September 10, 2024

“Who Are You?”

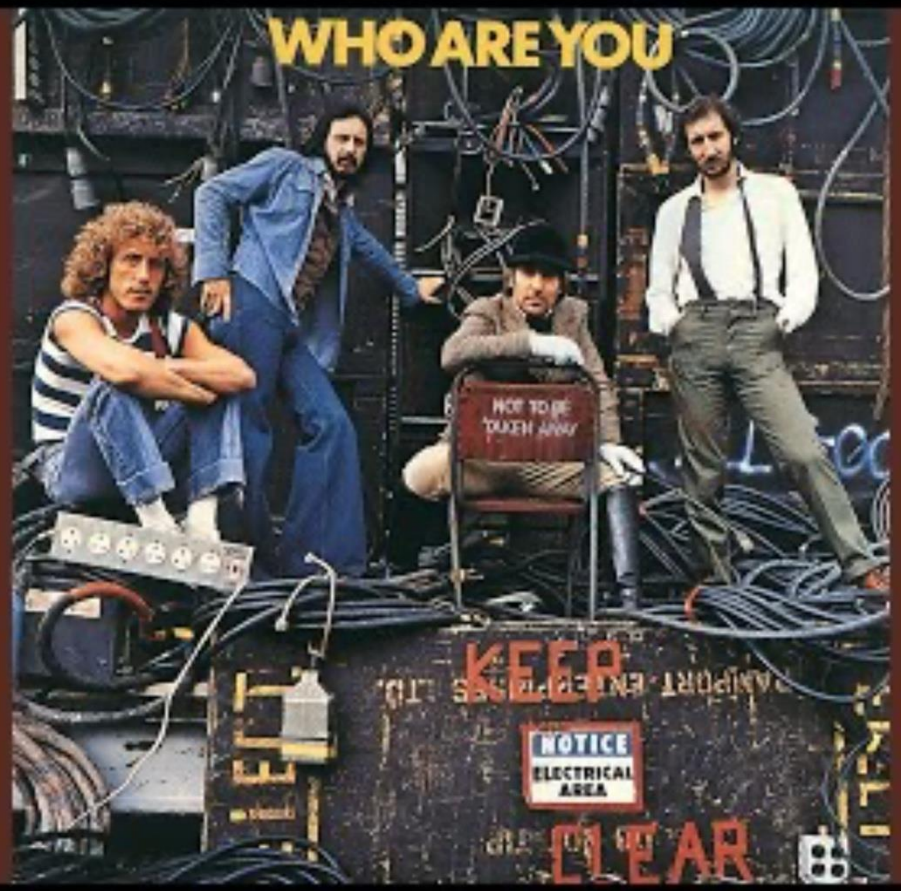
Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

OU Tulsa
SCHUSTERMAN CENTER

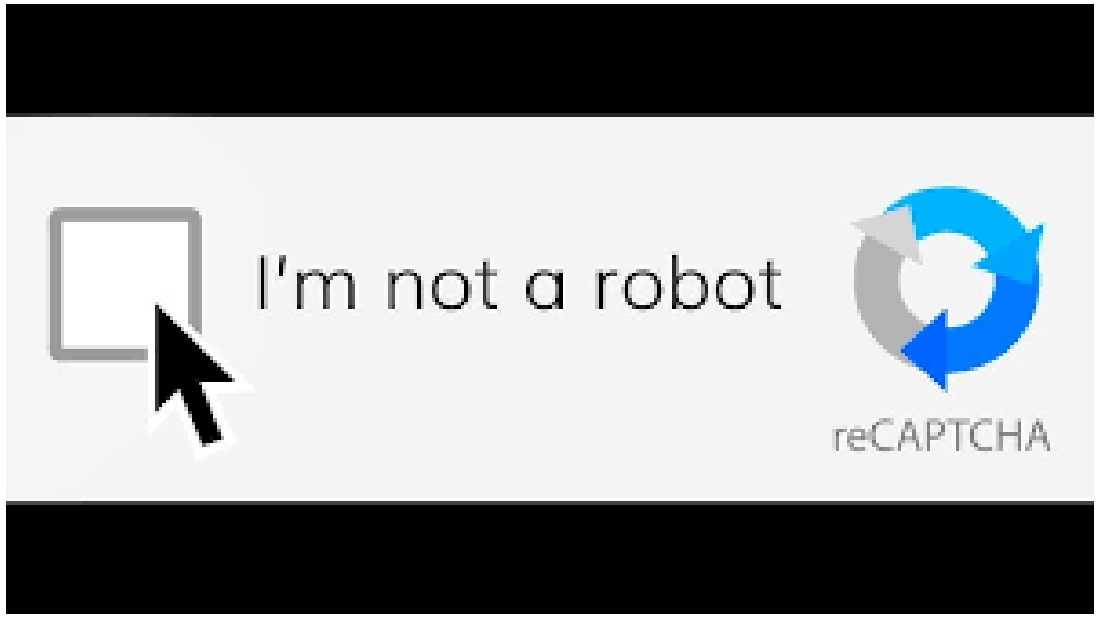
Checking In

- So far we've looked at the questions, "What is Cybersecurity?" "What is the weakest link in Cybersecurity?" and "How Do Spies Really Operate?"
- Since our last meeting, you have taken the first quiz.
- What questions do you have about the questions on the quiz or the focus of the quiz?


WHO ARE YOU
NOT TO BE TAKEN AWAY
KEEP
NOTICE
ELECTRICAL AREA
CLEAR

How Do You Prove Who You Are?

1. Something only you **know** (password)
2. Something only you **are** (biometrics)
3. Something only you **have** (phone for SMS, app, digital certificate)



https://medium.datadriveninvestor.com/why-do-i-need-to-prove-im-not-a-robot-ebc0809a4afd

Data Breach Data

1. 68% of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error.
2. The global average cost of data breach in 2024 is $4.88 million.
3. Most breaches linked to cyberattacks.
4. While organizations are moving quickly ahead with gen AI, only 24% of gen AI initiatives are secured.

https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c

https://medium.datadriveninvestor.com/why-do-i-need-to-prove-im-not-a-robo[illegible]9809-a4afd

security.org

Home Security | Smart Home | Digital Security | About Us

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

ENTER PASSWORD

https://www.security.org/how-secure-is-my-password/

Entries are 100% secure and not stored in any way or shared with anyone. Period.

AS SEEN ON

Inc. | The New York Times | THE VERGE | Entrepreneur | nerdwallet | The Guardian

Passwords are the bloodline of data and online security, but our research on the password habits in the U.S. shows that less than half of Americans feel confident that their password is secure. Is your password secure? We built this password checker tool to help you find

Home Notify me Domain search Who's been pwned Passwords API About Donate

https://haveibeenpwned.com/Passwords

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

password pwned?

Using Have I Been Pwned is subject to the terms of use

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

What is Identity and Access Management?

https://www.kiteworks.com/risk-compliance-glossary/identity-access-management/

Identity and Access Management

Identification:

- Username
- Certificate
- Token
- SSH Key
- Smart Card
  - Encryption is key

Authentication

- Factors
- Methods
- Protocols

Authorization

- Account Policies
- Account Controls
- Account Models

Authentication Factors

Knowledge – password or pin

Possession – smart card, phone

Inherence – biometrics

Location – GPS location

Behavior – action of user, finger on screen

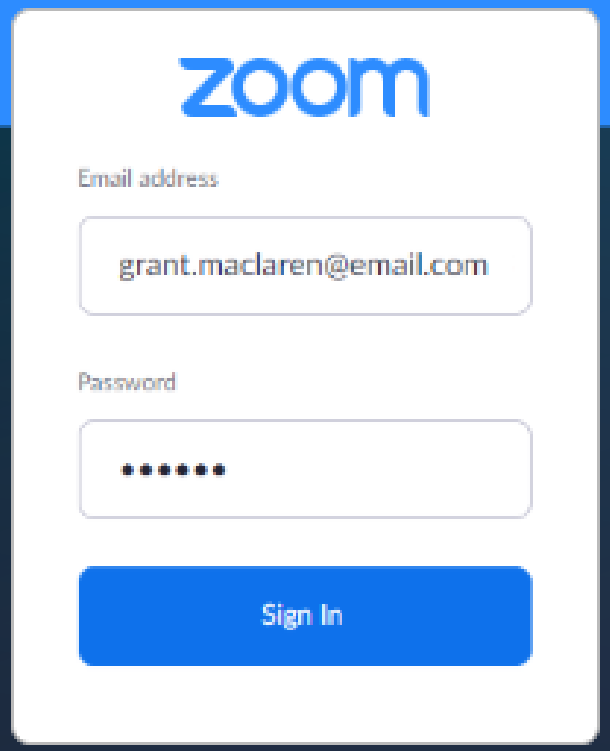
ttps://www.onelogin.com/blog/advanced-authentication-the-way-forward

Authentication Methods

Single-factor (SFA)
Two-factor (2FA)
Multifactor (MFA)

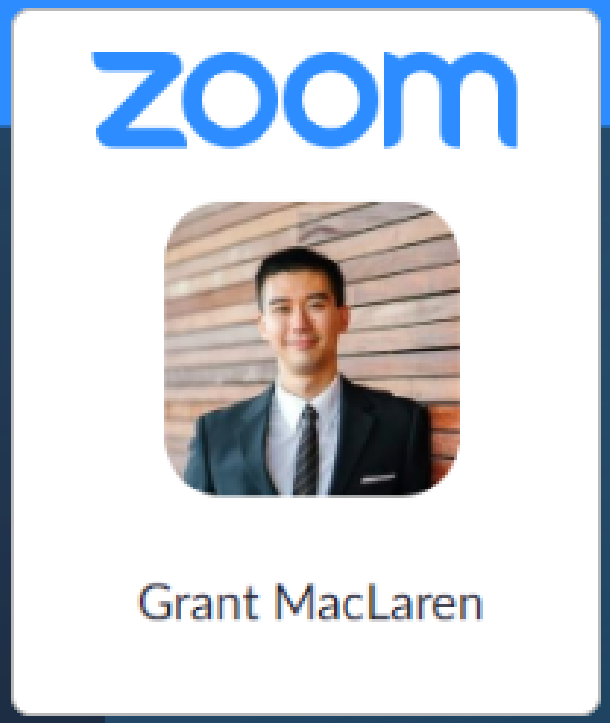
ttps://www.onelogin.com/blog/advanced-authentication-the-way-forward

Zoom sign-in

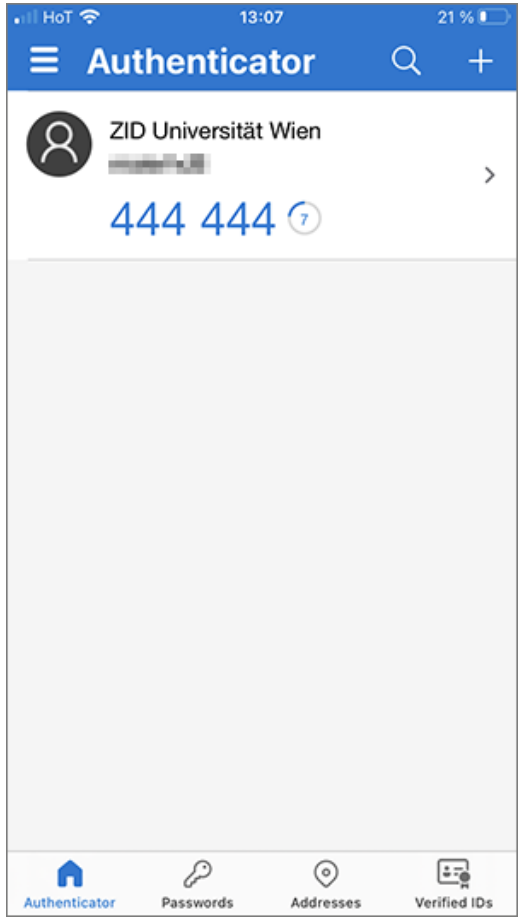


Enter code from 2FA app or text message

Zoom web portal, desktop client, mobile app, or Zoom Room



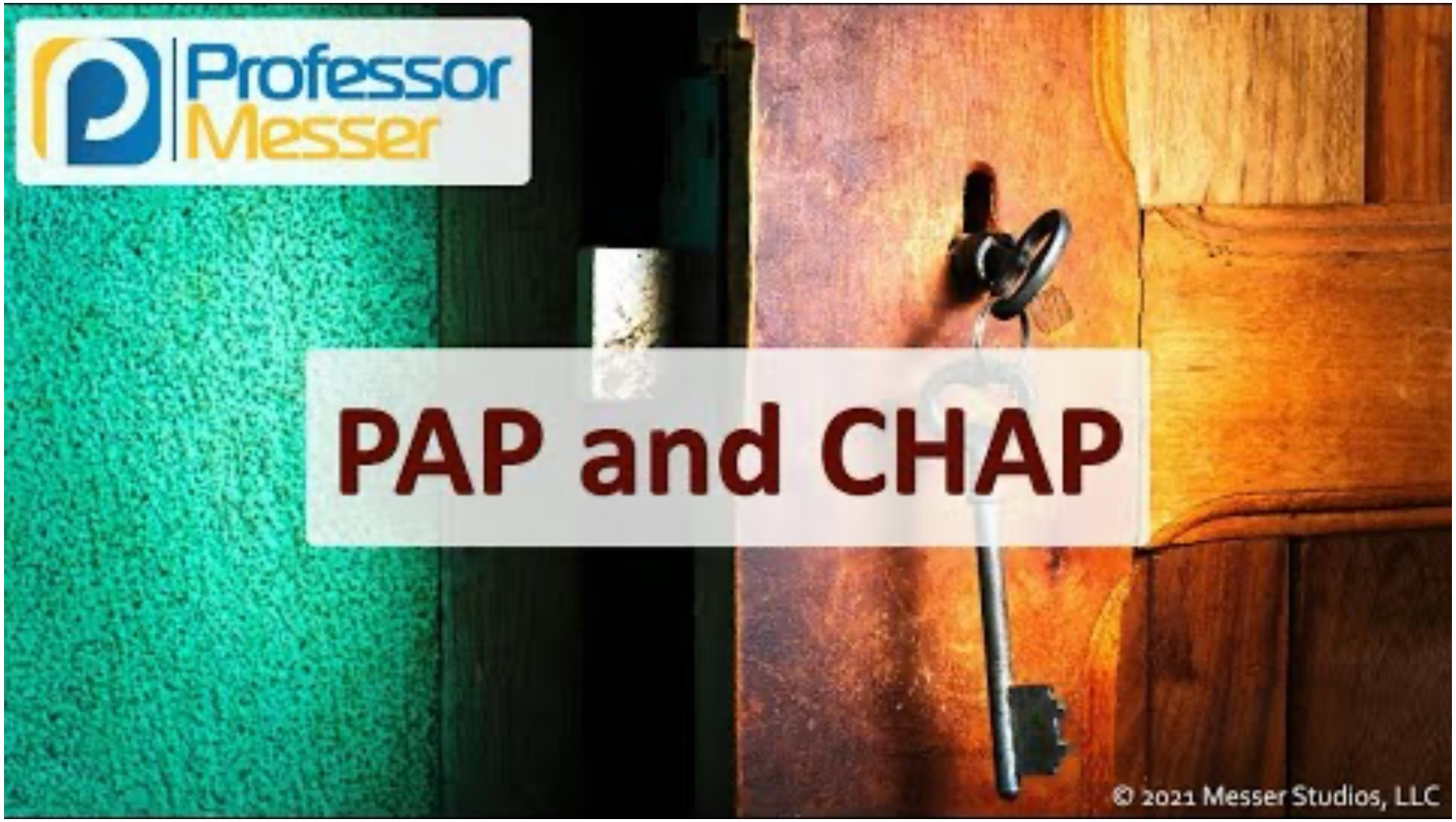
One-Time Password



1. Password Authentication Protocol
2. Challenge Handshake Authentication Protocol

Authentication Protocols

https://adaptive.live/blog/authentication-protocols-types-and-uses

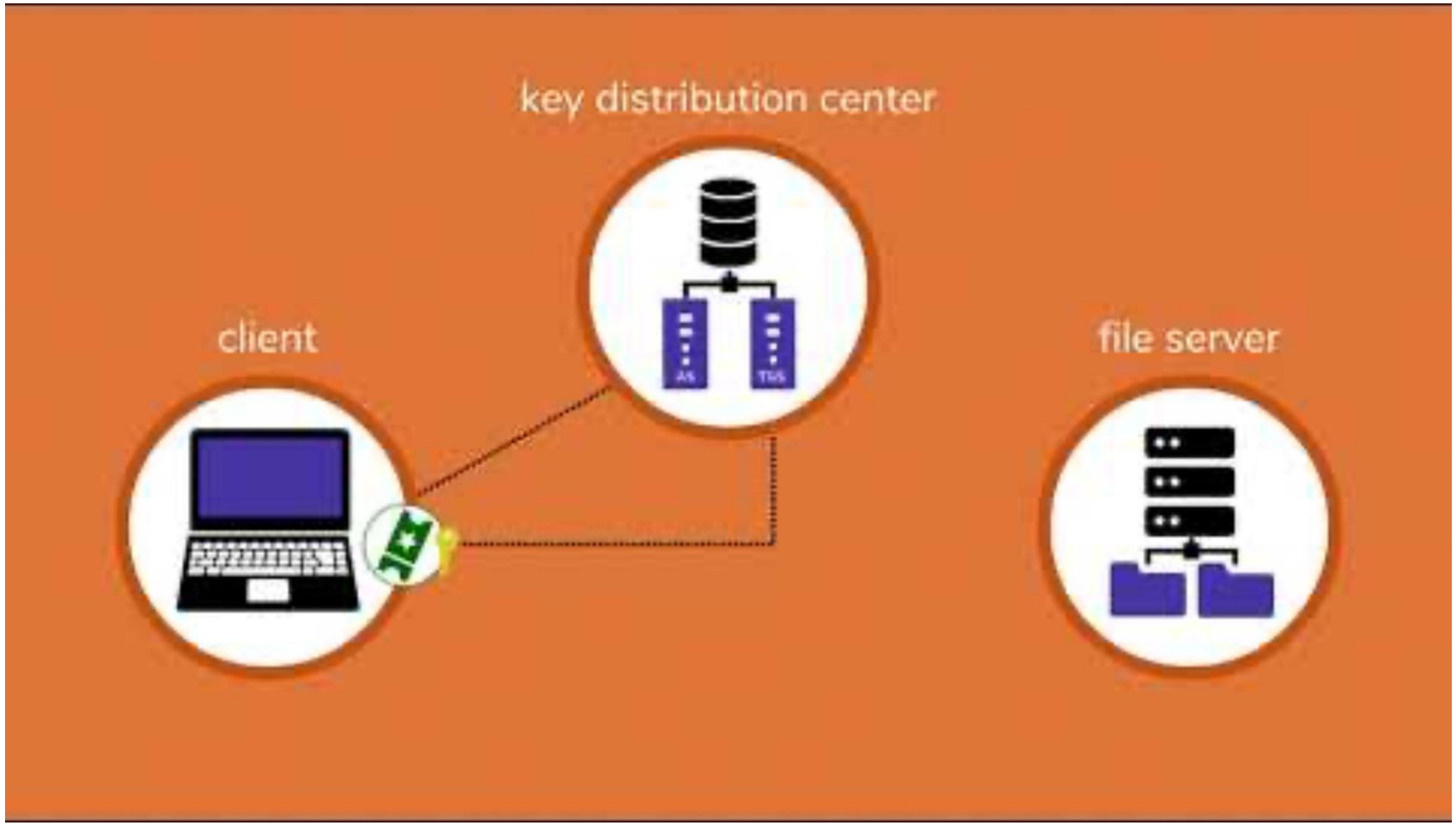


https://www.youtube.com/watch?v=y04xMlq7FXU&t=187s

1. Password Authentication Protocol
2. Challenge Handshake Authentication Protocol
3. Kerberos

Authentication Protocols

https://adaptive.live/blog/authentication-protocols-types-and-uses



Kerebos Explained

https://www.youtube.com/watch?v=1yWW7VQUX0A

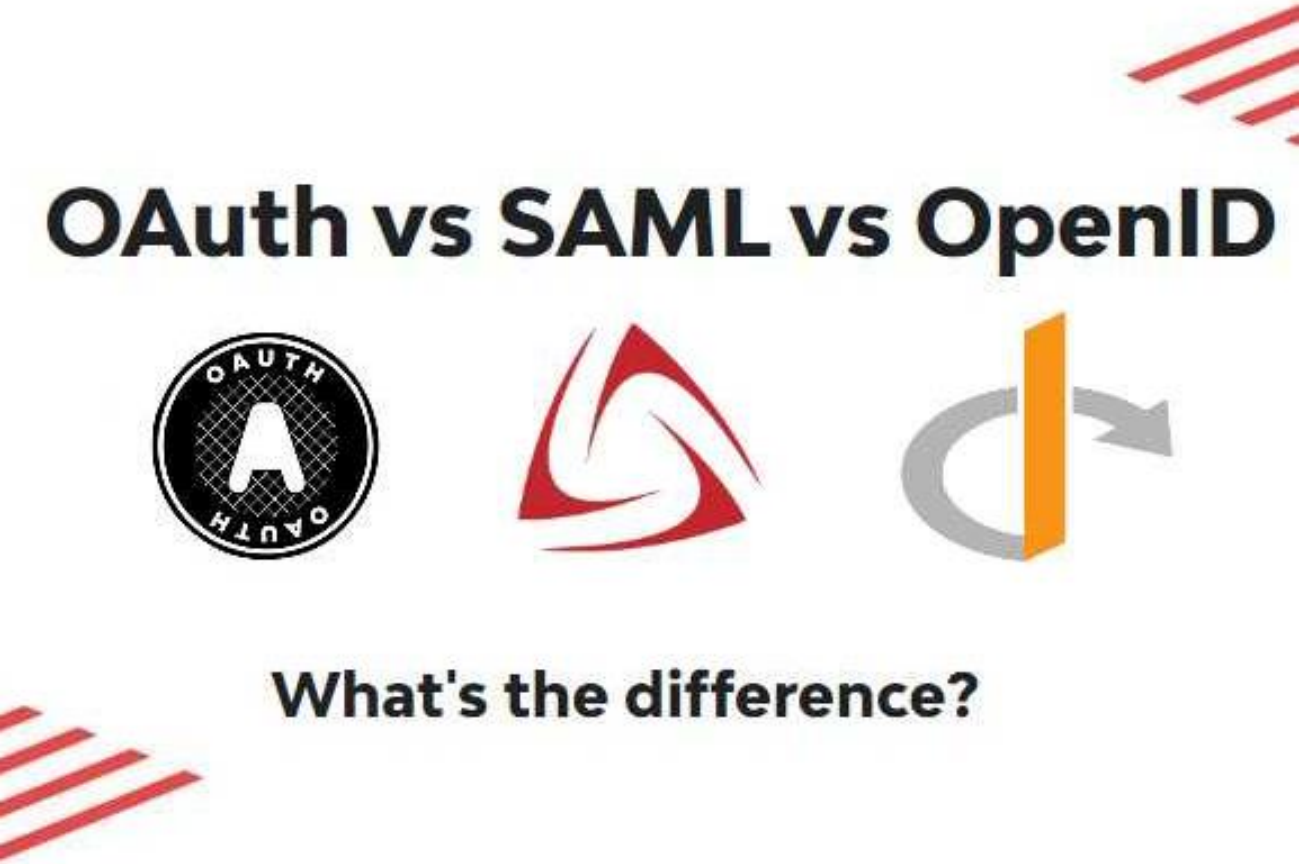
1. Password Authentication Protocol
2. Challenge Handshake Authentication Protocol
3. Kerberos
4. Extensible Authentication Protocol
5. RADIUS

Authentication Protocols

https://adaptive.live/blog/authentication-protocols-types-and-uses

RADIUS - *Remote Authentication Dial-In User Service (RADIUS)* is a networking protocol for centralized authentication, authorization, and accounting (AAA) services. The RADIUS protocol combines authentication and authorization services.

https://www.youtube.com/watch?v=oTSF4SuzOa4



SAML – (Security Assertion Markup Language) provides single sign-on (SSO) for web-based applications and is commonly used by web portals.

OpenID enables a user to log into multiple websites without the need to have login credentials for each website. (e.g., Using Google to sign in to different websites; but single point of failure.)

OAuth enables a user to grant a client (a website or an application) access to the user's information at other websites without sharing the user's credentials with a client. (e.g., upload picture on Google photo to social media; uses tokens).

OpenID is about logging you in, while OAuth is all about letting apps in.

https://www.wallarm.com/what/how-oauth-differs-from-saml-and-openid-learn-it-all

https://youtu.be/t2JFcHeQ3yg?si=ewio8EGSFBwO5ScG

Account Policies, Controls, and Maintenance

- What is an account policy?
  - Defines how computer account is created, used, maintained…
  - Includes password policies.
- What is an account control?
  - Controlling an account based on physical characterizes of a device such as IP address, location, boundary.
- What is Account Maintenance?
  - An audit ensuring user has the correct access based on policy.
- Examples:
  - MAC (mandatory) – sysadm sets rules user can't override
  - RBAC (role-based)
  - ABAC (attribute-based)
  - RBAC (rule-based)
  - DAC (discretionary)

https://www.youtube.com/watch?v=XQ8GDSUUvPY

https://publicrelationssydney.com.au/5-tips-for-better-public-speaking/

Prepare Media Article and Presentation

- Relevance to class topic (20%):
- Understanding of the issue (30%):
- Clear and organized summary (30%)
- Engagement with class (20%):
- IMPORTANT: Upload your article before the next class and provide a few sentences to answer each of the first three questions.