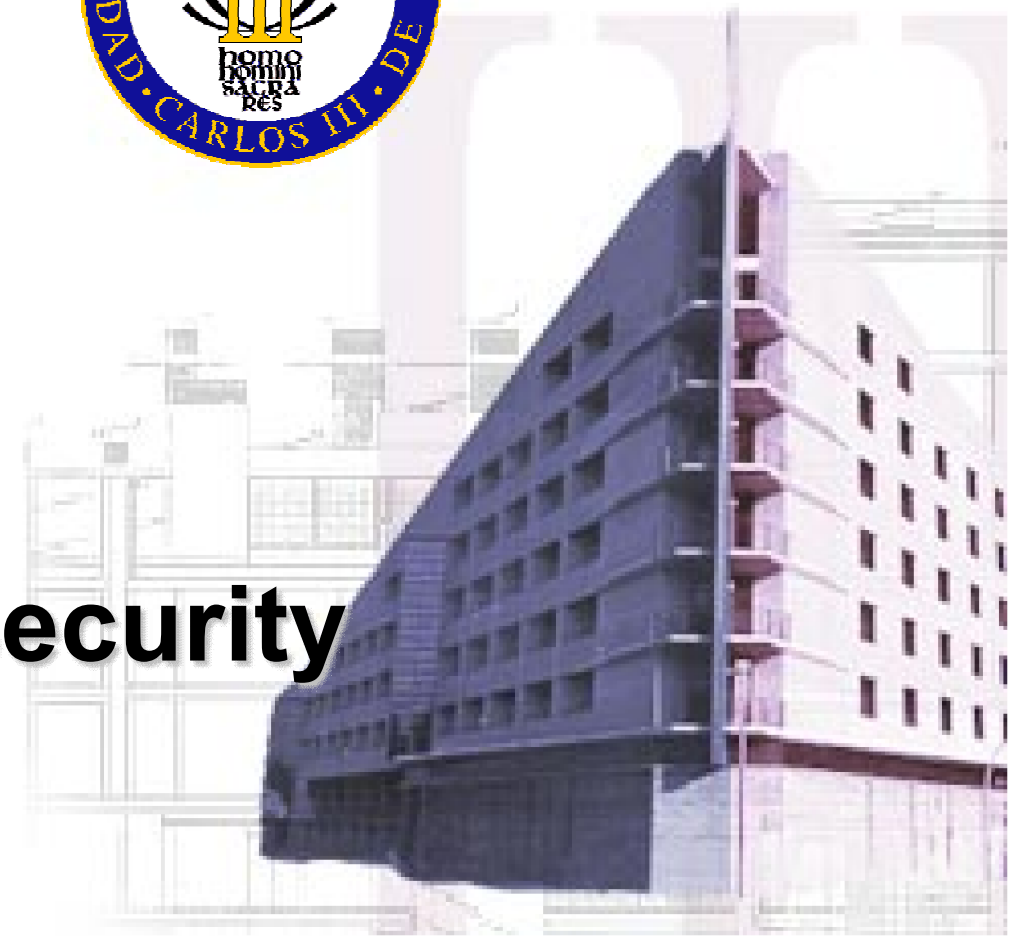


CHAPTER 2: Introduction to security

Coding Techniques

Francisco Valera Pintor

Departamento de INGENIERIA TELEMATICA
www.it.uc3m.es

WHAT IS SECURITY

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

Slightly modified version of a quotation from Gene Spafford (Professor of computer science at Purdue University, USA)

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

From: "Computer Recreations: Of Worms, Viruses and Core War" by A. K. Dewdney, in Scientific American, March 1989, pp 110.

THREATS

- **To physical resources:**
  - Theft, destruction, accidents, damage, usage errors
- **To resource utilization:**
  - Reduction of availability, economic loss (disk space, CPU time, data volume transmitted on a leased line etc.)
- **To stored information:**
  - Loss of integrity, confidentiality, availability
- **To transmitted data:**
  - Loss of integrity, confidentiality, availability, authenticity, non-repudiation
- **To the image and reputation:**
  - Inability to prevent or detect attacks or identify offenders, impact on third party assets, own responsibility

EXAMPLES OF DISPUTED DOMAINS

The disputed domain names:

1. <pccillen.com>
2. <pccillon.com>
3. <pcillian.com>
4. <trendmico.com>
5. <trendmicroeurope.com>
6. <trendmicrosystems.com>
7. <trendmirco.com>
8. <trenmicro.com>

The disputed domain names:

1. <amadon.com>
2. <amazaon.com>
3. <amoazon.com>
4. <amoson.com>
5. <amozen.com>
6. <amozom.com>
7. <amozone.com>
8. <azazon.com>
9. <wwamazon.com>
10. <wwwamozon.com>

http://arbiter.wipo.int/center/index.html

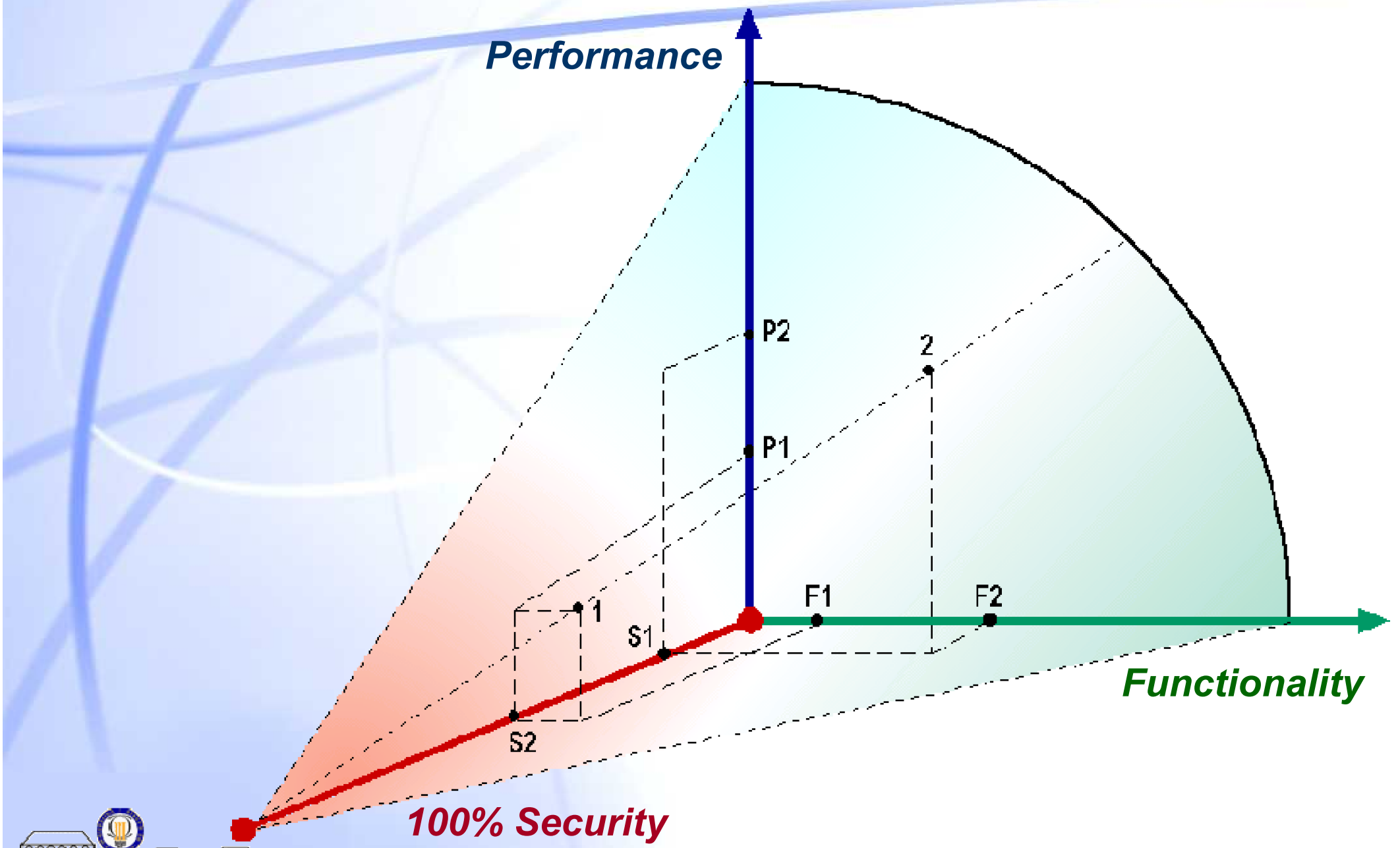
COMMON ATACKS

- Masquerading
  - Spoofing
  - Pharming
- Eavesdropping
  - Sniffing
- Tampering
- DoS
- Shoulder surfing
- Scavenging
- Buffer overflow
- Tiny Fragment
- Tear Drop
- ICMP flooding
- DDoS
- Spam
- Routing protocols
- SMTP, FTP, HTTP
- Social engineering
  - Phishing
- Malware

SECURITY COSTS

- Investment (equipment, systems)
- Expenses (maintenance/staff)
- Reputation
- Complexity of use
- Service restrictions
- Performance reduction

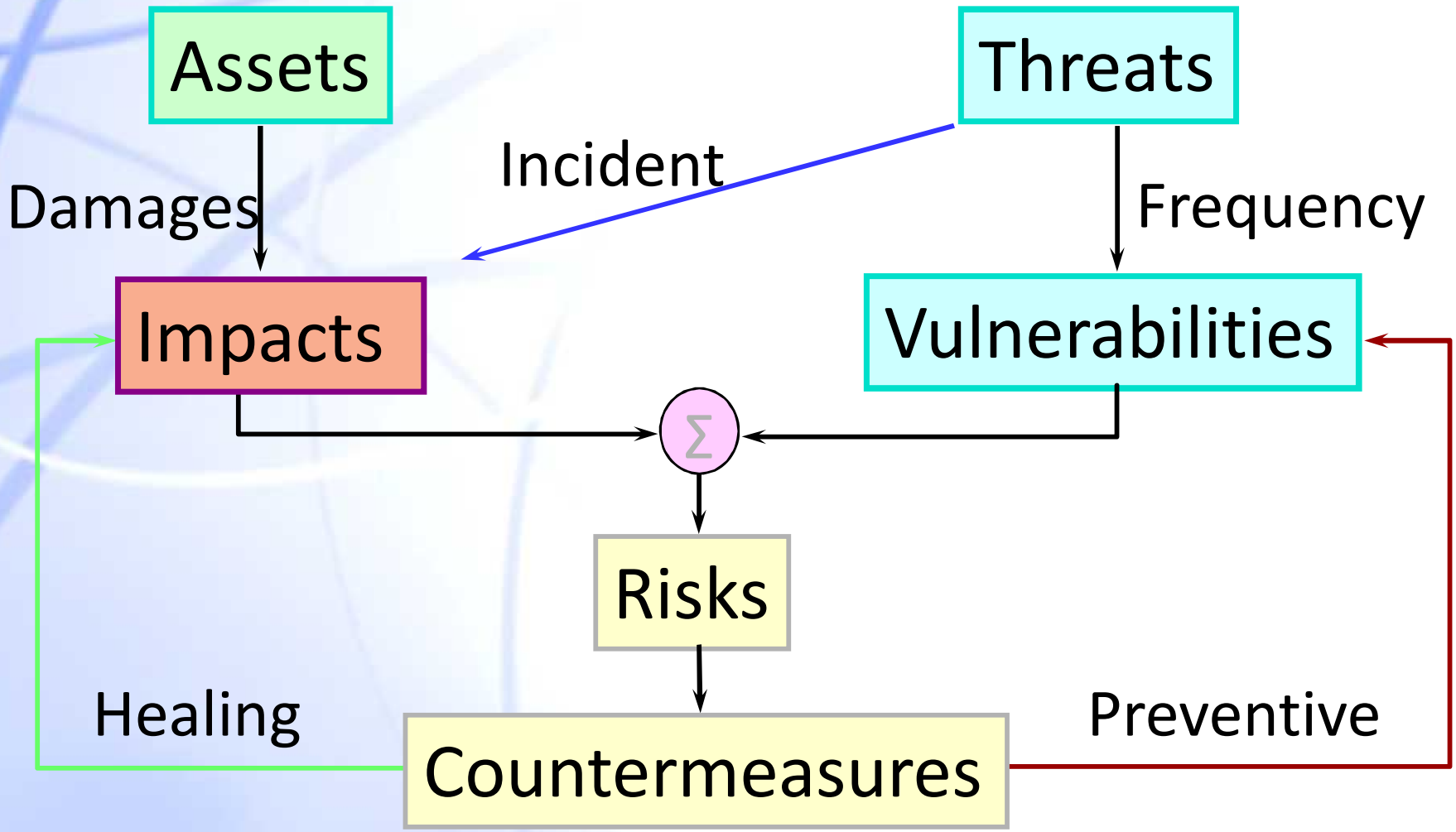
RESTRICTION CONE



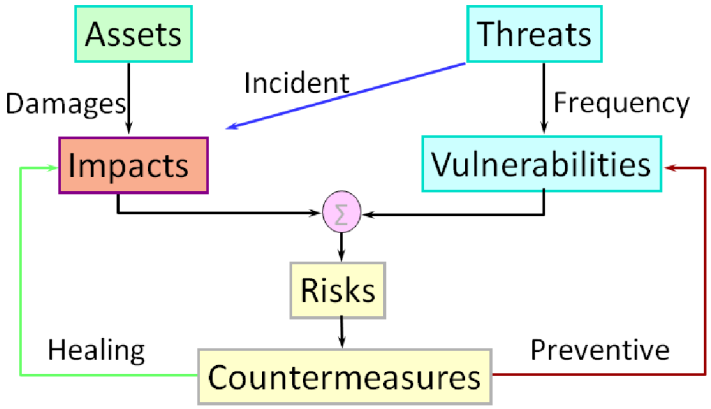
THE SECURITY CYCLE

- Identify the elements to protect
  - Named “assets”
- Determine the possible incidents (threats)
- Determine the likelihood of a threat
  - How critical they can potentially become?
- Implement countermeasures
- Review the process periodically

THE SECURITY CYCLE

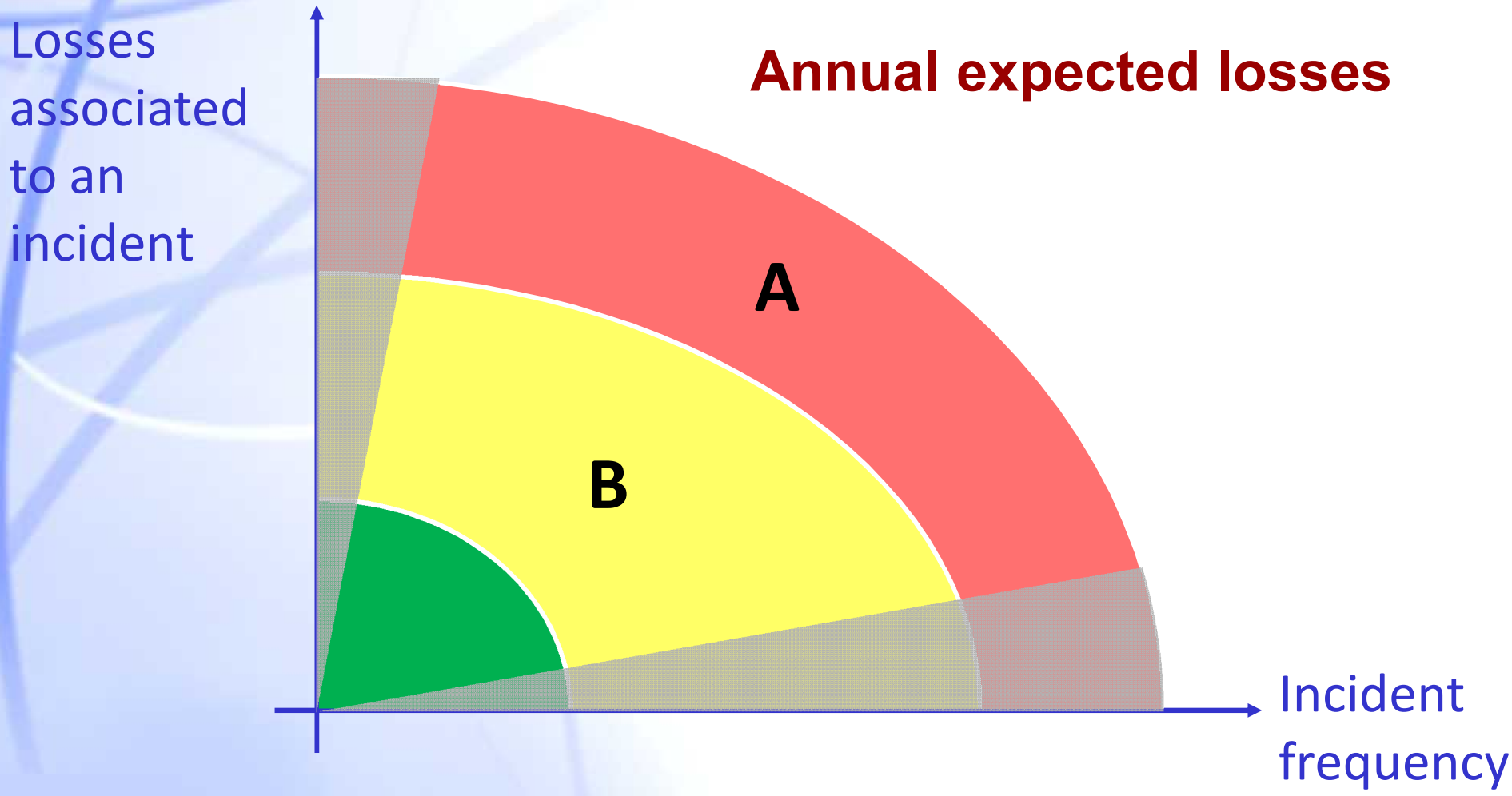


ELEMENTS

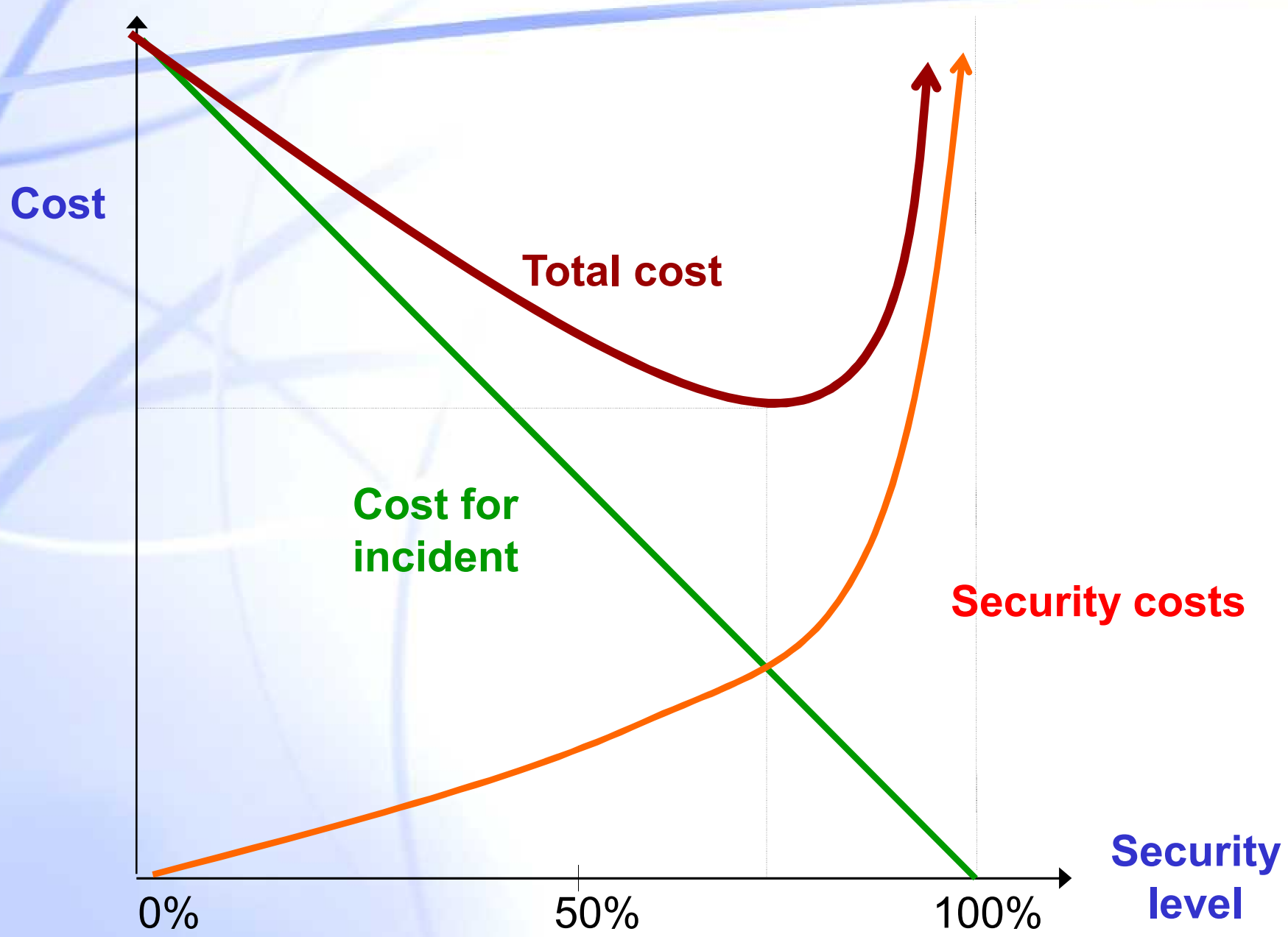


- **Assets to protect**
- **Threats to the assets**
  - **People, things, events…**
- **Vulnerabilities**
  - **Points where the threats may turn into an incident**
    - Vulnerabilities have a certain probability
- **Impact of the incident**
- **Risks of running in a real environment:**
  - **Never null, based on a compromise**
- **Countermeasures (or safeguards):**
  - **Reduce the vulnerabilities (preventive)**
  - **Limit the impact of an incident (healing)**

INCIDENT PRIORITIZATION



POINT OF FINANCIAL EQUILIBRIUM



GENERAL SOLUTION?

- Security audit

- Security policies

SECURITY DEFINITIONS

- **Security:** actions that allow one to
  - Detect and prevent: reducing the probability of harmful incidents
  - Recovery: reducing the negative consequences when a harmful incident occurs
  - Reporting: Identifying the causes when a harmful incident occurs
- **Attack:** any action capable of compromising the security of the information in an organization
- **Security mechanism:** any mechanism designed to detect, prevent or recover from a harmful incident
- **Security service:** a service that improves the security of data processing or transfer and that in general makes use of one or more security mechanisms

SECURITY SERVICES

- **Availability:**
  - **Guarantees the availability of the information for authorized entities whenever required**
    - Threat: Elimination of data or resources
- **Confidentiality:**
  - **Information only accessible to authorized entities**
    - Threat: Non-authorized access to data or traffic analysis
- **Integrity:**
  - **Only authorized entities may modify the information**
    - Threat: Modification of data or introduction of false data

SECURITY SERVICES

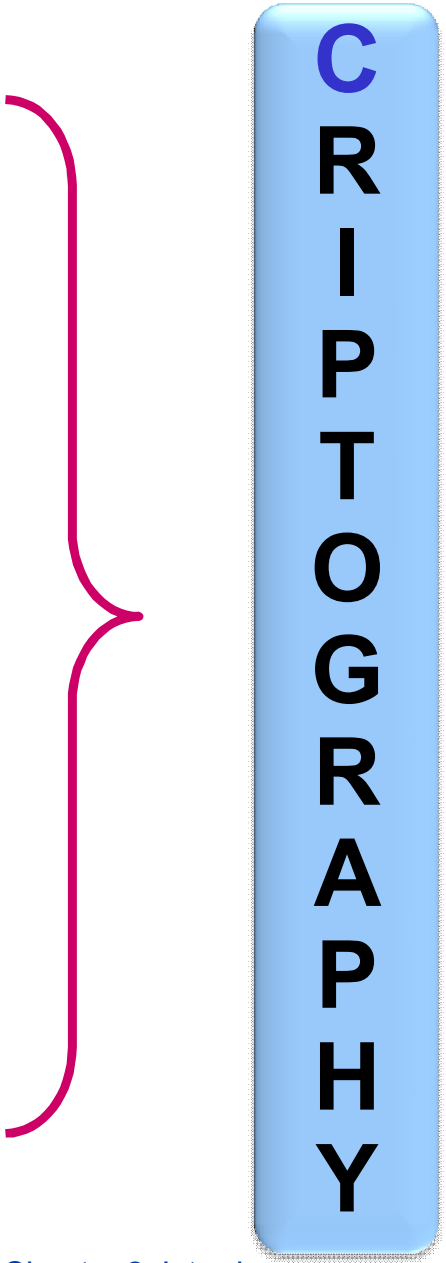
- **Authentication:**
  - **Guarantees the correct identification of origin and destination of the information**
    - Threat: Third-party masquerading as sender / receiver
- **Non-repudiation:**
  - **Guarantees that sender and receiver of a message can't deny its transmission**
    - Threat: Deny having transmitted or received certain data
- **Access Control:**
  - **Guarantees controlled access to information and systems to authorized entities**
    - Threat: Access of confidential data to non authorized entities

SCENARIOS

- **Integrity of the message**
  - How does B know that the message received from the sender A is the original and not a fake message?
- **Authenticity of the sender**
  - How does B know that the message received from the sender who says he is A is really that person?
- **Message Date**
  - How does B know that the message from A is recent and not a replay of a message previously sent from A?
- **Non-repudiation of the sender**
  - How can B prove that the message sent by A, and who now denies having sent it, really must have come from A?
- **Non-repudiation of the receiver**
  - How can A prove that the message sent to B, and who now denies having received it, really was sent?

SECURITY MECHANISMS

- Data encryption
- Message Digests
- Digital Signatures
- Authentication
- Key Exchange
- …



LOGICAL ACCESS CONTROL: AUTHENTICATION

- **Something that only one knows (password)**
  - ☺ Low costs, easy to invalidate / to configure / to register
  - ☹ Cession, capturing on introduction, guessing, induction
- **Something that is portable (key, intelligent card,...)**
  - ☺ Similar to passwords, but higher security
  - ☹ Multiple access, loss, robbery / copies / falsification, costs
- **Some physical characteristic (biometrics)**
  - ☺ Very secure
  - ☹ High costs

AUTHENTICATION: PASSWORDS

- Easy to remember
- Difficult to guess(?)
- Attacks on passwords very common:
  - Use well-known user accounts (“guest”)
  - Use known user accounts
    - Try trivial passwords, very often successfully!
  - Theft of data bases with ciphered keys
    - Used for password cracking
      - Example: dictionary attack (25% in less than 2 hours)
  - Copy ciphered keys and retransmit them

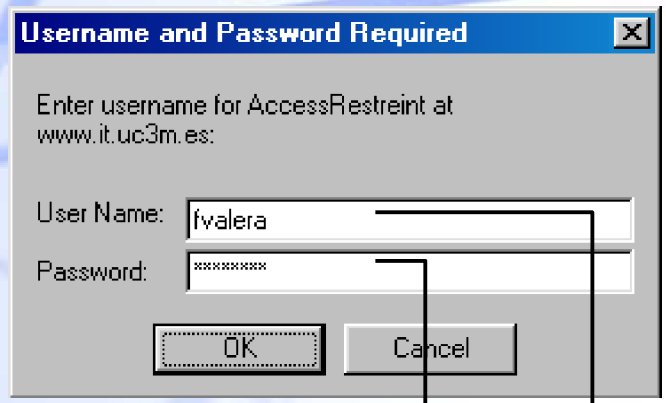
PASSWORDS POLICIES

- **Important: Users must choose good passwords**
  - A single bad key can compromise the whole system
- **Recommendation:**
  - Mix letters, digits and alphanumeric signs
  - Mix uppercase and lowercase
  - Never: Dictionary word or variations.
- **Example: UNIX passwords**
  - 8 characters, 7 bits/character, 56 bits DES
  - Problem: Passwords from a dictionary
    - ✓ Not equally probable (some are very popular)
    - ✓ Equivalent to a ~19 bit key
  - ➢ Easier to break using brute-force methods
- **Control mechanisms**

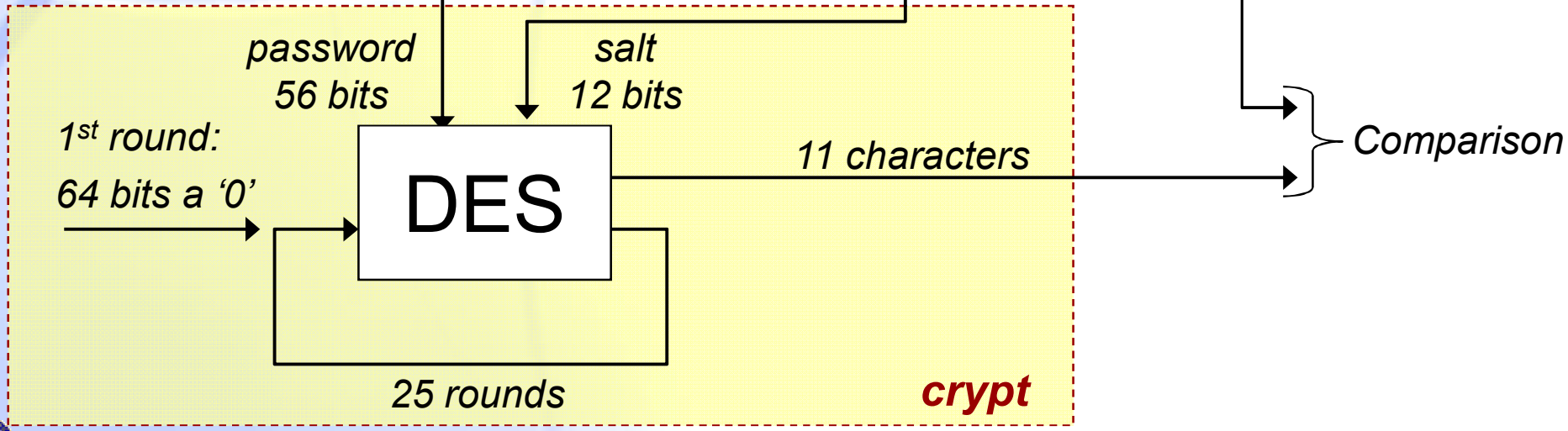
PASSWORDS POLICIES

- Change default passwords!
- Never store passwords in network files
- Restrict the access to files (/etc/passwd)
- Don’t give “hints” (finger daemon)
- Invalidation after “n” failures
  - Password blocking
- Force periodic password changes
  - Password aging
- Don’t send clear-text passwords
  - POP, telnet!

EXAMPLE: DES IN UNIX



LOGIN	SALT	PASSWORD
krogers	1w	tzf2DA0SZM.
pointer	oo	HJKJt8Ecqc6
master	13	mO7McGka4Kg
decimus	Gl	SMfUPWkhh/c
dracula	oo	CQMcBxVlb3l
cartman	xs	ARpupQK8hQE
fvalera	ro	tli3t3/cLql
smartman	lQ	YkoMoy0.O6w
michael	32	w3liMtCRAaE
jpintur	i1	V1k9xE4bH5g
japon	13	G7HMb/DMaXo
luke	po	rexMTCgEsHE



TERMINOLOGY

http://www.britannica.com

Cryptology. (from gr. *κρυπτος* hidden and *-logos*). *f.* the scientific study of cryptography and cryptanalysis

Cryptography. (from gr. *κρυπτος* hidden and *-grafía*). *f.* enciphering and deciphering of messages in secret code or cipher

Cryptanalisys. ***m.*** the solving of cryptograms or cryptographic systems

Cryptogram. ***m.*** a figure or representation having a hidden significance

TERMINOLOGY

http://www.britannica.com

Encrypt. *tr.* Encipher, encode.

Encode. *tr.* to convert from one system of communication into another; *especially*: to convert (a message) into code.

Code. *tr.* a system of symbols (as letters or numbers) used to represent assigned (and often secret) meanings.

Encipher. *tr.* to convert (a message) into cipher.

Cipher. *tr.* (a) a method of transforming a text in order to conceal its meaning. (b) a combination of symbolic letters

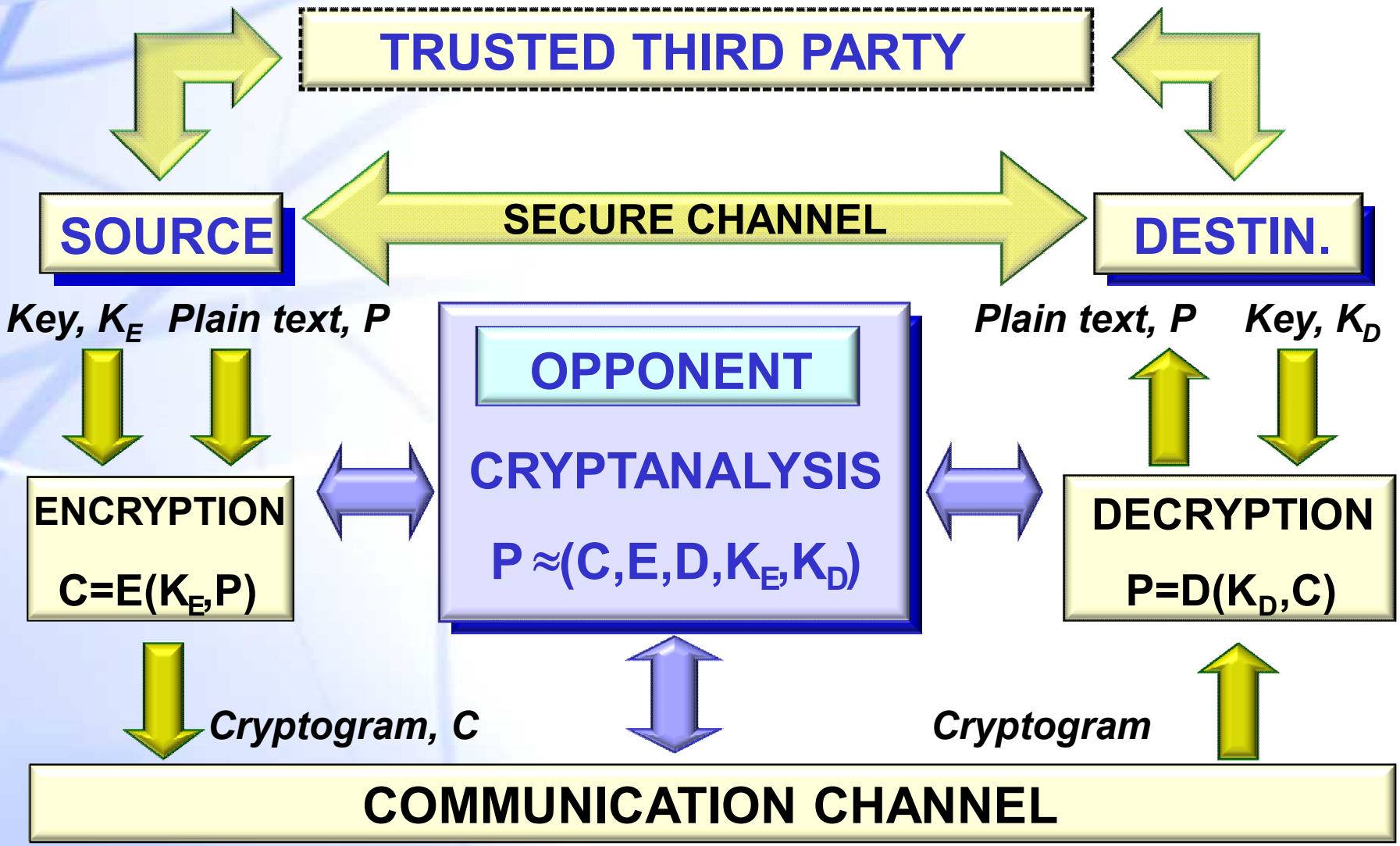
CRYPTOSYSTEM

- **Cryptosystems:**
  - Alphabet: for writing not encrypted text (P, plain text or clear text) and encrypted text (C, cryptograms)
  - Key space: all possible keys for encryption (kc) and decryption (kd)
  - Encryption (E) and decryption (D) transformations: function from the alphabet to the same alphabet.

$$D_{kd}[C=E_{ke}(P)]=P$$

- **Cryptosystem transformation:**
  - Symmetric (conventional encryption, secret key encryption): the encryption and decryption key are the same (ke=kd=k)
  - Asymmetric (public key encryption): the encryption key and decryption key are different (ke≠kd)

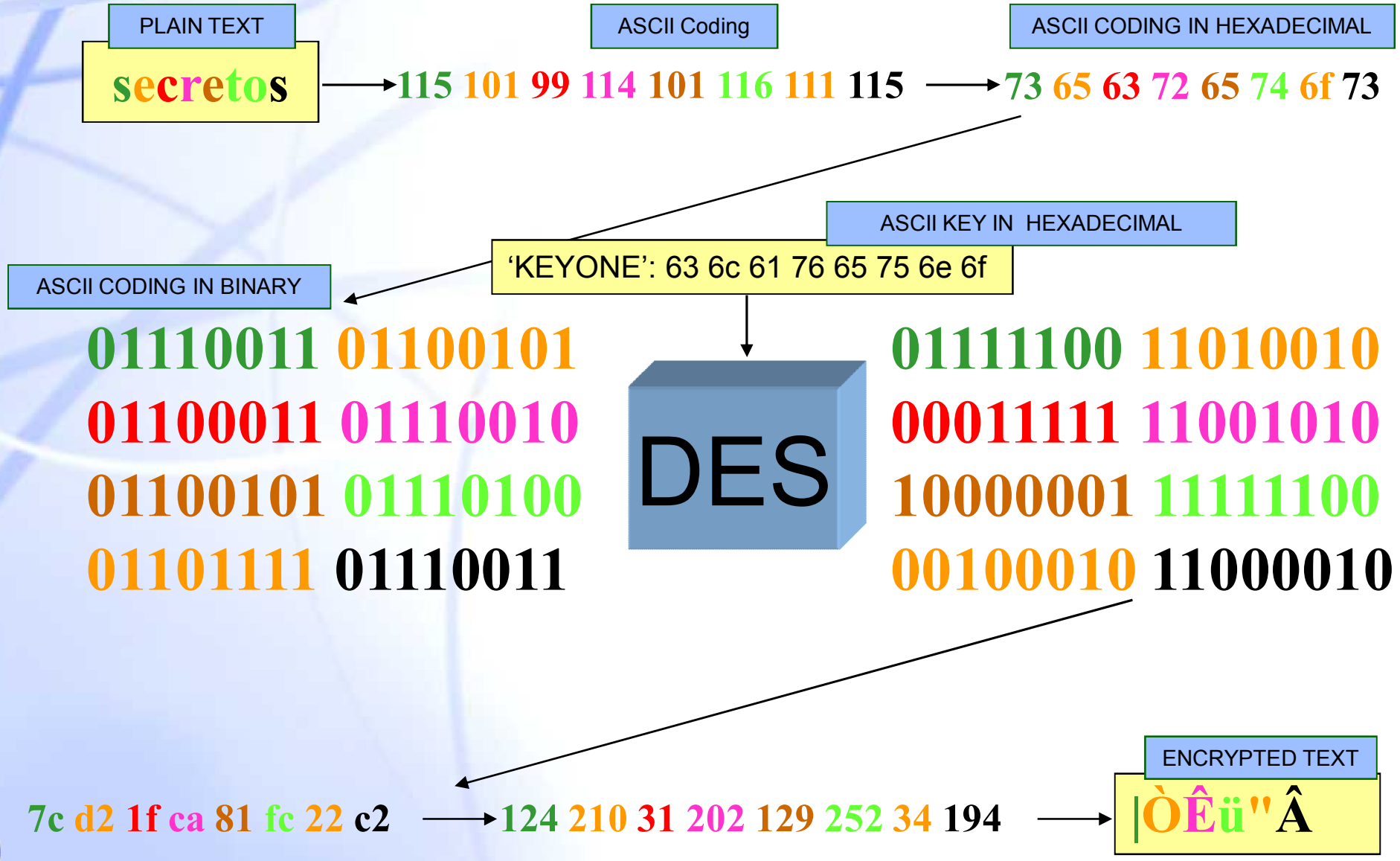
CRYPTOSYSTEM MODEL



ASSUMPTIONS

- **To carry out a "threats analysis" we have to suppose the opponent's resources**
- **Worst case (exaggerated?)**
  - Real time interception and inspection of every packet
  - Message alteration, creation and repetition
  - Brute-force attack against obsolete algorithms or when having enough information
  - Sources of attacks are known users
- **These days, wireless networks proliferation makes perfectly valid some of the above assumptions.**

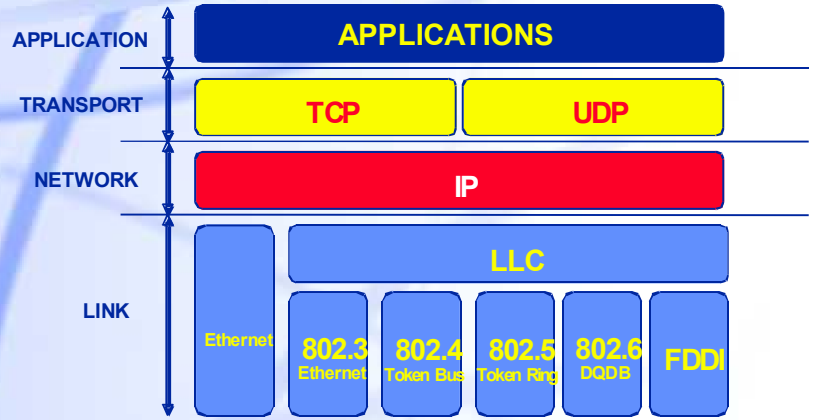
ENCRYPTION EXAMPLE

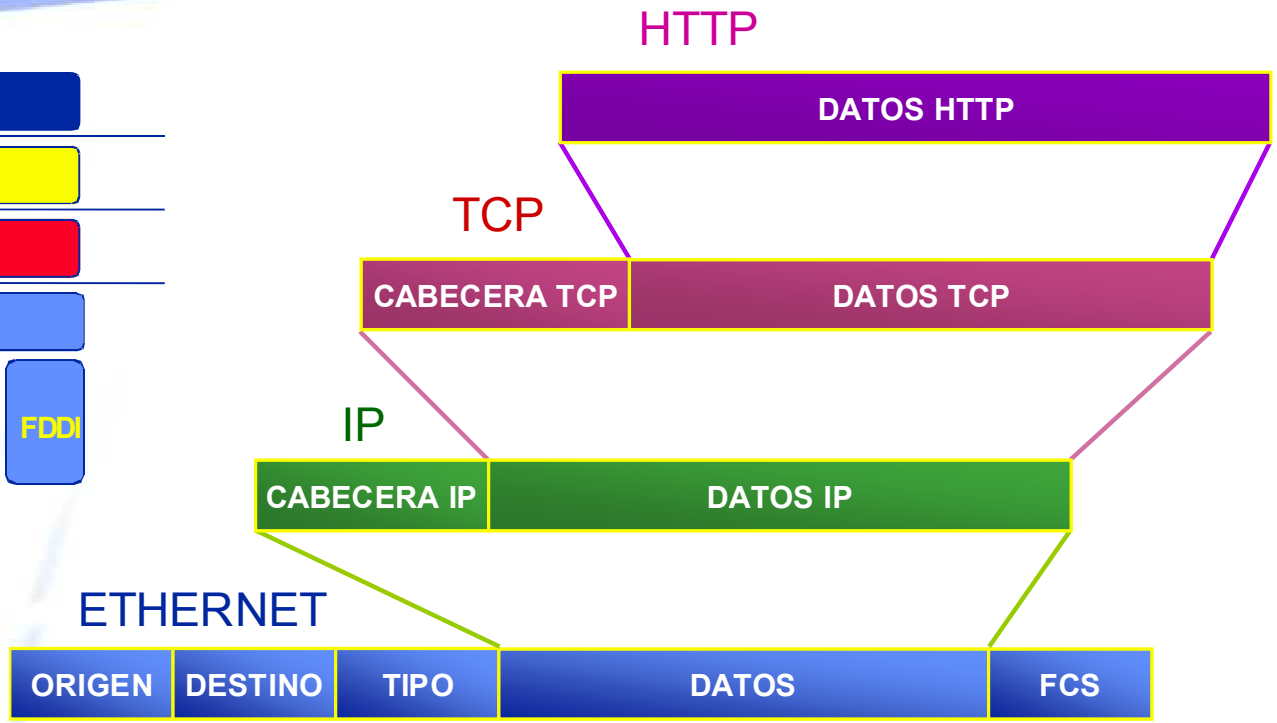


PLACEMENT OF ENCRYPTION

- Hop-by-bop
- End-to-end

PLACEMENT OF ENCRYPTION





- The lower you encrypt:
  - More information to encrypt
  - Easier to do it in hardware
  - Fewer keys in the open
  - Fewer keys necessary
  - Authentication at a coarser level