Security Design Patterns

Ed Rodriguez
rodriguez_ed @ bah.com

Annual Computer Security Application Conference
(ACSAC ’03)
December 11, 2003
Agenda

• What is a “Pattern”
• Why are “Patterns” Useful and Important
• What is a “Security Pattern”
• Key Question about Security Pattern & Response
• Additional Considerations
• Where is Security Pattern Work Being Done
• Looking to the Future
What is a “Pattern”

- patterns have been with us for a very long time
- Patterns on the other hand are a much more recent concept
What is a “Pattern”? 

- “The Timeless Way of Building”\(^1\) establishes design patterns as a viable architecture design strategy
- While this work’s genesis is based on buildings architecture, this concept has been extended into the realm of software design

What is a “Pattern”? 

- The software architecture/design classic “Design Pattern: Elements of Reusable Object-Oriented Software”\(^2\) by the “Gang of Four” (GoF) presents a comprehensive framework of software design patterns
  - Taxonomy for these design patterns presented
  - Standard template used to describe the design patterns
- This is important since so much of the work done in the area of security patterns has been modeled after the GoF framework

*More on this Later*

\(^2\): “Design Pattern: Elements of Reusable Object-Oriented Software”, Erich Gamma, Richard Helm, Ralph Johnson & John Vlissides (a.k.a., Gang of Four or GoF), October 1994
Still ….. What is a pattern?

- Numerous definitions exist in open press
- Let start with some words from Alexander:

> “Each pattern describes a problem that occurs over and over again in our environment and then describes the core of the solution to that problem in such a way that you can use this solution a million times over without ever doing it the same way twice.”

- From the GoF we get:

> Software design patterns are “descriptions of communicating objects and classes that are customized to solve a general design problem in a particular context.”
Why are patterns useful and important?

- Captures in a standardize manner reusable knowledge on how to solve a recurring class of problems
  - Building architectures (Alexander)
  - Software component design (GoF)
  - Software architecture frameworks (Fowler)
  - Security (Yoder/Barcalow, et al)
- Goals (Demonstrated or perhaps purported)
  - Creation of re-usable artifact
  - Leverages expert knowledge to a broader audience
  - Results in a high quality product with less effort
What is a security pattern?

• Again, numerous definitions exist in open press
• Candidate definitions exist from:
  – The Open Group
  – Schumacher and Roedig
  – Romanosky
  – NAI Labs

“A security pattern **describe** a particular **recurring** security problem that arise in a specific context and presents a **well-proven generic scheme for its** **solution**”
Key Question Not Widely Discussed…

Does the concept of security patterns directly extrapolate out from other pattern frameworks?

• This key question that has not been definitively stated or discussed
• Recent work by Michigan State University (MSU) touches on some important aspects of this question
  – Is the GoF template appropriate for capturing security patterns??
  – Is the GoF taxonomy appropriate for security patterns??
  – What’s missing?? What’s unnecessary??
MSU Findings

• GoF template extended and modified
• Reaffirmed the GoF taxonomy
  – Structural
  – Behavioral
  – Creational
• Furthermore they identified three levels of abstraction
  – Application level
  – Host level
  – Network level
• They also “overlayed” the ten guiding principals defined by Viega and McGraw to provide additional security insight within the patterns
### MSU Extended and Modified Security Pattern Template

#### GoF Template
- Pattern name and classification
- Intent
- Also Known as
- Motivation
- Applicability
- Structure
- Participants
- Collaborations
- Implementations
- Sample Code
- Known Uses
- Related Patterns

#### Modified and Extended Template
- Pattern name and classification
- Intent
- Also Known as
- Motivation
- Applicability
- Assumptions
- Structure
- Participants
- Collaborations
- Behavior
- Constraints
- Implementations
- Sample Code
- Known Uses
- Related Security Patterns
- Related Design Patterns
- Related Principals
Candidate Topics to Support Further Refinement

• As the topic of software patterns has matured and grown, two emerging areas of interest have emerged
  – Enterprise level software patterns
  – Pattern-driven system and architecture development.

• Fowler and Akur books focus on enterprise design patterns and J2EE enterprise design patterns, respectively. They represent some of the leading work in these areas.
  – How does this trend affect security pattern efforts?
Candidate Topics to Support Further Refinement

- IBM’s view of this topic focuses on “Business Security Patterns”.
- Public literature proposes 5 specific business security patterns
  - Web Presence
  - Business to Consumer
  - Business to Business
  - Operational Security
  - High Assurance
- These business security patterns are used “to identify and understand the relationships between business goals, business risks, and security solutions”.
- These patterns make a quick link to required security services
Candidate Topics to Support Further Refinement

• IBM also notes that “security isn’t just a product, and it isn’t just a service. It’s a condition that is expected to be embedded in the process of creating value”

• While it is understood that security IS NOT the same as software, there’s an additional observation to be made

• The physical manner in which security is implemented and integrated into a system has two distinctive flavors:
  – The integration of security oriented COTS sw and hw components into the system
  – The development of new security critical components in the same manner as other custom code

• This may require further refinement of the security pattern template and the community’s thinking
Candidate Topics to Support Further Refinement

• While providing a coupling from patterns to security requirements and services, in general, is an appealing idea, there is an important extension to this concept

• Use of security patterns to assist in the DoD certification process
  – System design that use “validated” security patterns could achieve certification quicker and at less cost
  – Questions remain
    • How can we validate security patterns methodology?
    • How do we ensure that an implementation based on a ‘validated” security pattern is in fact secure?

• Within the DoD, this could be a high value use for security patterns
Where is security pattern work being performed?

- **PLoP**
  - Steady, continuous work in the development of security patterns
  - UML used extensively
  - Publications available on web site
- **The Open Group**
  - Draft catalog of security patterns available for “Limited Peer Review” dated April 2002
  - Level of activity not clear from web site
- **Michigan State University**
  - Efforts supported by various government grants
  - Briefing released in Sept 2003
Where is security pattern work being performed?

• Various web site focused on this topic
  – secuitypatterns.org
  – romanosky.org (early and continuing contributor)
Looking to the Future

- Focused efforts required to validate security pattern template and underlying concepts
- Need a broader and well thought out consensus on some of the issues raised
- Depending on various factors and forces, chance exists for security patterns to do to the security community what software patterns did to software!