Authentication

- **Video:** Best practices for authentication
  6 min
- **Video:** Multifactor Authentication
  5 min
- **Video:** Multifactor Authentication Options
  5 min
- **Reading:** Physical Privacy and Security Components
  10 min
- **Reading:** Supplemental Reading for Authentication
  10 min
- **Video:** Certificates, Part Two
  3 min
- **Video:** RADIUS
  1 min
- **Video:** Kerberos
  7 min
- **Video:** TACACS+
  1 min
- **Video:** Single Sign-On
  3 min
- **Practice Quiz:** Authentication
  13 questions
- **Video:** Rob: My path to IT
  1 min

Authorization

Accounting

Graded Assessments

Physical Privacy and Security Components

Physical privacy and security

In this reading, you will learn more about physical privacy and security, including biometric and Near Field Communication authentication. You will also revisit the “confidentiality” aspect of the CIA Principle (Confidentiality, Integrity, Availability), which was introduced previously in this certificate program.

CIA Principle: Confidentiality

Preventing unauthorized access to an organization’s data and networks is imperative in protecting a company’s information systems. Regulations, standards, and laws may also require that certain information be kept confidential, like health records. Failing to ensure the confidentiality of specific types of data could result in damage to reputation, loss of customers, liability lawsuits, financial losses, penalty fines, criminal charges, and more. It is vital for IT Support specialists to take all measures possible to protect confidential information.

In a previous video, you learned about three types of authentication methods:

- **Something you know** - password or pin number
- **Something you have** - bank card, USB device, key fob, or OTP (one-time password)
- **Something you are** - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan

You will learn more about biometrics in this reading, along with two additional categories of authentication methods:

- **Somewhere you are** - geofencing, GPS, Indoor Positioning Systems (IPS)
- **Something you do** - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Some authentication technologies inherently require two factors:

- **Somewhere you are + Something you have** - Near Field Communication (NFC) uses both proximity to an NFC scanner and a device like an NFC-enabled smartphone or an RFID chip on an employee ID or bank card.

Something you are: Biometrics

Biometric authentication occurs in two steps: enrollment and authentication. Enrollment happens when the user provides their biometric data for the first time through a hardware scanner. Specific features of that biometric data are extracted, encrypted, and stored, often in a database or on a personal mobile device. Authentication, as the second step, happens when a user presents their biometric data again to the scanner to gain access to the secured item. This new scan is compared against the original stored biometric data to authenticate the person’s identity.

Fingerprint scanning

In a previous video, you learned about fingerprint scanners as an authentication method for mobile devices. Fingerprint scanners use small capacitive cells that are engineered to detect fingerprint ridges. Dirt and moisture can interfere with the scanner’s ability to do its job. As an IT Support specialist, you may need to replace damaged fingerprint scanners on customer devices.

Facial recognition

Many smartphone models provide the hardware and software to use facial recognition as a biometric authentication method. This often requires two cameras. The first camera uses normal color photography. The second camera uses infrared technology to measure depth and ensure your face is 3-dimensional. This prevents hackers from using photographs of the authorized users to unlock mobile devices.

Iris and Retinal scanning

Iris scanning is not a secure form of biometric authentication because a photograph of the user’s iris can be used to gain access. In contrast, retinal scanning is one of the more secure forms of biometric authentication. It is exceedingly difficult to impersonate the retinal features of a person’s eye. Our retinas have unique and complex patterns in how our blood vessels are arranged. These fingerprint-like patterns can be scanned by shining a beam of infrared light into the eye. Note that eye injuries and medical problems with the eyes can change retinal blood vessel patterns and cause users to be denied access to their devices. Although retinal scanning is secure, the technology can be expensive and difficult to implement.

Somewhere you are: Geolocation

The geographical location of a user can serve as one part of a multi-factor authentication policy or to deny access to users based on their locations. Geolocation services can use GPS, IP ranges, WiFi access points, cell phone towers, and/or Bluetooth beacons to estimate a mobile user’s location.

Geofencing

Geofencing is used to authenticate users who are physically within a certain radius of a specific location. For example, if you order food using McDonald’s smartphone app, the restaurant will not process your order until your smartphone is within a certain radius of the restaurant. You cannot send someone else to pick up your order either, as that person cannot authenticate without your smartphone being within the geofencing radius.

Global Positioning Systems (GPS)

Global Positioning Systems (GPS) use satellites orbiting Earth to map a device's longitude and latitude. The mobile device needs to be equipped with GPS sensors and have GPS services enabled to take advantage of GPS-based authentication technologies. GPS could be used to authenticate a device based on the physical location of the user. Insurance companies use GPS data to verify the authenticity of disaster claims filed through mobile apps.

Indoor Positioning Systems (IPS)

Indoor Positioning Systems (IPS) triangulate a device’s location by using WiFi access points, cell phone towers, and/or Bluetooth beacons. Users must grant permission to apps to use this technology. IPS locations might be used to deny network access when the user has entered a restricted area.

Near-field communication (NFC) and scanners

You may have interacted with a near-field communication (NFC) scanner by using contactless payments with a credit card, bank card, or smartphone. NFC technology can also be used for authentication and access to physical buildings through school or employment ID cards.

NFC transmits on the same frequency as high frequency RFID (13.56 MHz) and has a short distance range of 10 centimeters. The short distance range provides some protection from hackers attempting to intercept the connection to obtain your credit card information. However, NFC is not fully secure. An innocuous looking NFC scanner sitting next to an NFC-enabled payment device could record all NFC transactions that occur within the 10 cm of the device in a “man in the middle” security breach.

Something you do: Gestures and Behaviors

You may already be familiar with using gestures like swipe patterns to unlock a smartphone. Another gesture-based authentication method is the Picture Password, which requires the user to touch specific, secret points on a photograph to unlock the device.

Patterns of people’s behaviors can be used to authenticate identity. For example, an organization might keep track of computer system login and logout times of employees. These patterns could be monitored for any unusual changes in employee behavior, which may indicate that the “employee” is instead an imposter.

Turing tests are used to determine if an unknown entity is a human or a machine. You have probably responded to a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to authenticate that you are indeed a human and not a bot. This is accomplished by asking the user to identify items within a set of photographs. Photos are used for this test because images are more difficult for bots to identify than text.

Key takeaways

There are a variety of MFA protocols that can be implemented to protect the confidentiality, privacy, and security of data and networks. The 5 types of authentication can be categorized as:

1. Something you know - password or pin number
2. Something you have - bank card, USB device, key fob, or OTP (one-time password)
3. Something you are - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan
4. Somewhere you are - geolocation, geofencing, GPS, Indoor Positioning Systems (IPS), NFC scanning
5. Something you do - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Resources for more information

For more information about methods of authentication to protect data, please visit:

- Geolocation—The Risk and Benefits of a Trending Technology - Discusses impacts, benefits, risks, risk mitigation, security, governance, and privacy concerns of geolocation technologies.
- Understanding The 5 Factors Of Multi-Factor Authentication - Overview of the 5 Factors: Something you know, Something you have, Something you are, Somewhere you are, and Something you do.
- Homeland Security Biometrics - History and use cases of biometrics for maximum security and identification of criminals in the United States Departments of Homeland Security, Defense, Justice, and Commerce, as well as the National Institute of Standards and Technology.
- A Review on Authentication Methods - Informative peer-reviewed journal article on authentication methods.
- Modern Authentication Methods: A Comprehensive Survey - Peer-reviewed journal article with expanded coverage of two-factor and multi-factor authentication topics. Provides comprehensive comparisons of advantages and disadvantages of each authentication method.
- What is the Difference Between NFC and RFID? - A comparison of NFC and RFID technologies.
- Fingerprint Reader Replacement Guide - Provides photos of internal fingerprint scanner hardware parts, as well as instructions on how to replace a fingerprint scanner on a laptop.

Mark as completed

Like **Dislike** **Report an issue**