Security: The Goal

Computers are as secure as real world systems, and people believe it.

This is hard because:

- Computers can do a lot of damage fast.
- There are many places for things to go wrong.
- Networks enable
  - Anonymous attacks from anywhere
  - Automated infection
  - Hostile code and hostile hosts
- People don't trust new things.

Real-World Security

It’s about value, locks, and punishment.

- Locks good enough that bad guys don’t break in very often.
- Police and courts good enough that bad guys that do break in get caught and punished often enough.
- Less interference with daily life than value of loss.

Security is expensive—buy only what you need.

Elements of Security

Policy: *Specifying* security
What is it supposed to do?

Mechanism: *Implementing* security
How does it do it?

Assurance: *Correctness* of security
Does it really work?

Dangers

Vandalism or sabotage that	
– damages information	*integrity*
– disrupts service	*availability*
Theft of money	*integrity*
Theft of information	*secrecy*
Loss of privacy	*secrecy*

Vulnerabilities

Bad (buggy or hostile) *programs*

Bad (careless or hostile) *people*
giving instructions to good programs

Bad guy interfering with *communications*

Defensive strategies

Keep everybody out

- Isolation

Keep the bad guy out

- Code signing, firewalls

Let him in, but keep him from doing damage

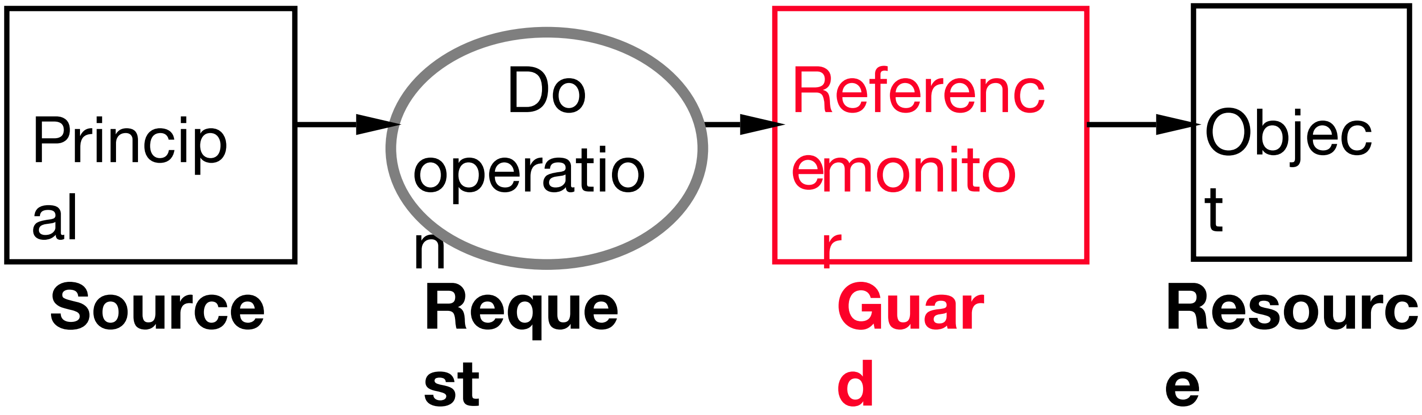
- Sandboxing, access control

Catch him and prosecute him

- Auditing, police

The Access Control Model

Guards control access to valued resources.



Principal → Do operation → Reference monitor → Object

Source **Request** **Guard** **Resource**

Mechanisms—The Gold Standard

Authenticating principals

- Mainly people, but also channels, servers, programs

Authorizing access.

- Usually for groups of principals

Auditing

Assurance

- Trusted computing base

Assurance: Making Security Work

Trusted computing base

- – Limit what has to work to ensure security
  - » Ideally, TCB is small and simple
- – Includes hardware and software
- – Also includes configuration, usually overlooked
  - » What software has privileges
  - » Database of users, passwords, privileges, groups
  - » Network information (trusted hosts, …)
  - » Access controls on system resources
  - » . . .

The unavoidable price of reliability is simplicity.—Hoare

Assurance: Configuration

Users—keep it simple

- At most three levels: self, friends, others
  - » Three places to put objects
- Everything else done automatically with policies

Administrators—keep it simple

- Work by defining policies. Examples:
  - » Each user has a private home folder
  - » Each user belongs to one workgroup with a private folder
  - » System folders contain vendor-approved releases
  - » All executable programs are signed by a trusted party

Today's systems don't support this very well

Assurance: Defense in Depth

Network, with a firewall

Operating system, with sandboxing

- Basic OS (such as NT)
- Higher-level OS (such as Java)

Application that checks authorization directly

All need authentication

Why We Don’t Have “Real” Security

A. People don’t buy it:

- – Danger is small, so it’s OK to buy features instead.
- – Security is expensive.
  - » Configuring security is a lot of work.
  - » Secure systems do less because they’re older.
- − Security is a pain.
  - » It stops you from doing things.
  - » Users have to authenticate themselves.

B. Systems are complicated, so they have bugs.

Standard Operating System Security

Assume secure channel from user (without proof)

Authenticate user by local password

- Assign local user and group SIDs

Access control by ACLs: lists of SIDs and permissions

- Reference monitor is the OS, or any RPC target

Domains: same, but authenticate by RPC to controller

Web servers: same, but *simplified*

- Establish secure channel with SSL
- Authenticate user by local password (or certificate)
- ACL on right to enter, or on user's private state

End-to-End Security

Authenticate secure channels

Work uniformly between organizations

- Microsoft can securely accept Intel’s authentication
- Groups can have members from different organizations

Delegate authority to groups or systems

Audit all security decisions