07- Implementing Authentication Controls

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

7.1- Summarize Authentication Design Concepts

7.2- Implement Knowledge-Based Authentication

7.3- Summarize Biometrics Authentication Concepts

Labs

Lab 8: Auditing Passwords with a Password Cracking Utility

Lab 9: Managing Centralized Authentication

7.1- Summarize Authentication Design Concepts

7.2- Implement Knowledge-Based Authentication

7.3- Summarize Biometrics Authentication Concepts

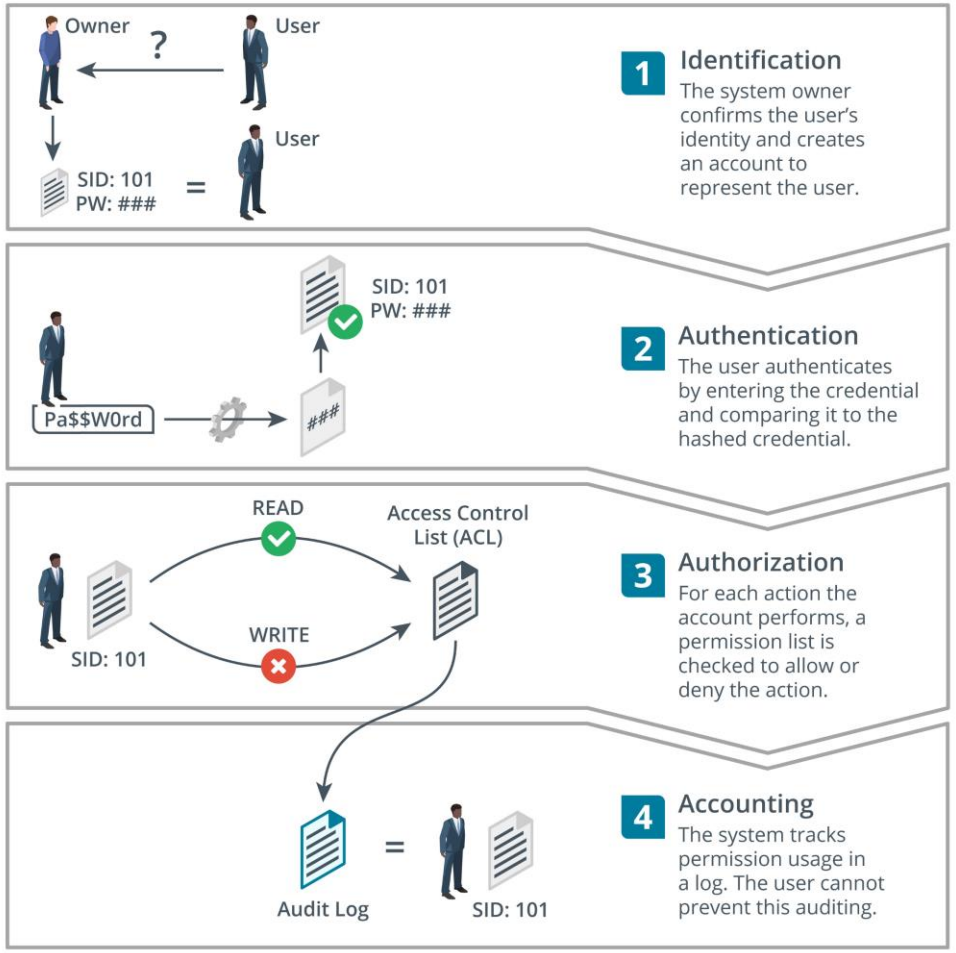
IDENTITY AND ACCESS MANAGEMENT

- An access control system is the set of technical controls that govern how **subjects** may interact with **objects**.
- **Subjects** in this sense are users, devices, or software processes, or anything else that can request and be granted access to a resource.
- **Objects** are the resources; these could be networks, servers, databases, files, and so on.

IDENTITY AND ACCESS MANAGEMENT (cont.)

- An identity and access management (IAM) system is usually described in terms of four main processes:
  - ✓ Identification—creating an account or ID that uniquely represents the user, device, or process on the network.
  - ✓ Authentication—proving that a subject is who or what it claims to be when it attempts to access the resource.
  - ✓ Authorization—determining what rights subjects should have on each resource, and enforcing those rights.
  - ✓ Accounting—tracking authorized usage of a resource or use of rights by a subject and alerting when unauthorized use is detected or attempted.

IDENTITY AND ACCESS MANAGEMENT (cont.)



AUTHENTICATION FACTORS

- Assuming that an account has been created securely (the identity of the account holder has been verified), authentication verifies that only the account holder is able to use the account, and that the system may only be used by account holders.
- Authentication is performed when the account holder supplies the appropriate credentials (or authenticators) to the system.
- These are compared to the credentials stored on the system.
- If they match, the account is authenticated.
- There are many different technologies for defining credentials and can be categorized as factors.

AUTHENTICATION FACTORS (cont.)

- Something You Know Authentication
  - ✓ The typical knowledge factor is the logon, composed of a username and a password.
  - ✓ The username is typically not a secret (although it should not be published openly), but the password must be known only to the account holder.
  - ✓ A personal identification number (PIN) is also something you know, although long PIN codes are hard to remember, and short codes are too vulnerable for most authentication systems.
  - ✓ Swipe patterns are often used for authentication to touch-based devices.

AUTHENTICATION FACTORS (cont.)

- Something You Have Authentication
  - ✓ An ownership factor means that the account holder possesses something that no one else does, such as a smart card, fob, or wristband programmed with a unique identity certificate or account number.
  - ✓ These ownership factors can be described as hard tokens.
  - ✓ A device such as a smartphone can also be used to receive a uniquely generated access code as a soft token.
  - ✓ Unlike a password, these tokens are valid for only one use, typically within a brief time window.

AUTHENTICATION FACTORS (cont.)

- Something You Are/Do Authentication
  - ✓ A biometric factor uses either physiological identifiers, such as a fingerprint, or behavioral identifiers, such as the way someone moves (gait).
  - ✓ The identifiers are scanned and recorded as a template.
  - ✓ When the user authenticates, another scan is taken and compared to the template.

AUTHENTICATION DESIGN

- Authentication design refers to selecting a technology that meets requirements for confidentiality, integrity, and availability:
  - ✓ Confidentiality, in terms of authentication, is critical, because if account credentials are leaked, threat actors can impersonate the account holder and act on the system with whatever rights they have.
  - ✓ Integrity means that the authentication mechanism is reliable and not easy for threat actors to bypass or trick with counterfeit credentials.
  - ✓ Availability means that the time taken to authenticate does not impede workflows and is easy enough for users to operate.

MULTIFACTOR AUTHENTICATION

- An authentication technology is considered strong if it combines the use of more than one type of knowledge, ownership, and biometric factor, and is called multifactor authentication (MFA).
- Single-factor authentication can quite easily be compromised: a password could be written down or shared, a smart card could be lost or stolen, and a biometric system could be subject to high error rates or spoofing.
- Two-Factor Authentication (2FA) combines either an ownership-based **smart card** or **biometric identifier** with something you know, such as a **password** or **PIN**.

MULTIFACTOR AUTHENTICATION (cont.)

- Three-factor authentication combines all three technologies, or incorporates an additional attribute, such as location; for example, a **smart card** with integrated **fingerprint reader**.
- This means that to authenticate, the user must possess the **card**, the user's **fingerprint** must match the template stored on the card, and the user must input a **PIN** or **password**.

7.1- Summarize Authentication Design Concepts

7.2- Implement Knowledge-Based Authentication

7.3- Summarize Biometrics Authentication Concepts

LOCAL, NETWORK, AND REMOTE AUTHENTICATION

- One of the most important features of an operating system is the authentication provider, which is the software architecture and code that underpins the mechanism by which the user is authenticated before starting a shell.
- This is usually described as a login (Linux) or a logon or sign-in (Microsoft).
- Knowledge-based authentication, using a password or personal identification number **(PIN)**, is the default authentication provider for most operating systems.

LOCAL, NETWORK, AND REMOTE AUTHENTICATION (cont.)

- Knowledge-based authentication relies on cryptographic hashes.
- A plaintext password is not usually transmitted or stored in a credential database because of the risk of compromise.
- Instead, the password is stored as a cryptographic hash.
- When a user enters a password to log in, an authenticator converts what is typed into a hash and transmits that to an authority.
- The authority compares the submitted hash to the one in the database and authenticates the subject only if they match.

Windows Authentication

- Windows authentication involves a complex architecture of components (docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication), but the following three scenarios are typical:
  - ✓ Windows local sign-in—the Local Security Authority (LSA) compares the submitted credential to a hash stored in the Security Accounts Manager (SAM) database, which is part of the registry.
  - ✓ Windows network sign-in—the LSA can pass the credentials for authentication to a network service, The preferred system for network authentication is based on Kerberos, but legacy network applications might use NT LAN Manager (NTLM) authentication.
  - ✓ Remote sign-in—if the user's device is not connected to the local network, authentication can take place over some type of virtual private network (VPN) or web portal.

Linux Authentication

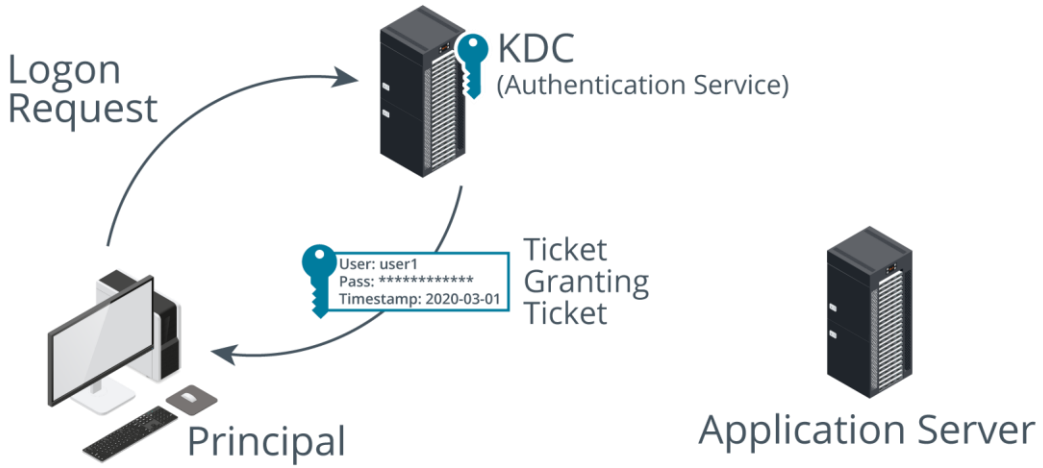
- In Linux, local user account names are stored in /etc/passwd.
- When a user logs in to a local interactive shell, the password is checked against a hash stored in /etc/shadow.
- Interactive login over a network is typically accomplished using **Secure Shell (SSH)**.
- With SSH, the user can be authenticated using cryptographic keys instead of a password.

Single Sign-On (SSO)

- A single sign-on (SSO) system allows the user to authenticate once to a local device and be authenticated to compatible application servers without having to enter credentials again.
- In Windows, SSO is provided by the Kerberos framework.

KERBEROS AUTHENTICATION

- Kerberos is a single sign-on network authentication and authorization protocol used on many networks, notably as implemented by Microsoft's Active Directory (AD) service.
- Kerberos was named after the three-headed guard dog of Hades (Cerberus) because it consists of three parts.



KERBEROS AUTHENTICATION (cont.)

- Clients request services from application servers, which both rely on an intermediary—a Key Distribution Center (KDC)—to vouch for their identity.
- There are two services that make up a KDC:
  - ✓The Authentication Service
  - ✓The Ticket Granting Service
- The KDC runs on port 88 using TCP or UDP.
- The Authentication Service is responsible for authenticating user logon requests.

KERBEROS AUTHENTICATION (cont.)

1. The client sends the authentication service (AS) a request for a Ticket Granting Ticket (TGT), This is composed by encrypting the date and time on the local computer with the user's password hash as the key.
2. The AS checks that the user account is present, that it can decode the request by matching the user's password hash with the one in the Active Directory database, and that the request has not expired, If the request is valid, the AS responds with the following data:
   - ✓ Ticket Granting Ticket (TGT)—this contains information about the client (name and IP address) plus a timestamp and validity period, This is encrypted using the KDC's secret key.
   - ✓ TGS session key for use in communications between the client and the Ticket Granting Service (TGS), This is encrypted using a hash of the user's password.

PAP, CHAP, AND MS-CHAP AUTHENTICATION

- Kerberos is designed to work over a trusted local network.
- Several authentication protocols have been developed to work with remote access protocols, where the connection is made over a serial link or virtual private network (VPN).

1. Password Authentication Protocol (PAP)

- ✓ The Password Authentication Protocol (PAP) is an unsophisticated authentication method developed as part of the Point-to-Point Protocol (PPP), used to transfer TCP/IP data over serial or dial-up connections.
- ✓ It is also used as the basic authentication mechanism in HTTP.
- ✓ It relies on clear text password exchange and is therefore obsolete for most purposes, except through an encrypted tunnel.

PAP, CHAP, AND MS-CHAP AUTHENTICATION (cont.)

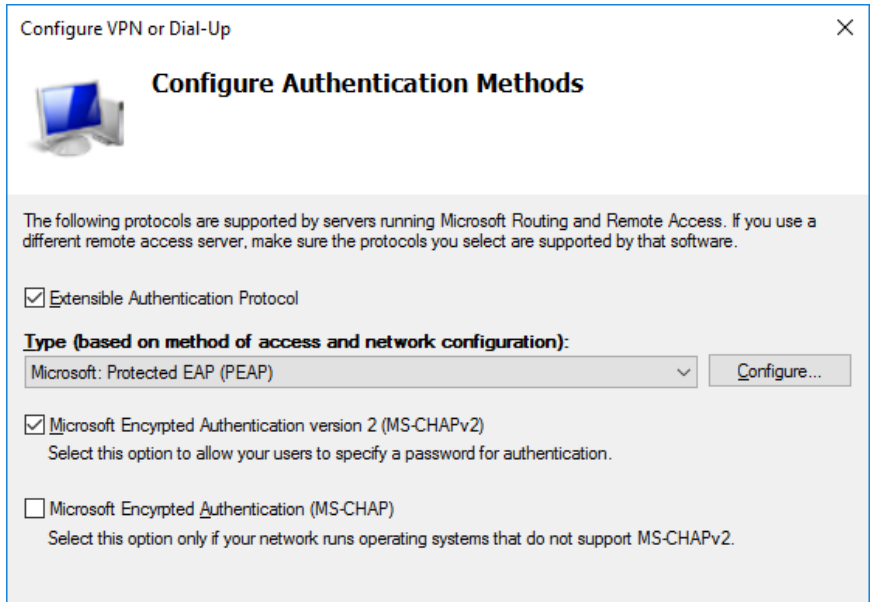
2. Challenge Handshake Authentication Protocol (CHAP)

- The Challenge Handshake Authentication Protocol (CHAP) was also developed as part of PPP as a means of authenticating users over a remote link.
- CHAP relies on an encrypted challenge in a system called a three-way handshake.
  - ✓ Challenge—the server challenges the client, sending a randomly generated challenge message.
  - ✓ Response—the client responds with a hash calculated from the server challenge message and client password (or other shared secret).
  - ✓ Verification—the server performs its own hash using the password hash stored for the client. If it matches the response, then access is granted; otherwise, the connection is dropped.
- The handshake is repeated with a different challenge message periodically during the connection (although transparent to the user), This guards against replay attacks, in which a previous session could be captured and reused to gain access.

PAP, CHAP, AND MS-CHAP AUTHENTICATION (cont.)

3. MS-CHAPv2

- ✓ Microsoft's implementation of CHAP.
- ✓ Because of the way it uses vulnerable NTLM hashes, MS-CHAP should not be deployed without the protection of a secure connection tunnel so that the credentials being passed are encrypted.



PASSWORD ATTACKS

- When a user chooses a password, the password is converted to a hash using a cryptographic function, such as MD5 or SHA.
- This means that, in theory, no one except the user (not even the system administrator) knows the password, because the plaintext should not be recoverable from the hash.

PASSWORD ATTACKS (cont.)

- Plaintext/Unencrypted Attacks
  - ✓ A plaintext/unencrypted attack exploits password storage or a network authentication protocol that does not use encryption.
  - ✓ Examples include **PAP**, basic **HTTP/FTP authentication**, and **Telnet**.
  - ✓ These protocols must not be used.
  - ✓ Passwords must never be saved to an unmanaged file.
  - ✓ One common source of credential breaches is passwords embedded in application code that has subsequently been uploaded to a public repository.

PASSWORD ATTACKS (cont.)

- Online Attacks
  - ✓ An online password attack is where the threat actor interacts with the authentication service **directly**—a web login form or VPN gateway, for instance.
  - ✓ The attacker submits passwords using either a database of known passwords (and variations) or a list of passwords that have been cracked offline.
  - ✓ Also, be aware that there are databases of **username and password/password hash combinations** for multiple accounts stored across the Internet.
  - ✓ These details derive from successful hacks of various companies' systems.
  - ✓ These databases can be searched using a site such as haveibeenpwned.com.

PASSWORD ATTACKS (cont.)

- Offline Attacks
  - ✓ An offline attack means that the attacker has managed to obtain a database of password hashes, such as **%SystemRoot%\System32\config\SAM**, **%SystemRoot%\NTDS\NTDS.DIT** (the Active Directory credential store), or **/etc/shadow**.
  - ✓ Once the password database has been obtained, the cracker does not interact with the authentication system.
  - ✓ The only indicator of this type of attack (other than misuse of the account in the event of a successful attack) is a file system audit log that records the malicious account accessing one of these files.

PASSWORD ATTACKS (cont.)

- Offline Attacks (cont.)
  - ✓ Threat actors can also read credentials from host memory, in which case the only reliable indicator might be the presence of attack tools on a host.
  - ✓ If the attacker cannot obtain a database of passwords, a packet sniffer might be used to obtain the client response to a server challenge in a protocol such as NTLM or CHAP/MS-CHAP.
  - ✓ Although these protocols avoid sending the hash of the password directly, the response is derived from it in some way.
  - ✓ Password crackers can exploit weaknesses in a protocol to calculate the hash and match it to a dictionary word or brute force it.

BRUTE-FORCE AND DICTIONARY ATTACKS

- Some password attacks exploit the weak credentials chosen by users.
- Others can exploit vulnerabilities in the storage mechanism.
- For Example:
  - ✓ The Windows SAM database can be configured to store hashes for compatibility with older versions (LM and NTLMv1 hashes).
  - ✓ These legacy hashes are cryptographically weak and highly vulnerable to password cracking.

Brute-Force Attack

- A brute-force attack attempts every possible combination in the output space in order to match a captured hash and guess at the plaintext that generated it.
- The output space is determined by the number of bits used by the algorithm (**128-bit MD5** or **256-bit SHA256**, for instance).
- The larger the output space and the more characters that were used in the plaintext password, the more difficult it is to compute and test each possible hash to find a match.
- Brute-force attacks are heavily constrained by time and computing resources, and are therefore most effective at cracking short passwords.
- However, brute-force attacks distributed across multiple hardware components, like a cluster of high-end graphics cards, can be successful at cracking longer passwords.

Dictionary and Rainbow Table Attacks

- Dictionary attack
  - ✓ can be used where there is a good chance of guessing the likely value of the plaintext, such as a non-complex password.
  - ✓ The software generates hash values from a dictionary of plaintexts to try to match one to a captured hash.
- Rainbow table
  - ✓ The attacker uses a precomputed lookup table of all possible passwords and their matching hashes.
  - ✓ Not all possible hash values are stored, as this would require too much memory.
  - ✓ Values are computed in chains, and only the first and last values need to be stored.
  - ✓ The hash value of a stored password can then be looked up in the table and the corresponding plaintext discovered.

Dictionary and Rainbow Table Attacks (cont.)

- Using a salt to add a random value to the stored plaintext helps to slow down rainbow table attacks, because the tables cannot be created in advance and must be recreated for each combination of password and salt value.
- Rainbow tables are also impractical when trying to discover long passwords (more than about 14 characters).
- UNIX and Linux password storage mechanisms use salt, but Windows does not.
- Consequently, in a Windows environment, it is even more important to enforce strong password policies.

Hybrid Attack

- A hybrid password attack uses a combination of attack methods when trying to crack a password.
- A typical hybrid password attack uses a combination of **dictionary** and **brute force** attacks.
- It is principally targeted against naive passwords with inadequate complexity, such as **james1**.

PASSWORD CRACKERS

- Although there are some Windows tools, including the infamous Cain and L0phtcrack (l0phtcrack.com) tools, most password crackers run primarily on Linux.
- For example, a tool such as Hashcat (hashcat.net/hashcat) is run using the following general syntax:

```
hashcat -m HashType -a AttackMode -o OutputFile InputHashFile
```

- The input file should contain hashes of the same type, using the specified format (hashcat.net/wiki/doku.php?id=example_hashes).
- Hashcat can be used with a single word list (dictionary mode `-a 0`) or multiple word lists (combinator mode `-a 1`).

PASSWORD CRACKERS (cont.)

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: NetNTLMv2
Hash.Target......: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.......: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 34233472/152587890625 (0.02%)
Rejected.........: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1....: $87r8678 -> dSDoRS12
```

Lab

Lab 8: Auditing Passwords with a Password Cracking Utility

7.1- Summarize Authentication Design Concepts

7.2- Implement Knowledge-Based Authentication

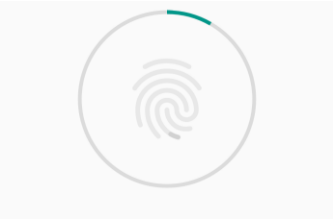
7.3- Summarize Biometrics Authentication Concepts

BIOMETRIC AUTHENTICATION

- The first step in setting up biometric authentication is enrollment.
- The chosen biometric information is scanned by a biometric reader and converted to binary information.
- There are generally two steps in the scanning process:
  1. A sensor module acquires the biometric sample from the target.
  2. A feature extraction module records the features in the sample that uniquely identify the target.
- The biometric template is kept in the authentication server's database.
- When the user wants to access a resource, he or she is re-scanned, and the scan is compared to the template.
- If they match to within a defined degree of tolerance, access is granted.

FINGERPRINT RECOGNITION

- Physiologic biometric features represent a something you are factor.
- They include fingerprint patterns, iris or retina recognition, or facial recognition.
- Fingerprint recognition is the most widely implemented biometric authentication method.
- The technology required for scanning and recording fingerprints is relatively inexpensive and the process quite straightforward.
- The technology is also non-intrusive and relatively simple to use, although moisture or dirt can prevent readings.



FINGERPRINT RECOGNITION (cont.)

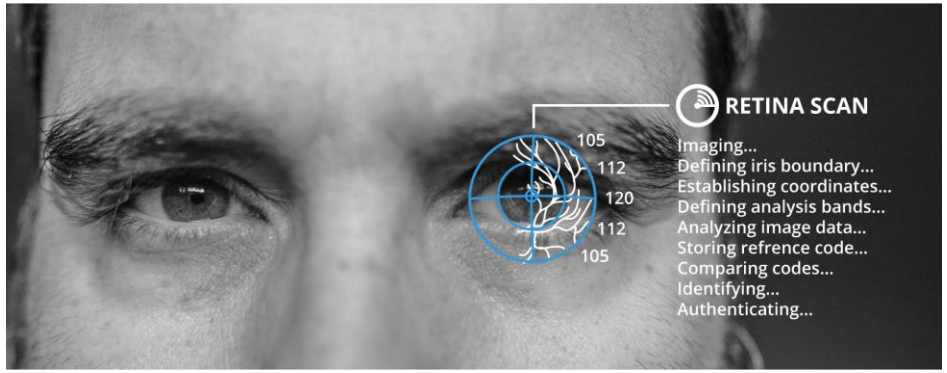
- The main problem with fingerprint scanners is that it is possible to obtain a copy of a user's fingerprint and create a mold of it that will fool the scanner (tomsguide.com/us/iphone-touch-id-hack,news-20066.html).
- These concerns are addressed by vein matching scanners, or vascular biometrics.
- This requires a more complex scanner—an infrared light source and camera—to create a template from the unique pattern of blood vessels in a person's finger or palm.

FACIAL RECOGNITION

- Facial recognition records multiple indicators about the size and shape of the face, like the distance between each eye, or the width and length of the nose.
- The initial pattern must be recorded under optimum lighting conditions; depending on the technology, this can be a lengthy process.
- Again, this technology is very much associated with law enforcement, and is the most likely to make users uncomfortable about the personal privacy issues.
- Facial recognition suffers from relatively high false acceptance and rejection rates and can be vulnerable to spoofing.
- Much of the technology development is in surveillance, rather than for authentication, although it is becoming a popular method for use with smartphones.

FACIAL RECOGNITION (cont.)

- The limitations of facial recognition can be overcome by scanning more detailed features of the eye:
  - ✓ Retinal scan—an infrared light is shone into the eye to identify the pattern of blood vessels, The arrangement of these blood vessels is highly complex and typically does not change from birth to death, except in the event of certain diseases or injuries, Retinal scanning is therefore one of the most accurate forms of biometrics, Retinal patterns are very secure, but the equipment required is expensive and the process is relatively intrusive and complex. False negatives can be produced by disease, such as **cataracts**.



FACIAL RECOGNITION (cont.)

- The limitations of facial recognition can be overcome by scanning more detailed features of the eye (cont.)
  - ✓ Iris scan—matches patterns on the surface of the eye using near-infrared imaging and so is less intrusive than retinal scanning (the subject can continue to wear glasses, for instance) and a lot quicker, Iris scanners offer a similar level of accuracy as retinal scanners but are much less likely to be affected by diseases, Iris scanning is the technology most likely to be rolled out for high-volume applications, such as airport security, There is a chance that an iris scanner could be fooled by a high-resolution photo of someone's eye.

BEHAVIORAL TECHNOLOGIES

- Something you do refers to behavioral biometric pattern recognition.
- Rather than scan some attribute of your body, a template is created by analyzing a behavior, such as **typing**, **writing a signature**, or **walking/moving**.
- The variations in motion, pressure, or gait are supposed to uniquely verify each individual.
- In practice, however, these methods are subject to higher error rates, and are much more troublesome for a subject to perform.

BEHAVIORAL TECHNOLOGIES (cont.)

- Voice Recognition
  - ✓ Relatively cheap, as the hardware and software required are built into many standard PCs and mobiles.
  - ✓ However, obtaining an accurate template can be difficult and time-consuming.
  - ✓ Background noise and other environmental factors can also interfere with logon.
  - ✓ Voice is also subject to impersonation.
- Gait Analysis
  - ✓ Produces a template from human movement (locomotion).
  - ✓ The technologies can either be camera-based or use smartphone features, such as an accelerometer and gyroscope.

BEHAVIORAL TECHNOLOGIES (cont.)

- Signature Recognition
  - ✓ Signatures are relatively easy to duplicate, but it is more difficult to fake the actual signing process.
  - ✓ Signature matching records the user applying their signature (stroke, speed, and pressure of the stylus).
- Typing
  - ✓ Matches the speed and pattern of a user's input of a passphrase.

Lab

Lab 9: Managing Centralized Authentication