

Security Architecture

[Author Name]

Université de Toulon, LIS UMR CNRS 7020

2026-10-14

Table des matières

1 Purpose of this Document	1
2 Security Strategy Overview	1
3 Threat Model	1
3.1 Threat Actors	1
3.2 Threat Scenarios	2
4 Security Architecture Diagram	2
5 Security Controls Framework	2
6 Authentication & Authorization	4
7 Data Classification & Handling	4
8 Encryption Strategy	4
9 Security Monitoring & Response	5
10 Compliance Requirements	5
11 Secure Development Lifecycle	6
12 Vulnerability Management	6
13 Security Testing	7
14 Template Validation Checklist	7
15 Related Views	7

1 Purpose of this Document

This document defines the security architecture for [System Name], including security controls, policies, and implementation approaches to protect the system from threats and vulnerabilities.

2 Security Strategy Overview

Security Philosophy: [Overall approach to security]
Primary Goals:
- [Goal 1, e.g., "Protect sensitive

customer data"]
- [Goal 2, e.g., "Ensure regulatory compliance"]
- [Goal 3, e.g., "Minimize security incident impact"]

Key Principles:

- [Principle 1, e.g., "Defense in depth"]
- [Principle 2, e.g., "Least privilege"]
- [Principle 3, e.g., "Secure by design"]

3 Threat Model

3.1 Threat Actors

External Threats:

- Actor: [Threat actor type, e.g., "Cybercriminals"]

Motivation: [Primary motivation, e.g., "Financial gain"]

Capabilities: [Skill/resource level, e.g., "Moderate technical skills"]

Targets: [Primary targets, e.g., "Customer data, payment information"]

- Actor: [Additional threat actor]
Similar structure as above

Internal Threats:

```

- Actor: [Threat actor type, e.g.,
"Privileged users"]
  Motivation: [Primary motivation,
e.g., "Accidental misuse"]
  Capabilities: [Skill/resource
level, e.g., "High system access"]
  Targets: [Primary targets, e.g.,
"Administrative functions, sensitive
data"]

- Actor: [Additional threat actor]
  # Similar structure as above

```

3.2 Threat Scenarios

ID	Scenario	Impact	Likelihood	Controls
TS-01	[Brief description]	[High/Medium/Low]	[High/Medium/Low]	[Control references]
TS-02	[Brief description]	[High/Medium/Low]	[High/Medium/Low]	[Control references]
TS-03	[Brief description]	[High/Medium/Low]	[High/Medium/Low]	[Control references]

4 Security Architecture Diagram

```

graph TD
  subgraph "External"
    A[Internet]
    B[Partners]
  end

  subgraph "DMZ"
    C[WAF]
  end

```

```

D[Load Balancers]
E[API Gateway]
end

subgraph "Application Layer"
  F[Authentication]
  G[Authorization]
  H[Application Services]
end

subgraph "Data Layer"
  I[Encryption]
  J[Data Access Control]
  K[Databases]
end

A --> C
B --> C
C --> D
D --> E
E --> F
F --> G
G --> H
H --> I
I --> J
J --> K

```

5 Security Controls Framework

```

Identity & Access Management:
  Authentication:
    - Control: [Control name, e.g.,
"Multi-factor authentication"]
    Implementation: [Implementation
approach]
    Coverage: [Where applied]
    Verification: [How effectiveness
is verified]

- Control: [Additional control]
  # Similar structure as above

```

```

Authorization:
  - Control: [Control name, e.g.,
"Role-based access control"]
    Implementation: [Implementation
approach]
    Coverage: [Where applied]
    Verification: [How effectiveness
is verified]

  - Control: [Additional control]
    # Similar structure as above

Data Protection:
  Encryption:
    - Control: [Control name, e.g.,
"Data-at-rest encryption"]
      Implementation: [Implementation
approach]
      Coverage: [Where applied]
      Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

  Data Loss Prevention:
    - Control: [Control name, e.g.,
"Data classification"]
      Implementation: [Implementation
approach]
      Coverage: [Where applied]
      Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

Network Security:
  Perimeter:
    - Control: [Control name, e.g.,
"Web application firewall"]
      Implementation: [Implementation

```

```

approach]
    Coverage: [Where applied]
    Verification: [How effectiveness
is verified]

  - Control: [Additional control]
    # Similar structure as above

  Segmentation:
    - Control: [Control name, e.g.,
"Network zones"]
      Implementation: [Implementation
approach]
      Coverage: [Where applied]
      Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

Application Security:
  Secure Development:
    - Control: [Control name, e.g.,
"Static code analysis"]
      Implementation: [Implementation
approach]
      Coverage: [Where applied]
      Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

  Runtime Protection:
    - Control: [Control name, e.g.,
"Input validation"]
      Implementation: [Implementation
approach]
      Coverage: [Where applied]
      Verification: [How effectiveness
is verified]

    - Control: [Additional control]

```

```

# Similar structure as above

Operations Security:
  Monitoring:
    - Control: [Control name,
e.g., "Security information and event
monitoring"]
    Implementation: [Implementation
approach]
    Coverage: [Where applied]
    Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

  Incident Response:
    - Control: [Control name, e.g.,
"Incident response plan"]
    Implementation: [Implementation
approach]
    Coverage: [Where applied]
    Verification: [How effectiveness
is verified]

    - Control: [Additional control]
      # Similar structure as above

```

6 Authentication & Authorization

```

@startuml
actor User
participant "Frontend" as FE
participant "API Gateway" as GW
participant "Auth Service" as Auth
participant "Resource Server" as RS
database "User Store" as US

User -> FE: Access application
FE -> GW: Request access
GW -> Auth: Authenticate user

```

```

Auth -> US: Verify credentials
US --> Auth: Valid credentials
Auth --> GW: Issue token
GW --> FE: Return token
FE -> GW: Request resource with token
GW -> Auth: Validate token
Auth --> GW: Token valid + user
permissions
GW -> RS: Forward request with context
RS -> RS: Check authorization
RS --> GW: Return resource if
authorized
GW --> FE: Return response
FE --> User: Display resource
@enduml

```

7 Data Classification & Handling

Classifi- cation	Descrip- tion	Examples	Hand- ling Re- quire- ments
Public	[Defini- tion]	[Examples]	[Re- quire- ments]
Internal	[Defini- tion]	[Examples]	[Re- quire- ments]
Confidential	[Defini- tion]	[Examples]	[Re- quire- ments]
Restric- ted	[Defini- tion]	[Examples]	[Re- quire- ments]

8 Encryption Strategy

```

Data at Rest:
  - Database: [Encryption approach]

```

- File Storage: [Encryption approach]
- Backups: [Encryption approach]
- Key Management: [Key management approach]

Data in Transit:

- External Communications: [Encryption approach]
- Internal Communications: [Encryption approach]
- API Endpoints: [Encryption approach]
- Certificate Management: [Certificate approach]

Data in Use:

- Memory Protection: [Protection approach]
- Secure Processing: [Processing approach]
- Tokenization: [Tokenization approach]

9 Security Monitoring & Response

Monitoring:

Log Sources:

- Application Logs: [Collection approach]
- Network Logs: [Collection approach]
- Security Logs: [Collection approach]
- Infrastructure Logs: [Collection approach]

Detection:

- Rule-based: [Detection approach]
- Anomaly-based: [Detection approach]

- Threat Intelligence: [Integration approach]

Alerting:

- Severity Levels: [Alert levels]
- Notification Channels: [Communication channels]
- Escalation Paths: [Escalation process]

Response:

Incident Handling:

- Classification: [Incident classification]
- Triage: [Triage process]
- Containment: [Containment approach]
- Eradication: [Eradication approach]
- Recovery: [Recovery approach]

Forensics:

- Evidence Collection: [Collection process]
- Analysis: [Analysis approach]
- Reporting: [Reporting process]

Communication:

- Internal: [Communication plan]
- External: [Disclosure approach]
 - Regulatory: [Compliance reporting]

10 Compliance Requirements

Regulatory:

- Regulation: [e.g., "GDPR"]

Key Requirements:

- [Requirement 1]
- [Requirement 2]

Implementation: [How addressed]

Audit: [Audit approach]

```

    - Regulation: [Additional
regulation]
    # Similar structure as above

Industry Standards:
- Standard: [e.g., "PCI DSS"]
  Key Requirements:
    - [Requirement 1]
    - [Requirement 2]
  Implementation: [How addressed]
  Audit: [Audit approach]

- Standard: [Additional standard]
  # Similar structure as above

Internal Policies:
- Policy: [Policy name]
  Key Requirements:
    - [Requirement 1]
    - [Requirement 2]
  Implementation: [How addressed]
  Audit: [Audit approach]

```

11 Secure Development Life-cycle

```

graph LR
  A[Requirements] --> B[Design]
  B --> C[Implementation]
  C --> D[Verification]
  D --> E[Release]
  E --> F[Maintenance]

  subgraph "Security Activities"
    A1[Threat Modeling]
    B1[Security Design Review]
    C1[Static Analysis]
    C2[Dependency Scanning]
    D1[Security Testing]
    D2[Penetration Testing]
    E1[Final Security Review]
    F1[Vulnerability Management]
  end

```

```

end

A --> A1
B --> B1
C --> C1
C --> C2
D --> D1
D --> D2
E --> E1
F --> F1

```

12 Vulnerability Management

```

Scanning:
- Code Scanning:
  Tools: [Tools used]
  Frequency: [How often performed]
  Coverage: [What's scanned]

- Dependency Scanning:
  Tools: [Tools used]
  Frequency: [How often performed]
  Coverage: [What's scanned]

- Infrastructure Scanning:
  Tools: [Tools used]
  Frequency: [How often performed]
  Coverage: [What's scanned]

Remediation:
- Risk Assessment:
  Methodology: [How risks are
assessed]
  Scoring: [Risk scoring approach]

- Prioritization:
  Criteria: [Prioritization
criteria]
  SLAs: [Time to fix by severity]

- Verification:
  Process: [Verification approach]

```

Documentation: [How fixes are documented]

13 Security Testing

Test Types:

- Static Analysis:
 - Tools: [Tools used]
 - Coverage: [What's tested]
 - Integration: [CI/CD integration]
- Dynamic Analysis:
 - Tools: [Tools used]
 - Coverage: [What's tested]
 - Frequency: [How often performed]
- Penetration Testing:
 - Approach: [Testing approach]
 - Scope: [What's tested]
 - Frequency: [How often performed]
- Security Reviews:
 - Types: [Review types]
 - Participants: [Who's involved]
 - Frequency: [How often performed]

14 Template Validation Checklist

- ☐ Security strategy defined
- ☐ Threat model documented
- ☐ Security controls identified
- ☐ Authentication and authorization approach specified
- ☐ Data classification and handling defined
- ☐ Encryption strategy outlined
- ☐ Monitoring and response approach described
- ☐ Compliance requirements documented
- ☐ Vulnerability management process defined
- ☐ Security testing approach specified

- ☐ Team review completed

15 Related Views

- System Context - System boundaries
- Infrastructure Architecture - Infrastructure security
- Data Architecture - Data security
- Integration Architecture - API security