# Secure Systems Development - Jaish Khan

# Table of Contents

# 1. Introduction to Secure Systems Development (SSD)

**Key Concept**

Secure Systems Development is akin to building a house with security in mind from the very beginning. Just as you wouldn't wait until after your house is built to think about locks and alarms, we don't wait until after software is developed to add security features.

This approach ensures that security isn't just an afterthought but a fundamental part of the system. Think of it as designing a house where security features like strong walls, secure windows, and a reliable alarm system are part of the original blueprint, rather than additions made later.

**Best Practice**

- Plan security features before coding
- Check for security issues at every step
- Conduct regular security testing
- Train everyone involved about security

# 2. Types of Risks

**Risk Categories**

Understanding different types of risks is crucial for developing secure systems. Each category requires different mitigation strategies.

## 2.1 Technical Risks #technical-risk

Technical risks are like the structural vulnerabilities in your house. These are the weak points that attackers might exploit to gain unauthorized access.

**Common Technical Risks**

- Bugs in the code (like cracks in your walls)
- Incorrect settings (like leaving windows unlocked)
- Weak points in the system
- Network vulnerabilities

- Database security issues

## 2.2 Operational Risks #operational-risk

**Critical**

Operational risks often lead to immediate security breaches if not properly managed.

Operational risks emerge from day-to-day activities and human interactions with the system. These are similar to the risks that come from how people use and maintain a house.

## 2.3 Business Risks #business-risk

Business risks affect the entire organization and its stakeholders. Think of these as the broader consequences of security failures.

# 3. Risk Analysis

**Remember**

"Prevention is better than cure" - This principle is fundamental to risk analysis in secure systems development.

Understanding and analyzing risks is crucial for developing secure systems. This process involves several key aspects that help us identify, assess, and address potential security threats effectively.

## 3.1 Types of Software Risks

Software risks come in various forms, each requiring different approaches to mitigation. Security risks are direct threats to your system's integrity. Imagine your software as a house - security risks are like different ways intruders might try to break in. This includes weak authentication, authorization problems, and data exposure.

Quality risks affect how well your system performs its intended functions. These are similar to maintenance issues in a house that might not be security-related but can still cause problems. Poor performance, reliability issues, and maintenance difficulties all fall into this category.

Operational risks are related to the deployment and maintenance of the system. These include deployment issues, integration problems, configuration errors, and resource constraints.

# 4. SDLC Models

Secure Systems Development Life Cycle (SDLC) models provide frameworks for integrating security into the development process. Each model has its strengths and is suited for different development environments.

## 4.1 Waterfall Model

The Waterfall model is a linear approach where each phase is completed before moving on to the next. This model emphasizes security requirements early in the development process and includes security testing at each phase.

## 4.2 Agile Model

The Agile model is an iterative approach that emphasizes flexibility and rapid delivery. It includes continuous security testing, sprint-based security reviews, and security user stories.

## 4.3 DevSecOps

DevSecOps integrates security into the DevOps process, emphasizing automation, continuous integration and deployment, and security as code.

## 4.4 Spiral Model

The Spiral model is a risk-driven approach that emphasizes iterative development and continuous evaluation. It includes security prototyping and is suited for projects with high security requirements.

# 5. Types of Hacking Techniques

Understanding the types of hacking techniques is essential for developing effective security measures. These techniques can be broadly categorized into social engineering, network attacks, and application attacks.

## 5.1 Social Engineering

Social engineering involves manipulating individuals into divulging sensitive information or performing certain actions. Techniques include phishing, pretexting, baiting, quid pro quo, and tailgating.

## 5.2 Network Attacks

Network attacks target the network infrastructure. Techniques include man-in-the-middle attacks, DDoS attacks, packet sniffing, DNS poisoning, and ARP spoofing.

## 5.3 Application Attacks

Application attacks target vulnerabilities in software applications. Techniques include SQL injection, cross-site scripting, CSRF attacks, buffer overflows, and directory traversal.

# 6. Biometric Security

Biometric security uses unique physical or behavioral characteristics to authenticate individuals. Types of biometrics include fingerprint recognition, facial recognition, iris scanning, voice recognition, and behavioral biometrics.

## 6.1 Implementation Considerations

Implementing biometric security requires careful consideration of accuracy rates, false acceptance and rejection rates, environmental factors, user acceptance, and privacy concerns.

# 7. Encryption Techniques - A Simple Guide to Keeping Data Safe

**Understanding Encryption**

Encryption is the process of converting readable data into a coded format that can only be decoded with the right key.

## 7.1 Symmetric Encryption: The Single Key Method #symmetric-encryption

**Real-World Analogy**

Think of symmetric encryption like a physical lock and key - the same key is used to both lock and unlock the data.

### 7.1.1 AES (Advanced Encryption Standard) - In Detail

**Industry Standard**

AES is the global standard for symmetric encryption, approved by the NSA for top-secret information.

**The Process:**

1. **Block Structure:**
    - 128-bit blocks
    - Multiple key lengths

> **Performance Note**
>
> AES-256 provides the highest security but requires more processing power than AES-128.

**Key Sizes:** #encryption-keys

- AES-128
- AES-192
- AES-256

**How AES Works:**

1. **Initial Round:** The data is combined with the round key
2. **Main Rounds:** Each round performs four operations:
    - SubBytes: Substitutes each byte with another according to a lookup table
    - ShiftRows: Shifts the rows of the data matrix
    - MixColumns: Mixes up the bytes in each column
    - AddRoundKey: Combines the data with the round key

**Real-world Applications:**

- Securing websites (HTTPS)
- Encrypting files on your computer
- Protecting wireless networks (WPA2/WPA3)
- Banking transactions

**Why AES is Secure:**

- No practical attacks have broken AES
- Would take billions of years to crack using current technology
- Officially approved for top secret information by the NSA

## 7.2 Asymmetric Encryption: The Two Key Method #asymmetric-encryption

> **Real-World Analogy**

Think of asymmetric encryption like a mailbox - anyone can put mail in using the public key, but only the owner can retrieve it using the private key.

## 7.2.1 RSA (Rivest-Shamir-Adleman) - In Detail

**Mathematical Foundation**

RSA's security is based on the mathematical difficulty of factoring large prime numbers.

**Process Overview:**


**Key Generation:**

1. **Choose two large prime numbers (p and q)**
2. **Calculate their product (n = p × q)**
3. **Generate public and private keys using mathematical functions**
   - Public key: (n, e) where e is the encryption exponent
   - Private key: (n, d) where d is the decryption exponent

**How RSA Works:**

1. **Encryption:**
   - Message is converted to a number (m)
   - Encrypted message = m^e mod n
2. **Decryption:**
   - Receive encrypted message (c)
   - Original message = c^d mod n

**Key Features:**

- Based on the difficulty of factoring large numbers
- Key sizes typically range from 1024 to 4096 bits
- Larger keys are more secure but slower

**Real-world Applications:**

- Digital signatures
- Secure email (PGP/GPG)
- SSL/TLS certificates

- Secure key exchange

**Why RSA is Secure:**

- Security based on mathematical problems that are hard to solve
- Would require quantum computers to break efficiently
- Different key pairs for each communication

## 7.3 Comparison Table

| Feature | [[#7.1.1 AES | AES]] |
|---|---|---|
| Speed | Fast ⚡ | Slower 🐌 |
| Keys Needed | One key 🔑 | Two keys 🔑🔑 |
| Key Size | 128-256 bits | 1024-4096 bits |
| Best Used For | Large data encryption | Key exchange & signatures |
| Security Base | Complex substitution & permutation | Mathematical factoring |
| Processing Power | Low | High |
| Key Distribution | Difficult (needs secure channel) | Easy (public key can be shared) |
| Real-world Example | Door lock | Mailbox system |

# 8. Cipher Text - Made Simple

Ciphers are algorithms used for encryption and decryption. Types of ciphers include block ciphers, stream ciphers, substitution ciphers, and transposition ciphers.

## 8.1 Types of Ciphers

Block ciphers encrypt data in fixed-length blocks. Stream ciphers encrypt data one bit or byte at a time. Substitution ciphers replace plaintext with ciphertext. Transposition ciphers rearrange plaintext to create ciphertext.

## 8.2 Common Operations

Common operations in cryptography include encryption, decryption, key management, and mode of operation.

# 9. Threat Modeling - A Strategic Approach to Security

Threat modeling is a systematic approach to identifying and addressing security risks. It involves understanding the system, identifying potential threats, and developing a defense strategy.

## 9.1 System Analysis

System analysis involves understanding what you're protecting, including assets, system boundaries, and information flow.

## 9.2 Threat Assessment

Threat assessment involves identifying potential attackers and their methods, including entry points, attack types, and weak points.

## 9.3 Defense Planning

Defense planning involves developing a robust defense strategy, including security controls, monitoring systems, and response plans.

---