Security Technology and Tools

Introduction to Key Technology Concepts

Contents

---

1. Transport Layer Security (TLS)

Overview

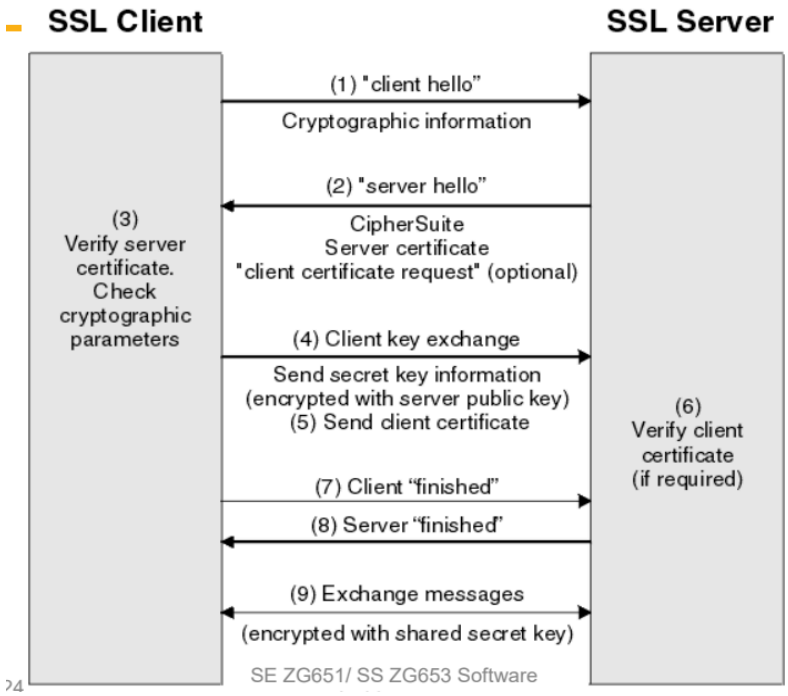
Transport Layer Security (TLS) is essential for secure communication between a client and server, such as a browser and a website. It ensures:

- **Privacy**: Protects communication from being intercepted.
- **Data Integrity**: Ensures data cannot be tampered with undetected.

How TLS Works

1. **Agree on TLS Version**: Client and server select the version to use.
2. **Select Algorithms**: Cryptographic algorithms for encryption are chosen.
3. **Authenticate with Certificates**: Both sides authenticate using digital certificates.
4. **Generate Shared Secret Key**: A key for faster symmetric encryption is generated.

Diagram Placeholder: TLS / SSL Steps



---

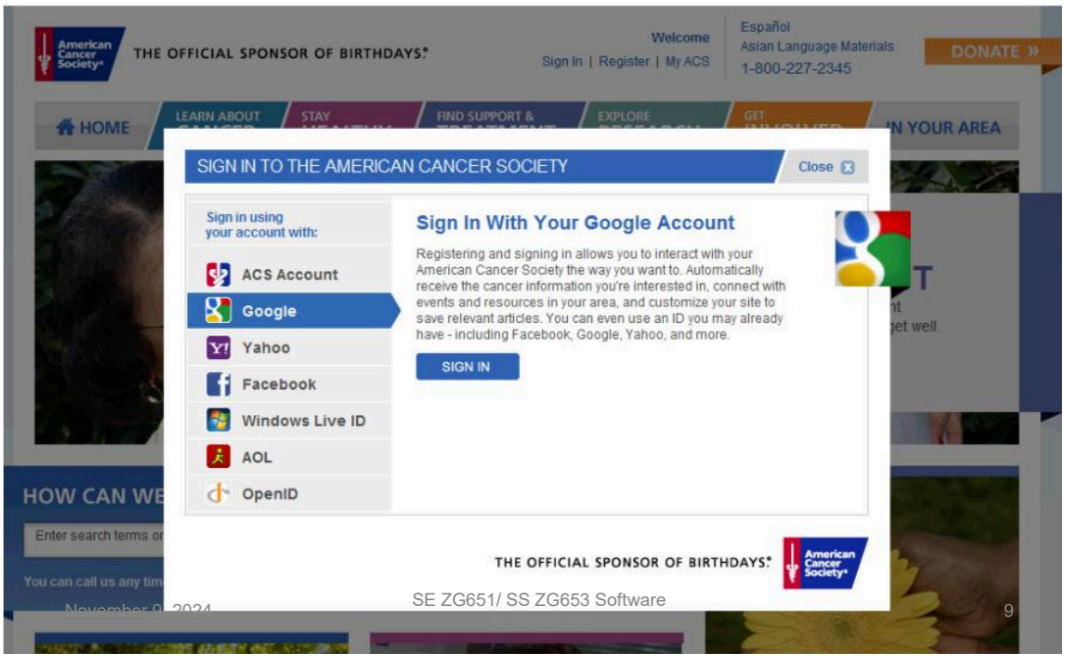
2. OpenID & OAuth

OpenID

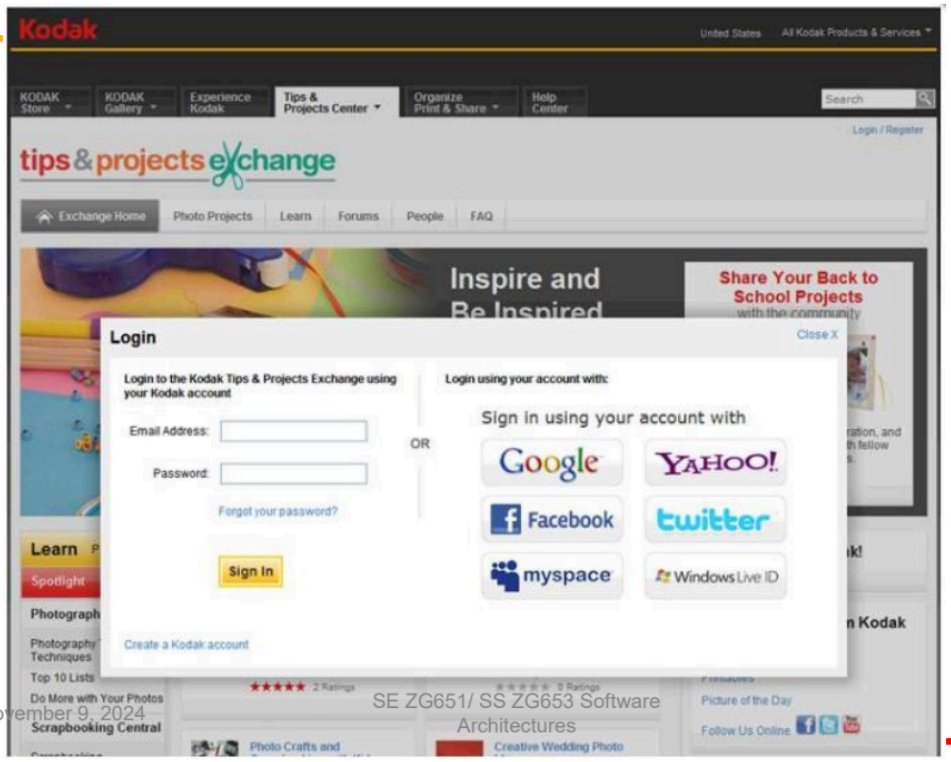
OpenID allows users to sign in to multiple websites using one account, such as Google or Facebook. This reduces the need to remember multiple credentials.

- **Example**: Use your Google account to sign in to other websites without creating new usernames and passwords.

Sample login page: American Cancer Society



Sample login page: Kodak Tips and project Exchange



How OpenID Works

1. **Website Redirects to OpenID Provider**: (e.g., Google).
2. **User Authenticates with Provider**: OpenID provider verifies the user.
3. **Website Receives Authentication**: The user is redirected back with credentials.

OAuth

OAuth authorizes third-party applications to access a user's data stored on another website.

- **Use Case 1**: A photo app accesses photos on Google Drive.
- **Use Case 2**: A printing service accesses images from a photo storage website.

---

3. LDAP (Lightweight Directory Access Protocol)

Overview

LDAP is a protocol used to access and manage directory information in a structured, hierarchical format, often used in large organizations to validate user information.

- **Example**: Using LDAP for user validation on a website with a high volume of registered users to improve performance.

Scenario Suitable for LDAP

LDAP is ideal when:

- You need quick access to frequently requested data.
- Data doesn't change often.
- Data entries are small in size.

---

4. Identity & Access Management (IAM)

Overview

IAM ensures the right people have access to the right technology resources in an organization. It's crucial for regulatory compliance and secure access management.

Features of IAM

1. **Authentication**: Verifying user identity.
2. **Authorization**: Granting permissions to users.
3. **Roles**: Defining user roles with specific permissions.

4. **Delegation**: Allowing users to delegate permissions.
5. **Interoperability**: Sharing identity information across platforms (e.g., using OpenID).

Leading IAM Products

- **IBM Security Identity and Access Assurance**
- **Oracle Identity Cloud Service**
- **Okta**
- **Azure Active Directory**

---

5. Firewalls

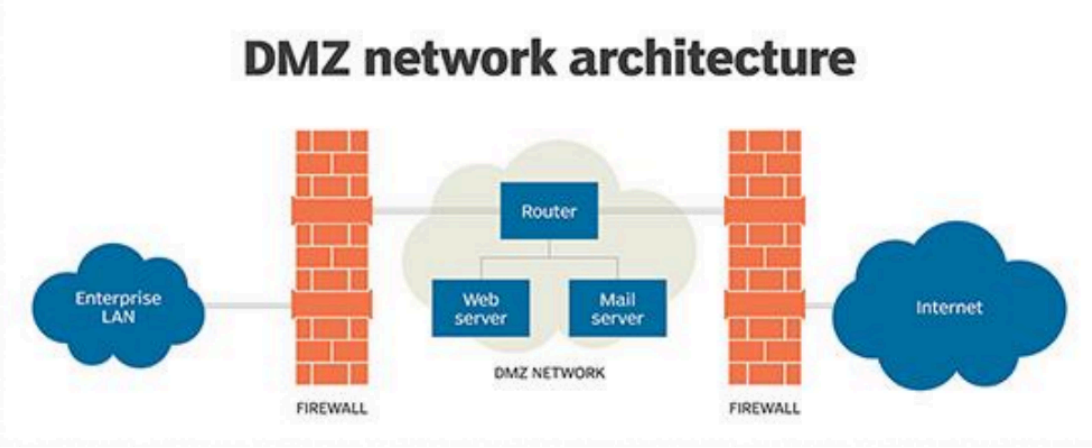
Overview

A firewall is a network security tool that monitors and controls incoming and outgoing traffic based on security rules, helping to protect the network.

De-Militarized Zone (DMZ)

A DMZ is a buffer zone between the internet and an organization's internal network, designed to add an additional layer of security.

Diagram Placeholder: DMZ Structure



Features of Firewalls

- **Intrusion Detection**: Identifies and blocks threats like malware.
- **Access Control**: Allows access based on business needs.
- **Bandwidth Management**: Allocates bandwidth to prioritized applications (e.g., Salesforce over YouTube).

Firewall Techniques

1. **Packet Filtering**: Blocks packets based on IP address or port.
2. **Circuit-Level Gateways**: Monitors sessions between endpoint pairs.
3. **Application Layer Filtering**: Blocks unauthorized applications and protocols.
4. **Address Hiding & NAT**: Protects internal IP addresses.

Diagram Placeholder: Firewall Techniques

Additional Concepts

Business Process Management (BPM) Tools

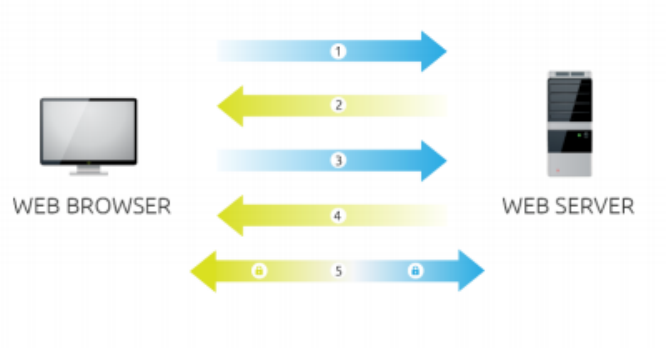
BPM tools help automate, measure, and optimize business processes, providing meaningful metrics to decision-makers.

- **Examples**: Appian, Zoho.

SSL Process

1. **Browser Requests Identity**: Connects to a secured server.
2. **Server Sends SSL Certificate**: Includes server's public key.
3. **Browser Verifies Certificate**: Checks trustworthiness of the certificate.
4. **Symmetric Key Exchange**: Browser creates a session key.
5. **Encrypted Communication**: All data is now encrypted.

Diagram Placeholder: SSL Handshake Process

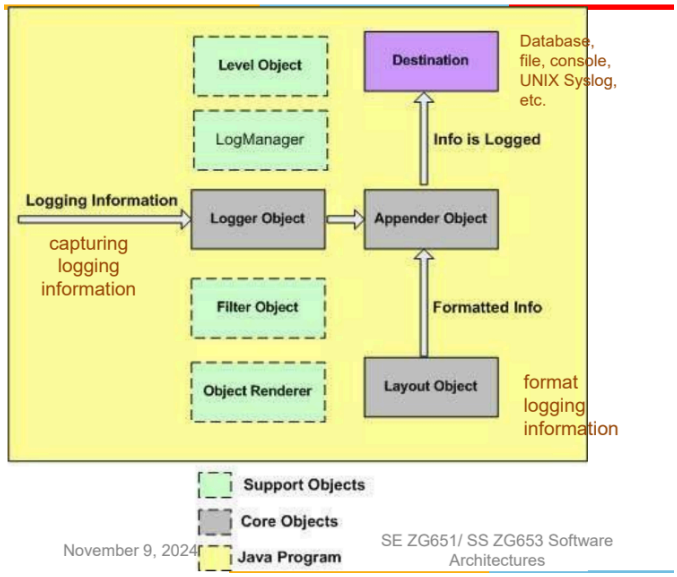


Logging

Logging is crucial for debugging and maintenance, offering a structured way to store application runtime information.

- **Example**: Apache Log4j logs information to databases, files, or consoles.

Diagram Placeholder: Logging Mechanism

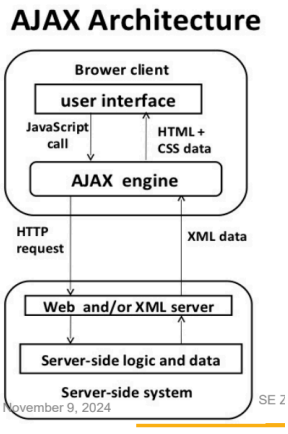


Asynchronous Operations (AJAX)

AJAX enables asynchronous web applications, allowing page updates without reloading.

- **Examples**: Google Maps, where users can drag the map; Google Suggest, where suggestions appear as users type.

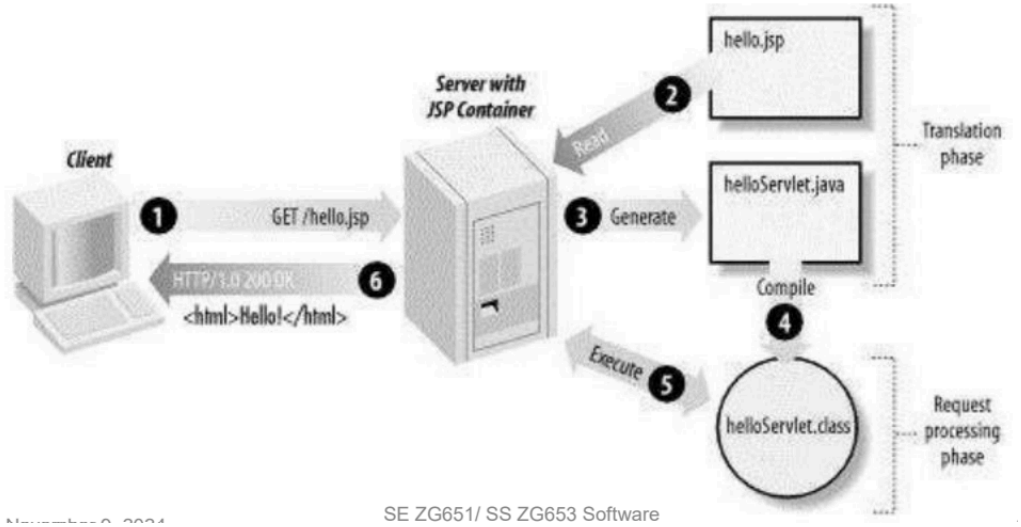
Diagram Placeholder: AJAX Operation



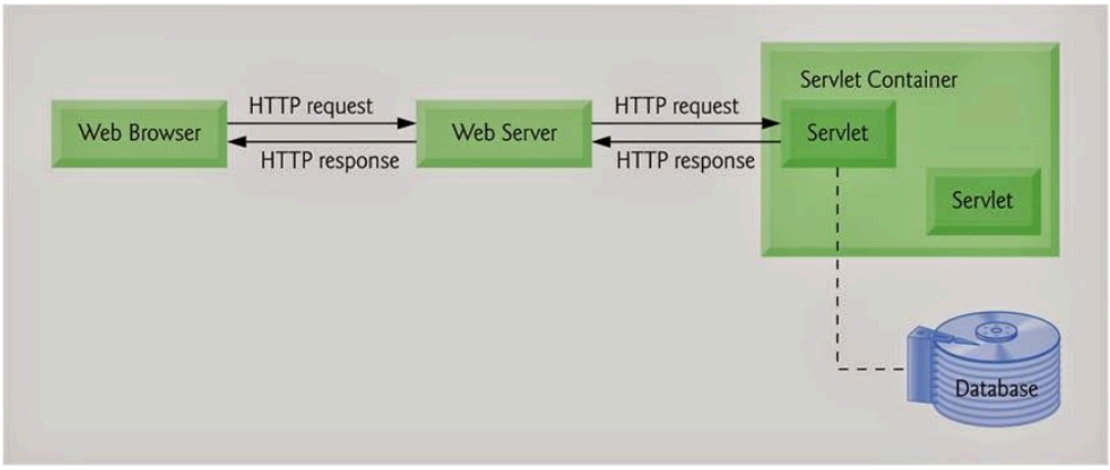
Web Application Architecture

Web applications use a client-server model, often involving dynamic content generated through JSP and Servlets.

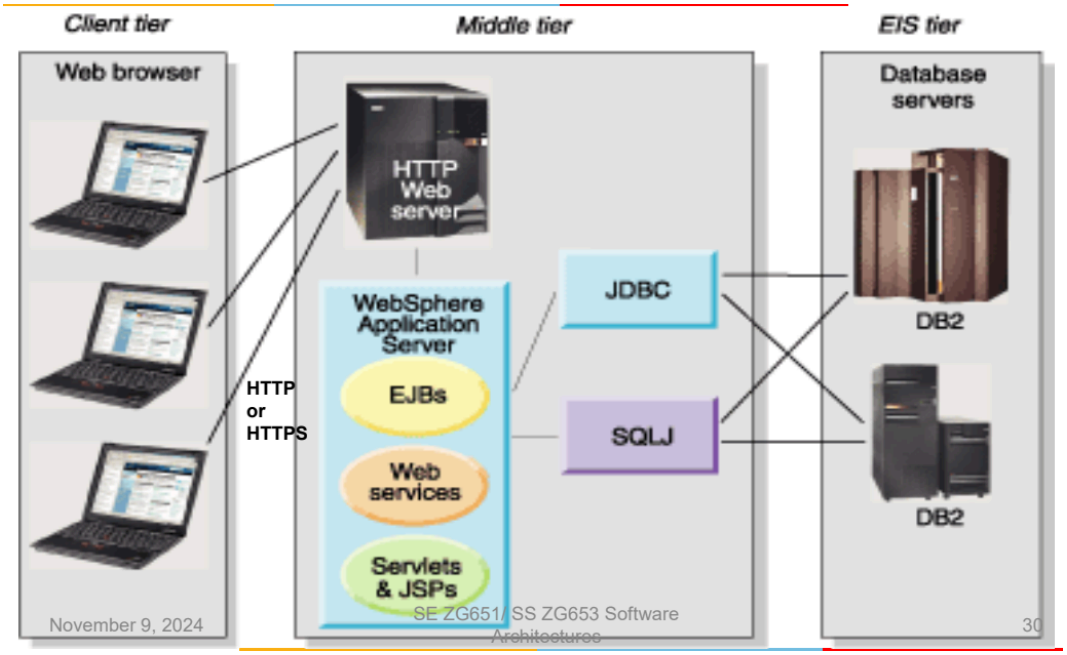
Diagram Placeholder: Web Application Architecture



Dynamic web pages



Web application architecture



Source: Wikipedia