Principles of Security

-Sanketh Iyer

Introduction

In the context of network security, several principles are crucial to safeguarding data and systems from unauthorized access and malicious attacks. This presentation explores four essential security principles: Confidentiality, Authentication, Integrity, and Non-Repudiation.

Confidentiality

Confidentiality ensures that sensitive information is accessed only by authorized individuals. It is about keeping data private and preventing unauthorized disclosure or access.

Examples of Confidentiality Measures

1. Encryption: Protecting data using cryptographic algorithms to make it unreadable to unauthorized users.

2. Access Controls: Restricting access to sensitive data based on user authentication and authorization levels.

3. Data Classification: Labeling data based on sensitivity to control access and handling.

4. Non-disclosure Agreements (NDAs): Legally binding agreements to prevent data disclosure to unauthorized parties.

"The lab accidentally faxed your test results to the wrong doctor's office. You'll get a bill for a second opinion."

Question - Confidentiality

What are some measures organizations can implement to ensure the confidentiality of sensitive data?

Answer - Confidentiality

Organizations can implement various measures to ensure confidentiality, including encryption, access controls, data classification, and the use of non-disclosure agreements (NDAs).

Authentication

Authentication is the process of verifying the identity of users or entities attempting to access a system or resource. It ensures that only authorized users gain entry.

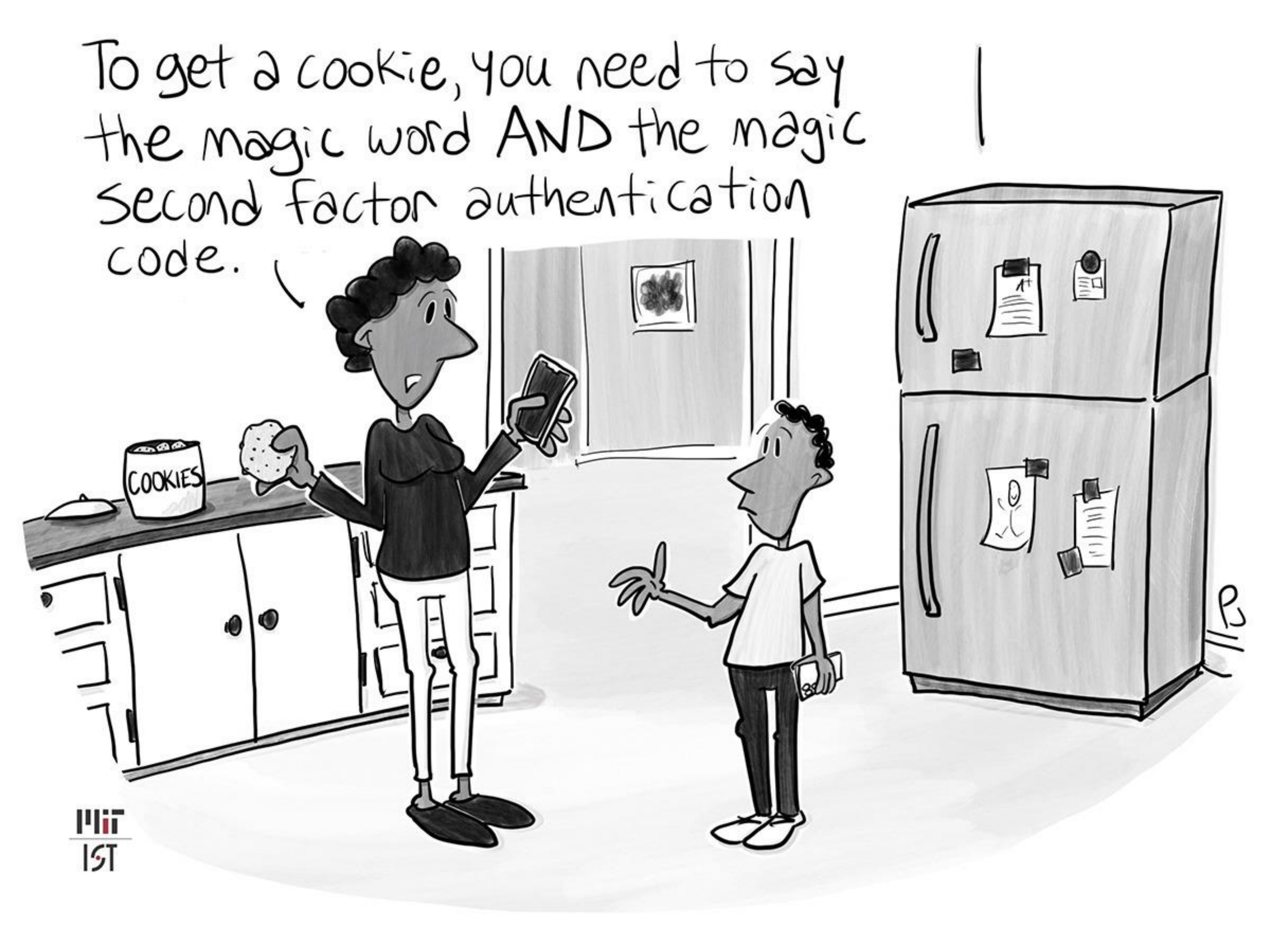
Examples of Authentication Methods

1. Passwords: Traditional method requiring users to enter a secret passphrase.

2. Biometrics: Using unique physical or behavioral characteristics for identification.

3. Multi-Factor Authentication (MFA): Combining multiple authentication factors for increased security.

4. Smart Cards: Secure tokens storing user credentials for authentication.

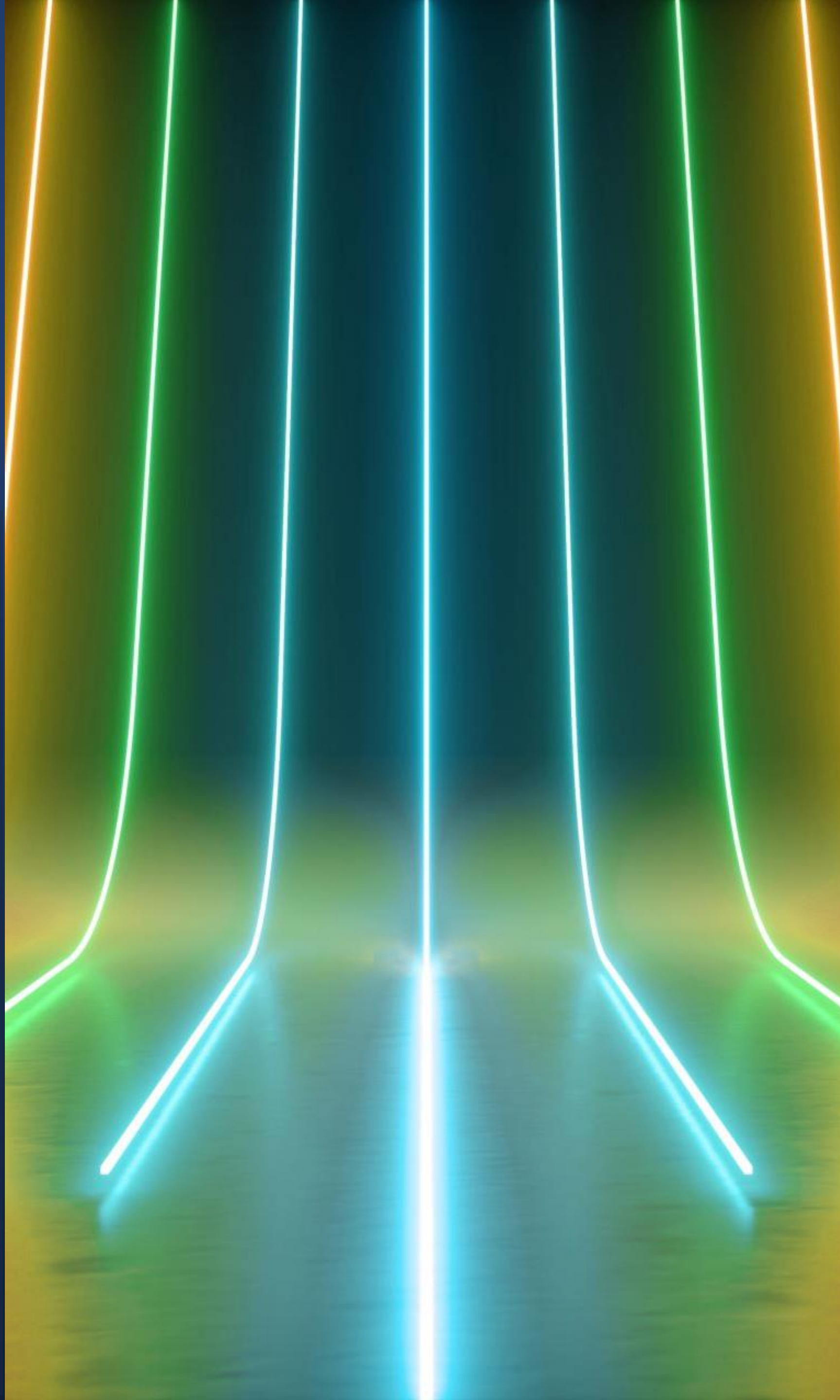

To get a cookie, you need to say the magic word AND the magic second factor authentication code.
COOKIES
MIT IST

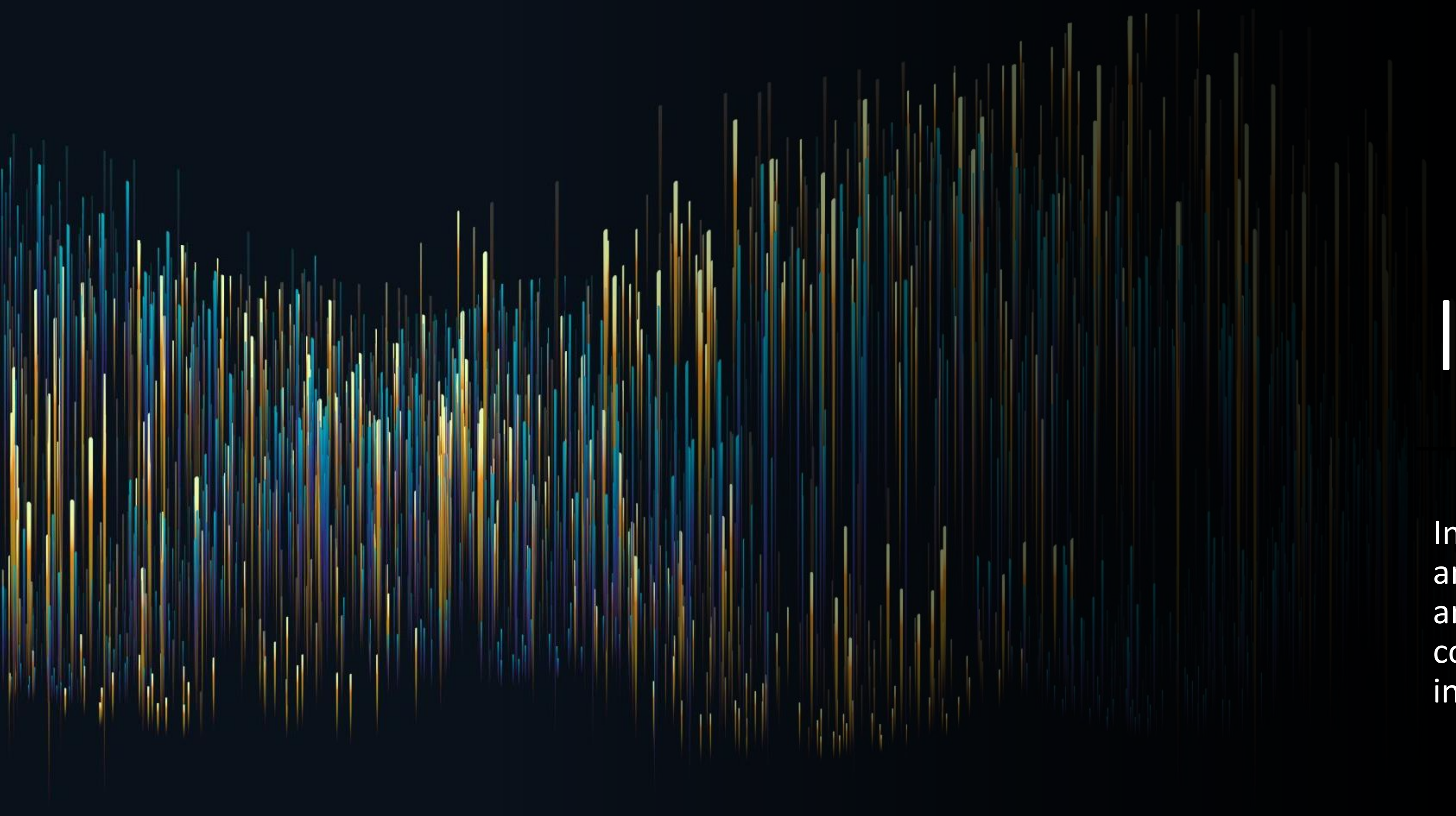
Question - Authentication

What are some examples of authentication methods used to verify user identity?

Examples of authentication methods include passwords, biometrics, multi-factor authentication (MFA), and smart cards.

Answer - Authentication





Integrity

Integrity ensures that data remains accurate and unaltered during storage, transmission, and processing. It is about maintaining the consistency and trustworthiness of information.

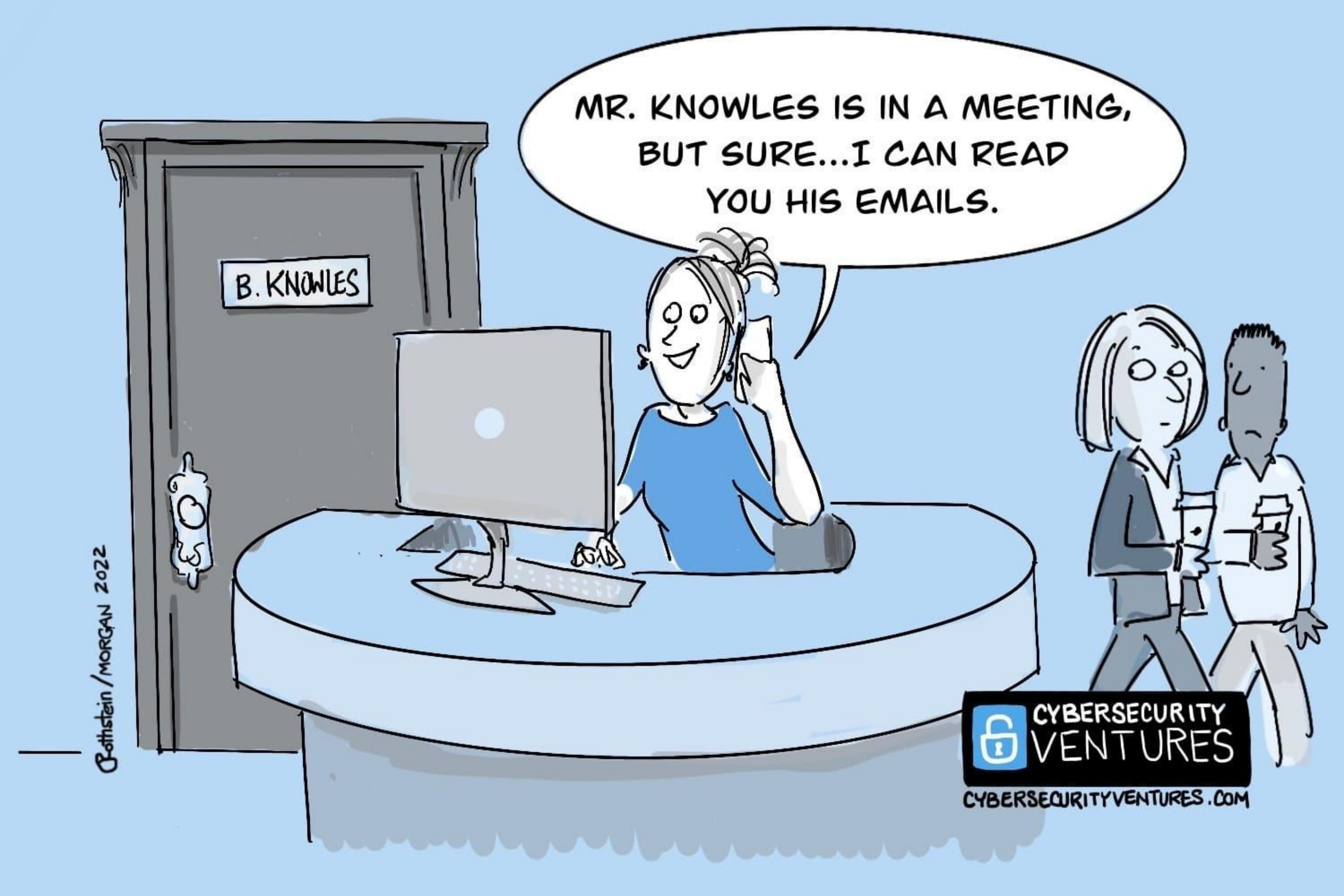
Examples of Integrity Measures

1. Checksums: Verifying data integrity by comparing checksum values before and after transmission.

2. Digital Signatures: Using cryptographic signatures to verify the authenticity and integrity of messages or files.

3. Error-checking Algorithms: Detecting and correcting errors in data to maintain accuracy.

4. Version Control: Managing changes to data and ensuring the integrity of the latest version.


MR. KNOWLES IS IN A MEETING, BUT SURE...I CAN READ YOU HIS EMAILS.
B. KNOWLES
Rothstein/MORGAN 2022
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Question - Integrity

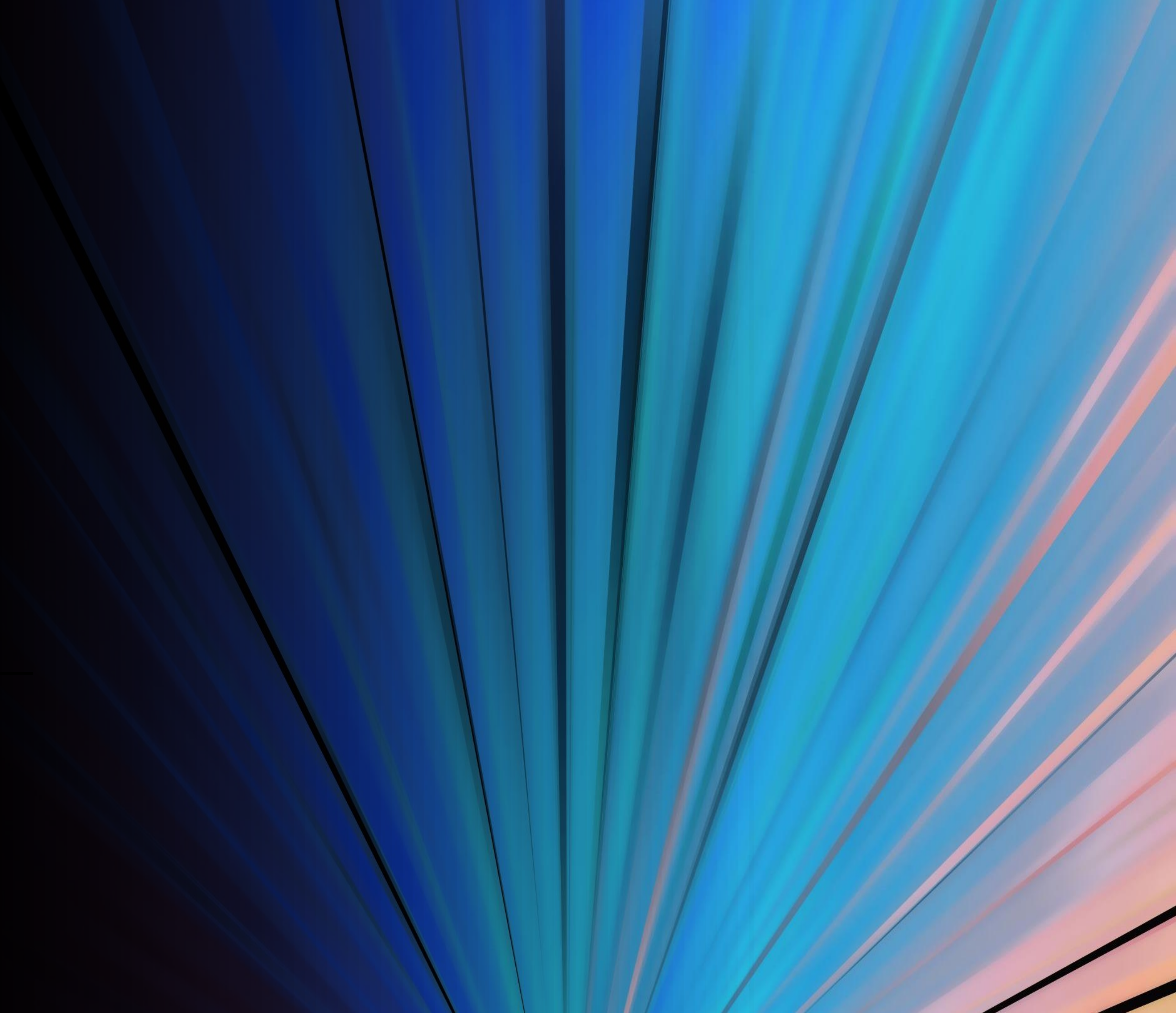
How can organizations verify the integrity of data during transmission?

Answer - Integrity

Organizations can verify data integrity during transmission using techniques such as checksums, digital signatures, and error-checking algorithms.

Non-Repudiation

Non-repudiation prevents individuals from denying their actions or transactions. It ensures that parties involved in a communication or transaction cannot refute the authenticity of their involvement.



Examples of Non-Repudiation Measures

- 1. Digital Signatures: Providing evidence of the authenticity and integrity of digital documents or messages.
- 2. Timestamps: Recording the time and date of a transaction or event to prevent denial of occurrence.
- 3. Audit Trails: Tracking and recording all activities performed by users to establish accountability.
- 4. Legal Agreements: Using legally binding contracts to prevent parties from denying their actions.

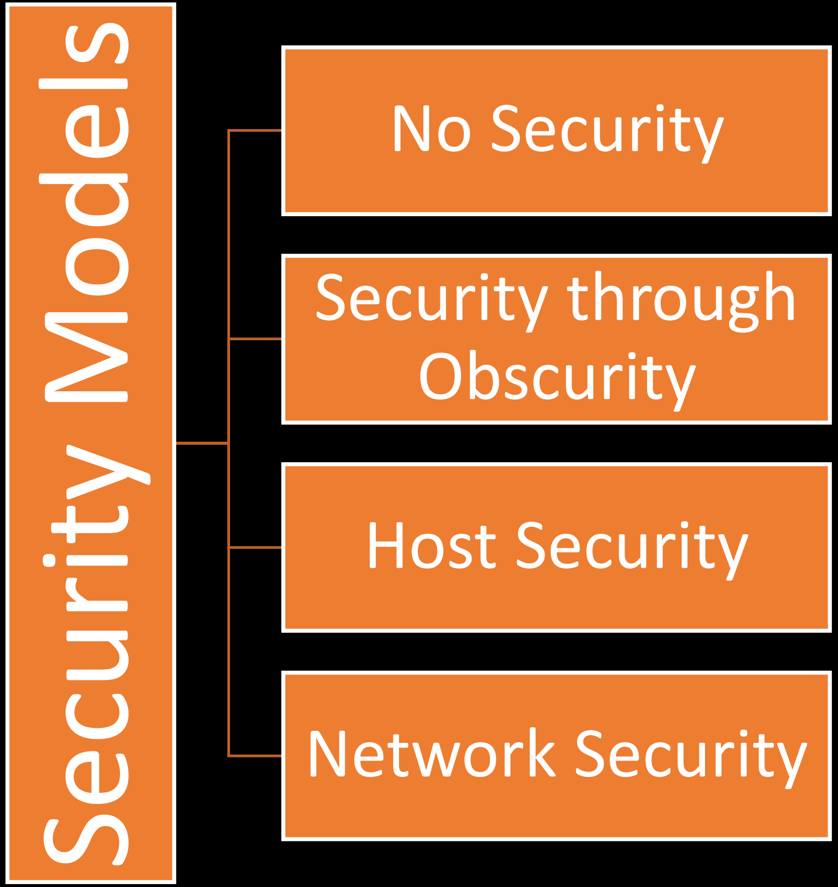
Question - Non-Repudiation

How does non-repudiation prevent parties from denying their actions or transactions?

Answer - Non-Repudiation

Non-repudiation ensures that parties involved in a communication or transaction cannot refute the authenticity of their involvement through methods such as digital signatures, timestamps, audit trails, and legal agreements.

Security Models



Security Models

- No Security
- Security through Obscurity
- Host Security
- Network Security

A Model for Network Security

- A comprehensive network security model involves the integration of various security principles and technologies.
- Such a model typically includes the application of encryption, firewalls, intrusion detection systems, access controls, and secure communication protocols.
- Remember, No security model can do it all.

Questions and Feedback