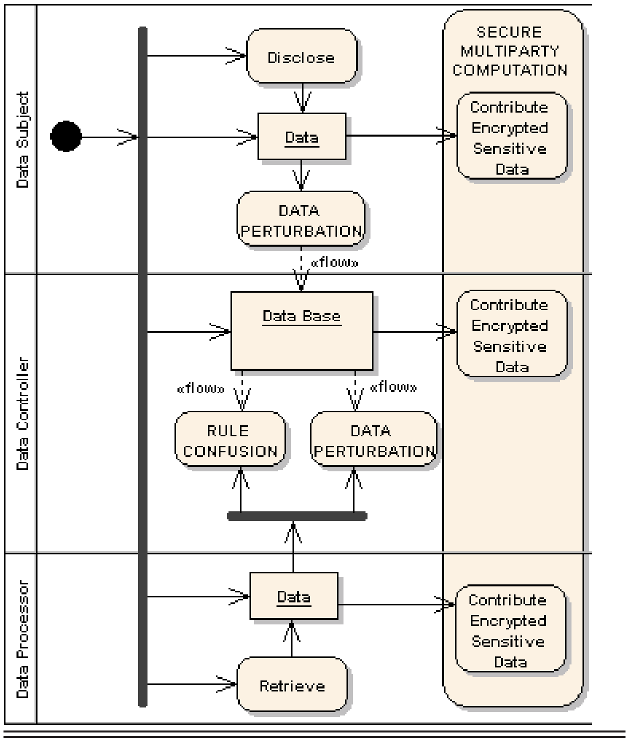
Description

Privacy of Data can be preserved at different stages before or at the actual time of processing. The first stage is at the disclosure of Data by Data Subject or Data Controller when DATA PERTURBATION can be used. The second stage is when Data are released to Data Processor from Data Base and at that point Data Controller can use RULE CONFUSION. The last stage is at the point of processing when SECURE MULTIPARTY COMPUTATION can be used.

Controls

- DATA PERTURBATION enables perturbation of Data so that their actual values are obfuscated, yet techniques exist which enable Data Processor to produce results of processing based on perturbed data of comparable quality as those obtained from the original Data;
- RULE CONFUSION makes possible truncation of data which gives Data Processor less cues to categorize raw Data and infer rules about their implicit associations, thus disabling Data profiling and deduction of sensitive personal identifying information, however this proportionally degrades the quality of results of processing;
- SECURE MULTIPARTY COMPUTATION enables parties to contribute encrypted or otherwise obfuscated Data to a processing which is capable to produce the same results out of these Data as though they were not obfuscated.

Definition



The following pattern describes one of the most typical data protection techniques, namely that of access control as described at the end of Section 3. The pattern, though, will try to introduce the idea of sticky policy into the decision process for controlling access. In such a setting this pattern is a strict precondition for almost any other privacy protection pattern, since without a close control which data and under what conditions and purposes are disclosed to whom also patterns such as Virtual Identity, Privacy Policy Negotiation or Sticky Policy have no actual effect.

Many problem situations need direct protection against intrusion in private data which this pattern can offer. Protection against Problem Situations 3, 4, 5, 6 and 7 can only be achieved with such a pattern in place and legal principles such as Finality principle, Data minimisation principle and Principle of right to object processing of personal data without this pattern have no definite power.

Access Control

Actors

Resource Controller – the person which controls access to Resource;
Requester – the person which requests Resource.

Properties

- Authorization: access to Resource is authorized according to predefined rules.

Context

- Resource: a particular resource requested by Requester;
- Access Control List: a list of requesters and their privileges to access resources;
- Credential: a piece of data encoding a voucher which somehow entails that Requester is entitled to access Resource;
- Sticky Policy: sticky policy adhering to Resource as defined in pattern Sticky Policy;
- Enforcement Point: the part of access control at the side where Resource is available;
- Decision Point: the part of access control where the decision about access to Resource is taken.

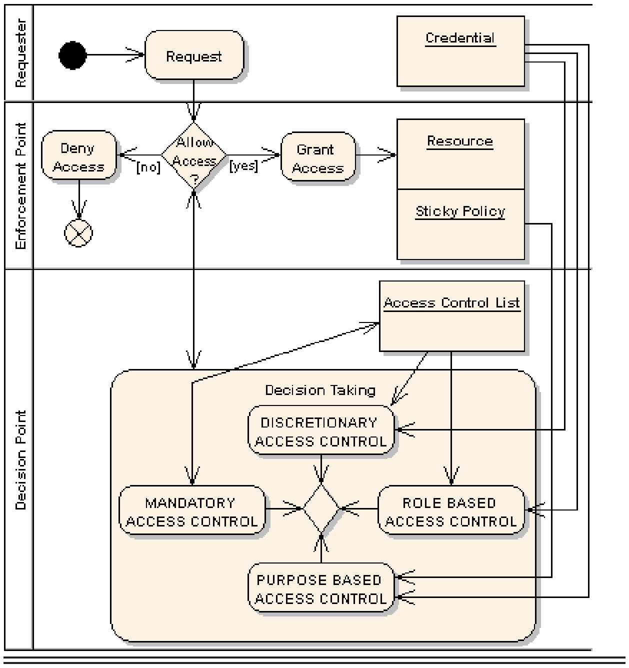
Description

Requester requests Resource at Enforcement Point which is in position to give access to Resource. However, for each type of resource a different Enforcement Point has to be implemented. Decision Point on the other hand can be centralized because decision can be taken based on formal methods and categorization of different types of resources, without need to know the special handling of each type of resource. Upon request Enforcement Point asks Decision Point whetehr access to Resource for Requester is allowed and if yes, then Enforcement Point enables Requester to use Resource. Decision is produced based on four different possible decision methods as described in **Controls** section.

Controls

Controlling that pattern is achieved through decision methods used by Decision Point, the four of them that have been used so far are:
- DISCRETIONARY ACCESS CONTROL enables granting access to Resource for Requester by defining this in Access Control List or by checking appropriate Credential of Requester;
- MANDATORY ACCESS CONTROL enables exact evaluation of sensitivities assigned to Requester and Resource as defined in Access Control List for the decision on whether Requester's sensitivity justifies access to Resource;
- ROLE BASED ACCESS CONTROL enables comparison of role of Requester, explicated by a suitable Credential, to permissions for accessing Resource as defined in Access Control List;
- PURPOSE BASED ACCESS CONTROL enables comparing purposes Requester shows by Credential stating Requester's legitimate business interests (or other kind of activities) to the actions allowed on Resource by Sticky Policy.

Definition



When data are processed, a record of all the actions and their committers should be preserved for later reference. On suspicion of abuse authorities should be able to access the logs and perform auditing. This can be achieved in two advancing levels of sophistication. On the basic level a record of the requester, the purpose or other inquiry related meta information, the time and the actual data requested should be taken at the point of access to the data by access control. It should be clear, however, that after this the data processor can freely ignore the sticky policy and handle data in disaccord with the data subject's will. This can be prevented by a notably more rigorous approach where data are held entirely in encrypted form and for any operation special trusted hardware modules (e.g. special hardware provided by trusted producers) have to be used that are able to perform computation based on techniques of secure multiparty computation or privacy homomorphisms as discussed at the end of Section 3. Using appropriate cryptosystems when encrypting data at disclosure data processors would be forced to design their software to make use of the application programming interface of trusted hardware module, because they would be unable to perform these operations themselves. This way data could only be processed using such trusted hardware modules which could then actually take records of details about who requested the operation, what was the operation, at which time and on what data it was performed, and whether this was in accord with sticky policy.

As it was pointed out at the end of Section 3 the techniques used for computing privacy homomorphisms may lead to severe message expension and this opens questions about feasibility of the second sophistication level. Nevertheless, there exist several efficient privacy homomorphism operations and other techniques from secure multiparty computation and, moreover, research could be done for optimization of complex parts in order to make possible entirely encrypted processing. Thus the second complexity level will be regarded as an interesting prospect and as a necessary conceptual part of the following pattern.

This pattern has potential to greatly mitigate Problem Situations 4 and 7, actually prosecution in case of any problematic situation can only be efficient with such an evidence in place. This evidence can be used in courts to prove violations of data protection principles in general.

Privacy Audit Trail

Actors

Data Subject – the person Data refer to;

Data Controller – the person which collects Data and defines rules for their processing;

Data Processor – the person which processes Data on behalf of Data Controller.

Properties

- Accounting: the ability to hold Data Processor liable for their actions;
- Auditing: the possibility to have insight into the actions of Data Processor.

Context

- Data: a particular data processed by Data Processor;
- Sticky Policy: the sticky policy, as defined in the pattern Sticky Policy, adhering to Data;
- Access Control: a component enabling control of access to data as defined in pattern Access Control;
- Trusted Hardware Module: a piece of hardware capable of secure encryption and decryption and running protocols for various operations based on techniques of secure multiparty computation and privacy homomorphisms;
- Log: a part of Trusted Hardware Module or Access Control where details of every operation performed on data are recorded, such as the requester, the action, and the time.

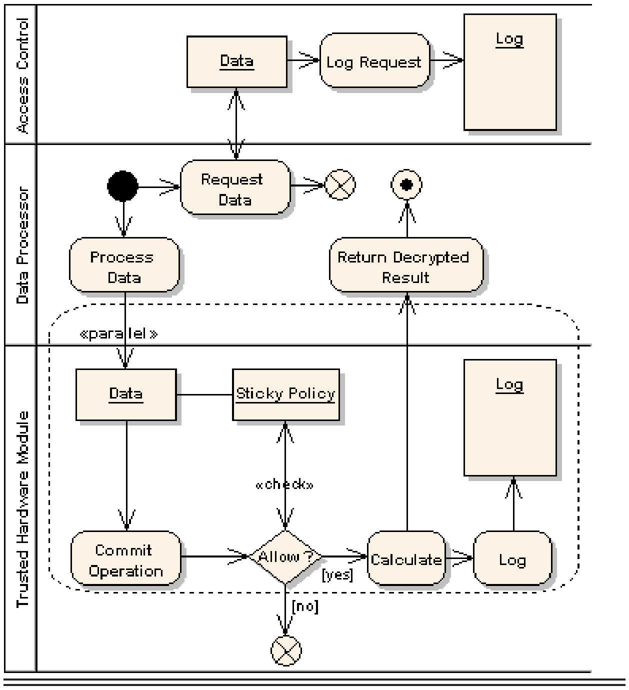
Description

At every request for Data Access Control logs Data Processor, the purpose, role, credentials, or other meta information, the time and the actual Data requested. Every processing of Data must be carried out by use of Trusted Hardware Module which logs the kind of operation, whether it was in accord with Sticky Policy, the Data Processor, the time and other important information. If the operation is in accord with Sticky Policy then the operation is performed. When Data are processed inside Trusted Hardware Module, they are kept in an encrypted form and special protocols enable processing despite their encrypted form; result is returned to Data Processor in a decrypted form.

Controls

Pattern changes behaviour depending on Sticky Policy.

Definition



The last pattern suggests a very social model for protecting privacy, namely that of a cyber police and prosecution through civil court. It should be clear that, ultimately, privacy can not be protected unless if legal frameworks and prosecution are not an integral part of the whole privacy protection paradigm.

Privacy Breach Prosecution

Actors

Perpetrator – the person who treats Data in disaccord with Sticky Policy;

Authorities – the agency or state department authorized to prosecute Perpetrator.

Properties

- Prosecutability: the ability to conduct criminal proceedings in court against Perpetrator.

Context

- Data: a particular data processed by Data Processor;
- Sticky Policy: the sticky policy as defined in pattern Sticky Policy adhering to Data;
- Privacy Audit Trail: logs obtained from privacy auditing as described in pattern Privacy Audit Trail.

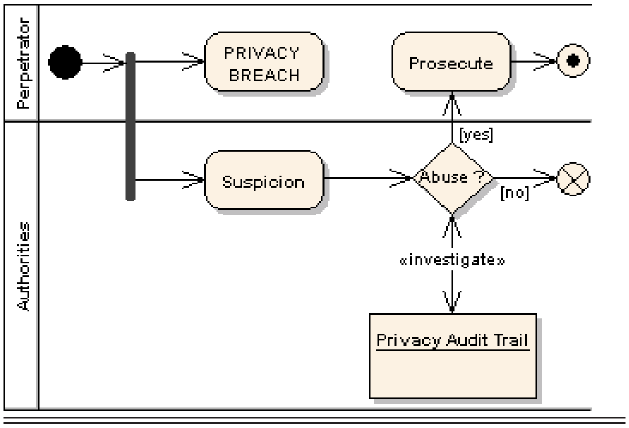
Description

When there exists a justified suspicion that Perpetrator has abused Data Authorities should collect relevant Privacy Audit Trail and check Perpetrator's actions regarding Data. In case Perpetrator really has abused data Authorities will prosecute Perpetrator.

Controls

- PRIVACY BREACH is an exploit of context done by Perpetrator whereby Data are handled in disaccord with Sticky Policy.

Definition



5. Privacy Protection Cycle

The proposed patterns can be combined into a higher order integration scheme showing how the patterns should be deployed in a real situation to make possible a systemic privacy protection. This integration scheme is referred to as the *privacy protection cycle* and is represented by the diagram on Figure 1.

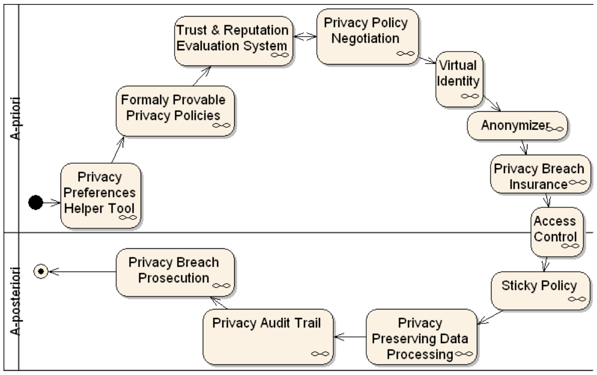

A-priori
Trust & Reputation Evaluation System
Privacy Policy Negotiation
Virtual Identity
Formaly Provable Privacy Policies
Anonymizer
Privacy Breach Insurance
Privacy Preferences Helper Tool
Access Control
A-posteriori
Privacy Breach Prosecution
Sticky Policy
Privacy Audit Trail
Privacy Preserving Data Processing

Figure 1. Integration scheme for privacy protection cycle

It should be noted that External Application of Privacy Preferences Helper Tool pattern was actually meant to be the Negotiation Agent of Privacy Policy Negotiation pattern; on the other hand, External Application of Privacy Policy Negotiation is Privacy Preferences Helper Tool. There are many more important correlations between patterns implied in privacy protection cycle. First of all, Privacy Policy Negotiation, although this was not explicitly mentioned in that pattern, should reflect on the level of reputation of peer when processing offers against privacy policy; privacy protection rules inside the privacy policy (e.g. subject to OBLIGATIONS) should define the level of reputation peer should meet in order to be allowed access to the resource; this way, if the reputation of data controller or processor would be too low, they would be refused at privacy policy negotiation time and automatically demand for their services would fall. This is the indispensable correlation between Trust & Reputation Evaluation System and Privacy Policy Negotiation if it should be possible to penalize misbehaving data processors or controllers automatically based on lower trust in electronic transactions. Close to this is another correlation which is that Authority of Trust & Reputation Evaluation System pattern could actually be Insurance of Privacy Breach Insurance pattern, because for Insurance it will be mandatory to be involved in investigations of privacy breaches; moreover, not only that Perpetrator of Privacy Breach Insurance should be blamed and their reputation lowered, but also if they were insured against abuse of private identifying information, then they should pay more for POLICY.

A more intuitive and illustrative presentation of privacy protection cycle is given on Figure 2. In this paper authors maintain that no weaker or partial scheme can be sufficient for actually protecting privacy of people given the facts pointed out in Subsection 2.2. Only a very systemic scheme where technologies and social models cooperate to make a total cover up of potential privacy threats can be regarded as a prospect towards a future where our private identifying information will be respected and the tremendous potential and capabilities of information technology for its exploitation regulated to the extent where the abuse in all its expressions will become an unlikely experience.

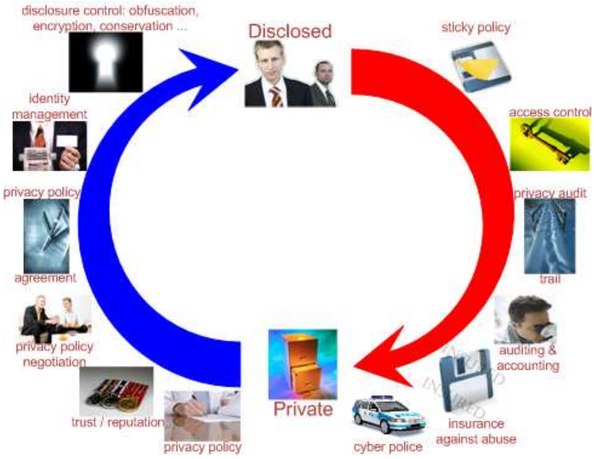


Figure 2. Intuitive representation of privacy protection cycle

6. Conclusions

A close look at the situation regarding protection of privacy shows that privacy related problems already are – and will in future become even more – a real and serious social problem. A thorough review of the state-of-the-art and existing research on the field of privacy protection reveals quite a rich assortment of potentially very powerful techniques for protecting privacy, but unfortunately legislation does not acknowledge them and brings no central organization into the field of privacy protection. Public initiatives and technologies which could potentially answer them are kept separated and social, legal and administrative frameworks that could promote and back up the technologies have not been established.

Authors of this paper believe that technologies have reached the point where most of the privacy protection patterns described in this paper can be implemented in their full potential and that the obstruction lies in the fact that there is no commercial interest in producing the kind of technology whatsoever on the current information technology market. This in turn owes much to the deficiency of privacy protection related legislation, which does not require of data controllers and processors to implement concrete schemes for privacy protection. For an illustration, if one takes Finality principle, it would make a lot of difference if instead of saying that

> *“Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes,”*

regulation would additionally demand that

> *“Prior to processing of personal data Privacy Policy Negotiation pattern should be implemented on the part of data collection and any subsequent disclosure of data should be done with respect to Sticky Policy pattern and Privacy Audit Trail pattern should be implemented on the part of data processing.”*

This way data controllers and data processors would be obliged to install in their information systems the software implementing the required privacy protection patterns which would create a real demand for such kind of software on information technology market. In this same light concepts such as virtual identity, privacy breach insurance or privacy preserving data processing would be given their exact and compelling legal formulations and regulation would actually fulfill its part in making privacy protection cycle a reality for the society.

References

[1] T. Otter, "Data protection law: The Cinderella of the software industry?" Computer law & security report 23, 2007, pp. 67-72.

[2] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L No.281, 23.11.1995.

[3] Y. Punie, S. Delaitre, I. Maghiros, D. Wright, (eds.) "Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities," SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. http://swami.jrc.es

[4] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.11.1950.

[5] Convention on Cybercrime, Budapest, 23.11.2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[6] DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178/1, 17.7.2000.

[7] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities L 201/37, 31.7.2002.

[8] Privacy Bird. http://www.privacybird.org

[9] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," World Wide Web Consortium Recommendation, April 2002. http://www.w3.org/TR/P3P/

[10] L. Cranor, M. Langheinrich, and M. Marchiori, "A P3P Preference Exchange Language 1.0 (APPEL1.0) W3C Working Draft," 2002.

[11] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, "Enterprise Privacy Authorization Language (EPAL 1.2) specification submitted to W3C," 2003. http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

[12] T. Moses, "eXtensible Access Control Markup Language 3 (XACML), Version 2.0," OASIS eXtensible Access Control Markup Language Committee Specification, 1 Feb 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[13] SAML. http://saml.xml.org/saml-specifications

[14] F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, P. F. Patel-Schneider: The Description Logic Handbook: Theory, Implementation, Applications. Cambridge University Press, Cambridge, UK, 2003. ISBN 0-521-78176-0

[15] OWL Web Ontology Language Overview, W3C Recommendation 10 February 2004. http://www.w3.org/TR/owl-features/

[16] http://kaon.semanticweb.org/

[17] http://kaon2.semanticweb.org/

[18] Travis Leithead, Wolfgang Nejdl, Daniel Olmedilla, Kent E. eamons, Marianne Winslett, Ting Yu, and Charles C. Zhang: "How to Exploit Ontologies in Trust Negotiation," ISWC – Workshop on Trust, Security, and Reputation on the Semantic Web, Hiroshima, Japan, November 7, 2004.

[19] Valentina Tamma, Michael Wooldridge, Ian Dickinson: "An Ontology Based Approach to Automated Negotiation," proceedings of the Fourth International Workshop on Agent-Mediated Elctronic Commerce (AMEC-2002), Bologna, Italy, July 2002.

[20] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, G. Lenzini, "Audit-based compliance control," International Journal of Information Security archive, Volume 6, Issue 2, Pages: 133 – 151, March 2007.

[21] S. Etalle, W. H. Winsborough, "A Posteriori Compliance Control," 12^{th} ACM Symposium on Access Control Models and Technologies (SACMAT), 20-22 June 2007, Nice, France. pp. 11 – 20.

[22] M. D'Agostino, D. Gabbay, R. Haehnle, J. Posegga (Eds), "Handbook of Tableau Methods," Kluwer,1999.

[23] J. Alan Robinson, "A Machine-Oriented Logic Based on the Resolution Principle," Journal of the ACM (JACM), Volume 12, Issue 1, pp. 23-41.

[24] http://www.cs.unm.edu/m̃ccune/otter/

[25] http://coq.inria.fr/

[26] Term Rewriting and All That. (1999) Baader, F. and Nipkow, T. Cambridge University Press.

[27] First Order Logic and Automated Theorem Proving. (1996) Fitting, M. Springer Verlag.

[28] http://owl.man.ac.uk/factplusplus

[29] http://www.mindswap.org/2003/pellet/index.shtml

[30] http://dl.kr.org/dig/

[31] http://jena.sourceforge.net/

[32] M. Nielsen, K. Krukow, "Towards a Formal Notion of Trust," PPDP'03 August 27-29, 2003, Uppsala, Sweden.

[33] A. Jøsang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 9, No. 3 (June 2001).

[34] A. Jøsang, R. Ismail, C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, 43(2), pages 618-644, March 2007.

[35] A. Jøsang, R. Hayward, S. Pope, "Trust Network Analysis with Subjective Logic," (ACSC2006), Hobart, Tasmania, Australia, January 2006.

[36] M. Carbone, M. Nielsen, V. Sassone, "A Formal Model for Trust in Dynamic Networks," In Proc. of International Conference on Software Engineering and Formal Methods (SEFM 2003), p. 54 – 63.

[37] M. Richardson, R. Agrawal, P. Domingos, "Trust Management for the Semantic Web," in Proceedings of the Second International Semantic Web Conference 2003, p. 351 – 368.

[38] Todd Barlow, Adam Hess, Kent E. Seamons: "Trust Negotiation in Electronic Markets," proceedings of the eighth research symposium on emerging electronic markets (RSEEM 01), Maastricht, The Netherlands, September 16-18, 2001.

[39] Wolfgang Nejdl, Daniel Olmedilla, and Marianne Winslett: "PeerTrust: Automated Trust Negotiation for Peers on the Semantic Web," proceedings of Secure Data Management, VLDB 2004 Workshop, Toronto, Canada, August 30, 2004.

[40] C.A. Ardagna, E. Damiani, S. De Capitani di Vimercati, and P. Samarati: "Towards Privacy-Enhanced Authorization Policies and Languages," in Proc. of the 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (IFIP), Nathan Hale Inn, University of Connecticut, Storrs, USA, August 2005.

[41] K. Dolinar, "Daidalos Deliverable DII-A451, Architecture and Design: Security and Privacy for Pervasive Systems," DAIDALOS FP6 project consortium, 2006.

[42] J. Miller, "Yadis Specification, Version 1.0." The Identity and Accountability Foundation for Web 2.0, 18 March 2006. http://yadis.org/papers/yadis-v1.0.pdf

[43] OpenID. http://openid.net/

[44] Light-Weight Identity. http://lid.netmesh.org/wiki/Main_Page

[45] D. Reed, D. McAlpin, "Extensible Resource Identifier (XRI) Syntax, V2.0," OASIS Extensible Resource Identifier (XRI) Committee Specification, 14 November 2005. http://www.oasis-open.org/committees/download.php/15377/xri-syntax-V2.0-cs.pdf

[46] D. Reed, M. Sabadello, P. Trevithick, "The XDI RDF Model V11," OASIS XRI Data Interchange Comitee Specifications, 21. 10. 2008. http://www.oasis-open.org/committees/download.php/29748/xdi-rdf-model-v11.pdf

[47] Simple eXtensible Identity Protocol. http://www.sxip.com/background

[48] Project Liberty. http://www.projectliberty.org/

[49] T. Wason, "Liberty ID-FF Architecture Overview," Version: 1.2-errata-v1.0.

[50] Shibboleth Initiative. https://spaces.internet2.edu/display/SHIB/WebHome

[51] Michael B. Jones, "A One-Page Introduction to Windows CardSpace," MSDN, Microsoft Corporation, January 2007. http://msdn.microsoft.com/sl-si/netframework/cc196951(en-us).aspx

[52] Higgins trust framework. http://www.eclipse.org/higgins

[53] J. Camenisch, A. Shelat, D. Sommer, S. Fischer-Hbner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, J. Tseng, "Privacy and Identity Management for Everyone," in ACM DIM 2005. http://www.zurich.ibm.com/%7Ejca/papers/cssf05.pdf

[54] A. Pfitzmann, M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology," version 0.31, Feb 15 2008. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[55] S. Fischer-Hübner, C. Andersson, "PRIME Deliverable: D14.0a – Framework V0," version 6, June 2005.

[56] D. Goldschlag, M. Reedy, P. Syversony, "Onion Routing for Anonymous and Private Internet Connections," Communications of the ACM, vol. 42, num. 2, February 1999. http://www.onion-router.net/Publications/CACM-1999.pdf

[57] M. Reiter, A. Rubin, "Crowds: Anonymity for Web Transactions," ACM Transactions on Information and System Security 1 (1), 23 November 2005. http://avirubin.com/crowds.pdf

[58] Tor: anonymity online. https://www.torproject.org/

[59] V. C. Hu, D. F. Ferraiolo, D. R. Kuhn, "Assessment of Access Control Systems," USA National Institute of Standards and Technology, Interagency Report 7316, September 2006. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[60] Ji-Won Byun, E. Bertino, N. Li, "Purpose Based Access Control of Complex Data for Privacy Protection," SACMAT05, June 1-3, 2005, Stockholm, Sweden.

[61] N. F. Johnson, S. Jajodia, "Exploring steganography: Seeing the unseen," Computer (1998A) 31(2):26-34. http://www.jjtc.com/pub/r2026.pdf

[62] R. Wishart, K. Henricksen, J. Indulska, "Context obfuscation for privacy via ontological descriptions," 1^{st} International Workshop on Location- and Context-Awareness (LoCA), volume 1678 of Lecture Notes in Computer Science, pages 276-288, Springer, 2005. http://henricksen.id.au/publications/LoCa05.pdf

[63] A. J. Blazic, "Long Term Trusted Archive Services," First International Conference on the Digital Society (ICDS'07), pp.29, 2007.

[64] Ronald L. Rivest, Len Adleman, Michael L. Dertouzous, "On data banks and privacy homomorphisms." In Richard. A. Demillo, David P. Dobkin, Anita K. Jones, and Richard J. Lipton, editors, "Foundations of Secure Computations," pages 169-177. Academic Press, New York, 1978.

[65] Kevin Henry, "The Theory and Applications of Homomorphic Cryptography." A thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Master of Mathematics in Computer Science Waterloo, Ontario, Canada, 2008.

[66] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Hippocratic Databases," in VLDB, 2002, pp. 143 – 154.

[67] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, Y. Theodoridis, "State-of-the-art in Privacy Preserving Data Mining," SIGMOD Record, Volume 33, 2004.

[68] R. Agrawal, R. Srikant, "Privacy-Preserving Data Mining," ACM SIGMOD 2000 5/00 Dallas, TX, USA.

[69] D. Agrawal, C. C. Aggarwal, "On the Design and Quantification of Privacy Preserving Data Mining Algorithms," PODS 2001, Santa Barbara, California, USA.

[70] C. Bryce, M.A.C. Dekker, S. Etalle, D. Le Métayer, F. Le Mouël, M. Minier, J. Moret-Bailly, S. Ubéda, "Ubiquitous Privacy Protection," PRIAM Position Paper.

[71] G. Karjoth, M. Schunter, M. Waidner, "Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data," 2^{nd} Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science. Springer Verlag, 2002.

[72] Activity Diagram, "UML 2.0 Superstructure Specification," Object Management Group, August 2003, p. 280.

[73] Jamey Heary, "Privacy Breach Insurance; new solution for mitigating the risk of credit card and identity breaches," Cisco Security Expert on Tue, 03/18/08. http://www.networkworld.com/community/node/26132

A. Corroborations for Problem Situations

The following is a list of references to real affairs supporting the problem situations from subsection 2.2.

[4] There are known court cases for that problem: In Halford v. United Kingdom (27 May 1997), the Court introduced the criterion of the "reasonable expectations of privacy". Miss Halford, a senior officer whose telephone calls were intercepted without warning, was granted privacy protection in her office space, although not absolute.

[5] cf. Zeller, Tom Jr., "Black Market in Stolen Credit Card Data Thrives on Internet", The New York Times, 21 June 2005: "A 'dump', in the blunt vernacular of a relentlessly flourishing online black market, is a credit card number. And what Zo0mer is peddling is stolen account information - name, billing address, phone - for Gold Visa cards and MasterCards at $100 apiece."
Vijayan, Jaikumar, "ID Theft Continues to Increase. More than 13 million Americans have been victimized, new study reveals," Computerworld, 30 July 2003. http://www.pcworld.com/news/article/0,aid,111832,00.asp
Zetter, Kim, "TSA Data Dump Leads to Lawsuit", Wired News, 14 July 2005. http://www.wired.com/news/privacy/0,1848,68560,00.html

[6] See Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling," The New York Times, 1 Oct 2005. The story reports cases where victims have been trying to overcome the consequences of identity theft for more than two years: "Victims are still left with the unsettling realization that the keys to their inner lives as consumers, as taxpayers, as patients, as drivers and as homeowners have been picked from their pockets and distributed among thieves."
cf. Solove, p. 110: "Identity theft can be a harrowing experience. According to estimates, a victim typically spends over two years and close to 200 hours to repair the damage that identity theft causes." And p. 110: "Most identity thefts remain unsolved. Research firm Gartner Inc estimates that less than 1 in 700 instances of identity theft result in a conviction."

[7] cf. OHarrow, Robert, No Place to Hide, p. 124: "LexisNexis, a subsidiary of the UK-based Reed Elsevier Group, maintains billions of records, including media reports, legal documents, and public records collected from thousands of sources around the world."
cf. OHarrow, p. 34: "Acxiom is not a household name. But as a billion-dollar player in the data industry, with details about nearly every adult in the United States, it has as much reach into American life as Pepsi or Goodyear. You may not know about Acxiom, but it knows a lot about you."
cf. OHarrow, p. 49: "'InfoBase Enhancement' enables Acxiom to take a single detail about a persons and append, on behalf of its customers, a massive dossier. This generally happened without the individual every knowing about it."
cf. Perez, E.: "Identity theft puts pressure on data sellers," The Wall Street Journal, 21 February 2005. http://www.post-gazette.com/pg/05052/460233.stm. A recent breakout: "Company ChoicePoint actually sold 145.000 peoples personal information to Nigerian scammers."

[8] cf. Safire, William, "Goodbye To Privacy", The New York Times, 10 April 2005: "Of all the companies in the security-industrial complex, none is more dominant or acquisitive than ChoicePoint of Alpharetta, Ga. This data giant collects, stores, analyzes and sells literally billions of demographic, marketing and criminal records to police departments and government agencies that might otherwise be criticized (or defunded) for building a national identity base to make American citizens prove they are who they say they are."

[9] See, for example, OHarrow, p. 222: "HNC monitors 90 per cent of all credit cards in the United States and half of those in the rest of the world using artificial intelligence to seek out indications of fraud and deceit."
Solove, Daniel J, The Digital Person, p. 20: "Wiland Services has constructed a database containing over 1,000 elements, from demographic information to behavioural data, on over 215 million people."
Tuohey, Jasey, "Government Uses Color Laser Printer Technology to Track Documents. Practice embeds hidden, traceable data in every page printed", 22 November 2004. http://www.pcworld.com/news/article/0,aid,118664,00.asp. See also Jardin, Xeni, "Your Identity, Open to All", Wired News, 6 May 2005. http://www.wired.com/news/privacy/0,1848,67407,00.html

[10] Singel, Ryan, "Nun Terrorized by Terror Watch", Wired News, 26 September 2005. http://www.wired.com/news/privacy/0,1848,68973,00.html

[11] cf. OHarrow, p. 48: "For years, the credit bureaus had been dogged by complaints. Information in their reports was chronically incorrect. They routinely failed to correct mistakes, and seemed arrogant when individuals called."

[12] Krebs, Brian, "Hacked Home PCs Fueling Rapid Growth in Online Fraud", Washington Post, 19 September 19 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091900026_pf.html