Course Overview

CS 450/650

Objectives

- Overview of Course topics, assignments, relevance and logistics
- Discuss the relevant ethical issues associated with computer security
- Define computer security
- Discuss common threats and recent computer crimes that have been committed
- List and discuss recent trends in computer security
- Describe common avenues of attacks
- Describe approaches to computer security
- Get set up for future class meetings!

Cybersecurity Ethics

Ethics

- Commonly defined as a set of moral principles that guides an individual's or group's behavior
  - Information security efforts frequently involve trusting people to keep secrets that could cause harm if revealed
  - Trust is a foundational element in the people side of security
  - Trust is built upon a code of ethics, a norm that allows everyone to understand expectations and responsibilities

Why it's important

- The study of cybersecurity requires understanding of tools and techniques used in hacking, cybercrime and cyberwarfare
- This class will introduce several of these tools and techniques and allow you to experiment with them in a controlled, virtual machine environment
- Using these tools and techniques outside of a strictly controlled environment is unethical and potentially illegal
- Using these tools and techniques outside of a strictly controlled environment has the potential to cause serious harm to you and others

When to experiment with hacking tools

- When using these tools insure they are used in a strictly controlled environment
  - Virtual machines and or test networks
- If others are involved, they must be informed of the risks and provide explicit consent to participate
  - It's not okay to try to hack a neighbor or coffee shop WiFi network
  - It's not okay to scan public websites to look for vulnerabilities, without their knowledge and permission
  - It is okay to setup your own vulnerable machines and sites in a controlled environment and experiment with them.

General Cyber Ethics

- To be considered a professional in cybersecurity, one must perform ethically
- The ACM Code of Ethics and Professional Conduct provides an excellent example of the rules we should follow: https://ethics.acm.org/code-of-ethics/
- The following points from The ACM Code of Ethics and Professional Conduct are most important during our studies
  - 1.2 Avoid harm
  - 1.3 Be honest and trustworthy
  - 1.6 Respect privacy
  - 1.7 Honor confidentiality

Course Overview

Class Strategy

- Theory - forms the foundation for our work
- Practice – labs and assignments where we apply the theory
- Current examples of these topics in practice

Course Topics

To Mid-term	To Final Exam
Security Trends	Cloud Computing and IoT Security
Computer Security Concepts	Secure Software Development
The Role of People in Security	Web Application Security
Cryptographic Concepts	Security Tools and Techniques
Authentication and Remote Access	Incident Response
Types of Attacks and Malware	Penetration Testing
System Hardening and Baselines	Digital Forensics
Physical Security	

Syllabus and Textbook

- Find all course materials and most current syllabus in Canvas.
- Text is required
  - *Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, Dwayne Williams. "Principles of Computer Security: CompTIA Security+ and Beyond, Sixth Edition (Exam SY0-601)*
  - Available online from UNR library
  - Excellent overview of most cybersecurity topics
- Chapters from 2 other books are linked in modules
- Quizzes will be from text readings

Software

- Virtual Machine Hypervisor
  - Oracle VirtualBox or equivalent
    - https://www.virtualbox.org/
- Labtainers VirtualBox VM Appliance
  - https://nps.edu/web/c3o/virtual-machine-images
- NCR or other virtual machines as required for in-class work

Assignments

- Generally one per week
  - Hands-on using Labtainer or other tools
  - Case studies

Quizzes

- 15 question quiz on each chapter
- Can be taken any time before the due date on Canvas
- ONE attempt 20 minute time limit

Projects

- Final Project
  - Task-based in a virtual environment
- Graduate (additional project for those enrolled in CS 650)
  - Research based project
- Requirement details in Canvas

Grading and Schedule

- Current schedule and grades always available in Canvas

Course Relevance and Context

- Fills in topics not covered in other CS classes
- Great preparation for Security+ certification
- Covering how attacks can happen and how to defend

Not a Cybersecurity Major?

- Data Analyst is one of the hottest Cybersecurity careers.
- Developers can use this information to bake security into whatever you do.
  - Secure Development Life Cycle
- If you have trouble with the technology, work with a classmate
  - Just submit your own work

Take Notes!

- Hands-on demonstrations in class will make assignments easier, but you have to take notes

The Punchline

- Fundamentals, standards and recommended practices form the foundation to build defenses.

- **Class Intro Poll - https://www.questionpro.com/a/TakeSurvey?tt=37rdbb8Y%2BoPTFneCZs3WPG943ob4ZyMj**

Chapter 1

Computer Security Defined

- " Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being *processed, stored, and communicated**"
  - *also known as in use, at rest and in transit

Source: The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013)

Information Assurance as a part of security

- *Information assurance* is a term used to describe not just the protection of information, but a means of knowing the level of protection that has been accomplished

Computer Security Challenges

- Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
- Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process
- Security requires regular and constant monitoring
- There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
- Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

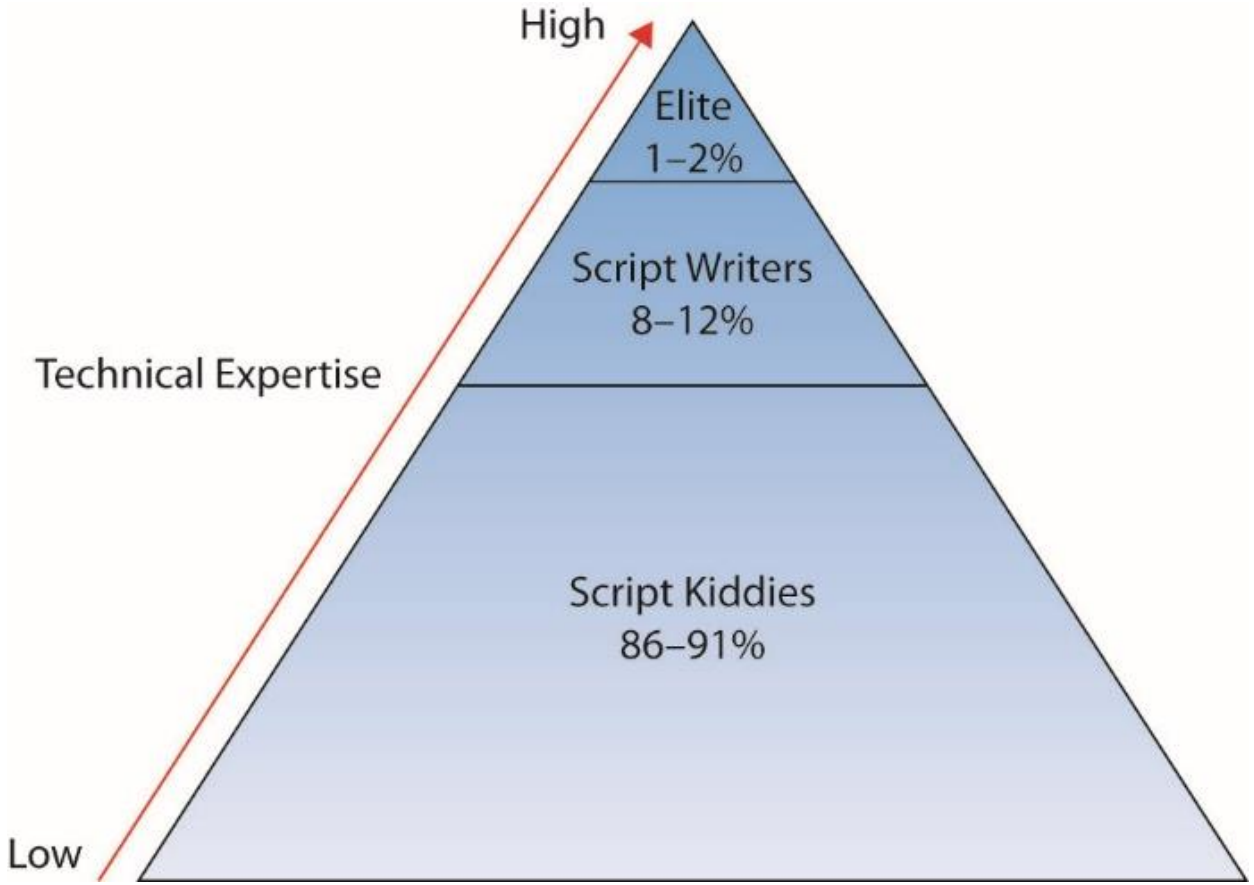
Common Terms

- **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.
- **Countermeasure (mitigation) -** A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information 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.
- **Security Policy -** A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- **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.
- **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.

Targets and Attacks

- Two general reasons a particular system is attacked
  - It is specifically targeted by the attacker
  - It is an opportunistic target

Threat Actors by Ability



Other Attributes of Actors

- Location (internal or external)
- Level of resources
- Intent

Threat Actors

http://e-mate2.s3-website-us-east-1.amazonaws.com/ThreatActors/ThreatActors.html

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT Characteristics

Advanced

- Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
- The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target

Persistent

- Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
- A variety of attacks may be progressively applied until the target is compromised

Threats

- Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
- The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

Approaches to Defense (1 of 2)

- Correctness: ensuring the system is fully up to date
  - All patches installed and proper security controls in place
- Isolation: protecting a system from unauthorized use
  - Access control and physical security
- Obfuscation: making it difficult for an adversary to know when they have succeeded
  - Increasing the workload of an attacker makes it more difficult for them to succeed in their attack
  - Not a favored solution

Approaches to Defense (2 of 2)

- Cybersecurity kill chain
  - Step-by-step process to model how attacks target and achieve results on victim systems
- Threat intelligence
  - Set of actions taken to properly utilize resources to target the actual threats an enterprise is facing
  - Basis of understanding adversary tactics, techniques, and procedures (TTPs)
- Open-source intelligence
  - Processes used to collect threat intelligence information
  - Example OSINT: https://www.youtube.com/watch?v=F7pYHN9iC9I&t=146s

The Importance of Doing Things Right

- https://www.nytimes.com/2020/08/20/technology/joe-sullivan-uber-charged-hack.html

How Secure Are You?

QuestionPro Poll

The Current Threat Environment

- Verizon DBIR
  - Increase in ransomware
- Crowd Strike Global Threat Report

Real-time attack maps

https://threatbutt.com/map

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

https://cybermap.kaspersky.com/

http://www.digitalattackmap.com

https://talosintelligence.com/fullpage_maps/pulse

Questions?

Assignments

- Read Chapter 1 and take quiz
- Read Chapter 2
- Login to Nevada Cyber Range
  - https://ncr.cse.unr.edu/
  - 2FA Authenticator apps:
    - Google Authenticator, Aegis, or Duo
  - **BRING AUTHENTICATOR DEVICE TO CLASS EVERY WEEK!**
- **Be ready to take notes next class**

NEVADA CYBER CLUB

https://www.nevadacyberclub.com/discord

U.S. DEPARTMENT OF ENERGY'S CYBERFORCE® COMPETITION

DEFENDING U.S. ENERGY INFRASTRUCTURE

NSA Codebreaker Challenge

NCAE CYBERGAMES

PLAY | LEARN | PROTECT

CCDC NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

THE NATIONAL CYBER LEAGUE

COLLEGIATE PENETRATION TESTING COMPETITION

Scholarship for Service Grant

- https://www.unr.edu/cybercorps-scholarship
- TLDR; Up to 2 years paid classes and cost of living and material stipends in exchange for up to 2 years of work in a government agency.
- Internships and job placement assistance
- Meeting Friday, August 30, 2024, 5:00 – 6:30 PM, WPEB130 – Pizza!
- RSVP here: https://unr.campuslabs.com/engage/event/10304015

Graduate Students Stick Around

Graduate Project

- Cybersecurity Conference Call for Posters/Demos
- Consider a topic related to a graduate thesis
- Actual analysis or experimentation.developement is preferred to literature review
- Small team projects may be considered if appropriate in scale
- Cyber competitions with grade based on results

Project Idea

- The goal of this prize challenge is to develop a mathematical model that uses as inputs:
  a) the system's architecture,
  b) the functions and functional threads that the system must perform,
  c) the hardware and software within the system needed for each thread,
  d) the known cyber vulnerabilities present on each hardware and software component, and
  e) the adversary threat actors and tactics, techniques, and procedures they will use to exploit the open cyber vulnerabilities on the system to cause a cyber effect to impact functionality and execution.
  The mathematical model will be implemented within software algorithms to form core functionality for the desired cyber resiliency assessment capability. The challenge will include developing a cyber resiliency assessment prototype GUI that displays the assessment results. The GUI will be used during the challenge demonstration phase.

Project Idea

- Vulnerability Testing
- https://hackerone.com/opportunities/all
- Create and document testing plan and results
- Professional Pen Testing Report

Computer Security Concepts

Overview

- News
- Key Terms
- Security Design Principles
- Fundamentals, Standards and Guidelines
- Labtainer preview
- Preview of next module

News Links

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
- https://www.justice.gov/usao-nj/pr/former-employee-national-industrial-company-arrested-attempted-data-extortion
- https://www.zaun.co.uk/zaun-data-breach-update/?ref=thestack.technology
- https://www.cisa.gov/news-events/bulletins
  - Subscribe at bottom

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

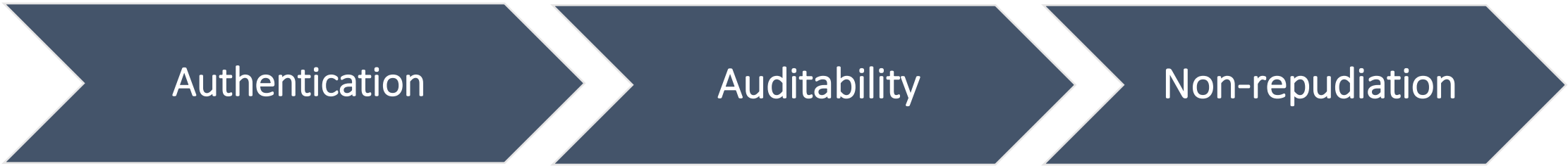
Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Expanded CIA



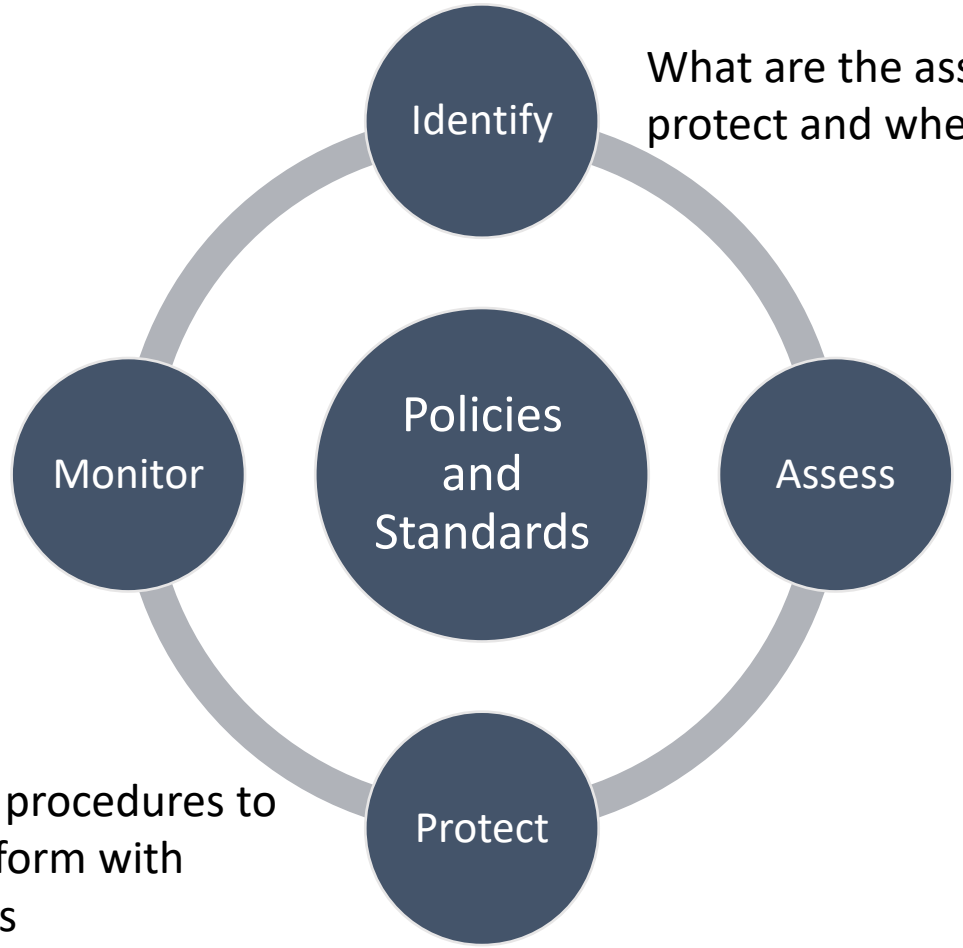
- Ensure that an individual is who they claim to be
- Or Accountability
- Ability to verify the functioning of controls
- Verify authenticated sending and receipt of messages

McCumber's Cube

- http://e-mate2.s3-website-us-east-1.amazonaws.com/cube/cube.html
- Cube Challenge First 10:
  - http://e-mate2.s3-website-us-east-1.amazonaws.com/cube_challenge/cube_challenge.html

Security Design Principles

Security Life Cycle



What are the assets you want to protect and where are they located

Consider the risk to the asset and vulnerabilities and prioritize highest risk assets

Configure systems and procedures to protect assets and conform with policies and procedures

Implement policies and tools to monitor for security incidents and comply with potential legal requirements for monitoring

Standards

Standards have been developed to cover management practices and the overall architecture of security mechanisms and services

- **National Institute of Standards and Technology (NIST)**
  - **NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation**
- **Internet Society (ISOC)**
  - **ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards**
- **International Telecommunication Union (ITU-T)**
  - **ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services**
- **International Organization for Standardization (ISO)**
  - **ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards**

Example Security Standards

- Center for Internet Security Controls
- https://www.cisecurity.org/
  - List in Canvas

Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design	Separation of privilege
Least privilege	Least common mechanism	Psychological acceptability	Isolation	Encapsulation
	Modularity	Layering	Least astonishment	

Source: The National Centers of Academic Excellence in Information Assurance/Cyber Defense

Security Design Principles in Detail

- http://e-mate2.s3-website-us-east-1.amazonaws.com/cybersecurity_principles_v4/cybersecurity_principles_v4.html

One More Example

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

- **How do you fix it?**

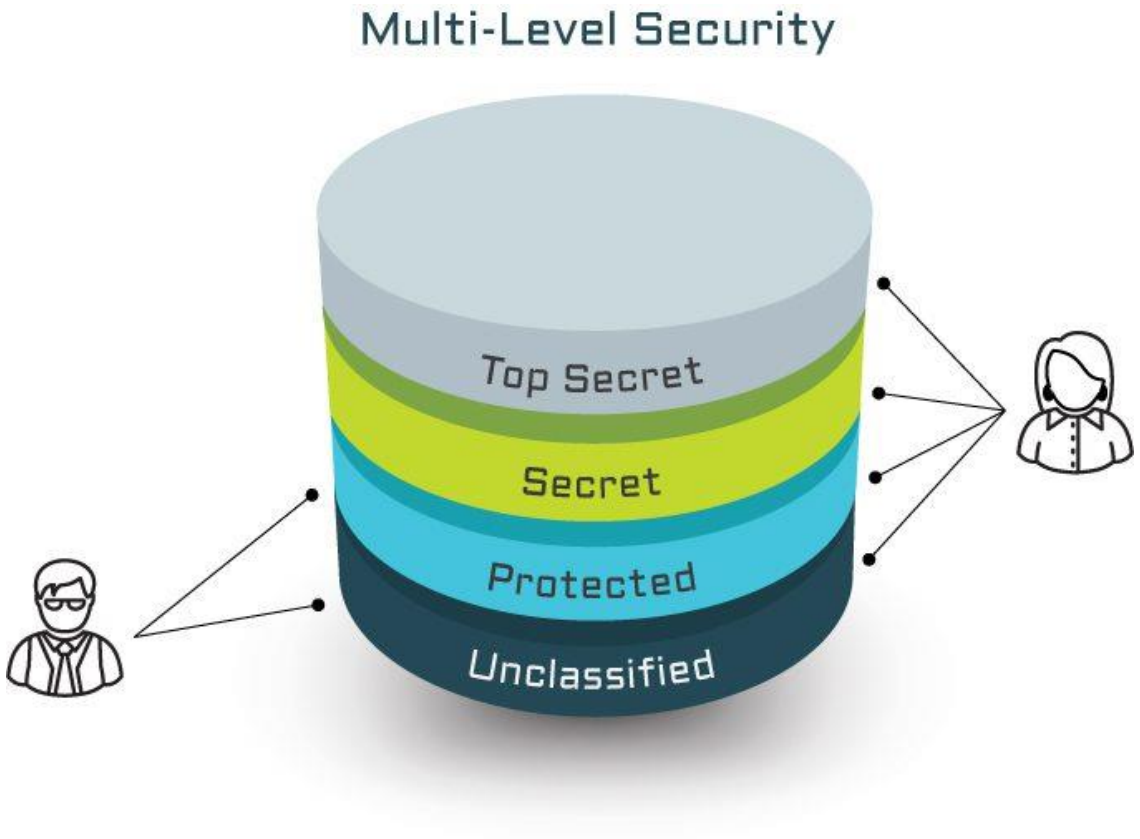
Theoretical Security Models

Overview

- Theoretical models form the basis for security implementations
- Achieving theoretically provable security is difficult
  - Even achieving functional security is difficult in large systems
- These models can be used to evaluate systems during development and production
- Different models have different objectives
  - CIA

Multi-Level Security

- no read up
  - subject can only read an object of less or equal security level
  - referred to as the *simple security property*
    - ss-property



Bell-LaPadula (BLP) Model

- AKA Multi-level Security
- formal model for access control and **Confidentiality**
- *subjects* and *objects* are assigned a security class
  - a *subject* has a *security clearance*
  - an *object* has a *security classification*
  - form a hierarchy and are referred to as security levels
    - top secret > secret > confidential > restricted >unclassified
  - security classes control the manner by which a subject may access an object

BLP Model Access Modes

- READ
  - the subject is allowed only read access to the object
- APPEND
  - the subject is allowed only write access to the object
- WRITE
  - the subject is allowed both read and write access to the object
- EXECUTE
  - the subject is allowed neither read nor write access to the object but may invoke the object for execution

BLP Summary

- **No Read Up**
  - subject can only read an object of less or equal security level
  - referred to as the *simple security property*
    - ss-property
- **No Write Down**
  - a subject can only write into an object of greater or equal security level
  - referred to as the *-property

Covert Channels

A covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

- What condition could exist if a user was allowed roles at two different security levels in the BLP model?

SS Property - Database Inference Problems

DBMS enforces simple security rule (no read up)

- easy if granularity is entire database or at table level
- inference problems if have column granularity or row
  - if a person can query on restricted data they can infer its existence
    - SELECT Ename FROM Employee WHERE Salary > 250
  - solution is to check access to all query data
- Inference creates a covert channel

Name	FName	City	Age	Salary
Smith	John	3	35	$280
Doe	Jane	1	28	$325
Brown	Scott	3	41	$265
Howard	Shemp	4	48	$359
Taylor	Tom	2	22	$250

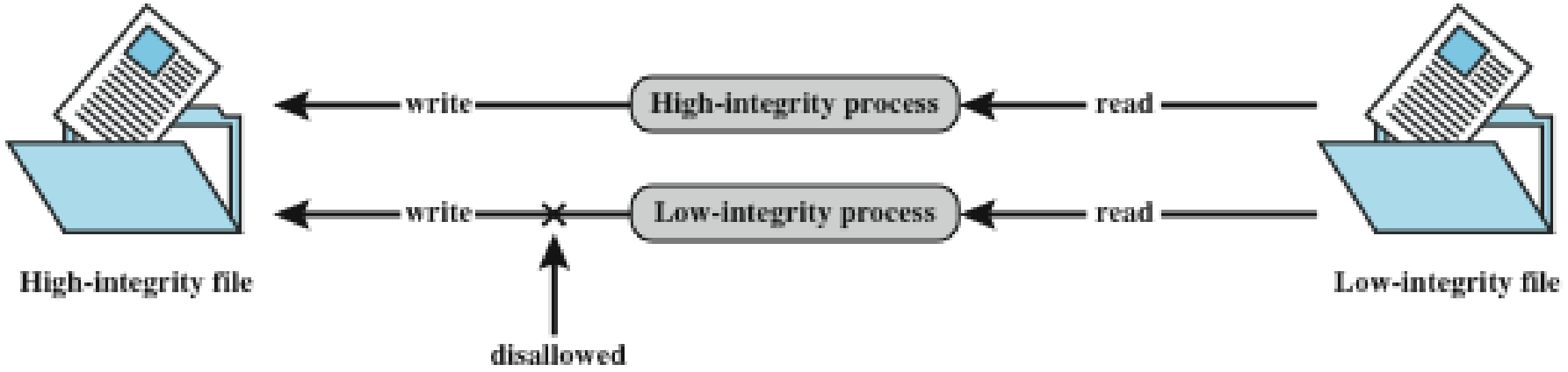
*-security rule Database Inference

- enforce *-security rule (no write down)
- problem if a low clearance user wants to insert or update a row with a primary key that already exists in a higher level row:
  - can reject, but user knows row exists - **inference**
  - can replace, compromises data integrity
- Solutions:
  - use database/table granularity
  - **polyinstantiation** and insert multiple rows with same key
    - creates other problems with conflicting entries

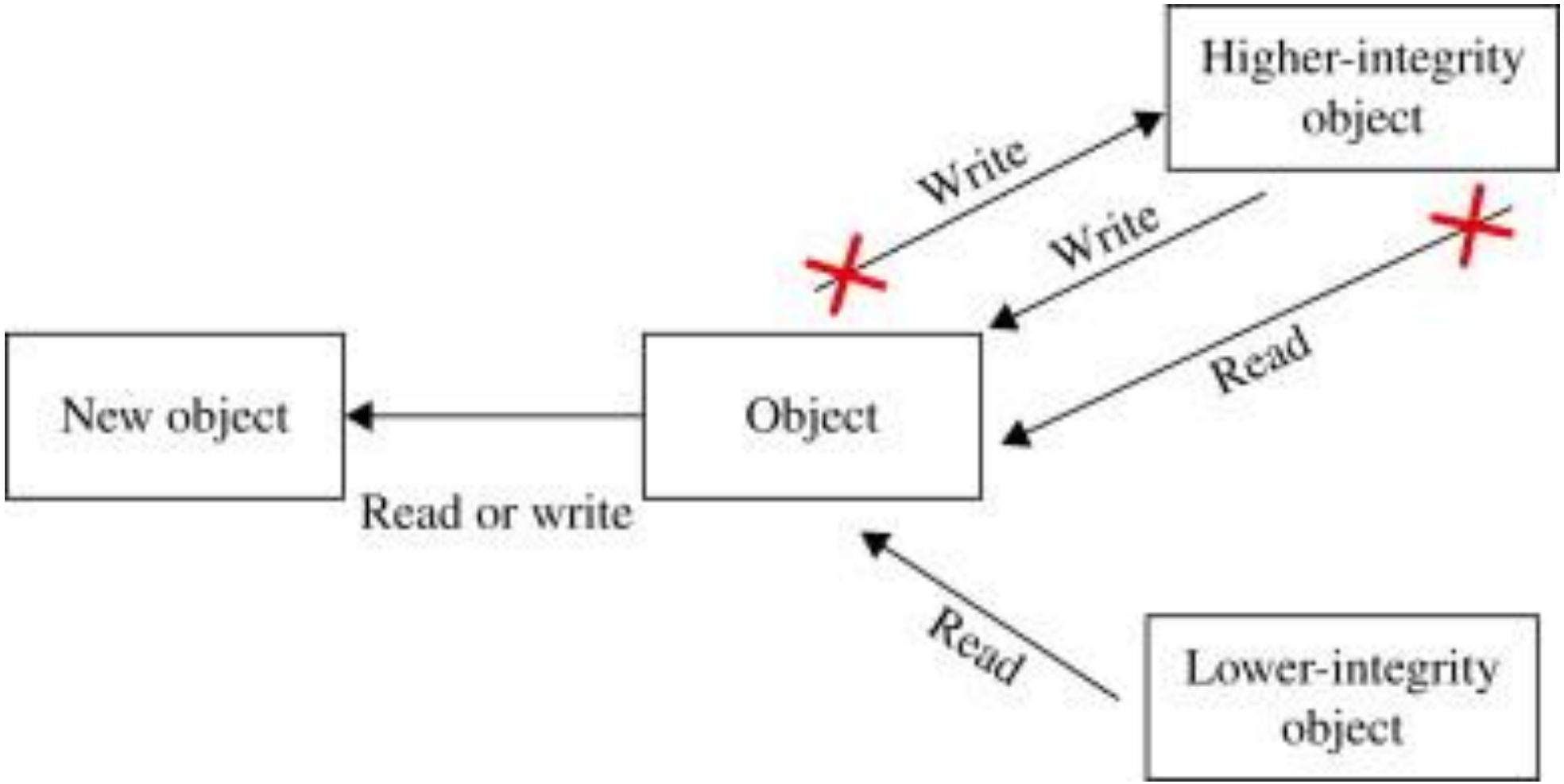
Name	FName	City	Age	Salary
Smith	John	3	35	$280
Doe	Jane	1	28	$325
Brown	Scott	3	41	$265
Howard	Shemp	4	48	$359
Taylor	Tom	2	22	$250

Biba Integrity Model

- Strict integrity policy
  - **Modify**: To write or update information in an object
  - **Observe**: To read information in an object
  - **Execute**: To execute an object
  - **Invoke**: Communication from one subject to another
- No Write UP, No Read DOWN



Biba Integrity Model



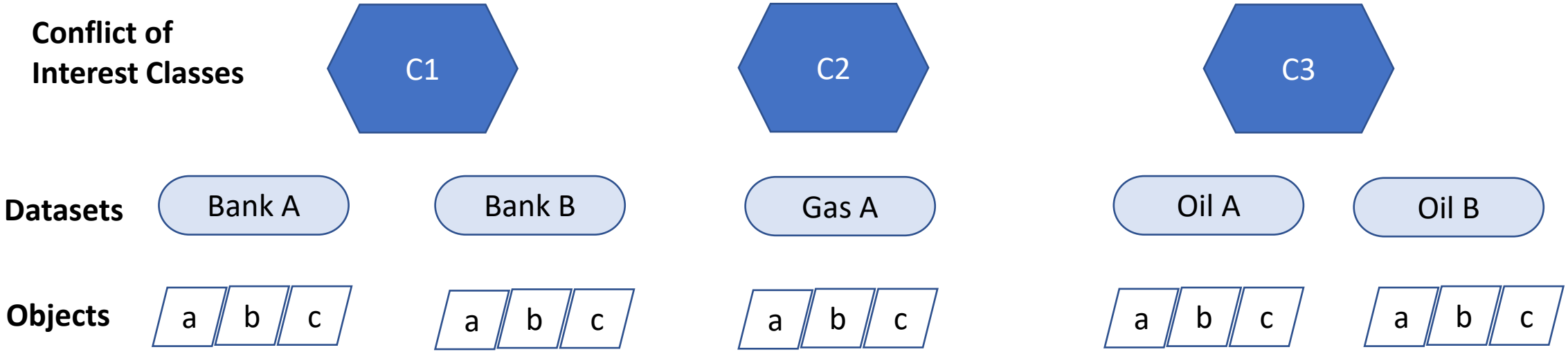
Clark-Wilson Integrity Model

- Closely models commercial operations
- Enforces separation of duties
- Uses transactions as a basis for rules
  - Two levels of integrity
    - Constrained data items (CDIs) are subject to integrity controls
    - Unconstrained data items (UDIs) are not subject to integrity controls
  - Two types of processes
    - The first are integrity verification processes (IVPs)
    - The second are transformation processes (TPs)

Brewer-Nash (Chinese Wall) Model

- Integrity, confidentiality **conflict of interest**
- Uses both discretionary and mandatory access
  - **Subjects**: Active entities that may wish to access protected objects
  - **Information**: Information organized into a hierarchy
    - **Objects**: Individual items of information, each concerning a single corporation
    - **Dataset** (DS): All objects that concern the same corporation
    - **Conflict of interest** (CI) **class**: All datasets whose corporations are in competition
  - **Access rules**: Rules for read and write access

Brewer-Nash Model Example



Operational Security Models

Fortress Model

- Keep the bad out, allow in the good
  - This was a natural model: build a series of defenses and your system can be secure
- Endpoint security
  - A new version of the fortress model
  - Involves securing of all endpoints in a network so they are secured from all threats

The Operational Model of Computer Security

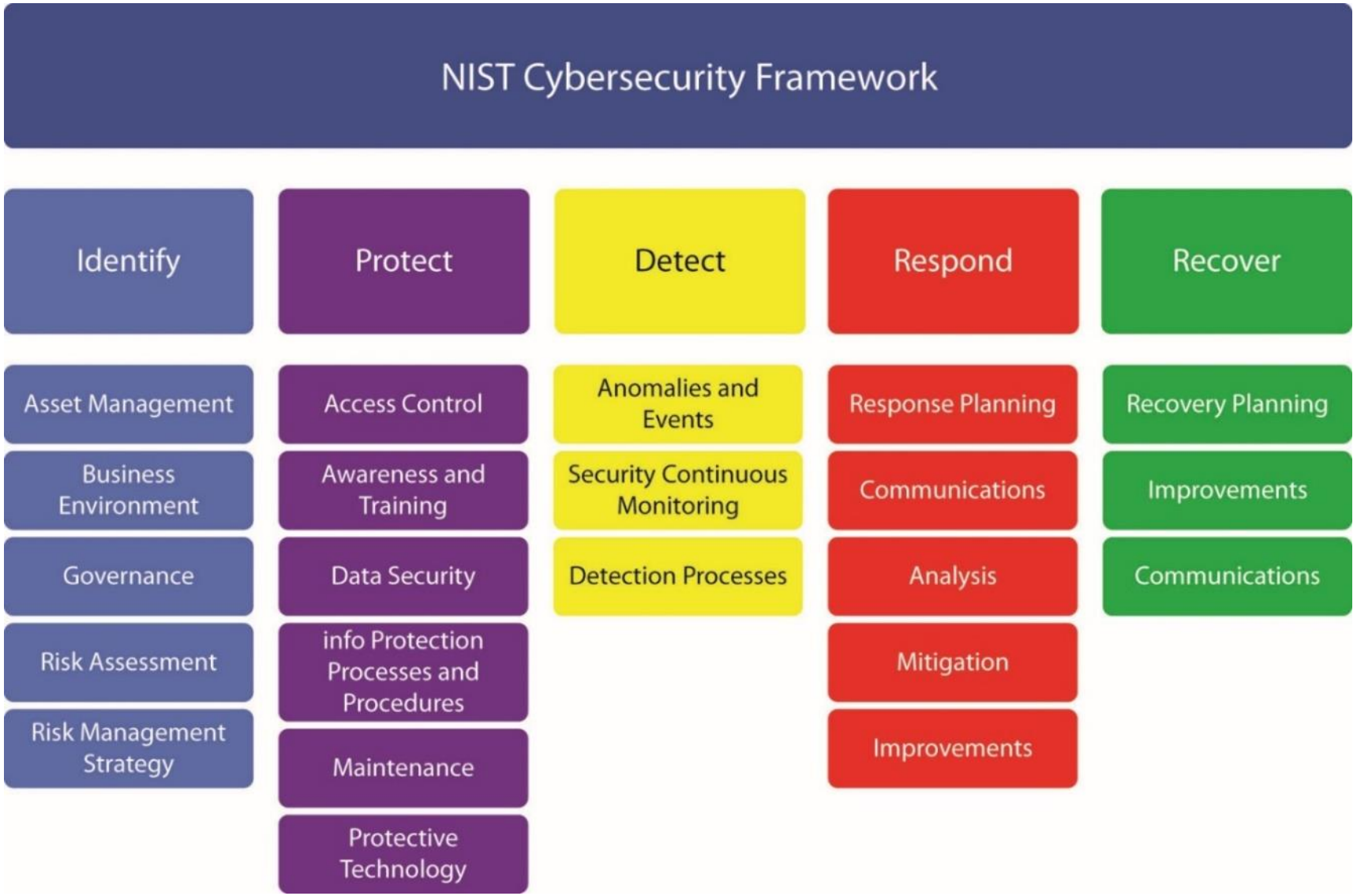
- Prevention was the focus of security for many years
  - Protection was equated with prevention
  - Somebody always seems to find a way around safeguards
- Operational model of computer security
  - One security equation is:
    Protection = Prevention + (Detection + Response)
    - Every security technique and technology falls into at least one of the three elements of the equation

Time-Based Security

- Time-based security allows us to understand the relationship between prevention, detection, and response
  - The amount of time offered by a protection device, P_t, should be greater than the time it takes to detect the attack, D_t, plus the reaction time of the organization, R_t:
    - $P_t > D_t + R_t$

Cybersecurity Framework Model

- *Framework for Improving Critical Infrastructure Cybersecurity*
  - Common taxonomy and mechanism to assist in aligning management practices with existing standards, guidelines, and practices
  - Complements and enhances risk management efforts
  - Core functions: identify, protect, detect, respond, and recover
  - Tiers represent the organization's ability, from Partial (Tier 1) to Adaptive (Tier 4)


NIST Cybersecurity Framework
Identify
Protect
Detect
Respond
Recover
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Access Control
Awareness and Training
Data Security
info Protection Processes and Procedures
Maintenance
Protective Technology
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Response Planning
Communications
Analysis
Mitigation
Improvements
Recovery Planning
Improvements
Communications

Active Defense Model

- The actual hunting of intruders inside the enterprise
  - This model capitalizes on elements of both the operational model and time-based security models
  - Built around the actions necessary to actively seek out attackers that make it past the defenses
  - Active hunters use their knowledge of baseline conditions for the systems and search for things that are abnormal

McCumber's Cube Last 10

Labtainer

- Select the file C:\tmp\Labtainer\Labtainer.ova
- Name the machine CS450, and use the provided storage path

For a copy on your personal machine, download the appropriate appliance here: https://nps.edu/web/c3o/virtual-machine-images

Assignments

- Assignment 2 Labtainer nix-commands
- Read Module 3 Chapter
- Create a disposable gmail account and **keep a record of the account name and password.** Consider violating a security rule and using the same password for all class-specific logins

NSA Codebreaker Challenge

- https://nsa-codebreaker.org/home

NSA Summer Internships

- UNR is an NSA partner institution
- Applications are NOW for next summer (Sept. 1 – Oct. 1)
- https://www.intelligencecareers.gov/NSA/students-and-internships

The Role of People in Security

Chapter 4

News

- https://it.slashdot.org/story/23/09/14/0120204/hackers-claim-it-only-took-a-10-minute-phone-call-to-shut-down-mgm-resorts?utm_source=feedly1.0mainlinkanon&utm_medium=feed

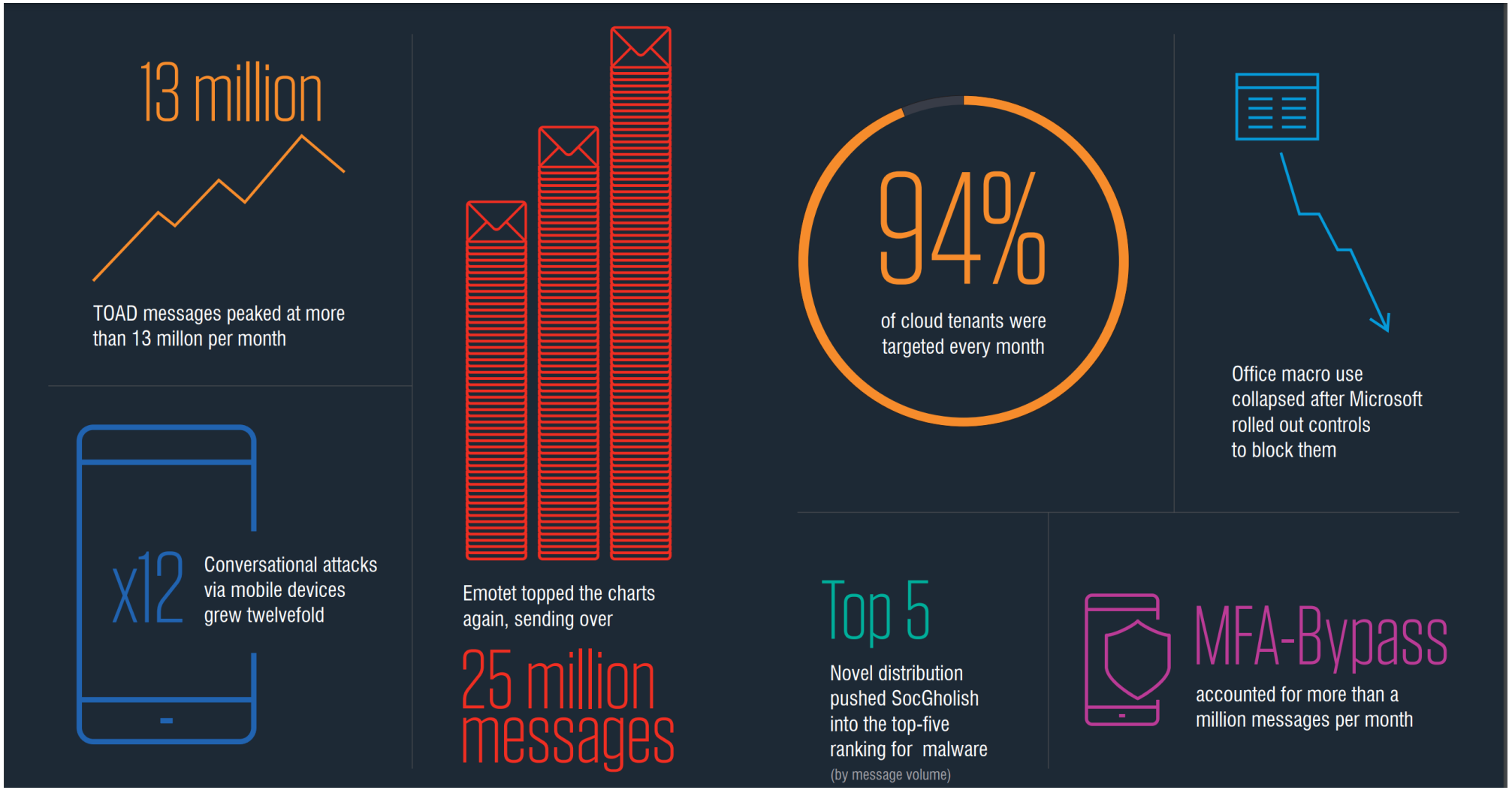
Objectives

- Define basic terminology associated with social engineering
- Describe steps organizations can take to improve their security
- Describe common user actions that may put an organization's information at risk
- Recognize methods attackers may use to gain information about an organization
- Determine ways in which users can aid instead of detract from security
- Recognize the roles training and awareness play in assisting the people side of security

People—A Security Problem

- Operational model of computer security acknowledges that prevention technologies are not sufficient to protect our computer systems and networks
  - The biggest reason is that every network and computer system has at least one human user
    - Humans are prone to make mistakes and are often easily misled or fooled

ProofPoint - The Human Factor 2023



Current Top Malware

- Emotet - https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a
- SocGholish - https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

OSINT – The Prequel to SE

http://e-mate2.s3-website-us-east-1.amazonaws.com/OSINT/OSINT.html

OSINT Challenge

http://e-mate2.s3-website-us-east-1.amazonaws.com/osint-pd/OSINT_PD_Challenge.html

What is the person's name?

What is the person's address?

What is the spouse's name?

What are the children's names?

OSINT Framework

- https://osintframework.com/

Other Tools For OSINT

https://ncr-remote.cse.unr.edu/accounts/login/

- theHarvester
- Maltego

Some Other OSINT Tools

- Google Dorking
  - https://www.stationx.net/google-dorks-cheat-sheet/
  - Filetype: This is used to find filetypes
  - Ext: This is used to identify files with specific extensions. Think of using it for finding such files like .log, which are not supposed to be indexed

Social Engineering

Social Engineering

- Social engineering is the process of convincing an authorized individual to provide confidential information or access to an unauthorized individual
- Various deceptive practices are used to convince the targeted person to:
  - Divulge information they normally would not divulge
  - Do something they normally wouldn't do

Why does social engineering work?

- One idea: Cialdini's Social Influence Theory
  - Reciprocity
  - Consistency and commitment
  - Social proof
  - Liking
  - Authority
  - Scarcity
- Another idea: Truth Default Theory
  - Assume that communication is honest until proven otherwise
  - Fits with the state of the world, where most communication is honest
  - Can usually detect deception based on whether the lie serves the potential liar's interests

Defenses

- Awareness and training
- In all the cases of impersonation, the best defense is to have processes in place that require employees to ask to see a person's ID before engaging with them if the employees do not personally know them
- Strong defenses including MFA and monitoring

Social Engineering Toolkit

- Several tools to launch SE attacks.

Example Defense Tools

- Netcraft anti-phishing
  - http://toolbar.netcraft.com/

Module 3 Assignments

- Phishing Quizzes
- Graduate Final Project Topic

Definitions

These slides are not presented in class, they are here for your reference

Tools

- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

Attacks

- Social engineering attacks target the people portion of your computing environment
  - Using psychology and technical means, the social engineer attempts to get a user to perform specific actions on a system—actions they normally would not do
  - These include clicking a link and going to a web page, running a program, saving information, and opening a file

Impersonation

- Impersonation is a common social engineering technique that can be employed in many ways
  - Third-party authorization
  - Contractors/outside parties
  - Help desk/tech support
  - Online attacks

Phishing

- Phishing is social engineering in which an attacker attempts to obtain sensitive information from a user
  - It masquerades as a trusted entity in an e-mail or instant message sent to a large group of often random users
  - Attacker attempts to obtain usernames, passwords, credit card numbers, and details about the user's bank accounts
  - Attacker points users to fake, non-reputable websites or sends bulk e-mails instructing users to click a fake link to verify that their account has not been tampered with
  - Phishing with open redirects: https://www.microsoft.com/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

Smishing

- Smishing is a version of a phishing attack using the Short Message Service (SMS) on victims' cell phones
  - It begins with an SMS message directing a user to a URL from which the attacker then can serve up a variety of attack vectors, including forms of malware
  - This attack works primarily because of the principles of urgency and intimidation

Vishing

- Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking
  - Takes advantage of the trust people place in the telephone network
  - Attackers can spoof (simulate) calls from legitimate entities using Voice over IP (VoIP) technology
  - Voice messaging can also be compromised
  - Attackers are after credit card numbers or other information that can be used in identity theft

Spam

- Spam is bulk unsolicited e-mail
  - It is not generally considered a social engineering issue
  - Spam can be a security concern
  - Legitimate spam is sent by a company advertising a product or service
  - Malicious spam includes an attachment containing malicious software designed to harm your system, or a link to a malicious website that may attempt to obtain personal information from you

Spam over Internet Messaging (SPIM)

- SPIM is spam delivered via an instant messaging application
  - The purpose of hostile SPIM is the same as that of spam—the delivery of malicious content or links and getting an unsuspecting user to click them, thus initiating the attack

Spear Phishing

- Spear phishing is the term used for a phishing attack that targets a specific group of people or businesses with something in common
  - Because a specific group is being targeted, such as senior executives, the ratio of successful attacks (that is, the number of responses received) to the total number of e-mails or messages sent usually increases
    - A targeted attack will seem more plausible than a message sent to users randomly

Whaling

- A whaling attack is one where the target is a high-value person, such as a CEO or CFO
  - Whaling attacks are not performed by attacking multiple targets and hoping for a reply, but rather are custom-built to increase the odds of success

Pharming

- Pharming consists of misdirecting users to fake websites made to look official
  - Using phishing, individuals are targeted one by one by sending out e-mails
  - To become a victim, the recipient must take an action

Dumpster Diving

- Dumpster diving is the process of going through a target's trash in hopes of finding valuable information that might be used in a penetration attempt
  - One common place to find information, if the attacker is in the vicinity of the target, is in the target's trash

Shoulder Surfing

- Shoulder surfing does not require direct contact
  - The attacker may simply look over the shoulder of the user at work, for example, or may set up a camera or use binoculars to view the user entering sensitive data
  - Example of information desired: PINs or gate codes
- Shoulder surfing prevention techniques
  - Small shield surrounding keypad or scramble location of the numbers on keypad
  - Best defense is user awareness of surroundings
  - Be aware of attacker starting conversation with target

Tailgating/Piggybacking

- Tailgating (or piggybacking) is the simple tactic of following closely behind a person who has just used his own access card or PIN to gain physical access to a room or building
  - An attacker can gain access to the facility without having to know the access code or acquire an access card
  - Prevent tailgating by using procedures ensuring nobody follows too closely or is in a position to observe actions
  - Can use a mantrap, which utilizes two doors to gain access to the facility

Eliciting Information

- Calls to or from help desk and tech support units can be used to elicit information
  - A skilled social engineer can use a wide range of psychological techniques to convince people whose main job is to help others to perform tasks resulting in security compromises

Prepending

- Prepending is defined as the act of adding something else to the beginning of an item
  - When used in a social engineering context, prepending is the act of supplying information that another will act upon, frequently before they ask for it, in an attempt to legitimize the actual request, which comes later

Identity Fraud

- Identity fraud is the use of fake credentials to achieve an end
  - This can be a high-risk endeavor, such as pretending to be an official representative of a government agency or a regulator, or it can be lower risk, such as showing up as the person who waters the plants

Invoice Scams

- Invoice scams are just that—a scam using a fake invoice in an attempt to get a company to pay for things it has not ordered
  - The premise is simple: send a fake invoice and then get paid

Credential Harvesting

- Credential harvesting is the collection of credential information, such as user IDs, passwords, and so on, thus allowing an attacker a series of passes to the system
  - The objective of a credential harvest is just that—credentials

Reverse Social Engineering

- Reverse social engineering occurs when the attacker hopes to convince the target to initiate the contact
  - Attack is successful since target is initiating the contact
    - Attacker may not have to convince target of their authenticity
    - The tricky part of this attack is convincing the target to make that initial contact
  - Methods to accomplish an attack
    - Send out a spoofed e-mail with contact information
    - Target an organization undergoing organizational change

Reconnaissance

- Reconnaissance is a military term used to describe the actions of surveying a battlefield to gain information prior to hostilities
  - In the field of cybersecurity, the concept is the same—an adversary will examine the systems they intend to attack, using a wide range of methods

Hoax

- A hoax can be very damaging if it causes users to take some sort of action that weakens security
  - Training and awareness are the best and first line of defense for both users and administrators
  - Users should be trained to be suspicious of unusual e-mails and stories and should know who to contact in the organization to verify their validity when received
  - Hoaxes often also advise the user to send it to their friends so they know about the issue as well—and by doing so, they help spread the hoax

Watering Hole Attack

- A watering hole attack involves the infecting of a target website with malware
  - In some of the cases detected, the infection was constrained to a specific geographical area
  - These are not simple attacks, yet they can be very effective at delivering malware to a specific groups of end users
  - Watering hole attacks are complex to achieve and appear to be backed by nation-states and other high-resource attackers

Typo Squatting

- Typo squatting is an attack form that involves capitalizing on common typographical errors
  - If a user mistypes a URL, then the result should be a 404 error, or "resource not found"
    - But if an attacker has registered the mistyped URL, then the user would land on the attacker's page
  - This attack pattern is also referred to as URL hijacking, using a fake URL, or brandjacking if the objective is to deceive based on branding

Influence Campaigns

- Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people's minds on a topic
  - One can engage in an influence campaign against a single person, but the effect is limited
  - Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation

Poor Security Practices (1 of 7)

- A significant portion of human-created security problems results from poor security practices
  - These poor practices may be:
    - Due to an individual user who is not following established security policies or processes
    - Caused by a lack of security policies, procedures, or training within the user's organization

Poor Security Practices (2 of 7)

- Password selection
  - Users tend to pick passwords that are easy to remember
    - Names of family members, pets, sports teams
  - The more the attacker knows about the user, the better the chance of discovering the user's password
    - Organizations have encouraged users to mix upper- and lowercase characters and to include numbers and special characters in their password

Poor Security Practices (3 of 7)

- Shoulder surfing
  - Involves the attacker directly observing the target entering sensitive information on a form, keypad, or keyboard
- Piggybacking
  - Happens because the person is not paying attention to the context of their situation
- Dumpster diving
  - Process of going through a target's trash in hopes of finding valuable information that can be used in a penetration attempt

Poor Security Practices (4 of 7)

- Installing unauthorized hardware and software
  - Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems
  - A backdoor is an avenue used to access a system while circumventing normal security mechanisms and can often be used to install additional executable files that can lead to more ways to access the compromised system
  - Common examples include unauthorized communication software and a modem; a wireless access point; and games

Poor Security Practices (5 of 7)

- Data handling
  - Understanding the responsibilities of proper data handling associated with one's job is an important training topic
  - Include a training clause for certain data elements requiring special handling because of contracts, laws, or regulations
  - The spirit of the training clause is you get what you train; if security over specific data types is a requirement, it should be trained

Poor Security Practices (6 of 7)

- Physical access by non-employees
  - Significant deterrent to unauthorized individuals is to require employees to wear identification badges at work
    - Method to quickly spot who has permission to have physical access to the organization and who does not
    - Requires employees to actively challenge individuals who are not wearing the required identification badge
  - Personnel with legitimate access may have an intent to steal intellectual property or exploit the organization
    - Contractors, consultants, partners, custodial staff

Poor Security Practices (7 of 7)

- Clean desk policies
  - Specify that sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian
    - Example: leaving the desk area and going to the bathroom can leave information exposed and subject to compromise
  - Policy should identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards and mouse pads or in unsecured desk drawers

People as a Security Tool

- Social engineering paradox
  - People are the biggest problem and security risk, but also the best tool in defending against a social engineering attack
- To fight social engineering attacks, create policies and procedures that establish roles and responsibilities for security administrators and all users
  - Management expectations, security-wise, from employees
  - Description of items the organization is trying to protect, and mechanisms important for that protection

Security Awareness (1 of 2)

- Active security awareness program
  - Single most effective method to counter potential social engineering attacks
  - The extent of the training will vary depending on the organization's environment and the level of threat
  - Training should stress the type of information that the organization considers sensitive and that may be the target of a social engineering attack
  - Employees should be aware of attack indicators
  - Employees should be taught to be cautious about revealing personal information

Security Awareness (2 of 2)

- Social networking and P2P
  - Confusing sharing information with friends and sharing business information with those who don't need to know it is a line people are crossing on a regular basis
    - Be careful not to mix social and business communications
  - Users also need to understand the importance of not using common programs such as torrents and other peer-to-peer (P2P) file-sharing communication programs in the workplace

Cryptographic Tools

News

- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.welivesecurity.com/2022/09/06/worok-big-picture/

NSA Code Breaker Challenge 2024

Overview

- The Codebreaker Challenge consists of a series of tasks that are worth a varying number of points based upon their difficulty. Schools will be ranked according to the total number of points accumulated by their students.
- Solutions may be submitted at any time for the duration of the Challenge.
- This year the tasks are strictly sequential, and one must be solved before the next one becomes available.
- Each task in this year's challenge will require a range of skills. We need you to call upon all of your technical expertise, your intuition, and your common sense.

Background

- Foreign adversaries have long strived to gain an advantage against the might of the United States Armed Forces. While matching the USA on the battlefield is a costly and risky proposition, our adversaries are always looking for ways to balance the playing field. A serious and real threat is the infiltration and sabotage of military operations before the fight even breaks out.
- Fortunately, the NSA is always recruiting bright young individuals to help protect our country! In fact, a bunch of your friends graduated last year and have been busy at work in their Developmental Programs.
- You have returned to NSA on your final Cooperative Education tour and are visiting your friend Aaliyah who is currently employed full-time in the Intelligence Analysis Development Program. Intelligence Analysts are always scouring through collected Signals Intelligence (SIGINT) for threat indicators. Aaliyah recently attended a briefing that highlighted Nation-State Advanced Persistent Threats (APT) targeting our Defense Industrial Base (DIB) contractors.

Warm Up Quiz

- What do you remember from the chapter?
- http://e-mate2.s3-website-us-east-1.amazonaws.com/cryptography/cryptography.html

Key Points to Remember

- Crypto strength vs speed and resources
  - Stronger crypto takes more power and time
- Keys must be protected
- Be aware of what part of the CIA Triad + 2 you are addressing
- Don't bake your own crypto
  - Unless you are an expert crypto developer

In Class Quiz

- Based on these slides – Don't jump ahead

Two Good Crypto Tools

- Online - https://gchq.github.io/CyberChef/
- https://www.cryptool.org/en/

Encoding vs. Encryption

Some developers attempt to use encoding as encryption:

https://www.zdnet.com/article/study-shows-programmers-will-take-the-easy-way-out-and-not-implement-proper-password-security/

Hexidecimal:

- 0 – 9, A - F
- Example:
  - 54 68 69 73 20 69 73 20 74 68 65 20 73 65 63 72 65 74 20 6d 65 73 73 61 67 65

Question 1 What is the plaintext?

Encoding vs. Encryption

Base 64:

- A – Z, a –z, 0 -9, +/=
- Example:
  - VGhpcyBpcyBhbm90aGVyIHNlY3JldCBtZXNzYWdl

Question 2 What is the plaintext?

NCL Decoding Example 1

- Question 3 Decode this stolen password:
  - 3477686963684649454c4437

NCL Decoding Example 2

Question 4 Decode the stolen password

NDlmaW5lYmx1ZTkx

Encryption Terminology

- Plaintext:
  - This is the original message or data that is fed into the algorithm as input.
- Encryption algorithm:
  - The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key:
  - The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext:
  - This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- Decryption algorithm:
  - This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Encryption Categories

- Hashing
- Symmetrical encryption
- Asymmetrical encryption

Hashing

Properties of a Useful Hash Function

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Uses of a Hash

- Used to verify file **Integrity**
  - Examples?
  - Intrusion detection?
- Used for **Confidentiality**
  - Password files – really just part of the encryption process
- Message **Authentication**

Hashing for File Integrity

- Check hash of CrypTool download on CyberChef – Sha2
  - Hash other strings and try MD5
- Intrusion detection
  - Store H(F) for each file on a system and secure the hash values

Hashing for Confidentiality

- Password files - in Labtainer – sudo cat /etc/shadow
  - Include a Salt
  - Duplicate passwords can improve chances of cracking passwords

Hashed Message Authentication

Protects against active attacks

- Verifies received message is authentic
  - Contents have not been altered
  - From authentic source
  - Timely and in correct sequence
- Can use conventional encryption
  - Only sender and receiver share a key

Message Authentication Without Confidentiality

- Message encryption by itself does not provide a secure form of authentication
- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically, message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
  - There are a number of applications in which the same message is broadcast to a number of destinations
  - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
- **Thus, there is a place for both authentication and encryption in meeting security requirements**

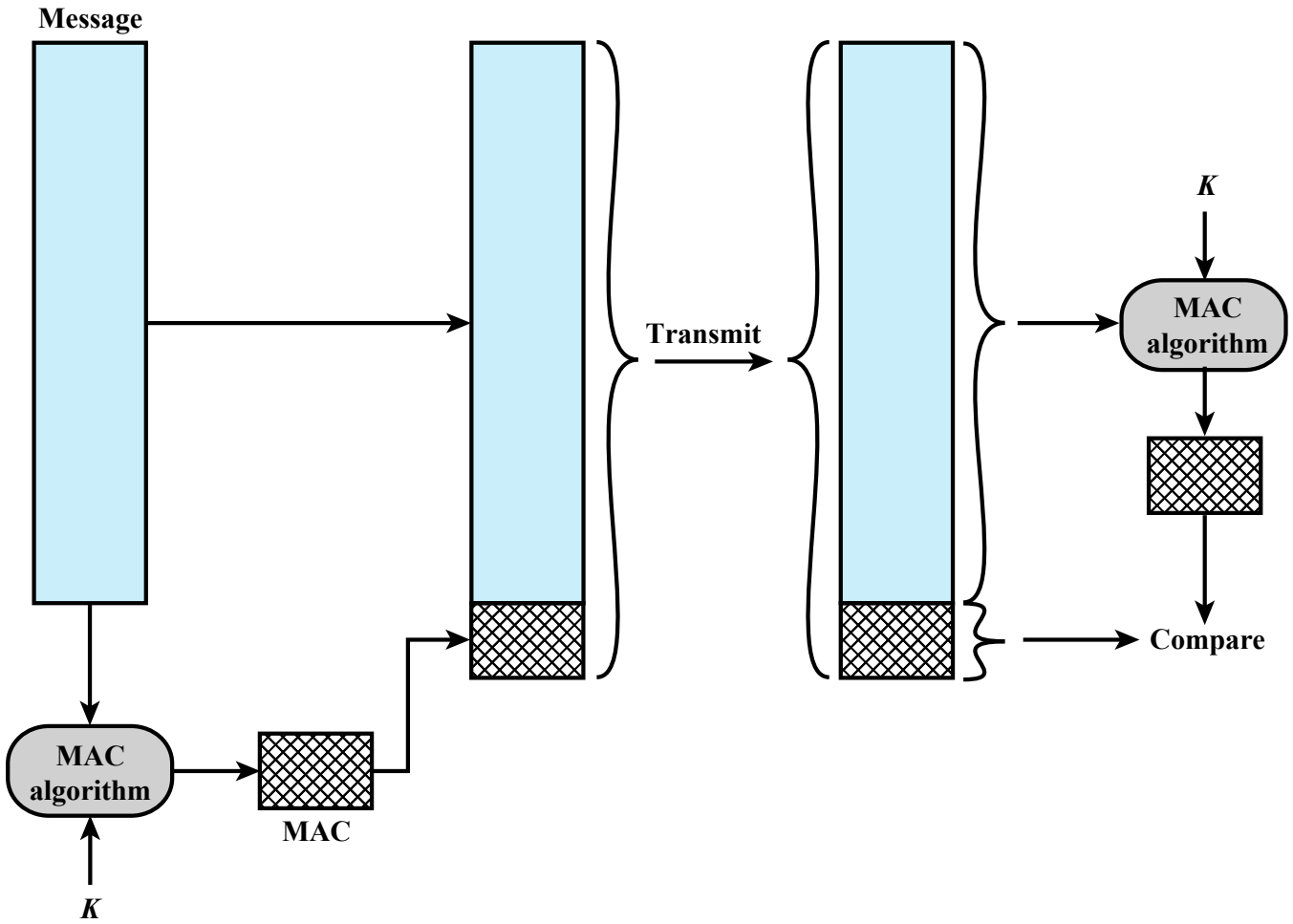


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Question 5 Does this provide message integrity?

This will be discussed in more detail in PKI section.

Security of Hash Functions

- There are two approaches to attacking a secure hash function:
  - Cryptanalysis
    - Exploit logical weaknesses in the algorithm
  - Brute-force attack
    - Strength of hash function depends solely on the length of the hash code produced by the algorithm
  - Cryptool2 hash collision demos
- SHA most widely used hash algorithm

Symmetric Encryption

Classic Encryption

Symmetric Encryption

- Goal
  - Confidentiality
- Classic Encryption Algorithms
  - Substitution
    - Caesar (ROT)
    - Vingenere Cipher
    - Pigpen

Caesar Cipher (ROT3)

https://www.dcode.fr/caesar-cipher

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

Vigenère Square

Plaintext: this is the secret message (row)
Key: wolfpack (column for encryption, row for decryption)
Ciphertext: pvtx xs vra gphgev wagdfve

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Challenge Example

Key: secretkeys (row)

Ciphertext: a eo r ltmocj

find letter, plaintext is column

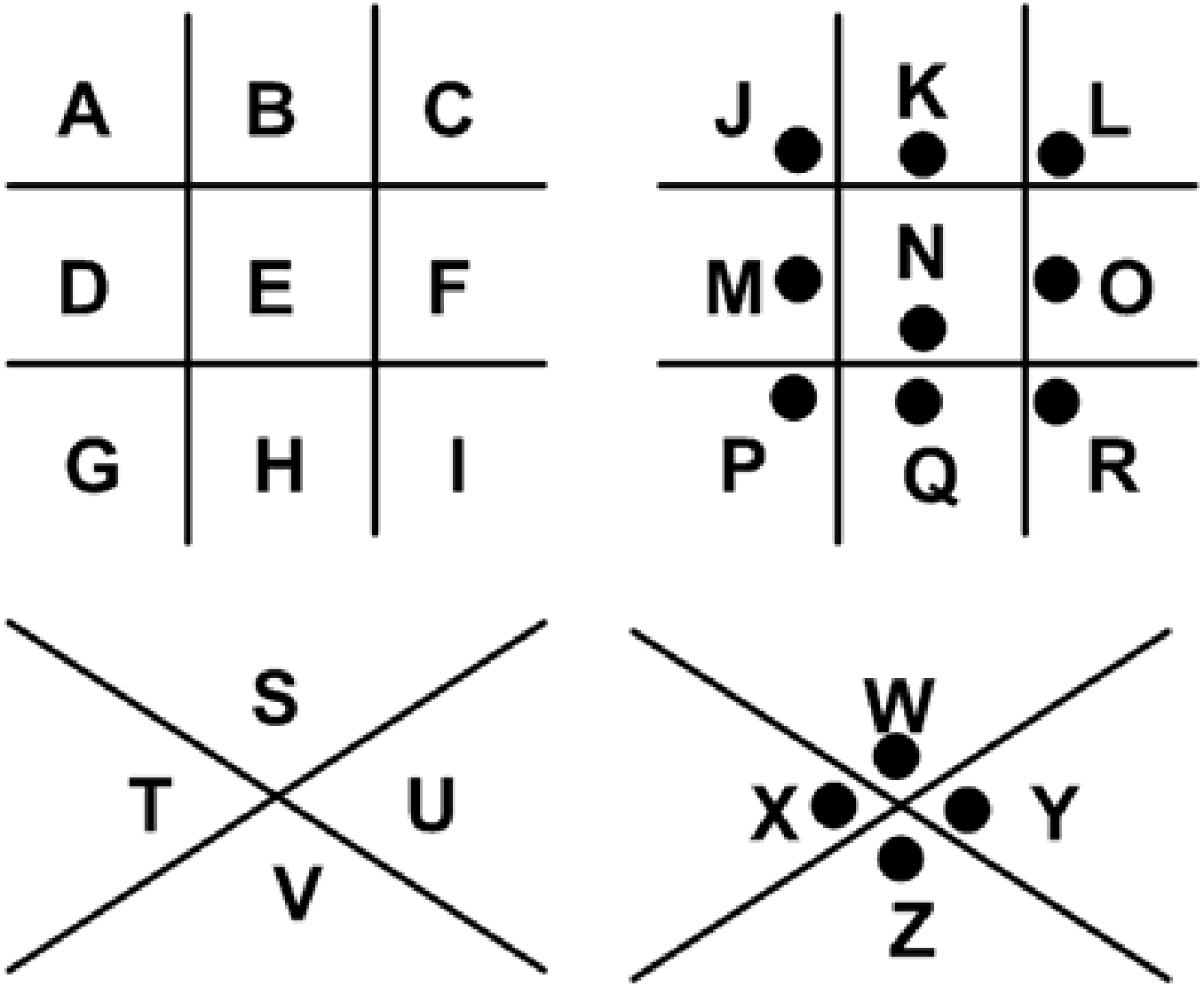
Question 6 What is the plaintext?

Link to bigger table: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Pigpen Cipher

Used by Freemasons in the 18th century



Modern Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements for secure use:
    - Need a strong encryption algorithm
    - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

Modern Symmetric Encryption

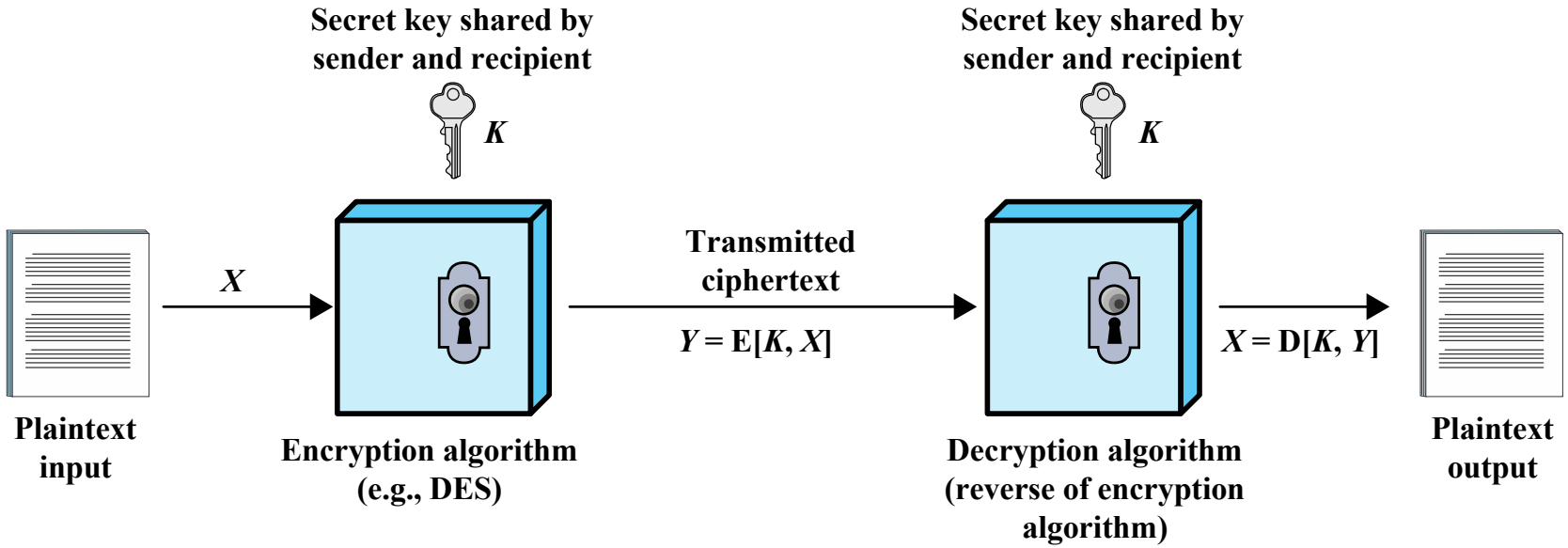


Figure 2.1 Simplified Model of Symmetric Encryption

Comparison of Three Popular Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Twofish was also a finalist to replace DES and supports up to 256 bits

Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
- If successful all future and past messages encrypted with that key are compromised

Brute-Force Attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - On average half of all possible keys must be tried to achieve success

Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
  - Alternative techniques developed to increase the security of symmetric block encryption for large sequences –*beyond scope of this class*
  - Overcomes the weaknesses of ECB

Block and Stream Ciphers

Block Cipher

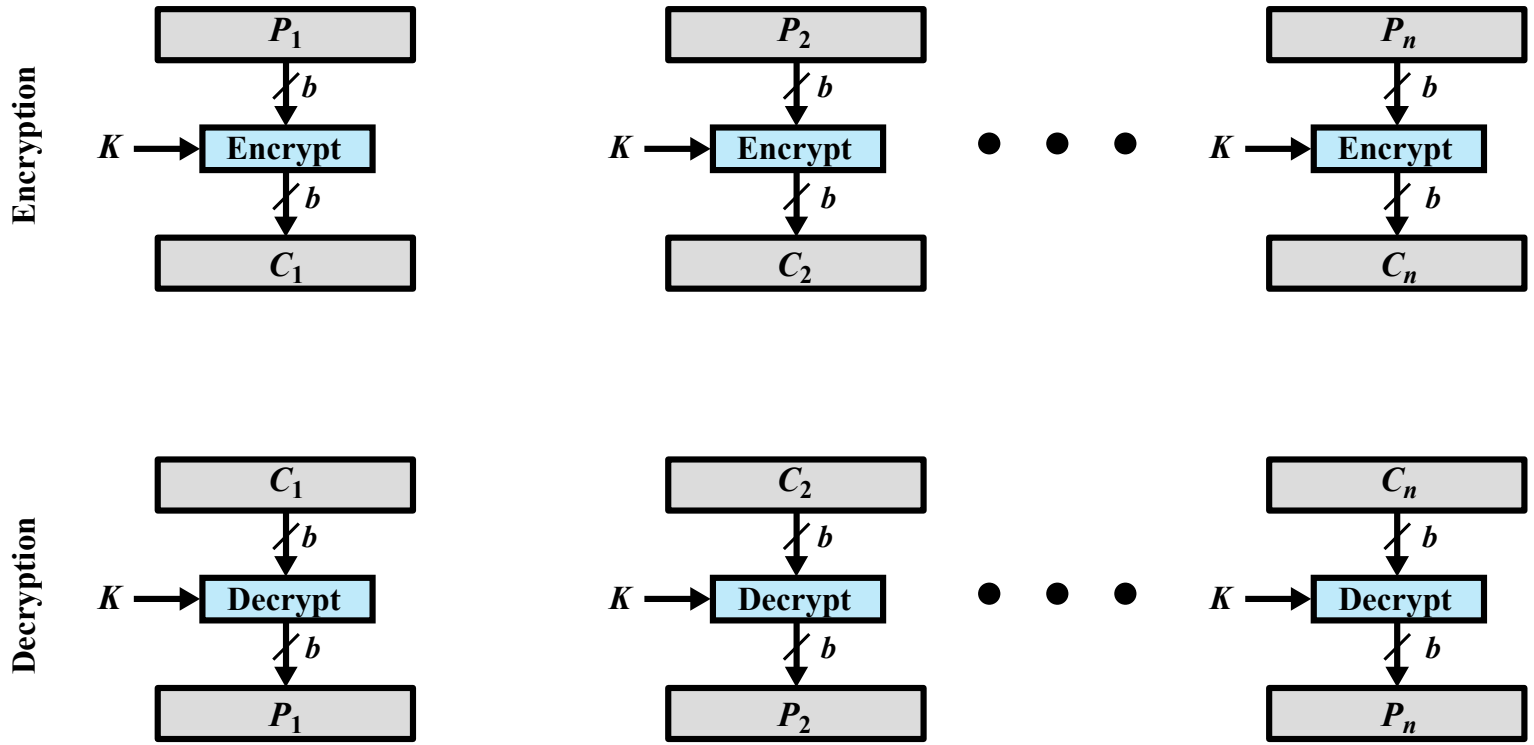
- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

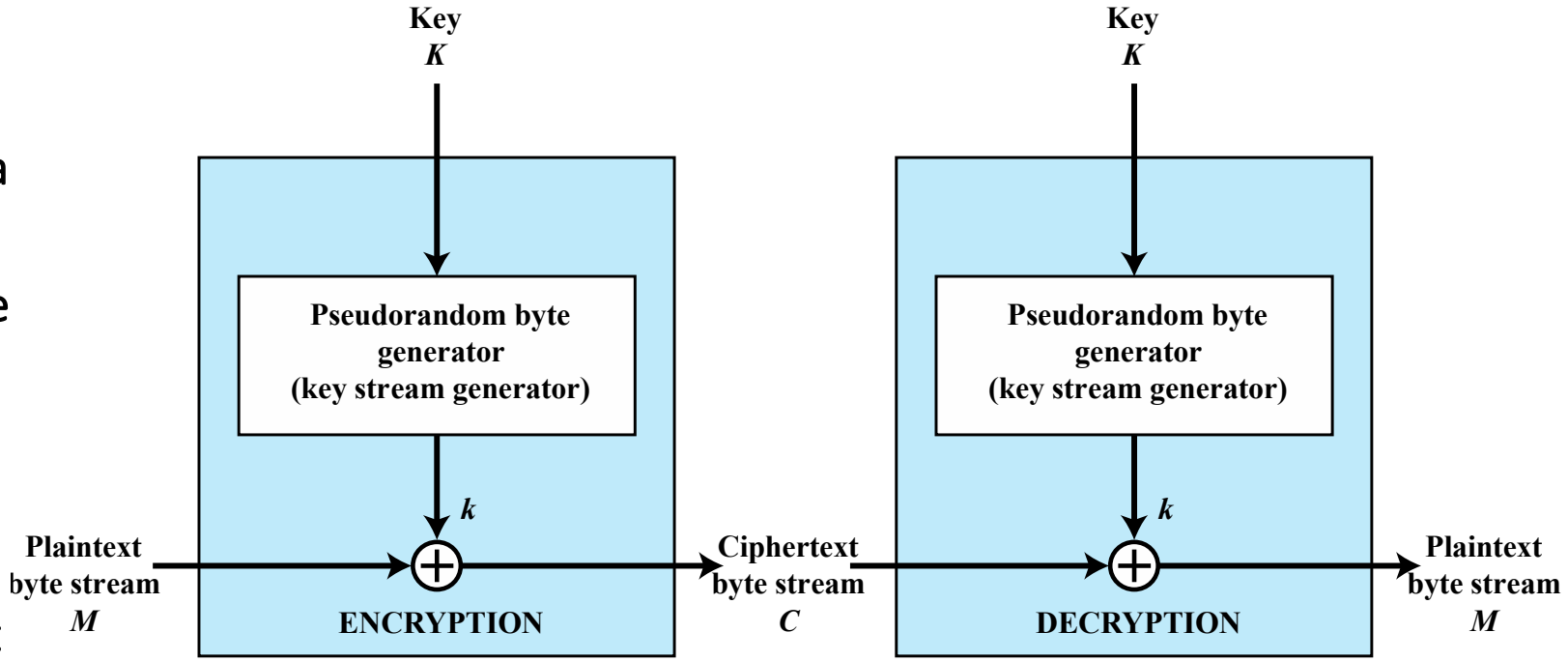
Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common



Stream Cipher

- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key



Asymmetric Encryption

Asymmetric Encryption Structure

Publicly proposed by Diffie and Hellman in 1976

Based on mathematical functions

Asymmetric

- Uses two separate keys
- Public key and private key

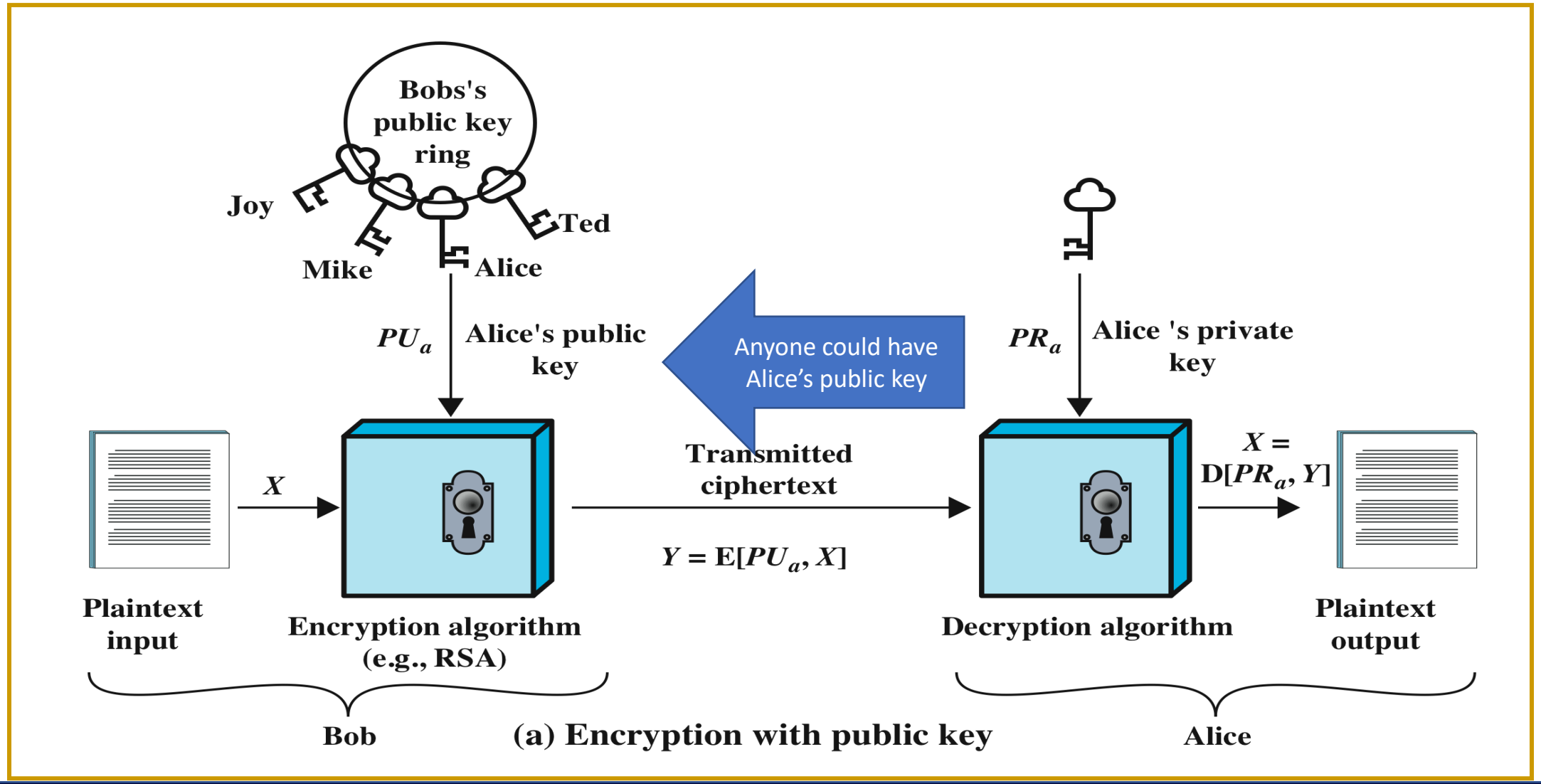
Some protocol is needed for key distribution

Using Asymmetric Encryption to Share a Symmetric Encryption Key

- Diffie-Hellman key exchange - https://www.youtube.com/watch?v=YEBfamv-_do

PGP Exercise

Public Key Encryption Without Authentication



Public-Key Crypto With Authentication

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

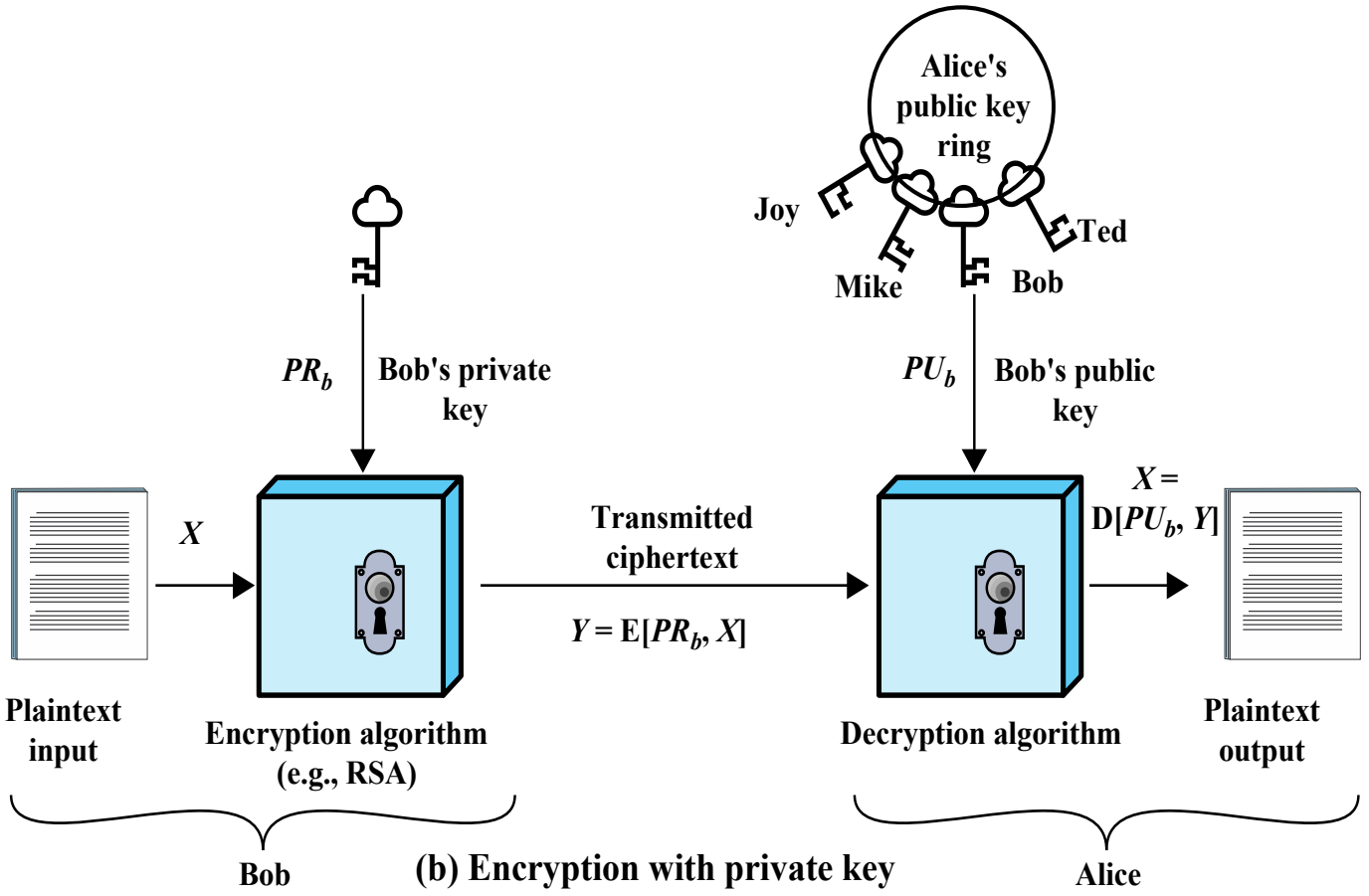


Figure 2.6 Public-Key Cryptography

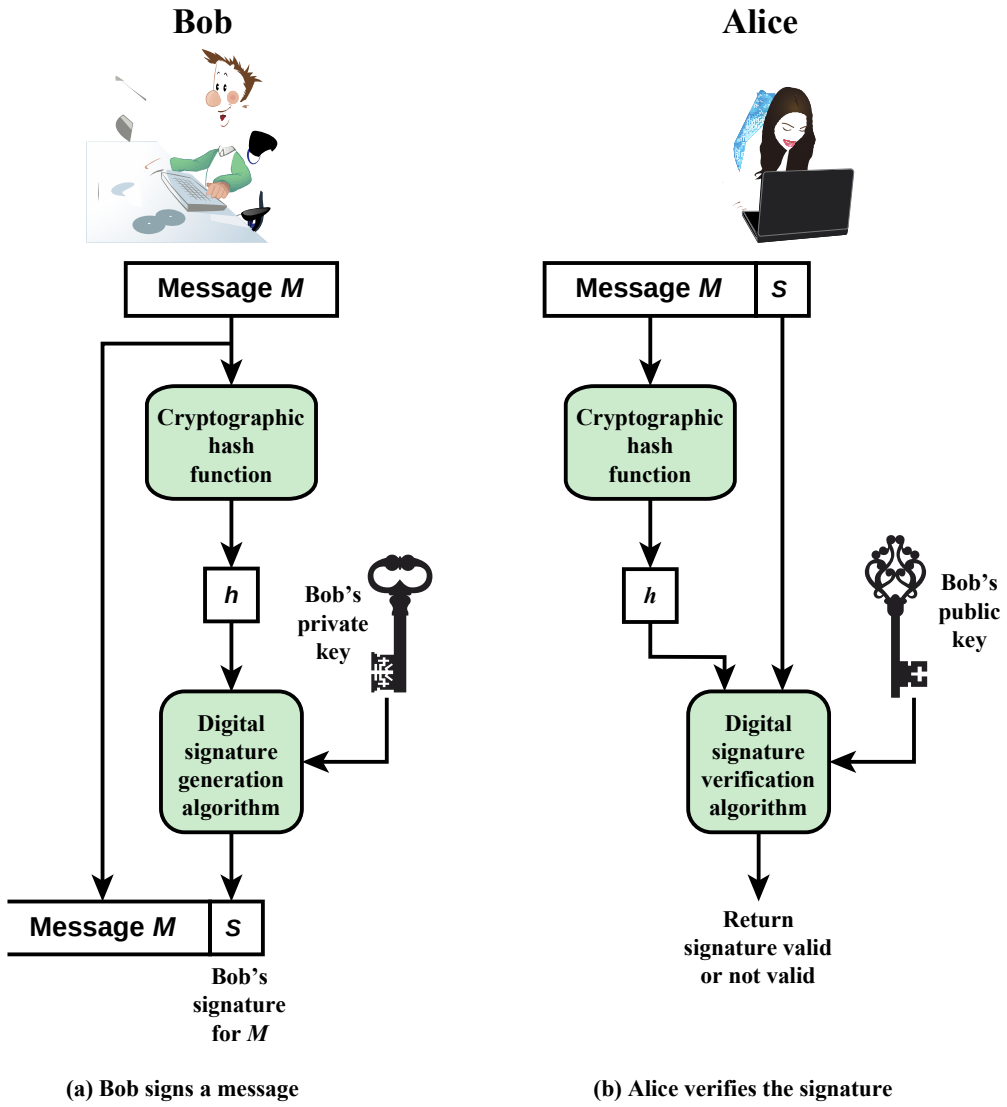
Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977
	Most widely accepted and implemented approach to public-key encryption
	Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
Diffie-Hellman key exchange algorithm	Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages
	Limited to the exchange of the keys
Digital Signature Standard (DSS)	Provides only a digital signature function with SHA-1
	Cannot be used for encryption or key exchange
Elliptic curve cryptography (ECC)	Security like RSA, but with much smaller keys

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:
  - ”The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.”
- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block
- FIPS 186-4 specifies the use of one of three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

Digital Signature Process

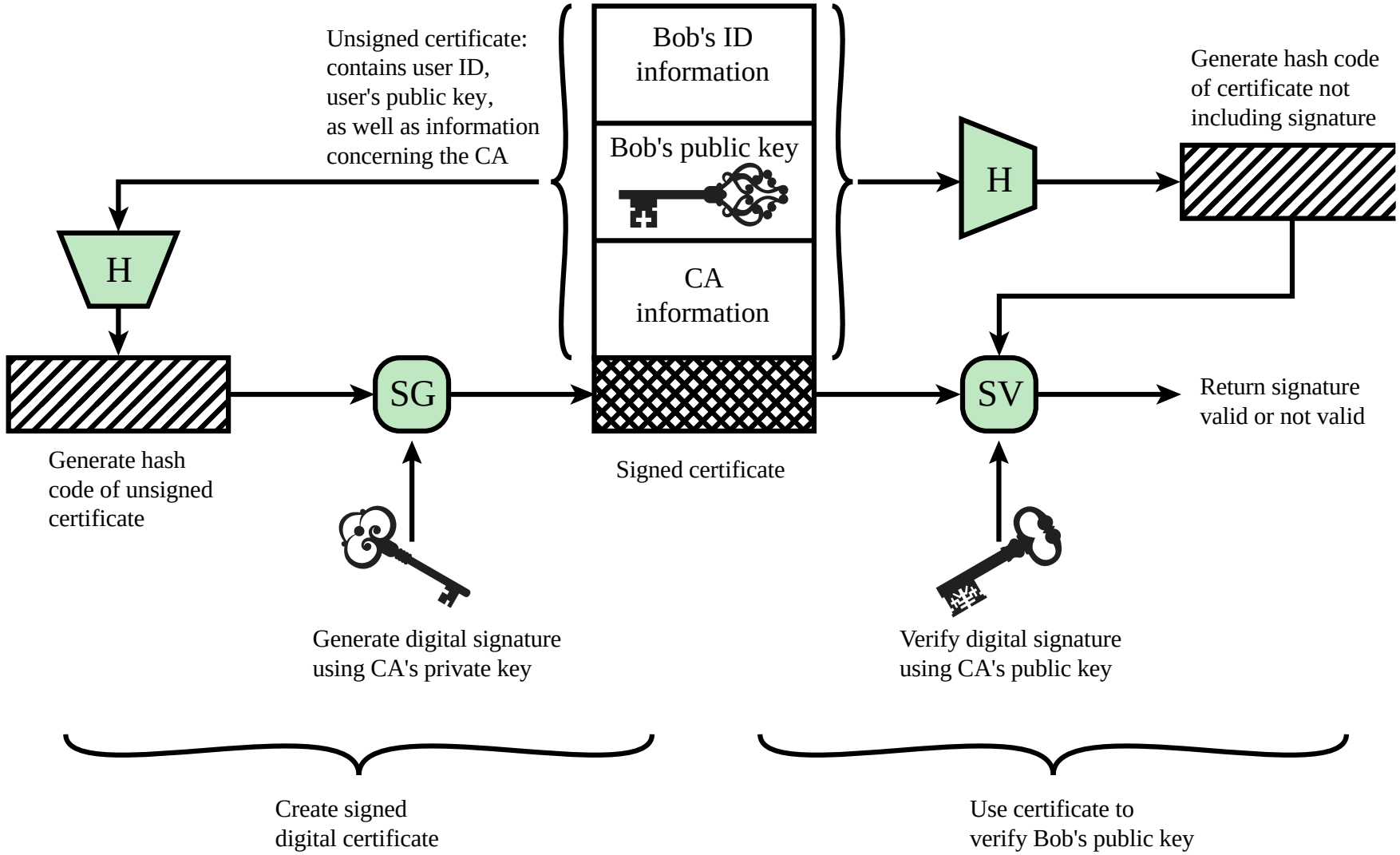


(a) Bob signs a message

(b) Alice verifies the signature

Public Key Infrastructure (PKI)

Public-Key Certificates



View Digital Certificates

- On Websites
- In Windows - certmgr

Post-Quantum PKI

https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum

Random Numbers Generators

Uses include generation of:

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

Random Number Requirements

Randomness

- Criteria:
  - Uniform distribution
    - Frequency of occurrence of each of the numbers should be approximately the same
  - Independence
    - No one value in the sequence can be inferred from the others

Unpredictability

- Each number is statistically independent of other numbers in the sequence
- Opponent should not be able to predict future elements of the sequence on the basis of earlier elements

Insecure Random Number Generation

- java.util.Random is not secure
  - https://intellipaat.com/community/31529/difference-between-java-util-random-and-java-security-securerandom
- Don't bake your own
  - https://owasp.org/www-community/vulnerabilities/Insecure_Randomness

Practical Encryption Applications

Common to encrypt data in transit

- VPNs
- HTTPS
- TLS

Less common to encrypt data at rest

- There is often little protection beyond domain authentication and operating system access controls
- Data are archived for indefinite periods
- Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt data at rest:

- Use a commercially available encryption package
- Back-end appliance
- Library based tape encryption
- Background laptop/PC data encryption

Steganography

Kali stego demonstration

Module 4 Assignment

- Complete the template AND spreadsheet
- Save them in their original directory on the VM

Authentication and Remote Access

News

- https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848
- https://blog.google/technology/safety-security/google-password-manager-passkeys-update-september-2024/
- https://www.huntress.com/blog/cracks-in-the-foundation-intrusions-of-foundation-accounting-software
- https://techcrunch.com/2024/09/19/apples-new-macos-sequoia-update-is-breaking-some-cybersecurity-tools

Module 4 Recap

- Start the lab with –r option on public machines
- Don't tamper with the .lab file
- Question 7 – more than 16 attempts is possible because it is hashing random strings – there may be duplicates on the last digit
- Question 12 – The first script was trying to match a known hash. The second script was trying to find any two hashes that matched.
- Comments were good
  - The redundant commands was intended to let you observe the results and see how yours matched theoretical averages
- Study PKIP in the text if you are going to take Security+

Introduction

- There are three steps in the establishment of proper privileges
  - Authentication, authorization (access control), and accounting
    - Commonly combined and simply referred to as AAA
- The privileges process:
  - Credential Management (ICAMS)
  - Authentication
  - Remote Access Authentication
  - Authorization (Access Control)
  - Accounting (logging) is covered in later module

Identity, Credential, and Access Management (ICAM)

Identity Management

- Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE
- Goal is to establish a trustworthy digital identity that is independent of a specific application or context
- Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program

Identity Management

- An IDENTITY is the set of characteristics (also called "attributes") that describe an individual within a given context:
  - Your identity within the context of the Department of Motor Vehicles (DMV) is different from your identity within the context of your bank.

- IDENTITY PROOFING is the process by which an identity is first established.

Credential Management

- Credential management is the processes, services, and software used to store, manage, and log the use of user credentials
  - Credential management solutions are typically aimed at helping end users manage their growing set of passwords
- Credential management products
  - Provide secure means of storing user credentials
  - Make credentials available across a wide range of platforms

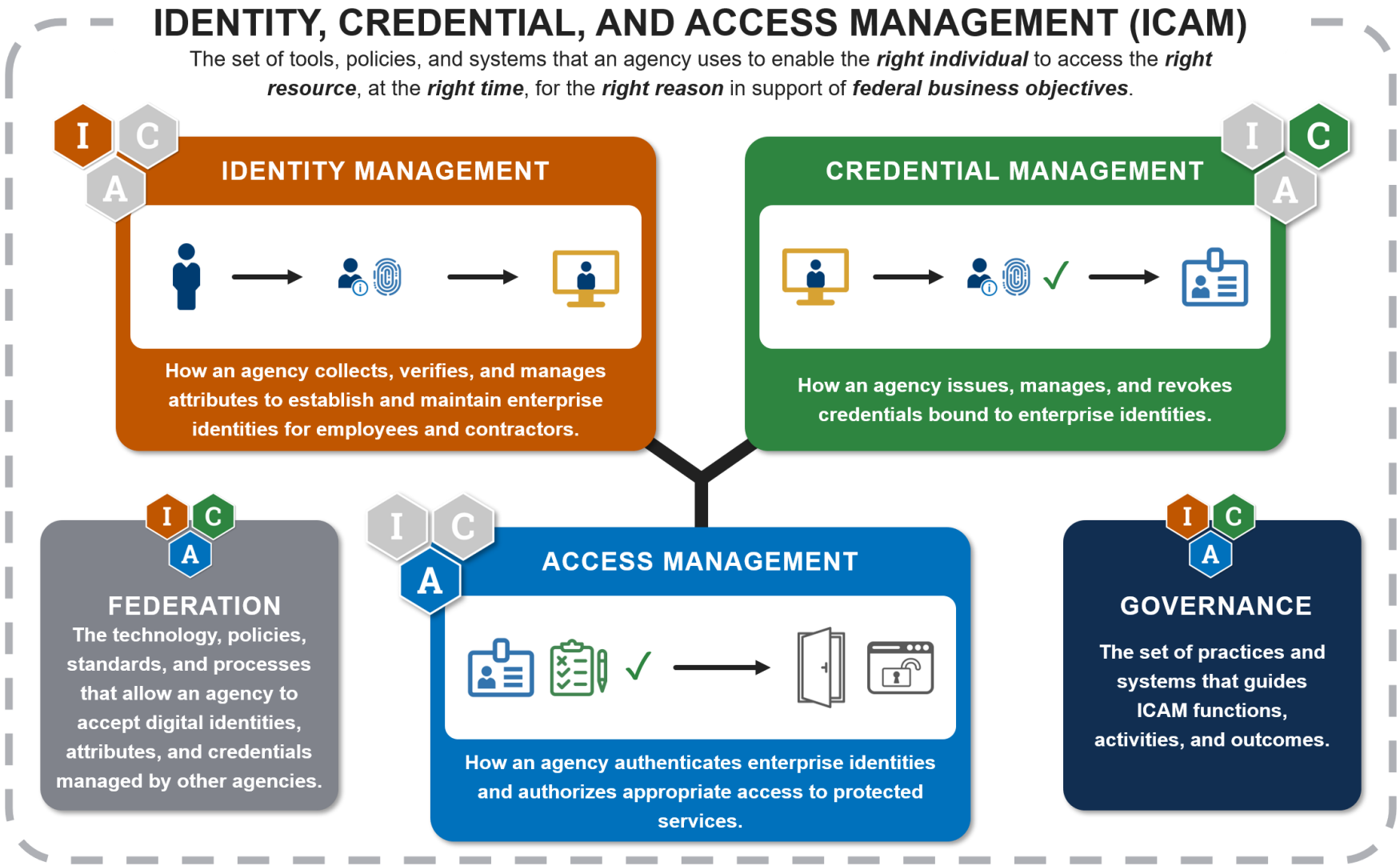
Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Designed to:
  - Create trusted digital identity representations of individuals and **nonperson entities (NPEs)**
  - Bind those identities to credentials that may serve as a proxy for the individual of NPE in access transactions
    - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
  - Use the credentials to provide authorized access to an agency's resources

ICAM

A great introduction to ICAM:

https://www.dni.gov/files/ISE/documents/DocumentLibrary/INTRO-TO-ICAM.pdf



Authentication

NIST SP 800-63-3 (*Digital Authentication Guideline*, October 2016) defines digital user authentication as:

"The process of establishing confidence in user identities that are presented electronically to an information system."

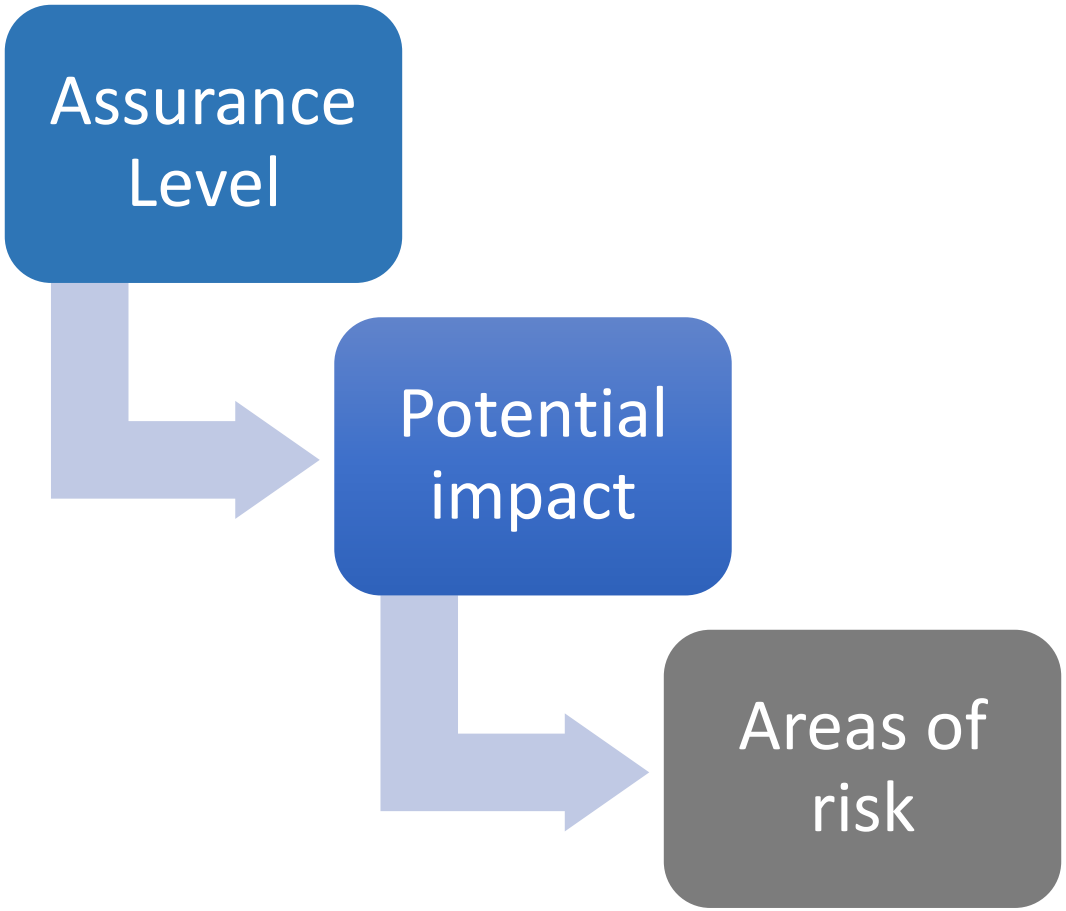
Table 3.1 Identification and Authentication Security Requirements (SP 800-171)
For protection controlled, unclassified information

	Basic Security Requirements:
1	Identify information system users, processes acting on behalf of users, or devices.
2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

	Derived Security Requirements:
3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
5	Prevent reuse of identifiers for a defined period.
6	Disable identifiers after a defined period of inactivity.
7	Enforce a minimum password complexity and change of characters when new passwords are created.
8	Prohibit password reuse for a specified number of generations.
9	Allow temporary password use for system logons with an immediate change to a permanent password.
10	Store and transmit only cryptographically-protected passwords.
11	Obscure feedback of authentication information.

(Table can be found on page 65 in the textbook)

Risk Assessment for User Authentication



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1
- Little or no confidence in the asserted identity's validity

Level 2
- Some confidence in the asserted identity's validity

Level 3
- High confidence in the asserted identity's validity

Level 4
- Very high confidence in the asserted identity's validity

Areas of Risk

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
	Low	Mod	Mod	High
Financial loss or organization liability	None	Low	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	None	Low	Mod/ High
Personal safety				
Civil or criminal violations	None	Low	Mod	High

Maximum Potential Impacts for Each Assurance Level

Poll 1

What do you remember from the text

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Poll 2

Authentication Factors

- Single-factor authentication
    - Using just one type of authentication

- Multifactor authentication
    - When a user is using more than one type of authentication credential
    - Example: what a user knows and what a user has could be used together for authentication
    - Two uses of the same type of authentication don't apply

Authentication with something you know

Password-Based Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

Poll 3

Common Patterns for Weak Passwords

- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Explore Scores for Various Passwords

- How Secure is My Password
- The Password Meter
- Create strong random password
  - https://www.random.org/passwords/

Tips for Creating Strong Passwords

- **Tip #1 - LENGTH**
  - Make your passwords long
  - Use pass phrases or sentences
- **Tip #2 – Complexity**
  - Include letters, punctuation, symbols, and numbers.
  - Use the entire keyboard, not just the letters and characters you use or see most often
- https://blog.avast.com/strong-password-ideas

- Password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use

Most People Reuse Passwords

- https://www.inc.com/jason-aten/google-says-66-of-americans-still-do-this-1-thing-that-puts-their-personal-information-at-a-huge-risk-heres-how-google-wants-to-help.html

How Reused Passwords can be Attacked

- https://osintframework.com/
- Recon-ng
- Sherlock

Reuse Defense – Password Managers

- https://www.digitaltrends.com/computing/best-password-managers/
- https://www.forbes.com/sites/kateoflahertyuk/2019/02/20/password-managers-have-a-security-flaw-heres-how-to-avoid-it/#112ff90d4e16

Attacks on Passwords

- ***Social engineering***
  - Phishing, shoulder surfing, dumpster diving
- ***Capturing***
  - Keylogger, protocol analyzer
  - Man-in-the-middle and replay attacks
- ***Resetting***
  - Attacker gains physical access to computer and resets password
  - Popular on Facebook – then use account for SE
- ***Offline cracking***
  - Method used by most password attacks today
  - Attackers steal file of password digests
- ***Online brute force***
  - Linux hydra

Sources of Stolen Credentials Study

- Google Study
  - 788,000 potential victims of keylogging; 12.4 million potential victims of phishing; and 1.9 billion usernames and passwords exposed by data breaches
  - 7% of victims in third party data breaches have their current Google password exposed, compared to 12% of keylogger victims and 25% of phishing victims
- Passwords Stolen or Leaked - https://en.wikipedia.org/wiki/RockYou
- Passwords leaked from devices
  - https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
- Developers Handling Passwords Poorly
  - https://threatpost.com/medical-data-leaked-on-github-due-to-developer-errors/158653/

Check Your Account

- Have I been pwnd (https://haveibeenpwned.com/)

Offline Cracking Types

- ***Dictionary or preimage attack***
  - Attacker creates digests of common dictionary words
  - Compares against stolen digest file
  - It is estimated that over 100 million passwords were stolen and published online in one year
  - Websites now host lists of leaked passwords along with statistical analysis
  - Demo:
    - https://gchq.github.io/CyberChef/ - Create hash
    - crackstation.net

Dictionary Attack Activity

- Uses John the Ripper
  - https://ncr.cse.unr.edu/
  - Instructions in Canvas

Offline Cracking Types – Brute Force

- Every possible combination of letters, numbers, and characters used to create encrypted passwords and matched against stolen file
- Slowest, most thorough method
- Hashcat on Linux – needs a GPU
- ***Automated brute force parameters***
  - Password length
  - Character set
  - Language
  - Pattern
  - Skips of nonsensical words
- ***Hashcat on linux – best with gpu***

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

“Brute Force” Activity

- Brute Force attacks can be simplified by creating your own word list using crunch

Other Offline Cracking Types

- ***Hybrid attack***
  - Combines a dictionary attack with a brute force attack and will slightly alter dictionary words
    - Adding numbers to the end of the password
    - Spelling words backward
    - Slightly misspelling words and leetspeak
    - Including special characters
    - e.g. John the Ripper
- ***Birthday attack***
  - The search is for any two digests that are the same (collision)
  - In a class of 30 students there is a 70% probability that two students will have the same birthday
  - https://en.wikipedia.org/wiki/Birthday_attack

Other Offline Cracking Types

- Rainbow tables
  - **Ophcrack for Windows**
  - Creates a large pre-generated data set of candidate digests
  - Uses a reducing function to convert hashes to alphanumeric strings
  - Matches digest to password that was used to create it
  - Because of collisions, it may not be actual password, but will work
  - https://en.wikipedia.org/wiki/Rainbow_table
- Free and commercial rainbow tables - http://project-rainbowcrack.com/table.htm
- How to generate your own rainbow tables
  - https://null-byte.wonderhowto.com/how-to/create-rainbow-tables-for-hashing-algorithms-like-md5-sha1-ntlm-0193022/

Offline Cracking Defenses

- ***Password Hashing Algorithms***
  - Microsoft Windows OS stores passwords in two ways
    - LM (LAN Manager) hash - uses a cryptographic one-way function where the password itself is the key
    - NTLMv2 (New Technology LAN Manager) hash - addresses security issues in the LM hash
  - Key stretching - a hashing algorithm that requires significantly more to create the digest
    - bcrypt and PBKDF2 are two popular options
- ***Salts***
  - Consists of a random string that is used in hash algorithms
  - Passwords can be protected by adding a random string to the user's plaintext password before it is hashed
  - Make dictionary attacks and brute force attacks much slower and limit the impact of rainbow tables on large databases

Defense - Proactive Password Checking

- Strong Password Rule enforcement
  - Specific rules that passwords must adhere to
- Password checker
  - Compile a large dictionary of passwords not to use
- Bloom filter
  - Used to build a table based on hash values
  - Check desired password against this table
- **Password audit using John or Ophcrack to check existing passwords**

Poll 4

Authentication with Other Things You Know

- Security questions
  - Should not be able to obtain answers through OSINT

Authentication with something you have

What you have:

- Tokens
- Phones
- Cards
- Passkeys

Tokens

- Currently phones are most popular tokens
- Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects

Tokens

- Two types of OTPs
  - Time-based one-time password (TOTP)
    - Synched with an authentication server
    - Code is generated from an algorithm
    - Code changes every 30 to 60 seconds
  - HMAC-based one-time password (HOTP)
    - "Event-driven" and changes when a specific event occurs

2FA with OTP is not Always Secure

- SMS OTP Authentication: Not As Safe As You May Think
- FBI warns about attacks that bypass multi-factor authentication (MFA)

Tokens

- Advantages over passwords
  - Token code changes frequently
    - Attacker would have to crack code within time limit
  - User may not know if password has been stolen
    - If token is stolen it becomes obvious, and steps could be taken to disable account

Electronic Identity Cards (eID)

Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic

Most advanced deployment is the German card *neuer Personalausweis*

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)

Common Access Card (CAC)

- Issued by US Department of Defense
    - Bar code, magnetic strip, and bearer's picture
- The smart card standard covering all U.S. government employees is the Personal Identity Verification (PIV) standard

Keys and Passkeys

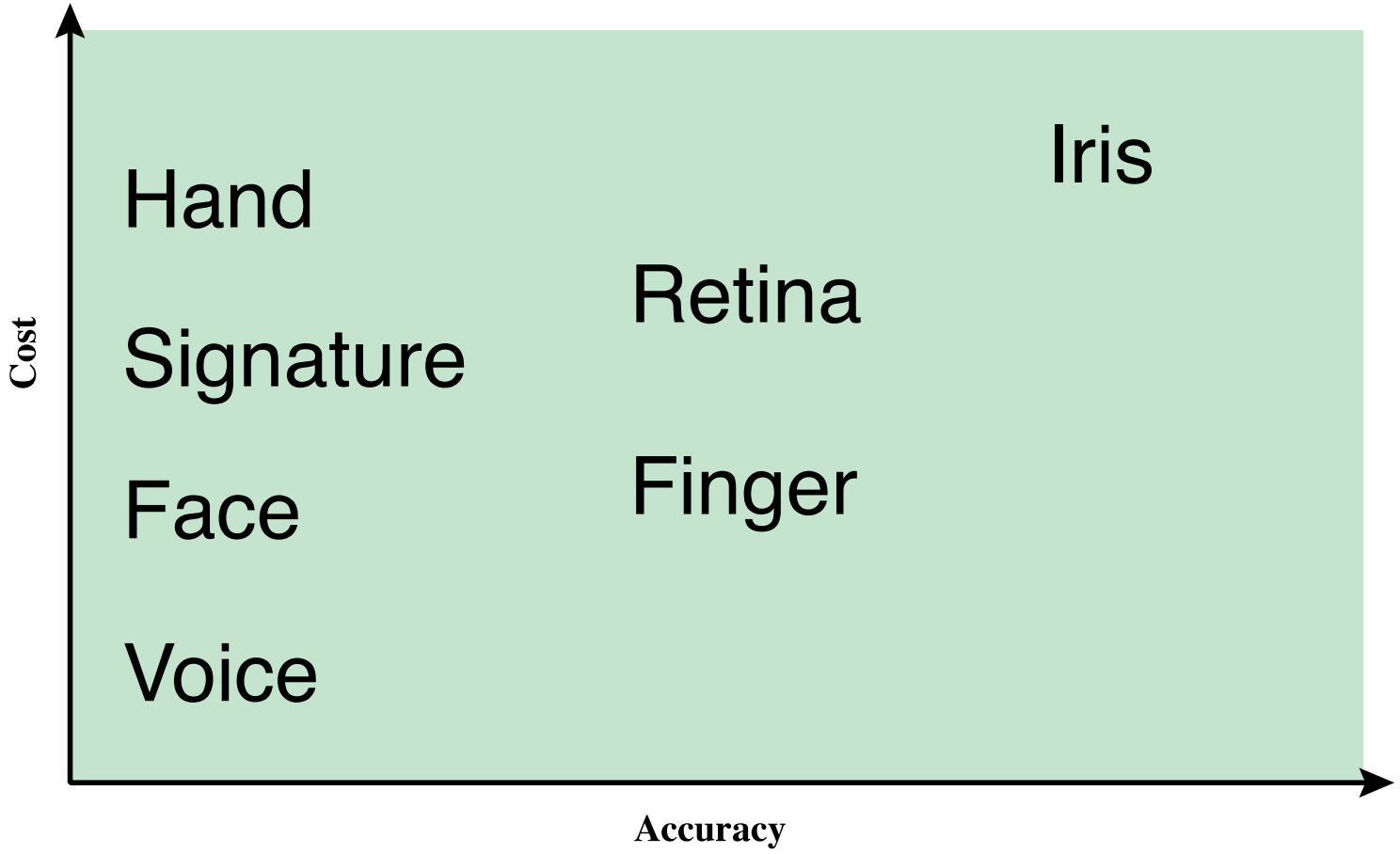
- Yubikey – can be linked to app
- Passkeys
  - Uses Asymmetric keys (public-private) to encode challenge message and response
  - https://www.passkeys.io/technical-details
  - Private key is protected by device security (hopefully)
  - Created by FIDO alliance - https://fidoalliance.org/what-is-fido/

Authentication with something you are

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

Cost vs Accuracy of Biometrics



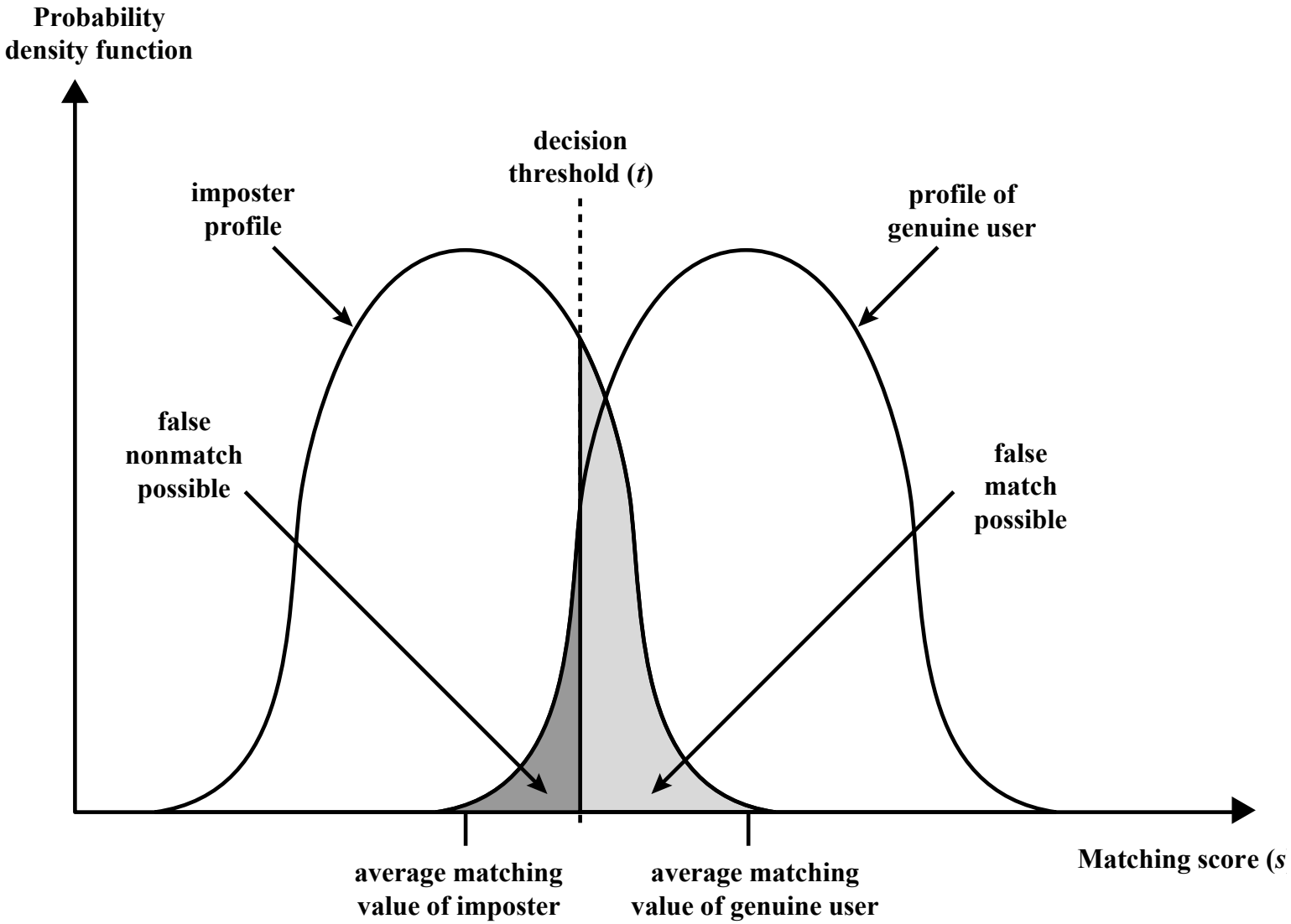
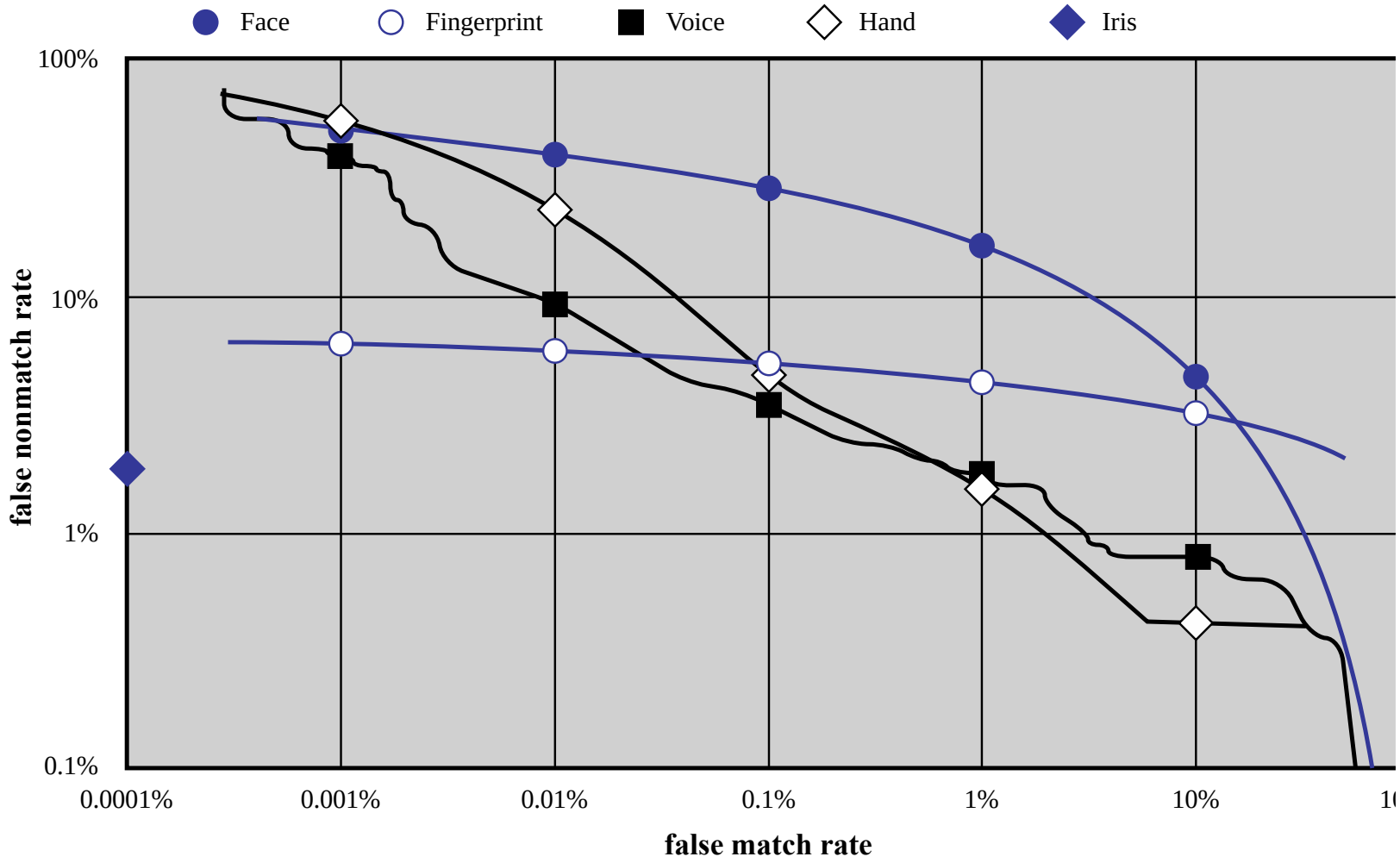


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (*s*) is greater than a preassigned threshold (*t*), a match is declared.

Actual Biometric Measurement Operating Characteristic Curves



Face ID Issues

- https://discussions.apple.com/thread/251560470

Authentication with something you do

Examples of “things you do”

- Keystroke dynamics
  - Keystroke 2 demo
- Emotional Response

Remote Access

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally, rely on some form of a challenge-response protocol to counter threats

Authentication Services

- Authentication
  - Process of verifying credentials
- Authentication services provided on a network
  - Dedicated authentication server
  - A server that performs authentication, authorization, and accounting is called a AAA server
- Common types of authentication and AAA servers
  - RADIUS (Replaced by Diameter), Kerberos, Terminal Access Control Access Control Systems (TACACS), generic servers built on the Lightweight Directory Access Protocol (LDAP), Security Assertion and Markup Language (SAML)

IEEE 802.1x

- Authentication standard that supports port-based authentication services between a user and an authorization device, such as an edge router
  - Used by all types of networks
  - Describes methods used to authenticate a user prior to granting access to a network and the authentication server, such as a RADIUS server
  - Acts through an intermediate device, such as an edge switch, enabling ports to carry normal traffic if the connection is properly authenticated

Remote Authentication Methods

- LDAP - Lightweight Directory Access Protocol (LDAP)
  - Commonly used to handle user authentication/authorization as well as control access to Active Directory objects X.500 standard was created as a standard for directory services
- Remote Authentication Dial-In User Service (RADIUS) is an AAA protocol
  - Designed as a connectionless protocol
- Diameter
  - Name of an AAA protocol suite, designated by the IETF to replace the aging RADIUS protocol
- Terminal Access Controller Access Control System Plus protocol
  - Fundamental design aspect is the separation of authentication, authorization, and accounting and encrypted transmission

Other Authentication Protocols

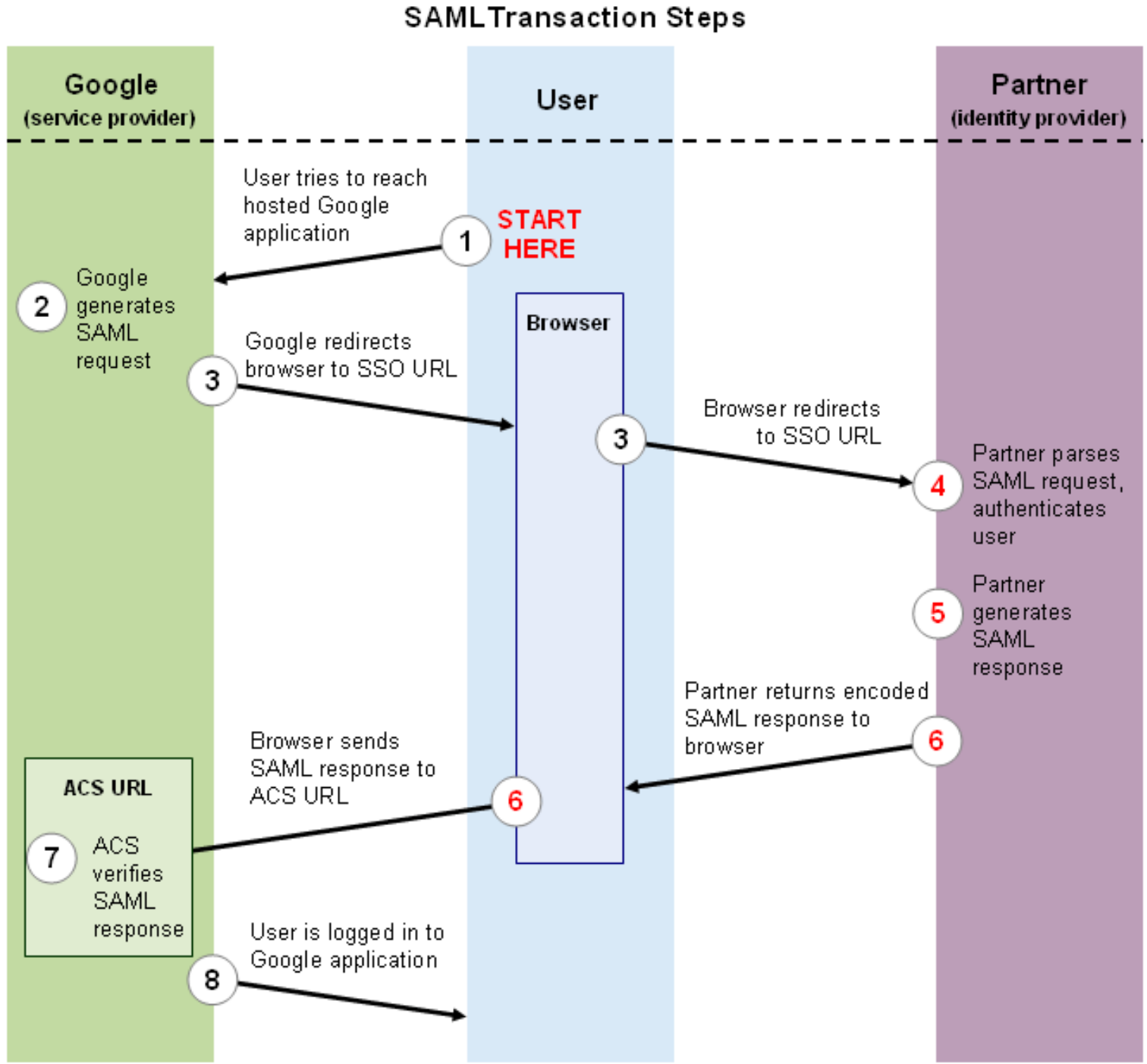
- Widely used for authentication to WiFi
- EAP
  - Extensible Authentication Protocol
  - A universal authentication framework defined by RFC 3748
- CHAP
  - Challenge-Handshake Authentication Protocol
  - Used to provide authentication across a point-to-point link using PPP

Identity Federation

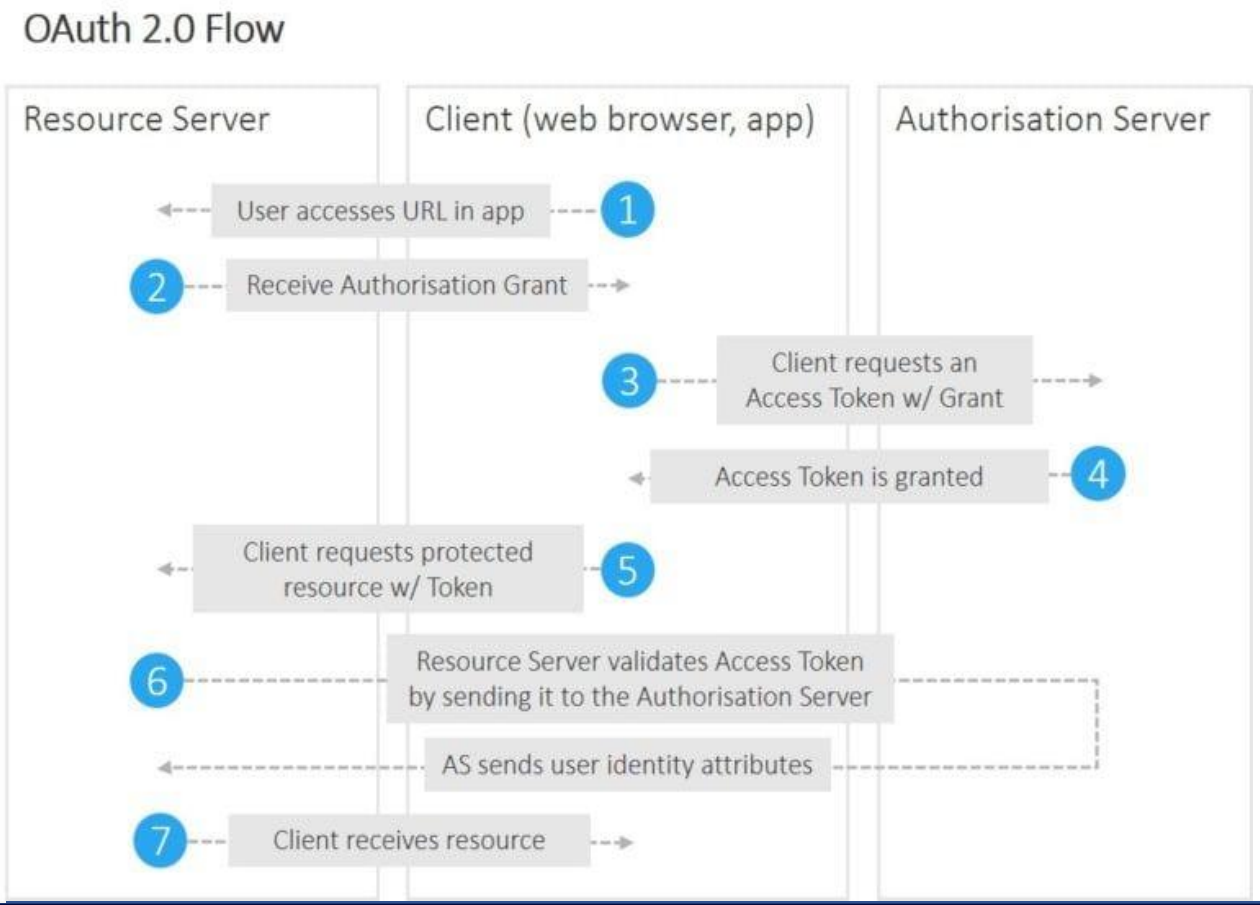
- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
  - How do you trust identities of individuals from external organizations who need access to your systems
  - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations
  - https://developer.okta.com/blog/2019/01/23/nobody-cares-about-oauth-or-openid-connect
  - https://www.scottbrady91.com/OAuth/Why-Developers-Do-Care-About-OAuth-and-OpenID-Connect

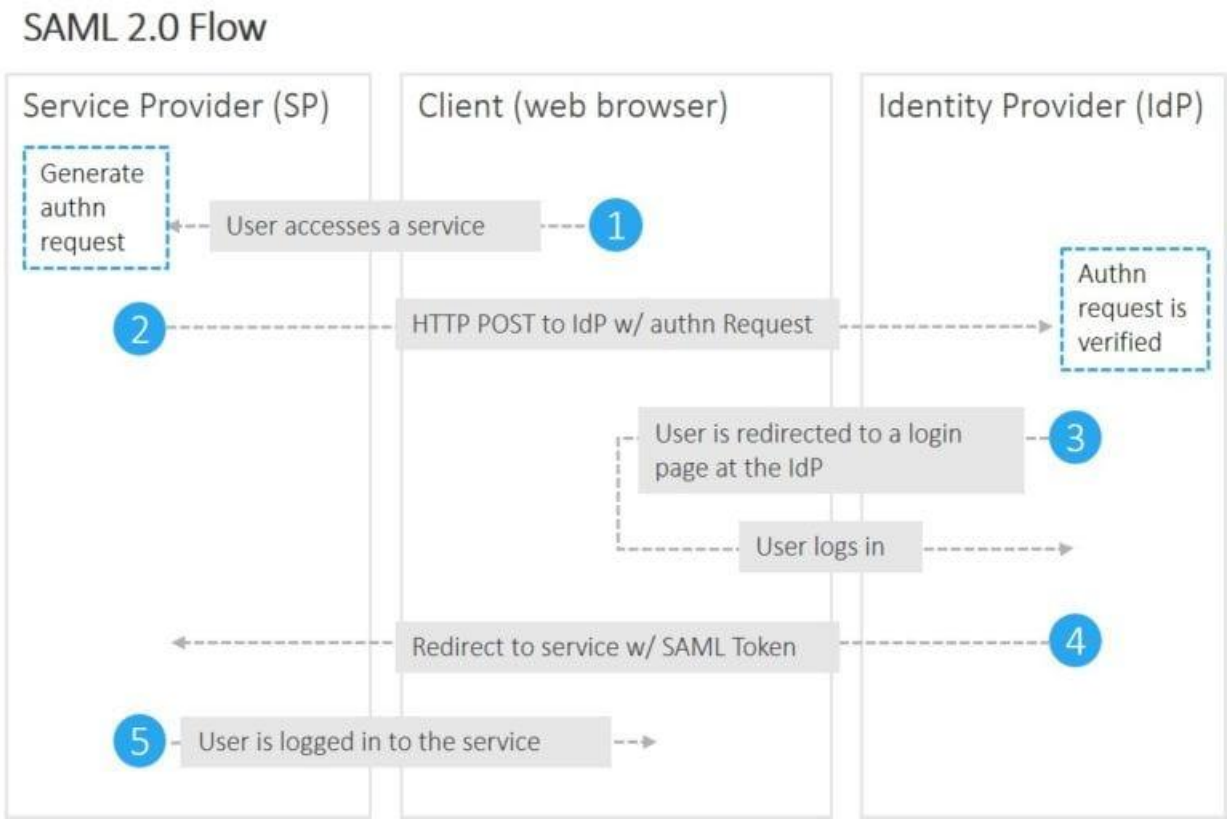
ID Federation Authentication Protocols

- SAML
  - Security Assertion Markup Language
  - A single sign-on capability used for web applications to ensure user identities can be shared and are protected
- OAuth
  - Open Authorization
  - An open protocol that allows secure token-based authentication and authorization in a simple and standard method from web, mobile, and desktop applications, for authorization on the Internet


SAML Transaction Steps
Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Google redirects browser to SSO URL
3
Browser
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
User is logged in to Google application
8

OAUTH and SAML Flow





Other Authentication Protocols

- OpenID Connect
  - Simple identity layer on top of the OAuth 2.0 protocol
  - Allows clients of all types to request and receive information about authenticated sessions and end users
- Shibboleth
  - Designed to enable single sign-on and federated identity-based authentication and authorization across networks
- Secure token - Kerberos
  - Secure token service is responsible for issuing, validating, renewing, and cancelling security tokens

Misused Tokens Example

- https://www.theverge.com/2018/9/28/17914524/facebook-bug-50-million-affected-security-token-access-view-as-feature

Single Sign-On

- Single sign-on (SSO) is a form of authentication that involves the transferring of credentials between systems
  - Allows a user to transfer her credentials, so that logging into one system acts to log her into all of them
  - Usually a little more difficult to implement than vendors would lead you to believe
- UNR formerly used Okta service

Access Control

Start NICE Challenge Exercise

Access Management

Deals with the management and control of the ways entities are granted access to resources

Covers both logical and physical access

May be internal to a system or an external element

Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

Three support elements are needed for an enterprise-wide access control facility:

- Resource management
- Privilege management
- Policy management

Usability of Security (A Big Idea)

- Make it easy to do the right thing
- Make it hard to do the wrong thing
- Make it easy to recover when the wrong thing happens

Ref: https://csrc.nist.gov/Projects/Usability-Of-Security

Those Security Design Principles Again

Poll 1

Principle of Least Privilege

- **The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task.**
  - If a subject does not need an access right, the subject should not have that right.
  - Furthermore, the function of the subject (as opposed to its identity) should control the assignment of rights. If a specific action requires that a subject's access rights be augmented, those extra rights should be relinquished immediately on completion of the action.
- *In practice, most systems do not have the granularity of privileges and permissions required to apply this principle precisely. The designers of security mechanisms then apply this principle as best they can. In such systems, the consequences of security problems are often more severe than the consequences for systems that adhere to this principle.*

Principle of Fail-Safe Defaults

- **The *principle of fail-safe defaults* states that, unless a subject is given explicit access to an object, it should be denied access to that object.**

- *This principle requires that the default access to an object is none. Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied. Moreover, if the subject is unable to complete its action or task, it should undo those changes it made in the security state of the system before it terminates. This way, even if the program fails, the system is still safe.*

Principle of Economy of Mechanism

- **The *principle of economy of mechanism* states that security mechanisms should be as simple as possible.**

- *If a design and implementation are simple, fewer possibilities exist for errors. The checking and testing process is less complex, because fewer components and cases need to be tested. Complex mechanisms often make assumptions about the system and environment in which they run. If these assumptions are incorrect, security problems may result.*

Principle of Complete Mediation

- **The *principle of complete mediation* requires that all accesses to objects be checked to ensure that they are allowed.**

- *Whenever a subject attempts to read an object, the operating system should mediate the action. First, it determines if the subject is allowed to read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should check that the subject is still allowed to read the object. Most systems would not make the second check. They would cache the results of the first check and base the second access on the cached results.*

Subject

An entity capable of accessing objects

Three classes

- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access Right

Describes the way in which a subject may access an object

Could include:

- Read
- Write
- Execute
- Delete
- Create
- Search

Implementing Access Control

- Technologies used to implement access control
  - Permissions
    - Access control lists (ACLs)
    - Group Policy
    - Account restrictions

Access Control Models

- Access control models provide a predefined framework for hardware or software developers
  - Use the appropriate model to configure the necessary level of control

- Major access control models
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role Based Access Control (RBAC)
  - Rule Based Access Control
  - Attribute Based Access Control (ABAC)

Mandatory Access Control (MAC)

- Most restrictive access control model
- Typically found in military settings
- Two elements
  - ***Labels*** - Every entity is an object and is assigned a classification label that represents the relative importance of the object
    - Subjects are assigned a privilege label (clearance)
  - ***Levels*** - a hierarchy based on the labels is used
    - Top secret has a higher level than secret, which has a higher level than confidential

POLL 2

Poll 2

Mandatory Access Control (MAC)

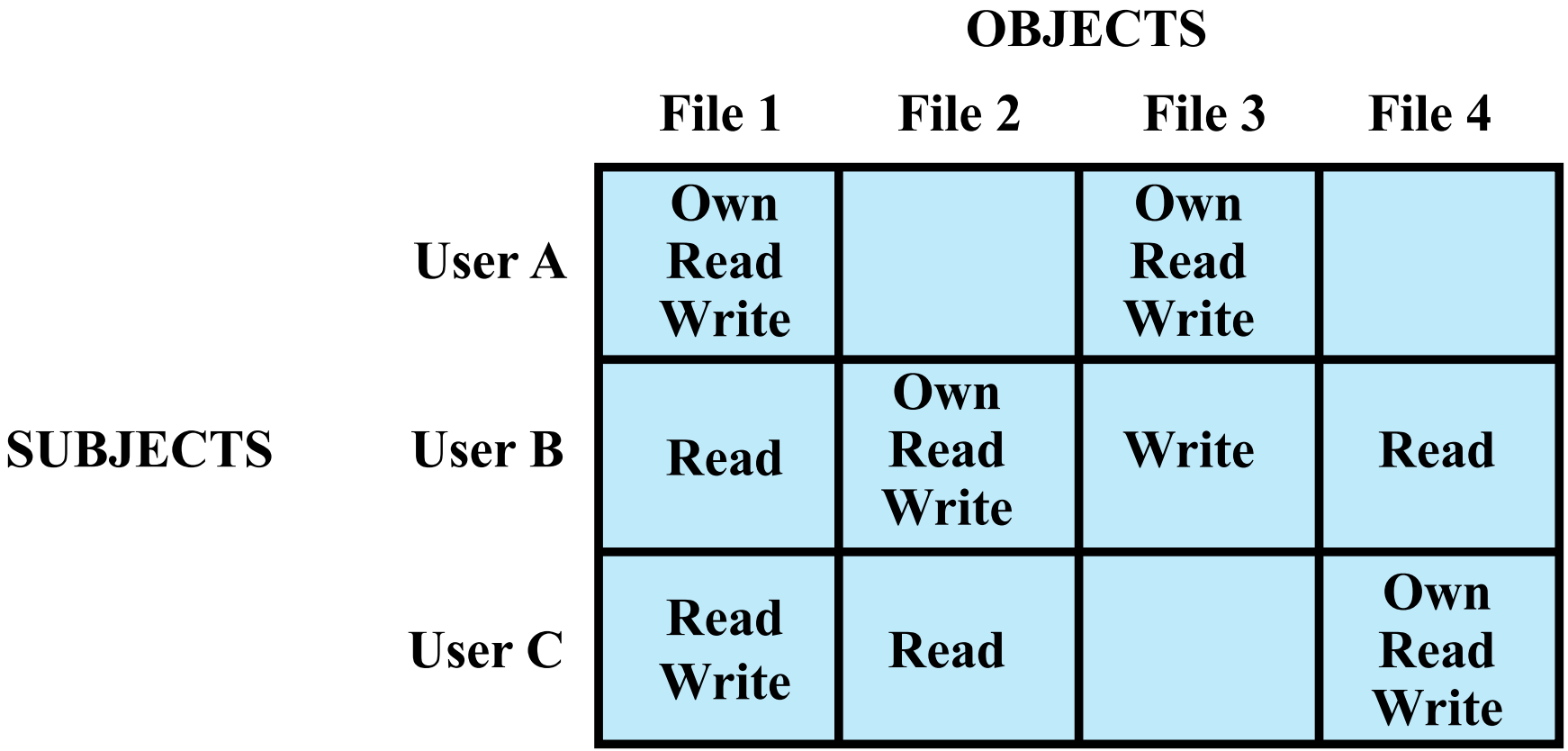
- Two major implementations of MAC
  - Lattice model -Rule Based Access Control (RBAC)
  - Bell-LaPadula model (no read up, no write down)
  - Windows Example UAC

MAC Implementations

- https://github.com/SELinuxProject/selinux-notebook/blob/main/src/selinux_overview.md#selinux-overview
- https://ubuntu.com/server/docs/security-apparmor
- https://docs.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control?redirectedfrom=MSDN

Discretionary Access Control (DAC)

- Least restrictive model
- Every object has an owner that has total control over their objects
- Owners can give permissions to other subjects over their objects
- Often provided using an access matrix
    - One dimension consists of identified subjects that may attempt data access to the resources
    - The other dimension lists the objects that may be accessed
- Used on operating systems such as most types of UNIX and Microsoft Windows
    - Windows Example – file properties
    - Linux example – permissions and ACLs

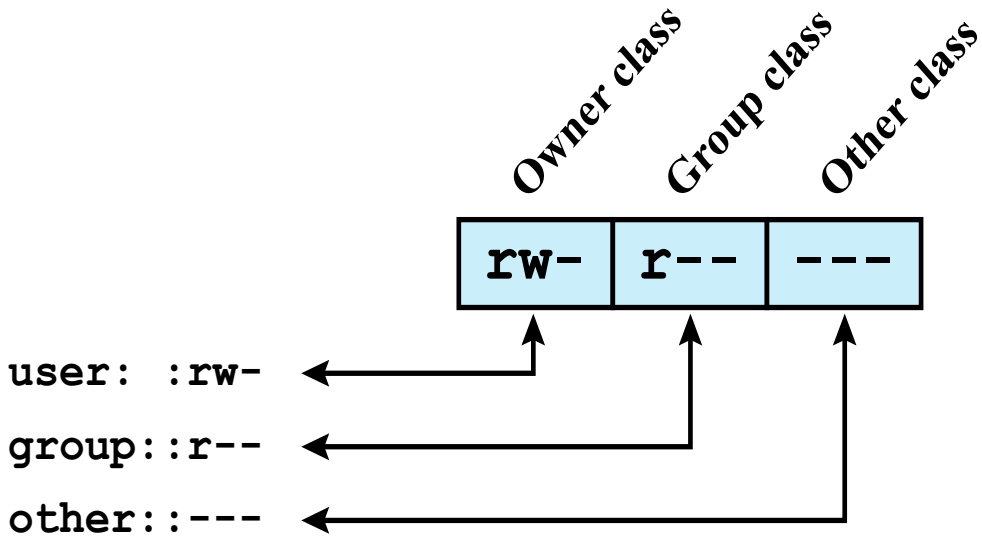


(a) Access matrix

Figure 4.2 Example of Access Control Structures

UNIX File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



(a) Traditional UNIX approach (minimal access control list)

Traditional UNIX File Access Control

- "Set user ID"(SetUID)
- "Set group ID"(SetGID)
  - System temporarily uses rights of the file owner/group in addition to the real user's rights when making access control decisions
  - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
  - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
  - Is exempt from usual access control restrictions
  - Has system-wide access

Linux Permissions

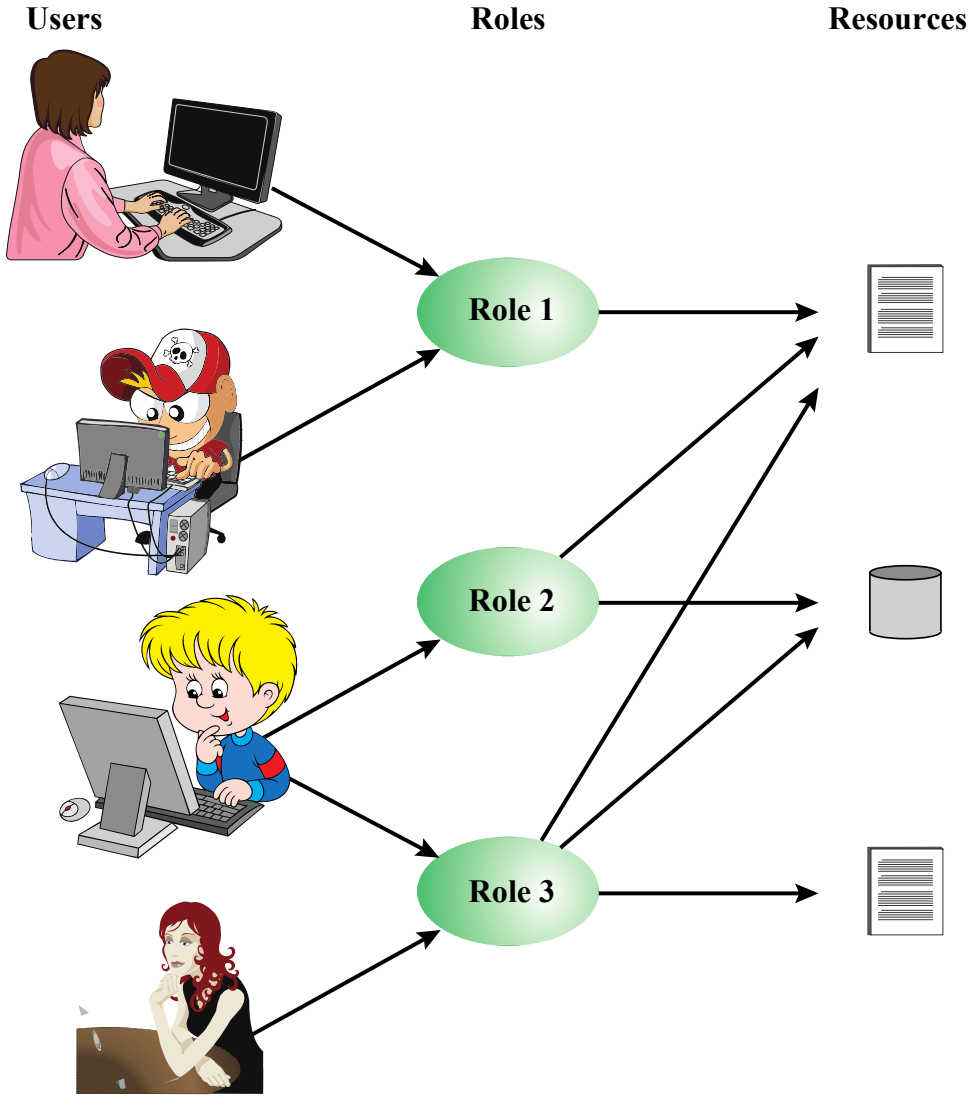
- https://www.linux.com/tutorials/understanding-linux-file-permissions/
- https://www.unixtutorial.org/difference-between-chmod-and-chown
  - *View in Labtainer*
  - *Ls –l*
  - *Find by -user*
- Linux Capabilities labtainer
  - https://ncr-remote.cse.unr.edu/accounts/login/

Role Based Access Control (RBAC)

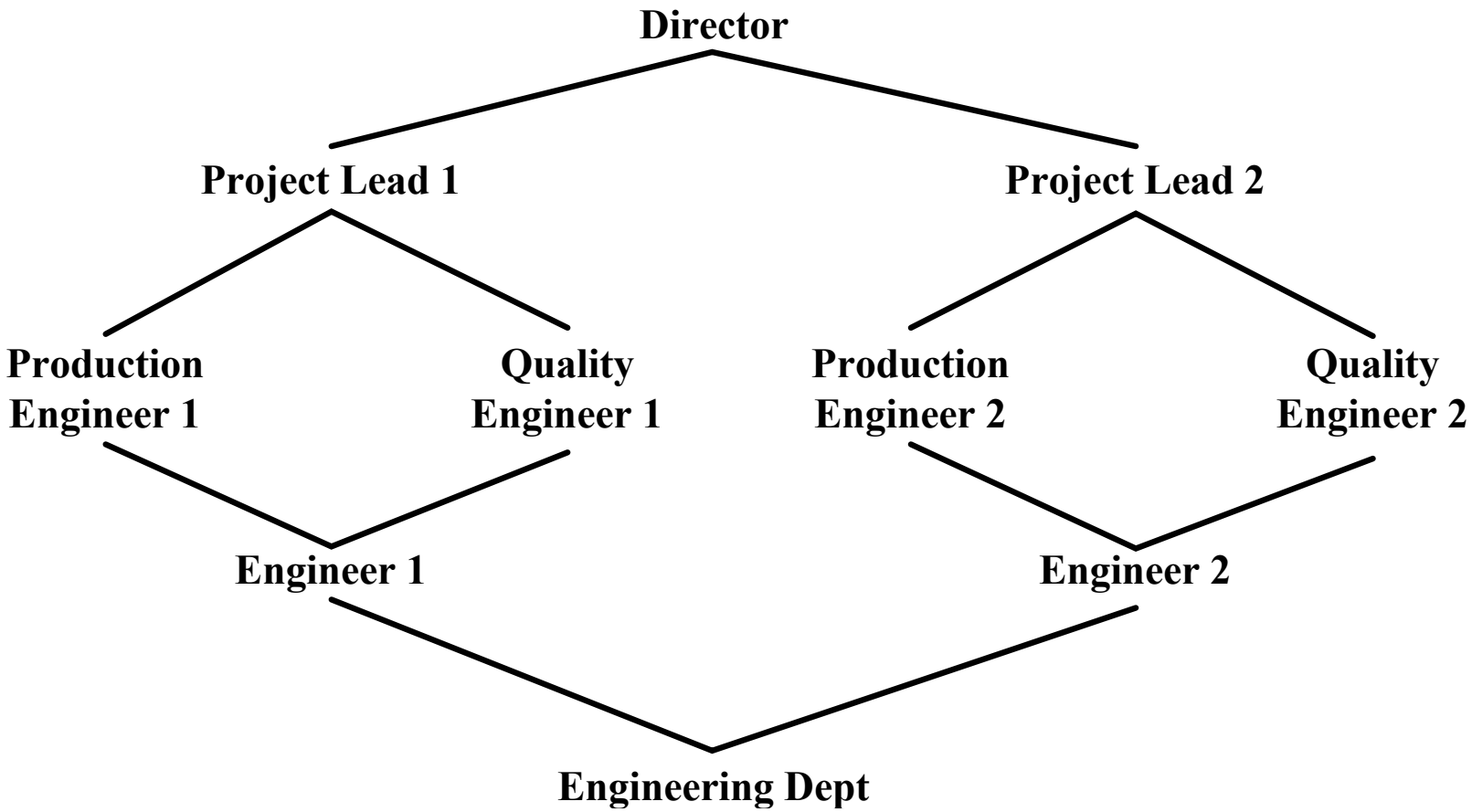
- Also called *Non-Discretionary Access Control*
- Access permissions are based on user's job function
- RBAC assigns permissions to particular roles in an organization
- Users are assigned to those roles

- Rule Based Access Control (RRBAC)
  - Dynamically assigns roles to subjects based on a set of rules defined by a custodian

Where have you used RBAC?



Example of Role Based Access Control



Rule-Based Access Control

- In rule-based access control, access is either allowed or denied based on a set of predefined rules
  - Each object has an associated ACL (much like DAC), and when a particular user or group attempts to access the object, the appropriate rule is applied
- A good example for rule-based access control is permitted logon hours
  - Many operating systems give administrators the ability to control the hours during which users can log in

Attribute-based access control (ABAC)

- Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

- https://www.ekransystem.com/en/blog/rbac-vs-abac

ABAC Model: Attributes

Subject attributes

- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

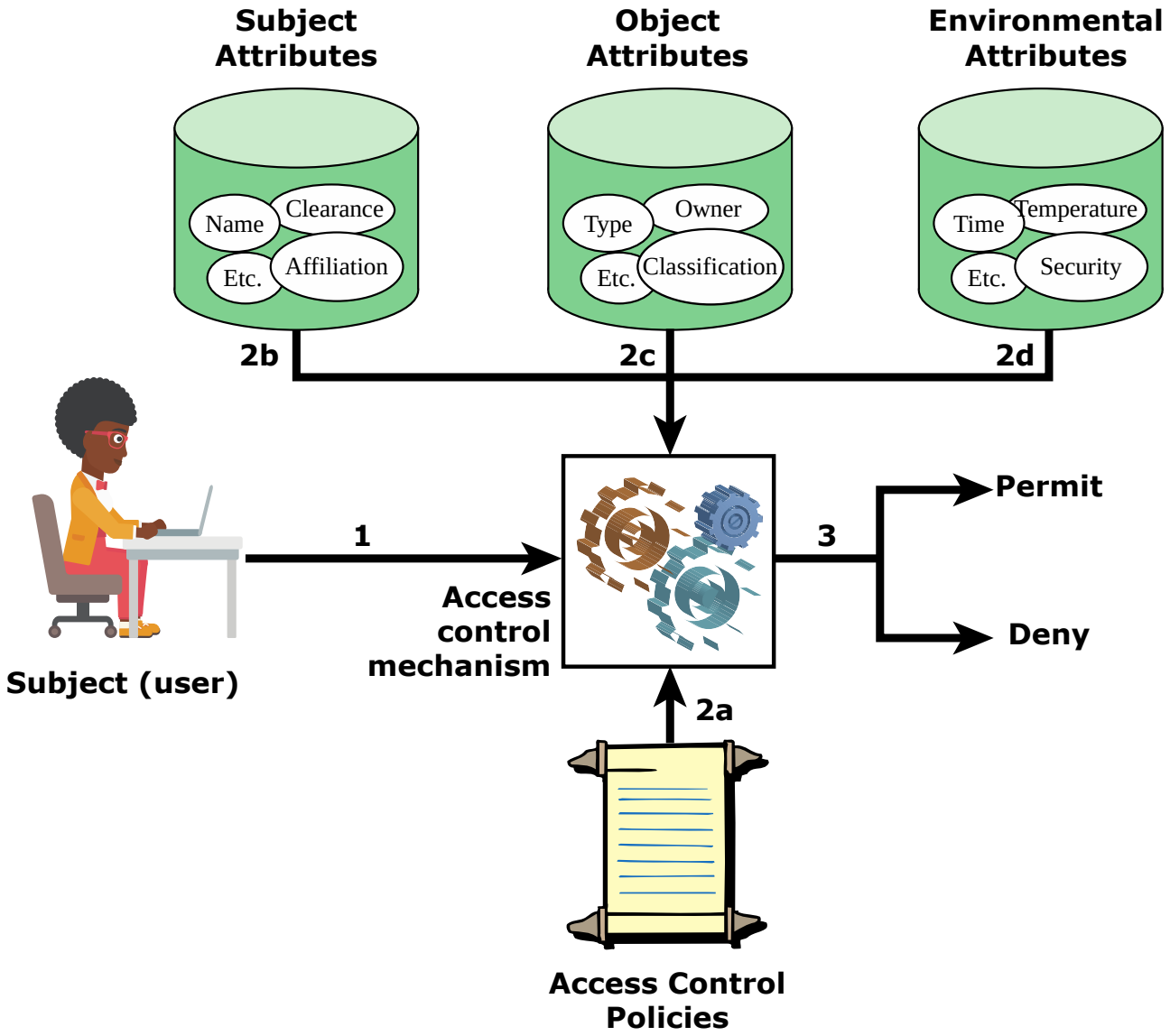
Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leveraged to make access control decisions

Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies

ABAC Scenario



Example ABAC Policy

- An example of ABAC would be:
  - allowing only users who are type=employees and have department=HR to access the HR/Payroll system and only during business hours within the same timezone as the company.

Polls 3 and 4

Practical Examples – may need for final project

Polls 5-7

Module 5 Assignment 1

- Labtainer – crack hashed passwords with basic scripts
- Start with –r and put in your name

Module 5 Assignment 2 - ACLs

- For script pay special attention to providing access to the information, instead of providing access to the file
  - WHY?

Types of Attacks and Malicious Software

Chapter 6

News

- https://www.ic3.gov/ - Industry Alerts
- https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

Module 5 Labs Review

- Pass-Crack lab
  - The longer the password, the longer cracking takes
  - Salts don't typically add much to cracking time
    - If the cracking program knows that salts are added to the beginning of the password, it will do the same before hashing and looking for a match. It may take a few iterations to add at beginning, end middle, etc.
    - It does increase the size of the input to the hash algorithm, making it more difficult to match
- ACL lab
  - Default ACLs – some did multiple attempts and ended up with something that seemed to work.
  - Script – Alice does not have default access to bob directory. If your default ACL works, you could write to Alice directory for Bob access
    - No ACL required in the script

Classification of Malware

Classified into two broad categories:

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

Propagation Mechanisms

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Payloads

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Data Encryption for ransom
- Stealthing/hiding its presence on the system

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

Attack or Exploit Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
- Toolkits are often known as “crimeware”
- Examples are:
    - Zeus
    - Angler
    - Magnitude
    - Nuclear
- https://www.privacyaffairs.com/dark-web-price-index-2023/

Classification by Propagation Technique

Poll 1 – Questionpro.io

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

Detecting Malware Lab 1

- Virus Total Lab
- Go to NCR Kali Machine
  - Download VirusTotalLab files from Web Campus

Virus Components

Infection mechanism

- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a ***logic bomb***

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

Macro and Scripting Viruses

NISTIR 7298 defines a macro virus as:

"a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate"

- Macro viruses infect scripting code used to support active content in a variety of user document types
- Are threatening for several reasons:
  - Is platform independent
  - Infect documents, not executable portions of code
  - Are easily spread because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them
  - Are much easier to write or to modify than traditional executable viruses

Virus Classifications

Classification by target

- Boot sector infector
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
  - Infects files that the operating system or shell considers to be executable
- Macro virus
  - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
  - Infects files in multiple ways

Classification by concealment strategy

- Encrypted virus
- Stealth virus
- Polymorphic virus
- Metamorphic virus

Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Worm Replication

Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media
Remote execution capability	• Worm executes a copy of itself on another system
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Target Discovery

- Scanning (or fingerprinting)
- Random
  - Each compromised host probes random addresses in the IP address space using a different seed
- Hit-list
  - The attacker first compiles a long list of potential vulnerable machines
- Topological
  - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
  - If a host can be infected behind a firewall that host then looks for targets in its own local network

WannaCry – Based on NSA's Eternal Blue

- Ransomware attack in May 2017 that spread extremely fast over a period of hours to days, infecting hundreds of thousands of systems belonging to both public and private organizations in more than 150 countries
- It spread as a worm by aggressively scanning both local and random remote networks, attempting to exploit a vulnerability in the SMB file sharing service on unpatched Windows systems.
- This rapid spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher
- Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

Mobile Code as Infection Vector

NIST SP 800-28 defines mobile code as

> "programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics"

- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits

- Popular vehicles include:
  - Java applets
  - ActiveX
  - JavaScript
  - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
  - Cross-site scripting
  - Interactive and dynamic Web sites
  - E-mail attachments
  - Downloads from untrusted sites or of untrusted software

Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Communicate through Bluetooth wireless connections or MMS
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

Poll 2

Drive-By-Downloads

Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user's knowledge or consent

In most cases the malware does not actively propagate as a worm does

Spreads when users visit the malicious Web page

Watering-Hole Attacks

- A variant of drive-by-download used in highly targeted attacks
- The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- They then wait for one of their intended victims to visit one of the compromised sites
- Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- This greatly increases the likelihood of the site compromise remaining undetected

Malvertising or Madware

- Places malware on websites without compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems
- Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track
- Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

Clickjacking

- Also known as a user-interface (UI) redress attack
- A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page
- Using a similar technique, keystrokes can also be hijacked as a user could be typing into an invisible frame controlled by the attacker

Mitigation:

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

BankofAmerica.com example

- Use developer tools to view Response Header
  - Script-scr 'self' limits loading of scripts to this site
  - Unsafe-inline and unsafe-eval blow that up
  - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src

Social Engineering

Spam

- Unsolicited bulk e-mail
- Significant carrier of malware
- Used for phishing attacks

Trojan horse

- Program or utility containing harmful hidden code
- Used to accomplish functions that the attacker could not accomplish directly

Mobile Trojans

- First appeared in 2004 (Skuller)
- Target is the smartphone

Poll 3

Detecting Malware Lab 2

- Hashing-Yara Lab on NCR

Classification by Propagation Payload

Payload - System Corruption

- Real-world damage
  - Causes damage to physical equipment
    - Chernobyl virus rewrites BIOS code
  - Stuxnet worm
    - Targets specific industrial control system software
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
  - Code embedded in the malware that is set to "explode" when certain conditions are met

Ransomware

- WannaCry
  - Infected a large number of systems in many countries in May 2017
  - When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoin to recover them
  - Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan
  - Targets widened beyond personal computer systems to include mobile devices and Linux servers
  - Tactics such as threatening to publish sensitive personal information, or to permanently destroy the encryption key after a short period of time, are sometimes used to increase the pressure on the victim to pay up

Poll 4

Payload – Attack Agents: Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

Remote Control Facility

- Also called command and control or C&C
- Distinguishes a bot from a worm
  - Worm propagates itself and activates itself
  - Bot is initially controlled from some central facility
- Typical means of implementing the remote-control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands
  - More recent botnets use covert communication channels via protocols such as HTTP
  - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Poll 5

Payload – Information Theft

- Keylogger
  - Captures keystrokes to allow attacker to monitor sensitive information
  - Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)
- Spyware
  - Subverts the compromised machine to allow monitoring of a wide range of activity on the system
    - Monitoring history and content of browsing activity
    - Redirecting certain Web page requests to fake sites
    - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Malware Analysis Lab - Keylogger

- Analyze with strings command using – n 20
- Analyze with grep
- Analyze with ghidra and search strings
  - Other options include:
    - Radare2 on Kali
    - Ida or Ida Pro – commercial software

Payload – Information Theft - Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
- Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
- Suggests that urgent action is required by the user to authenticate their account
- Attacker exploits the account using the captured credentials

- Spear-phishing
  - Recipients are carefully researched by the attacker
  - E-mail is crafted to specifically suit its
    recipient, often quoting a range of information to convince them of its authenticity

Poll 6

Payload – Backdoor

- Also known as a ***trapdoor***
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- ***Maintenance hook*** is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications
- Mostly an insider threat

Poll 7

Malware Analysis Lab - GREP/Strings Lab

Payload – Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Rootkit Classification Characteristics

- **Persistent**
  - Activates each time the system boots. The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention. This means it is easier to detect, as the copy in persistent storage can potentially be scanned.
- **Memory based**
  - Has no persistent code and therefore cannot survive a reboot. However, because it is only in memory, it can be harder to detect.
- **User mode**
  - Intercepts calls to APIs (application program interfaces) and modifies returned results. For example, when an application performs a directory listing, the return results don't include entries identifying the files associated with the rootkit.

Rootkit Classification Characteristics

- **Kernel mode**
- Can intercept calls to native APIs in kernel mode. The rootkit can also hide the presence of a malware process by removing it from the kernel's list of active processes.

- **Virtual machine based**
- This type of rootkit installs a lightweight virtual machine monitor, and then runs the operating system in a virtual machine above it. The rootkit can then transparently intercept and modify states and events occurring in the virtualized system.

- **External mode**
- The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware
- https://otx.alienvault.com/pulse/615da17a17aebe726ae818f1

Kali Rootkit Lab

Check Root Kit from Kali terminal:

- git clone https://github.com/Magentron/chkrootkit.git
- cd chkrootkit
- ./chkrootkit

RK-hunter from Kali terminal:

- wget http://downloads.sourceforge.net/project/rkhunter/rkhunter/1.4.6/rkhunter-1.4.6.tar.gz
- cd Downloads
- tar -xvf rkhunter-1.4.6.tar.gz
- rkhunter --check

Fileless Malware

- Link to malicious website
- Website loads Flash or other plugin that launches PowerShell commands
- https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/

Malware Counter Measures

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention
- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection
  - Identification
  - Removal

Four main elements of prevention:

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

Counter Measure Discussion

- What Policies?
- What Vulnerability Mitigation?
- What Threat Mitigation?

Generations of Anti-Virus Software

- First generation: simple scanners
  - Requires a malware signature to identify the malware
  - Limited to the detection of known malware
- Second generation: heuristic scanners
  - Uses heuristic rules to search for probable malware instances
  - Another approach is integrity checking
- Third generation: activity traps
  - Memory-resident programs that identify malware by its actions rather than its structure in an infected program
- Fourth generation: full-featured protection
  - Packages consisting of a variety of anti-virus techniques used in conjunction
  - Include scanning and activity trap components and access control capability

Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations
• Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Perimeter Scanning Approaches

- Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS
- May also be included in the traffic analysis component of an IDS
- May include intrusion prevention measures, blocking the flow of any suspicious traffic

Ingress monitors

Located at the border between the enterprise network and the Internet

One technique is to look for incoming traffic to unused local IP addresses

Egress monitors

Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet

Monitors outgoing traffic for signs of scanning or other suspicious behavior

Two types of monitoring software

Researching Malware

- Simple consumer tools
  - https://www.virustotal.com
  - https://www.hybrid-analysis.com/
- Research
  - https://malpedia.caad.fkie.fraunhofer.de/
    - Look at Process Injection in BugSleep Loader
  - https://virusshare.com/about.4n6
- Advanced tools
  - https://otx.alienvault.com/preview

Malware Hunting - Sandbox Analysis

- Running potentially malicious code in an emulated sandbox or on a virtual machine
- Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- The most difficult design issue with sandbox analysis is to determine how long to run each interpretation

Malware Monitoring Lab - Windows

In-class Malware Challenge

Important Tips for NICE Challenge

- Update the virus definitions
- DO NOT scan the entire machine. You have a good clue of where the problem is, so start with user files
- Beware of processes that re-install files
- If you can move the quarantine files to the security desk and still not get a check, take a screen shot

Module 6 Assignment

- Labtainer lab using Metasploit
  - A bit repetitive, but do all of them
  - You may need to enter a “y” or CTL-C to end some processes

System Hardening and Baselines

A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.

News

- https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so
- https://www.cisa.gov/news-events/news/joint-advisory-top-cyber-misconfigurations-highlights-urgency-software-manufacturers-incorporate

Controls Standards

The foundation of your work

CIS - 18 Critical Controls

- 1. Inventory and Control of Enterprise Assets
- 2. Inventory and Control of Software Assets
- 3. Data Protection
- 4. Secure Configuration of Enterprise Assets and Software
- 5. Account Management
- 6. Access Control Management
- 7. Continuous Vulnerability Management
- 8. Audit Log Management
- 9. Email and Web Browser Protections

Source: https://www.cisecurity.org/controls/cis-controls-navigator/

18 Critical Controls continued

- 10. Malware Defenses
- 11. Data Recovery
- 12. Network Infrastructure Management
- 13. Network Monitoring and Defense
- 14. Security Awareness and Skills Training
- 15. Service Provider Management
- 16. Application Software Security
- 17. Incident Response Management
- 18. Penetration Testing

Source: https://www.cisecurity.org/controls/cis-controls-navigator/

Secure Configuration of Enterprise Assets and Software

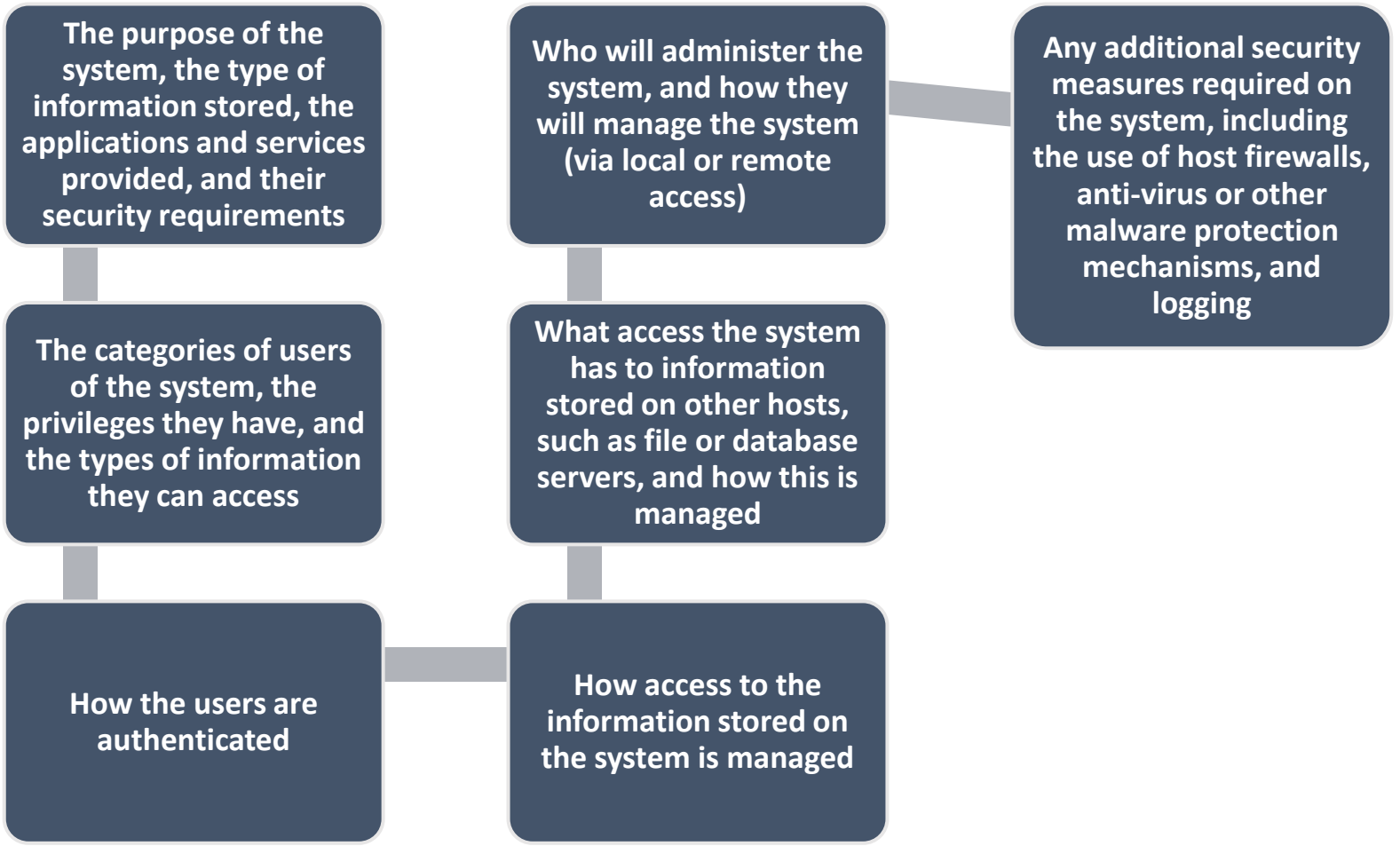
Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.
Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.
Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Operating System Hardening

Operating System Security

- Building and deploying a system should be a planned process designed to counter a compromise before installation
- Process must:
  - Assess risks and plan the system deployment
  - Secure the underlying operating system and then the key applications
  - Ensure any critical content is secured
  - Ensure appropriate network protection mechanisms are used
  - Ensure appropriate processes are used to maintain security

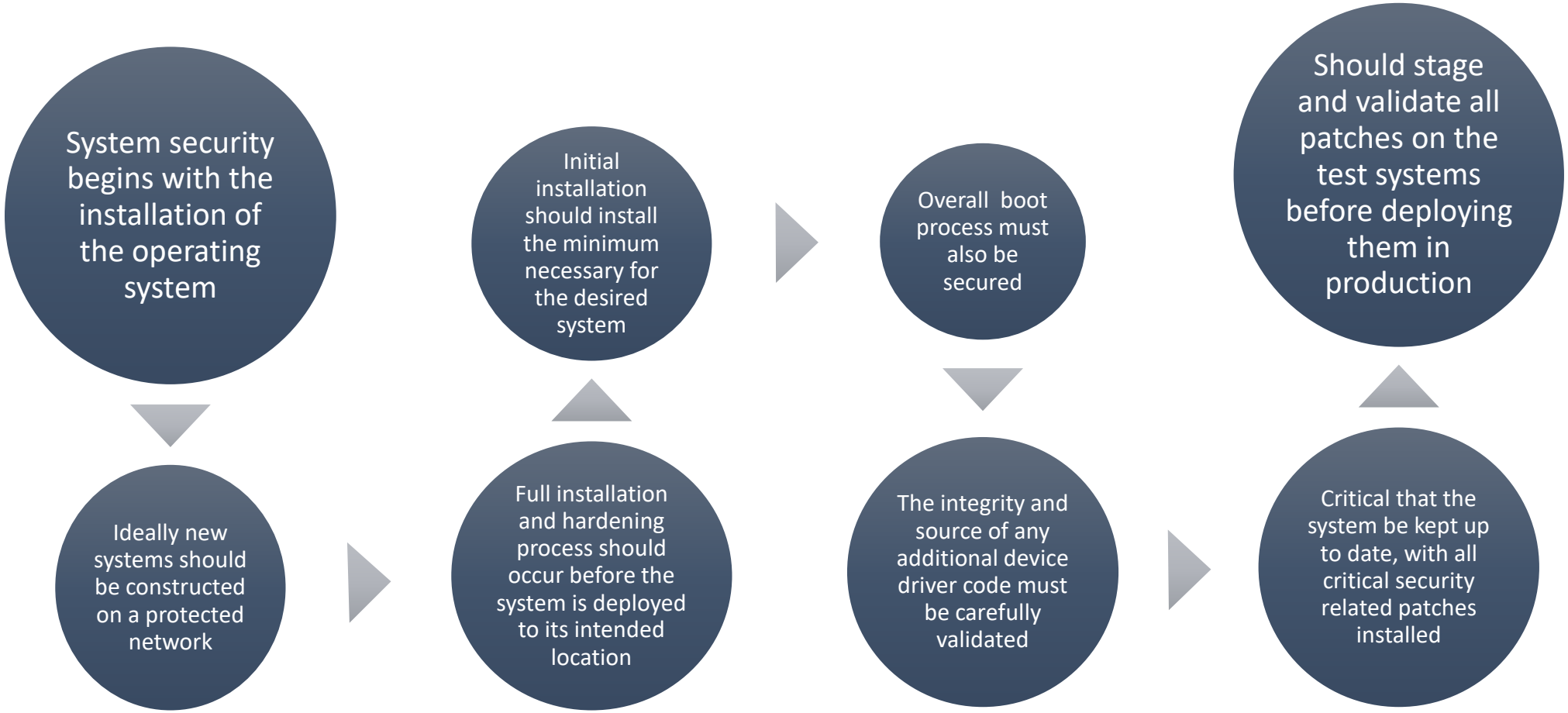
System Security Planning Process
NIST SP 800-123



Operating Systems Hardening

- First critical step in securing a system is to secure the base operating system:
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the indentified security needs of the system by:
    - Removing unnecessary services, applications, and protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls
  - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
  - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

Initial Setup and Patching



- If fewer software packages are available to run the risk is reduced
- System planning process should identify what is actually required for a given system

- When performing the initial installation the supplied defaults should not be used
  - Default configuration is set to maximize ease of use and functionality rather than security
  - If additional packages are needed later they can be installed when they are required

- Not all users with access to a system will have the same access to all data and resources on that system
- Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

- System planning process should consider:
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where they are defined and authenticated
- Default accounts included as part of the system installation should be secured
  - Those that are not required should be either removed or disabled
  - Policies that apply to authentication credentials configured
  - https://ubuntu.com/server/docs/security-users

- Once the users and groups are defined, appropriate permissions can be set on data and resources
- Many of the security hardening guides provide lists of recommended changes to the default access configuration

- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing

- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities
- Checklists are included in security hardening guides
- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done following the initial hardening of the system
- Repeated periodically as part of the security maintenance process

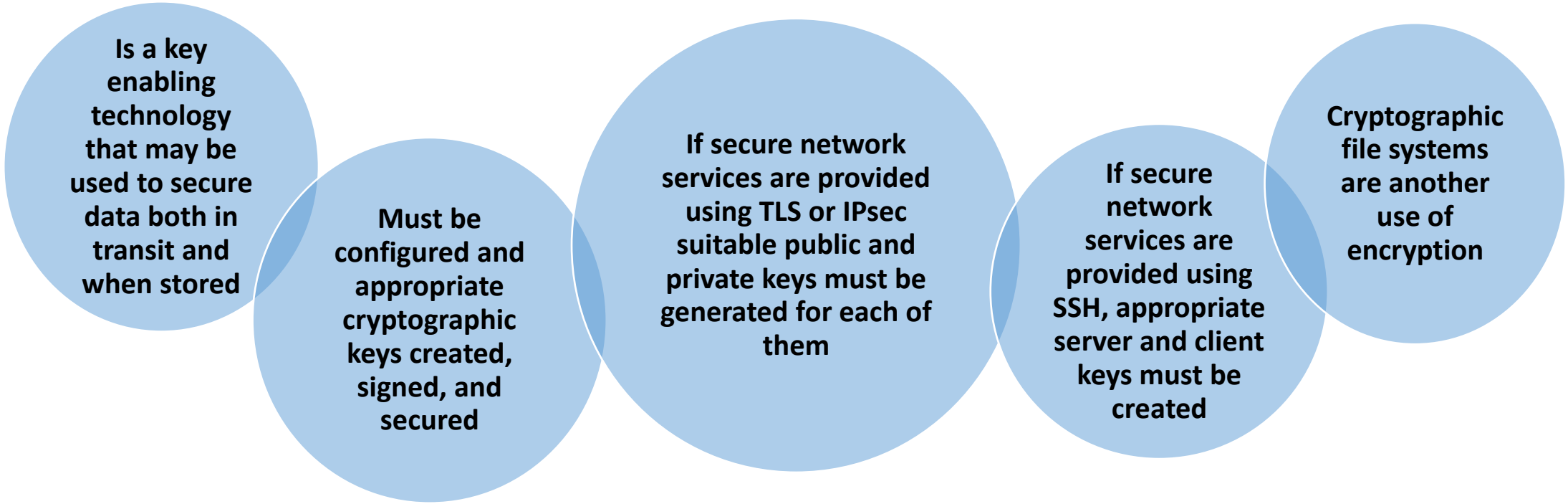
Example Policy Checklist

- https://security.utexas.edu/os-hardening-checklist/linux-7

Example Detailed Hardening Checklists

- Windows and Linux Examples in Canvas Learning Resources.

Configure Encryption



Application/Encryption Security Policy Example

- https://security.ucop.edu/files/documents/policies/secure-software-configuration-standard.pdf

Security Maintenance

- Security maintenance is continuous and includes:
  - Monitoring and analyzing logging information
  - Performing regular backups 3-2-1
    - Create 3 backups on at least 2 different types of storage media, of which 1 copy is kept off-site
  - Recovering from security compromises
  - Regularly testing system security
  - Using appropriate software maintenance processes **to patch and update all critical software**, and to monitor and revise configuration as needed

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

Generates significant volumes of information and it is important that sufficient space is allocated for them

Automated analysis is preferred

Data Backup and Archive

- Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data
  - May be legal or operational requirements for the retention of data
- Backup
  - The process of making copies of data at regular intervals
- Archive
  - The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data
- Needs and policy relating to backup and archive should be determined during the system planning stage
  - Kept online or offline
  - Stored locally or transported to a remote site
    - Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

File Integrity Management

- OSSEC - https://www.ossec.net/
- Tripwire article in Canvas
  - Limit noise by:
  - Identifying key files to track
  - Identifying who made changes – to know if the are authorized

“Poor Man’s” File Integrity Lab

Application Hardening

Application Configuration

- May include:
  - Creating and specifying appropriate data storage areas for application
  - Making appropriate changes to the application or service default configuration details
- Some applications or services may include:
  - Default data
  - Scripts
  - **User accounts**
- Of particular concern with remotely accessed services such as Web and file transfer services
  - Risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server
- https://httpd.apache.org/security/vulnerabilities_24.html

Example for a Specific Application

- https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html

Prep for Exercise

- https://portal.nice-challenge.com/

Windows Security

Windows Security

- Patch management
  - "Windows Update" and "Windows Server Update Service" assist with regular maintenance and should be used
  - Third party applications also provide automatic update support
- User administration and access controls
  - Systems implement discretionary access controls resources
  - Mandatory integrity controls are available
    - Objects are labeled as being of low, medium, high, or system integrity level
    - System ensures the subject's integrity is equal or higher than the object's level

Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
  - Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - Can be dangerous if mistakes are made
  - More useful for making bulk changes

Windows Security

Other security controls

- Essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
- Current generation Windows systems include basic firewall and malware countermeasure capabilities

Windows systems also support a range of cryptographic functions:

- Encrypting files and directories using the Encrypting File System (EFS)
- Full-disk encryption with AES using BitLocker

“Microsoft Baseline Security Analyzer”

- Free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Evaluating Windows Policies

- Open Windows browser and search for Microsoft Security Compliance Toolkit
- Download PolicyAnalyzer.zip and Windows 11 Security Baseline.zip

Linux Security

Patch Management

- Keeping security patches up to date is a widely recognized and critical control for maintaining security
- Subscribe to service to be notified of patches
- Use a tool like Landscape to identify machines needing the patch and distribute it
- Attempt to patch with minimal downtime
  - Update parts of a cluster at a time

Application and Service Configuration

- Most commonly implemented using separate text files for each application and service
- Generally located either in the /etc directory or in the installation tree for a specific application
- Individual user configurations that can override the system defaults are located in hidden "dot" files in each user's home directory
- Most important changes needed to improve system security are to disable services and applications that are not required

Linux Config Files

- On NCR:
- cd to etc directory
- ls –a to see config and . files

Users, Groups, and Permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
- Guides recommend changing the access permissions for critical directories and files
- Local exploit
  - Software vulnerability that can be exploited by an attacker to gain elevated privileges
- Remote exploit
  - Software vulnerability in a network server that could be triggered by a remote attacker

Other Linux Hardening

- Remote access controls
  - Several host firewall programs may be used
  - Most systems provide an administrative utility to select which services will be permitted to access the system
- Logging and log rotation
  - Should not assume that the default setting is necessarily appropriate

chroot Jail

- chroot jail
  - Restricts the server's view of the file system to just a specified portion
  - Uses chroot system call to confine a process by mapping the root of the filesystem to some other directory
  - File directories outside the chroot jail aren't visible or reachable
  - Main disadvantage is added complexity and difficult troubleshooting
- Example exercise
  - https://www.geeksforgeeks.org/linux-virtualization-using-chroot-jail/
  - Can be broken: If program or user has root privileges, they can do another chroot

Windows and Linux Config Exercise

NICE Challenge – Calamitous Configurations

- Windows – eliminate unnecessary services
- Linux - Restrict root login

Group Policy Configurations

https://portal.nice-challenge.com/

Virtualization Security

Virtualized Systems

- In virtualized systems, the available hardware resources must be appropriately shared among the various guest OS's
- These include CPU, memory, disk, network, and other attached devices
- CPU and memory are generally partitioned between these, and scheduled as required
- Disk storage may be partitioned, with each guest having exclusive use of some disk resources
- Alternatively, a "virtual disk" may be created for each guest, which appears to it as a physical disk with a full file-system, but is viewed externally as a single "disk image" file on the underlying file-system
- Attached devices such as optical disks, or USB devices are generally allocated to a single guest OS at a time

Hypervisor

- Software that sits between the hardware and the VMs
- Acts as a resource broker
- It allows multiple VMs to safely coexist on a single physical server host and share that host's resources
- Virtualizing software provides abstraction of all physical resources and thus enables multiple computing stacks, called virtual machines, to be run on a single physical host
- Each VM includes an OS, called the guest OS
    - This OS may be the same as the host OS, if present, or a different one

Hypervisor Functions

The principal functions performed by a hypervisor are:

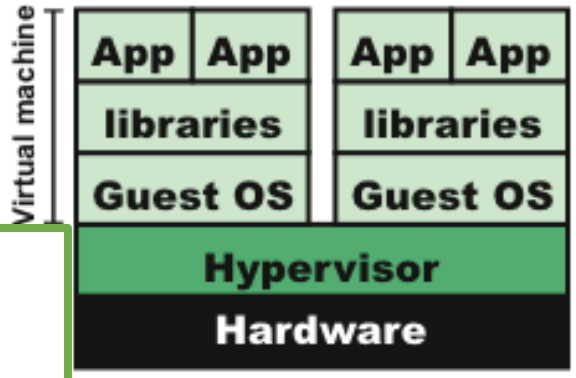
- Execution management of VMs
- Devices emulation and access control
- Execution of privileged operations by hypervisor for guest VMs
- Management of VMs (also called VM lifecycle management)
- Administration of hypervisor platform and hypervisor software

Containers

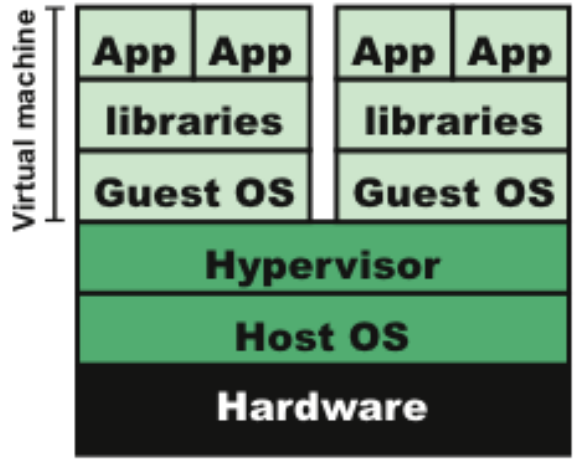
- In this approach, software known as a virtualization container, runs on top of the host OS kernel and provides an isolated execution environment for applications
- Unlike hypervisor-based VMs, containers do not aim to emulate physical servers
- All containerized applications on a host share a common OS kernel
- For containers, only a small container engine is required as support for the containers
- Containerization sits in between the OS and applications and incurs lower overhead, but potentially introduces greater security vulnerabilities

Comparison of Virtual Machine Containers

Proxmox
KVM
Hyper-V
Vmware Esxi

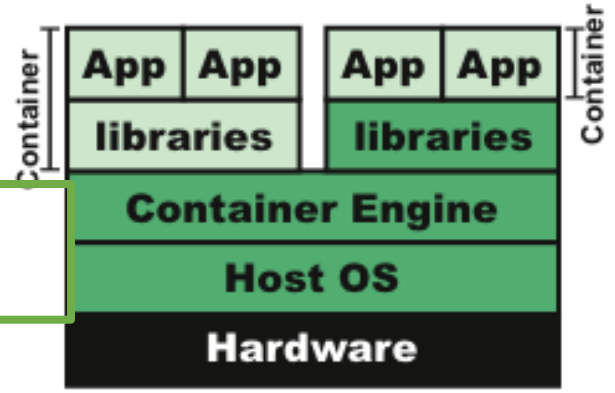


(a) Type 1 hypervisor
(native virtualization)



(b) Type 2 hypervisor
(hosted virtualization)

Docker
Kubernetes



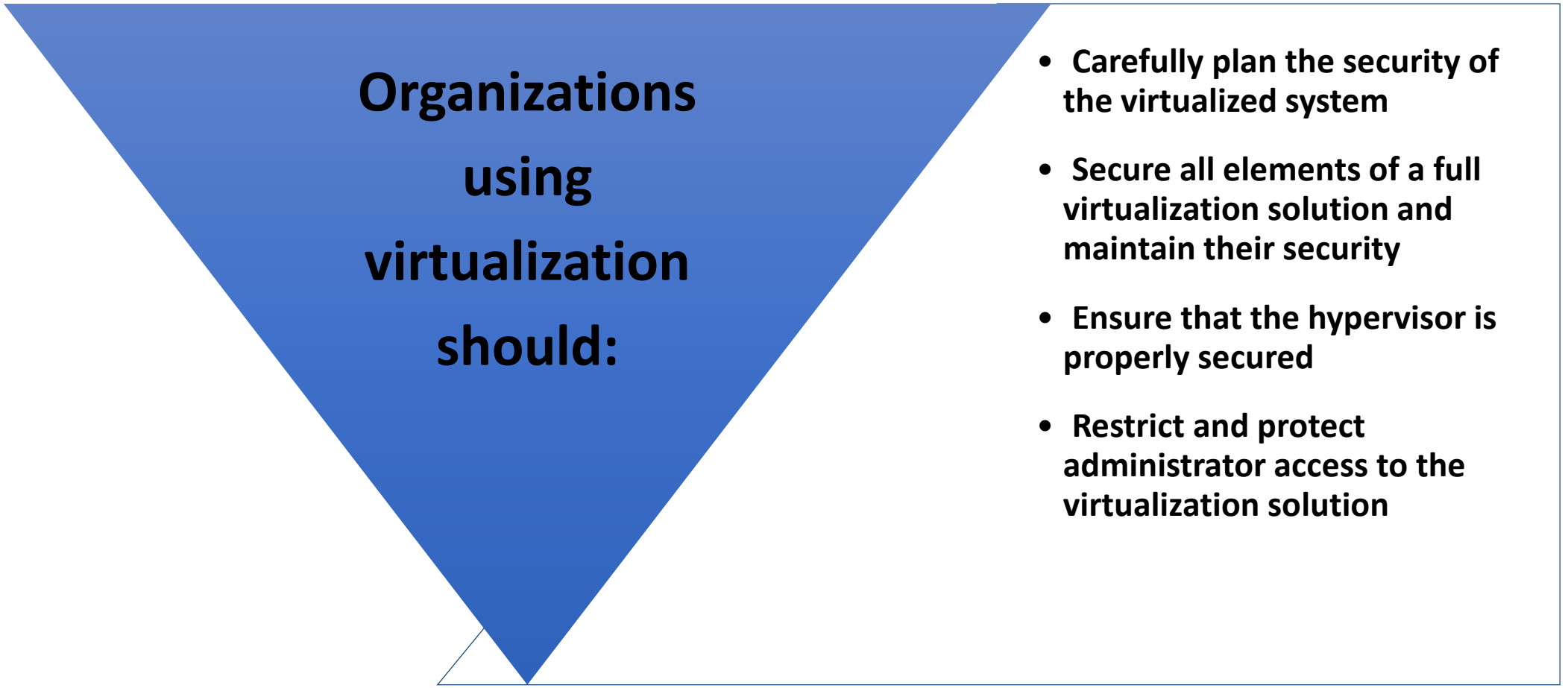
KVM
VirtualBox
Vmware Desktop

(c) Container (application virtualization)

Virtualization Security Issues

- Security concerns include:
  - Guest OS isolation
    - Ensuring that programs executing within a guest OS may only access and use the resources allocated to it
  - Guest OS monitoring by the hypervisor
    - Which has privileged access to the programs and data in each guest OS
  - Virtualized environment security
    - image and snapshot management which attackers may attempt to view or modify
    - Shared folders and clipboards

Securing Virtualization Systems



- Carefully plan the security of the virtualized system
- Secure all elements of a full virtualization solution and maintain their security
- Ensure that the hypervisor is properly secured
- Restrict and protect administrator access to the virtualization solution

Hypervisor Security

- Should be
  - Secured using a process similar to securing an operating system
  - Installed in an isolated environment
  - Configured so that it is updated automatically
  - Monitored for any signs of compromise
  - Accessed only by authorized administration
- Ideally administration traffic should use a separate network with very limited access provided from outside the organization
  https://www.virtualbox.org/manual/ch13.html

Module 7 Assignment

- Modify the spreadsheet template to reflect ONLY the things in the scenario
- Your model will have fewer things in each category, but a good analysis of each
- List any assets that you think might be related to the vulnerability
- On threat sheet, estimate potential damage and probability
  - In mitigations, list what should be done to prevent or recover from attack
  - In issues give brief description of specific issues that could arise

Physical and Infrastructure Security

News

- https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Exec%20Summary_2024%20Microsoft%20Digital%20Defense%20Report.pdf
- https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/

Physical and Infrastructure Security

Logical security

- Protects computer-based data from software-based and communication-based threats

Physical security

- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems
- Must prevent any type of physical access or intrusion that can compromise logical security

Premises security

- Also known as corporate or facilities security
- Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
- Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

Physical Security Threats

Physical Security Threat Categories

- Environmental threats
- Technical threats
- Human-caused threats
  - Physical access can overcome logical controls

Environmental Threats and Mitigations

Natural Disasters

	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/ blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

Source: ComputerSite Engineering, Inc.

Examples

- https://mha-it.com/blog/business-emergencies

Natural Disaster Mitigation

- Location of data center – avoid flood zones
- If possible, avoid tornado and hurricane zones

Fire and Smoke

- Fire threats can be wildfire, building fire or electrical fire
- Fire suppression around equipment is a key concern
  - Sprinklers can make equipment unusable and pose electrocution threat to people
  - Clean gas systems can reduce oxygen, but are one-shot and may not extinguish fire
  - Some combination is ideal
- Smoke damage related to fires can also be extensive as smoke is an abrasive.
  - Collected particles can prevent heat dissipation or cause electrical shorts
  - It collects on the heads of unsealed magnetic disks, optical disks, and tape drives

Fire Extinguishers (For Security+)

Table 8.1	Types of Fire and Suppression Methods		
Class of Fire	**Type of Fire**	**Examples of Combustible Materials**	**Example Suppression Method**
A	Common combustibles	Wood, paper, cloth, plastics	Water or dry chemical
B	Combustible liquids	Petroleum products, organic solvents	CO_2 or dry chemical
C	Electrical	Electrical wiring and equipment, power tools	CO_2 or dry chemical
D	Flammable metals	Magnesium, titanium	Copper metal or sodium chloride

Water Damage

- Primary danger is an electrical short
- A pipe may burst from a fault in the line or from freezing
- Sprinkler systems set off accidentally
- Floodwater leaving a muddy residue and suspended material in the water
- **Mitigation**
  - Equipment location: due diligence should be performed to ensure that water from as far as two floors above will not create a hazard
  - Cutoff sensors to turn off power in case of water release

Humidity and Condensation

- Long-term exposure to high humidity can result in corrosion nab also cause a galvanic effect that results in electroplating, in which metal from one connector slowly migrates to the mating connector, bonding the two together.
- Condensation can threaten magnetic and optical storage media and cause a short circuit, which in turn can damage circuit boards
- Low humidity - Static electricity discharges as low as 10 volts can damage particularly sensitive electronic circuits, and discharges in the hundreds of volts can create significant damage to a variety of electronic circuits.
  - Discharges from humans can reach into the thousands of volts
- In general, relative humidity should be maintained between 40% and 60% to avoid the threats from both low and high humidity.

Dust and Infestation

Dust

- Rotating storage media and computer fans are the most vulnerable to damage
- Can also block ventilation
- Influxes can result from a number of things:
  - Controlled explosion of a nearby building
  - Windstorm carrying debris
  - Construction or maintenance work in the building
- Mitigation is filtered air system

Infestation

- Covers a broad range of living organisms:
  - High-humidity conditions can cause mold and mildew
  - Insects, particularly those that attack wood and paper
  - Rodents that chew wire insulation

Mitigation for Environmental Threats

- Environmental control equipment for temperature, humidity and dust

Chemical, Radiological, and Biological Hazards

- Pose a threat from intentional attack and from accidental discharge
- Discharges can be introduced through the ventilation system or open windows, and in the case of radiation, through perimeter walls
- Flooding can also introduce biological or chemical contaminants

Technical Threats

Electricity Issues

- Under-voltage - dips/brownouts/outages, interrupts service
- Over-voltage - surges/faults/lightening, can destroy chips
- Noise - on power lines, may interfere with device operation

Electromagnetic interference (EMI)

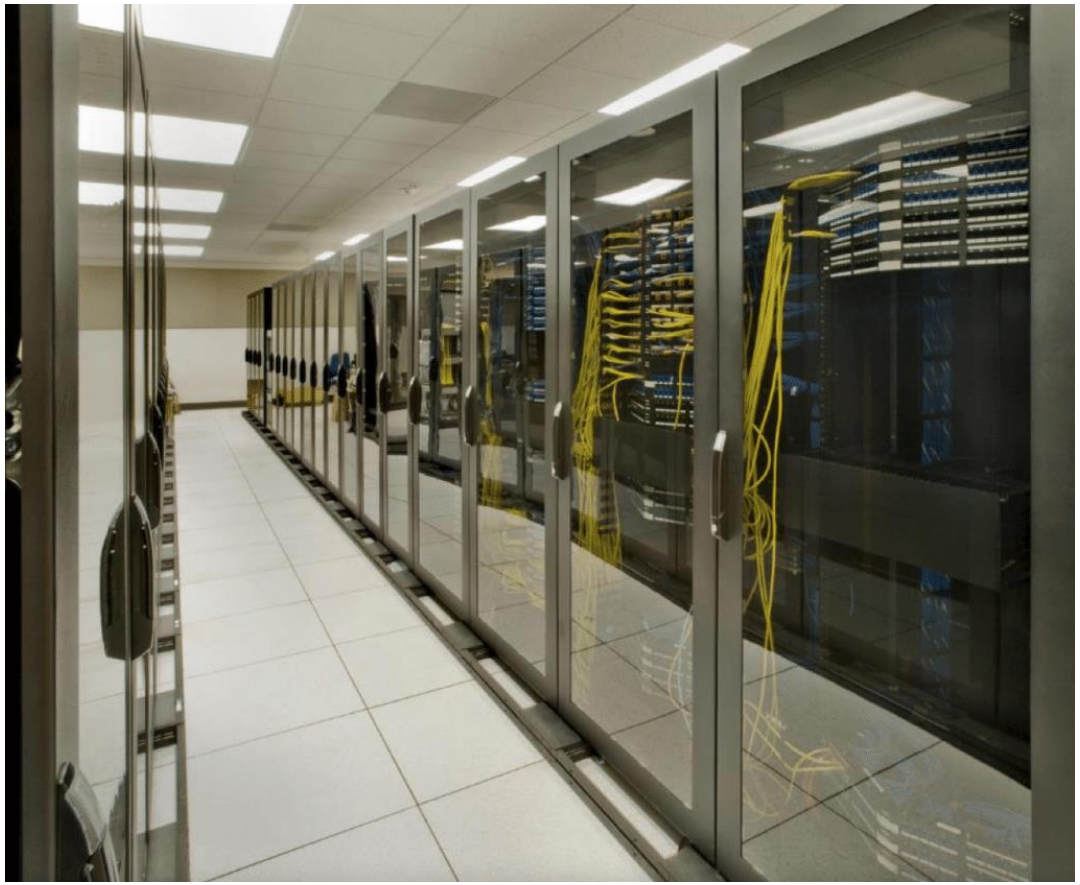
- Noise along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations
- Noise can be transmitted through space as well as through power lines
- Can cause intermittent problems with computers

Mitigation Measures For Technical Threats

- Uninterruptible power supply (UPS) for each piece of critical equipment
- Critical equipment should be connected to an emergency power source (like a generator)
- To deal with electromagnetic interference (EMI) and evesdropping a combination of filters and shielding can be used

TEMPEST Standard
https://en.wikipedia.org/wiki/Tempest_(codename)

Faraday Cage



Faraday Cage

Human Caused Threats

The Physical Security Problem

- Physical access negates all other security measures
  - No matter how impenetrable the firewall and intrusion detection system (IDS), if an attacker can find a way to walk up to and touch a server, he can break into it
- Physically securing information assets does not mean just the servers
  - It means protecting physical access to all the organization's computers and its entire network infrastructure

Physical Security – Data Theft

- Physical access is the most common way of imaging a drive
  - Biggest benefit for the attacker is that drive imaging leaves absolutely no trace of the crime

Physical Security – DoS

- A denial-of-service (DoS) attack can also be performed with physical access
  - Physical access to the computers can be much more effective than a network-based DoS attack

Physical Security – Boot Media

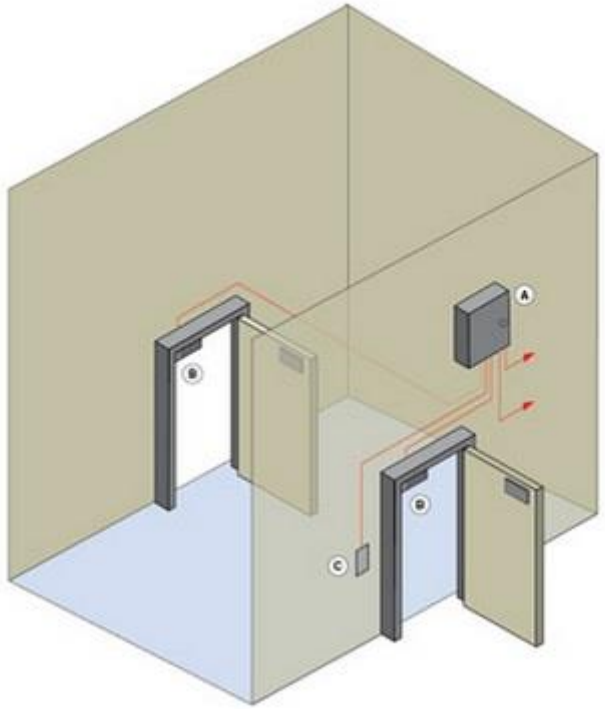
- Any media used to boot a computer into an operating system that is not the native OS on its hard drive can be classified as a bootdisk
- A LiveCD or bootable flash drive contains a bootable version of an entire operating system, typically a variant of Linux, complete with drivers for most devices
  - LiveCDs give an attacker more permissions and a greater array of attack tools
- With a LiveCD, an attacker would likely have access to the hard disk and also to an operational network interface that would allow him to send the drive data over the Internet if properly connected

Kali Boot to Root Demo

Mitigation Measures
Human-Caused Physical Threats

- Physical access control
  - Restrict building access -perimeter security
  - Controlled areas patrolled or guarded
  - Locks or screening measures at entry points
  - Equip movable resources with a tracking device
  - Power switch controlled by a security device
  - Surveillance systems that provide recording and real-time remote viewing
  - Intruder sensors and alarms
  - **Restrict access to critical rooms**

Mantrap Entrance



Overall Physical Security Mitigation

- Use of cloud computing
  - This just shifts who is responsible

Physical Security Standards

- https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PE
- ISO 27002

Open Nice Challenge Workspace

Physical Security Summary

Prevent damage to physical infrastructure	Prevent physical infrastructure misuse that leads to the misuse or damage of protected information
• Concerns include system hardware, physical facility, support facilities, and personnel	• Includes vandalism, theft of equipment, theft by copying, theft of services, and unauthorized entry

Recovery from Physical Equipment Damage

- **Most essential element of recovery is redundancy**
  - Provides for recovery from loss of data
  - Ideally all important data should be available off-site and updated as often as feasible
  - Can use batch encrypted remote backup
  - For critical situations a remote hot-site that is ready to take over operation instantly can be created
    - Can also have warm sites and cold sites

Data Center Security

Includes Redundancy and Resilience

Data Center

- An enterprise facility that houses a large number of servers, storage devices, and network switches and equipment
- Generally includes redundant or backup power supplies, redundant network connections, environmental controls, and various security devices
- Can occupy one room of a building, one or more floors, or an entire building
- Examples of uses include:
  - UNR Pronghorn
  - Cloud service providers
  - Large scientific research facilities
  - IT facilities for large enterprises

TIA-942 Data Center Tiers

- **Rated-1: Basic Site Infrastructure**
  A data center which has single capacity components and a single, non-redundant distribution path serving the computer equipment. It has limited protection against physical events.

- **Rated-2: Redundant Capacity Component Site Infrastructure**
  A data center which has redundant capacity components and a single, non-redundant distribution path serving the computer equipment. It has improved protection against physical events.

- **Rated-3: Concurrently Maintainable Site Infrastructure**
  A data center which has redundant capacity components and multiple independent distribution paths serving the computer equipment. Typically, only one distribution path serves the computer equipment at any time. The site is concurrently maintainable which means that every capacity component, including elements which are part of the distribution path, can be removed/replaced/serviced on a planned basis without disrupting the ICT capabilities to the end user. It has protection against most physical events.

- **Rated-4: Fault Tolerant Site Infrastructure**
  A data center which has redundant capacity components and multiple independent distribution paths serving the computer equipment which all are active. The data center allows concurrent maintainability and one (1) fault anywhere in the installation without causing downtime. It has protection against almost all physical events.

(Table is on page 177 in textbook)

Google Data Center

- https://goo.gl/w03sJ

- Security:
- https://www.google.com/about/datacenters/data-security/

Data Center Security Standards

- https://www.iso.org/standard/75106.html
- Legal Requirements:
  - https://cloud.google.com/security/compliance/#/

NICE Challenge OS Hardening

- STIGs

Midterm Exam

- Review Chapter Outlines and past quizzes
- 50 Questions 70 Minutes
- Take any time before due date/time

Prep for Cloud Computing

- **For Assignment:**
  - Check your UNR email from Qwiklabs or Cloud Skills Boost for training credits for assignment
    - Sign up with **UNR email**
- **For in-class work:**
- Watch for email from me to claim your $50 cloud credits for in-class work next week.
  - Enter UNR email at link to receive the credit voucher
  - Use Google account to redeem the voucher
    - If you have a Google account tied to a credit card, it might be safer to create a new account