Lecture 15:

Security Patterns

Dr. Raimundas Matulevičius
email: rma@ut.ee

Lecture outline

• What is pattern?
• Security pattern landscape
• SREBP and SRPs
• Pattern identification and security requirements elicitation
• Case study
What is a Pattern?

A solution to a problem that arises within specific context

Context – Problem – Solution
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

Lecture 15:
Security Patterns
Part 2

Security Pattern Landscape

Dr. Raimundas Matulevičius
email: rma@ut.ee
Security Patterns

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
1. Enterprise Security and Risk Management

- **Content**: The enterprise has some function or mission and wants to address security issues as they relate to that mission.
2. Identification and Authentication

- **Content**: Specific requirements and design for the identification and authentication services

![Diagram of I&A requirements and design alternatives]

3. Access Control Model

- **Content**: High level models represent the security policies of the requirements. These models define security constraints at the architectural level, the application level, and are enforced by the lower levels.

![Diagram of Access Control Model]
4. System Access Control Architecture

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

5. 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
6. 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.

7. Firewall Architecture

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

9. 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
Patterns on Threats to the System


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

Lecture 15:
Security Patterns
Part 3
SREBP and SRPs

Dr. Raimundas Matulevičius
email: rma@ut.ee
SREBP: Security Requirements Elicitation from Business Processes

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
Understanding work practices and their changes

Processing of Information

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

**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

[Ahmed and Matulevičius, 2014]
1. Organisational scenario & security context identification

**Pattern name**
Securing data that flow between the business entities

**Pattern description**
This pattern protects the data transmitted between the business entities.

**Related pattern(s)**
No related patterns

2. Asset identification & Security objective determination

<table>
<thead>
<tr>
<th>Business Asset</th>
<th>IS Asset</th>
<th>Security criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data submitted and employed by server</td>
<td>Input interface, Transmission medium that transfers data, and Server</td>
<td>Confidentiality of data; Integrity of data</td>
</tr>
</tbody>
</table>

3. Risk analysis & assessment

<table>
<thead>
<tr>
<th>Risk</th>
<th>Impact</th>
<th>Event</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Threat agent</th>
<th>Attack method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Harm data submitted and employed in server. Loss of reliability of the transmission medium. Negation of data confidentiality and integrity.</td>
<td>An attacker intercepts the transmission medium due to its characteristics to be intercepted and misuses the data due to the lack of crypto-functionality at the input interface and server [26].</td>
<td>An attacker intercepts the transmission medium and misuses the data.</td>
<td>Characteristics of transmission medium to be intercepted [26].</td>
<td>An attacker with means to intercept transmission medium by acting as a proxy.</td>
<td>Capture, read and keep data for later use. Capture, modify and pass data to the server.</td>
</tr>
</tbody>
</table>

4. Risk treatment & Security requirements

**Risk treatment**

<table>
<thead>
<tr>
<th>Security requirement</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Make data unreadable to attackers (Mitigates the risk of data confidentiality);</td>
<td>改变传输介质，使得没有能力进行拦截。</td>
<td>- Verify the received data with the original (Mitigates the risk of data integrity).</td>
</tr>
</tbody>
</table>

**Control**

| Cryptographic algorithm | Physical delivery of data. |
| Checksum algorithm      | Employee enters data. |
Security Risk-oriented Patterns

**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

SRP1: Secure data from unauthorized access

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

**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

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

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

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

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

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

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

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

**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

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

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

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

**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

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

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

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

[Ahmed and Matulevičius, 2014]

Lecture 15:
Security Patterns
Part 4
SRP Identification and Security Requirements Elicitation

Dr. Raimundas Matulevičius
email: rma@ut.ee
Pattern application

Football Federation Case
Football Federation Case

SRP1: Secure data from unauthorized access
Football Federation Case

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)

Role-based Access Control
Role-based Access Control

SecReq.1: *Umpire* should be able to **update** the `GameReport.gameDetails`.

SecReq.2: *FootballFederationEmloyee* should be able to **insert** the `GameReport` (i.e., create a new instance of `GameReport`).

SecReq.3: *FootballFederationEmloyee* should be able to **update** the `GameReport.gameInfo`, `GameReport.gameDetails` and `GameReport.confirmation`.

Football Federation Case

**SRP2**: Secure data transmitted between business entities
SRP2: Securing data that flow between the business entities

Requirements to Secure Communication

Umpire: Client

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

ERIS: Server

1. Client Hello
   Random Number

2. Server Hello
   Server Certificate + Certificate Authority

3. Secret Key Exchange
   Secret encrypted with ERIS's Public key

4. Decrypt Secret using Private key
5. Generate Symmetric Key

Initial game details
Secure session for data exchange over the Internet
SRP2: Securing data that flow between the business entities

Requirements to Secure Communication

- **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 *Initial game details* (and other data communicated to ERIS) using keys before sending it to ERIS.

Football Federation Case

SRP3: Secure business activity after data is submitted

1. Identify input interfaces
2. Identify input data
Football Federation Case

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

1. Identify input interfaces
2. Identify input data

**SecReq.7**: Update game details should filter the input (i.e., Initial game details and Updates game details).

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

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

Football Federation Case

**SRP4**: Securing business activity after data is submitted

1. Identify functional-unit
2. Identify business partner
SecReq.10: Update game details should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with Umpire.

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

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

SecReq.13: State Firewall should maintain the state table to check the Umpire’s request for additional conditions of established communication.
Football Federation Case

**SRP5**: Securing 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 database.

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

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

**SecReq.2**: FootballFederationEmployee should be able to **insert** the GameReport (i.e., create a new instance of GameReport).

**SecReq.3**: FootballFederationEmployee should be able to **update** the GameReport.gameInfo, GameReport.gameDetails and GameReport.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 **Initial game details** (and other date communicated to ERIS) using keys before sending it to ERIS.

**SecReq.6**: Update game details should filter the input (i.e., **Initial game details** and **Updates game details**).

**SecReq.7**: Update game details should sanitise the input (i.e., **Initial game details** and **Updates game details**) to transform it to the required format.

**SecReq.8**: Update game details should canonicalise the input (i.e., **Initial game details** and **Updates game details**) to verify against its canonical representation.

**SecReq.9**: Update game details should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with Umpire.

**SecReq.10**: Packet Filter Firewall should filter the Umpire’s address to determine if it is not a host used by the threat agent.

**SecReq.11**: Proxy Based Firewall should communicate to the proxy which represents Update game details to determine the validity of request received from Umpire.

**SecReq.12**: State Firewall should maintain the state table to check the Umpire’s request for additional conditions of established communication.

**SecReq.13**: The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game database.

**SecReq.14**: The ERIS should perform operations to hide/unhide data when they are stored/retrieved to/from the Game database.

---

1. **Prioritise security requirements**
2. **Introduce security requirements and the security constraints to the business process model**
3. **Implement security requirements**
Lecture 15:

Security Patterns

Part 5

Case Study

Dr. Raimundas Matulevičius

email: rma@ut.ee
Pattern-based versus Traditional

Research questions

Which approach – pattern based or traditional – contributes with more complete set of requirements?

INPUT:

16 diagrams of operational business processes
Pattern-based versus Traditional

SREBP versus SQUARE

- **SREBP:** Application of the SRP patterns

- **SQUARE:** System Quality Requirements Engineering
  1. Agreement on definitions
  2. Identification of security goals
  3. Development of artefacts
  4. Perform risk assessment
  5. Select elicitation techniques
  6. Elicit security requirements
  7. Categorise requirements
  8. Prioritize requirements
  9. Inspect requirements

- **Seven** business assets:
  - Project offer, Project, Sample quality, Purchase order, Sample plate, Process sample sheet, and Sample result

- **SREBP** – around **220** security requirements
- **SQUARE** – around **170** security requirements
Pattern-based versus Traditional

SREBP versus SQUARE

- **Seven** business assets:
  - Project offer, Project, Sample quality, Purchase order, Sample plate, Process sample sheet, and Sample result

- **SREBP** – around 220 security requirements
- **SQUARE** – around 170 security requirements

<table>
<thead>
<tr>
<th>Requirements categories</th>
<th>CIA</th>
<th>SREBP</th>
<th>SQUARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identification</td>
<td>C</td>
<td>75%</td>
<td>4.69</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>75%</td>
<td>4.69</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>75%</td>
<td>4.69</td>
</tr>
<tr>
<td>2. Authentication</td>
<td>C</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td>3. Authorization</td>
<td>C</td>
<td>75%</td>
<td>3.13</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>0%</td>
<td>0.00</td>
</tr>
<tr>
<td>4. Accounting</td>
<td>C</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td>5. Audit</td>
<td>C</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>0%</td>
<td>0.00</td>
</tr>
<tr>
<td>6. Non repudiation</td>
<td>C</td>
<td>100%</td>
<td>12.5</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Immunity</td>
<td>C</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>I</td>
<td>100%</td>
<td>4.17</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>100%</td>
<td>4.17</td>
</tr>
</tbody>
</table>

83 % versus 44 %
SREBP results in more complete set of security requirements than SQUARE

Message to take home

- What is pattern?
- Security pattern landscape
- SREBP and SRPs
- Pattern identification and security requirements elicitation
- Case study