Privacy Enhancing Technologies: A Review

John Argyrakis, Stefanos Gritzalis, and Chris Kioulafas

Department of Information and Communications Systems Engineering
University of the Aegean, Samos, GR 832 00, GREECE
{cs98004,cs98020}@icsd.aegean.gr
sgritz@aegean.gr

Abstract. The spread and development of e-Government services caused significant interest in maintaining security, trust and privacy. This paper presents a state-of-the-art review of the widely accepted Privacy Enhancing Technologies (PETs). A strict classification of several parameters is performed in order to conduct a comparative analysis among *Anonymizer*, *Crowds*, *Onion Routing*, *TRUSTe*, *P3P*, *LPWA*, *Hordes* and *Freedom*. The selection of the comparison criteria is relevant to Security Threats, Technological Issues and User Demands.

1 Introduction

E-Government focuses on relatively simple transactions between identifiable customers and a multitude of government organisations in charge of Web activities. The nature of these Web-transactions endangers anonymity [2]. Moreover, certain malicious tactics may be used to decline privacy over e-Government services [1], [5], [8]. These technologies focus not only on achieving trust and security among users and Web sites, but they also apply to e-Government transactions, such as voting procedures.

The current section presents relations between PETs and e-Government needs and provides a description of several PETs. A comparative analysis is presented in the second section. The final section refers to concluding remarks about PETs.

2 Privacy Enhancing Technologies Description

Although there are several PETs, we choose to describe only the most important for e-Government users. *Anonymizer* is a proxy-based service that submits HTTP requests to Web sites on behalf of its users [1]. *Crowds* is an agent based on the idea that people can be anonymous when they blend into a crowd [3]. *Onion Routing* provides anonymous connections using different layers of encryption [2], [5]. *TRUSTe* is a non-profit, privacy seal program for web sites [4], [5]. *P3P* is a framework for informed online interactions [7]. *LPWA* is a software system designed to allow users browse the Web using aliases and other LPWA features [5]. *Hordes* employs multiple proxies to anonymously route a packet towards the responder and uses multicast for replying to the initiator [2]. *Freedom* intends to protect the privacy of users sending e-mail, browsing the web, posting to newsgroups and participating in Internet chat [6].

R. Traunmüller (Ed.): EGOV 2003, LNCS 2739, pp. 282–287, 2003.

3 Privacy Enhancing Technologies Comparison

3.1 Confronted Security Threats

3.1.1 Trace Back Attack

An attacker may start from a known responder and trace the path back to the initiator along the forward path or the reverse path [2]. *Anonymizer* and *LPWA* do not protect from this attack since there is no data processing. Although *Crowds* protects the forward paths, several jondos could be exploited to obtain routing information. *Onion Routing* protects forward paths with different layers of symmetric cryptography, but *Crowds* drawback applies in the reverse path. *Crowds* and *Onion Routing's* static paths decrease protection. *TRUSTe* and *P3P* do not protect from these attacks. *Crowds*' unicast techniques are also applied to *Hordes* although the connections are not static. *Hordes'* IP multicast protects the reverse path. *Freedom's* asymmetric cryptography and dynamic paths protects only forward paths [6].

3.1.2 Malicious Collaborators

A group of collaborators are malicious if they try to discover the identity of the initiator [2]. *Anonymizer, TRUSTe, P3P, LPWA* and *Freedom* architecture is based on a single proxy. The criterion is not applicable since legitimate actions could be carried out against it. *Crowds'* and *Onion Routing's* users may choose the jondos at the establishment of the protocol and the random creation of the path increases the provided protection. *Onion Routing* uses different layers or encryption. The use of IP multicast through the backward routing protects *Hordes'* users from malicious collaborators.

3.1.3 Eavesdroppers

Attackers are able to monitor all communications of one participant in order to find either the initiator or the receiver. Connections among users, *Anonymizer* and *LPWA* could be easily compromised. *Crowds* protects against eavesdroppers due encryption of emitted data. The strong cryptography used by *Onion Routing* protects from eavesdroppers. *TRUSTe* and *P3P* focus on presenting and negotiating security policies among different Web sites. *Hordes'* packets are encrypted and its members use shared multicast groups so that they receive and discard unnecessary traffic. *Freedom* uses a symmetric encryption algorithm that prevents eavesdropping attacks.

3.1.4 Message Attacks

A global observer is able to associate a communication relation and trace messages, if their coding is not changed during transmission. *Anonymizer* and *LPWA* do not protect from these attacks, although data could not be correlated with their initiator. *Crowds* protects from message attacks triggered outside the crowd. *Onion's Routing* different layers of encryption protects against these attacks. *TRUSTe* and *P3P* are not focused on protecting from these attacks. *Hordes* uses pair-wise keys between two jondos and multiple routing to prevent deciphering of data. *Freedom's* asymmetric cryptography (Key Query Server) prevents data decryption [6].

3.1.5 Timing Attacks

Packets that are transmitted periodically could be analyzed due to timing correlations. Any host outside a secure group is vulnerable to timing attacks. *Crowds*, *Onion Routing*, *Hordes* and *Freedom* are able to prevent timing attacks against internal proxies.

3.1.6 Flooding Attacks

If a router supports n users an attacker may send n-1 packets to trace the original one back to its source. User's authentication counter attacks flooding. Thus, *Crowds*, *Onion Routing Hordes* and *Freedom* provide means of authentication.

3.1.7 Connection Periods Attacks

Most users establish a limited number of connections and have a fixed type of Web behavior. These activities could be analyzed and dramatically decrease the size of anonymous users in a specific group of *Crowds*, *Onion Routing*, and *Hordes*.

3.1.8 Cookies

They threat users' privacy since personal data may be processed by various Web entities. *Anonymizer* does not allow the use of Cookies. *Crowds, Onion Routing, Hordes, and Freedom* do not protect against this threat [6]. *TRUSTe* may take measures against untrustworthy partners in case the mentioned policies have been compromised. *P3P* is more flexible than *TRUSTe* since it can also modify policies that refer to Cookies [7]. The pseudonyms that are provided by *LPWA* replace Cookies.

3.1.9 Personalized Services

There is always the threat of revealing personal information during registration procedure. *Anonymizer* could not exchange any real credentials of the user with those services and no registration could be submitted. *Crowds, Hordes* and *Onion Routing* do not use any pseudonyms and personal data could not be concealed. *TRUSTe* uses trust marks to ensure the proper management of personal information. *P3P* users have the right to know and negotiate the policies followed by a Web site and then entrust personal data. *LPWA* proxy supports the creation and storage of different pseudonyms for each Web site. *Freedom's* multiple nyms ensures the secure use of these services [6].

3.2 Applied Technological Issues

3.2.1 Reliability

This criterion refers to the trustworthiness of PET entities. *Anonymizer, TRUSTe, P3P, LPWA, and Freedom* authorized proxies are trusted, since in case of a deliberate information disclosure the users know whom to blame. *Crowds'* users have to trust several participants by revealing their true identity. *Onion Routing* is reliable due to multi-layer cryptography and the capability to select the connection path. The use of pair-wise cryptography keys protects personal data against any member of the horde or other entities. Moreover, the increase of *Hordes* members protects users' anonymity, as it is more difficult to compromise their identities.

3.2.2 Installation Complexity

PETs' installation procedure is an important issue. *Anonymizer, TRUSTe* and *P3P* are Web services so there is no installation need. *Crowds'* and *Hordes'* installation demands source code's download and compilation. Although *Onion Routing's* next version has not been available yet, the previous one requires a lot of effort to be installed [2]. *LPWA* requires the submission of users' personal information and some changes in browser's settings. *Freedom* provides help through installation procedure.

3.2.3 Performance

The performance of PETs is judged by the link utilization of each connection. *Anonymizer's* and *LPWA's* communication line is separated into two connections and this causes no-detectable latencies. *Crowds'* and *Onion Routing's* communication path is separated into several TCP connections among different jondos so the performance is not optimized. *TRUSTe* and *P3P* provide the best performance since they do not interfere with TCP connections or add any traffic to existing links. *Hordes* uses UDP packets to transfer data between jondos and therefore re-transmission of packets is prevented. *Freedom* performance depends on the use of asymmetric cryptography and the continuous queries for the public keys and nyms [6].

3.2.4 Overhead Latencies

The protection of privacy may cause overhead latencies to browser Web activities. *Anonymizer, TRUSTe, P3P, LPWA,* and *Freedom* demand no further actions during Web browsing since the relevant proxies perform all necessary actions. *Hordes*' members do not perform any complex activity during the backward routing procedure and the initiator has no capability to choose the path. *Crowds* is better than *Onion Routing* as it does not support complex cryptography techniques [2].

3.3 Satisfied Users Demands

3.3.1 Anonymity

Anonymity can be applied to separate aspects such as data anonymity, connection anonymity, and personalization [1], [2]. *Anonymizer* provides poor connection anonymity since there is only one proxy. It also provides average data anonymity as each exchanged Web page is secured by hiding the users requests. Finally, it does not provide any kind of personalization. *Crowds, Onion Routing* and *Hordes* provide high-level connection anonymity because of jondos. Although *Crowds* and *Hordes* achieve medium level of data anonymity, *Onion Routing* provides a higher level because it uses stronger cryptography techniques. However, none of these systems supports personalization. *P3P* and *TRUSTe* do not provide any kind of connection anonymity. They support data anonymity and personalization, though the degree of success depends on the users' decisions. *LPWA's* connection anonymity is low since there is only one HTTP proxy. It achieves average data anonymity as well as high personalization due to pseudonyms. *Freedom* supports connection anonymity due to asymmetric cryptography. It also achieves data anonymity and personalization because of pseudonyms and cryptography.

3.3.2 Low Cost

Nowadays Web users insist on buying tools of low cost and average quality. Most of PETs, except Anonymizer and *Freedom*, are freely provided through Internet. There is also a development cost concerning application based on *Crowds*, *P3P* and *Hordes*.

3.3.3 Usability

Easy to use applications are preferred. *Anonymizer* and *LPWA* are very usable, as only a few fields should be completed with usual or special characters. *Crowds* and *Onion Routing* are demanding protocols due to selection of companions and multi-layer cryptography. *TRUSTe* is the most convenient PET because the user should only read a comprehensible document. *P3P* provides average usability since the user should be familiar with privacy policies to make the appropriate decisions. *Hordes'* forward routing and the cryptographic techniques being used specify its usability. *Freedom* provides average usability since the user has to create an asymmetric pair of keys.

3.3.4 Services

The majority of the examined tools or protocols do not directly support Internet services. On the other hand *LPWA* and *Freedom* use anti-spamming e-mail filters.

3.4 Comparison Results

The following comparison table summarizes the deductions from the above sub-sections according to three categories of comparison criteria.

Table 1. Comparative Analysis of PETs (**H**igh, **M**edium, **L**ow, x ≡ Not applied)

Criteria / Technologies	Trace back attack (active)	Trace back attack (passive)	Malicious Collaborators	Eavesdroppers	Message Attacks	Timing Attacks	Flooding Attacks	Connection Period Attacks	Cookies	Personalized Service	Reliablility	Installation Complexity	Performance	Overhead Latencies	Connection Anonymity	Data Anonymity	Personalization	Low Cost	Usability	Services
	Confronted Security Threats							Applied Techn. Issues							Satisfied User Demands					
Anonymizer	–	–	x	–	–	–	–	–	–	–	H	L	H	L	L	M	x	L	H	L
Crowds	+	–	+	+	+	–	–	–	–	–	L	H	L	H	H	M	x	M	L	L
Onion Routing	+	–	+	+	+	–	–	–	–	–	L	H	L	H	H	H	x	H	L	M
TRUSTe	x	x	x	–	–	–	–	–	+	+	H	L	H	L	x	x	x	H	H	L
P3P	x	x	x	–	–	–	–	–	+	+	H	L	H	L	x	x	x	M	M	L
LPWA	–	–	x	–	–	–	–	–	+	+	H	M	H	L	L	M	H	H	M	H
Hordes	+	–	+	+	+	–	–	–	–	–	M	H	M	H	H	M	x	M	L	L
Freedom	–	+	x	+	+	–	–	–	+	+	H	M	M	L	H	H	H	L	M	H

4 Conclusions

The weakest and strongest points of each system differ since their design is not focused on identical parameters. Indeed, technologies that are based on single HTTP proxies such as *Anonymizer*, and *LPWA* could be easily used to achieve anonymous browsing while *Crowds*, *Onion Routing* and *Hordes* succeeds in data protection and attackers' confrontation. On the other hand, *TRUSTe* and *P3P* have great performance and guarantee the presentation and negotiation of security policies provided from e-Government services. Although *Freedom* provides average protection from security threats its high cost downsides these advantages. Moreover, *Onion Routing* could be used as a basis over which other protocols would be established in order to achieve higher level of protection. Furthermore, *TRUSTe* and *P3P* negotiation techniques may be used as a trusted third party so as to ensure that e-Government sites do not violate legitimate security policies or diffuse privacy data.

References

1. Carlos A. Osorio: A new framework for the analysis of solutions for privacy – enhanced Internet commerce. eJeta-PRIVACY (2001)
2. Brain Neil Levine, Clay Shields: A Protocol for Anonymous Communication Over the Internet. Conference on Computer and Communications Security, Proceedings of the 7th ACM conference on Computer and communications security Athens, Greece (2000)
3. Reiter M., Rubin A., "*Crowds*: Anonymity for Web transactions", in *ACM Transactions on Information and System Security*, Vol. 1, (1998)
4. McCullagh A., "The establishment of trust in the electronic commerce environment", in the *Proc. of the Information Industry Outlook Conference*, Australia, (1998)
5. Goldberg I, Wagner D. Brewer E., "Privacy-enhancing technologies for the Internet", in *Proc. of IEEE COMPCON '97 Conference*, (1997)
6. Philippe Boucher, Adam Shostack, Ian Goldberg: *Freedom* System 2.0 Architecture. Zero-Knowledge Systems, Inc. (2000)
7. *The Platform for Privacy Preferences 1.0 Spec,* W3C Candidate Recommendation 15, (2000)
8. Cranor L., "Internet privacy", in *Com. of the ACM*, Vol. 42, No. 2, pg. 29-66, (1999)