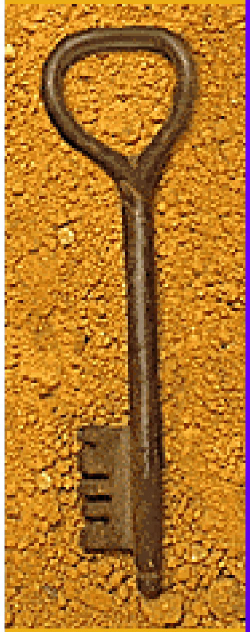
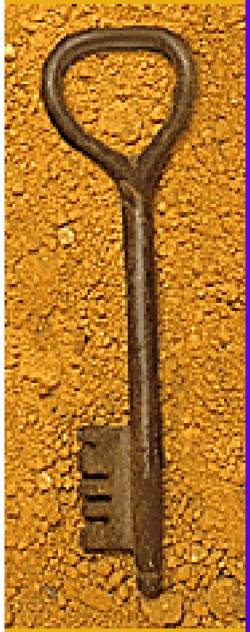
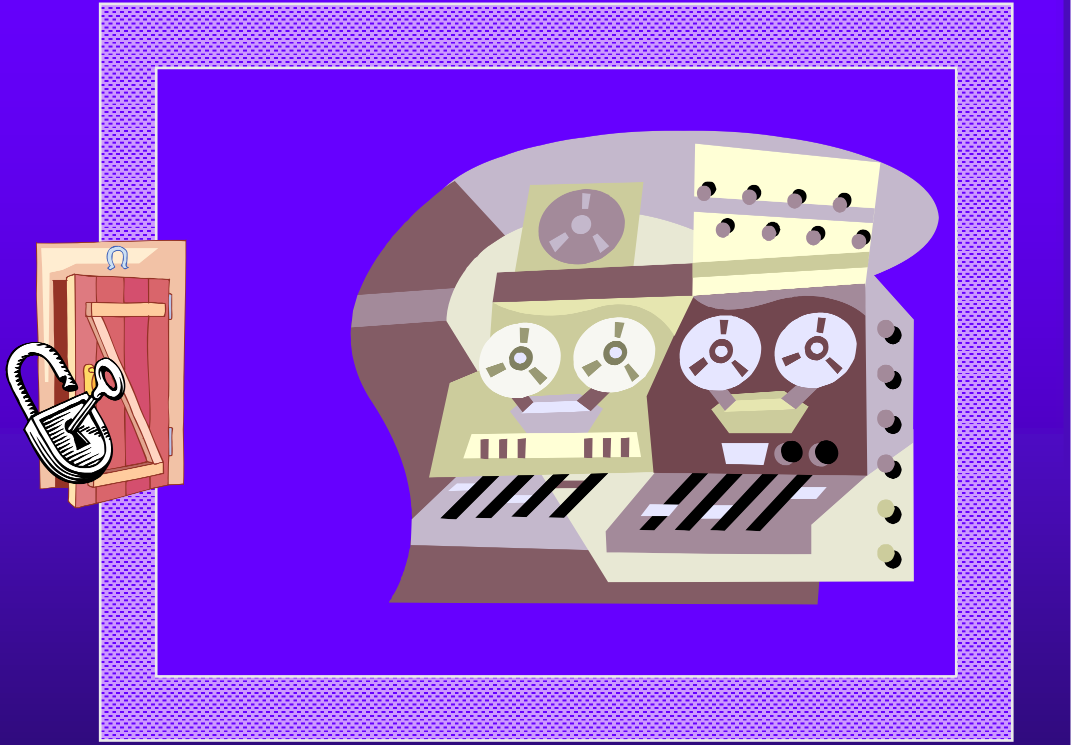


Basic of Information Security

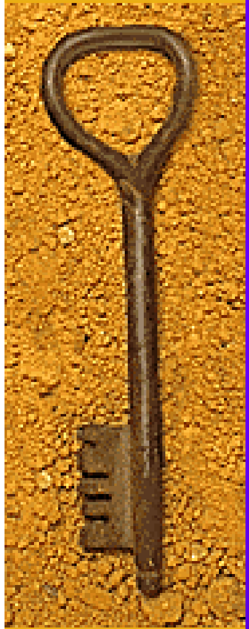


What is Information Security?

- Confidentiality
  - *Is this all?*
  - *Why not?*
- Availability
  - *To whom?*
- Integrity

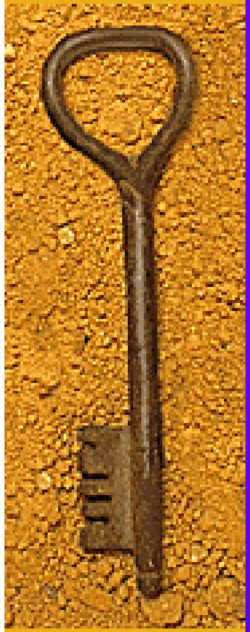


It's about more than network security!



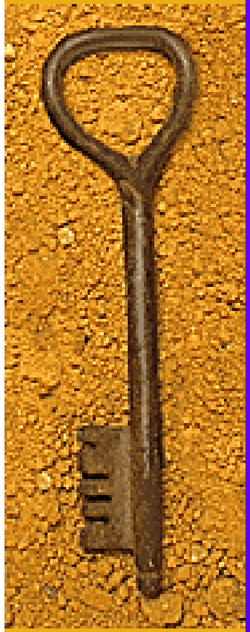
Basic Components

- ♦ Confidentiality: can others see your data?
  - – Keeping data and resources hidden
- ♦ Availability: will the resource be accessible?
  - – Enabling access to data and resources
- ♦ Integrity: can the data be illegally changed?
  - – Data integrity (integrity)
  - – Origin integrity (authentication)



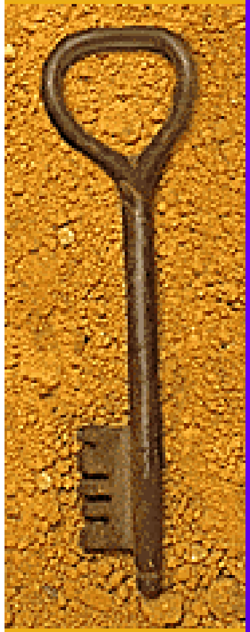
Introduction

- Threats/Attacks
- Policies and mechanisms
- Assurance
- Operational Issues & Human Issues



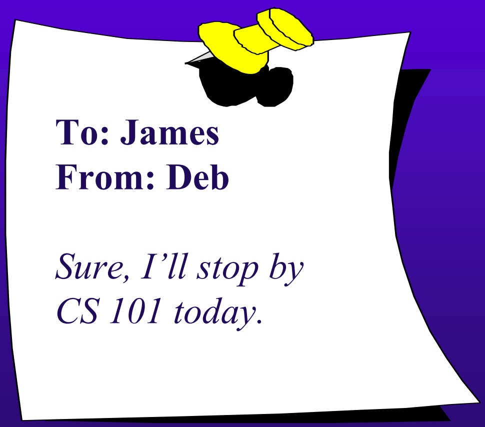
Classes of Threats/Attacks

- Passive Attacks
  - Snooping, Traffic Analysis
- Active Attacks
  - Modification, spoofing, repudiation of origin, denial of receipt
  - Delay (ex. Forge the second-tier server)
  - Replay
  - Denial of service



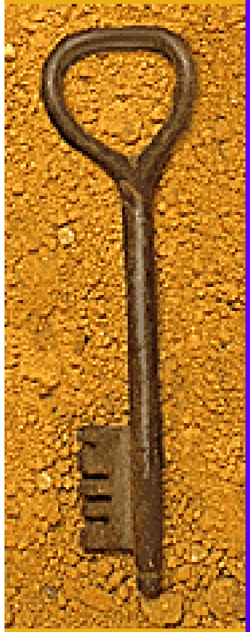
Simplest form of Mail

- ♦ The simplest form of mail is like a postcard:
  - – Sender’s address
  - – Recipient’s address
  - – Data



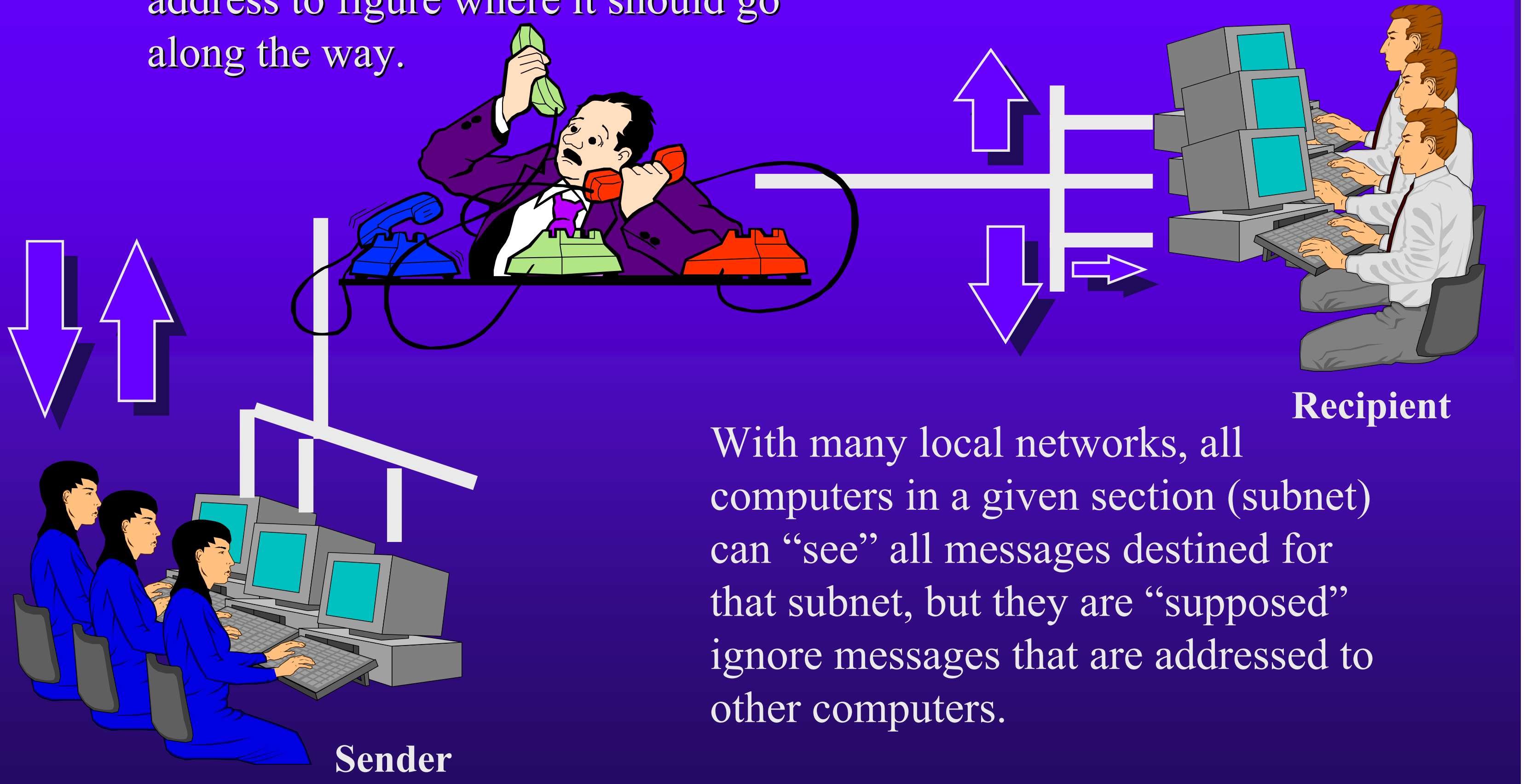
To: James
From: Deb

Sure, I’ll stop by
CS 101 today.

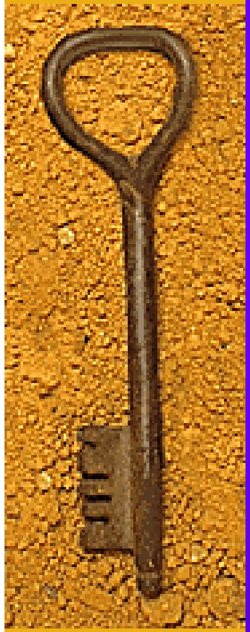


Electronic Communication

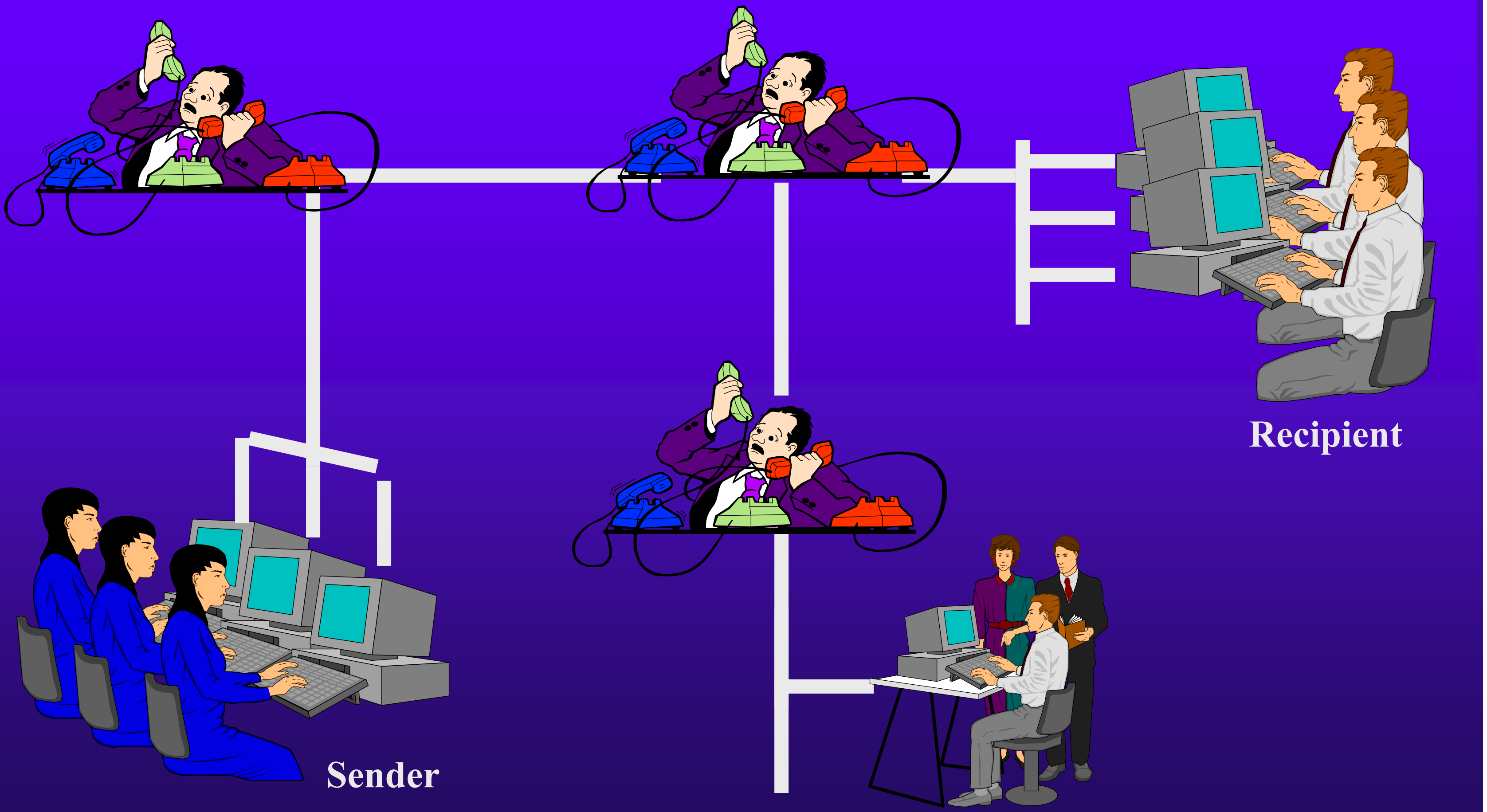
Intermediaries forward messages along the way, using the messages' address to figure where it should go along the way.

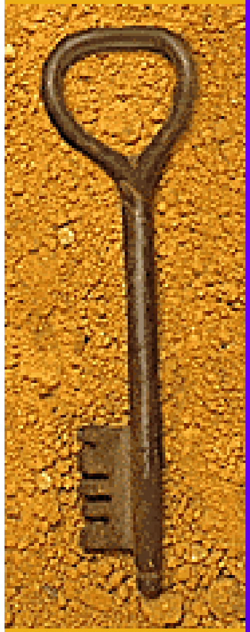


With many local networks, all computers in a given section (subnet) can "see" all messages destined for that subnet, but they are "supposed" ignore messages that are addressed to other computers.

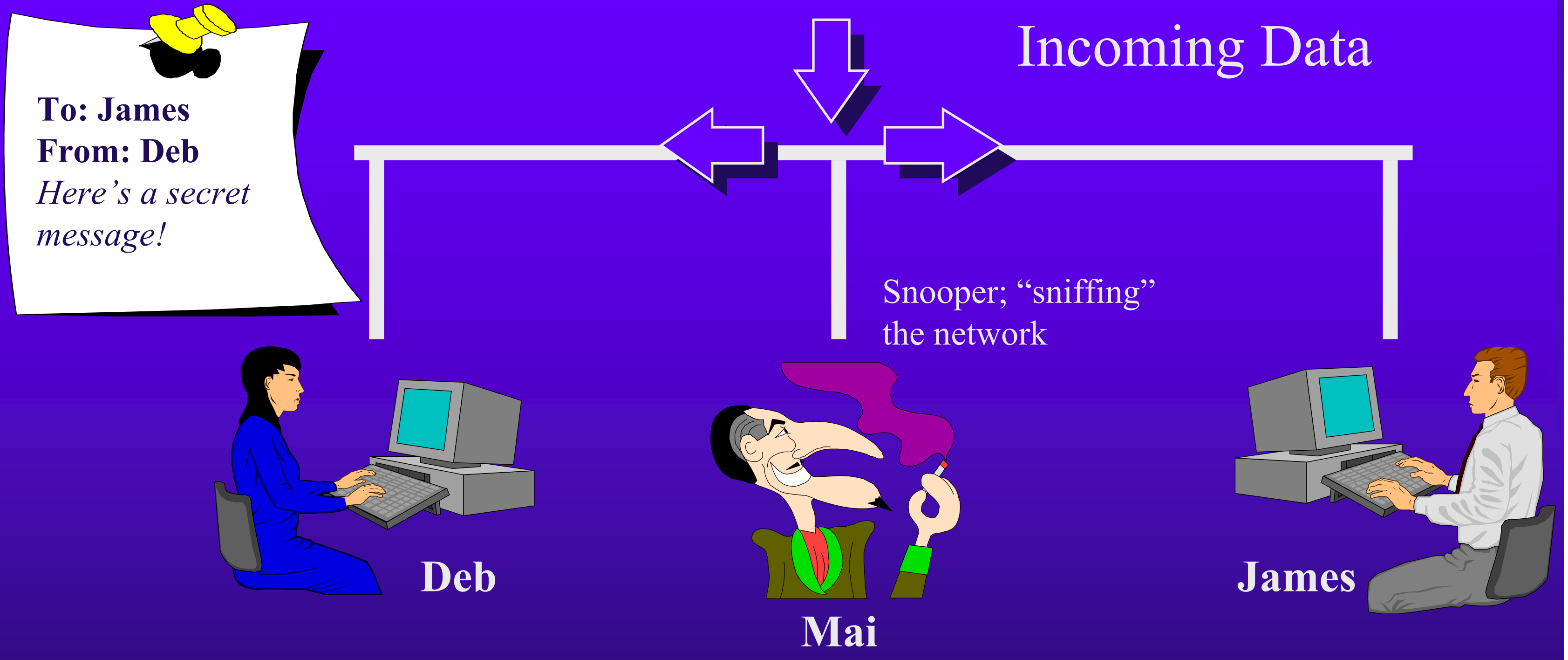


There might be several intermediaries ...





There are lots of security implications ...



To: James
From: Deb
Here's a secret message!

Incoming Data

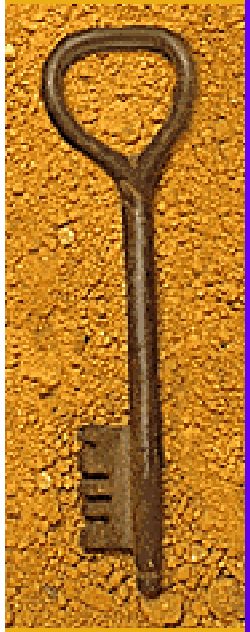
Snooper; “sniffing” the network

Deb

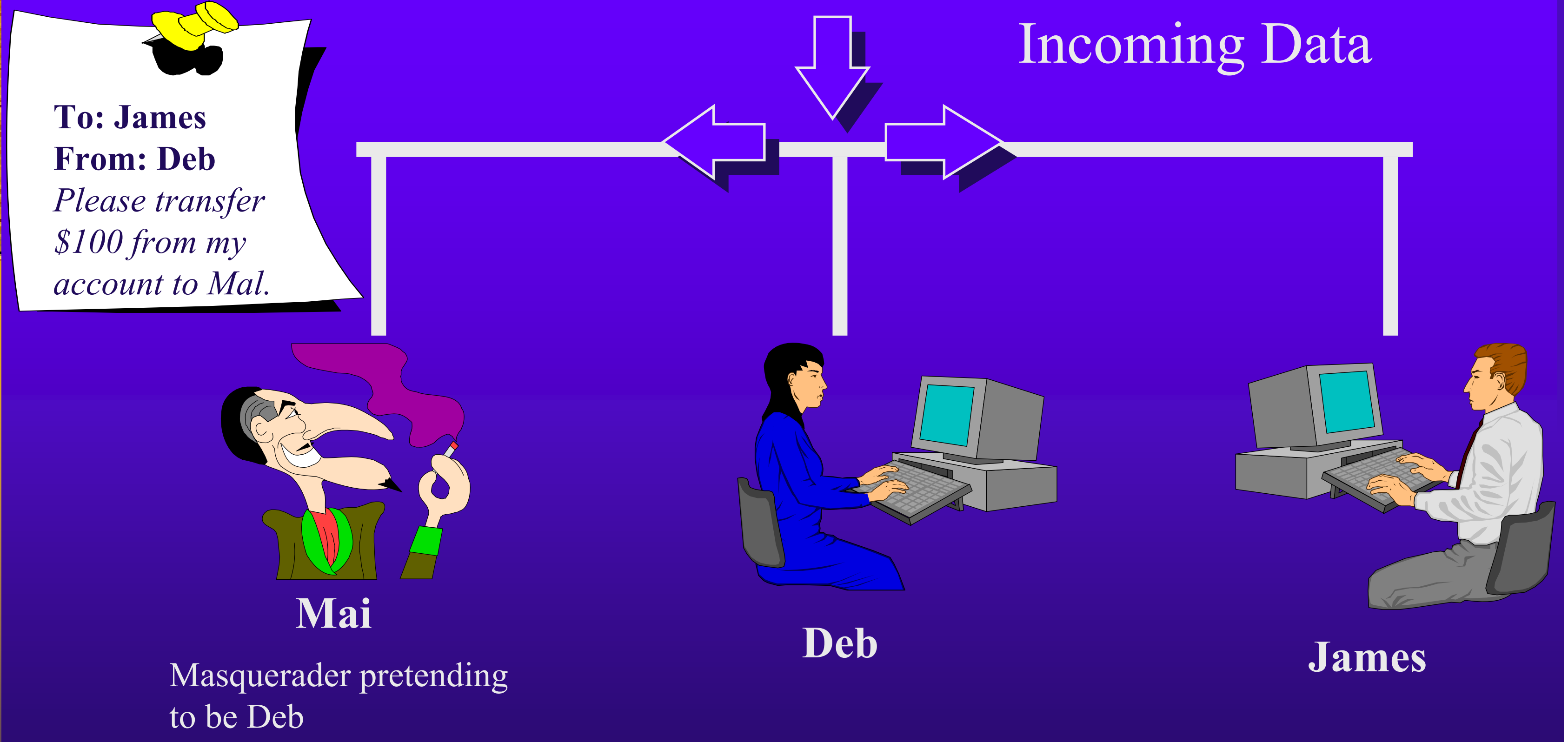
Mai

James

- On the local subnet, computers might read messages not intended for them.



Fake messages can be inserted locally ...



To: James
From: Deb
Please transfer $100 from my account to Mal.

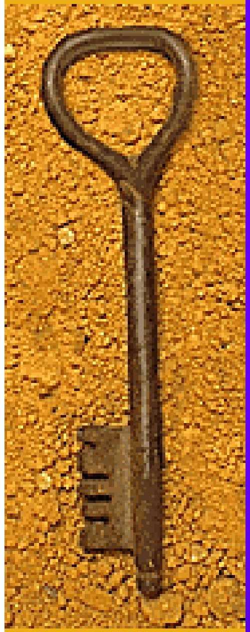
Incoming Data

Mai

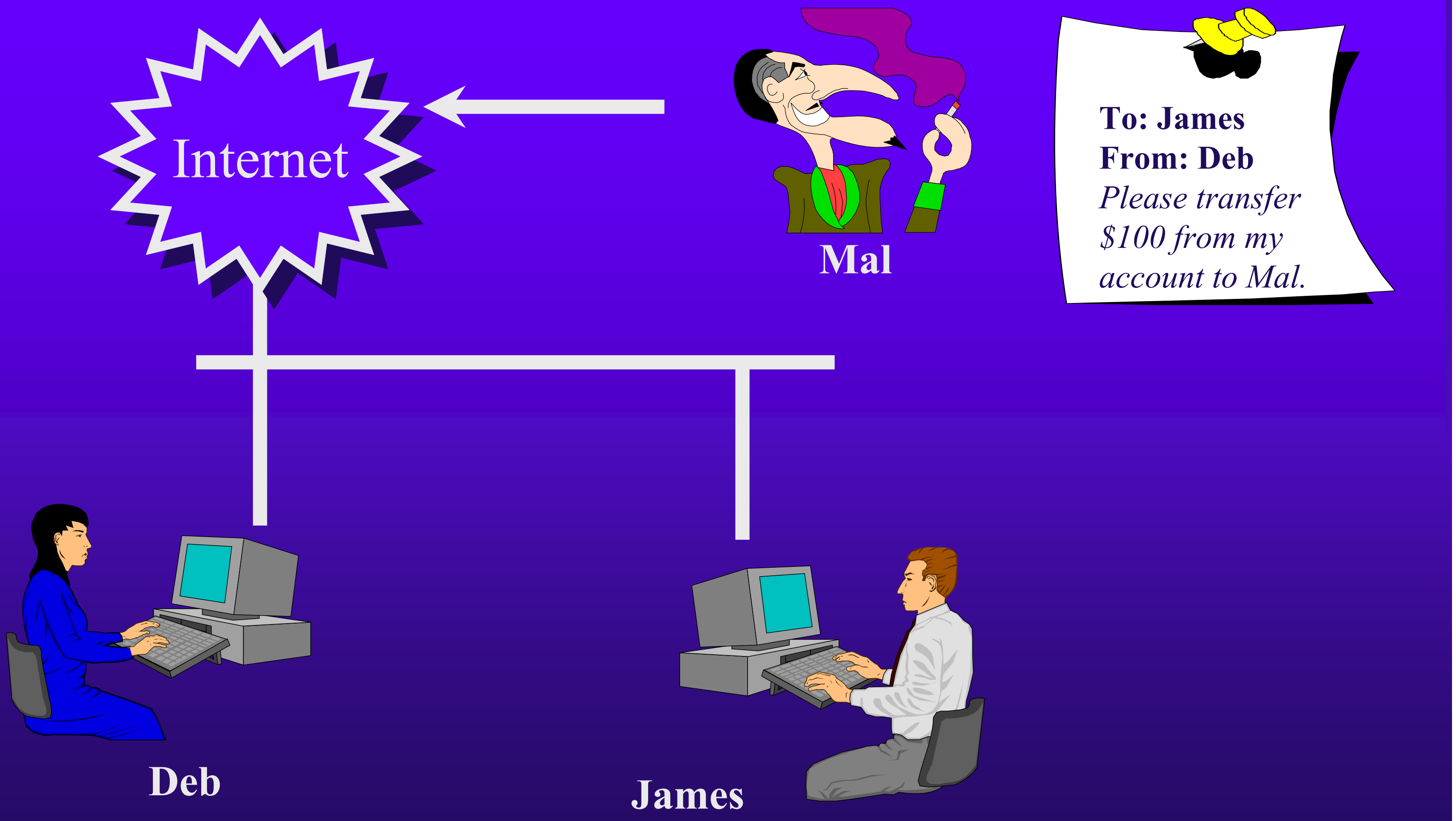
Masquerader pretending to be Deb

Deb

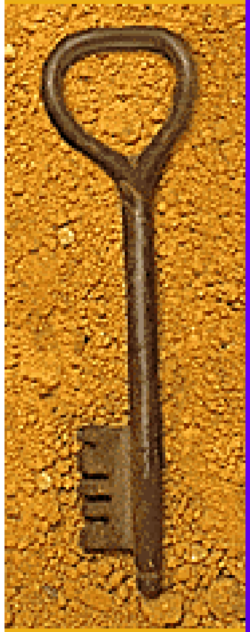
James



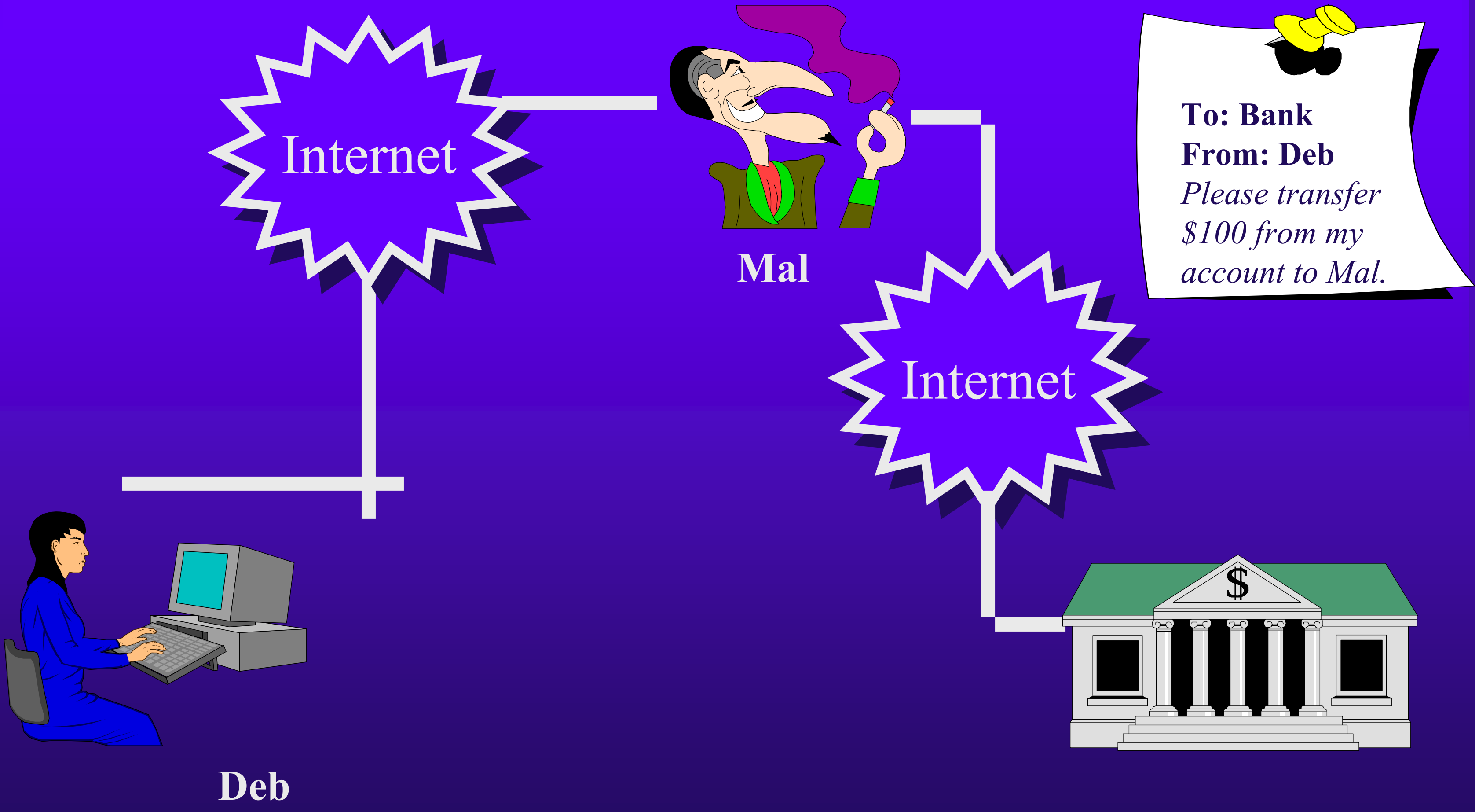
Fake messages can be inserted from outside into the local net ...



To: James
From: Deb
Please transfer
$100 from my
account to Mal.

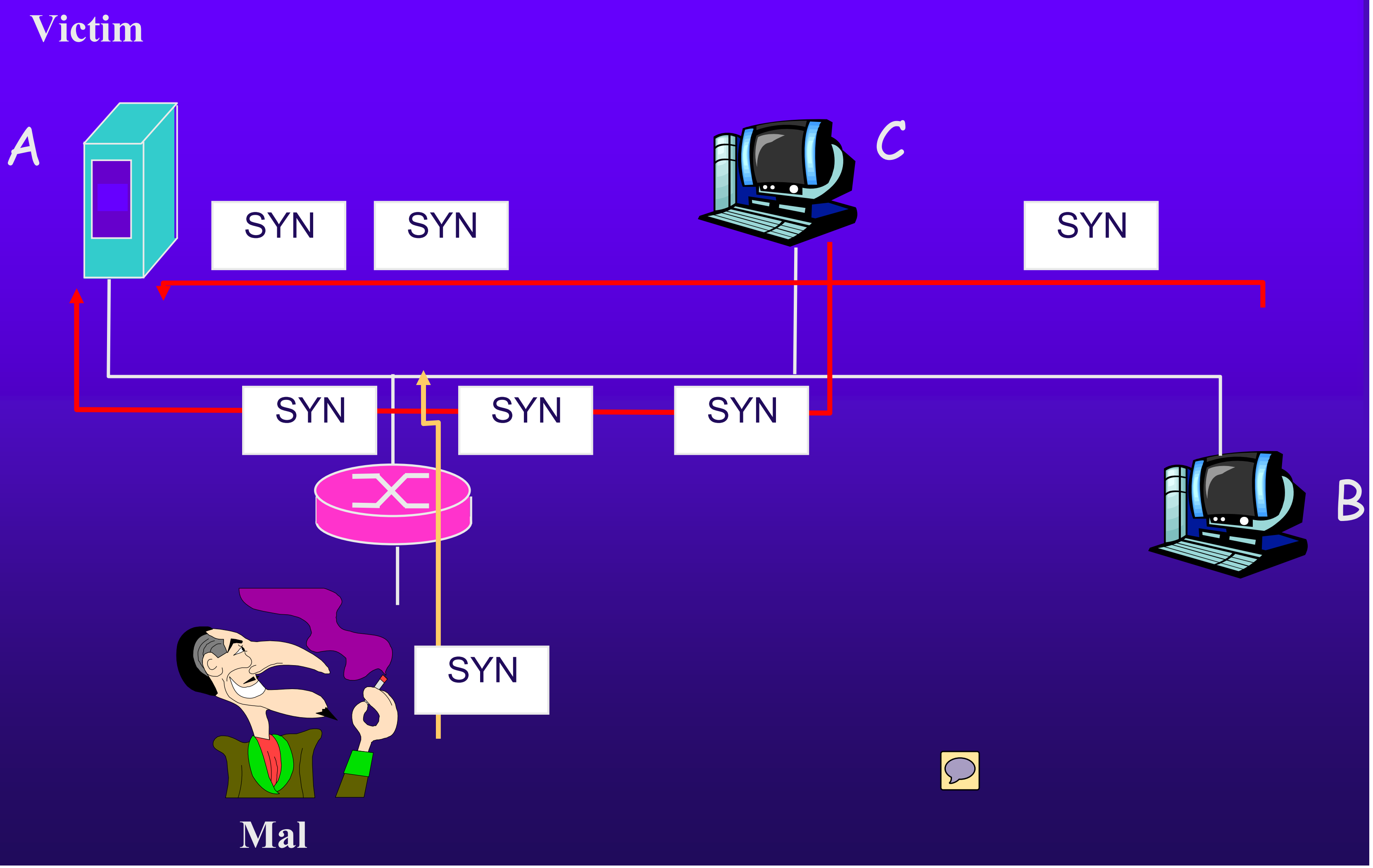


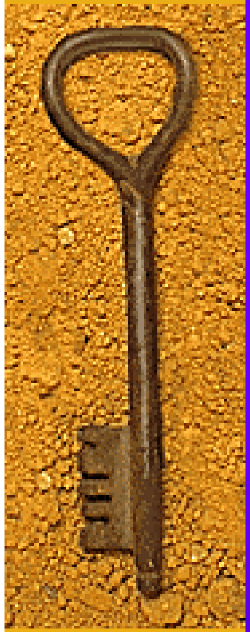
… Or could bypass the local network altogether!



To: Bank
From: Deb
Please transfer $100 from my account to Mal.

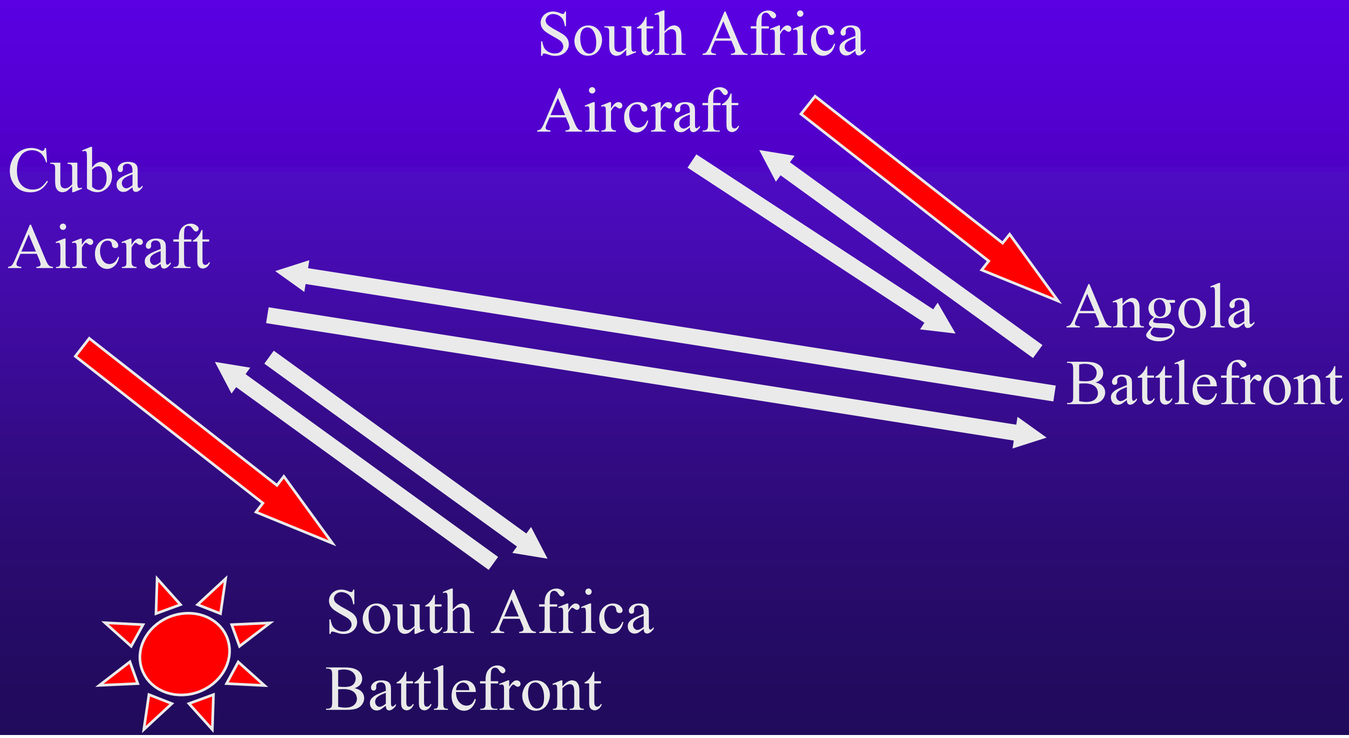
Active Attacks: Denial of Service

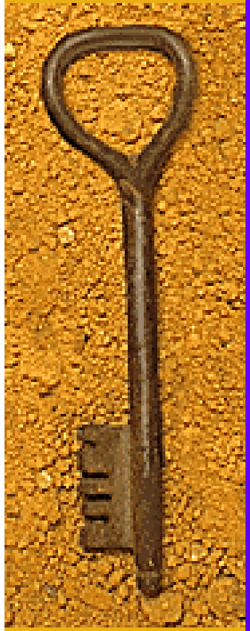




Active Attacks: Replay

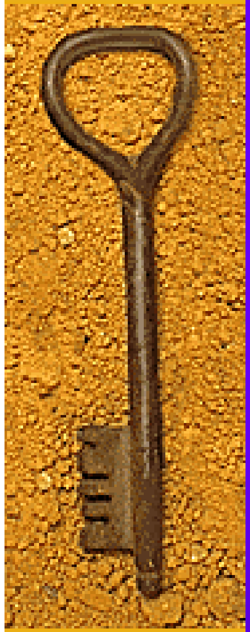
- Time: late in 1980s
- Subject: Cuba vs. South Africa Airforce





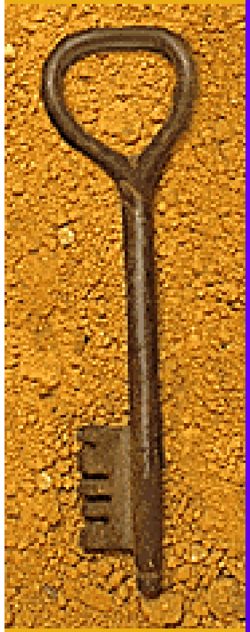
Introduction

- Threats
- Policies and mechanisms
- Assurance
- Operational Issues & Human Issues



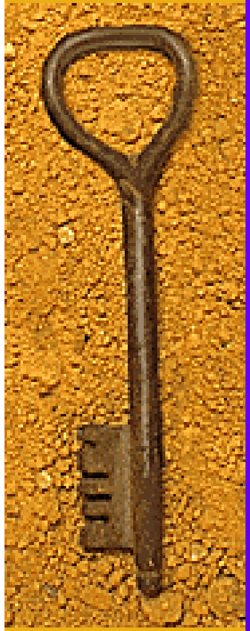
Policies and Mechanisms

- Policy says what is allowed, and what is not allowed
  - This defines "security" for the site/system/*etc*.
  - Policy definition: Informal? Formal? POLICY-LANGUAGE
  - Ex. no internet users can access internal database server
- Mechanisms enforce policies
  - Technical? Procedural?
  - Ex. Firewalls
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities
  - Ex. Student/faculty; partition



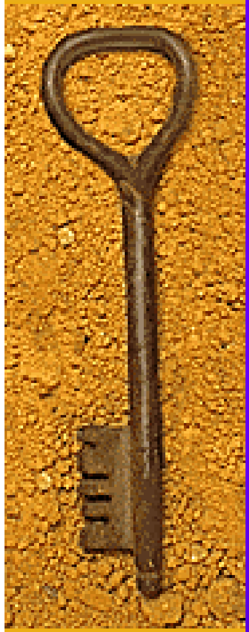
Goals of Security

- ♦ Prevention
  - – Prevent attackers from violating security policy
- ♦ Detection
  - – Detect attackers' violation of security policy
- ♦ Recovery
  - – Attack is stopped, system is fixed, resume operations
  - – (Advanced Version) Continue to function correctly even if attack succeeds



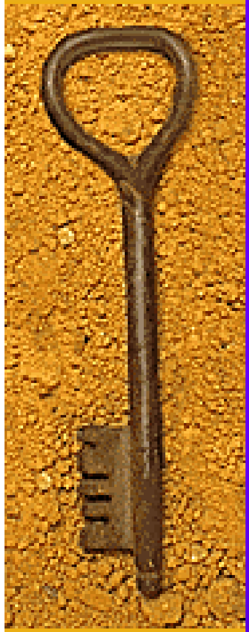
Advanced TOPIC

Intrusion-Tolerant DBMS

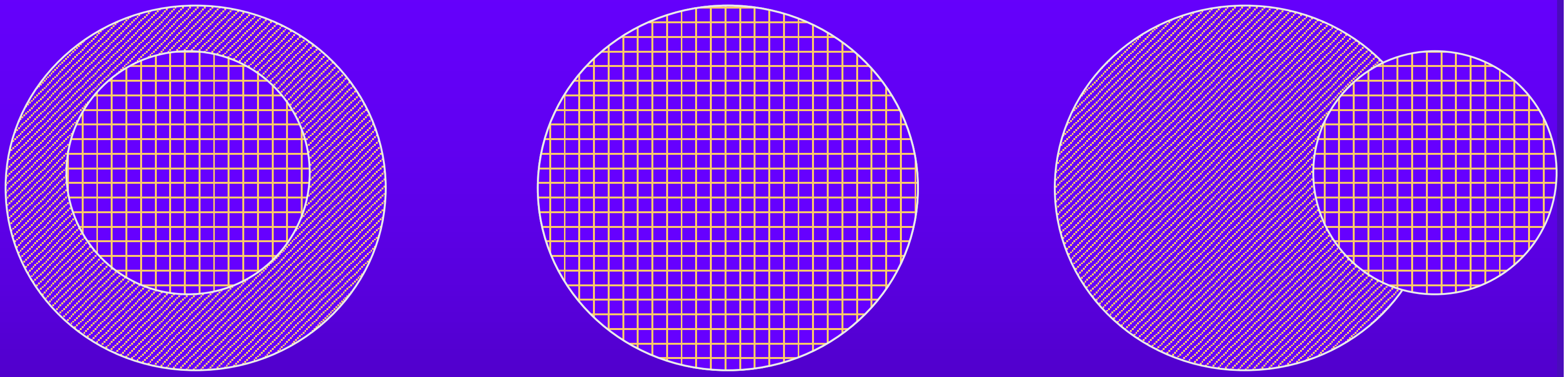


Trust and Assumptions

- Underlie *all* aspects of security
  - Ex. Always need the key to access the room?
- Policies
  - Correctly capture security requirements
  - Unambiguously partition system states
    - Ex. Account Transfer < 10K$, but to himself ?
- Mechanisms
  - Assumed to enforce policy
  - Rely on supporting infrastructure (ex. Ken Thompson's modified C preprocessor) (p. 615)



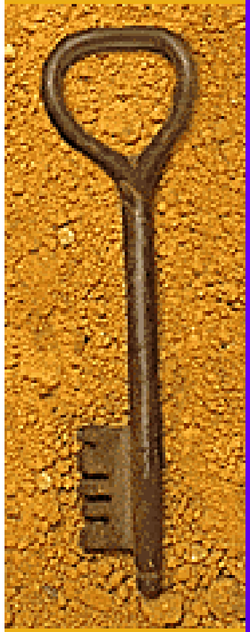
Types of Mechanisms



▦ set of reachable states

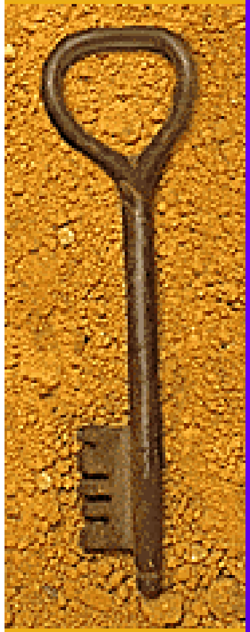
▨ set of secure states

A reachable state is one that the computer can enter. A secure state is a state defined as allowed by the security policy.



Introduction

- Threats
- Policies and mechanisms
- Assurance
- Operational Issues & Human Issues

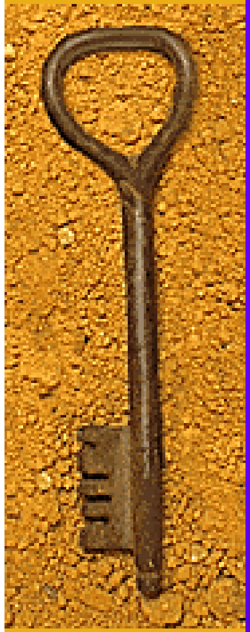


Assurance

Assurance is a measure of how well the system meets its requirements

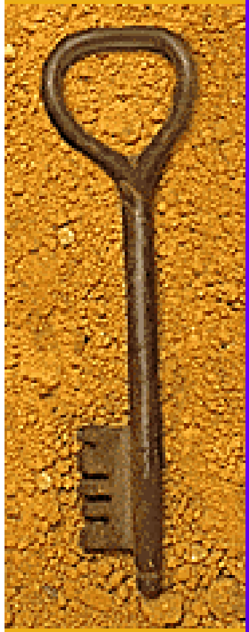
More informally, how much you can trust the system to do what it is supposed to do. It does not say what the system is to do; rather, it only covers how well the system does it.

- Specification
  - The goals of the system are determined
  - It is a statement of functionality, not assurance
  - (ex. Traffic control; no damage from internet)
- Design
  - How system will meet specification
  - (ex. No NIC/Modem, no driver in O.S.)
- Implementation
  - Programs/systems that carry out design
  - Remember the Thompson's modified compiler?



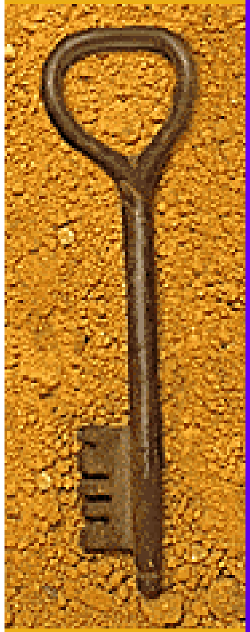
Introduction

- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues & Human Issues



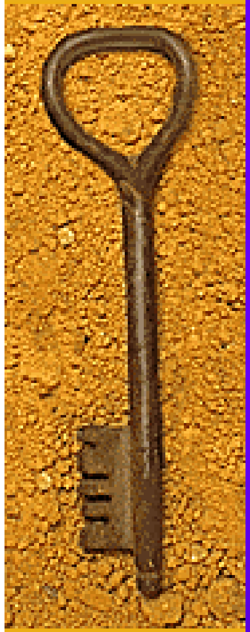
Operational Issues

- ♦ Cost-Benefit Analysis
  - – Is it cheaper to prevent or recover?
- ♦ Risk Analysis
  - – Should we protect something?
  - – How much should we protect this thing?
- ♦ Laws and Customs
  - – Are desired security measures illegal?
    - • Ex1. export control of US government (DES)
    - • Ex2. key-escrow regulation by France, → US
  - – Will people do them?
    - • Ex1. use urine specimens to determine identity?

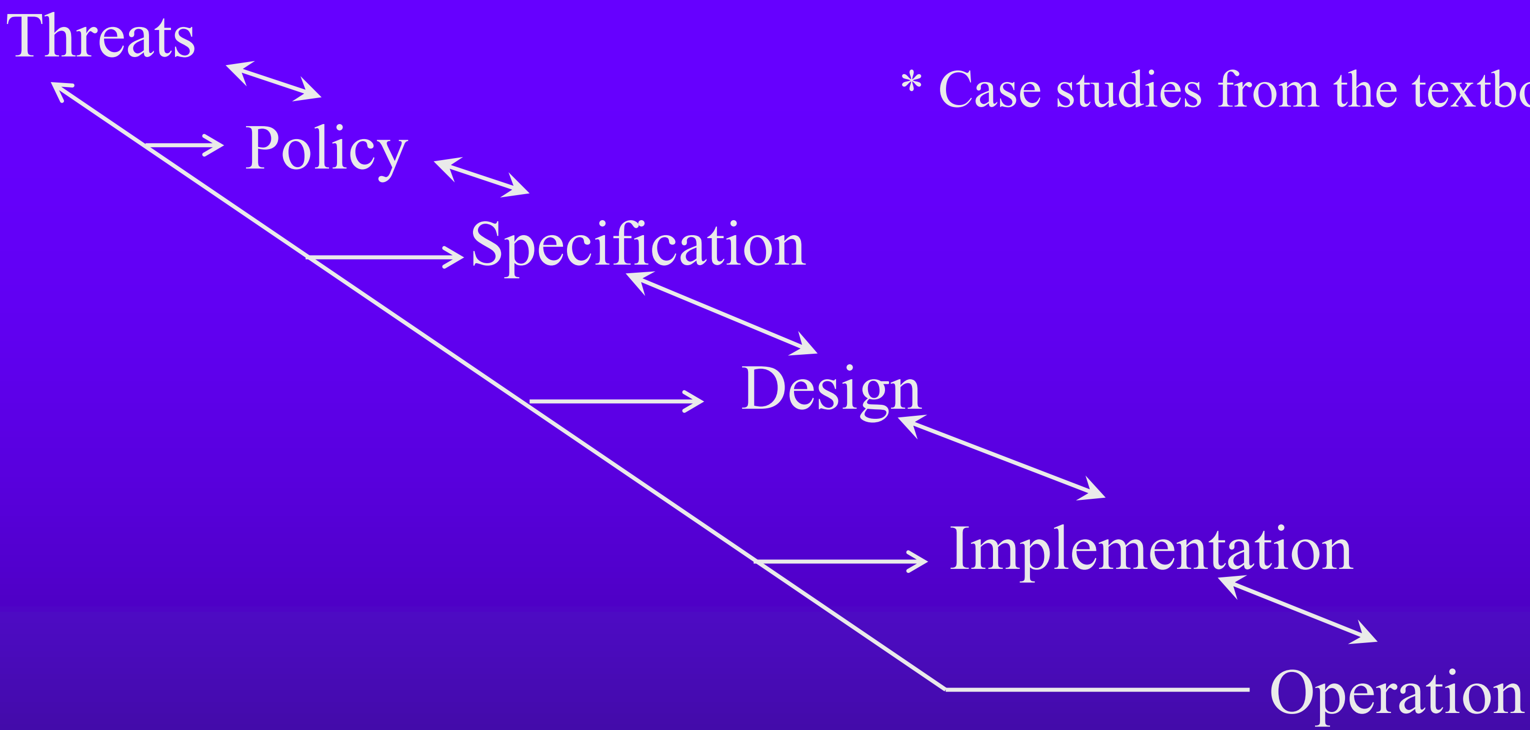


Human Issues

- 30% technical, 70% management
- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
    - *Which do you think is the real threat?*
  - Untrained People, ex. Unverified backup tape
  - Social engineering ex. Night call from executive



Tying the Definitions Together



Threats

Policy

Specification

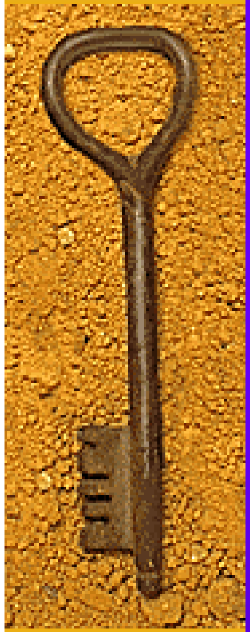
Design

Implementation

Operation

* Case studies from the textbook

- Each step feeds into the earlier steps. In theory, each of these should only affect the one before it, and the one after it.
- In practice, each affects all the ones that come before it.
- Feedback from operation and maintenance is critical, and often overlooked. It allows one to validate the threats and the legitimacy of the policy.



Key Points

- Policy defines security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions
- Importance of assurance
- The human factor