SECURITY IN COMPUTING, FIFTH EDITION

Review – introduction & toolbox

CISC 3325 - Information Security

- Tzipora Halevi, Assistant Professor
  email: halevi@cis.brooklyn.cuny.edu
  Office Hours: Mondays, 2:30 - 4:30pm
  Ingersol room 2156A
- Book:
  - Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, Security in Computing, 5th edition, Prentice Hall imprint, Pearson Education, Inc., 2015

What Is Computer Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data
- What is the value of the assets?
  - Is the asset easily replaced?
    - Cost of replacement.
  - Is the asset unique?

What is Computer Security?

- Traditionally, computers are protected against:
  - Theft/damage to hardware
  - Theft/damage to information
  - Disruption of service

Growing Importance of Computer Security

- Increasing reliance on computer systems and the Internet
- Use of wireless networks such as Bluetooth and Wi-Fi
- Expanding array of smart devices
  - and ‘Internet of Things’ (IoT) devices

Why is computer security important?

- Attacks Impact everyone's day-to-day life
  - Millions of compromised computers
  - Millions of stolen passwords
    - Risk of identity theft
- Serious financial damage caused by security breaches

How can we help?

- Security education can help us
  - Avoid attacks
  - Create safer systems
- We start by defining risk management

Risk Management

- High-level goals of computer security:
  - identification, evaluation, prioritization of risks
    - Defined as a threat model
    - Estimate the effects of uncertainty
  - Not perfect protection
  - Efforts concentrate on making it harder to attack
    - Finding ways to spend time & money efficiently
    - minimize the probability or impact of unfortunate events

Threat Model

- Key notion of threat model:
  - what/who are you defending against?
    - Determines which defenses to consider
      - E.g., where are valuable assets stored, where is the system most vulnerable to attacks, etc.

How to protect from loss, destruction and illegal access

- Identify vulnerabilities – weaknesses that can be exploited to cause harm
- Monitor for threats – methods or situations that can cause harm
- Recognize an attack that exploits the vulnerabilities
- Take countermeasures or use methods to control an attack

Computer Security

- To protect computer systems, you must know your enemy
- Security is not about perfection: it’s about defenses that are good enough to stop the threats you’re likely to encounter

FUNDAMENTAL CONCEPTS

Computer Network

- A digital telecommunications network which allows nodes to share resources
- Networked computing devices exchange data with each other using a data link
- The connections between nodes are established using either cable media or wireless media

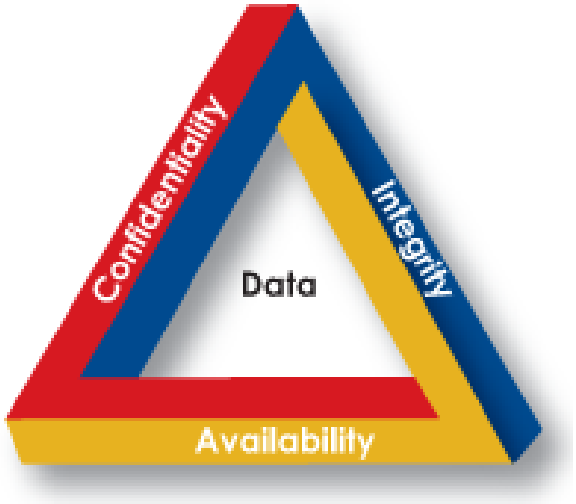
https://nizamtaher.wordpress.com/topics/topic-1-introduction-of-computer-network/

Cyber Vulnerabilities

- **Vulnerability** is a cyber-security term that refers to a flaw in a system that can leave it open to attack.
- A **vulnerability** may also refer to any type of weakness in a computer system itself
  - Either in a set of procedures, or in anything that leaves information security exposed to a threat
- Cutting down vulnerabilities provides fewer options for malicious users to gain access to secure information.

https://www.techopedia.com/definition/13484/vulnerability
http://blog.escanav.com/2014/06/vulnerabilities-recorded-by-us-cert-cyber-security-bulletin/

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (C.I.A.)



Confidentiality

- Avoidance of the unauthorized disclosure of information
  - Protect data, keep information secret
  - Provide access only to authorized users

Tools to ensure confidentiality

- Encryption:
  - Information encrypted using a secret key
  - Transformed info can be read using decryption key
    - Info essentially can not be read without this key
- Access Control:
  - Policies that limit access to confidential info
    - To people/systems with a “need to know”
    - May be based on person’s id, name or his role

Tools to ensure confidentiality (cont.)

- Authentication:
  - Process of confirming someone's ID or role
  - Maybe based on:
    - Something that the person has
      - Smart card, radio key, etc.
    - Something the person knows:
      - Password, etc
    - A physical trait of a person:
      - Fingerprints, etc.

Authentication Vs. Identification

- These are two different concepts
- **Identification:**
  - **T**he act of asserting who a person is.
- **Authentication**
  - **T**he act of proving that asserted identity that the person is who she says she is

Tools to ensure confidentiality (cont.)

- Authorization:
  - Is the person allowed access to the info?
    - Based on access control policy
  - Mechanism should be secure, prevent an attacker from tricking the system and gaining unauthorized access
- Physical Security:
  - Physical barriers that limit access to protected info
    - Such as locks, cabinets, doors.
    - Placing a computer in a windowless room.
    - Building a Faraday cage to prevent electromagnetic signals
      - To prevent side-channel attacks

Integrity

- Ensure information has not been altered in an unauthorized way
- Information may be compromised maliciously or by accident
  - Through hard drive crashes
  - Through a computer virus

Tools to protect integrity

- Regular backups
- Checksums:
  - Map the content to a numerical value and save that value
  - Read it back upon reading the information
- Data correcting codes:
  - Store data in such a way that small changes can be easily detected
    - and corrected
- The above tools all use redundancy
  - Replication of some of the information content or content

Availability

- Information is available when it is needed
  - Accessible and modifiable
    - to those authorized to do so
- Tools for ensuring availability:
  - Physical protections:
    - housing that can withstand unexpected situations
      - Such as earthquakes, storms, etc.
      - Powered with generators
  - Computational redundancies:
    - Extra disks or web servers, such that failure of a single device will not degrade availability of data

C-I-A Triad - Summary

- Confidentiality – only those individuals or accounts who have permission can access a system.
- Integrity – a system or account can be altered only by authorized users
- Availability – a system/account is available when expected

C-I-A Triad - Summary

- Sometimes two other desirable characteristics:
  - Authentication:
    - Ability of a system to confirm the identity of a sender
  - Nonrepudiation or accountability:
    - The ability of a system to confirm that a sender cannot convincingly deny having sent something

Types of threats

- Interception
  - the asset or data is accessed by someone other than the intended receiver
- Interruption
  - the asset or data is not available
- Modification
  - an unauthorized change is made
- Fabrication
  - false information is installed

Types of Threads vs. CIA Triad

- Interception:
  - Threat to confidentiality
    - Attacker can see data
- Interruption
  - Threat to availability
- Modification and fabrication
  - Threat to data integrity

Threats and Attacks

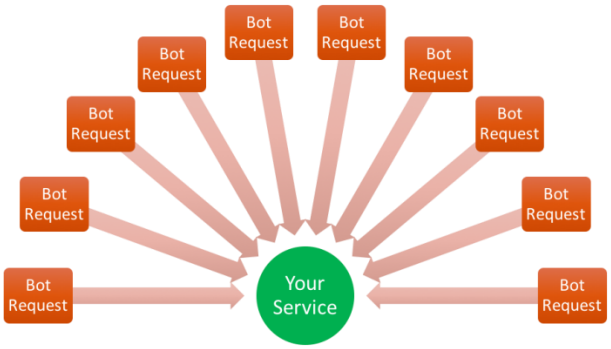
- Eavesdropping: interception of information during transmission
  - Includes side channel attacks
  - May be audio, electromagnetic, power, etc.

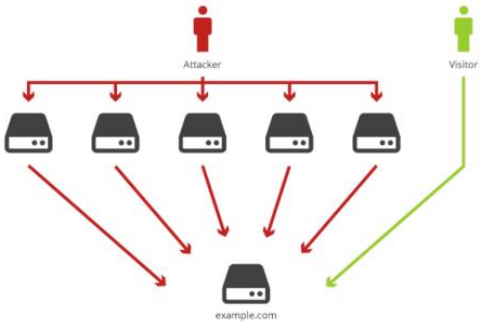
- Alteration: unauthorized modification of information
  - False information may be installed

http://blog.jammer-store.com/2011/09/cell-phone-spying-with-eavesdropping-trojan-danger/

Threats and Attacks (cont.)

- Denial-of-service: interruption or degradation of data or information
  - This is an attack on availability
  - For example, email spam, which fills the mailbox



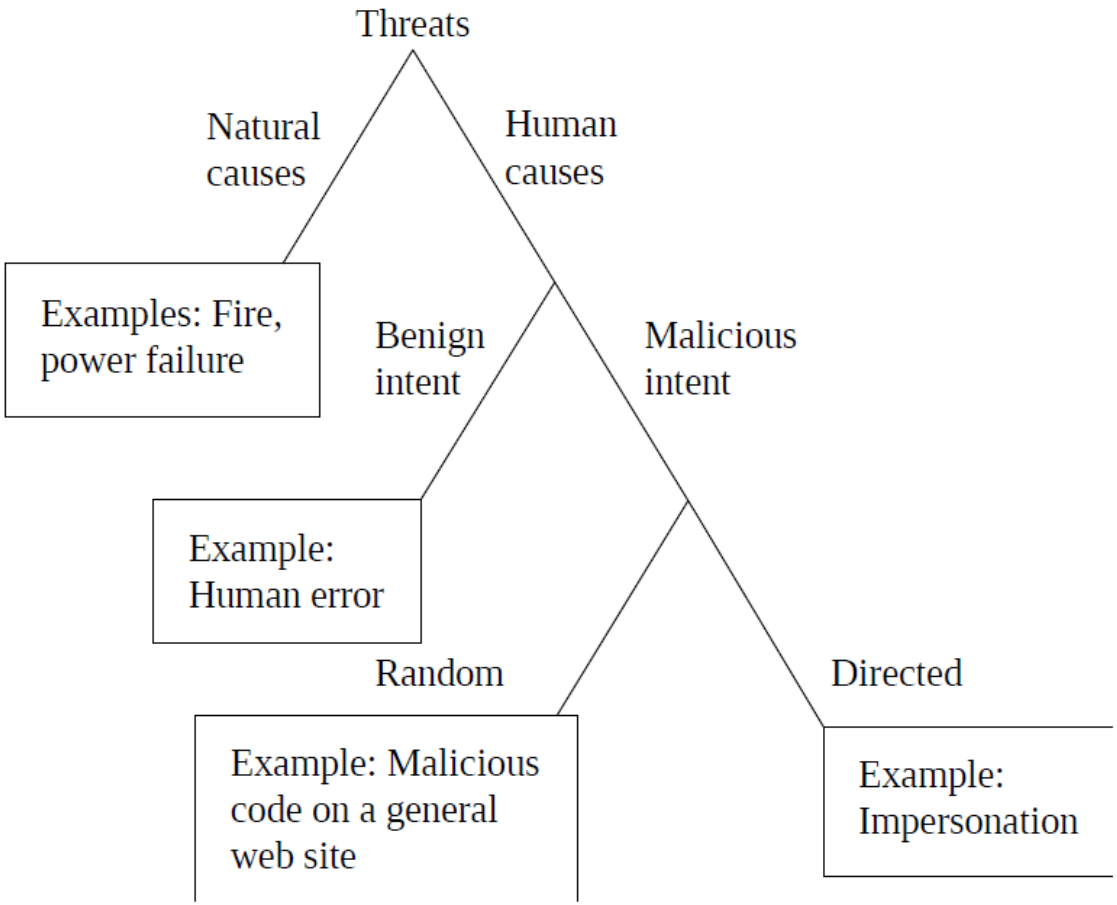


https://www.cyberdominance.com/cybersecurity/your-local-supermarket-holds-the-key-to-defending-against-distributed-denial-of-service-attacks/
https://steemit.com/ddos/@clumsysilverdad/dos-and-ddos-attacks

Threats and Attacks (cont.)

- Masquerading: fabrication of information, purported to be from some who is not the actual author
  - For example, phishing and spear-phishing attacks
- Repudiation: denial of commitment or data receipt
  - Attempt to back out of a contract

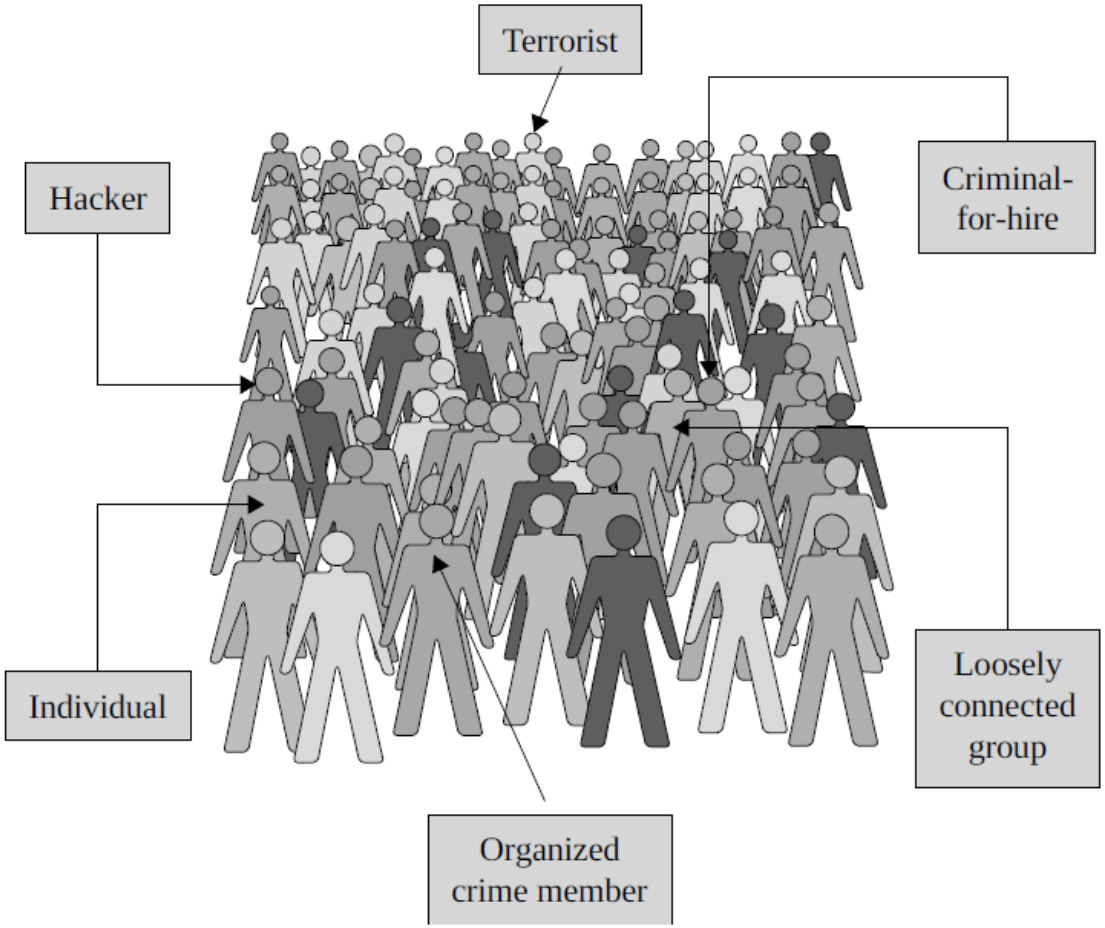
Source of the threat



Advanced Persistent Threat (APT)

- Attacks by a collection of attackers
- Organized, well financed, patient assailants
  - Often affiliated with governments or quasi-governmental groups
- Engage in long term campaigns
- Carefully select their targets, crafting attacks that appeal to specifically those targets

Who are the attackers?



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

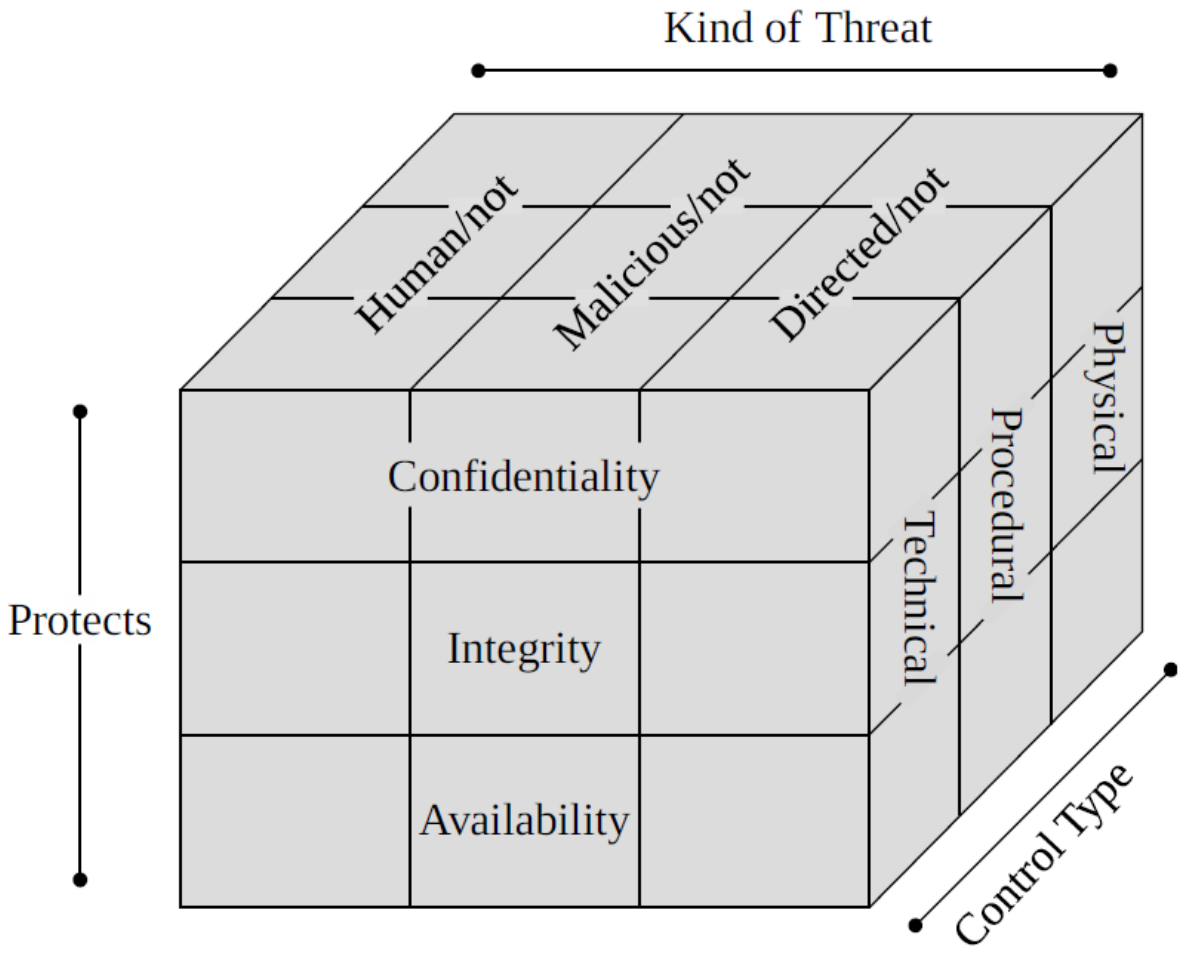
Vulnerabilities Databases

- http://cve.mitre.org - a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cybersecurity issues.
- https://nvd.nist.gov - the U.S. government repository of standards-based vulnerability management data

How are attacks accomplished?

- Method of attack:
  - A group or individual uses their knowledge of the hardware or software to access the system
  - A group or individual downloads the information needed to access the system
- Opportunity for an attack – unsecured access or data
- Motive – why is the attack occurring

Controls/Countermeasures



Risk Management

- Can not protect against every attack:
  - Decide what is most valuable and analyze how to protect it
  - Estimate how likely an attack is
  - What is the impact of the attack

How to prevent or respond to an attack

- Block the attack or remove the vulnerability
- Make the attack harder to accomplish
- Decrease the attractiveness of the target
- Have counter measures that make the attack less severe
- Detect that an attack is in progress and take counter measures
- Have a plan to recover from an attack

Summary

- Vulnerabilities are weaknesses in a system; threats exploit those weaknesses; controls protect those weaknesses from exploitation
- Confidentiality, integrity, and availability are the three basic security primitives
- Different attackers pose different kinds of threats based on their capabilities and motivations
- Different controls address different threats; controls come in many flavors and can exist at various points in the system

Questions?

AUTHENTICATION AND ACCESS CONTROL

CISC 3325 - Information Security

Authentication

- The ability to prove that a user or application is genuinely who they claims to be
  - Not just for end-users:
    - For example, a web server and client need to authenticated each other
- Usually the user has no control over the type of authentication

https://teamtreehouse.com/library/user-authentication-with-rails

Impersonation

- Pretending to be someone else
  - Attacker may impersonate user, web client or web server
- Authentication can protect against impersonation

https://cyberbullyingisevil.weebly.com/impersonation.html

Authenticating Users

- How can a computer authenticate the user?
- Authentication basics:
  - Something you ***know***
    - Password, pin, etc.
  - Something you ***have***
    - House key, ATM card, tokens, etc.
  - Something you ***are***
    - Captcha (differentiating humans and computers), fingerprints, face recognition

https://www.smartpaymentassociation.com/index.php/publications-smart-payment-association/position-papers-smart-payment-association/entry/spa-s-position-on-the-regulatory-technical-standard-on-strong-customer-authentication

Something the user knows

- What does the user know?
  - Passwords, pins, etc.
  - Security questions
  - Recognition of an image

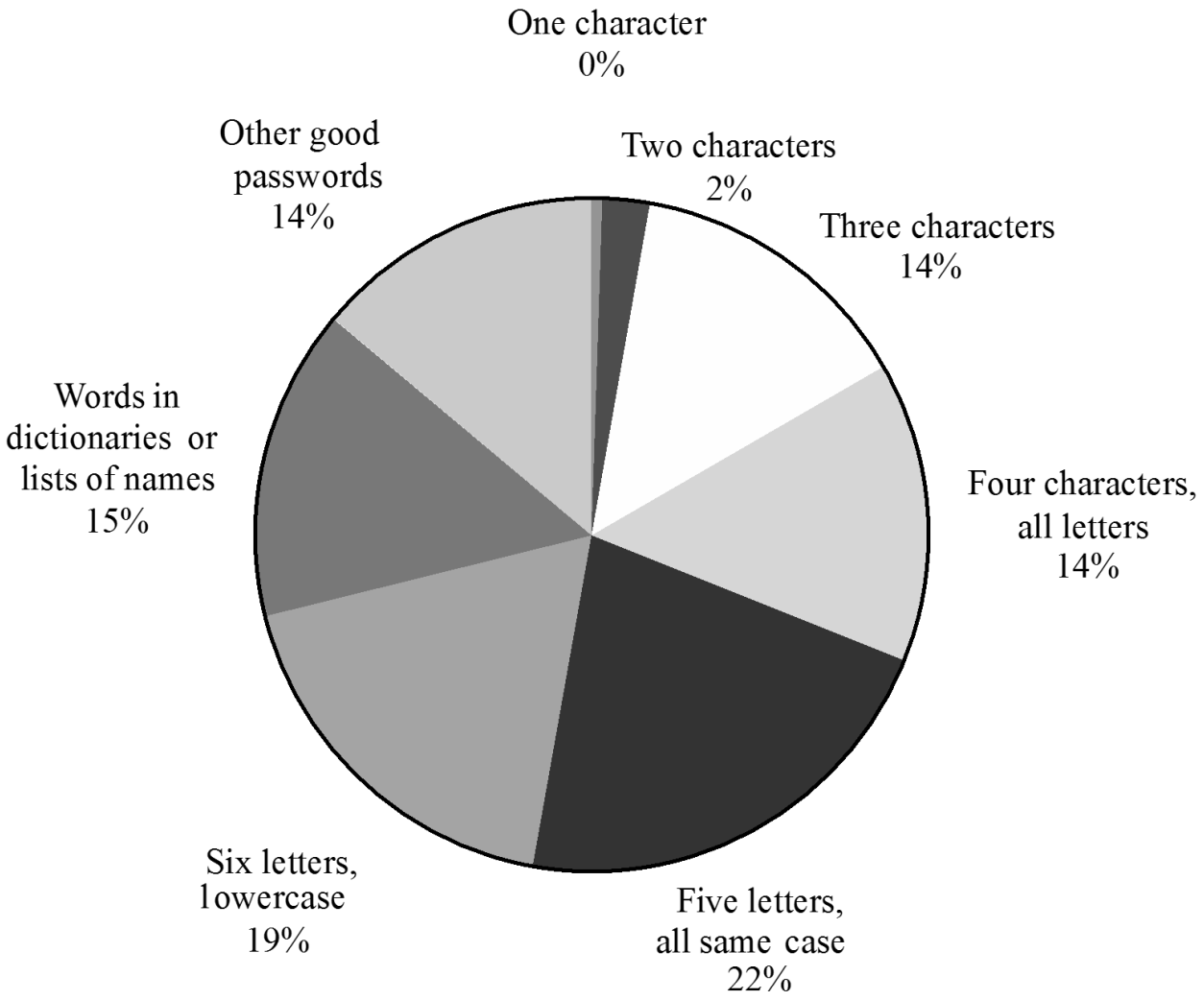
Something the user knows

- Attacks on “something the user knows”:
  - Dictionary attacks
  - Inferring likely passwords/answers
  - Guessing
  - Detecting how a password is stored
    - Defeating concealment
  - Exhaustive or brute-force attack
  - Rainbow tables
    - a precomputed **table** for reversing cryptographic hash functions

What is a good password?

- Many passwords are poorly chosen
- A good password has the following characteristics:
  - At least 8 characters
  - Not a word in several languages
  - Must contain several types of ASCII chars
    - uppercase and lowercase letters, digits, punctuation
  - Try not to begin with an uppercase letter

Distribution of Password Types



Secure Passwords

- Recent studies reaffirm the users' weak passwords
  - Show that the vast majority of passwords used on the Internet are extremely easy to crack
- Case studies, such as Ashley Madison, showed that a large number of passwords can be detected
  - Using off-the-market cracking tools

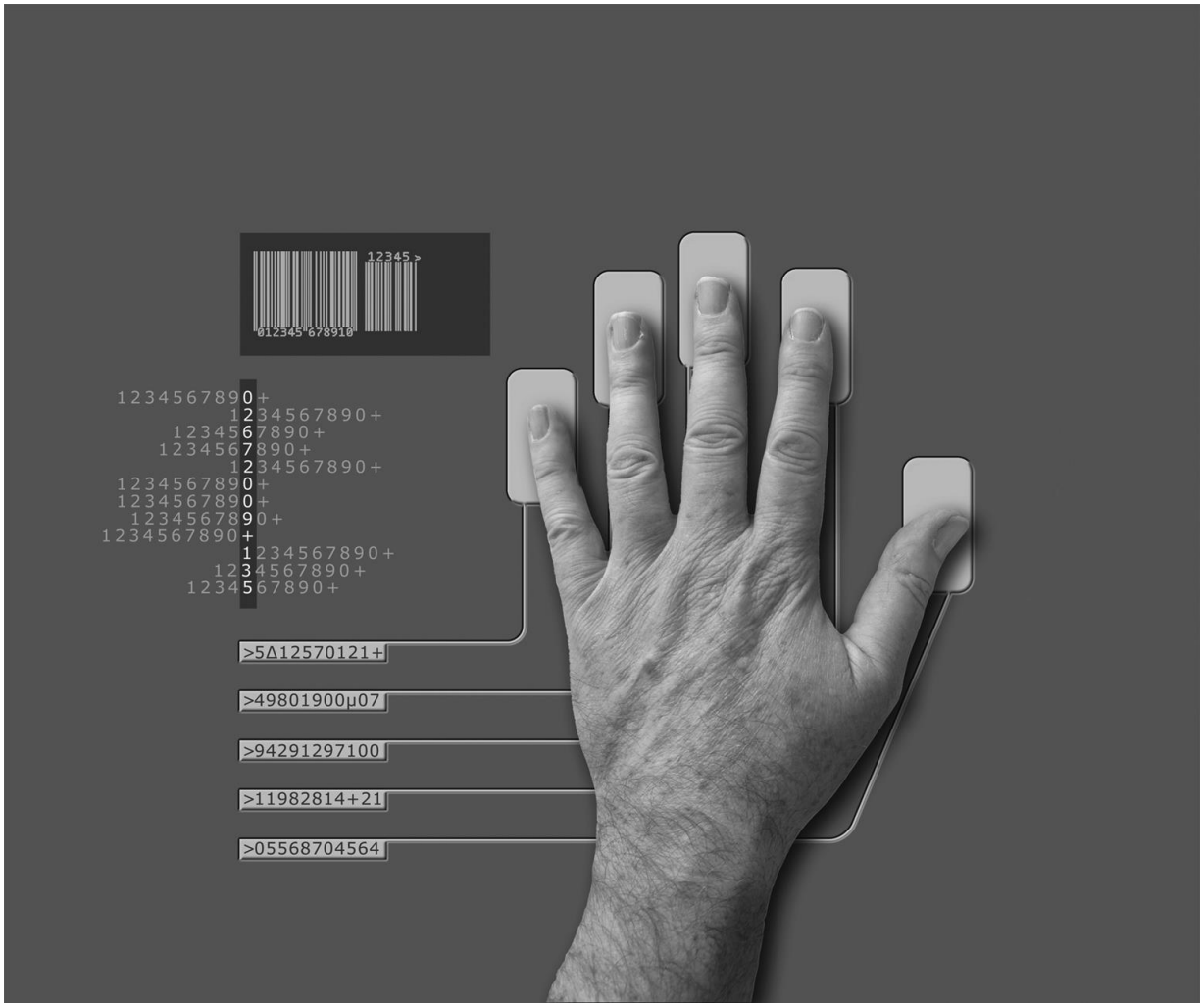
Secure Passwords

- Conclusions:
  - Weak passwords easier to guess
    - Vulnerable even when hashed
  - Many passwords can be guessed
    - by exploiting the predictability in the way most end users choose passwords
  - Password cracking tools significantly improved
  - Passwords should be hashed
    - Using a strong hashing mechanism

http://www.enterprisefeatures.com/secure-passwords-a-cautionary-tale/

BIOMETRICS AND TOKEN-BASED AUTHENTICATION

Biometrics: a physical attribute of the user



Types of biometric authentication

- Fingerprints
- Hand geometry
- Scan of the eye
- Voice
- Handwriting
- Typing style
- Face or facial features

Problems with Biometrics

- Intrusive
- Expensive
- Single point of failure
- Sampling error
- False readings
- Speed
- Forgery

Biometrics Passwords

- Recent advances in smartphones have begun to make biometrics cheaper and easier to use.
- Biometrics are still inadequate for extremely sensitive applications
  - but their convenience makes them a great alternative to weak passwords

Authentication Mechanisms

- Companies are developing authentication methods
  - To be used by third-party applications for authentication
  - So applications do not have to implement it themselves
- Examples: RSA SecureID, Federated Identity Management

Authentication Mechanisms

- RSA Secure ID:
  - Has a code that changes every 60 seconds.
  - Physical possession of the token should be necessary for successful authentication.

Tokens: Something You Have

Time-Based Token Authentication

Login: mcollings
Passcode: 2468159759

PASSCODE = PIN + TOKENCODE

Token code:
Changes every
60 seconds

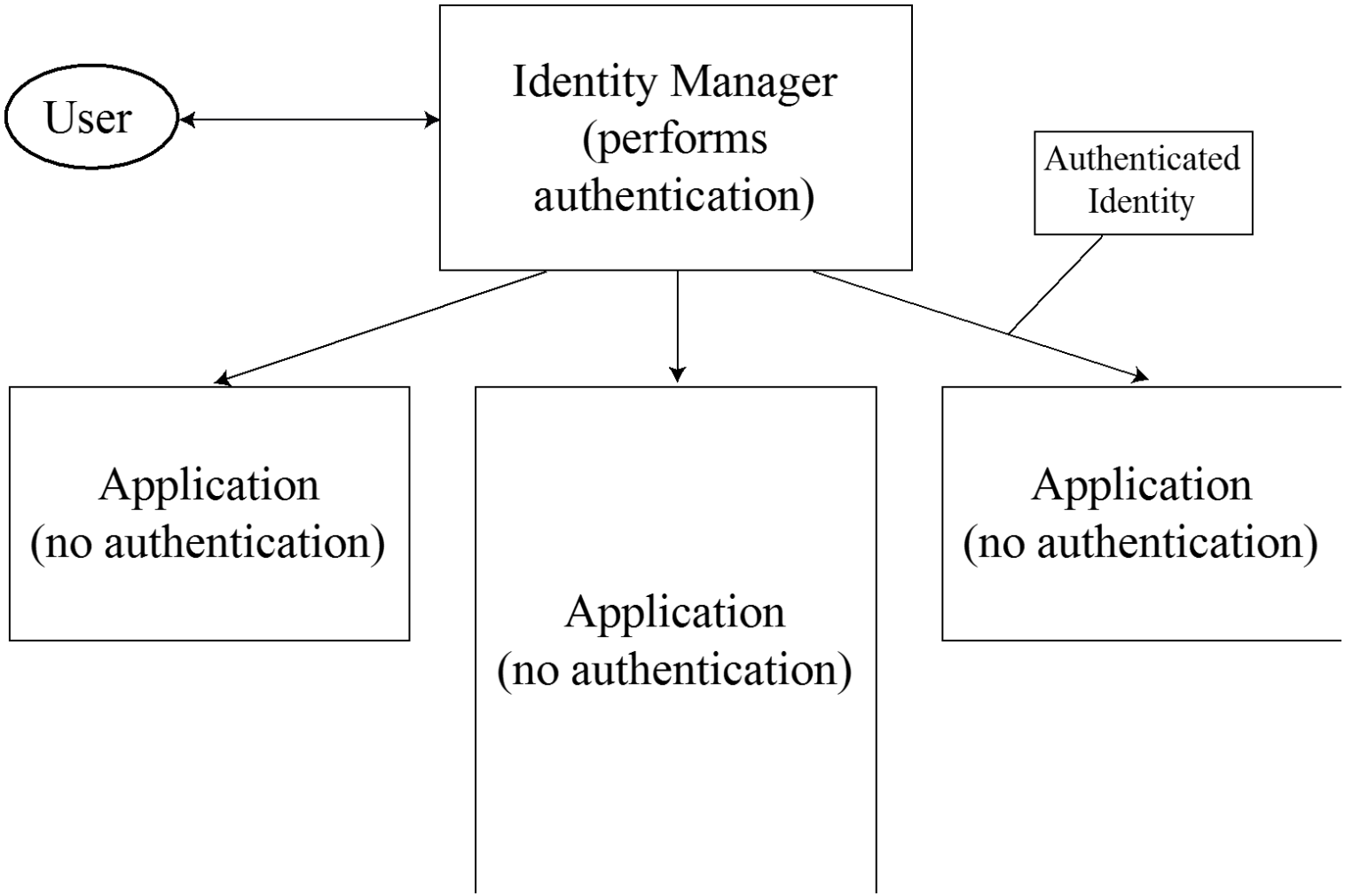
Clock
synchronized to
UCT

Unique seed

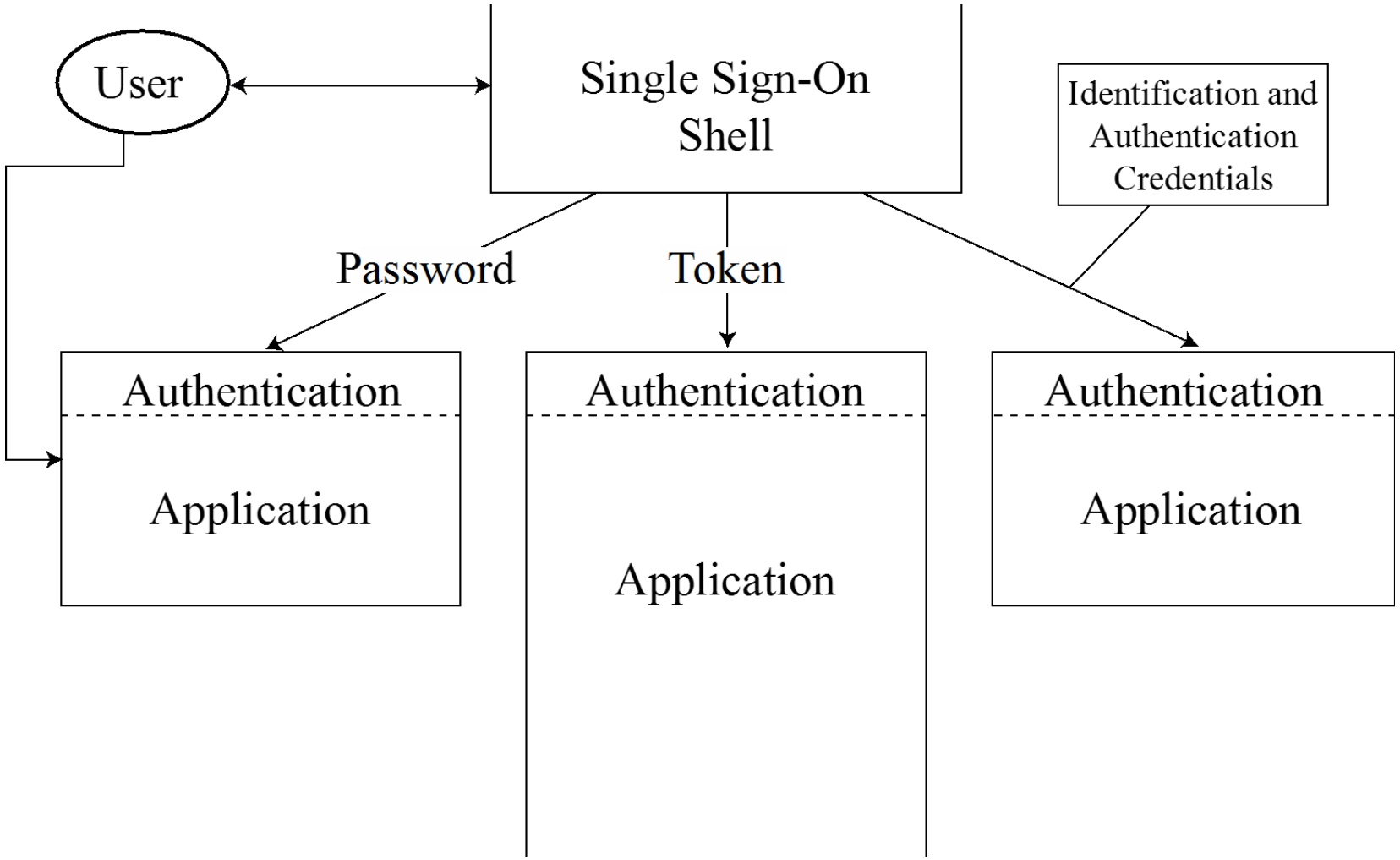
Authentication Mechanisms

- Federated Identity Management:
  - A union of separate identification and authentication systems.
  - Authentication is performed in one place,
  - Separate processes and systems determine that an already authenticated user is to be activated.
- Single sign-on lets a user log on once per session but access many different applications/systems.
  - Often works in conjunction with federated identity management
    - with the federated identity provider acting as the source of authentication for all the applications.

Federated Identity Management



Single Sign-On



Questions?

Access Control

- Some resources (files, web pages, …) are sensitive.
  - Need to protect their confidentiality
- How do we limit who can access them?
- This is called the access control problem

http://checkinhere.org/attribute-based-access-control/

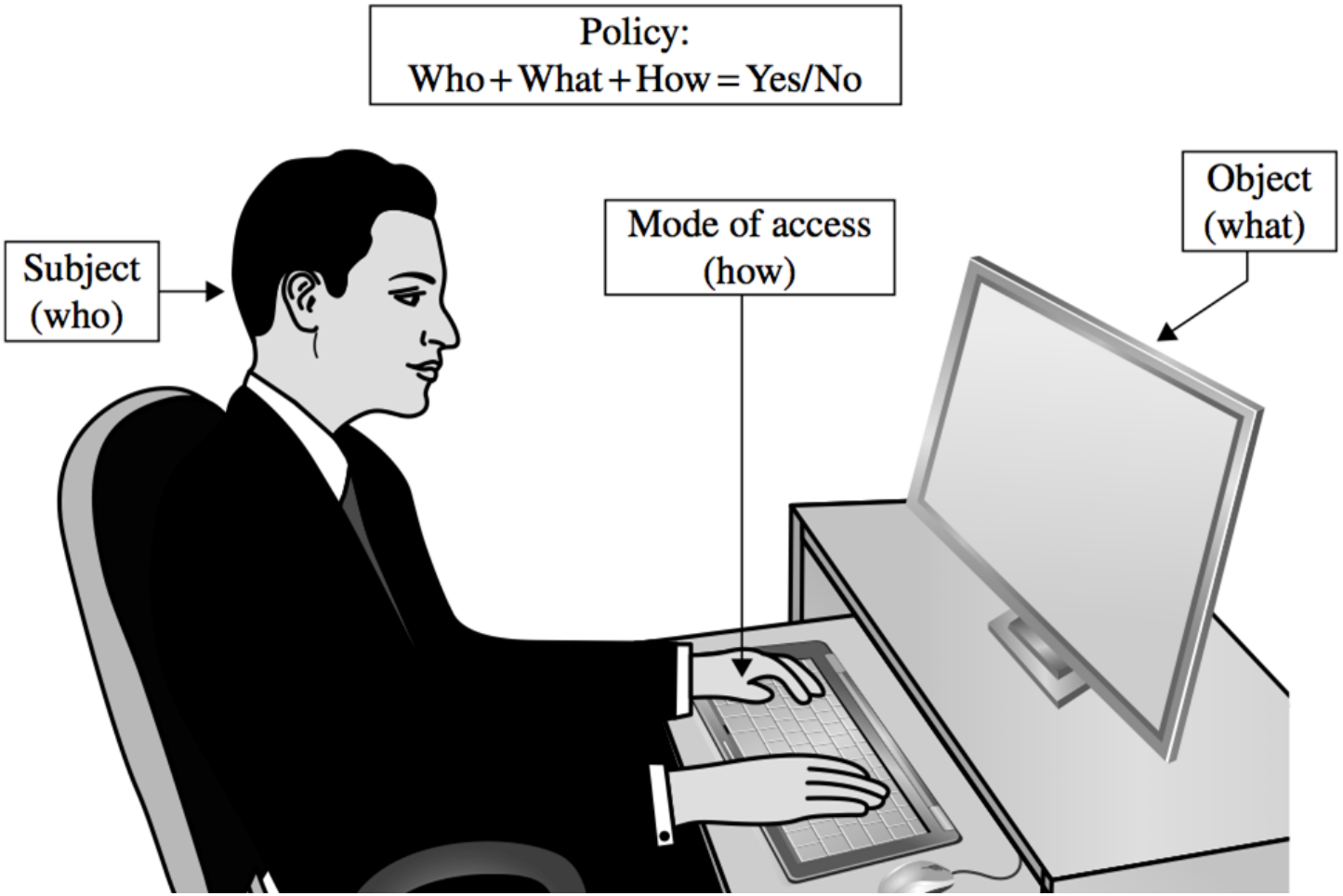
Access Control

- Basic tasks access control manages:
  - Allow access
  - Deny access
  - Limit access
    - Allowing access to a resource up to a certain point
  - Revoke access
    - Access may change over time

Access Control Fundamentals

- Selective restriction of access to a place or other resource
- The system makes a decision to grant or reject an access request from an already authenticated subject
  - based on what the subject is authorized to access

Access Control



Access Policies

- Goals:
  - Check every access
  - Enforce least privilege
  - Verify acceptable usage
- Track users' access
- Enforce at appropriate granularity
- Use audit logging to track accesses

Access Control Fundamentals

- *Subjects:* entities that can perform actions on the system
- *Objects*: entities representing resources to which access may need to be controlled
- *Policy:* the restrictions we'll enforce
- *Example:*
  access(*S*, *O*) = true if subject *S* is allowed to access object *O*

Principle of Least Privilege

- Minimal user profile privileges is set based on users' job necessities
- Applies to users, user accounts, processes, etc.
  - To allow performing needed functionality
- Example: a teacher should not need access to data internal to a human resource system in order to do their job

Access Control Fundamentals

- Identification and authentication:
  - only legitimate subjects can log on to a system
- Access approval:
  - grant access during operations
    - by associating users with resources they may access
    - based on the authorization policy
- Accountability: identify what a subject did
  - (or all subjects associated with a user)

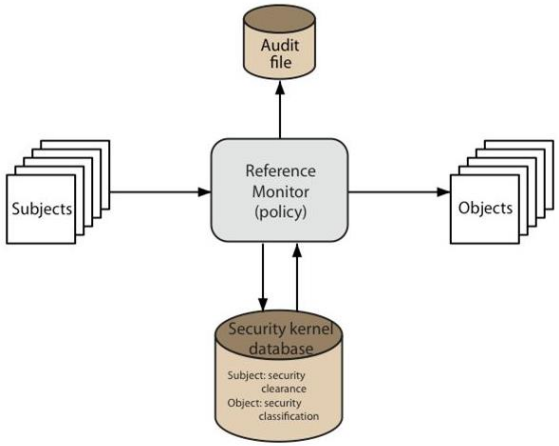
Questions?

Implementing Access Control

- Reference monitor
- Access control directory
- Access control matrix
- Access control list
- Capability-based security
- Procedure-oriented access control
- Role-based access control

Reference Monitor

- Defines a set of design requirements on a reference validation mechanism
- Enforces an access control policy over subjects ability to perform operations on objects
  - Subjects, e.g., processes and users
  - Operations, e.g. read and write
  - Users, e.g. files, etc.

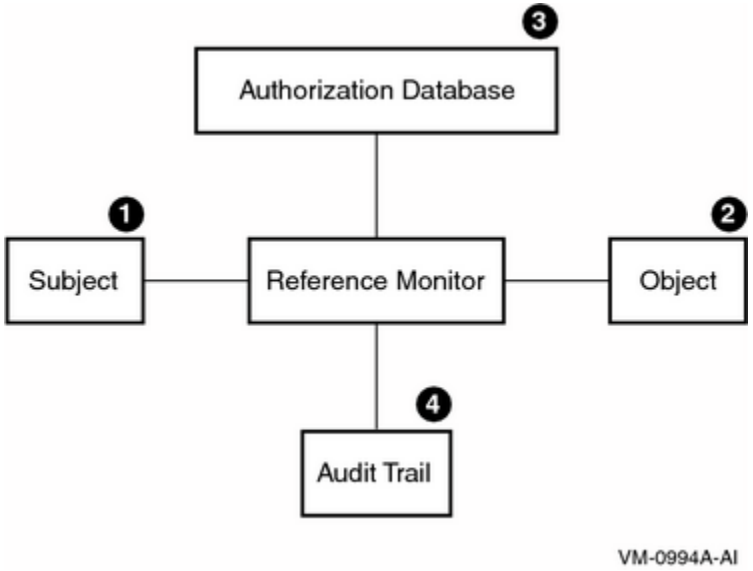


http://slideplayer.com/slide/697485/

Reference Monitor

- A reference monitor is responsible for mediating all access to data
- Subject cannot access data directly; operations must go through the reference monitor, which checks whether they’re OK

Reference Monitor



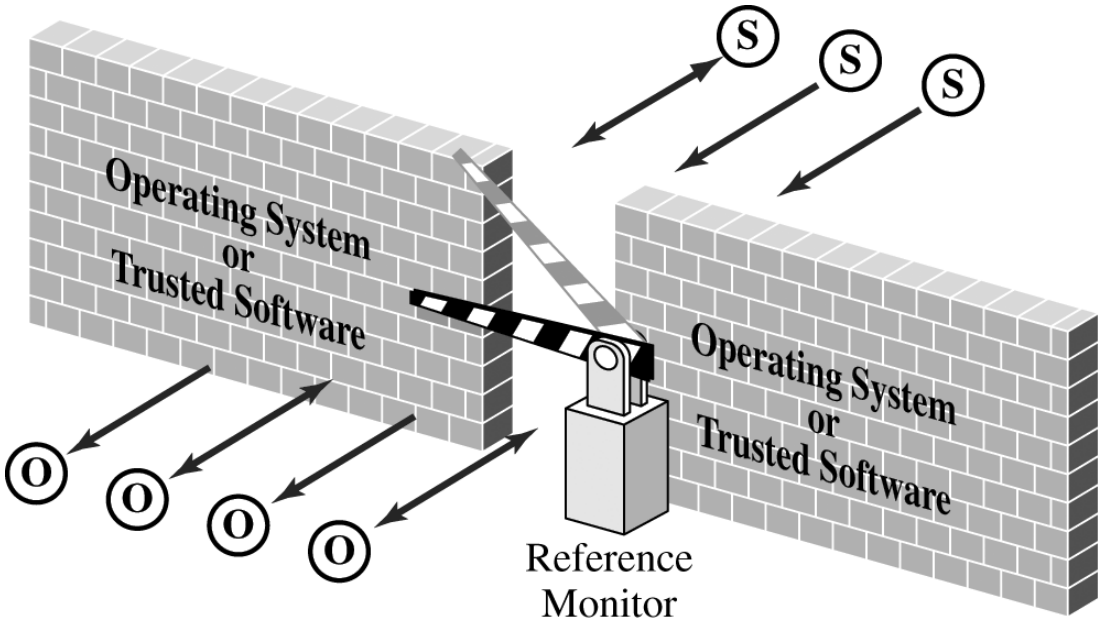
- Authorization Database: Repository for the security attributes of subjects and objects
- Audit trail: Record of all security-relevant events

Criteria for a Reference Monitor

- Ideally, a reference monitor should be:
  - Non-bypassable: mediate every attempt by a subject to gain access to an object
  - Tamper-resistant: Provide a tamperproof database and audit trail
    - that are thoroughly protected from attackers
  - Verifiable: should be simple and well-structured software
    - so that it is effective in enforcing security requirements
    - Unlikely to have bugs

Reference Monitor

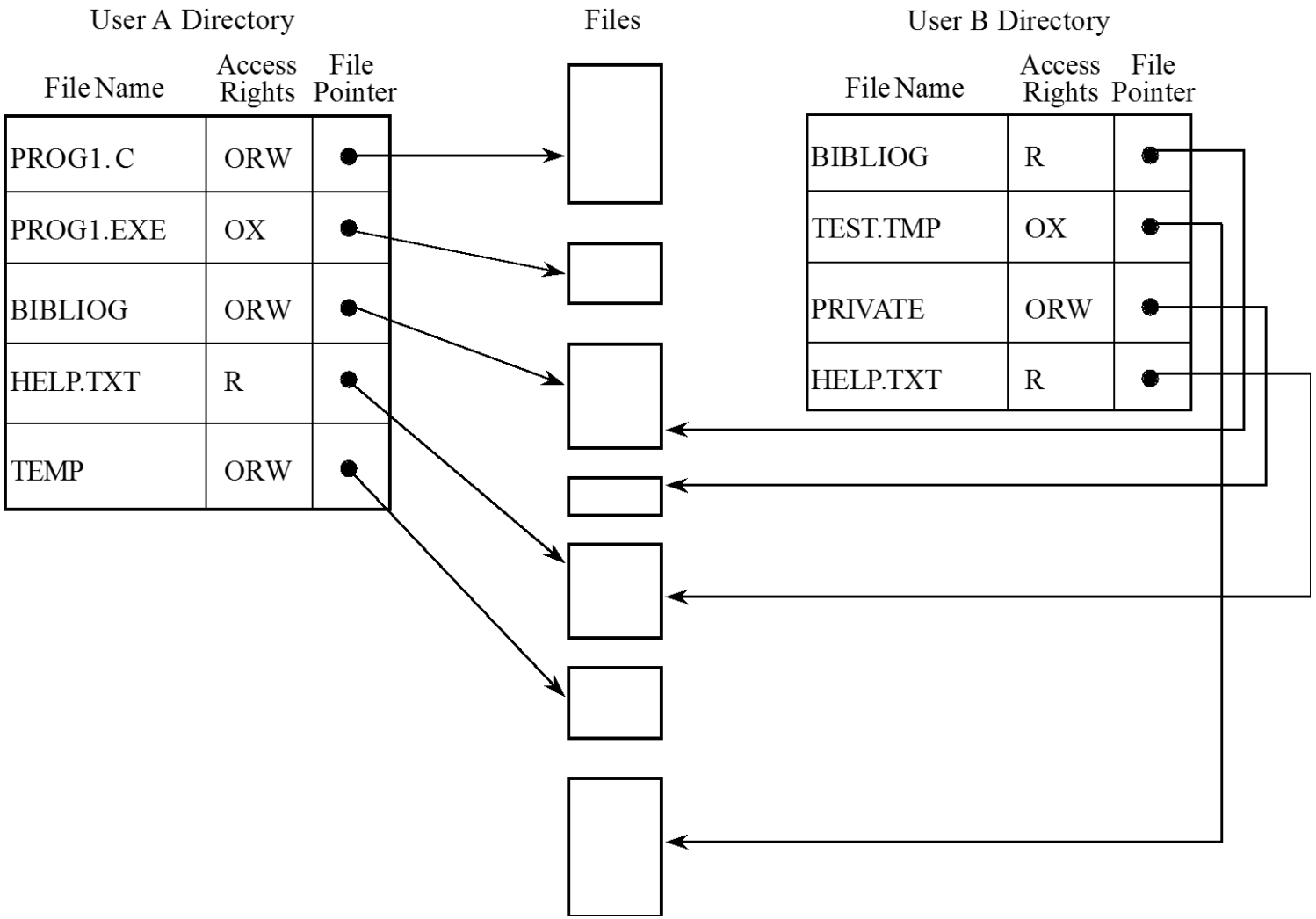
- A reference monitor is the primary access control enforcement mechanism of the operating system



Access Control Fundamentals

- Examples:
- *access*(Alice, Alice's data) = true
- *access*(Alice, Bob's data) = true
- *access*(Alice, Charlie's data) = false

Access Control Directory



Access Control Matrix

- Characterizes the rights of each subject with respect to every object in the system
- Can be written as a rectangular array of cells,
  - one row per subject and one column per object
  - The entry for a particular subject-object pair indicates the access mode
    - that the subject is permitted to exercise on the object
  - Each column is an access control list for the object
  - Each row is an *access profile* for the subject

Access Control Matrix

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W

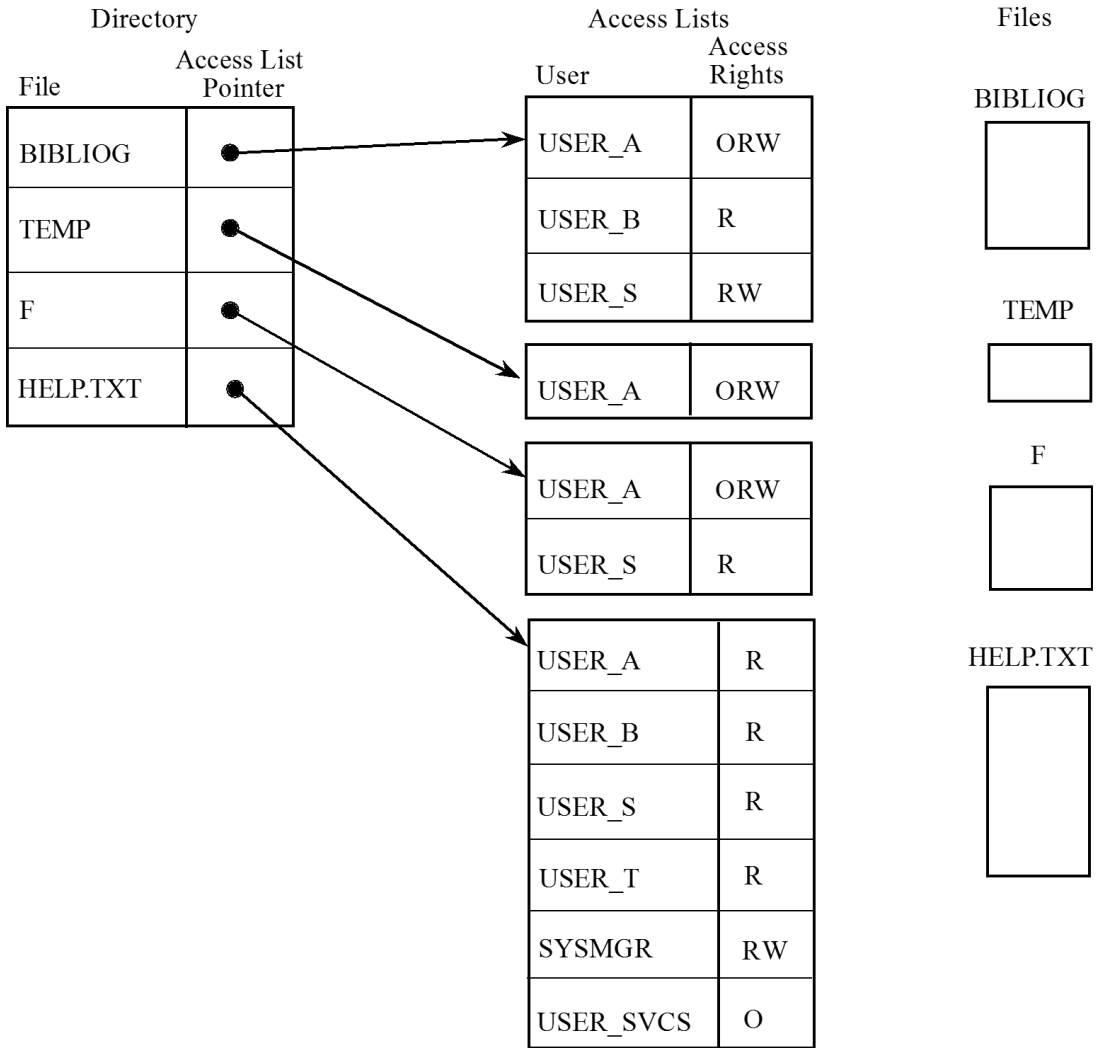
Access Control List (ACL)

- A list of permissions attached to an object
- An ACL specifies which users or system processes are granted access to objects
  - as well as what operations are allowed on given objects
- Each entry in a typical ACL specifies a subject and an operation
- Example: A file that contains the line:

  Alice: admin, Bob: write

https://internetdevels.com/blog/using-acl-api-to-create-access-control-lists

Access Control List

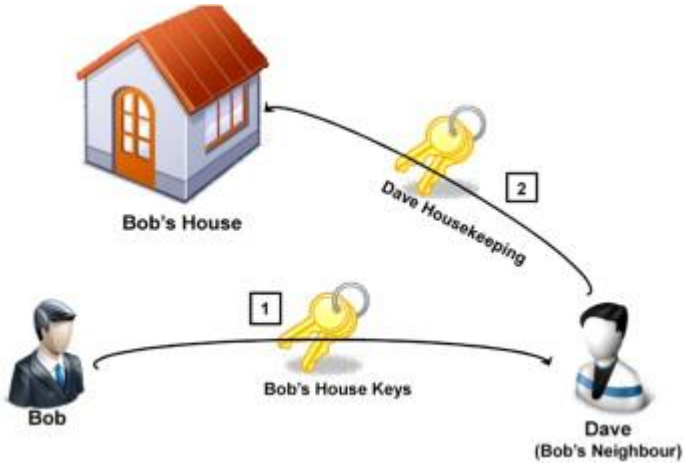


Capability-Based Security

- Oriented around the use of a token that controls an access
- Based entirely on the possession of the token and not who possesses it
- In a capability-based operating system, the capabilities are passed between processes and storage
  - OS maintains the integrity of those capabilities

Capability-Based Security

- Example: Bob gives his key to his neighbor Dave while he goes on vacation.



https://www.sciencedirect.com/science/article/pii/S089571771300054X

Procedure-Oriented Access Control

- Provides a more complex access control
- A procedure that controls access to objects
  - for example, by performing its own user authentication to strengthen the basic protection provided by the basic operating system)
- The procedure forms a “capsule” around the object
  - permitting only certain specified accesses

Procedure-Oriented Access Control Example

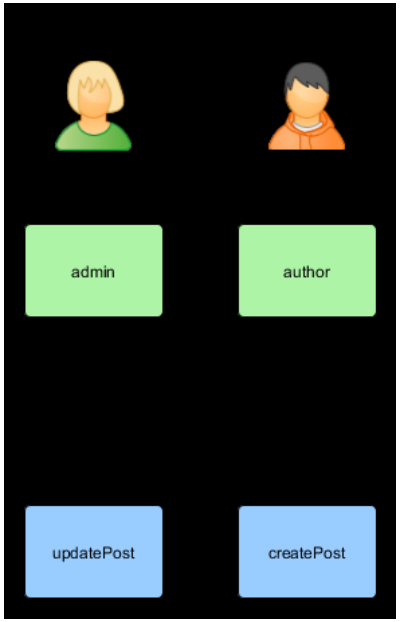
- Procedures can ensure that accesses to an object be made through a trusted interface.
- Example:
  - Neither users nor general operating system routines might be allowed direct access to the table of valid users.
  - The only accesses allowed might be through three procedures:
    - one to add a user
    - one to delete a user
    - one to check whether a particular name corresponds to a valid user.
  - These procedures could use their own checks to make sure that calls to them are legitimate
    - especially add and delete

Procedure-Oriented Access Control

- Implements the principle of information hiding
  - the means of implementing an object are known only to the object's control procedure
- However, this carries a penalty of inefficiency
  - No fast access checking, even if the object is frequently used

Role-Based Access Control (RBAC)

- Access control set by an authority designated for the task
- Access is based on the role each subject has in the system



http://www.yiiframework.com/doc-2.0/guide-security-authorization.html

Summary

- Users can authenticate using something they know, something they are, or something they have
- Systems may use a variety of mechanisms to implement access control

Questions?