

An introduction to

Security Patterns

Matus Korman, 2009-04-17

What is a pattern?

- Solution to a problem that arises within a specific context
 - Describes both static (structural) and dynamic (processual) relationships of a solution
 - Presents a high-quality and proven solution that resolves the given problem
 - Tells a story and initiates a dialog on problem resolution
 - Promotes and requires human intelligence, never being an obvious solution

Other types of patterns

- Architectonic patterns of buildings
 - include different kinds of architectonic features describable as reusable patterns
- Patterns of behavior
- Patterns of object-oriented software design (introduced by the [Gang of Four])
- etc...

What a pattern should consist of (1)

- **Names** under which the pattern is known
- A real-world **example**
- **Context** in which the pattern may apply
- The fundamental **solution** principle
- **Structure** specification, using appropriate notations
- **Dynamics** describing the run-time behavior of the pattern in typical scenarios
- **Implementation** guidelines

What a pattern should consist of (2)

- Discussions on resolving the example, which have not yet been mentioned
- **Variants** or specializations of the pattern
- **Known uses** for the pattern, taken from existing systems
- **Consequences** – potential benefits and liabilities the pattern provides
- **See Also** or references to patterns in some way similar to the one described

Organizational context and the security-extended Zachman Frw.

	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION	SECURITY
Scope	List of things important to the business	List of processes the business performs	List of locations of business operation	List of business-important organizations	List of business-significant events/cycles	List of business goals/strategies	List of key business assets and protection needed
Business model	e.g. Semantic model	e.g. Business process model	e.g. Business logistics system	e.g. Workflow model	e.g. Master schedule	e.g. Business plan	e.g. Security risk assessment
System model	e.g. Logical data model	e.g. Application architecture	e.g. Distributed system architecture	e.g. Human interface architecture	e.g. Processing structure	e.g. Business rule model	e.g. Security service
Technology model	e.g. Physical data model	e.g. System design	e.g. Technology architecture	e.g. Presentation architecture	e.g. Control structure	e.g. Rule design	e.g. Security mechanisms
Detailed representations	e.g. Data definition	e.g. Program	e.g. Network architecture	e.g. Security architecture	e.g. Timing definition	e.g. Rule specification	e.g. Security device

Inspired by [Security Patterns]

Some groups of security patterns

- Enterprise Security and Risk Management patterns
- Identification and Authentication (I&A) patterns
- Access Control Model patterns
- System Access Control Architecture patterns
- Operating System Access Control patterns
- Accounting patterns
- Firewall patterns
- Secure Internet Application patterns
- Cryptographic Key Management patterns

Some examples of specific SPs

- Access Control Model patterns
 - Role-Based Access Control
 - Multilevel Security
- System Access Control Architecture patterns
 - Single Access Point
 - Security Session
- Firewall Architecture patterns
 - Proxy-Based Firewall
 - Stateful Firewall

References

- [Security Patterns]
Schumacher, M., Fernandez-Bugolini, E., Hybertson, D., Buschmann, F., Sommerlad, P.: *Security Patterns: Integrating Security and Systems Engineering*, John Wiley & Sons Ltd, England, 2006.
- [Patterns]
information available online at <http://hillside.net/patterns/>
- [Gang of Four]
Gamma, E., Helm, R., Johnson, R., Vlissides, J.: *Design Patterns – Elements of Reusable Object-Oriented Software*, Addison-Wesley Professional, 1995
- [PLoP]
Pattern Languages of Programming (conferences)
online information at <http://hillside.net/conferences/plop.htm>