

Secure Distributed Computing

David Slattery

781-271-5543 • djslatte@mitre.org

NSA Secure Systems Research Office

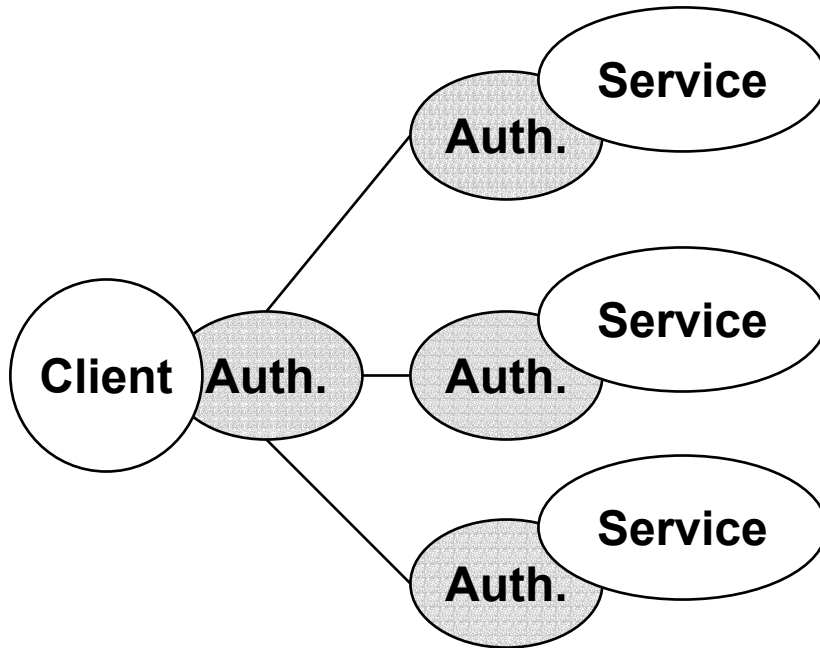
The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

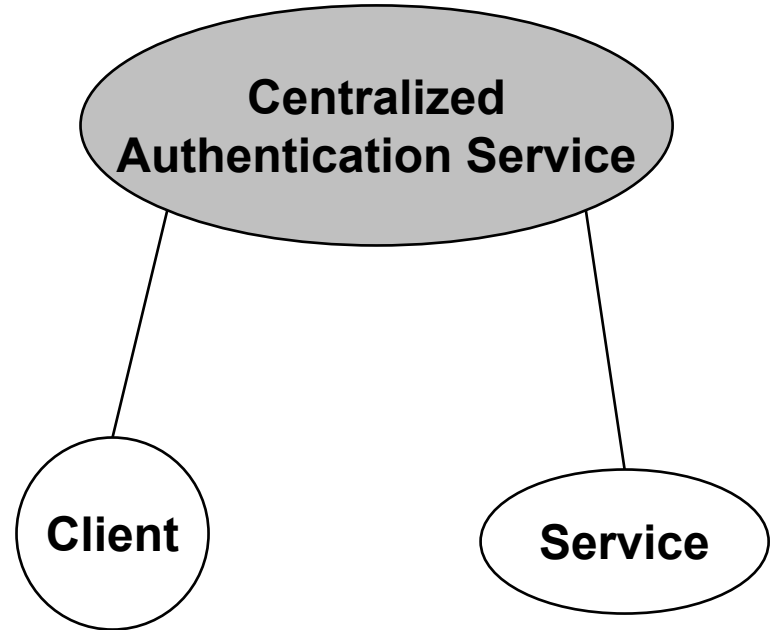
Problem

- How can critical security services be made highly available and secure, while individual service components may be faulty?
- Focus specifically on fault-tolerant distributed authentication
 - Available: ensure that legitimate users get authenticated
 - Secure: ensure that illegitimate users cannot get authenticated

Background



Allows for increased availability, but it comes at the risk of decreased security.



Allows for increased security, but it comes at the cost of decreased availability.

Objective

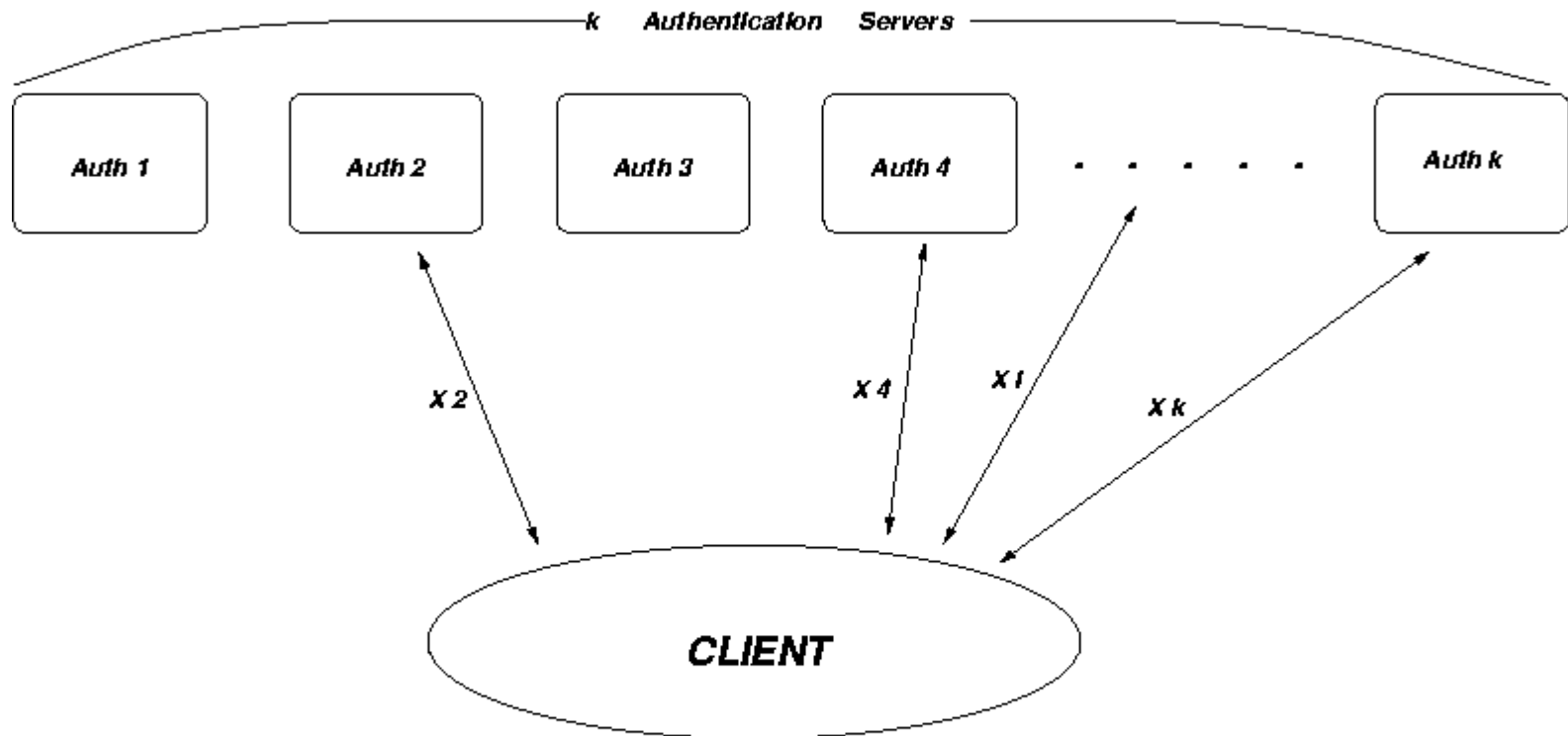
- **Overall Objective: Address security concerns for information processing and management in large, distributed systems.**
- **FY02 Objective: Discover how to simultaneously increase the availability and security of distributed authentication services.**
- **Apply our solution to existing Jini enabled distributed authentication service.**
 - **Retain all security properties**
 - **Increase fault-tolerance and availability**

Activities

- **Study how Threshold Cryptography and other techniques can be used to improve current distributed authentication prototype**
- **Design improved authentication mechanisms for Jini services**
- **Produce and present theoretical paper describing solution**
- **Test our theories with a proof-of-concept prototype based on our research**

Highlight

Distributing Token-Granting ability with Threshold Cryptography



* Any t out of k servers can produce valid authentication token

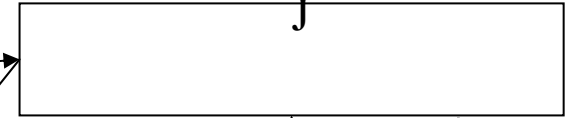
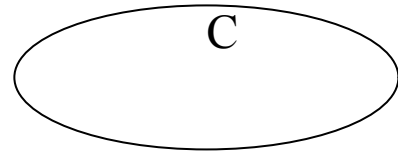
* Client contacts servers to get t valid responses

* Client constructs token X out of t valid X_i pieces

Demonstration

Client's Java Virtual Machine (JVM)

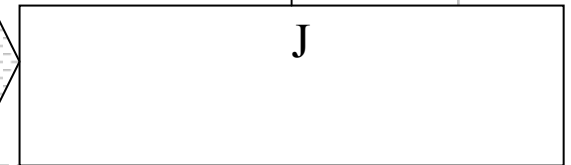
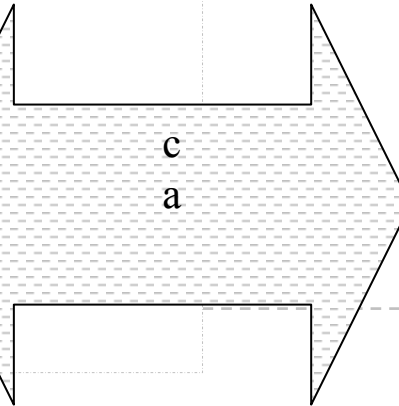
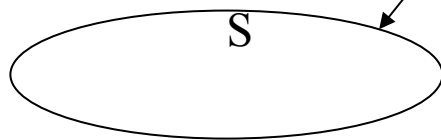
2



4

3

1



FY01 Jini Prototype

Impacts

■ Academic / R&D Community:

- Novel and creative application of theory
- Synthesis of distinct areas of protocol design

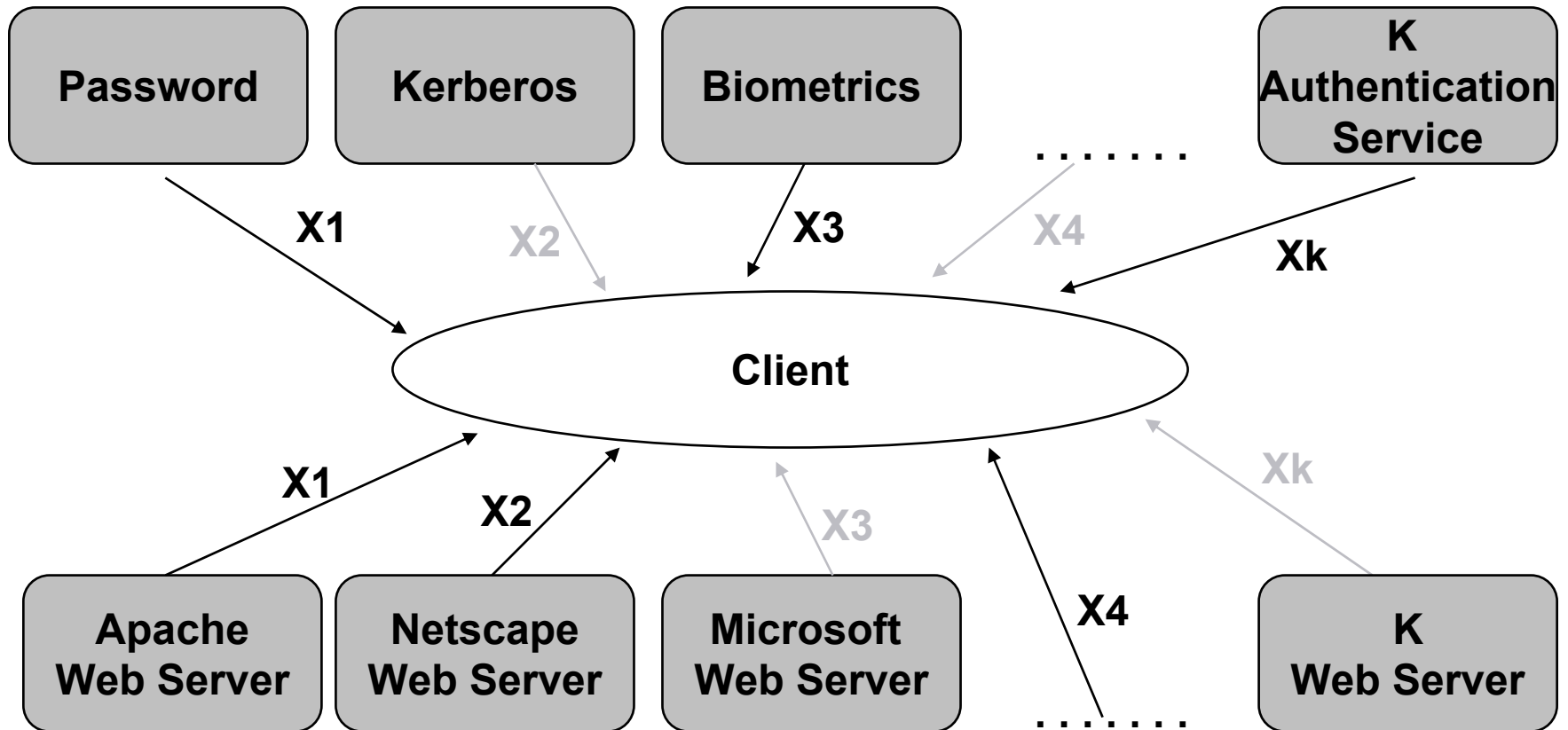
■ Customer Operational Missions:

- Improve the security and availability of distributed systems
- Military systems increasingly required to be distributed, dynamic, functional in hostile environments

Future Plans

Security and application fault-tolerance for critical software services

Example 1: Heterogeneous group of authentication services



Example 2: Heterogeneous group of critical software services