

Security

What and How



Password Strength

- *There are only two types of companies: Those that have been hacked and those that will be hacked.* – Robert S. Mueller III, former Director of the FBI.
- How secure is your password?
<https://www.passwordmonster.com/>
- US president's nuclear briefcase passcode.
- Marine password policy: at least 12 characters long, mix of number, special chars, change it every 3 months. Most write the passcode in a note and attach it to the device.

Security

- Privacy
- Authentication
- Authorization
- Integrity
- Non-repudiation
- Availability
- Audit and forensics

Privacy

- **Privacy** is the right of individuals to control their personal information and to ensure that it is not disclosed to unauthorized parties.
- Information security measures, such as **encryption and access controls**, help to protect individual privacy and prevent data breaches.

Authentication

- **Authentication** is the process of verifying the identity of users, devices, or systems.
- This is achieved through various methods, **including passwords, biometrics, and tokens**.
- Authentication ensures that only authorized entities have access to sensitive information and systems.

Authorization

- **Authorization** is the process of determining what actions a user or system can perform once they have been authenticated.
- This includes **access controls**, such as role-based access control and mandatory access control, which ensure that users only have access to the resources and data they need to perform their tasks.

Integrity

- **Integrity** refers to the protection of data from unauthorized modification, deletion, or alteration.
- This is achieved through measures such as **digital signatures and checksums**.

Non-repudiation

- **Non-repudiation** is the assurance that a sender of a message cannot deny having sent the message.
- This is achieved through **digital signatures and certificates**, which provide a **tamper-evident record** of transactions and communications.

Availability

- **Availability** refers to the accessibility and usability of information and systems.
- This includes ensuring that systems are operational and accessible when needed, and that data is retrievable and usable.

Audit

- **Audit** is a formal process of evaluating an organization's information systems to ensure compliance with security **policies** and identify potential vulnerabilities.
- The audit process typically includes planning, gathering system and user **activity data** (all activities are **logged**), identifying vulnerabilities through scanning or testing, and generating a report with findings and recommended improvements.

Forensics

- **Digital forensics** is the practice of collecting, preserving, and analyzing digital evidence to investigate and understand security incidents or cybercrimes.
- Implementation of forensics involves several stages: data acquisition (creating an exact copy of the affected systems), integrity preservation (ensuring evidence is not altered), in-depth analysis (**examining files, logs, and metadata**), and reporting (documenting the findings for legal or organizational action).

Example: Messages Between Alice and Bob


- **Privacy**: Alice wants to ensure that only Bob can read the message, and no one else can access it. She uses encryption to protect the message, so even if an unauthorized party intercepts it, they won't be able to understand its contents.
- **Authentication**: Before sending the message, Alice verifies Bob's identity through a digital certificate or password to ensure she's sending it to the right person.
- **Authorization**: Alice checks Bob's access level and ensures he has the necessary clearance to receive the message.
- **Integrity**: Alice uses a digital signature or checksum to ensure the message isn't tampered with or altered during transmission. When Bob receives the message, he can verify its integrity using the same digital signature or checksum.
- **Non-repudiation**: Alice uses a digital signature that includes a timestamp and her unique identity, so Bob can verify the message came from her and when it was sent. This prevents Alice from denying she sent the message.
- **Availability**: Alice ensures the message is stored on a reliable server and transmitted through a secure channel, so Bob can access it when needed.

Audit and Forensics

- **Audit:** Alice wants to ensure that systems are protected against unauthorized access, data breaches, and other cyber threats. Both security policies and system/user activity data (**logs**) are used in the audit process.
- **Forensics:** When an attack happens, Alice wants to find out how an attack occurred, what were affected, and who is responsible. System/user activity data (**logs**) are important in digital forensics.



Malware: Malicious Software

- Virus: A self-replicating program that attaches itself to a file or program on a computer.
 - Worm: A self-replicating program that can travel from computer to computer **without needing to be sent as an attachment.**
- 

More Forms...

- Trojan: A program that appears to be legitimate but contains malicious code.
- Spyware: A program that secretly monitors and collects personal information about a user.
- Adware: A program that displays unwanted advertisements on a computer, often in the form of pop-ups or banners.
- Ransomware: A program that encrypts a user's files and demands payment in exchange for the decryption key.
- ...

How Can Malware Break Into?

- **Vulnerable System:** Security bugs vulnerabilities in software or operating systems or **outdate** systems allowing malware to gain access.
- **Download and Install Infected Software:** Downloading software from untrusted sources, which may bundle malware.
- **Social Engineering (Phishing):** Tricking users into revealing login credentials or installing malware through emails, messages, or social media.
- **Weak Passwords:** Using easily guessable passwords, allowing hackers to gain access.

Antivirus? No for Me

- It **cannot** prevent malware from infecting your system because it cannot detect any **NEW** malware (virus or worms)
- And it comes with the cost of anti virus software to provide real time protection. Two big costs are
 - Subscription fee
 - Resource utilization: **20%** performance lose

How to Protect

- Keep your system and software up-to-date - simply turn on **auto system updates**.
- **Don't download software** from untrusted sources. Be cautious with emails and messages and avoid suspicious links or attachments.
- Use **strong, unique passwords** and enable two-factor authentication.
- Don't leak your password to untrusted ones.
- **Have multiple data copies.**

DOS and DDOS

- A DOS (Denial of Service) attack is a type of cyberattack where an attacker attempts to make a computer or network resource unavailable by flooding it with traffic or exploiting a vulnerability.
- A DDOS (Distributed Denial of Service) attack is a type of DOS attack where the traffic or requests come from **multiple sources**, often compromised devices or bots.
- Protection
 - Network infrastructure: **Firewalls** and Intrusion Prevention Systems (IPS)
 - Content Delivery Networks (CDNs)
 - Network monitoring
 - Auditing.

Security Policies

- Can you play video games on a company computer?
- Is your email on a company computer private?
- Computer security policies outline the rules and guidelines for employees to follow.
- It is not uncommon for companies to monitor and inspect employee computers and email accounts.