



# BlingBank

2023/24 SIRS Project

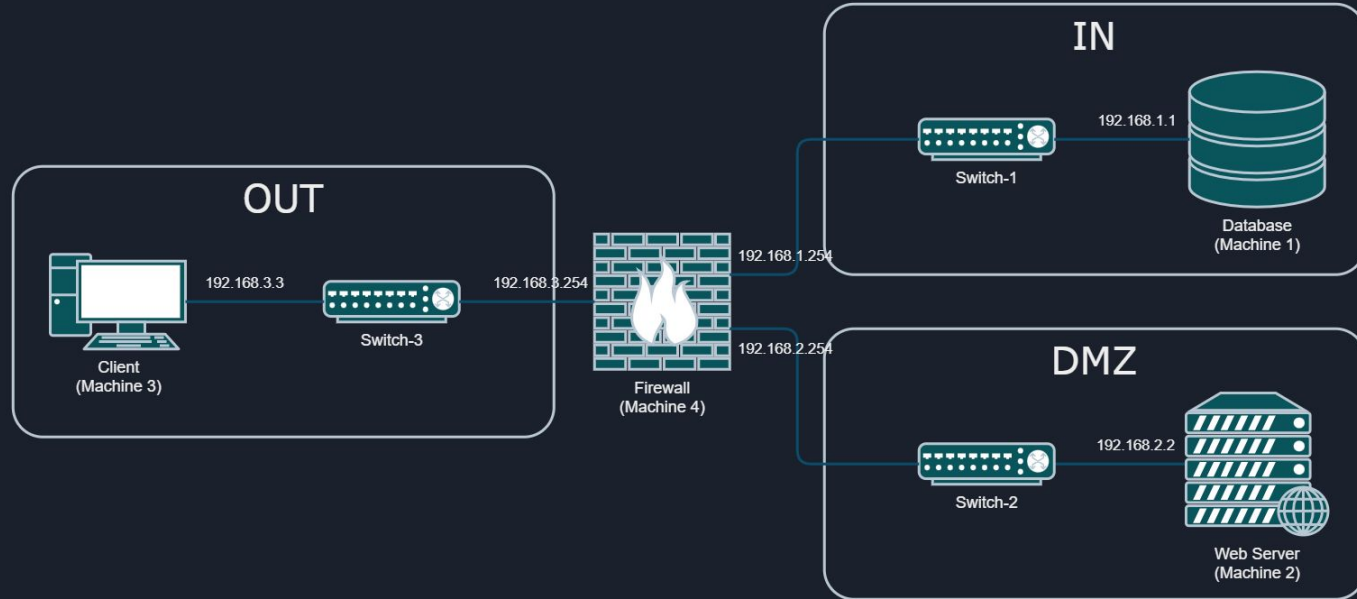
99180 - André Caseiro  
99085 - Ivan Fortes  
99258 - Jorge Santos



# Index

- Infrastructure
- Secure Documents
- Security challenge

# Infrastructure





# Advantages

- Adds an additional layer of security to the internal subnet
- Exposes the services in a more controlled manner
- Minimizes the resource utilization



# Disadvantages

- Single point of failure
- Single filter for all packets in the network



# Secure channels

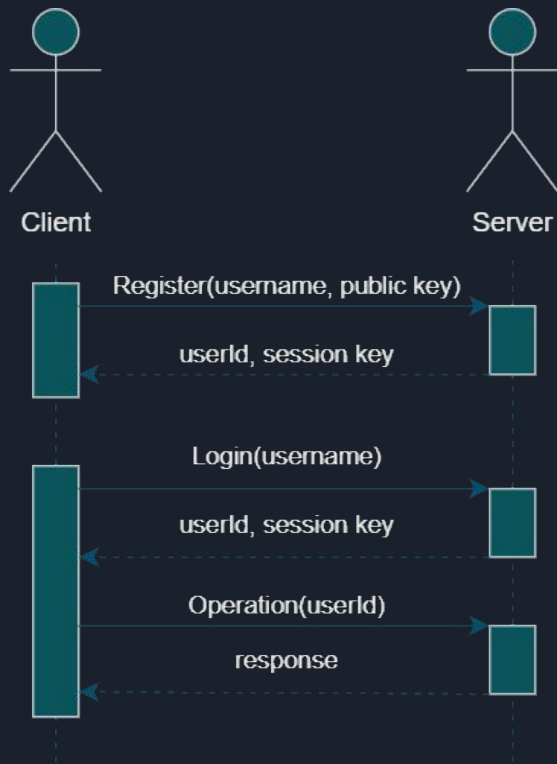
- Https (Client <-> Server)
- Certification authority (CA)
  - Shares certificate with client
  - Signs server certificate
- Server level database encryption



# Security challenge

- New secure document format
- Robust freshness measure
- Dynamic system for key distribution
- Ensure non repudiation of transfers from accounts with multiple owners

# Key distribution







# Secure document format - Server

- Authenticity
- Confidentiality

```
{  
  "value": "+VLbgNxDAQ4dOzumnaUMqr1avBr9k0bPqIfNmK+JfEI1IDhXuBo1+sNp5RQQNNGNAKEjJPo4=",  
  "timestamp": 1703171053131,  
  "mac": "8eFFcDszX8hsUh6l3m6ltQqLKp+7Y2G+ftetG0aE1t8="
```



# Secure Document format - Client

- Confidentiality
- Authenticity
- Non-repudiation

```
{  
  "value": "a00/XSAqJVHhN01Ax35NBMPsEKKL0kzCqr9qJuebTkGtc0xU5d6n9u9hk8A+rNJi",  
  "timestamp": 1703259394960,  
  "signature": "mrgbMxsLBCfnjxvo4 [...] Y4GS7hChXwycxTPKceMzFxVi+yCQ=="  
}
```



# Robust freshness measure

1. Request transfer

```
PUT users/{userId}/transfers/register  
> {origin, destination, amount, description, [...]}
```

2. All account holders approve by signing unique transfer Id

```
POST users/{userId}/transfers/confirm  
> {transferId, signature, [...]}
```

3. Store the list of signatures



# Demonstration

```
***Welcome to BlingBank!***
```

```
1 - Register
```

```
2 - Login
```

```
0 - Exit
```

```
>
```

Recorded version at:

[https://drive.google.com/file/d/1uv\\_uPj3JJAVMkCkK7c6K1P4ZW9jHRwB6/view](https://drive.google.com/file/d/1uv_uPj3JJAVMkCkK7c6K1P4ZW9jHRwB6/view)



# Conclusion

With this project, we conceptualized and implemented a multi-layer infrastructure for an online banking system from the ground up. We assembled the entire infrastructure while ensuring its integrity against external attacks.

Suggestions:

- Login with passwords and identity verifications
- Adding a second firewall

This project provided hands-on experience in creating and protecting a system, reinforcing theoretical knowledge in a practical manner



# Q&A



Ivan Fortes



André Caseiro



Jorge Santos