1. What does security pattern describe?

☐ A fundamental structure and workflow of application domain
☐ A particular recurring security problem
☐ A specific security context where security problem arises
☐ A well-proven generic scheme for a security solution
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
1. What does security pattern describe?

☐ A fundamental structure and workflow of application domain
☒ A particular recurring security problem
☒ A specific security context where security problem arises
☒ A well-proven generic scheme for a security solution
2. Patterns for firewall architecture represent trade-offs between complexity, speed and security, which are tailored to control attacks on specific layers of the network. What are the major types of the firewall architecture patterns?

- Proxy-base firewalls
- Address filtering lanes
- Packet filter firewalls
- Statefull firewalls
- Keep state procurements
Firewall Architecture

• Represent trade-offs between complexity, speed, and security, and which are tailored to control attacks on specific layers of the network
2. Patterns for firewall architecture represent trade-offs between complexity, speed and security, which are tailored to control attacks on specific layers of the network. What are the major types of the firewall architecture patterns?

- Proxy-base firewalls
- Address filtering lanes
- Packet filter firewalls
- Stateful firewalls
- Keep state procurements
3. What does acronym SREBP mean?

☐ Security requirements engineering from banned products
☐ Security requirements elicitation from business processes
☐ Software requirements elicitation from business processes
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
3. What does acronym SREBP mean?

☐ Security requirements engineering from banned products
☒ Security requirements elicitation from business processes
☐ Software requirements elicitation from business processes
4. What components needs to be identified when creating role-based access control security model?

☐ Resources, roles (and users)
☐ Secured operations
☐ Permissions and security constraints
☐ Confirmations and reports
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
SRP1: Secure data from unauthorized access

RBAC security model
4. What components needs to be identified when creating role-based access control security model?

- Resources, roles (and users)
- Secured operations
- Permissions and security constraints
- Confirmations and reports
5. What are next engineering activities once security requirements are elicited using the SREBP method?

☐ Lean back and get some refreshments
☐ Prioritise security requirements
☐ Introduce security requirements and the security constraints to the business process model
☐ Implement security requirements to the developed system
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: Update game report should filter the input (i.e., game report).

SecReq.7: Update game report should sanitise the input (i.e., game report) to transform it to the required format.

SecReq.8: Update game report should canonicalise the input (i.e., game report) to verify against its canonical representation.

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

SecReq.10: Proxy Based Firewall should communicate to the proxy which represents Update game report to determine the validity of the request received from Umpire.

SecReq.11: State Firewall should maintain the state table to check the Umpire’s request for additional conditions on established communication.

SecReq.12: The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game storage.

SecReq.13: The ERIS should perform operations to hide/unhide data when they are stored/retrieved 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
5. What are next engineering activities once security requirements are elicited using the SREBP method?

☐ Lean back and get some refreshments
☒ Prioritise security requirements
☒ Introduce security requirements and the security constraints to the business process model
☒ Implement security requirements to the developed system