Secure Programming

A.A. 2022/2023

Corso di Laurea in Ingegneria delle Telecomnicazioni

F. Security & Protection 2

Paolo Ottolino

Politecnico di Bari

DIPARTIMENTO DI INGEGNERIA ELETTRICA E DELL'INFORMAZIONE

Secure Programming Lab: Course Program

A. Intro Secure Programming: «Who-What-Why-When-Where-How»
B. Building Security in: Buffer Overflow, UAF, Command Inection
C. SwA: Weaknesses, Vulnerabilities, Attacks
D. SwA (Software Assurance): Vulnerabilities and Weaknesses (CVE, OWASP, CWE)
E. Security & Protection: Objectives (CIA), Risks (Likelihood, Impact), Rating Methodologies
F. Security & Protection: Security Indicators, BIA, Protection Techniques (AAA, Listing, Duplication etc.)
G. Architecture and Processes: App Infrastructure, Three-Tiers, Cloud, Containers, Orchestration
H. Architecture and Processes 2: Ciclo di Vita del SW (SDLC), DevSecOps (OWASP DSOMM, NIST SSDF)
I. Free Security Tools: OWASP (ZAP, ESAPI, etc), NIST (SAMATE, SARD, SCSA, etc), SonarCube, Jenkins
J. Dynamic Security Test: VA, PT, DAST (cfr. VulnScanTools), WebApp Sec Scan Framework (Arachni, SCNR) :
K. Operating Environment: Kali Linux on WSL
L. Python: Powerful Language for easy creation of hacking tools
M. Exercises: SecureFlag

F Security & Protection

Agenda

1. **Protection Techniques: Crypt, AAA, Awareness, Duplication etc.**
2. **BIA: Business Impact Analysis**
3. **Security Indicators: KPI, KGI, SLA etc.**
4. **Security Risk Management**

F1 Protection Techniques

O.S. Mechanisms 1/2

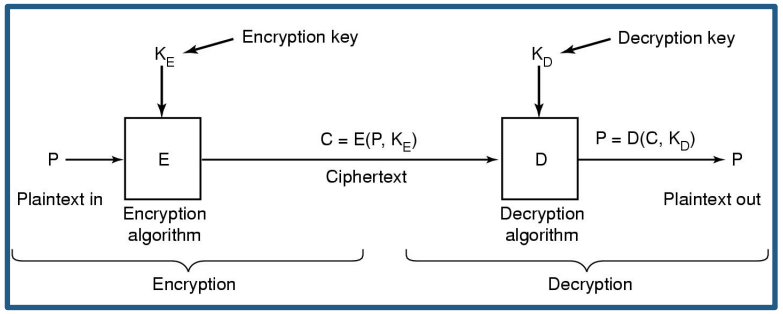
Mechanisms implemented in the OS, depending on the functionality to provide and the attacks to defend against.

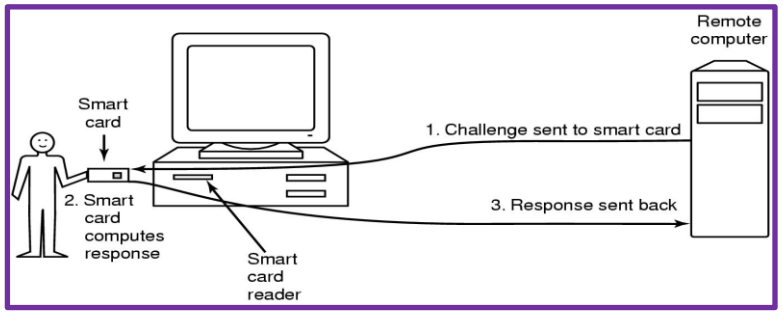
1. **Cryptography**: **Secret (Symmetric) Key**, **Public (Asymmetric) Key**, **Digital Signature**
   Information codifying ➔ κρυπτός = hidden, γραφω = write

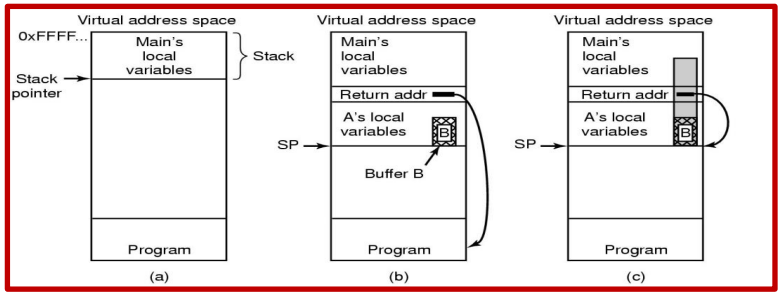
2. **AAA**: **Password**, **Physical Object**, **Biometrics**, **Permission**, **Log-Trails**
   Methods for ascertaining the declared identity:
   - Something you know
   - Something you have
   - Something you are

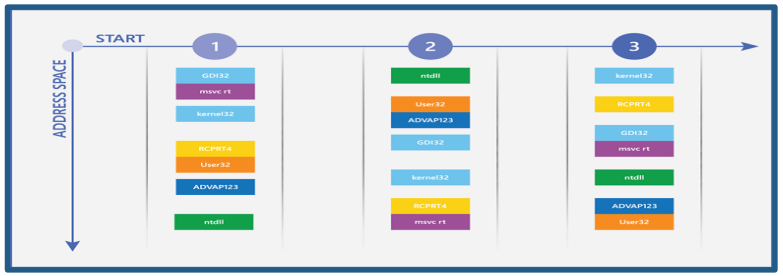
3. **Attacks**: **Trap Doors**, **Buffer Overflow**, **Code Injection**, **Rootkits**
   Typical systems breach methodologies.

4. **Protection**: **ACL**, **NX**, **ASLR**, **Code Signing**, **Jailing**, **TCB**
   Defense Mechanisms.









F1 Protection Techniques

O.S. Mechanisms 2/2

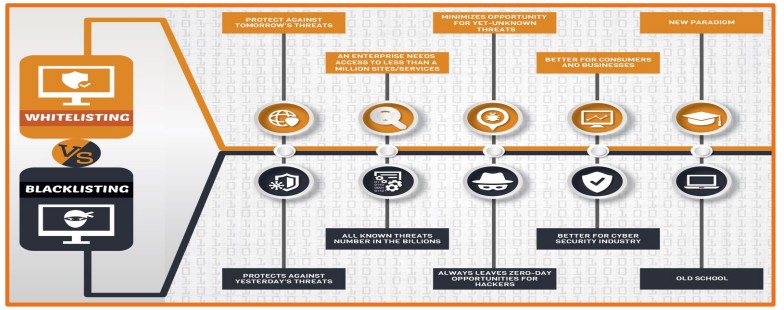
Mechanisms implemented in the OS, depending on the functionality to provide and the attacks to defend against.

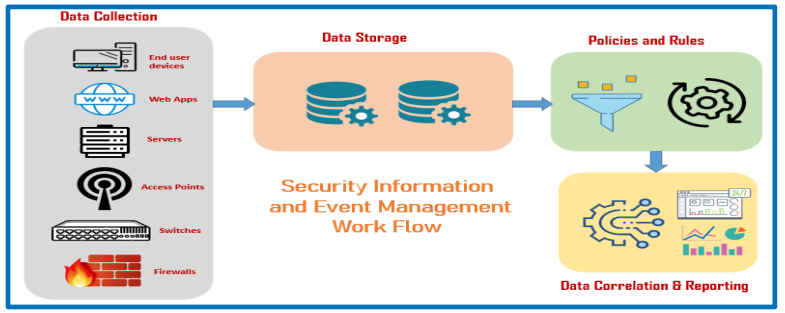
5. **Filters**: allow or deny, based on lists of known items, to be recognized through some IDs (like IP, Uid, DomainName etc.)
   - **Whitelist** → allow
   - **Blacklist** → deny

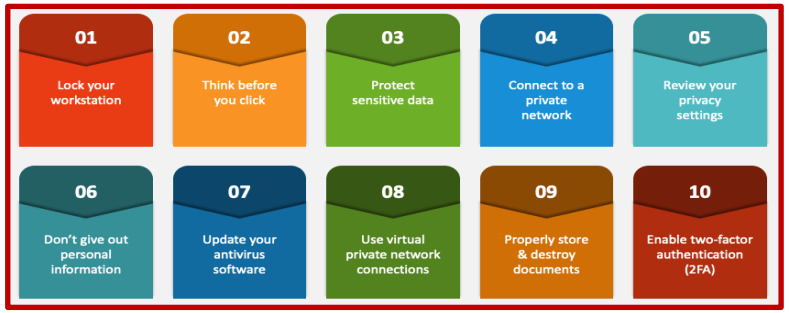
6. **Logging**: record of the events occurring within an organization's systems and networks. Mandatory requirements inside the company should entail:
   - **Log Generation**: logging requirements
   - **Log Trasmission**: saving to a log management infrastructure
   - **Log Storage**: rotation, retention

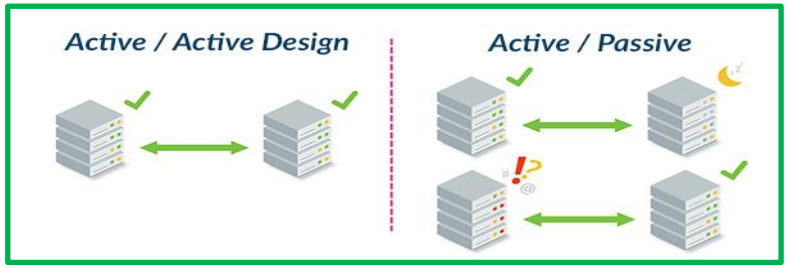
7. **Awareness**: improvement of IT user knowledge and consciousness about IT, in order to remediate from easiest cyberattacks

8. **Duplication**: automated process of copying data, as well as providing additional elaboration capabilities, in order to preserve from accidental losses and denial of services





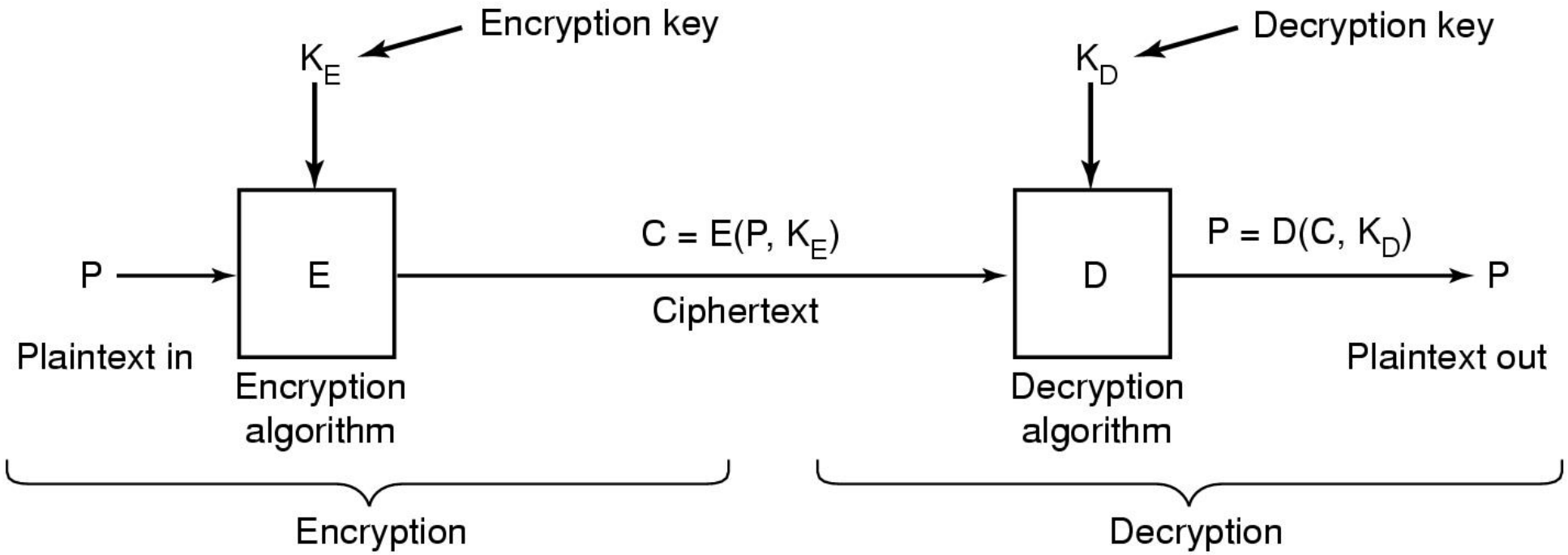




F1a1 Protection Techniques

Cryptography 1/8

General encryption mechanism (encryption)

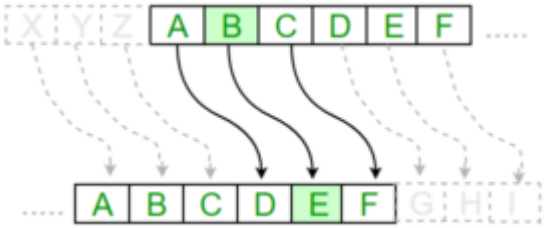


1. **Secret (Symmetric) Key**: $K_E = K_D$ (the key should be maintained secret/shared on another channel)
2. **Public (Asymmetric) Key**: $K_E \neq K_D$ (the key K_D is publicly available; K_E is private: never shared)

F1a2 Protection Techniques

Cryptography 2/8

Secret (Symmetric) Encryption: secret key



Substitution cypher(Giulio Cesare): the cyphertext is obtained by replacing each letter P with the letter P + K. Julius Caesar first used K = «C» (as in the figure) and then «D»

Usage: message and key must be exchanged on 2 different channels :

- **Key**: preliminary exchange channel

- **Message**: usual channel

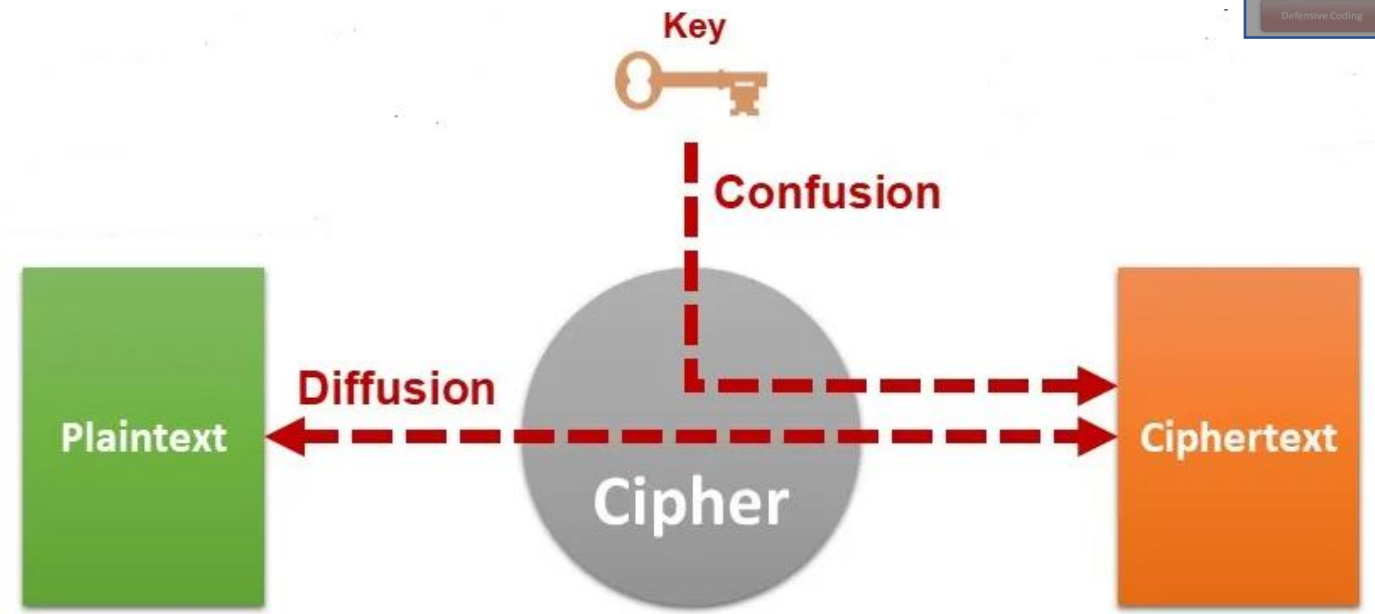
F1a3 Protection Techniques

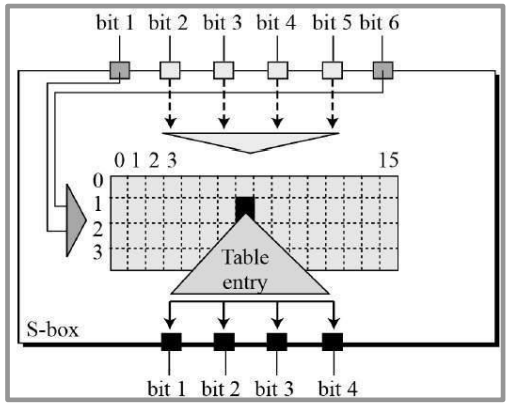
Cryptography 3/8

Secret (Symmetric) Encryption: secret key

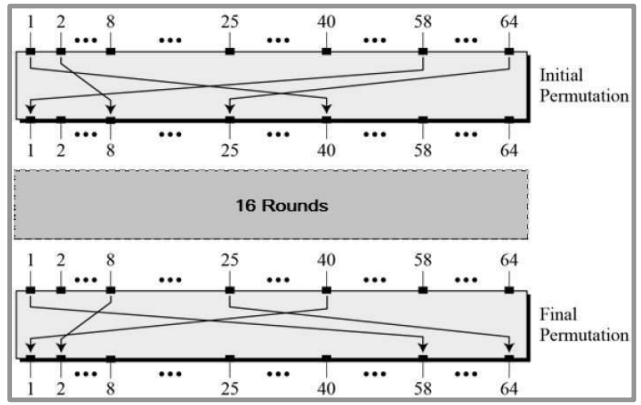
Confusion & Diffusion (Claude Shannon): from «*A Mathematical Theory of Cryptography*", 1945 the 2 qualities of a secure cipher are reported :

- **Confusion**: each binary digit (bit) of the ciphertext must depend on multiple parts of the key, obscuring the connections between the two. This is for hiding the relationship between the ciphertext and the key ➔ difficult to find the key from the ciphertext. Provided by the **Substitution Boxes** (**S-Box**)
- **Diffusion**: changing a single bit of the plaintext changes about half of the bits in the ciphertext ➔ hide the statistical relationship between the ciphertext and the plaintext. Provided by **Permutation Boxes** (**P-Box**)





S-Box

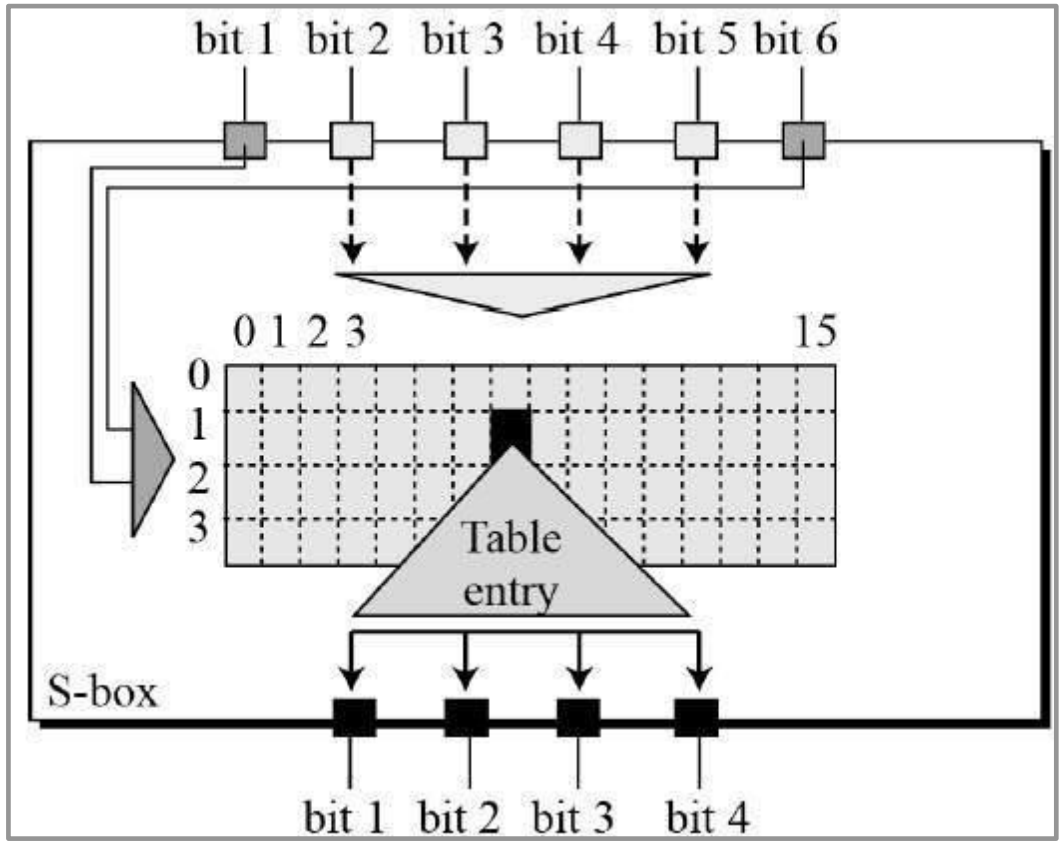


P-Box

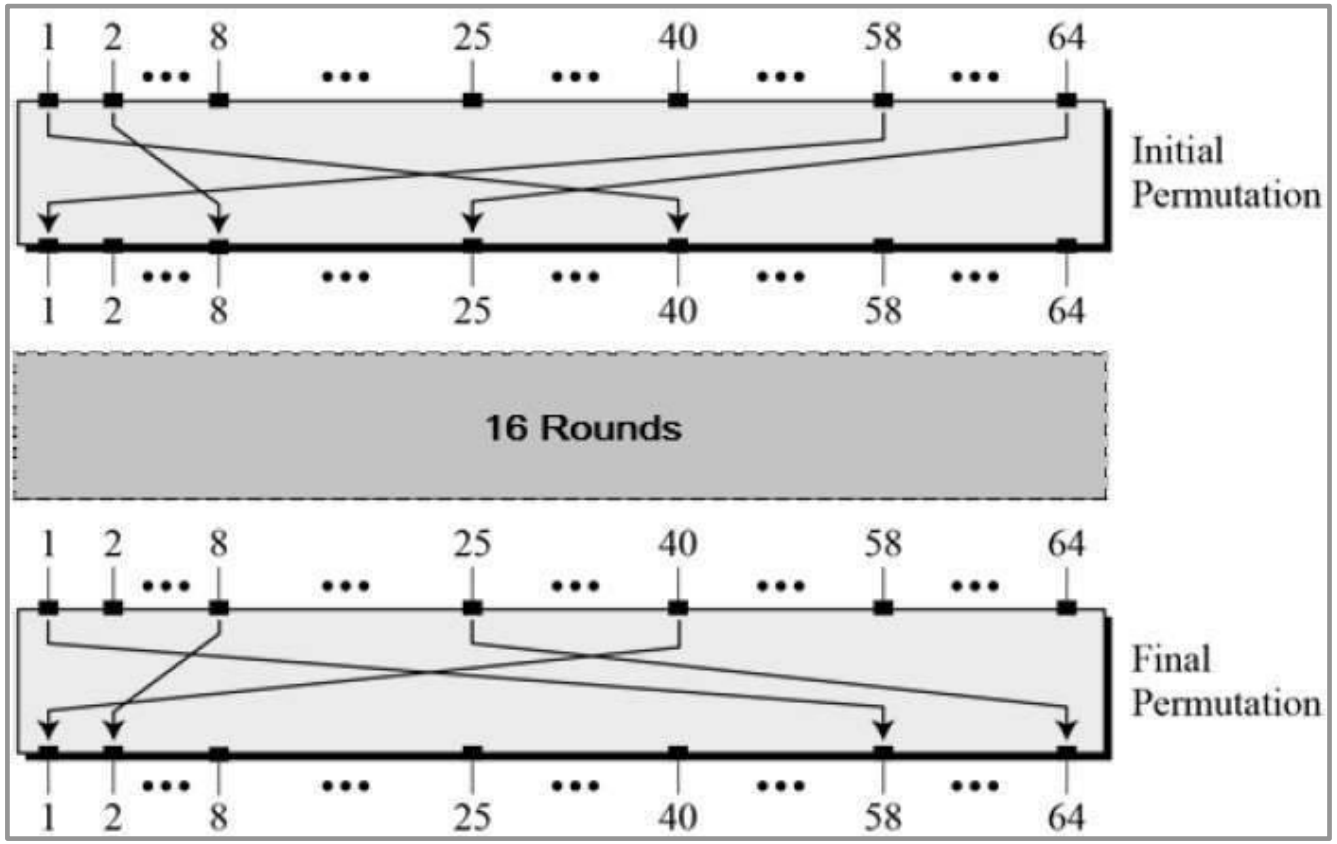
F1a3 Protection Techniques

Cryptography 3b/8

Secret (Symmetric) Encryption: S-Box, P-Box



S-Box



P-Box

F1a4 Protection Techniques

Cryptography 4/8

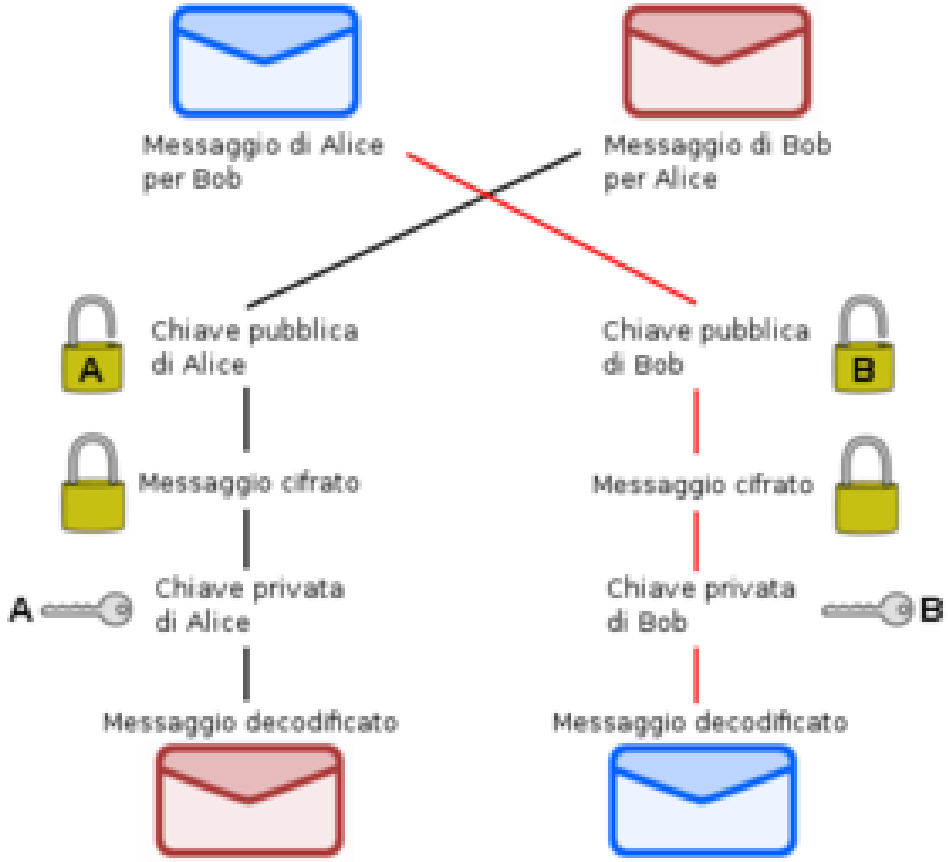
Public (Asymmetric) Encryption: asymmetric cryptography (public and private keys). RSA algorithm from 1973, at Government Communications Headquarters, by Clifford Cocks, declassified 1997.

Encryption: $C = E(P, K_E)$
Es. $K_E = (17,23)$
RSA_{2048} ➔ (p_{1024}, q_{1024})

Decryption: $P = D(C, K_D)$
Unable to figure out the key K_E (p, q) from K_D (p x q)
Es. $K_D = 17 \times 23 = 391$; $K_E = (17,23)$ to find K_E we need to factor prime numbers

Usage: possible also to:

- encrypt with K_D (public key, known among the interlocutors)
- Decrypt with K_E (private key, known only by the owner)

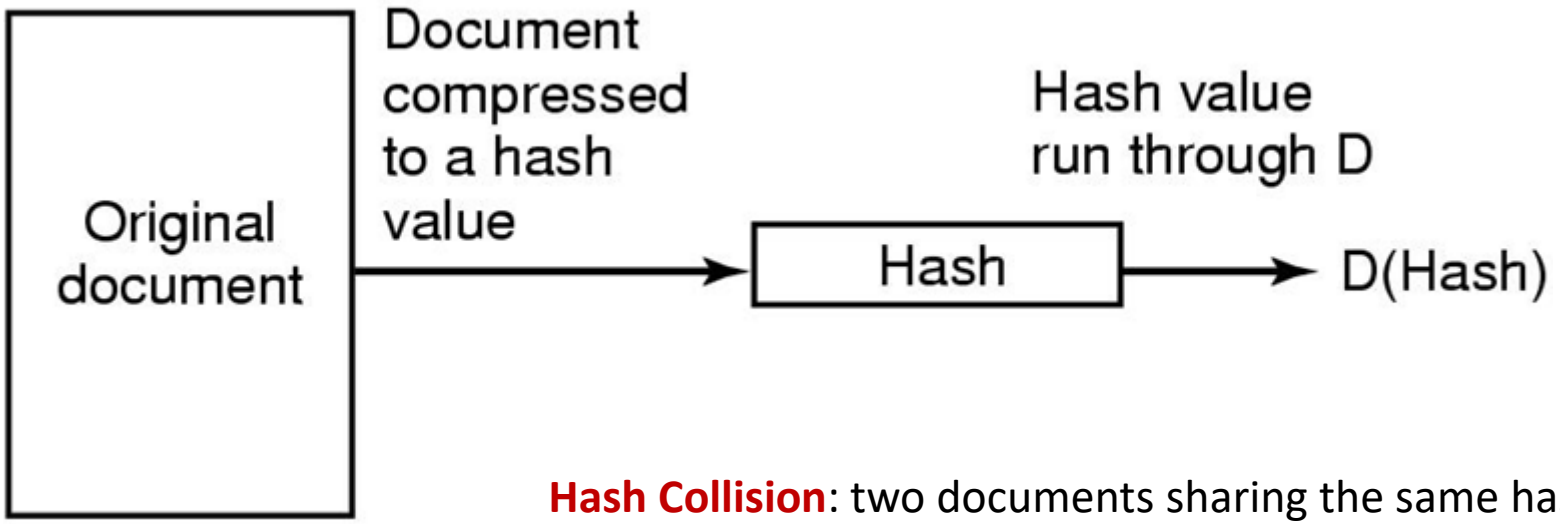


➔ **Same channel** for sharing the keys (public only)
➔ **Crypting** + **Key-Sharing** → **Non-Repudiation**
➔ **Much more expensive** than symmetric encryption

F1a5 Protection Techniques

Cryptography 5/8

Hash: irreversible operation. Calculation of a plaintext attribute

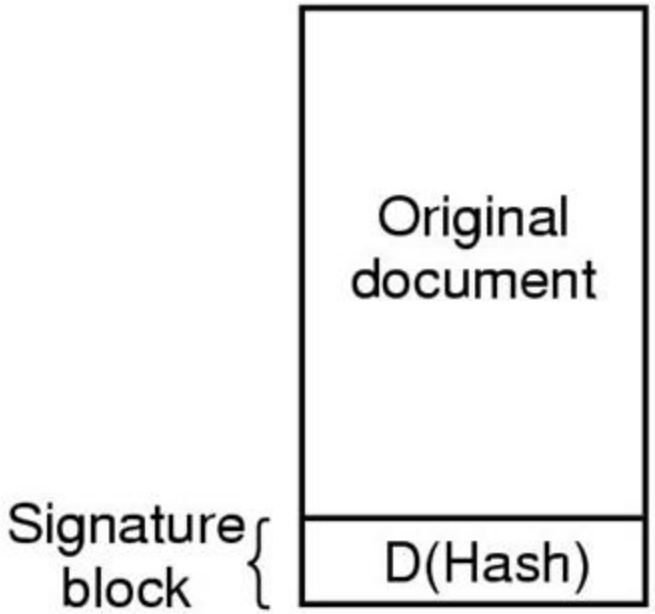


Hash Collision: two documents sharing the same hash
Possible since documents can be much longer than the hash (ca. 256 bits)
eg. MD5 and SHA-1 are algorithms in widespread use but **vulnerable** to hash-collision, based on **differential cryptanalysis**

F1a6 Protection Techniques

Cryptography 6/8

Digital Signature: "Signing" of the hash made using the private key



Signature: E(Hash, K_E). To verify, it is possible :

- Get the Hash = D (E, K_D) (decrypt using Public-key mechanism)
- Recalculate H (Original Document)
- Compare with Hash

Signature = **Public (Asymmetric) Encryption** + **Hash**

F1a7 Protection Techniques

Cryptography 7/8

Cypher Suite: set of algorithms used to secure network connections based on Transport Layer Security (TLS).

TLS Specification: RFC 8446, Transport Layer Security 1.3

- Key Exchange
- Certificate Key ➔ Asymmetric Encryption
- Transport Cipher ➔ Symmetric + Cypher Block Mode
- Integrity ➔ Hash


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After : Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                 OU=Certification Services Division,
                 CN=Thawte Server CA/Email=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                    68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                    85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                    6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                    6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                    29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                    6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                    3a:c2:b5:66:22:12:d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8c:ca:d9:
        a0:6f:49:1a:e6:da:51:e3:60:70:6c:04:61:11:a1:1a:c0:40:
        3e:59:43:7d:4f:95:3d:a1:6b:b7:0b:62:98:7a:75:8a:dd:68:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:cf:c7:f2:18:f9:89:bc:a3:ff:8a:23:2c:
        70:47
```

Digital Certificate x509v3 (RFC 2459)

➔ Delegation of responsibility: identity

➔ PKI: Public Key Infrastructure

F1a7 Protection Techniques

Cryptography 7b/8

Cypher Block Mode: how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

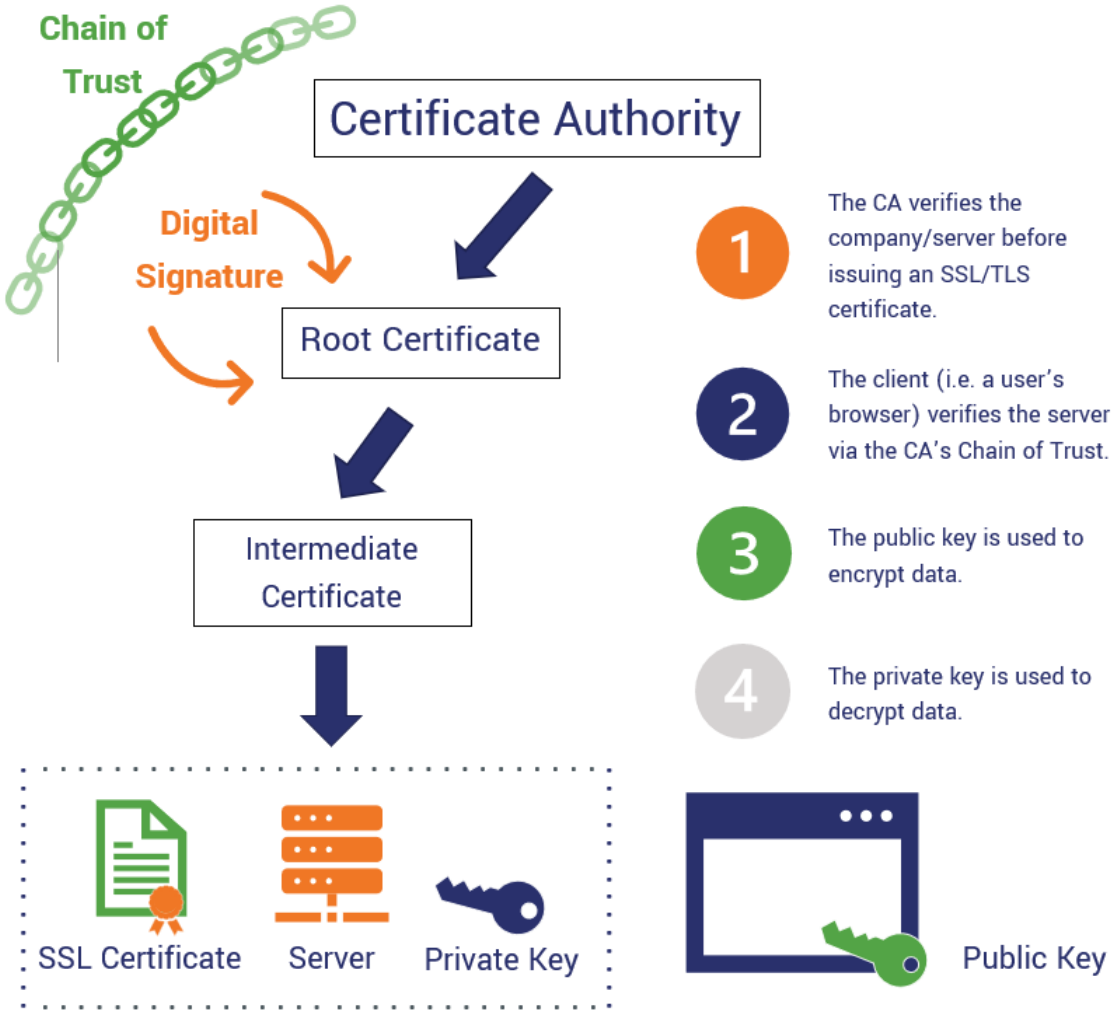
The earliest modes of operation, ECB, CBC, OFB, and CFB (see below for all), date back to 1981 and were specified in FIPS 81, *DES Modes of Operation*. In 2001, the US National Institute of Standards and Technology (NIST) revised its list of approved modes of operation by including AES as a block cipher and adding CTR mode in SP800-38A, *Recommendation for Block Cipher Modes of Operation*. Finally, in January, 2010, NIST added XTS-AES in SP800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*. Other confidentiality modes exist which have not been approved by NIST. For example, CTS is ciphertext stealing mode and available in many popular cryptographic libraries.

Mode		Formulas	Ciphertext
Electronic codebook	(ECB)	$Y_i = F(\text{PlainText}_i, \text{Key})$	Y_i
Cipher block chaining	(CBC)	$Y_i = \text{PlainText}_i \text{ XOR } \text{Ciphertext}_{i-1}$	$F(Y, \text{Key})$; $\text{Ciphertext}_0 = \text{IV}$
Propagating CBC	(PCBC)	$Y_i = \text{PlainText}_i \text{ XOR } (\text{Ciphertext}_{i-1} \text{ XOR } \text{PlainText}_{i-1})$	$F(Y, \text{Key})$; $\text{Ciphertext}_0 = \text{IV}$
Cipher feedback	(CFB)	$Y_i = \text{Ciphertext}_{i-1}$	Plaintext XOR $F(Y, \text{Key})$; $\text{Ciphertext}_0 = \text{IV}$
Output feedback	(OFB)	$Y_i = F(Y_{i-1}, \text{Key})$; $Y_0 = F(\text{IV}, \text{Key})$	Plaintext XOR Y_i
Counter	(CTR)	$Y_i = F(\text{IV} + g(i), \text{Key})$; IV = token()	Plaintext XOR Y_i

F1a7 Protection Techniques

Cryptography 7c/8

Digital Certificate: electronic document used to prove the validity of a public key



The 6 Main Components of PKI: several critical components within the public key infrastructure

- **X.509 digital certificates** — These types of certificates include a key, information about the identity of the owner (of the certificate and keys), and the digital signature of the certificate authority. These types of certificates include:
  - SSL/TLS website security certificates,
  - S/MIME (client authentication) certificates,
  - Code signing certificates, and
  - Document signing certificates.
- **Digital signatures** — Digital signatures are what guarantees that a message, file, or data hasn't been altered in any way. It uses an encrypted hash of a message to ensure the integrity of your data by making it so that nobody can modify the message without the recipient finding out.
- **Public and private key p**airs (**asymmetric** and **symmetric**) — PKI works because of the key pairs that encrypt and decrypt data. In asymmetric encryption, there's a public key that's shared with everyone and a matching private key that's kept secret. In symmetric encryption, there is one key that both parties use to communicate.
- **Certificate authorities** (**CAs**) — Certificate authorities are what make the whole PKI system trustworthy. CAs verify parties and issue certificates. Without CAs, PKI simply wouldn't work because anybody could just issue certificates to themselves saying that they're Amazon.com, Bill Gates, or whomever they feel like impersonating.
- **Chain of trust** — The chain of trust is a series of certificates (root, intermediate, and leaf certificates) that links back to the issuing CA who signed off on it.
- **Proper certificate management tools**, policies, processes, and procedures — This includes the use of a certificate management tools such as a certificate manager.

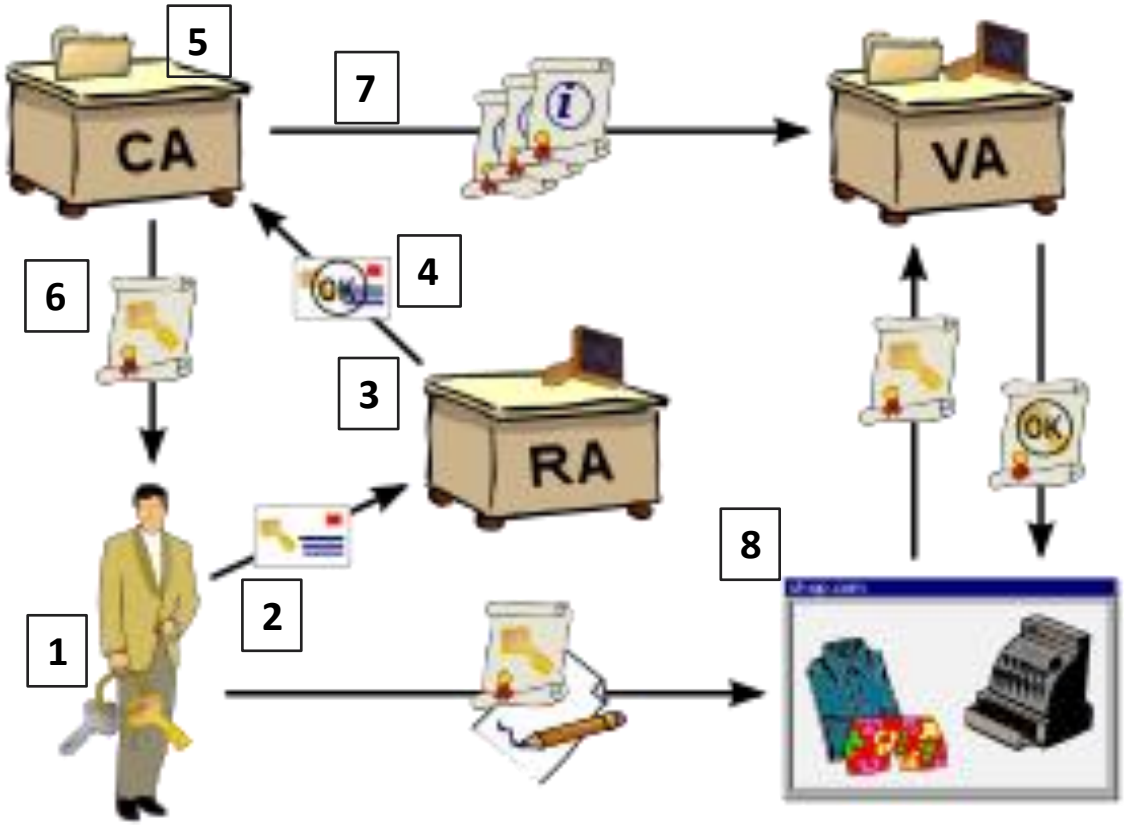
F1a7 Protection Techniques

Cryptography 7d/8

Public Key Infrastructure: electronic document used to prove the validity of a public key

Digital Certificate Process: several critical components within the public key infrastructure

1. Bob generates her key pair.
2. Contact the territory's Registration Authority, identifying and providing the public key to be certified.
3. The RA (Registration Authority) asks the CA, chosen by Bob or predefined for the territory, to generate a certificate for.
4. The RA approves the certification request after appropriate checks.
5. The CA signs the certificate generated for Bob with its private key.
6. Bob receives her certificate signed by the CA and the root certificate of the CA by e-mail.
7. Bob certificate is published by the CA on its own certificate server or on a linked site of the VA Validation Authority type.
8. Every time she signs a document, Bob will attach her own digital certificate or its serial number.



F1a8 Protection Techniques

Cryptography 8/8

PKCS (Public-Key Cryptography Standards): cryptographic specifications produced by RSA Inc. laboratories since 1991.

PKCS	Argomento	Standard Attuale
PKCS#1	RSA Cryptography	RFC 3447
PKCS#3	Diffie-Hellman Key Exchange	RFC 2631
PKCS#5	Password Enchyphering	RFC 2898
PKCS#7	Message Signing and Encryption using PKI	RFC 2315
PKCS#8	Information syntax for the Private Key	RFC 5208
PKCS#9	Attribute types in the PKCS	RFC 2985
PKCS#10	Syntax for the Certificate Sign Request (**CSR**)	RFC 2986
PKCS #11	Uniform Resource Identifier (URI)	RFC 7512
PKCS #12	Syntax for Transferring Identity Information	RFC 7292
PKCS #15	Cryptographic applications in Smart Cards	ISO/IEC 7816-15

RFC: Request for Comment https://www.ietf.org/standards/rfcs/. IETF: Internet Engineering Task Force

F1b Protection Techniques

AAA 1/16

Identification: preliminary process of assigning a unique identifier to a user.

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. [PCI-DSS]

IdM: Identity Management

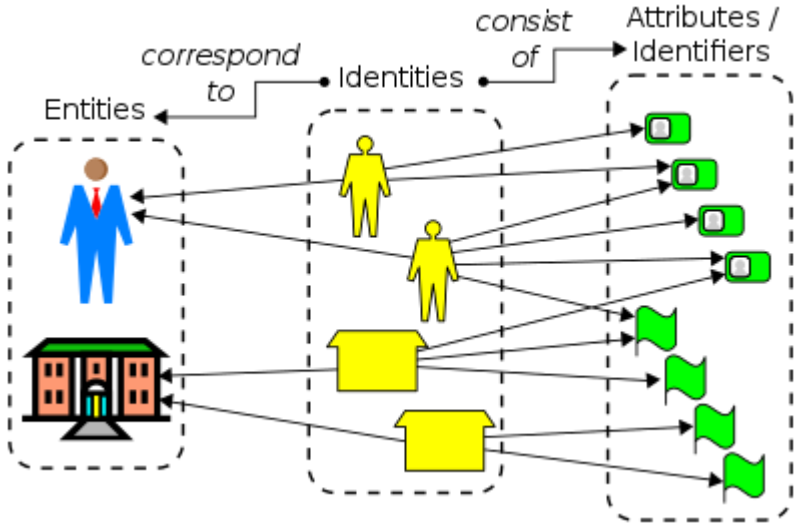
IdG: Identity Governance

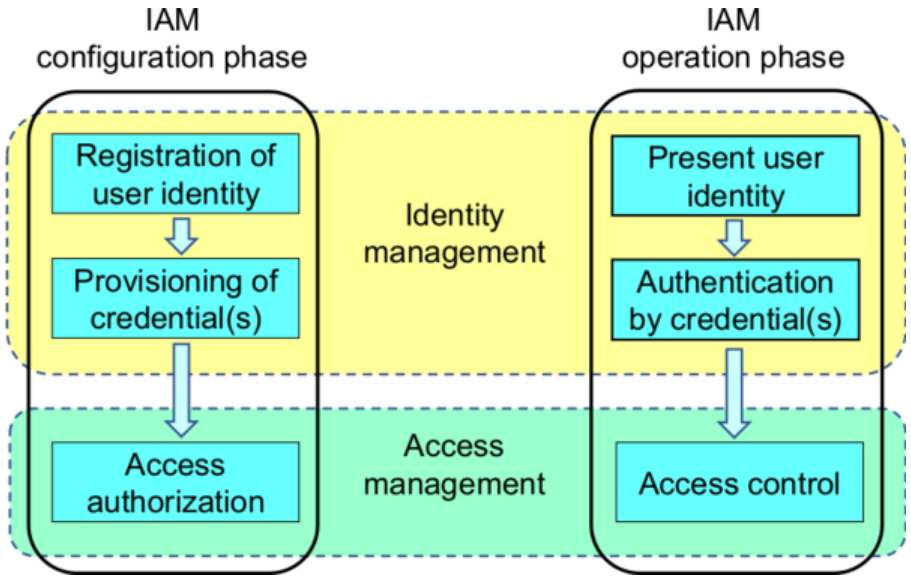
F1b Protection Techniques

AAA 2/16

Identification: preliminary process of assigning a unique identifier to a user.

IdM (Identity Management) framework of policies and technologies to ensure that the right users (that are part of the ecosystem connected to or within an enterprise) have the appropriate access to technology resources. Identity and access management systems not only identify, authenticate, and control access for individuals who will be utilizing IT resources but also the hardware and applications employees need to access





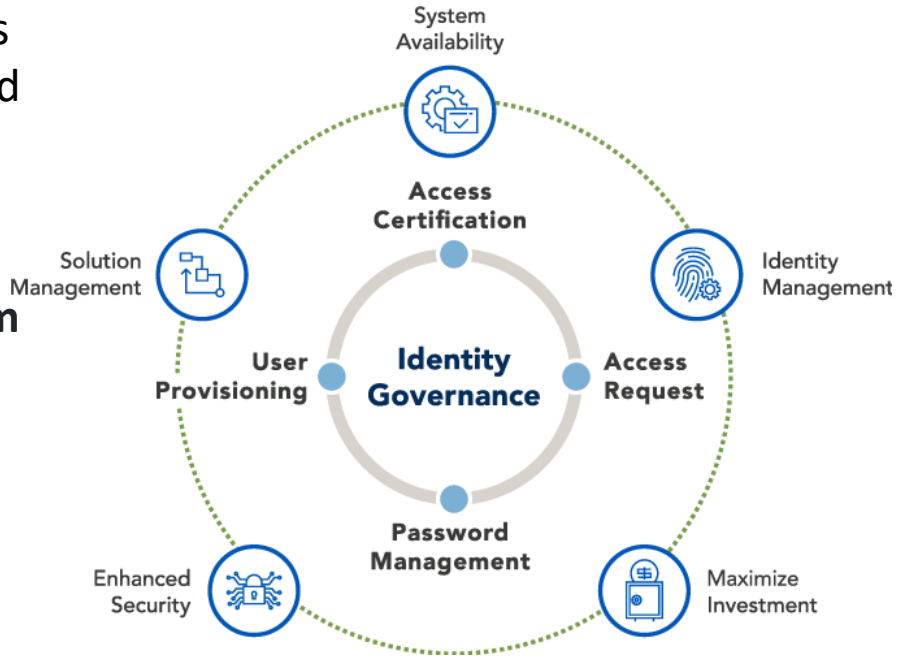
IAM (Identity & Access Management): organizational and technical processes for first registering and authorizing access rights in the configuration phase, and then in the operation phase for identifying, authenticating and controlling individuals or groups of people to have access to applications, systems or networks based on previously authorized access rights

F1b Protection Techniques

AAA 3/16

Identification: preliminary process of assigning a unique identifier to a user.

IdG (Identity Governance): organizational and technical processes for first registering and authorizing access rights in the configuration phase, and then in the operation phase for identifying, authenticating and controlling individuals or groups of people to have access to applications, systems or networks based on previously authorized access rights.
Involved functionalities:



- **Access Request -** Empower your business with a robust **self-service platform** for requesting and approving access to applications.

- **User Provisioning -** Streamline your **onboarding** and **off–boarding** process with best practice configurations and workflows.

- **Access Certification -** Automate the process of **reviewing** user access **privileges** across your organization.

- **Password Management -** Offer users an intuitive, **self-service experience** for managing and resetting passwords from any device.

F1b Protection Techniques

AAA 4/16

Authentication: procedure aimed at certifying the authenticity of the user who is preparing to interact with the system.

3 Factors

Knowledge: Something you know(e.g. Password, PIN)

Possession: Something you have (e.g. Smart Card, SmartPhone)

Biometric: Something you are (e.g. retina, fingerprints)

Multifactor Authentication: use of multiple types of factors during the same authentication

F1b Protection Techniques

AAA 5/16

Password: code established by the user and stored (generally in encrypted form) on the system.

User Guessing: possible to establish the login-name in the

Bobbie, 4238, e(Dog, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron,1092)

LOGIN: mitch
PASSWORD: FooBar!-7
SUCCESSFUL LOGIN

(a)

LOGIN: carol
INVALID LOGIN NAME
LOGIN:

(b)

LOGIN: carol
PASSWORD: Idunno
INVALID LOGIN
LOGIN:

(c)

Encryption + Salt: in Unix passwords are stored encrypted (encrypted) together with a salt to prevent cracking.

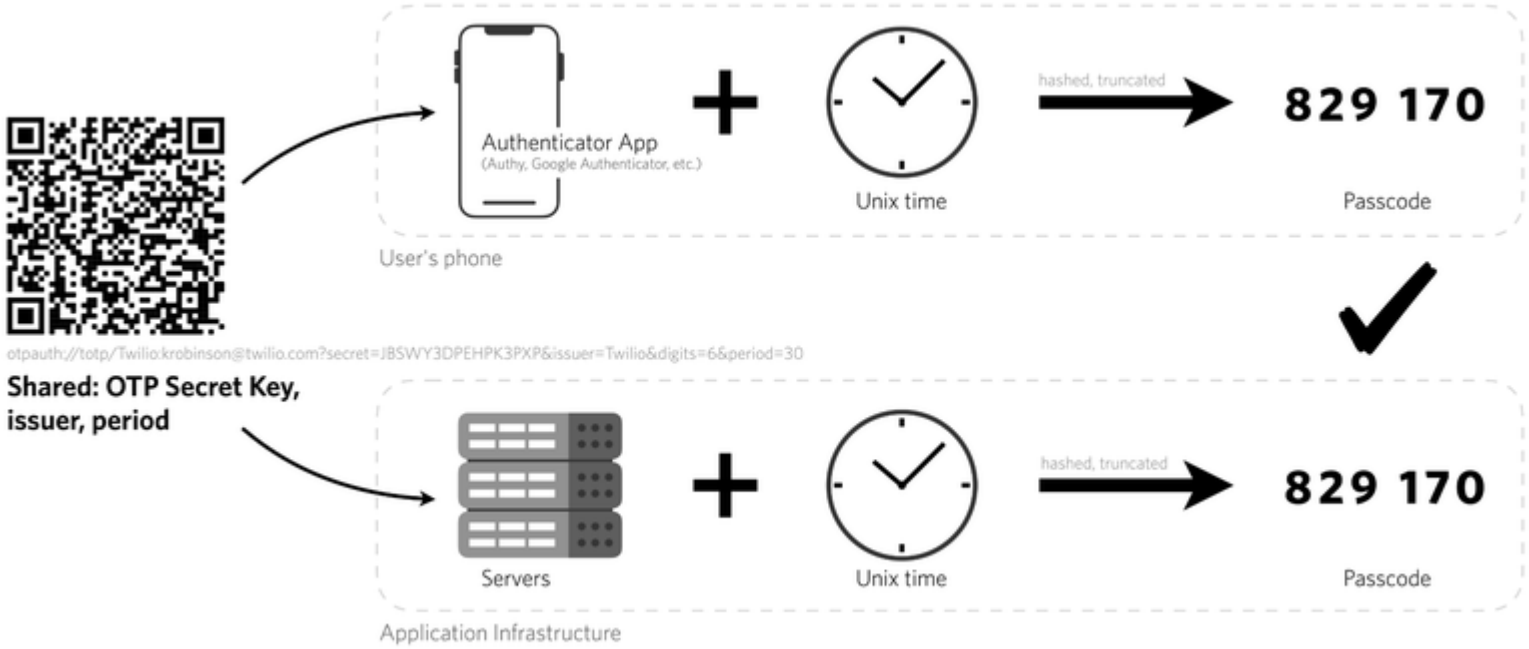
Password Quality (complexity): to make passwords less predictable, they must have certain characteristics (cfr. `/etc/security/pwquality.conf`)

- **minlen**: minimum lenght
- **minclass**: the minimum number of character types (uppercase, lowercase, numbers, special characters)**dictcheck**: password non nel dizionario (cracklib)
- **gecoscheck**: password does not contain user information present in the GECOS fields
- **usercheck**: password does not contain the user's login in any form
- **remember**: number of passwords contained in the history (non-reconfigurable)
- **aging**: maximum number of days a password can be used before it needs to be changed

F1b Protection Techniques

AAA 6/16

Physical Object: object you own. Provides for the use of libraries/external systems (e.g. TOTP)



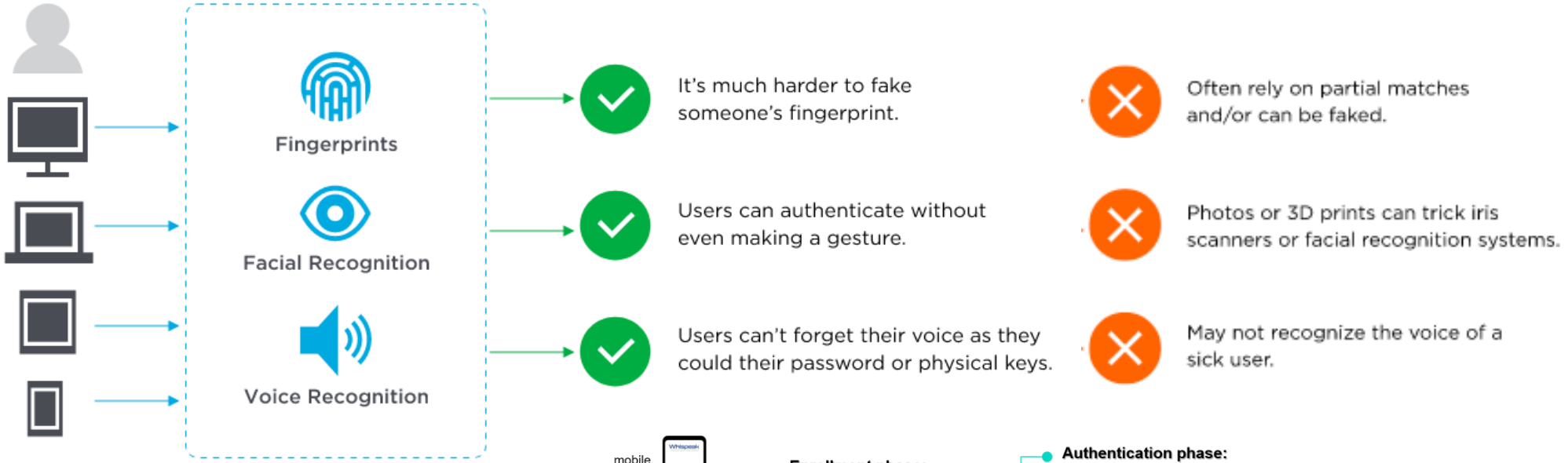
TOTP, or Time-based One-time Passwords, is a way to generate short lived authentication tokens commonly used for two-factor authentication (2FA). The algorithm for TOTP is defined in RFC 6238, which means that the open standard can be implemented in a compatible way in multiple applications. You might be familiar with TOTP from apps like Authy or Google Authenticator, but there are a lot of other options including Duo and Microsoft Authenticator.

About implementin TOTP in Aplication: https://www.twilio.com/blog/authy-api-and-google-authenticator

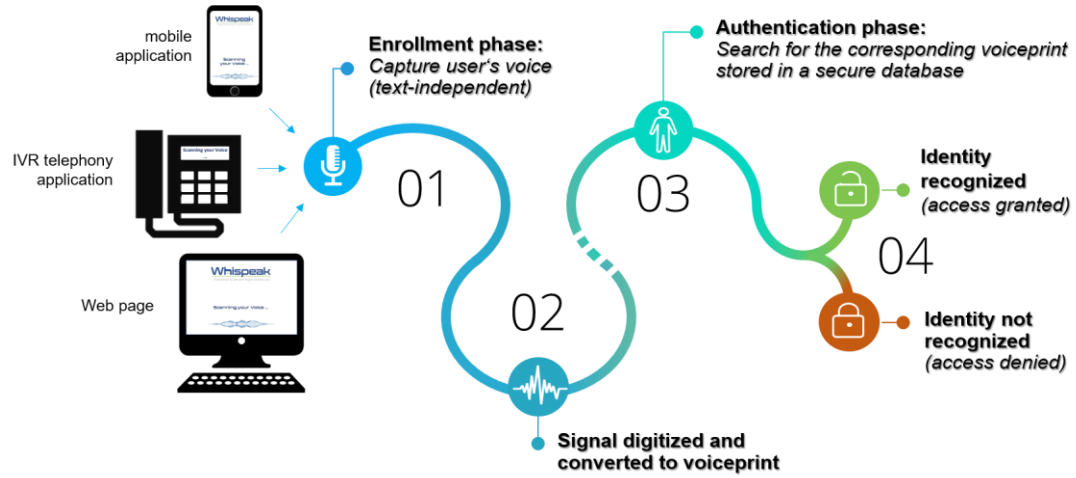
F1b Protection Techniques

AAA 7/16

Biometrics: user property. It involves the use of libraries and/or external systems



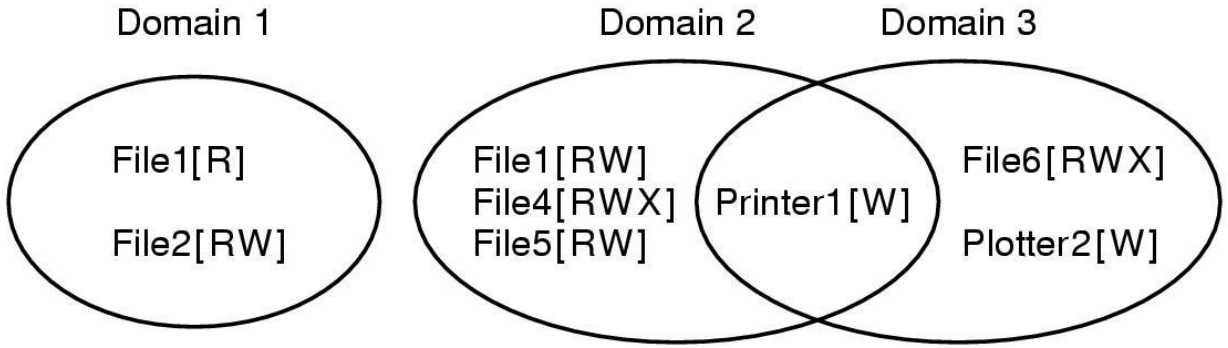
Enrollment: initial registration of user characteristics



F1b Protection Techniques

AAA 8/16

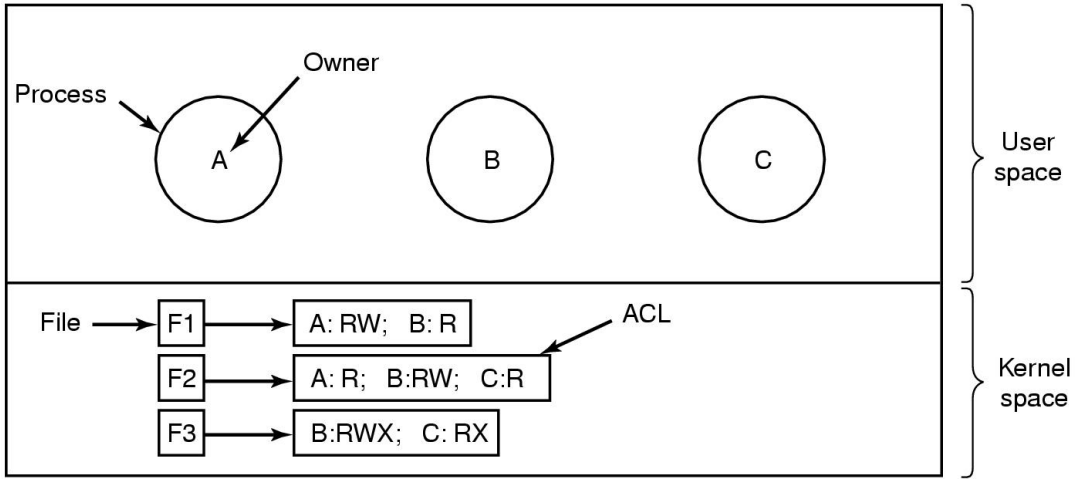
Permission: access authorization through rules.



Domains: sets of resources to organize access

Domain	Object										
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

Protection Domain: ...



ACL: Access Control List

F1b Protection Techniques

AAA: Access Control Types 9/16

MAC: Mandatory Access Control ➔ security policy: security labels

R(o)BAC: Role Based Access Control ➔ Role != Group

RBAC: Rule Based Access Control ➔ ACL: Access Control List

DAC: Discretionary Access Control ➔ ACL: Access Control List

F1b Protection Techniques

AAA: Access Control: MAC 10/16

MAC: Mandatory Access Control ➔ security policy: security labels

E1b Security Objectives

Confidentiality ➔ Bell-La Padula Model 3/3

Cosa facciamo
- L'intelligence
- Collaborazione istituzionale
- Rapporti con l'Autorità giudiziaria
- Tutela delle informazioni
  - Autorità nazionale per la sicurezza
  - Il segreto di Stato
  - Classifiche di segretezza
  - Rilascio delle abilitazioni di sicurezza
- I controlli sul Sistema

Home » Cosa facciamo » Tutela delle informazioni » Classifiche di segretezza

Classifiche di segretezza

La classifica di segretezza è l'**indicatore del livello di segretezza** attribuito in ambito nazionale a una determinata informazione. Si configurano come **documenti classificati** qualsiasi supporto – materiale o immateriale, analogico o digitale – contenente informazioni classificate e, pertanto, sottoposto a misure di protezione fisica, logica e tecnica dal momento della sua origine fino a quello della sua distruzione o declassifica. Durante tale arco di vita, la sua trattazione e gestione sono disciplinate da modalità specifiche. Le singole parti di un documento possono richiedere classifiche differenti. In questo caso il livello generale di classifica dell'intero documento è pari almeno a quello della parte con classifica più elevata.

Le classifiche sono quattro:

- **segretissimo** (SS)
- **segreto** (S)
- **riservatissimo** (RR)
- **riservato** (R)

Rep. Italiana	NATO
Segretissimo (**SS**)	Top Secret
Segreto (**S**)	Secret
Riservatissimo (**RR**)	Confidential
Riservato (**R**)	Reserved

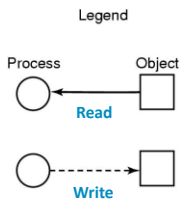
➔ Nulla Osta di Sicurezza (NOS) ➔ Livello (R, RR, S, SS)

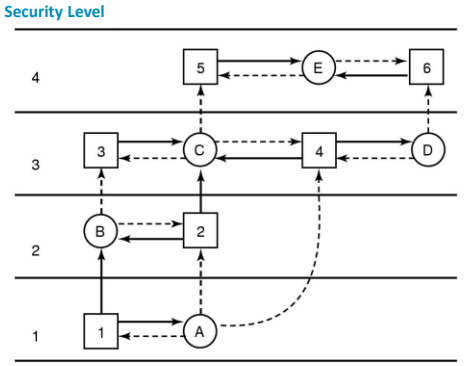
E1b Security Objectives

Confidentiality ➔ Bell-La Padula Model 2/3

Bell-La Padula Model: 2 rules (properties)

1. **No Read Up** (Simple Security Property ➔ do not read potentially more confidential information
2. **No Write Down** (* Property) ➔ do not inadvertently write more confidential information



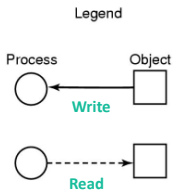


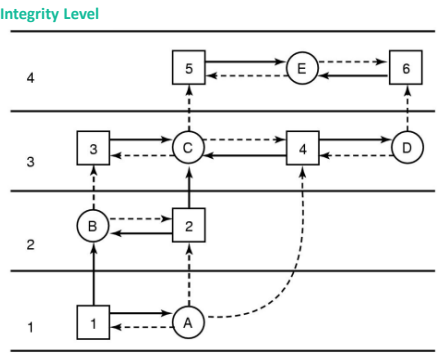
E1c Security Objectives

Integrity ➔ Biba Model 2/2

Biba Model: 2 rules (properties)

1. **No Write Up** (Simple Integrity Principle) ➔ do not insert information with lower integrity level
2. **No Read Down** (Integrity * Property) ➔ do not make use of information with lower integrity level





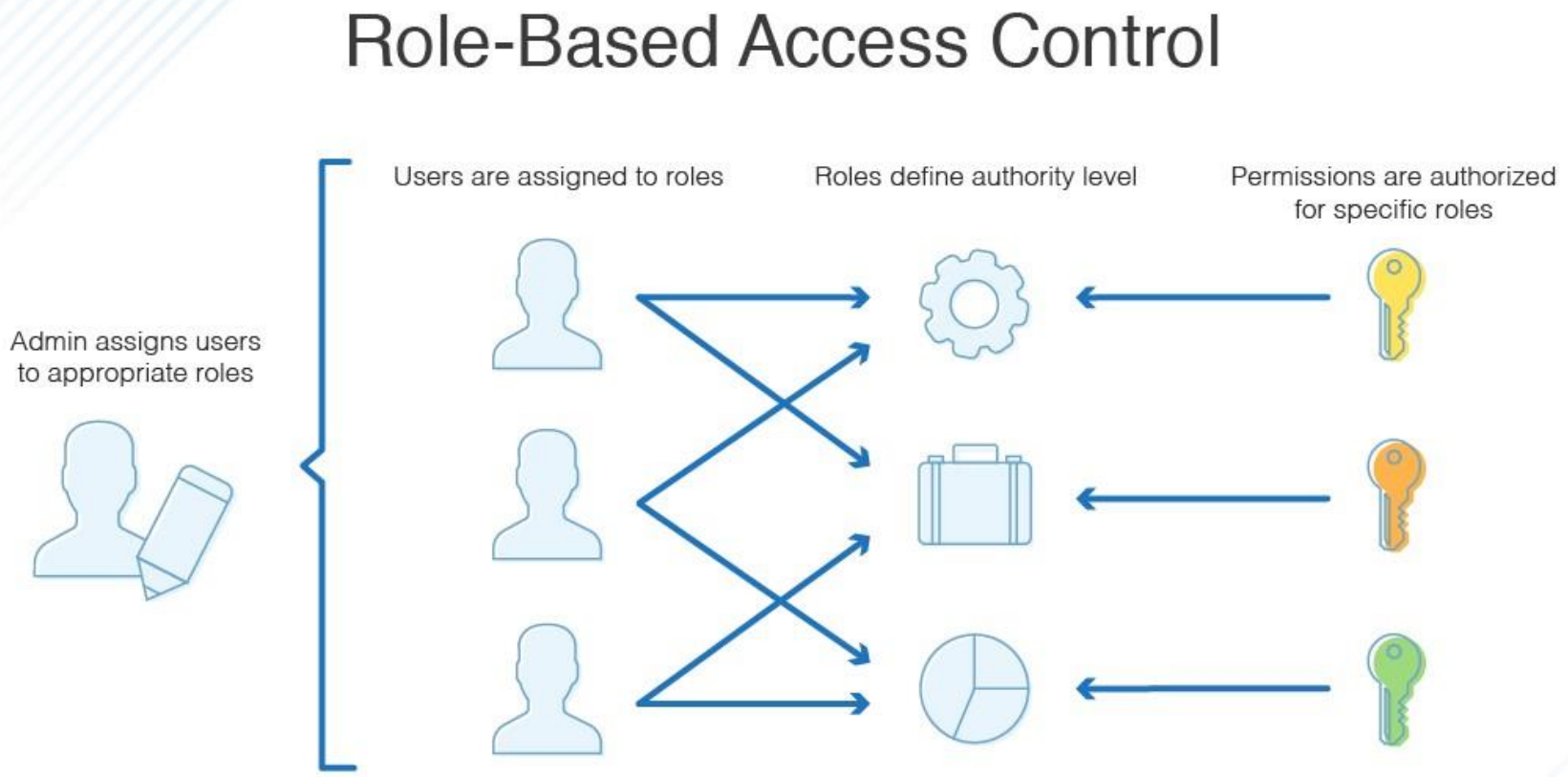
F1b Protection Techniques

AAA: Access Control: RBAC 11/16

RBAC: Role Based Access Control ➔ Role != Group

Implementato tramite Directory Server (LDAP): DB gerarchico

es. OpenLDAP, MS-AD (Microsoft Active Directory)



F1b Protection Techniques

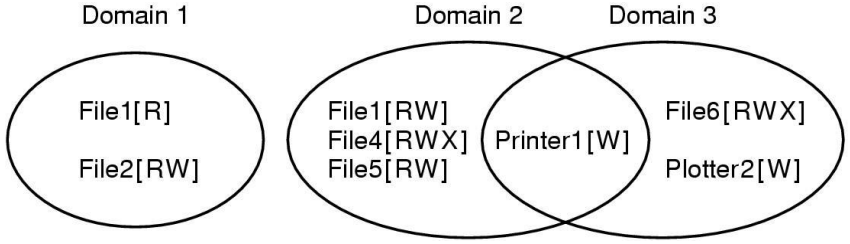
AAA: Access Control: R(u)BAC 12/16

R(u)BAC:
Rule Based Access Control
➔ ACL:
Access Control List

F1b Protection Techniques

AAA 6/8

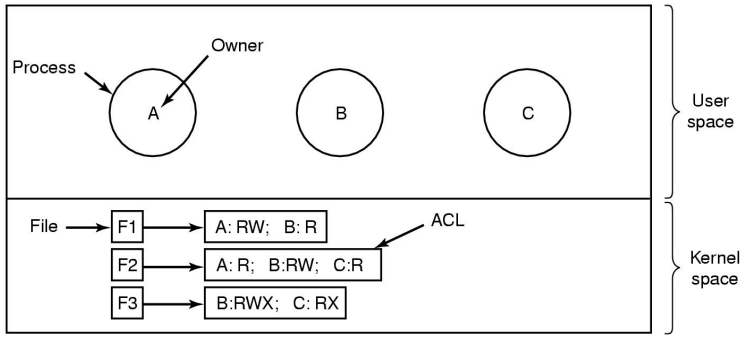
Permission: access authorization through rules.



Domains: sets of resources to organize access

Domain	Object										
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

Protection Domain: …



ACL: Access Control List

F1b Protection Techniques

AAA: Access Control: DAC 13/16

DAC: Discretionary Access Control ➔ ACL: Access Control List

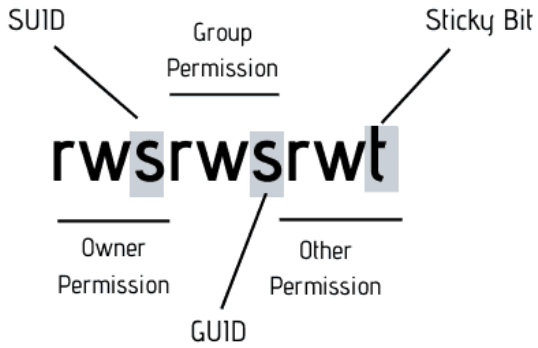
F1d Protection Techniques

Permissions 1/6

ACL: Access Control List

ACL: permissions included in a list

File	Access control list
Password	tana, sysadm: RW
Pigeon_data	bill, pigfan: RW; tana, pigfan: RW; ...



Changes to normal execute permissions (x) in Unix-like systems:

SUID (s): Set User ID. Indicates that the file should be run with the privileges of the user who owns the file rather than the user who launches it. Does not apply to directories.

GUID (s): Set Group ID. indicates that the file should be run with the permissions of the group assigned to the file rather than those of the main group of the user starting it. Does not apply to directories.

Sticky (t): applied to executable files, it tells the kernel to keep a copy of the executable file in the swap file even after it has finished. Applied to directories, the files contained in it can only be deleted and moved by the users who own them, or by the user who owns the directory that contains them, or by the superuser

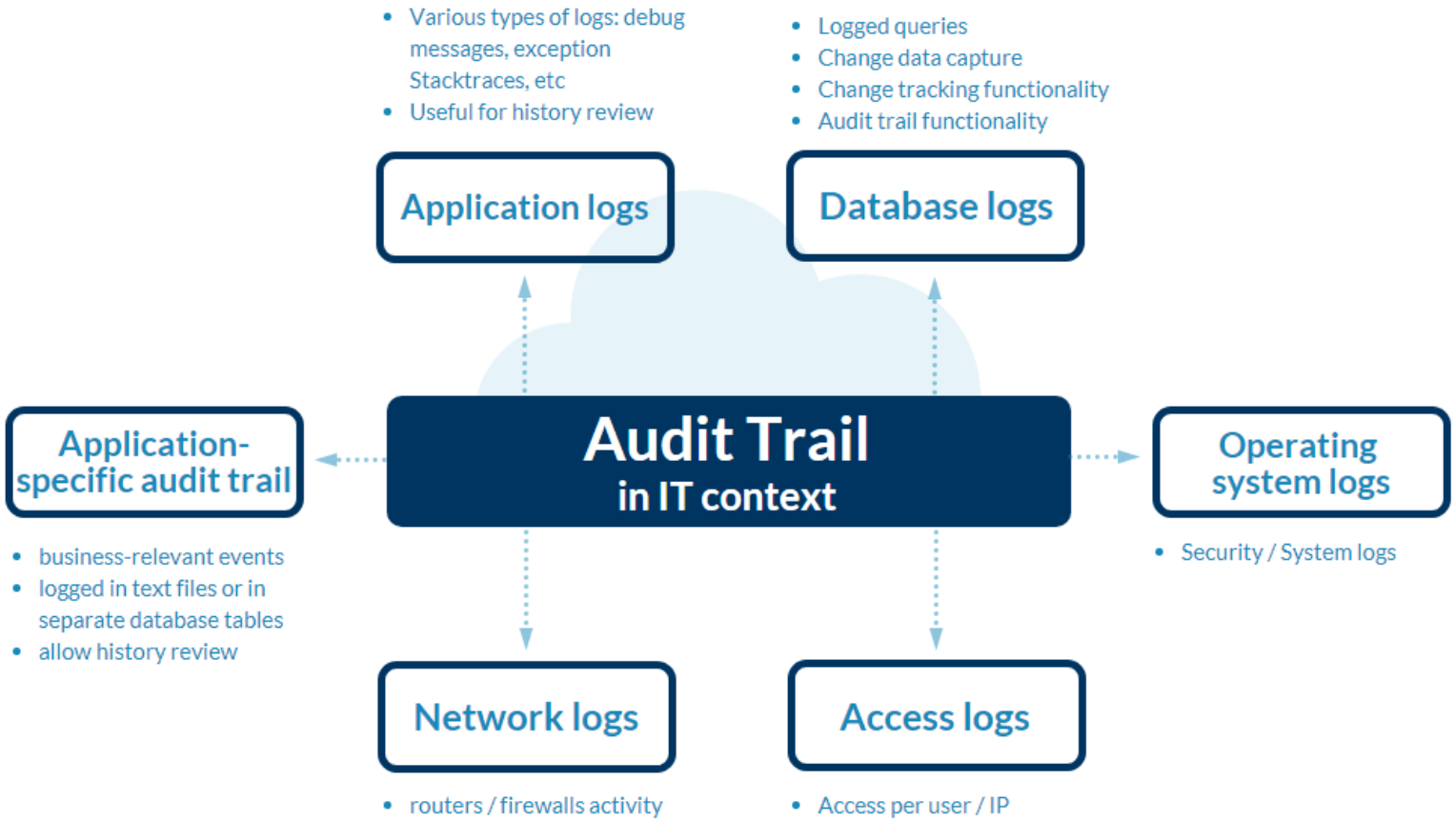
F1b Protection Techniques

AAA 14/16

Log-Trails: logs of events that have occurred on the application.

Log: records related to:

- (Un)Successful Authentications
- Accesses
- Performed Actions
- Eventual Errors



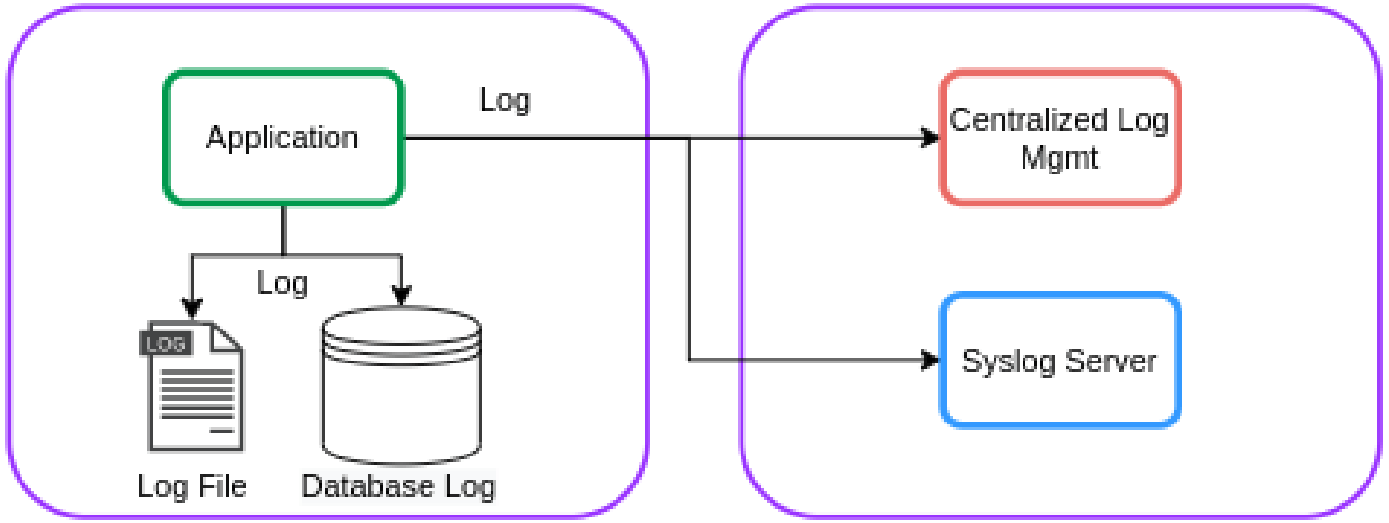
F1b Protection Techniques

AAA 15/16

Log-Trails: logs of events that have occurred on the application.

Sending the logging data to a centralized logging management application like Syslog, using standard configuration also for Log4J

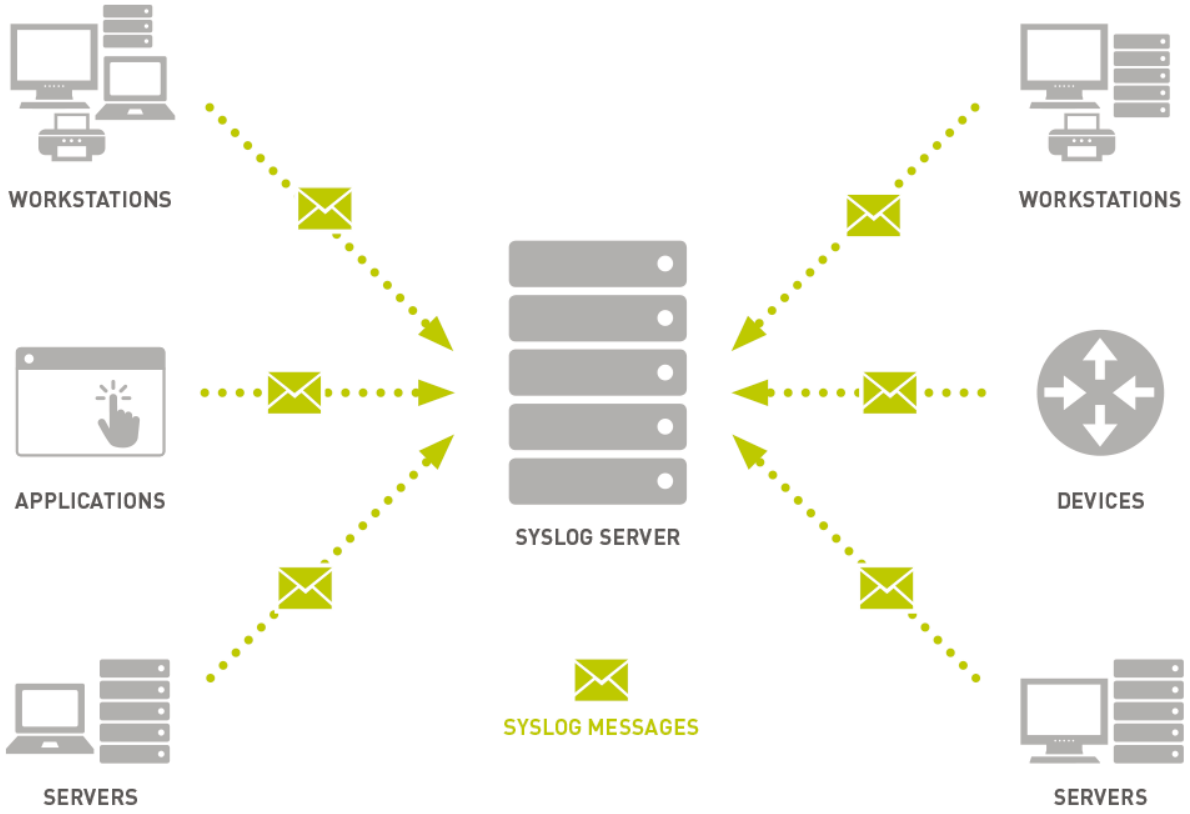
(see https://www.baeldung.com/log4j-to-syslog)



F1b Protection Techniques

AAA 16/16

SysLog: network protocol used to transmit simple log information across a network.



Log: need to send the logs off the machine, in order to preserve any local deletions made during the attack.

Syslog can be configured by modifying the /etc/syslog.conf file, indicating a logging activity on each line:

```
facility.loglevel /var/log/file.log
```

where

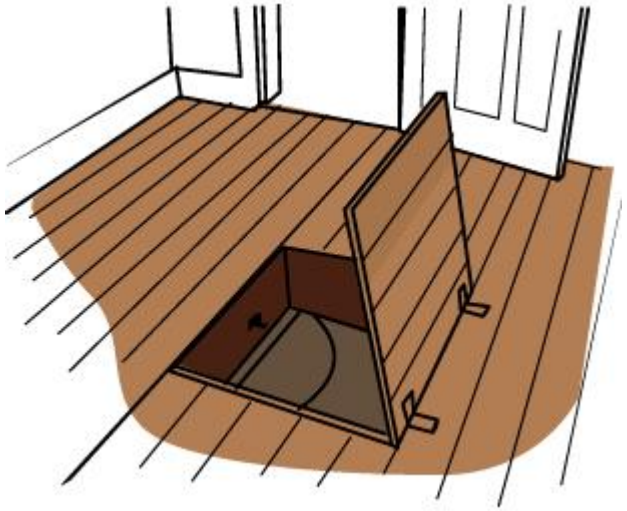
- **Facility**: auth, auth-priv, cron, daemon, kern, local0-7, lpr, mail, news, user, syslog, uucp

- **LogLevel**: message criticality level: debug, info, notice, warning, error, crit, alert, emerg

F1c Protection Techniques

Attacks 1/4

Trap Doors: secret entry point that allows access without the normal security access procedures



```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

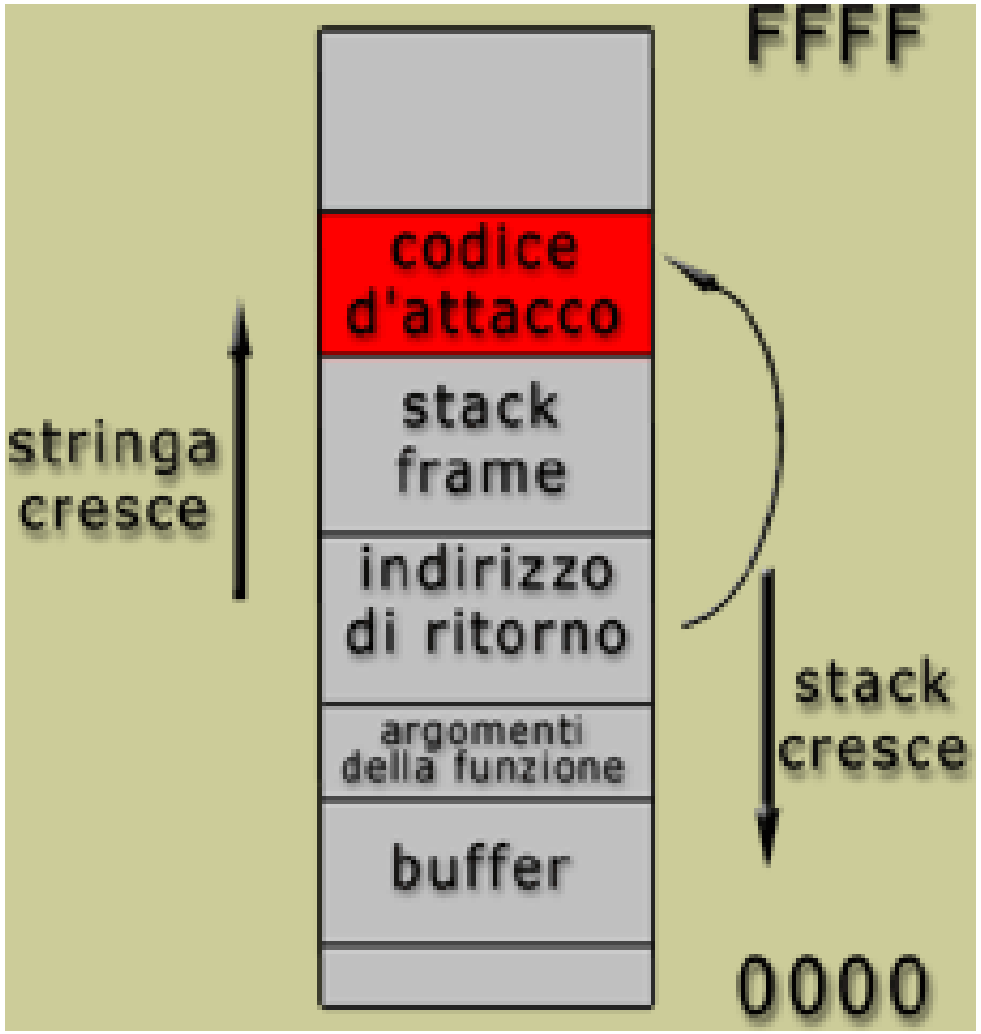
(b)

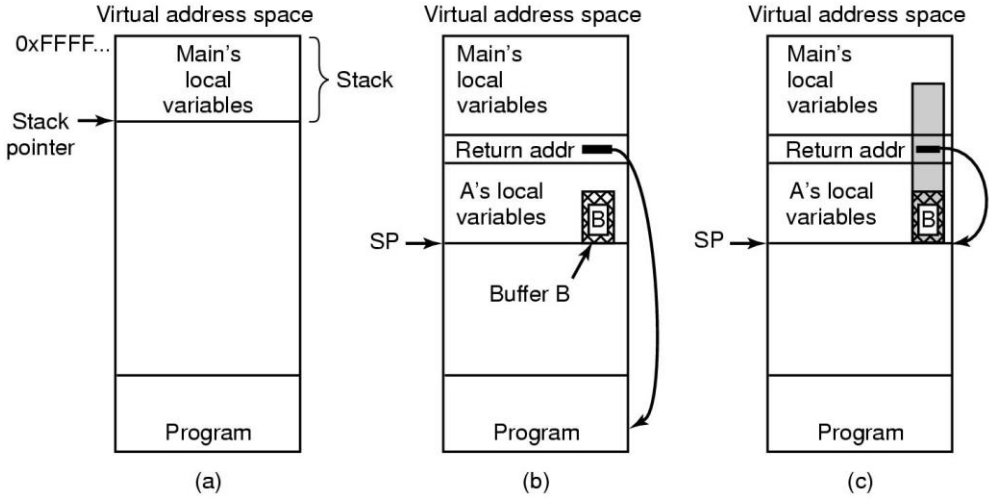
(a) Normal code.
(b) codice with trap door (“zzzzz”)

F1c Protection Techniques

Attacks 2/4

Buffer Overflow: overflow of a buffer, with no control over the limit of its inputs, due to too much data supplied.





subvert the normal progression of a program so that the attacker can take control of it. It is necessary :

1. Prepare the appropriate code to be executed in the program's address space.

2. Allow the program to jump to that code, with exact parameters, loaded into registers and memory

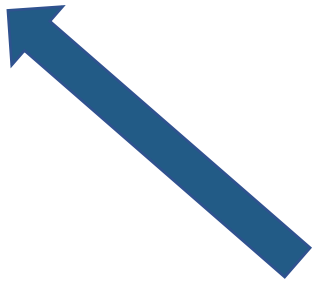
F1c Protection Techniques

Attacks 3/4

Code Injection: processing of invalid data, surreptitiously entered through a software bug.

No input validation

```
int main(int argc, char *argv[])
{
  char src[100], dst[100], cmd[205] = "cp ";          /* declare 3 strings */
  printf("Please enter name of source file: ");       /* ask for source file */
  gets(src);                                          /* get input from the keyboard */
  strcat(cmd, src);                                   /* concatenate src after cp */
  strcat(cmd, " ");                                   /* add a space to the end of cmd */
  printf("Please enter name of destination file: ");  /* ask for output file name */
  gets(dst);                                          /* get input from the keyboard */
  strcat(cmd, dst);                                   /* complete the commands string */
  system(cmd);                                        /* execute the cp command */
}
```

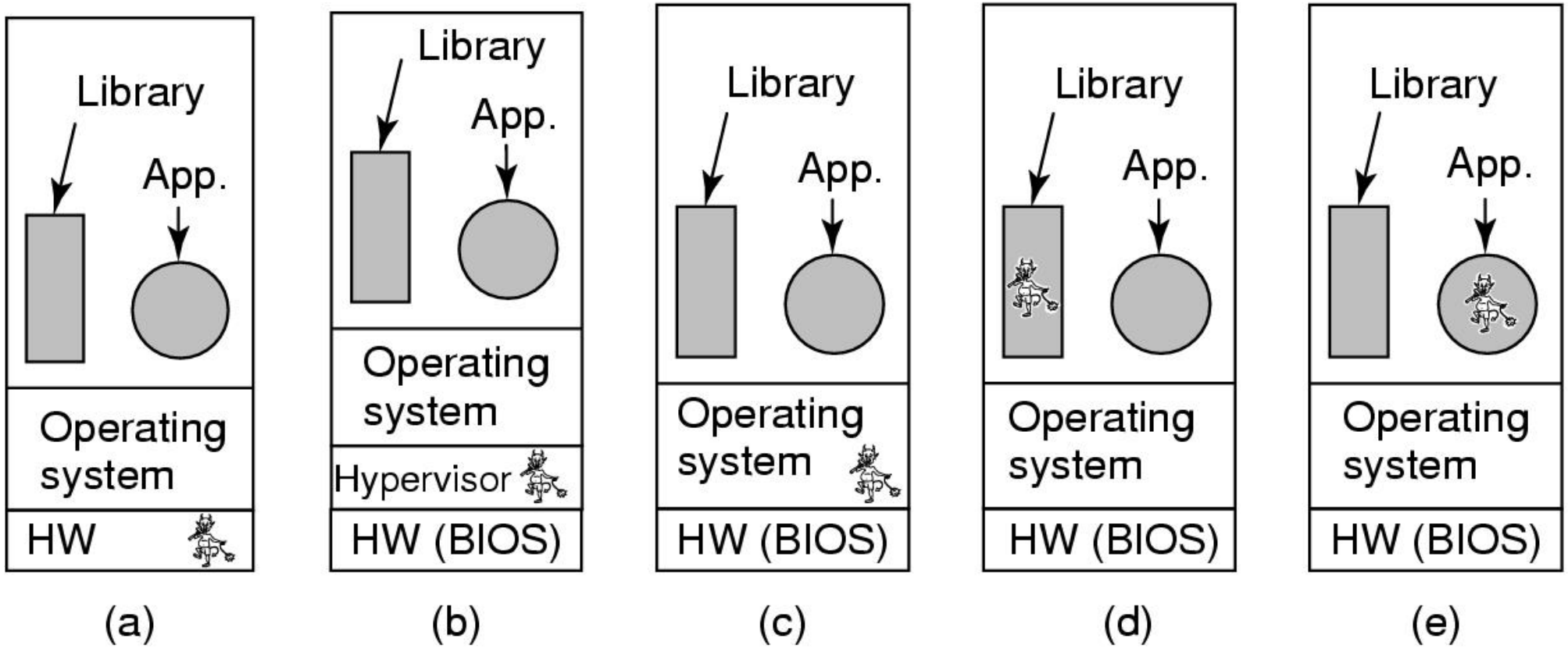


Using the input string

F1c Protection Techniques

Attacks 4/4

Rootkits: malware designed to give people with low technical skills a command and control tool.



(a) Firmware rootkits

(b) Hypervisor rootkits

(c) Kernel rootkits

(d) Library rootkits

(e) Application rootkits

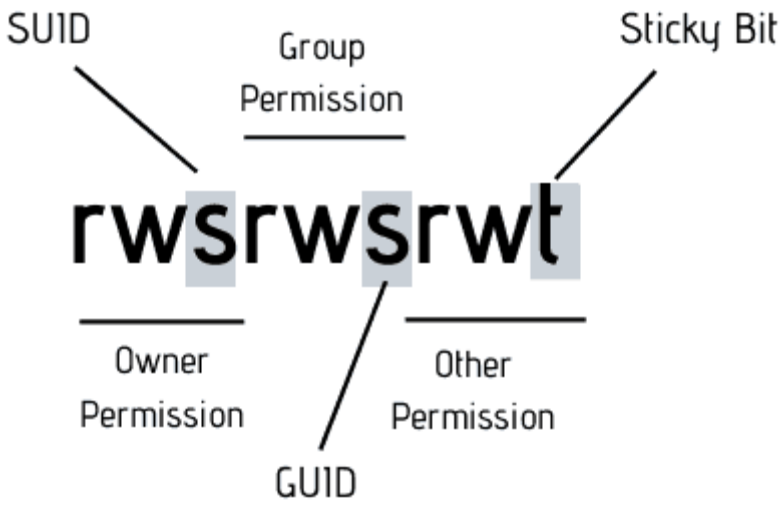
F1d Protection Techniques

Permissions 1/6

ACL: Access Control List

ACL: permissions included in a list

File	Access control list
Password	tana, sysadm: RW
Pigeon_data	bill, pigfan: RW; tana, pigfan: RW; ...



Changes to normal execute permissions (x) in Unix-like systems:

SUID (s): Set User ID. Indicates that the file should be run with the privileges of the user who owns the file rather than the user who launches it. Does not apply to directories.

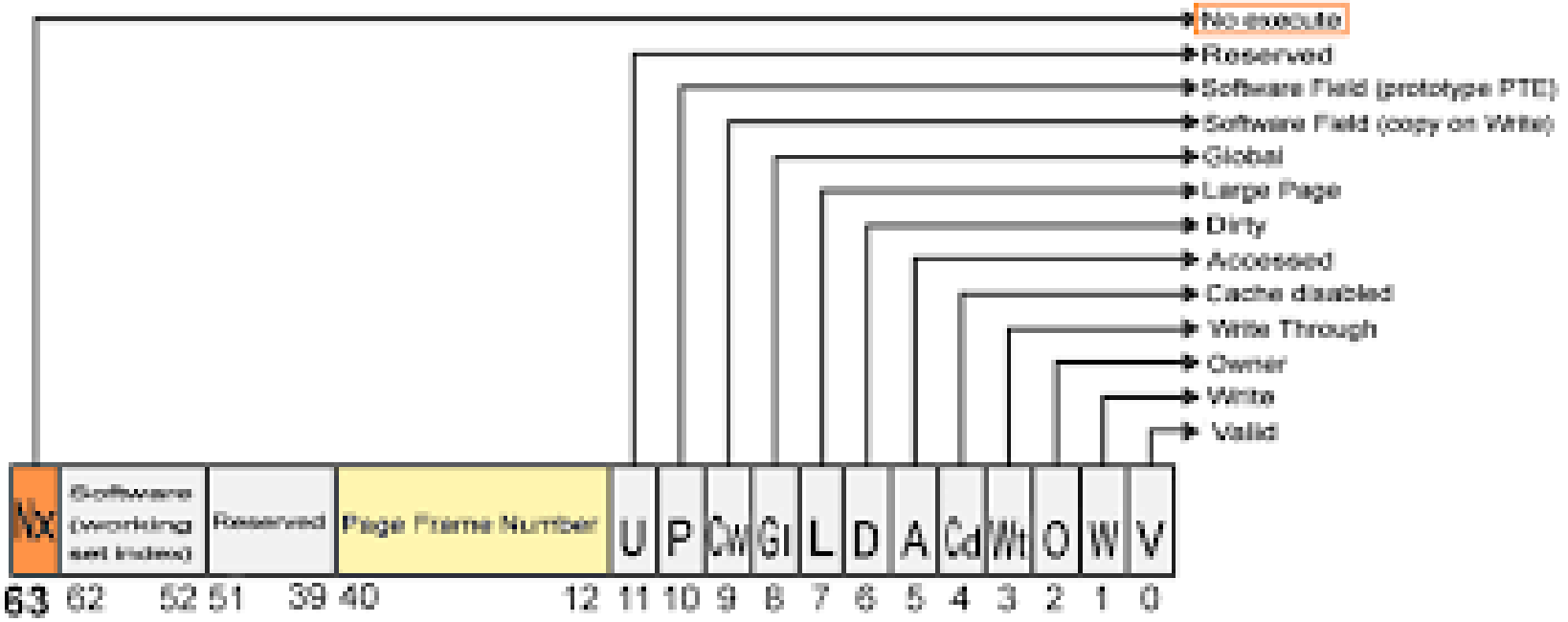
GUID (s): Set Group ID. indicates that the file should be run with the permissions of the group assigned to the file rather than those of the main group of the user starting it. Does not apply to directories.

Sticky (t): applied to executable files, it tells the kernel to keep a copy of the executable file in the swap file even after it has finished. Applied to directories, the files contained in it can only be deleted and moved by the users who own them, or by the user who owns the directory that contains them, or by the superuser

F1d Protection Techniques

Permissions 2/6

NX: No eXecution. Inhibition of the execution of a certain fraction of data. Also called Data Execution Prevention (DEP).



NX/DEP runs in two modes:

1. **NX bit**: Hardware-enforced DEP for CPUs that can mark memory pages as non-executable

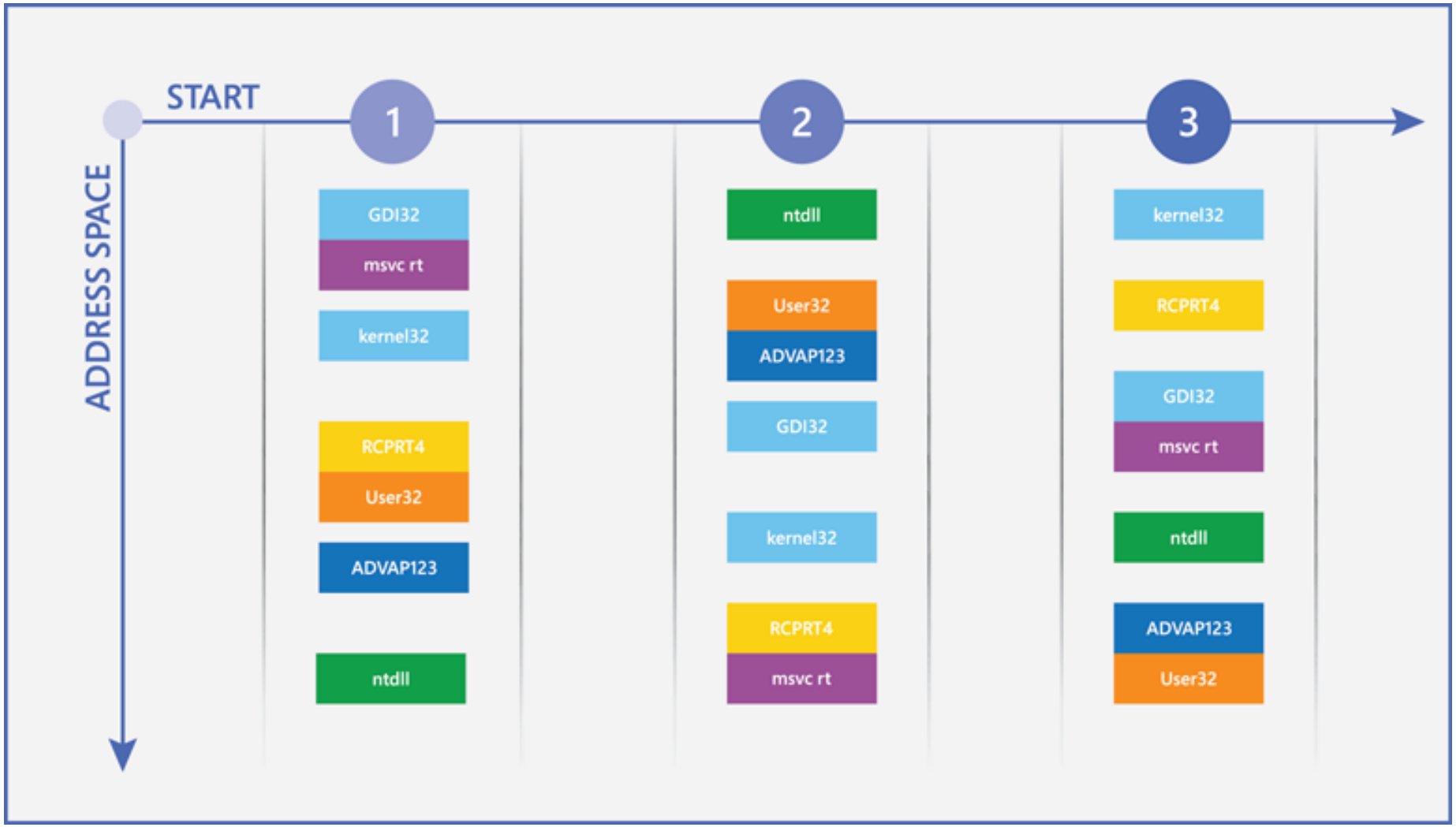
2. **SW**: Software-enforced DEP with limited prevention for CPUs that lack hardware support. Software-enforced DEP does not protect against code execution on data pages, but against another type of attack.

DEP was introduced on Linux in 2000, on Windows in 2004 with Windows XP Service Pack 2, while Apple introduced DEP in 2006

F1d Protection Techniques

Permissions 3/6

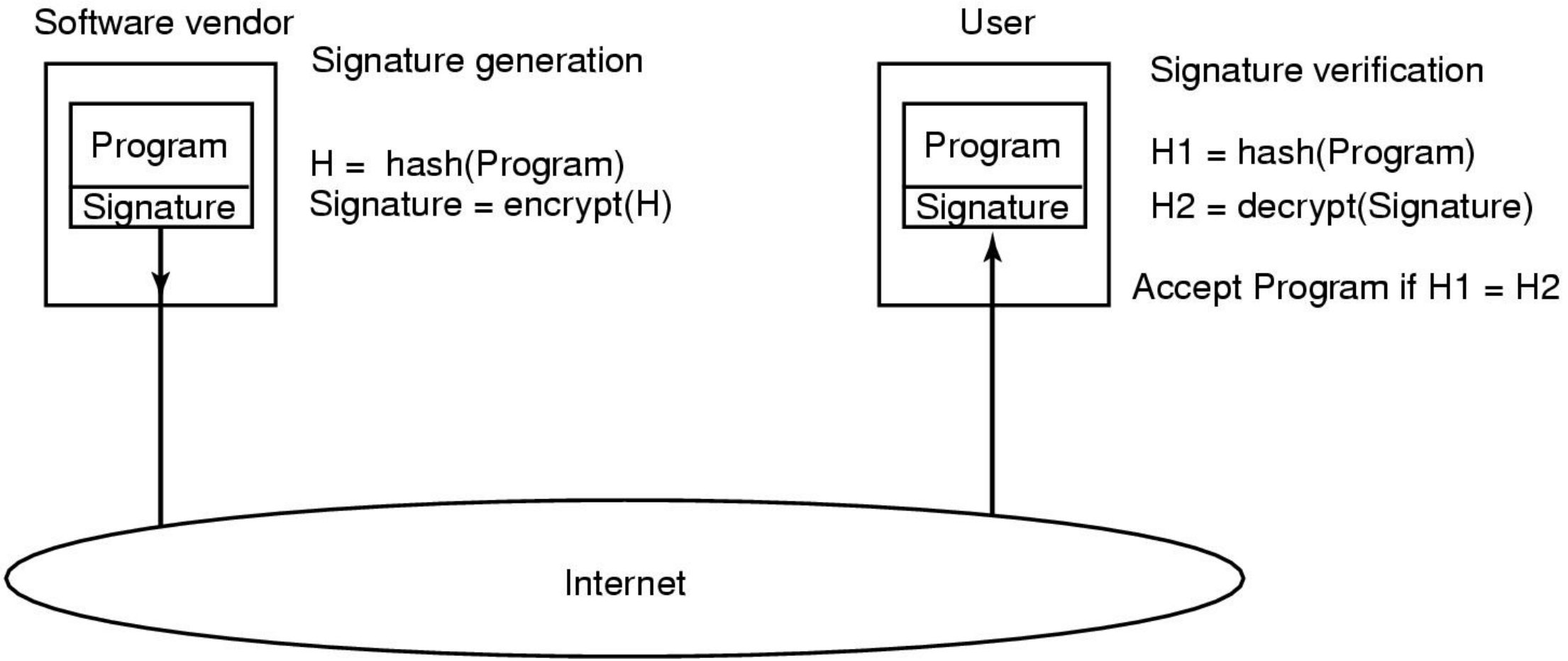
ASLR: Address Space Layout Randomization. Always different placement of the process in memory, at each execution.



F1d Protection Techniques

Permissions 4/6

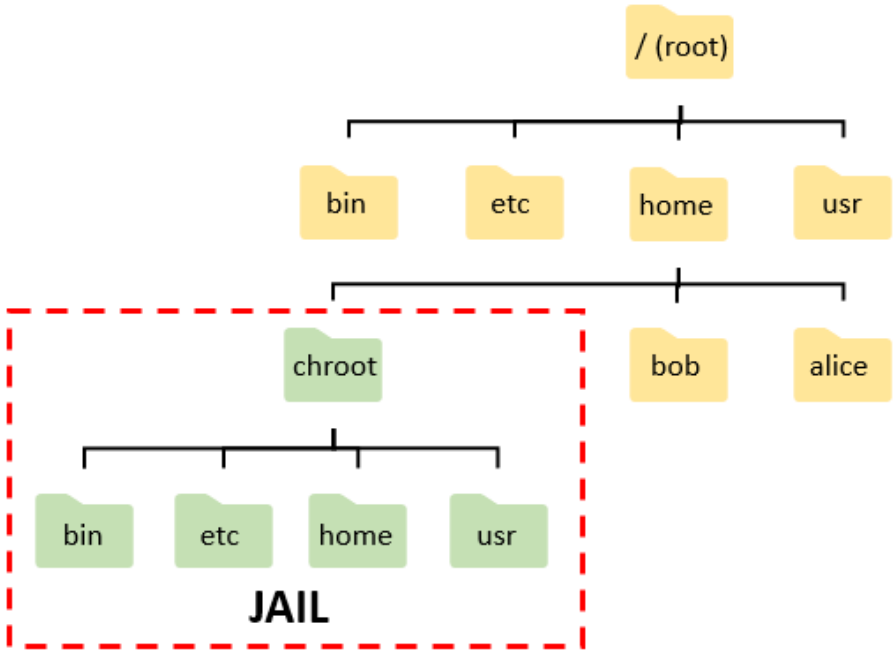
Code Signing: confirm the author of the software, ensuring that the code has not been altered or corrupted after signing.



F1d Protection Techniques

Permissions 5/6

Jailing: way to isolate a process and its children from the rest of the file system (➔ Containers).
Sandboxing: way to isolate a process from the rest of the system's memory as well (➔ Containers).



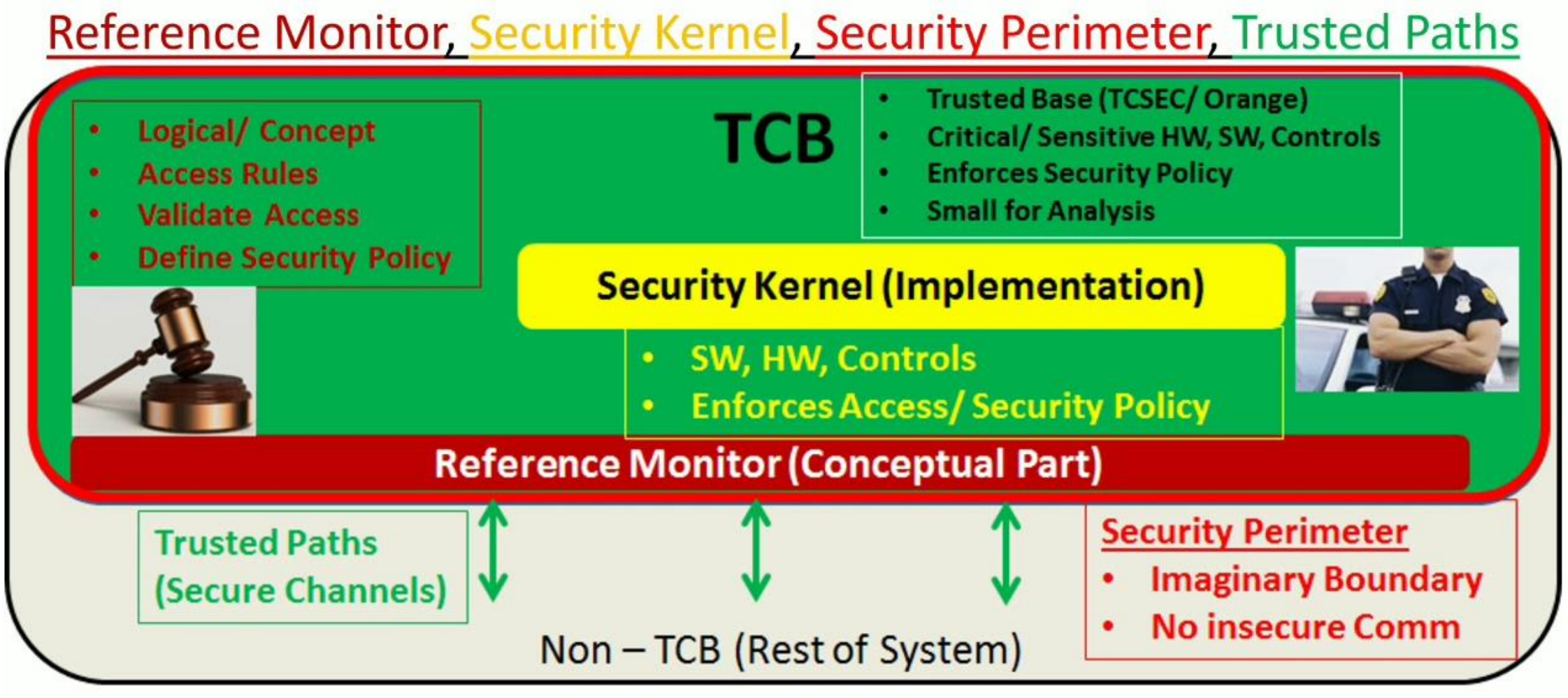
ChRoot: Change Root
Making a process believe that a subtree is the entire file system.
The file outside this subtree simply doesn't exist.

Sandboxing: Change Root
Prevent a process from accessing chunks of memory that it doesn't necessarily care about (including system calls, which expose data from other processes).

F1d Protection Techniques

Permissions 6/6

TCB: Trusted Computing Base.



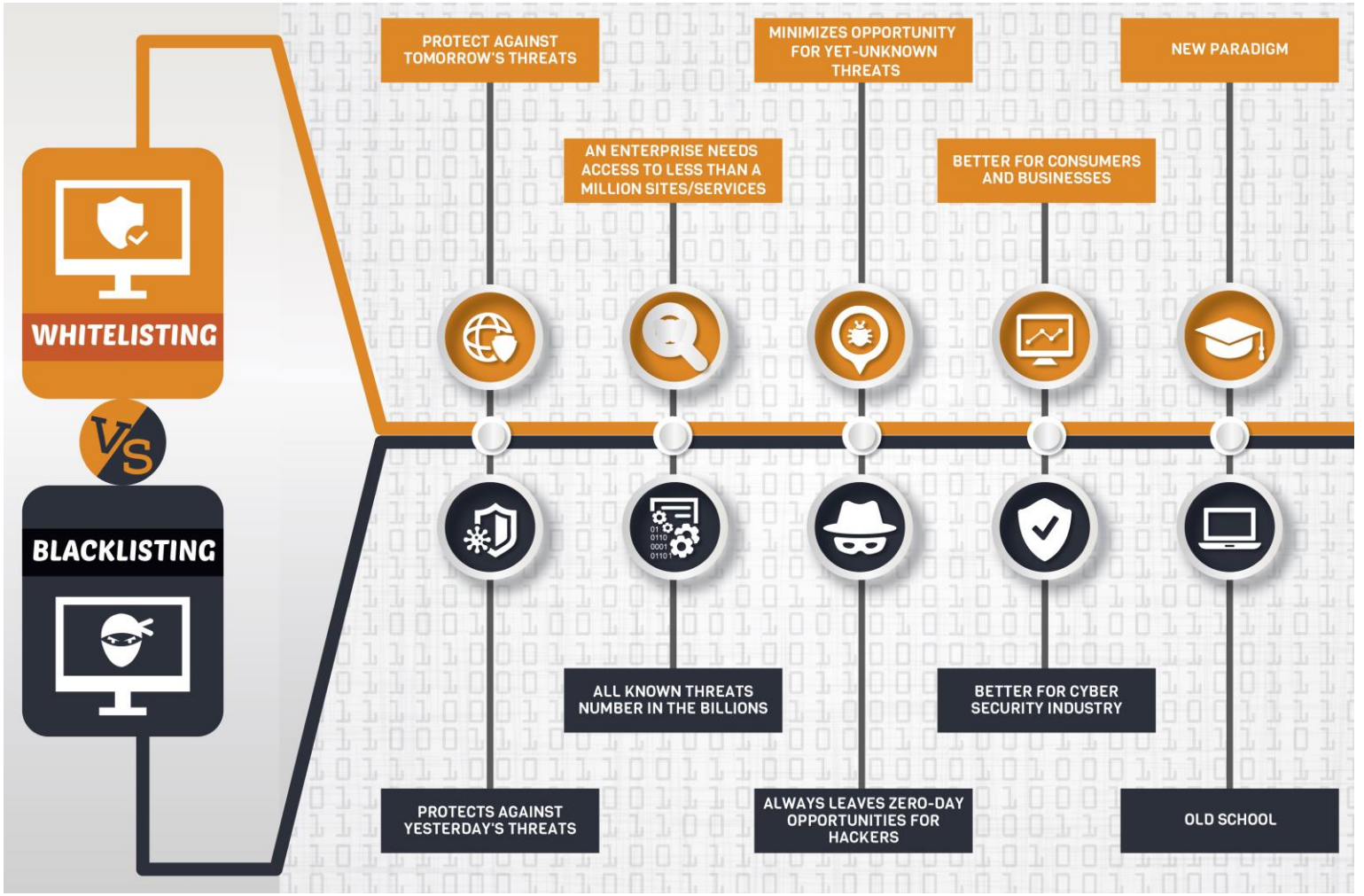
F1e Protection Techniques

Filter

Block the bad, allow the good

- **Blacklisting**: traditional approach, old school:
  - Allow everything,
  - Block some (well-known as very dangerous).

- **Whitelisting**: new paradigm
  - Block Everything
  - Allow Some



F1f Protection Techniques

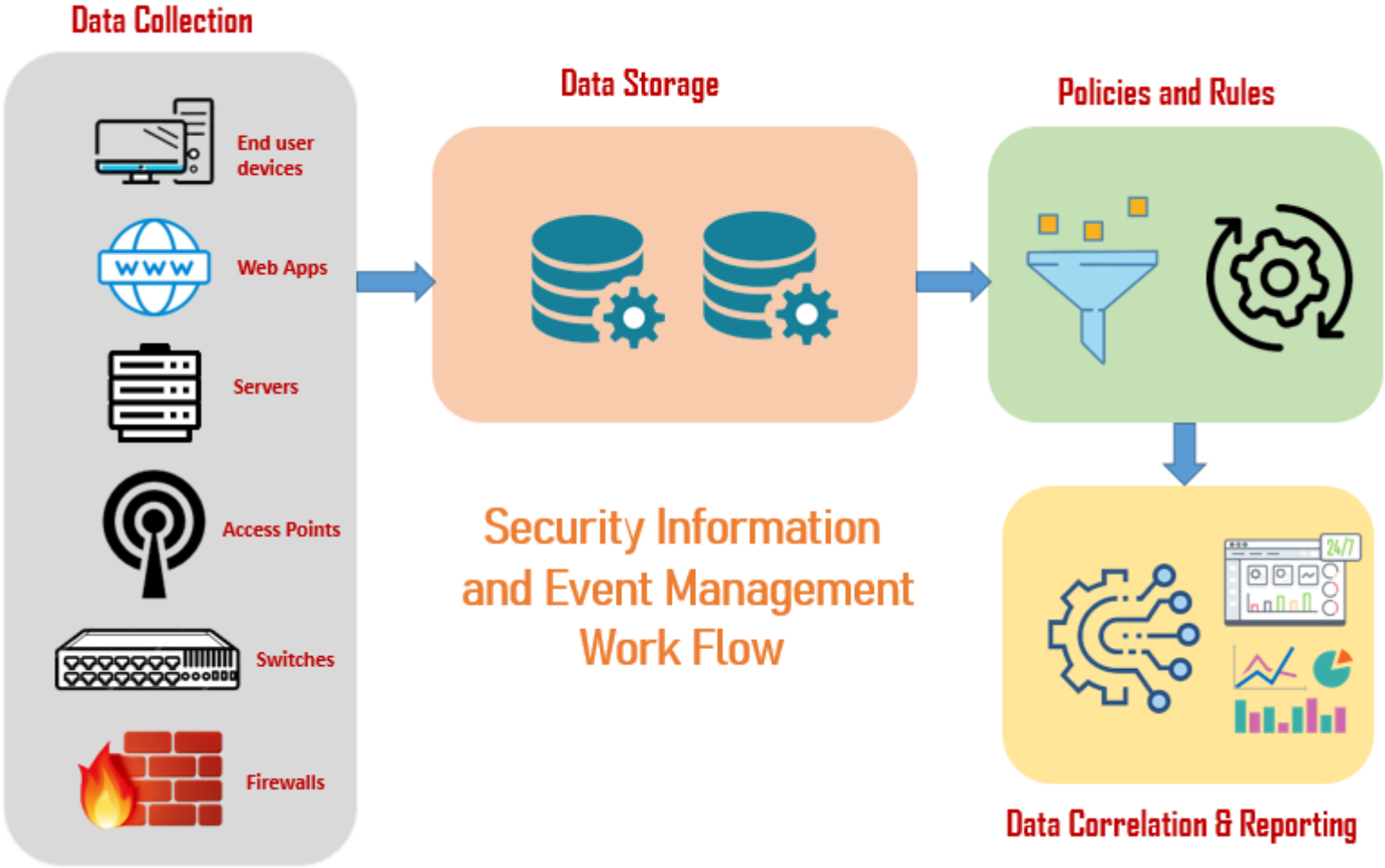
Logging

Events to log:

- authentication successes and failures;
- access control successes and failures;
- session activity, such as files and applications used, particularly system utilities;
- changes in user privileges;
- processes starting or stopping;
- changes to configuration settings;
- software installed or deleted;
- devices attached or detached;
- system or application errors and alerts; and
- alerts from executed transaction

Log Entry

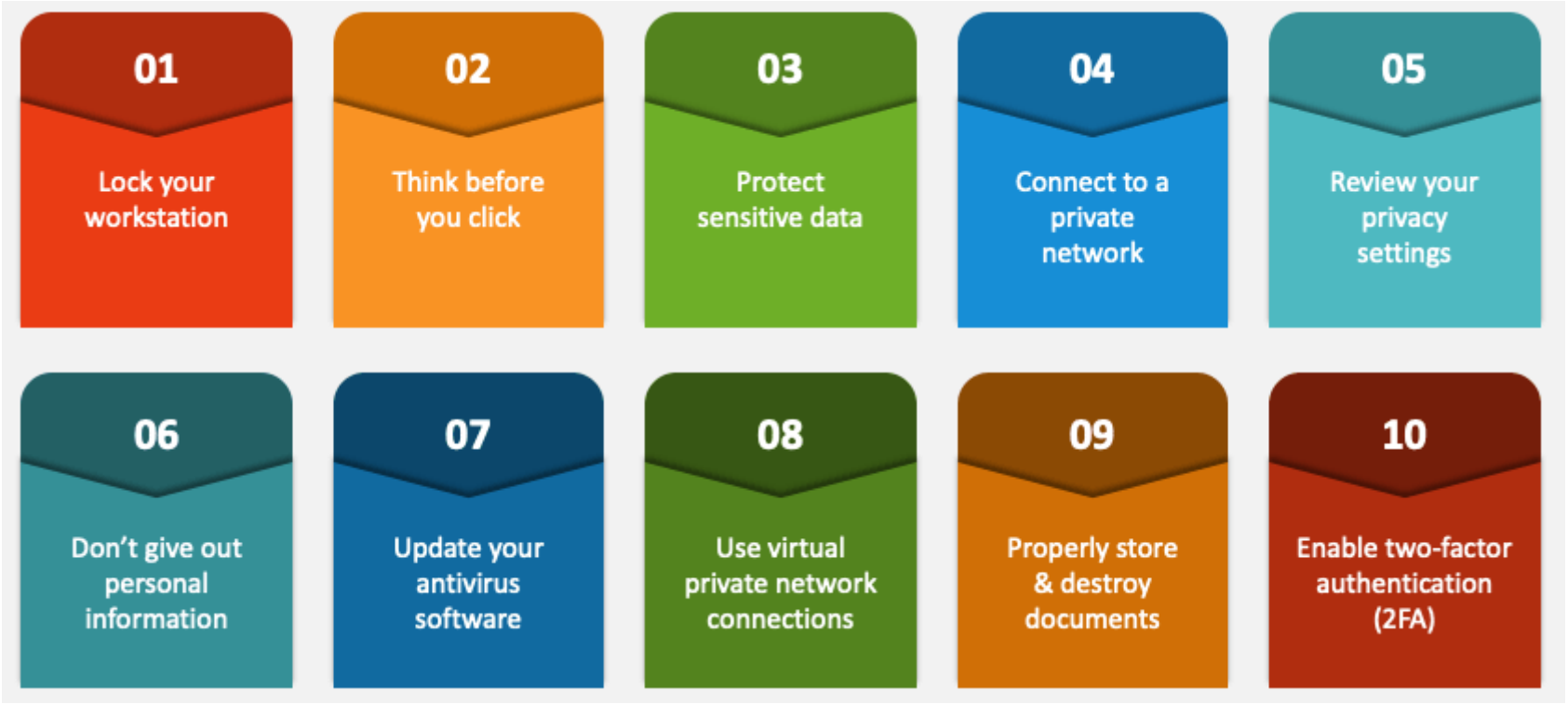
- **date and time**
- **user and/or device ID**
- **network address and protocol**
- **location when possible**
- **event or activity**



F1g Protection Techniques

Awareness

Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches. Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyber attacks they may encounter via email and the web.

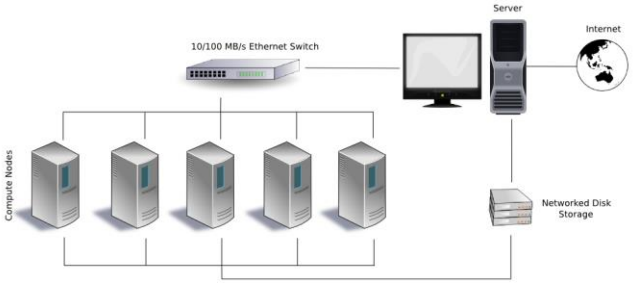


F1h Protection Techniques

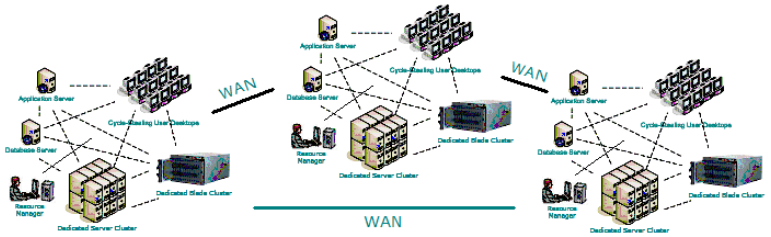
Duplication

Duplication or distributed elaboration

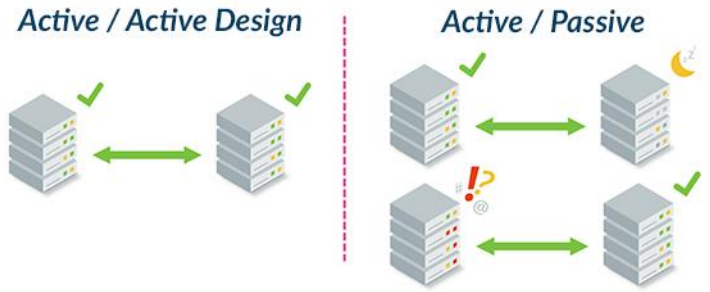
- **High Performance Computer (HPC)**: physically located close to each other in order to solve problems more efficiently. Generally, they run the same OS image.



- **Grid Computing**: use of a computational grid (workstations, blade servers, etc.) applying grid resources, via network, to a single problem at the same time, while crossing political and theoretical boundaries.



- **High Availability (HA)**: a computer system acts as a backup system for one or more primary systems, all located close to each other. When there is a failure in a primary system, critical applications running on that system are transferred to the designated backup system.
  - **Load Balancing** (**LB**): as HA but all systems running and participating in the cluster share the workload (Active/Active).
  - **Cluster Geografico**: same as HA but the systems are located remotely.



F2 BIA

BCM and Always On

As soon as Always On has became a must, Business Continuity Management arose as a set of methodology for ensuring Business Sustainability and Resilience.

The **Business Impact Anal**ysis is the first step of BCM and it is mainly focused on

How Much: identifying the best countermeasures for avoiding possible accidents

more than

How To: fighting against possible accidents. This is a task for BC/DR

F2a BIA

BIA: Overview

Business Impact Analysis (BIA) is

- a **systematic process**
- to **evaluate** or design the needed **countermeasures**
- to **put in action**
- in order to **neutralize** the potential effects of an **interruption**
- to **critical business** operations.

To neutralize: ‘to reduce to a level that is no more financially dangerous for the company’

Interruptions: results of a disaster, accident or emergency.

F2b BIA

BCI Good Practice Guide

The BCI Good Practice Guide suggests to perform BIA in the following steps:

1. **Scope:** To develop a framework for further analysis and clarify the BCM programme scope

2. **Prioritization:** To identify and prioritise the organisation's products and services, and understand the organisation's recovery timescales and disruption tolerance levels

3. **Impacts:** To determine the dependent activities for the most urgent products and services and assess the impact of a disruption on them

4. **Countermeasures:** To determine the required resources for the continuity and recovery for the most urgent activities.

F2c BIA

BCI Good Practice Guide

The BCI Good Practice Guide suggests 4 types of BIA, based on detailing level, infrastructure coverage and time-to-loss:

- **Initial BIA:** core business, early losses
- **Strategic BIA:** main infrastructure, late & permanent losses
- **Tactical BIA:** company processes, early losses
- **Operational BIA:** technical infrastructure, early losses

F2d BIA

BCI Good Practice Guide: Initial BIA

The Framework could be simplified as composed by the following logical steps:

- **Threats:** To identify the threats that could affect (Core) Business Continuity
- **Critical Processes:** To individuate the most negative economic impact processes for the Company. These relate to functions strictly connected to revenue and earnings and are identified in the light of drivers' economic losses associated with the company
- **IT System Mapping**: to identify the systems providing the support to Critical Processes
- **RTO & RPO Calculation:** based on these times the best countermeasures could be selected

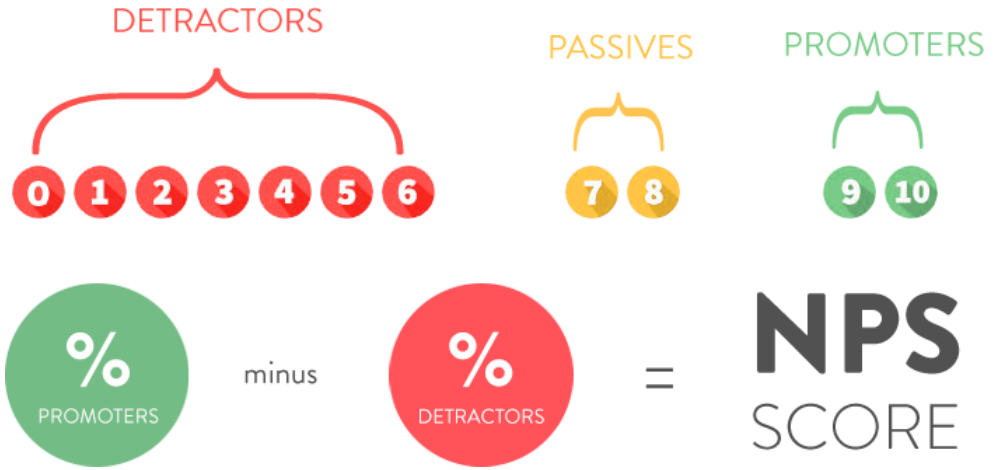
Class	Total Disruption Time
A	1 hour
B	4 hours
C	6 hours
D	8 hours
E	12 hours
F	1 day
G	1 week
H	1 mounth
I	3 mounths
J	1 year

F2e BIA

BCI Good Practice Guide: Strategic BIA

The Framework could be simplified as composed by the following logical steps:

- **Threats:** To identify the threats that could affect (Core) Business Continuity
- **Critical Processes:** To individuate the most negative economic impact processes for the Company. These relate to functions strictly connected to revenue and earnings and are identified in the light of drivers' economic losses associated with the company
- **IT System Mapping**: to identify the systems providing the support to Critical Processes
- **RTO & RPO Calculation:** based on these times the best countermeasures could be selected



F2f BIA

BCI Good Practice Guide: Tactical BIA

A mapping between Organisation products/services and process is needed to provide the following:

- **Dependent Activities:** To determine the dependent activities for the most urgent products and services
- **Distruction Impact**: assess the impact of a disruption on them

Dependent Activity	Risk Driver	Service
Selling	Missed Income Customer Loss Reputational Damage	Web Retails
Finance Management	Dataflow Stop	InterBanking

Distruction Impact	Service
1M€/day	Web
200K€/day	Retails
10K€/day	InterBanking

F2g BIA

BCI Good Practice Guide: Operational BIA

A technical analysis is needed:

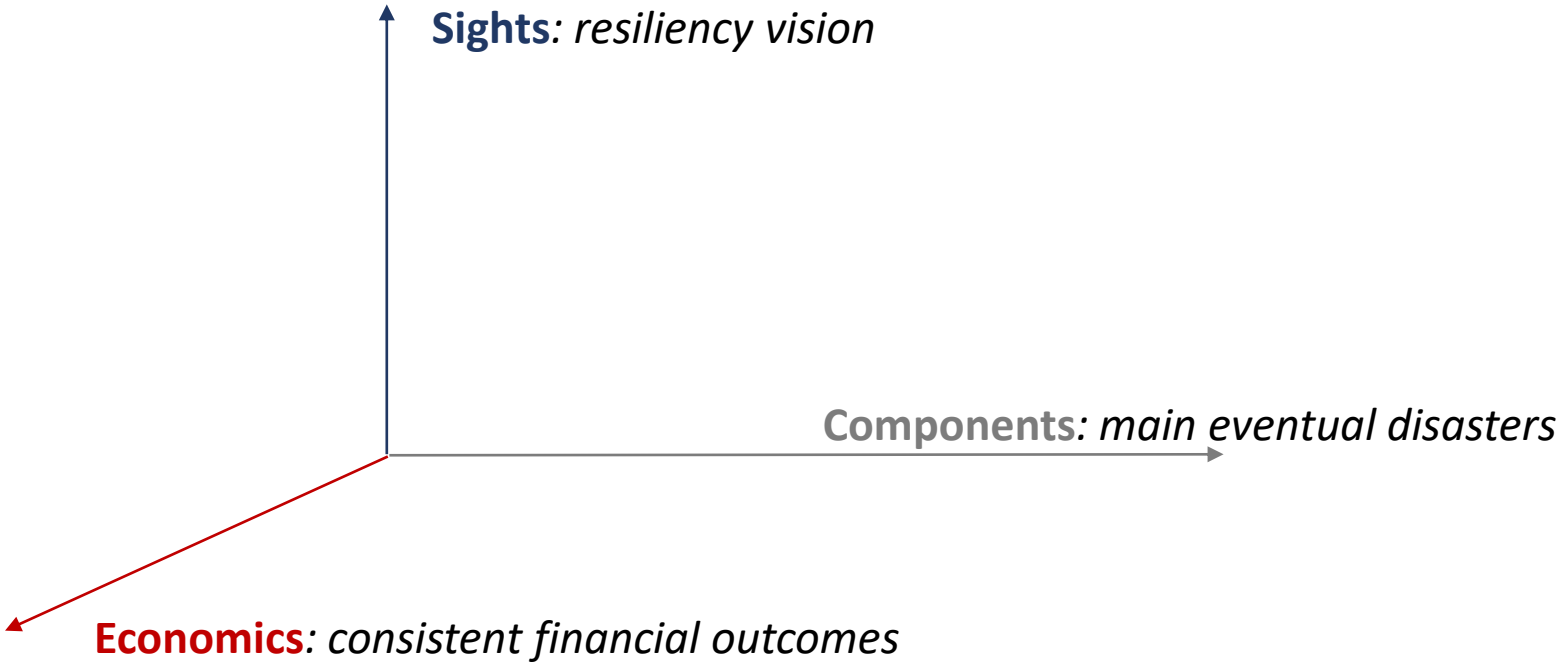
- **RTO/RPO**: determine time requirement for the most urgent activities/systems

Service	RTO	RPO	Notes	€
Web	KO	OK	Improve SLA on contract	100K€
Retail	OK	OK	-	-
InterBanking	KO	OK	Improve recovery capability in DC	1K€

- **Best Solution:** To determine the implementation requirements for intended resources

F2h BIA

BIA Evaluation - Dimensions: Economics, Components, Sights



BIA:

1. the starting component of the BCP
2. Strategy for reducing Money-Loss
3. simplifications for easier analysis

BIA analyzes only *consistent financial outcomes* as a result of *main eventual disasters* applied to *essential business components*

F2i BIA

BIA Evaluation – Economic Figures

Main Financial Measures are the following:

- **EBIT**: Earning Before Interests and Taxes (Revenue – Operating Expenses). EBIT(*) measures the profit a company generates from its operations, making it synonymous with "operating profit“.
- **Risk Appetite**: maximum amount of loss sustainable by company. The money a company could loose at a time by unexpected incident or disaster without encountering financial disaster
- **Money Loss**: the actual desumed amount of money a company could loose at a time, based on analysis

(*) For Start-Up EBIT < 0. It should be substituted by “theoretical EBIT”:
Average (EBIT of already-started company)$|_{\text{same Business Sector}}$

F2j BIA

BIA Evaluation – Essential Business Components

Main Disaster Considerations:

- **Relevancy**: consistent outcomes are those making the company not more solvable, comparable to earning (e.g. x% of EBIT). Risk Appetite is the maximum amount of loss sustainable by company

- **Emergency**: main disasters are very huge in consequences. Probability is not more needed (e.g. no Annual Rate of Occurrence)

- **Criticality**: essential components are a restricted number of overall ones (e.g. 4-5)

F2k BIA

BIA Evaluation – Company Sights

The analysis should be treated by a 3rd dimension: different sights (Business, Operation and Risk), in order to provide the needed parameters for resiliency: RTO (Recovery Time Objective) and RPO (Recovery Point Objective)

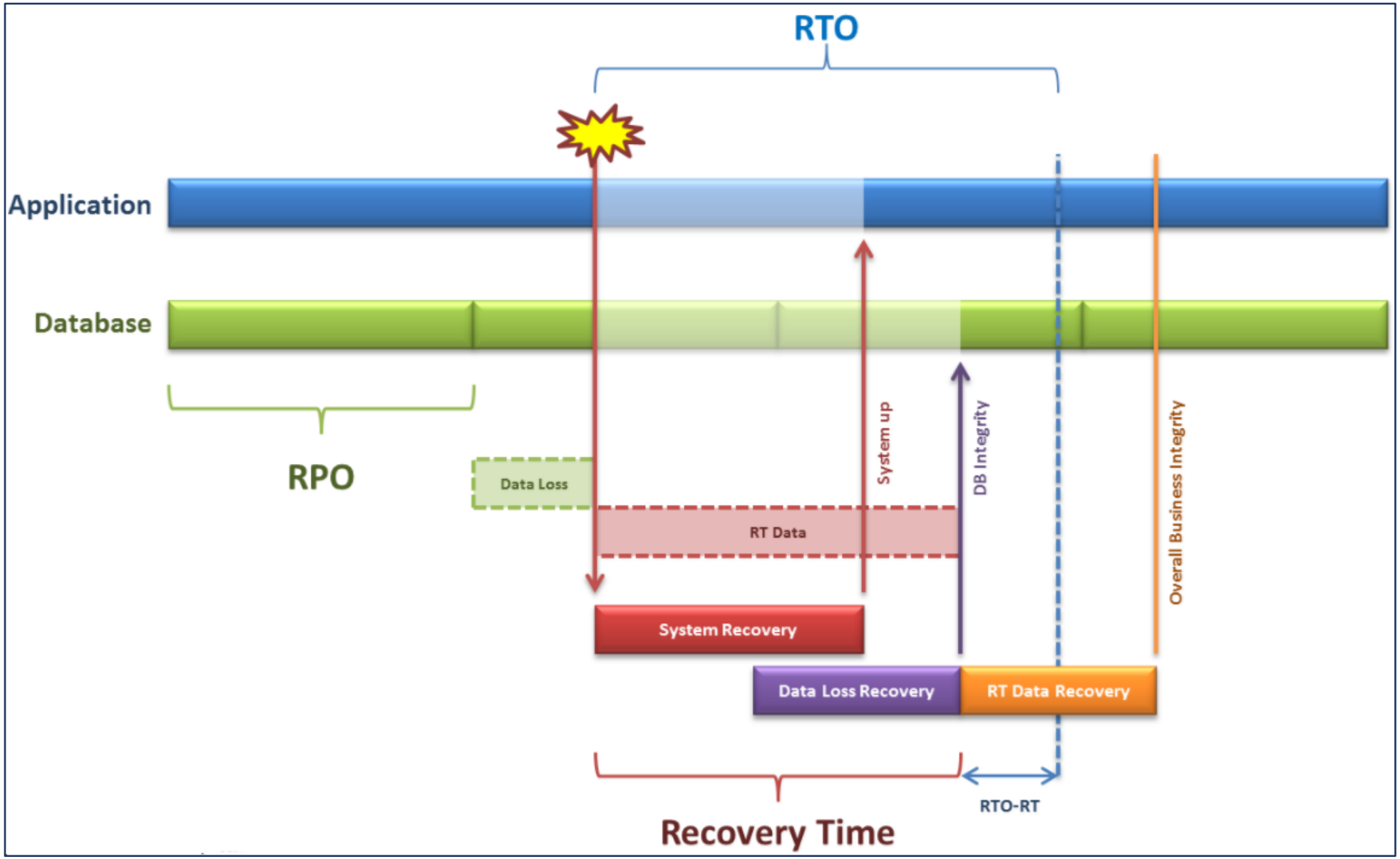
- **Business**: characterization of the company business: Revenue/EBIT, (possible) Disaster or Accident, Risk Drivers (e.g. no earning, customer escape, reputational risk)

- **Operation**: characterization of company internals: Risk Appetite (usually 2%), Outages caused on company premises by identified emergencies, Processes involved by applicable Risk Drivers

- **Risk**: characterization of company risk: Money Loss ($/time, coming from outages of an application), Countermeasures (technical solution to counter-effect outages), IT Applications (technical premises surrouding identified processes)

F2I BIA

RTO & RPO – 3x3 Quadrant



F2m BIA

RTO & RPO – Calculation

To calculate the RTO and RPO values, you should compare the economic losses from a disruption of the identified systems and services, with the value of Risk Appetite, that is, the risk to the Company's risk. This amount must amount to a loss for the Company of a small size so that it can be faced without financial-economic repercussions. For this reason, it is established consistently with business strategies.

Quantification of the Risk Appetite may be related to the value of the EBIT parameter, as deduced from the balance sheet, accounting for a portion equal to 2%

F2n BIA

RTO & RPO – Risk Appetite

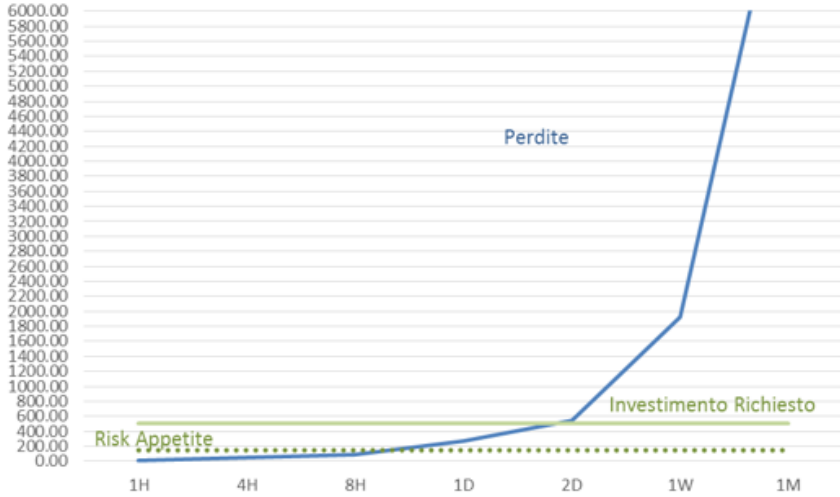
Risk Appetite:

1. “amount and type of risk that an organization is willing to pursue or retain.” [ISO Guide 73:2009 Risk Management – Vocabulary]

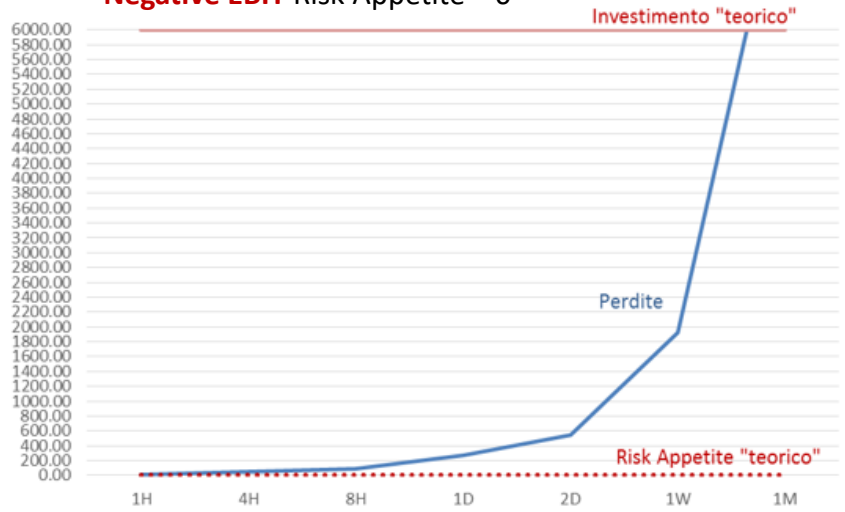
2. the level of risk that an organization is willing to accept while pursuing its objectives, and before any action is determined to be necessary in order to reduce the risk. It allows organizations to determine how much they are willing to take risks (including financial and operational impacts) in order to innovate in pursuit of objectives. [Wolters Kluwer]

3. 2% of EBIT

Positive EBIT Risk Appetite > 0



Negative EBIT Risk Appetite = 0

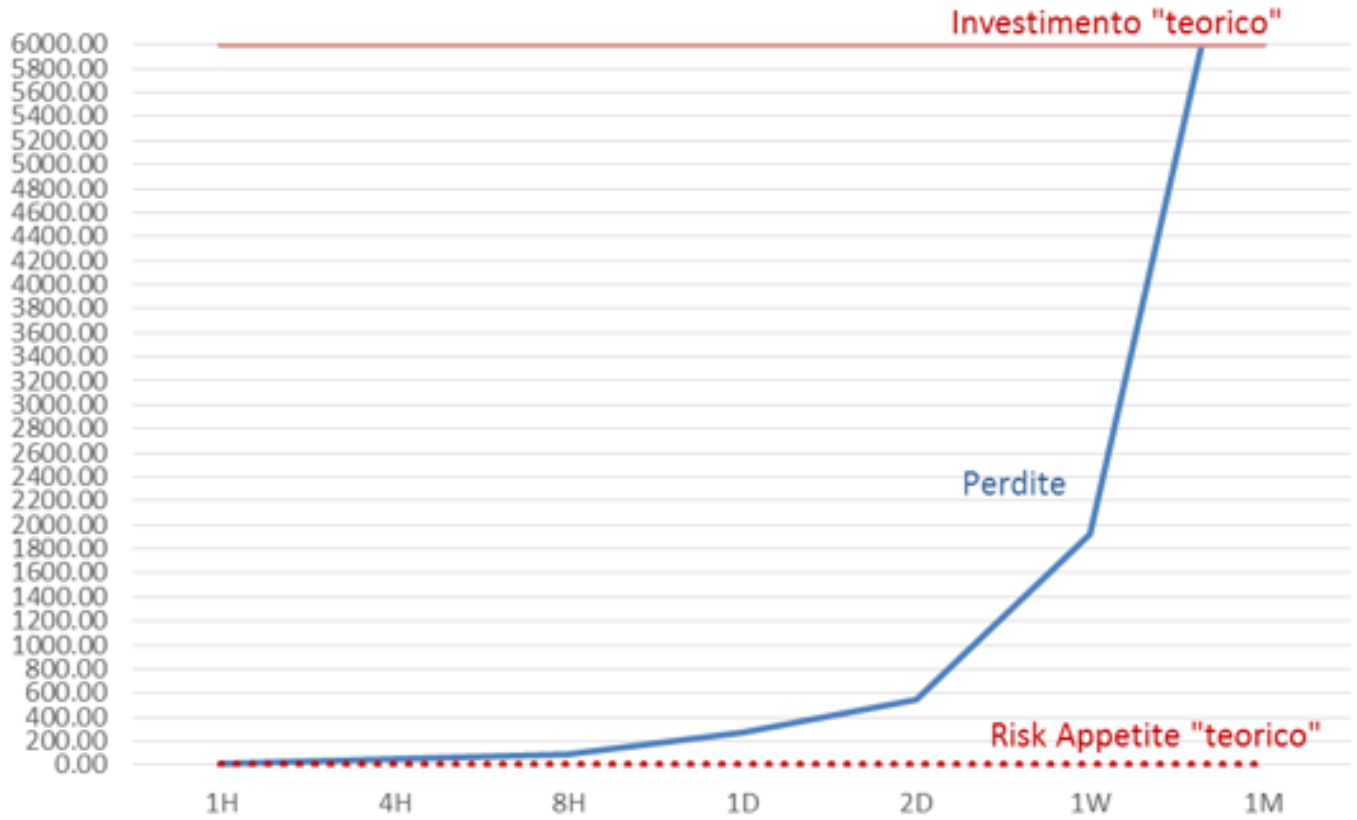


F2o BIA

EBIT < 0 Risk Appetite Calculation 1/2

The value of the EBIT can be calculated in different ways:

1. **Mathematical EBIT**: Calculation done by mere application of the Business Continuity theory. This parameter equates to what is derived from the budget outturn. Using budget outcomes of the last fiscal year, EBIT could be deduced. In the case of negative EBIT, Risk Appetite = 0 (Risk Appetite can not be negative)



The figure compares the loss values (blue line) with the RTO resulting from the Risk Appetite (dashed red line) and the amount of alleged investments, depending on the hours of disruption (Continuous red line).
This scenario involves excessive overdrafts that the Company should support in order to implement all necessary countermeasures

F2p BIA

EBIT < 0 Risk Appetite Calculation 2/2

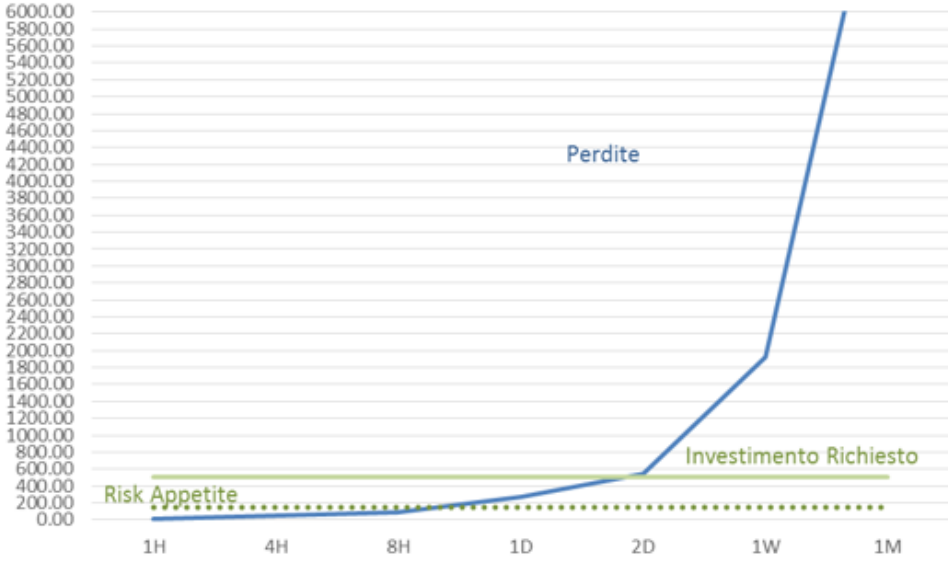
The value of the EBIT can be calculated in different ways:

2. **Theoretical EBIT**: Calculation done by comparison with usual financial values of the business sector financial values. That is, using the typical EBIT Margin

$$EBIT\ Margin = \frac{EBIT}{Revenue}$$

Thus

$$EBIT = (EBIT\ Margin) * Revenue$$



Using the EBIT Margin usually obtained by

- Direct Competitors
- Worldwide Sector Analysis

and substituting Revenue as the last budget outturn

$$Theoretical\ EBIT = (EBIT\ Margin) * Last\ Company\ Revenue$$

F2p BIA

3x3 Quadrant

Components and Sights should be arranged in a 3x3 quadrant:

- “Relevancy” component column maps Economics
- «Emergency» component column shows threats and remediations
- «Criticality» component column addresses items to drive into

	Relevancy	**Emergency**	**Criticality**
Business	**EBIT** (real or calcutaled from Revenue)	Disaster/Accident	Risk Drivers
Operation	**Risk Appetite**	Outages	Processes
Risk	**Money Loss**	Countermeasures	IT Applications

F2q BIA

3x3 Quadrant: RPO & RTO Calculation

	Relevancy	Emergency	Criticality
Business	**EBIT** (real or calcutaled from Revenue)	Disaster/Accident	Risk Drivers
Operation	**Risk Appetite**	Outages	Processes
Risk	**Money Loss**	Countermeasures	IT Applications

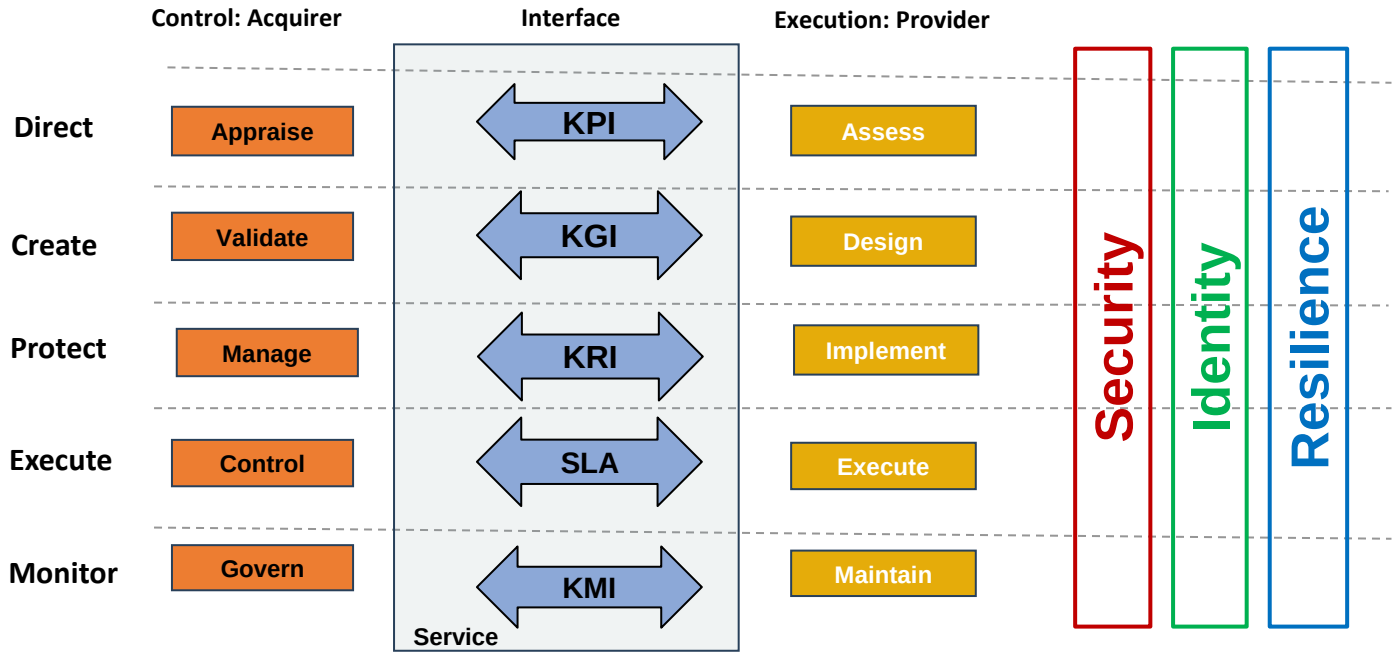
RTO and RPO calculation is straightforward

```
For each identifies IT Application {
   for every eventual emergencies {
     place (countermeasures); //that assures that Money Loss <
Risk Appetite.
     deduce (RTO); //RTO <= Risk Appetite / Money Loss
     deduce (RPO); //RPO >= Delay introduced in Processes in
treating data
   } // end for every
} // end for each
```

F3a Security Analysis

IT as a Service: Operational Governance Interface

What you cannot measure, you cannot manage. An interface should help managing (underpinning) contracts between Acquirer and Provider



Key Performance Indicators (KPIs) are the foundation of any continuous improvement analysis. KPIs measure how effectively an activity was performed.

Key Goal Indicators (KGIs) are a measure of *"what"* has to be accomplished.

Key Risk Indicators (KRIs) indicate how much risky an activity is, early signalling the increasing of risk exposures

Service Level Agreement (SLA) are part of a service where a service is formally defined. In practice, the term *SLA* is sometimes used to refer to the contracted delivery time (of the service or performance).

Key Management Indicators (KMIs) are used to refer to a comprehensive set of KPIs, sometimes involving quality and environment metrics. In addition to Key Activity Indicators (KAIs), KMIs they can be rolled under KPIs.

F3a1 Security Analysis

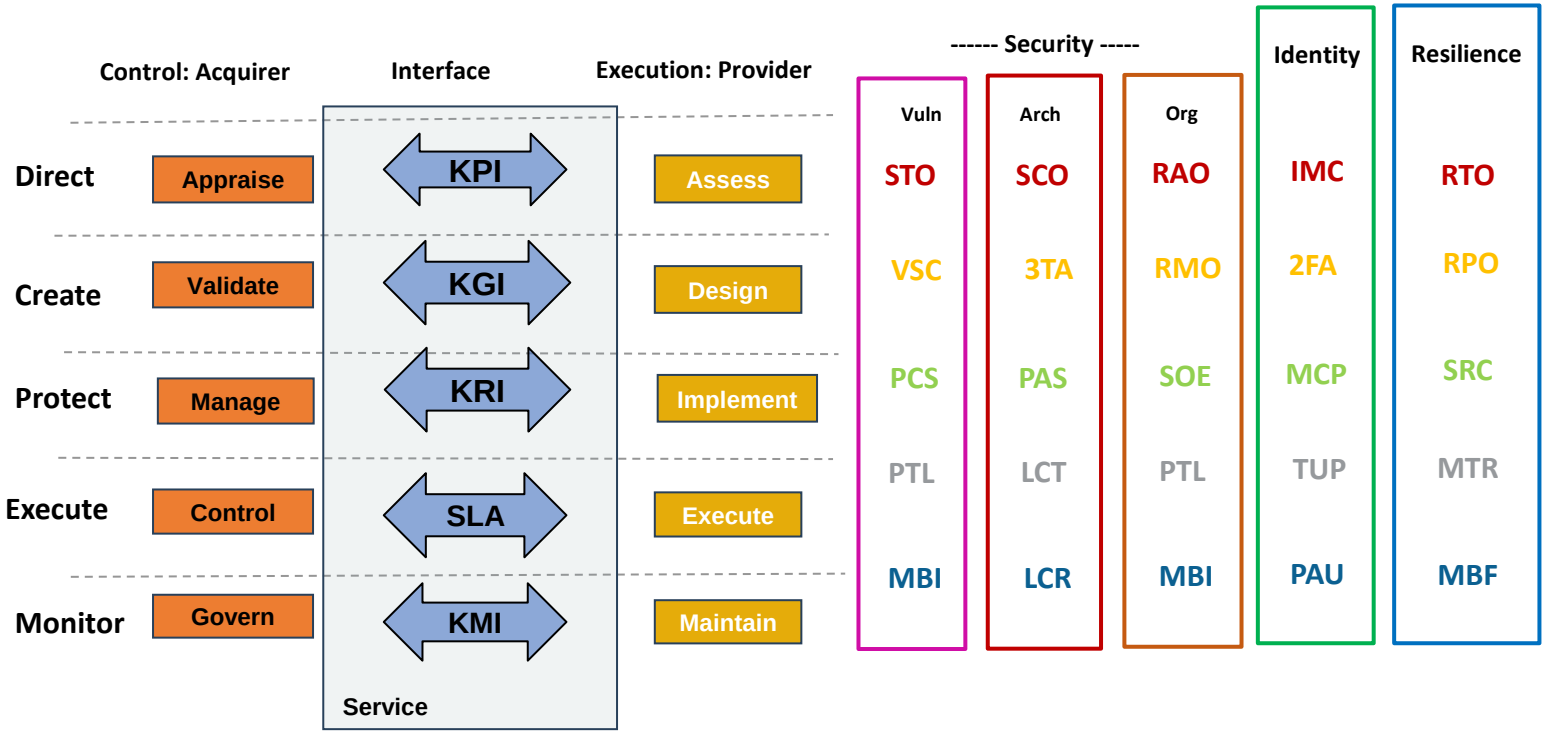
IT as a Service: Operational Governance Dimensions

Identity mapping between physical individuals and cyber ones

Security protection of cyber items

- Vuln: no lack
- Arch: properly built
- Org: properly managed

Resilience ability to withstand changes and still function



F3a2 Security Analysis

IT as a Service: Operational Governance Indicators

Resilience

Recovery Time Objective (RTO) maximum time needed for recover the service
Recovery Point Objective (RPO) time the transaction occurred before accident could not be recovered
System Recovery Coverage (SRC) percentage of systems covered by BC/DR
Meantime To Repair (MTR) average time to recover the service
Meantime Between Failure (MBF) average time from a failure to another one

SECURITY

Vulnerability

Security Testing Objectives (STO) how much time from one pen test to another
Vulnerability Scan Coverage (VSC) percentage of system VA is performed upon
Platform Compliance Score (PCS) percentage of system meeting best-practice standards
Patch Latency (PTL) time between a patch's release and your successful deployment of that patch
Meantime Between Incident (MBI) incident rates: how often these occur

Architecture

Security Control Coverage (SCO) how many technical control in places
Three Tier Architecture (3TA) percentage of systems designed in a 3-tier fashion
Platform Access Score (PAS) percentage of systems protected by access control (FW, WAF)
Log Collection (LCT) percentage of system log are collected from
Log Correlation (LCR) average number of correlation rule per system

Identity

Identity Management Coverage (IMC) proportion of account (privileged and unprivileged) vaulted and managed
Two Factor Authentication percentage (2FA) percentage of user that should use 2FA for accessing the systems
Meantime to Certified Privileged Account (MCP) time a Privileged Account is certified
Time for User Provisioning average (TUP) how long a new user waits to get access to the resources they need
Privileged Account average per User (PAU) amount of «duties» owned by a user (SoD)

Organization

Risk Analysis Objective (RAO) how much time from one RA to the following
Risk Management Objective (RMO) percentage of suggested countermeasure implemented
Security Objective Enforcement (SOE) percentage of countermeasures implemented
Log Collection Latency (LCL) delay from event and trasmission of log to central SIEM
Log Correlation Effectiveness (LCE) percentage of incidents identified by correlation

F3a3 Security Analysis

IT as a Service: Operational Governance Interface

Vulnerability Indicators

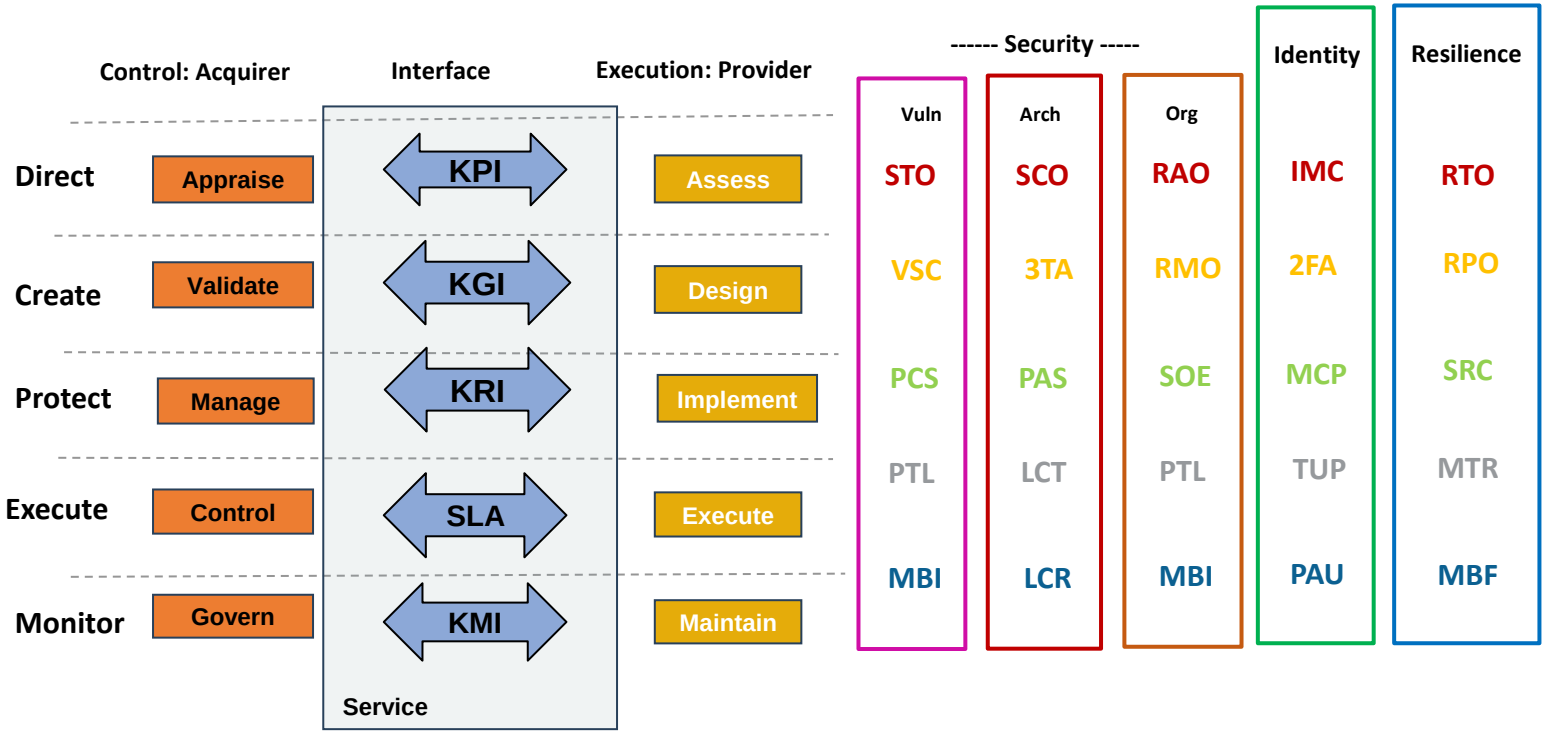
Security Testing Objectives (STO) how much time from one pen test to another

Vulnerability Scan Coverage (VSC) percentage of system VA is performed upon

Platform Compliance Score (PCS) percentage of system meeting best-practice standards

Patch Latency (PTL) time between a patch's release and your successful deployment of that patch

Meantime Between Incident (MBI) incident rates: how often these occur



F3a4 Security Analysis

IT as a Service: Operational Governance Interface

Architecture Indicators

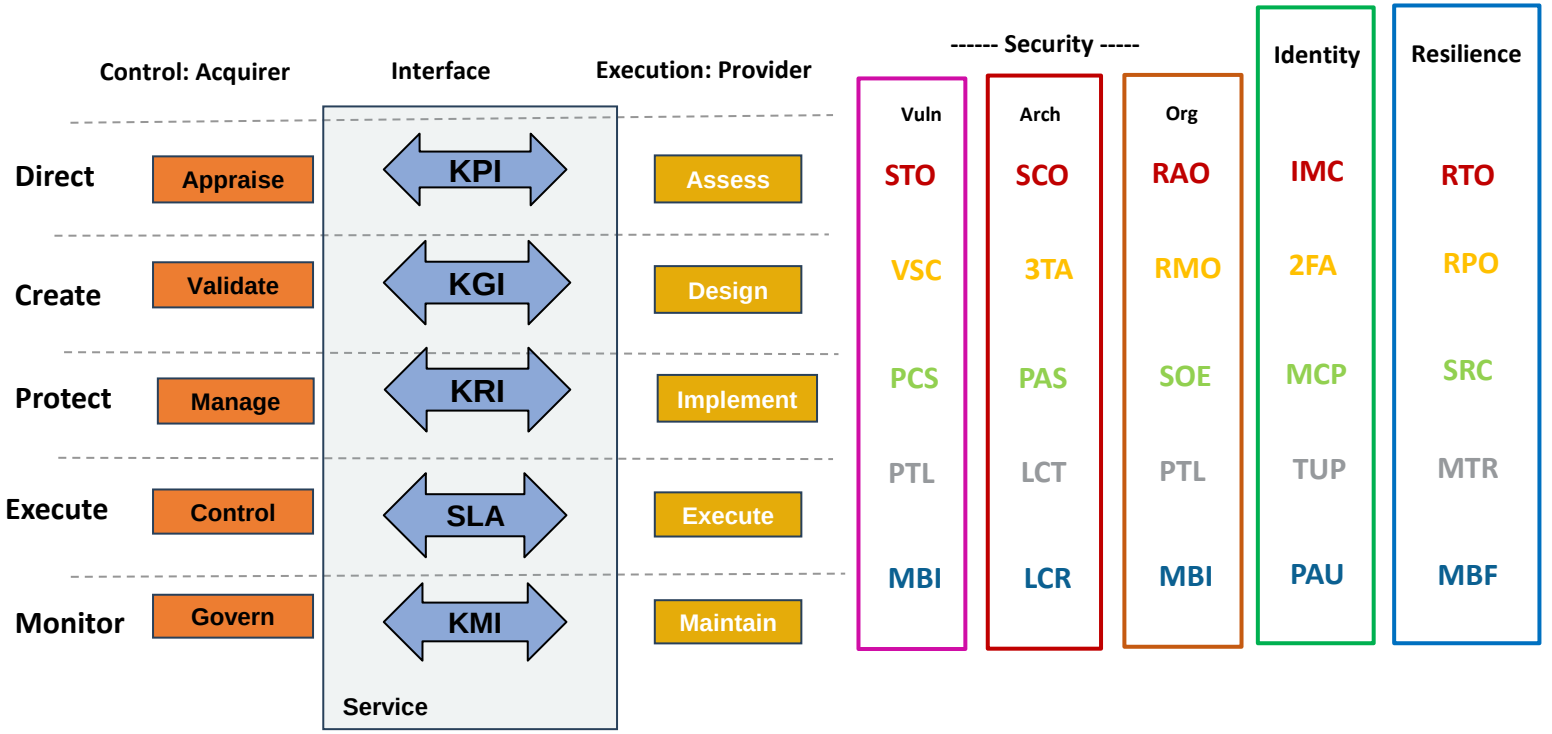
Security Control Coverage (SCO) how many technical control in places

Three Tier Architecture (3TA) percentage of systems designed in a 3-tier fashion

Platform Access Score (PAS) percentage of systems protected by access control (FW, WAF)

Log Collection (LCT) percentage of system log are collected from

Log Correlation (LCR) average number of correlation rule per system



F3a5 Security Analysis

IT as a Service: Operational Governance Interface

Organization Indicators

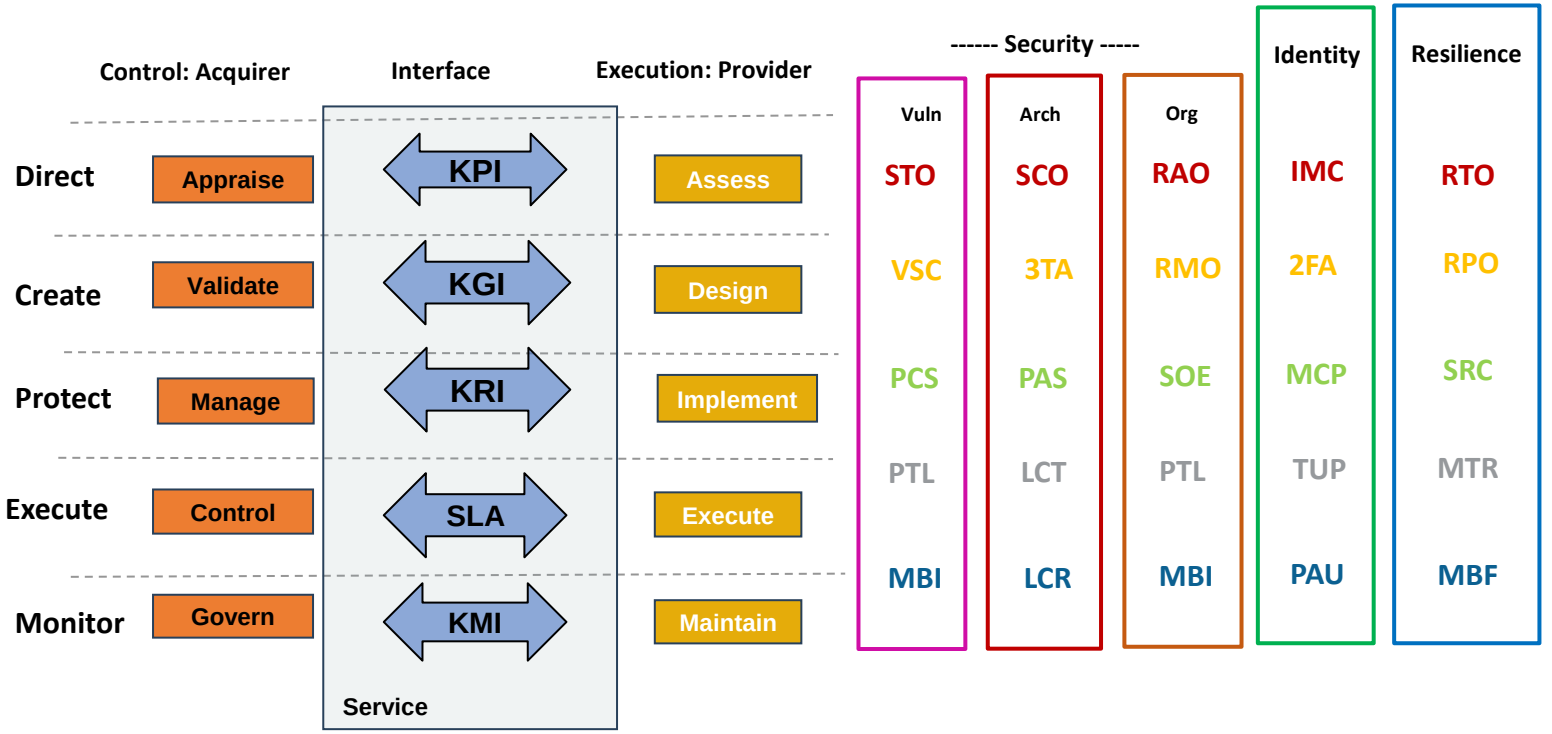
Risk Analysis Objective (RAO) how much time from one RA to the following

Risk Management Objective (RMO) percentage of suggested countermeasure implemented

Security Objective Enforcement (SOE) percentage of countermeasures implemented

Log Collection Latency (LCL) delay from event and trasmission of log to central SIEM

Log Correlation Effectiveness (RCE) percentage of incidents identified by correlation



F3a6 Security Analysis

IT as a Service: Operational Governance Interface

Identity Indicators

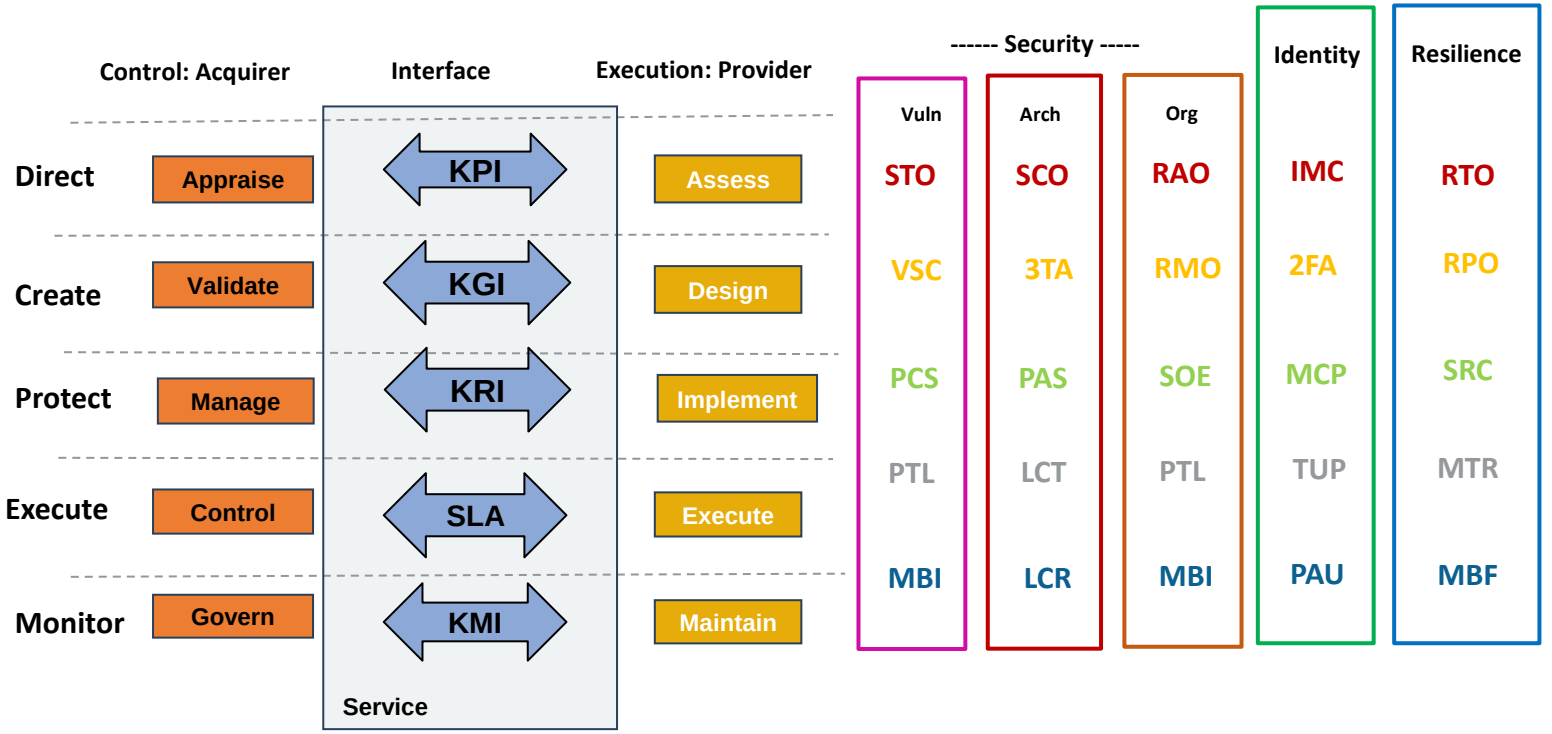
Identity Management Coverage (IMC) proportion of account (privileged and unprivileged) vaulted and managed

Two Factor Authentication percentage (2FA) percentage of user that should use 2FA for accessing the systems

Meantime to Certified Privileged Account (MCP) time a Privileged Account is certified

Time for User Provisioning average (TUP) how long a new user waits to get access to the resources they need

Privileged Account average per User (PAU) amount of «duties» owned by a user (SoD)



F3a7 Security Analysis

IT as a Service: Operational Governance Interface

Resilience Indicators

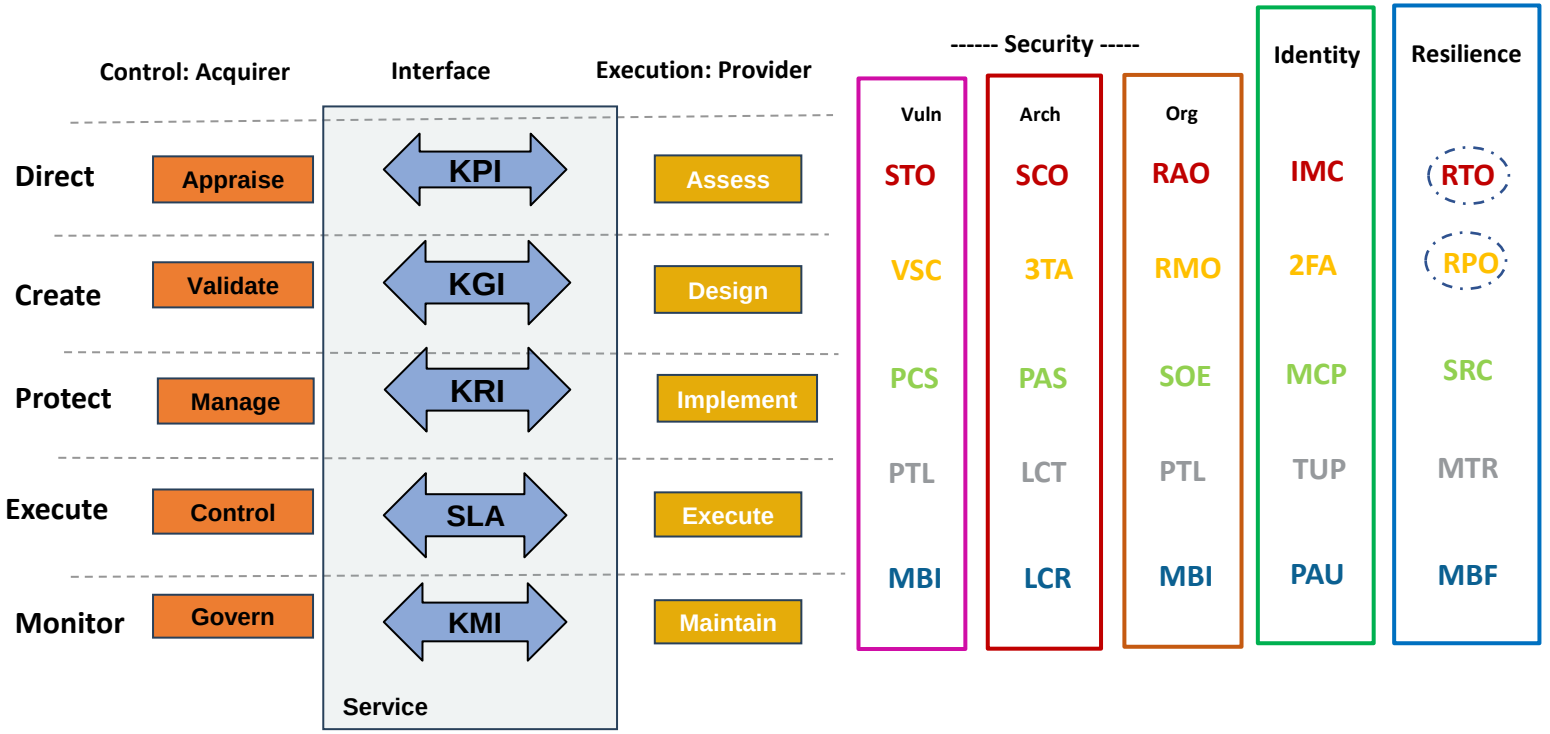
Recovery Time Objective (RTO) maximum time needed for recover the service

Recovery Point Objective (RPO) time the transaction occurred before accident could not be recovered

System Recovery Coverage (SRC) percentage of systems covered by BC/DR

Meantime To Repair (MTR) average time to recover the service

Meantime Between Failure (MBF) average time from a failure to another one



F3b Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

General Measurement of Compliance

	Domain	Control (Countermeasure)	RATING	WEIGHT	VALUE
800-53	**Access Control**	**ISO/IEC 27001**	**1,04**	**2,93**	**3,05**
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Considered	Best-Practice	1,75
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	Considered	Best-Practice	1,75
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3	Considered	Essential	1,63
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	Considered	Essential	1,63
AC-5	Separation of Duties	A.6.1.2	Considered	Critical	1,35
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	Considered	Critical	1,35
AC-7	Unsuccessful Logon Attempts	A.9.4.2	Considered	Critical	1,35
AC-8	System Use Notification	A.9.4.2	Considered	Critical	1,35
AC-9	Previous Logon (Access) Notification	A.9.4.2	Considered	Critical	1,35
AC-10	Concurrent Session Control	None	Considered	Critical	1,35
AC-11	Session Lock	A.11.2.8, A.11.2.9	Considered	Critical	1,35
AC-12	Session Termination	None	Defined	Critical	4,05
AC-13	Withdrawn	---	Defined	Critical	4,05
AC-14	Permitted Actions without Identification or Authentication	None	Defined	Critical	4,05
AC-15	Withdrawn	---	Defined	Critical	4,05
AC-16	Security Attributes	None	Defined	Critical	4,05
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	Defined	Critical	4,05
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1	Defined	Critical	4,05
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.2.6, A.13.2.1	Defined	Critical	4,05
AC-20	Use of External Information Systems	A.11.2.6, A.13.1.1, A.13.2.1	Defined	Critical	4,05
AC-21	Information Sharing	None	Defined	Essential	4,88
AC-22	Publicly Accessible Content	None	Defined	Best-Practice	5,25
AC-23	Data Mining Protection	None	Defined	Important	6,38
AC-24	Access Control Decisions	A.9.4.1*	Defined	Critical	4,05

For each control (countermeasure)

- **Rating**: evaluation of implementation level
- **Weight**: evaluation of the fit into the company environment

F3b Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

General Measurement of Compliance: Rating

Value	Rating	Description
0,5	**Non-Existent**.	Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.
1	**Considered**	The organisation has recognised the importance of this issue and agree that it should be addressed. Some planning is underway but the organisation is still not completely convinced that the proposed security measure makes undeniable business sense.
1,5	**Defined.**	Initial acceptance of the security issue and active consideration of its proposed benefits has developed into detailed planning, formalised objectives and clear deliverables. Any security intervention is still somewhat reactive and approached on a case by case basis.
2	**Initiated**	Decisive action is underway to implement the proposed security measure. Success is still very much reliant on the experience and skills of a few individuals but formalised processes are being developed to ensure measurable results.
2,5	**Operational**	The security measure has been implemented and is considered functional. It is possible to monitor and measure compliance with the proposed security measure and processes appear to be working effectively. Processes (where applicable) are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
3	**Optimised**.	The proposed security measures have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations and/ or stakeholders. Executive management can state with confidence that adequate security measures have been implemented as a demonstration of due diligence in Corporate Governance standards.

- **Rating**: evaluation of implementation level

F3b Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

General Measurement of Compliance: Weight

Value	Rating	Description
0,5	**Optional**	In essence this control objective is regarded as a discretionary measure rather than compulsory. It should be seen as complementary to other security initiatives in the enterprise. The tangible value to be derived from implementing this control objective should be evaluated within the context of constraints such as cost of implementation, technical complexity and resource requirements.
1	**Recommended**	This control objective is expected to add measurable value to the overall security posture of the enterprise. However, it may not be applicable to "all" organisations under "all" circumstances. Instead, the implementation of this control measure should be considered on a case by case basis. At the very least, its implementation should be viewed as a positive recommendation.
1,5	**Important**	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.
2	**Best-Practice**	The implementation of this control objective should be regarded as generally accepted best practice for information security. Any organisation who is serious about demonstrating good corporate governance will regard this measure as a pre-requisite for effective security. Without it, most organisation's will find it virtually impossible to achieve the status of pro-active security management and response.
2,5	**Essential**	Without this control measure, it is likely that the organisation will suffer from the negative effects of regular security incidents. Such incidents may not necessarily bring the organisation to a complete stop, but is set to have grave consequences for operational efficiency, finances and brand value.
3	**Critical**	Critical security control measures should be regarded as "non-negotiable" safeguards to ensure the long-term survival of the organisation. Failure to implement these control measures may result in security breaches that may have catastrophic results for the enterprise.

- **Weight**: evaluation of the fit into the company environment

F3b Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

General Measurement of Compliance: Rating x Weight

	Weight →	Optional	Recommended	Important	Best-Practice	Essential	Critical
	Rating ↓	1	1,5	1,75	2,5	2,75	3,3
	Rating ↓	5	4,5	4,25	3,5	3,25	2,7
Non-Existent	**0**	0	0	0	0	0	0
Considered	**0,5**	2,5	2,25	2,13	1,75	1,63	1,35
Defined	**1,5**	7,5	6,75	6,38	5,25	4,88	4,05
Initiated	**2**	10	9	8,5	7	6,5	5,4
Operational	**2,75**	13,75	12,38	11,69	9,63	8,94	7,43
Optimised	**3**	15	13,5	12,75	10,5	9,75	8,1

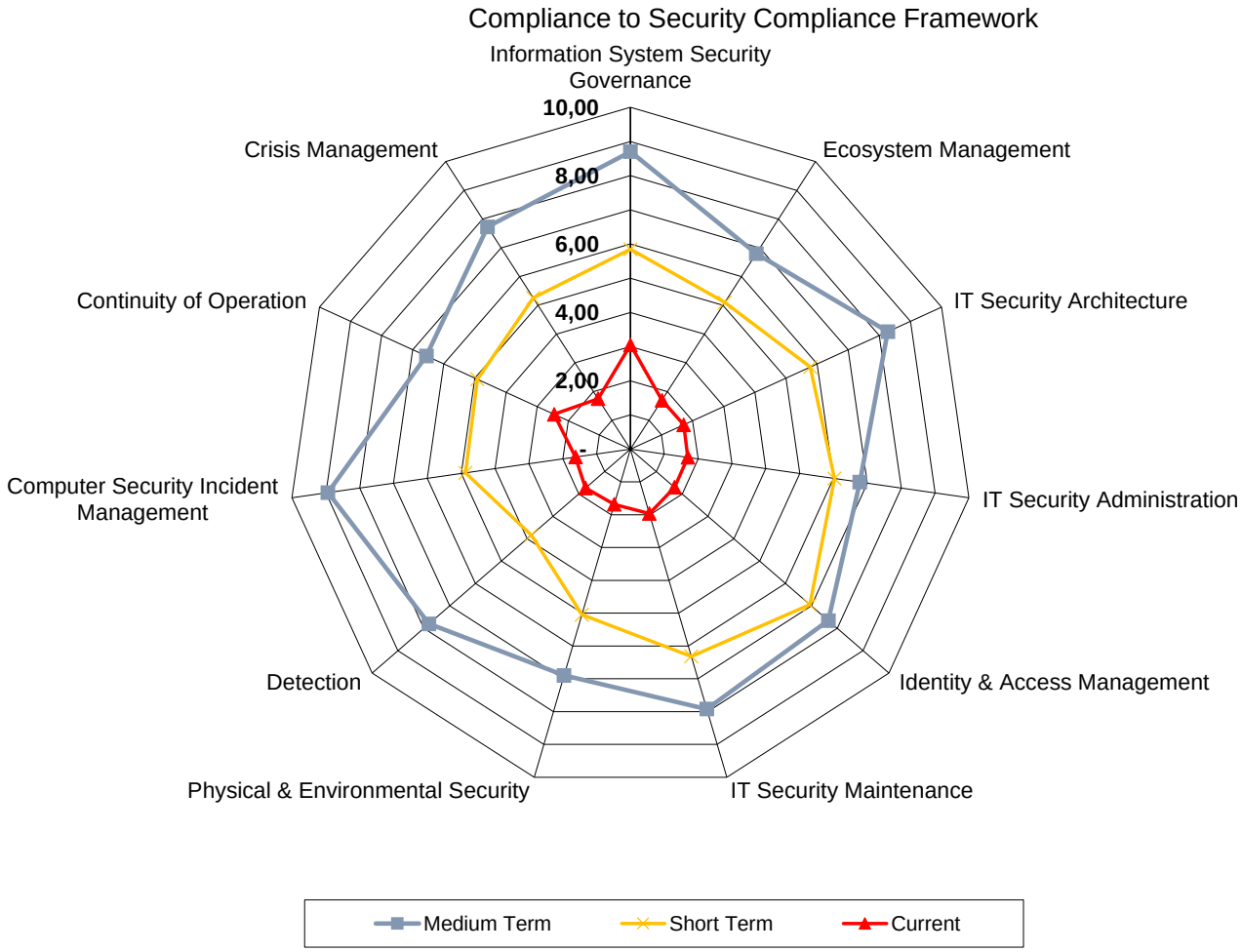
- **Rating**: evaluation of implementation level
- **Weight**: evaluation of the fit into the company environment

F3b Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

General Measurement of Compliance: Risk Map

- Compliance By **Domains** (or Categories), usually 10-15, obtained averaging the values of the **controls** that fit into, usually, 8-10
- **Current**: AS-IS scenario
- **Short Term**: after the implementation of Quick-Wins countermeasures (usually 6 months)
- **Medium Term**: after the implementation of all the Critical and High level countermeasures



F3b1 Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

Es. NIST Cyber Security Framework (CSF): https://www.nist.gov/cyberframework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

The Main Goals Of The NIST CSF

- "facilitate and support the development of" cybersecurity risk frameworks, according to the Cybersecurity Enhancement Act of 2014 (CEA)
- **Framework Core**: set of activities, organized in 5 Functions, 23 Categories and 108 Subcategories
- **Tiers**: context on cybersecurity risk views and managing processes
- **Profiles**: alignment with business requirements

F3b2 Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

Es. CSA Cloud Controls Matrix (CCM): https://cloudsecurityalliance.org/research/cloud-controls-matrix/

CCM™

CLOUD CONTROLS MATRIX VERSION 4.0

Control Domains	Control Specifications
Audit and Assurance - A&A	6
Application and Interface Security - AIS	7
Business Continuity Management and Operational Resilience - BCR	11
Change Control and Configuration Management - CCC	9
Cryptography, Encryption and Key Management - CEK	21
Datacenter Security - DCS	15
Data Security and Privacy Lifecycle Management - DSP	19
Governance, Risk and Compliance - GRC	8
Human Resources - HRS	13
Identity and Access Management - IAM	16
Interoperability and Portability - IPY	4
Infrastructure and Virtualization Security - IVS	9
Logging and Monitoring - LOG	13
Security Incident Management, E-Discovery, and Cloud Forensics - SEF	8
Supply Chain Management, Transparency, and Accountability - STA	14
Threat and Vulnerability Management - TVM	10
Universal Endpoint Management - UEM	14

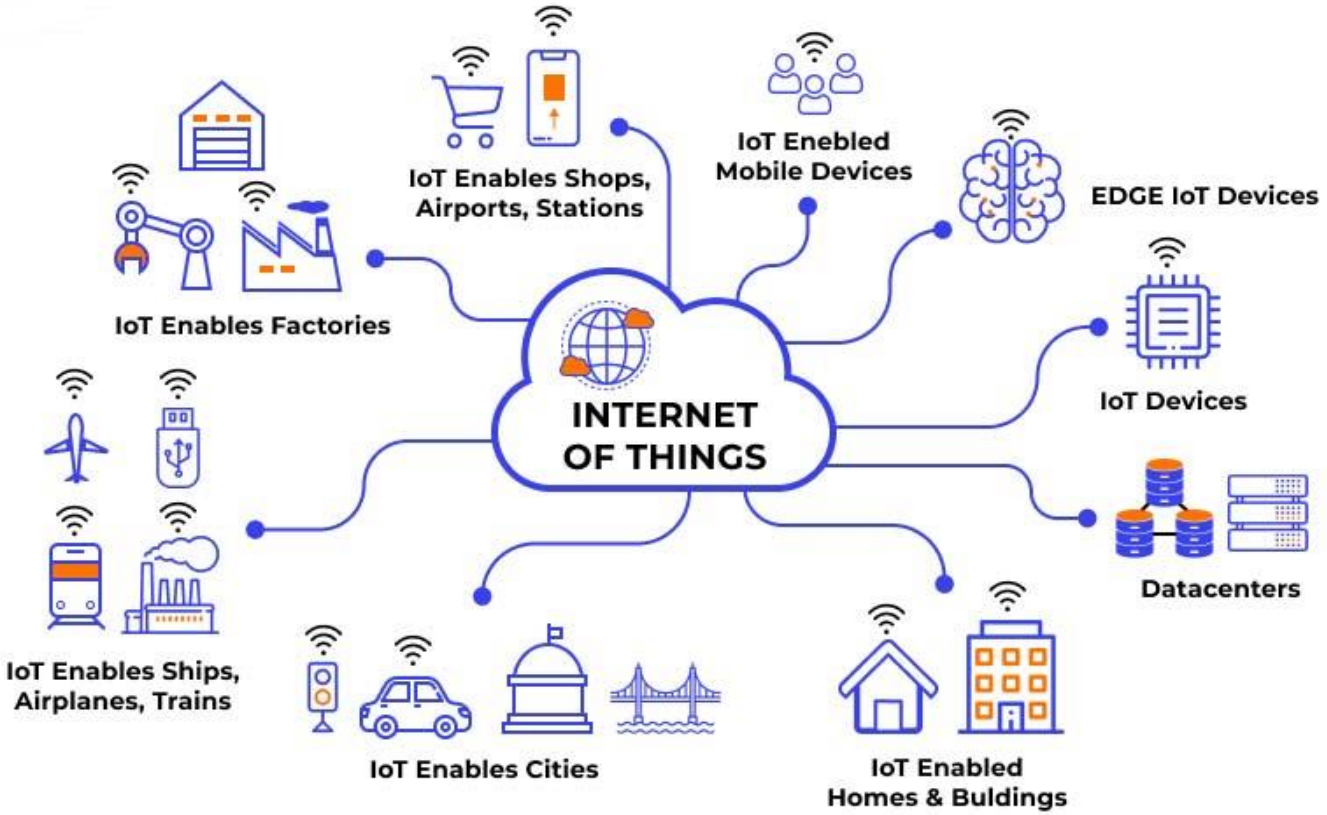
The Main Goals Of The CSA CCM

- Cybersecurity **control framework** for cloud computing: **197 control objectives** that are structured in **17 domains** covering all key aspects of cloud technology.
- **Tool** for the **systematic assessment** of a cloud implementation: Guidance on **which security controls** should be implemented by **which actor** within the cloud supply chain.
- Aligned to the CSA Security Guidance for Cloud Computing, and is considered a **de-facto standard** for cloud security assurance and compliance

F3b3 Security Analysis

Measuring Risk as Compliance Level against a Countermeasure Checklist (Framework)

Es. IoT Security Foundation (IoTSF): https://www.iotsecurityfoundation.org/



The Main Goals Of The IoTSF

- Fabricate a sustainable IoT security framework that can help protect the services and products
- Promote to use of best IoT security practices
- Aware IoT clients and service providers about the importance of adopting of the compliance framework
- Establish well-coordinated assurance processes that align well with the IoTSF compliance framework

F4 Security Risk Management

4 ways to manage

Option	Description	
Avoid	If a risk is deemed too high, then you simply **avoid the activity** that creates the risk.	if flying in an airplane is too risky, you **avoid taking** the flight in the first place, and completely avoid the risk. hiring an individual whose references would not recommend rehiring him — by **avoiding hiring** him, you avoid the risk that he would not be an asset to your company.
Transfer	transfer the risk you take to **another party**	**Insurance companies** exist for exactly this reason. **Outsource providers** perform the process in which the risk is present.
Reduce	one of the **most crucial steps** for processes or activities that cannot be avoided, and where risk cannot be transferred to another party	training your staff on how to identify a phishing email, or on best practices involving login credentials and password hygiene
Accept	there is no option but to accept the risk. Of course, these instances should only involve low risk, or repercussions that are easily managed. Some risks might be completely acceptable and require you to take no action at all	missed deadline on an open-ended project schedule

F4a Security Risk Management

4 ways to manage… as in SW development

B.4k Defenses

Risk treatment Options

break risk treatment options down in a number of types:

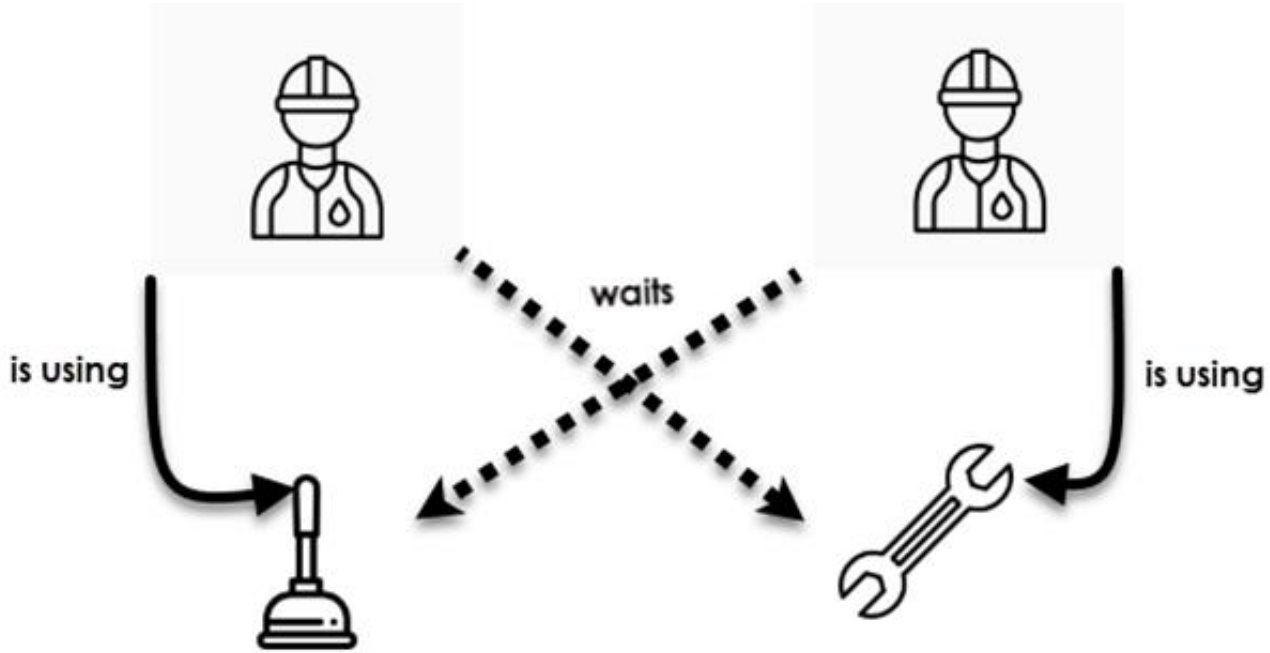
Option			
Avoid	avoid the activity that creates the risk	**Checking Whitelisting**	reject strings that seems invalid (safer than fix it).
Transfer	transfer the risk you take to another party	**Sanitization Escaping**	Replace problematic characters with safe ones
Reduce	security actions for reducing the vulnerabilities	**Checking Blacklisting**	Reject strings with possibly bad chars
Accept	no action at all (or reduced one)	**Sanitization Blacklisting**	Delete the characters you don't want

F4b1 Security Risk Management

4 ways to manage… as in Dealock Management

➔ **Deadlock**: Situation arising from the need to:

- use of 2 or more resources
- by 2 or more processes.



F4b2 Security Risk Management

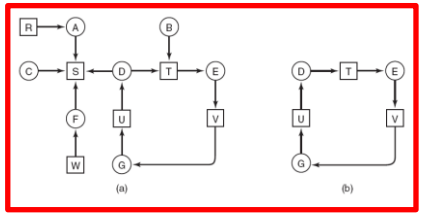
4 ways to manage… as in Deadlock Management

- **Ignore**: justified by the low occurrence of the deadlock. Requires manual user intervention.

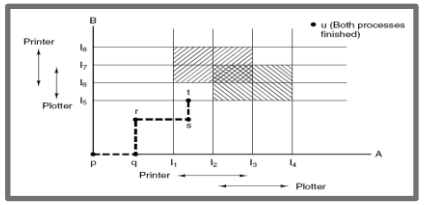
- **Prevent**: prevent all four necessary conditions from occurring. They describe how resources are to be requested.

Condition	Approach
Mutual exclusion	Spool everything
Hold and wait	Request all resources initially
No preemption	Take resources away
Circular wait	Order resources numerically

- **Detect and Recover** detect the occurring conditions and acting for removing one or more of them.



- **Avoid**: The O.S. decides what resource request to accept, on the basis of the knowledge of which resources each process will use, when executed.



No method is optimal, better a combination of them depending on the "resource class“ and “process aim”.

F4b3 Security Risk Management

4 ways to manage… as in Deadlock Management

Risk Option		Deadlock Option	
Avoid	avoid the activity that creates the risk	**Avoid**	The O.S. decides what resource request to accept, on the basis of the knowledge of which resources each process will use, when executed.
Transfer	transfer the risk you take to another party	**Detect and Recover**	detect the occurring conditions and acting for removing one or more of them.
Reduce	security actions for reducing the vulnerabilities	**Prevent**	Prevent all four necessary conditions from occurring. They describe how resources are to be requested.
Accept	no action at all (or reduced one)	**Ignore**	Justified by the low occurrence of the deadlock. Requires manual user intervention.