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

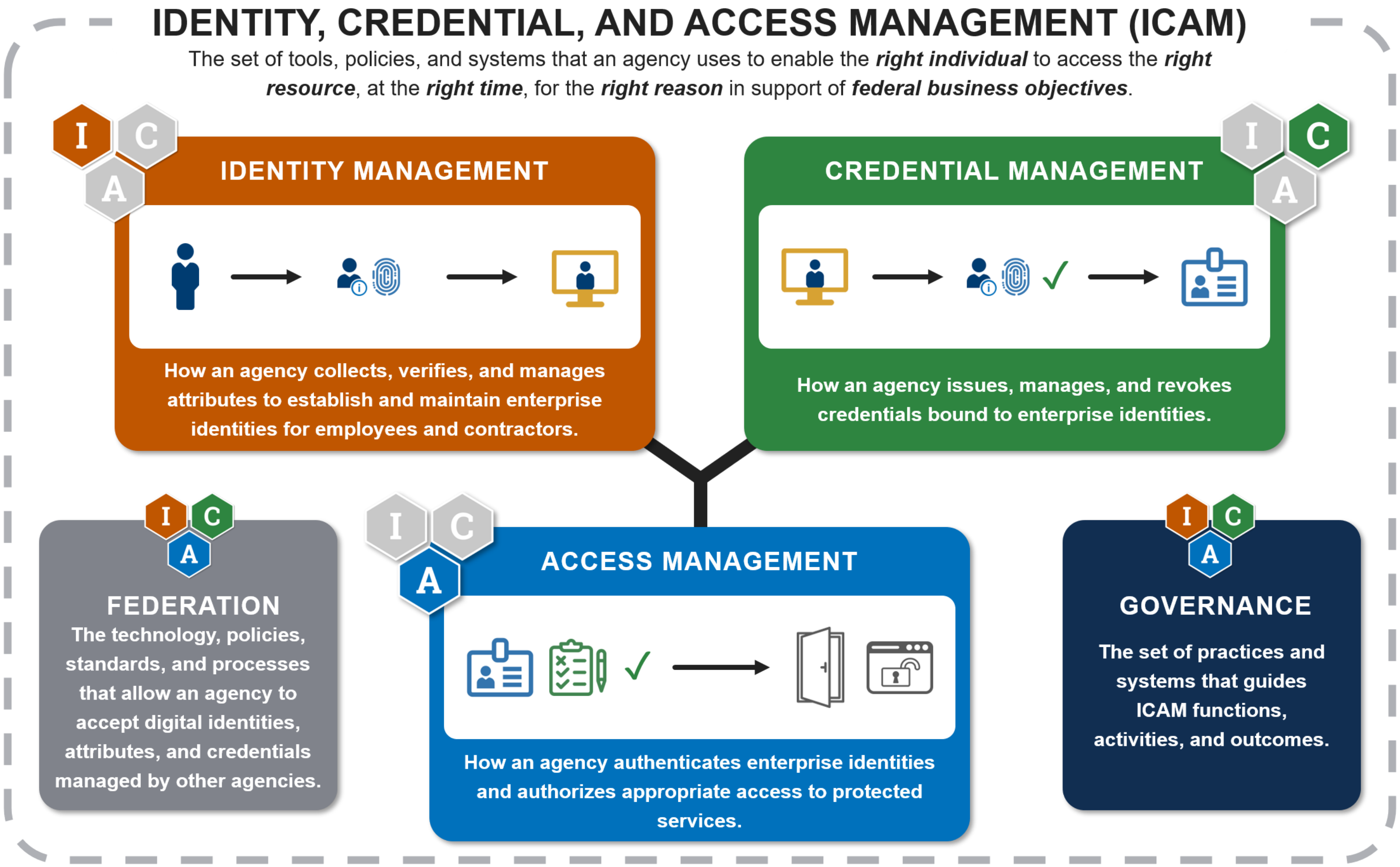
Identity, Credential, and Access Management (ICAM)

- 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



IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

The set of tools, policies, and systems that an agency uses to enable the ***right individual*** to access the ***right resource***, at the ***right time***, for the ***right reason*** in support of ***federal business objectives***.

IDENTITY MANAGEMENT

How an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.

CREDENTIAL MANAGEMENT

How an agency issues, manages, and revokes credentials bound to enterprise identities.

FEDERATION

The technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.

ACCESS MANAGEMENT

How an agency authenticates enterprise identities and authorizes appropriate access to protected services.

GOVERNANCE

The set of practices and systems that guides ICAM functions, activities, and outcomes.

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)

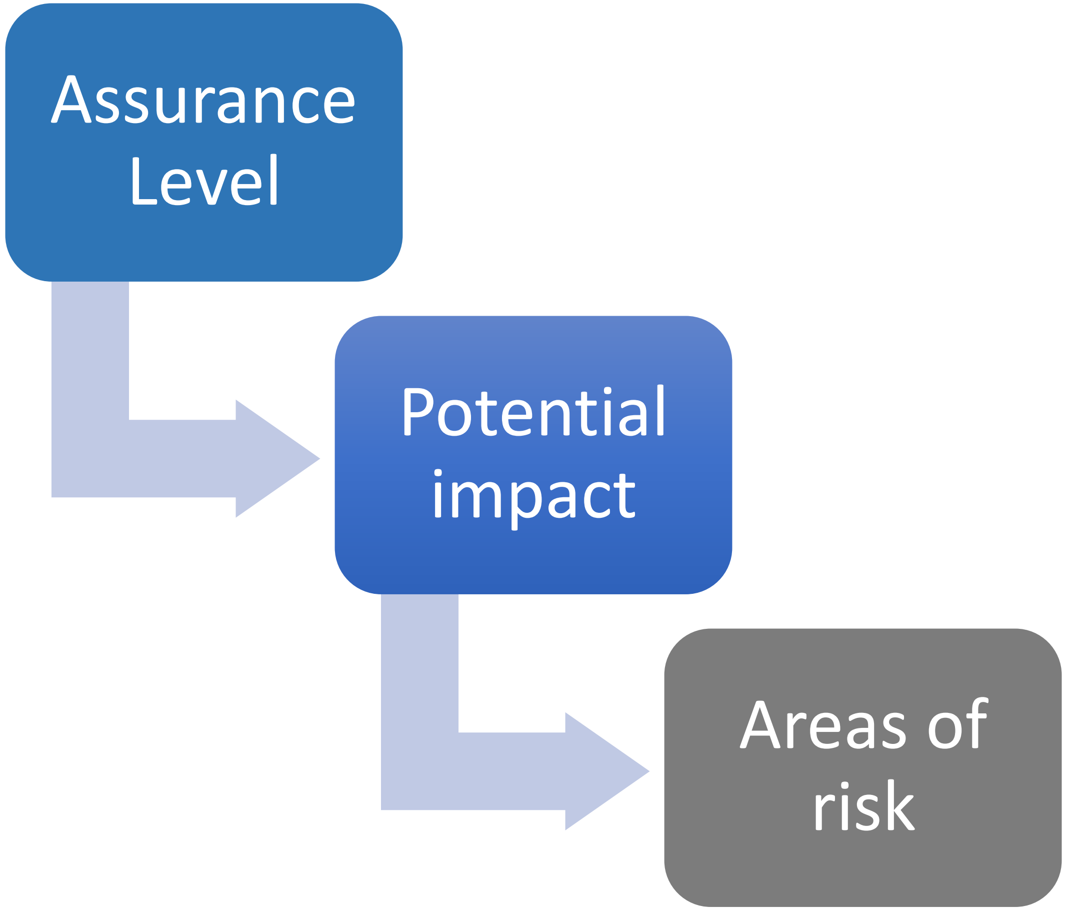
For protection controlled, unclassified information

	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

Potential impact

Areas of risk

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

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	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

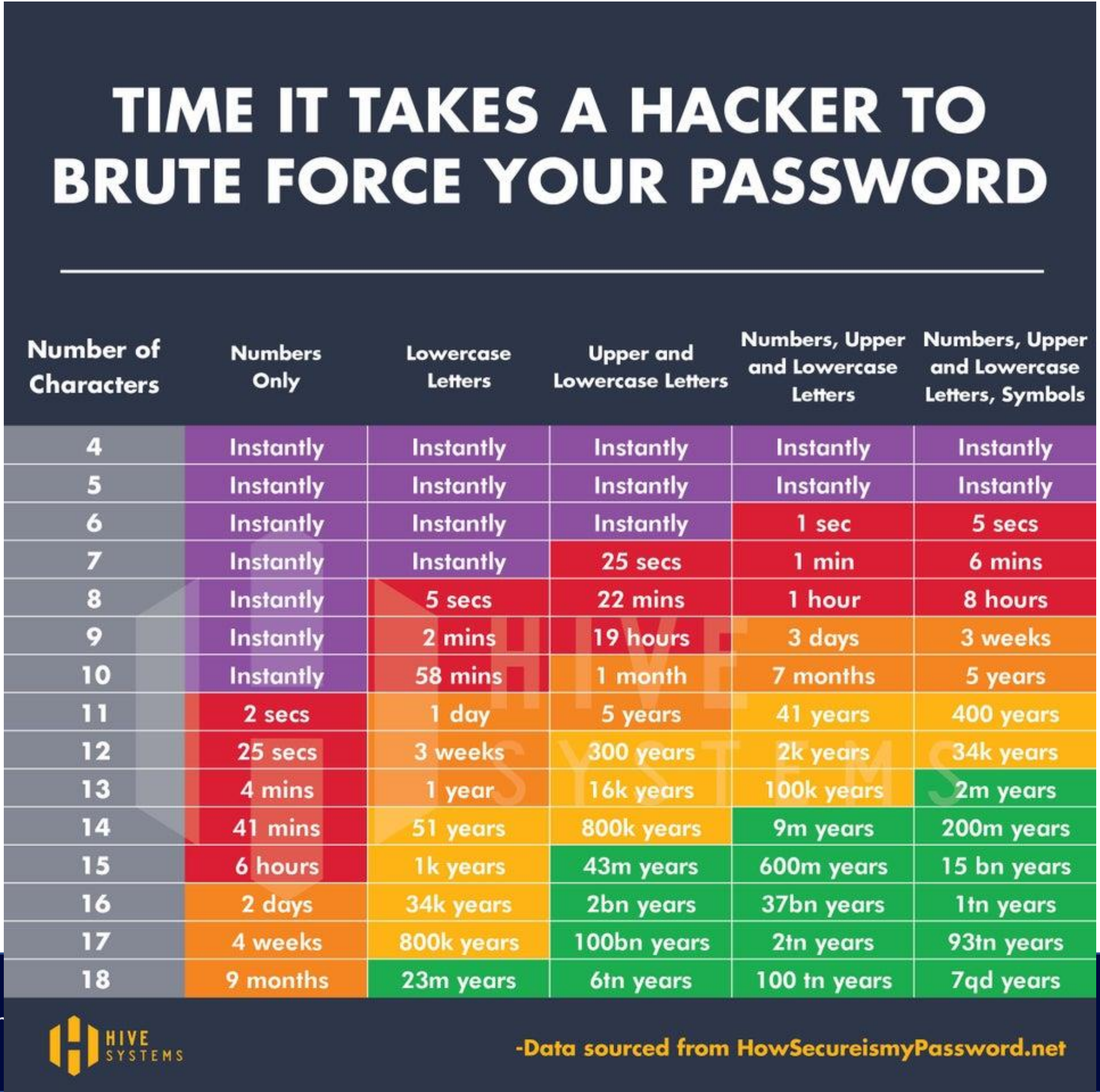
- ***Dictionary or preimage attack***
  - Attacker creates digests of common dictionary words
  - Compares against stolen digest file
  - It is estimated that over 100 million passwords were stolen and published online in one year
  - Websites now host lists of leaked passwords along with statistical 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

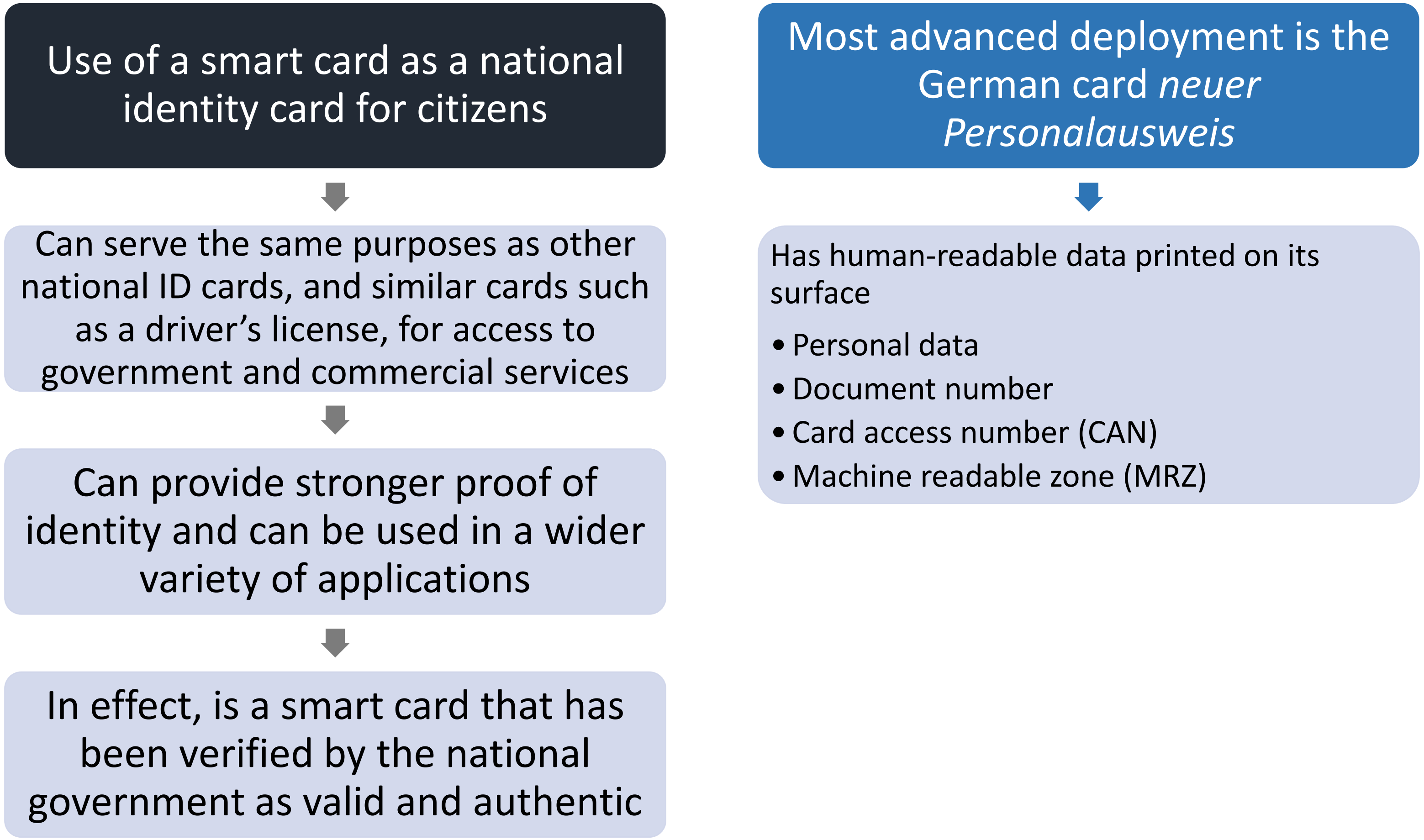
2FA with OTP is not Always Secure

- 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

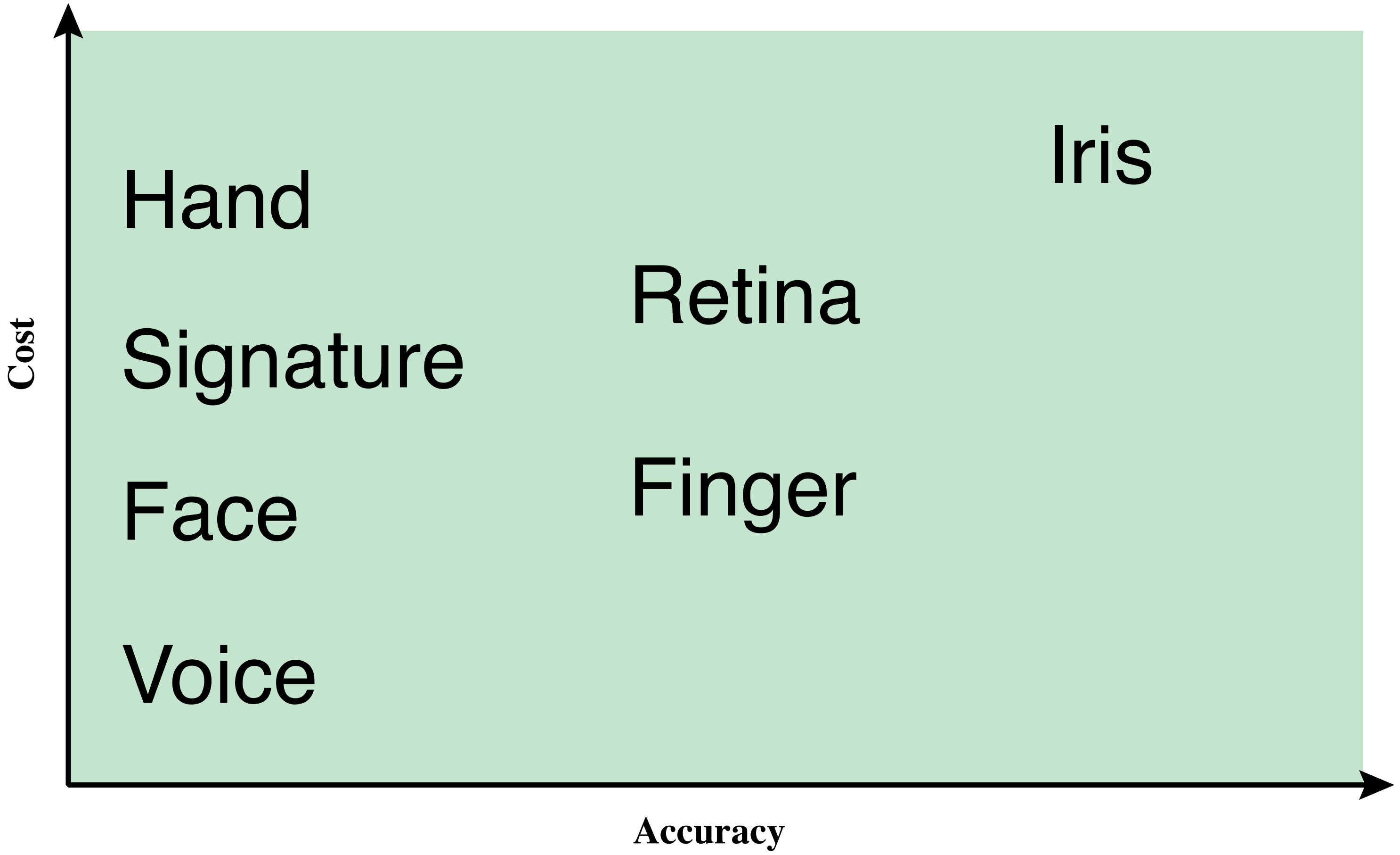
- Yubikey – can be linked to app
- Passkeys
  - Uses Asymmetric keys (public-private) to encode challenge message and response
  - https://www.passkeys.io/technical-details
  - Private key is protected by device security (hopefully)
  - Created by FIDO alliance - https://fidoalliance.org/what-is-fido/

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



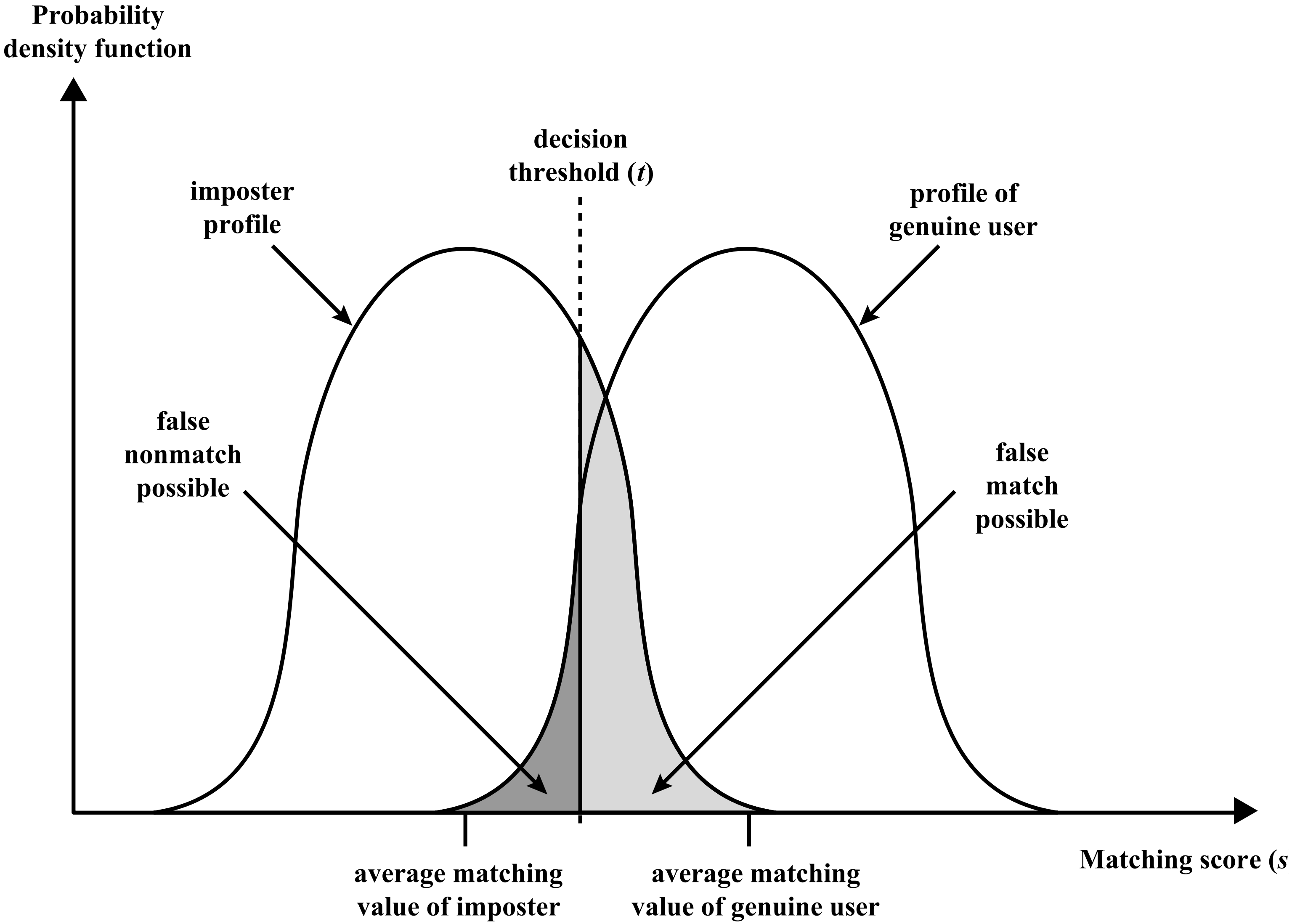
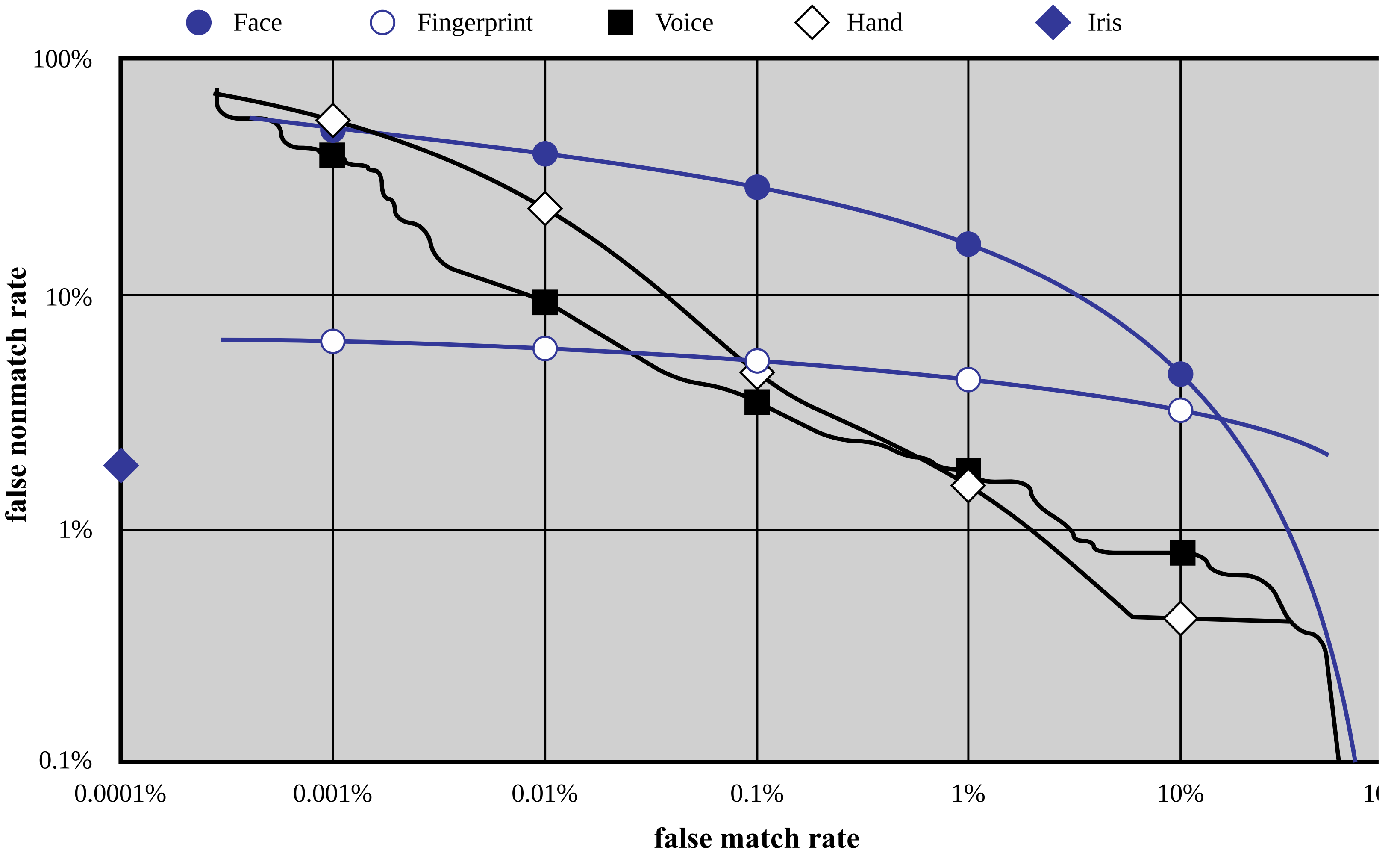


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (*s*) is greater than a preassigned threshold (*t*), a match is declared.

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

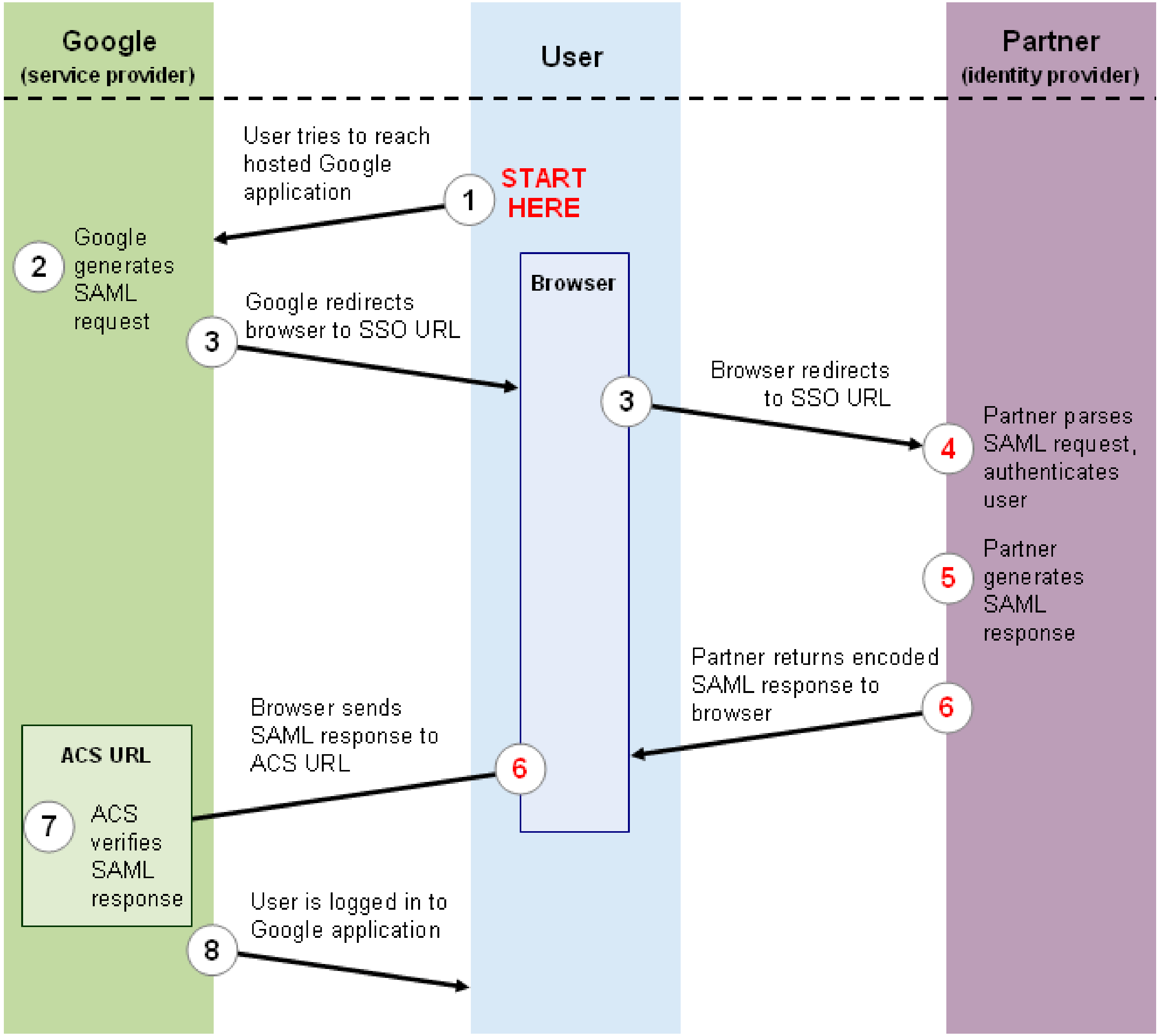
- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization

- 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

SAMLTransaction Steps



Google
(service provider)

User

Partner
(identity provider)

1 START HERE
User tries to reach hosted Google application

2 Google generates SAML request

3 Google redirects browser to SSO URL

Browser

3 Browser redirects to SSO URL

4 Partner parses SAML request, authenticates user

5 Partner generates SAML response

6 Partner returns encoded SAML response to browser

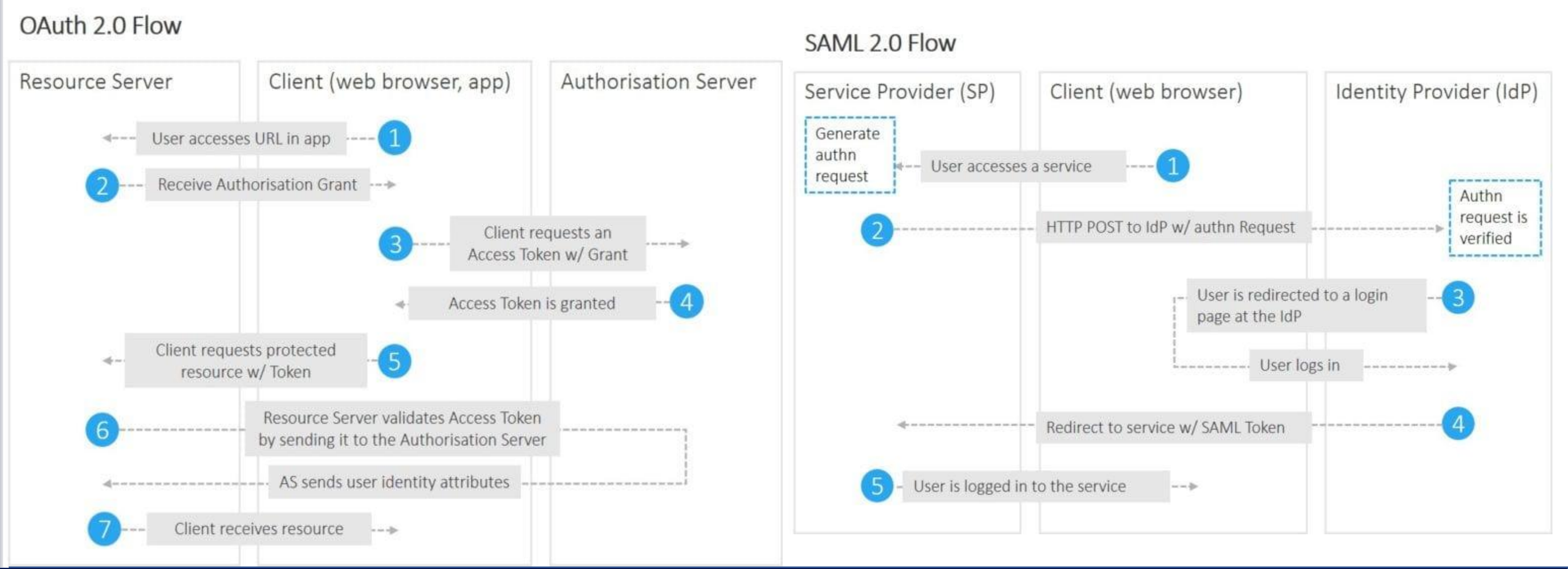
6 Browser sends SAML response to ACS URL

ACS URL

7 ACS verifies SAML response

8 User is logged in to Google application

OAUTH and SAML Flow



OAuth 2.0 Flow

Resource Server | Client (web browser, app) | Authorisation Server

1. User accesses URL in app
2. Receive Authorisation Grant
3. Client requests an Access Token w/ Grant
4. Access Token is granted
5. Client requests protected resource w/ Token
6. Resource Server validates Access Token by sending it to the Authorisation Server

AS sends user identity attributes

7. Client receives resource

SAML 2.0 Flow

Service Provider (SP) | Client (web browser) | Identity Provider (IdP)

Generate authn request

1. User accesses a service
2. HTTP POST to IdP w/ authn Request

Authn request is verified

3. User is redirected to a login page at the IdP

User logs in

4. Redirect to service w/ SAML Token
5. User is logged in to the service

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

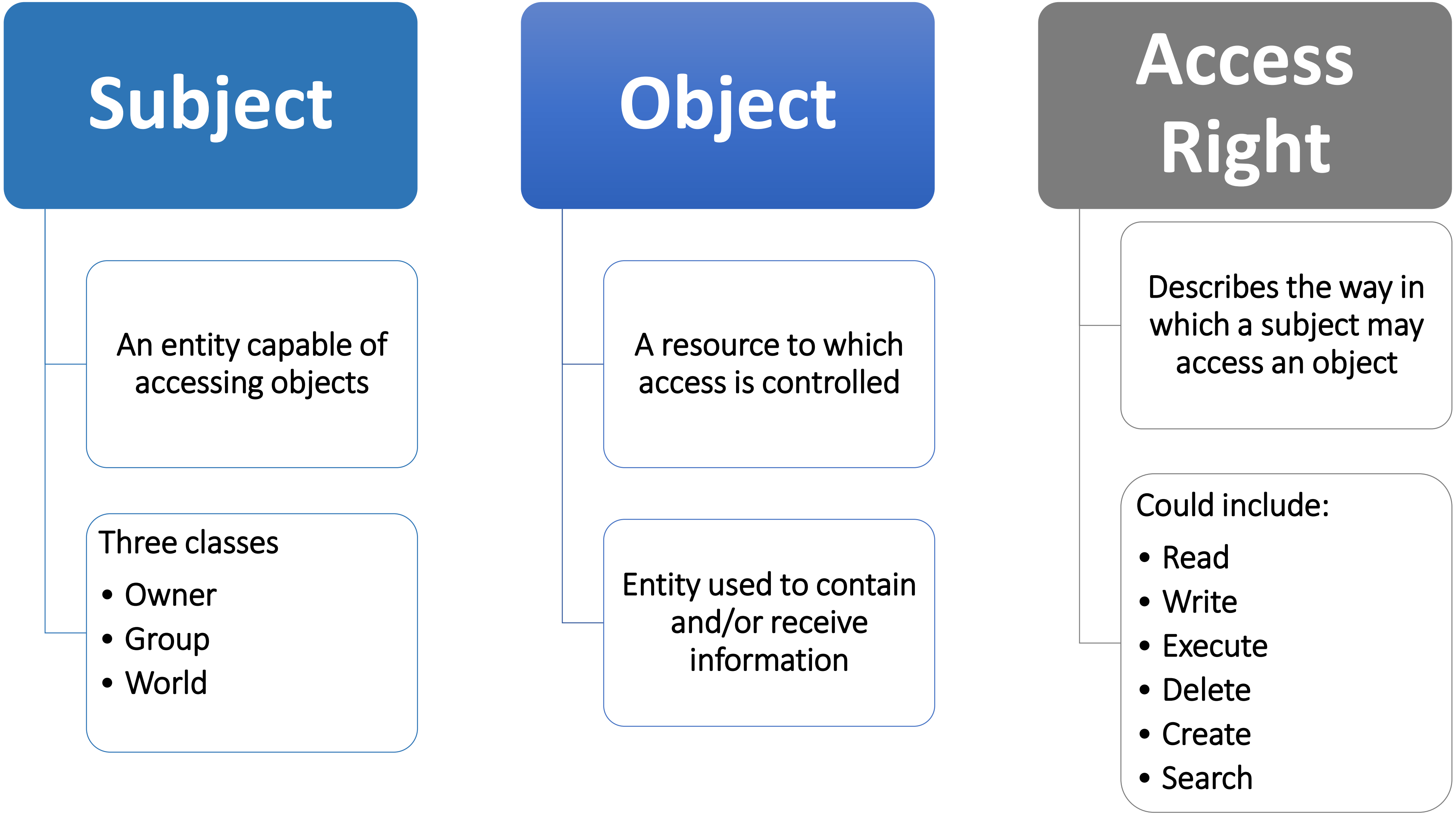
- **The *principle of economy of mechanism* states that security mechanisms should be as simple as possible.**

- *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

OBJECTS

SUBJECTS

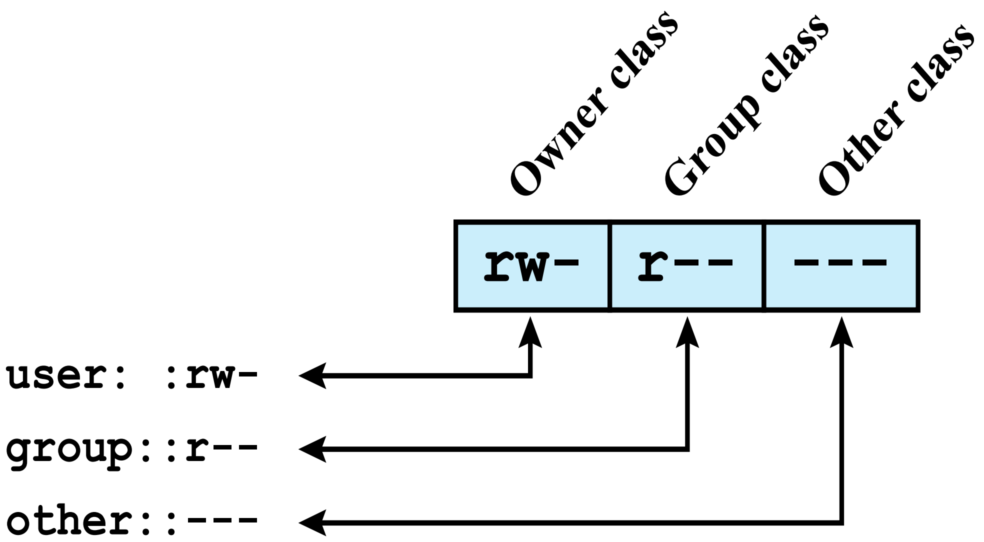
	File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

(a) Access matrix

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

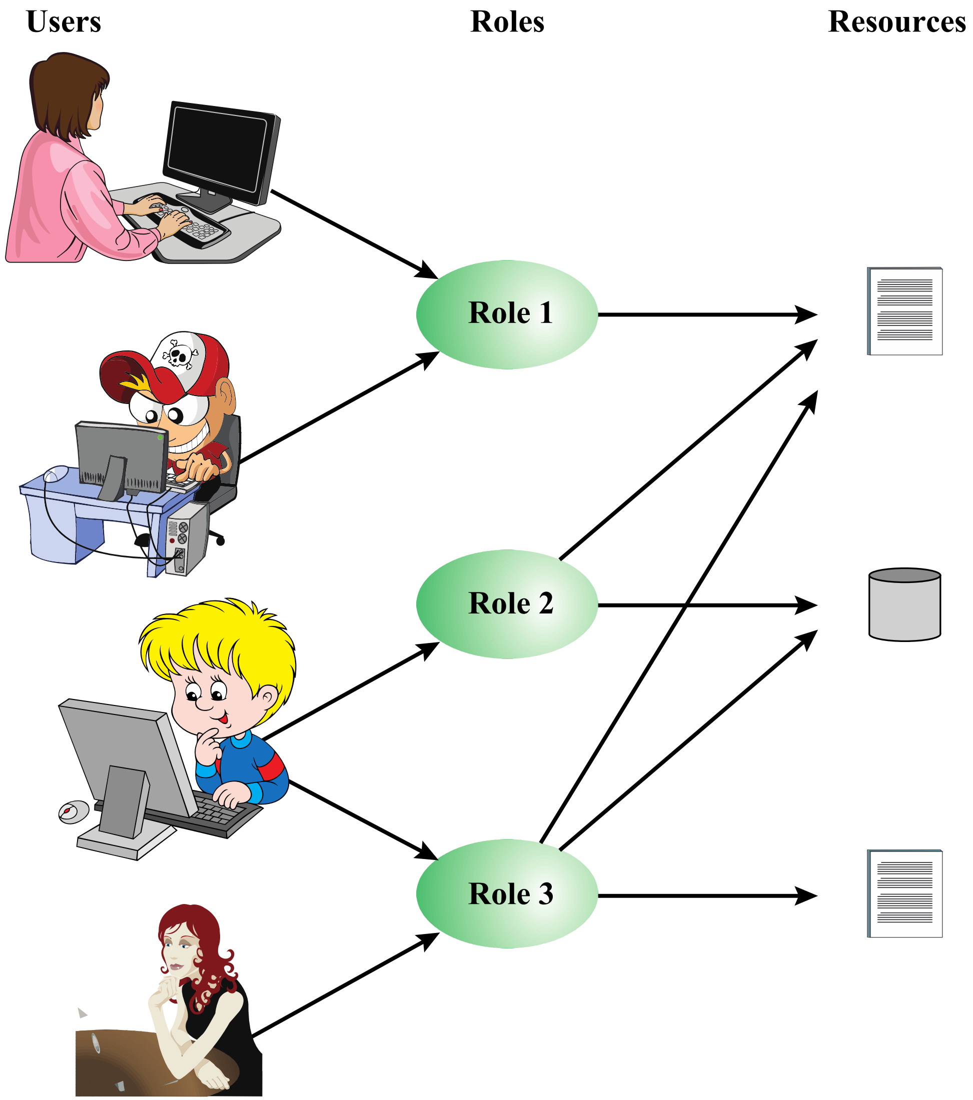
- https://www.linux.com/tutorials/understanding-linux-file-permissions/
- https://www.unixtutorial.org/difference-between-chmod-and-chown
  - *View in Labtainer*
  - *Ls –l*
  - *Find by -user*
- Linux Capabilities labtainer
  - https://ncr-remote.cse.unr.edu/accounts/login/

Role Based Access Control (RBAC)

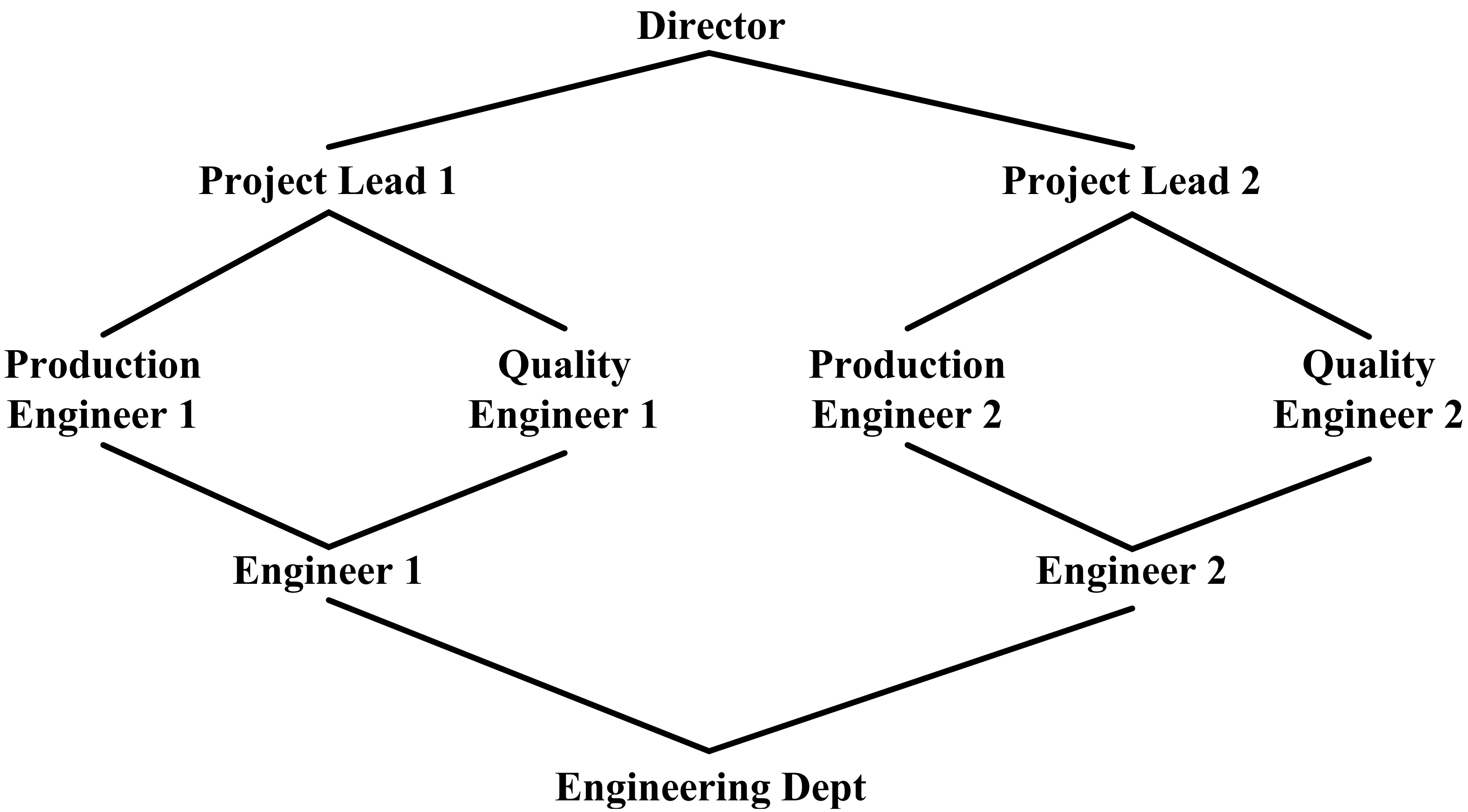
- Also called *Non-Discretionary Access Control*
- Access permissions are based on user's job function
- RBAC assigns permissions to particular roles in an organization
- Users are assigned to those roles

- 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



Director

Project Lead 1

Project Lead 2

Production Engineer 1

Quality Engineer 1

Production Engineer 2

Quality Engineer 2

Engineer 1

Engineer 2

Engineering Dept

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

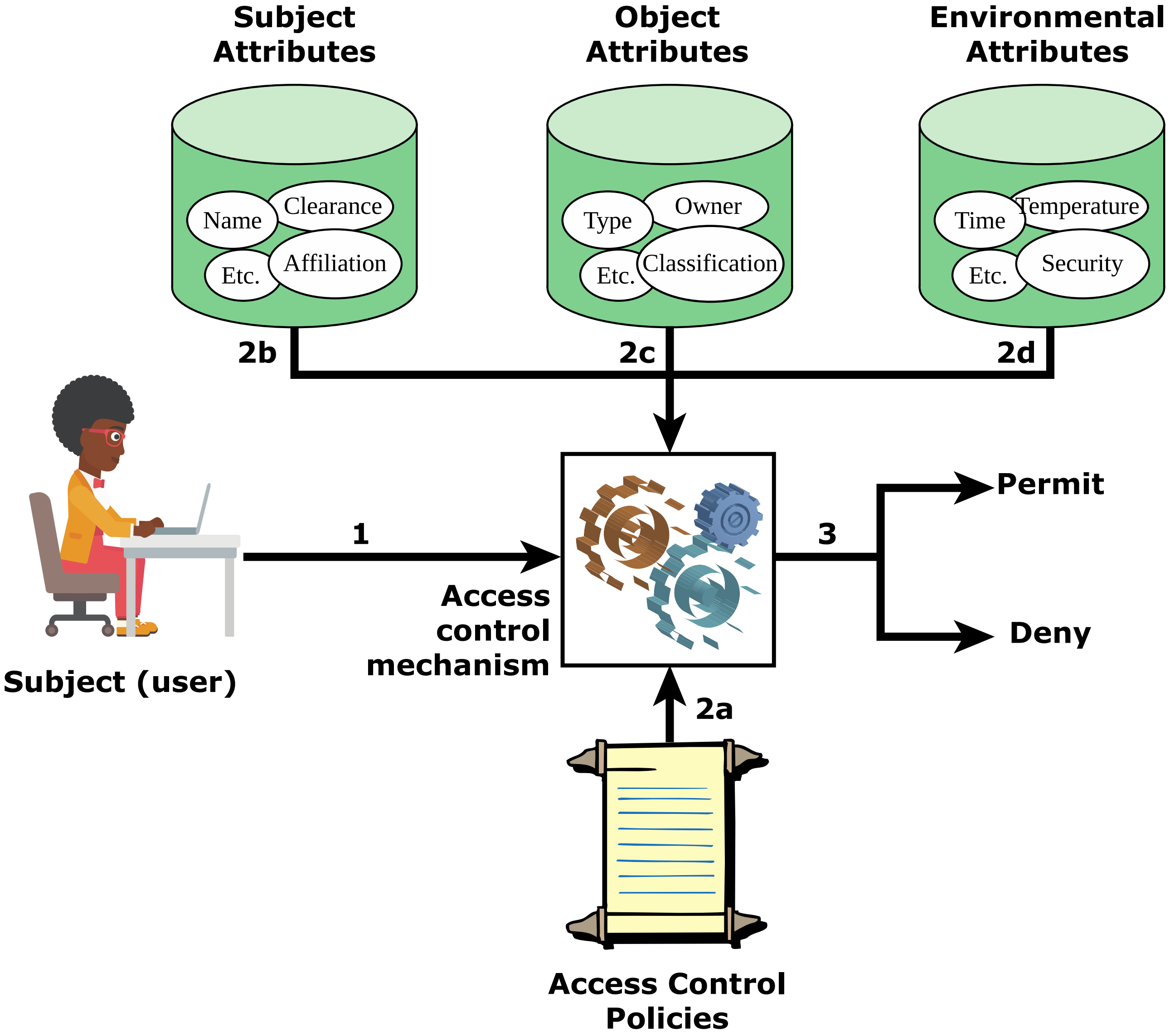
Object attributes

- 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?