DISTRIBUTED SYSTEMS
Principles and Paradigms
Second Edition
ANDREW S. TANENBAUM
MAARTEN VAN STEEN

Chapter 9
Security

Security Threats, Policies, and Mechanisms

Types of security threats to consider:

- Interception
- Interruption
- Modification
- Fabrication

Example: The Globus Security Architecture (1)

1. The environment consists of multiple administrative domains.
2. Local operations are subject to a local domain security policy only.
3. Global operations require the initiator to be known in each domain where the operation is carried out.

Example: The Globus Security Architecture (2)

4. Operations between entities in different domains require mutual authentication.
5. Global authentication replaces local authentication.
6. Controlling access to resources is subject to local security only.
7. Users can delegate rights to processes.
8. A group of processes in the same domain can share credentials.

Example: The Globus Security Architecture (2)

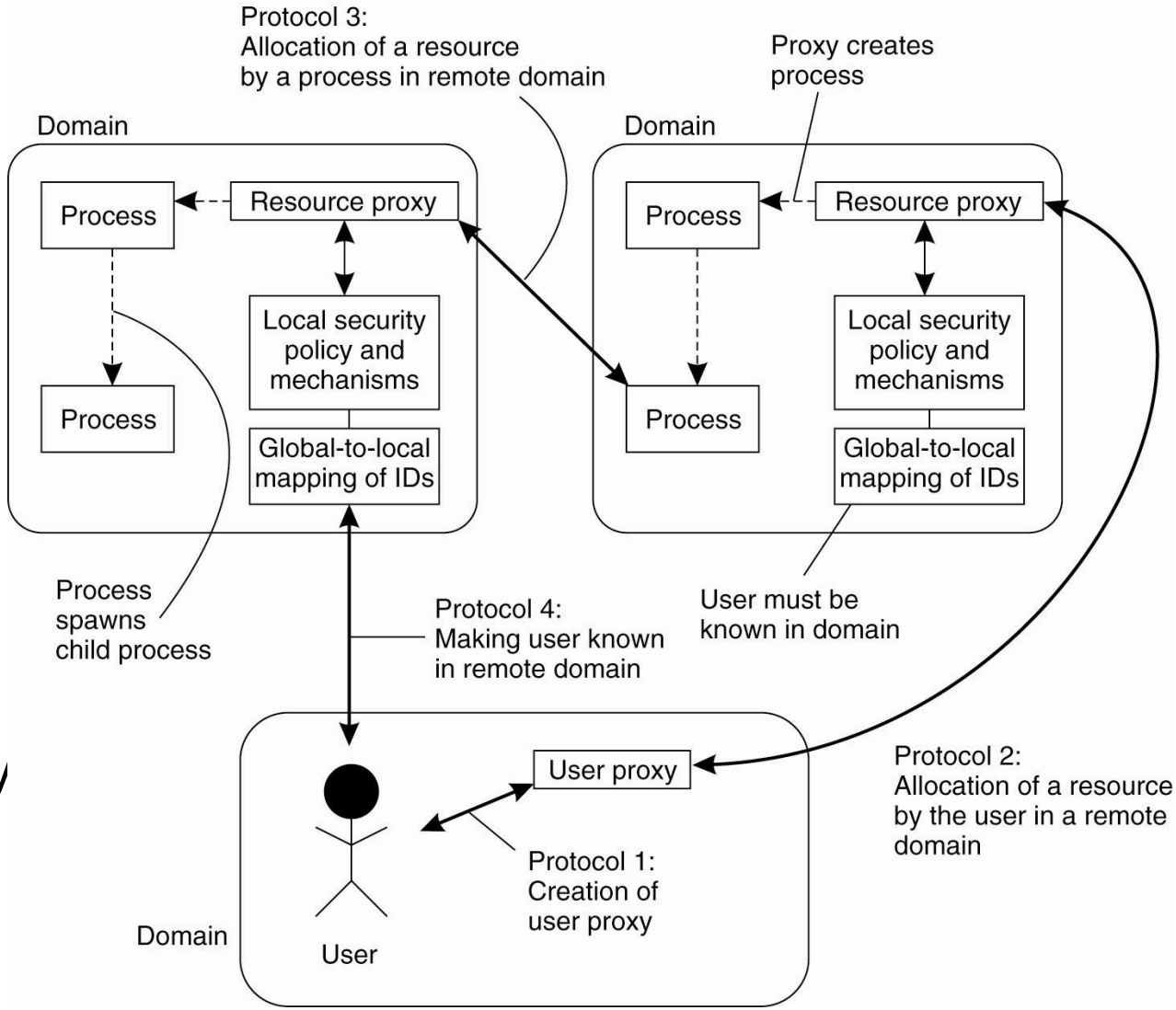
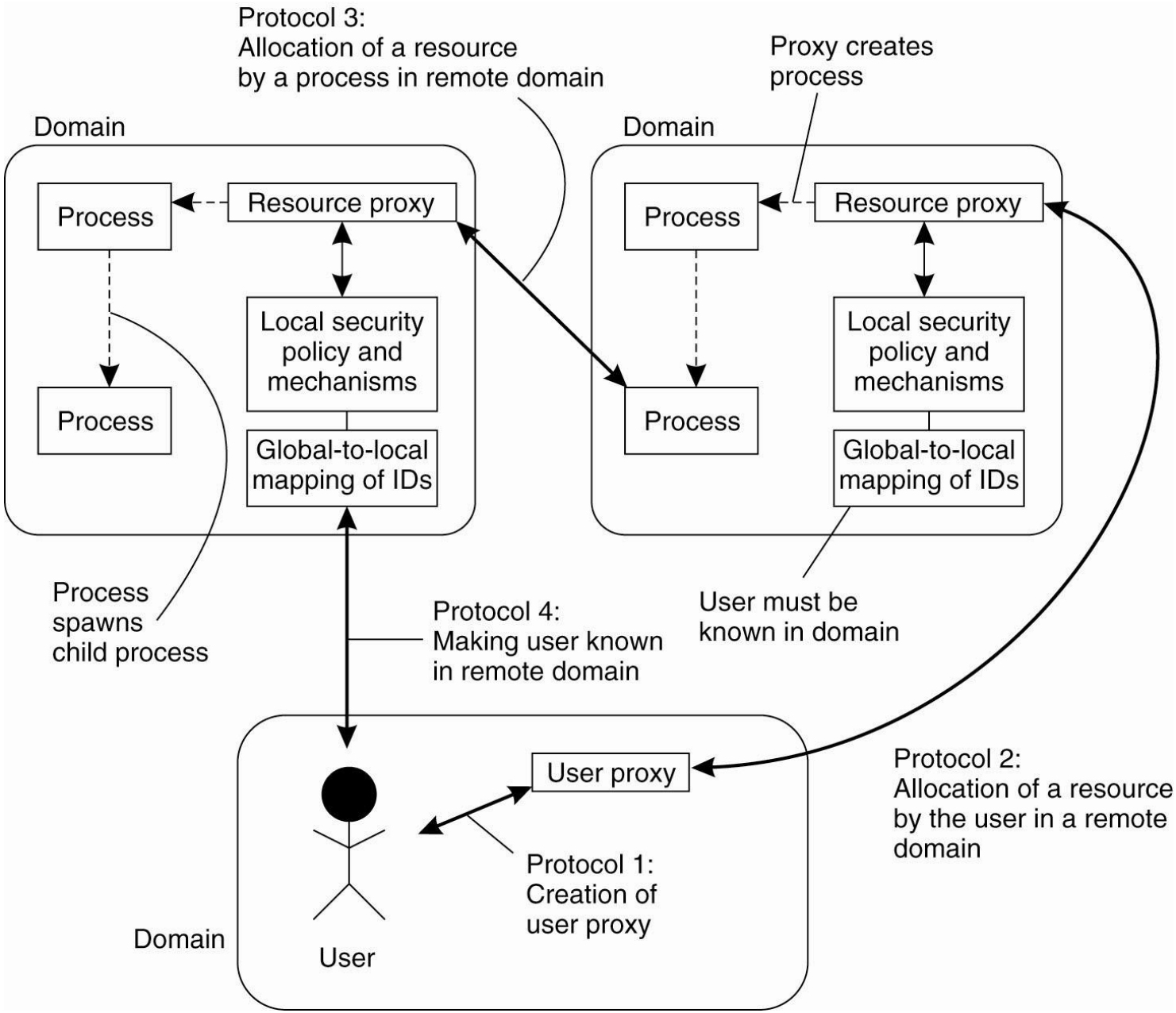


Figure 9-1. The Globus security architecture.



Tanenbaum & Van Steen, Distributed Systems: Principles and Paradigms, 2e, (c) 2007

Focus of Control (1)

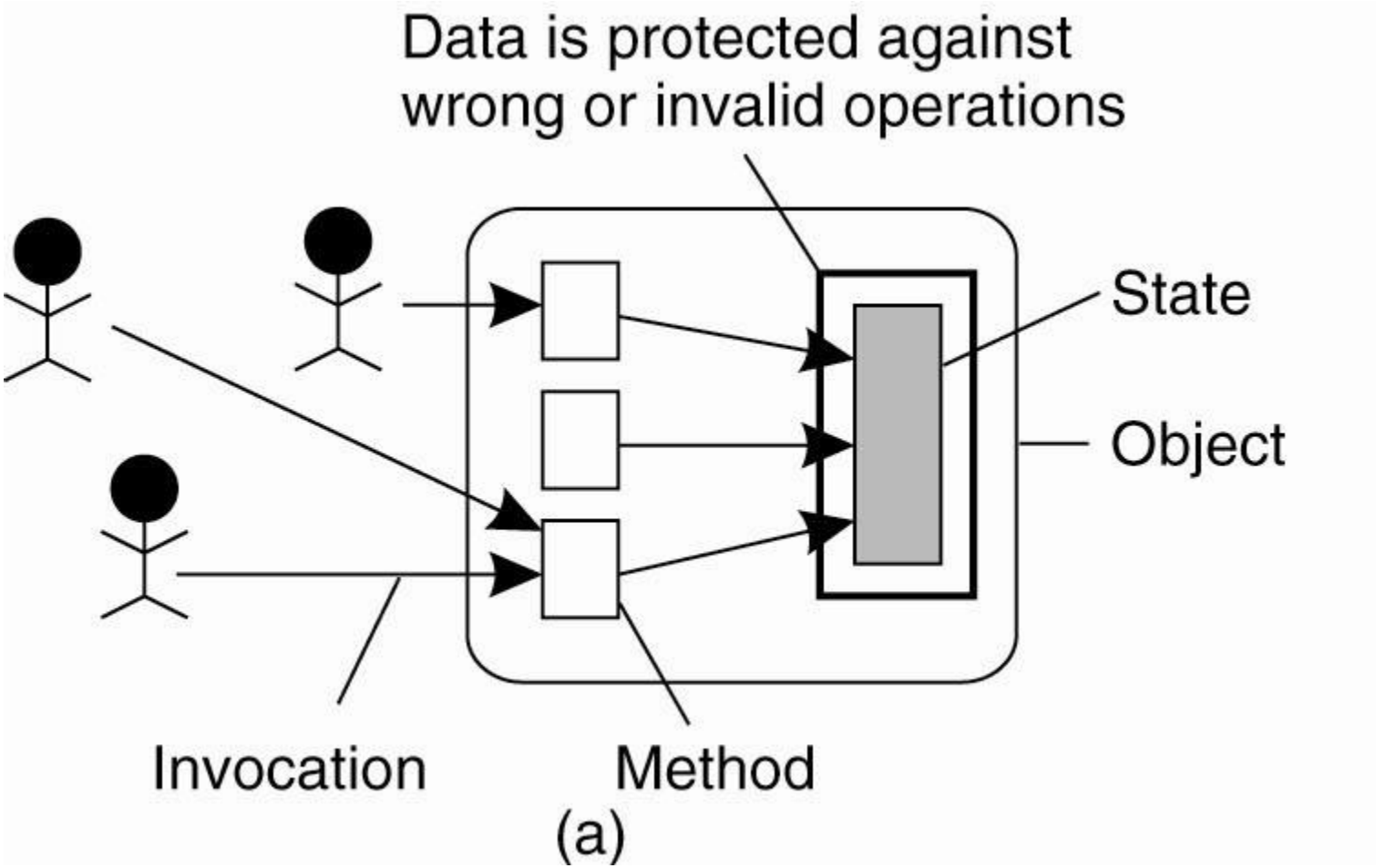


Figure 9-2. Three approaches for protection against security threats. (a) Protection against invalid operations

Focus of Control (2)

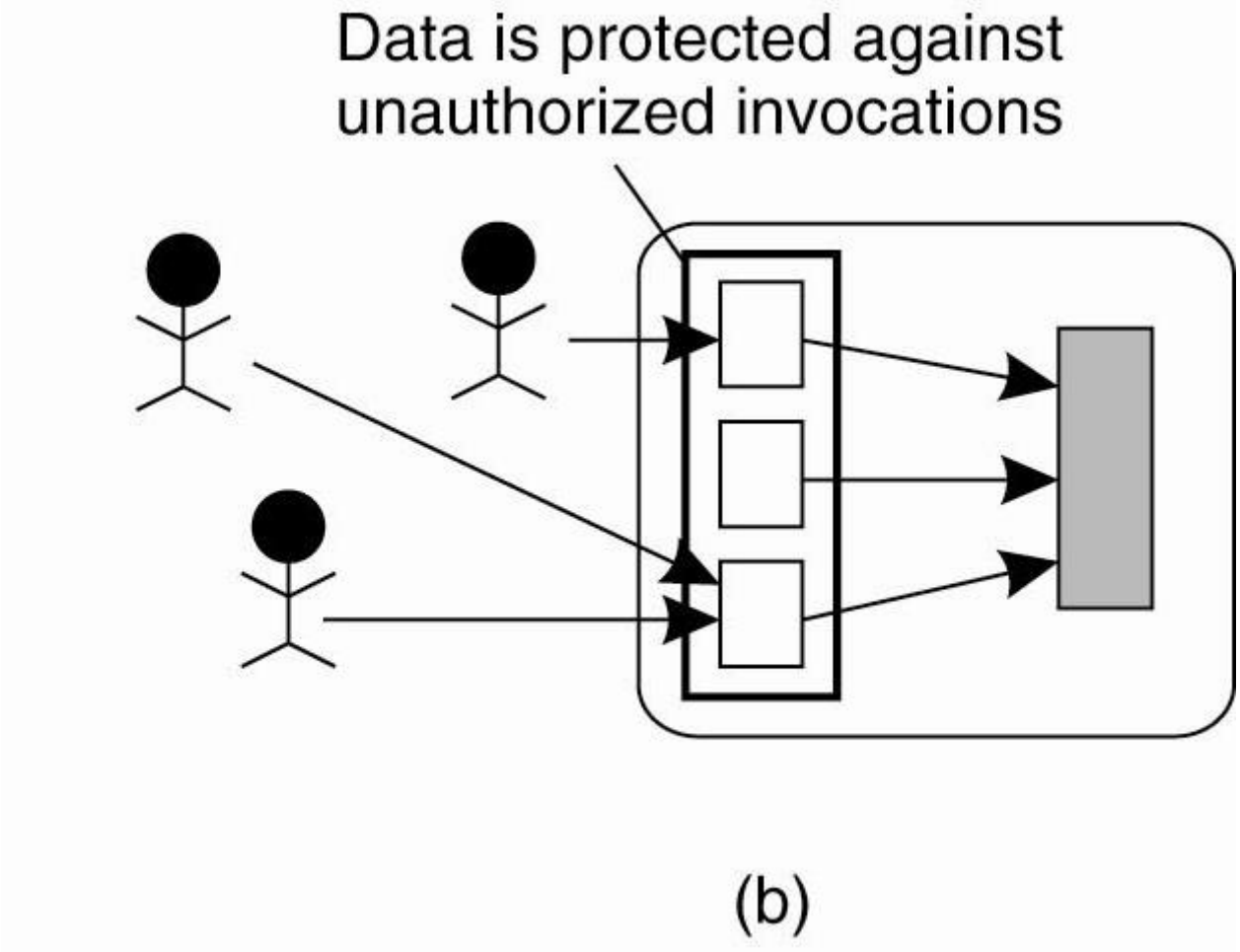


Figure 9-2. Three approaches for protection against security threats. (b) Protection against unauthorized invocations.

Focus of Control (3)

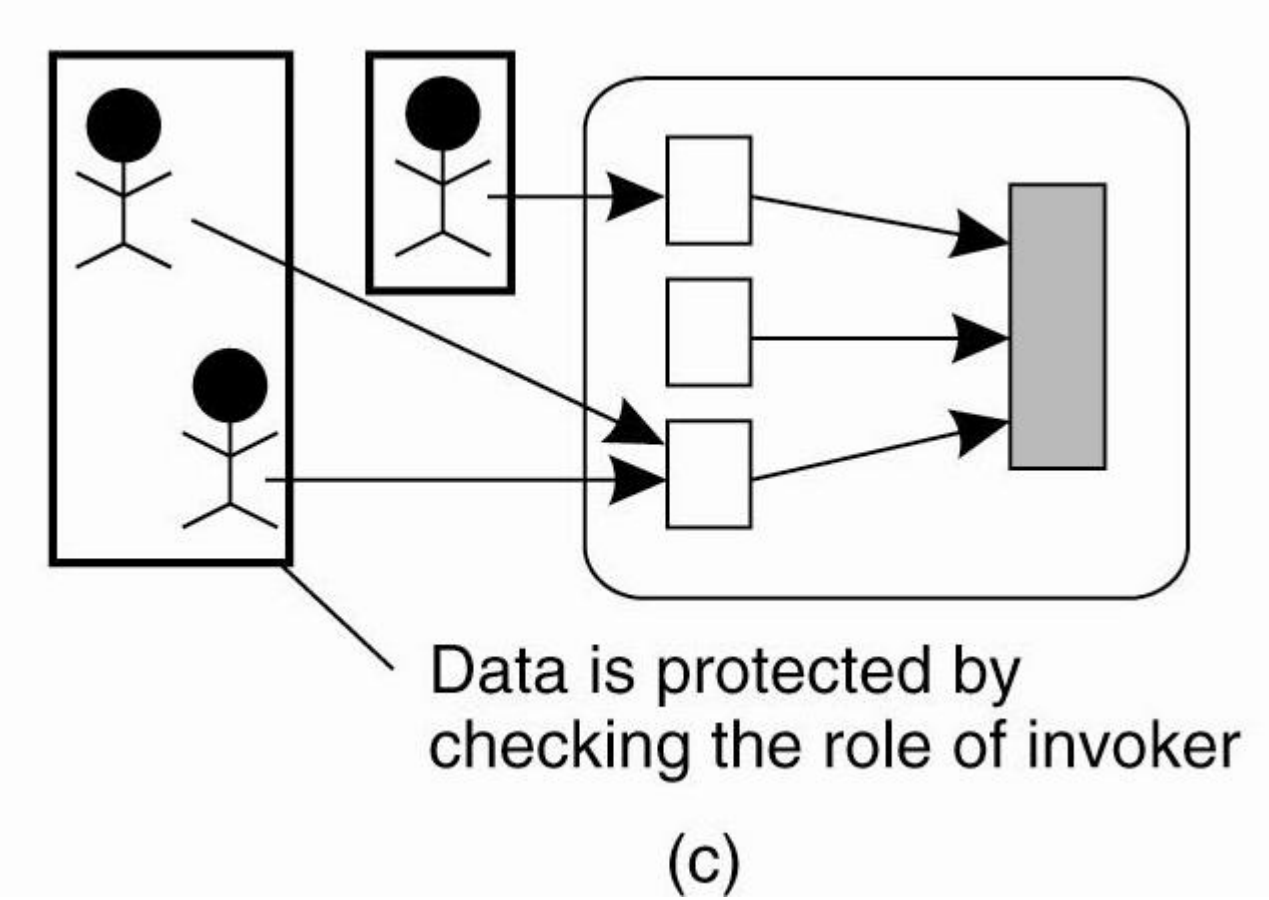


Figure 9-2. Three approaches for protection against security threats. (c) Protection against unauthorized users.

Layering of Security Mechanisms (1)

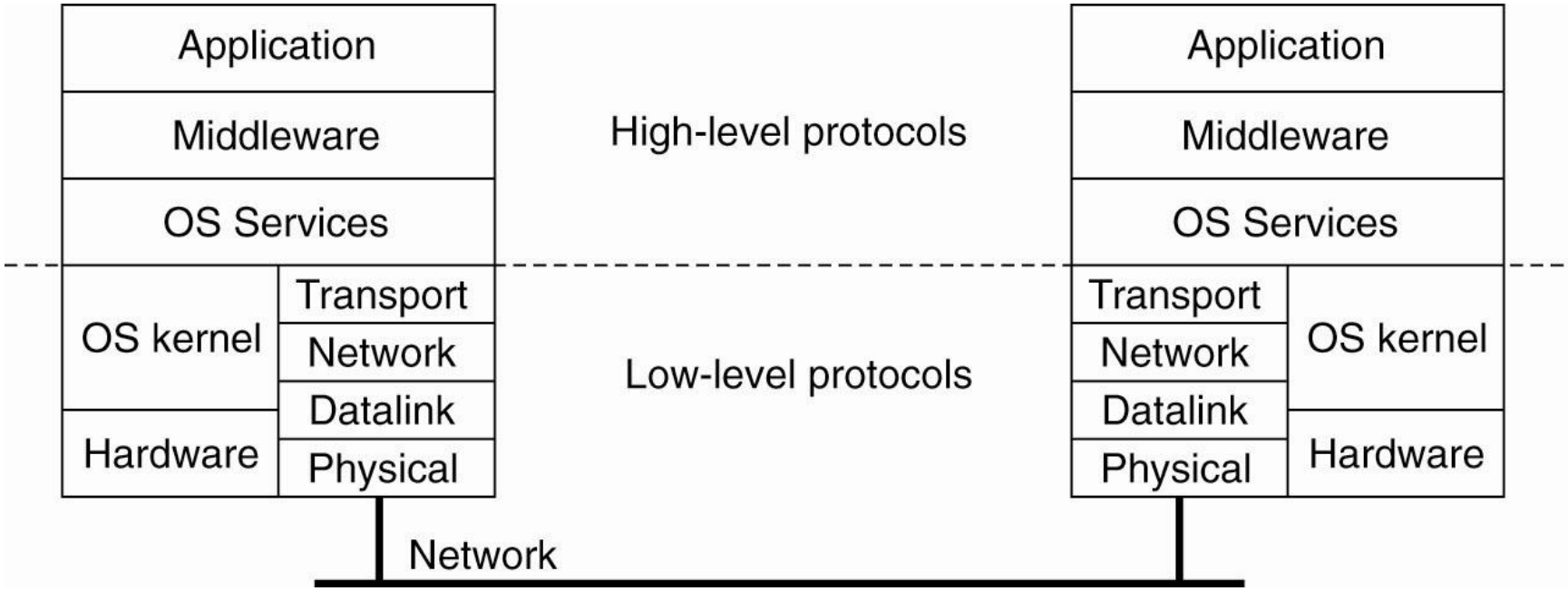


Figure 9-3. The logical organization of a distributed system into several layers.

Layering of Security Mechanisms (2)

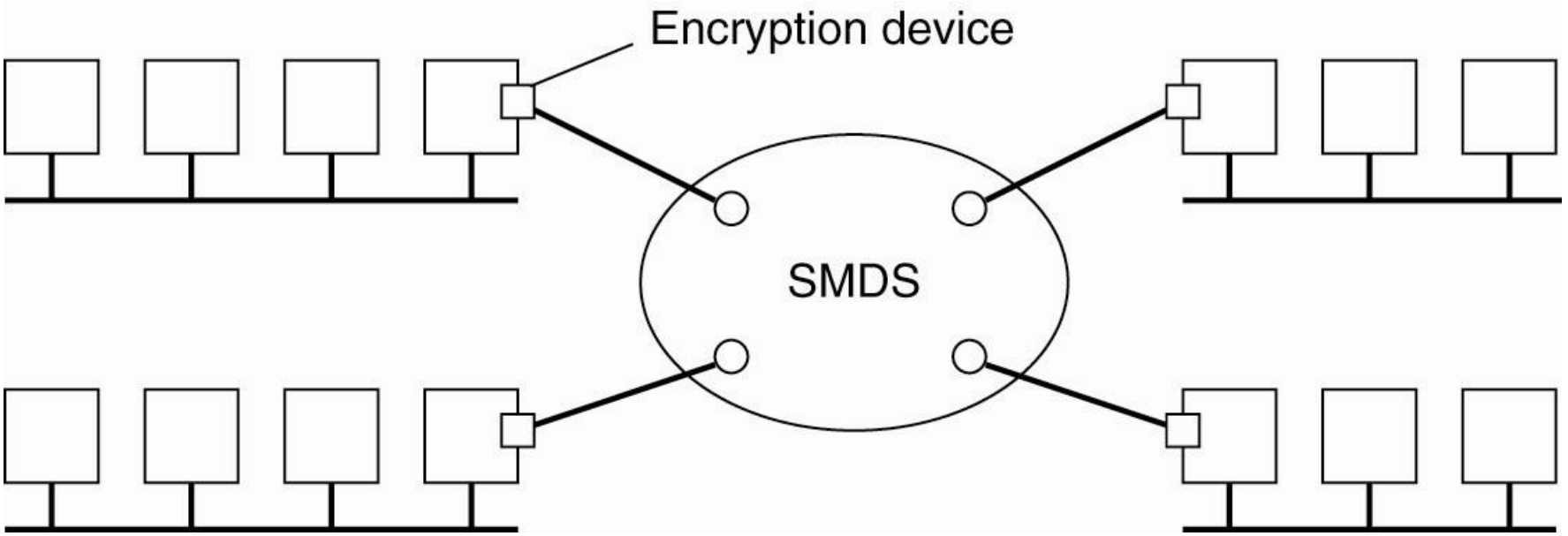


Figure 9-4. Several sites connected through a wide-area backbone service (Switched Multi-megabit Data Services).

Distribution of Security Mechanisms

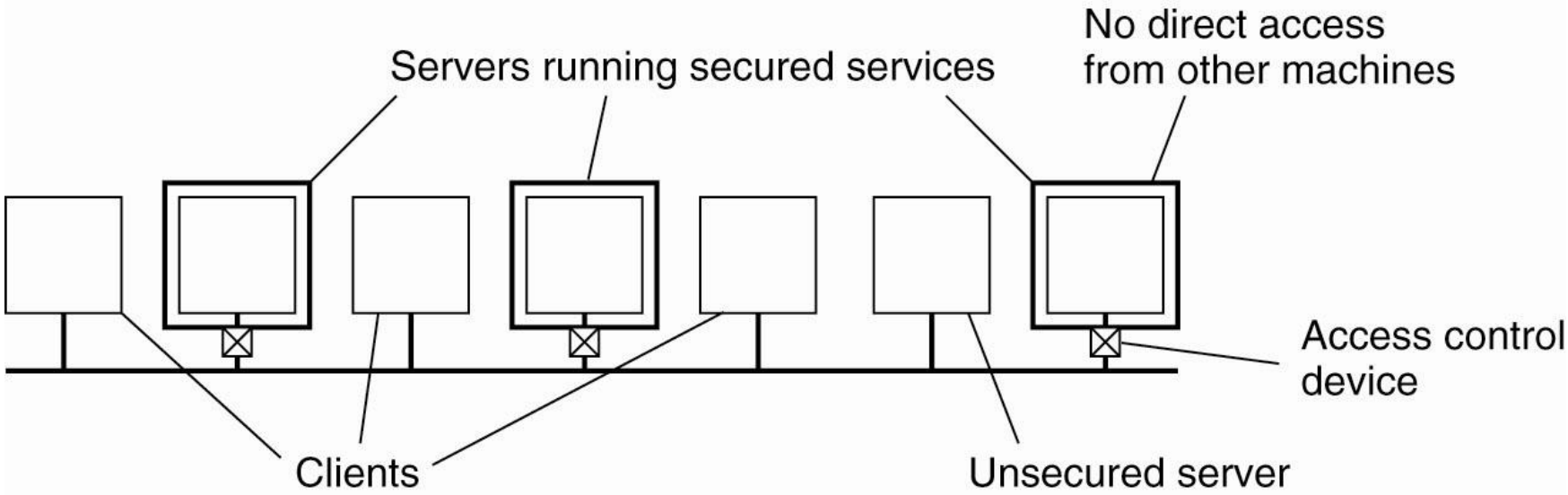


Figure 9-5. The principle of RISSC
(Reduced Interfaces for Secure Systems Components)
as applied to secure distributed systems.

Authentication Based on a Shared Secret Key (1)

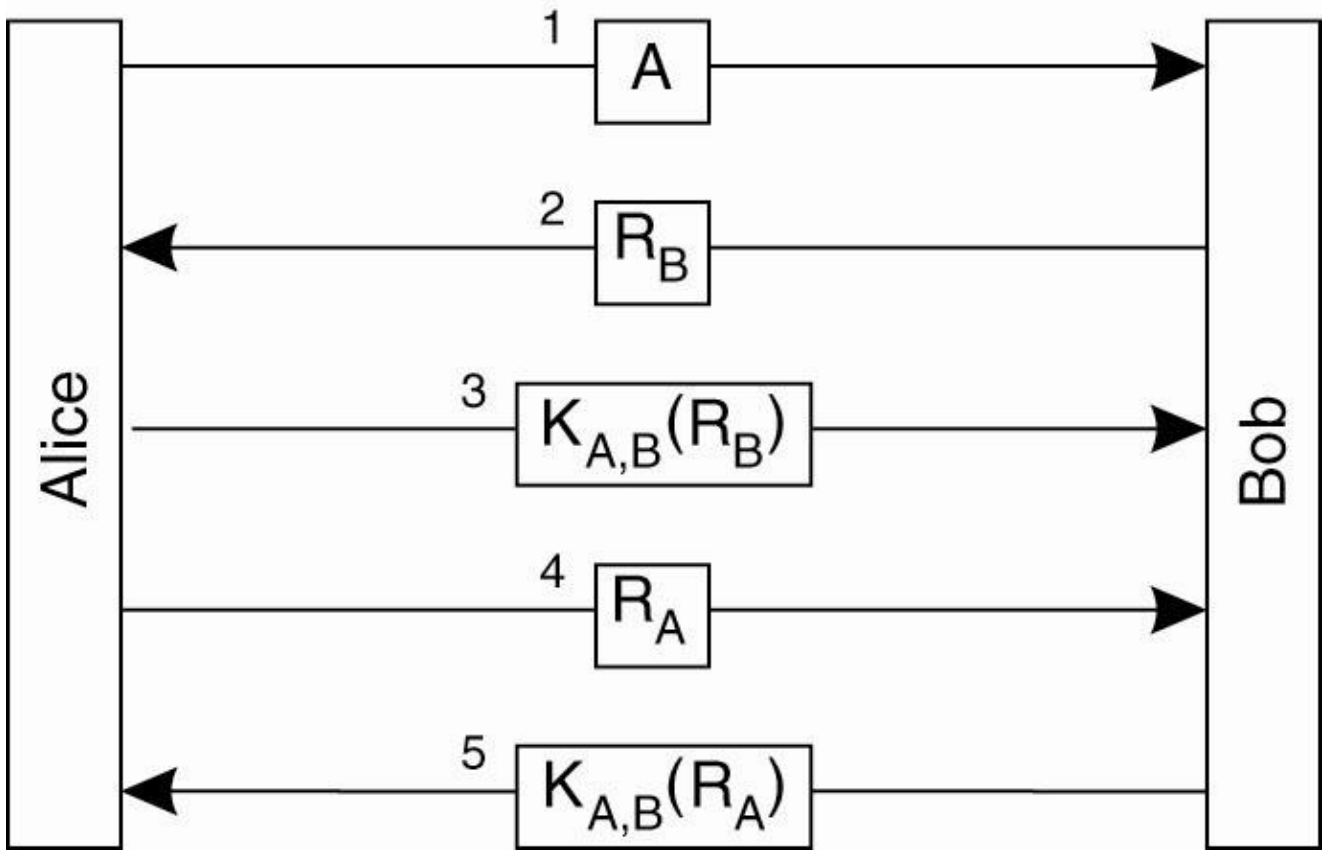


Figure 9-12. Authentication based on a shared secret key.

Authentication Based on a Shared Secret Key (2)

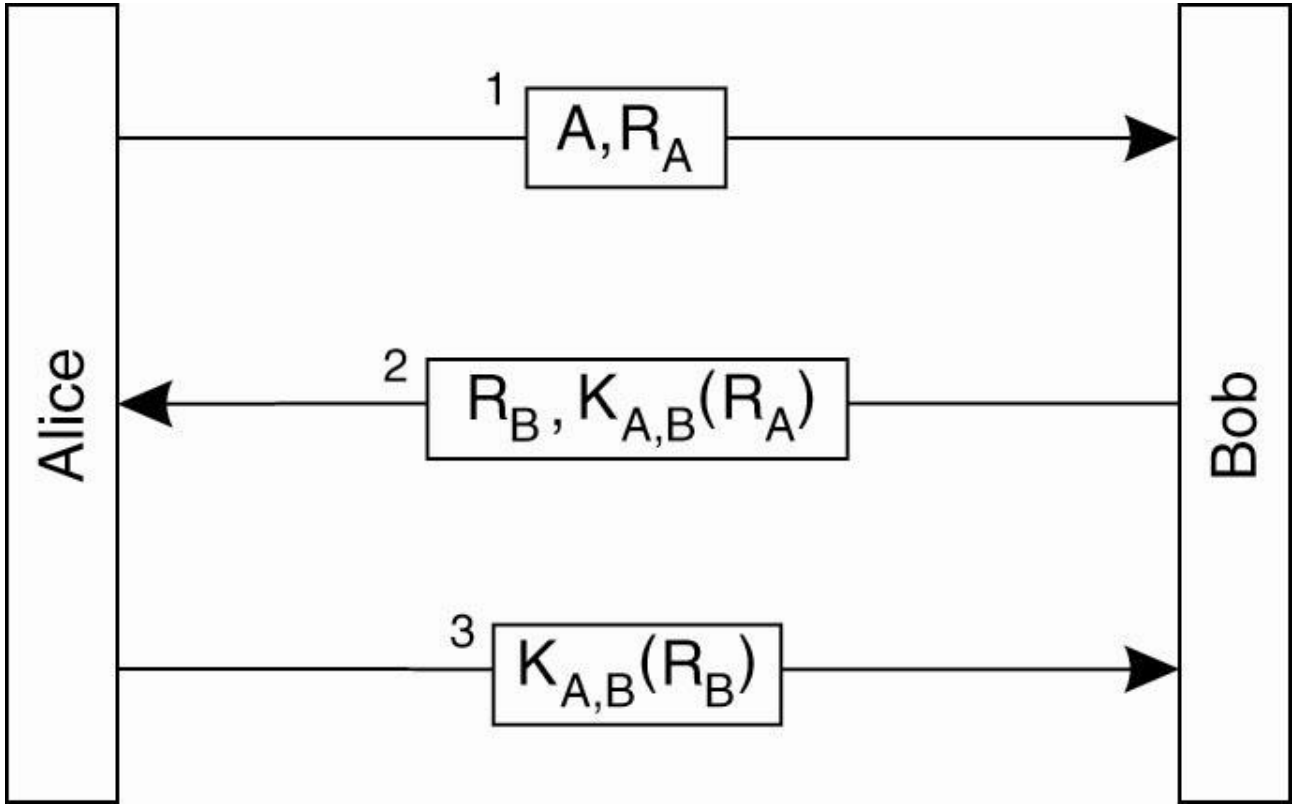


Figure 9-13. Authentication based on a shared secret key, but using three instead of five messages.

Authentication Based on a Shared Secret Key (3)

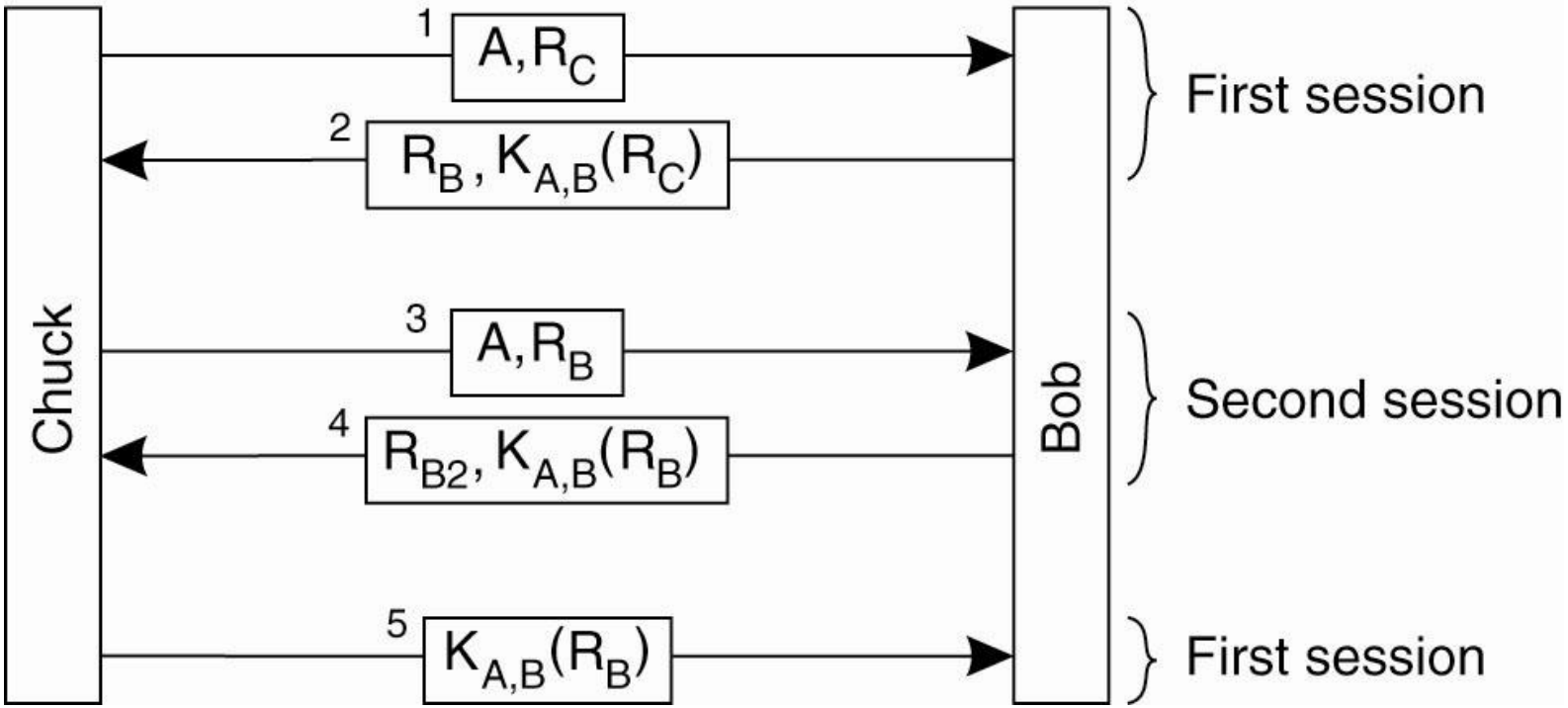


Figure 9-14. The reflection attack.

Authentication Using a Key Distribution Center (1)

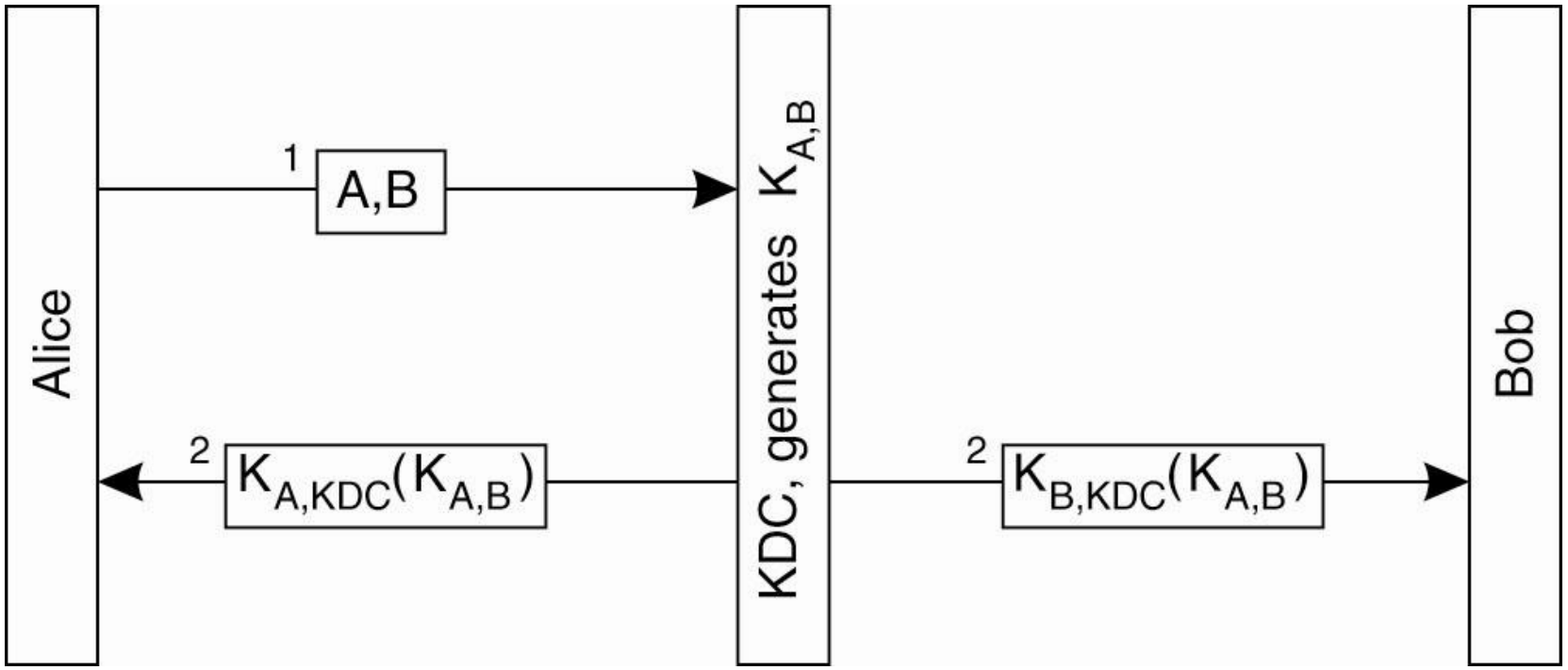


Figure 9-15. The principle of using a KDC.

Authentication Using a Key Distribution Center (2)

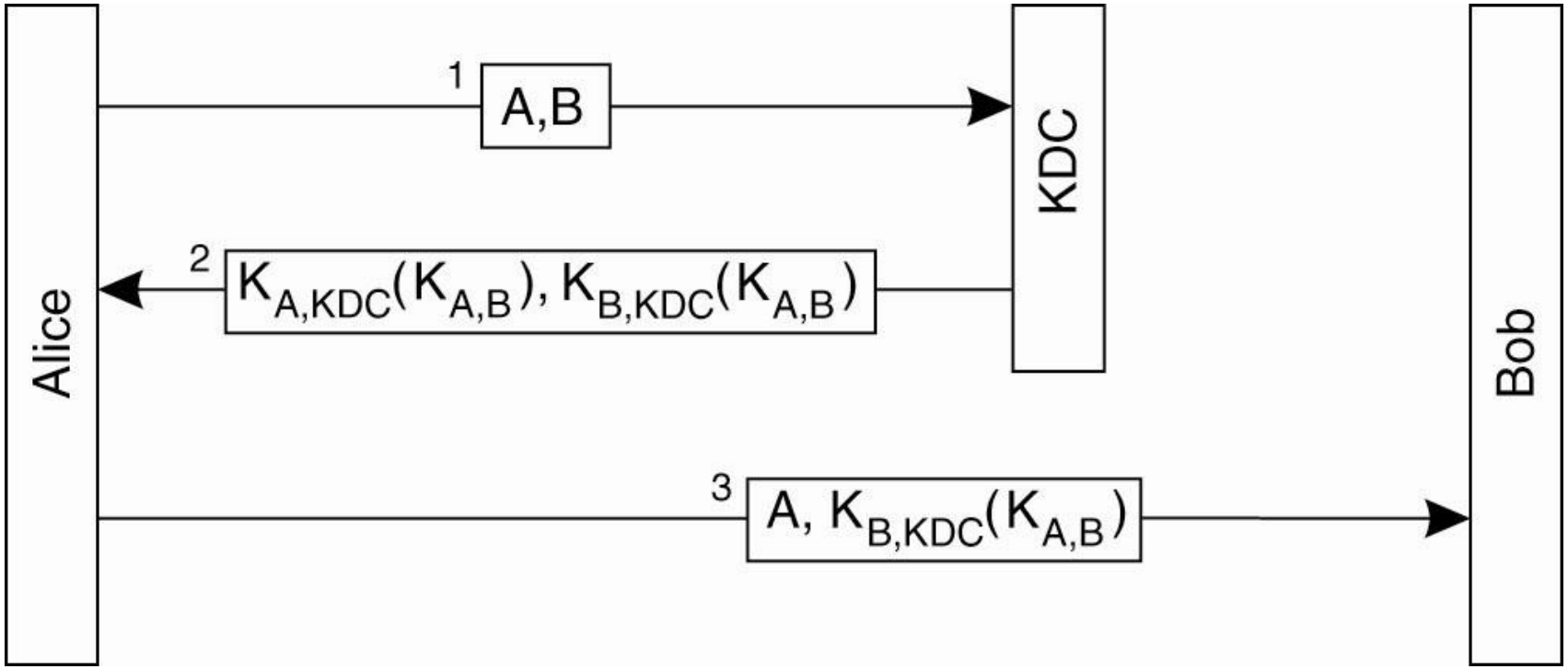


Figure 9-16. Using a ticket and letting Alice set up a connection to Bob.

Authentication Using a Key Distribution Center (3)

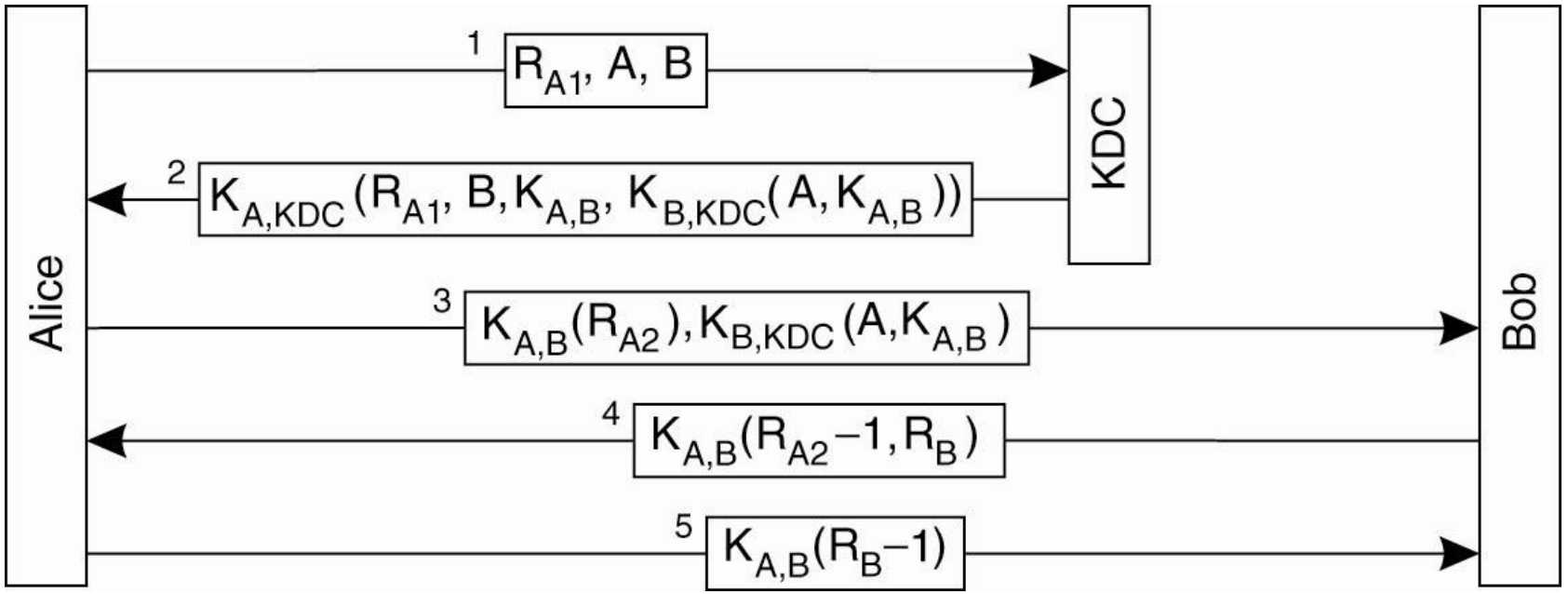


Figure 9-17. The Needham-Schroeder authentication protocol.

Authentication Using a Key Distribution Center (4)

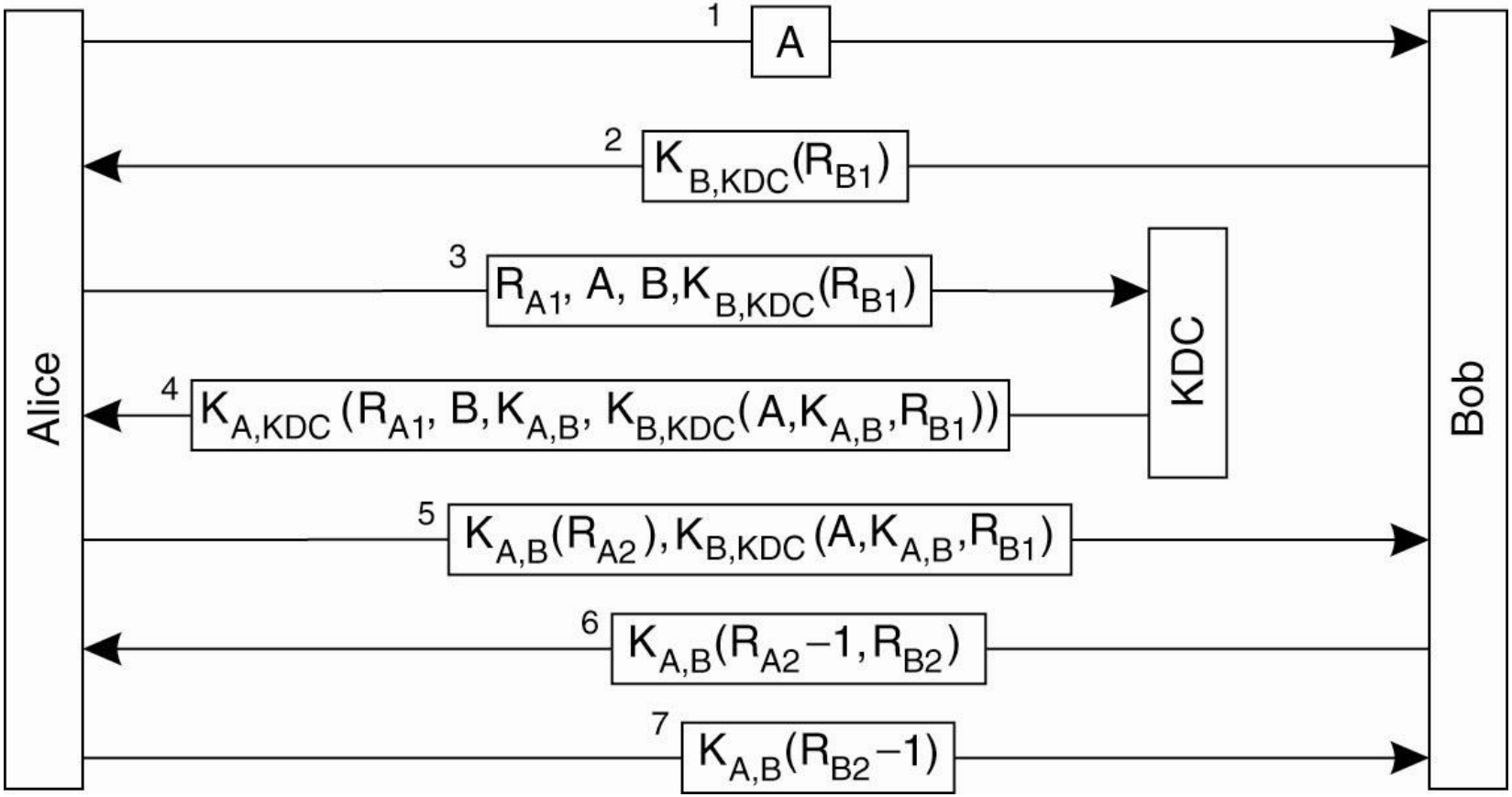


Figure 9-18. Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.

Authentication Using Public-Key Cryptography

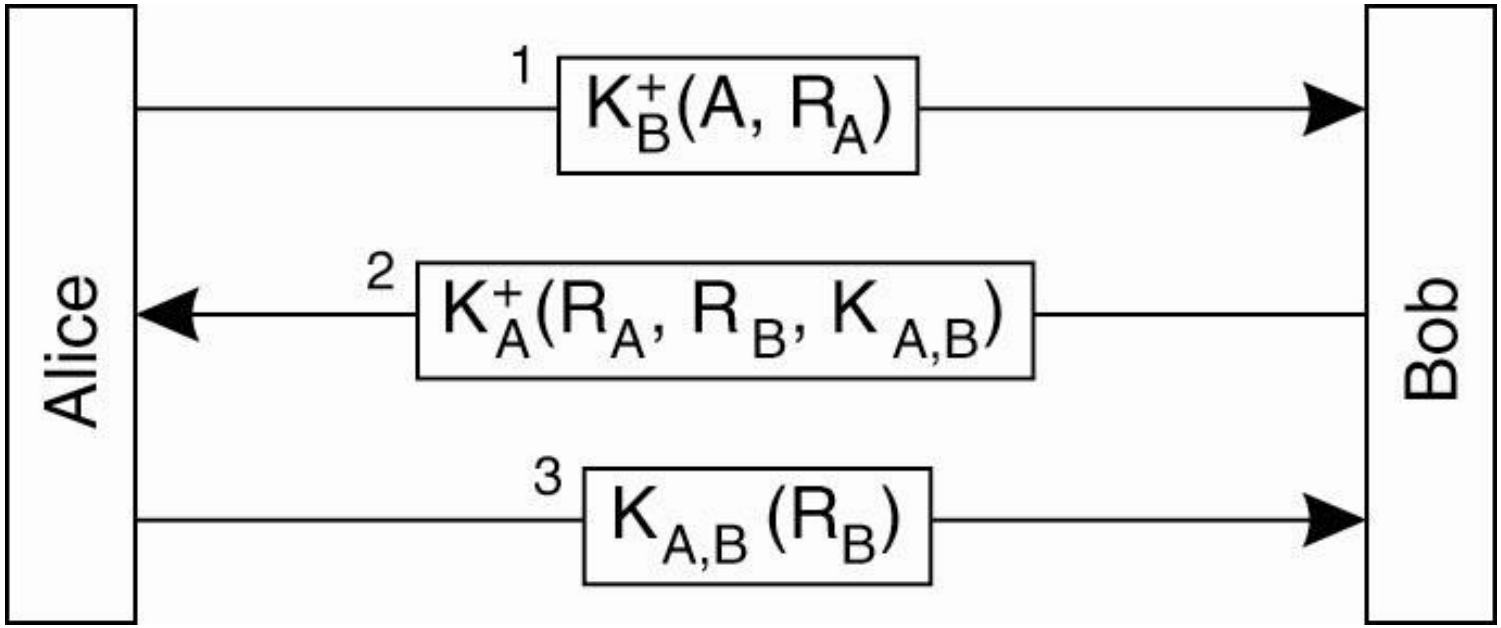


Figure 9-19. Mutual authentication in a public-key cryptosystem.

Digital Signatures (1)

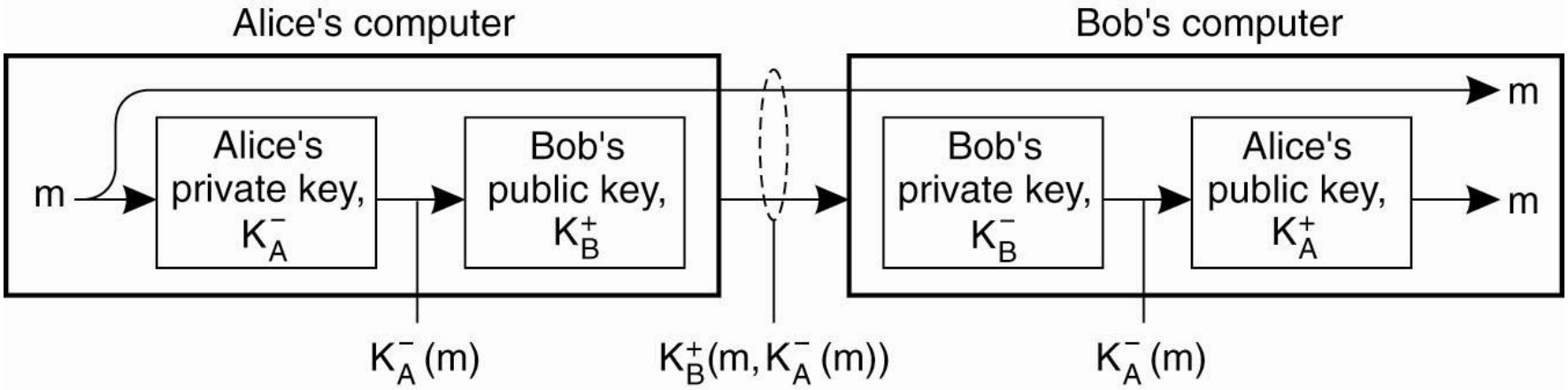


Figure 9-20. Digital signing a message using public-key cryptography.

Digital Signatures (2)

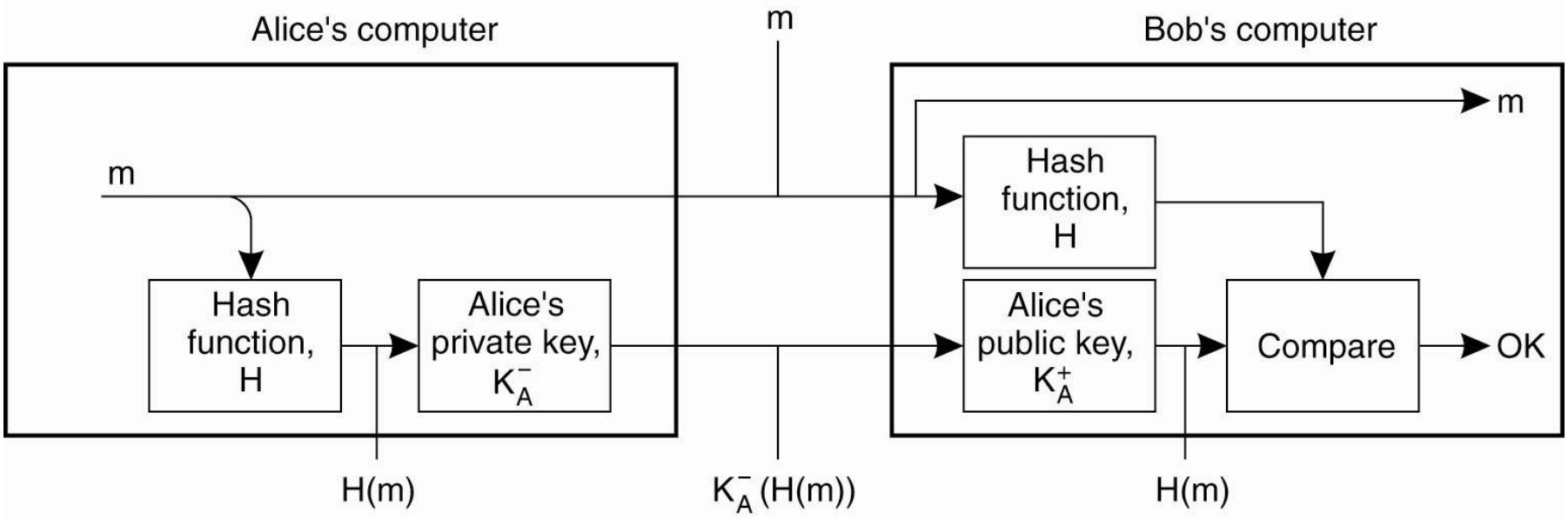


Figure 9-21. Digitally signing a message using a message digest.

Secure Replicated Servers

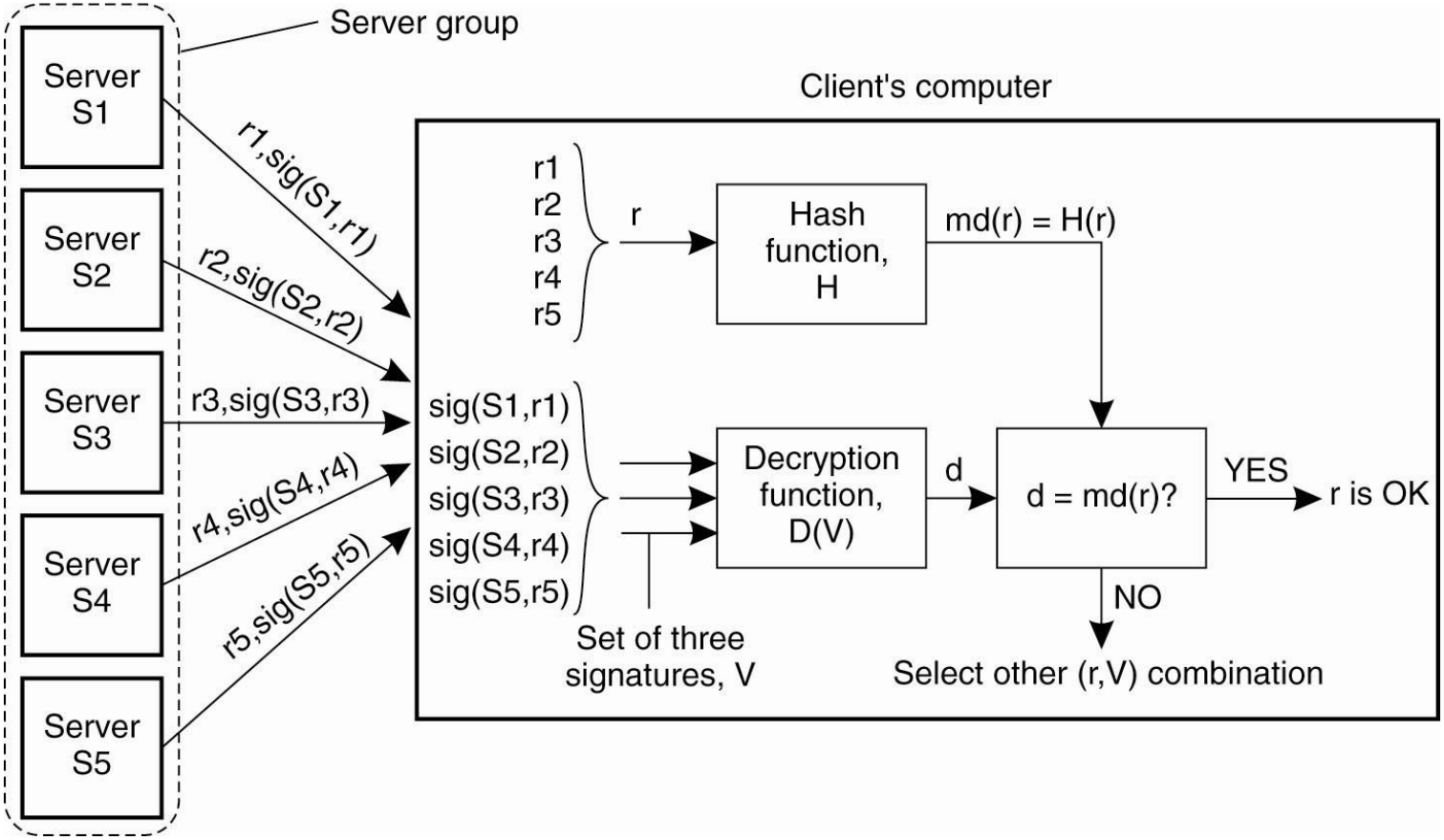


Figure 9-22. Sharing a secret signature in a group of replicated servers.

Example: Kerberos (1)

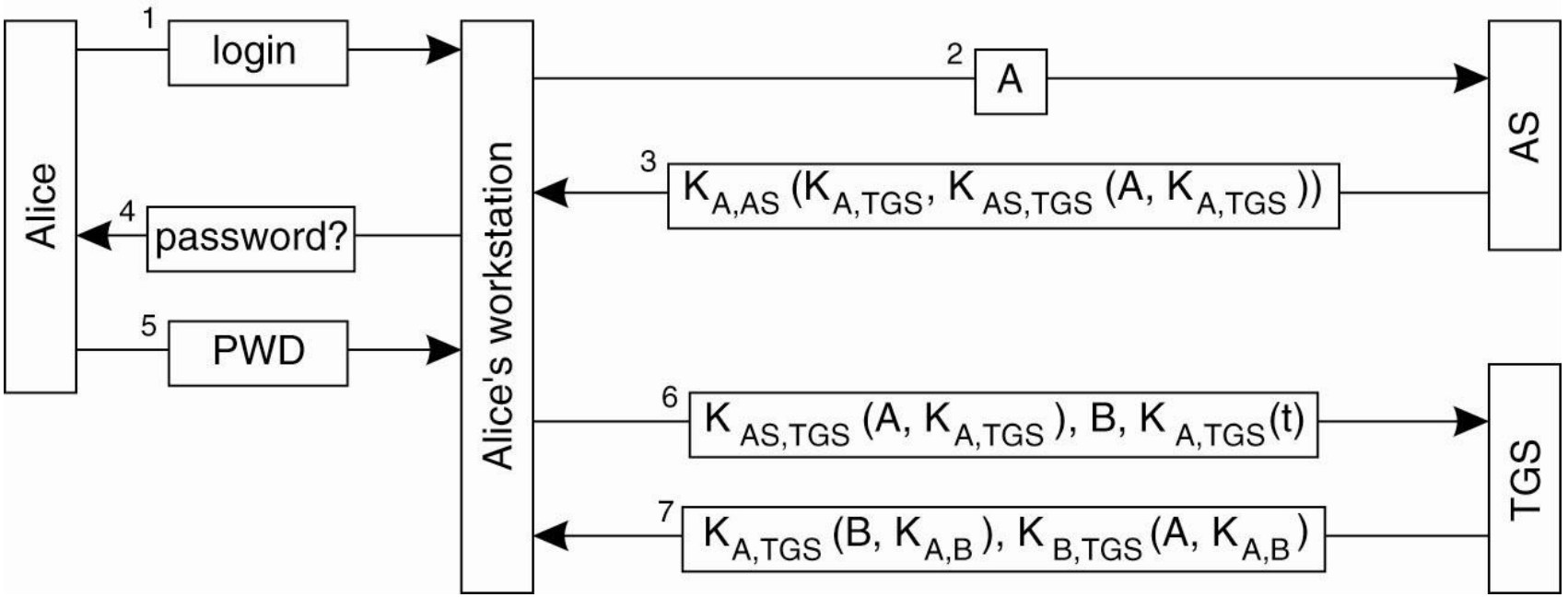


Figure 9-23. Authentication in Kerberos.

Example: Kerberos (2)

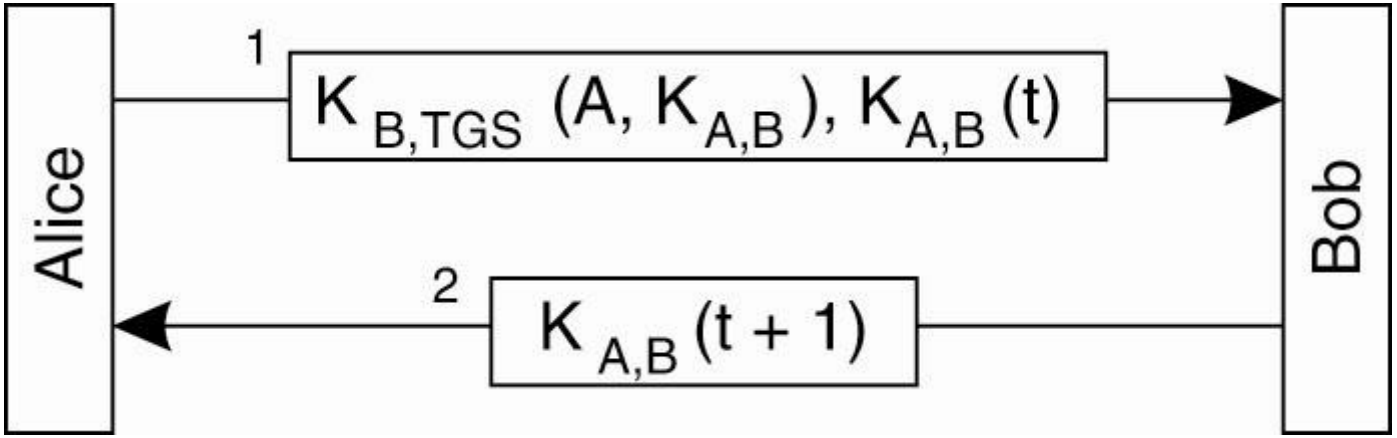


Figure 9-24. Setting up a secure channel in Kerberos.

General Issues in Access Control

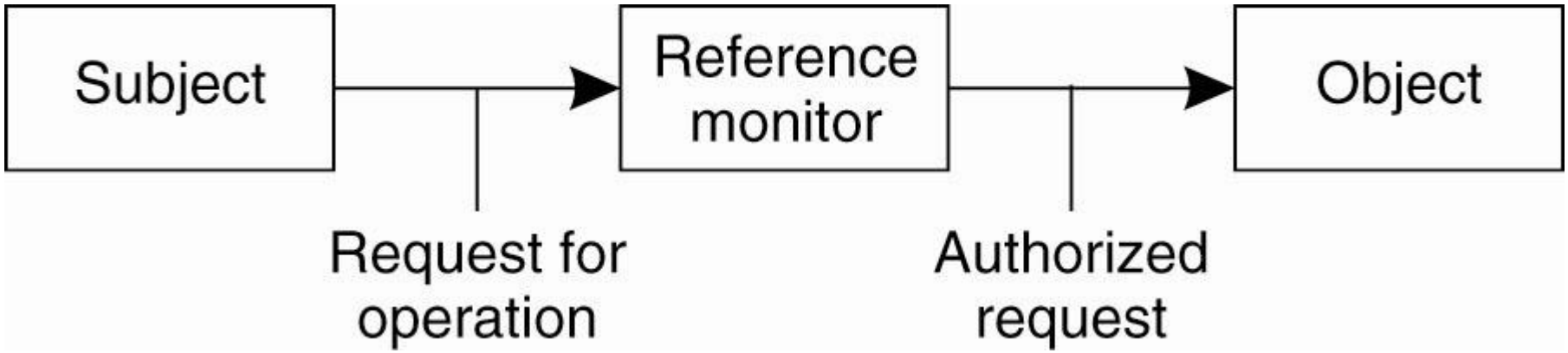


Figure 9-25. General model of controlling access to objects.

Access Control Matrix (1)

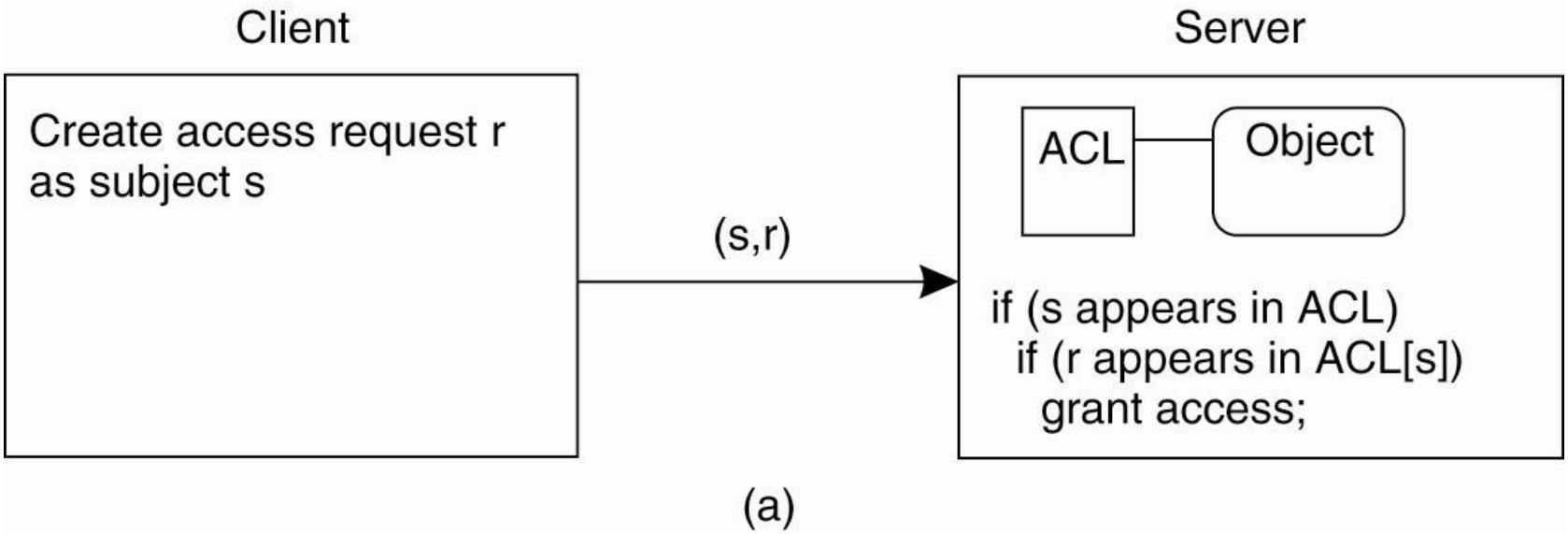


Figure 9-26. Comparison between ACLs and capabilities for protecting objects. (a) Using an ACL.

Access Control Matrix (2)

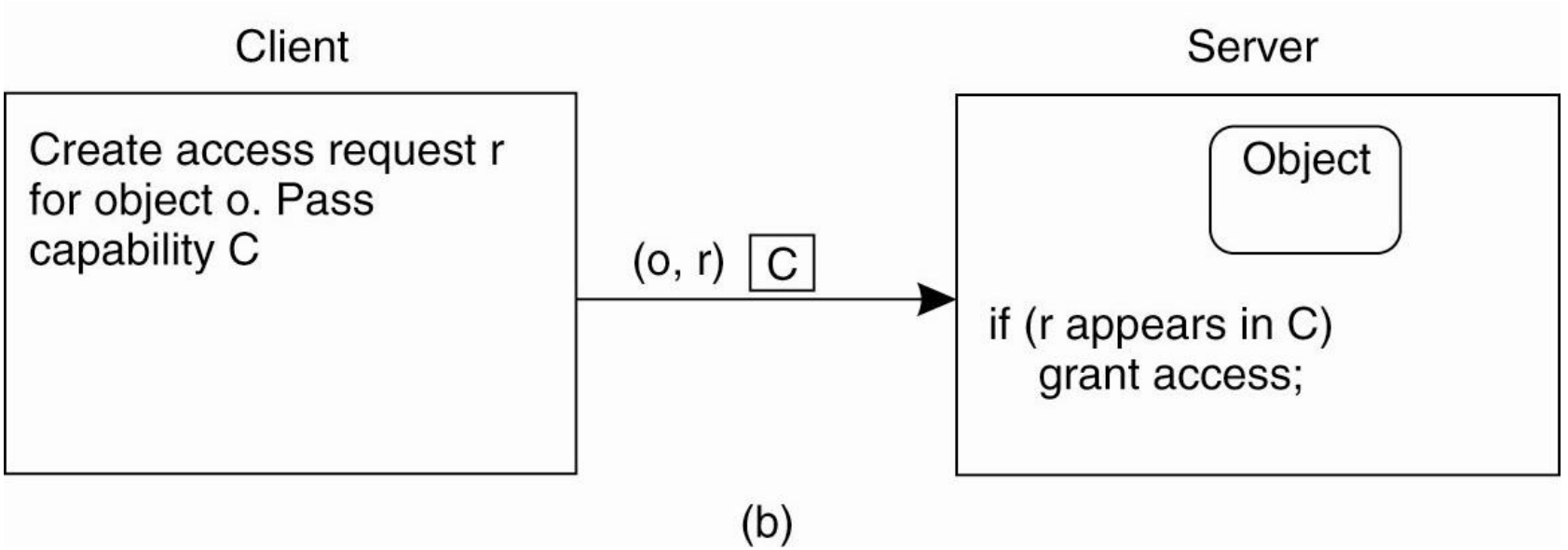


Figure 9-26. Comparison between ACLs and capabilities for protecting objects. (b) Using capabilities.

Protection Domains

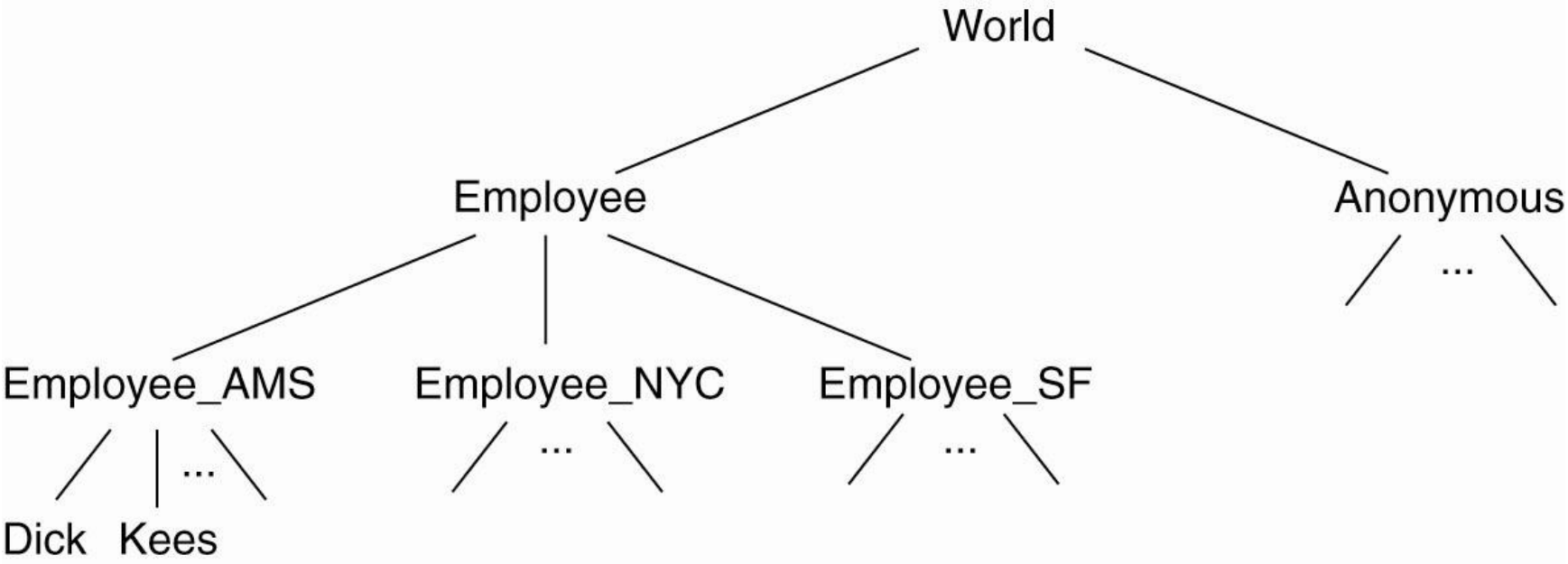


Figure 9-27. The hierarchical organization of protection domains as groups of users.

Firewalls

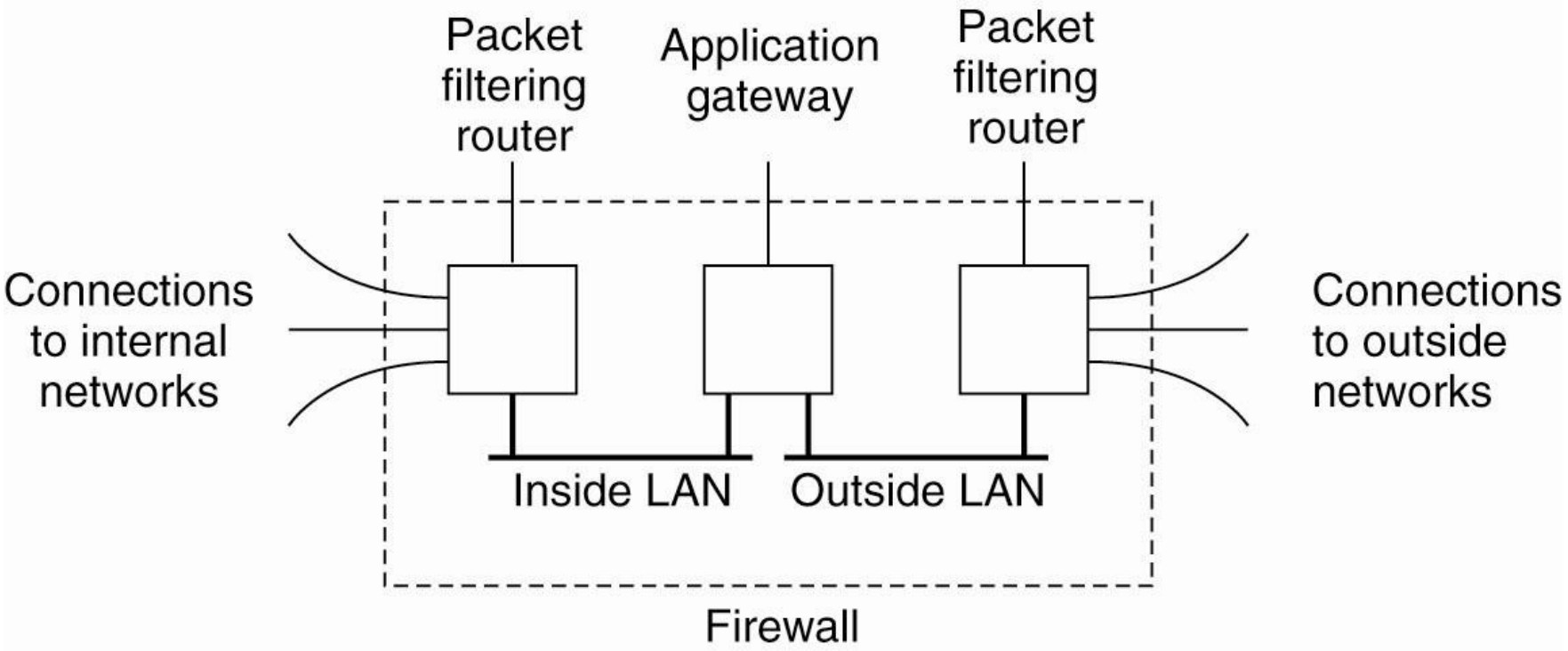


Figure 9-28. A common implementation of a firewall.