Privacy Control for E-Services Using Selective Disclosure and Smart Cards

George Yee, Larry Korba, and Ronggong Song
Institute for Information Technology
National Research Council Canada
{George.Yee, Larry.Korba, Ronggong.Song}@nrc-cnrc.gc.ca

Abstract

The growth of the Internet has been accompanied by the growth of e-services (e.g. e-commerce, e-health). This proliferation of e-services and the increasing regulatory and legal requirements for personal privacy have fueled the need to protect the personal privacy of e-service users. Existing approaches for privacy protection include data anonymization, the use of pseudonym technology, and the use of personal privacy policies along with appropriate compliance mechanisms. These approaches are all predicated on the e-service provider having possession and control over the user's private data. In this paper, we propose a new paradigm for protecting personal privacy in e-services: keeping possession and control over the user's private information in the hands of the user with the help of a trusted authority, removing this possession and control from the e-service provider. This is accomplished with the use of selective disclosure and smart cards, in conjunction with personal privacy policies. The smart cards are provided by a trusted authority. We begin by examining privacy legislation to derive the necessary content of personal privacy policies. We then propose a framework for using selective disclosure and smart cards to protect privacy and analyze the security vulnerabilities of our approach.

1. Introduction

1.1. Privacy

In order for e-services to be successful, private information submitted to an e-service must be protected. Various approaches have been used to protect private information, including data anonymization and pseudonym technology.

Data anonymization [1,2] involves processing the private information so that it is indistinguishable from private information belonging to other people, thus removing the risk of identifying the owner of the private information, effectively rendering the information non-private. Data anonymization has been applied in networking to remove privacy concerns in the tracing of packets [3]. It has also been used to provide anonymous network communication [4]. Data anonymization is a contentious issue in data mining, where the question is how much anonymization can be done without rendering the information useless for data mining purposes [5]. Healthcare data has indicated another problem for data anonymization, where the linking of remaining data (e.g. hospitalization dates and disease) after anonymization can lead to the identification of the data owner [6]. Such identification depends on the effectiveness of the anonymization algorithm, the amount of data left after anonymization, the size of the candidate population from which a candidate owner of the data can be selected, and the linkability of the owner's data from diverse sources [2, 6]. By maximizing the size of the candidate population (entire Internet community), improving the effectiveness of the anonymization algorithm, and limiting the amount of personal information needed (e.g. limiting application to a particular class of e-services that does not require much personal information) data anonymization for e-services can be made largely immune to this problem.

Pseudonym technology [7] allows a user to access an e-service using a pseudonym (like an alias) instead of his/her real name, while still allowing the e-service to authenticate him/her as a valid user. We do not require pseudonym authentication in this work.

Pseudonym technology differs from data anonymization in that pseudonym technology hides the user from the start and provides user authentication whereas data anonymization hides the user's already existing personally identifiable data.

Less mature approaches (i.e. those in the research stage) for privacy protection include treating privacy protection as an access problem and then bringing the tools of access control to bear for privacy control [8], treating privacy protection as a privacy rights management problem using the techniques of digital rights management [9], and considering privacy protection as a privacy policy compliance problem, verifying compliance with secure logs [10]. As defined by Goldberg in 1997 [11], privacy refers to the ability of individuals to

control the collection, retention, and distribution of information about themselves. In keeping the control of private data in the hands of the owner of the data and a trusted authority, our approach is consistent with this definition.

Smart cards have been around for over 3 decades and have been applied across many domains including e-commerce [12, 13]. Their computational, memory, and security features make them ideal for portable data applications requiring security [13]. Smart cards have been applied in networked applications [14], including web-based medical information systems [15] and distributed information systems [16]. Our use of smart cards in this work is also network-based.

Our approach in this work uses selective disclosure of the user's information and a smart card in conjunction with the user's personal privacy policy to keep *control* of the user's private data in the hands of the user and a trusted authority rather than in the hands of the provider. Selected disclosure is related to anonymization and may also suffer from the potential identification of the information owner based on the information disclosed. We consider this below.

1.2. E-Services

An e-service for the purposes of this paper is characterized by the following attributes:

- The service is performed by application software (service processes) that is owned by a provider (usually a company); the service is accessible across the Internet.
- The provider's service processes can make use of the service processes of other providers in order to perform its service; in this case, the provider is also a consumer.
- A provider can have more than one e-service.
- The provider has a privacy policy that spells out what consumer private information is needed to perform the service and how the private information will be handled.
- The service is consumed by a person or another application accessing the service across the Internet.
- The consumer also has a personal privacy policy that defines what private information he is willing to give up and how that information is to be handled by the provider.
- There is usually a fee that the consumer pays the provider for use of the service.

Examples of current e-services are Amazon.com (online retailer), optionsxpress.com (online stockbroker), and WebMD.com (health information and technology solutions provider). Figure 1 shows a network view of an e-service.

The rest of this paper is organized as follows. Section 2 examines privacy legislation to derive necessary content for a personal privacy policy. Section 3 presents our framework for using selective disclosure and smart cards to protect consumer private information. Section 3 also discusses security measures in our approach and presents a security vulnerability analysis focused on our security measures. Section 4 gives an example of applying our approach to an e-service. Finally, Section 5 presents our conclusions and plans for future research.

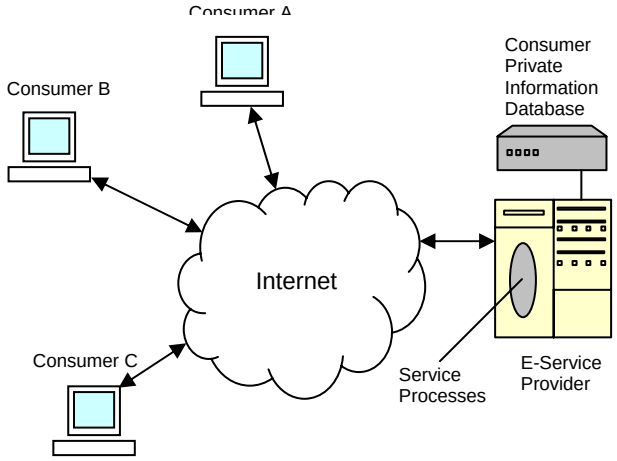

Figure 1. Network view of an e-service

2. Personal privacy policies

As mentioned above, our approach for privacy protection makes use of personal privacy policies. It is therefore necessary to define the content of a personal privacy policy. We examine privacy legislation to obtain necessary (because it's the law) content.

2.1. Privacy Legislation

To protect consumer privacy, legislative bodies in many countries have enacted legislation that define personal information and spell out the obligations of the service provider with respect to consumer privacy. In Canada, privacy legislation is enacted in the *Personal Information Protection and Electronic Documents Act* [17] and is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* [18] recognized as a national standard in 1996. This Code consists of ten Privacy Principles that for convenience, we label as CSAPP. Data privacy in the European Union is governed by a very comprehensive set of regulations called the Data Protection Directive [19]. In the United States, privacy protection is achieved through a patchwork of legislation at the federal and state levels. Privacy

legislation is largely sector-based [20]. The CSAPP (Table 1) is representative of principles behind privacy legislation in many countries, including the European Union.

Table 1. CSAPP - The Ten Privacy Principles from the Canadian Standards Association [18]

Principle	***Description***
1. Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the privacy principles.
2. Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent	The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.
4. Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for fulfillment of those purposes.
6. Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards	Security safeguards appropriate to the sensitivity of the information shall be used to protect personal information.
8. Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access	Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

2.2. Attributes of consumer private information

In Table 1, we interpret “organization” as “provider” and “individual” as “consumer”. Principle 2 implies that there could be different providers requesting the information, thus implying a *collector* attribute. Principle 4 implies that there is a *what* attribute, i.e. what private information is being collected. Principles 2, 4, and 5 state that there are *purposes* for which the private information is being collected. Principles 3, 5 and 9 imply that the private information can be disclosed to other parties, giving a *disclose-to* attribute. Principle 5 implies a *retention time* attribute for the retention of private information. Thus, from the CSAPP we derive 5 attributes of consumer private information, namely *collector*, *what*, *purposes*, *retention time*, and *disclose-to*. Yee et al [21] found that these attributes are also supported by the privacy legislation of the European Union and the privacy regulations of the health sector in the United States.

Based on the above examination of CSAPP, the contents of a personal privacy policy should, for each item of private data, identify a) *collector* - who wishes to collect the information, b) *what* - the nature of the information, c) *purposes* - the purposes for which the information is being collected, d) *retention time* – the amount of time for the provider to keep the information, and e) *disclose-to* – the parties to whom the information will be disclosed. The attribute grouping <collector, what, purposes, retention time, disclose-to> is called a *privacy rule*. A personal privacy policy then consists of a header section followed by one or more privacy rules, where there is one rule for each item of private information. The header consists of the fields: *Policy Use* (for what application?), *User* (name of the user who owns the policy), and *Valid* (period of time during which the policy is valid). Figure 2 shows an example personal privacy policy based on the above development.

Header	*Policy Use:* E-learning *User:* Alice User *Valid:* unlimited
Privacy Rule	*Collector:* Any *What:* name, address, tel *Purposes:* identification *Retention Time:* unlimited *Disclose-To*: none
Privacy Rule	*Collector:* Any *What:* Course Marks *Purposes:* Records *Retention Time:* 2 years *Disclose-To*: none

Figure 2. Example personal privacy policy based on the Ten Privacy Principles [8]

The content of the above personal privacy policy is the minimum needed to satisfy legislative requirements and we term it a *minimum* policy since it can contain additional privacy provisions. Additional provisions could include, for example, a) elaborated retention time using conditions such as "6 months unless I call to have it deleted right away", b) negative purposes such as "not for purposes A or B", and c) negative disclose-to such as "not to be disclosed to persons C or D". However, for the purposes of this work, it is not necessary to consider these additional provisions.

The provider also has a privacy policy that has similar privacy rules as in the consumer's privacy policy. The provider's privacy policy specifies the provider's requirements for private information. Figure 3 shows an example of a provider privacy policy that corresponds to the personal policy in Figure 2.

Header	*Policy Use:* E-learning *Provider:* E-learning, Inc. *Valid:* unlimited
Privacy Rule	*Collector:* Elearning, Inc. *What:* name, address, tel *Purposes:* identification *Retention Time:* 1 year *Disclose-To*: none
Privacy Rule	*Collector:* Elearning, Inc. *What:* Course Marks *Purposes:* Records *Retention Time:* 1 year *Disclose-To*: none

Figure 3. Example provider privacy policy corresponding to Figure 2

Privacy policies need to be machine-readable and may be expressed using a XML-based language such as APPEL [22].

3. Using anonymization and smart cards to protect privacy

We first sketch our proposal before giving further details. Our goal is to protect an e-service user's privacy according to his/her personal privacy policy. This policy can be violated by the service provider (or other potential attackers) who would normally be in possession and control of the user's submitted private information. Our answer to privacy protection is simple: *remove the user's private information from the possession and control of the provider*. We accomplish this by having the user's private information in a smart card, called a *privacy controller*, owned by the user and in his/her possession. The private information in the privacy controller can only be entered and accessed by the user. Using the privacy controller, the user is able to selectively disclose (explained below) to the provider's service processes only information that is not personally identifiable, thus preserving the user's privacy. Further, the privacy controller smart card will process the user's information according to his/her privacy policy. The user is anonymous to the provider at all times. We further require the services of a trusted authority to program the smart card to act as a privacy controller, to install security mechanisms into the smart card, to keep the true identity of the user should there be a need to recover it (e.g. in legal proceedings), and to distribute the smart card. Figure 4 illustrates our approach.

In the next subsections, we will look at how selective disclosure transforms the privacy policy, followed by privacy controller and service process requirements imposed by the user's privacy policy and our framework.

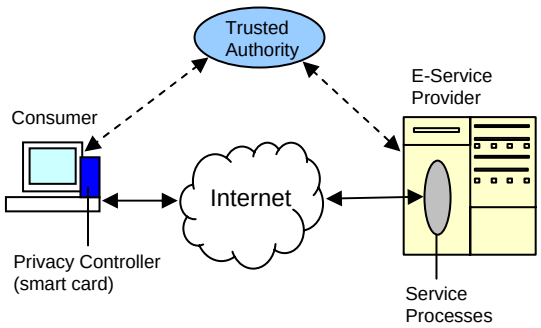

Figure 4. Using anonymization and smart card to protect user privacy

3.1. Selective disclosure and resultant privacy policy transformations

The selective disclosure process performed by the privacy controller is very straight forward – it simply holds back from the service processes any information that would identify the user. Such information is identified in the user's privacy policy which makes it very easy for the privacy controller to know what to hold back. For example, the personal policy in Figure 2 contains the identification rule:

Collector: Any
What: name, address, tel
Purposes: identification
Retention Time: unlimited
Disclose-To: none

The values for "purposes" and "what" indicate that this is personally identifiable information that must be withheld. However, this means that the privacy policies of both user and provider must be changed to reflect the fact that such information will not be given to the provider. The information must still be given though, for business purposes, not to the provider but to a trusted party who will maintain the anonymity of the user. Such trusted parties include a trusted shipper (for shipping purposes) or a bank (for credit card payment purposes). Thus in the case of a trusted shipper, Global Shipping, Inc., the above rule would be transformed to:

Collector: Global Shipping, Inc.
What: name, address, tel
Purposes: shipping
Retention Time: unlimited
Disclose-To: Global Shipping, Inc.

The corresponding rule in the provider's policy would be similarly transformed. We assume that privacy rules describing personally identifiable information can and are transformed as above into disclosures for trusted parties that provide business services (e.g. trusted shipper) in the user and provider privacy policies. This results in the privacy controller selectively disclosing only non-personally identifiable information (non-PII) to the service processes and disclosing personally identifiable information (PII) to trusted parties who perform business services, since the controller processes the user's information according to his/her privacy policy.

3.2. Privacy controller and service process requirements

The privacy attributes of the user's privacy policy impose the following requirements on the privacy controller and the service processes:

For each item of private information,

a) *Collector*: The privacy controller must confirm that the collector named by the service processes is the collector specified in the user's policy.
b) *What*: The privacy controller must confirm that the information item requested by the service processes is as specified in the user's policy.
c) *Purposes*: The privacy controller must confirm that the purposes for which the information will be used are as specified in the user's policy.
d) *Retention Time*: The privacy controller must destroy the user's private information at the end of its retention time. Although this may seem unnecessary since the privacy controller only gives the provider non-personally identifiable information, it is important for avoiding eventual storage overflow.
e) *Disclose-To*: The privacy controller must confirm that the receiving party in the case of a disclosure request is the party specified in the user's privacy policy.
f) The service processes must cooperate with the privacy controller where necessary in order to carry out the above requirements (e.g. private information disclosure requests to the privacy controller).

These requirements dictate the functionality of the privacy controller and the provider's service processes (PSP). The privacy controller handles the tasks of ensuring compliance with the user's privacy policy. It does this in two phases. In phase 1, the controller connects to the provider, downloads the provider's privacy policy, and verifies that the provider's privacy policy matches the user's privacy policy (comparing privacy policies for a match is outside the scope of this paper but see [23]). In phase 2, the controller enforces the user's privacy policy (see below). Phase 2 can only be reached if phase 1 is successful (if phase 1 is unsuccessful, the consumer and provider can enter into negotiation [24, 25] failing which the consumer can try another provider).

Privacy controller processing for user privacy policy compliance

In phase 1,

- Establish a connection with the provider and download the provider's privacy policy.
- Verify that the privacy rules in the provider's privacy policy matches the privacy rules in the user's privacy policy. If this verification fails, inform the user and terminate (or negotiate privacy policies as indicated above). Otherwise, proceed to phase 2.

In phase 2,

- Prompt user for each information item (II) and accept only II of the types specified in the user's privacy policy.
- Store user's II in its private information store.
- Destroy the user's II if the retention time is up (it has full control over the II in its store).
- Disclose only non-PII to the service processes as described in section 3.1 above.
- Accept requests from the PSP to disclose the user's II (PII and non-PII) to other providers as allowed by the user's privacy policy, passing along the II's retention time. The PII would be disclosed to trusted providers who would respect the retention time. Note: the typical public user would normally not be receiving disclosures. In this work, only providers receive disclosures, e.g. a trusted shipping company receiving an address disclosure for shipping purposes.

Service processing

The PSP executes during the controller's phase 2 processing, as follows:

- Perform normal processing required for the service that is offered by the provider. This includes requesting non-PII from the privacy controller needed for service processing.
- If needed, request the controller to disclose information to other parties.

Figure 5 illustrates the phases of controller and PSP processing using state machines.

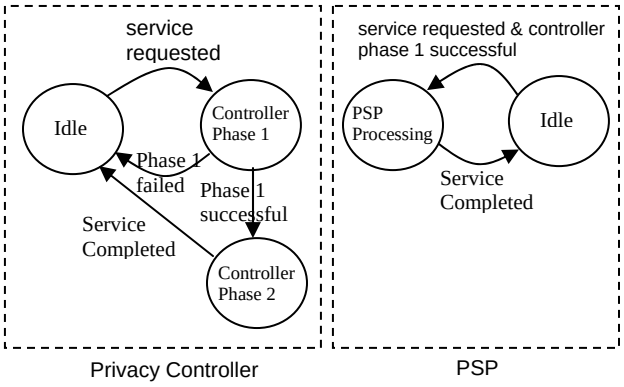

Figure 5. High-level state machines for privacy controller and PSP

3.3. Additional operational details

In this subsection we cover additional operational details not mentioned above using operating scenarios.

Prior to the commencement of any e-service, the trusted authority works to familiarize providers and users with its services. Providers that subscribe to the trusted authority must arrange their service processes to work with the privacy controller smart card (e.g. conform to smart card interfacing requirements). The trusted authority supplies these smart cards to e-service users. The trusted authority also selects and confirms a number of providers as trusted parties for business services such as shipping and banking.

A service user who wants to use a provider that subscribes to the trusted authority accesses the authority's web site and selects a subscribed provider. The trusted authority then assigns a pseudonym to the user and sends the provider the user's public key (for authentication purposes), using the pseudonym to identify the user. The trusted authority next programs a smart card to be used as the privacy controller and to work with the e-service (e.g. download provider's privacy policy, upload user's information). The trusted authority also installs in the smart card a private/public keys package for use in authenticating the provider and the recipients of information disclosures. Finally, the trusted authority sends the prepared smart card to the user. To use the e-service, the user connects the smart card to a USB port on his computer. The controller then begins phase 1 processing. A pop-up window appears indicating an anonymous connection to the service with successful 2-way authentication through a secure channel and with the provider's privacy policy downloaded (controller phase 1 processing). The privacy controller then compares the user's privacy policy (previously entered) with the provider's privacy policy for compatibility. If this is successful, the privacy controller initiates phase 2 processing. Otherwise, the privacy controller initiates a privacy policy negotiation session with the provider that takes place via the privacy controller. If this negotiation is successful, the privacy controller can begin phase 2. If neither the original phase 1 nor the negotiation is successful, the user must try a different provider. Once the controller starts phase 2, the provider's service processes are initiated. The latter then requests non-PII from the controller and requests it to send information disclosures (possibly sending PII to trusted parties (e.g. address for shipping)) as the service requires. Service output is sent back to the user via the controller-service processes channel.

It follows from the above that the trusted authority can link the user's pseudonym with the user. This is allowed on purpose, so that when necessary the provider can request the true identity of the user. For example, this may be necessary in a medical emergency where an e-pharmacy service provider needs to contact the user, or where there is a dispute involving the user and the user's real name is needed for legal proceedings.

3.4. Security measures

Based on the above operating scenarios, the vulnerability areas include: a) storage of private data, b) delivery of the smart card to the user by the trusted authority, c) sending data disclosures, d) communication between the privacy controller and the service processes, e) disclosure of non-PII to the service processes, i.e. although the data is non-PII, could their combinations collected over time compromise the anonymity of the user? f) traceable communications over the Internet, g) dishonest parties masquerading as trusted parties.

We discuss our security measures for each vulnerability area in turn as follows:

a) Storage of private data: the data is secured on the smart card (processor-enabled) using cryptographic techniques [12]. Further, the smart card incorporates tamper proof technology to foil any physical attempts break into it to steal the data.

b) Delivery of the smart card by the trusted authority to the user: this is done using a bonded courier. However, if the smart card is stolen or lost, the user's PII is not compromised since the smart card does not yet contain the user's PII. The user can notify the trusted authority once the smart card has gone missing and the authority can issue new private keys to parties that would have interacted with the missing controller.

c) Sending / receiving data disclosures: the privacy controller establishes a secure channel (SSL or secure VPN) to the receiving party for use in data conveyance; the sending controller authenticates the receiving party before any data is sent. Receiving parties are pre-screened by the trusted authority, and are assigned special public / private key pairs for authentication purposes. These public keys are placed in the user's smart card by the trusted authority who also delivers the required private keys to the receiving parties. In this way, the receiving parties are "blessed" by the trusted authority, inspiring more trust in making disclosures.

d) Communication between privacy controller and service processes: the controller establishes a secure channel (SSL or secure VPN) to the service processes to be used for communication purposes. The controller authenticates the service processes using a public key that matches (via a digital signature) a special private key assigned by the trusted authority to the service processes. Similarly, the service processes authenticates the controller using a public key that matches a special private key assigned by the trusted authority to the controller. The public and private keys required by the controller for these authentications are part of the keys package installed in the smart card by the trusted authority. In this way, both parties are "blessed" by the trusted authority, inspiring more trust on each side.

e) Disclosure of non-PII leads to compromising anonymity: we do not believe there is any significant risk here for most types of Internet available e-services; if we assume that selective disclosure is like anonymization, then identity discovery depends on the size of the candidate population, the method of selective disclosure, and the amount of personal data in circulation pertaining to the individual. We minimize the risk by specifying the candidate population to be the whole Internet community. We may further minimize the risk by employing more effective methods for selective disclosure. Further, the majority of Internet-based e-services are concerned with e-retailing that requires minimal PII, reducing the chances of identity discovery as described here.

f) Traceable communications over the Internet: the controller not only establishes a secure channel for communication with the service processes but establishes it using a mix network (e.g. JAP at http://anon.inf.tu-dresden.de/desc/desc_anon_en.html). By so doing, the provider would find it very difficult to trace the identity of the user using only the user's Internet connection.

g) Dishonest parties masquerading as trusted parties: first, the reputation of the trusted authority is established (as for a Certificate Authority in PKI); for example, the trusted authority could be subjected to inspection audits and other forms of testing to ensure that processes and responsibilities carried out are trustworthy. After the trusted authority is established to be trustworthy, it has the responsibility to make sure that all trusted parties are indeed trustworthy, perhaps by using a similar series of inspections and testing as was done for it.

3.5. Security vulnerability analysis

We affirm the security of our approach by analyzing all the possible attacks that we can think of to see if they have any chance of success.

- *Substitution attack* – the attacker replaces the privacy controller with versions that appear to function normally but allow the covert capture of the user's PII. *Chance of success: very low – since the trusted authority installed a special private key in the smart card for authentication with the*

service processes, the bogus controller would fail to authenticate with the service processes.

- *Modification attack* – the attacker modifies the privacy controller in order to obtain copies of the user's PII. This includes malicious attempts to read the PII from the store of the privacy controller. *Chance of success: very low – the data is encrypted and the hardware of the smart card is tamper proof. Unfortunately, an insider attack may be successful.*
- *Man-in-the-middle attack* – the attacker makes copies of the user's PII disclosures on their way to the recipients (e.g. trusted shipping company). *Chance of success: low – the PII is sent using a secure channel. There may be an attractive incentive for this attack: although the private data of any one individual may not have significant value, the private data of many thousands of individuals would have some significant value (though small).*
- *Provider spoofing attack* – the attacker pretends to be the legitimate recipient of a disclosure involving PII and captures the user's PII. *Chance of success: very low – the fake recipient would fail authentication by the sending controller.*
- *Trusted authority spoofing attack* – the attacker pretends to be the trusted authority and issues the user a bad privacy controller designed to steal the user's PII for the attacker. *Chance of success: very low – the fake authority would fail authentication.*
- *Privacy policy attack* – the attacker modifies the user's and provider's privacy policies to possibly direct PII disclosures to self (if allowed by the PSP) or to extend the retention time hoping that more time will allow a modification attack to succeed. *Chance of success: very low – the provider's privacy policy is encrypted and protected while on route to the privacy controller. Further, both policies are securely stored in the controller.*
- *Inferred identity attack* – the attacker captures a user's non-PII by compromising the PSP; the attacker accumulates this data over a long period of time in the hope that by analyzing this data, some pattern will emerge that will identify the user. *Chance of success: very low – already discussed above.*

The above brief analysis shows that our security measures are not fool proof against attacks. However, they probably provide enough of a deterrent to discourage most attacks. Given that PII for Internet commerce is probably not of high intrinsic value, this is probably sufficient.

4. Application example

Personal health information is recognized as being among the most privacy sensitive in the world. Consider an online pharmacy, E-Drugs, Inc., where prescriptions can be filled online and delivered to the patient the next day. The application of our approach would involve the following steps:

1. E-Drugs, Inc. (fictitious name) subscribes to use the privacy protection services of Privacy Watch, Inc. (fictitious name), the trusted authority that is marketing our approach.
2. Privacy Watch (PW) makes sure that E-Drugs service processes can interface to the privacy controller and adds E-Drugs to its web site as a subscriber.
3. A patient wishing to anonymously fill an electronic prescription finds E-Drugs on PW's web site and selects it. PW then assigns a pseudonym "patient21" to the patient and informs E-Drugs that patient21 is now its client. PW further provides E-Drugs with special public and private keys to be used for 2-way authentication with the patient.
4. PG programs a smart card to be used as a privacy controller for patient21 and installs special private and public keys in a special protected area in the smart card. The smart card is now ready to be used by patient21 to fill prescriptions anonymously with E-Drugs. PW sends the smart card to the user using a bonded courier.
5. Patient21 receives the smart card and connects it to the USB port on his/her computer. He/she is connected to the matching service processes at E-Drugs automatically and anonymously through a secure channel and mix network. After successful mutual authentication, the smart card downloads E-Drugs' privacy policy. After successfully verifying that patient21's privacy policy is compatible with E-Drugs' privacy policy, the privacy controller requests patient21's electronic prescription, shipping address, and credit card number.
6. Patient21 enters the requested information (disk location for the prescription) on his/her computer with the privacy controller making sure that the information corresponds with his/her privacy policy. The information is securely stored in the privacy controller. Upon request from E-Drugs' service processes, and after checking again with patient21's privacy policy, the controller discloses to the service processes details about the prescription (including the digital signature of the prescribing physician) but withholds patient21's name, address, and credit card number. Upon

request from the service processes, the controller sets up a secure channel to a trusted payment center and authenticates the payment center before disclosing to the center patient21's credit card number. The trusted payment center maintains the patient's anonymity to the outside world by keeping the pseudonym-patient link secret (as do all trusted business providers). The trusted payment center was designated as trusted by PW beforehand and assigned special private / public keys for authentication purposes. Similarly, the controller discloses patient21's name and address to a trusted shipping center that also keeps the pseudonym-patient link secret. Both the trusted payment center and the trusted shipping center use the pseudonym-patient link to link the order to the patient.

7. Patient21 receives the medicine the next day from the trusted shipping center.

5. Conclusions and future research

We have presented a novel approach to protect the PII of e-service users based on a new paradigm: keeping control of the PII in the hands of the user and a trusted authority. Our approach involves the use of a smart card acting as a privacy controller in the possession of the user. In this role, the smart card establishes an anonymous secure channel to the provider's service processes, checks to see if user and provider privacy policies are compatible, allows the user to enter his/her PII and non-PII, provides storage for the user's information, and processes the disclosure of the user's information according to the user's privacy policy. In performing the latter, it provides non-PII to the provider's service processes and may disclose PII to trusted parties (e.g. trusted shipper). We described a number of security measures to secure our approach and presented a security vulnerability analysis using several forms of attack. We showed that our security measures, although not foolproof, probably act as sufficient deterrent to discourage most attacks.

An advantage of our approach is that it is simple, employs existing technology, and should be fairly easy to set up. A possible disadvantage is that the use of selective disclosure is probably susceptible to some pattern being discovered among combinations of non-PII that would reveal the user's identity. However, most e-services on the Internet today are essentially sellers of products that do not require very much additional PII other than name, address, and credit card number. Given that the buyer community is Internet wide, this means that the chances of discovering a buyer's identity based on such little amounts of non-PII are extremely small.

We note also that the role of trusted authority represents a very profitable opportunity for an entrepreneur. A similar role already exists, namely the role of certificate authority.

As future research, we would like to develop appropriate anonymity algorithms with the aim of improving upon our method of selective disclosure. We would also like to build a prototype of our approach to prove the concept and experiment with usability, performance, and scalability.

References

[1] V.S. Iyengar, "Transforming Data to Satisfy Privacy Constraints", Proceedings, SIGKDD'02, Edmonton, Alberta, 2002.

[2] A. Kobsa, J. Schreck, "Privacy Through Pseudonymity in User-Adaptive Systems", ACM Transactions in Internet Technology, Vol. 3, No. 2, pp. 149-183, May 2003.

[3] R. Pang, V. Paxson, "A High-Level Programming Environment for Packet Trace Anonymization and Transformation", Proceedings, Sigcomm'03, Karlsrube, Gernmany, Aug. 25-29, 2003.

[4] H. Berghel, K. Womack, "Anonymizing the Net", Communications of the ACM, Vol. 46, No. 4, April 2003.

[5] A. Meyerson, R. Williams, "General k-Anonymization is Hard", report CMU-CS-03-113, Carnegie Mellon University, March 2003, available as of April 11, 2005 at: http://reports-archive.adm.cs.cmu.edu/anon/2003/CMU-CS-03-113.pdf

[6] A.A. El Kalam et al, "A Generic Approach for Healthcare Data Anonymization", Proceedings, WPES'04, Washington, DC, October 28, 2004.

[7] R. Song, L. Korba, and G. Yee, "Pseudonym Technology for E-Services", chapter to appear in Privacy Protection for E-Services, Edited by G. Yee, Idea Group, Inc., 2005.

[8] C. Adams and K. Barbieri, "Privacy Enforcement in E-Services Environments", chapter to appear in Privacy Protection for E-Services, Edited by G. Yee, Idea Group, Inc., 2005.

[9] S. Kenny and L. Korba, "Adapting Digital Rights Management to Privacy Rights Management", Computers & Security, Vol. 21, No. 7, November 2002, 648-664.

[10] G. Yee, L. Korba, "Privacy Policy Compliance for Web Services", Proceedings, 2004 IEEE International Conference on Web Services (ICWS 2004), San Diego, California, July 6-9, 2004.

[11] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-Enhancing Technologies for the Internet", *IEEE COMPCON'97*, pp. 103-109, 1997.

[12] K.M. Shelfer, J.D. Procaccino, "Smart Card Evolution", Communications of the ACM, Vol. 45, No. 7, July 2002.

[13] M.R. Carr, "Smart card technology with case studies", Proceedings, 36th Annual 2002 International Carnahan

Conference on Security Technology, pp. 158-159, Oct. 20-24, 2002.

[14] R. Toji et al, "A network-based platform for multi-application smart cards", Proceedings, Fifth IEEE International Enterprise Distributed Object Computing Conference (EDOC'01), pp. 34-45, Sept. 4-7, 2001.

[15] A.T.S. Chan, "Integrating Smart Card Access to Web-based Medical Information Systems", Proceedings, SAC 2003, Melbourne, Florida, 2003.

[16] V. Mornar, D. Palavra, D. Kalpic, "Application of smart cards in distributed information systems", Proceedings, 26th International Conference on Information Technology Interfaces, Vol. 1, pp. 187-192, June 7-10, 2004.

[17] Government of Canada, Personal Information Protection and Electronic Documents Act, available as of February 28, 2005 at: http://www.privcom.gc.ca/legislation/index_e.asp

[18] Department of Justice, Privacy Provisions Highlights, retrieved July 3, 2002 from: http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

[19] European Union, "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", unofficial text retrieved Sept. 5, 2003 from: http://aspe.hhs.gov/datacncl/eudirect.htm

[20] D. Banisar, "Privacy and Data Protection Around the World", 21st International Conference on Privacy and Personal Data Protection, September 13, 1999.

[21] G. Yee, L. Korba, and R. Song, "Legislative Bases for Personal Privacy Policy Specification", chapter to appear in Privacy Protection for E-Services, Edited by G. Yee, Idea Group, Inc., 2005.

[22] W3C, "A P3P Preference Exchange Language 1.0 (APPEL 1.0)", retrieved April 22, 2004 at: http://www.w3.org/TR/P3P-preferences/

[23] G. Yee, L. Korba, "Comparing and Matching Privacy Policies Using Community Consensus", Proceedings, 16th IRMA International Conference, San Diego, California, May 15-18, 2005.

[24] G. Yee, L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida, Jan. 27-31, 2003.

[25] G. Yee, L. Korba, "The Negotiation of Privacy Policies in Distance Education", Proceedings, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.