Advanced Spring

Principles of Security in Distributed Systems

Boris Fresow, Markus Günther

Adesso eduCamp 2023

Mastichari, Kos

Security in Distributed Systems

- A general issue and not caused by distributed systems
  - ... but amplified

- Resource-intensive and complex to implement
  - ... but significantly more costly and damaging when not implemented effectively.

What's the worst that could happen?

- Temporary loss of access to business critical information
- Loss of credibility/damage to company reputation
- Temporary loss of ability to trade
- Huge cost for legal & technical consequences

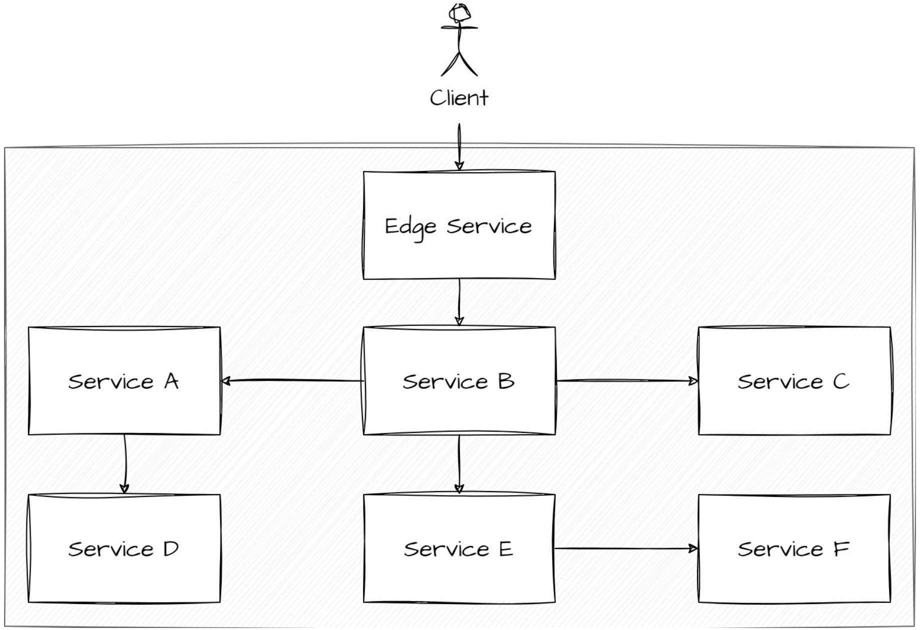
"The Costliest Cyberattacks of 2022" https://securityintelligence.com/articles/13-costliest-cyberattacks-2022/ "Cost of Data Breach Report 2022": https://www.ibm.com/downloads/cas/3R8N1DZJ "Damage Control: The Cost of Security Breaches" https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Amplified - why?

- More systems equals more parts that can break / be broken
- *Monolith vs. Distributed* is not *Bad vs. Good* but a set of tradeoffs, we get ...
  - Loose coupling, **but** communication overhead
  - Scalability, **but** more complex deployment and monitoring
  - Smaller, optimized systems, **but** consistency issues
- Especially **communication** between systems open up additional attack vectors

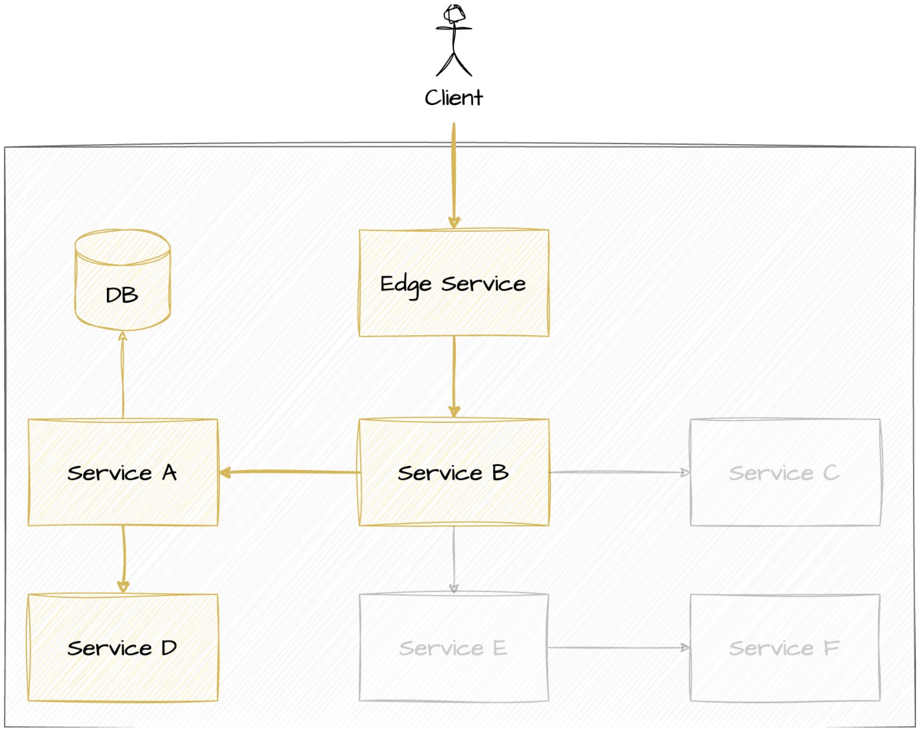
Case study

- Edge Service example
- Clients use-case involve *Service D*
- What does that mean from a security PoV?



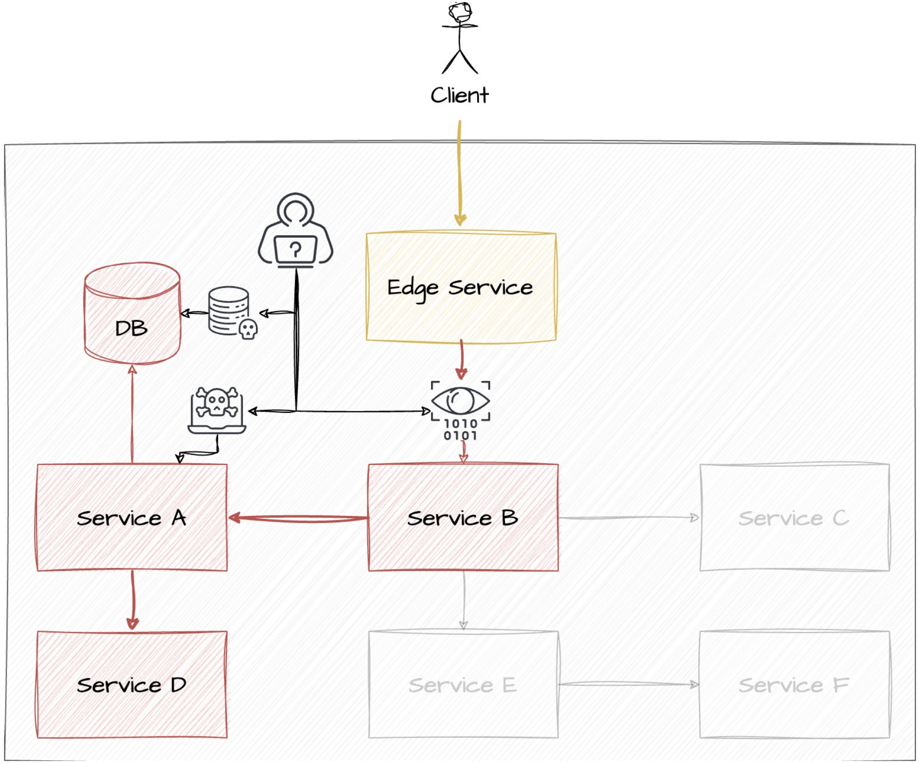
Case study (cont.)

- Everything in yellow is involved
- (We added a database to *Service A* for good measure)
- **What are possible attack vectors?**
  - (within our system)



Case study (cont.)

- **Network** (e.g. man in the middle)
  - The attacker can read information in transit
- **Storage** (e.g. weak credentials)
  - The attacker can read/manipulate information at rest
- **Service** (e.g. remote code execution)
  - The attacker can act as a service



Case study (cont.)

Conclusion

- A distributed system offers potentially a lot of attack vectors
- Communication paths are not always that clear
  - proxies, network segmentation, routing, ...
- Security has to protect us from **internal** and **external** threats

Security Requirements

Key Requirements

What do we want to **guarantee** with security measures?

- **Confidentiality** via Encryption, Authentication
- **Integrity** via Signatures, Hashing, Consensus
- **Availability** via Load Balancing, Redundancy, Monitoring & Recovery

Security measures contribute to ensuring that a system runs in a predictable and reliable way.

Requirements - Confidentiality

- Protection from unauthorized ...
  - access
  - disclosure
  - use
- Ensures the safety of sensitive information
- The absolute basis for any form of trust in a system landscape

Requirements - Integrity

- Assurance that data is ...
    - accurate
    - consistent
    - unaltered (except modified explicitely)
- Non-repudiation only works if we can assure integrity
- Also offers protection against data corruption due to a non-malicious source

Requirements - Availability

- Assurance that information, systems and resources are accessible
- The basis of operational continuity
- Has the most drastic impact on user experience for **all** users

Security Threats

Security Threats

The security measures taken must be adequate in the context of the given security threats. Threats can be categorized in one of these categories:

- Fabrication
- Interception
- Modification
- Interruption

Every threat (except interception) is a **form of data falsification**

Threats - Fabrication

- The creation and injection of false or malicious data
- The Intention is to deceive or disrupt normal operations
- Can be triggered over the air or via data at rest

Example

An attacker has gained access to a messaging system that handles financial transactions. The attacker sends a message to transfer funds to a certain account.

Threats - Interception

- Unauthorized access or acquisition of (sensitive) information
- Also possible over the air or at rest

Example

An attacker has managed to intercept traffic between two nodes exchanging information. These information contain credit card infos as well as user logins. This allows the attacker to login and act as the leaked user.

Threats - Modification

- Alteration of data **and/or** system components
- Potentially compromises the integrity of information
- Can change the behavior of a system

Example

> *An attacker has used a security exploit to alter the configuration of a system. The system now logs every data processed to an additional external system the attacker has full control over.*

Threats - Interruption

- The disruption of denial of access to services / resources
- Impacts the availability and might lead to unexpected behavior

Example

> *An attacker has identified a critical component in a distributed landscape and floods the component with invalid requests/data. The component is rendered unable to respond to legitimate requests which could have significant consequences.*

Security Mechanisms

Security Mechanisms

Security mechanisms are **concrete measures** to mitigate security threats and fulfill our security requirements.

We will focus on parts of:

- Network security
- Access control and authentication
- Data security
- Monitoring, tracing and auditing

Security Mechanisms - continued

There are more aspects to this, that are out of scope for this workshop but you should still keep in mind:

- Physical security
- Device Management
- Patch management
- Disaster recovery / incident response
- Application security
- General Awareness & training

Security Mechanisms - Network security

Ensure the confidentiality, integrity, and availability of data and resources while in transit.

- Firewalls to filter incoming and outgoing traffic
- Intrusion Detection and Prevention Systems (IDPS) to identify and block malicious activities
- Virtual Private Networks (VPN) to secure data transmission
- Secure communication protocols (e.g., SSL/TLS, HTTPS)

Security Mechanisms - Access control and authentication

Ensure that only authorized users can access specific resources or perform certain actions

- User authentication methods
    - passwords
    - multi-factor authentication
- Role-based access control (RBAC) to assign appropriate permissions
- Single sign-on (SSO) solutions for simplified and centralized authentication

Security Mechanisms - Data Security

Protect sensitive information from unauthorized access, disclosure, alteration, or destruction, both when stored and during transmission, ensuring the confidentiality and integrity of the data.

- Encryption for data at rest and in transit
- Data masking and anonymization
- Data backup and recovery solutions

Security Mechanisms - Monitoring and tracing

Continuously observing, logging, and analyzing system activities to detect and respond to potential security threats and maintain the overall health and performance of IT systems.

- Systems to collect and analyze events & logs
- Continuous monitoring and logging of system activities
- Exposure of endpoints that allow the collection of metrics

Questions?