User Authentication

Learning Objective

After studying this chapter, you should be able to:

- Understand the distinction between identification and verification.
- Recognizing the various methods that can be used for user authentication.
- Present an overview of techniques for remote user authentication using symmetric encryption and asymmetric encryption.
- Present an overview of social engineering.

1.Introduction

In computer security, user authentication, or identity verification, is the fundamental building block and the primary line of defense. User authentication allows the verifier to gain assurances that the identity of the claimant is as declared. Typically user authentication is established at the start of a connection. It prevents impersonation, and is the basis for most types of access control and for user accountability.

User authentication process consists of two steps:

1. Identification step: Presenting an identifier, or user name, to the security system. Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.
2. Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

For example, user Alice could have the user identifier Alice_1234. This information needs to be stored on any server or computer system that Alice wishes to use and could be known to system administrators and other users. A typical item of authentication information associated with this user ID is a password, which is kept secret (known only to Alice and to the system). If no one is able to obtain or guess Alice's password, then the combination of Alice's user ID and password enables administrators to set up Alice's access permissions and audit her activity. Because Alice's ID is not secret, system users can send her email, but because her password is secret, no one can pretend to be Alice. In essence, identification is the means by which a user provides a claimed identity to the system, user authentication is the means of establishing the validity of the claim.

There are two Types of entity authentication:

1. Unilateral entity authentication is assurance of the identity of one entity to another (and not vice-versa).
2. Mutual entity authentication occurs if both communicating entities provide each other with assurance of their identity.

2.Entity Authentication Functions

The procedure of confirming a user's authenticity, is the action of comparing the provided credentials of the user against an existing database of validated identities. The most common ways of providing entity authentication are by using one, or a combination, of the following:

1. Something that you have.
2. Something that you are.
3. Something that you know.

All of these methods, properly implemented and used, can provide secure user authentication. However, each method has its pros and cons.

Multifactor authentication (MFA) uses any two or more authentication factors. A key part of this is that the authentication factors must be in at least two of the categories. For example, using a smart card and a PIN is multifactor authentication since the two factors are something you have and something you know. However, if a user were required to enter a password and a PIN, it would not be multifactor authentication since both methods are from the same factor (something you know). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

2.1.Something you have Authentication

Hardware tokens are small devices that a user uses to authorize access to a system or application. They come in different forms, including cryptographic keys, electronic keycards, smart cards, and physical keys. There are two types of hardware token:

1. Dumb tokens: Any physical device without a memory that can be used as a type of electronic key. Dumb tokens typically operate with a reader that extracts some information from the token and then indicates whether the information authenticates the entity or not. A good example of a dumb token is a plastic card with a magnetic stripe. The security of the card is based entirely on the difficulty of extracting the information from the magnetic stripe.

2. Smart cards: A plastic card that contains a chip, which gives the card a limited amount of memory and processing power. A smart card can store secret data more securely, and can also engage in cryptographic processes that require some computations to be performed (e.g. challenge/response). Smart cards are widely used in most countries for banking operations, electronic ticketing applications, etc.

In general, hardware tokens are widely used with a PIN providing multi-factor authentication. In other words, the user must have something (the hardware token) and know something (the PIN). since they provide strong security and they are easily integrated. On the other hand, some of the disadvantages that has to be taken into consideration is the high cost of implementing the authentication procedure, the fact that the hardware tokens can be inconvenient for the user (extra item to carry and keep safe).

2.2.Something you are Authentication

Biometric methods provide the something you are factor of authentication. Biometrics are techniques for human user authentication that are based on physical characteristics of the human body. Biometrics characteristics can be divided into three main classes namely:

1. Morphological: is related to the shape of the body such as retina, face recognition, prints (finger, thumb, palm), iris, hand geometry, etc.
2. Behavioral is related to the behavior of a person such as gait, signature, keystroke dynamics, etc.
3. Biological is related to the inner part of a living organism such as heart beat, DNA, blood.

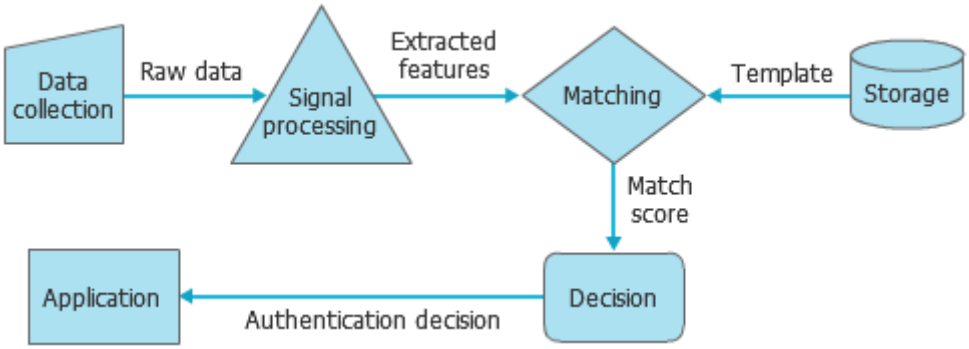
Figure(7.1): Something you are Authentication

Preparing the biometric data can be summarized in two main steps namely data collection and signal processing figure(7.2):

1. **Data Collection**: also referred to as data acquisition, comprises input device or sensor that reads the biometric information from the user. Converts biometric information into a suitable form for processing by the remainder of the biometric system (e.g. image data). Examples: video camera, fingerprint scanner, digital tablet (signatures), microphone, accelerometer (gait recognition), etc.
2. **Signal Processing**:
   - Used for extraction of features from raw sensor data:
   - Receives raw data from the data collection system.
   - Transforms data into the format required by the Matching Subsystem.
   - Relevant features are typically extracted from raw biometric data.
   - Filtering and further signal processing operations (e.g. contrast enhancement, noise reduction) may be applied.

Biometric authentication can be summarized in two steps namely enrolment and authentication. The stage of the enrolment is where the user provide his/her biometric data. The biometric data will be captured and then, the features will be extracted and

stored into the database. During the authentication process, the stored features will be compared with the ones currently presented for an access. If it matches, then, an access will be granted.



Figure(7.2): Biometric Authentication Model

While biometrics does provide the strongest authentication, it is susceptible to errors. A false rejection error (also called type 1 error) occurs when a system falsely rejects a known user and indicates the user is not known. A false acceptance error (also called a type 2 error) occurs when a system falsely identifies an unknown user as a known user. Biometric systems typically can be adjusted for sensitivity, but the sensitivity affects the accuracy. The false accept rate decreases as the sensitivity increases. In other words, a less sensitive system falsely authenticates unknown users. In contrast, the false reject rate increases as the sensitivity increases more known users are rejected as unknown. The most serious drawback in biometric authentication is that if a biometric authentication factor is compromised, this situation is not reversible. For example, a password can be reset, while a user's fingerprints cannot. Specifically in the second case, the fingerprints of a user can be easily copied, since a fingerprint can be left on any surface.

2.3.Something you Know Authentication

Something the individual knows: Examples include a password, a personal identification number (PIN), pass-phrase, or answers to a prearranged set of questions. This method is far the most used authentication method. It is widely used despite its obvious lack of security. This fact is due to the ease of implementation of this solution, and to the immediate recognition of that system by the users that facilitates its deployment and acceptance.

Password Authentication Vulnerabilities: A key problem with user name and password (ID/Password), the human factor:

- Most users select passwords from a small subset of the password space (e.g., short passwords, dictionary words, proper names).
- Passwords are easy to guess or search if easy to remember.
- Passwords are easily stolen if written down.
- Users may share passwords.
- Passwords can be forgotten if difficult to remember.

With weaker password, the attackers will be able to hack the system easily. When utilizing passwords, it is imperative to utilize solid passwords. A solid secret key has a blend of capitalized, lower case, numbers, and unique characters. There are three factors that determine the strength of the password namely length, cardinality and entropy. A cardinality of 94 means the password has been created from a pool of 94 characters including uppercase, lower case, numbers and special characters. Entropy is the calculated strength of the password in bits. For example, a password of eight character length, with a cardinality of 94 is equivalent to entropy of 52.4 bits. A normal PC will able to crack the 94 cardinality password in 20 minutes using brute force. Using super computers, it will take 0.07 seconds to crack. Hence an entropy of 52.4 bits or 8 character length is a weak password. Now security administrators recommend at least 12 characters passwords.

Attack on Passwords

There are various forms of password attacks, the most important ones are:

- Brute force attack: In a brute force attack, an attacker uses a computer program to check all possible password combinations.
- Dictionary attack: A dictionary attack only tries possibilities of passwords most likely to succeed. It takes up common Dictionary words to decode a password, like January 2020 or April@2020.
- Phishing: In a phishing attack, an attacker disguises their phishing attacks as unsuspecting emails, posing as legitimate and known services. From these emails, the attacker takes users to fake login pages disguised as a legitimate service. Often, the attacker adds a subtle, threatening dimension to their emails like the prospect of service cancellation. This forces the users to hand over their credentials before giving it careful consideration.
- Rainbow table attack: Traditional brute force attacks store no pre-computed data and compute each hash at run time using minimal space and taking a long time. Rainbow table acts as a database that contains the pre-computed hashed output for most or all possible passwords. Rainbow tables take a considerable amount of time to generate and are not always complete.
- Credential stuffing: In a credential stuffing attack, attackers use lists of stolen usernames and passwords in combination on various accounts, automatically trying over and over until they hit a match. Credential stuffing relies on users' tendency to reuse their passwords for multiple accounts, often to great success. Further, hackers share stolen passwords on the Dark Web or sell them.
- Password spraying: A Password spraying attack is made by hackers by getting a list of the most commonly used passwords across the web or even from past intelligence gathered on the target, and attacking the target by trying these concrete sets of passwords.
- Key logger Attack: One of the most insidious kinds of attacks hackers increasingly use involve "key loggers". Key loggers record every keystroke a device user types into a mobile, laptop, or desktop computer. The server records user ids, passwords, account details, and SMS messages.

Cybercriminals can then monitor user communications and even withdraw money from victims bank accounts.

- Traffic interception: In this attack, the cybercriminal uses software such as packet sniffers to monitor network traffic and capture passwords as they are passed. Similar to eavesdropping or tapping a phone line, the software monitors and captures critical information, where the attack is made easier when passed on the network without any encryption. Although, encrypted information may be decrypted, depending on the strength of the encryption method used.
- Man-in-the-middle: In this attack, the hacker's program does not just monitor information being passed but actively inserts itself in the middle of the interaction, usually by impersonating a website or app. This allows the program to capture the user's credentials and other sensitive information, such as account numbers, social security numbers, etc. Man in the middle attacks are often facilitated by social engineering attacks which lure the user to a fake site.

Selecting a Good Password

Good passwords can be constructed in several ways:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~- =\`{}[]:",'<>?,./).
- Are at least 12 alphanumeric characters long and is a passphrase.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.
- Try to create passwords that can be easily remembered: One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

One-time Password (OTP)

One-time password systems provide a mechanism for logging on to a network or service using a unique password that can only be used once. This prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time. Typically the user's logon name stays the same, and the one-time password changes with each login. One-time passwords can be generated in several ways, and each one has trade-offs in terms of security, convenience, cost, and accuracy. Some examples are:

Grid Cards: Simple methods such as transaction numbers lists and grid cards can provide a set of one-time passwords. These methods offer low investment costs but are slow, difficult to maintain, easy to replicate and share, and require the users to keep track of where they are in the list of passwords.

Security Tokens: A more convenient way for users is to use an OTP security token which is a hardware device capable of generating one-time passwords. Some of these devices are PIN-protected, offering an additional level of security. Although this is a proven solution for enterprise applications, the deployment cost can make the solution expensive for consumer applications. Because the token must be using the same method as the server, a separate token is required for each server logon, so users need a different token for each Web site or network they use.

As OTP generates a password, the verification requires synchronization between the token and the authentication server. There are several methods for synchronization such as counter synchronized and time synchronized.

Cryptographic Challenge-response based Authentication

PAP (Password Authentication Protocol) is a simple protocol for authentication over a network, which sends clear passwords and identifiers over the network. Subsequently, CHAP (Challenge Handshake Authentication Protocol) is an improvement of PAP, but it still requires transmitting a hashed password. The main idea of a challenge-response based authentication is that the claimant proves he knows the secret without sending it clear over the channel. Thus, CHAP is a challenge-based authentication protocol, but the transmission of a hashed password is still a problem due to brute force and dictionary attacks. Besides, hashed passwords still contain a lot of information about the secret password. The main response to solve that problem is the use of

cryptography, either symmetric or asymmetric in order to implement a challenge-response authentication. Generally speaking, a challenge-response authentication system is a system that issues a “challenge” on the client request i.e. challenge in this context: question of identification, and verifies it in the “response” of the claimed identity i.e. response in this context: provide a proof of identification.

In the symmetric case, the server sends a challenge to the claimant. The challenge may be a nonce, timestamp, sequence number, or any combination. Generally, the claimant then enciphers the challenge with the shared key and sends the result back to the server, which compares the result with the one it has also calculated.

In the asymmetric case, the claimant owns a private key associated with a certificate that contains the relative public key. The claimant provides the server his certificate. The server sends a random number as a challenge, and the claimant uses his private key to sign the challenge (or to encipher it), and sends the result back to the server. The server then verifies the signature with the public key (or decipher the response) to check the challenge is verified.

3.Social Engineering

Social engineering is a nontechnical method of breaking into a system or network. It is the process of deceiving users of a system and convincing them to perform acts useful to the hacker, such as giving out information that can be used to defeat or bypass security mechanisms. Social engineering is important to understand because hackers can use it to attack the human element of a system and circumvent technical security measures. This method can be used to gather information before or during an attack.

A social engineer commonly uses the telephone or Internet to trick people into revealing sensitive information or to get them to do something that is against the security policies of the organization. It includes the acquisition of sensitive information or inappropriate access privileges by an outsider, based on the building of inappropriate trust relationships. It preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people, and the fear of getting in trouble. Hackers who are able to blend in and appear to be a part of the organization are the most successful at social-engineering attacks. People are usually the weakest link in

the security chain this principle is what makes social engineering possible. A successful defense depends on having good policies in place and teaching employees to follow the policies.

The most dangerous part of social engineering is that companies with authentication processes, firewalls, virtual private networks, and network-monitoring software are still wide open to attacks, because social engineering does not assault the security measures directly. Instead, a social-engineering attack bypasses the security measures and goes after the human element in an organization. Social engineering is the hardest form of attack to defend against because a company cannot protect itself with hardware or software alone.

3.1.Types of Social Engineering-Attacks

Social engineering can be broken into two common types:

Human-Based Social Engineering

This type refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password. Human-based techniques can be broadly categorized as follows:

- Impersonating an Employee or Valid User: In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor. Once inside the facility, the hacker gathers information from trashcans, desktops, or computer systems.
- Posing as an Important User: In this type of attack, the hacker pretends to be an important user such as an executive or high-level manager who needs immediate assistance to gain access to a computer system or files. The hacker uses intimidation so that a lower-level employee such as a help desk worker will assist them in gaining access to the system. Most low-level employees will not question someone who appears to be in a position of authority.
- Using a Third Person: Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or cannot be contacted for verification.

- Calling Technical Support: Calling tech support for assistance is a classic technique. Help desk and technical support are trained to help users, which makes them good prey for social-engineering attacks.
- Shoulder Surfing: Shoulder surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system. A hacker can watch a valid user log in and then use that password to gain access to the system.
- Dumpster Diving: Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information.
- Reverse social engineering: this method is a more advanced method of gaining illicit information. Using this technique, a hacker creates a persona that appears to be in a position of authority so that employees ask the hacker for information, rather than the other way around. For example, a hacker can impersonate a help desk employee and get the user to give them information such as a password.

Computer-Based Social Engineering

Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an email and asking them to reenter a password in a web page to confirm it. This type of attacks include, but not limited to the following:

- Phishing Attacks: Phishing involves sending an email, usually posing as a bank, or other financial organization. The email requests that the recipient confirm banking information or reset passwords or PINs. The user clicks the link in the email and is redirected to a fake website. The hacker is then able to capture this information and use it for financial gain or to perpetrate other attacks. Emails that claim the senders have a great amount of money but need your help getting it out of the country are examples of phishing attacks. These attacks prey on the common person and are aimed at getting them to provide bank account access codes or other confidential information to the hacker.
- Online Scams: Some websites that make free offers or other special deals can lure a victim to enter a username and password that may be the same as those

they use to access their work system. The hacker can use this valid username and password once the user enters the information in the website form. Mail attachments can be used to send malicious code to a victim's system, which could automatically execute something like a software key logger to capture passwords. Viruses, Trojans, and worms can be included in cleverly crafted emails to entice a victim to open the attachment. Mail attachments are considered a computer-based social-engineering attack.

- Pop-up windows: Pop-up windows can also be used in a similar manner to email attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.
- URL Obfuscation: The URL (uniform resource locator) is commonly used in the address bar of a web browser to access a particular website. URL obfuscation consists of hiding a fake URL in what appear to be a legitimate website address. URL obfuscation is used in phishing attacks and some online scams to make the scam seem more legitimate. A website address may be seen as an actual financial institution name or logo, but the link leads to a fake website or IP address. When users click the link, they are redirected to the hacker's site.

3.2.Social-Engineering Countermeasures

Knowing how to combat social engineering is critical for any secure system. There are a number of ways to do this:

- Documented and enforced security policies and security awareness programs are the most critical component in any information security program. Good policies and procedures are not effective if they are not taught and reinforced to employees. The policies need to be communicated to employees to emphasize their importance and then enforced by management.
- The corporate security policy should address how and when accounts are set up and terminated, how often passwords are changed, who can access what information, and how policy violations are to be handled. Also, the policy should spell out help desk procedures for the previous tasks as well as a process for identifying employees.
- The destruction of paper documents and physical access restrictions are additional areas the security policy should address. In addition, the policy should

address technical areas, such as use of modems, wireless networks, Internet Access, and virus control.

- One of the advantages of a strong security policy is that it removes the responsibility of employees to make judgment calls regarding a hacker's request. If the requested action is prohibited by the policy, the employee has guidelines for denying it.
- The most important countermeasure for social engineering is employee education. All employees should be trained on how to keep confidential data safe. Management teams are involved in the creation and implementation of the security policy so that they fully understand it and support it throughout the organization. The company security awareness policy should require all new employees to go through a security orientation. Annual classes should be required to provide refreshers and updated information for employees.

Exercises:

True or False

Question	True	False
1. Examples of dynamic biometrics include recognition by fingerprint, retina, and face.		
2. User authentication is the means by which a user provides a claimed identity to the system.		
3. User authentication is the basis for most types of access control and for user accountability.		
4. For network based user authentication the most important methods involve cryptographic keys and something the individual possesses, such as a smart card.		
5. There are a variety of problems including dealing with false positives and false negatives, user acceptance, cost, and convenience with respect to biometric authenticators.		
6. Any timestamp based procedure must allow for a window of time sufficiently large enough to accommodate network delays yet sufficiently small to minimize the opportunity for attack.		
7. An e-mail message should be encrypted such that the mail handling system is not in possession of the decryption key.		
8. The operating system cannot enforce access-control policies based on user identity.		

Multiple Choice Questions

1. A common item of authentication information associated with a user is a _____ .
   A. nonce
   B. timestamp
   C. ticket
   D. password

2. _____ is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.
   A. Identification
   B. Message authentication
   C. Verification
   D. User authentication

3. Presenting an identifier to the security system is the _____ step.
   A. authentication
   B. verification
   C. identification
   D. clarification

4. Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the _____ step.
   A. identification
   B. verification
   C. clarification
   D. authentication

5. In an unprotected network environment any client can apply to any server for service. The obvious security risk of this is _____ .
   A. certification
   B. authentication
   C. impersonation
   D. authorization

6. What is it called when a hacker pretends to be a valid user on the system?
   A. Impersonation
   B. Third-person authorization
   C. Help desk
   D. Valid user

7. Faking a website for the purpose of getting a user's password and username is which type of social-engineering attack?
   A. Human-based
   B. Computer-based
   C. Web-based
   D. User-based

8. Dumpster diving can be considered which type of social-engineering attack?
   A. Human-based
   B. Computer-based
   C. Physical access
   D. Paper-based

9. Which of the following is the best example of reverse social engineering?
   A. A hacker pretends to be a person of authority in order to get a user to give them information
   B. A help desk employee pretends to be a person of authority
   C. A hacker tries to get a user to change their password
   D. A user changes their password

10. What is the best reason to implement a security policy?

A. It increases security

B. It makes security harder to enforce

C. It removes the employee's responsibility to make judgments

D. It decreases security

11. Using pop-up windows to get a user to give out information is which type of social-engineering attack?

A. Human-based

B. Computer-based

C. Nontechnical

D. Coercive

12. What is the best way to prevent a social-engineering attack?

A. Installing a firewall to prevent port scans

B. Configuring an IDS to detect intrusion attempts

C. Increasing the number of help desk personnel

D. Employee training and education

References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice, 7th edn. Prentice Hall (2017).
2. Graves, K.: CEH Certified Ethical Hacker, STUDY GUIDE, Wiley Publishing, (2010).
3. Zulkarnain, S., Idrus, S. , Cherrier, E. , Rosenberger, C. , Schwartzmann, J.: A Review on Authentication Methods, Australian Journal of Basic and Applied Sciences, (2013), 7 (5), pp.95-107. hal-00912435.

Number of the Question	True	False
1		✓
2	✓	
3	✓	
4		✓
5	✓	
6	✓	
7	✓	
8		✓

Number of the Question	Answer
1	D
2	B
3	C
4	B
5	C
6	A
7	B
8	A
9	A
10	C
11	B
12	D