Empowering Users to Specify and Manage Their Privacy Preferences in e-Government Environments

Prokopios Drogkaris[1], Aristomenis Gritzalis[2], and Costas Lambrinoudakis[2]

[1] Laboratory of Information and Communication Systems Security,
Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, GR-83200, Greece
pdrogk@aegean.gr
[2] Systems Security Laboratory,
Department of Digital Systems,
University of Piraeus, GR-18534, Greece
agritz@ssl-unipi.gr, clam@unipi.gr

Abstract. The provision of advanced e-Government services has raised users' concerns on personal data disclosure and privacy violation threats as more and more information is released to various governmental service providers. Towards this direction, the employment of Privacy Policies and Preferences has been proposed in an attempt to simplify the provision of electronic services while preserving users' personal data and information privacy. This paper addresses the users' need to create, manage and fine-tune their privacy preferences in a user friendly, yet efficient way. It presents a Graphical User Interface (GUI) that empowers them to articulate their preferences in machine readable format and resolve possible conflicts with Service Provider's (SP) Privacy Policy, without being obliged to go through complex and nuanced XML documents or being familiar with privacy terminology. Users can now be confident that their personal data will be accessed, processed and transmitted according to their actual preferences. At the same time they will be aware of their privacy-related consequences, as a result of their selections.

Keywords: e-Government, Privacy Policy, Privacy Preferences, GUI.

1 Introduction

The notion of privacy is a complex and challenging concept, especially since the evolution and spread of Information and Communications Technologies (ICT). Most widely accepted definitions, revolve around the idea that privacy is the right to protect personal information or to limit and control access to them. The advanced provision of electronic services has not only braced users' demand for online privacy but has also raised their privacy awareness [1]. Equivalently, from the provider's perspective, the need to protect users' privacy and to comply with privacy legislation is also a growing concern, let alone obligation. The increased number of e-Government services, offered by Central Government, entails a continuously increasing amount of data

A. Kő and E. Francesconi (Eds.): EGOVIS 2014, LNCS 8650, pp. 237–245, 2014.

collected, processed and retained by Governmental Service Providers without the users being aware to whom, for what purpose and for how long their personal data is released to.

This situation has raised users' concerns regarding data privacy, data disclosure and emerging privacy violation threats, thus affecting their trust level to the service and, in turn, their willingness to accept and use therm. As a result, the formalization of providers' commitments regarding privacy practices and privacy requirements is an indispensable task since users will be able to review these requirements and practices and preserve their personal data privacy [2], [3] & [4]. A privacy policy can be regarded as a statement or document describing what information is collected by an electronic service and how this information will be used [5]. Most commonly, a privacy policy states explicitly what personal information (such as email addresses and users' names) is collected, whether shared or sold to third parties and for how long it will be retained. On the other side, users should also be able to formally express acceptable privacy practices and requirements. Such formal statements comprise the so called privacy preferences. Usually they affirm which personal information can be collected, for what purpose, whether they can be transmitted to third parties and for how long they can be retained.

This paper addresses the need of users to create, manage and fine-tune their privacy preferences in a user friendly, yet efficient way. It presents a Graphical User Interface (GUI) that empowers them to articulate their preferences in machine readable format, identify situations where their data privacy might be at risk and resolve possible conflicts with Service Provider's (SP) policy, without being obliged to go through complex and nuanced XML documents or being familiar with privacy terminology[1]. Users can now be confident that their personal data will be accessed, processed and transmitted according to their actual preferences. At the same time they will be aware of their privacy-related consequences, as a result of their selections. The rest of the paper has been structured as follows: Section 2 presents an architecture for incorporating Privacy Policy and Privacy Preferences in e-Government environments and Section 3 presents the proposed Graphical User Interface. Section 4 discusses existing research work on user interfaces for privacy preferences selection while Section 5 concludes the paper providing directions for future work.

2 Privacy Policy and Preferences Embodiment in e-Government Environments

The concept of embodying Privacy Policy and Privacy Preference documents in modern e-Government environments has been explored in [6], in an attempt to simplify the provision of advanced electronic services while preserving user's privacy. Through Privacy Policy documents, Service Providers deliver a formal commitment

[1] This work has been supported by the national project "Secure and Privacy-Aware eGovernment Sevices – SPAGOS" (Grant Agreement 11SYN_9_2059), under "SYNERGAGIA 2011" programme, of the Operational programme "Competitiveness and Entrepreneurship".

of the data required, the purpose of this request as well as of how data will be processed and to whom it will be disclosed. Data subject consents to the use of her personal data by specifying, for each data item or group of items, fine-grained privacy preferences defining how these data items should be used. This approach has the advantage of coping with situations where the data subject decides to revoke the right that has previously granted to the data collector. By properly updating the preferences stored, the data subject can constitute certain personal data be no longer validly accessible. Architecture's design has been based on modern – government environments structure which involves a central portal that operates as a one-stop shop being the front end for every service provider [7], [8] & [9]. Typically this portal implements the authentication and registration procedures or incorporates the federated identity management infrastructure for every Service Provider. Alongside to these entities, the Privacy Controller Agent (PCA) was introduced, being in charge of storing and comparing Service Providers' privacy policies and user privacy preferences. An overview of the architecture is presented in Fig. 1 below.

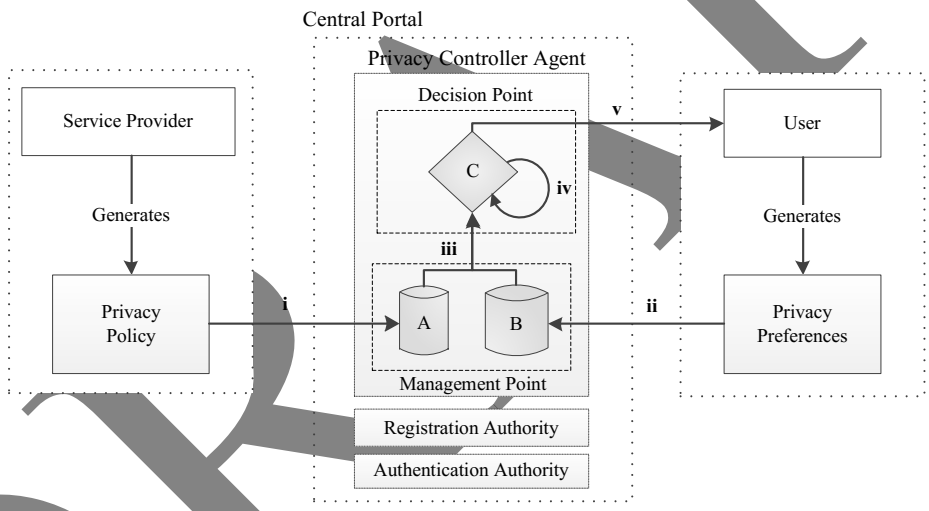

Fig. 1. Privacy Controller Agent Architecture [6]

The Privacy Controller Agent consists of two main units: the Management Point and the Decision Point. The Management Point features two storage repositories which are in charge of retaining the privacy policy of each service (A) and the privacy preferences of each user (B). When a service provider (SP) enrolls an electronic service to the central portal (CP), apart from the remaining information required, it is necessary to submit the corresponding Privacy Policy. The policy states explicitly the data required for the provision of the service, the purpose for which the data are required, how they will be processed, if they will be stored, for how long they will be retained and if they will be communicated to another service provider. The privacy preferences, defined by the user, apply to the entire set of her personal data

irrespective of the specific service that utilizes them. Therefore the user needs to submit only one document (privacy preferences) that applies to all electronic services. User will have to specify what type of data will be included in the privacy preferences document, for what purpose these data can be used and by which service provider. After submission, the Privacy Controller Agent validates preference's origin and stores them at the Preferences Repository (action ii). Additionally, a simple XML schema has been proposed, in [6], to create the aforementioned documents. This schema consists of simple elements along with specific attributes, in an attempt to describe a strict privacy policy in a structured yet easy way.

3 Proposed Interface

This paper proposes the enhancement of e-Government environments with a privacy-enhancing mechanism that supports users to create, manage and fine-tune their privacy preferences in a user friendly, yet efficient way. The proposed mechanism pertains a Graphical User Interface (GUI) which enables users them to articulate their preferences in machine readable format and resolve possible conflicts with Service Provider's (SP) policy, without being obliged to go through complex and nuanced XML documents or being familiar with privacy terminology [6]. As discussed in [10], designing a user interface for specifying privacy preferences is challenging for several reasons: privacy policies are complex, user privacy preferences are often complex and nuanced, users tend to have little experience articulating their privacy preferences, users are generally unfamiliar with much of the terminology used by privacy experts, and users often do not understand the privacy-related consequences of their behavior. Consequently, in such interfaces, the privacy concepts must be presented through easily understood illustrations [11].

3.1 Specification Taxonomy

Based on the XML schema proposed in [6], two discrete categories have been identified; Personal Identifiers and Personal Data. For each one, the XML elements `Process`, `Process Type`, `Storage`, `Service Provider` and `Retention Period` must be specified. An overview of the taxonomy is presented in Fig. 2 below.

It is apparent that the specification of Personal Identifiers and Personal Data for each Service Provider would increase the amount of information and time required from users while creating their preferences. Moreover, a detailed description of each electronic service would be difficult for a user to administer and solelythe inclusion of SPs could not imprint actual user's preferences. To overcome this impediment, the establishment of sets and supersets has been adopted. Each Service Provider will constitute a superset that will contain all the electronic services that he offers; when a user allows his data to be processed or stored by this SP then this permission is transferred to each service. Similarly, a Ministerial Department will comprise a superset that will contain all applicable Service Providers. On the contrary, an acceptance

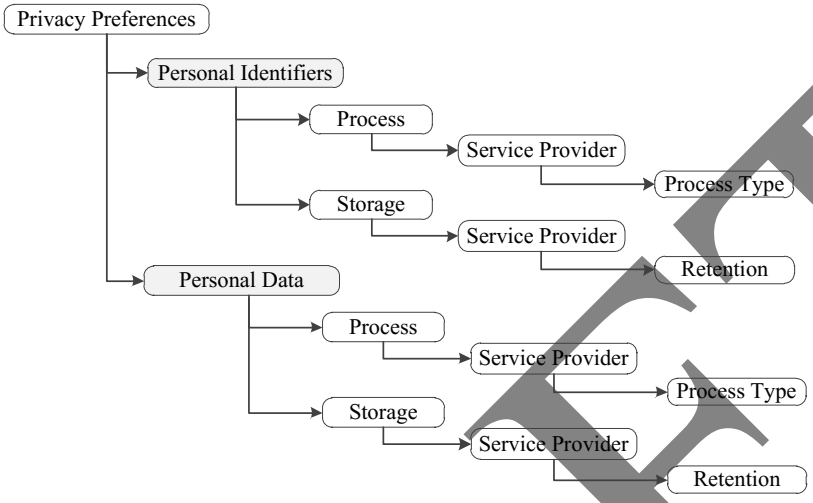

Fig. 2. Taxonomy of Specifications in User's Privacy Preferences

of a specific service does not imply approval of all SP's services. In addition to this principle, the lack of a SP or an electronic service shall be interpreted as a denial of data provision. Based on the approach of sets and supersets, the inclusion of attributes, relating to how data will treated by SP's, into specific supersets is also proposed. For instance, the Public attribute will also contain the Confidential one.

3.2 Graphical User Interface (GUI)

The Graphical User Interface (GUI) has been developed using Xcode[2], a development framework based on an Integrated Development Environment (IDE) which runs GNU Compiler Collection (GCC). The selection of Xcode allows for the exploitation of the proposed GUI by both mobile and desktop applications. Even though, at this point, they will not be directly connected to an e-Government Information System, the multi-platform functionality will allow for broader end-user engagement and participation during the foreseen e-acceptance use cases and trials. The overall interface's design has adopted principles discussed in [12], [13] and [14]. Furthermore it is expected to be improved based on the feedback received by participants during simulation trials. The main screen of the interface comprises of 4 distinct parts and is presented in Fig. 3 below.

Through the search function (Part I), the user is able to look for specific Personal Identifiers (e.g. National Identity Card Number (IdN), National Taxation Identifier (AFM), Social Security Number (AMKA) and Personal Data (e.g. First and Last Name, Address). The selected Identifier or Personal Data for which the user will specify her preferences are separately presented below. In Part II, the user can add or remove Ministerial Departments and Service Providers, specify how the selected data

[2] Xcode – Apple Developer: `https://developer.apple.com/xcode/`

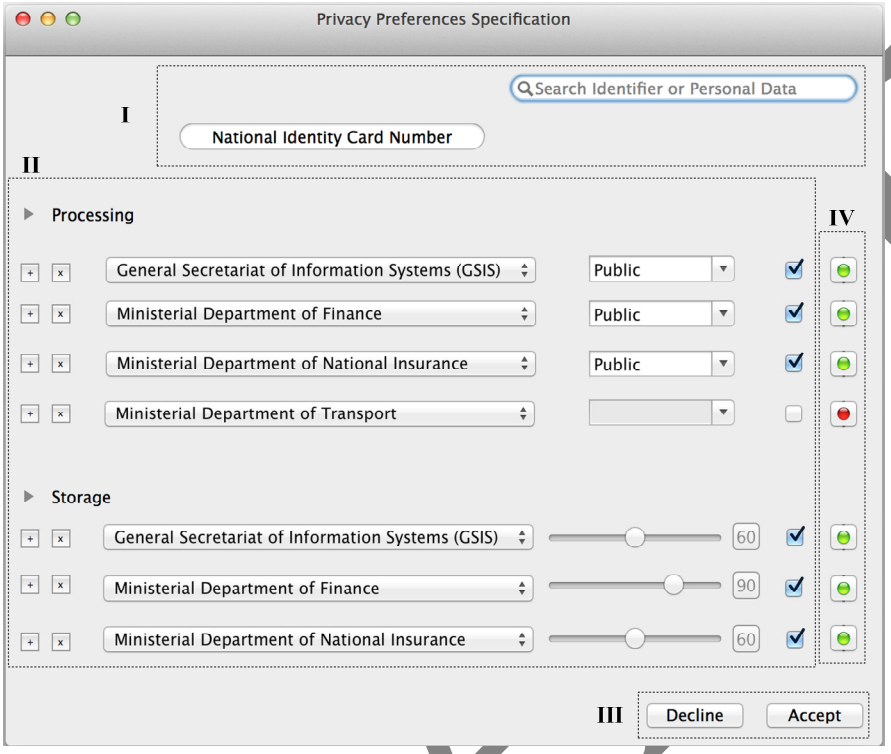

Fig. 3. Graphical User Interface (GUI) for Privacy Preferences Specification

will be processed and the maximum permissible retention period. Through the available check boxes, a Service Provider or Ministerial Department can be easily selected or deselected, without being obliged to completely remove it. Finally, in Part III, the user can accept to submit all her preferences to the Privacy Controller Agent or to cancel the procedure. Following the submission, the GUI creates the corresponding XML document, which is actually submitted to the Privacy Controller Agent. Based on the schema discussed in Section 2, the XML document generated from the interface selections is presented in Fig. 4 below.

When the user decides to invoke an electronic service, the comparison procedure is being invoked and her preferences are checked against service's privacy policy. If the user's preferences assent on the usage of data through the operations and for the purpose described in the policy, the agent informs the user, through the portal, of the concurrence and forwards service's request to the applicable Service Provider. Through this comparison and notification process, the user is now confident that her personal data will be accessed, processed and transmitted according to her preferences. In the case where these preferences don't match the policy of the SP, the PCA informs the user of the conflict. In part IV of the developed GUI, the deployment of visual notifications enable the user to quickly identify the conflict and review her preferences.

```
D.1  <Privacy_Preferences>
D.2   <Preferences_ID="[number assigned by Central Portal]">
D.3      </Preferences_ID>
D.4    <Data>
D.5     <Personal_Identifiers>
D.6      <Identifier_ID="="[number assigned by Central Portal]">National
D.7        Identity Card Number(IdN)
D.8        <Processed="Public">General Secretary of Information Systems
D.9                  (GSIS)</Processed>
D.10         <Storage="Yes" Conserve="60">General Secretary of
D.11                 Information Systems (GSIS)</Storage>
D.12       <Processed="Public">Ministerial Department of
D.13                 Finance</Processed>
D.14         <Storage="Yes" Conserve="90">Ministerial Department of
D.15                 Finance</Storage>
D.16       <Processed="Public">Ministerial Department of National
D.17                 Insurance</Processed>
D.18         <Storage="Yes" Conserve="60">Ministerial Department of
D.19                 National Insurance</Storage>
D.20       </Identifier_ID>
D.21     </Personal_Identifiers>
D.22   </Data>
D.23 </Privacy_Preferences>
```

Fig. 4. Generated XML Document

3.3 Security Evaluation

Even if Privacy Preferences documents do not contain personal or sensitive user data, it could be argued that they comprehend predilections on them and should thus not be made available to unauthorized entities. Furthermore, the integrity and availability of these documents should also be preserved so that the user is confident and assured that they are not modified or made unavailable. The incorporation of the Privacy Controller Agent and the provision of Privacy Preferences Specification service by the Central Portal, as described in Section 2, can indeed ensure these characteristics. Utilizing the underlying Public Key Infrastructure (PKI) of e-Government Information Systems, the user is able to digital sign her preferences document, after each creation, prior to submitting it to the PCA. After submission, the PCA validates preference's origin and stores them at the Preferences Repository, after encrypting them with the PCA's public encryption key [6].

4 Related Work

Several research projects funded by the E.C., including PRISE: Privacy enhancing shaping of security research and technology[3], PACT: Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action[4], PRISMS: The PRIvacy and Security MirrorS: Towards a European

[3] PRISE Project: www.prise.oeaw.ac.at
[4] PACT Project: www.projectpact.eu

framework for integrated decision making[5] have conducted analysis and assessment on existing knowledge and technologies about the trade-off model between privacy and security and trust and concern. Additionally, they have proposed methodologies and frameworks for reconciling privacy, security, trust and concern that could assist end users and policy makers to consider privacy and fundamental rights when they evaluate security and privacy preserving technologies. A significant aspect of these proposals pertains users being able to hide and reveal personal information based on a particular usage context, user controlled information flows, where user can manage her privacy on different levels of detail and finally promoting guidance and awareness through advisory procedures.

As acknowledged in [15], "privacy poses a very difficult HCI problem"; GUI's not only represent an extremely complex decision space, depending on the context and the commitment of the user, in a simplified way but should also highlight context significant information and provide feedback and suggestions. The creation of Graphical User Interfaces for specifying Privacy Preferences has been initially explored at [16] and [17] where a user agent was developed for Internet Explorer 5.01, 5.5, and 6.0, as a browser helper object. The design approach focused on a subset of the P3P vocabulary, which could be easily realized by users, along to privacy options that used combinations of P3P data elements. During the development, authors attempted to avoid setting defaults for the main privacy settings as they wanted to compel users in selecting the actual settings themselves. Finally, they also developed appropriate agents that provide feedback, through icons and messages, about whether a privacy policy matched a user's preferences and make privacy suggestions as a more direct and appropriate mean to inform the user.

5 Conclusions

Privacy Enhancing Technologies (PET) pertaining Privacy Policies and Preferences have been largely accepted as suitable mechanisms to overcome user concerns regarding data disclosure and emerging privacy violation threats. The complexity however of SP's Privacy Policies pose significant difficulties on the automated development of personalized and fine graded Privacy Preferences since it inevitably requires intense interaction with the user. Towards this direction, a Graphical User Interface (GUI) was developed and proposed, as an addition to Privacy Controller Agent, enabling users to create, manage and fine-tune their preferences in machine readable format, taking also into account possible conflicts with Service Provider's privacy policy. The work, which is currently underway, is to create a sufficient number of Privacy Policies and exploit them during GUI validation use cases and trails, based on different types of users.

References

1. Chellappa, R., Pavlou, P.: Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions. Logistics Information Management 15(5), 358–368 (2002)

[5] PRISMS Project: `www.prismsproject.eu`

2. McDonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F.: A Comparative Study of Online Privacy Policies and Formats. In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 37–55. Springer, Heidelberg (2009)
3. Proctor, R.W., Vu, K.-P.L., Ali, M.A.: Usability of user agents for privacy-preference specification. In: Smith, M.J., Salvendy, G. (eds.) Human Interface, Part II, HCII 2007. LNCS, vol. 4558, pp. 766–776. Springer, Heidelberg (2007)
4. Bodorik, P., Jutla, D., Wang, M.: Consistent privacy preferences (CPP): model, semantics, and properties. In: 2008 ACM Symposium on Applied Computing, SAC 2008, Ceara, Brazil, pp. 2368–2375 (2008)
5. Salas, P.P., Krishnan, P.: Testing Privacy Policies Using Models. In: Sixth IEEE International Conference on Software Engineering and Formal Methods, Cape Town, pp. 117–126 (2008)
6. Drogkaris, P., Gritzalis, S., Lambrinoudakis, C.: Employing Privacy Policies and Preferences in Modern e-Government Environments. International Journal of Electronic Governance 6(2), 101–116 (2013)
7. Charalabidis, Y., Lampathaki, F., Sarantis, D., Sourouni, A.-M., Mouzakitis, S., Gionis, G., Koussouris, S., Ntanos, C., Tsiakaliaris, C., Tountopoulos, V., Askounis, D.: The Greek Electronic Government Interoperability Framework: Standards and Infrastructures for One-Stop Service Provision. In: 12th Panhellenic Conference on Informatics (PCI 2008), Samos. Greece, pp. 66–70 (2008)
8. Pei, Y., Jiao, G.: Researching and Designing the Architecture of E-government Based on SOA. In: International Conference on E-Business and E-Government (ICEE 2010), Guangzhou, pp. 512–515 (2010)
9. Drogkaris, P., Geneiatakis, D., Gritzalis, S., Lambrinoudakis, C., Mitrou, L.: Towards an Enhanced Authentication Framework for eGovernment Services: The Greek case. In: Ferro, E., Scholl, J., Wimmer, M. (eds.) 7th International Conference on Electronic Government, EGOV 2008, Torino, Italy, vol. 1, pp. 189–196. Trauner Verlag (2008)
10. Cranor, L., Guduru, P., Arjula, M.: User Interfaces for Privacy Agents, pp. 135–178 (2006)
11. Kolter, J., Pernul, G.: Generating User-Understandable Privacy Preferences. In: Barolli, L., Jakoubi, S., Tjoa, S. (eds.) International Conference on Availability, Reliability and Security (ARES 2009), Fukuoka, vol. 1, pp. 299–306 (2009)
12. McNamara, N., Kirakowski, J.: Defining usability: quality of use or quality of experience? In: Professional Communication Conference, IPCC 2005 (2005)
13. Nillson, E.: Design patterns for user interface for mobile applications. Advances in Engineering Software: Designing, Modelling and Implementing Interactive Systems 40(12), 1318–1328 (2009)
14. Lee, G., Eastman, C., Taunk, T., Ho, C.: Usability principles and best practices for the user interface design of complex 3D architectural design and engineering tools. International Journal of Human-Computer Studies 68(1-2), 90–104 (2010)
15. Ackerman, M., Cranor, L.: Privacy Critics: UI Components to Safeguard Users' Privacy. In: Altom, M., Williams, M. (eds.) Conference on Human Factors in Computing Systems (CHI 1999), Pittsburgh, vol. 1, pp. 258–259 (1999)
16. Cranor, L.: Designing a Privacy Preference Specification Interface: A Case Study. In: Patrick, A., Long, A., Flinn, S. (eds.) Workshop on HCI and Security Systems (CHI 2003), Tampa, vol. 1, pp. 38–47 (2003)
17. Ackerman, M., Cranor, L., Reagle, J.: Privacy in e-commerce: Examining User Scenarios and Privacy Preferences. In: Feldman, S., Wellma, S. (eds.) 1st ACM Conference on Electronic Commerce (EC 1999), New York, vol. 1, pp. 1–8 (1999)