WEEK 7 : LECTURE 6 - OS SECURITY & PROTECTION

Bachelor's Degree in Information Technology
BITOS4111, OPERATING SYSTEMS
Trimester: 05
From **July 2024** to **October 2024**

OBJECTIVES/TOPICS

- The Security Problem.
- Program Threats.
- System and Network Threats.
- Cryptography as a Security Tool.
- User Authentication

INTRODUCTION

- Both protection and security are vital to computer systems
- Security is a measure of confidence that the integrity of a system and its data will be preserved
- Protection is the set of mechanisms that control the access of processes and users to the resources defined by a computer system.

INTRODUCTION

- Security involves guarding computer resources against unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency

- Computer resources include the information stored in the system (both data and code), as well as the CPU, memory, secondary storage, tertiary storage, and networking that compose the computer facility

THE SECURITY PROBLEM

- In many applications, ensuring the security of the computer system is worth considerable effort.

- Large commercial systems containing payroll or other financial data are inviting targets to thieves.

- Systems that contain data pertaining to corporate operations may be of interest to unscrupulous competitors.

- Also, loss of such data, whether by accident or fraud, can seriously impair the ability of the corporation to function.

THE SECURITY PROBLEM

- In many applications, ensuring the security of the computer system is worth considerable effort.

- Large commercial systems containing payroll or other financial data are inviting targets to thieves.

- Systems that contain data pertaining to corporate operations may be of interest to unscrupulous competitors.

- Also, loss of such data, whether by accident or fraud, can seriously impair the ability of the corporation to function.

THE SECURITY PROBLEM

- Even raw computing resources are attractive to attackers for bitcoin mining, for sending spam, and as a source from which to anonymously attack other systems

- We say that a system is secure if its resources are used and accessed as intended under all circumstances.

- Unfortunately, total security cannot be achieved.

- Nonetheless, we must have mechanisms to make security breaches a rare occurrence, rather than the norm.

THE SECURITY PROBLEM

- Security violations (or misuse) of the system can be categorized as intentional (malicious) or accidental.

- It is easier to protect against accidental misuse than against malicious misuse.

- For the most part, protection mechanisms are the core of accident avoidance.

THE SECURITY PROBLEM

- the terms intruder, hacker, and attacker are for those attempting to breach security.

- A threat is the potential for a security violation, such as the discovery of a vulnerability, whereas an attack is an attempt to break security

THE SECURITY PROBLEM

- The following list includes several forms of accidental and malicious security violations.
  - **1. Breach of confidentiality:** This type of violation involves unauthorized reading of data (or theft of information).
  - **2. Breach of integrity:** This violation involves unauthorized modification of data
  - **3. Breach of availability:** This violation involves unauthorized destruction of data
  - **4. Theft of service:** This violation involves unauthorized use of resources.

THE SECURITY PROBLEM

- **5. Denial of service.** This violation involves preventing legitimate use of the system. Denial-of-service (DOS) attacks are sometimes accidental

- Attackers use several standard methods in their attempts to breach security.

- The most common is masquerading, in which one participant in a communication pretends to be someone else (another host or another person)

THE SECURITY PROBLEM

- The most common is masquerading, in which one participant in a communication pretends to be someone else (another host or another person)
    - By masquerading, attackers breach authentication, the correctness of identification; they can then gain access that they would not normally be allowed

THE SECURITY PROBLEM

- Another common attack is to replay a captured exchange of data.
  - A replay attack consists of the malicious or fraudulent repeat of a valid data transmission.
  - Sometimes the replay comprises the entire attack—for example, in a repeat of a request to transfer money.
  - But frequently it is done along with message modification , in which the attacker changes data in a communication without the sender's knowledge.

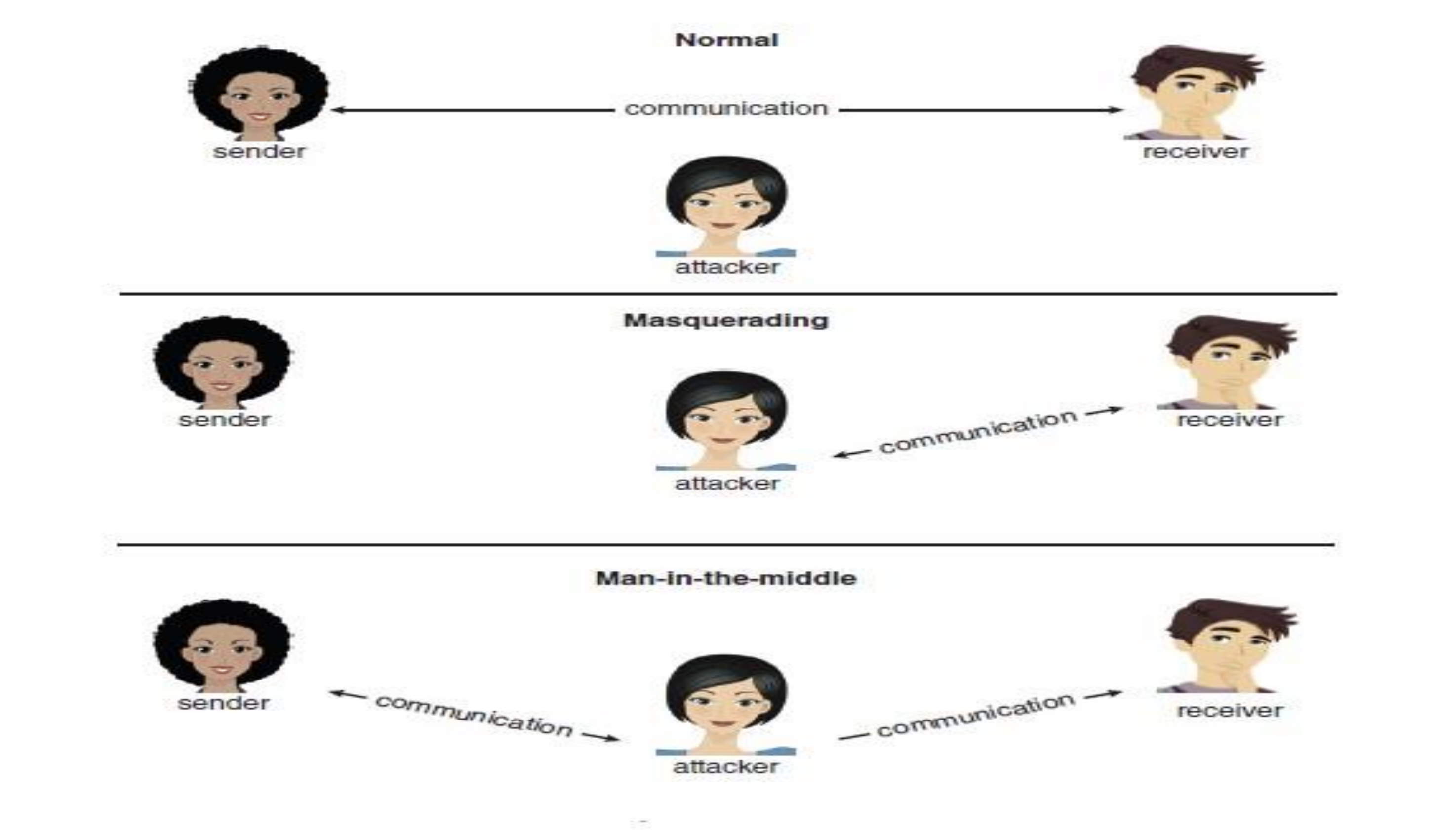
THE SECURITY PROBLEM

- Another common attack is to replay a captured exchange of data.
  - A replay attack consists of the malicious or fraudulent repeat of a valid data transmission.
  - Sometimes the replay comprises the entire attack—for example, in a repeat of a request to transfer money.
  - But frequently it is done along with message modification , in which the attacker changes data in a communication without the sender's knowledge.

THE SECURITY PROBLEM

- another kind of attack is the man-in-the-middle attack, in which an attacker sits in the data flow of a communication, masquerading as the sender to the receiver, and vice versa.
  - In a network communication, a man-in-the-middle attack may be preceded by a session hijacking, in which an active communication session is intercepted.

THE SECURITY PROBLEM



Standard security attacks.[1]

THE SECURITY PROBLEM

- Another broad class of attacks is aimed at privilege escalation.
  - Every system assigns privileges to users, even if there is just one user and that user is the administrator.
  - Privilege escalation gives attackers more privileges than they are supposed to have

THE SECURITY PROBLEM

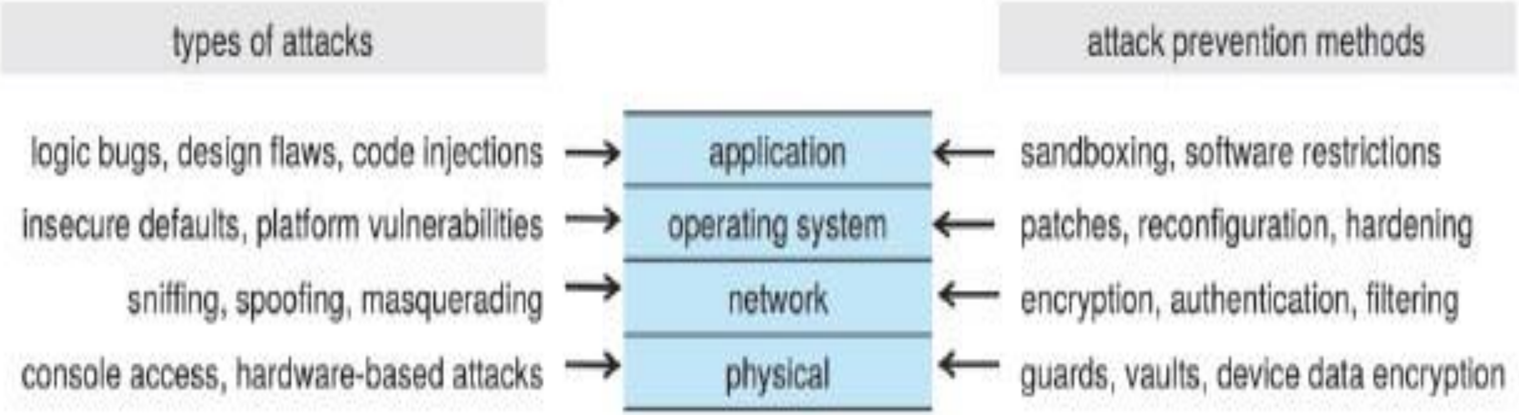
- To protect a system, we must take security measures at four levels:
  - **1. Physical:** The site or sites containing the computer systems must be physically secured against entry by intruders
  - **2. Network:** Most contemporary computer systems—from servers to mobile devices to Internet of Things (IoT) devices—are networked. Networking provides a means for the system to access external resources but also provides a potential vector for unauthorized access to the system itself.

THE SECURITY PROBLEM

- **3. Operating system:** The operating system and its built-in set of applications and services comprise a huge code base that may harbor many vulnerabilities. Insecure default settings, misconfigurations, and security bugs are only a few potential problems

- 4. Application. Third-party applications may also pose risks, especially if they possess significant privileges. Some applications are inherently malicious, but even benign applications may contain security bugs

THE SECURITY PROBLEM


types of attacks
attack prevention methods
logic bugs, design flaws, code injections
application
sandboxing, software restrictions
insecure defaults, platform vulnerabilities
operating system
patches, reconfiguration, hardening
sniffing, spoofing, masquerading
network
encryption, authentication, filtering
console access, hardware-based attacks
physical
guards, vaults, device data encryption

The four-layered model of security.

PROGRAM THREATS

- Processes, along with the kernel, are the only means of accomplishing work on a computer.

- Therefore, writing a program that creates a breach of security, or causing a normal process to change its behavior and create a breach, is a common goal of attackers.

- In fact, even most nonprogram security events have as their goal causing a program threat.

PROGRAM THREATS

- For example, while it is useful to log in to a system without authorization, it is quite a lot more useful to leave behind a back-door daemon or Remote Access Tool (RAT) that provides information or allows easy access even if the original exploit is blocked.

PROGRAM THREATS

- We describe common methods by which programs cause security breaches.
- **1. Malware**
  - Malware is software designed to exploit, disable or damage computer systems.
  - There are many ways to perform such activities.
  - A program that acts in a clandestine or malicious manner, rather than simply performing its stated function, is called a Trojan horse

PROGRAM THREATS

- **1. Malware**
  - Another variation on the Trojan horse is spyware, which is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent
  - Ransomware a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom (usually monetary) for their return

PROGRAM THREATS

- **2. Code Injection**
  - Most software is not malicious, but it can nonetheless pose serious threats to security due to a code-injection attack, in which executable code is added or modified.
  - Even otherwise benign software can harbor vulnerabilities that, if exploited, allow an attacker to take over the program code, subverting its existing code flow or entirely reprogramming it by supplying new code

PROGRAM THREATS

- **2. Code Injection**
  - Code-injection attacks are nearly always the result of poor or insecure programming paradigms, commonly in low-level languages such as C or C++, which allow direct memory access through pointers.
  - This direct memory access, coupled with the need to carefully decide on sizes of memory buffers and take care not to exceed them, can lead to memory corruption when memory buffers are not properly handled.

PROGRAM THREATS

- **3. Viruses and Worms**
  - A virus is a fragment of code embedded in a legitimate program.
  - Viruses are self-replicating and are designed to “infect” other programs.
  - They can wreak havoc in a system by modifying or destroying files and causing system crashes and program malfunctions.

PROGRAM THREATS

- **3. Viruses and Worms**
  - Viruses are usually borne via spam e-mail and phishing attacks.
  - They can also spread when users download viral programs from Internet file-sharing services or exchange infected disks.
  - A distinction can be made between viruses, which require human activity, and worms, which use a network to replicate without any help from humans.

SYSTEM AND NETWORK THREATS

- Program threats, by themselves, pose serious security risks.
  - But those risks are compounded by orders of magnitude when a system is connected to a network.
  - Worldwide connectivity makes the system vulnerable to worldwide attacks.

- The more open an operating system is—the more services it has enabled and the more functions it allows—the more likely it is that a bug is available to exploit it.

SYSTEM AND NETWORK THREATS

- All hackers leave tracks behind them—whether via network traffic patterns, unusual packet types, or other means.

- For that reason, hackers frequently launch attacks from zombie systems—
  - Zombie systems are independent systems or devices that have been compromised by hackers but that continue to serve their owners while being used without the owners' knowledge for nefarious purposes including denial-of-service attacks and spam relay.

SYSTEM AND NETWORK THREATS

- Common attacks includes
  - Attacking Network Traffic (Sniffing)
  - Denial of Service (DoS) and Distributed Denial of Service (DDoS)
  - Port scanning

CRYPTOGRAPHY AS A SECURITY TOOL

- In an isolated computer, the operating system can reliably determine the sender and recipient of all interprocess communication, since it controls all communication channels in the computer.

- In a network of computers, the situation is quite different.
  - A networked computer receives bits "from the wire" with no immediate and reliable way of determining what machine or application sent those bits.

CRYPTOGRAPHY AS A SECURITY TOOL

- Similarly, the computer sends bits onto the network with no way of knowing who might eventually receive them.

- Additionally, when either sending or receiving, the system has no way of knowing if an eavesdropper listened to the communication.

CRYPTOGRAPHY AS A SECURITY TOOL

- Commonly, network addresses are used to infer the potential senders and receivers of network messages.

- Network packets arrive with a source address, such as an IP address.

- And when a computer sends a message, it names the intended receiver by specifying a destination address

CRYPTOGRAPHY AS A SECURITY TOOL

- However, for applications where security matters, we are asking for trouble if we assume that the source or destination address of a packet reliably determines who sent or received that packet

- A rogue computer can send a message with a falsified source address, & numerous computers other than the one specified by the destination address can (and typically do) receive a packet

CRYPTOGRAPHY AS A SECURITY TOOL

- It is generally considered infeasible to build a network of any scale in which the source and destination addresses of packets can be trusted in this sense.

- Therefore, the only alternative is somehow to eliminate the need to trust the network.
  - This is the job of cryptography.

- Abstractly, cryptography is used to constrain the potential senders and/or receivers of a message

CRYPTOGRAPHY AS A SECURITY TOOL

- It is generally considered infeasible to build a network of any scale in which the source and destination addresses of packets can be trusted in this sense.

- Therefore, the only alternative is somehow to eliminate the need to trust the network.
  - This is the job of cryptography.

- Abstractly, cryptography is used to constrain the potential senders and/or receivers of a message

CRYPTOGRAPHY AS A SECURITY TOOL

- Modern cryptography is based on secrets called keys that are selectively distributed to computers in a network and used to process messages.

- Cryptography enables a recipient of a message to verify that the message was created by some computer possessing a certain key.

- Similarly, a sender can encode its message so that only a computer with a certain key can decode the message.

CRYPTOGRAPHY AS A SECURITY TOOL

- Unlike network addresses, however, keys are designed so that it is not computationally feasible to derive them from the messages they were used to generate or from any other public information.

- Thus, they provide a much more trustworthy means of constraining senders and receivers of messages.

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - Because it solves a wide variety of communication security problems, encryption is used frequently in many aspects of modern computing.
  - It is used to send messages securely across a network, as well as to protect database data, files, and even entire disks from having their contents read by unauthorized entities.

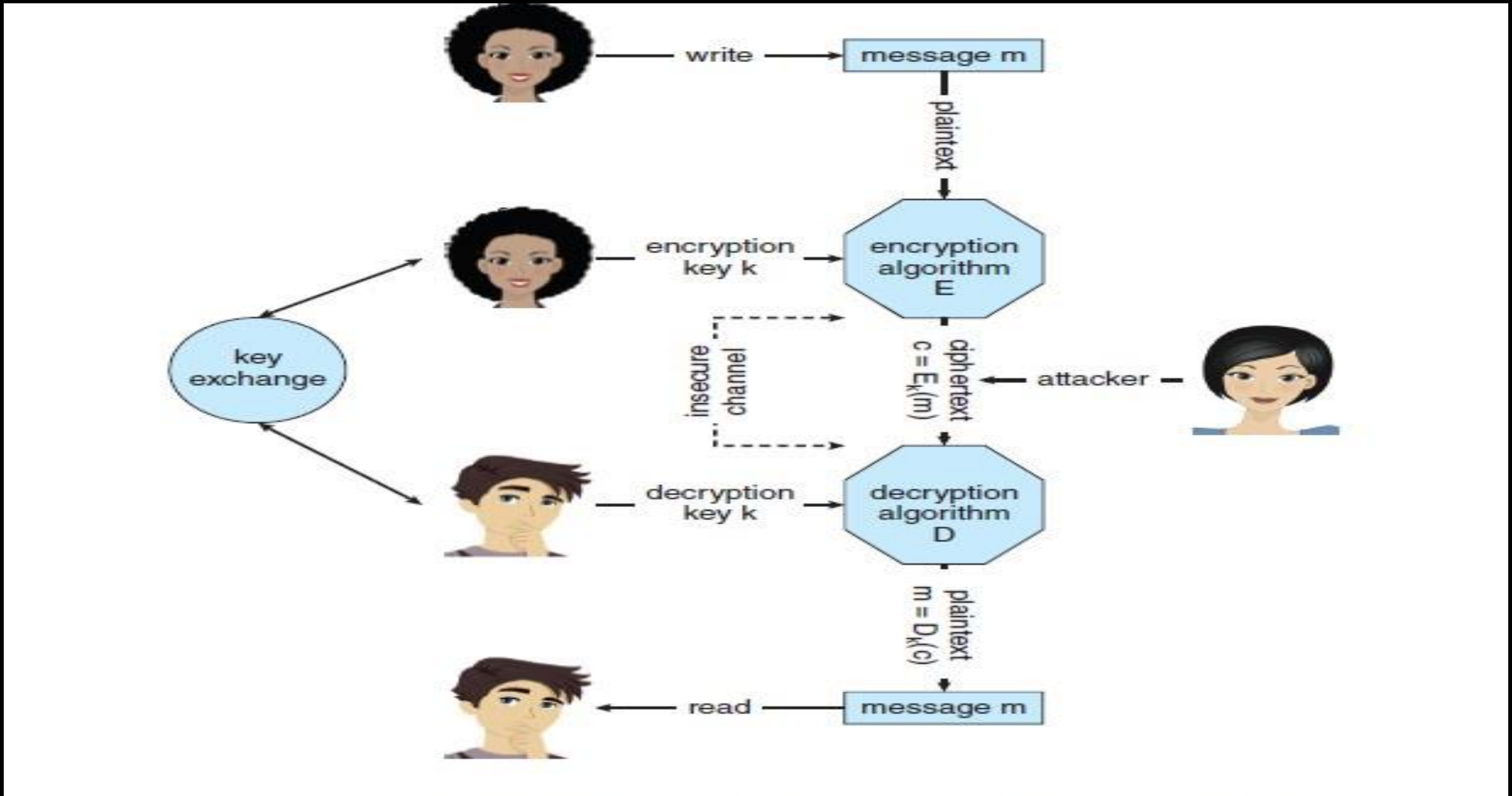
CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - An encryption algorithm enables the sender of a message to ensure that only a computer possessing a certain key can read the message or to ensure that the writer of data is the only reader of the data.

  - Encryption of messages is an ancient practice, of course, and there have been many encryption algorithms historically

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**



A secure communication over an insecure medium.[2]

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - An encryption algorithm consists of the following components:
    - A set K of keys.
    - A set M of messages.
    - A set C of ciphertexts.
    - An encrypting function E : K → (M → C).
    - A decrypting function D : K → (C → M).

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - An encryption algorithm must provide this essential property:
    - given a ciphertext c ∈ C, a computer can compute m such that $E_k(m)$ = c only if it possesses k.
  - Thus, a computer holding k can decrypt ciphertexts to the plaintexts used to produce them, but a computer not holding k cannot decrypt ciphertexts.
    - Since ciphertexts are exposed, it's important that it be infeasible to derive k from the ciphertexts

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - There are two main types of encryption algorithms: symmetric and asymmetric.
  - **Symmetric Encryption**
    - In a symmetric encryption algorithm, the same key is used to encrypt and to decrypt.
    - Therefore, the secrecy of k must be protected.
    - E.g. the Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES),

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
  - **Asymmetric Encryption**
    - In an asymmetric encryption algorithm, there are different encryption and decryption keys.
    - An entity receiving an encrypted communication creates two keys & makes 1 of them (the public key) available to anyone who wants it.

CRYPTOGRAPHY AS A SECURITY TOOL

- **Encryption**
    - **Asymmetric Encryption**
        - Any sender can use that key to encrypt a communication, but only the key creator can decrypt the communication.
        - This scheme, known as public-key encryption
        - As an example of how public-key encryption is an algorithm known as RSA, after its inventors, Rivest, Shamir, and Adleman

CRYPTOGRAPHY AS A SECURITY TOOL

- **Authentication**
  - We have seen that encryption offers a way of constraining the set of possible receivers of a message.
  - Constraining the set of potential senders of a message is called authentication.
  - Authentication is thus complementary to encryption.
  - Authentication is also useful for proving that a message has not been modified.

CRYPTOGRAPHY AS A SECURITY TOOL

- **Authentication**
  - An authentication algorithm using symmetric keys consists of the following components:
    - A set K of keys.
    - A set M of messages.
    - A set A of authenticators.
    - A function S : K → (M → A).
    - A function V : K → (M × A → {true, false}). That is, for each k ∈ K, V_k is a function for verifying authenticators on messages.

CRYPTOGRAPHY AS A SECURITY TOOL

- **Authentication**
  - The critical property that an authentication algorithm must possess is this:
    - for a message m, a computer can generate an authenticator a ∈ A such that $V_k(m, a)$ = true only if it possesses k.
    - Thus, a computer holding k can generate authenticators on messages so that any computer possessing k can verify them

CRYPTOGRAPHY AS A SECURITY TOOL

- **Authentication**
    - there are 2 main varieties of authentication algorithms.
        - **1. message-authentication code (MAC)**
            - uses symmetric encryption
            - In a MAC, a cryptographic checksum is generated from the message using a secret key.
        - 2. **digital-signature algorithm**
            - the authenticators are called digital signatures.
            - Digital signatures are very useful in that they enable anyone to verify the authenticity of the message.

USER AUTHENTICATION

- If a system cannot authenticate a user, then authenticating that a message came from that user is pointless.
- Thus, a major security problem for operating systems is user authentication.
- Users normally identify themselves, but how do we determine whether a user's identity is authentic?

USER AUTHENTICATION

- Generally, user authentication is based on 1 or more of three things:
  - the user's possession of something (a key or card),
  - the user's knowledge of something (a user identifier and password), or
  - an attribute of the user (fingerprint, retina pattern, or signature).

USER AUTHENTICATION

- Passwords
  - The most common approach to authenticating a user identity is the use of passwords.
  - When the user identifies herself by user ID or account name, she is asked for a password.
  - If the user-supplied password matches the password stored in the system, the system assumes that the account is being accessed by the owner of that account.

USER AUTHENTICATION

- Passwords
  - Passwords are extremely common because they are easy to understand and use.
  - Unfortunately, passwords can often be guessed, accidentally exposed, sniffed (read by an eavesdropper), or illegally transferred from an authorized user to an unauthorized one

USER AUTHENTICATION

- Passwords
  - There are three common ways to guess a password.
    - 1. One way is for the intruder (either human or program) to know the user or to have information about the user.
      - All too frequently, people use obvious information (such as the names of their cats or spouses) as their passwords.

USER AUTHENTICATION

- Passwords
  - There are three common ways to guess a password.
    - 2. Another way is to use brute force, trying enumeration—or all possible combinations of valid password characters (letters, numbers, an punctuation on some systems)—until the password is found
    - 3. The third, common method is dictionary attacks where all words, word variations, and common passwords are tried

USER AUTHENTICATION

- Passwords
  - One-Time Passwords (OTP) can also be used
  - OTPs are also used in two-factor authentication

USER AUTHENTICATION

- Biometrics
  - Yet another variation on the use of passwords for authentication involves the use of biometric measures.
  - Palm- or hand-readers are commonly used to secure physical access—for example, access to a data center.
  - These readers match stored parameters against what is being read from hand-reader pads.

USER AUTHENTICATION

- Biometrics
  - The parameters can include a temperature map, as well as finger length, finger width, and line patterns.
  - Fingerprint readers have become accurate and cost-effective.
  - These devices read finger ridge patterns and convert them into a sequence of numbers

THE END