Principles of Cryptography

Lecture 1

Safety Vs Security

Safety is also related to security in that the lack of security may pose a safety risk (absence of IT security may lead to a system that is compromised which in turn may not be safe anymore).

SAFETY:

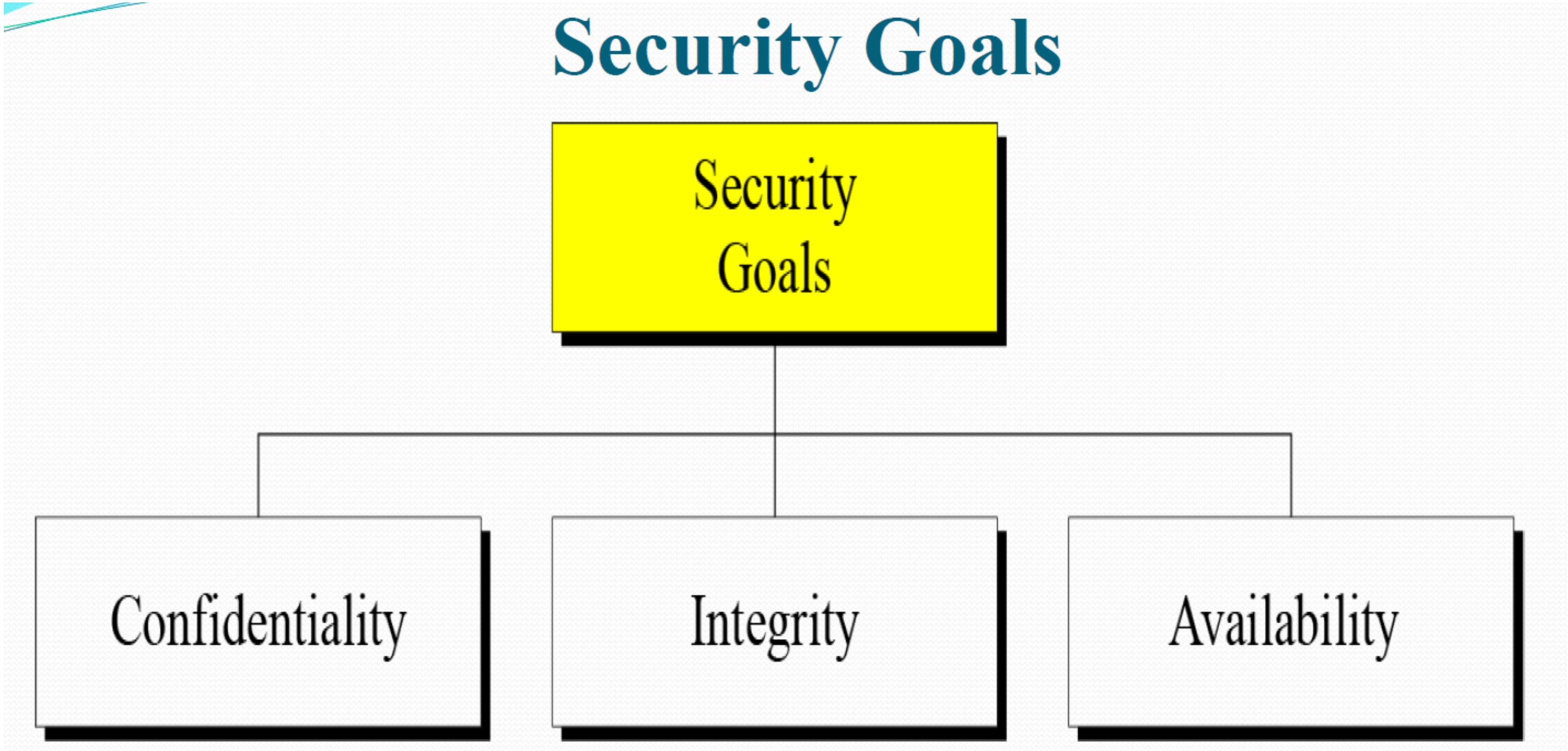
- **To be safe requires measures to prevent accidents (cause harm to humans or machines).**
- **Examples: Redundant systems to guarantee availability, fire extinguisher.**

SECURITY:

- **Security requires measures to prevent fraud, crime, illegal activities.**
- **Examples: Firewalling, security policy, use of encryption.**

Security is a necessary but not sufficient prerequisite for achieving safety (a system without security is probably unsafe, but a system with security is not necessarily safe).

What are the three 3 aspects of security?



Security Goals

Security Goals

Confidentiality

Integrity

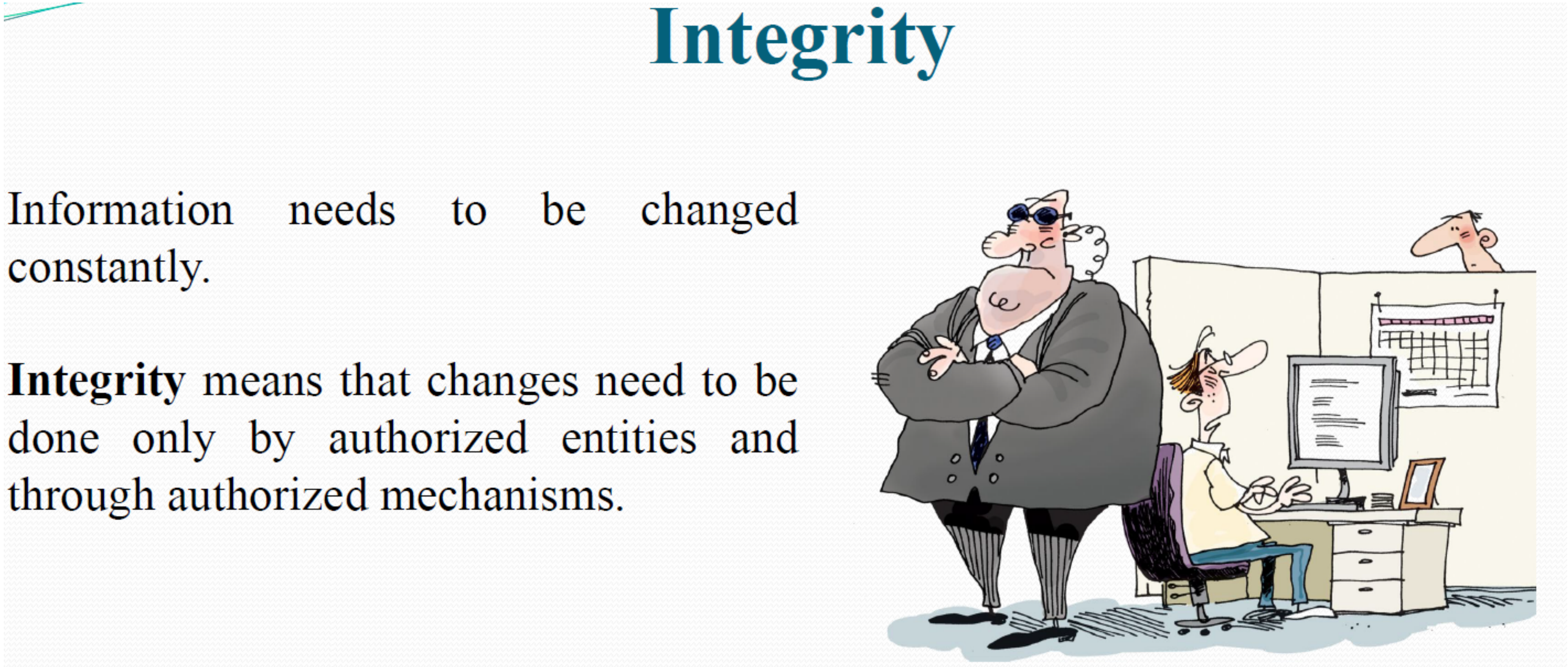
Availability

Confidentiality

Confidentiality is very important of information security.

We need to protect our confidential information.

An organization needs to guard against those malicious actions.



Integrity

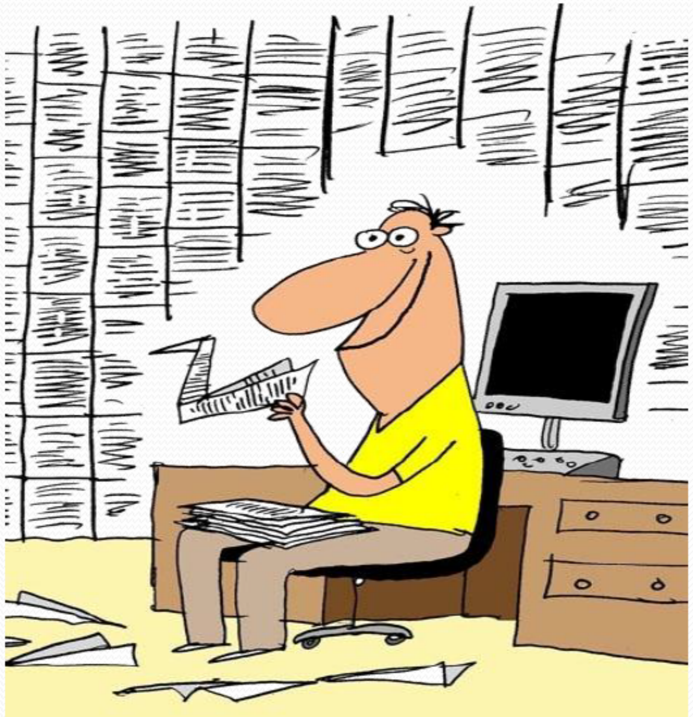
Information needs to be changed constantly.

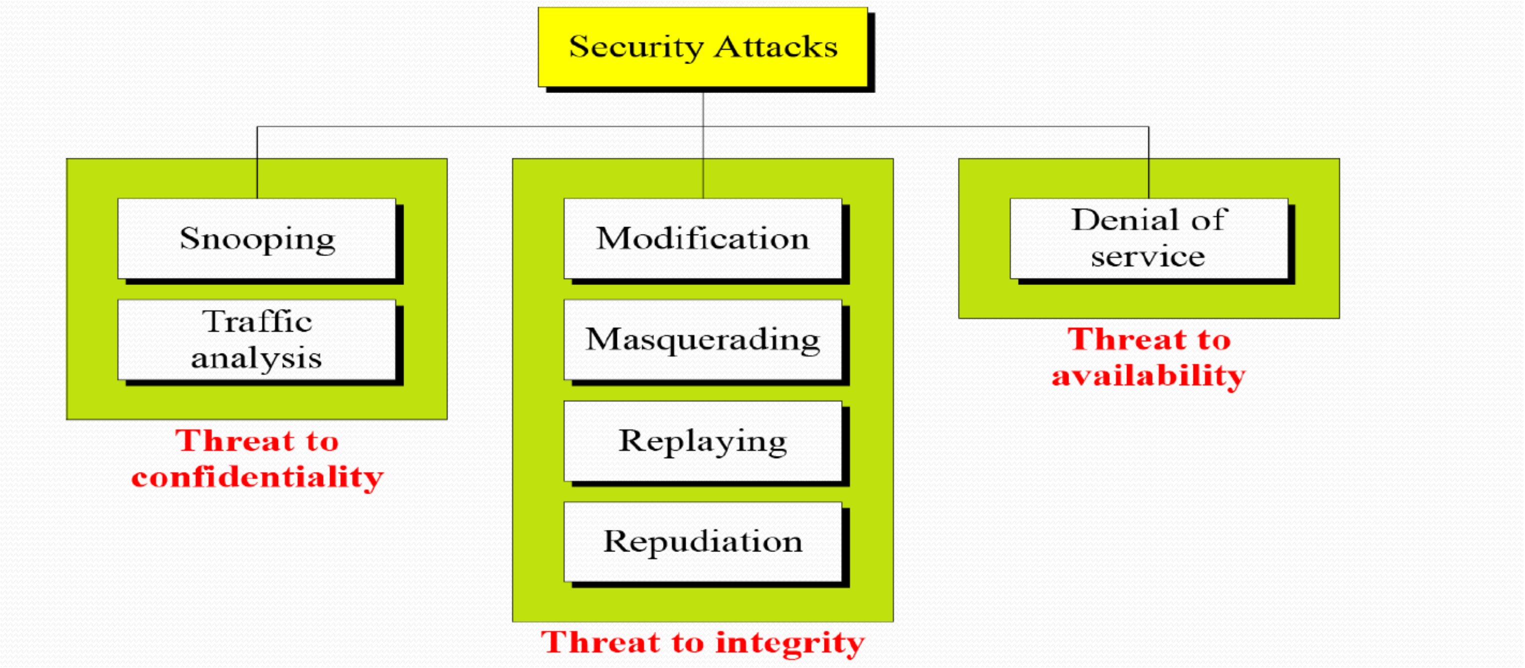
Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Availability

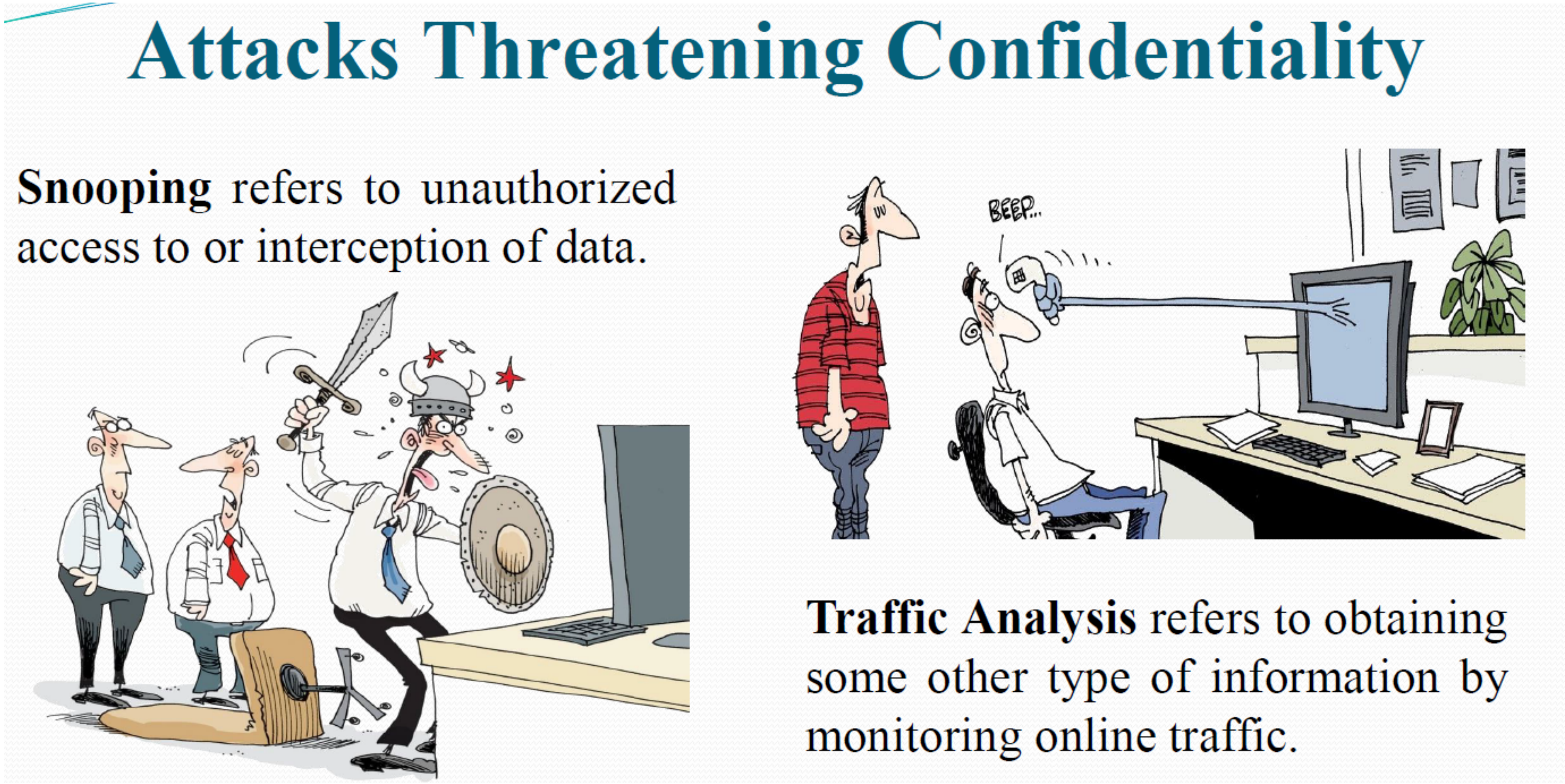
The information created and stored by an organization needs to be available to authorized entities.

Information needs to be constantly changed.





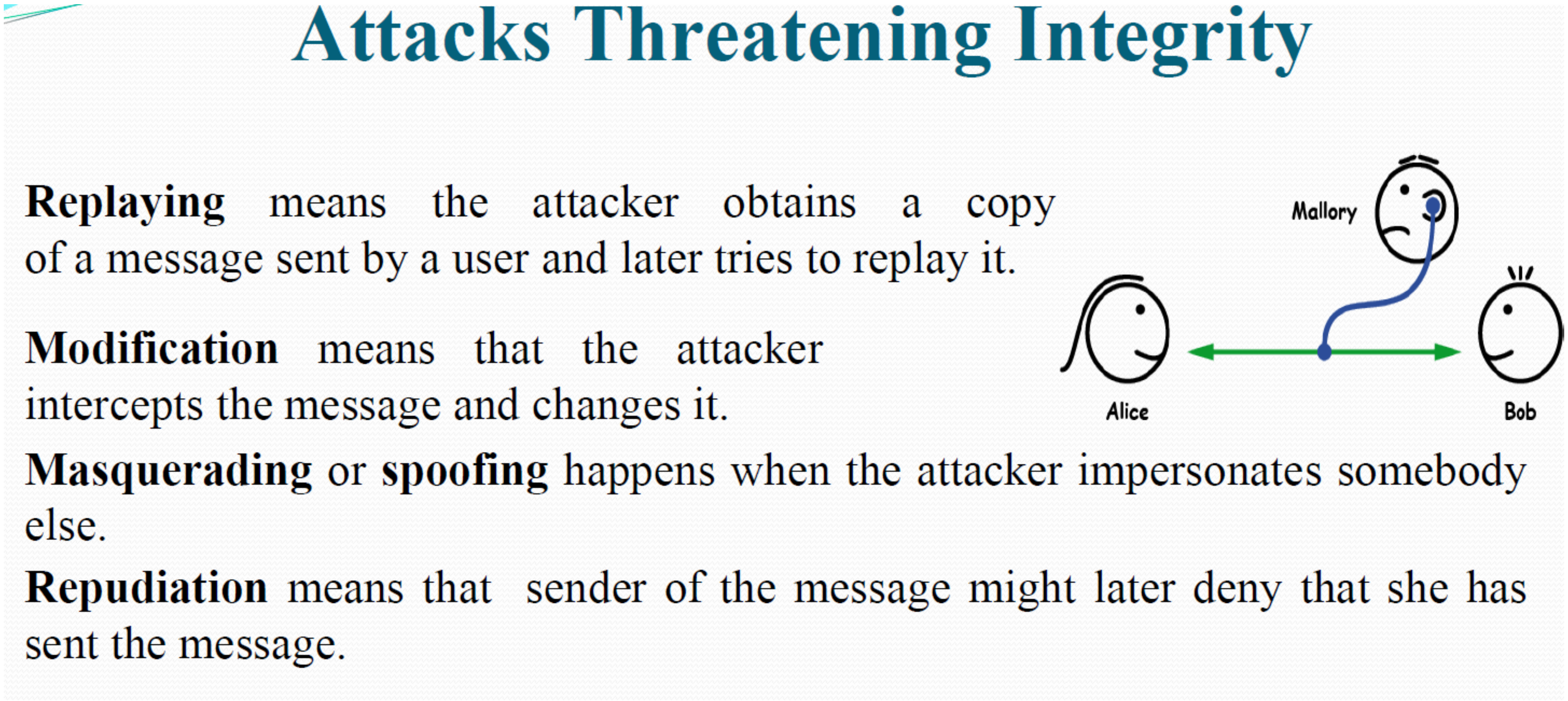
- **Active attack**: An attempt to alter system resources or affect their operation.
- **Passive attack**: An attempt to learn or make use of information from the system that does not affect system resources.



Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

Traffic Analysis refers to obtaining some other type of information by monitoring online traffic.



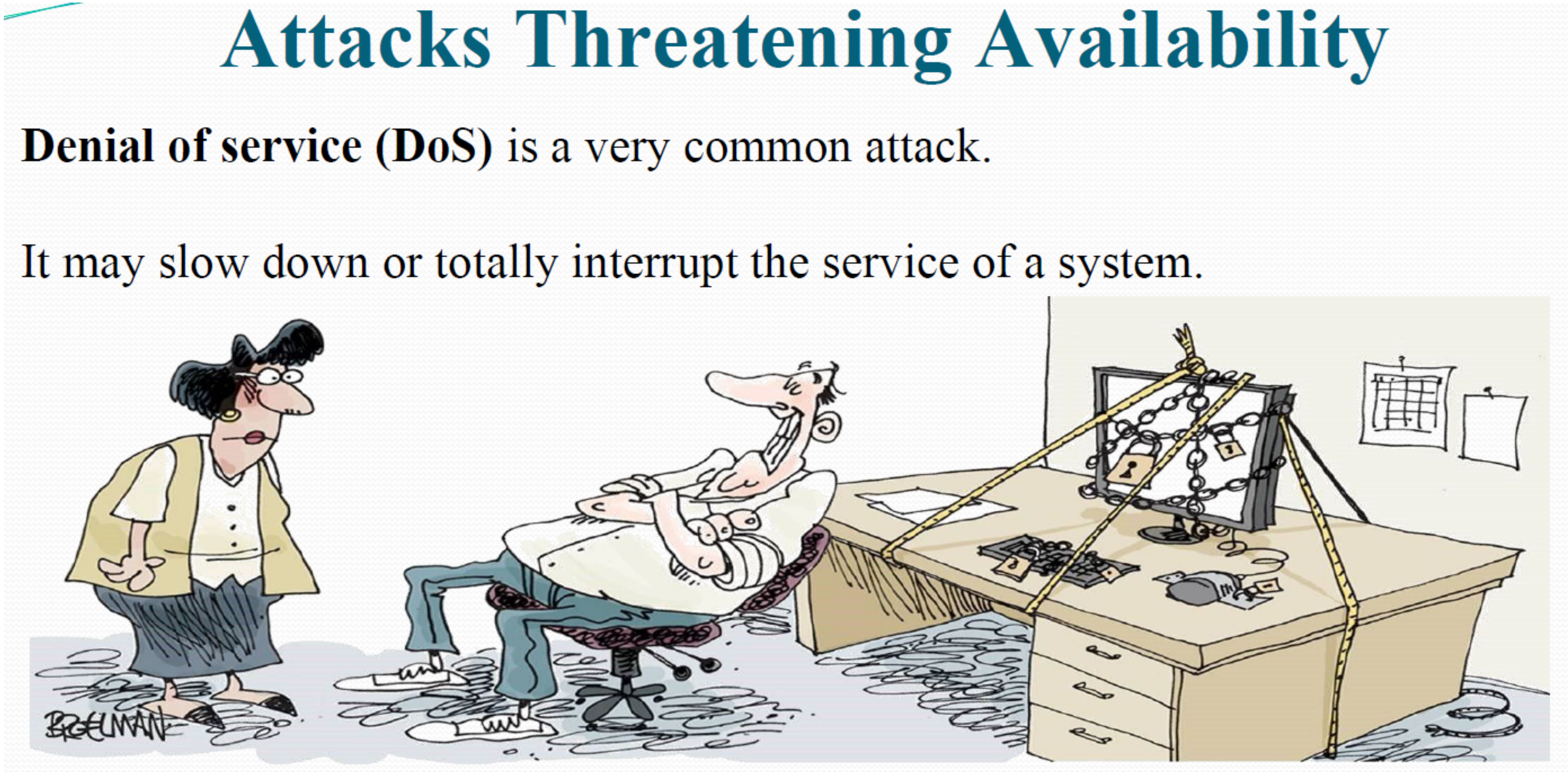
Attacks Threatening Integrity

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Modification means that the attacker intercepts the message and changes it.

Masquerading or **spoofing** happens when the attacker impersonates somebody else.

Repudiation means that sender of the message might later deny that she has sent the message.



Attacks Threatening Availability

Denial of service (DoS) is a very common attack.

It may slow down or totally interrupt the service of a system.

Digital Security

- **COMPUTER SECURITY - generic name for the collection of tools designed to protect data and to thwart hackers.**
- **NETWORK SECURITY - measures to protect data during their transmission.**
- **INTERNET SECURITY - measures to protect data during their transmission over a collection of interconnected networks.**

Risks Involved in Digital Security

- **Vulnerabilities**
- **Phishing**
- **Computer Virus**
- **Computer Worms**
- **Sniffers**
- **Hacking**

Vulnerability: In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. To be vulnerable, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

Phishing: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

PHISHING TECHNIQUES

- **Link manipulation**
- **Filter evasion**
- **Phone phishing**

Computer Virus: A computer virus is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability.

Computer Worms: A computer worm differs from a computer virus in that a computer worm can run itself. A computer worm can spread without a host program, although some modern computer worms also use files to hide inside. It can damage your files and operation systems. It can spread rapidly on your system or to other computers on network.

Sniffers: Sniffers is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. Hackers can sniff your packets with some software or hardware and they can steal your credit card numbers, passwords or e-mails.

Hacking: In common usage, a hacker is a stereotypical person who breaks into computers and computer networks, either for profit or motivated by the challenge.

HACKING TECHNIQUES:

- **Vulnerability scanner**
- **Password cracking**
- **Packet sniffer**
- **Spoofing attack**
- **Social engineering**
- **Trojan horses**
- **Viruses**

Avoid Risks In Digital Security

- Apply antivirus software's for system security.
- Apply firewall and other network security tools (IDPS) for hacker attacks.
- Use network security protocols. (IPsec,SSL, TLS)
- Apply UTM systems. (Unified Threat Management)
- Adopt Behavioral based Security
- Apply DLP.
- ACL on firewall/ network/applications
- Enforce strong password policy.
- User Awareness
  - We shouldn't open every file.
  - When we receive an email we should be careful.
  - We shouldn't share our personal information on internet.
  - We should be very careful in sharing files when we chat.

Cryptography

Cryptography (or *cryptology)* is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electronic commerce.

Cryptographic Terms:

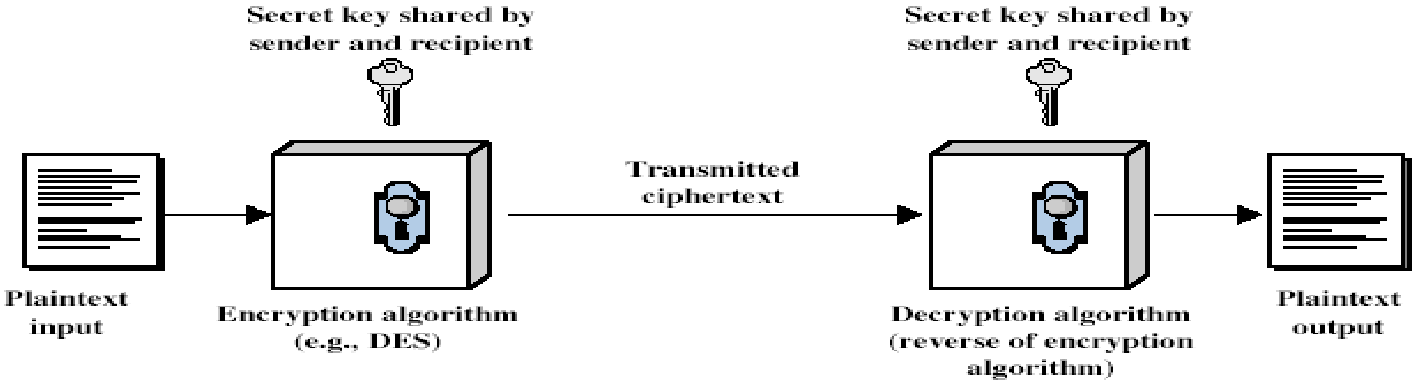
- Cryptography - study of encryption principles/methods
- Cryptanalysis (code breaking) - study of principles/ methods of deciphering ciphertext *without* knowing key
- Cryptology - field of both cryptography and cryptanalysis
- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext

Symmetric Key Encryption (Private Key Cryptography)

- Sender and receiver share a single common key.
- All classical encryption algorithms are private-key.
- Was only type prior to invention of public-key in 1970's and by far most widely used.
- If this key is disclosed communications are compromised.
- Symmetric, parties are equal, hence does not protect sender from receiver forging a message & claiming that it is sent by sender.

Asymmetric Key Encryption (Public Key Cryptography)

- Probably most significant advance in the 3000 year history of cryptography.
- Uses two keys – a public & a private key.
- Uses clever application of number theoretic concepts to function.
- Complements rather than replaces private key cryptography.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Mathematical Background

- Modular

- Finite fields

- Probability

Modular arithmetic

Modular arithmetic is an important concept in encryption. It involves performing arithmetic operations on numbers within a fixed range, known as the modulus. In encryption, the modulus is often a prime number or a power of a prime number.

The modulus determines the range of possible values for the encrypted message. For example, if the modulus is 26, the possible values range from 0 to 25, representing the 26 letters of the alphabet. This is commonly used in encryption techniques like the Caesar cipher or the Vigenère cipher.

When encrypting a message using modular arithmetic, each letter or character is assigned a numerical value. The encryption process involves performing mathematical operations, such as addition or multiplication, on these numerical values and taking the remainder when divided by the modulus. The resulting remainders are then converted back into letters or characters to form the encrypted message.

For example, let's consider the encryption of the letter 'A' using a modulus of 26. If 'A' is assigned the numerical value of 0, and we add 3 to it, the result is 3. Taking the remainder when divided by 26, we get 3. So, 'A' encrypted with a shift of 3 becomes 'D'.

Modular arithmetic is also used in more advanced encryption algorithms, such as the RSA algorithm. In RSA, modular arithmetic is used to perform calculations involving large prime numbers, which are crucial for the security of the encryption.

In summary, modular arithmetic is a fundamental concept in encryption that allows for the transformation of plaintext into ciphertext using mathematical operations within a fixed range determined by the modulus. It is used in various encryption techniques and algorithms to ensure the confidentiality and security of sensitive information.

Features of prime numbers in encryption:

1. Security

   : Prime numbers play a crucial role in encryption algorithms, such as RSA, because they provide a high level of security. The difficulty of factoring large numbers into their prime factors makes it computationally infeasible to break the encryption .

2. Key Generation

   : Prime numbers are used in the generation of encryption keys. In asymmetric encryption, two large prime numbers are multiplied together to create the encryption key. The prime numbers remain hidden, and only someone who knows the prime factors can decrypt the message [1].

3. Uniqueness

   : Prime numbers are unique and have no divisors other than 1 and themselves. This property ensures that the encryption keys generated using prime numbers are unique and not easily guessable.

4. Trapdoor Function

: Prime numbers are used in trapdoor functions, which are mathematical functions that are easy to compute in one direction but difficult to reverse. This property allows for secure encryption and decryption processes.

5. Increased Security

: The use of multiple prime numbers in encryption algorithms, such as RSA, enhances the security of the encryption. By using more prime numbers, the difficulty of factoring the encryption key increases, making it harder for unauthorized individuals to decrypt the message

In summary, prime numbers are essential in encryption due to their unique properties, security features, and their role in generating encryption keys. They provide the foundation for secure communication and protect sensitive information from unauthorized access.

Probability:

Probability in encryption is used to ensure that the generated numbers are sufficiently random and unpredictable.

1. Random Number Generation

: In encryption, random numbers are often used for key generation, initialization vectors, and other cryptographic purposes. Probability is used to ensure that the generated numbers are sufficiently random and unpredictable. Random number generators based on modular arithmetic algorithms use probability to distribute the numbers evenly across the range of possible values.

2. Cryptographic Security

: Probability is used to analyze the security of encryption algorithms. Cryptanalysts use probability theory to assess the likelihood of successfully breaking an encryption scheme. By analyzing the probability of different events occurring, such as the occurrence of certain patterns or the likelihood of finding a collision, they can evaluate the strength of the encryption algorithm.

3. Cryptanalysis

   : Probability is also used in cryptanalysis, the study of breaking encryption. Cryptanalysts use probability to analyze the likelihood of certain events or patterns occurring in encrypted data. By understanding the probabilities associated with different encryption techniques, they can develop attacks or exploit weaknesses in the encryption algorithm.

4. Error Detection and Correction

   : In some encryption schemes, modular arithmetic is used for error detection and correction. Probability is used to assess the likelihood of errors occurring during transmission or storage of encrypted data. Techniques like error-correcting codes use probability to detect and correct errors, ensuring the integrity of the encrypted information.

In summary, probability is an important aspect of modular arithmetic in encryption. It is used for random number generation, assessing cryptographic security, analyzing encryption algorithms, and error detection and correction. Probability helps ensure the strength and reliability of encryption schemes.