Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

Course Overview (cont)

CSU Cybersecurity Center
Computer Science Dept

Today

- Security Architecture
- Key terms
- Access control and authentication

Course Outline 6

Risk mitigation

Reducing the breach likelihood, Reducing the breach cost.

Security Economics, Security investment ROI, Attack surfaces and connectivity, Threat containment strategies and their effectiveness.

Emerging topics

Vulnerability markets: Legitimate (for example rewards programs), Gray (vulnerability brokers) and black markets, Potential buyers and sellers of Zero-day vulnerabilities and exploits

People: Well known Vulnerability finders/cyber criminals

Assignments/Readings/Discussion

- Almost every weekend there will be an on-line quiz on canvas. Available Fri 8 PM, due Mon 11 PM.
- There may be some embedded questions during the lectures.
- Some assignments will involve reading some articles (assigned/found) and discussing them
  - May involve looking up background and recent developments
  - Look for a quiz and an assignment late Fri this week.

Term Project

- Term project: You will choose a topic from a given list. Other topics may be permitted by the instructor. Need to be aligned with the objectives of the class.
- Project will involve
  - Preliminary research to identify the sources of information and the topic/problem to be investigated.
  - Proposal (9/30), Progress report (10/28), Final report (12/9)
    - At least some original ideas
    - Presentations required
  - Presentations and discussions are required
  - Peer reviews and comments needed

Extra credit project?

Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS 559

Security System Architecture

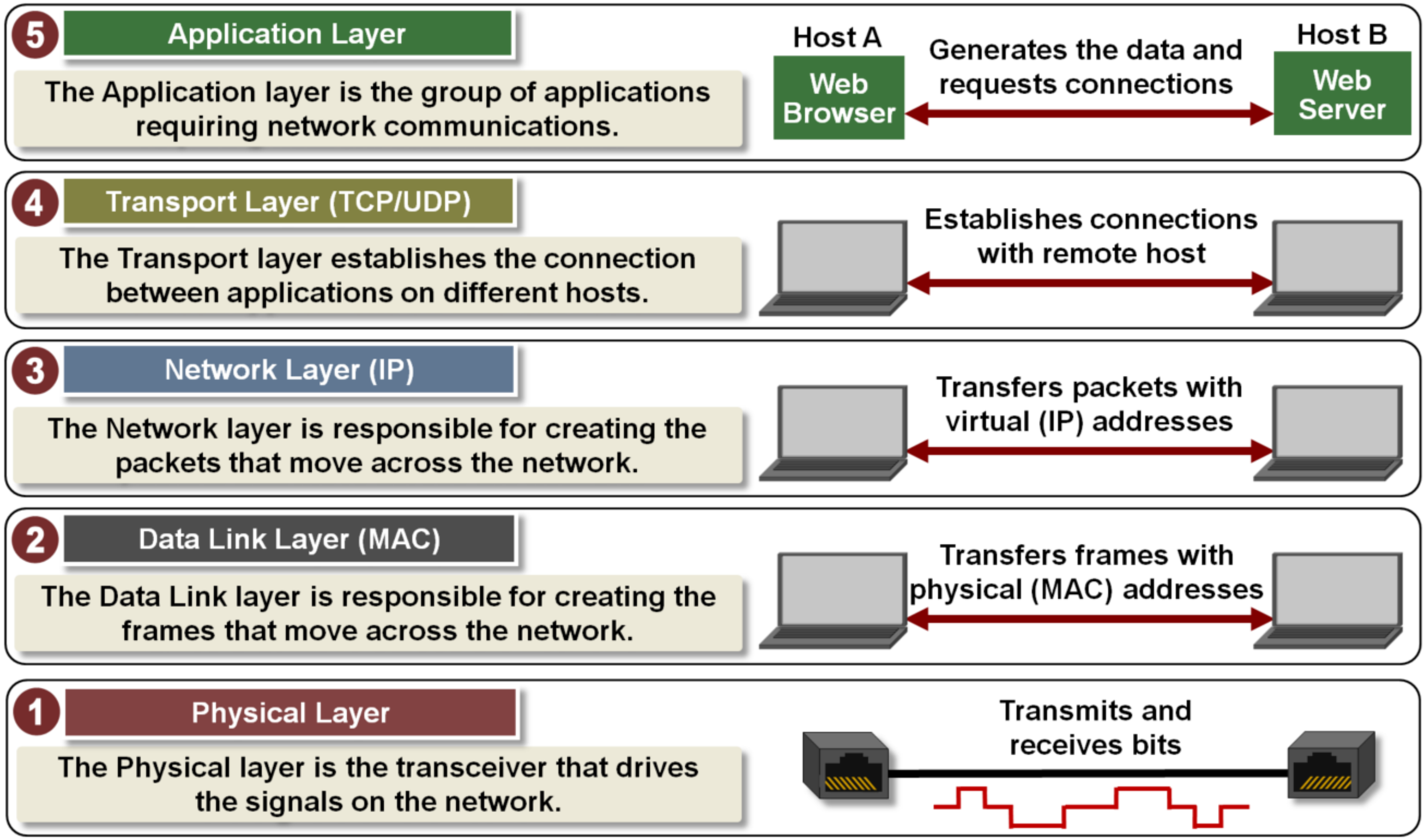
CSU Cybersecurity Center
Computer Science Dept

Security System Architecture

- Networked systems
  - Use of firewalls
- Single computing System: OS
  - Isolation of processes, cgroups, virtual machines

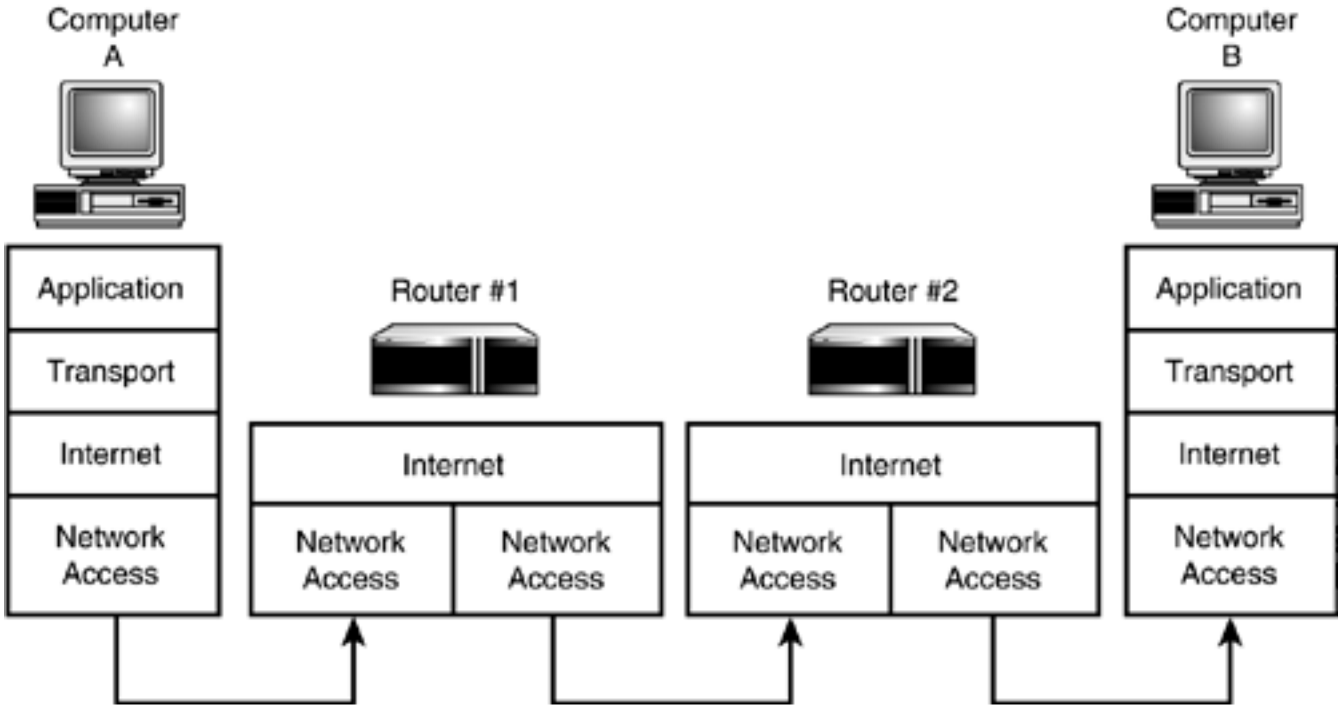
Internet: IP, TCP

- Networking protocols have multiple layers.


5
Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4
Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3
Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2
Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1
Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits

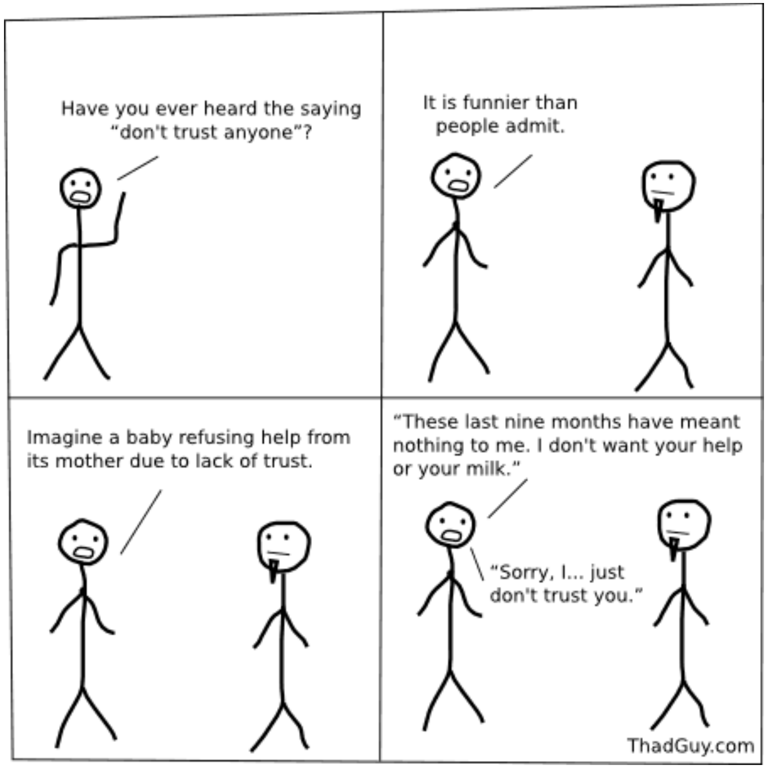
https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

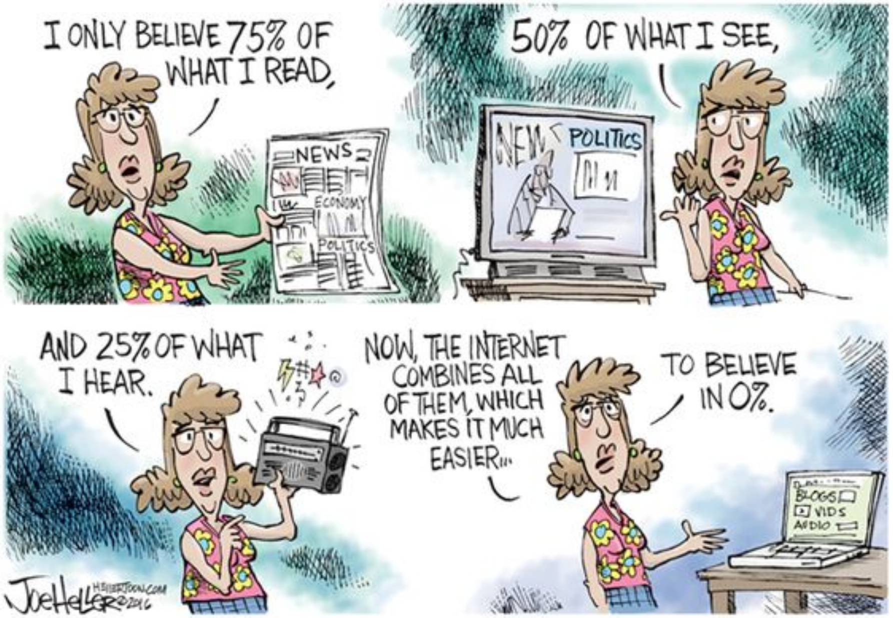
Internet architecture



https://www.yaldex.com/tcp_ip/FILES/06fig07.gif

Trusted and Untrusted Actors

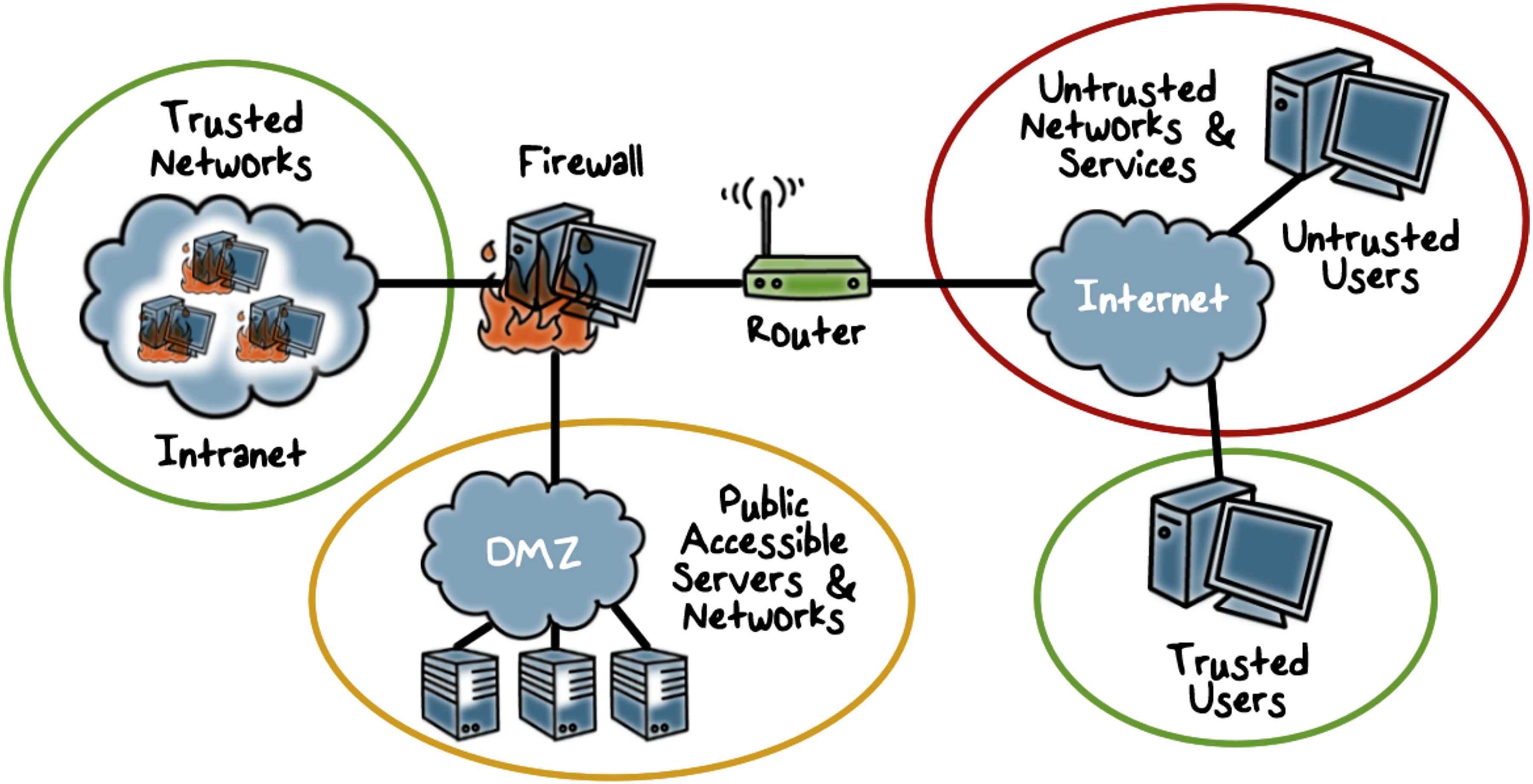

Have you ever heard the saying "don't trust anyone"?
It is funnier than people admit.
Imagine a baby refusing help from its mother due to lack of trust.
"These last nine months have meant nothing to me. I don't want your help or your milk."
"Sorry, I... just don't trust you."
ThadGuy.com


I ONLY BELIEVE 75% OF WHAT I READ,
NEWS
ECONOMY
POLITICS
50% OF WHAT I SEE,
NEWS
POLITICS
AND 25% OF WHAT I HEAR.
NOW, THE INTERNET COMBINES ALL OF THEM, WHICH MAKES IT MUCH EASIER...
TO BELIEVE IN 0%.
BLOGS
VIDS
AUDIO
JoeHeller HellerToon.com ©2016

forbes.com/cartoons

A binary trusted/untrusted classification is an approximation.

Firewalls



DMZ: “Demilitarized zone”, distributed firewalls, From Georgia Tech
Note multiple levels of trust.

Firewalls

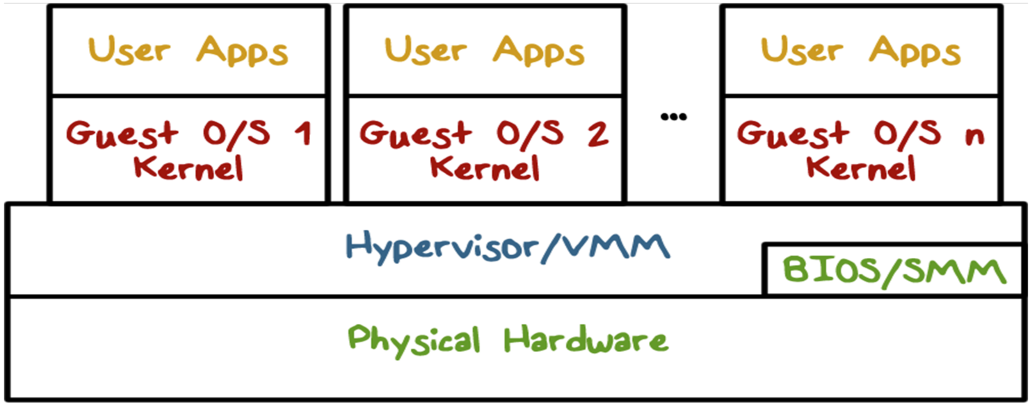
- A firewall checks traffic (packets or sessions) passing through it
- Can be programmed to check address ranges (IP addresses, ports), protocols, applications and content types.
- Can provide address translation, encryption

Operating System

- The operating system serves as as trusted computing base (TCB) that controls access to protected resources.
  - Must establish the source of a request for a resource (authentication is how we do it)
  - Authorization or access control
  - Mechanisms that allow various policies to be supported
- How
  - Hardware support for memory protection
  - Processor execution modes (system and user modes)
  - Privileged instructions - can only be executed in system mode
  - System calls - transfer control between user and system code

Isolation in a system

- OS isolates address spaces of different processes using address translation. Also data vs code isolation.
  - Page tables governed by OS.
- In virtualization, hypervisor isolates virtual machines.
- Containers (Docker): Linus cgroups isolate process groups.



Colorado State University

Summary

Security must be a consideration in a

- Networked system
- Operating Systems
- Security protocols, cryptography (later)

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Terminology

CSU Cybersecurity Center
Computer Science Dept

Key Security Attributes

INTEGRITY
INFORMATION SECURITY
CONFIDENTIALITY
AVAILABILITY

Confidentiality: Preserving authorized restrictions on information access and disclosure,

- including means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper information modification or destruction. Can be considered to include

- **Authenticity**: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Non-repudiability/Accountability**: requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action. recovery and legal action.

Availability

Ensuring timely and reliable access to and use of information.

Computer security : Principles and Practice, William Stallings, Lawrie Brown

Key Security Attributes: losses

The **CIA Triad** provides a classification of the types of security losses:

- Confidentiality: A loss of confidentiality is the unauthorized disclosure of. information.
- Integrity: A loss of integrity is the unauthorized modification or destruction of information.
- Availability: A loss of availability is the disruption of access to or use of information or an information system.

Questions:

Why is availability a security attribute?

What about non-repudiability?

Adversary, Attack, Countermesure

Adversary (threat agent): Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Attack types

- Passive – attempt to learn or make use of information from the system that does not affect system resources
- Active – attempt to alter system resources or affect their operation
- Insider – initiated by an entity inside the security parameter
- Outsider – initiated from outside the perimeter

Countermeasure: A device or techniques that has as its objective the impairment of operational effectiveness of undesirable or adversarial activity, or prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

RFC 2828, Internet Security Glossary

Assets, Risk, Threat, Vulnerability

System Resource (Asset): A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

- To be studiesd in detail.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

RFC 2828, Internet Security Glossary

Assets, Risk, Threat, Vulnerability

System Resource (Asset): what needs protection by the defenders.

Risk: A measure of the adverse impacts and the likelihood of occurrence.

Threat: potential attempts by an adversary.

Vulnerability: Weakness in an information system that may be exploited.

Note of caution: In pre-cyber-security days, classical risk literature used the term vulnerability with a different meaning.

RFC 2828, Internet Security Glossary

Assets and threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

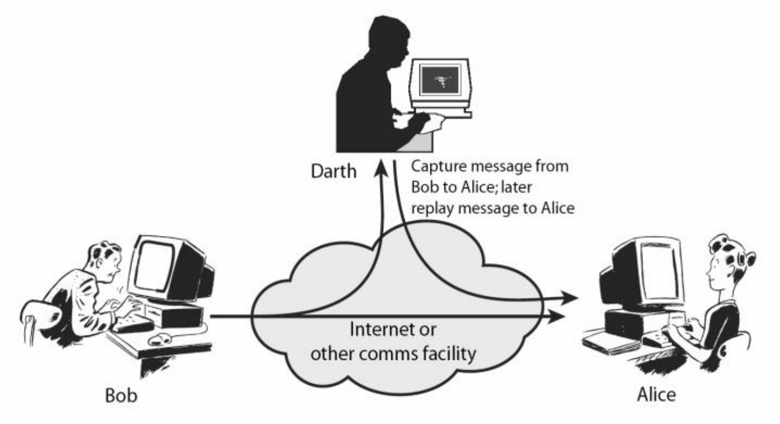
Question: where does ransomwere fit? Viruses?

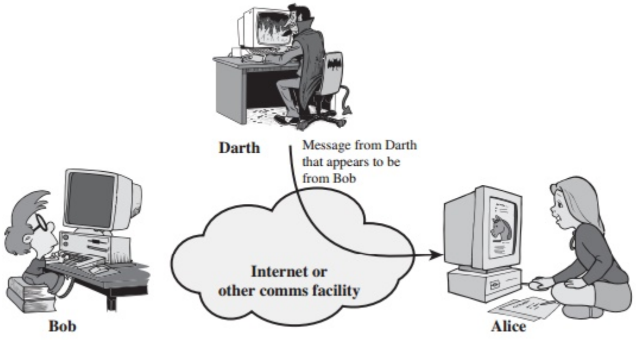
Computer security : Principles and Practice, William Stallings, Lawrie Brown

Attacks

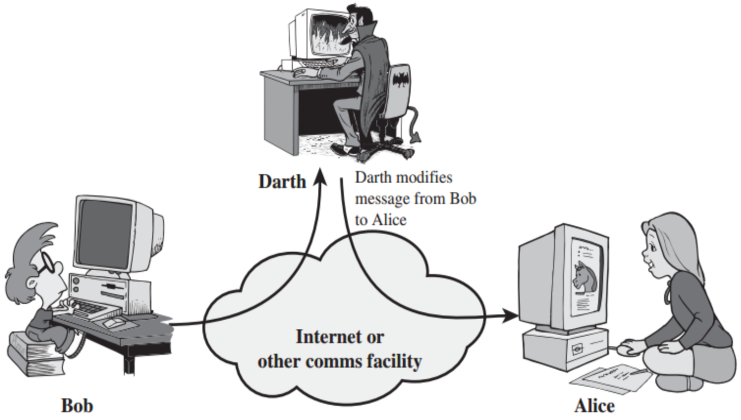
Passive Attack	Active Attack
• Attempts to learn or make use of information from the system but does not affect system resources • Eavesdropping on, or monitoring of, transmissions to obtain information that is being transmitted • Two types: • Release of message contents • Traffic analysis	• Attempts to alter system resources or affect their operation • Involve some modification of the data stream or the creation of a false stream • Four categories: • Replay • Masquerade • Modification of messages • Denial of service

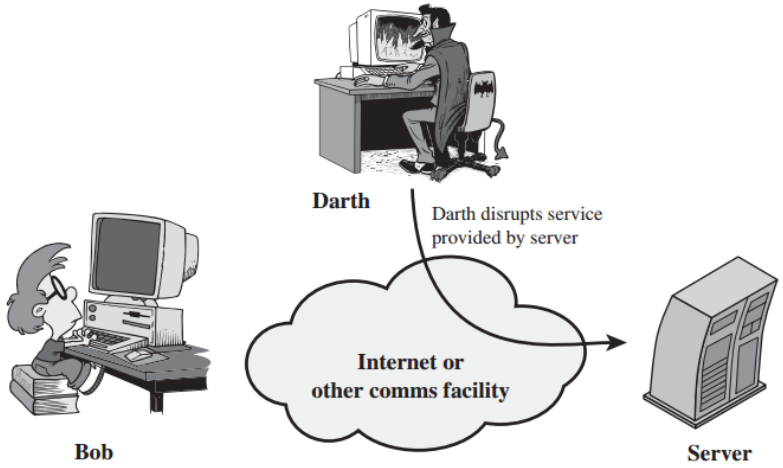
Alice and Bob Diagrams


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

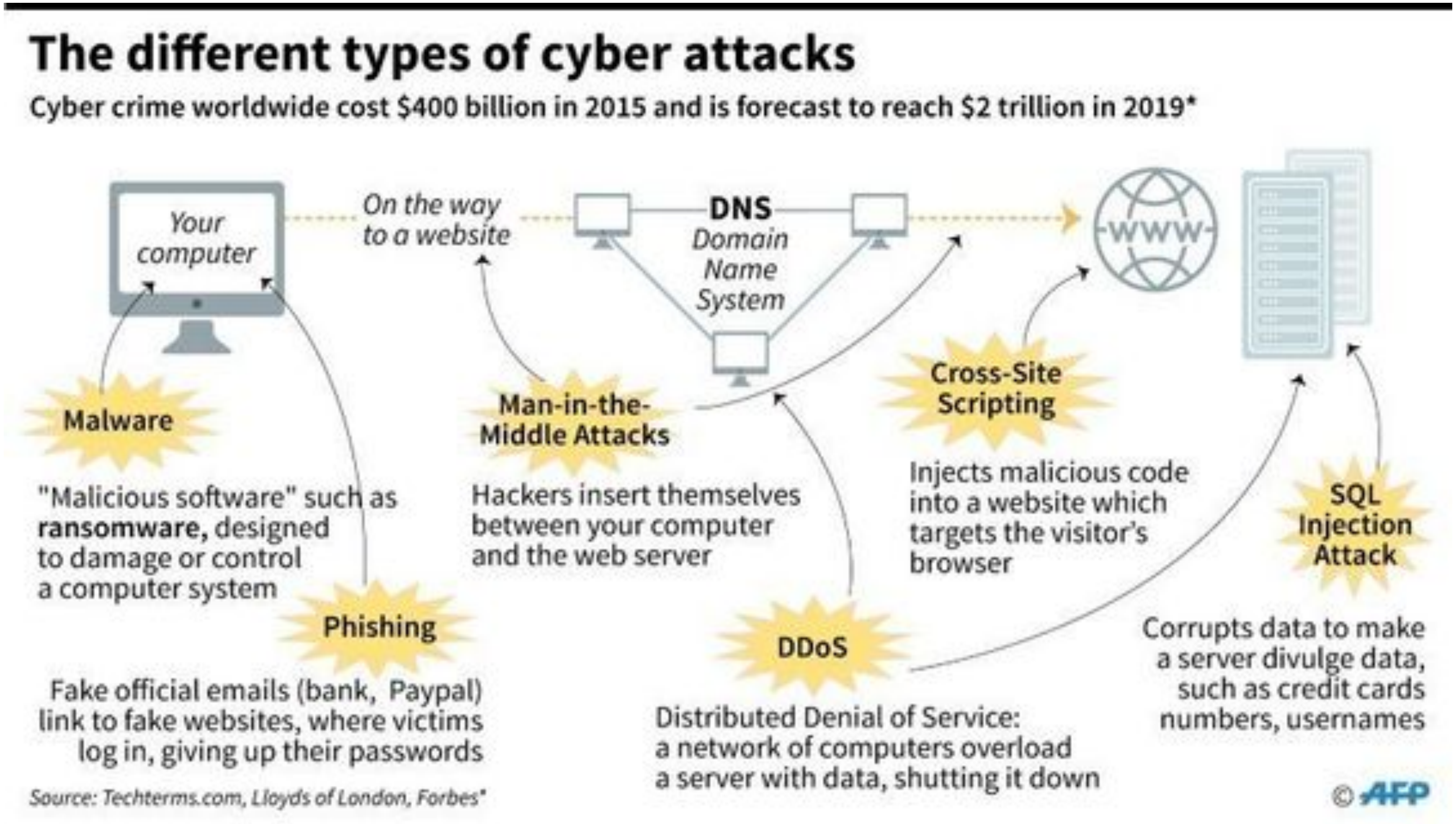
(a) Masquerade


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

History: Rivest, Shamir, and Adleman's 1978 article "A method for obtaining digital signatures and public-key cryptosystems”.

Cyber attack types



The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*

Malware

"Malicious software" such as **ransomware,** designed to damage or control a computer system

Phishing

Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Man-in-the-Middle Attacks

Hackers insert themselves between your computer and the web server

DDoS

Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Cross-Site Scripting

Injects malicious code into a website which targets the visitor's browser

SQL Injection Attack

Corrupts data to make a server divulge data, such as credit cards numbers, usernames

Source: Techterms.com, Lloyds of London, Forbes*

© AFP

Attack Surfaces

Surfaces: where the "holes" might be.

Network attack surface: vulnerabilities over an enterprise network, wide-area network, or the Internet.

- Including network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.

Software attack surface: vulnerabilities in application, utility, or operating system code.

- Web server, browser, Operating System.

Human attack surface: vulnerabilities in the personnel behavior

- social engineering, human error, and trusted insiders

Malware

- Malware ("malicious software"):
  - a catch-all term for any type of malicious software,
  - regardless of how it works, its intent, or how it's distributed.
- Virus
  - a specific type of malware that self-replicates by inserting its code into other programs. Types:
  - The **file infector** can burrow into executable files and spread through a network. A file infector can overwrite a computer's operating system or even reformat its drive.
  - The **macro virus** takes advantage of programs that support macros. Macro viruses usually arrive as Word or Excel documents attached to a spam email, or as a zipped attachment.
  - **Polymorphic viruses** modify their own code. The virus replicates and encrypts itself, changing its code just enough to evade detection by antivirus programs.

https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/malware-vs-viruses.html

Malware: Functional types

- **Worm:** a standalone program that can self-replicate and spread over a network. Unlike a virus, a worm spreads by exploiting a vulnerability in the infected system or through email as an attachment masquerading as a legitimate file.
- **Ransomware**: demands that users pay a ransom—usually in bitcoin or other cryptocurrency—to regain access to their computer.
- **Scareware**: attempts to frighten the victim into buying unnecessary software or providing their financial data.
- **Adware and spyware**: Adware pushes unwanted advertisements at users and spyware secretly collects information about the user. Spyware may record the websites the user visits, information about the user's computer system and vulnerabilities for a future attack, or the user’s keystrokes.
  - Spyware that records keystrokes is called a keylogger.
- **Fileless malware**: Unlike traditional malware, fileless malware does not download code onto a computer, so there is no malware signature for a virus scanner to detect. Instead, fileless malware operates in the computer's memory and may evade detection by hiding in a trusted utility, productivity tool, or security application.

https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/malware-vs-viruses.html

In-Class Quiz

- Record the date, question number and answer you chose. You will need to use that in the weekend quiz.
- Q1: The terms risk, threat and vulnerability, as we use in this class ..

A. They all mean the same thing

B. Threat and vulnerability mean the same thing

C. Risk and threat mean the same thing

D. None of the above

Record answer in 15 seconds

Colorado State University

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Access Control

CSU Cybersecurity Center
Computer Science Dept

Access Control

Definition according to RFC 4949:

> “a process by which use of system resources is regulated according to a security policy and is permitted only by **authorized entities** (*users, programs, processes, or other systems*) according to that policy”

RFC 4949 defines security as

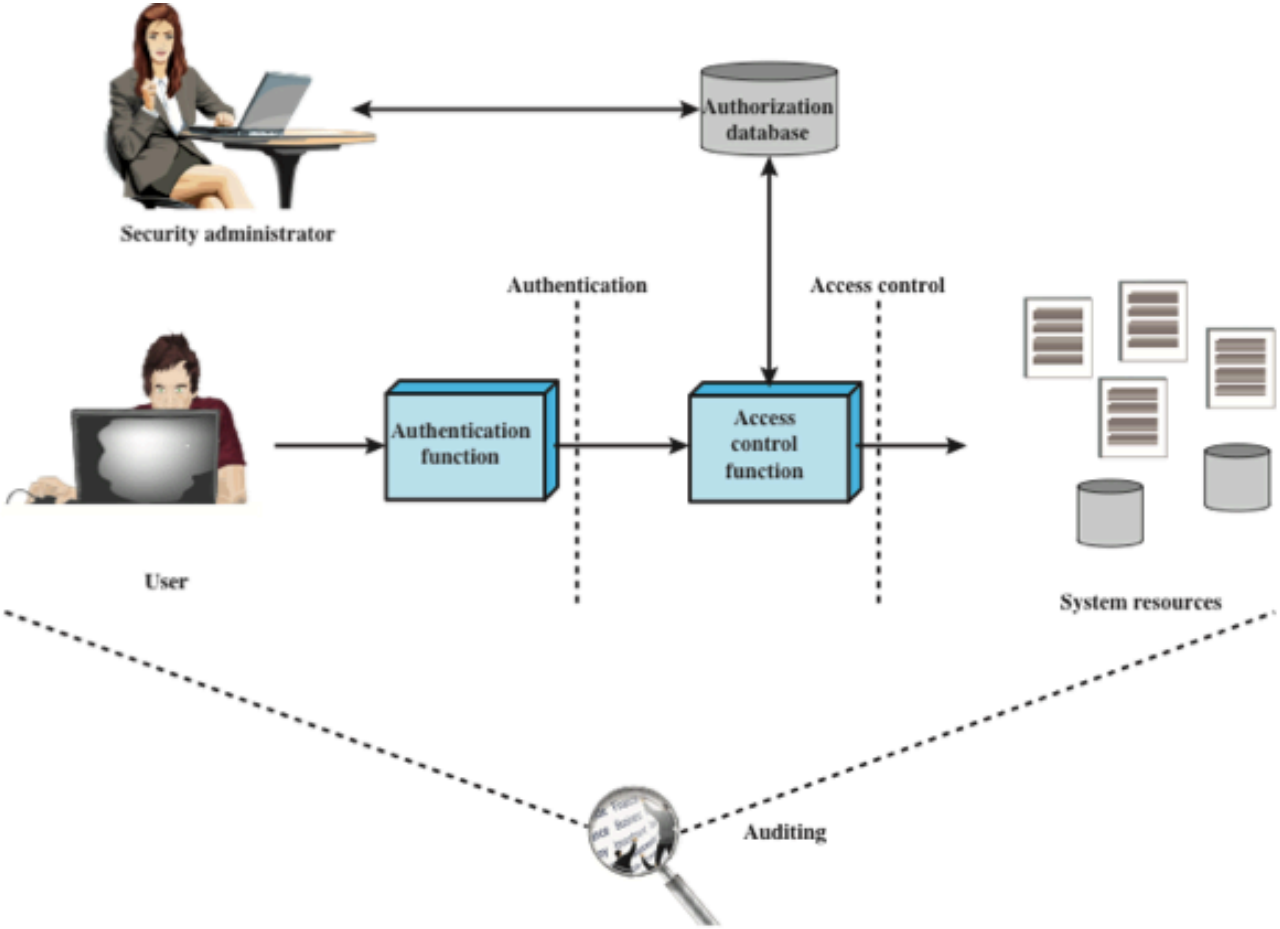
> “measures that implement and assure security services in a computer system, particularly those that assure access control service”

Thus all of computer security is concerned with access control.

Enforced by the Trusted Computing Base (OS) which performs

- authentication
- authorization

Access Control as a Security Function



Subjects, Objects, and Access Rights

- A **subject** is an entity capable of accessing objects.
  - represented by a process. A user/application gains access to an object by means of a process that represents that user/application. The process takes on the attributes of the user, such as access rights.
  - Held accountable for the actions.
  - Classes: Owner (u in linux), Group (g), World (o), people with specific roles
- An object is a resource to which access is controlled.
  - an entity used to contain and/or receive information.
  - Examples: pages/segments, files/directories/programs, ports, devices etc.

Subjects, Objects, and Access Rights

An access right describes the way in which a subject may access an object.

- **Read**: User may view information in a system resource (e.g., a file, selected records in a file, selected fields within a record, or some combination). Read access includes the ability to copy or print.
  - Directory: ability to list the directory.
- **Write**: User may add, modify, or delete data in system resource (e.g., files, records, programs). Write access includes read access.
  - Directory: create new files
- **Execute:** User may execute specified programs.
  - Directory: enter it to access the files within it.

- Delete: User may delete certain system resources, such as files or records.

- Create: User may create new files, records, or fields.

- Search: User may list the files in a directory or otherwise search the directory.

Colorado State University

Access Control Schemes

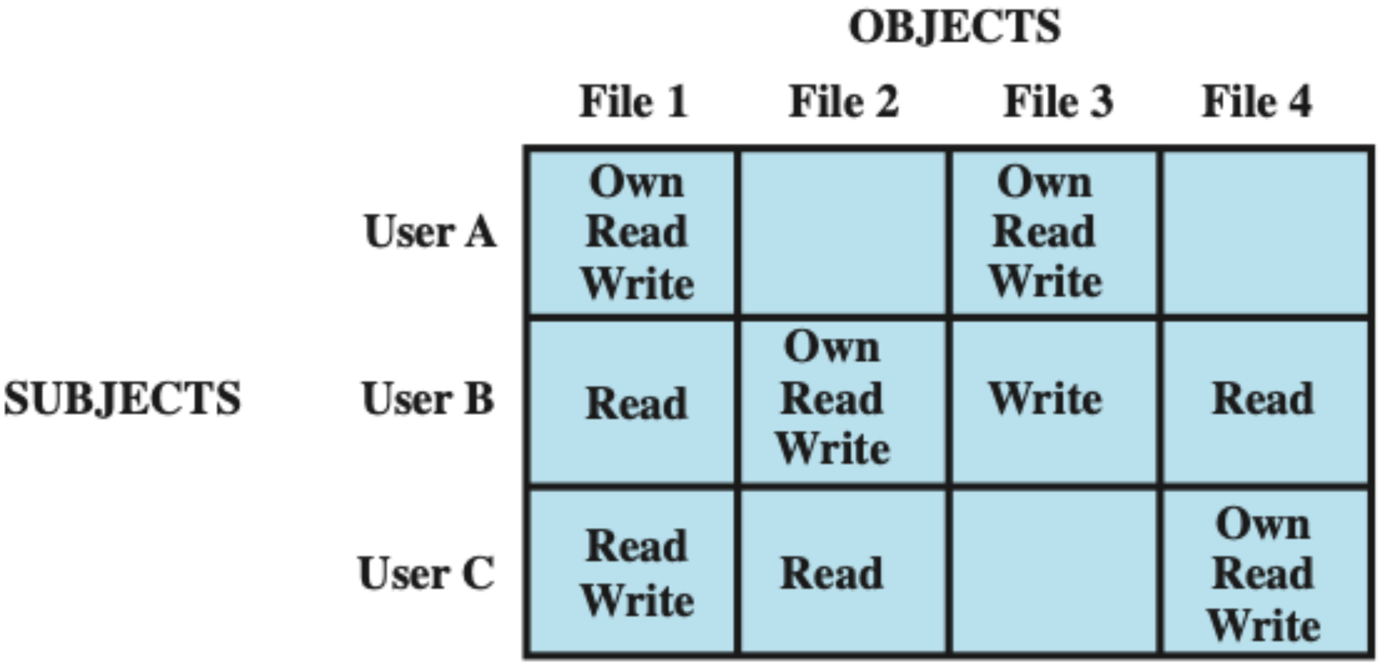
Discretionary Access Control (DAC): Scheme in which an entity may be granted access rights that permit the **owner** entity, by its own violation, to enable another entity to access some resources.

- Provided using an access matrix

Mandatory Access Control: **Centralized authority** sets security policy for all resources

- Example: SELinux

Example: Access Control Matrix



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Access Control List (ACL): Every object has an ACL that identifies what operations subjects can perform. Each access to object is checked against object's ACL.

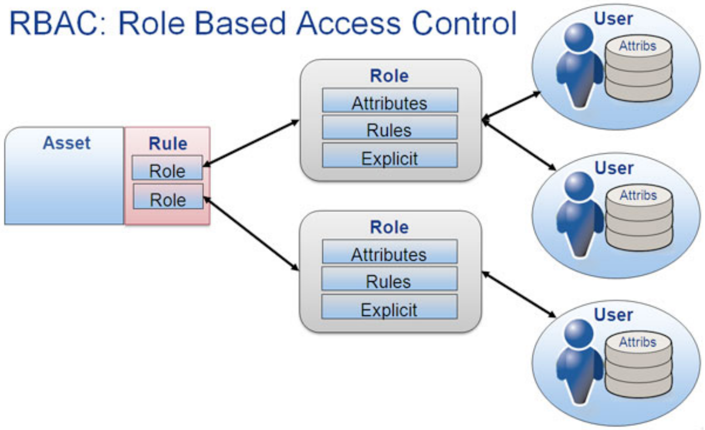
May be kept in a relational database. Access recorded in file metadata (inode).

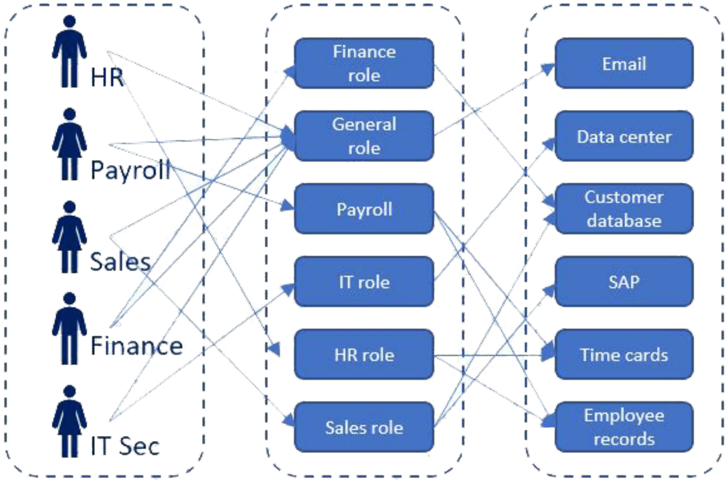
Unix Access Control

- Subjects (Who?)
  - Users
- Objects (What?)
  - Files, directories
  - Files: sockets, pipes, hardware devices, kernel objects, process data
- Access Operations
  - Read, Write, Execute
  - Set by root or owner of the object
- Linux is an example of *discretionary access control*.
  - Resource owners can set the security policy for objects they own
- Superuser (root) allowed to do anything.
  - System administrators assume superuser role to perform privileged actions – Good practice to assume superuser role only when necessary

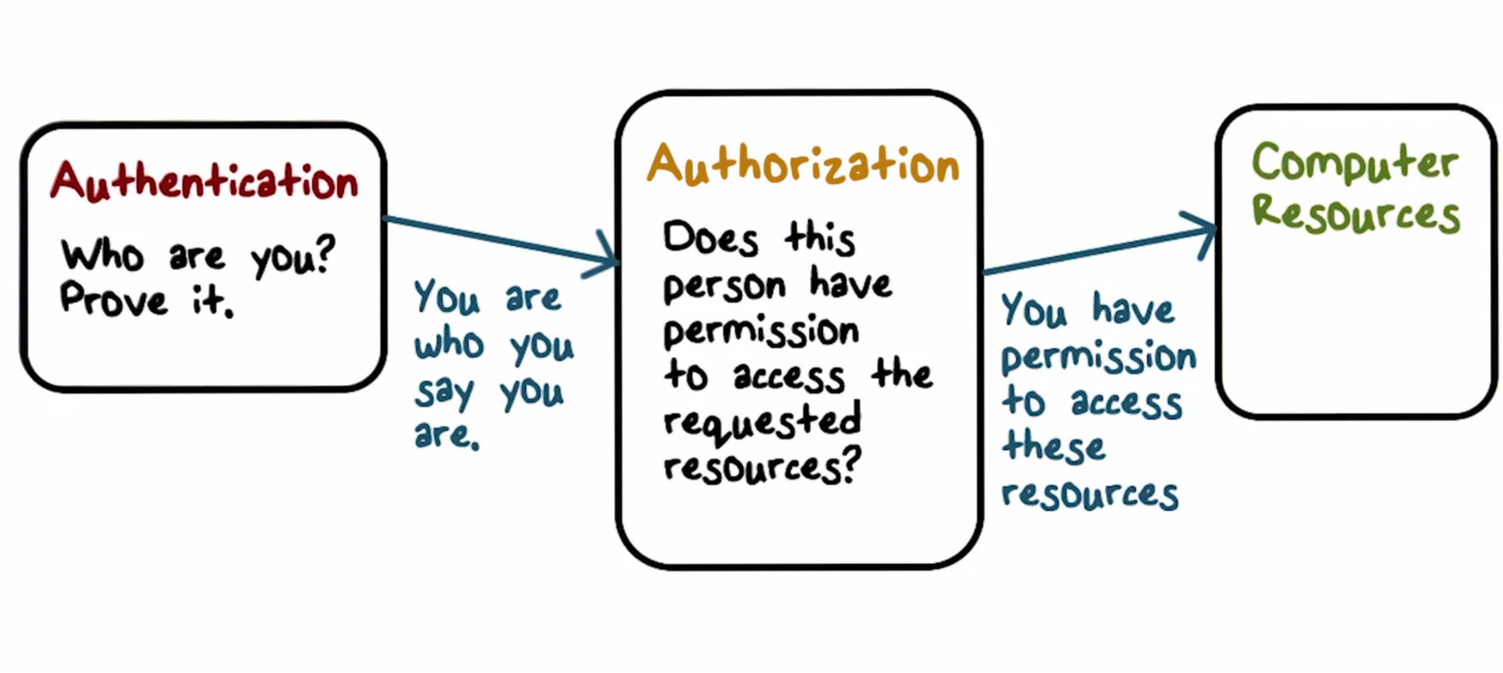
Role Based Access Control (RBAC)

- **Role-based access control (RBAC):** based on the roles that users have within the system and on rules specifying the accesses are allowed to users in given roles.
- Widely used commercially in larger organizations.





Authentication


Authentication
Who are you? Prove it.
You are who you say you are.
Authorization
Does this person have permission to access the requested resources?
You have permission to access these resources
Computer Resources

Georgia Tech

Authentication

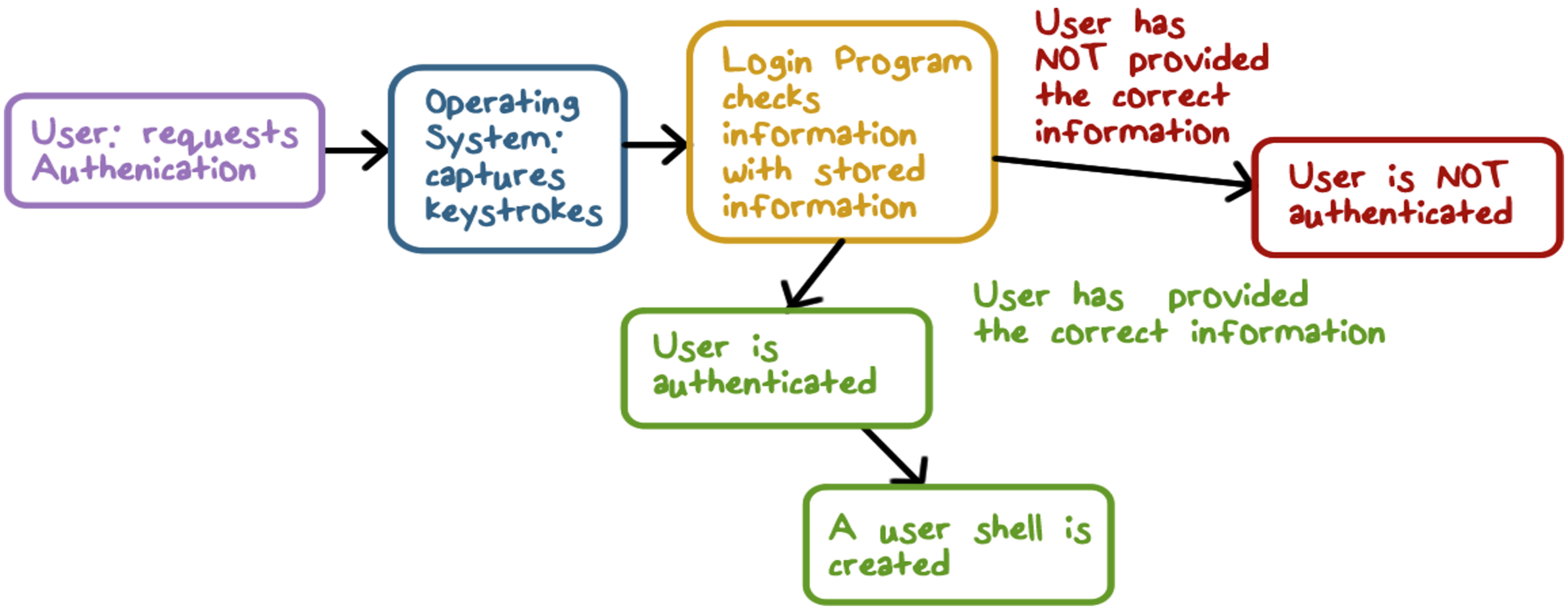
- OS (TCB) needs to know who makes a request for a protected resource
- A process that makes the request does it on behalf of a certain user
- Authentication handles the question: on whose behalf the requesting process runs?
- Involves
  - claims about an identity and
  - verification of the claimed identity
- Goals
  - No false negatives
  - No false positives (major consideration)

Colorado State University

Authentication Methods

- Something a user knows
  - password
- Something a user has
  - Ex. Id card
- Something a user is
  - Biometric (face or fingerprint)
- Can be multifactor to reduce false positives

Implementation


User: requests Authenication
Operating System: captures keystrokes
Login Program checks information with stored information
User has NOT provided the correct information
User is NOT authenticated
User has provided the correct information
User is authenticated
A user shell is created

The system must provide a trusted path from keyboard to the OS.

Georgia Tech

Password authentication

Possible approaches

1. Store a list of passwords, one for each user in the system file, readable only by the root/admin account
   - Why the admin need to know the passwords?
   - If security is breached, the passwords are available to an attacker. No longer used.
2. Do not store passwords, but store something that is derived from them
   - Use a hash function and store the result
     - More about that later
   - The password file is readable only for admin

Security Challanges

- Password guessing
  - List of bad passwords. 123456, password, ..
- Brute force guessing
  - more later
- Good passwords are the ones harder to remember
- May be stolen using
  - keyloggers,
  - compromised websites where same password was used
  - eavesdropping *(Alice, Bob and Eve?)*

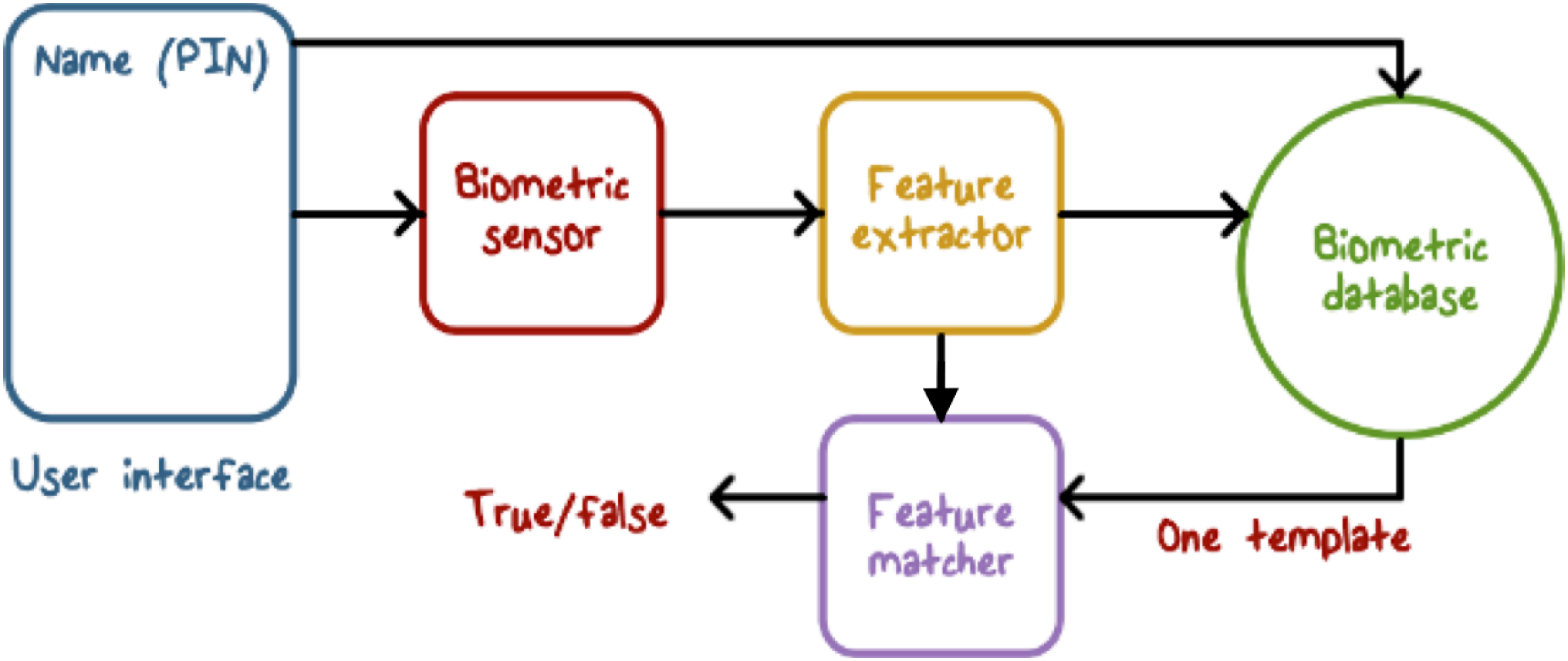
Biometric Authentication

- Fingerprints (finger swipes)
- Keystroke dynamics
- Voice
- Retina scans

Issues

- Feature value distribution or a range
- False positives and negatives

Implementing Biometric Authentication



Summary

Access control

- Who can access what
- Authentication