Privacy-Aware Network Client Pattern

Mauricio Sadicoff, Maria M. Larrondo-Petrie, and Eduardo B. Fernandez
Dept. of Computer Science and Engineering
Florida Atlantic University, Boca Raton, FL 33431
mlevy@hypersol.com, petrie@fau.edu, ed@cse.fau.edu

This pattern provides a way to make a user of a network site aware of the privacy policies followed by that site. It introduces the concept of a Privacy Proxy to enhance the user's comprehension of any privacy-related concerns. Even though the current uses of this pattern are constrained to the web browsing domain, it can have a more general use.

1. Example

The users in our company connect to websites for a variety of purposes, including product search, component purchasing, and looking for general information. Every interaction may require the user to provide some information and our users may unwittingly provide too much information. This extra information could be used later to steal their identities or to send spam to them. We would like our users to be aware of what information the sites really need to collect and to learn to avoid sites that require unnecessary information and do not guarantee privacy.

2. Context

Users interacting with Internet sites that sell goods or provide services, where to have access one needs to provide some personal information.

3. Problem

A main concern about privacy is the awareness level of the user. A network server can use a standard such as P3P to conveniently publish privacy policies [P3p01], which describe how each connecting user's private data is gathered and utilized. However, how can we ensure that a user connecting through a network client will be made aware of these policies prior to divulging this data?

The possible solution is constrained by the following forces:

- Privacy policies must be displayed to the user in a form that can be clearly understood.
- The user must be able to select what information can be gathered and used through a simple, easy-to-use interface.
- Privacy policies may change and the user must be able to see the latest ones; otherwise she might follow obsolete policies that may compromise her privacy.

4. Solution

Define a privacy proxy that will be able to understand the machine-readable policies made available by the server and translate them to easy-to-use human-readable form for the user.

Structure

Figure 1 shows a class diagram for the relationships between the user, the server, and the proxy. Each server can publish many policies and each user can be made aware of many policies at a time through the proxy.

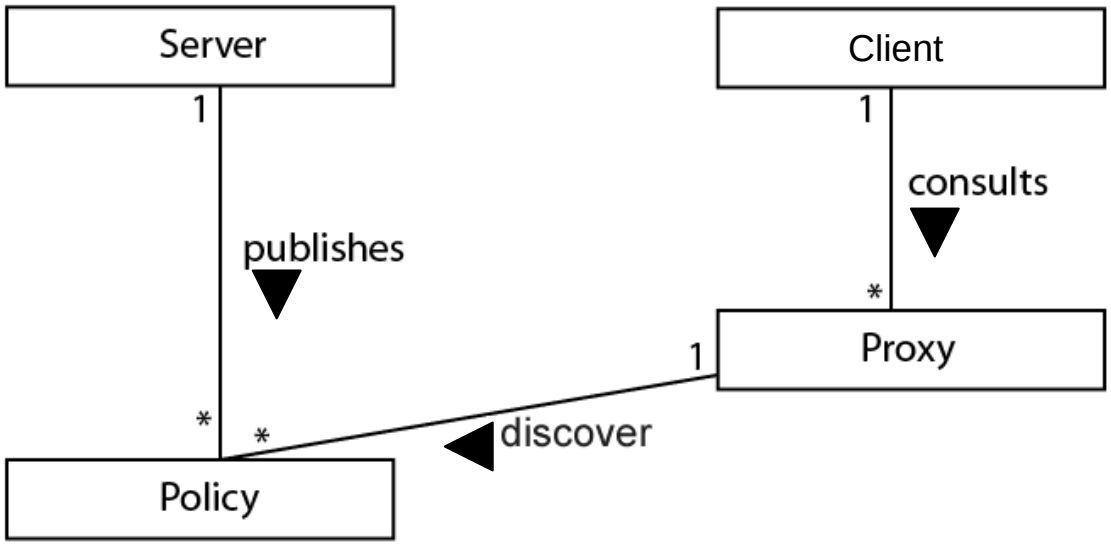

Figure 1: The Privacy-aware Network Client pattern

Dynamics

In Figure 2, a user wishes to access some information or interact with files on the server, which publishes its privacy Policy. The access occurs in the following sequence:

- The User interacts with the Server through a network Client.
- The Client consults the Proxy for privacy policies.
- The Proxy discovers the correct Policy (or Policies) made available by the Server, for the information or files in question.
- The Proxy displays a user-friendly screen to the User requesting approval of the Policy, prior to allowing access to the information or permitting the interaction.
- The User makes a decision after reviewing the Policy.

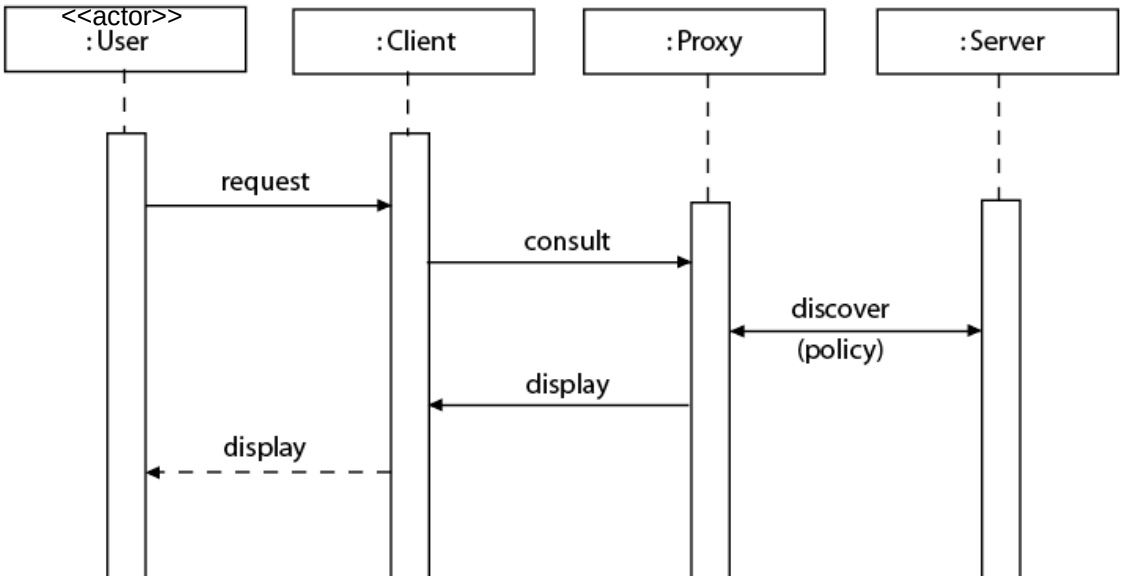

Figure 2: Sequence diagram for performing an interaction through a privacy-aware client.

5. Implementation

- Design and implement a proxy able to parse and interpret privacy policies written in some standard language. This proxy could be built as a specialized version of the Proxy pattern [Gam95]. The proxy could be able to interpret several privacy languages or just one of them. Successful use of the pattern requires that the proxy can understand the server's privacy language.
- Design and implement a secure communication channel between network clients and their proxies. This is necessary to avoid interception of the user choices by malicious users.

6. Example resolved

With the use of this pattern our users have now a clear view of the privacy policies of the sites they visit. Unnecessary information is not provided anymore and they know what sites to avoid.

7. Known uses

- JRC P3P Proxy Version 2.0
    i. From [P3p01]: "*The JRC P3P Proxy Version 2.0 is a P3P user agent, which acts as an intermediary agent (the middleman) that controls access to remote web servers dependent upon the privacy preferences a User specifies.*"
- Mozilla P3P Privacy Policy Viewer

i. Version 7 of the Mozilla web browser has an extension called Privacy Policy Viewer [Net01], which implements a P3P reader and displays privacy policies for each site in human-readable format. Figure 3 shows its interactions.

ii. From [Net01]: "*The new Privacy Policy Viewer lets a user easily locate and view the privacy policies of P3P-compliant sites.*"

- AT&T Privacy Bird
  i. AT&T's Privacy Bird implements a complete Proxy for web browsing which displays warnings when a website gathers private information. Note that the user's response may have been previously determined and saved in a local software profile.
  ii. From [Att01]: "*The AT&T Privacy Bird lets you see what's really going on at Web sites. The bird icon alerts you about Web site privacy policies with a visual symbol and optional sounds.*"
- Internet Explorer 6 for Windows XP (cookie privacy)
  i. Internet Explorer is a partial implementation of this pattern. It protects only cookies and its policy display capabilities are minimal, only supporting reading of P3P policies.
  ii. It allows the user control over cookie privacy, however. From [Mxp01]: "After reviewing the P3P privacy policy, you can specify how you want Internet Explorer to handle cookies from the selected Web site. If you want Internet Explorer to determine whether or not to allow this Web site to save cookies on your computer by comparing the privacy policy with your privacy settings, select **Use my privacy settings**. If you want Internet Explorer to always allow cookies from this Web site to be saved on your computer, select **Always allow this site to use cookies**. If you want Internet Explorer to never allow cookies from this Web site to be saved on your computer, select **Never allow this site to use cookies**.″

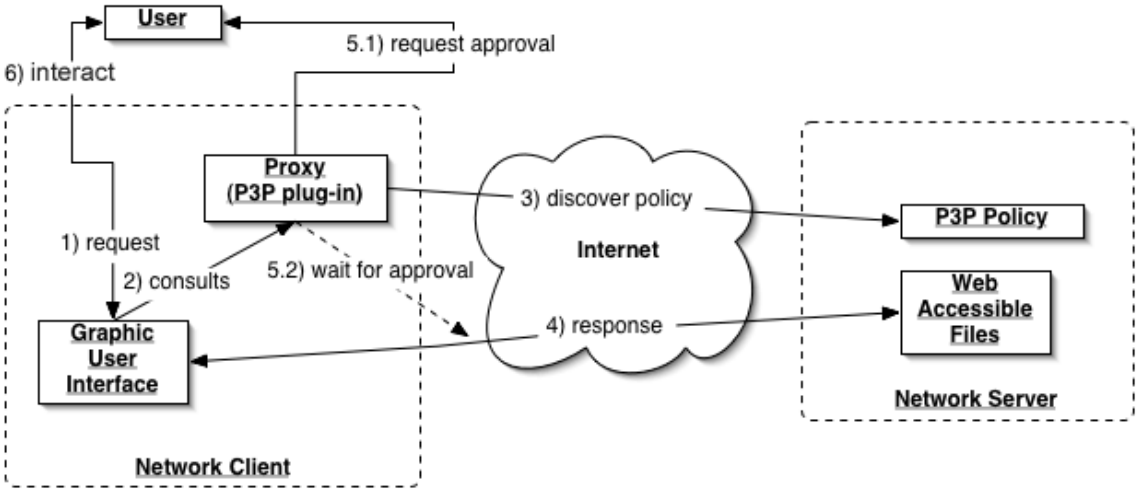

Figure 3: Privacy-aware Network Client (Mozilla) example

Figure 3 illustrates a typical use of the pattern, using the Mozilla P3P Privacy Policy Viewer example, which follows the steps:

1. User requests interaction with Server to Network Client.
2. Client consults Proxy, which can be internal to client or an external plug-in.
3. Proxy discovers the Policy published by the server over the Internet.
4. The Server responds to the Client's request.
5. Proxy seeks the User's approval to the interaction. This may or may not include a step in which the Proxy can block the interaction in case the User does not approve the Policy.
6. Privacy conscious, the User continues the interaction.

8. Consequences

The Privacy-Aware Network Client Pattern has the following advantages:

- The User can always be conveniently aware of the privacy policies for a specific interaction, allowing a better informed decision prior to releasing private information.
- Though it has been used only for web-related activities, it is an appropriate pattern for general use, such as database access that could potentially deal with private information.
- Changes in privacy policies of the server will automatically be detected through the Proxy.

The Privacy-Aware Network Client Pattern has the following liabilities:

- Extra overhead in network connectivity, since every access to a privacy-sensitive area needs a separate secure connection for the Proxy. This can potentially be reduced through the use of a cache.
- The pattern's concern is with the connection to the Server and the network connectivity issues only. The privacy-related constraints need to be stored locally in the Client's operating environment. Any knowledgeable attack to that machine could potentially compromise privacy.
- If the Server administrators can show (based on the user interactions) that a Privacy-Aware client has been used for a specific access, then any claims of privacy breaches can be directly blamed on the client.
- It requires that all sites use one or a small set of privacy languages.

9. Related patterns

Proxy [Gam95]. The Privacy-Aware Network Client uses a specialized version of the Proxy pattern.

Web Shopping Process [Fer01]. This is one of the patterns most likely to be combined with this pattern.

Adaptive Web Applications [Koc02]. These are patterns for web applications that change their behavior according to the current user. They would display more or less complete privacy disclosures depending on the type of user.

Acknowledgements

This work was supported by a grant from the US Dept. of Defense (DISA), administered by Pragmatics, Inc. Our shepherd, Bob Hanmer, provided valuable comments.

References

[Att01] AT&T Privacy Bird, http://www.privacybird.com

[Fer01] E. B. Fernandez, Y. Liu, and R.Y. Pan, "Patterns for Internet shops ", *Procs. of PLoP 2001,* http://jerry.cs.uiuc.edu/~plop/plop2001/accepted_submissions/accepted-papers.html

[Gam95] E. Gamma, R. Helm,R. Johnson, and J. Vlissides, *Design patterns –Elements of reusable object-oriented software*, Addison-Wesley 1995.

[Koc02] N. Koch and G. Rossi, "Patterns for adaptive web applications", *Procs. of EuroPLoP 2002.*

[Mxp01] Microsoft Windows XP Professional Product Documentation, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/privacy_policy_view.mspx

[Net01] Netscape 7 Reviewers Guide, http://channels.netscape.com/ns/browsers/7/learnmore/NS70pr1_reviewersguide.pdf.

[P3p01] P3P Resources in the Joint Research Centre (JRC), http://p3p.jrc.it/

[W3c01] W3C References for P3P Implementations, http://www.w3.org/P3P/implementations