ملخص النص

Worms, viruses, and bacteria are all types of malicious software. Worms are self-replicating programs that spread across networks, consuming resources and potentially causing network shutdowns. Viruses require a host program to replicate and spread by inserting copies of themselves into other programs. Bacteria are not mentioned in the provided text. Infected programs cause system harm by self-replicating exponentially, consuming system resources. Intrusion detection uses audit records to identify unauthorized activity. Firewalls control network traffic, allowing or blocking connections. Profiles define normal system behavior to detect anomalies. Audit records track user logins, locations, and logon/off actions; program executions (frequency, resource use); and file access activities (read, write, create, delete, append). This text describes fundamental cybersecurity concepts: user identification, authentication (verifying user identity), authorization (assigning access rights), access control (enforcing those rights), confidentiality (protecting secrets), and data integrity (detecting unauthorized data changes). Data transmission errors occurred. Non-repudiation ensures data origin and delivery can be proven. Denial-of-service attacks involve resource takeover. Authentication methods include biometric verification (fingerprints, voice) and possession of physical items (keys, badges). Access control regulates user access to resources based on security policies. Capability lists define a subject's access rights to specific objects, with each subject having its own list. Access rights specify how a subject can access an object.

Audit trails record important security events for later review. Audit requirements include automatic collection of security-sensitive activity data, storage in a standard format, automatic record creation without administrator intervention, minimal performance impact, and secure audit log protection. One-time passwords (OTPs) are also mentioned. This document describes single-use passwords from token cards and one-way hash functions used for error detection in data transmission. The hash function requirements include handling variable-sized data blocks, producing a fixed-size digest, and ease of implementation. Finally, it defines a client as a user-interactive program and operating system that prepares access requests. A server provides services (e.g., databases, image processing) and responds only to client requests. Encrypted messages and digital signatures ensure message confidentiality and sender authentication, respectively. Decryption verifies the signature's validity. Message digests provide a concise representation of data to detect changes. Access Control Lists (ACLs) specify access rights for subjects. Anomaly records flag deviations from normal behavior. Encryption converts data into an unreadable ciphertext, recoverable only with decryption and a key; the original data is plaintext. Asymmetric encryption uses separate keys for encryption and decryption, while symmetric encryption uses the same key for both. Public-key cryptography involves a private key known only to the user and a public key available to everyone.