

## Security

Chapter 8

---

---

---

---

---

---

---

---

## Types of Threats

- Interception
- Interruption
- Modification
- Fabrication

---

---

---

---

---

---

---

---

## Security Mechanisms

- Encryption
- Authentication
- Authorization
- Auditing

---

---

---

---

---

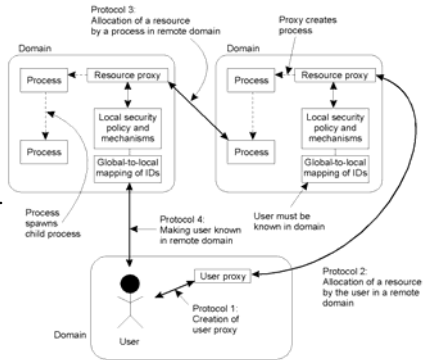
---

---

---

## Example: Globus Security Architecture

Diagram of Globus security architecture.




---

---

---

---

---

---

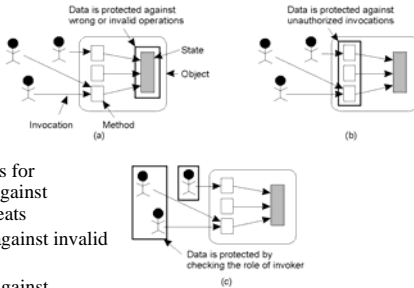
---

---

---

---

## Focus of Control



Three approaches for protection against security threats

- Protection against invalid operations
- Protection against unauthorized invocations
- Protection against unauthorized users

---

---

---

---

---

---

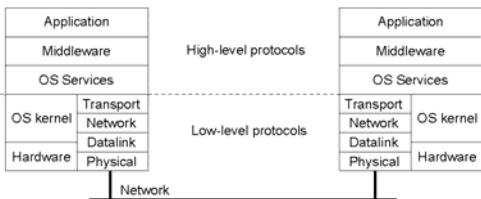
---

---

---

---

## Layering of Security Mechanisms (1)



The logical organization of a distributed system into several layers.

---

---

---

---

---

---

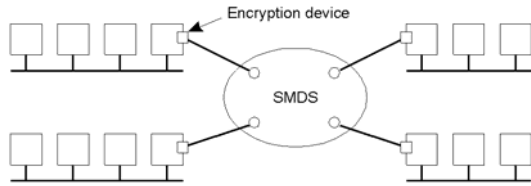
---

---

---

---

## Layering of Security Mechanisms (2)



Several sites connected through a wide-area backbone service.

---

---

---

---

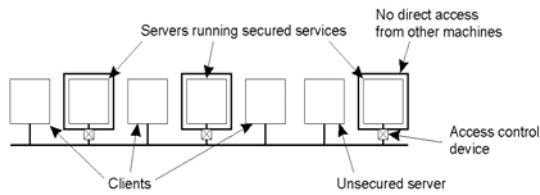
---

---

---

---

## Distribution of Security Mechanisms



The principle of RISSC as applied to secure distributed systems.

---

---

---

---

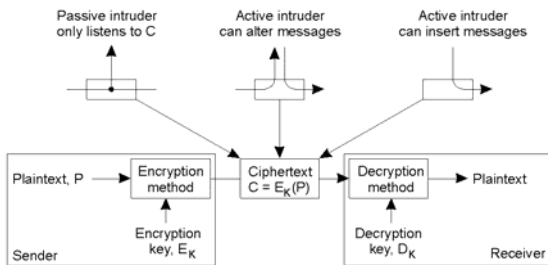
---

---

---

---

## Cryptography (1)



Intruders and eavesdroppers in communication.

---

---

---

---

---

---

---

---

## Cryptography (2)

Notation	Description
$K_{A,B}$	Secret key shared by A and B
$K_A^+$	Public key of A
$K_A^-$	Private key of A

Notation used in this chapter.

---

---

---

---

---

---

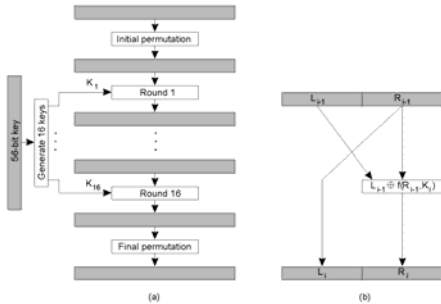
---

---

---

---

## Symmetric Cryptosystems: DES (1)



- a) The principle of DES
- b) Outline of one encryption round

---

---

---

---

---

---

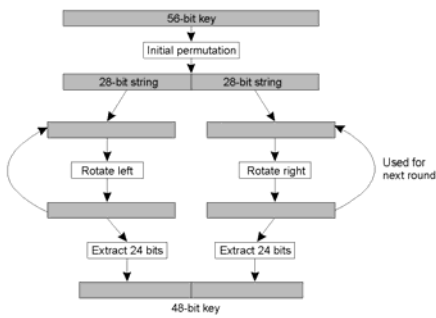
---

---

---

---

## Symmetric Cryptosystems: DES (2)



Details of per-round key generation in DES.

---

---

---

---

---

---

---

---

---

---

## Public-Key Cryptosystems: RSA

Generating the private and public key requires four steps:

1. Choose two very large prime numbers,  $p$  and  $q$
2. Compute  $n = p \times q$  and  $z = (p - 1) \times (q - 1)$
3. Choose a number  $d$  that is relatively prime to  $z$
4. Compute the number  $e$  such that  $e \times d = 1 \pmod{z}$

---

---

---

---

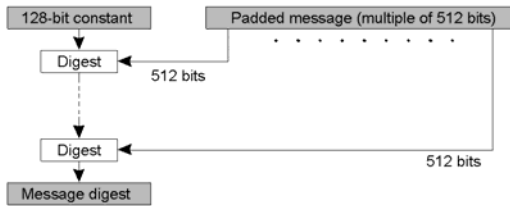
---

---

---

---

## Hash Functions : MD5 (1)



The structure of MD5

---

---

---

---

---

---

---

---

## Hash Functions : MD5 (2)

Iterations 1-8	Iterations 9-16
$p \leftarrow (p + F(q, r, s) + b_0 + C_1) \ll 7$	$p \leftarrow (p + F(q, r, s) + b_8 + C_9) \ll 7$
$s \leftarrow (s + F(p, q, r) + b_1 + C_2) \ll 12$	$s \leftarrow (s + F(p, q, r) + b_9 + C_{10}) \ll 12$
$r \leftarrow (r + F(s, p, q) + b_2 + C_3) \ll 17$	$r \leftarrow (r + F(s, p, q) + b_{10} + C_{11}) \ll 17$
$q \leftarrow (q + F(r, s, p) + b_3 + C_4) \ll 22$	$q \leftarrow (q + F(r, s, p) + b_{11} + C_{12}) \ll 22$
$p \leftarrow (p + F(q, r, s) + b_4 + C_5) \ll 7$	$p \leftarrow (p + F(q, r, s) + b_{12} + C_{13}) \ll 7$
$s \leftarrow (s + F(p, q, r) + b_5 + C_6) \ll 12$	$s \leftarrow (s + F(p, q, r) + b_{13} + C_{14}) \ll 12$
$r \leftarrow (r + F(s, p, q) + b_6 + C_7) \ll 17$	$r \leftarrow (r + F(s, p, q) + b_{14} + C_{15}) \ll 17$
$q \leftarrow (q + F(r, s, p) + b_7 + C_8) \ll 22$	$q \leftarrow (q + F(r, s, p) + b_{15} + C_{16}) \ll 22$

The 16 iterations during the first round in a phase in MD5.

---

---

---

---

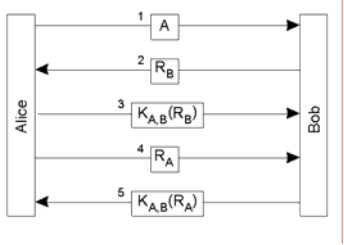
---

---

---

---

### Authentication (1)



Authentication based on a shared secret key.

---

---

---

---

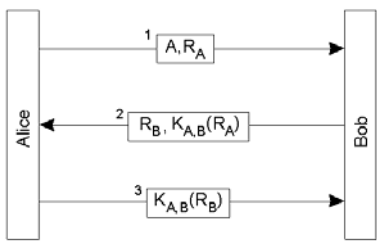
---

---

---

---

### Authentication (2)



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

---

---

---

---

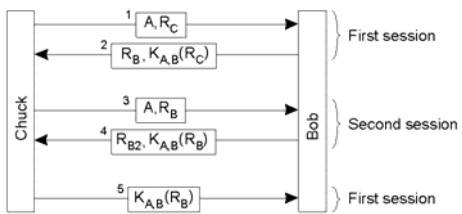
---

---

---

---

### Authentication (3)



The reflection attack.

---

---

---

---

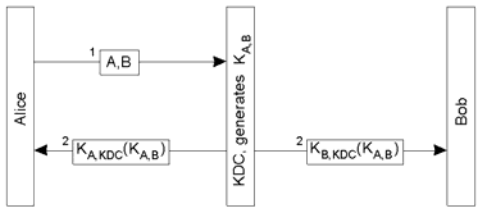
---

---

---

---

### Authentication Using a Key Distribution Center (1)



The principle of using a KDC.

---

---

---

---

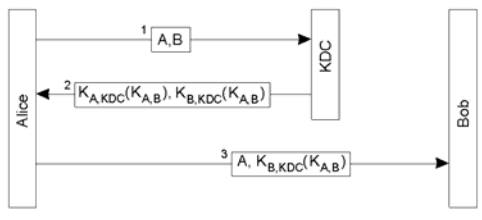
---

---

---

---

### Authentication Using a Key Distribution Center (2)



Using a ticket and letting Alice set up a connection to Bob.

---

---

---

---

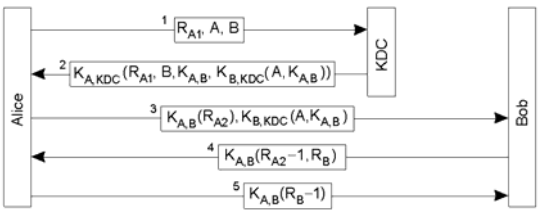
---

---

---

---

### Authentication Using a Key Distribution Center (3)



The Needham-Schroeder authentication protocol.

---

---

---

---

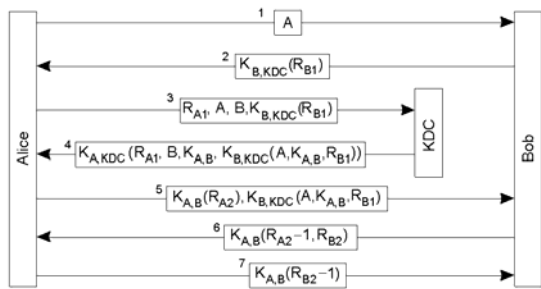
---

---

---

---

### Authentication Using a Key Distribution Center (4)



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

---

---

---

---

---

---

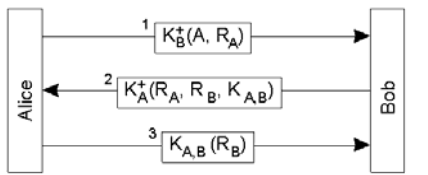
---

---

---

---

### Authentication Using Public-Key Cryptography



Mutual authentication in a public-key cryptosystem.

---

---

---

---

---

---

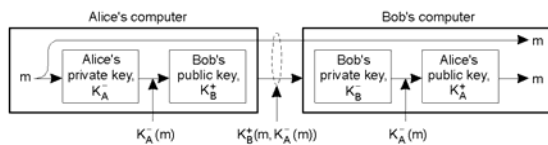
---

---

---

---

### Digital Signatures (1)



Digital signing a message using public-key cryptography.

---

---

---

---

---

---

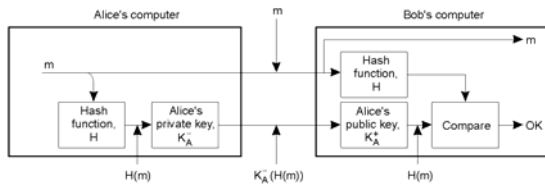
---

---

---

---

## Digital Signatures (2)



Digitally signing a message using a message digest.

---

---

---

---

---

---

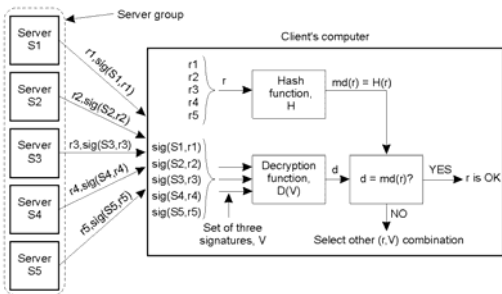
---

---

---

---

## Secure Replicated Services



Sharing a secret signature in a group of replicated servers.

---

---

---

---

---

---

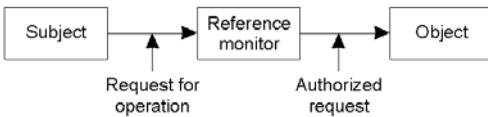
---

---

---

---

## General Issues in Access Control



General model of controlling access to objects.

---

---

---

---

---

---

---

---

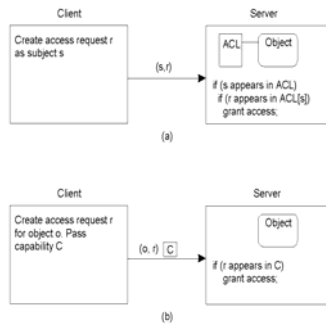
---

---

## Access Control Matrix

Comparison between ACLs and capabilities for protecting objects.

- a) Using an ACL
- b) Using capabilities.




---

---

---

---

---

---

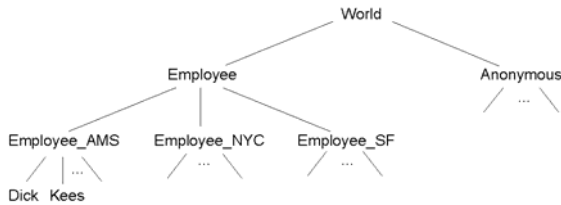
---

---

---

---

## Protection Domains



The hierarchical organization of protection domains as groups of users.

---

---

---

---

---

---

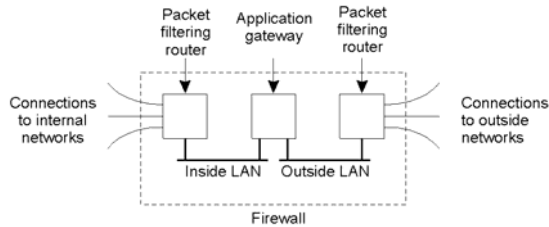
---

---

---

---

## Firewalls



A common implementation of a firewall.

---

---

---

---

---

---

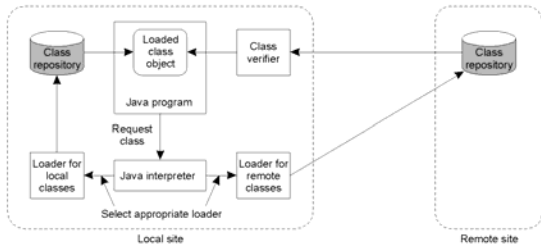
---

---

---

---

### Protecting the Target (1)



The organization of a Java sandbox.

---

---

---

---

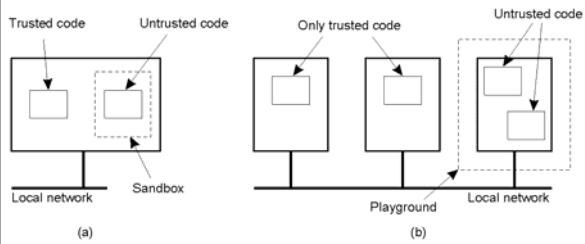
---

---

---

---

### Protecting the Target (2)



- a) A sandbox
- b) A playground

---

---

---

---

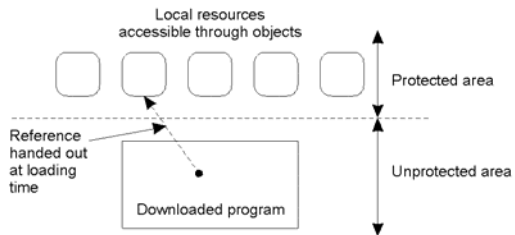
---

---

---

---

### Protecting the Target (3)



The principle of using Java object references as capabilities.

---

---

---

---

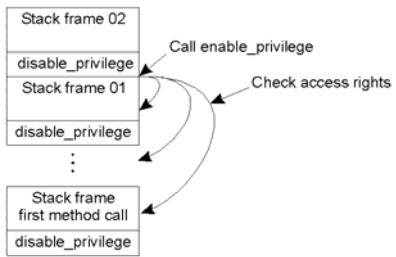
---

---

---

---

## Protecting the Target (4)



The principle of stack introspection.

---

---

---

---

---

---

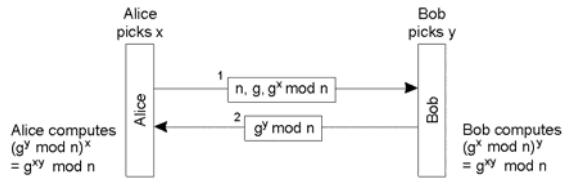
---

---

---

---

## Key Establishment



The principle of Diffie-Hellman key exchange.

---

---

---

---

---

---

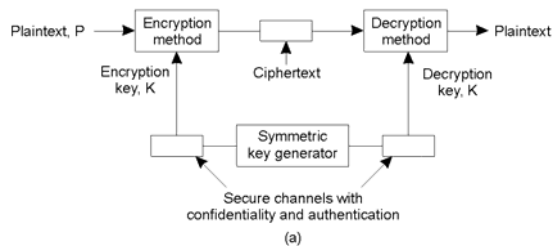
---

---

---

---

## Key Distribution (1)



Secret-key distribution

---

---

---

---

---

---

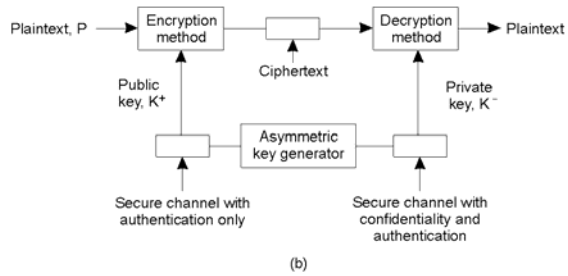
---

---

---

---

## Key Distribution (2)



(b)  
Public-key distribution (see also [menezes.a96]).

---

---

---

---

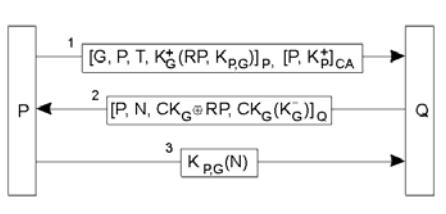
---

---

---

---

## Secure Group Management



Securely admitting a new group member.

---

---

---

---

---

---

---

---

## Capabilities and Attribute Certificates (1)

48 bits	24 bits	8 bits	48 bits
Server port	Object	Rights	Check

A capability in Amoeba.

---

---

---

---

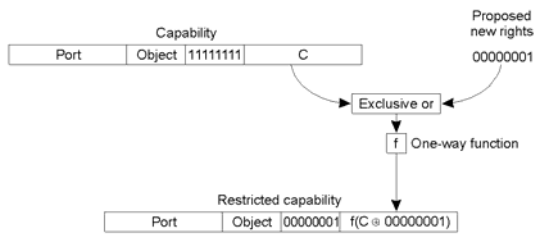
---

---

---

---

## Capabilities and Attribute Certificates (2)



Generation of a restricted capability from an owner capability.

---

---

---

---

---

---

---

---

## Delegation (1)



The general structure of a proxy as used for delegation.

---

---

---

---

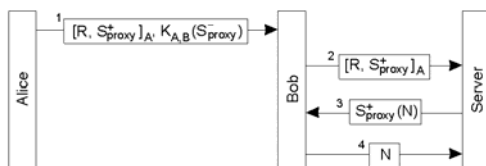
---

---

---

---

## Delegation (2)



Using a proxy to delegate and prove ownership of access rights.

---

---

---

---

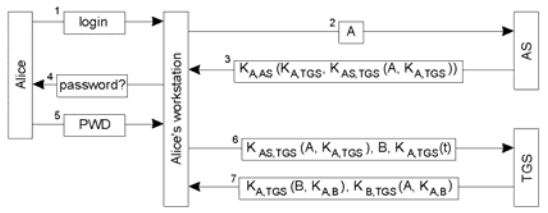
---

---

---

---

### Example: Kerberos (1)



Authentication in Kerberos.

---

---

---

---

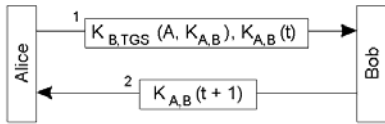
---

---

---

---

### Example: Kerberos (2)



Setting up a secure channel in Kerberos.

---

---

---

---

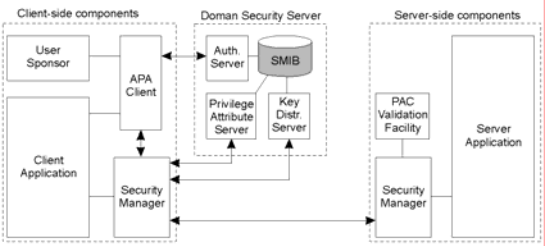
---

---

---

---

### SESAME Components



Overview of components in SESAME.

---

---

---

---

---

---

---

---



## Privacy (1)

	Merchant	Customer	Date	Amount	Item
<b>Merchant</b>	Full	Partial	Full	Full	Full
<b>Customer</b>	Full	Full	Full	Full	Full
<b>Bank</b>	None	None	None	None	None
<b>Observer</b>	Full	Partial	Full	Full	Full

Information hiding in a traditional cash payment.

---

---

---

---

---

---

---

---

---

---

## Privacy (2)

Information					
Party	Merchant	Customer	Date	Amount	Item
<b>Merchant</b>	Full	Full	Full	Full	Full
<b>Customer</b>	Full	Full	Full	Full	Full
<b>Bank</b>	Full	Full	Full	Full	None
<b>Observer</b>	Full	Partial	Full	Full	Full

Information hiding in a traditional credit-card system (see also [camp.lj96a])

---

---

---

---

---

---

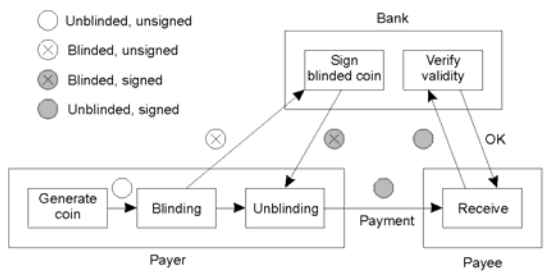
---

---

---

---

## E-cash



The principle of anonymous electronic cash using blind signatures.

---

---

---

---

---

---

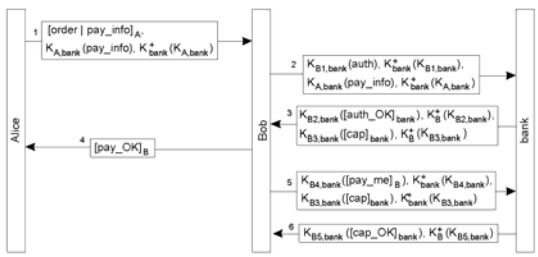
---

---

---

---

## Secure Electronic Transactions (SET)



The different steps in SET.

---



---



---



---



---



---



---