Compartir Inteligencia:
Construcción de un Catálogo de Patrones de Seguridad

Universidad Tecnológica Nacional, Argentina

Facultad Regional Santa Fe – CIDISI

CIBSI 2013 – Ciudad de Panamá - 29/10/2013

Agenda

- ✓ Software Seguro
- ✓ Atributos de seguridad
- ✓ Pregunta guía
- ✓ Concepto de patrón de seguridad
- ✓ Catálogos: Necesidad
- ✓ Atributos de un patrón
- ✓ Ejemplo de catalogación
- ✓ Prototipo de catalogación y búsqueda
- ✓ Trabajo futuro

Software Seguro

Proceso de desarrollo seguro

Procesos y practicas

Reducir:

- Errores
- Debilidades

<u>Etapas Básicas:</u>

- Especificación
- Diseño
- Desarrollo
- Despliegue

Problemas de seguridad

Características

Atributos

- Confidencialidad
- Integridad
- Disponibilidad
- Responsabilización
- No-Repudio

Los atributos en sí:
No hacen seguro al software en forma directa.
Ayudan a caracterizar cuando es seguro.

Atributos I

- **Confidencialidad**: Tiene que asegurar que sus características, activos que administra y contenido esta enmascarado u oculto de entidades no autorizadas.

- **Integridad**: El software y sus activos es resistente y flexible a la subversión, ya sea de modificaciones no autorizadas por entidades autorizadas o cualquier tipo de modificación por parte de entidades no autorizadas. Involucra tanto desarrollo como ejecución.

Atributos II

- **Disponibilidad**: El software tiene que estar operativo y accesible a usuarios autorizados y sus privilegios y funcionalidad inaccesibles a usuarios no autorizados en todo momento. Se definen dos atributos adicionales asociados a los usuarios.

- **Responsabilización**: Toda acción relevante relacionada con la seguridad debe ser registrada y rastreada con atribución de responsabilidad, permitiendo que sea posible tanto durante como a posteriori de las acciones.

- **No-Repudio**: Prevenir que el software que actua como usuario desmienta o niegue la responsabilidad de las acciones. Evita subvertir o eludir el atributo responsabilización.

Pregunta Guía

- ✓ **¿Cómo encontrar un solución probada y reutilizable a un problema de seguridad en el desarrollo de una solución de software?**

Patrón de Seguridad

Teoría  Practica

Patrón de Seguridad

- ✓ **“Cada patrón es una regla de tres partes, expresada como una relación entre un determinado contexto, un determinado sistema de fuerzas que ocurren repetidamente en este contexto, y una determinada configuración de software que permite que estas fuerzas se resuelvan a sí mismas.” (Coplien, J.)**

- ✓ **Es una solución probada a un problema de seguridad recurrente en un sistema de software.**

Catálogos

- ✓ **Los patrones existentes no siguen un criterio común de definición (plantilla).**
- ✓ **Necesidad de definir un criterio común para catalogar los patrones.**
- ✓ **Un *catálogo centralizado* es una herramienta que actúa como *punto de partida* para la búsqueda e identificación de una o más soluciones a un problema de seguridad.**

Atributos de un Patrón

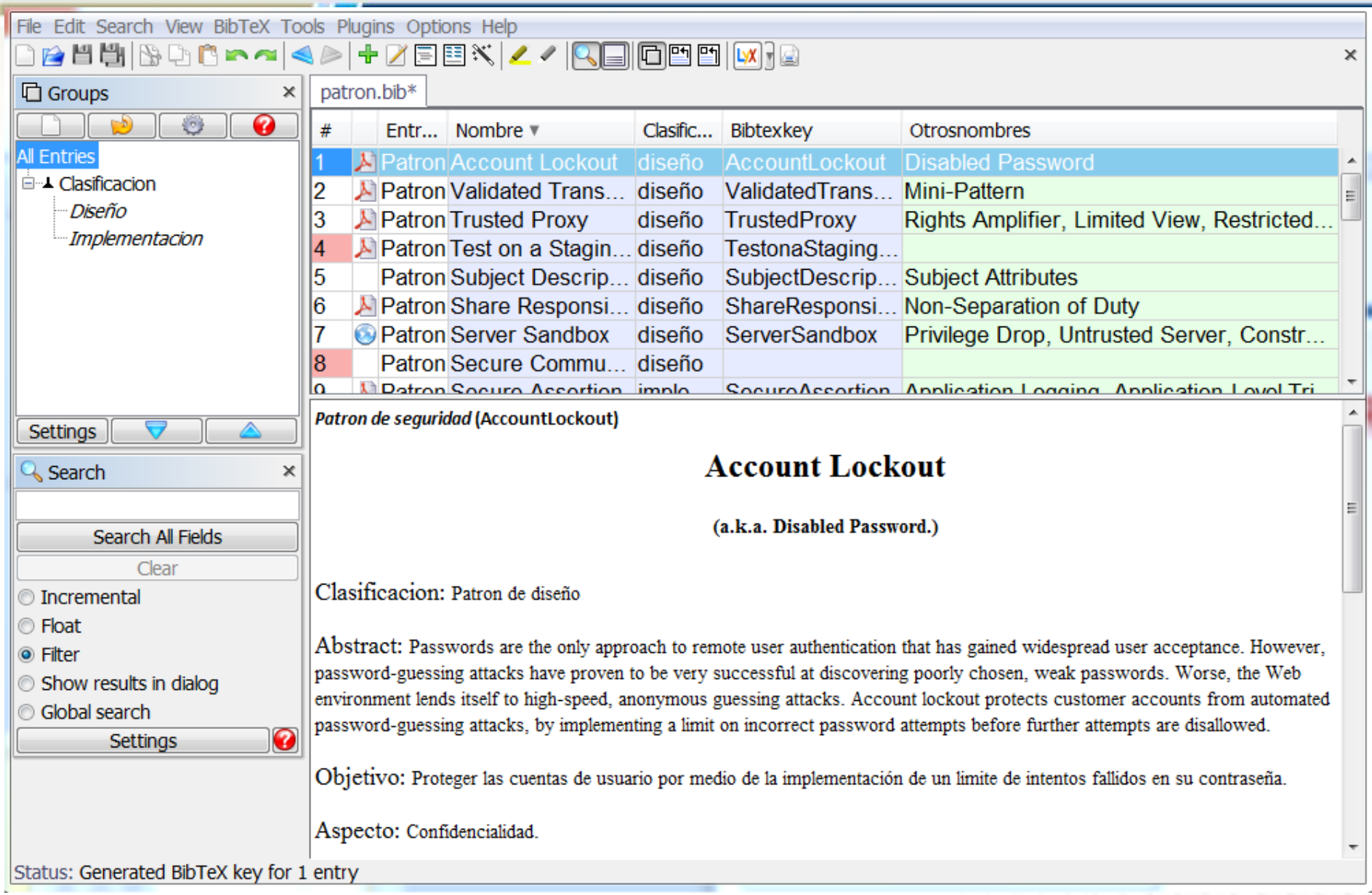
Nombre	El nombre de la definición original del patrón de seguridad.
Objetivo	Problema que resuelve el patrón de seguridad. Es una respuesta a un problema de seguridad presente.
Clasificación	En base a la fase del proceso de desarrollo de software en la que normalmente se aplica el patrón: requerimientos, análisis, diseño, codificación, pruebas, implementación.
Aspecto de seguridad afectado	Confidencialidad, integridad, disponibilidad, responsabilización, no-repudio
Palabras claves	Sirven como una referencia complementaria al patrón.
Referencia bibliográfica	Enlaces hacia los documentos y/o páginas web donde se encuentra la descripción detallada del patrón.

Ejemplo

Nombre	**Authenticated Session**
Objetivo	Permitir el acceso a múltiples páginas con acceso restringido, sin tener que re-autenticarse cada vez. Mantener información de autenticación en la navegación de un sistema.
Clasificación	Diseño
Aspecto de seguridad afectado	Responsabilización, Integridad.
Palabras claves	Autenticación, Single Sign-On
Referencia bibliográfica	Security Patterns Repository v1.0.pdf Cunningham, C. “Session Management and Authentication with PHPLIB”. http://www.phpbuilder.com/columns/chad19990414.php3, (Rev. Mayo 2013). Kärkkäinen, S. “Session Management”. Unix Web Application Architectures. http://webapparch.sourceforge.net/#23, October 2000. (Rev. Mayo 2013)

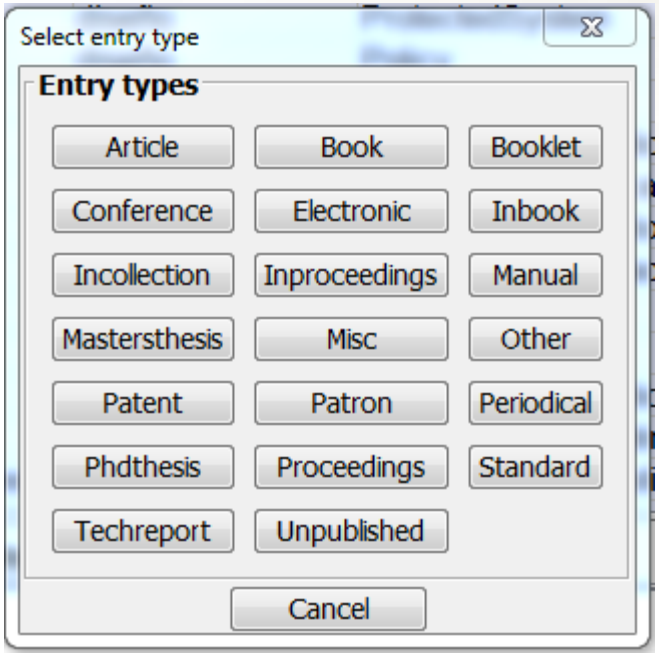
Prototipo

- ✓ **JabRef : software de gestión de referencias bibliográficas configurable.**
- ✓ **Entry Types: definición de un tipo especial.**
- ✓ **Portabilidad aplicación y de documentos referenciados**


File Edit Search View BibTeX Tools Plugins Options Help
Groups
All Entries
Clasificacion
Diseño
Implementacion
Settings
Search
Search All Fields
Clear
Incremental
Float
Filter
Show results in dialog
Global search
Settings
patron.bib*
Entr... Nombre Clasific... Bibtexkey Otrosnombres
1 Patron Account Lockout diseño AccountLockout Disabled Password
2 Patron Validated Trans... diseño ValidatedTrans... Mini-Pattern
3 Patron Trusted Proxy diseño TrustedProxy Rights Amplifier, Limited View, Restricted...
4 Patron Test on a Stagin... diseño TestonaStaging...
5 Patron Subject Descrip... diseño SubjectDescrip... Subject Attributes
6 Patron Share Responsi... diseño ShareResponsi... Non-Separation of Duty
7 Patron Server Sandbox diseño ServerSandbox Privilege Drop, Untrusted Server, Constr...
8 Patron Secure Commu... diseño
Patron de seguridad (AccountLockout)
Account Lockout
(a.k.a. Disabled Password.)
Clasificacion: Patron de diseño
Abstract: Passwords are the only approach to remote user authentication that has gained widespread user acceptance. However, password-guessing attacks have proven to be very successful at discovering poorly chosen, weak passwords. Worse, the Web environment lends itself to high-speed, anonymous guessing attacks. Account lockout protects customer accounts from automated password-guessing attacks, by implementing a limit on incorrect password attempts before further attempts are disallowed.
Objetivo: Proteger las cuentas de usuario por medio de la implementación de un limite de intentos fallidos en su contraseña.
Aspecto: Confidencialidad.
Status: Generated BibTeX key for 1 entry

JabRef

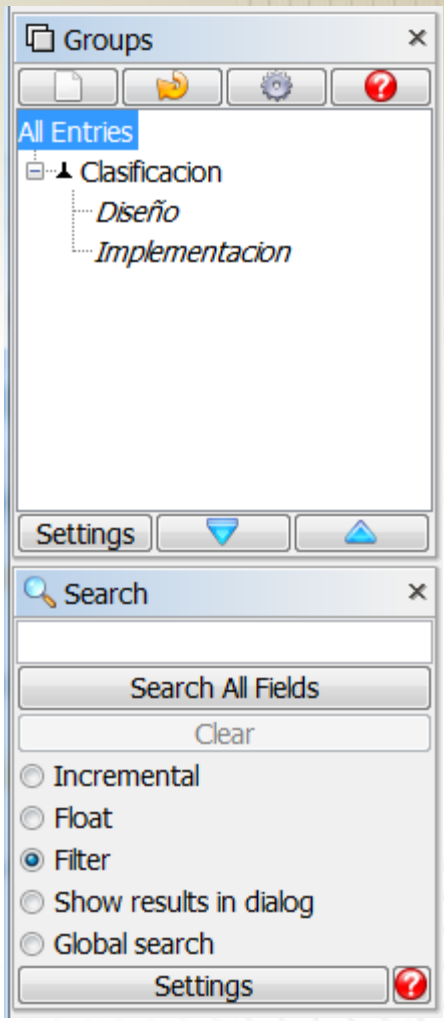
Tipos de entrada



JabRef

Selección por grupo, ya definido uno para la clasificación por Fase de desarrollo.

Campo de búsqueda, filtrado de palabras por campo o todos los campos según se requiera.



patron.bib*

#		Entry...	Nombre	Clasifica...	Bibtexkey	Otrosnombres
1		Patron	Account Lockout	diseño	AccountLockout	Disabled Password
2		Patron	Validated Transaction	diseño	ValidatedTransacti...	Mini-Pattern
3		Patron	Trusted Proxy	diseño	TrustedProxy	Rights Amplifier, Limited View, Restricted Chann...
4		Patron	Test on a Staging S...	diseño	TestonaStagingSe...	
5		Patron	Subject Descriptor	diseño	SubjectDescriptor	Subject Attributes
6		Patron	Share Responsibilit...	diseño	ShareResponsibilit...	Non-Separation of Duty
7		Patron	Server Sandbox	diseño	ServerSandbox	Privilege Drop, Untrusted Server, Constrained Ex...

Patron de seguridad **(ShareResponsibilityforSecurity)**

Share Responsibility for Security

(a.k.a. Non-Separation of Duty.)

Clasificacion: Patron de diseño

Abstract: The Share Responsibility for Security pattern makes all developers building an application responsible for the security of the system. Security consists of more than just encryption, anti-virus software, and firewalls. Any element of a system can have security concerns, and system developers have to understand and address those concerns. Use of this pattern avoids the common problem of "the security guy" or security team being pitted against the rest of the development team.

Objetivo: Distribuir la responsabilidad de los criterios de seguridad a todos los desarrolladores y no solo a una persona o equipo, buscando asi el equilibrio entre este aspecto y el resto de requerimientos funcionales y no-funcionales.

Aspecto: Responsabilización, No repudiación.

Patrones relacionados:

- Document Security Goals

Trabajo Futuro

- ✓ **Seguir completando el prototipo.**
- ✓ **Probar si los criterios definidos efectivamente funcionan y sirven.**
- ✓ **Analizar la factibilidad de desarrollar una aplicación Web para el Catálogo.**

Integran el equipo de trabajo

Marta Castellaro (UTN-FRSF)

Susana Romaniz (UTN-FRSF)

Juan Carlos Ramos (CIDISI – UTN-FRSF)

Ignacio Ramos (UTN-FRSF)

Contacto: iRamos@frsf.utn.edu.ar

¡¡¡ MUCHAS GRACIAS !!!