

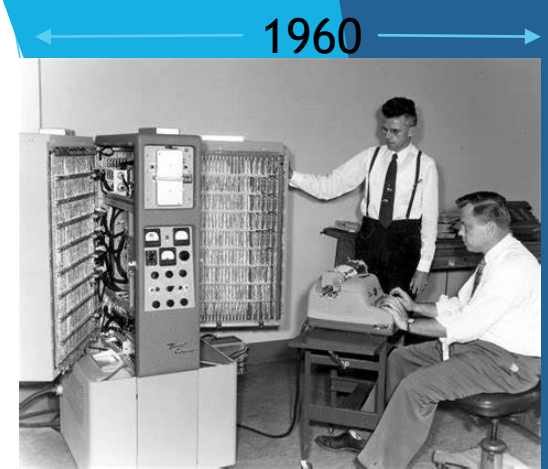
Dependability and Cybersecurity

DACYS

Critical systems

- ▶ On the 80's the paradigm of computing and IT changed dramatically
- ▶ This was possible due to two almost simultaneous happenings
 - ▶ The introduction of high capacity processors
 - ▶ The development of high speed and low latency networks, either Local Area Networks (LAN) and Wide Area Networks (WAN)
- ▶ After a few years and improvements on both cases, the monolithic and centralized systems started to be exchanged by distributed systems
- ▶ A distributed system can be defined as a group of independent systems that presents themselves to the users as a unique, single and coherent system¹

¹ Tanenbaum, A., van Steen, M., Distributed Systems, Principles and Paradigms

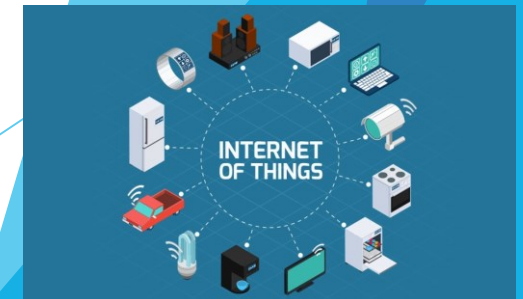


Source: <https://secutirtonlinux.com>

← Séc. XXI →



Source: <https://cbr.com>



Source: <https://www.techzilo.com/>

Critical systems

- ▶ The characterization of distributed systems can be summarized on the following aspects
 - ▶ Differences and characteristics of the single systems are hidden from users
 - ▶ How computers communicate is hidden from users
 - ▶ There is a consistent and uniform interaction
 - ▶ It must be possible to change the systems without users perception
- ▶ This principles originated the definition of *middleware*

Critical systems



Critical systems

- ▶ With the characteristic of hiding their reality of the processes and resources be in fact physically distributed between several systems, the concept of transparency emerged in terms of
 - ▶ Access
 - ▶ Localization
 - ▶ Migration
 - ▶ Relocation
 - ▶ Replication
 - ▶ Concurrency
 - ▶ Failure

Critical systems

- ▶ Access
 - ▶ Hide differences on data representation and in the access mode to a resource
- ▶ Localization
 - ▶ Hides where the resource is physically placed
- ▶ Migration
 - ▶ Hides resource displacement
- ▶ Relocation
 - ▶ Same as relocation but during resource use

Critical systems

- ▶ Replication
 - ▶ Hides that the resource is replicated, i.e., that there are multiple copies
- ▶ Concurrency
 - ▶ Hides that the resources are being used simultaneously by several users
- ▶ Failure
 - ▶ Hides the failure and recover of the resource
- ▶ We can also add another important characteristic, the Openness
 - ▶ The services are and must be offered according to defined rules

Critical systems

- ▶ The types of distributed systems vary and continue to evolve
- ▶ Some examples are
 - ▶ Web pages (Google, Microsoft, Amazon, Portal, etc.)
 - ▶ Files (Dropbox, Google Docs, ISEP/P.PORTO)
 - ▶ Home systems (Smart TV, Network Attached Storage (NAS), CCTV, alarm, Smart watch/phone)
 - ▶ Health (wearable device)
 - ▶ Sensors
 - ▶ These do not cooperate, they just send data to a server and/or process specific requests

Critical systems

- ▶ How to assure that the services provided by these distributed systems are available?
- ▶ What could happen if they fail?
- ▶ Let's consider some of them
 - ▶ Flight control
 - ▶ Health system
 - ▶ Nuclear weapons control

Critical systems

- ▶ A critical system is any system whose failure could result in threats to human life or the existence of an organization, significant economic losses and/or environmental harm
- ▶ They can be roughly classified in 3 major areas
 - ▶ Safety-critical systems
 - ▶ Failure results in loss of life, injury or damage to the environment;
 - ▶ Chemical plant protection system;
 - ▶ Mission-critical systems
 - ▶ Failure results in failure of some goal-directed activity;
 - ▶ Spacecraft navigation system;
 - ▶ Business-critical systems
 - ▶ Failure results in high economic losses;
 - ▶ Customer accounting system in a bank

Critical systems

- ▶ On these systems the most important property is its dependability
- ▶ This reflects
 - ▶ The user's degree of trust in that system
 - ▶ The extent of the user's confidence that it will operate as users expect
 - ▶ That it will not 'fail' in normal use
- ▶ When building a critical systems some aspects must be considered
 - ▶ Application development
 - ▶ The socio-technical environment

Critical systems

- ▶ The cost of a critical system is usually so high that development methods may be used that are not cost-effective for other types of systems
- ▶ Some examples are
 - ▶ Software developed using formal methods
 - ▶ Static analysis
 - ▶ External quality assurance

Critical systems

- ▶ The socio-technical environment includes everything that can go wrong
 - ▶ Hardware failure
 - ▶ Hardware may fail because of design and manufacturing errors, or because components have reached their end of life
 - ▶ Software failure
 - ▶ Software may fail due to specification and/or implementation errors
 - ▶ Operational failure
 - ▶ Operators and humans, and humans fails and make mistakes
 - ▶ This is probably the most common cause of failures

Critical systems

- ▶ None of these threats are easy to avoid, so we must make them easy to repair, restore, and monitor
- ▶ Repair
 - ▶ According to the principles of distributed systems, the repair of one of them is hidden to the end users
 - ▶ In terms of critical systems this should suffice in the operation of the system as a whole
- ▶ Restore
 - ▶ Same principle as repairing applies
- ▶ Monitor
 - ▶ Monitoring system(s) should be implemented to continuously check the system as a whole

Critical systems

- ▶ However, there are emerging situations that might imply problems
- ▶ Specifically, security and cybersecurity problems
- ▶ In practical terms the operations between the systems that perform the critical operations are standardized by communication protocols
 - ▶ Starting from the internal network where each of them lies up to the communication between them
- ▶ And, probably, with human interaction
- ▶ How confident can one be about the safety and correctness of the operation?
 - ▶ And keep in mind that the application of those protocols implies latency (delay) of the operation and demands a greater performance of the system as a whole

Critical systems

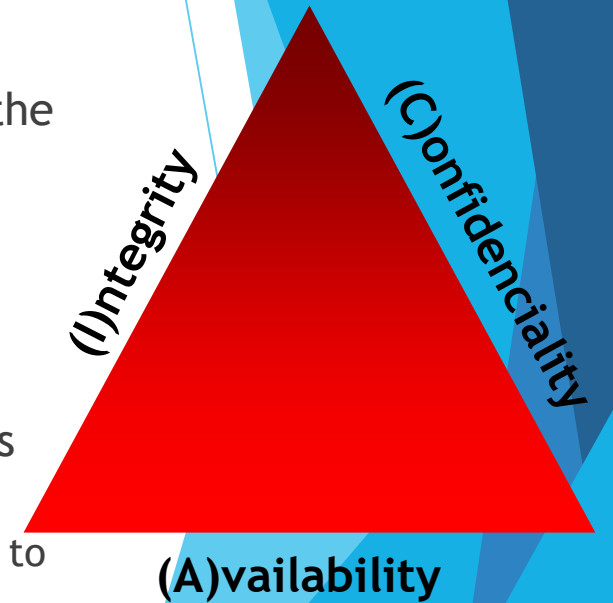
- ▶ In spite of this, security must be present on all operating layers
- ▶ From the physical layer (who has access?) up to the human interaction layer (who did this?)
- ▶ Let's now focus about security and cybersecurity

Cybersecurity

- ▶ What is Cybersecurity?
- ▶ One can define it as the set of processes, best practices and technology solutions that help protect critical systems and networks from digital attacks
- ▶ As so, it includes the installation and configuration of our assets, as well as their monitoring and procedures to mitigate the risks - and correct all the ones that nevertheless happens
- ▶ But let's start from the beginning

Cybersecurity

- ▶ The security of an infrastructure is represented by the CIA (Confidentiality, Integrity, Availability) triangle
- ▶ In spite of being usually represented with all sides of the same size, that is not the common situation
 - ▶ An advertisement webpage might take a closer look on Availability than in Confidentiality, for example
- ▶ Confidentiality is the characteristic of keeping the information understandable only for the intended users
- ▶ Integrity is the characteristic of assuring that the information is exactly as it was when it was stored or sent
 - ▶ Also includes the guarantee that the sender or who stored it was indeed who it claims to be
- ▶ Availability is the characteristic of being available when is it needed
 - ▶ In the expected timeframe



Cybersecurity

- ▶ Take a close look into the definitions of the previous slide
- ▶ Indeed, it must be kept in mind that all data *can* be achievable by anyone
- ▶ If it is stored, it will have probably authorization restrictions (which in turn is a different subject, access control), nevertheless no one can feel confident that they cannot be surpassed
 - ▶ And that points simultaneously to *confidentiality* and *integrity*
- ▶ Some key points also applies if the data is in transit between a sender and a receiver
- ▶ Concerning availability, it must not be confused with immediate access
 - ▶ There is a Service Level Agreement (SLA) that defines the maximum amount of time which can take until the data is obtained
 - ▶ And this points to infrastructure design and maintenance

Cybersecurity

- ▶ Confidentiality and integrity needs a cryptographic algorithm to be realized
- ▶ The point here is *what cryptographic algorithm must/can I use?*
 - ▶ And have in mind that “*Cryptography is rarely ever the solution to a security problem*” (D. Gollmann, Computer Security, p. 203)
- ▶ One can think in two completely different ways to choose a cryptographic algorithm
 - ▶ Develop a new one
 - ▶ Use a standard one
- ▶ Which one is best?

Cybersecurity

- ▶ By developing one algorithm, who can certify its robustness?
 - ▶ By *robustness* we are defining that two different plain text (let's call each one as **P**) encrypted with the same key (let's call it **K**) will not produce equal cipher text (and let's call it **C**)
- ▶ However, when using standard algorithms there are several people (mathematics, academics, specialists, etc.) that will test them and will certify its robustness
- ▶ Does this mean that a private algorithm is or should not be used?
 - ▶ No, it doesn't!
 - ▶ There is a saying that military organizations produce their own algorithms

Cybersecurity

- ▶ So the secret must reside on the key (K) (Kerckhoffs, 1883)
- ▶ And when not automatically generated (and even if they are), this is the beginning of our problems
- ▶ How can we define the robustness of a key?
 - ▶ By its keyspace!
- ▶ The *keyspace* represents the number of different character sets that are covered by the key
 - ▶ Let's consider the PIN code of an ATM card
 - ▶ It consists of four positions and each one can have any (numeric) character between 0 (zero) and 9 (nine), that is, 10 (ten) different choices for each position
 - ▶ Its keyspace is calculated as possibilities of each position powered to the number of positions, $10^4 = 10.000$

Cybersecurity

- ▶ How much time would it take to find it?
- ▶ In fact, not too much taking in consideration the performance of modern systems
 - ▶ And that's why a secure failure has been implemented on the system, after 3 wrong entered keys the card is kept inside the ATM and not returned
- ▶ Unfortunately, the majority of the systems doesn't implement such criteria, leaving the discovery and analysis of wrong authentications to the IT
- ▶ So, how can we communicate and store data applying a cryptographic algorithm and a key?

Cybersecurity

- ▶ We must first define a way to apply them
- ▶ In a high level degree, one can obtain a ciphertext (C) from a plain text (P) using a cryptographic algorithm with a key (K) in an operation that can be expressed as $C=E(P,k)$, and decrypt (D) it by the operation $P=D(C,k)$
 - ▶ It can also be expressed as $C=E(P,k_e)$ or $C=E(P,k^+)$ and $P=D(C,k_d)$ or $P=D(C,k^-)$
- ▶ Again, the question here lies on the key

Cybersecurity

- ▶ The key for encryption and decryption can be equal (applied in reverse way), in which case it is called shared secret
- ▶ That is the principle of symmetric encryption
- ▶ The most famous use of symmetric encryption is Ceaser's Cipher
- ▶ In this system, for encryption each letter is shifted right 3 letters and shifted left 3 letters for decryption
 - ▶ It must be noted that this used the modulus operation
 - ▶ Keep in mind that Ceaser's Cipher used a single character in each operations but more than one can be used


Cybersecurity

- ▶ Let's suppose the message DACYS IS GREAT encrypted with Ceaser's Cipher
- ▶ The correspondence between plain text (P) and cipher text (C) is shown below

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- ▶ To encrypt just drop from first line to second, to decrypt the opposite way (or swap the lines that was the option here)


E



D	A	C	Y	S	I	S	G	R	E	A	T
G	D	F	B	V	L	V	J	U	H	D	W

G	D	F	B	V	L	V	J	U	H	D	W
D	A	C	Y	S	I	S	G	R	E	A	T

D



Cybersecurity

- ▶ Later, on the 16^o century, a different approach than that of a Ceaser cypher was introduced by Vigenère
- ▶ It consists of a matrix with 26 rows and columns, containing each row the alphabet right shifted by (row_number - 1) positions
- ▶ The columns must be used to cipher each letter of the plaintext message indexed by the key letter on that position, resulting on the intersection of row_position with column_position
- ▶ Vigenère table clearly introduced the concept of block cipher (that we will discuss later) and avoided the ciphering of the same plaintext letter to the same letter of the ciphered text

-- PLAINTEXT --

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

- ▶ Let's suppose the message DACYS IS GREAT encrypted with the key ISEP
- ▶ The message is divided into blocks with the same dimension of the key:
- ▶ DACY SISG REAT
- ▶ ISEP ISEP ISEP
- ▶ The intersection (1) of "D" column with "I" row is "L", of (2) "A" with "S" is "S", and so on, resulting on the cipher "LSGNAAWVZWEI"

28

Cybersecurity

- ▶ Symmetric encryption is very fast, so it is appropriate for large volumes of data
- ▶ However, there is a constraint with symmetric keys
- ▶ Let's suppose one wants to store data in such a way that only a specific person can decrypt and understand it
 - ▶ Or consider that one wants to send such data to a receiver in such a way that only the intended receiver can decrypt and understand it
- ▶ He will need to share a secret with the intended person
- ▶ That might not be easy if the person is not nearby the owner of the data!
- ▶ Also, what if he has the same intention for several people/receivers?

Cybersecurity

- ▶ For several people, a different shared secret should be agreed with each one, individually
 - ▶ Why? To avoid that a message sent to a wrong receiver by mistake can be decrypted
- ▶ Now consider that each one of them also needs to transfer or store data between each pair of people
 - ▶ How many shared secrets will be needed?
- ▶ The mathematic expression for the number of shared secrets is $N(N-1)/2$
- ▶ Feasible, although difficult
- ▶ Nevertheless, not achievable if the pair is far away from each other

Cybersecurity

- ▶ That led to asymmetric encryption
- ▶ With this artefact there is a pair of keys, usually called public key and private key
- ▶ As for their usual name, one of them (the public one) can and must be made available for everyone, no matter being a possible receiver or not
- ▶ The other (the private one) must be kept secret
- ▶ There are some rules about the relationship between the two keys ...
 - ▶ From the private key it is possible to deduce the public key
 - ▶ From the public key it is not feasible to get the private key

Cybersecurity

- ▶ ... and their use
 - ▶ A plain text encrypted with a public key can only be decrypted with the related private key
 - ▶ A plain text encrypted with a private key can only be decrypted with the related public key
- ▶ With asymmetric encryption/keys the problem of sharing a secret with each receiver just disappears
- ▶ However asymmetric algorithms implies a very heavy and costly processing, so they aren't appropriate for large volumes of data

Cybersecurity

- ▶ So, why not combine their characteristics (hybrid system)?
- ▶ Using asymmetric encryption to agree a shared secret that will be in fact used for encryption and decryption
- ▶ This is the operation mode for several security protocols, like *Transport Layer Security* (TLS) and *IP Security* (IPsec)

Cybersecurity

- ▶ The cryptographic transformations are usually of 3 types

- ▶ Substitution

- ▶ Exchange of elements (S-box)

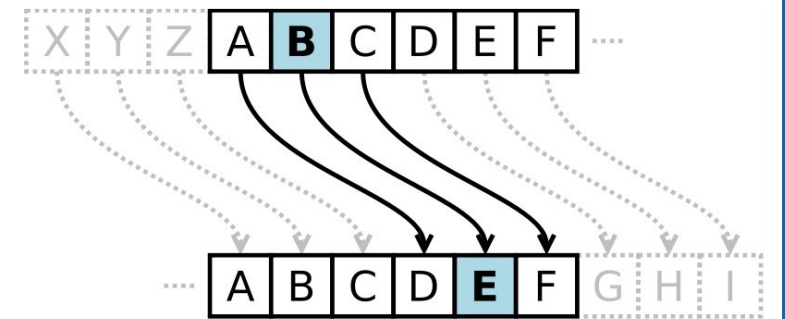
- ▶ Transposition

- ▶ Exchange or permutation of element positions (P-box)

- ▶ Combination

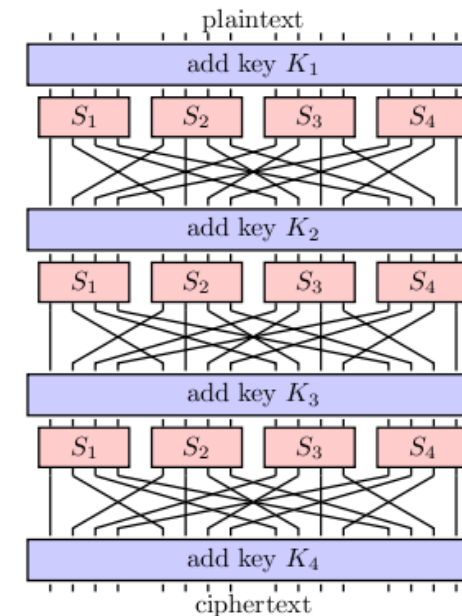
- ▶ Cascading transposition and substitution

Substitution



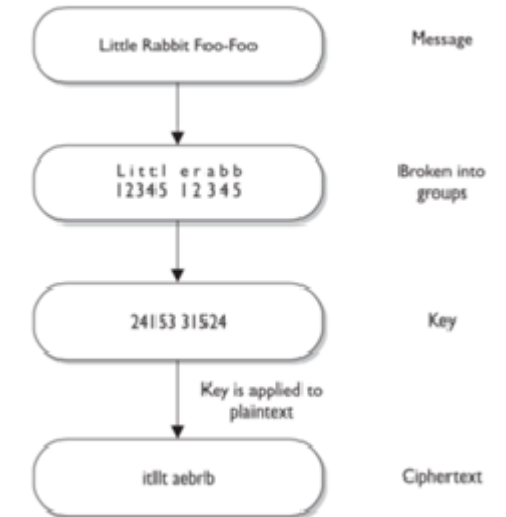
Source: Fatal Errors

Combination



Source: Barry Watson

Transposition



Source: Forensics Digest

Cybersecurity

- ▶ Now, let's see how can the text be encrypted
- ▶ The simple linear displacement of letters is not feasible nowadays
 - ▶ Why?
- ▶ More robust systems with cryptographic transformations must be used, which leads to a newer definition
 - ▶ Mono-alphabetic: if given a character of the plain text it will be encrypted always with the same character in the cypher text
 - ▶ Poly-alphabetic: if given a character of the plain text it will be encrypted with different characters in the cypher text according to its position

Cybersecurity

- ▶ The cipher method can be of two types of operation
 - ▶ Block
 - ▶ The plain text is divided into blocks of equal size of the key
 - ▶ Each block is encrypted with the same key
 - ▶ Stream
 - ▶ The plain text is divided into blocks of equal size of the key
 - ▶ Each block is encrypted with a different key
- ▶ Let's look closer to the block mode

Cybersecurity - Block Mode

- ▶ The text is splitted in blocks of the same size as the key length

$$P = P_1P_2P_3...P_N$$

- ▶ Each block is ciphered with the same key

$$C = C_1C_2C_3...C_N = K(P_1)K(P_2)K(P_3)...K(P_N)$$

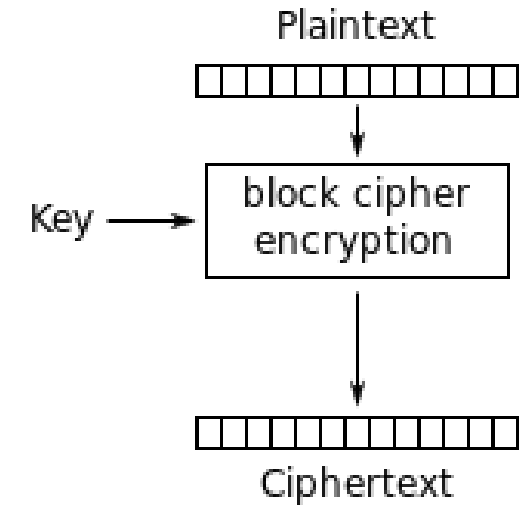
- ▶ If the length of the plain text is not a multiple of the length of the key, two mechanism can be used (yet, they must have been previously agreed)

Cybersecurity - Block Mode

- ▶ Mechanism 1: the last key is truncated to the size of the last block
 - ▶ Plain text: DACYS IS GREAT
 - ▶ Key: PORTUGAL
 - ▶ Encryption: $E(\text{DACYSISG}, \text{PORTUGAL}) E(\text{REAT}, \text{PORT})$
- ▶ Mechanism 2: Random characters are right added to the last block to fill the key size
 - ▶ Plain text: DACYS IS GREAT
 - ▶ Key: PORTUGAL
 - ▶ Encryption: $E(\text{DACYSISG}, \text{PORTUGAL}) E(\text{REATABCD}, \text{PORTUGAL})$

Cybersecurity - Block Mode

- ▶ There are some threats about block mode
- ▶ Let's assume the message is I'M READING AT READING and we will use the key IPP to encrypt
 - ▶ Plain text: I'M READING AT READING
 - ▶ Key: IPP
 - ▶ Plain text division into blocks of same size of the key: IMR EAD ING ATR EAD ING
 - ▶ Cipher text: RCH NQT RDW JJH NQT RDW → RCHNQTRDWJJHNQTRDW
- ▶ It can be noted that equal blocks produce equal ciphers and same letter on same position are also ciphered with same letter
- ▶ Using the frequency of the letters on the appropriate alphabet, the message can be deciphered
- ▶ This method of block encryption is called Electronic Code Book (ECB)

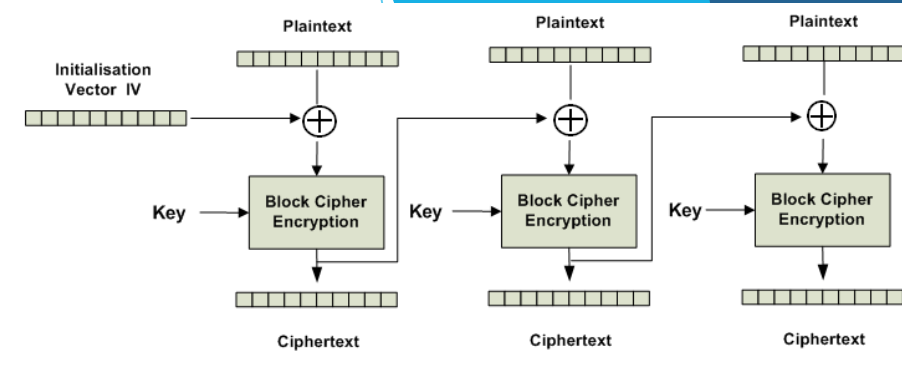


Source: Wikimedia Commons

Cybersecurity - Block Mode

- ▶ Different methods for block encryption emerged to avoid this problem
- ▶ For example, Cipher Block Chaining (CBC), Output Feedback Mode (OFM) and Counter Mode (CTR)

Cybersecurity - Block Mode

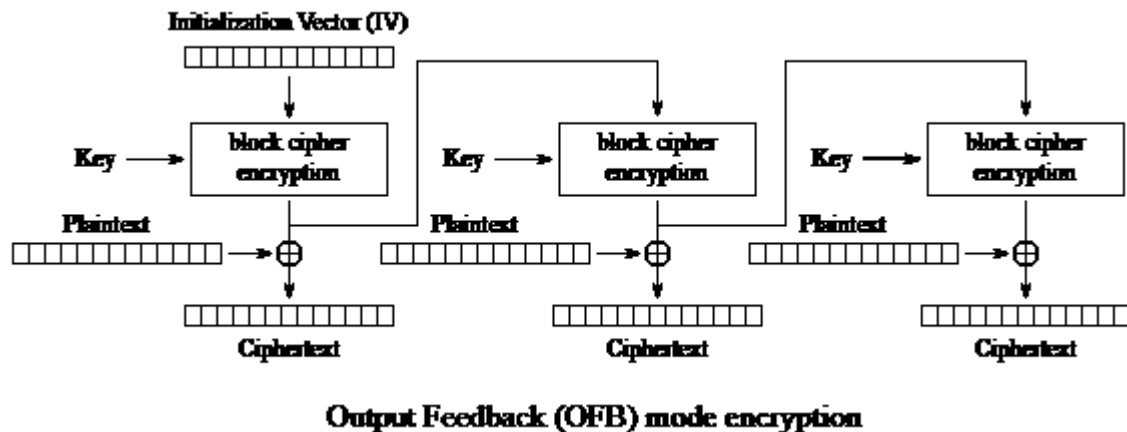


Source: Research Gate

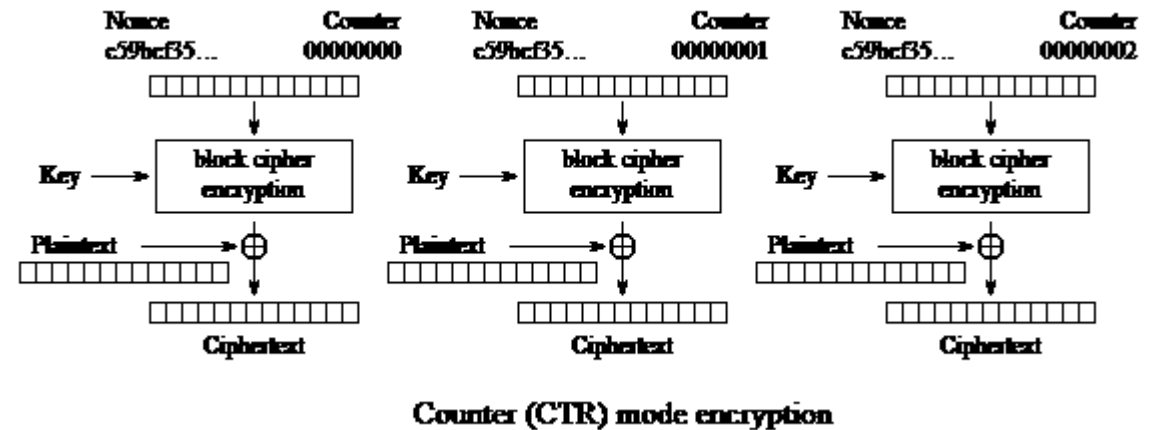
- ▶ In Cipher Block Chaining (CBC) the previous cipher block is XOR'ed with the next block before the key is applied
- ▶ It might have an initialization vector (IV) for the first block
- ▶ Using the same plain text example, what will be the differences?
 - ▶ Plain text: I'M READING AT READING
 - ▶ Key: IPP
 - ▶ Plain text division into blocks of same size of the key: IMR EAD ING ATR EAD ING
 - ▶ Ciphertext: RCH DTB XNY IXG WOA QSX → RCHDTBXNYIXGWOAQSX

Cybersecurity - Block Mode

- ▶ Output Feedback Mode operates at similar way, the difference being where the previous block cipher is applied
- ▶ Counter Mode operates by having a counter that is increased and applied before each block is ciphered

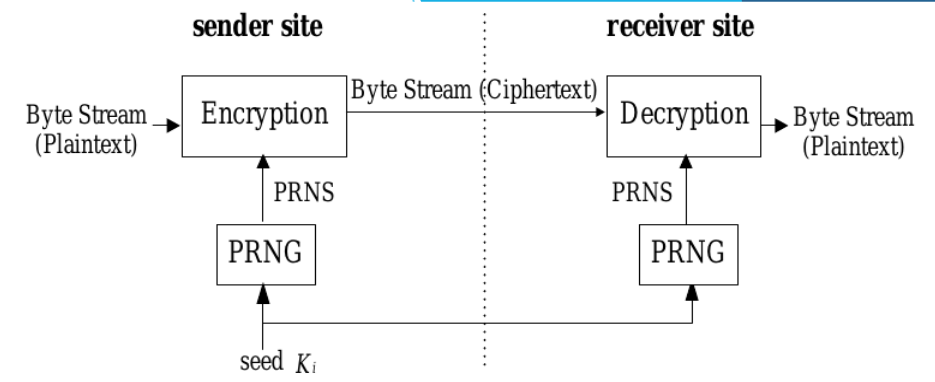


Source: Tex4TUM



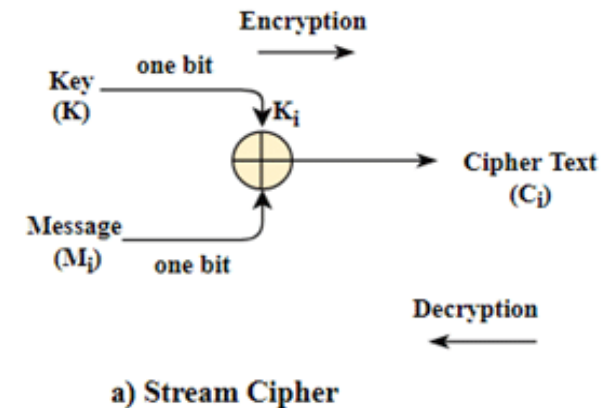
Source: Alexey Smalko

Cybersecurity - Stream Mode



Source: Research Gate

- ▶ The behavior of stream mode is to apply a different key for each block of the plain text
- ▶ This is a better approach in security terms, yet the problem lies on the number of different keys one might have
 - ▶ Because the number of characters of the plain text is unknown
- ▶ As so, it might happen that the number of keys is less than the number of the blocks of the plain text
- ▶ In that case, after exhaust the number of keys first key is applied again, then the second, and so on
- ▶ If this happens, the system is said to be periodic
- ▶ It uses usually a Pseudo Random Number Generator (PRNG) and a Pseudo Random Number Sequencer (PRNS)



Source: Research Gate

Cybersecurity

- ▶ The last characteristic of cryptography is the application type
- ▶ Before diving into this point, let's consider the needs of cryptography
- ▶ It is evident that secrecy (confidentiality) is needed
- ▶ But is this enough?
- ▶ If one wants to avoid the transfer of information between a sender and a receiver, it might just randomly change at least one bit of each message
- ▶ By this, it is expected that the message would not be feasible to be deciphered

Cybersecurity

- ▶ Thus, the need for secrecy (confidentiality) must be accompanied by the need for integrity
- ▶ As so, two different types of cryptographic algorithms has been developed, one for each need
 - ▶ Bidirectional (also called two-way) algorithms
 - ▶ Unidirectional (also called one-way) algorithms

Cybersecurity - Bidirectional algorithms

- ▶ Bidirectional (also called two-way) algorithms are responsible for providing secrecy of the data
- ▶ A plain text encrypted (E) with a bidirectional algorithm must be possible to decrypt (D) to the original
 - ▶ So we are talking again about robustness
- ▶ It provides confidentiality
 - ▶ Some authors defend that they provide authenticity as the key must be shared between the parts involved
 - ▶ However, this must not be taken for granted as the key can be captured
- ▶ It must be simple, resistant and uniqueness

Cybersecurity - Bidirectional algorithms

- ▶ Simple
 - ▶ Encryption and decryption must be easy given the key
- ▶ Resistant
 - ▶ Given a text and its cipher it is not feasible to find the key
- ▶ Uniqueness
 - ▶ Given a text P and a key k_1 it is not feasible to find another key k_2 such that $E(P, k_1) = E(P, k_2)$
 - ▶ Have you read Dan Brown's "The Da Vinci Code" and "Digital Fortress"?

Cybersecurity - Bidirectional algorithms

- ▶ Some examples of bidirectional algorithms are
 - ▶ Data Encryption Standard (DES) - should not be used
 - ▶ Symmetrical, block
 - ▶ Triple Data Encryption Standard (3DES)
 - ▶ Symmetrical, block
 - ▶ Advanced Encryption Standard (AES)
 - ▶ Symmetrical, block
 - ▶ Rivest, Shamir, Adleman (RSA)
 - ▶ Asymmetrical, block

Cybersecurity - Unidirectional algorithms

- ▶ Unidirectional (also called one-way) algorithms are intended to provide integrity
- ▶ Given a plain text P an hash H (also called the *message digest* or *Hash Message Authentication Code* HMAC) that is a characteristic of P is computed
- ▶ Given an hash H the original plain text P is not recoverable
- ▶ The hash H has a fixed length that depends of the used algorithm
- ▶ It must be simple, irreversible and uniqueness (collision avoidance)

Cybersecurity - Unidirectional algorithms

- ▶ Simple
 - ▶ Hash calculation is easy
- ▶ Irreversible
 - ▶ Given a plain text P and its hash H it is not feasible to invert the function $P \neq D(H)$
- ▶ Uniqueness (collision avoidance)
 - ▶ Given a plain text $P1$, it is not feasible to find another plain text $P2$ such that $H(P1) = H(P2)$

Cybersecurity - Unidirectional algorithms

- ▶ Message Digest 5 (MD5) - should not be used
- ▶ Secure Hash Algorithm (SHA)
 - ▶ Nowadays up to version 3 (SHA-3)

Cybersecurity - Irrefutability

- ▶ There is a more recent characteristic that is necessary
 - ▶ Irrefutability
 - ▶ Why?
- ▶ Irrefutability can only be assured with asymmetric algorithms
- ▶ That's a simple process!

Cybersecurity - Irrefutability

- ▶ Intended operation
 - ▶ Send a message P from a sender to a receiver with irrefutability (and authenticity will also be present)
- ▶ Actors
 - ▶ A sender that has an asymmetric key pair, Sk_{priv} and Sk_{publ}
 - ▶ A receiver that has an asymmetric key pair, Rk_{priv} and Rk_{publ}
- ▶ Operation
 - ▶ The sender computes H_s (H computed on sender) and encrypts it with Sk_{priv} $H_{se}=Sk_{priv}(H_s)$
 - ▶ The message plus H_s is encrypted with Rk_{publ} and sent $MessageSent=Rk_{publ}(M \cup H_{se})$
 - ▶ The receiver decrypts the full message with Rk_{priv}
 - ▶ The receiver computes H_r (H computed on receiver)
 - ▶ The receiver decrypts H_s he has received by applying $D((H_s, Sk_{priv}), Sk_{publ})$
 - ▶ The receiver can now compare H_r and H_s

Cybersecurity - Irrefutability

- ▶ If equal, authenticity, integrity and irrefutability is assured, as:
 - ▶ Authenticity
 - ▶ The message was indeed sent by the sender as only he knows Sk_{priv}
 - ▶ Integrity
 - ▶ The message is exactly as it was sent because $H_r = H_s$
 - ▶ Irrefutability
 - ▶ The sender cannot deny that he sent the message as only he could had encrypt H_s with Sk_{priv}

Let's talk a little about maths...

▶ Modular arithmetic

- ▶ $a = b \pmod{n}$
- ▶ $a - b$ is a multiple of n
- ▶ $a = b \% n$
- ▶ a is the rest of b / n
 - ▶ Example: $2 = 12 \pmod{10}$

▶ Basic properties

- ▶ $a \pmod{n} + c \pmod{n} = (a + c) \pmod{n}$
- ▶ $a \pmod{n} \times c \pmod{n} = (a \times c) \pmod{n}$
- ▶ $a^c = (a \pmod{n})^c \pmod{n}$

Let's talk a little about maths...

- ▶ Basic properties (continuation)
 - ▶ $a^c = a^{c \pmod{\Phi(N)}} \pmod{n}$
 - ▶ If n is a prime number
 - ▶ If n is a product of prime numbers
- ▶ The totient function, Φ , is a function that returns the number of positive prime numbers that are coprime with its argument and lower than it
 - ▶ For example, $\Phi(12) = 4 : \{1, 5, 7, 11\}$
- ▶ If n is a prime number, $\Phi(n) = n - 1$
 - ▶ For example, $\Phi(13) = 12 : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Let's talk a little about maths...

- ▶ Basic properties (continuation)
 - ▶ If p and q are prime numbers and $n = p \times q$, then $\Phi(n) = (p - 1) \times (q - 1)$
 - ▶ For example, $\Phi(3 \times 5) = 2 \times 4 = 8 : \{1, 2, 4, 7, 8, 11, 13, 14\}$
 - ▶ If $c \pmod{\Phi(n)} = 1$, $a^c = a \pmod{n}$
 - ▶ For example
 - ▶ $n = 15$
 - ▶ $\Phi(15) = 8$
 - ▶ $c = 9 \pmod{8} = 1$
 - ▶ $2^9 = 512 \pmod{15} = 2$
- ▶ Modulus and totient are very used on cryptographic algorithms

Cybersecurity

- ▶ The way that cryptographic algorithms are implemented and used on standard protocols varies according to the provider of the protocol
 - ▶ For example, IPsec uses a different way to address the used algorithms than TLS
- ▶ So let's analyze two cipher suites of TLS
 - ▶ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - ▶ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Cybersecurity

- ▶ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - ▶ ECDHE: Elliptic Curve Diffie-Hellman Ephemeral
 - ▶ ECDSA: Elliptic Curve Digital Signature Authentication
 - ▶ AES_128_GCM: AES with key size of 128 bits with CTR
 - ▶ SHA256: Message Authentication Code with SHA256 variant of SHA-2
- ▶ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 - ▶ ECDHE: Elliptic Curve Diffie-Hellman Ephemeral
 - ▶ RSA: Integrity with RSA
 - ▶ AES_256_CBC: AES with key size of 256 bits in CBC
 - ▶ SHA384: Message Authentication Code with SHA384 variant of SHA-2

Cybersecurity

- ▶ The technical aspects of cybersecurity are linked with the previous slides
- ▶ But some different aspects should and must be thought
 - ▶ Social
 - ▶ Political
 - ▶ Economic

Cybersecurity

▶ Social

- ▶ We can all agree that nowadays Internet use is mandatory
- ▶ As individuals, we all use it for bank interaction, schedule health appointments and many more actions
- ▶ As society, it is used for airplane control, manufacturing control, patients situation, infrastructure vital services, and many others
- ▶ We will probably also agree that when a problem arises, the weakest people are more exposed to it than the strongest
 - ▶ Take a look at <https://blog.secureset.com/the-social-impact-of-cybersecurity-b55c12a72fa2>
- ▶ At the same time, a disturbingly large portion of our world lives in poverty
- ▶ Can we ignore it?

Cybersecurity

▶ Political

- ▶ More and more data that varies from personal subjects to political and defense agreements and actions are stored on huge databases
- ▶ An attacker - that might be a single person, an organization or another country - might consider (and indeed they do) that collecting information about an enemy that might provide a way to avoid defenses or at least intuit the expected behavior of others, increasing its success chances
 - ▶ Have you read Sun-Tzu “The art of war”?
- ▶ It is imperative for a country (that is to say, the politicians that rules it) to avoid or at least mitigate as much as possible the risk of having its data reachable by unwanted people

Cybersecurity

▶ Economic

- ▶ Does anything need to be said?
 - ▶ Banks relies on network infrastructures
 - ▶ Manufacturing relies on network infrastructures
 - ▶ Defense relies on network infrastructures
 - ▶ Health relies on network infrastructures
 - ▶ Social aspects of todays societies relies on network infrastructures (including some individual areas like IoT)
- ▶ In fact, everything relies on infrastructure networks nowadays and since a long time
- ▶ The big difference between the past and now, is that for economical and social reasons the (previous) internal, isolated, infrastructure is now connected to the Internet

Cybersecurity

- ▶ On critical systems, this represents an huge risk!
- ▶ Nevertheless, security was never considered as a area where significant investment should be made
- ▶ *“In the past, Industrial Control Systems were operated as separated networks unconnected to public communication infrastructures, but as businesses have turned to exploit the services and data provided by the Internet, such isolation that protected these systems has declined. The benefits afforded by real time monitoring, peer to peer communications, multiple sessions, concurrency, maintenance and redundancy have enhanced the services provided for consumers and operators”* (in Maglaras, L.A., Kim, K., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., Cruz, T. J., *Cyber security of critical infrastructures*)

Cybersecurity

- ▶ As so, the previously isolated systems have become (one might say, *are becoming*) more and more exposed to an increasingly range of threats
- ▶ There is a need to stop this spiral of happenings, correct the existing threats, and start a new attitude
- ▶ How and where we can start?

Cybersecurity

- ▶ Critical systems usually consist of distinct systems that are interconnected in a transparent way
- ▶ Some of them are *de facto* computers, others are sensors and/or actuators, others infrastructure actives, others programmable logic controllers among other types
- ▶ They all stand on a physical place and rely on communication networks, human interface, data codification, environment, and others aspects (like power supply)
- ▶ Is there a more important point that we must address?

Cybersecurity

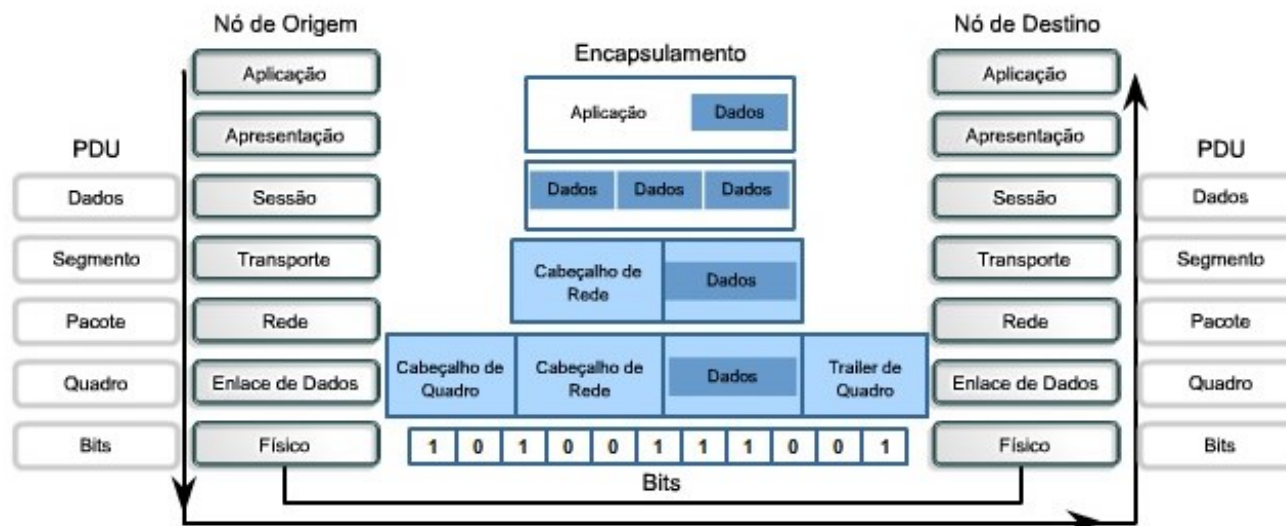
- ▶ Let's recall how systems and networks operate
- ▶ The OSI (Open Systems Interconnection) reference model was presented on 1984 by ISO (International Organization for Standardization) with the objective to propose and define the interconnection of systems from different manufacturers
- ▶ It was never implemented, however in abstract terms it is usually used for study

Cybersecurity

- ▶ It consists of 7 (seven) layers where each one of them interacts with and only with the contiguous ones
- ▶ When data travels downwards, it is *encapsulated*
- ▶ When it travels upwards, it is *unencapsulated*



Source: Ethernetd!



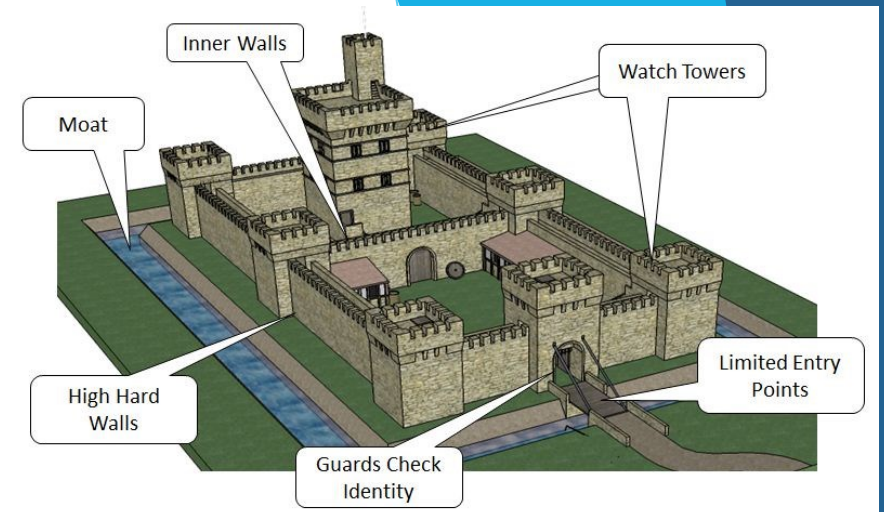
Cybersecurity

- ▶ It isn't intention of this class to discuss or present the encapsulation / unencapsulation methods and principles
- ▶ But remember some of the operations taken on some layers
 - ▶ Layer 4 - Transport
 - ▶ Establishment of the TCP connection
 - ▶ Layer 3 - Network
 - ▶ Best effort
 - ▶ Provides a route for sending the data to the destination
 - ▶ Layer 2 - Data link
 - ▶ Transfer of data inside internal network

Cybersecurity

- ▶ Is there any layer more susceptible to be attacked?
- ▶ No, there isn't
- ▶ Each layer can and should also be thought as a security issue
- ▶ Also, keep in mind that this reality is not limited to the internal network
- ▶ Indeed, some of these layers have been object to defenses since a long time ago
- ▶ Let's see some of them
- ▶ Just a note about *"Hack the stack - Using snort and ethereal to master the 8 layers of an insecure network"* in though it is so old

Cybersecurity



Source: WyzGuys

- ▶ Layer 1 - Physical
- ▶ Should security and cybersecurity be thought just as an IT subject?
- ▶ *If physical access to a system is obtained, its security can be jeopardized*
- ▶ That's why there were (and are?) always physical protection for assets
 - ▶ Watch dogs
 - ▶ CCTV circuits
 - ▶ Doors, fences, locks, biometric devices, and many other artefacts

Cybersecurity

- ▶ Layer 1 - Physical
- ▶ Let's take a deeper look into this layer
- ▶ Our usual attitude when entering home, leaving the car, and so on, is to close it
- ▶ On physical terms, that's the *border* of our asset
- ▶ And what about technology?
- ▶ What is its border?

Cybersecurity

- ▶ Layer 1 - Physical
- ▶ Usually, the router that connect our systems to the Internet
- ▶ Remember the castle two slides ago
- ▶ The moat only try to prevent one from reaching the walls
 - ▶ But if surpassed, it does not provide any other kind of defense
- ▶ An artefact whose role is only to avoid unauthorized access to the inside network is said to be the perimeter defense
 - ▶ Like moats, doors, fences, and many others
 - ▶ What do you think that watch dogs are? Perimeter defense?

Cybersecurity

- ▶ Layer 2 - Data link
- ▶ As already said, this layer is responsible for the communications inside internal network
- ▶ What happens when you arrive somewhere and power on your system to reach the Internet?
 - ▶ Your system doesn't know where he is
 - ▶ He also does not know how can he reach the Internet
 - ▶ He is going to ask for that information
 - ▶ To whom?

Cybersecurity

- ▶ Layer 2 - Data link
- ▶ To all systems available on the internal network!
- ▶ Can they be trusted?
- ▶ Who can hear the information that is exchanged inside the internal network?
- ▶ As stated above, *all systems available on the internal network*
 - ▶ This subject will be discussed later on other classes

Cybersecurity

- ▶ Layer 2 - Data link
- ▶ Is this something that we should worry about on outside networks?
- ▶ Not really, as data link layer role is limited to the internal network

Cybersecurity

- ▶ Layer 3 - Network
- ▶ This layer is responsible to provide a path to transfer the data from the sender to the receiver
- ▶ That's where Internet Protocol (IP) addresses works
- ▶ Its true and most effective role is to provide the best effort to allow the data sent by someone to reach as quickly as possible its destination

Cybersecurity

- ▶ Layer 3 - Network
- ▶ Let's consider this layer on two network approaches
 - ▶ Internal network
 - ▶ External network

Cybersecurity

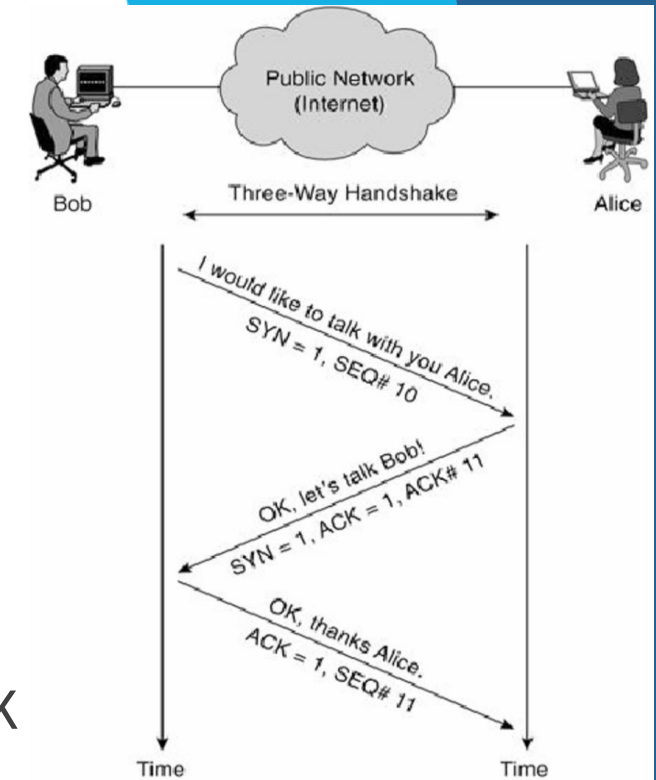
- ▶ Layer 3 - Network
- ▶ The question *Can we trust on the systems inside internal network?* has already been placed
- ▶ If the answer is *Yes* no problem should exist
- ▶ But are we confident about this *Yes*?
- ▶ Just imagine that an outsider was able to enter in you castle (house) and connect his system to your internal network
 - ▶ What can he do?
 - ▶ This subject will be discussed later on other classes

Cybersecurity

- ▶ Layer 4 - Transport
- ▶ This layer is responsible for the reliable and efficient communication between applications (*endpoints*)
- ▶ The exchange can be peer-to-peer or a client-server interaction
- ▶ The protocols on this layer allow a connection-oriented or a connectionless
- ▶ What could be the threats on connection-oriented communication?

Cybersecurity

- ▶ Layer 4 - Transport
- ▶ This kind of communication starts with a three-way handshake starting from the initiator (client) to the receiver (server)
- ▶ As it can be seen in the image, apart from the SYN - SYN/ACK - ACK sequence there are additional fields that needs to be formatted
- ▶ Why?



Source: ResearchGate

Cybersecurity

- ▶ Layer 4 - Transport
- ▶ Let's assume that client is A, server is B and the attacker is X
- ▶ What is expected to happen is these transfers:
 1. A sends a packet to B with SYN + ISN_A
 2. B answers with a packet with SYN + ISN_B + ACK + (ISN_A+1)
 3. A sends a packet to B with ACK + (ISN_B+1)
- ▶ Imagine that an attacker performs the following exchanges
 1. X sends a packet to B with forged address of A and SYN + ISN_X
 2. B answers to A with a packet with SYN + ISN_B + ACK + (ISN_X+1)
 3. X sends a packet to B with forged address of A and ACK + (ISN_B+1)
 1. As long as X is able to guess or calculate the expected ISN_B

Cybersecurity

- ▶ Layer 5 - Session, 6 - Presentation and 7 - Application
- ▶ These layers can be attacked in several forms
- ▶ In these layers several and essential parts of a communication occurs
 - ▶ Network Basic Input / Output System (NETBIOS)
 - ▶ Server Message Block (SMB)
- ▶ As well as other operations like the adapt the codification according to the endpoint requirements

Cybersecurity

- ▶ Layer 5 - Session, 6 - Presentation and 7 - Application
- ▶ On the existing real implementation of the OSI Reference Model, the TCP Model, these three layers are grouped as a single one
- ▶ More than the threats that can exist (and do) exist on each of them, the application layer stands out as the most dangerous
- ▶ And is, perhaps, the most used and worrying in cybersecurity

Cybersecurity

- ▶ Layer 5 - Session, 6 - Presentation and 7 - Application
- ▶ Threats like SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Buffer Overflows, Broken Access Control, among others, happens in these layers
 - ▶ Nowadays SQL Injection is grouped with other attacks (like XSS) and called Injection, CSRF is also grouped with other attacks and called Server-Side Request Forgery (SSRF), and so on
 - ▶ This subject will be more deeply discussed on other classes

Cybersecurity

- ▶ Previously, the concept of perimeter defense was presented, and a question have probably emerged
 - ▶ Can one trust on an infrastructure that relies only on a perimeter defense?
- ▶ What and how many artefacts do you have at home to avoid robbery?
- ▶ Think again of the middle age castle
- ▶ If an attacker was able to surpass the moat, he still has to defeat the walls, defenders, and so on

Cybersecurity

- ▶ On actual networks, obviously the perimeter defense exists, but it is completed with other defenses *inside* the infrastructure
- ▶ That is the concept of defense in depth
- ▶ The security of a network is as good as its weakest link
- ▶ That's why several layers of security must be configured
- ▶ The defenses as a whole are stronger than each of the individual components
- ▶ How can one implement it?

Cybersecurity

- ▶ Several ways / approaches, but let us focus on some of them
 - ▶ Weakest Link Security
 - ▶ Defense in Depth
 - ▶ Secure Failure
 - ▶ Minimal Privilege
 - ▶ Compartmentation
 - ▶ Simplicity
 - ▶ Distrust by default
- ▶ Think and propose additional / alternative approaches

Cybersecurity

- ▶ Weakest Link Security
 - ▶ Infrastructure security is equal to the security of the weakest link
 - ▶ What is more often stolen? A bank or a supermarket?
 - ▶ An attacker tends to search and look to the weakest points
 - ▶ Identify components / parts that have the greatest risk
 - ▶ Raise the level of safety in order to reduce the risk to an acceptable level

Cybersecurity

▶ Defense in Depth

- ▶ Put a series of defense mechanisms so that if one level of defense fails, another may possibly avoid a full exposure
- ▶ Bank security
 - ▶ Double Doors + Video Cameras + Little money in the service boxes + Safe box with delayed opening

Cybersecurity

▶ Secure Failure

- ▶ If security is surpassed, configure the infrastructure / system to go to a safe state
- ▶ Example: ATM cards
 - ▶ After inserting three wrong pin, the card is kept and not returned
- ▶ It is better to shutdown the system or service than to deal with the consequences of the attack

Cybersecurity

- ▶ Minimal Privilege
 - ▶ Only the minimum permissions required to perform an operation should be assigned
 - ▶ And for the minimum time possible
 - ▶ When any type of permissions is assigned to a component, some risk is always incurred

Cybersecurity

▶ Compartmentation

- ▶ Split the infrastructure into different units and / or zones, to isolate a possible problem from each other
- ▶ In addition, it simplifies the implementation of the minimal privilege
- ▶ Use Virtual LAN (VLAN), different broadcast or collision zones, etc.

Cybersecurity

▶ Simplicity

- ▶ *There are two ways to make a system. One is to make it so simple that there are obviously no deficiencies. The other is to make it so complex that there are no obvious deficiencies.* (adapted from C.A.R. Hoare)
- ▶ Complexity increases risks, so avoiding complexity is avoiding problems
- ▶ But couldn't this collide with safety?
 - ▶ Building a system without cryptography is simpler than one with

Cybersecurity

- ▶ Distrust by default
 - ▶ Don't forget that we are considering critical systems with all the systems, sensors, actuators, and many other artefacts
 - ▶ The faster the communication between assets, the better the usability of the solution
 - ▶ However, in Industry 4.0 we are talking about Internet of Things (IoT), Cloud, mobile applications, and many other possibilities
 - ▶ That should not mean that when building a solution one can assume that the link between two endpoints are trustable by default
 - ▶ Implement Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS)
 - ▶ But do not assume that these artefacts are 100% reliable on detection

Cybersecurity

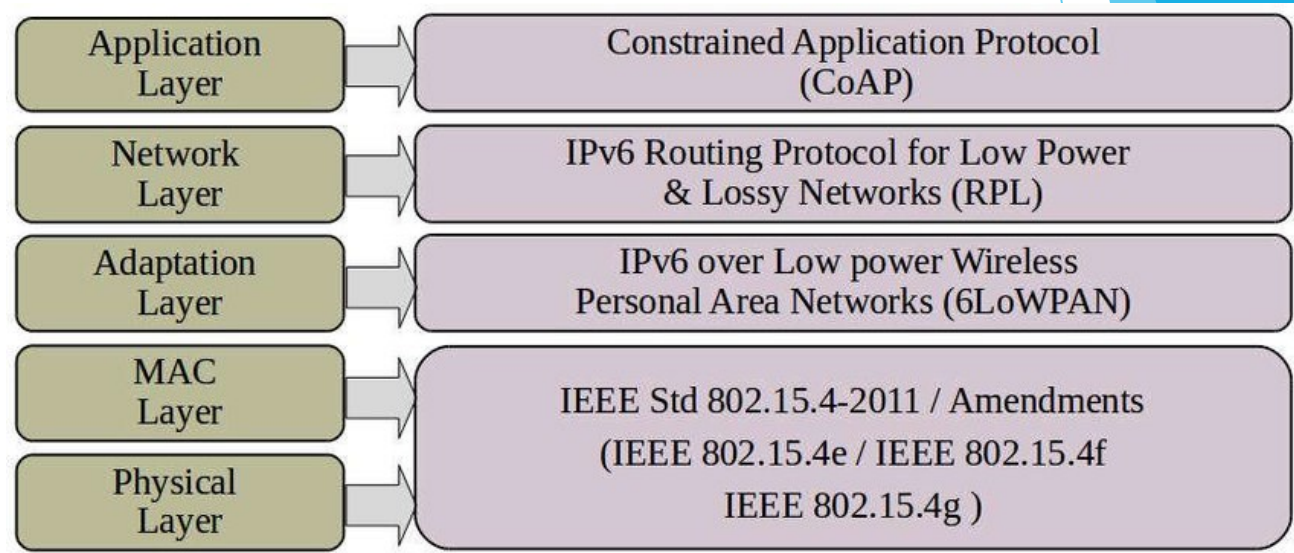
- ▶ Consider again the protocols (rules) that sustain systems interaction
- ▶ Some of them were developed a very long time ago, when security was not a concern
- ▶ As that, they suffer of security issues
- ▶ On other classes of DACYS we had the opportunity to discuss and test some of them
- ▶ Are they new ones that must be thought right now?

Cybersecurity

- ▶ Wait!
- ▶ About the existing protocols - how can one mitigate and prevent them?
 1. Foster a culture of cybersecurity
 2. Implement cyber hygiene best practices
 3. Invest in both digital and physical security
 4. Promote clear communication and clarity leadership
 5. Audit devices, assets, and all network components

Cybersecurity

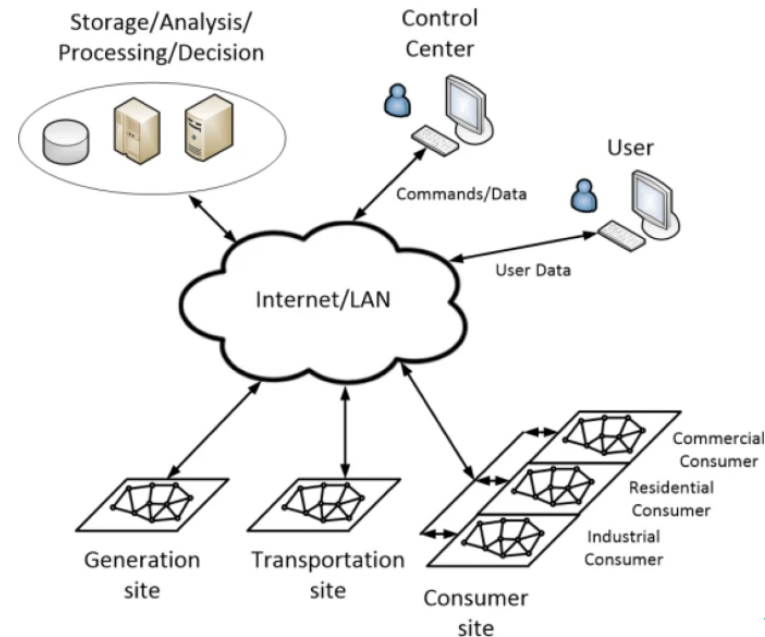
- ▶ Some new technologies are emerging that will be probably applied to critical systems
- ▶ Some of them are
 - ▶ IoT



Source: ResearchGate, Antar Abdul-Qawy

Cybersecurity

- ▶ Some new technologies are emerging that will be probably applied to critical systems
- ▶ Some of them are
 - ▶ IoT
 - ▶ Smart cities



Source: Jawhar, I., Mohamed, N., Al-Jaroodi, J.,
Networking architectures and protocols for smart
city systems

Cybersecurity

- ▶ Some new technologies are emerging that will be p applied to critical systems
- ▶ Some of them are
 - ▶ IoT
 - ▶ Smart cities
 - ▶ Critical technologies

As safety critical systems evolve, completely new technologies will be developed. At times, these new technologies may interact within a single application that is a part of a system of systems. It is paramount that these systems work collaboratively so that the failure of one system does not either adversely affect another system or compromise the platform as a whole.

This will require the creation and adoption of definitive software development processes, specifications, and standards that focus on the importance of integration and verification. Safety critical system developers will need to balance the costs and time constraints required to build these future system while identifying and mitigating limitations when they arise.

The challenge to develop these safety critical systems will become much more difficult as machines become more complex and autonomous. In the global race to develop autonomous, life-changing technologies, the development and integration of safety critical systems needs to be at the forefront.

Source: Mellati, L., CoreAVI