dit UPM

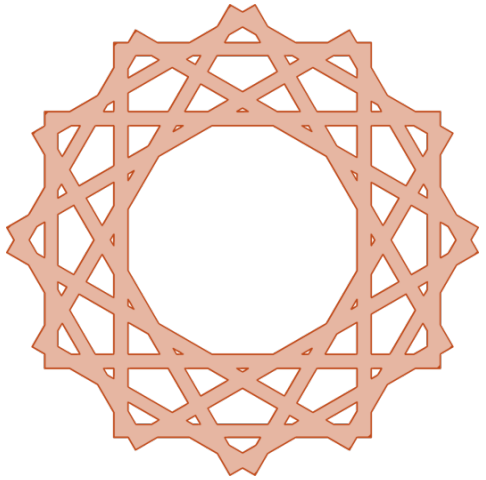
ESCUELA POLITÉCNICA NACIONAL

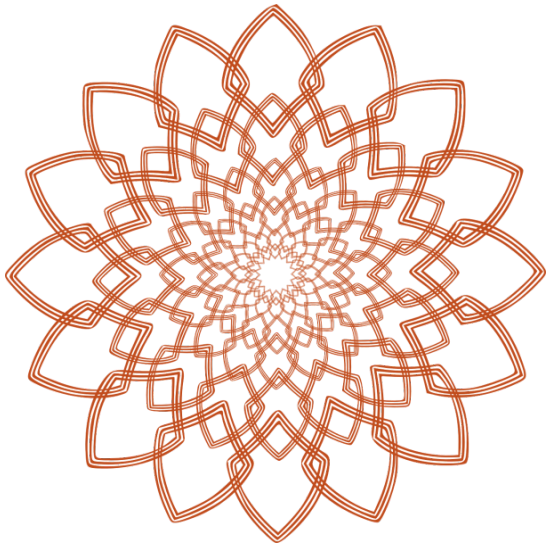
Patrones de privacidad

Julio César Caiza

En colaboración con:
José María del Álamo
Danny Santiago Guamán

Patterns





A simple definition:
"A **solution** for a recurrent **problem** in an specific **context**".

Their roots appear in Alexander's work in Architecture domain (1977).

Basic example (Door Lock*)

- Context: You are the owner of a house in an area where you cannot leave your property freely accessible to all people because this might attract thieves. The building can be accessed through doors.
- Problem: You want to control access to the building.
- Forces:
  - Ÿ Selective access rights: You want to ensure that only you and some selected other people have access to the building. Others shall not.
  - Ÿ Protection: You want to protect your property but you cannot be at home all the time or ask somebody else to watch your belongings. Even when you are at home you might want to protect yourself together with your belongings to have a peaceful sleep.

* Example from site http://www.europlop.net/

Basic example (Door Lock*)

- Forces:
  - Ÿ Effort of access: Access to your property should be easy for you any time whereas it should be very difficult for any intruders to get inside.
  - Ÿ Storage of permission: Permission should be easy to use and reliable to store.
  - Ÿ Change of permission: While it should be easy to enable other people to get in, it should be easily possible to revoke this ability from them.
- Solution: Integrate a mechanism to all relevant doors of the building that can be repeatedly operated from both sides of the door by a matching key to allow or prevent the door from being opened.

Patterns in Computer Science

- A concept applied to other domains as Computer Science. Well known examples exposed by Gamma et al. (Gang of Four) in "*Design patterns: elements of reusable object-oriented software*".

Figure from [B. Bafandeh Mayvan, A. Rasoolzadegan, Z. Ghavidel Yazdi, The state of the art on design patterns: A systematic mapping of the literature]

Patrones de privacidad

- Resuelven problemas recurrentes en contextos determinados en el dominio de la privacidad.
- Estructura básica:
  - Nombre
  - Contexto
  - Problema
  - Solución
- Secciones opcionales
  - Implementación
  - Consecuencias
  - Ejemplos
  - Relaciones

Ejemplo 1 (Privacy policy display)

Problem

Users need to be well informed about possible consequences when releasing personal data upon certain actions such as login, registration, payments, etc. Art. 10 EU Directive 95/46/EC requires that data subjects are at least informed about what personal data are processed, by whom (i.e. the identity of the controller), and for what purposes.

However Jensen and Potts (2004) as well as Protor et al. (2006) showed that privacy statements posted on web sites contain long legal phrases that are usually not comprehensible to most end users.

Solution

Provide the user with all necessary information on what kind of data is to be disclosed to whom and for what purposes it is used. The user should not be given too much and unnecessary information. The user should not be bothered with cumbersome work, for example in case of recurring visits. Therefore he should have the possibility to create customized settings. It is utterly important that the user understands possible consequences in order to make well-informed decisions.

The complexity of privacy notices can be better managed by following the Art. 29 Working Party's recommendation of providing information in a "multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions" [3]. They suggest three layers of information provided to individuals:

- short notice (layer 1)
- condensed notice (layer 2)
- full notice (layer 3)

The prototype of a menu-based approach for selecting Credentials developed within PRIME, which follows the Art. 29 Working party recommendation is shown below and is further described in (Pettersson 2008).

Ejemplo 1 (Privacy policy display)

Figure 1: Prototype of a menu-based approach for selecting Credentials

Ejemplo 1 (Privacy policy display)

Use when

This approach should be employed whenever the user is required to enter personal data such as login, credit card or other private information. Through this multi-layered approach, the user obtains information on why what information is requested, by whom it is required and what it is used for. Furthermore, a link to the condensed or full privacy policy needs to be displayed.

How

The Art. 29 Working Party (2004) recommends providing information in a "multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions". They suggest three layers of information provided to individuals: The short notice (layer 1) must offer individuals the core information required under Article 10 of the Directive 95/46/EC, which includes at least what data is requested, the identity of the controller and the purpose of processing. In addition, a clear indication must be given as to how the individual can access additional information. The condensed notice (layer 2) includes in addition all other relevant information required by Art. 10 of the Directive such as recipients or categories of recipients, whether replies to questions are obligatory or voluntary and information about the individual's rights. The full notice (layer 3) includes in addition to layers 1 and 2 also "national legal requirements and specificities."

Why

Informed users are able to make informed decisions which lead to a more responsible handling of their personal data. The EU Directive 95/46/EC therefore also requires that certain information needs to be provided to the user when personal data is requested from him.

Related Patterns

- Dynamic Privacy Policy Display
- Privacy Aware Wording

Ejemplo 2 (Privacy Options in Social Networks)

Problem

In social networks users have the possibility to provide data about themselves, but not all data should be visible to all users. To differentiate which user is allowed to see which data is very important for privacy, so the users should be able to control their visibility of information.

Solution

The solution for this problem is a selective access control for social networks.

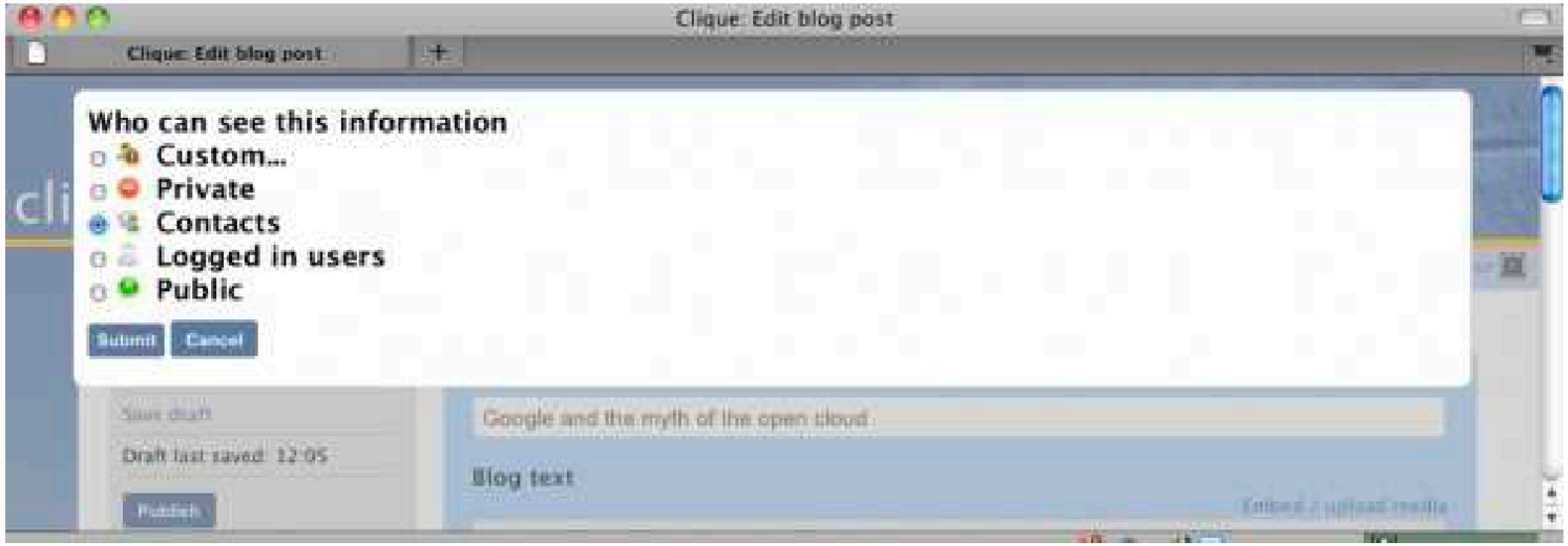


Figure 48: Selective Access Control

Ejemplo 2 (Privacy Options in Social Networks)

Use when

This tool should be used in social networks to guarantee privacy.

How

Give users the possibility to create different social groups like family, friends, co-workers…

Another point is the possibility to create "pseudonyms" – this means that a user has one login with one address book and one administration screen but more than one identity inside the system.

If a user creates or modifies a message he should be asked each time for the privacy settings, e.g. just the social group "family" is allowed to read is post.

A selective access control gives users the possibility to choose in their privacy settings who can see which information.

Users should be also able to look at their own profile from the view of another user; this view helps users to maintain control over their audiences.

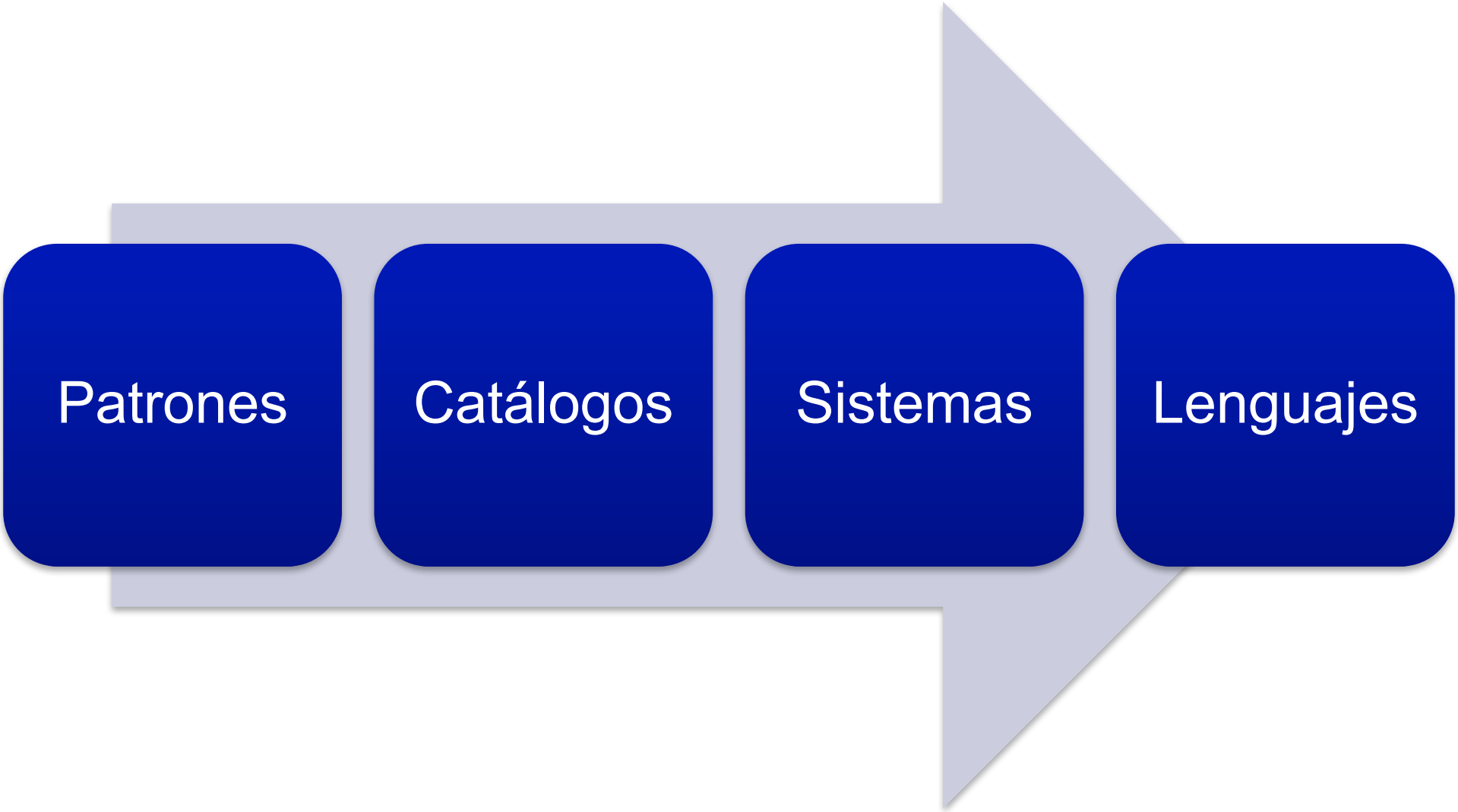
Why

The goal is, to give the user the possibility for individual privacy settings and guarantee higher privacy in social networks.

Related Patterns

- Privacy Awareness Panel in Collaborative Workspaces
- Privacy Enhanced Group Scheduling
- Selective Access Control in Forum Software

Evolución de los patrones



Colecciones de patrones de privacidad

- E.S. Chung,et al., Development and evaluation of emerging design patterns for ubiquitous computing. 2004.
- S.Fischer-Hübner et al., HCI Pattern Collection – Version 2. 2010.
- N. Doty and M. Gupta. Privacy Patterns. 2011. https://privacypatterns.org/
- PRIPARE Project. Collecting patterns for better privacy. 2015. https://privacypatterns.eu/

privacypatterns.org

Colecciones de patrones de privacidad

- O.Drozd. Privacy Patterns. 2016. http://privacypatterns.wu.ac.at:8080/catalog/
- M. Colesky et al., A system of privacy patterns for user control. 2018. Integrated in https://privacypatterns.org/
- M. Colesky et al., A System of Privacy Patterns for Informing Users: Creating a Pattern System. 2019 Integrated in https://privacypatterns.org/

Patterns for Privacy - P4P

Privacy Design Patterns (Community)

Contributions:

- A common online catalog.
- A common template for patterns.
- Systems of patterns

Patrón: ENRUTAMIENTO POR LOTES

- Estrategia: Ocultar
- Táctica: Mezclar
- Nombre: ENRUTAMIENTO POR LOTES
- Resumen:
  - ENRUTAMIENTO POR LOTES sugiere recoger los paquetes entrantes en una “red de mezcla” (mix network), y enrutarlos en un lote.

Patrón: ENRUTAMIENTO POR LOTES

- Contexto: ANONYMITY SET in a mix network is created by mixing a sender's incoming packets with packets from other sources, and morphing data representation. However, there remains a strong causal relationship between between incoming and outgoing messages. Unless this relationship is hidden, an adversary can correlate input with output messages.
- Problema: How can the output ofa mix node prevent timing analysis attacks?
- Solución: Collect the input data packets, and when the collection reaches a limit, output all the data packets together in a batch.

Patrón: ENRUTAMIENTO POR LOTES

- Ejemplos:
- El reto principal es identificar la estrategia de agrupación por lotes para un dominio de aplicación en particular. Aquí algunos ejemplos:
  - Ÿ - En una "red de mezcla" (mix network), se pueden adoptar diferentes estrategias de agrupación. Una mix network basada en umbral recoge n mensajes y luego los envía a todos. Una mix network basada en tiempo, envía un lote completo cada t segundos. Una mix network puede combinar las dos estrategias, por ejemplo, enviar un lote cuando transcurre un tiempo t y solo si se ha alcanzado el umbral. Mixmaster [9] y Mixminion [13] siguen esta estrategia, pero en vez de enviar el lote entero, ellos envían solo una fracción del lote.
- …
  - Ÿ - Algunos sistemas basados en localización utilizan el mecanismo de camuflaje temporal [29]. En este mecanismo, un sistema oculta la información de la ubicación de un agente, hasta que k agentes hayan visitado la zona de la mix network. El tiempo transcurrido hace que las coordenadas espaciales de un agente sean menos precisas.

Patrón: ENRUTAMIENTO POR LOTES

- Consecuencias:
  - Ÿ La agrupación por lotes aumenta el coste de un ataque de combinación [30] y de un ataque de intersección [30]. Sin embargo, genera otros problemas ya que hace que el anonimato dependa del comportamiento de los otros usuarios. Los mensajes en una mix network en reposo pueden ser retrasados por un largo tiempo. Una mix network en reposo puede eliminar un mensaje o enviarlo con el riesgo de violar el anonimato.
- Relaciones:
  - Ÿ ENRUTAMIENTO POR LOTES es usado con TRÁFICO DE RELLENO.

- ¡Gracias!