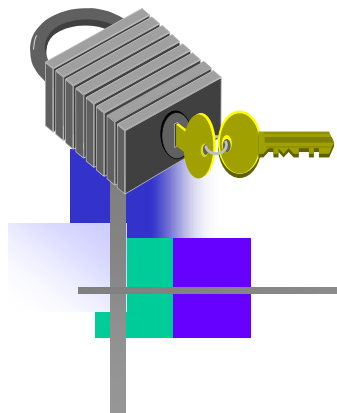


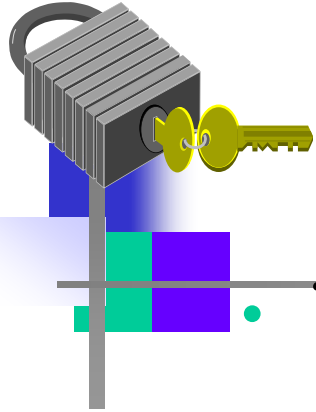
# Computer and Information Security

## Chapter 1 Introduction



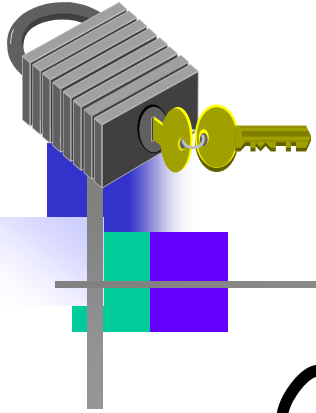
# Information Security: Principles and Practice

Mark Stamp  
Second Edition



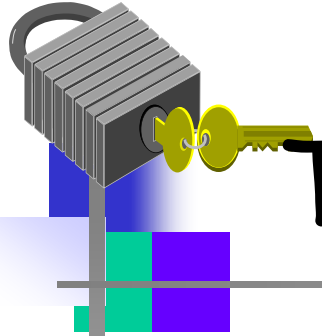
# Overview

- The Cast of Characters
- About the Book
  - Cryptography
  - Access Control
  - Protocols
  - Software
- The People Problem
- Principles and Practice
- Security Goals (CIA Triad)
- The Need for Security



# Chapter 1: Introduction

“Begin at the beginning,” the King said, very gravely,  
“and go on till you come to the end: then stop.”  
— Lewis Carroll, *Alice in Wonderland*

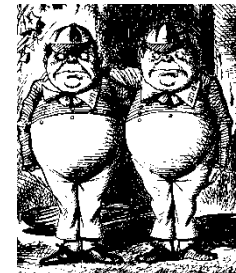


# The Cast of Characters

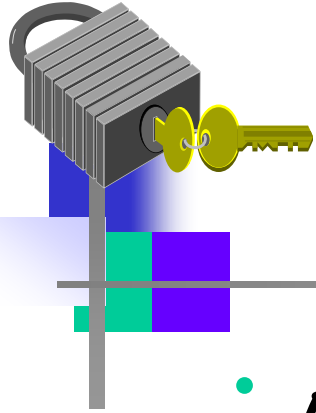
- Alice and Bob are the *good guys*



- Trudy is the **bad “guy”**



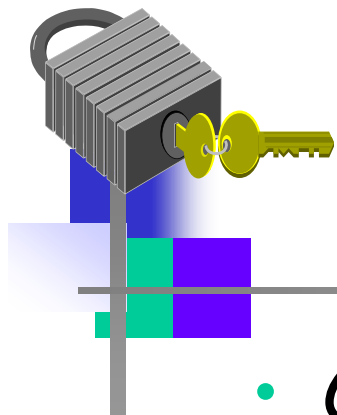
- Trudy is our generic “intruder”



# Alice's Online Bank

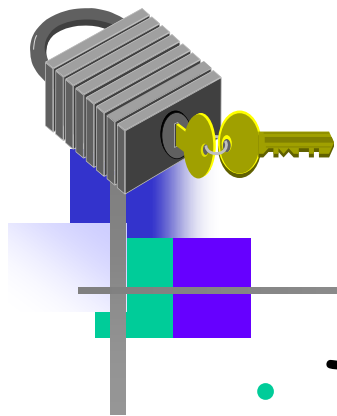
---

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Trudy view the situation?



# CIA

- CIA == Confidentiality, Integrity, and Availability (Authenticity)
- AOB must prevent Trudy from learning Bob's account balance
- **Confidentiality:** prevent unauthorized reading of information
  - Cryptography used for confidentiality

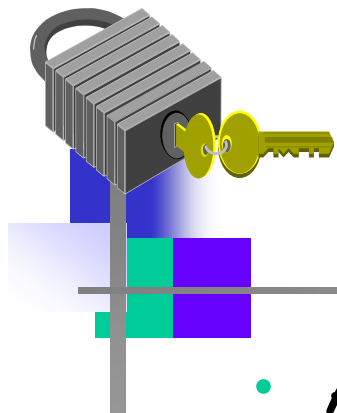


# CIA

---

- Trudy must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- **Integrity:** detect unauthorized *writing* of information
  - Cryptography used for integrity





# CIA

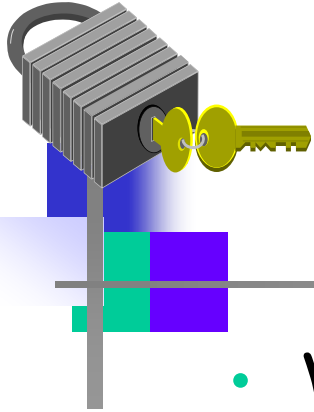
- AOB's information must be available whenever it's needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a timely manner when needed
- Availability is a "new" security concern
  - Denial of service (DoS) attacks



# Beyond CIA: Crypto

---

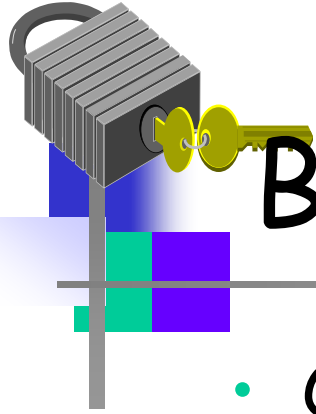
- How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
  - This requires some clever **cryptography**
- What are security concerns of pwds?
- Are there alternatives to passwords?



# Beyond CIA: Protocols

---

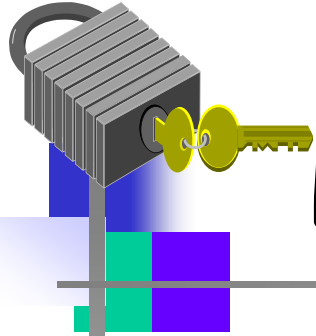
- When Bob logs into AOB, how does AOB know that “Bob” is really Bob?
- As before, Bob’s password is verified
- Unlike the previous case, **network** security issues arise
- How do we secure network transactions?
  - **Protocols** are critically important
  - Crypto plays critical role in protocols



# Beyond CIA: Access Control

---

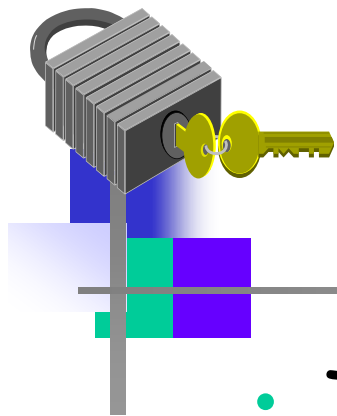
- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions: *authorization*
- **Access control** includes both authentication and authorization



# Beyond CIA: Software

---

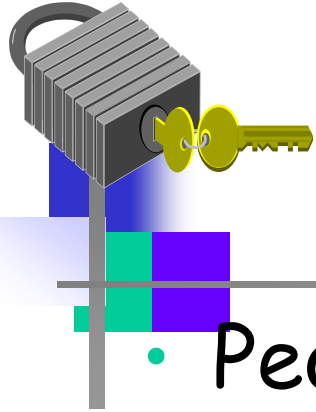
- Cryptography, protocols, and access control are implemented in **software**
  - Software is foundation on which security rests
- What are security issues of software?
  - Real world software is complex and buggy
  - Software flaws lead to security flaws
  - How does Trudy attack software?
  - How to reduce flaws in software development?
  - And what about **malware**?



# Your Textbook

---

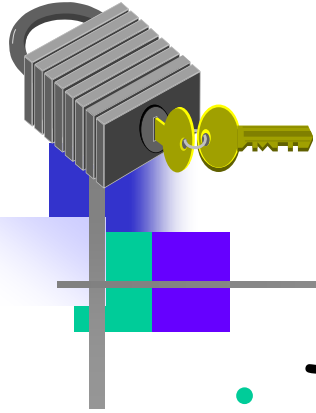
- The text consists of four major parts
  - Cryptography
  - Access control
  - Protocols
  - Software
- Note: Our focus is on technical issues



# The People Problem

---

- People often break security
  - Both intentionally and unintentionally
  - Here, we consider the unintentional
- For example, suppose you want to buy something online
  - To make it concrete, suppose you want to buy *Information Security: Principles and Practice*, 2<sup>nd</sup> edition from amazon.com

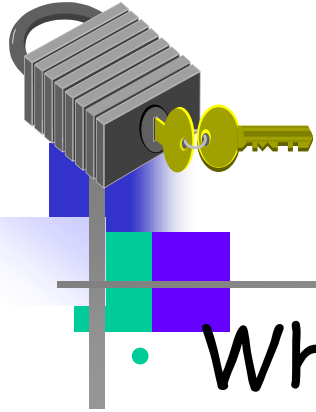


# The People Problem

---

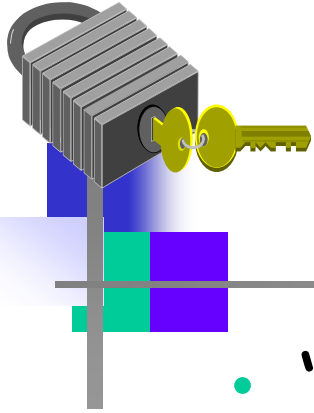
- To buy from amazon.com...
  - Your Web browser uses SSL protocol
  - SSL relies on cryptography
  - Access control issues arise
  - All security mechanisms are in software
- Suppose all of this security stuff works perfectly
  - Then you would be safe, right?





# The People Problem

- What could go wrong?
- Trudy tries man-in-the-middle attack
  - SSL is secure, so attack doesn't "work"
  - But, Web browser issues a warning
  - What do you, the user, do?
- If user ignores warning, attack works!
  - None of the security mechanisms failed
  - But user *unintentionally* broke security



# Cryptography

---

- "Secret codes"
- The book covers
  - Classic cryptography
  - Symmetric ciphers
  - Public key cryptography
  - Hash functions++
  - Advanced cryptanalysis



# Access Control

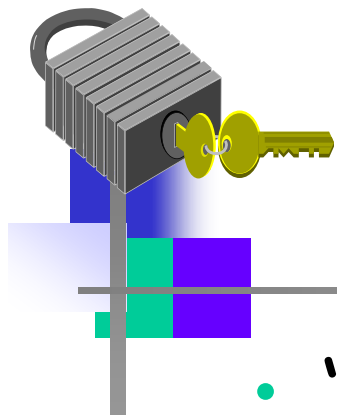
---

## Authentication

- Passwords
- Biometrics
- Other methods of authentication

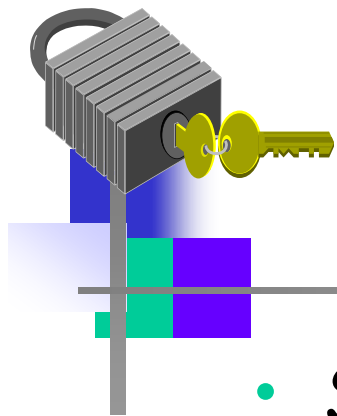
- Authorization

- Access Control Lists/Capabilities
- Multilevel security (MLS), security modeling, covert channel, inference control
- Firewalls, intrusion detection (IDS)



# Protocols

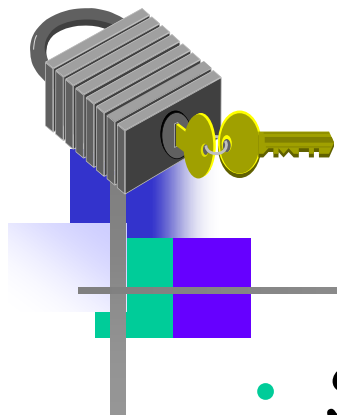
- “Simple” authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Real-world security protocols
  - SSH, SSL, IPSec, Kerberos
  - Wireless: WEP, GSM



# Software

---

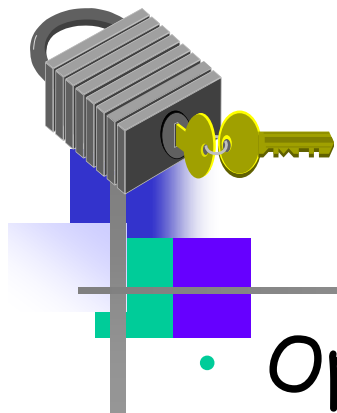
- Security-critical flaws in software
  - Buffer overflow
  - Race conditions, etc.
- Malware
  - Examples of viruses and worms
  - Prevention and detection
  - Future of malware?



# Software

---

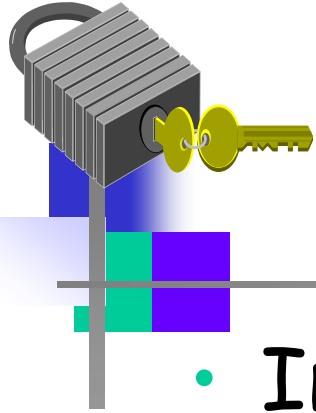
- Software reverse engineering (SRE)
  - How hackers “dissect” software
- Digital rights management (DRM)
  - Shows difficulty of security in software
  - Also raises OS security issues
- Software and testing
  - Open source, closed source, other topics



# Software

---

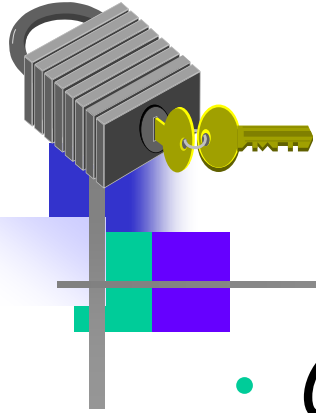
- Operating systems
  - Basic OS security issues
  - "Trusted OS" requirements
  - NGSCB (Next Generation Secure Computing Base): Microsoft's trusted OS for the PC
- Software is a **BIG** security topic
  - Lots of material to cover
  - Lots of security problems to consider
  - But not nearly enough time available...



# Think Like Trudy

- In the past, no respectable sources talked about “hacking” in detail
  - After all, such info might help Trudy
- Recently, this has changed
  - Lots of books on network hacking, evil software, how to hack software, etc.
  - Classes teach virus writing, SRE (Software Reverse Engineering), etc.

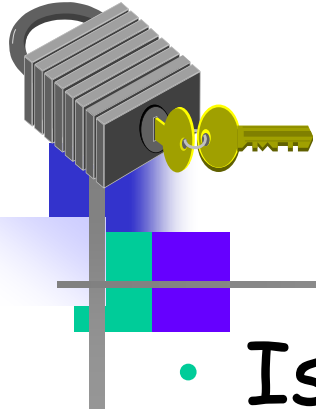




# Think Like Trudy

---

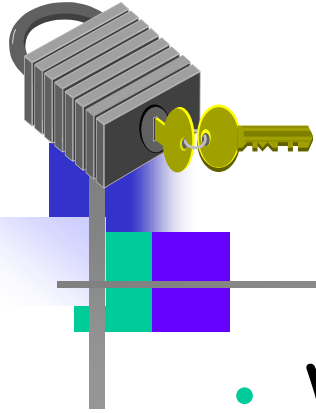
- Good guys must think like bad guys!
- A police detective...
  - ...must study and understand criminals
- In information security
  - We want to understand Trudy's methods
  - Might think about Trudy's motives
  - We'll often pretend to be Trudy



# Think Like Trudy

---

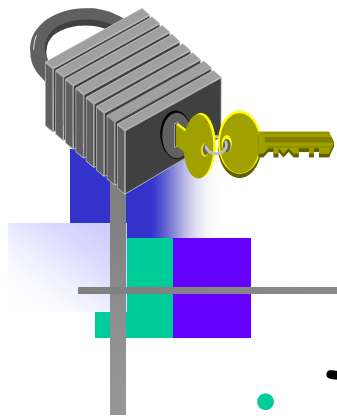
- Is all of this security information a good idea?
- Bruce Schneier (referring to *Security Engineering*, by Ross Anderson):
  - "It's about time somebody wrote a book to teach the good guys what the bad guys already know."



# Think Like Trudy

---

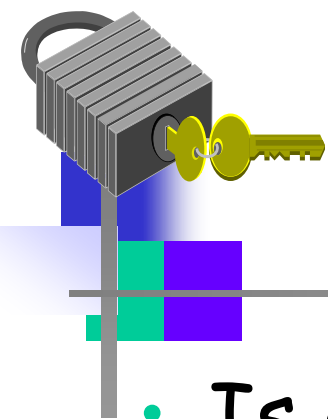
- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice's and/or Bob's stupidity
- But, we **cannot** act like Trudy
  - Except in this class...



# In This Course...

---

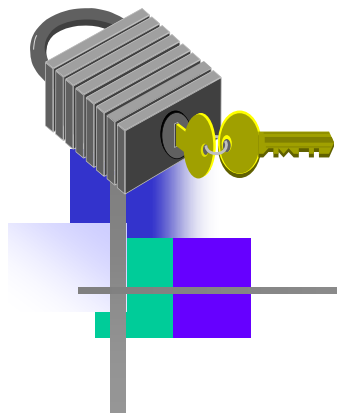
- Think like the bad guy
- Always look for weaknesses
  - Find the *weak link* before Trudy does
- It's OK to break the rules
  - What rules?
- Think like Trudy
- But don't do anything illegal!



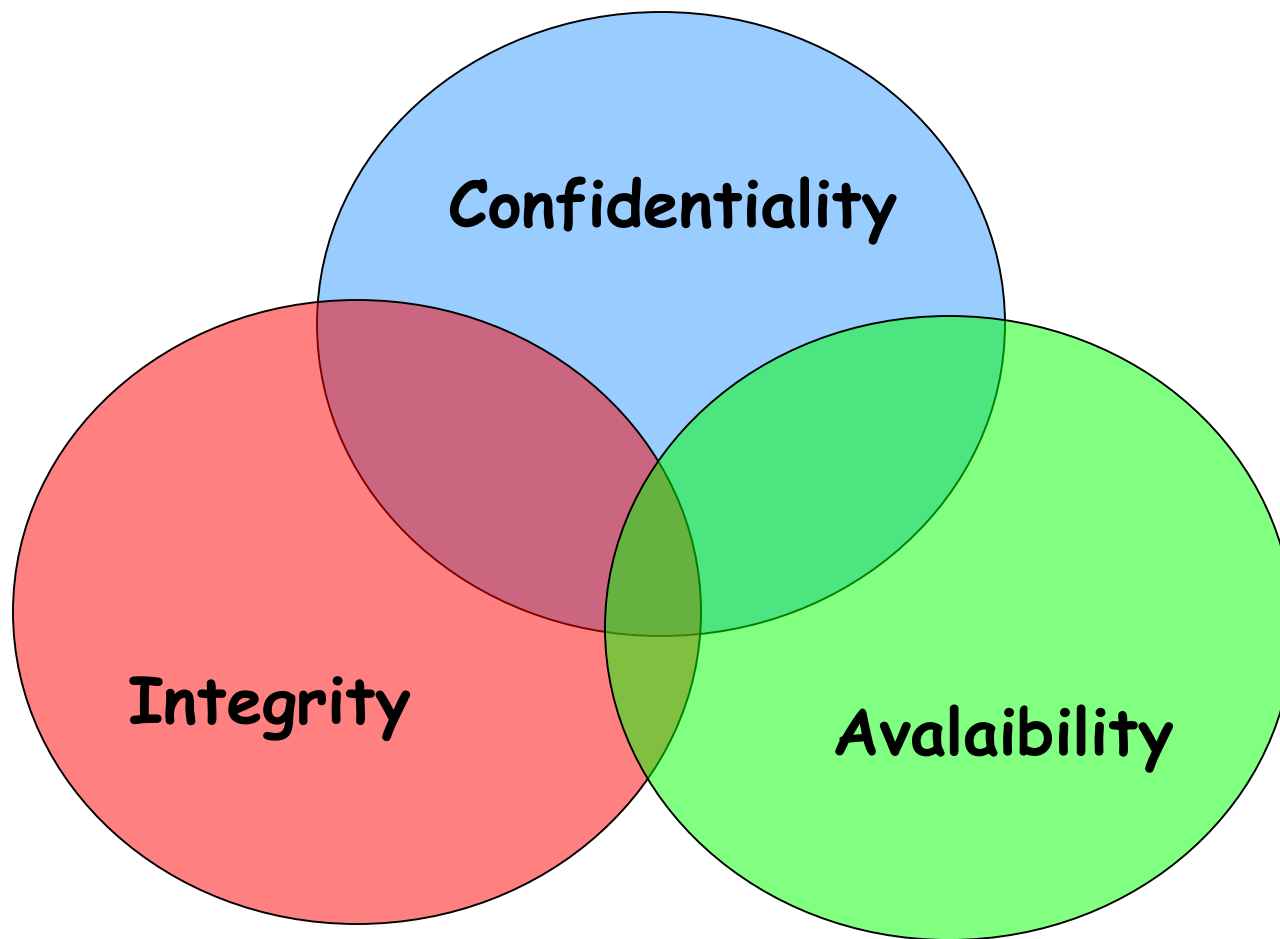
# Computer Security

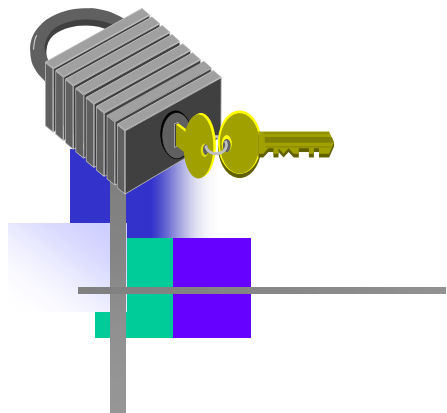
---

- Is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

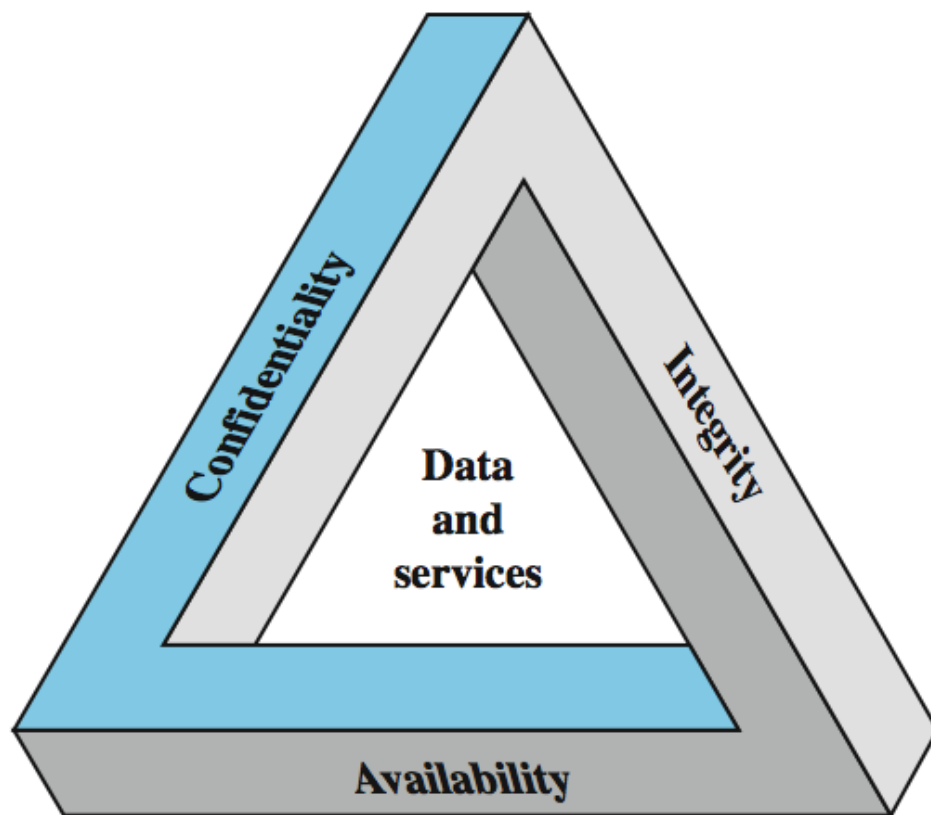


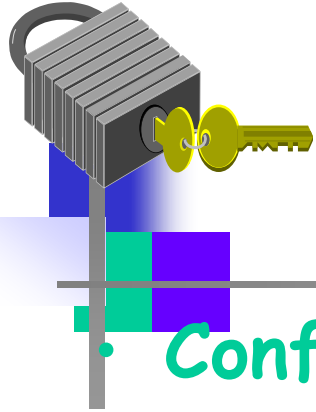
# Security Goals





# CIA Triad





# Key Objectives

- **Confidentiality**

- **Data Confidentiality**-information not disclosed to unauthorized individuals
- **Privacy**- individuals control how their information is collected, stored, shared

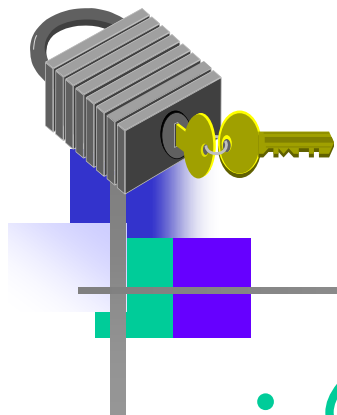
- **Integrity**

- **Data Integrity**
- **System Integrity**

- **Availability**- service not denied to authorized users

- **Authenticity**- user is who he/she claims to be

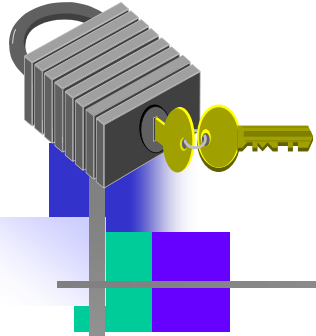




# Security Goals

---

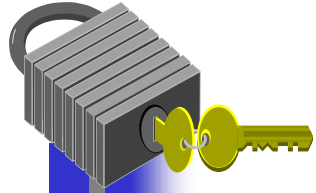
- Confidentiality
  - Concealment of information or resources
- Integrity
  - Trustworthiness of data or resources
- Availability
  - Ability to use information or resources



# Confidentiality

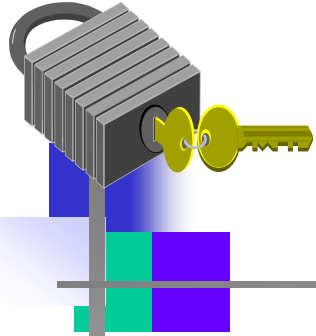
---

- Need for keeping information secret arises from use of computers in sensitive fields such as government and industry
- Access mechanisms, such as cryptography, support confidentiality
  - Example: encrypting income tax return
- Lost through unauthorized disclosure of information



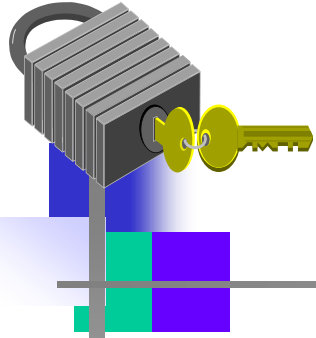
# Integrity

- Often requires preventing unauthorized changes
- Includes data integrity (content) and origin integrity (source of data also called authentication)
- Include prevention mechanisms and detection mechanisms
  - Example: Newspaper prints info leaked from White House and gives wrong source
- Includes both correctness and trustworthiness
- Lost through unauthorized modification or destruction of information



# Availability

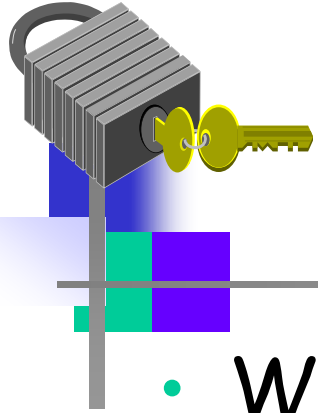
- Is an aspect of reliability and system design
- Attempts to block availability, called **denial of service attacks (DoS)** are difficult to detect
  - Example: bank with two servers -one is blocked, the other provides false information
- Ensures timely and reliable access to and use of information
- Lost through disruption of access to information or information system



# Authenticity and Accountability

Two additional objectives:

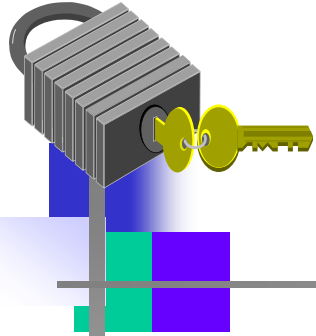
- **Authenticity**- being genuine and able to be verified or trust; verifying that users are who they say they are
- **Accountability**-actions of an entity can be traced uniquely to that entity; supports nonrepudiation, deterrence, fault isolation, intrusion, detection and prevention.



# Levels of Impact

---

- We can define 3 levels of impact from a security breach:
  - Low
  - Moderate
  - High



# Security Breach Low Impact

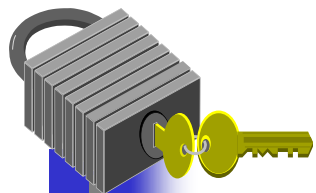
- Loss has limited adverse effect
- For example:
  - Effectiveness of the functions of an organization are noticeably reduced
  - Results in minor damage to organizational assets
  - Results in minor financial loss
  - Results in minor harm to individuals



# Security Breach Moderate Impact

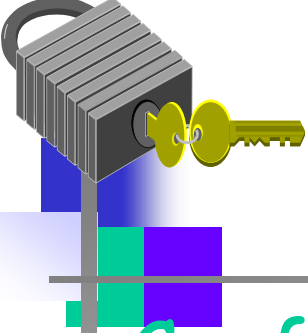
- Loss may have serious adverse effect on organizational operations, assets or individuals.
- For example:
  - Effectiveness of the functions of an organization are significantly reduced
  - Results in significant damage to organizational assets
  - Results in significant financial loss
  - Results in significant harm to individuals





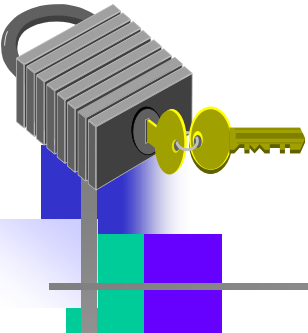
# Security Breach High Impact

- Loss is expected to have severe or catastrophic adverse effect on organizational operations, assets or individuals.
- For example:
  - Effectiveness of the functions of an organization are reduced so that the organization cannot perform its primary function(s).
  - Results in major damage to organizational assets
  - Results in major financial loss
  - Results in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries



# Examples of Security Requirements

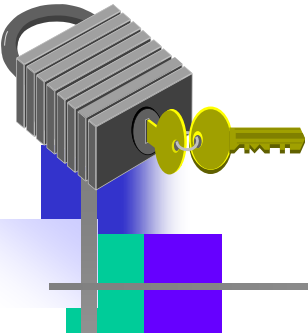
- **Confidentiality** - student grades
  - **High confidentiality** - grades
    - Regulated by FERPA
    - Only available to students, parents and employees (who need it to do their job)
  - **Moderate confidentiality** -enrollment
  - **Low confidentiality** - Directory information
    - Lists of departments, faculty, students
    - Available to the public
    - Often published on Web site



# Examples of Security Requirements

---

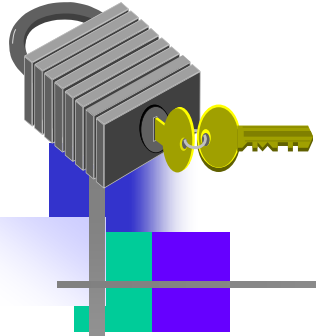
- **Integrity**- patient information
  - **High requirement for integrity**
    - -Medical database, if falsified or inaccurate, could cause harm ( allergies, etc.)
  - **Medium requirement for integrity**
    - Web site that offers a forum for discussion of medical topics, not for research
  - **Low requirement for integrity**
    - Anonymous poll (such as a patient satisfaction)



# Examples of Security Requirements

**Availability** – The more critical a component or service is, the higher the level of availability required:

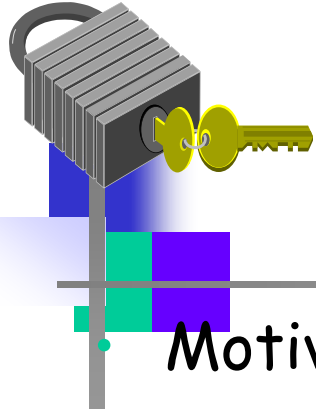
- **High availability**- authentication service
  - Interruption of service results in being unable to access computing resources
- **Moderate availability**- College web site
  - Provides information but is not critical
- **Low availability**- online phone directory
  - Other sources of information are available



# The Need for Security

---

- **Computer Security** - the collection of tools designed
  - to protect data and
  - to thwart hackers
- **Network security or internet security** - security measures needed to protect data during their transmission



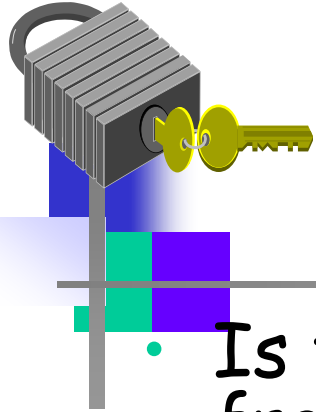
# Security

- Motivation: **Why do we need security?**
- Increased reliance on Information technology with or without the use of networks
- The use of IT has changed our lives drastically.
- We depend on E-mail, Internet banking, and several other governmental activities that use IT
- Increased use of E-Commerce and the World wide web on the Internet as a vast repository of various kinds of information (immigration databases, flight tickets, stock markets etc.)



# Security Concerns

- Damage to any IT-based system or activity can result in severe disruption of services and losses
- Systems connected by networks are more prone to attacks and also suffer more as a result of the attacks than stand-alone systems (Reasons?)
- Concerns such as the following are common
  - How do I know the party I am talking on the network is *really* the one I want to talk?
  - How can I be assured that no one else is listening and learning the data that I send over a network
  - Can I ever stay relaxed that no hacker can enter my network and play havoc?

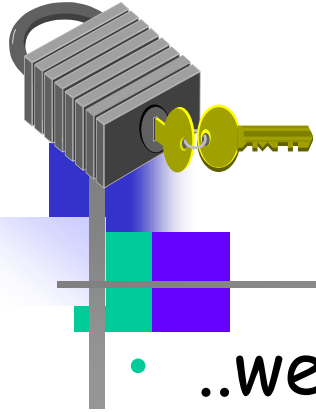


# Concerns continued...

---

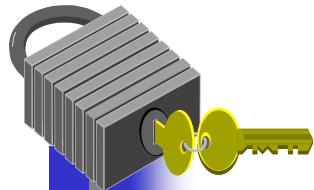
- Is the web site I am downloading information from a legitimate one, or a fake?
- How do I ensure that the person I just did a financial transaction denies having done it tomorrow or at a later time?
- I want to buy some thing online, but I don't want to let them charge my credit card before they deliver the product to me





# That is why...

- ..we need security
  - To safeguard the confidentiality, integrity, authenticity and availability of data transmitted over insecure networks
  - Internet is not the only insecure network in this world
  - Many internal networks in organizations are prone to insider attacks
  - In fact, insider attacks are greater both in terms of likelihood of happening and damage caused



https://

(V.Shmatikov)

Wells Fargo Account Summary - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home

Address [https://online.wellsfargo.com/mn1\\_aa1\\_on/cgi-bin/session.cgi?sessargs=coAn76axS2xltPX8uoCT8rRBFMMdJldx](https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76axS2xltPX8uoCT8rRBFMMdJldx) Go Links Yahoo maps Mapblast Dictionary

Home | Help Center | Contact Us | Locations | Site Map | Apply | **Sign Off**

**WELLS FARGO**

**Account Summary** Last Log On: January 06, 2004

> Account Summary

- Brokerage
- Bill Pay
- Transfer
- Account Services
- My Message Center

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.

Wells Fargo Accounts | **OneLook Accounts**

**Tip:** Select an account's balance to access the Account History.

**NEW** [Enroll for Online Statements](#) [My Message Center](#)

**Cash Accounts**

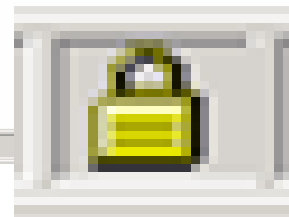
Account	Account Number	Available Balance
Checking <a href="#">Add Bill Pay</a>		
<b>Total</b>		

To end your session, be sure to Sign Off.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off  
Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.

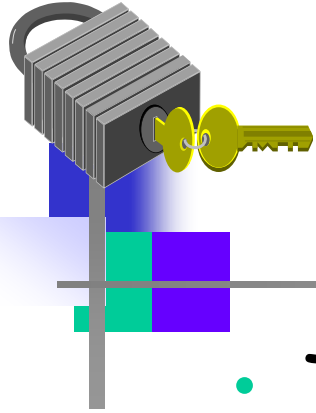
Internet





# However, in reality

- Security is often over looked (not one of the top criteria)
- Availability, efficiency and performance tend to be the ones
- Buggy implementations
- Systems too complex in nature and rich in features can be filled with security holes
- Incorporation of security into networks, not growing with the rapidly growing number and size of networks
- Attacking is becoming so common and easy - there are books clearly explaining how to launch them
- Security and attacks are a perpetual cat-and-mouse play. The only way to avoid attacks is to keep up-to-date with latest trends and stay ahead of malicious netizens



# The Good News...

- There a lot of techniques for defense
- Educating people on security solves many problems
- About threats and on the existence of security mechanisms, qualified personnel, usability and economics
- We will study a lot of network defenses
  - Certainly not **all**



# Computer Security Challenges

---

Computer Security is both fascinating and complex:

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms

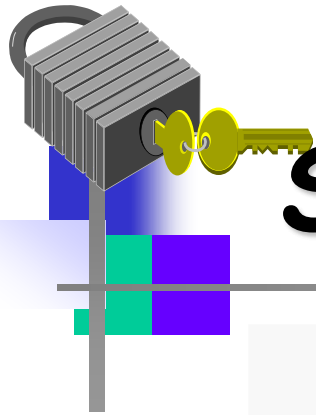


# Computer Security Challenges

---

6. battle of wits between attacker/administrator
7. not perceived to be a benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to efficient and user friendly use of system

These difficulties will be explored throughout the course.



# Security Threats/Attacks

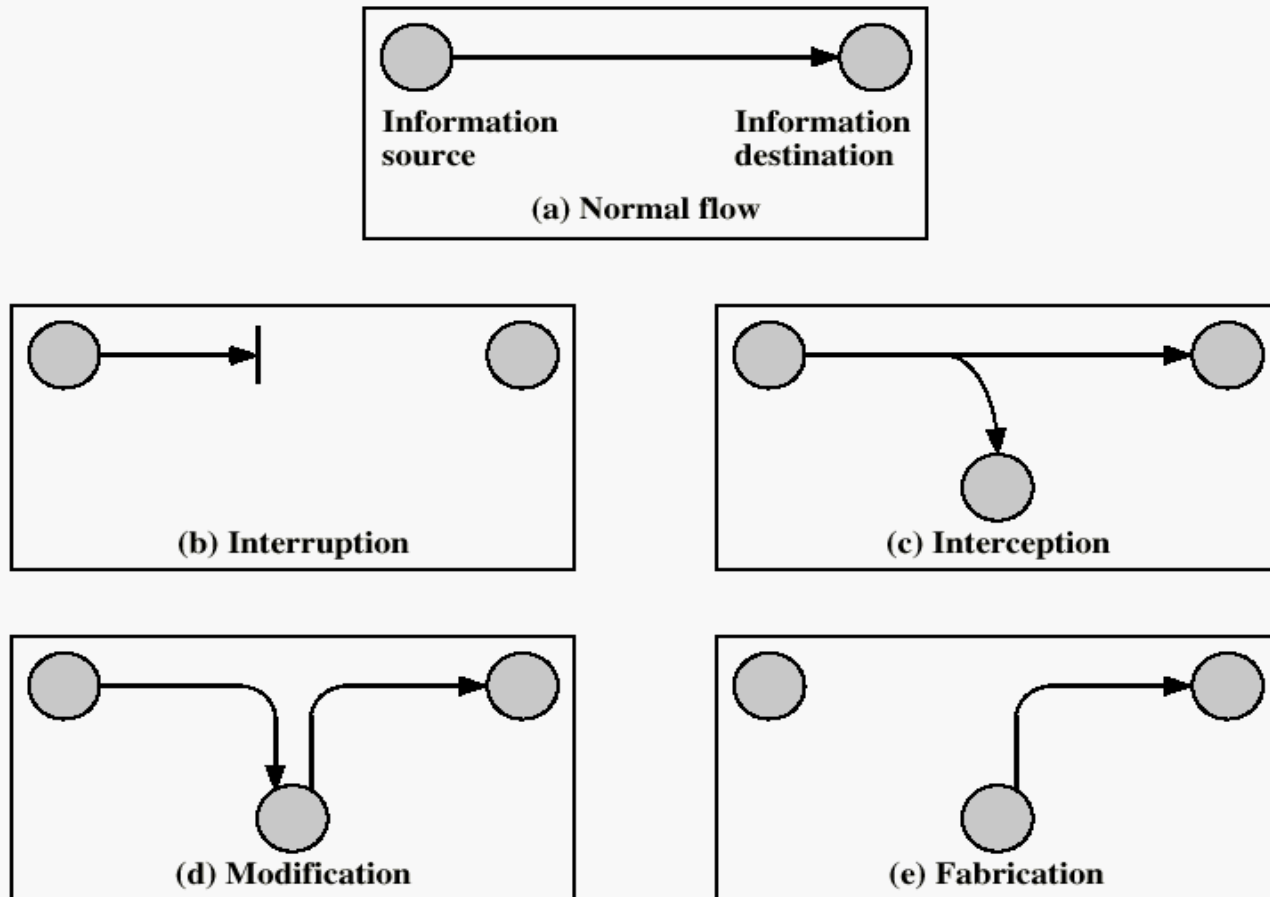


Figure 1.1 Security Threats

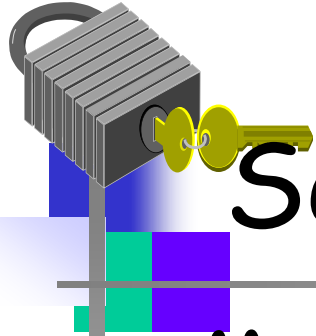


# Security Attacks

---

- **Interruption:** This is an attack on **availability**
  - Disrupting traffic
  - Physically breaking communication line
- **Interception:** This is an attack on **confidentiality**
  - Overhearing, eavesdropping over a communication line

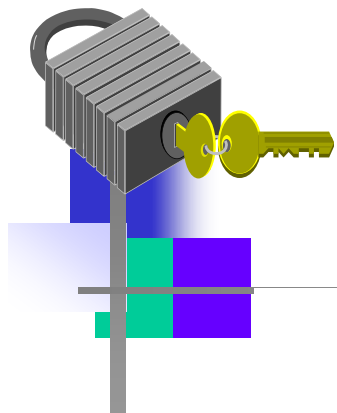




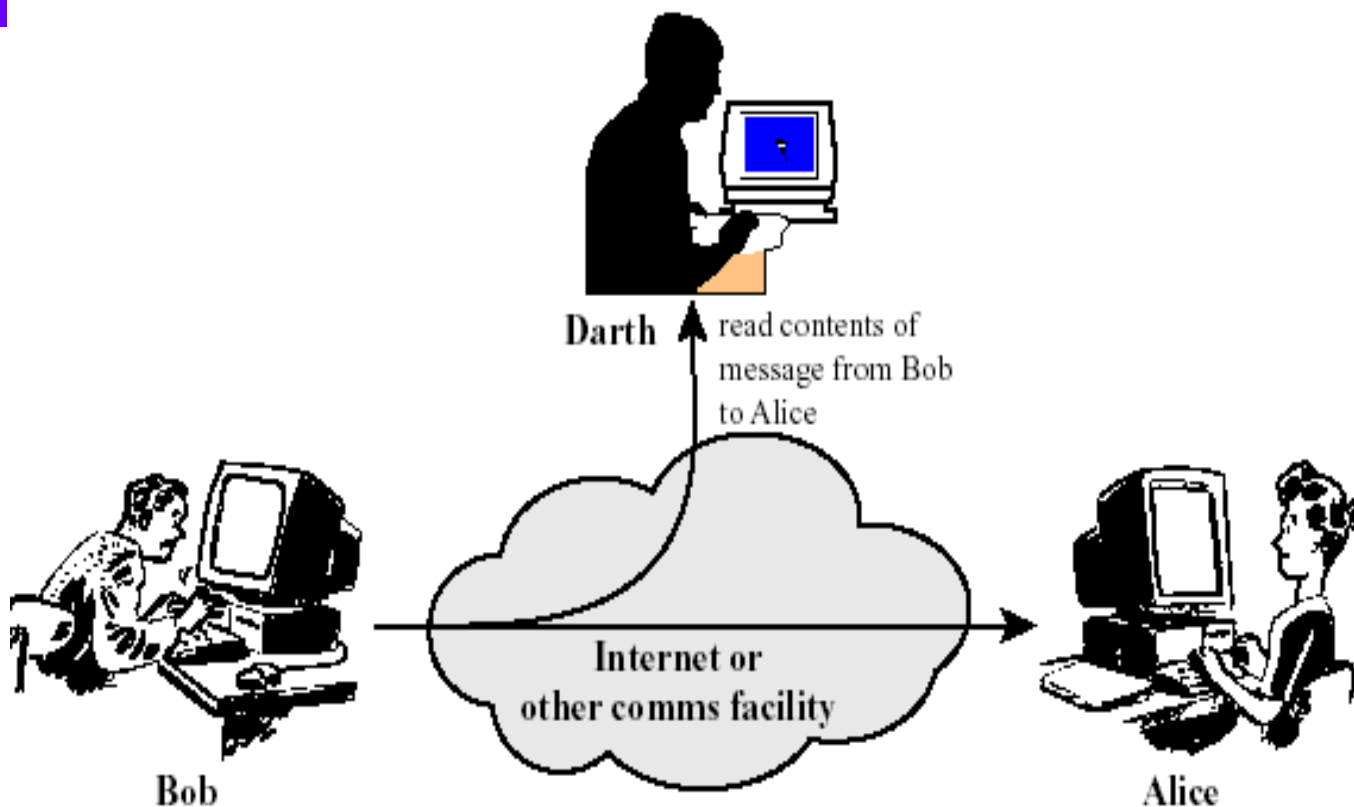
# Security Attacks (continued)

---

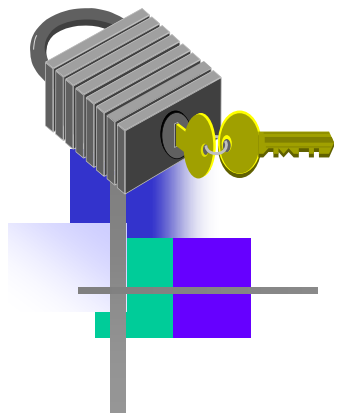
- **Modification:** This is an attack on **integrity**
  - Corrupting transmitted data or tampering with it before it reaches its destination
- **Fabrication:** This is an attack on **authenticity**
  - Faking data as if it were created by a legitimate and authentic party



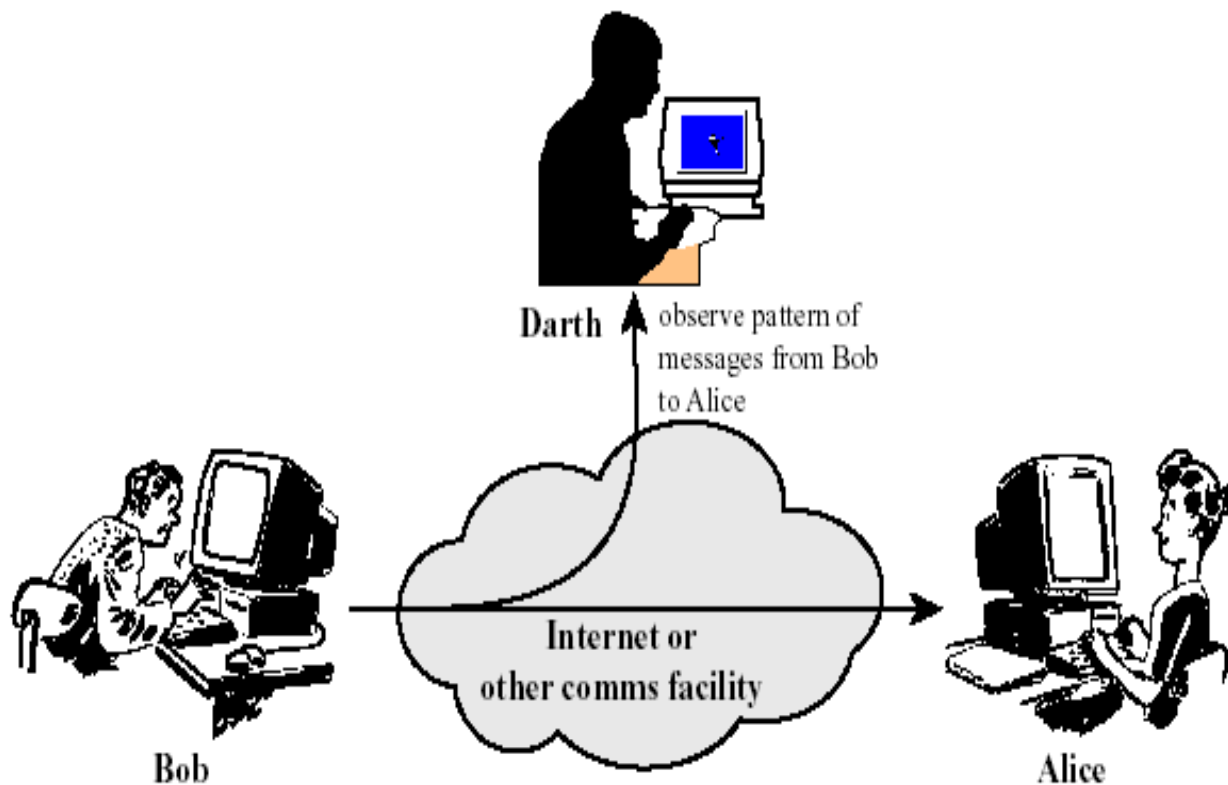
# Passive Attacks



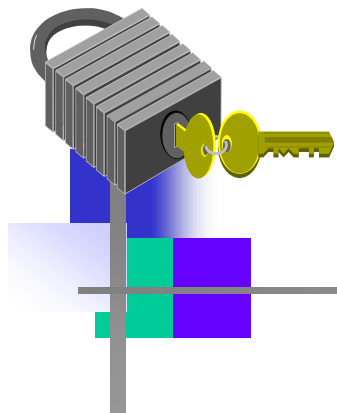
(a) Release of message contents



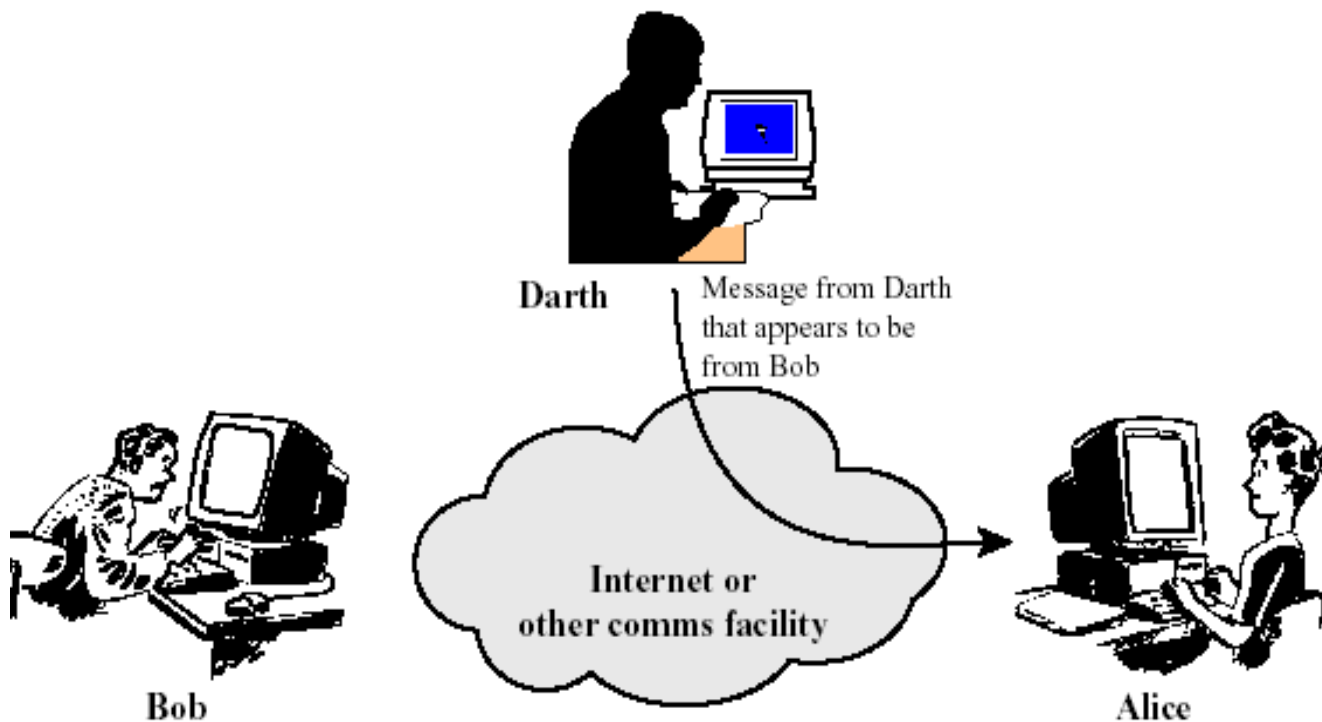
# Passive Attacks



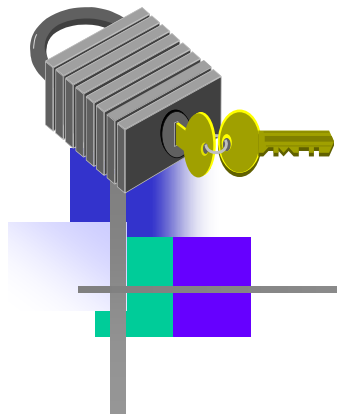
(b) Traffic analysis



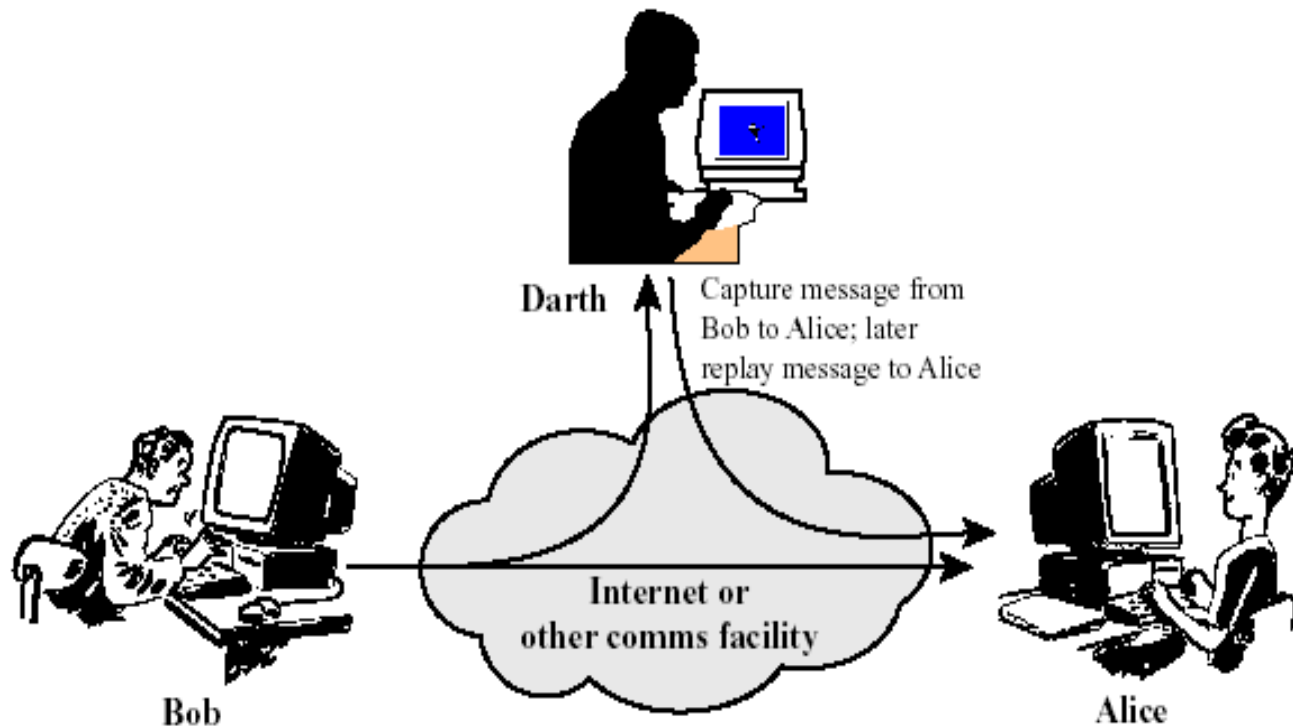
# Active Attacks



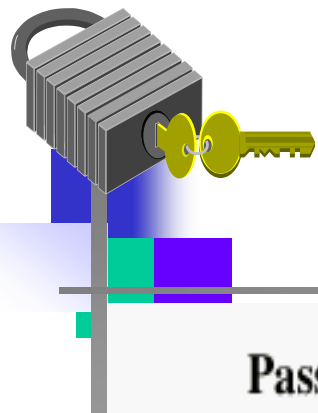
(a) Masquerade



# Active Attacks



(b) Replay



# Summary of Passive and Active Threats

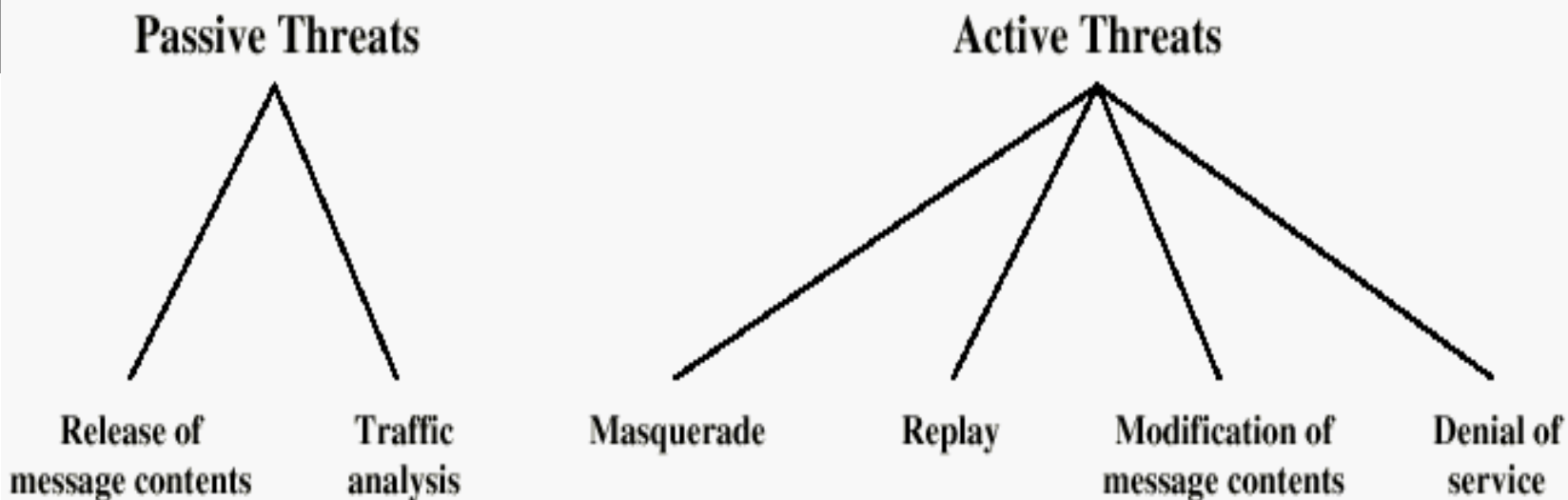


Figure 1.2 Active and Passive Security Threats



# Outline of Course

---

- Part One - Introduction
- Part Two-Use of Cryptographic algorithms and security protocols to provide security over the Internet. Topics include: key management, authentication, as well as transport-level, wireless, email and IP security
- Part Three-Deals with security facilities to protect against threats, including intruders, viruses and worms.