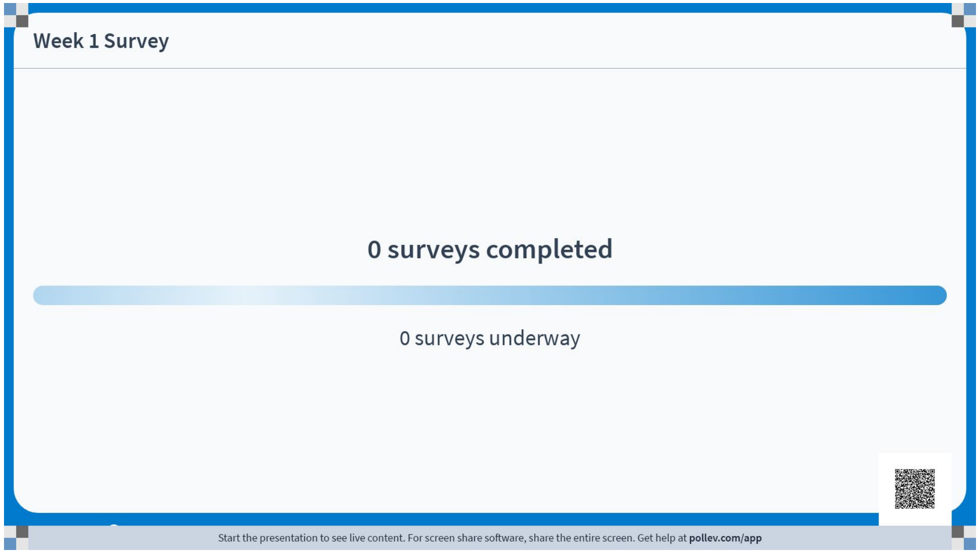
CSE 523S: Systems Security

Computer & Network Systems Security

Fall 2024
Prof. Patrick Crowley

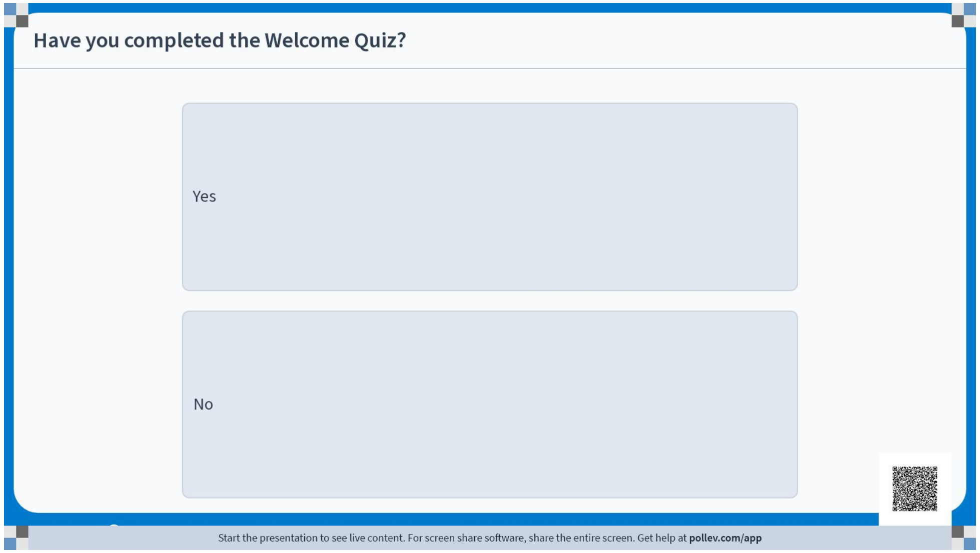


Week 1 Survey

0 surveys completed

0 surveys underway

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

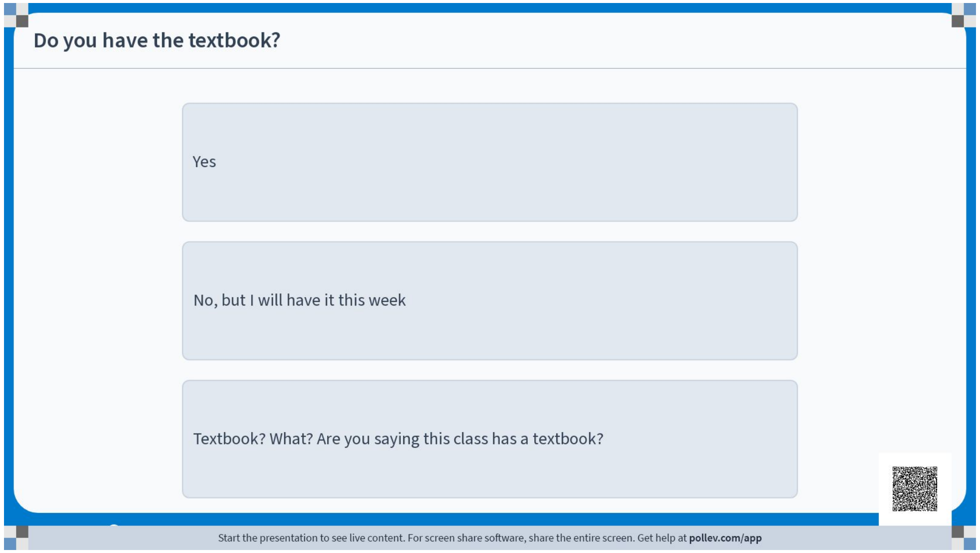


Have you completed the Welcome Quiz?

Yes

No

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**



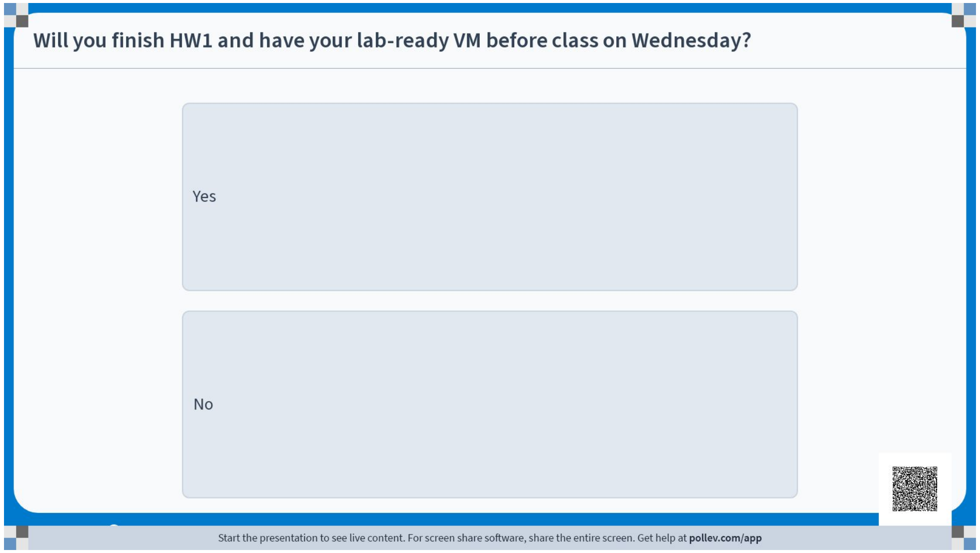
Do you have the textbook?

Yes

No, but I will have it this week

Textbook? What? Are you saying this class has a textbook?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

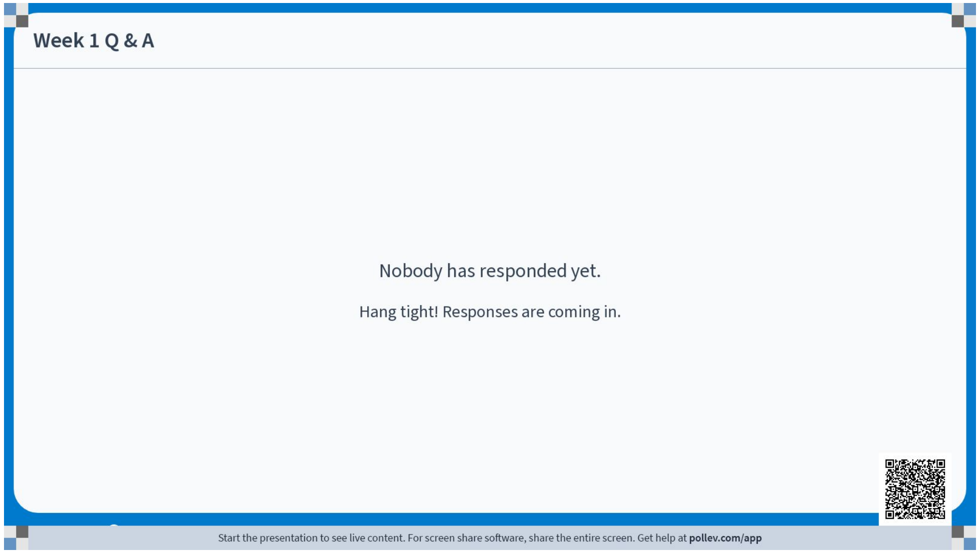


Will you finish HW1 and have your lab-ready VM before class on Wednesday?

Yes

No

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**



Week 1 Q & A

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Lab, Wednesday Sep 4

- In-person attendance is optional; you can choose to work remotely
  - Piazza “lab_getting_to_know_our_systems” will be used for questions
  - A zoom Q/A session will be available for you to join
- You can work with a partner for Lab 1
  - Gradescope will allow two students to submit a single lab report
- Some students have no laptops, and must work from home
  - So, I am likely to continue supporting remote labs

Virtual Machines

- What is VM?
  - a virtual machine is an emulation of a computer system.
- Why a VM? Why not a WashU lab?
  - It is always recommended to use VMs when doing security-related work.
  - Many of the studios and HW require Superuser privileges. Hard to get in a shared lab setup such as Urbauer labs.
- Is this course for beginners? Are we gonna get in touch with many hard core things?
  - If you have not take a computer systems organization class, this will be a difficult course for you but with effort you can succeed
  - The course was designed for students with no security experience.
  - Some of the exploits we'll play with are harder than others

SECURITY PRINCIPLES

Three Natural Questions

- Does it work?
- What will it cost?
- Is it secure?
- Question: are these 3 questions similar in nature?

Does it work? & What will it Cost?

- Does it work?
  - Does our system meet the functional requirements?
  - A lot of the field focuses on “correctness”.

- What will it cost?
  - Time?
  - Money?

- What about “is it secure”?

What does “Is it secure?” Mean?

1. Can anyone else access my data?
2. Can I control who uses the device?
3. Can anyone interfere with or prevent my usage of the device?
4. Can someone spy on my usage of the device?
5. Can someone delete or corrupt my data?
6. Can anyone see the data I send or receive on a network?

“1. Can anyone else access my data?”

- An easy source of trouble: the word “anyone”

- Suppose some are authorized and others are not

- Let’s try to be precise and systematic in answering this question

“1. Can anyone else access my data?”

- Does the device have authenticated users?
  - Are data access control mechanisms in place?
  - Is it a multi-user device?
  - If users sign-in, how do they do so?
  - Is it possible for someone to trick the system into accepting a false user identity?

- Can unauthorized users gain access?
  - Has the device been determined to be hack-proof, and impervious to unauthorized access through technical means?

“1. Can anyone else access my data?”

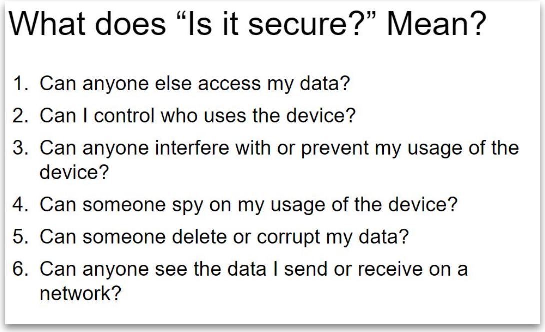
- Can authorized users delegate access to their data?
  - If a user can grant data access to another user, does the original user have any control over who else might get access?
- Is there an administrative user account that can create and modify user accounts?
  - If so, then whoever controls the administrative account can control access to data.
- Can the system be reset to factory defaults without destroying data?
  - Some systems provide means to reset a system following a lost account credential that keeps the original data intact.

“1. Can anyone else access my data?”

- Is the data archived on a backup service or device?
  - If so, how is access to that data managed?

- Do local laws require a back-door for access by government authorities?
  - If so, can a user verify either that such an access request is legitimate, or whether such accesses have taken place?

Have we reached the bottom?



What does “Is it secure?” Mean?

1. Can anyone else access my data?
2. Can I control who uses the device?
3. Can anyone interfere with or prevent my usage of the device?
4. Can someone spy on my usage of the device?
5. Can someone delete or corrupt my data?
6. Can anyone see the data I send or receive on a network?

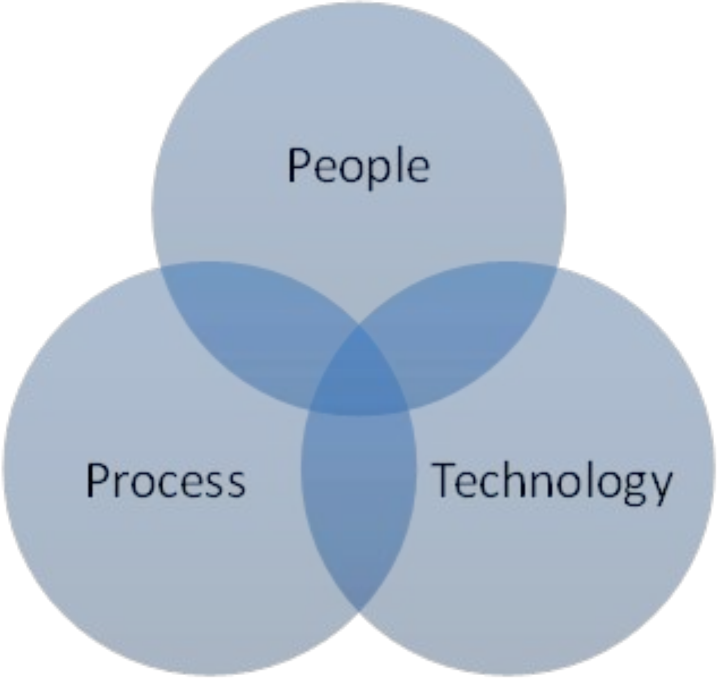
- That was question 1 of 6...

- It seems clear that “Is the system secure?” is a different kind of question

- **We need to develop a perspective to manage the seemingly boundless complexity**

People, Process, Technology

- Security has non-technical aspects
- Our systems are vulnerable from many angles.
- To answer "Is it secure?" we need to address each



Security is a consequence of people, process and technology.

People

Security measure: Provide training periodically to ensure that users have an understanding of security risks and are aware of common pitfalls

Attack: Fool users into divulging their access credentials by sending convincing email messages that appear to be legitimate requests. Phishing attacks.

Process

Security measure: Design rules and procedures for users and systems that are intended to improve security, and increase the effort required on the part of the attacker. e.g. a policy may dictate that a user account be locked out after 5 failed login attempts. Remote attackers cannot endlessly attempt different passwords.

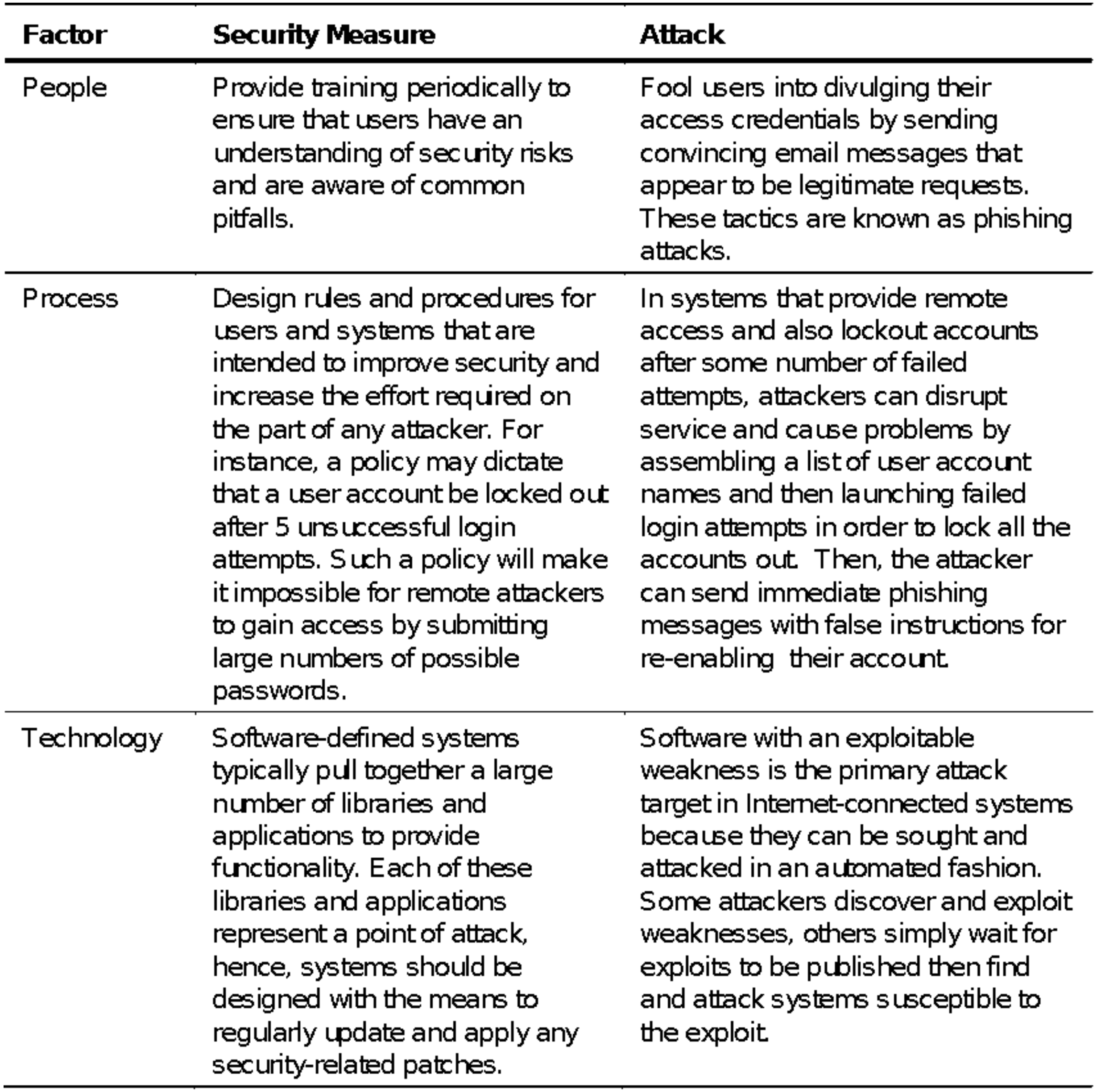
Attack: Attacker can still disrupt service by attempting multiple logins and forcing accounts to be locked. Then send phishing email with “instructions” for unlocking account.

Technology

Security Measure: Software systems use a lot of libraries and applications to provide functionality.

Attack: Software with an exploitable weakness is the prime target for attackers. Attackers find vulnerabilities, exploits get published and attacks spread.

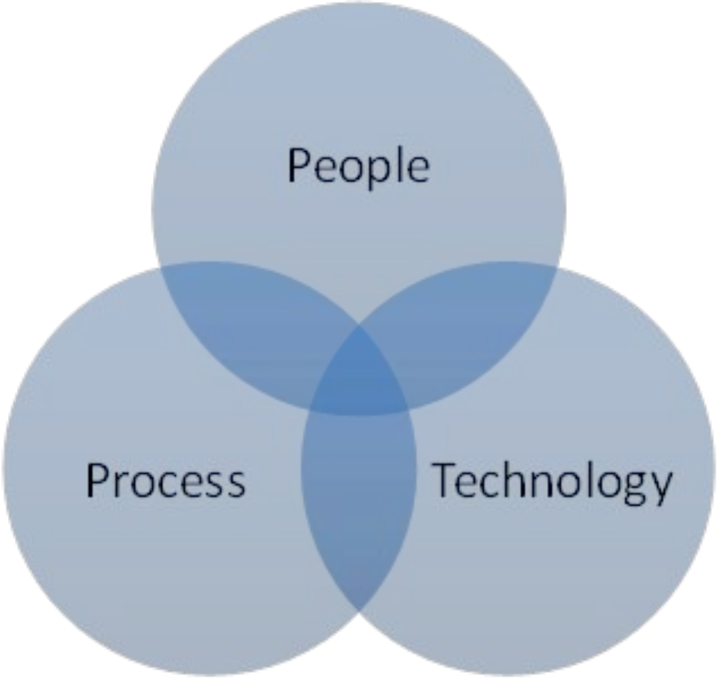
Summary



Factor	Security Measure	Attack
People	Provide training periodically to ensure that users have an understanding of security risks and are aware of common pitfalls.	Fool users into divulging their access credentials by sending convincing email messages that appear to be legitimate requests. These tactics are known as phishing attacks.
Process	Design rules and procedures for users and systems that are intended to improve security and increase the effort required on the part of any attacker. For instance, a policy may dictate that a user account be locked out after 5 unsuccessful login attempts. Such a policy will make it impossible for remote attackers to gain access by submitting large numbers of possible passwords.	In systems that provide remote access and also lockout accounts after some number of failed attempts, attackers can disrupt service and cause problems by assembling a list of user account names and then launching failed login attempts in order to lock all the accounts out. Then, the attacker can send immediate phishing messages with false instructions for re-enabling their account.
Technology	Software-defined systems typically pull together a large number of libraries and applications to provide functionality. Each of these libraries and applications represent a point of attack, hence, systems should be designed with the means to regularly update and apply any security-related patches.	Software with an exploitable weakness is the primary attack target in Internet-connected systems because they can be sought and attacked in an automated fashion. Some attackers discover and exploit weaknesses, others simply wait for exploits to be published then find and attack systems susceptible to the exploit.

People, Process, Technology

- Security has non-technical aspects
- Our systems are vulnerable from many angles.
- To answer “Is it secure?” we need to address each



Security is a consequence of people, process and technology.

Sleight of hand?

- Many of these issues seem like apples and oranges.
  - Do they all fit what you thought of as security?
- Unauthorized access is clearly a security violation
- What about obstructing authorized access?
  - Is it really the same thing?
- How many issues might we dream up?
- What about time?
  - Someone has access, do they keep it forever?
  - Can they make copies of data and keep them?

Information Security (InfoSec)

- As a field, InfoSec deals with these broader issues

- InfoSec encompasses computer and network systems security

- “CIA” triad is one contribution of the field

Confidentiality, Integrity & Availability

- Confidentiality
  - Is it secret?
  - Is it kept secret even while being transmitted to an authorized user?
  - Is it important to keep even the existence of the data secret?
  - Is the list of authorized users kept secret?

- Integrity
- Availability

Confidentiality, Integrity & Availability

- Confidentiality
- Integrity
  - Has it been tampered with?
    - In storage?
    - While being transmitted to authorized user?
- Availability

Confidentiality, Integrity & Availability

- Confidentiality

- Integrity

- Availability
  - Is it accessible?
  - Is time to access it a factor?
    - What if an attacker just makes it slow and painful for an authorized user to get their data?

SECURITY BUILDING BLOCKS

Computer Networks

Security Concepts & Building Blocks

- Encryption & Cryptography
  - What most people think of as Security.

- Authentication
  - Identifying who or what we are talking to?

Encryption & Cryptography

- Single-key crypto (aka symmetric crypto)
  - Encrypted data (i.e., ciphertext) is indistinguishable from random data
  - Use a “shared secret” or “key” to encrypt/decrypt
- Public-key crypto (aka asymmetric crypto)
  - I have a pair of keys, public and private
  - I give you my public key
  - To send me a private message
    - You use the public key to encrypt
    - I use my private key to decrypt
  - To send you a digitally signed message (msg)
    - I use my private key and the msg to make signature
    - You use the public key & msg to check signature

How do we share and manage keys?

- How do I get your public key?
  - Web, email, USB stick?
  - Automatically in software you use?

- How do I get a stranger’s public key?

- What problems arise?

Certificates

- We place our trust in “Certificate Authorities”, or CAs
- A certificate (e.g., the X.509 format) contains
  - a public key,
  - the name of the owner of the public key,
  - the name of the attesting CA,
  - and the signature of the CA.
- Which CAs can we trust?
  - Up to Microsoft, Google, Apple, Firefox, etc.

VeriSign, March 2001

- Issued two Microsoft root/CA certs to a fraudster

- Oops!

- All MSFT up-to-date software “revokes” these certificates
  - No public admissions of fraud

- MSFT also lost a signing key for email in 2023
  - https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

Authentication:
Matching Identity with Credentials

- Can be based on
  - Something you know: password
  - Something you have: a key
  - Something you are: fingerprint

Two-Factor Authentication

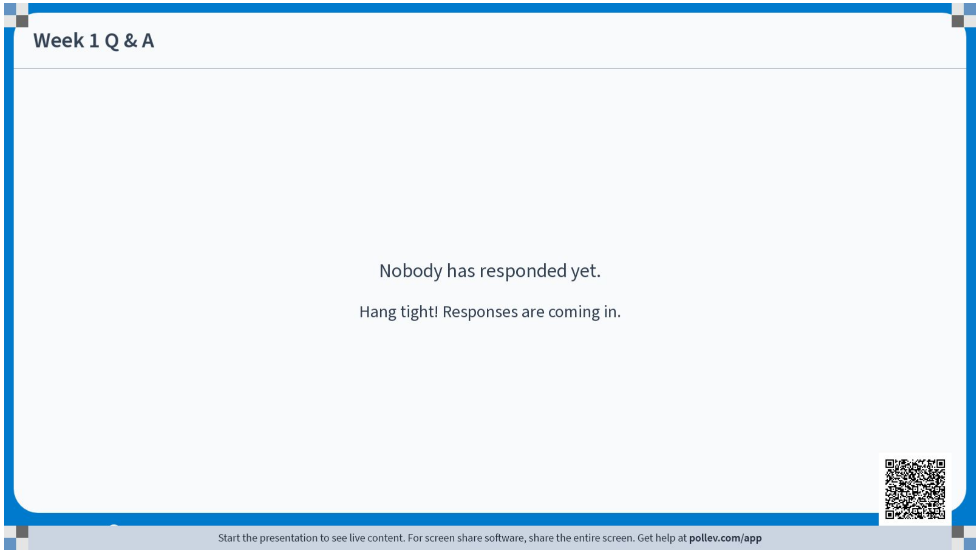
- Biometrics were unreliable prior to smartphones

- A best practice is to rely on two methods to authenticate
  - Maybe not every time, but periodically

- Does anyone here use passkeys?
  - Passwords are being phased out!

- Check out:

  https://safety.google/authentication/passkey/



Week 1 Q & A

Nobody has responded yet.

Hang tight! Responses are coming in.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**