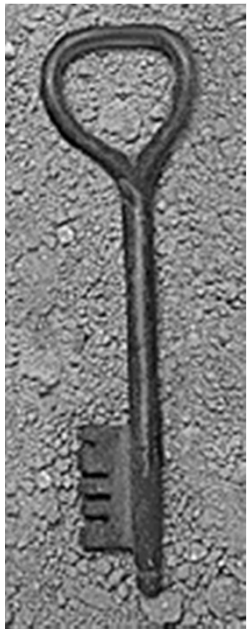
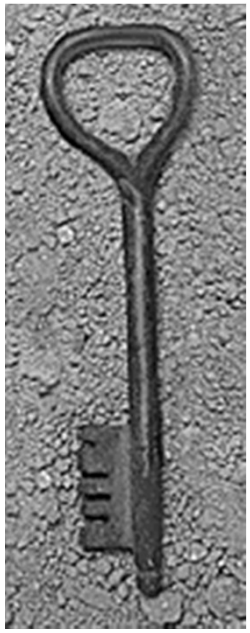


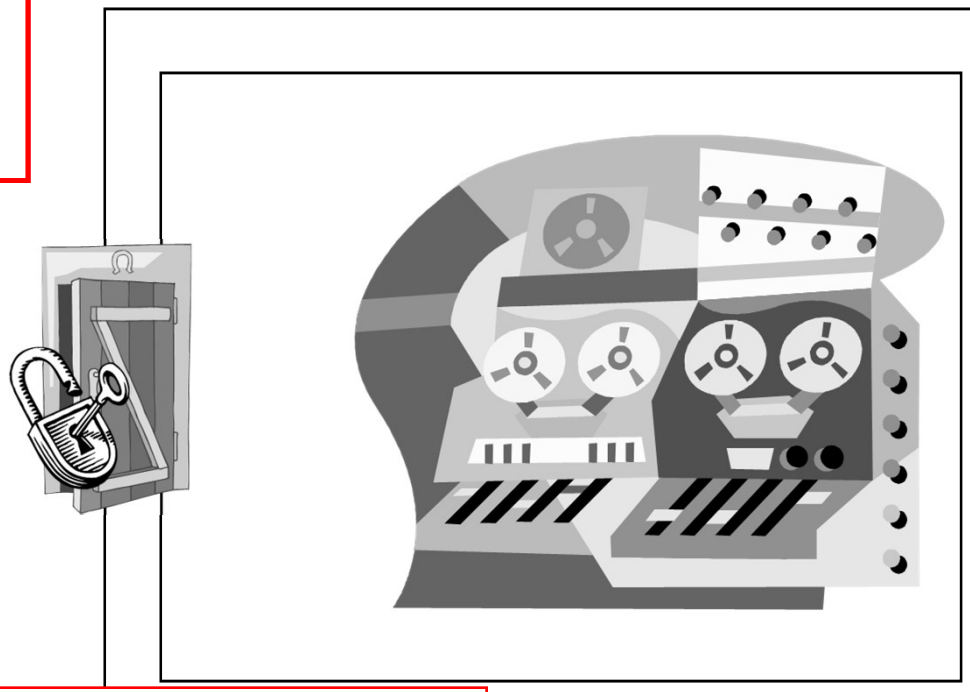
Basic of Information Security



What is Information Security?

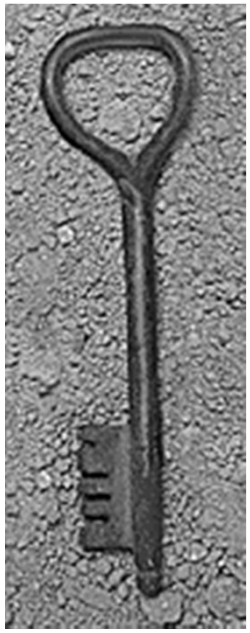
会考到

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



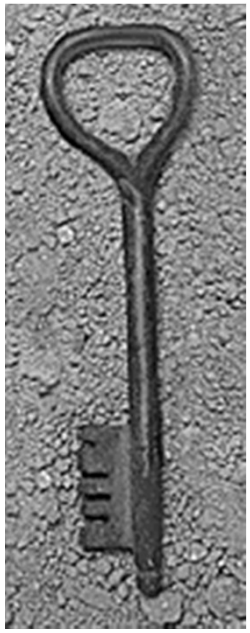
内容完整性，
信息来源完整性，（政府网站，cc98网站，同一信息，在不同网站，效果不一样，比如胖子发射一颗导弹）

ork security!



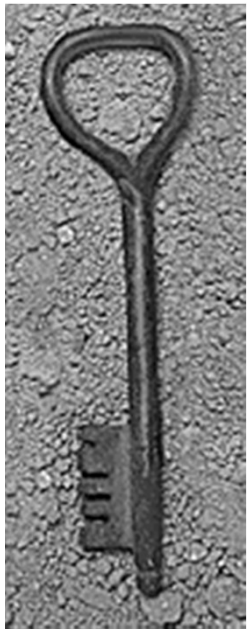
Basic Components

- 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)



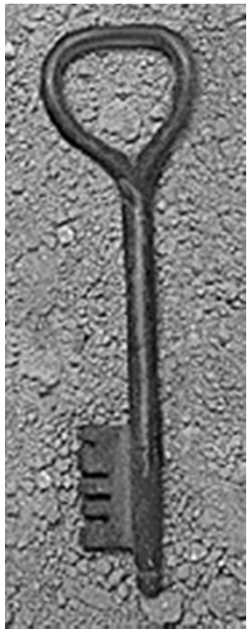
Introduction

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



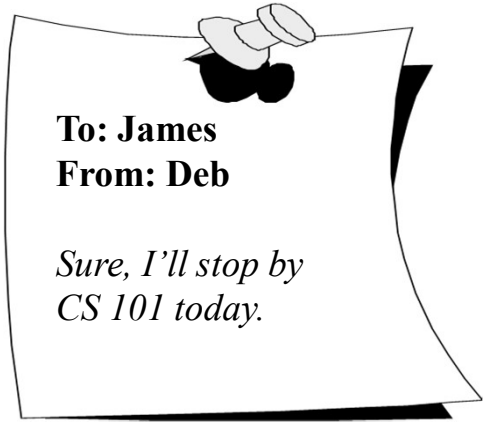
Classes of Threats/Attacks

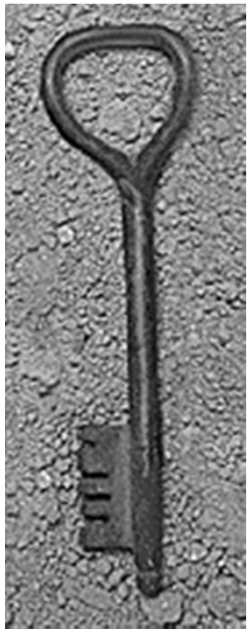
- Passive Attacks 被动攻击：窃听，流量监听。
  - Snooping, Traffic Analysis
- Active Attacks 主动攻击：信息修改，modification。
  - Modification, spoofing, repudiation of origin, denial of receipt 欺骗攻击
    淘宝收件
  - Delay (ex. Forge the second-tier server)
    信息的延迟攻击，备用服务器防御弱，但是主系统防御好，用肉鸡让主系统慢很多，启用备用系统。
  - Replay
  - Denial of service



Simplest form of Mail

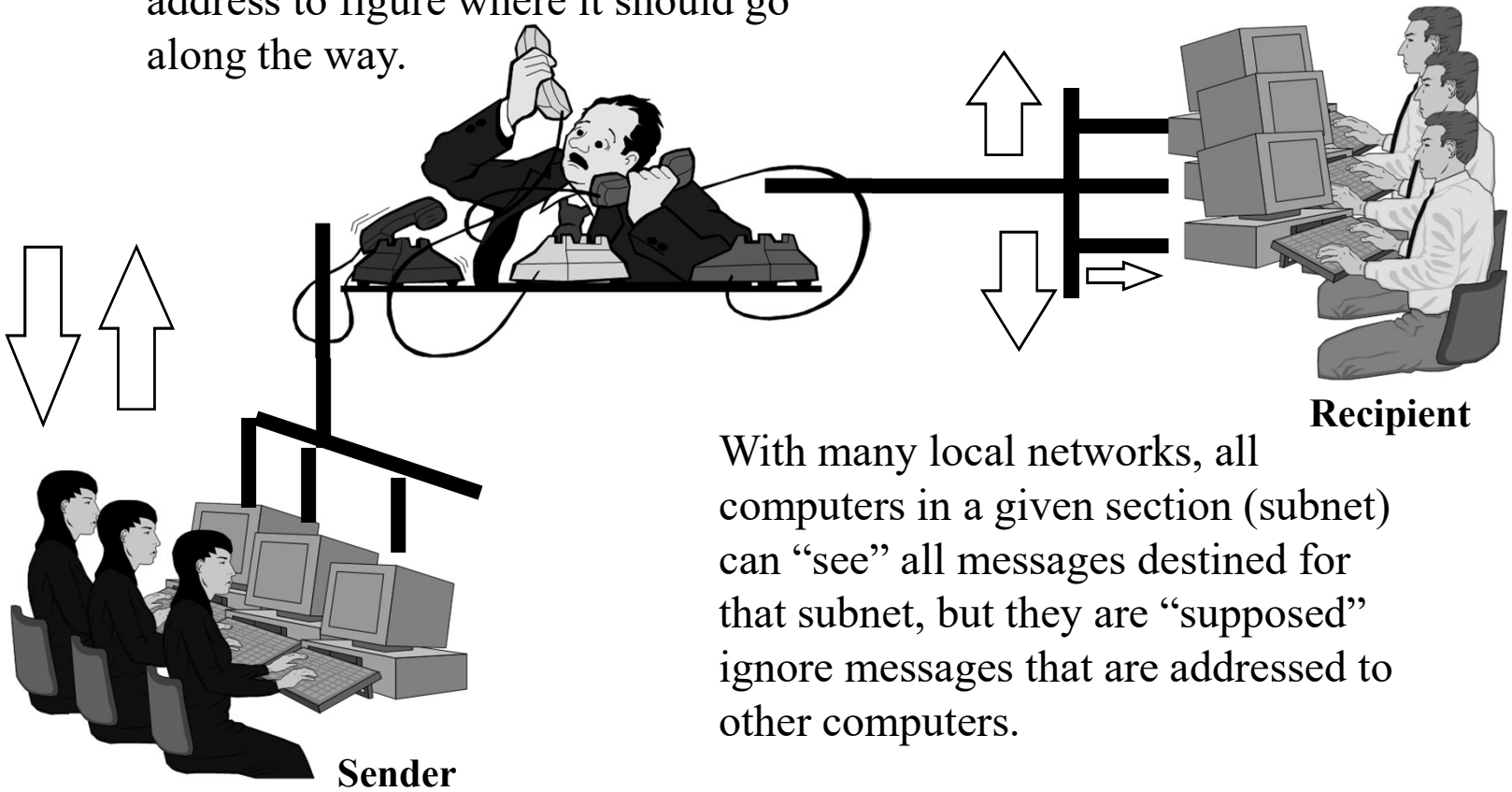
- The simplest form of mail is like a postcard:
  - Sender's address
  - Recipient's address
  - Data



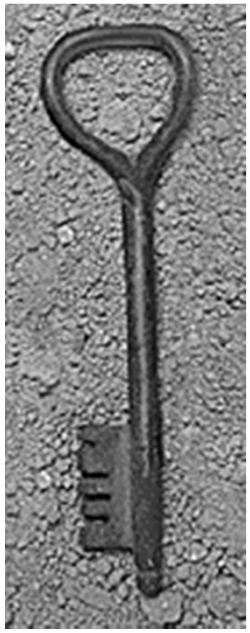


Electronic Communication

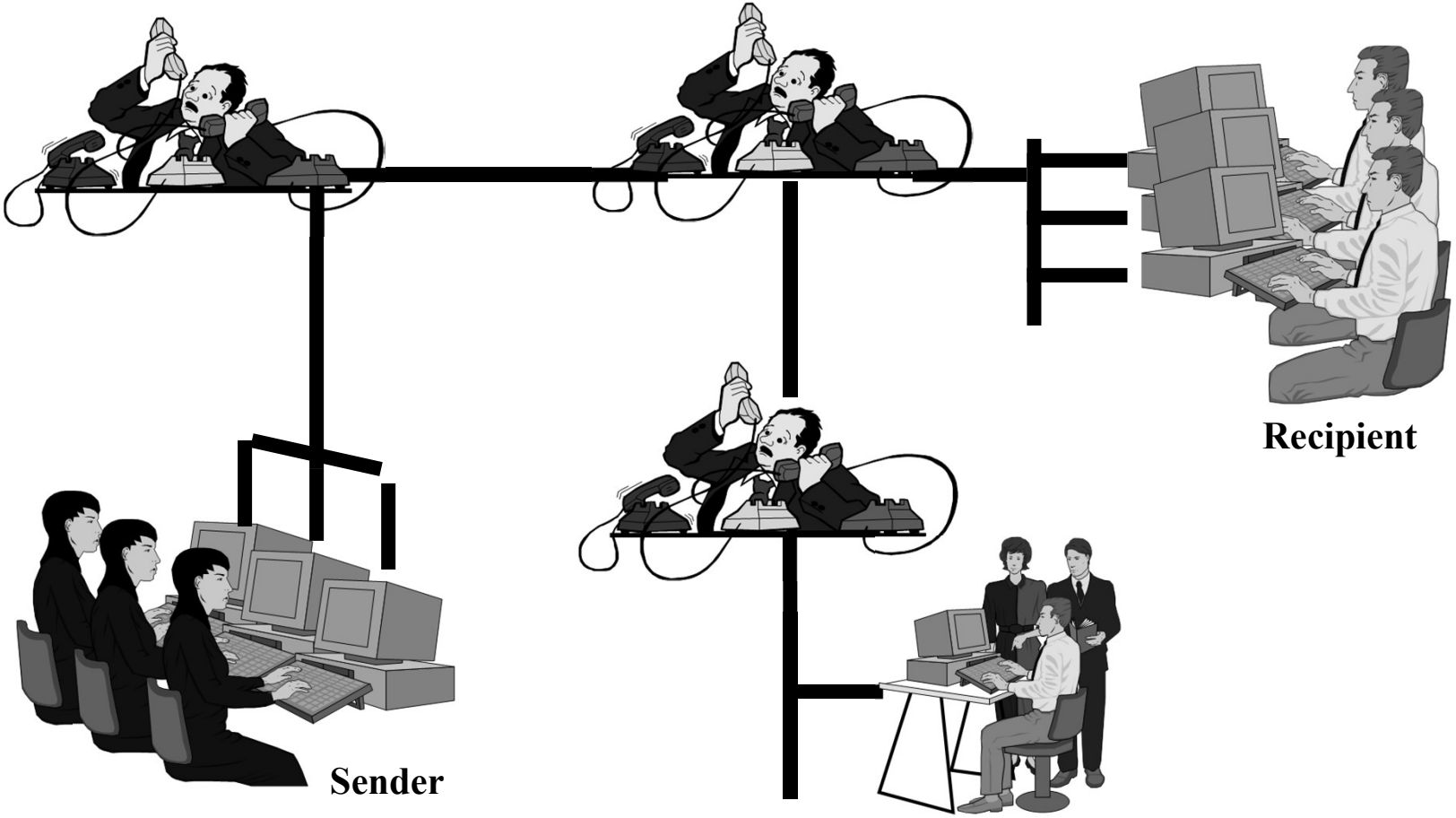
Intermediaries forward messages along the way, using the messages' address to figure where it should go along the way.

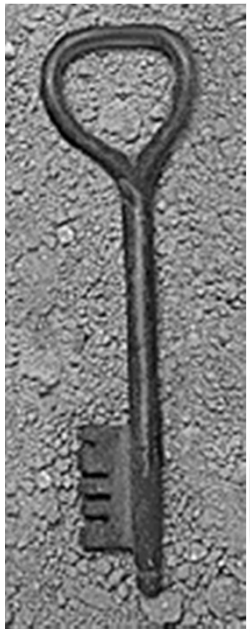


With many local networks, all computers in a given section (subnet) can "see" all messages destined for that subnet, but they are "supposed" ignore messages that are addressed to other computers.

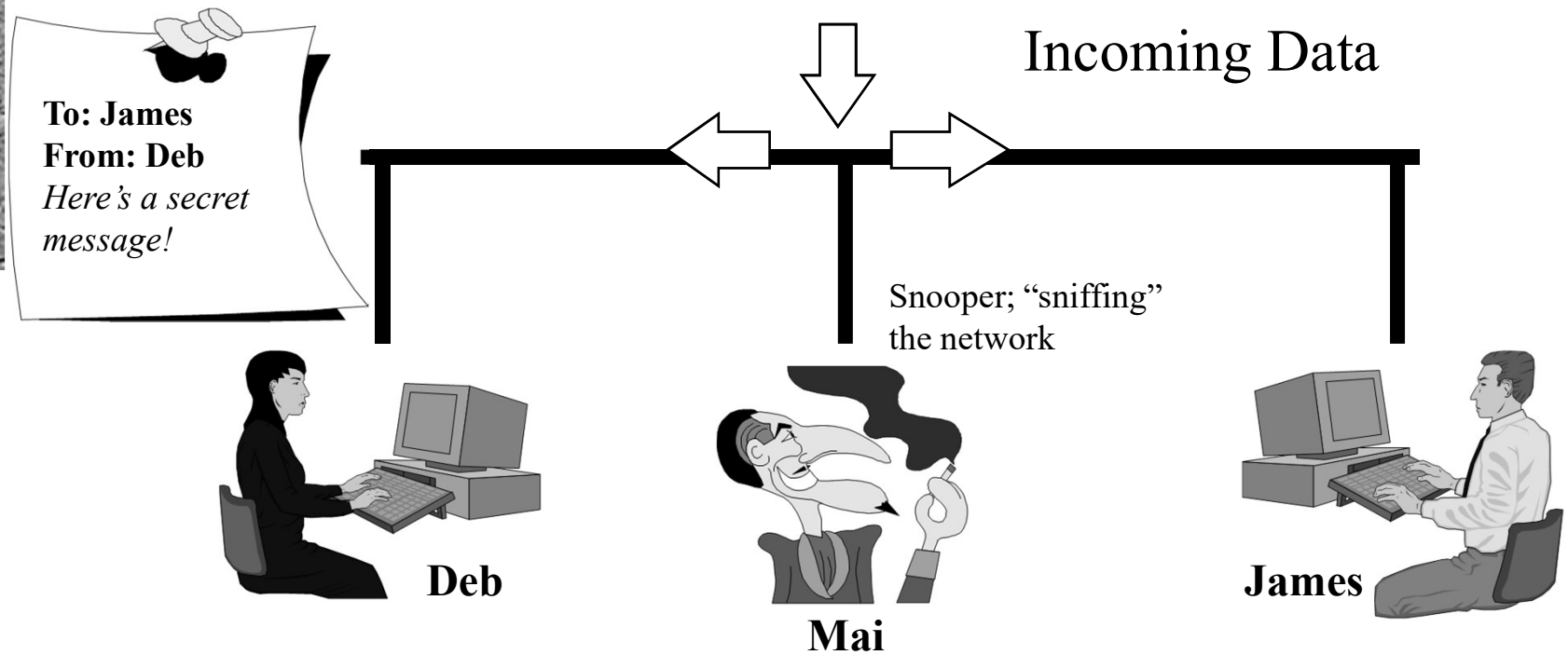


There might be several intermediaries ...

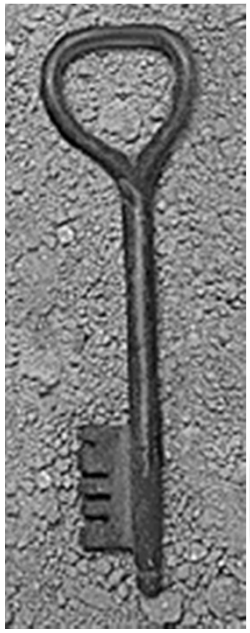




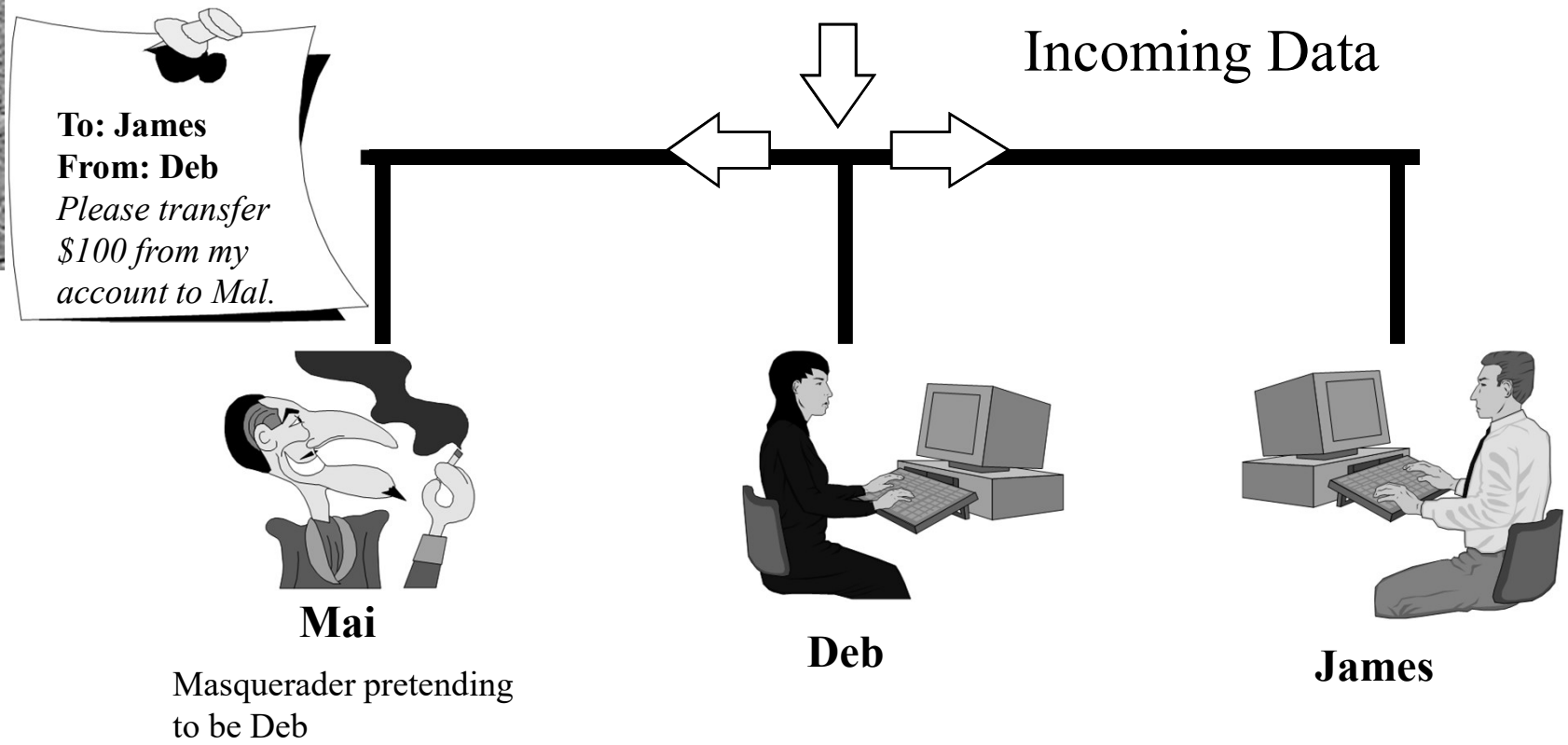
There are lots of security implications ...

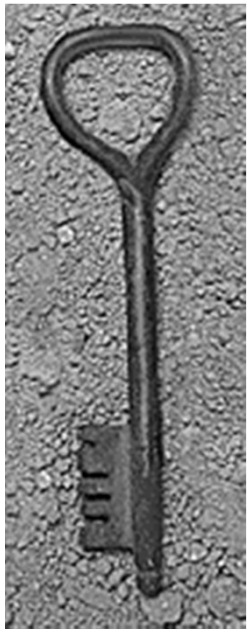


- On the local subnet, computers might read messages not intended for them.

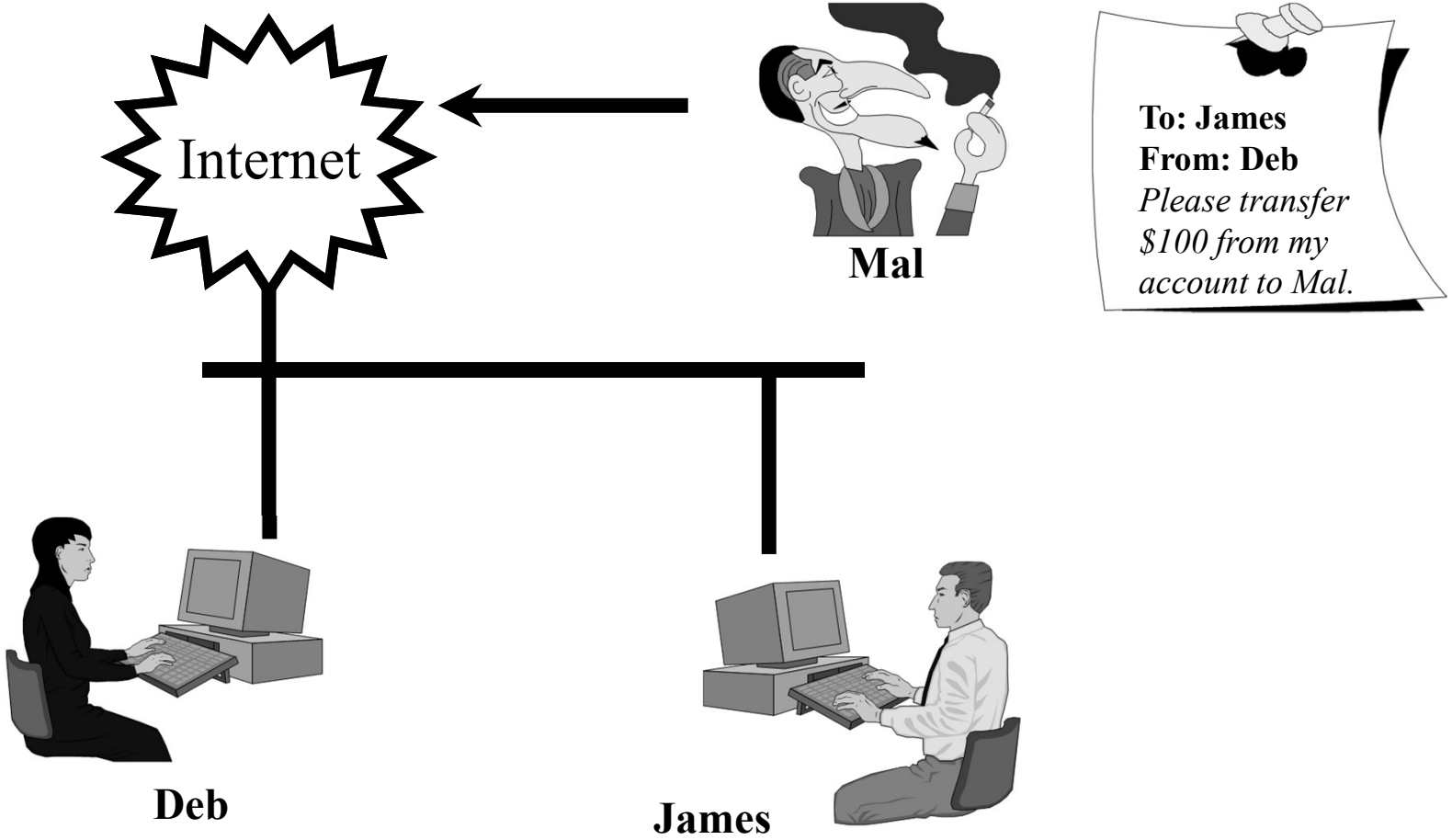


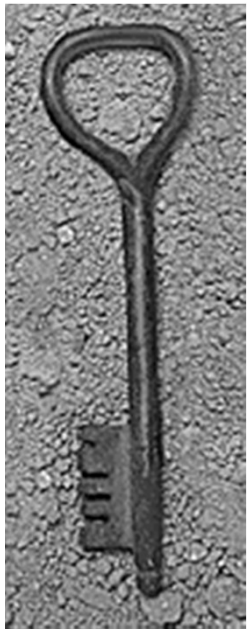
Fake messages can be inserted locally ...



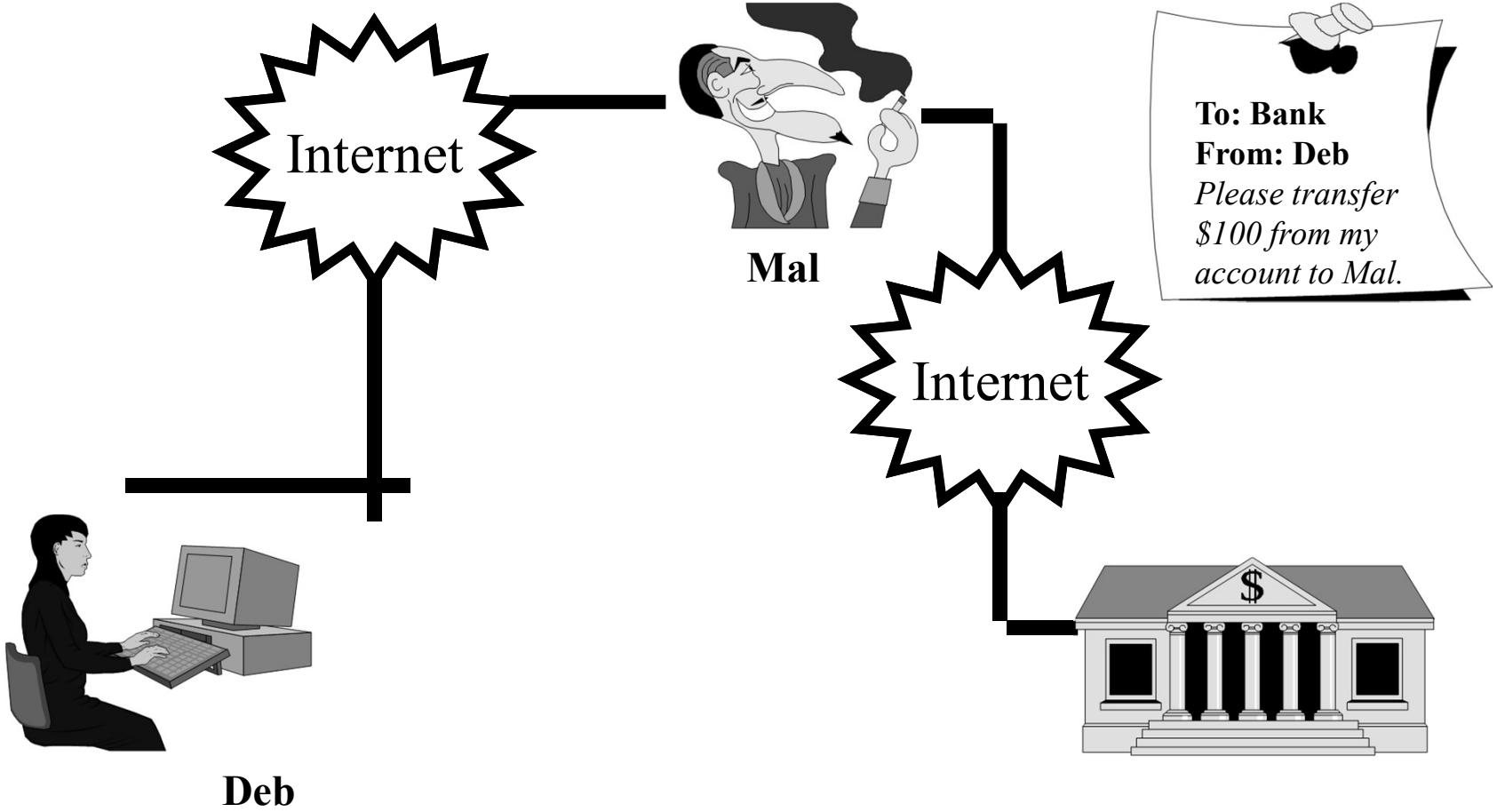


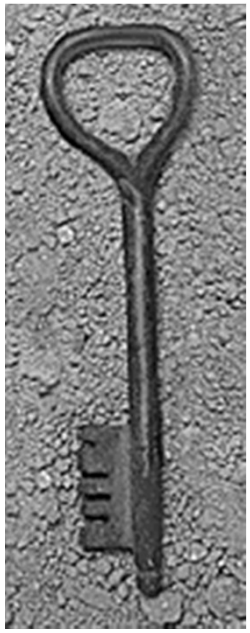
Fake messages can be inserted from outside into the local net ...



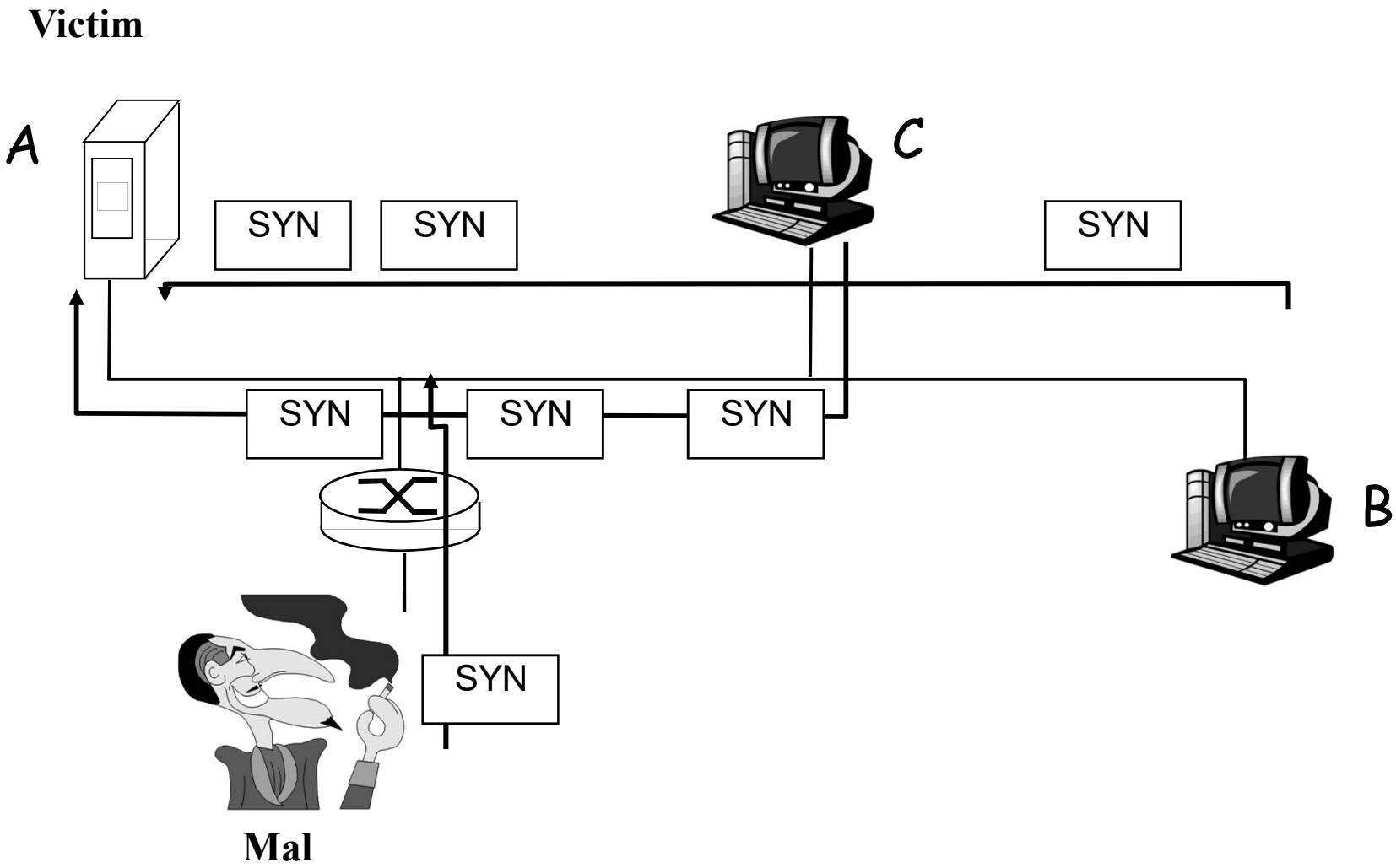


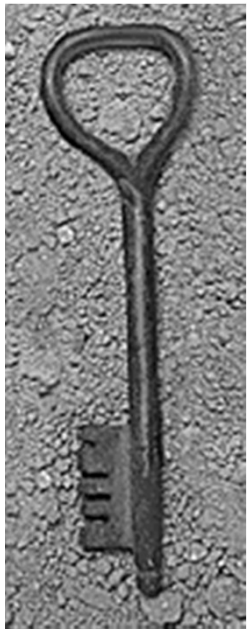
... Or could bypass the local network altogether!





Active Attacks: Denial of Service



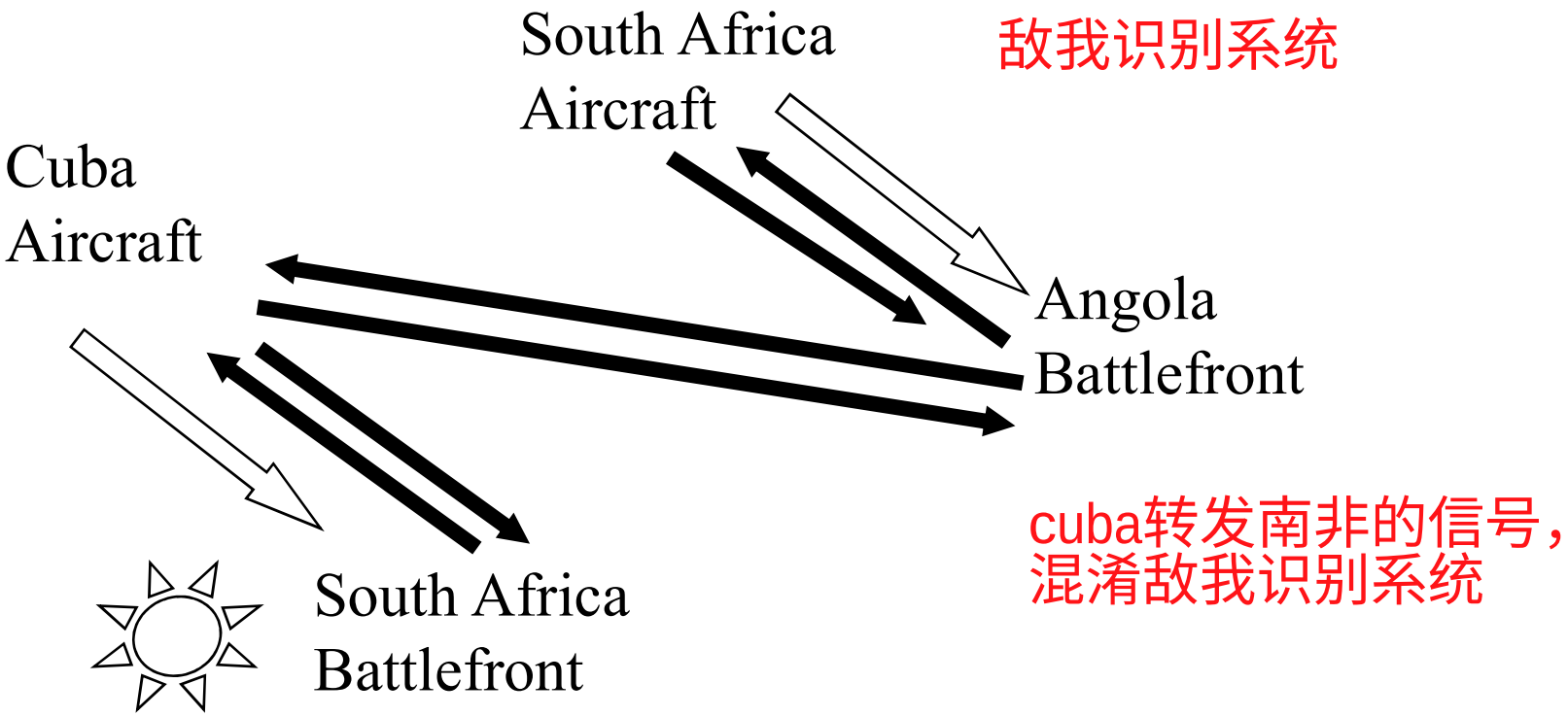


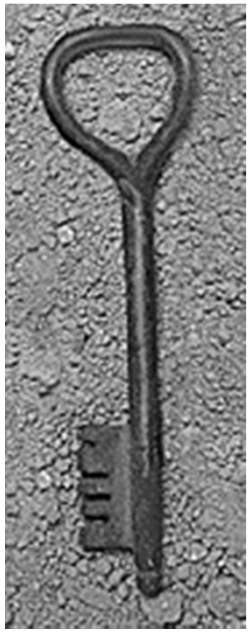
Active Attacks: Replay

重放攻击

空战，古巴vs南非

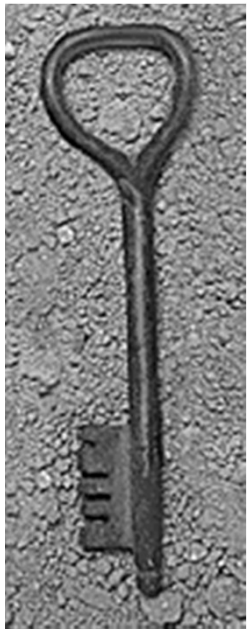
- Time: late in 1980s
- Subject: Cuba vs. South Africa Airforce





Introduction

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



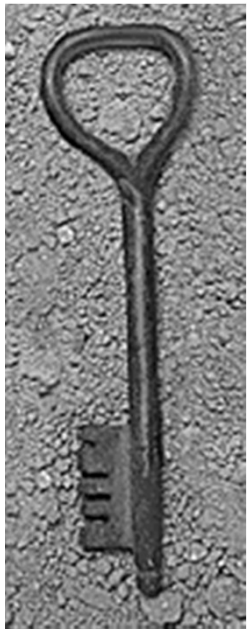
Policies and Mechanisms

policy相当于制定游戏规则，什么是正确的，什么是错误的。

- 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

machanism 机制，比如查重的手段。
使目标系统得到安全策略的手段。

- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities
  - Ex. Student/faculty; partition



Goals of Security

升官发财，给老板讲解。

- Prevention

  黑客完全进不来。

  – Prevent attackers from violating security policy
- Detection

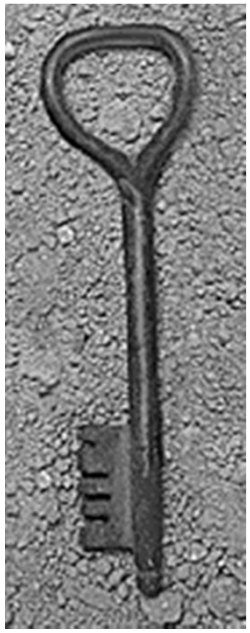
  可以检测到黑客进来。

  – Detect attackers' violation of security policy
- Recovery

  黑客攻击之后，破坏了 发现，然后修复。

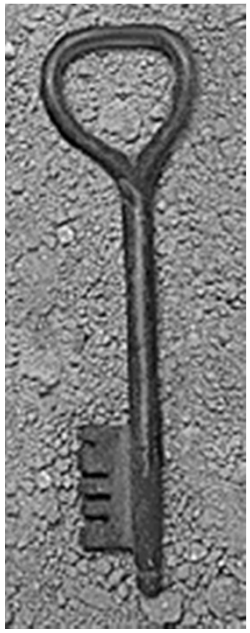
  – Attack is stopped, system is fixed, resume operations

  – (Advanced Version) Continue to function correctly even if attack succeeds



Advanced TOPIC

Intrusion-Tolerant DBMS



Trust and Assumptions

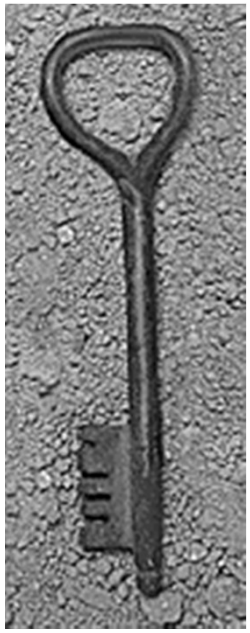
- Underlie *all* aspects of security
  - Ex. Always need the key to access the room?

不一定从门进去金库偷金子

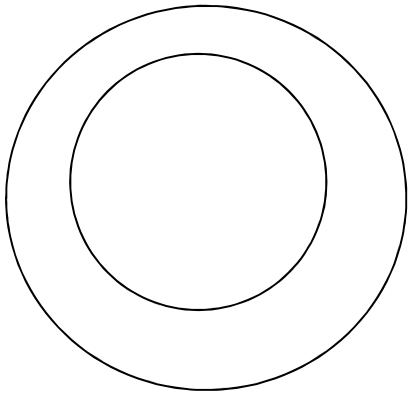
- Policies
  - Correctly capture security requirements
  - Unambiguously partition system states

有源程序也不一定安全。

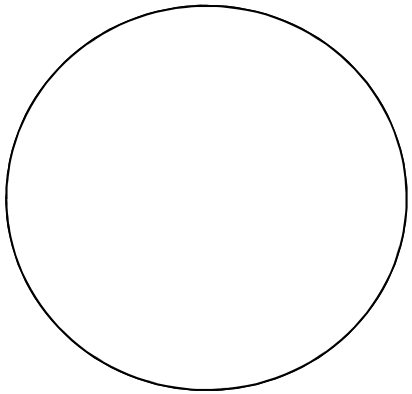
    - Ex. Account Transfer < 10K$, but to himself ?
- Mechanisms
  - Assumed to enforce policy
  - Rely on supporting infrastructure (ex. Ken Thompson's modified C preprocessor) (p. 615)



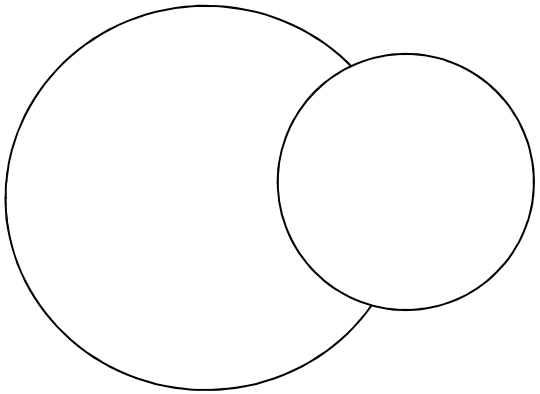
Types of Mechanisms



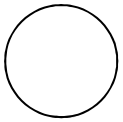
secure



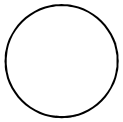
precise



partial

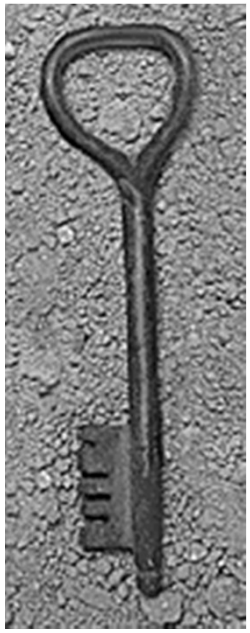


set of reachable states



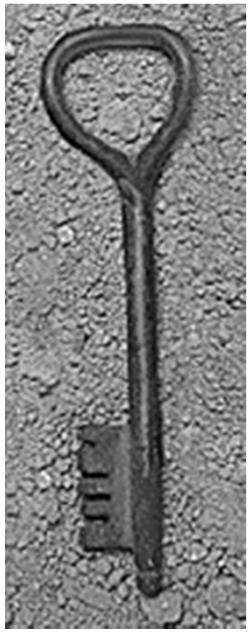
set of secure states

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



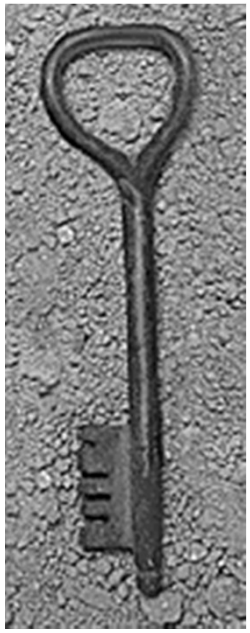
Assurance

度量。信息安全保障是一种度量。

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

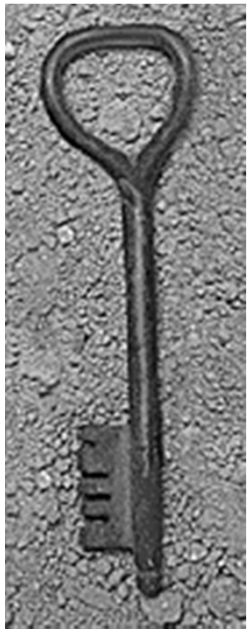
More informally, how much you can trust the system to do what it is supposed to do. It does not say what the system is to do; rather, it only covers how well the system does it.

- 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?



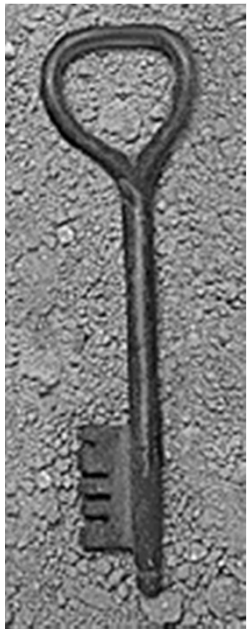
Introduction

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



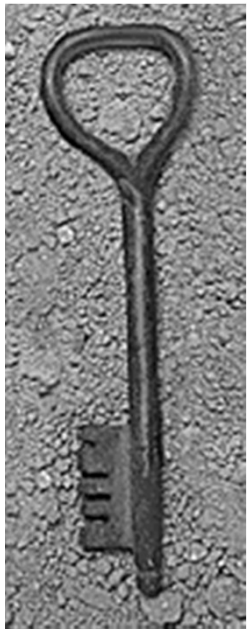
Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis 风险分析，只有100块，有必要买一个超过100的钱包嘛。
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs 法律方面的限制，进出口的限制。生活习惯。
  - Are desired security measures illegal?
    - Ex1. export control of US government (DES)
    - Ex2. key-escrow regulation by France, → US 密钥托管系统，要先把密钥交给国家。
  - Will people do them?
    - Ex1. use urine specimens to determine identity?

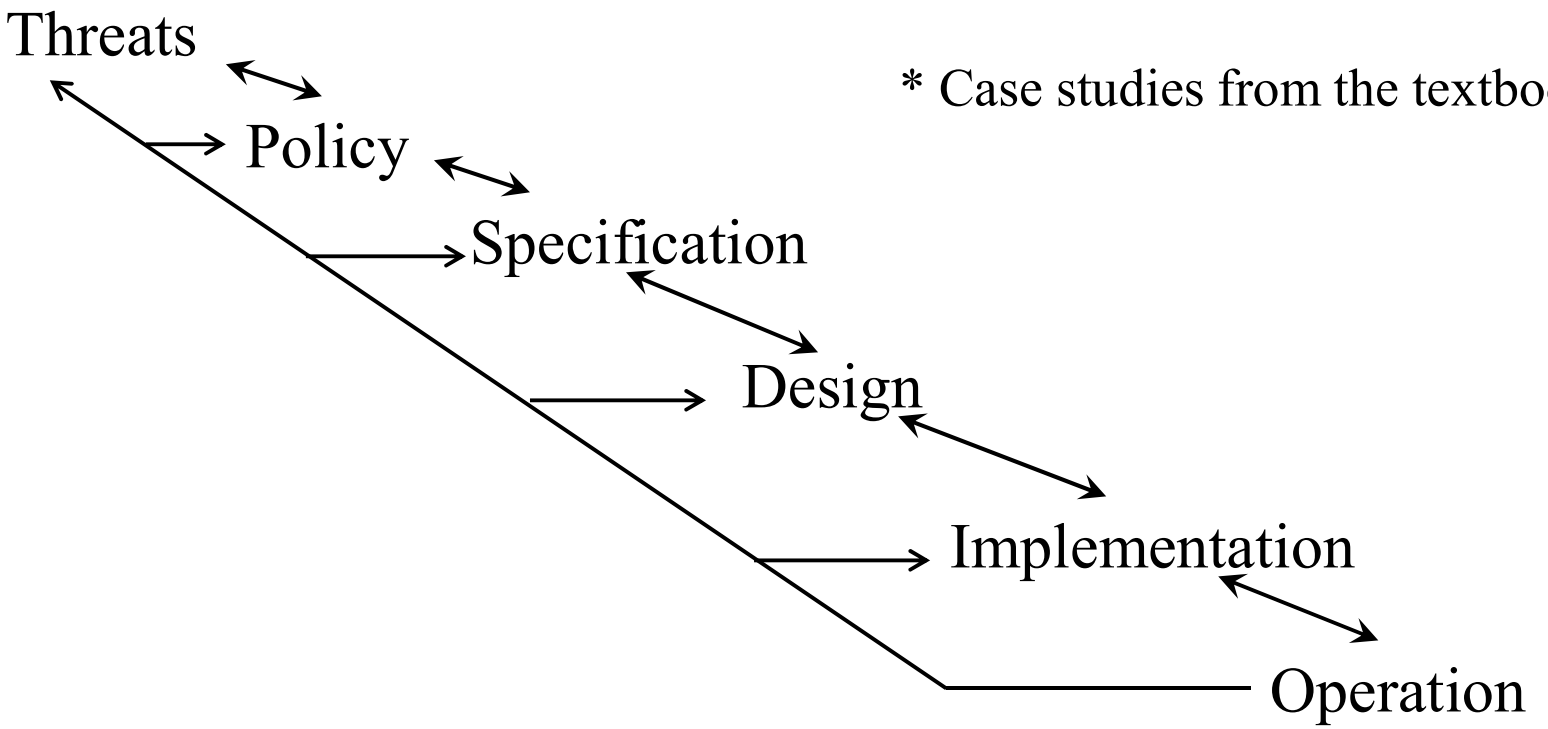


Human Issues

- 30% technical, 70% management
- Organizational Problems
  - Power and responsibility 权力责任相匹配但是并未实现
  - Financial benefits —出事，钱越多。
- People problems
  - Outsiders and insiders 外部人员和内部人员作案
    - *Which do you think is the real threat?*
  - Untrained People, ex. Unverified backup tape
  - Social engineering ex. Night call from executive

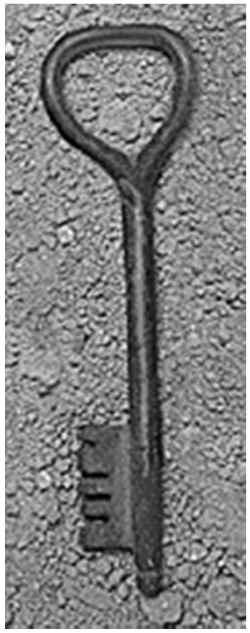


Tying the Definitions Together



* 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

定义了安全

- Policy defines security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions 基本的假设是否成立
- Importance of assurance 信息安全的保障，如何度量。
- The human factor 人的因素。