Chapter 11: Secure System Development Using Patterns

Raimundas Matulevičius
University of Tartu, Estonia, rma@ut.ee

© Springer International Publishing AG 2017

Goal

• Overview of security patterns
• Discuss how security patterns should be applied to secure business processes and systems
• Presents a method for security requirements elicitation from business processes (SREBP)
Outline

• Security patterns
• Security pattern taxonomy
• Security risk-oriented patterns
• Security requirements elicitation from business processes
  – SREBP method
  – Pattern application
• Further reading
What is a Pattern?

A solution to a problem that arises within specific context

<table>
<thead>
<tr>
<th>Context</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>

How does pattern distinguish from an ordinary solution?

- Pattern describes:
  - Configuration of elements
    - Design outline
    - Code
  - Set of instruction to create the configuration of elements
    - Process
  - Presents high-quality proven solution
  - Reusability
  - Well expressed - initiates a dialog
No Pattern is an Island

• A pattern provides a self-contained solution for a specific problem but they are **not independent** of one another

• Refinement
  – Solution proposed by a particular pattern can often be implemented with help of other patterns
    • which resolve the problem of the original problem
  – Each pattern depends on the smaller patterns it contains and on the larger patterns in which it is contained

Patterns are Everywhere

• Mid 1990s - Object Oriented Design patterns
  – Most widely known patterns
    “Gang-of-Four” book in 1995

• Software architecture
• Programming levels
• Fundamental structure and workflow of application domain
  – Health Care, Corporate Finance
• Patterns spread in many other specific areas:
  – Concurrent networked systems and programming
  – Server Components
  – Human-computer Interaction
  – … many other specific areas

**Security** – interesting area
Security Patterns

[Schumacher et al., 2005]

- A security pattern describes
  - a particular recurring security problem
  - that arises in a specific security context
  - presents a well-proven generic scheme for a security solution

- Codify security knowledge in structured and understandable way
- Presentation is familiar to the audience
- Proven solutions improve the integration of security into enterprises where needed

Outline

- Security patterns
  - Security pattern taxonomy
    - Security risk-oriented patterns
    - Security requirements elicitation from business processes
      - SREBP method
      - Pattern application
      - Once Security Requirements Are Elicited
  - Further reading
Enterprise Security and Risk Management

- Enterprise considers security issues to fulfill the enterprise’s mission and to reach its goals.
Identification & Authentication

- Specific requirements and design for the identification and authentication services

Access Control Model

- High level models represent the security policies of the requirements
- Models define security constraints at
  - architectural level, application level, etc.
  - enforced by the lower levels
System Access Control Architecture

- Essential for systems that permit or deny their use explicitly
- Patterns deal with the architecture of the software systems

Operating System Access Control

- Access control in operating systems
  - Authenticator
  - Controlled process creator
  - Controlled object factory
  - Controlled object monitor
  - Controlled virtual address space
  - Execution domain
  - Controlled execution environment
  - File authorization
Accounting

• Security audit and accounting
  – Risk events are violations that occur during operational activities
    Decision makers need to be aware of the events that occur involving the assets

Firewall Architecture

• Represent trade-offs between complexity, speed, and security, and which are tailored to control attacks on specific layers of the network
Secure Internet Applications

Cryptographic Key Management

- Fundamental role in secure communication
  - Secure communication
  - Cryptographic key generation
  - Session key exchange with public keys
  - Public key exchange
  - Public key database
  - Session key exchange with server-side certificate
  - Session key exchange with certificates
  - Certificate authority
  - Cryptographic smart card
  - Certificate revocation
Threat Patterns
[Uzunov and Fernandez, 2014]

First level threats
• Identify attacks
• Network communication attacks
• Network protocol attacks
• Passing illegal data attacks
• Stored data attacks
• Remote information inference
• Loss of accountability
• Uncontrolled operations

Second level threats
• Cryptography attacks
• Countermeasure design
• Configuration/ administration
• Network protocol threats

Outline
• Security patterns
• Security pattern taxonomy
• Security risk-oriented patterns
  • Security requirements elicitation from business processes
    – SREBP method
    – Pattern application
    – Once Security Requirements Are Elicited
• Further reading
Understanding work practices and their changes

Processing of Information (Alter, 2006)

Everything that IT does, reduces to six functions

- **Capturing information**
  - Keyboard, bar code reader, digital camera

- **Transmitting information**
  - Wired-, wireless-phone

- **Storing information**
  - Hard disk, memory card, internet

- **Retrieving information**
  - From any storage device

- **Manipulating information**
  - Calculations, combinations of data

- **Displaying information**
  - Monitor, printer

Security Risk-oriented Patterns [Ahmed and Matulevičius, 2014]

**SRP1**: Secure data from unauthorized access

**SRP2**: Secure data transmitted between business entities

**SRP3**: Secure business activity after data is submitted

**SRP4**: Secure business services against denial of service attacks

**SRP5**: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

**SRP1**: Secure data from unauthorized access

**SRP2**: Secure data transmitted between business entities

**SRP3**: Secure business activity after data is submitted

**SRP4**: Secure business services against denial of service attacks

**SRP5**: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

**SRP1**: Secure data from unauthorized access

---

Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

**SRP1**: Secure data from unauthorized access
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

SRP1: Secure data from unauthorized access

SRP2: Secure data transmitted between business entities

SRP3: Secure business activity after data is submitted

SRP4: Secure business services against denial of service attacks

SRP5: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]
SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

SRP1: Secure data from unauthorized access

SRP2: Secure data transmitted between business entities

SRP3: Secure business activity after data is submitted

SRP4: Secure business services against denial of service attacks

SRP5: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in/retrieved from the data store

© Springer International Publishing AG 2017
SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in / retrieved from the data store
Security Risk-oriented Patterns

[Ahmed and Matulevičius, 2014]

SRP1: Secure data from unauthorized access

SRP2: Secure data transmitted between business entities

SRP3: Secure business activity after data is submitted

SRP4: Secure business services against denial of service attacks

SRP5: Secure data stored in / retrieved from the data store
Outline

- Security patterns
- Security pattern taxonomy
- Security risk-oriented patterns
- Security requirements elicitation from business processes
  - SREBP method
    - Pattern application
    - Once Security Requirements Are Elicited
- Further reading

SREBP framework
SREBP process

1. Business asset identification and security objective determination
   - Identify business assets
   - Determine security objectives

2. Security requirements elicitation
   - Identify pattern
   - Extract security model
   - Derive security requirements

SRP application

1. Business asset identification and security objective determination
   - Identify business assets
   - Determine security objectives

2. Security requirements elicitation
   - Identify pattern
   - Extract security model
   - Derive security requirements

- Identify resource
- Identify roles
- Assign users
- Identify secured operations
- Assign permissions
- Identify data store resources
- Identify data store operations
- Identify data store actions
- Identify input data
- Identify input interfaces
- Identify functional units
- Identify business partners
- Identify data transmissions
- Instantiate the security model with extracted information

© Springer International Publishing AG 2017
Outline

• Security patterns
• Security pattern taxonomy
• Security risk-oriented patterns
• Security requirements elicitation from business processes
  – SREBP method
  – Pattern application
    – Once Security Requirements Are Elicited
• Further reading
Identify business assets

- Team, Player, Umpire, League and region, Timetable, and Game

Determine security objectives

- **Game** should be **confidential**
  - no unauthorised individual should read it and its relevant data
- **Game** should be **integral**
  - should not be tampered
- **Game** should be **available**
  - to the business partners at any time
SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in / retrieved from the data store
Security Requirements Elicitation

**SRP1:** Secure data from unauthorized access
Security Requirements Elicitation

**SRP1**: Secure data from unauthorized access

1. Identify resource
2. Identify roles
3. Assign users
4. Identify secured operations
5. Assign permissions and security constraints

**RBAC security model**
SRP1: Secure data from unauthorized access

**Security requirements**

**SecReq.1:** Umpire should be able to *update* the gameReport.

**SecReq.2:** FootballFederationEmployee should be able to *insert* the Game (i.e., create a new instance of Game, including gameInfo, gameReport, and confirmation).

**SecReq.3:** FootballFederationEmployee should be able to *update* the confirmation.

---

**Football Federation**

Security Requirements Elicitation

SRP1: Secure data from unauthorized access

SRP2: Secure data transmitted between business entities

SRP3: Secure business activity after data is submitted

SRP4: Secure business services against denial of service attacks

SRP5: Secure data stored in / retrieved from the data store
SRP2: Secure data transmitted between business entities
SRP2: Secure data transmitted between business entities

Security Requirements Elicitation

1. Identify communicators
2. Identify data transmission

Security model

Umpire: Client

1. Verify Registry’s Public key
2. Generate Secret
3. Encrypt Secret using ERIS’s Public key

Client Hello
Random Number

Server Hello
Server Certificate + Certificate Authority

Secret Key Exchange
Secret encrypted with ERIS’s Public key

game report
Secure session for data exchange over the Internet

ERIS: Server

4. Decrypt Secret using Private key
5. Generate Symmetric Key
SRP2: Secure data transmitted between business entities

**Security requirements**

**SecReq.4**: ERIS should have unique identity in the form of key pairs (public key, private key) certified by a certification authority.

**SecReq.5**: Umpire should encrypt and sign game report (and other data communicated to ERIS) using keys before sending it to ERIS.

**Football Federation**

**Security Requirements Elicitation**

**SRP1**: Secure data from unauthorized access

**SRP2**: Secure data transmitted between business entities

**SRP3**: Secure business activity after data is submitted

**SRP4**: Secure business services against denial of service attacks

**SRP5**: Secure data stored in / retrieved from the data store
Security Requirements Elicitation

**SRP3**: Secure business activity after data is submitted
Security Requirements Elicitation

**SRP3**: Secure business activity after data is submitted

1. Identify input interfaces
2. Identify input data

**SRP3**: Secure business activity after data is submitted

**Security requirements**

- **SecReq.7**: Update game report should filter the input (i.e., game report).
- **SecReq.8**: Update game report should sanitise the input (i.e., game report) to transform it to the required format.
- **SecReq.9**: Update game details should canonicalise the input (i.e., game report) to verify against its canonical representation.
Football Federation

Security Requirements Elicitation

**SRP1**: Secure data from unauthorized access

**SRP2**: Secure data transmitted between business entities

**SRP3**: Secure business activity after data is submitted

**SRP4**: Secure business services against denial of service attacks

**SRP5**: Secure data stored in / retrieved from the data store
SRP4: Secure business services against denial of service attacks

1. Identify functional-unit
2. Identify business partner
SRP4: Secure business services against denial of service attacks

Security model

SecReq.10: Update game report should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with the Umpire.

SecReq.11: Packet Filter Firewall should filter the Umpire’s address to determine if that is not a host used by the threat agent.

SecReq.12: Proxy Based Firewall should communicate to the proxy which represents Update game report to determine the validity of the request received from Umpire.

SecReq.13: State Firewall should maintain the state table to check the Umpire’s request for additional conditions on established communication.
SRP1: Secure data from unauthorized access
SRP2: Secure data transmitted between business entities
SRP3: Secure business activity after data is submitted
SRP4: Secure business services against denial of service attacks
SRP5: Secure data stored in / retrieved from the data store
**SRP5: Secure data stored in / retrieved from the data store**

1. Identify Datastore resource
2. Identify Datastore’s operations:
**SecReq.14**: The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game storage.

**SecReq.15**: The ERIS should perform operations to hide/unhide data when they are stored/retrieved to/from the Game storage.
Security Requirements

**SecReq.1**: Umpire should be able to *update* the gameReport.

**SecReq.2**: FootballFederationEmployee should be able to *insert* the Game (i.e., create a new instance of Game, including gameInfo, gameReport, and confirmation).

**SecReq.3**: FootballFederationEmployee should be able to *update* the confirmation.

**SecReq.4**: ERIS should have unique identity in the form of key pairs (public key, private key) certified by a certification authority.

**SecReq.5**: Umpire should encrypt and sign game report (and other data communicated to ERIS) using keys before sending it to ERIS.

**SecReq.7**: Update game report should filter the input (i.e., game report).

**SecReq.8**: Update game report should sanitise the input (i.e., game report) to transform it to the required format.

**SecReq.9**: Update game details should canonicalise the input (i.e., game report) to verify against its canonical representation.

**SecReq.10**: Update game report should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with the Umpire.

**SecReq.11**: Packet Filter Firewall should filter the Umpire’s address to determine if that is not a host used by the threat agent.

**SecReq.12**: Proxy Based Firewall should communicate to the proxy which represents Update game report to determine the validity of the request received from Umpire.

**SecReq.13**: State Firewall should maintain the state table to check the Umpire’s request for additional conditions on established communication.

**SecReq.14**: The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game storage.

**SecReq.15**: The ERIS should perform operations to hide/unhide data when they are stored/retrieved to/from the Game storage.

Outline

- Security patterns
- Security pattern taxonomy
- Security risk-oriented patterns
- Security requirements elicitation from business processes
  - SREBP method
  - Pattern application
    - **Once Security Requirements Are Elicited**
- Further reading
Security Requirements

SecReq.1: Umpire should be able to update the gameReport.
SecReq.2: FootballFederationEmployee should be able to insert the Game (i.e., create a new instance of Game, including gameInfo, gameReport, and confirmation).
SecReq.3: FootballFederationEmployee should be able to update the confirmation.
SecReq.4: ERIS should have unique identity in the form of key pairs (public key, private key) certified by a certification authority.
SecReq.5: Umpire should encrypt and sign game report and other data communicated to ERIS using keys before sending it to ERIS.
SecReq.6: Packet Filter Firewall should filter the Umpire’s address to determine if that is not a host used by the threat agent.
SecReq.7: Proxy Based Firewall should communicate to the proxy which represents Update game report to determine the validity of the request received from Umpire.
SecReq.8: State Firewall should maintain the state table to check the Umpire’s request for additional conditions on established communication.
SecReq.9: The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game storage.
SecReq.10: The ERIS should perform operations to hide or hide data when they are stored/retrieved to/from the Game storage.

1. Prioritise security requirements
2. Introduce security requirements and the security constraints to the business process model
3. Implement security requirements

Security Constraints
Outline

• Security patterns
• Security pattern taxonomy
• Security risk-oriented patterns
• Security requirements elicitation from business processes
  – SREBP method
  – Pattern application
  – Once Security Requirements Are Elicited

Further reading

• Software requirements patterns [Withall, 2009]
• Security pattern taxonomies [Blakley and Heath, 2004]
  – Available system patterns
  – Protected systems patterns
• Security design patterns [Dougherty et al., 2009]
  – Architectural-level patterns
  – Design-level patterns
  – Implementation-level patterns
Further reading

- Feature diagrams for pattern classification [Slavin et al., 2014]
- Language construct comparison for pattern presentation [Bandara et al., 2010]
- Framework to link security standards with a security engineering method [Becker, 2015]
- Security risk-oriented patterns in Secure Tropos [Rrenja and Matulevičius, 2015]

Summary

- Security patterns
- Security pattern taxonomy
- Security risk-oriented patterns
- Security requirements elicitation from business processes
  - SREBP method
  - Pattern application
  - Once Security Requirements Are Elicited
- Further reading