Topic 1 - Introduction

Eric Casanovas

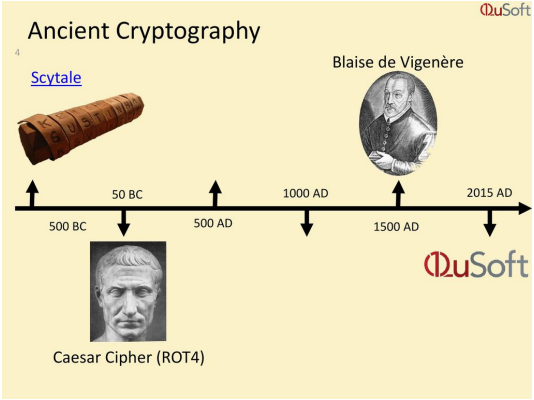
Universitat d'Andorra

9th February, 2022

Ancient History I

- Since ancient times, humans have sought forms of private communication.
- The main applications were for diplomacy or for military purposes.
- However, all "historical" cryptosystems are broken nowadays.
- We didn't know the properties needed to achieve the purpose.
- These ancient cryptosystems are breakable thanks to the computational power of today's PC, but not for human brute-force.

Ancient History II

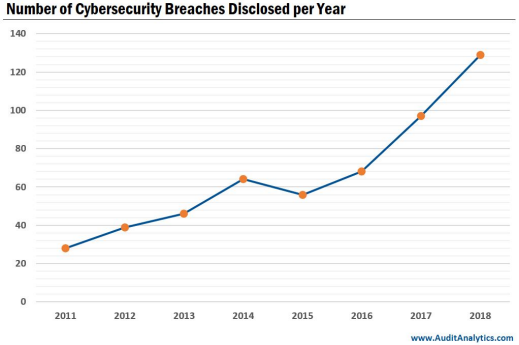


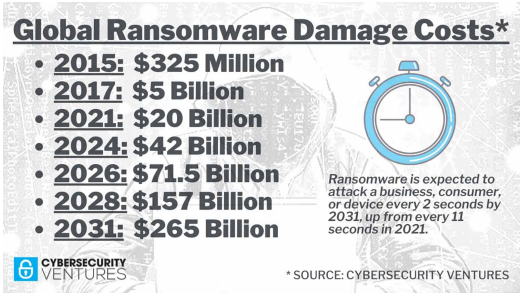
Recent History I

- In 1918 was created the enigma machine, which was used by the German army before and during the WWII.
- However, in 1939 Alan Turing broke many German variations of the enigma machine, which was very important for the allied victory.
- In 1970s we can consider the birth of cybersecurity when Bob Thomas creates a virus "the Creeper" that could move across ARPANET's network, leaving a message wherever it went.
- In 1987 was the birth year of commercial antivirus.
- In 1990s "The world goes online" and organised crime entities saw this as a potential source of revenue and started to steal data from people and governments.

Recent History II

- Cybercrime increased right up to the present day and it doesn't look like the trend is going to stop.



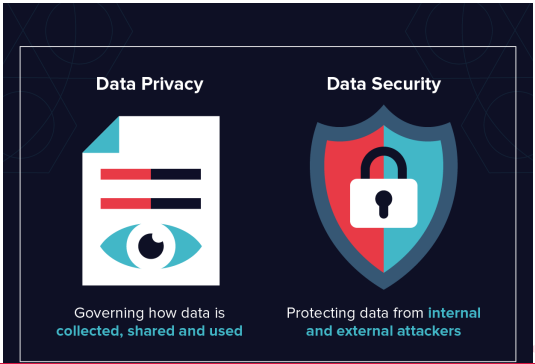


Definition

- Cyber + Security
- Cyber: Related to computers.
- Security: The state of being free from danger or threat.

Main purposes of cybersecurity

- Secure communications
- Secure data
- Privacy
- Anonymization (?)



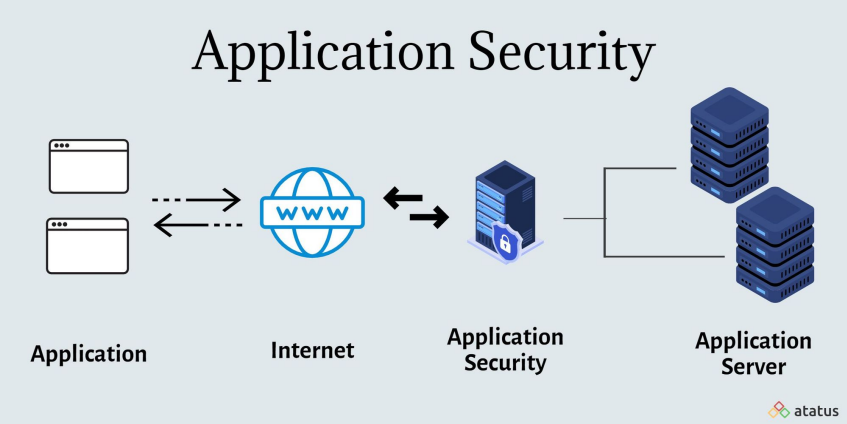
Types of cybersecurity

- Application Security
- Network Security
- Data Security

Application security I

- We have to take care about the technologies used in applications
- Security of communications in applications (i.e. DB accesses)
- Maintain the applications up to date
- Attack examples:
  - DDoS
  - XSS
  - SQLInjection
  - Privilege escalation

Application security II



Network security I

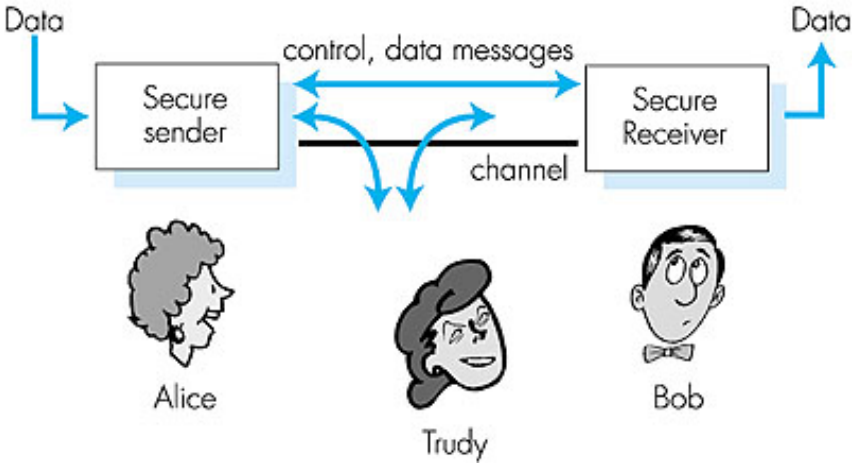
- Unauthorized access to an organization network
- We can divide in 2 attacks:
  - Active: encrypting, damaging data...
  - Passive: monitoring, steal data...
- Attack examples:
  - DDoS
  - Man in the Middle
  - Unauthorized access (worms, trojans...)

Network security II

Data security I

- The data has to be secured before sending it over insecure networks (i.e. Internet)
- This is possible thanks to **Cryptography**
- Cryptography: The study of secure communications techniques that allow only the sender and intended recipient to view the contents and check the integrity of a message
- Attack examples:
  - Brute force
  - Rainbow tables

Data security II



In sum

Encryption I

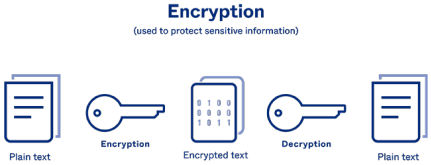
- According to Wikipedia the encryption is the process of converting the original representation of the information, known as plaintext, into an alternative form known as ciphertext
- Usually is used a key to do the transformation between the plain text and the ciphertext
- To encrypt we can use:
  - Algorithms of transformation
  - Keys (Symmetric or asymmetric)

Encryption II

Use Cases:

- Send messages secure way
- Protect databases
- Protect hard drives data

Encryption III



Encryption IV

Examples of encryption algorithms:

- AES
- DES / 3DES
- RSA
- Elliptic curves

Hash functions I

- According to Wikipedia a hash function is any function that can be used to map data of arbitrary size to fixed-size values
- But this is an incomplete definition if we want to use secure hash functions
- Hash functions must satisfy some properties in order to be considered secure

Hash functions II

Being hash() the hash function m the messages and h the digest Properties:

- Preimage resistance:It should be hard to find any message m such that h = hash(m)
- Collision resistance: Given m1 and m2, it should be hard to find a hash such that hash(m1) = hash(m2)
- Second preimage resistance: Given m1, It should be hard to find a different message m2 such that hash(m1) = hash(m2)
- Deterministic: For a given input value it must always generate the same hash value

Hash functions III

In sum:

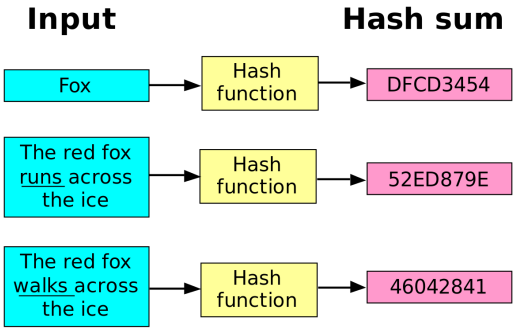
- One way (not reversible)
- The image does not reveal information on input
- No collision

Hash functions IV

Use Cases:

- Send messages secure way
- Protect databases
- Protect hard drives data

Hash functions V



Hash functions VI

Examples of hash functions:

- The modulo (NOT SECURE! JUST FOR EXAMPLE)
- SHA-3
- MD5
- SHA-2
- CRC32

Encryption vs hash I

Encryption	Hashing
Encryption is a reversible, bi-directional function.	Hashing is irreversible and unidirectional.
The original message can be retrieved using a decryption key.	The original message can not be retrieved.
The resultant encrypted string is of variable length.	The resultant hash is of fixed length.
Length of the encrypted string depends on the length of the input string.	Length of the hash is fixed and does not depend on the length of the input string.
Purpose of encryption is to ensure data confidentiality.	Purpose of hashing is to ensure data integrity.
Encryption is used to keep data secret from others.	Hashing is used for indexing, data retrieval and storing passwords.
Encryption is accomplished with the use of keys.	There is no use of keys in hashing.
In encryption, messages are scrambled in a way that only the authorized receiver is able to view the contents.	Hashing is a process to condense input strings into a fixed length. It can be used as checksums.

Encryption vs hash II

Hash or encryption?

- Store passwords in a DB
- Check integrity of a downloaded software
- Online payment

The END!