comptia 701

CAP. 1
di 28

Security controls

Prevent security events, minimize the impact, and limit the damage.

1) Technical controls (logical) → implemented using systems/computer/technology } encryption, IDSs, Firewall

2) Managerial controls (administrative)
→ admin controls associated with security design and implementation
→ Security policies, standard operating procedures (day to day processes)
→ Policy, Risk Assessment, awareness Training
} Focused on reducing the risk of security incidents

3) Operational Control (day-to-day procedure) by people instead of systems : security guards, awareness programs

4) Physical control: limit physical access : guard shack, fences, locks, badge readers.

→ Operational = Configuration Management,
System Backups,
Patch Management, User Access Management, Incident Respond Procedures.

(Physical = material Asset.)

1) Preventive: encryption, Firewalls, AV software

2) Deterrent : Warning signs, lighting, fencing/Bollards.

3) Detective : Log monitoring, Security Audits, CCTV, IDS, Vulnerability scanning → SIEM systems

4) Corrective : recovering data from backup copies,
applying SW updates and patches to fix vulnerabilities,
developing and implementing IRPs to respond to and recover from security incidents;
activating and executing DRPs to restore operations after a major incident.

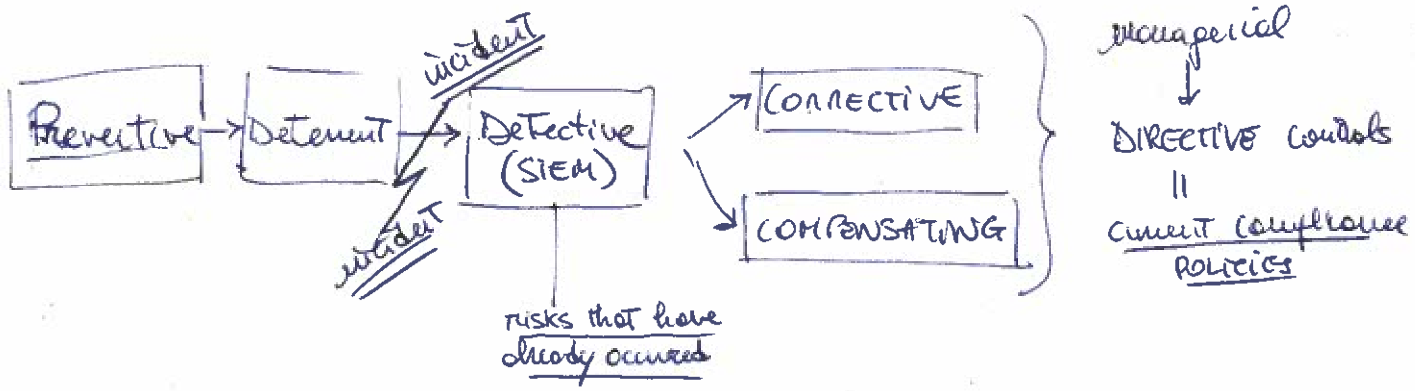
) Compensating : backup power systems;
MFA;
application sandboxing,
network segmentation.

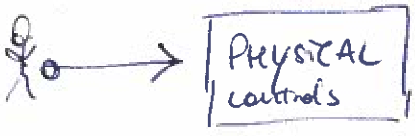
5) Directive : direct a subject towards security compliance.
ex. store all sensitive files in a protected folder.
→ IRP - Incident Response Plan
AUP - AcceptTable Use Policy

} Plan, Policy, Guidelines → RBAC (AC)

Ex. ACL are a combination of Directive and Administrative controls because they provide who can access and under what conditions.
However, the enforcement of ACL - via authentication and authorization - is categorized as Technical/physical control. So, ACL implementation involves different types of controls. ||

0





- CCTV
- Guards
- Barrier

= "a visitor log" produced by reception registration.

what you can touch !

(they would DETER someone from entering)

- Administrator uses Technical controls (technology) to protect and secure data: (ex. encryption and firewalls)

- Managerial controls want to MINIMIZE RISKS → via RISK ASSESSMENT = identification + ~~analy~~ evaluation + mitigation.

↓

establish policies and procedures to guide operations

↓

OPERATIONAL controls = ensure day-to-day activities in a physical environment

↓

PHYSICAL controls = safeguards assets.

Comptia 701 — Lez 2/28

Security concepts

- CIA Triad /
  - C → Authorization
  - I → data unaltered = hashing alg.
  - A → DDoS

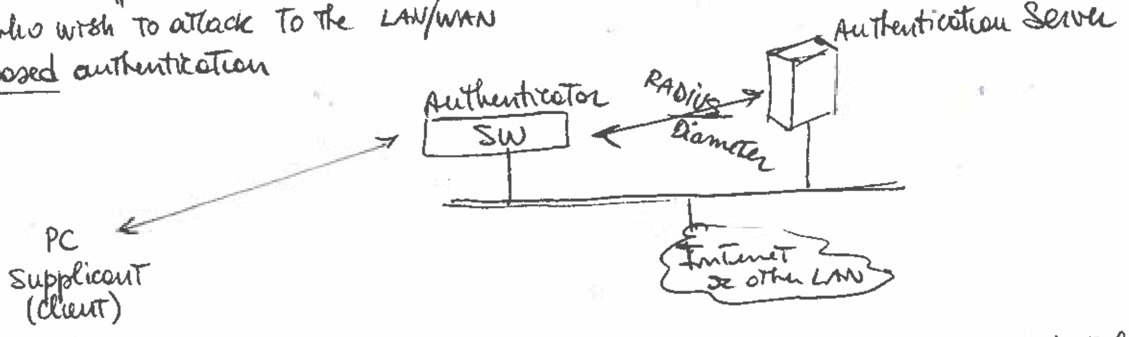
- Non-Repudiation = prevents denial of actions (Trust and accountability) →
  - authentication
  - digital signature (ex. email)
  - Audit Trials = records of actions (user + system logs)
    (is essential for tracking insider attacks!)

↓

- AAA framework = AAA server /protocols :
  - RADIUS
  - Diameter (successor)
  - TACACS+ (cisco)

(IEEE standard)
- 802.1X is the network leader authentication protocol for network access who wish to attack to the LAN/WAN

Port-based authentication

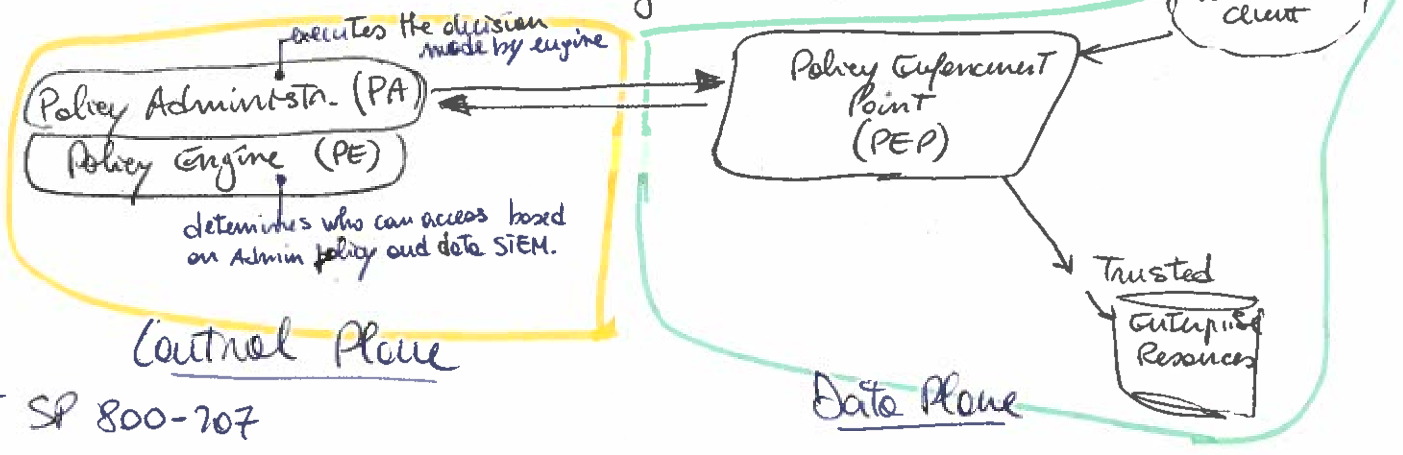


- With 802.1X port-based authentication, the supplicant PC must provide the required credentials to the authenticator (name/passw and or digital certificate).
- The authenticator forward these credentials to the server to decide

(in next page see : internal/external, DMZ)

- Zero Trust : "never trust, always verify"
  ↳ distinct roles :
  - ① The data plane ensures efficient movement of information (the PEP sits here controlling access to resources)
  - ② The control plane manages the intelligence behind (data routing ...)

— Policy-driven Access Control → Logical component of Zero Trust Architecture


executes the decision made by engine
Policy Administr. (PA)
Policy Engine (PE)
determines who can access based on Admin policy and data SIEM.
Control Plane
Untrusted client
Policy Enforcement Point (PEP)
Trusted
Enterprise Resources
Data Plane

- NIST SP 800-207

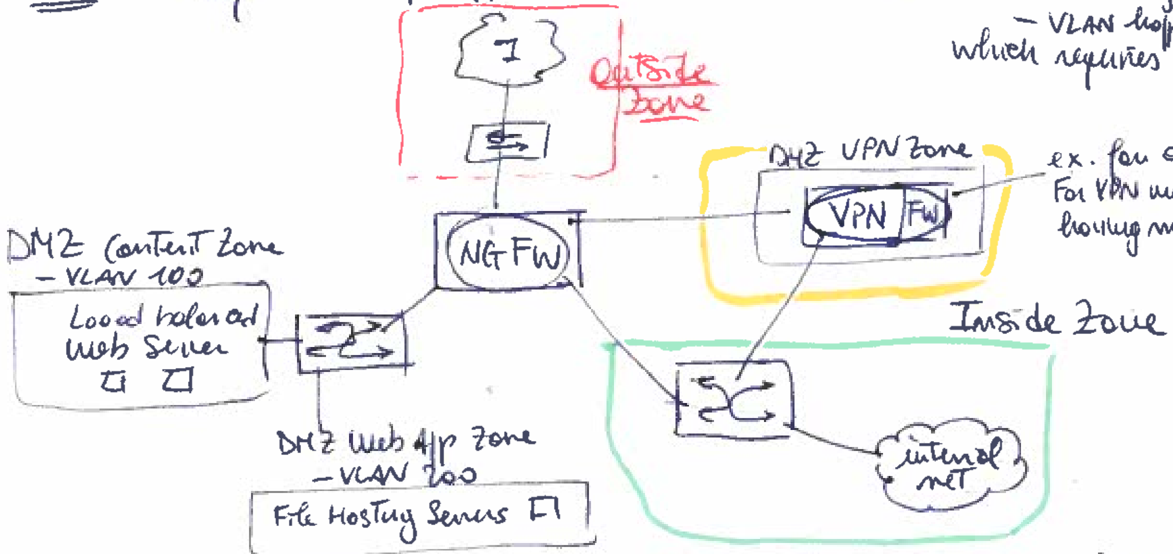
Control Plane : looks at company policies coupled with Threat intell. data.

- Policy engine : determines who can access on a per-user basis. Operates based on policy. (CONTEXT is crucial, with many data for decision)
- Policy Administr.: executes decision made by the PE to control access to the network. It can communicate with Data Plane!

Data Plane ("zones") : network Topology

- VLAN are widely used to keep traffic in their own lanes → the only attack against VLAN is
  - double tagging
  - VLAN hopping attack

  which requires knowledge on untagged VLA

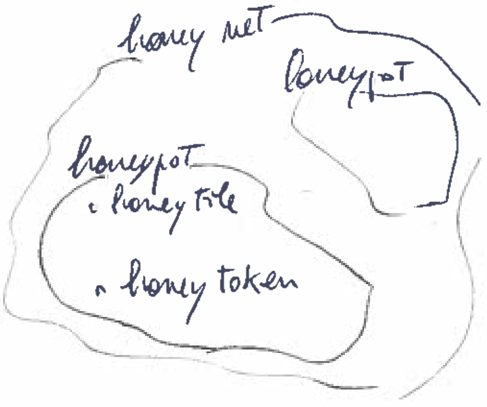


ex. for a BYOD environment. For VPN we have a VPN-FW, for having more granular policies.

The design has tagged TRUNK interfaces moving down to distributed switches with the NGFW acting as the default-GW for each VLAN.
- When traffic travels from zone to zone (inter-VLAN) we have the ability to apply FW Policy.
- if a new server is added, we can create a new VLAN on the switches and FW.

Deception and Disruption :

- honeypot: to find out the (most recent) attack methods → ex Website
- honeynet: a group of honeypot
- honey file: for deception, once accessed it sets off alarms to SOC - pro-active defence - (ex. passwd file)
- honeytoken: designed to track the attackers, it's dummy data presented itself as a prized target.



RADIUS is a centralised authentication, authorization and accounting server. RADIUS clients could be VPN-, WAP-, or 802.1X-managed switches. When authenticated, they are added to SQL DB that tracks logs.

- Federation Services is used for 3rd-party authentication.
- Kerberos is Microsoft authentication.
- OAuth is used for internet-based authentications.

change management

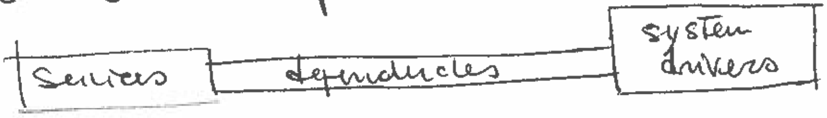
- system upgrade
- new software installation
- switching from one technology to another

→ in term of security, clear ownership is crucial → handled by the CISO (who'll be responsable)

\ having a BACKOUT plan : helps return everything to the way it was ((Rollback!))

* Before a network administrator can make changes to any network device, They must seek approval from the CAB to ensure the changes are aligned with the organization's goals

- the actual network infrastructure is represented (visual) by UPDATING DIAGRAMS.

- 

- golden rule: we won't to impact the Production environment (running)
  - So a Service Restart (close + reopen) has a "downtime".
  - Like a maintenance window for system updates & changes may disrupt users! (logged)
  - weakness may emerge on restart.

comptia 701 cap. 4/28

cryptographic solution

PKI

- Public Key:
  - the format PKCS is P7b and the file extension is .cer.
- private key: used for DECRYPTION + for generating DIGITAL CERTIFICATE. in PKCS is P12 and .pfx
  Recipients can verify the sender's identity using public key.
- Key escrow (custode):
  Trusted third party responsible for securely storing copies of crypto keys. → using HSM

Encryption

- Full-Disk Enc. (FDE) to protect hard drive or SSD → associated with Full-Disk Encry. There's always the Trusted Platform Module (TPM) chip where keys are stored
- Encrypted File System (EFS) can be used to encrypt files where the keys are stored in the user's profile.
- Communication/transport → SSL/TLS protocol over TCP/IP protocol = HTTPS for web browsing

Assymmetric alg.:
RSA, Diffie-Hellman, Elliptic Curve (ECC).
↓
Symmetric alg:
DES (56 bit), 3DES (168 bit), and more popular AES (256 bit).
→ key exchange (securely delivery keys): ex Diffie-Hellman key exchange.

Tools (for Root of Trust)

1) TPM chip integrato in un dispositivo. Archivia keys, Secure Boot e autentica.
- Apple iOS = Secure Enclave (T2 chip
- Android = TrustZone (ARM)

2) (più esteso) HSM
per Server e Cloud con alto livello di sicurezza.
gestione totale delle keys in ambito aziendale.
→ Non è integrato, ma stand-alone!
} FIPS 140-2 e 140-3

HASHING

- one way function:
  - SHA1 (160 bit)
  - MD5 (128 bit)

* data integrity
* password security + "SALTING" → added random data according in clear. On this way 2 same passwords does not have same hash! stored.

Brute Force or Dictionary attack (rainbow table) cap.172-701

Cryptographic solution

Cap. 4/28 bis

- key stretching = designed to transform a password into a longer, more complex key.
  Using ex: - PBKDF2
  - Bcrypt

- Digital Signature = a signer uses is signature = private key that is specific to the document. it's generated.

  the recipient uses the signer' publick key to validate the signature, ensuring the document's integrity and origin.

CERTIFICATES

A digital signature adds TRUST.

- PKI uses Cert. Authorities for additional Trust
- certificate creation can be built into the OS ; ex. part of Windows Domain services.

What's in a digital certificate (Lock in the browser for each website)?

→ X.509 standard format for digital certificate
(we have inside SN, version, public key...)

We need a good way to trust an unknown entity (random website):

- Certificate Authority (CA) has digitally signed the website certificate
- → you trust the CA, therefore you trust the website → (real-time verification means validation)

Where is this mechanism?

Built-in To your BROWSER

Inside our organization: you are your own CA. In fact Microsoft has its own Windows certificate Services.

→ internal certificates don't need to be signed by a public CA. Install the CA certificate/trusted chain on all devices. → Self-signed dig.ce

- Wildcard (certificates) - extension = Subject Alternative Name (SAN) ← multiple servers, but in the same domain name.
  it's an extension of X.509; Allows a certificate to support the same Domains name (Fully qualified Domain Names - FQDNs)

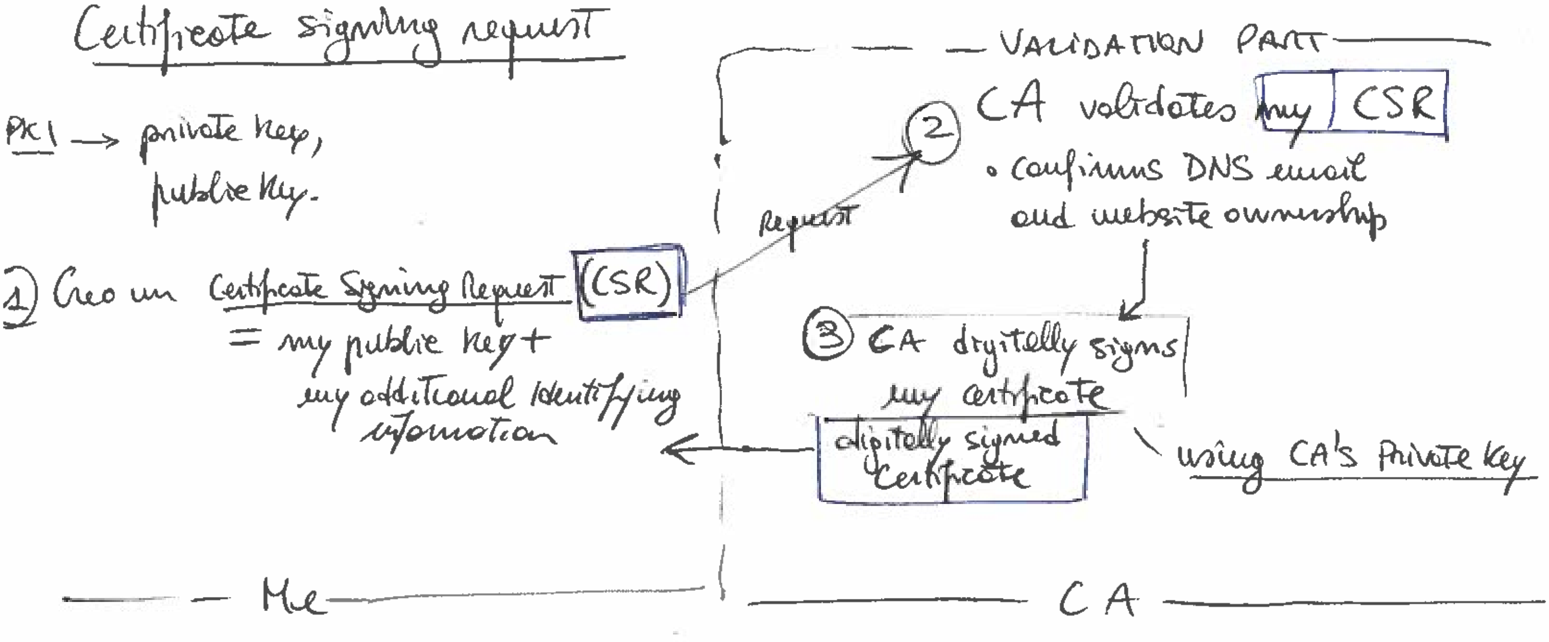
KEY REVOCATION

→ CRL - Cert. Revocation List (maintened by the CA) ← ex heartbleed vulnerability (2014)
  it's a list of URI in your own browser!

→ Online C. Status Protocol _ is "stapled" into the SSL/TLS handshake.
(OCSP) ← What we're using today!

Certificate signing request

PKI → private key,
public key.



VALIDATION PART

1) Creo un Certificate Signing Request (CSR)
= my public key +
my additional identifying
information

Request

2) CA validates my CSR
- confirms DNS email
and website ownership

3) CA digitally signs
my certificate

using CA's Private Key

digitally signed
certificate

Me

CA