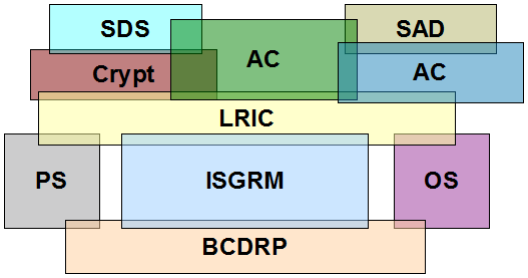
CISSP: Certified Information System SecurityProfessional

Appunti per l'Esame di Certificazione

1 agosto 2012



Paolo Ottolino (PMP CISSP-ISSAP CISA CISM OPST ITIL)

Prefazione
Questo manuale in Italiano fornisce appunti schematici per superare l'esame CISSP. Io ho superato l'esame nel 2004: alcuni aggiustamenti sono stati operati al CBK (Common Body of Knowledge) negli anni. Però nessun cambiamento sostanziale è stato adottato; questo testo riflette gli aggiornamenti necessari.

Indirizzamento
Il CISSP certifica le necessarie competenze nella progettazione, realizzazione e manutenzione di sistemi atti ad indirizzare la sicurezza delle informazioni. Cioé, esso è stato ideato per quei professionisti che realizzano nel campo IT infrastrutture e componenti di protezione, ovvero abilitano le funzioni di sicurezza nei sistemi esistenti.
Diversamente da altre certificazioni storiche del settore, il CISSP è stato pensato per chi opera fattivamente nella realizzazione di infrastrutture tecnologiche ad un livello intermedio, tattico. E' indirizzato a coloro i quali siano chiamati a comprendere le esigenze strategiche di business (es. certificazioni ISACA: CISM, etc) e del relativo auditing (es. ISACA: CISA) ma tuttavia sappiano interagire proficuamente a livello operativo con gli addetti specializzati (es. certificazioni SANS: GCUX, GCIH, etc).
Queste caratteristiche rendono l'esame CISSP altamente tecnico e di dimensioni ragguardevoli (difatti si compone di 10 domini). La preparazione all'esame risulta, quindi, più complessa di quella delle altre certificazioni rivolte ad altre figure professionali.

Esame di Certificazione
A partire dal 1° Settembre 2012 gli esami saranno nella forma CBT (Computer Based Test), la qual cosa comporta i seguenti vantaggi:

- sostenere l'esame non è più vincolato alle 2 dati annuali fissate da (ISC)2
- nel tempo verranno abilitate più sedi d'esame; attualmente i centri Pearson/Vue abilitati sono Roma (2) e Milano (1)
- non è più necessario allenarsi ad annerire i pallini con precisione e rapidità, come nell'esame PBT (Paper Based Text)

Indice

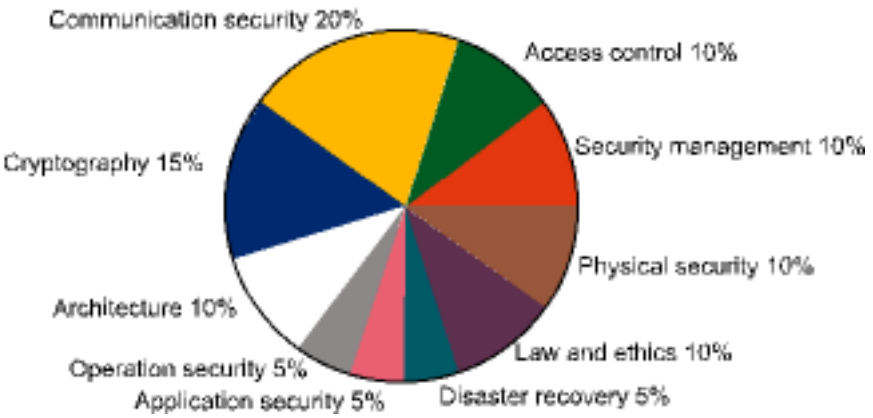
Introduzione

Domini CISSP

Come in tutte le certificazioni, il BoK è diviso in domini. Il CISSP è piuttosto corposo e ne annovera ben 10. Vediamoli nella tabella seguente:

Dominio	**Acronimo**	%
Access Control	AC	10
Telecommunication & Network Security	TNS	20
Information Security Governance & Risk Management	ISGRM	10
Software Development Security	SDS	5
Cryptography	Crypt	15
Security Architecture & Design	SAD	10
Operational Security	OS	5
Business Continuity & Disaster Recovery Planning	BCDRP	5
Legal, Regulation, Investigation and Compliance	LRIC	10
Physical (Environmental) Security	PS	10

La figura seguente illustra l'importanza relativa di ciascun dominio nei quiz d'esame:



Nel seguito sono sinteticamente indicati i contenuti di ciascun dominio, suddivisi per tipologia:

Information Security Governance & Risk Management: Gestione Strategica ed Organica della Sicurezza. Si tratta del dominio di più alto livello d'astrazione; esso rappresenta il cardine centrale sul quale sono imperniati tutti gli altri

Policy: indica un dominio che illustra il modo di indirizzare i requisiti mandatori cui si può essere soggetti:

Business Continuity & Disaster Recovery Planning: Meccanismi da adottare per garantire la Disponibilità dei Dati e della Infrastruttura IT

Legal, Regulation, Investigation & Compliance: Aspetti Legali legati al mondo IT, quali

- normative da rispettare
- modalità che devono essere abilitate per l'esecuzione delle investigazioni (anche con validità forense)
- metodi e meccanismi per eseguire il controllo di conformità

Approccio: indica un insieme di conoscenze che devono essere impiegate come linea guida tecnica nella progettazione e realizzazione delle infrastrutture di sicurezza, al fine di soddisfare i requisiti che provengono dai domini relativi alle Policy (BCDRP e LRIC)

Access Control: Meccanismi di segregazione dell'infrastruttura, partizionamento delle risorse, ammissione d'ingresso e sorveglianza

Telecommunication & Network Security: Caratteristiche, Peculiarità e relativi Dispositivi per la sicurezza in ambito distribuito e di rete

Security Architecture & Design: Metodi, Architetture e Modelli da adottare per comporre la struttura IT in modo sicuro

Prassi: indicazioni operative, relative ai costumi, alle consuetudini ed alle usanze che devono essere introdotte nell'operatività quotidiana, al fine di aumentare il livello generale di sicurezza, in modo da non inficiare quanto realizzato da un buon Approccio (AC, TNS, SAD)

Operational Security: Prassi ed Istruzioni da adottare per operare nell'IT in modo sicuro

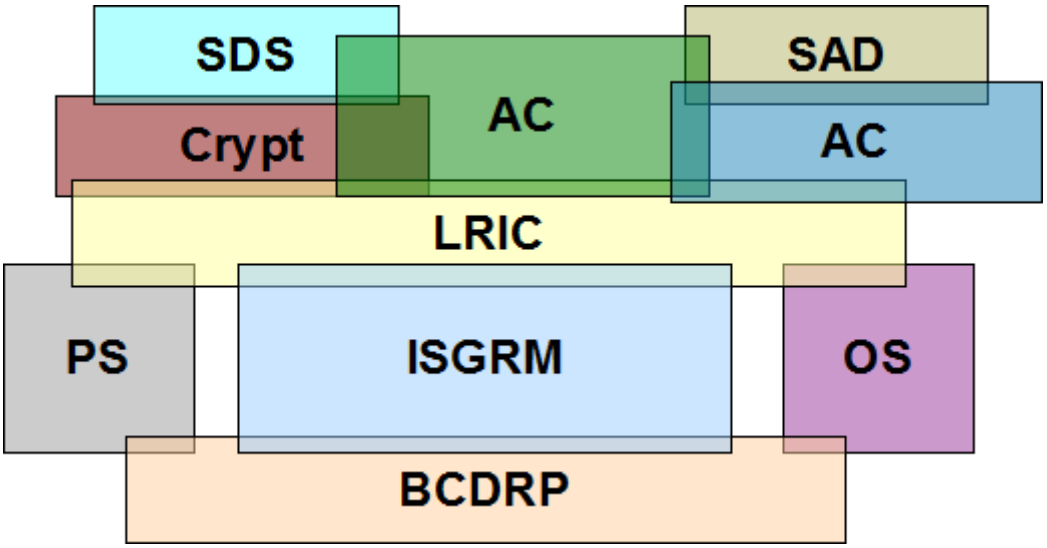
Software Development Security: Prassi e Metodi per lo sviluppo protetto di software. Modelli e Meccanismi per aumentare la sicurezza nel software

Tecniche: domini relativi a specifiche tecnologie, capacità e competenze da padroneggiare per poter essere impiegate nella sicurezza, soprattutto come ausilio per i domini di Approccio (AC, TNS, SAD)

Cryptography: Meccanismi ed algoritmi matematici di codifica dei dati, al fine di garantirne la Confidenzialità, l'Integrità

Physical (Environmental) Security: Aspetti di sicurezza dell'ambiente fisico: • anti-intrusione • fuoco ed esplosione • calamità naturali

La figura seguente mostra graficamente le interdipendenze logiche tra i diversi domini:



Strutturazione Quiz CISSP

Domande: 250 (225 in valutazione, 25 di esperimento)

Tempo: 6 ore

Passing Score: determianto dinamicamente. In generale, varia, intorno al 70%-75% (158 - 169)

Quiz Response Tips

Nel presente paragrafo vengono forniti dei suggerimenti di carattere generale allo scopo di determinare dei criteri per rispondere alle domande poste nei quiz, indipendentemente dall'argomento trattato.

Tipi di Quiz

Può essere utile capire la modalità con cui è stato ideato ogni quiz (domanda + le 4 possibili risposte), nel momento in cui ci si accinge a rispondere, allo scopo di determinare quale sia i processi mentali che ci si aspetti vengano seguiti, in funzione del livello di preparazione, e non cadere in facili trabocchetti. In questa ottica i quiz Le domande possono essere classificate in vari modi, in funzione di:

- formulazione della domanda
- scelta delle 4 risposte possibili

Formulazione della Domanda

What-is: domanda chiara e semplice, quale delle quattro seguenti possibili risposte è giusta

What-is-not: simile alla precedente ma con una o più negazioni, in modo da confondere

The-Best: domanda insidiosa, si chiede quale sia la migliore delle risposte sottoelencate

The-Most: domanda insidiosa,

Scelta delle 4 possibili Risposte

2-Bad: vi sono due risposte palesemente non corrette, occorre scegliere fra le restanti altre due

All-Valid: tutte le risposte corrispondono a concetti dell'esame ma solo una interessa la domanda posta

General Response Tips

Very Closer Choise

Letio Difficiliora

Acronyms

ATM: Automatic Teller Machine

CAAT: Computer Assisted Audit Tecniques

CobiT: Control Objectives for Information and related Technology

CORBA: Common Object Request Broker Architecture

CPA: Control Process Accounting (?)

CSA: Control Self-Assessment

EDI: Electronic Data Interchange

EFT: Electronic Found Transfer

FAR: False Acceptanse Rate

FRR: False Rejection Rate

ISACA: Information System Audit and Control Association

ITF: Integrating Test Facility

IPF: Integrated Processing Facility (CED)

PoS: Point of Sales

SOAP: Simple Object Access Protocol

SPOOL: Simultaneous Peripheral Operation On-Line

Chapter 1

Access Control

1.1 Access Control Concepts

Una delle basi dell'Information Security è il controllo delle modalità di accesso alle risorse, in modo congruente ai tre principi AIC. Tali controlli possono essere, ovviamente, Administrative, Technical (Logical) e Physical.

Access Control: caratteristica di sicurezza per il controllo delle interazioni fra utenti, sistemi e risorse

Access: flusso di informazioni fra un subject ed un object

Subject: entità attiva (utente, programa o processo) che richiede l'accesso ad un oggetto o ai dati in esso contenuti

Object: entità passiva che contiene informazioni

1.2 AAA

AAA sta per Identification, Authentication, Authorization and Accountability

1.2.1 Definitions

Identification: descrive un metodo per assicurarsi che l'entità sia effettivamente chi dichiara di essere. Si espleta mediante l'assegnazione di un ID: login o un codice

Authentication: controllo effettivo della identità di una entità effettuato apartire da una seconda informazione (credenziale) fornita assieme all'ID

Authorization: controllo, effettuato mediante Access Control Matrix o Security Labels, della possibilità realemnte assegnata di accedere una determinata risorsa

Accounting: atto del tracciare gli accessi alle risorse

1.2.2 Identification e Authentication

Sebbene separati logicamente, ad ogni autenticazione vengono fornite assieme le credenziali necessarie, formate dall' ID e dalle informazioni di authentication.

1.2.2.1 Authentication Factors

- Somethings you Know
- Something you Have
- Something you Are

Strong Authentication: two factor authentication

1.2.2.2 Biometrics

Verifica l'identità mediante un unico attibuto personale; è il metodo più efficace e accurato.

Type I Error: rifiuto di una persona autorizzata (False Negative)

Type II Error: accesso ad un impostore (False Positive)

Sensitivity: sensibilità dell'apparato da calibrare secondo le esigenze. All'aumentare di tale parametro aumentano i Type I e diminuiscono i Type II e viceversa al diminuire

Cross Error Rate: percentuale di errore, che si ottiene ad un determinato livello di sensitivity, in cui si uguagliano le occorrenze di Type I e Type II

I meccanismi biometrici sono poco utilizzati in quanto:

- most expensive
- little user acceptance
- high enrollment time frame
- low throughput

I sistemi biometrici più noti sono:

Fingerprint: confronto tra le minutie (terminazioni e biforcazioni delle linee sui polpostrelli) lette dall'apparecchio e la immagine conservata. Poichè tale imagine occupa molto spazio, spesso si usa il finger-scan, in cui vengono conservate solo specifiche caratteristiche

Palm-Scan: come il fingerprint ma esteso a tutta la mano

Hand Geometry: controllo delle dimensioni di dita e della mano

Retina Scan: scansione dei blood-vessel pattern presenti sulla retina in fondo all'occhio

Iris Scan: scansione dei patterns, colors, ring, coronas, rift (fessure), furrows (rughe) presenti sull'iride. Occorre installare l'apparato in un luogo isolato dalla luce del sole

Signature Dynamics: controllo dei movimenti effettuati durante una firma

KeyBoard Dynamics: controllo della frequenza e stile di battitura di una frase

Voice Print: controllo dell'impronta vocale

Facial Scan: controllo delle caratteristiche facciali

Hand Topology: controllo degli avvallamenti, montagne,etc presenti sulla mano e sulle dita

1.2.2.3 Password

Password: la forma più comune di identificazione ed autenticazione. Una buona gestione delle password deve prevedere:

- Password Checkers (controlli periodici mediante Brute Force, Dictionary Attack)
- Password Aging (configurazione di appropriate Expiration Date)
- Clipping Level (Limit Unsucessful Logon Attempt)
- Password Hashing
- Password Shadowing (Strict Access Control over Password Repository)

PassPhrase: frase utilizzata come password. Più lunga, di più facile memorizzazione. Da essa deriva la virtual password

Cognitive Password: informazioni oggettive (fact) o soggettive (opinion-based) usate per verificare una identità. Utili per accessi non giornalieri (e.g. cliente di un Customer Care)

1.2.2.4 Devices

One-Time_Password: password valida per un solo accesso. Tipicamente facente uso di generatori dinamici (token o lista di password generati dal server e consegnati "brevi manu" all'utente")

Token Device: dynamic password generator. Possono essere di due tipologie sulla base del tipo di sincronizzazione con il server di autenticazione:

Cryptographic Keys: public key, private key. Digital Signature

Memory Cards: memorizza le credenziali, come BancoMat e ATM. Fa uso di PIN. Possibile un attacco di tipo reverse engineering o tampering

Smart Card: memorizza le credenziali ma contiene anche un meccanismo di sicurezza che provvede a cancellare le informazioni qualora ci sia un tentativo di "Tampering" o un Brute Force sul PIN

1.2.3 Authorization

1.2.3.1 Access Criteria

Nodo cruciale dell' Access Control. I differenti criteri possono essere di uno dei seguenti tipi:

Roles: basato sul job assignment o function

Group: raggruppare le persone che necessitano di accedere a determinati object

Physical or Logical Location: localizzare gli object in una determinata zona (e.g. rete)

Time of Day: consentire l'accesso solo in determinati lassi di tempo

Transaction Type: consentire l'accesso a seconda del tipo di transazione

1.2.3.2 Default to No Access

What is not Explicitly Allowed, it is Implicitly Denied

1.2.3.3 Need to Know (Least Privilege)

Ogni soggetto deve avere accesso esclusivamente alle risorse assolutamente necessarie per eseguire i suoi compiti.

1.2.4 Single Sign On

Sistema tramite il quale è possibile eseguire una singola autenticazione valida per diversi sistemi e piattaforme. Presenta i seguenti vantaggi:

- Reducing the Probability of User Writing Down Password
- Reduce Amount of Authentication Spent Time
- Administrator Ability to StreamLine User Account
- Reduce the Administrator Time Spent in Resetting Password

Lo svantaggio è che un eventuale cracker acquisisce con una sola forzatura tutti i privilegi di un utente

1.2.4.1 Scripting

Il sistema più semplice di SSO. Si crea una strutura di script sui vari sistemi contenenti le credenziali di accesso da un sistema all'altro. E' cura degli amministratori IT gestire, aggiornando opportunamente tali script, le modifiche delle password.

1.2.4.2 Kerberos

Sistema sviluppato al MIT, nell'ambito del progetto Athena, negli anni '80. Si basa sulla crittografia a chiave simmetrica, cui sono demandate Authentication e Confidentiality.

Key Distribution Center:

Principals: user, application o service

Ticket:

Authentication Service:

Ticket Granting Service:

1.2.4.3 SESAME

Secure European System for Application in a Multi-vendor Environment. Sistema che estende il Kerberos allo scopo di eliminarne le debolezze. Funziona con crittografia simetrica ed asimetrica.

Privilege Attribute Certificate: analogo del ticket, da presentare alla risorsa; contiene:

- Identity
- Access Capabilities
- Access TIme Period
- PAC Lifetime

Privileged Attribute Server: analogo del KDC. Genera il PAC al ricevimento di un token da parte dell'utente

1.2.4.4 Thin Clients (Dumb Terminal)

Diskless Computer. Necessitano di autenticazione al server centrale per caricare il Sistema Operativo

1.2.4.5 Directory Services

Contiene le informazioni sulle varie risorse, fornendo lo schema dei nomi. Esempi tipici sono:

- LightWeight Directory Access Protocol
- Novell Netware Directory Service
- Microsoft Active Directory

1.2.5 Accountability

Tracciamento degli eventi e delle attività effettuate, fondamentalmente per mezzo di log, in modo da essere in grado di:

- track bad deeds back to individuals
- detect intrusion
- reconstruct event and system conditions
- provide legal recourse material
- produce problem report

1.2.5.1 Account Event Level

Le informazioni possono essere raccolte a 3 livelli

System Level Event

- System Performance
- Logon Attempts
- Logon ID
- etc

Application Level Event

- Error Messages
- lsof
- File Modification
- Application Security Violation

User Level Event

- Authentication Attempts
- lsof
- Command
- Security Violations

Key Stroke Monitoring: auditing costituito dalla visione e registrazione della sequenza dei tasti premuti dall'utente durante una sessione (di lavoro). Utile per accertare un sospetto comportamento fraudolento. Deve essere notificato ed autorizzato dall'utente.

1.2.5.2 Audit Information Review

Audit Reduction: scrematura delle informazioni non utili alla analisi effettuata da un security professional o un administrator

Variance Detection: determinazione automatica di valori fuori dalla norma

Attack Signature Detection: discernimento automatico di attacchi (contenuti in un DB apposito)

1.2.5.3 Intrusion Detection System

Abbiamo i due tipi:

- Host-based Intrusione Detection System
- Network-based Intrusion Detection System

Time-based Induction Machine: macchina capace di rivelare le anomalie in tempo reale

1.2.5.4 Honeypot

Agnello sacrificale, utilizzato come specchio per le allodole

enticement: allettamento rappresentato da una macchina che presenta palesi vulnerabilità. Le informazioni da essa raccolte possono essere usate in sede legale

entrapment: trappola rappresentata dall'invito a commettere un crimine. Illegale: non può essere usata per incolpare qualcuno di cracking o unauthorized activity

1.2.5.5 Network Sniffer

Non ho capito in che modo lo vuole utilizzare

1.2.5.6 Protecting Audit Data

I dati di Audit possono essere usati in giudizio onde è necessario prestare attenzione alla integrity (e.g. tramite dispositivi Write-Once) ed alla confidentiality (dando accesso ai dati esclusivamente al personale di sicurezza)

Scrubbing: l'atto del cancellare, fraudolentemente, dati specifici incriminatori

1.3 Access Control Model

Framework, basato su Access COntrol Technique e Security Mechanism, che impone le modalità con cui i subject accedono agli object. Ogni Sistema Operativo e Applicazione di supporto adotta uno dei modelli di seguito descritti.

1.3.1 Discretionary Access Control

MOdello impiegato nella maggior parte dei sistemi operativi ad uso civile (Windows, Machintosh, molti Unix). Chi crea la risorsa diviene automaticamente l'owner della stessa. Decide autonomamente quali subject possono accedere ogni risorsa specifica.

Access Decision ⇒User Right vs. ACL

Non prevede un contollo centralizzato.

1.3.2 Mandatory Access Control

Modello impiegato principalmente negli ambienti militari (e.g. SE Linux). Prevede la classificazione preventiva della risorsa. L'owner della risorsa non ha la libertà di decidere quali subject possano accedervi.

Sensitivity Labels: label posseduta da ogni object contiene:

Object Classification: specifica il livello di trust che un subject deve avere per accedere alla risorsa

Subject Categories: impone le regole di need-to-know

Access Decision ⇒Subject's Clearance vs. Nedd-To-Know Level

Non prevede un controllo centralizzato.

1.3.3 Role Base (Nonmandatory) Access Control

Modello che prevede l'utilizzo di un insieme di controlli amministrato centralmente, sulla base del ruolo ricoperto dall'utente. RBAC è il sistema migliore per le organizzazioni nelle quali vi sia un notevole turn-over.
L'assegnazione dei privilegi avviene secondo il concetto della "Separation of Duties":

1. L'owner decide quali permessi assegnare al ruolo e quali utenti assegnare al ruolo
2. L'administrator crea i ruoli e le funzioni sul sistema amministrato
3. Il Security Administrator aggiunge i privilegi necessari agli utenti ed i gruppi

I diritti vengono assegnati in modo implicito.

1.3.3.1 Criteri di Accesso

Role-Based Access: determinato del ruolo che ha il particolare utente nella compagnia

Task-Based Access: determinato dal compito assegnato all'utente

Lattice-Based Access: determinato dal sensitivity level assegnato al ruolo. Variante dell'RBAC in cui ogni utente ha accesso esclusivamente "allo spazio compreso fra due listelli della grata" determinato dal minor limite superiore e maggior limite inferiore ai labeled object

1.4 Access Control Technique

Tecniche tramite le quali vengono posti in opera gli Access Control Model

Rule Based Access Control: regole che impongono in modo ferreo quali risorse si possano accedere o meno (firewall, router). Contrariamente alle ACL, la modifica di tali regole è possibile esclusivamente per l'administrator

Constrained User Interface: controllo d'accesso "cablato" nella interfaccia, eliminando la visibilità delle risorse non necessarie

- menu and shells (restricted shell, windows policies)
- database view
- physically constrained (tastiera del POS)

Access Control Matrix: matrice del tipo

User/Resource	Res 1	Res 2	...	Res n
User 1	r–	rwx	...	rwx
User 2	rws	r–	...	r–
...	...	...	...	...
User m	r–	rw-	...	rw-

Capacibility Tables: riga di una Access Control Matrix

Access Control List: colonna di una Access Control Matrix. Utilizzata nei DAC (⇒l'utente può modificare i permessi)

Content-Dependent Access Control: basato sul contenuto dell'oggetto (e.g. URL Filtering)

1.5 Access Control Administration

1.5.1 Centralized Access Control

Amministrazione gestita da una entità appositamente preposta.

1.5.1.1 RADIUS

Remote Authentication Dial-In User Service, protocollo standard di authentication e authorization per connessioni dial-up (connessioni PPP e SLIP ⇒PAP, CHAP, EAP)

1.5.1.2 TACACS

Terminal Access Controller Access Control System, protocllo proprietario CISCO, di cui esistono tre versioni differenti (non completamente compatibili fra di loro):

TACACS: combina i processi di autenticazione a e autorizzazione

XTACACS: separa authentication, authorization e accounting

TACACS+: estende XTACACS con la "two factor authentication"

1.5.1.3 Diameter

Protocollo che consente di autenticare diversi tipi di device su diversi tipi di connessioni (e.g. IP, X.25, etc). Molto più flessibile di RADIUS e TACACS (ma io non l'ho mai visto!)

1.5.2 Decentralized Access Control

Amministrazione gestita dalle persone che trattano le risorse, che dovrebbero meglio comprendere quali siano gli utenti che necessitano dei permessi di accesso. E' conveniente usare tale tipo di amministrazione qualora:

- i manager abbiano migliore giudizio sulle necessità di accesso
- non ci siano motivi di business che impongano stretti controlli

Presenta le seguenti caratteristiche:

- più veloce
- probabili conflitti di interessi
- non uniforme
- probably overlapping controls

1.5.3 Hybrid

Amministrazione mista

1.6 Access Control Methods

1.6.1 Access Control Functionality

Ogni controllo lavora secondo un diverso livello di granularità ma anche di funzionalità:

Preventive-Control: rileva e evita un evento indesiderato

Detective-Control: identifica un evento indesiderato già avvenuto

Corrective-Control: corregge un evento indesiderato che sta avvenendo

Deterrent-Control: scoraggia l'accedere di un evento

Recovery-Control: ripristina le risorse

Compensating-Control: alternativa o ausilio ad altri controlli

Ovviamente si desidererebbe avere la massima efficienza dai controlli preventivi. Ma questo non sempre avviene, per questo esistono anche gli altri tipi di controllo. In generale si utilizzeranno in modo sinergico i controlli preventive, detective, corrective.
Vi sono dei controlli che includono più funzionalità (e.g. una guardia armata è sia preventive, sia detective, sia deterrent).

1.6.2 Access Control Type

Administrative-Control:

Physical-Control:

Technical-Control:

1.6.2.1 Administrative

Security Documents

Personnel Control

Supervisor Structure

Security Awareness Training

Testing

1.6.2.2 Physical Controls

Network Segregation

Perimeter Security

Computer Controls

Work Area Separation

Data Backups

Cabling

1.6.2.3 Technical Controls

System Access

Network Architecture

Network Access

Encryption and Protocols

Auditing

1.7 Access Control Best Practices

Occorre controllare continuamente che non siano presenti porte aperte non necessarie e che la sicurezza sia allo stesso livello di quando è stata progettata e realizzata.

1.7.1 Task

- Deny Access to System by “guest” or “everyone”
- Limit and Monitor the usage of root
- Suspend or Delay Access for unsucessful attempt (Clipping Level)
- Remove Obsolete User Account
- Suspend Inactive Account
- Strict Access Criteria
- Nedd-to-Know and Least Privilege
- Disable unneeded system service, ports, service, program
- Replace Default Password
- Limit and Monitor Global Access Rules
- No Job Descriptive Logon ID

- Remove Redundent Resource Rules
- Remove Redundant Account, ID, Group, Role-Based Account
- Password Rotation
- Good Password (lenght, content, lifetime, distribution, storage, transmission)
- Audit
- Protect Audit

1.7.1.1 Unauthorized Disclosure of Information

Object Reuse: riassegnare un dispositivo, contente dati, ad un altro subject. Occorre formattare nei casi normali. Qualora i dati contenuti siano classificati occorre cancellare, degauss od eventualmente distruggere il dispositivo

Tempest: studio dei segnali elettrici spuri emessi dagli apparati. Deriva dal nome di un programma, divenuto poi uno standard, sviluppato negli anni 1950 dai governi U.S.A. e U.K. Prevede l'aggiunta di gabbie di Faraday o altro per limitare le emissioni

White Noise: meno costoso dello standard Tempest, prevede l'inseimento nella stanza di generatori di rumore bianco, in modo da confondere un eventuale intruder

Control Zones: costituzione di apposite zone ad accesso limitato, in cui sia presente una sorta di gabbia di Faraday (tramite appositi materiali inseriti nei muri) e generatori di rumore bianco. Ovviamente l'accesso deve essere controllato

1.7.1.2 Penetration Test

Eseguito da personale specializzato, che deve essere dotato di un permesso scritto. Il livello di conoscenza del target, prima di iniziare il test, da parte dei pentester, può essere classificato in:

Zero Knowledge

Partial Knowledge

Full Knowledge

Chapter 2

Telecommunications and Network Security

2.1 Introduction

2.1.1 Telecommunications

Telecommunication: trasmissione elettrica di dati fra sistemi

2.1.1.1 Standard Organization

FCC: Federal Communications Commission

ITU: International Telecommunications Union

ISO: International Standard Organization

2.1.2 Networking

- Instaurare comunicazioni fra computer
- Condividere le Informazioni
- Condividere le Risorse
- Fornire una Amministrazione Centralizzata

2.1.3 Open System Interconnect

2.1.3.1 Application (Layer 7)

Protocollo utilizzato dall'applicazione per provvedere alle richieste di networking. Esempi tipici:

SMTP Simple Mail Transfer Protocol

HTTP Hyper Text Transfer Protocol

2.1.3.2 Presentation (Layer 6)

Traduzione in formato standard (sintassi e formato dei dati), Compressione e Cifratura. Esempi tipici:

ASCII American Standard Code for Information Interchange

EBCDIC Extended Binary-Coded Decimal InterChange mode

TIFF Tagged Image File Format

2.1.3.3 Session (Layer 5)

Stabilisce la connessione fra due applicazioni, effettuando il dialog management:

- Connection Establishment
- Connection Maintain (Data Transfer)
- Connection Release

Esempi tipici:

NFS: Network File System

RPC: Remote Procedure Call

SQL: Structured Query Language

2.1.3.4 Transport (Layer 4)

Stabilisce la connessione fra due sistemi, creando un data stream e garantendo:

- integrity check
- multiplexing
- flow control
- sequencing
- congestion control

Connection-Oriented Protocol: protocollo che assicura che i pacchetti siano arrivati al destinatario (attraverso l'hand shake di quest'ultimo)

Port: meccanismo per identificare quale servizio debba rispondere

Well-Known Ports: porte 1-1024

Ephemeral Ports: porte utilizzate come client

Socket: coppia $(IP - Address, Port)$

Esempi tipici:

TCP Transfer Control Protocol (full-duplex, reliable communication)

UDP User Datagram Protocol (faster, requires fewer resources)

SPX Sequenced Packet eXchange

2.1.3.5 Network (Layer 3)

INstradamento corretto dei pacchetti fra reti diverse. Esempi tipici:

IP Internet Protocol

BGP Border Gateway Protocol

RIP Routing Information Protocol

OPSF Open Shortest Path First

ICMP Internet COntrol Message Protocol

IPX Internet Packet eXchange

2.1.3.6 Data Link (Layer2)

Converte i datagram in frame per la trasmissione, converte i messaggi in sequenze di bit. Esempi tipici:

PPP Point-to-Point Protocol

SLIP Serial Line Internet Protocol

FDDI Fiber Distribuited Data Interface

ATM Asyncronous Transfer Mode

2.1.3.7 Physical (Layer 1)

Converte i bit in segnali elettrici (livelli di potenziale) diversi a seconda del protocollo e del supporto utilizzato (e.g. UTP, Coax). Esempi tipici:

HSSI High-Speed Serial Interface

X.21

2.2 Physical Layer

2.2.1 Trasmission Definitions

Analog Trasmission Signals: il segnale generato è "analogo" al segnale originale da trasmettere

Digital Trasmission Signals: i dati sono convertiti sotto forma di numero binario e quindi in segnali formati da livelli di voltaggio differenti

Asynchronous Communication: i due dispositivi non sono minimamente sincronizzati. Per trasmissioni di piccola entità

Synchronous Communication: esiste una sincronizzazione, tramite clock. Per trasmissioni corpose

BroadBand: multiplazione in frequenza su un supporto trasmissivo (e.g. Coax cAble TeleVision)

BaseBand: mezzo trasmissivo dedicato (e.g. Ethernet)

Unicast Trasmission: one to one

Multicast Transmission: one to many

Broadcast Trasmission: One to All

2.2.2 Network Topology

Ring: connessione a cappio. Ogni sistema connesso è diopendente dagli altri

Bus: connessione ad un cavo singolo

- **linear bus:** un singolo cavo
- **tree:** diramazioni

Star: connessione di ogni nodo ad un dispositivo centrale. Richiede meno cavi delle altre soluzioni (?). Permette di realizzare topologie logiche a Bus e a Ring. Le cablature LAN ormai vengono effettuate esclusivamente così

Mesh: connessione a grafo completo. Grossa ridondanza

2.2.3 Media Access Technology

2.2.3.1 Token Passing

Usato da Token Ring e FDDI. Solo chi possiede il token ha diritto a comunicare. Il token viene fatto girare da un sistema ad un altro

2.2.3.2 Carrier Sense Multiple Access

Usato da [Gigabit, Fast] Ethernet. Ogni sistema prima di trasmettere controlla che non vi sia nessun altro che attualmente stia utilizzando il canale.

Contention: due sistemi devono contendere per l'utilizzo del medesimo canale condiviso

Collision: i frami provenienti da due sistemi sono stati trasmessi (quasi) in simultanea

Collision Domain: insieme dei sistemi che si trovano in contention

Vi sono due tipi distinti di CSMA:

CSMA/CD CSMA with Collision Detection): in cui qualora venga accertata una collisione il sistema smette all'istante di trasmettere ed esegue il back-off algorithm per calcolare il tempo che attenbderà prima di ritrasmettere

CSMA/CA (CSMA with Collision Avoidance): prima di trasmettere ogni sistema lo segnala agli altri

2.2.3.3 Polling

Utilizzato in ambito Mainframe. Vi sono dei sistemi primary station e secondary station. Questi ultimi possono comunicare solo qualora interpellati dalle primary station

2.2.4 Cabling

Bandwidth: larghezza di banda utilizzabile, in MHz

Data Rate: banda passante in Mbps

2.2.4.1 Coaxial Cable

Resistente alle EMI.

50-ohm: digital signaling

75-ohm: analog signaling or high speed transmission

Per la Ethernet esistono i seguenti standard:

10Base2 (ThinNet): facile installazione, fino a 185 metri, 10 Mbps, British Naval Connector

10Base5 (ThickNet): difficile installazione, fino a 500 metri, 10 Mbps, British Naval Connector

2.2.4.2 Twisted Pair Cable

Insieme di copper wire isolati.

UTP Unshielded Twisted Pair

STP Shielded Twisted Pair (IBM)

Per la Ethernet esistono i seguenti standard (UTP):

10Base-T: facile installazione, fino a 100 mt, 10 Mbps, RJ-45

100Base-T4: facile installazione, fino 100 mt, 4 copper wire UTP cat. 3, 4 o 5, RJ-45

100Base-TX: facile installazione, fino 100 mt, 2 copper wire UTP cat. 5, RJ-45

1000Base-Cx: fino 25 mt, UTP cat. 7, RJ-45

1000Base-T: fino a 100, 4 copper wire UTP cat. 5, RJ-45

I cavi UTP sono stati classificati, in base alla destinazione d'uso

Categoty	Data Rate	Usage
1	voice	modem
2	up to 4 Mbps	old token ring
3	10Mbps	10Base-T
4	16Mbps	new token ring
5	100Mbps	100Base-TX, ATM
6	155Mbps	ATM
7	1 Gbps	1000Base-T

2.2.4.3 Fiber-Optic Cable

Presenta le seguenti caratteristiche:

- high transmission speed
- longer distance
- minor attenuation
- no EMI
- no Ratiation
- difficult to tap into

Per la Ethernet esistono i seguenti standard:

10Base-FL: fino a 4 Km

100Base-FX: fino a 2 Km

1000Base-LX: fino a 550 mt. (Multimode), fino a 3 Km (single-mode)

1000Base-SX: multimode

2.2.4.4 Cabling Problems

Noise: causato da EMI e RFI

Attenuation: maggiore a frequenze più elevate

Crosstalk: accoppiamento. quelli che ne risentono di più sono i twisted pair

Radiation: emissione di onde che possono rivelare i segnali trasmessi

2.3 Data Link Layer

2.3.1 Local Area Network

Definita da:

- physical topologies
- data link layer
- protocols
- devices

2.3.2 Metropolitan Area Network

Backbone di dimensioni cittadine, utilizzato per connettere LAN e WAN. Le tecnologie usate sono analoghe a quelle WAN.

2.3.3 Wide Area Network

Backbone Internazionale utilizzato per fornire connettività fra Stati e Continenti.

2.3.3.1 Definitions

PVC (Permanent Virtual Circuit): circuito virtuale stabilito in modo fisso, onde garantire una determinata banda

SVC (Switched Virtual Circuit): circuito virtuale costituito di volta in volta

CIR (Committed Information Rate): banda garantita dedicata, pattuita a livello di contratto

2.3.3.2 WAN Technology

CSU/DSU (Channel Service Unit/Data Service Unit): apparato che connette una LAN ad una WAN

T-Carriers: linee dedicate per il passaggio fonia e dati

- **T1:** 1,544 Mbps (24 linee telefoniche) North America
- **T3:** 45 Mbps (28 linee T1) North America
- **E1:** 2,048 Mbps (32 linee telefoniche) Europe
- **E3:** 34,368 Mbps (16 linee E1) Europe

Frame Relay: packet switching connection-oriented technology. Permette PVC, SVC, CIR

X.25: switching technology, sviluppata negli anni '70. Protocollo non efficiente in quanto contiene numerosi controlli di errore (all'epoca i device erano meno affidabili). Utilizza l'HDLC

SONet (Synchronous Optical Network): Optic Carrier Ring. North America

SDH (Synchronous Digital Hierarchy): analogo del SONet, per l'Europa

ATM (Asynchronous Transfer Mode): cell-switching connetcion-oriented technology. Permette PVC, SVC, QoS

SMDS (Switched Multimegabit Data Service): high speed packet switched technology

SDLC (Synchronous Data Link Control): protocollo seriale utilizzato nello SNA

HDLC (High-level Data Link Technology): evoluzione del SDLC

HSSI (High-Speed Serial Interface): protocollo di livello 1 utilizzato per ATM e Frame Relay

2.3.3.3 MultiService Access Technology

H.323: protocollo per la multimedialità definito dalla ITU-T.

latence:

jittering:

2.3.3.4 Remote Access

Remote Access Server: server che consente l'accesso remoto, gestendo l'instaurazione delle aconnessione oon il modem e l'autenticazione

Call-Back: ulteriore meccanismi di autenticazione, che prevede di richiamare l'utente al numero telefonico fisso da esso indicato. Aggirato tramite call-forwarding

WarDialing: scansione di un insieme di numeri telefonici allo scopo di trovare un modem lasciato collegato ad un computer. Molto pericoloso in quanto, qualora il risultato della ricerca fosse positivo, si ottiene un accesso diretto alla rete interna aggirando il firewall

Integrated Service Digital Network: protocollo di comunicazione digitale su doppino

Basic Rate Interface ISDN: 2 B (data) channels, 1 D (control) channel. 144 Kbps

Primary Rate Interface ISDN: 23 B (data) channels, 1 D (control) channel, 1,544 Mbps (T1)

BroadBand ISDN: via SONet o ATM

Digital Subscriber Line: fino a 52 Mbps, su doppino, modulando oltre la banda telefonico (always connected)

Cable Modem: accesso a Internet su cavo coassiale TV (always connected)

Le seguenti indicazioni passono essere utilizzate come guide linea:

- abilitare una utenza RAS solo se necessario
- il modem dovrebbe rispondere dopo il quarto squillo (per scoraggiare i wardialer impazienti)
- RAS su macchine afferenti ad una stessa LAN e stessa stanza (stessi amministratori)
- two-factor authentication
- caller-ID functionality
- call-back functionality

2.3.4 Ethernet (IEEE 802.3)

Tecnologia sviluppata negli anni '70a partire e commercializzata negli anni '80. Presenta le seguenti caratteristiche:

- CSMA/CD
- Collision Domains
- Broadcast
- 10-1000 Mbps

2.3.5 Token Ring (IEEE 802.5)

Tecnologia sviluppata da IBM. Presenta le seguenti caratteristiche:

- start topology
- Multistation Access Unit
- Token Passing
- 4-16 Mbps
- active monitor
- beaconing

2.3.6 FDDI (IEEE 802.8)

Tecnologia sviluppata dall'ANSI. Presenta le seguenti caratteristiche:

- Token Passing
- Dual Counter-Rotating Ring (fault tolerance)
- 100 Mbps
- fino a 100 Km

Esiste anche la versione Copper Distributed Data Interface che opera su UTP

2.3.7 Wireless

2.3.7.1 Spread Spectrum

Frequency Hopping Spread Spectrum: Frequence Division Multiple Access + Hop (come il GSM)

Direct Sequence Spread Spectrum: utilizzo delle pseudo-noise sequence (come l'UMTS)

2.3.7.2 WLAN Components

Access Point: bridge fra la WLAN e la LAN cablata

Service Set ID: identificativo di una particolare WLAN (canale)

Open System Authentication: autenticazione del dispositivo all'AP effettuata presentando il SSID corretto

Shared Key Authentication: autenticazione del dispositivo all'AP tramite preshared-key

Wired Equivalent Privacy: protocollo (bacato) con il quale viene effettuata la SKA. Fa uso di RC4 (40 o 104 bit) e Initializing Vector.

Integrity Check Value: codice di controllo di integrità (ottenuto senza supporto crittografico e quindi modificabile)

War Driving: identificazione degli AP presenti in una certa area

2.3.7.3 Wireless Application Protocol

Protocol Stack imposto dal mercato.

Wireless Markup Language: analogo dell'HTML e XML

WMLScript: analogo dei JavaScript

Wireless Transport Layer Security: analogo del TLS. Vi sono tre livelli:

> **Anonymous Authentication:** il client ed il server non si autenticano affatto
>
> **Server Authentication:** il server si autentica al wireless
>
> **Two-way Authentication:** autenticazione mutua

gap in the WAP: il mondo IP non capisce il WAP, onde è necessario inserire un WAP Gateway, nel quale le connessioni WTLS vengono spezzate

2.3.7.4 WLAN IEEE Standards

802.11 primo standard IEEE per il wireless. Modulato FHSS, 1-2 Mbps

802.11a modulato OFDM, 54 Mbps, 5 GHz (United States)

802.11b modulato DSSS, 11 Mbps, 2,4 GHz

802.11e aggiunta del QoS

802.11f aggiunta del Roaming

802.11g come l'802.11b ma fino a 54 Mbps

802.11h come 802.11a ma per le frequenze europee

802.11i introduce TKIP, EAP, 802.1x (Settembre 2003)

802.15 Broadband Wireless Access per MAN

802.16 Wireless Personal Area Network. Praticamente il Bluetooth

2.3.7.5 WLAN Best Practices Decalog

1. Enable WEP
2. Change Default SSID
3. Disable SSID broadcast
4. Another Authentication (magari a livello applicativo)
5. AP in the core of building
6. AP in specific DMZ
7. 104 bit RC4 Key
8. VPN on WLAN
9. ACL based on MAC address
10. No DHCP, only static IP

2.3.7.6 New Wireless Standard 802.11i

L'802.11 presenta enormi problemi di sicurezza.

802.11 Issue	802.11i R
weak auth	802.1x
static WEP keys	TKIP e CCMP
repeated IV values	TKIP
weak Integrity	MIC (TKIP)

L'IEEE ha costituito un nuovo Task Group per definire uno standard robusto (l'802.11i appunto) che dovrebbe essere stato emesso a Settembre 2003. Alcuni accorgimenti presenti nel draft sono stati già raccolti ed implementati da taluni vendor prima della uscita ufficiale dello standard.
L'802.11i può essere schematizzato come la interazione di tre componenti (802.1x, TKIP, CCMP) in due layer diversi:

Authentication	802.1x
Cryptography	TKIP or CCMP

802.1x: meccanismo di autenticazione mutua server/user. Fa in modo tale che nessuna operazione possa essere intrapresa prima di aver portato a termine l'autenticazione. Utilizza l'EAP:

Leightweight EAP: solo login e password (CISCO)

Protected EAP: certificato per il server, password per l'utente

EAP-TLS: TLS classico su EAP

Temporal Key Integrity Protocol: meccanismo ideato per la compatibilità con i precedenti protocolli wireless, in modo tale da poter essere inserito nei dispositivi che consentano l'aggiornamento del firmware. La caratteristica più importante è la genreazione di chiavi dinamiche: $NewKey = WEPKey+IV+MAC$. Inoltre si occupa della generazione del Message Integrity Check, basato hash

Counter CBC-MAC Protocol: meccanismo nuovo, incompatibile con i precedenti protocolli. Viene usato l'algoritmo AES in modalità counter con il MAC Cipher Block Chaining

2.4 Network Layer

2.4.1 Protocols

Address Resolution Protocol: conosco l'IP ed esegue un broadcast per sapere l'indirizzo MAC corrispondente

Reverse Address Resolution Protocol: conosco l'indirizzo MAC ed esegue un broadcast per sapere l'IP corrispondente

BOOT Protocol: creato successivamente al RARP fornisce più servizi

Internet Control Message Protocol: riporta messaggi di vario genere risposta, richiesta, errore, routing, test, troubleshoot) relativi al TCP/IP o altri protocolli connectionless

2.4.2 Virtual Private Network

2.4.2.1 Tunneling Protocol

Point-to-Point Protocol: rimpiazza lo SLIP

- funziona su più protocolli (non solo IP)
- peer-to-peer
- non encryption
- header e data compression
- error correction
- IP dinamico

Point-to-Point Tunneling Protocol: protocollo sviluppato da Microsoft

- client server connectivity
- single point to point connection
- data link layer
- solo over IP
- Generic Routing Encapsulation

Layer 2 Forwarding: sviluppato da CISCO

- mutual authentication
- no encryption

Layer 2 Tunneling Protocol: sviluppato da CISCO, su richiesta della IETF.

- fonde PPTP e L2F
- single computer to computer connection
- data link layer
- no encryption (usare con IPSec)

IPSec: componente di IPv6 utilizzabile anche su IPv4

S/WAN: IPSec per le WAN. Prodotto RSA da cui deriva FreeS/WAN che implementa IPSec per Linux 2.4.x

2.4.2.2 PPP Authentication Protocol

Password Authentication Protocol: invia le credenziali in chiaro

Challenge Handshake Authentication Protocol: challenge e response cifrato con la password

Extensible Authentication Protocol: framework di authentication (tipo PAM)

2.5 Transport Layer

2.6 Application Layer

2.6.1 Network Operating System

S.O. costruiti appositamente per fornire il controllo d'accesso alla rete.

2.6.2 Domain Name System

Database distribuito delle associazioni IP-hostname.

2.6.3 Directory Services

Database gerarchico di:

- utenti
- computer
- stampanti
- risorse
- attributi

Si basa generalmente sul X.500.

Schema: struttura del repository che definisce le relazioni tra gli oggetti

2.7 Network Devices

2.7.1 Repeater (layer 1)

- Amplifica e rigenera il segnale
- Connette due segmenti di rete
- Fa passare inalterate le collisioni
- Fa passare inalterati i broadcast

Hub: repeater multiporta per reti Ethernet

2.7.2 Bridge (layer 2)

- Segmenta la rete in più pezzi
- MAC based Filtering
- Connette differenti tecnologie di rete (e.g. Token Ring + Ethernet)
- Isola i Collision Domain
- Fa passare inalterati i Broadcast

Vi sono differenti tipologie di Bridge:

Local Bridge: connette due segmenti di una stessa LAN

Remote Link Bridge: connette segmenti di LAN su una WAN, mediante un telecommunication link

Transparent Bridge: connette segmenti di rete che utilizzano protocolli diversi

2.7.2.1 Forwarding Tables

L'inoltro dei frame avviene mediante l'ausilio delle forwarding tables, le quali vengono costruite secondo uno dei due seguenti metodi:

Transparent Bridging: l'apparato si costruisce autonomamente le forwarding tables analizzando il traffico

Source Routing: il sistema sorgente comunica al bridge il posizionamento del destinatario, che ha appreso precedentemente tramite richiesta esplicita al destinatario, inserendo tali informazioni nei direttamente pacchetti. Pericoloso in quanto permette di modificare le tabelle di routing

2.7.3 Router (layer 3)

- Crea un nuovo Header per ogni frame
- Costruisce le Routing Tables
- Assegna un indirizzo differente ad ogni porta
- Filtra il traffico basandosi sugli IP (ACL)
- Non permette il forwarding del broadcast
- Ferma il traffico contenente un indirizzo che non sa come ruotare

2.7.3.1 Routing Tables

Il routing avviene per mezzo delle Routing Tables, una volta costruite staticamente. Il routing dinamico è stato sviluppato per rendere più agevole la modifica delle tabelle di routing all'occorrere di:

- link down
- congested route
- more economical route
- problematic router

Autonomous System: network individuale, amministrata da una autorità specifica (e.g. la rete di una azienda)

Interior Router: router interno ad una AS. Utilizza Interior Routing Protocol (e.g. OSPF, RIP)

Perimeter (Border) Router: router di contatto fra AS. Utilizza Exterior Routing Protocol (e.g. BGP)

2.7.4 Switch (layer 2+)

Bridge multiporta, consente di eliminare i problemi strutturali del protocollo ethernet

MultiLayered Switch: switch layer 3, layer 4, etc

Virtual LAN: LAN logica. I sistemi che ne fanno parte non comunicano con i sistemi attestati sullo stesso apparato fisico che non ne fanno parte

2.7.5 Gateway (layer 4+)

Software a bordo di un dispositivo che consente di connettere due ambienti (protocolli, reti, etc) che necessitano di una traduzione o adattamento formale.

2.7.6 PBX

Prvivate Branch eXchange

2.7.7 Firewall

I firewall devono realizzare, oltre ai compiti di filtro esposti di seguito:

- AntiSpoofing (AntiMasquerading)
- Fragmented Packet Rebuilding
- Stop Source Routing Packet
- Authentication (opzionale)

2.7.7.1 Firewall Type

First-Generation: Packet Filter

Second-Generation: Proxy Firewall

Application-Level Proxy

Circuit-Level Proxy

Third-Generation: Stateful Inspection

Fourth-Generation: Dynamic Packet Filtering

Fifth-Generation: Kernel Proxy

2.7.7.2 Firewall Architecture

Bastion Host: macchina hardenizzata. Base di installazione di ogni firewall

Dual Homed Host: macchina con più interfacce di rete

Screened Host: macchina collegata direttamente al router periferico, contente software che implementa un firewall

Screened Subnet (DMZ): porzione di rete posta fra due firewall

2.7.7.3 Network Address Translation

Tecnica nata per compensare il limitato numero e l'elevato costo degli indirizzi IPv4, consente di nascondere all'esterno la struttura della rete interna. Tipicamente vengono usate internamente le classi dedicate (non routabili su Internet):

10.0.0.0/8: classi A

172.16.0.0/12: classi B

192.168.0.0/16: classi C

Si usano i seguenti termini:

Intranet: rete interna ad una azienda facente uso di tecnologie Internet

Extranet: rete estesa a più aziende, comunicazioni B2B, facente uso di tecnologie Internet

2.7.7.4 Honeypot

Computer che risiede Screened Subnet. Deve effettuare Enticement. Esegue servizi emulati, in modo da attirare attaccanti ma non consentire di attaccare le altre macchine.

Chapter 3

Information Security Governance & Risk Management

Rappresenta il cuore della struttura di Computer & Information Security.
Il suo compito è creare un Security Program.
Lo scopo del Security Program è la protezione degli Asset societari.

3.1 Security Management Concepts

3.1.1 I 3 Principi Fondamentali della Sicurezza

Detta anche AIC Triad, sono i tre principi fondamentali che ispirano i vari obiettivi di sicurezza contenuti nel programma di sicurezza.

3.1.1.1 Availability

Assicura l'affidabilità e l'efficienza nell'accesso ai dati e alle risorse per gli individui autorizzati.

3.1.1.2 Integrity

Assicura l'accuratezza e l'affidabilità delle informazioni e dei sistemi, prevenendo la modifica non autorizzata dei dati.

3.1.1.3 Confidentiality

Assicura che sia raggiunto il necessario livello di segretezza in ogni fase del processamento dei dati e previene l'information disclosure non autorizzata.

3.1.2 Security Definitions

Vulnerability: vulnerabilità, fragilità hardware, software o procedurale che può provocare accessi indesiderati

Threat: minaccia, pericolo potenziale per le informazioni o i sistemi, con riferimento ad una particolare vulnerabilità

Threat Agent: entità che agisce in modo tale da trasformare la minaccia in pericolo reale

Risk: probabilità che un threat agent esperisca la minaccia

Exposure: istanza di una perdita derivante dall'azione di un therat agent

Safeguard (CounterMeasure): configurazione del software, hardware o procedura che elimina una particolare vulnerabilità o ne mitiga il rischio

Asset: bene della compagnia da difendere

3.1.3 Top-Down Approach

Metodologia usata in un Security Program, nel momento in cui:

Top-Management: initiation, support, direction (Security Policies?)

Middle-Management: work

Staff-Member: work

3.2 Operational Security Model

Framework costituito da entità di generi disparati, che sinergicamente forniscono un adeguato livello di sicurezza all'ambiente. L'obiettivo è la assurance, ovvero la somma di tutti i componenti di sicurezza di un ambiente che forniscono un determinato livello di confidenza.
Ogni compagnia è libera di creare un adeguato Operational Security Model, effettuando le adeguate scelte dei componenti da inserirvi.

3.2.1 Layers

Ogni modello è strutturato in livelli, in cui:

- ogni layer fornisce supporto al livello direttamente sovrastante
- ogni layer fornisce protezione al livello sottostante

3.2.2 Planning Horizon

Inoltre ogni componente può necessitare di un determinato periodo di tempo per essere esercitato. La pianificazione dell'utilizzo dei diversi componenti viene detta Planning Horizon, in cui vi sono tre tipi di obiettivi, a secondo del tipo di "time frame" necessario:

Operational Goals: obiettividi durata giornaliera

Tactical Goals: obiettivi di media durata (mesi)

Strategical Goals: obiettivi di lunga durata (anni, lustri)

3.2.3 Business Requirement (Private vs. Military)

L'Operational Security Model viene influenzato soprattutto da quelle che sono le missioni critiche della compagnia. In generale vi è una grossa differenza tra ambito privato e amito militare. Con riferimento alla AIC Triad:
Military ⇒Confidentiality
Private ⇒Availability, Integrity

3.3 Security Management Responsabilities

Le responsabilità della sicurezza devono essere affibiate al più alto livello di management, dal quale devono essere determinati:

- obiettivi
- scopi
- politiche
- priorità
- standard
- strategie

Responsabilità del Management è quindi provvedere alla protezione delle risorse (umane o sotto forma di capitali, hardware o informazioni) delle quali è responsabili e sulle quali la compagnia fa affidamento.

3.3.1 Security Administration

Gruppo di persone, che lavorano in modo centralizzto e distribuito, in relazione alla struttura della compagnia, responsabile del controllo del Security Program, facendo uso di una chiara Reporting Structure per le comunicazioni.

3.3.2 Supporting Controls

Strumenti tramite i quali vengono raggiunti gli obiettivi del Security Management.

3.3.2.1 Administrative Controls

Tutto quello che ha a che fare con le scartoffie:

- stesura e pubblicazione di:
  - policies
  - standard
  - procedures
  - guidelines
- screening del personale
- training di sicurezza
- procedure di change control (change management?)

3.3.2.2 Technical (Logical) Controls

Tutto quello che ha a che fare con l'adozione di dispositivi che ostano l'accesso a risorse "fisicamnte raggiungibili":

- Access Control Mechanism
- Password and Resource Management
- Identification and Authentication Methods
- Security Devices
- Configuration of the Infrastructure

3.3.2.3 Physical Controls

Controllano l'accesso fisico individuale:

- Facility Protection
- Locking Systems
- Removing Unnecessary Devices
- Perimetral Protection
- Intrusion Detection
- Environmental Control

3.3.3 Security Roles

3.3.3.1 Information Owner

Generalmente un senior executive, che ha la responsabilità della protezione e dell'uso di dati e risorse, additato come responsabile in caso di negligenze nella protezione degli asset della compagnia. Stabilisce:

- classificazione delle informazioni
- permessi di accesso alle risorse
- criteri di protezione dei dati

3.3.3.2 Data Custodian

Ha la responsabilità della manutenzione eprotezione dei dati, in modo da garantirne l'AIC, mediante:

- backup periodici
- security mechanism
- integrity check
- data restoring
- security document implementation

3.3.3.3 User

Colui che utilizza i dati

3.3.3.4 Senior Manager

Responsabile ultimo della sicurezza dell'organizzazione e della protezione degli asset

3.3.3.5 Security Professional

Responsabile Funzionale della sicurezza che conduce il senior manager alla emissone delle direttive

3.3.3.6 Auditor

Esamina i meccanismi e le pratiche di sicurezza della organizzazione

3.3.4 Hiring Practices

Duty Separation: nessuno può completare un task interamente da solo, in modo tale che non possa detenerne il controllo completo

Collusion: almeno due persone devono lavorare insiem per procurare distruzione o frode

Job Rotation: nessuno deve rimanere troppo a lungo nella stessa posizione, in modo tale che non assuma il controllo completo di un processo

Forced Vacation: per i dipendenti di aree sensibili, in modo tale da venir sotituiti da altri che rivelino eventuali frodi

Non Dislosure Agreement: impegno che deve essere sottoscritto da parte di ogni nuovo dipendente per proteggere le informazioni sensibili della compagnia

Account Disabling: i privilegi di accesso devono essere subito disabilitati qualora un utente si congedi dall'azienda, soprattutto se licenziato (disgruntled)

3.4 Risk Management

Processo di identificazione, valutazione e riduzione del rischio ad un livello accettabile, implementando i giusti meccanismi. Si avvale della Risk Analysis. I rischi tipici possono ricadere in una delle categorie seguenti:
Physical Damage
Human Error
Equipment Malfunction
Attacks (Inside, Outside)
Data Misuse
Data Lost
Application Error

3.4.1 Risk Analysis

Metodo di identificazione valutazione dei possibili danni arrecabili, in modo da giustificare l'adozione di adeguate contromisure di sicurezza. I compiti principali sono:

1. Assets Value and Threats Identification
2. Potential Threats Business Impact
3. Risk Calculation
4. Countermeasures Implementation Cost/Benefit Comparison

Indefinitiva offre come risultato un concreto ausilio ai manager per dimensionare il budget necessario a:

- proteggere gli asset riconosciuti
- sviluppare security policies
- fornire una direzione per le security activities

Risk Analysis Team: data la complessità strutturale di molte realtà, deve essere costituito un gruppo che comprenda persone provenienti da ogni dipartimento della compagnia

3.4.2 Quantitative Risk Analysis

L'analisi quantitativa si divide nelle seguenti 5 fasi fondamentali. Per ognuna di esse vengono:

- definiti i concetti chiave utilizzati (nelle formule)
- elencati i singoli item da eseguire

I valori vengono riportati a quantità su base annua in modo da poter essere facilmente confrontati ed integrati con i bilanci aziendali.

3.4.2.1 Asset and Information Evaluation

In questa fase sono utilizzati i seguenti concetti:

AV = Asset Value

Calcolare gli Asset Values. Il valore degli asset deve essere calcolato sulla base dei seguenti fattori:

- Cost to Acquire or Develop the Asset
  - Amount of Work
  - Intellectual Property
  - Replacement Cost
- Cost to Mantain the Asset
- Value of the Asset to Owner and Users
  - Usefulness
  - Operational and Production Activities Dependent on it
- Value of the Asset for the Competitors (or other Third Party)

3.4.2.2 Potential Loss per Risk Estimation

In questa fase sono utilizzati i seguenti:

EF = Exposure Factor (percentuale di perdita che si può verificare su un determinato Asset al realizzarsi di una determinata minaccia)

SLE = Single Loss Expectancy (AV $\star$EF)

Potential Loss: perdita è potenziale in quanto si verifica solo qualora effettivamente u threat agent vada ad effettuare un exploit su una vulnerabilità

Delayed Loss: perdita che si verifica anche a distanza nel tempo

Elencare tutti i possibili rischi Tale ricerca deve essere condotta a partire dagli asset e dalle loro possibili vulnerabilità

Elencare tutte le Potential Loss Per ogni richio devono essere valutate le perdite, espresse dall' EF, da esso potenzialmente derivanti, con particolare riferimento a:

- productivity lost
- information disclosure
- recovering cost

Calcolare tutti gli SLE Per ogni rischio ed ogni Asset calcolare lo SLE relativo

3.4.2.3 Threat Analyis

In questa fase sono utilizzati i seguenti:

ARO = Annual Rate of Occurence (frequenza di occorrimento di una determinata threat in un anno [0,1])

Stabilire l'occorrenza di ogni rischio Raccogliere le informazioni mediante tutti i mezzi disponibili:

- addetti in ogni dipartimento
- statistiche precedenti
- official security resources

Probabilità di occorrenza dei threat Calcolare la probabilità di occorrenza di ogni threat identificato

Calcolare gli ARO Calcolare gli Annualized Rate of Occurence per ogni minaccia

3.4.2.4 Loss Potential per Threat (Risk?)

In questa fase sono utilizzati i seguenti:

ALE = Annual Loss Expectancy (SLE ⋆ARO)

Calcolare gli ALE Calcolare gli Annual Loss Expectancy per ogni Threat utilizzando le quantità ricavate nelle tre fasi precedenti

3.4.2.5 Recommendetion, Safeguard, Countermeasures and Action

In questa fase sono utilizzati i seguenti:

SafeGuard Value = (ALE before Safeguard) - (ALE after Safeguard) - Annual Safeguard Cost

Total Risk = Threat ⋆Vulnerability ⋆AV

Residual Risk = Total Risk ⋆Controls Gap

Countermeasure Cost Selection Scegliere le adeguate contromisure per ogni Threat evidenziato, sulla base di seguenti fattori:

- Product Cost
- Design/Planing Cost
- Implementation Cost
- Environment Modification
- Compatibility with other Countermeasures
- Manteiance Requirement
- Testing Requirement
- Repair, Replace, Update Cost
- Operating/Support Cost
- Effect on Productivity

Countermeasure Functionality and Effectiveness Deve essere valutata la funzionalità e la efficienza, tipicamente tenendo presenti le caratteristiche nella tabella seguente:

Characteristic	Description
Modular	installata senza problemi per gli altri meccanismi
Uniform Protection	proteggere secondo il metodo standard
Override Functionality	aggirabile in caso di necessità
Default to Least Privilege	— per default
Safeguards and Assets Indipendance	
Flexibility and Functionality	configurabilità
Distinction between User and Administrator	
Minimum Human Intervention	meno errori
Easily Upgraded	
Auditing Functionality	
Minimum Dependance over other Component	no dipendenza dall'ambiente
Useable, Accetable and Tolerable by Personnel	
Usable and Understandable Output	
Safeguard Resetting	
Testable	
No other Compromise	no covert channel or backdoor
System and User Performance Safeness	
Proper Alerting	
No Asset Affection	

3.4.3 Qualitative Risk Analysis

Metodologie che non prevedono l'impiego di mezzi matematici per l'assegnazione di un valore monetario al rischio, bensì:

- analisi dei possibili scenari di rischio
- valutazione dellaserietà delle minacce
- confronto della validità di differenti contromisure possibili

Deve essre condotta con estrema capacità di giudizio, intuizione ed esperienza

3.4.3.1 Delphi Technique

Metodo di decisione di gruppo in cui si cerca di far convergere i pareri di un gruppo di persone sui costi, perdite e probabilità di occorrenza evitando il confronto diretto.

3.4.4 Handling Risk

Total Risk = threat ⋆vulnerability ⋆asset value

Residual Risk = Total Risk ⋆Control Gap

3.5 Security Documents

Documenti che contengono le direttive del management inerenti la sicurezza.

Due Care: implementazione diligente delle policies, procedures e standards

Due Diligence: investigazione e comprensione dei rischi reali

3.5.1 Strategical Goals

3.5.1.1 Policies

Documenti prodotti da senior management, che asseriscono quale sia il ruolo che la sicurezza debba giocare all'interno dell'organizzazione.

Policy Address Classification

Organizational Security Policy: stabilisce come debba essere realizzato il Security Program, descrive gli obiettivi, assegna le responsabilità, mostra i valori strategici e tattici dlla sicurezza e sottolinea come l'enforcement debba essere portato avanti.

Issue Specific (Functional Implementing) Policy: tratta uno specifico argomento del quale il management ha sentito il bisogno di dare spiegazioni o prestare particolare attenzione

System Specific Policy: mostra le decisioni del management su un particolare sistema

Policy Type Classification

Regulatory Policy: assicura che l'organizzazione segua gli standard imposti da specifiche industiali e regolati dalla legge

Advisory Policy: suggerisce caldamente determinati tipi di comportamento e attività nella organizzazione. Evidenzia la possibilità di punizione qualora il dipendente non vi si attenga

Information Policy: informa i dipendenti di determinate specificità. Non è enforceable ma mostra quationi specifiche importanti per la società

3.5.2 Tactical Goals

3.5.2.1 Standards

Specificano le modalità di utilizzo degli asset hardware e software nelle condizioni normali. Possono anche indicare il comportamento che gli utenti devono seguire.

3.5.2.2 Baselines

Descrivono il minimo livello di sicurezza necessario all'organizzazione, che si raggiunge qualora si attuino diligentemente gli standard.

3.5.2.3 Guidelines

Insieme di azioni raccomandate e guida alle operazioni. Rivestono un carattere meno obbligatorio rispetto agli standard in quanto lasciano il doveroso margine di discrezionalità necessario alla amministrazione di circostanze impreviste.

3.5.3 Operational Goals

3.5.3.1 Procedures

Documenti operazionali. Descrizione dettagliata dei compiti, passo per passo, da eseguire per ottenere un certo scopo. Spiegano come i documenti precedentemente menzionati devono essere posti in pratica.

3.6 Information Clasification

3.6.1 Classes

3.6.1.1 Commercial Business Classification

1. Confidential
2. Private
3. Sensitive
4. Public

3.6.1.2 Military Classification

1. Top Secret
2. Secret
3. Confidential
4. Sensitive But Unclussified
5. Unclassified

3.6.2 Data CLassification Procedure

La classificazione dei dati deve essere eseguita dal Data Owner. Per implementare una procedura generale occorre seguire i seguenti passi:

1. Identificare il Data Custodian
2. Specificare il criterio seguito nella classificazione
3. Indicare la classificazione cui è responsabile
4. Indicare i controlli di sicurezza che necessita ogni livello di classificazione
5. Documentare ogni deroga
6. Indicare i metodi di trasferimento di custodia
7. Indicare le procedure di termine per la declassificazione dei dati
8. Inserire tale procedura nei Security Awareness

3.7 Security Awareness

I Security Awarenes Training hanno come scopo principale la modificare del comportamento e della attitudine degli impiegati verso la sicurezza. Questi incontri devono essere schedulati priodicamente, almeo una volta l'anno. Porta ad ogni impiegato le informazioni in modo tale che ciascuno possa lavorare secondo gli stessi obiettivi di sicurezza.

3.7.1 Security Awareness Audiences

3.7.1.1 Management

Illustrare i benefici economici, i vantaggi finanziari, etc

3.7.1.2 Mid-Management

Illustrazione di:

- Procedures
- Guidelines
- Policies
- Standards (Baselines?)

3.7.1.3 Technical Department

Illustrare configurazioni tecniche, incident handling, security compromises

3.7.1.4 Staff

Illustrare l'importanza della sicurezza, il ruolo che devono svolgere individualmente

Chapter 4

Software Development Security

4.1 Introduction

4.2 System Development

La sicurezza non deve essere inserita solo all'ultimo momento tramite un interfaccia costrittiva o un prodotto di terze parti, in quanto questo approccio costa di più. La sicurezza deve essere analizzata e integrata durante tutta la fase di sviluppo del software.

4.2.1 Management and Development

Deve essere sviluppato un piano di sicurezza all'inizio dello sviluppo di un progetto:
$SecurityManagement \in ProjectManagement \in ProductDevelopment$
Il Security Plan deve aver un ciclo di vita esso stesso e deve essere soggetto, assieme al Project Management ad audit, in modo da far comprendere il perchè di determinate scelte di sicurezza.

4.2.1.1 Risk Management

Una adeguata gestione del rischio deve essere condotta, intraprendendo ed aggiornando ad ogni step:

- Security Risk Analysis (rischi che il software può far correre)
- Project Risk Analysis (rischi che il software non veda sviluppato)

4.2.1.2 Change Control

Change Control: Processo di amministrazione e approvazione dei cambiaenti in un ambiente

Configuration Management: procedura di gestione del cambiamento

4.2.1.3 Software Escrow

Accordo con una terza società che acquisisce know how e il sorgente del progetto in modo da limitare il rischio provenente dal fallimento del fornitore

4.2.2 Life Cycle Phases

4.2.2.1 Project Initiation

Comprensione delle motivazioni e degli obiettivi del progetto sia in caso di nuovo prodotto sia in caso di applicazione custom.

- Project Definition
- Proposal and Initial Study
- Initial Risk Analysis

4.2.2.2 Functional Design, Analysis and Planning

Delineamento delle funzionalità richieste e documentazione. Vengono identificate le risorse, schedulati i test, sviluppati i criteri di valutazione

- Requirement
- System Environment Specification
- Formal Design
- Risk Analysis Update

4.2.2.3 System Design Specification

I requisiti sono visti sotto gli aspetti:

Informational: tipo di informazioni che devono essere processate e come

Functional: i compiti e le funzioni che il software deve svolgere

Behavioral: stati in cui l'applicazione si trova durante la computazione

Si avranno quindi:

- Functional Design Review
- Functional Broken Down
- Detailed Plan
- Code Design (e.g. Design Pattern, UML)
- Risk Analysis Update

Il Code Design viene effettuato tramite:

Data Design: strutture dati

Architectural Design: definisce le interazioni fra le strutture create

Procedural Design: definisce procedure, funzioni e metodi

4.2.2.4 Software Development

Il codice astratto viene tradotto in codice sorgente e testato:

- Development and Programming
- Testing

I test devono essere condotti da persone che non abbiano direttamente partecipato alla stesura del codice.

Verification: determina se il prototto incontra le specifiche

Validation: determina se affronta in modo adeguato i problemi

4.2.2.5 Implementation/Installation

- Product Installation
- Testing

I test vengono condotti anche dal cliente

Certification: processo di verifica e valutazione del security control e functionality

Accreditation: accettazione formale del sistema (e non del solo software) da parte del management

4.2.2.6 Operational/Maintenance

- Maintenance, Fix
- Minor Modifications
- Risk Analysis Update

4.2.2.7 Disposal

- Rimpiazzamento del vecchio podottto con il nuovo

4.2.3 Software Development Methods

Le fasi descritte nel paragrafo precedente fanno parte, organizzate in vario modo, di molti modelli di sviluppo

4.2.3.1 WaterFall

A cascata, una fase dopo l'altra

4.2.3.2 Spiral Model

Basato sul modello Waterfall, pone l'enfasi su:

- Risk Analysis
- Prototypes
- Simulations

4.2.3.3 Joint Analysis Developer

Team Approach, in un ambiente collaborativo (brainstorming a manella?)

4.2.3.4 Rapid Application Developer

Metodo per velocizzare molto le User Requirement Determination, System Development

4.2.3.5 CleanRoom

Approccio per cercare di eliminare gli errori, mediante l'utilizzo di metodi formali di sviluppo e test. Utilizzato per applicazioni high-quality e critical

4.2.4 Capability Maturity Model

Questo modello fornisce un framework, formato da:

- Policies
- Procedures
- Guide Lines
- Best Practices

per consentire alle compagnie di migliorare in continuazione i processo di sviluppo. Prevede una valutazionedei risultati raggiunti, mediante una scala a 5 valori, elencati di seguito dal più basso al più alto:

Initial: development chaotic

Repeteable: Formal Management Structure, Change Control, Quality Assurance

Defined: Formal Procedure

Managed: Formal Processes

Optimizing: ottimizzazioni dei processi e dei costi

4.3 DataBase Management

4.3.1 Definizioni

Record: insieme di dati relazionati fra loro

File: contenitore di record

Database: insieme di file cross-relazionati

DBMS (DataBase Management System): insieme di programmi e strutture per gestione di DB

Schema: metadati che descrivono la struttura del DB

Data Dictionary: repository centrale degli elmenti del DB e delle loro relazioni. Contiene:

- Schema
- Data Elements Definition (Data Format)
- Reference Keys (Data Source, Data Relationship)
- General Information (Data Usage)

4.3.1.1 DataBase Models

Hierarchical Data Model: le informazioni sono incasellate mediante un modello ad albero. Descrive bene le relazioni uno-molti (nei RDBMS occorre fare una tabella apposita per questo). Meno flessibile del RDBMS, più antico.

Relational Data Model: modello inventato dall'IBM con il DB2. Prevede una organizzazione a tabelle bi-dimensionali. Il più usato

Distribuited Data Model: i dati sono conservati in più di un DB, interconnesi fra di loro in modo da sembrare all'utente un solo repository centrale di informazioni. Ogni DB è amministrato singolarmente, mentre il DB Logico è amministrato centralmente

Object-Oriented DB: progettato per maneggiare dati di tipo ed origine diversa (e.g. film, immagini, suoni, documenti). Vantaggi sono gli stessi della programmazione ad oggetti: ogni oggetto ha le sue proprietà fra cui anche i metodi con cui vi si ha accesso

4.3.1.2 Relational DataBase Definitions

Base Relation: tabella conservata in DB relazionale

Tuple: riga di una tabella

Attribute (Field): colonna di una tabella

Primary Key: colonna che rende unica ogni riga

Foreign Key: attributo di una tabella che in un'altra tabella è Primary Key

View: tabella virtuale definita per mezzo di relazioni fra tabelle. Serve principalmente per creare correlazioni fra tabelle o come strumento di mascheramento delle informazioni

Cell: intersezione di una tupla ed un attribute

4.3.1.3 Relational DB Components

Data Definition Language (DDL): definisce la struttura e lo schema del DB

Data Manipulation Language (DML): contiene le primitive ed i comandi per la manipolazione dei dati

Query Language (QL): interfaccia per l'utente

4.3.2 Security Issues

4.3.2.1 Integrity

Semantic Integrity: integrità dei tipi di dati e delle struttura

Referential Integrity: integrità dei riferimenti con particolare enfasi riguardo le Foreign Keys

Entity Integrity: garantisce la univocità di ogni tupla mediante le chiavi primarie

4.3.2.2 Integrity Operation

RollBack: comando che termina una transazione cancellando tutti i cambiamenti apportati ad un DB

Commit: comando che termina la transazione eseguendo tutte le operazioni richieste

Savepoint: punto in cui viene effettuato un sync su disco in modo da non perdere le immissioni fatte. Ovviamente fa decadere notevolmente le prestazioni. Difficile calibrare il numero giusto in modo da garantire le prestazioni ed assicurare un adeguato salvataggio

CheckPoint: molto simile al save point. Vengono salvati i dati residenti in memoria su file

4.3.2.3 OnLine Transaction Processing

Tecnica utilizzata nei DB organizzati in clusters, in cui occorre effettuare Load Balance e verifica di Consistenza. In ambiente distribuito si utilizza l'ACID test, composto dai seguenti:

Atomicity: la transazioe è divisa in entità atomiche la cui esecuzione non è frazionabile

Consistency: ogni transazione deve avvenire in modo da non violare la Integrity Policy del DB (Semantic, Referential, Entity Integrity)

Isolation: ogni transazione deve essere eseguita senza interazione con altre transazioni

Durability: la transazione, qualora verificata ed eseguita con successo, NON può essere soggetta a RollBack

come si può facilmnt notare tale modello è simile a quanto si compie nello sviluppo dei sistemi operativi uqalora ci si trova in una "Critical Region"

4.3.2.4 Confidentiality

Aggregation: desumere informazioni, cui non si dovrebbe avere accesso, dalla correlazione delle componenti delle stesse

Inference: desumere informazioni, cui non si dovrebbe avere accesso, tramite inferenza logica

4.3.2.5 Confidentiality Tricks

Content-Dependent Access Control: controllo d'accesso eseguito in base al contenuto, ovvero in dipendenza dal contesto

Cell Suppression: mancata visualizzazione delle informazioni contenute in una cella da parte di chi non possiede la clearance necessaria. Permette comunque di conoscere l'eistenza di tali entità

Partitioning: divisione del DB in più parti

Noise and Perturbation: inseriemento di informazioni fasulle, nella speranza di sviare

View: viste logiche

PolyInstantiation: Raffinamento logico del cell suppression; copie multiple di una stessa tupla, contenenti dati discordanti a seconda della classificazione, in modo che solo le persone dotate della clearance sufficiente possono vedere le informazioni giuste

4.4 Application Development Methodology

4.4.1 General Definitions

Machine Language:

Assembly Language:

High-Level Language:

Compiler:

Interpreter:

4.4.1.1 Data Structure

Data Structure: rappresentazione delle relazioni logiche fra elementi di dati

Cohesion: capacità di un modulo software di svolgere autonomamente tutte e sole le funzioni assegnategli. Maggiore è più sono indipendenti i moduli, più sono riusabili, etc meglio è

Coupling: grado di "complicazione" delle interfacce tra moduli. Minore è più semplici e standard sono le interfacce, più riciclabile è il software, bla bla, meglio è

Data Modeling: analisi di corretta computazione di un determinato dato

Structural Analysis Approach: analisi dei dati necessari alla soluzione del problema e loro collegamenti

4.4.2 Object Oriented Concepts

Object Oriented Programming (OOP): programmazione ad oggetti

Object: istanza univoca di una struttura dati definita per mezzo di un template fornito dalla classe corrispondente

Method: funzione o procedura di una classe

Encapsulation:

Information Hiding:

Abstraction:

Messaging: mezzo tramite il quale avvengono le comunicazioni fra oggetti

Object-Oriented Design (OOD): rappresentazione del mondo reale tramite oggetti e sua mappatura nel software

Object-Oriented Analysis (OOA): classificazione degli oggetti appropriati per una determinata soluzione e delle loro interrelazioni possibili

Polymorphism: differenti oggetti rispodono allo stesso comando, input o messaggio in differenti modi

4.4.3 Software Architecture

Riguarda tutte le componenti che compongono una soluzione software. Implica il partizionamento del problema in sotto-problemi che possono essere risolti da componenti software a sè stanti.
Un Software Architect dovrebbe avere la capacità di una visione ad alto livello degli obiettivi dell'applicazione e dei traguardi del progetto

Prototype: prototipo da presentare al cliente

Computer-Aided Software Engineering (CASE): strumenti di sviluppo del software. In ordine di tempo sono stati inventati:

- traduttori, compilatori, assemblatori
- Program Editor, Code Analyzer, Debugger
- GUI visuali

Lower CASE: creazione degli eseguibili

Medium CASE: creazione delle GUI, menu. etc

Upper CASE: creazione della documentazione

Integrate CASE: ausilio durante tutto il Life Cycle

4.4.4 Technology

4.4.4.1 Object Request Broker e CORBA

4.4.4.2 Distribuited Computing Environment

Creato dalla Open SOftware Foudation (OSF),chiamata anche Open Group, fornisce, attraverso uno strato RPC, le funzionalità:

- Time Service (XNTP?)
- Directory Service (LDAP?)
- Security Service (NIS+?)
- Distribuited File Services (Secure NFS?)
- Thread Service

Utilizza lo Universal Unique IDentifier (UUID).

4.4.4.3 COM e DCOM

Component Object Model e Distribuited COM. Tecnologia sviluppata da Microsoft. Analoga al DCE. Fornisce, attraverso lo strato Microsoft RPC, le funzionalità:

- Object Request Broker Service
- Data Connectivity Service
- Distribuited Messaging Service
- Distribuited Transaction Service

Utilizza il Global Unique IDentifier (GUID)

4.4.4.4 ODBC

Open DataBase Connectivity. Middleware di comunicazione tra applicazioni e DB. Costituisce uno standard de-facto, mediante un dialetto dell'SQL.

4.4.4.5 Object Linking ane Embedding

Tecnica di condivisione degli oggetti fra applicazioni locali, per mezzo di COM.

Linking capacità diun programma di chiamare un altro programma

Embedding capacità di integrare un pezzo di un oggetto all'interno di un programma o documento

4.4.4.6 Dynamic Data Exchange

Permette di condividere dati fornendo un InterProcess Communication.

4.4.4.7 Enterprise Java Beans

Piccoli pezzi di programma scambiati tramite Internet Inter-ORB Protocol, in modo da consentire a differenti applicazioni la comunicazione.

4.4.4.8 Expert System and Knowledge Base Systems

Sistemi Esperti. Necessitano di:

- Inference Engine
- Automatic Logical Processing
- General Method of Searching Solution
- Knowledge Base

4.4.4.9 Artficial Neural Network

Sistemi costruiti analogamente ai neuroni celebrali:

- la potenza proviene dalla capacità di imparare dalle esperienze
- deve essere presente una classificazione di importanza dei link tra neuroni (non sono potenzialmente infiniti come nei cervelli)

4.4.4.10 Java

Linguaggio sviluppato da Sun Microsystems. E' possibile scrivere:

- Servlet
- Applet (⇒SandBox per il controllo d'accesso sui computer client)

4.4.4.11 ActiveX

Tecnologia sviluppata da Microsoft. Fa uso dell'Authenticode.

4.4.5 Attacks

4.4.5.1 Malware

Spftware malevolo, scritto con la chiara intenzione di causare danni.

Virus: spezzone di programma che attacca ai puntatori liberi di eseguibili e librerie, infettandoli, generando danni e autoreplicandosi

Worm: programma che, qualora incautamente eseguito, provoca danni e si autoreplica

Trojan Horse: programma che lo stesso nome ed apparenza di uno innocuo, ma qualora eseguito procura danni

Remote Trojan Horse (Maintenance Hook): programma che viene eseguito su un computer offrendo la possibilità di connettersi da remoto

Logic Bomb: programma che eseguirà qualche comando qualora una determinata corcostanza si verifichi, all'insaputa dell'utente

4.4.5.2 Techniques

Sniffing: Ascoltare sulla rete

Spoofing: sostituire l'indirizzo del mittente reale con uno appositamente scelto

Smurfing: utilizzo di un amplifying network con ICMP

Fraggle: utilizzo di una amplifying network con UDP

Blind Spoofing: predizione del "Sequence Number"

IP Attack: acquisizioni delle informazioni sul traffico generato od indirizzato ad un certo host

Hijacking: attacco di tipo "Man in the Middle" a livello TCP

ACK Division: inviare più ACK, con numeri diversi, per lo stesso pacchetto $\Longrightarrow$più pacchetti indietro$\Longrightarrow$più banda

Dup ACK Spoofing: inviare duplicati di ACK per lo stesso pacchetto $\Longrightarrow$ aumento della finestra

Optimistic Acking: inviare ACK su pacchetti ancora non ricevuti $\Longrightarrow$Allargamento della finestra

4.4.5.3 Denial of Service

Flooding letteralmente allagamento di:

1. SYN
2. Ping of Death
3. FingerBomb

Land Attack Invio di pacchetti malformati (riconoscibili tramite Network Analisys). Tipicamente si agisce su:

- indirizzo IP
- numero di porta
- Flags TCP

TearDrop Frammentazione dei pacchetti, con inserimento di indiciazioni false riguardo la ricostruzione (non si possono ricostruire). Appartengono alla stessa categoria:

- Bonk
- Boink
- Nestea

DNS Cache Poisoning inserimento nella cache di un DNS di corrispondenze fasulle

4.4.5.4 Timing Attack

- Between the Lines Entry
- NAK/ACK
- Line Disconnect Attack

Chapter 5

Cryptography

Cryptography: scienza che studia le metodologie per conservare e trasmettere i dati in modo tale che solo chi di dovere possa averne accesso

Cryptoanalysis: scienza che studia il modo con cui rompere i segreti degli algoritmi di cifratura ed i loro componenti

5.1 Introduzione

5.1.1 Breve Storia della Crittografia

5.1.1.1 Antichità

Geroglifici Egiziani Utilizzati per abellire le storie più che per nascondere le informazioni

Atbash Metodo analogo a quello di Giulio Cesare

Skytale Metodo utilizzato dagli spartani dal 400 A.C. Le informazioni venivano scritte su un nastro di pelle di pecora dopo averlo avvoltolato attorno ad un legno. Solo chi possedeva un legno di misura giusta poteva sapere il contenuto del messaggio

Giulio Cesare Crittografia per sostituzione (ad ogni lettera veniva aggiunto D, ed in seguito la chiave fu cambiata in C)

5.1.1.2 World War II

Enigma Sistema usato dai tedeschi, in particolare per colloquiare con gli U-Boat. Costituito da tre rotori, azionati durante la digitazione dei tasti. Prima di cominciare a digitare la macchina andava portata in una ben determinata posizione. Ad ogni tasto digitato si accendeva la lettera da inserire al posto e veniva effettuata una rotazione, di modo che la cifratura cambiasse (effettuando una sorta di CBC). Fu rubata una di queste macchine e fu impiantato vicino Londra un "campus" di studiosi, capeggiato da Alan Turing, che riuscì a craccare il sistema.

5.1.2 Definizioni

Algorithm: insieme di regole matematiche per la definizione dei vari standard di encryption e decryption

Plaintext:

Cyphertext:

Encipher

Decipher

Key:

KeySpace: spazio delle chiavi (di tutti i possibili valori assumibili dalle chiavi) per un determinato algoritmo

Key Clustering: isyanza in cui due distinte chiavi, applicate allo stesso plaintext, generano il medesimo cyphertext

Cryptology: lo studio di crittografia e crittoanalisi

Cryptosystem: implementazione hardware e software delle critpografia

Work Factor (Strenght): stima del tempo, risorse e sforzo necessario alla rottura di un criptosystem

Collision: circostanza in cui due differenti plaintext danno luogo allo stesso ciphertext

Link Encryption: cifratura del collegamento (dal Data Link in sù)

End to End Encryption: cifratura a livello applicativo

5.1.3 Obiettivi della Crittografia

Confidentiality:

Authenticity:

Integrity:

Non-Repudiation:

5.1.4 Ciphers Types

5.1.4.1 Algorithm Based Ciphers

Substitution Cyphers: implementato odiernamente dai Substitution Box

Transposition Cyphers:

5.1.4.2 Spy Ciphers

Running Ciphers:

Concealment Cipher:

5.1.4.3 Steganography

5.1.5 Cryptography e Government

5.1.5.1 Clipper Chip

Key Escrow:

5.1.6 Cryptographic Principles

5.1.6.1 Auguste Kerckhoff

Kerckhoff pubblico nel 1883 un paper in cui apparivano i suoi 6 principi applicati alle comunicazioni sicure con il telegrafo. Nolti di questi principi hanno una validità generale e possono essere applicati, con gli ooportuni aggiornamenti alla crittografia attuale

Secret Key: l'unico segreto del sistema. Troppi segreti rendono il sistema vulnerabile

Public Algorithm: pubblico e ben testato. Generalmente questo principio viene seguito in ambito civile ma non in quello militare

5.1.6.2 Claude Shannon

Shannon pubblicò nel 1936 (?) un paper con la sua teoria dell'informazione"Information Theory".

Information Entropy:

Shannon Theorem: l'unica cifratura matematicamente non violabile è quella in cui la chiave è lunga quanto il messaggio. Da questo deriva il One-Time-Pad (implementato solitamente con pseudo-noise)

Confusion:

Diffusion:

5.1.7 Cryptographic Attack

5.1.7.1 Key Discoverer (Cryptoanalysis) Attack

Lo scopo di questi attacchi è riuscire a trovare la chiave. Adaptive Attacks

CipherText: l'attaccante possiede solo qualche ciphertext

Known-Plaintext: l'attaccante è in possesso di coppie (cipher, plain)

Chosen-Plaintext: l'attaccante possiede molte coppie (cipher, plain) onde può scegliere quelle che meglio soddisfano determinati criteri di frequency analysis sul plain

Chosen-Ciphertext: l'attaccante possiede molte coppie (cipher, plain) onde può scegliere quelle che meglio soddisfano determinati criteri di frequency analysis sul cipher

5.1.7.2 Man-in-the-Middle Attack

Uomo che intercetta le comunicazioni ed impersona uno dei due principal. Per difendersi:

- Digital Signature
- CA

5.1.7.3 Dictionary Attack

Tipicamente usato per decifrare le password, confrontando gli hash "rubati" con gli hash cacolati su ogni parola contenuta in un dizionario. Per difendersi:

- difendere il file delle password (e.g. shadowing)
- usare un meccanismo di hash moderno (e.g. MD5)

5.1.7.4 Replay Attack

Per difendersi:

- timestamp
- sequence number

5.1.7.5 Birthday Attack

Attacco che prende spunto dal famoso paradosso statistico dei complenni:
$Prob(\exists x \in X : birthday(x) = y) = 1/2\text{e } n = |X| \Rightarrow n = 253$
mentre:
$Prob(\exists x, y \in X : birthday(x) = birthday(y)) = 1/2\text{e } m = |X| \Rightarrow m = 23$
dove me $n$sono legati dalla formula di Galoises:
$m = (n * (n - 1))/2$
Onde, dato un algortimo di hashing che genera MD di $n$bit di lunghezza, si ha:
$Prob(MD(A) = X) = 1/2^n$
mentre:
$Prob(MD(B) = MD(C)) = 1/2^{(n/2)}$
Lo spazio delle soluzioni della ricera di due messaggi (B e C) che abbiano lo stesso hash (non ancora calcolato) è dimezzato rispetto a quello della ricerca di un messaggio (A) che abbia un hash predeterminato.

5.1.7.6 Side Channel Attack

Reperimento delle informazioni attraverso canali inconsueti, impensati e quindi non cifrati (e.g. pedinamento, rilevazione delle emissioni elettromagnetiche)

5.2 Encryption Methods

5.2.1 Symmetric

Tali metodi lavorano sull'uso di una sola chiave, conosciuta solo ai due principal e sulla inversione dell'algoritmo tra cifratura e decifratura.

block cipher: i dati sono divisi in tanti blocchi, aventi la stessa lunghezza, che vengono processati uno per uno dall'algoritmo. Usata in ambito civile

stream cipher: i dati vengono trattati come un flusso continuo, effettuando uno XOR con la chiave (ottenuta da un keystream generator). Un buon sistema stream deve contenere le seguenti caratteristiche :

- no repeating patterns
- statistically unpredictable keystream
- linear-correlation (key, keystream) = 0
- statistically unbiased (tanto 0 e tanti 1)

in pratica potrebbe andare bene un generatore pseudo-noise. Usata in ambito militare

5.2.1.1 Data Encryption Standard

Standard del NIST del 1977. Deriva dall'algoritmo Lucifer (128 bit) che IBM sviluppò negli anni '70. Cifratore di Feistel.

- 64 data bit
- 64 (true 56) key bit
- 16 round

5.2.1.2 3DES

- 3DES-EEE3
- 3DES-EDE3
- 3DES-EEE2
- 3DES-EDE2

Il 2DES non si usa in quanto presenta una strenght simile a quella del DES normale

5.2.1.3 Blowfish

Algoritmo sviluppato da Bruce Schneier.

- 64 data bit
- up to 448 key bit
- 16 round

5.2.1.4 Internation Data Encryption Algorithm

Algoritmo brevettato.

- 64 data bit
- 128 key bit
- 8 round

5.2.1.5 RC4, RC5, RC6

Algoritmi ideati da Ron Rivest, analizzati e brevettati dalla RSA Data Security Inc. RC5 presenta:

- 32, 64, 128 data bit
- up to 2048 key bit

5.2.1.6 Advanced Encryption Standard

Nel Gennaio 1997 il NIST ha indetto il bando per scegliere il sostituto del DES. Fu scelto l'algoritmo Rijndael, ideato da Joan Daemon e Vincent Rijmen.

- 128, 192, 256 key bit

5.2.1.7 Mode of Operation

Modi di utilizzo definiti dal NIST per i cifratori a blocchi approvati dal FIPS, per criptare messaggi più lunghi del blocco trattato da ogni algoritmo. Alcuni di essi emulano esplicitamente uno stream cipher mediante l'utilizzo di un keystream generator.

Electronic Code Block: ogni blocco viene cifrato indipendentemente dagli altri. Usato in caso di trasmissione di singoli caratteri.

Cipher Block Chaining: la chiave $K_i$usata per cifrare il blocco B_iè il risultato C_{i-1}della cifratura del blocco B_{i-1}

Cipher FeedBack: la chiave $K_i$usata per cifrare il blocco $B_i$risulta dalla computazione di una funzione $KS(K, C_{i-1})$dove C_{i-1}è il risultato della cifratura del blocco B_{i-1} , K è la chiave originale e KS è un key-stream generator

Output FeedBack: la chiave $K_i$usata per cifrare il blocco $B_i$risulta dalla computazione di una funzione $KS(K, K_{i-1})$dove C_{i-1}è il risultato della cifratura del blocco B_{i-1} , K è la chiave originale e KS è un key-stream generator

CounTeR: ?

5.2.2 Asymmetric (Public Key Cryptography)

Gli algoritmi asimmetrici lavorano su due concetti:

- facilità nel cifrare e difficoltà nel decifrare
- public-key e private-key

5.2.2.1 Rivest Shamir Adleman

Ideato nel 1978 al MIT. Si basa sulla difficoltà di rifattorizzare in numeri primi la potenza calcolata nella fase di cifratura. Defacto standard.

5.2.2.2 Elliptic Curve Cryptosystem

Si basa sulle proprietà delle curve ellittiche. Richiede meno potenza di calcolo e chiavi meno lunghe (adatto per i cellulari e PDA).

5.2.2.3 Diffie-Hellman

Metodo di scambio delle chiavi ideato nel 1976, aprendo la strada alla crittografia asimmetrica. Permette di scambiare le chiavi in modo sicuro.

5.2.2.4 El Gamal

Basato sul calcolo di logaritmi in campi di diemnsione finita

5.2.2.5 Digital Signature Algortihm

5.2.2.6 Knapsack

5.2.3 Hybrid

Utilizzo combinato delle due tecnologie sopra esposte, in modo da garantire:

- scambio sicuro delle chiavi
- buone performance (cifratura simmetrica)
- authentication (asymmetric negoziation)
- digital signature

5.2.4 One-Way-Hash

Questi algoritmi funzionano senza chiave di cifratura, semplicemente creano un fingerprint (hash) del messaggio sulla base di regole predefinite. Lo scopo è quello di combinare tali hash con altri metodi crittografici per garantire la integrità anche in occasione di modificazioni intenzionali

5.2.4.1 Message Authentication Code

$MAC = Hash(Message, SecretKey)$

Server Authentication: autenticazione di ciò che conosce la chiave simmetrica (generalmente il server)

5.2.4.2 Digital Signature

$DS = Crypt_{Priv}(Hash(Message))$

5.2.4.3 Hash Algorithm

MD2: progettato da Ron Rivet. Slow, 128 bit

MD4: progettato da Ron Rivest. Weak, 128 bit

MD5: miglioramento di MD4, 128 bit

SHA: progettato da NIST e NSA per essere usato nel DSS. 160 bit

Haval: modifica dell'MD5. Hash a lunghezza variabile

5.2.4.4 Digital Signature Standard

Standard proposto dal NIST per la Digital Signature nel 1991:

- RSA, DSA o ECC
- SHA

5.3 Public Key Infrastructure

5.3.1 Objectives

- Confidentiality
- Access Control
- Integrity
- Authentication
- Non-Repudiation

5.3.2 Components

5.3.2.1 Certificate Authority

5.3.2.2 Registration Authority

5.3.2.3 Certificate Repository

5.3.2.4 Certificate Revocation List

5.3.2.5 Key backup e Recovery

5.3.2.6 Key History Management

5.3.2.7 Timestamping

5.3.2.8 Client-side Software

5.3.3 Key Management

- Good Key Lenght
- Secure Key Transmission
- Extremely Randomness
- More Sensitivity, Shorter Lifetime
- More Usage, Shorter Lifetime
- Key Backup and Escrow
- End-of-Life Key Destruction

5.4 Internet Security

5.4.1 E-Mail

5.4.1.1 Multipurpose Internet Mail Extension

5.4.1.2 Secure/MIME

5.4.1.3 Pretty Good Privacy

Cryptosystem proposto nel 1991 da Phil Zimmerman, divenuto un programma usatissimo.
Utilizza Passphrase per proteggere la chiave privata dell'utente

Web of Trust: chiavi scambiate "per conoscenza" anzichè in base ad una autorità centrale

Key Ring: contenitore delle chiavi

5.4.2 HTTP

Stateless protocol.

5.4.2.1 S-HTTP

- protegge il messaggio
- non ha bisogno di certificati
- funziona su crittografia simmetrica

5.4.2.2 HTTPS

Si basa sul Secure Socket Layer (ora Transport Layer Security)

- protegge la connessione
- lavora a livello trasporto (per il CISSP)
- funziona su crittografia ibrida (asimmetrica + simmetrica)

5.4.2.3 Secure Electronic Transaction

Tecnologia proposta da Visa e MasterCard per proteggere le transazioni con Credit Card su Internet.
Non è molto efficiente in quanto necessita di molte operazioni, molto software e molte parti da coordinare:

- issuer (cardholder's bank
- cardholder
- merchant
- merchant's bank
- payment gateway

5.4.2.4 Cookie

Messaggi di testo inviati tramite browser e tenuti su disco. Permettono di tener conto dello stato di una sessione.

5.4.3 IPSec

Aggiunta all'IP per la creazione di VPN. Lavora a livello Network.

Authentication Header:

Encryption Security Payload:

transport mode: solo ESP

tunnel mode: AH + ESP

Security Association:

Security Parameter Index: insieme delle SA

5.4.3.1 Internet Key Exchange

Protocollo "de facto" standard per lo scambio delle chiavi e delle configurazioni di sessione. Si compone dei due seguenti:

Internet Security Association and Key Management Protocol: protocollo che stabilisce il framework per lo stabilimento della sessione IPSec

OAKLEY: protocollo per la negoziazione dei parametri su ISAKMP

Chapter 6

Security Architecture & Design

6.1 Introduzione

Nei moduli SMA e AC abbiamo visto

Security Policy: insieme di regole e spiegazioni sui metodi di accesso ai dati, livelli di sicurezza richiesti e azioni conseguentemente necessarie

In questo modulo vedremo i seguenti due concetti:

Security Model: attestazione dei requisiti necessari per supportare e realizzare la Security Policy

Architecture: struttura dei sistemi di computazione che adempie al Security Model

E' importante che la sicurezza sia presa in considerazione durante la fase di progetto e non successivamente, in quanto necessita le fasi di:

- engineering
- implementing
- testing
- auditing
- evaluation (secondo i criteri di Availability, Integrity e Confidentiality)
- certification
- accreditation

Poichè i prodotti, in genere, si comprano già fatti, le fasi necessarie sono solo le ultime 3:

evaluating: attraverso uno dei metodi standard (TCSEC, ITSEC, CC)

certification: verifica tecnica dei meccanismi e controlli di sicurezza e della loro efficacia

accredition: accetazione ufficiale da parte del management delle informazioni fornite dalla certification

6.1.1 BS 7799

British Standard 7799 è un metodo basato sul rischio per l'assessment, l'evaluation ed il management del rischio, mediante un approccio olistico.
E' diviso in 10 sezioni:

- Security Policies
- Security Organization

- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Computer and Network Management
- System Access Control
- System Development and Manteinance
- Business Continuity Planning
- Compliance

Divenuto ISO 17799 (Code of Practice for Infromation Security Management)

6.1.2 Trust e Assurance

Trust: fiducia nel sistema e nel livello di sicurezza fornito

Assurance: confidenza che il sistema agisca sempre in modo corretto e predicibile in ogni situazione (in pratica trust++)

6.2 Computer Architecture

6.2.1 von Neumann

6.2.1.1 Central Processing Unit

ALU: Arithmetic Logic Unit

CU: Control Unit

Reg: Register

CPU Mode: modalità di funzionamento della CPU, sulla base dei permessi accordati al processo in esecuzione. Nei sistemi moderni si distinguono almeno:

- supervisor mode (privileged)
- user mode (unprivileged)

Protection Ring: confini di accesso dei CPU Mode. Ogni ring accede a tutti i ring con numero superiore ma non viceversa

Ring 0: Operating System Kernel

Ring 1: Operating System (init, etc)

Ring 2: I/O Driver and Utilities

Ring 3: Application

6.2.1.2 Memory

Rappresenta l'insieme dei dispositivi di Primary Storage

RAM: Random Access Memory

Static RAM (flip flop)

Dynamic RAM (richiede refresh)

EPROM: Erasable and Programable Read Only Memory

Cache:

Memory Mapping: accesso alla memoria mediante virtual (linear) address

Paging: swapping

Virtual Storage: RAM + Secondary Storage

ROM: Read Only Memory

6.2.1.3 I/O Devices

Secondary Storage: supporti non volatili (floppy, disk, CD-ROM)

deadlock: incastramento di due processi derivante da una gestione errata del rilascio di una risorsa

6.2.2 Processes

Address Space: insieme di pagine di memoria dedicate ad un processo

Process: programa in esecuzione che lavora nel suo address space e comunica con gli altri processi in modo controllato (IPC)

Thread: pezzo di codice che viene eseguito all'interno di un processo

Virtual Machine: astrazione ottenuta mediante il S.O. che fa credere al Processo che sia solo ad essere in esecuzione

Operating State: stato della computazione in cui si trova un processo:

Stopped not running

Waiting in attesa di un evento

Running caricato nella CPU

Ready pronto per essere caricato

system call: richiesta, da parte di un processo, di effettuare un determinato task

multithreading: sistema che può evadere più di una richiesta alla volta

multitasking: sistema che può ospitare più di un processo alla volta

multiprocessing: sistema dotato di più di un processore

multiprogramming: sistema che può ospitare più di un processo alla volta, dando al processo il controllo sulle risorse (e.g. Windows 95). Non si usa sui sitemi nuovi

6.2.2.1 Threats

Buffer Overflow: accade qualora un programma non controlli la lunghezza di un dato inserito in un buffer. Può causare l'esecuzione di codice arbitrario (⇒no_exec_flag)

Asynchronous Attack: dipende dai passi necessari ad un programma per eseguire un task. ad esempio:

TOC/TOU: Time of Check/Time of Use

race condition: due processi che devono accedere alla stessa risorsa

Backdoor (Management Hook): punti di entrata inseriti appositamente dal programmatore all'insaputa di committente e utilizzatori

Covert Channel: utilizzo di un canale in modo non convenzionale, in modo da aggirare i controlli di accesso. Esistono due modi principali:

Covert Timing Channel: metacomunicazione mediante l'utilizzo di dispositivi secondo certe tempistiche

Covert Storage Channel: comunicazione su canale non ideato per quello scopo (e.g. Loki su ICMP)

6.3 System Architecture

I meccanismi di sicurezza possono essere posizionati nei livelli:

- Hardware
- Kernel
- Operating System
- Services (Libraries?)
- Application

Nei livelli più alti si ha maggiore funzionalità, maggiore complessità, maggiore granularità

6.3.1 Trusted Computing Base

L'espressione TCB è stata introdotta con l'Orange Book e indica il livello di fiducia formito da un sistema di computazione.

TCB: combinazione della totalità dei meccanismi di protezione (hardware, software, firmware) presenti in un sistema di computazione

Non tutte le parti di un sistema devono ottenere il trust.

Trusted System: dispositivo HW o SW che fa uso di adeguate misure per proteggere l'integrità dei dati (classificati o meno) per un insieme di utenti, senza violare i diritti e le Security Policies

Security Perimeter: confine tra le risorse che devono essere presenti nel TCB e quelle che sono esterne. Le comunicazioni fra elementi interni ed esterni deve avvenire secondo modalità prestabilite

Reference Monitor (Concept): macchina astratta che controlla l'accesso dei subject e gli object secondo i permessi. E' un concetto, non un dispositivo

Security Kernel: dispositivo (HW, SW o FW) che realizza ed impone i dettami del Reference Monitor. Rappresenta il meccanismo di protezione più importante del TCB:

- tamperproof
- impossible to circumvent
- verifiable
- small (per essere adeguatamente verificato)

Domain: insieme di object cui un subject può avere accesso. I domini devono essere individuati, separati e imposti. Strettamente collegato con i ring

6.3.2 Best Practices

Resource Isolation: separazione delle risorse, ottenuta al livello minore possibile (e.g. hardware segmentation)

Multilevel Security Policy: security policy che previene il flusso di informazioni da un livello ad un altro

Least Privilege: ogni processo deve accedere solamente alle risorse strettamente necessarie

Layering: separazione di processi e risorse e aggiunta di modularità al sistema

Data (Information) Hiding: un layer non deve accedere ai dati cui accede un altro layer

Astraction: assegnazione di permessi a classi di oggetti

6.4 Security Models

I security model sono delle descrizioni, generalmente molto formali, mediante l'ausilio della matematica, delle regole che occorre seguire per implementare le security policies. Fanno uso dei seguenti concetti:

State Machine Model: modello a stati finiti, descritti dall'insieme dei permessi e delle istanza di accesso dei subject verso gli object in un dato momento

Basic Security Theorem: un sistema che si trovi in uno stato sicuro e su cui sia possibile eseguire unicamente secure transaction raggiungerà sempre stati sicuri a prescindere dai dati forniti in input

6.4.1 Information Flow Model

6.4.1.1 Information Flow Model

In questo tipo di modelli l'attenzione viene rivolta principalmente all'imposizione del flusso delle informazioni in modo tale che non vengano meno le condizioni della Security Policy

6.4.1.2 Bell-LaPadula Model

Modello che protegge la confidentiality. Sviluppato negli anni 1970 per l'U.S. Military

Simple Rule: no read up

*** Property Rule:** no write down

Strong Star Property Rule: read/write at the same security level

6.4.1.3 Biba Model

Modello che protegge la integrity. Sviluppato successivamente al Bell-LaPadula.

Simple Integrity Axiom: no read down (per non utilizzare informazioni meno integre)

*** Integrity Axiom:** no write up (per non inserire informazioni meno integre)

6.4.2 Practical Model

6.4.2.1 Graham-Denning Model

Modello che crea i diritti per l'utente in dipendenza dalle operazioni che possono essere eseguite sull'object

6.4.2.2 Harrison-Russo-Ullman Model

Modello che descrive il modo con cui devono essere modificati i permessi e creati e rimossi i subject e gli object

6.4.3 Misc Model

Altri modelli presentati per i quali è difficile una classificazione

6.4.3.1 Clark-Wilson Model

Modello che protegge l'Integrity dei dati e che assicura che le transazioni abbiano il giusto formato

Access Triple: subject ↔application ↔object

Duty Separation: dividere le operazioni in differenti parti

Audit: tener traccia delle infrmazioni intransito da e verso il sistema

6.4.3.2 Noninterference Model

Modello secondo il quale le attività effettuate ad un livello non devono influenzare livelli differenti

6.4.3.3 Brewer and Nash Model

Modello secondo il quale i controlli di accesso devono cambiare dinamicamente, in modo da evitare conflict of interests

6.5 Security Modes of Operation

Dedicated Security Mode: ogni utente possiede la clearance ed il need-to-know

System-High Security Mode: ogni soggetto possiede la clearance, ma non è detto che possieda il need-to-know

Compartmented Security Mode: ogni soggetto possiede la clearance ma può non avere il need-to-know, nè l'access approval

Multilevel Security Mode: permette che siano processati più livelli di classificazione in contemporanea

6.6 System Evaluation Methods

6.6.1 Orange Book

Trusted Computer Security Evaluation Criteria sono stati sviluppati dal DoD nel 1985 e sono rimasti in uso fino a dicembre del 2000, sostituiti dai CC. Danno molto enfasi ai requirement di tipo militare (⇒Confidentiality) e poca alle caratteristiche richieste in ambito commerciale.
Il processo di valutazione utilizza i seguenti:

NCSC: National Computer Security Center

TPEP: Trusted Product Evaluation Program (processo di valutazione)

EPL: Evaluation Production List (lista di tutti i prodotti valutati e del livello raggiunto)

I criteri di valutazione prevedono i seguenti argomenti:

- Security Policy
- Identification

- Labels
- Documentations
- Accountability
- Life Cycle Assurance
- Continous Protection

6.6.1.1 D: Minimal Protection

Non soddisfa i requisiti

6.6.1.2 C: Discretionary Protection

Discretionaty Access Control

C1: Discretionaty Security Protection

C2: Controlled Access Protection

6.6.1.3 B: Mandatory Protection

Mandatory Access Control, basato sul Bell-LaPadula.

B1: Labeled Security

B2: Structured Protection

B3: Security Domains

6.6.1.4 A: Verified Protection

Analogo a B3, ma i controlli eseguiti sono più formali (dovrebbe esserci più assurance)

6.6.1.5 Rainbow Series

Poichè l'Orange Book comprendeva la valutazione esclusivamente dei computer, il DoD decise di emettere altri documenti per coprire gli altri argomenti di sicurezza. Ognuno di essi aveva una copertina di un colore diverso (da qui l'arcobaleno)

Red Book: libro riguardante la Trusted Network Interpretation

6.6.2 ITSEC

Information Technology Security Evaluation Criteria è stato il primo tentativo di stabilire un unico standard per la valutazione degli attributi di sicurezza di un sistema di elaborazione da parte di alcuni stati europei.
Valuta 2 attributi fondamentali:

Functionality: (F1 - F10)

Assurance: (E0 - E6)

Meno restrittivo rispetto al TCSEC.

6.6.3 Common Criteria

Progetto avviato nel 1993 da parte della ISO, cui hanno preso parte U.S.A., U.K., Francia, Germania, Olanda, Canada, per l'allineamento e la fusione degli standard TCSEC, ITSEC, CTCPEC a Federal Criteria.
Il processo di valutazione utilizza i seguenti concetti:

Protection Profile: descrizione delle necessità di sicurezza, scritte da chiunque riscontri una particolare esigenza non ancora coperta. Deve contenere le seguenti informazioni:

Description Elements: nome e descrizione sommaria

Rationale: giustificazione del profile e spiegazione dettagliata del problema

Functional Requirements: stabilisce il confine di protezione

Development Assurance Requirements: specifiche richieste relative la fase di design e realizzazione

Evaluation Assurance Requirements: tipo e intensità di valutazione

ToE: Target of Evaluation. Prodotto proposto per il test

Security Target: documento del fornitore che illustra le funzionalità e le assurance

EAL: Evaluation Assurance Level. Votazione finale raggiunta tramite la valutazione di:

- Security Functionality Requirements
- Security Assurance Requirements

Chapter 7

Operational Security

Molti dei concetti afferenti a tale dominio sono stati presentati nelle descrizione degli altri domini. Si farà un rapido riassunto.

7.1 Operational Security Concepts

Due Care:

Due Diligence:

Prudent Person: persona respnsabile, accorta, pratica. Concetti cui si rifanno Due Care e Due Diligence

7.1.1 Administrative Management

Separation of Duties:

Job Rotation:

Need to Know: esigenza di accesso alle risorse che srvono per compiere il proprio compito

Least Privilege: permessi che implementano il need to know

Mandatory Vacation:

7.1.2 Accountability

I log vanno generati, ma poi qualcuno se li deve leggere!

7.1.3 Product Evaluation

7.1.3.1 Operational Assurance

Si concentra sugli aspetti:

- architettura
- features
- functionalities

Ad esempio:

Control Mechanism

Separation of Privilege

User Program Code

7.1.3.2 Life Cycle Assurance

Modo in cui il software viene sviluppato e mantenuto. Esempi di standard:

Design Configuration

Clipping Level: threshold in base alle quali scatta un HIDS

Testing:

Configuration Management

Change Management Control: management delle features di sicurezza e del livello di assurance fornito mediante controlli sui cambiamenti effettuati su system, hardware e firmware. La policy generalmente si compone delle seguenti fasi:

Request for Change: rivolta ad un gruppo apposito

Approval Of the Change: ovviamente deve essere giustificata

Documentation: ovviamente se ne deve tenere traccia

Tested and Presented: sviluppata e testata a siffucienza

Implemented: schedulazione delle fasi di progetto

Report to Management: alfine presentata a chi comanda

Trusted Distribution: magari con Authenticode?

Media Control: amministrazione dei mezzi di immagazzinamento dei dati.

Access Control:

Librarian Control: controllo delle cassettine. Ci deve essere scritto su:

- Data di Creazione
- Persone che ha creato il Backup
- Periodo di Retention (Scadenza di Validità)
- Classification
- Volume Name e Version

Sanitization: procedura mediante la quale vengono eliminate le informazioni dai supporti:

OverWriting: dati "normali"
Degaussing: dati sensibili
Destruction: dati ad elevata sensibilità o condifentialità

System Control:

Trusted Recovery: O.S. crash e Freeze

System Reboot: riavvio attended

Emergency System Restart: riavvio unattended, con soegnimento pulito

System Cold Start: riavvio attended, in seguito a spegnimento improvviso (crash e freeze)

7.1.4 Input/Output Control

Controllo dei dati immessi e dei risultati della computazione.

7.2 Internet Security

7.2.1 E-Mail

7.2.1.1 Simple Mail Transfer Protocol

7.2.1.2 Post Office Protocol 3

7.2.1.3 Internet Message Access Protocol

7.2.1.4 SMTP Relaying

7.2.2 Fax

Fax Server:

Fax Encryptor: lavora a livello Data Link

7.3 Hack and Attack

7.3.1 Network Map and Fingerprint

7.3.2 Techiques

SuperZapping: programma per entrare nei MainFrame IBM eludendo i controlli

Browsing: termine che indica il generico accesso ad informazioni cui non si hanno i permessi

Sniffers: programmi che mettono le schede in promiscous mode

Session Hijacking: man in the middle a livello network

Password Cracking: brute force e dictionary

BackDoor: Maintenance Hook o ingresso illegale, con lo scopo di ottenre un accesso amministrativo:

- Back Orifice
- Root Kit
- NetBus
- SubSeven

7.3.3 Attacks

Denial of Service

Man-in-the-Middle

Spamming

Wardialing

Ping of Death

WinNuk: invio di pacchetti alla porta 139 per Win NT e Win 9x

Fake Login Screen: programma installato sulle macchine client, magari mediante troiano

Teardrop

Traffic Analysis: analisi, magari statistica, dei mittenti e destinatari delle comunicazioni

Slamming: cambio di gestore telefonico alla insaputa dell'utente

Cramming: aggiunta di un servizio che l'utente non voleva

7.3.3.1 Penetration Test

Deve essere eseguito periodicamente.

7.3.4 Operation Department

Team di persone che cura l'operational security.

7.3.4.1 Unusual and Unexplained Occurrences

7.3.4.2 Deviation from Standard

7.3.4.3 Unscheduled Initial Program Load

Chapter 8

Business Continuity & Disaster Recovery Planning

8.1 Introduction

8.1.1 Business World Characteristics

- Guidare la produzione di un gran prodotto o servizio. Portare tale prodotto sul mercato
- Intuizione ed Esperienza per prevedere i problemi inaspettati che possono facilmente presentarsi

Il Business Continuity tratta evidentemente il secondo punto.

8.1.1.1 AIC Triad

L'Availability è la proprietà cercata per eccellenza da questa materia. Integrity e Confidentiality devono essere prese in considerazione specialmente nel Disaster Recovery, poichè in caso di emergenza l'azienda è più vulnerabile in genere.

8.1.2 Definitions

Business Continuity: materia che fornisce i metodi e le procedure per il trattamento di sciagure prolungate

Business Continuity Plan: processo di

Disaster Recovery: materia che tratta la minimizzzione degli effetti di un disastro. Descrive i passi necessari alla riabilitazione del corretto funzionamento di risorse, personale e dei processi di business

Disaster Recovery Plan: piano di preparazione al disastro prima che esso si verifichi, con la pseranza di minimizzare le perdite ed assicurare i servizi critici. Si compone di:

- Emergency Response
- Recovery
- Resumption

8.1.2.1 Threats Types

Classificazione delle minacce, in base alla causa scatenante, usata nella Business Impact Analysis:

ManMade: generate da un essere umano in modo doloso o per incuria o errore

Natural: disastro naturale (e.g. heartquake, tiphon)

Technical: rottura di un dispositivo (e.g. disco, power failure, data corruption)

8.1.2.2 Disruption Types

Classificazione delle rotture possibili, in base alla tipologia e alla durata del danno arrecato, usata nella scelta del BackUp:

Non-Disaster: malfunzionamento di un servizio derivante dalla rottura di un dispositivo

Disaster: inagibilità di un intera costruzione (e.g. allagamento). Si risolve mediante l'utilizzo di un sito alternativo

Catastrophe: rottura totale di una costruzione (e.g. heartquake). Può prevedere l'intera ricostruzione dell'edificio

8.1.2.3 Business Continuity Plan Goals

Responsibility: ogni individuo coinvolto nel recovery deve avere la sua responsabilità, scritta

Authority: deve essere ben chiaro chi ha il comando di quali operazioni

Priorities: deve essere ben chiaro cosa è critico da cosa è comodo (nice to have)

Implementing and Testing: deve essere scritto, eseguito e custodito

8.2 Business Continuity Plan

Deve far parte del Security PlanSi compone dei seguenti steps.

8.2.1 Basilar Steps

Un business continuity plan si compone dei seguenti steps.

8.2.1.1 Project Initiation

Getting Management Support:

Developing Plan Scope:

Securing Funding:

8.2.1.2 Business Impact Analysis

Una delle fasi più importanti. Qualitative and Quantitative Data:

- Gathering
- Analyzing
- Interpreting
- Presentig (to Management)

Occorre:

1. Identificare le Business Critical Functions
2. Identificare le Resources che Supportano le Business Critical Functions
3. Stimare i potenziali Disastri

8.2.1.3 Recovery Strategy Development

E' indispensabile l'Executive Commitment e Support ⇒Business Case Presentation

8.2.1.4 Recovery Plan Development

Si cura di analizzare ogni singola sciagura possibile e provvede le soluzioni per:

- End-User Environment
- BackUp Alternatives
- Recovery
- Restoration

Ovviamente ogni possibile disastro necessita di strumenti diversi (con efficacia ed efficienza diversi).

8.2.1.5 Implementation

Si cura di rendere fruibile il piano:

- stesura dei documenti necessari
- distribuzione delle copie dei documenti su più siti

8.2.1.6 Testing (Maintenance)

Il Business Continuity Plan deve essere revisionato:

- almeno una volta l'anno
- ad ogni cambiamento rilevante della organizzazione e dell'ambiente

La revisione del BCP può essere comodamente integrata nelle procedure di "Change Management", in modo tale che ogni cambiamento dell'ambiente venga riflesso automaticamente sul piano.
Vi sono vari tipi di test, ognuno avendo vantaggi e svantaggi e rivolgendosi a differenti componenti da testare. Qualora venga effettuato un test devono essere avvisati i manager di competenza.

Test Scartoffiari

CheckList Test: presentazione dei BCP al responsabile di ogni area per verificare se sia stato omesso qualcosa o qualche approccio debba essere modificato

Walk-Through Test: rappresentanti di ogni area si riuniscono insieme per garantirne l'accuratezza

Test Operativi

Simulation Test: simulazione vera e propria del disastro, magari dividendo per aree

Parallel Test: verifica della validità dell'Off-Site, spostando effettivamente i sistemi sul sito di backup e procedendo alla elaborazione dei dati. Le performance del processamento dati vengono confrontate

Full-Interruption Test: il test più completo ed intrusivo. Si spegne il sito primario e si sposta tutto sul secondario

Other Test: antincendio, primo soccorso, procedure di comunicazione d'emergenza

8.3 Provided Procedures

8.3.1 Extended Backup

8.3.1.1 OffSite Hardware BackUp

Generalmente le compagnie pagano società di servizi che forniscono OffSite Facility Sites. I costi di solito si dividono in:

- basic subscription cost
- activation cost
- timely based (hours/days) charge

In generale le facility di backup devono essere almeno a 25 miglia (40 Km) di distanza, in modo da evitare la distruzione di entrambi i siti in caso di grave calamità naturale.

SubScription Services

Hot Site: backup completo, cui mancano solo le persone ed i dati. Per essere operativo necessita di poco tempo (ore). Il più costoso. Annual Test

Warm Site: backup intermedio. Mancano le persone, i dati e le apparecchiature più costose (e.g. unusual hardware).

Cold Site: praticamente solo le mura. No dispositiv di trattamento dati

Not Owned Services

Reciprocal Agreement: accordo bilaterale fra due società che si impegano reciprocamente ad ospitare l'altra società qualora le occorresse qualche disastro. Non è consigliabile in quanto:

- la convivenza è difficile
- il personale dell'azienda ospitata guadagna un facile accesso ai segreti della ospitante

Owned Services

Redundant Site: tecnicamente analogo ad un hot site ma di proprietà della compagnia. In generale la soluzione più costosa

Rolling Hot Site: TIR o furgone contenente un mini CED o un'area di lavoro

8.3.1.2 Software BackUp

Occorre effettuare dei backup periodici di:

- applicazioni
- utilities
- databases
- operating systems

I backup devono:

- salvare versioni a differente livello di aggiornamento dei file (online files ⇒transaction log)
- essere conservati in online e offsite area
- posti in fire-resistant safe (armadi ignifughi)

8.3.1.3 BackUp Types

Poichè non sarebbe efficiente eseguire il backup di tutti gli elementi tutte le volte, si utilizzano anche altri metodi. Per gestire i tipi di backup non completi si utilizza un attributo di stato: l'archive attribute che, qualora presente, indica che l'elemento cui si riferisce non è stato ancora oggetto di backup (full o incremental)

Incremental Backup: backup dei soli elementi che sono cambiati rispetto al precedente backup (full o incremental). Modifica l'attributo archive

Differential Backup: backup dei soli elementi che sono stati modificati rispetto all'ultimo full backup (ovvero tutti gli elementi che hanno settato l'attributo archive). Non modifica l'attributo archive

Full Backup: backup completo (tutti gli elementi). Modifica l'attributo archive

8.3.1.4 Backup Technologies

Disk Shadowing:

Electronic Vaulting: spedizione immediata del file modificato verso una sede remota

Remote Journaling: spedizione immediata del journal (transaction log) verso una sede remota

Hierarchical Storage Management: spostamento dei dati verso supporti via via meno costosi man mano che i dati perdono di reliability

Storage Area Network: infrastruttura apposita, generalmente basata su switch in fibra verso storage appositi

Tape Vaulting: copia su cassetta e trasferimento in altro sito. Soggetto a smagnetizzazione dei nastri durante il trasporto

Automatic Tape Vaulting: trasferimento dei dati via collegamento verso sede remota

8.3.1.5 Human Resources

Spesso non vengono neanche considerate, ma sono le risorse più difficili da rimpiazzare.

8.3.2 Disaster Recovery

Insieme delle attività necessarie a riportare i servizi critici on-line.

8.3.2.1 Disaster Recovery Team

Booh Team: si occupa della messa in funzione del sito di backup

Salvage Team: si occupa del recovery del sito originale (restoration)

8.3.3 Emergency Response

Si occupa di proteggere le vite ed evitare ulteriori danni.

Emergence: stato nel quale la compagnia sussiste fintanto che non viene eseguita completamente la restoration

Gli scopi fondamentali, nell'ordine, sono:

- proteggere le vita umane
- evitare ulteriori danni

I compiti da eseguire sono, in ordine di importanza ed occorrenza:

1. far conoscere le procedure di emergency exit e destinationi
2. il responsabile di ogni gruppo deve controllare che tutti i suoi siano in salvo
3. la persona designata deve avvertire le autorità (e.g. CC, VVF, Polizia, Ospedali)
4. se non vi e' pericolo: spegnere le macchine in modo pulito e portare con sè i dati critici
5. una o più persone devono interfacciarsi con il mondo esterno. L'azienda deve presentare subito le sue informazioni orima che circolino rumori
6. evitare i piccoli danni procurati da vandalismo, sciacallaggio e frodi

Chapter 9

Law, Regulation, Investigation & Compliance

I crimini informatici sono solo un nuovo modo, tecnologico, di effettuare crimini. In questo capitolo si tratta:

- I metodi di indagine resi possibili dalle leggi
- le leggi, che derivano direttamente dall'etica, riguardanti i crimini in formatici
- l'etica in riferimento ai crimini non trattati dalle leggi

9.1 Ethics and Hackers

9.1.1 Principles

9.1.1.1 $(ISC)^2$Code of Ethics

Il codice etico che dovremmo firmare. Un breve riassunto:

1. Honestly, Justly, Responsibly, Legally
2. Work Diligently
3. Encourage the research, teach, value the certification
4. No FUD
5. Discourage Unsafe practices
6. Prudent Advice
7. Avoid conflict of interests. Take only the job you are qualified to perform
8. No involve in injure activities

9.1.1.2 Computer Ethics Institute

Organizzazione no-profit che lavora per aiutare la tecnologia avanzata con mezzi etici. Hanno scritto un decalogo

9.1.1.3 Internet Architecture Board

Commitee coordinato per la progettazione, lo sviluppo e la gestione di Internet. Si avvale delle Task Force:

IETF: INternet Engineering Task Force

IRTF: Internet Research Task Force

9.1.1.4 Generally Accepted System Security Principles

Commitee che si cura di creare principi di guida per i Security Profesional, IT developer, Information Owner. Vi sono chiari riferimenti ai Common Criteria.

9.1.2 MOM

9.1.2.1 Motive

Intellectual Game: sfida

Self Challenge: e.g. Kevin Mitnick

Profit: rubare informazioni per estorcere, ricattare o semplicemente venderle o utilizzarle

9.1.2.2 Opportunity

9.1.2.3 Means

Hackers: persone che hanno piena padronanza degli strumenti e delle metodologie di attacco

Script Kiddies: persone che usano i tools manon sanno esattamente come funzionano e che danni possono causare

9.1.3 Attacks

9.1.3.1 Internal Attackes

Salami: attacco composto da tanti piccoli crimini nella speranza che essi non vengano rilevati

Data Diddling: modifica di dati. Tecnica che puo' essere utlizzata per il Salami

Excessive Privileges: privilegi eccessivi assegnati ad una persona in confronto ai compiti assegnatigli

Authorization Creep: mancata rimozione di autorizzazioni nei confronti di un utente che cambia mansione

9.1.3.2 External Attacks

Password Sniffing: ascolto del traffico su una rete, nella speranza di rilevare credenziali in transito

IP Spoofing: tipo di attacco Masquerading. Si impersona qualcun altro utilizzando l'IP di costui nei pacchetti inviati

Denial of Service: tentativo di rendere non disponibile un determianto servizio. VI sono vari tipi:

- SYN Flooding
- Ping of Death
- Fragment (TearDrop,)
- DDoS

Dumpster Diving: rovistare nella monnezza

Emanation Capturing: catturare le emissioni elettromagnetiche

Wiretapping: inserimento su una linea dati o telefonica

Social Engineering: arte di ingannare le persone, usando le informazioni che esse inconsciamente forniscono

Information Warfare: spianoggio industriale o gevernativo

9.1.3.3 Phreaking

Tecniche che venivano usate quando vi erano le centraline telefoniche analogiche

Blue Boxing: scatola che emette una frequenza di 2600 Hz, in modo da consentire le long-distance phone call

Red Boxing: scatola che simula il rumore dei gettoni inseriti nel telefono

Black Boxing: scatola che manipola il voltaggio della linea telefonica, in modo da effettuare ogni tipo di chiamata

9.2 Law

9.2.1 Liability

Le Federal Sentencing Guidelines sono state estese nel 1997 per contemplare anche i crimini di tipo informatico. Di tali misfatti sono reposnsabili anche i Senior Corporate Officers qualora la società non sia compliant con i requisiti imposti dalle leggi in vigore (richiano fino a $ 290 milioni).

Responsability: comportamento ed azioni attese

Liability: responsabilità in senso legale

Accountability: possibilità di ritenere qualcuno responsabile per determinate azioni

Due Care: indica l'aver adempiuto a tutte le pratiche possibili per garantire la sicurezza

Due Diligence: indica l'investigare in modo completo i possibili rischi e le minacce

Prudent Person Rule: comportarsi in modo prudente e responsabile, soprattutto per il management (vedi Federal Sentence Guidelines)

DownStream Liability: responsabilità nei confronti di una società con la quale ci siano scambi di informazioni

Negligence: accusa che può essere rivolta in tribunale ad una azienda, nel caso non siano stati soddisfatti i requisiti di sicurezza di legge

Legally Recognized Obligation: standard di condotta cui ci si aspetta che la compagnia si attenda

Proximate Causation: possibilità di provare la causalità del danno

9.2.2 Types of Laws

9.2.2.1 Categories of Laws

Civil Law (Tort): tratta dei torti subiti da individui o compagnie, il cui risultato è un danno od una perdita

Criminal Law: tratta delle condotte individuali che violano le leggi governative, prodotte per difendere il pubblico

Administrative (Regulatory) Law: tratta i regulatory standard, creati dalle agenzie governative

9.2.2.2 Intellectual Property Laws

Trade Secret: qualcosa di proprietario ed importante per l'azienda

Copyright: protezione dell'espressione di una idea (e non dell'idea stessa) dalla copia

Trademark: protezione del Brand

Patent: brevetto che consente (per 20-25 anni) di usufruire esclusivamente o far pagare delle royalty a chi utilizza tale invenzione

Internal Protection: classificazione dei dati e access control internamente all'azienda

9.2.2.3 Software Piracy

La decompilazione è illegale.

SPA: Software Protection Association. Associazione delle maggiori compagnie per proteggere il software

FAST: Federal Against Software Theft. Gruppo internazionale con sede a Londra

BSA: Business Software Alliance. Gruppo con sede a Washington D.C.

DMCA: Digital Millennium Copyright Act. Rende illegale l'aggiramento dei meccanismi di protezione di un software

9.2.3 Law, Directives, Regulations

Legiferare sulla sicurezza informatica è difficile:

- le tecnologie sono in rapida evoluzione
- chi legifera non conosce l'argomento
- ogni stato ha le sue leggi

Molti stati hanno cercato di rendere l proprie leggi più efficaci contro tali crimini includendo i dati nella definizione di proprietà.

9.2.3.1 Health Insurance Portability and Accoutability Act (HIPAA)

Standard nazionali e procedure per l'uso, la trasmissione e laregistrazione di dati medici per gli U.S.A. Prevede pesanti sanzioni pecuniarie

9.2.3.2 Gramm-Leach-Bliley Act

Emanato nel 1999 riguarda il trattamento dei dati per gli istituti finanziari.

9.2.3.3 Computer Fraud and Abuse Act

Emanato nel 1986. VI sono stati degli emendamenti nel 1996. Il primo statuto federale antihacking. Categorizza 7 forme di attività come crimini federali:

9.2.3.4 Federal Privacy Act

Negli anni '60 a lungo fu dibattuta la possibilità, da parte delle stituzioni governative americane, di tenere un DB unico repository centrale di informazioni personali.

Record: fascicolo personale riguardante tutto

Alla fine fu emanato questo atto che difende la privacy. Tale atto richiede:

- Divulgazione delle informazioni pesonali solo agli autorizzati
- fascicolo completo, aggiornato, accurato
- Contromisure per assicurare la sicurezza e la confidenzialità del fascicolo

9.2.3.5 European Union Principles on Privacy

Principi molto restrittivi della Comunità Europea, relativi al trattamento di dati personali:

- il motivo della raccolta dei dati deve essere specificato al momento
- i dati non possono essere utilizzati per scopi diversi da quelli originali
- Dati non necessari non devono essere raccolti
- I dati raccolti devono essere mantenuti solo fino a quando sia necessario
- Solo chi ne ha stretto bisogno può essere autorizzato ai dati
- Il data owner deve evitare in tutti i modi il "data leakage"

9.2.3.6 Computer Security Act

Atto federale del 1987 con il quale vengono identificati i sistemi di elaborazione che contengono informazioni sensibili

9.2.3.7 Security and Freedom From Encryption

Atto approvato nel 1997 che stabilisce il diritto da parte di cittadini e residenti in U.S.A. di usare qualsiasi algoritmo crittografico con qualsiasi lunghezza di chiave. Proibisce allo stato il Key Escrow.

9.2.3.8 Federal Sentencin Guidelines

Sviluppate nel 1991 per coadiuvare i giudici. Stabilisce la responsabilità del management nel trattamento dei dati

9.2.3.9 Economic Espionage Act

Emesso nel 1996, fornisce la struttura necessaria per trattare tali casi e definisce i trade secret: technical, business, engineering, scientific, financial (un asset non deve per forza avere una entità fisica).
Permette all'FBI ed ai servizi Segreti di indagare in casi di spionaggio industriale.

9.2.4 International Cooperation Effort

9.2.4.1 G8

9.2.4.2 Interpol

9.2.4.3 European Commission

9.3 Investigation

9.3.1 Computer Forensic

9.3.1.1 Crime Scene

In caso di incidente di sicurezza occorre:

1. In generale fare attenzione a non rovinare eventuali prove
2. Fotografare la Scena del Crimine
3. Computer: dump della memoria e copia del disco
4. Chiamare le forze dell'ordine
5. In caso di chiaro coinvolgimento di qualcuno del personale nel crimine, chiamare un rappresentante delle risors umane

9.3.1.2 Incident Response Team

Gruppo che interviene all'occorrere di un Incidente di sicurezza. E' formato da:

- senior management
- network administrator
- security officer
- network engineer
- liaison (public affair)

9.3.1.3 Chain of Custody

Storia di come è stata reperita, analizzata, trasportata e preservata la prova. Per le prove di tipo informatico è necessario porre particolare attenzione dal momento che sono facilmente modificabili (⇒perdita d'Integrity).

9.3.2 Incident Handling

Procedura contenuta nel Disaster Recovery Plan. Lo scopo principale è contenere e rimediare al danno e prevenirne di ulteriori. Occorre prestare attenzione a non rovinare le prove.

9.3.3 Evidence

9.3.3.1 Evidence Life Cycle

1. Collection and Identification
2. Storage, Preservation and Trasportation
3. Presentation in Court
4. Return to Victim or Owner

9.3.3.2 Admisible Evidence Characteristics

Sufficient: oggettiva e convincente

Reliable: credibile

Relevant: pertinente al fatto in oggetto

9.3.3.3 Evidence Categories

Best Evidence: prova primaria in quanto fornisce la maggior reliability (e.g. contratto scritto)

Secondary Evidence: non è credibile e robusta quanto una best (e.g. testimonianza)

Direct Evidence: prova del fatto in se stesso

Conclusive Evidence: prova irrefutabile

Circumstantial Evidence: prova di un fatto collegato

Corroborative Evidence: prova a sostegno, non utilizzabile singolarmente

Opinion Evidence: prova ottenuta dalla testimonianza di un esperto

Hearsay Evidence: chiacchiere, inammissibile in aula

9.3.4 Surveillance, Search, Seizure

I metodi per reperire le prove devono essere legali

9.3.4.1 Surveillance

Sorveglianza, auditing. Vi sono due categorie fondamntali:

- Physical
  - Security Agents
  - Security Cameras
  - CCTV
- Computer
  - Auditing
  - Network Sniffers
  - Keyboard Monitors
  - Wiretaps
  - Line Monitoring

9.3.4.2 Search

Praticamente è l'analogo informatico del pedinamento. Può essere eseguito da qualsiasi privato. La polizia è soggetta, in America, al Quarto Emendamento: per poter effettuare un pedinamento deve ottenere l'autorizzazione dal giudice (o dalla corte).

Exigent Circumstances: qualora vi possa essere la possibilità che il pedinato cancelli delle prove si può procedere per exigent circumstances (il giudice poi deciderà se l'azione era leggitima o no).

9.3.4.3 Seizure

Confisca. Valgono gli stessi discorsi fatti per il search

9.3.4.4 Interrogating

Chapter 10

Physical (Environmental) Security

Layered Model: sicurezza implementata a livelli, in modo che, qualora ne fallisse uno, gli altri possono ancora proteggere i beni fisici

10.1 Introduction

10.1.1 Physical Security Risks

10.1.1.1 Physical Theft

10.1.1.2 Service Interruption

10.1.1.3 Physical Damage

10.1.1.4 Compromised System Integrity

10.1.1.5 Unauthorized Disclosure

10.1.2 Physical Security Components Selection Process

Security Musts: obblighi di legge

Security Shoulds: attività di protezione della compagnia convenienti (e.g. locks)

10.1.2.1 Hardware

SLA: Service Level Agreement

MTBF: Mean Time Between Failure

MTTR: Mean Time To Repair

10.1.3 Planing Process

Critical Path: cammino critico per le funzionalità del business. Una sua buona descrizione deve includere i dettagli dei meccanismi di supporto e le ridondanze

Critical Path Analysis: elenco di tutti i pezzi della infrastruttura, le interazioni, ciò che è necessario per la buona funzionalità. Devono essere creati dei diagrammi che mostrino power, data, water, sewer lines

10.2 Administrative Controls

I più alti vertici del management sono responsabili per quasi tutto quello che accade all'interno di una compagnia.

10.2.1 Facility Selection

Le responsabilità di tale fase comincia prima della costruzione vera e propria. Ciò che deve essere tenuto presente nella scelta della locazione:

- Visibility
  - Surrounding Terrain
  - Building Marking and Sign
  - Type of Neighbors
  - Population of the Area
- Surrounding Area and External Entities
  - Crime Rate
  - Proximity to Police, Fire Station and Medical
  - Possible Hazards from Surrounding Area
- Accessibility
  - Road Access
  - Traffic
  - Proximity to Airport, Train Station and Highway
- Natural Disaster
  - Floods, Tornadoes, Earthquakes, Hurricanes
  - Hazardous Terrain (Mudslides, Falling Rock)

Occorre procedere ad una vera e propria Risk Analysis per valutare tali entità.

10.2.2 Facility Construction

Caratteristiche differenti degli edifici implicano differenti possibilità di utilizzo.

10.2.2.1 Building Issues

- Walls
  - Combustibility
  - Fire Rating
  - Reinforcement (Secured Areas)
- Doors
  - Combustibility (same as walls)
  - Fire Rating
  - Emergency Marking
  - Directional Opening
  - Electric Door Locks (Disabled for State Evacuation)
  - Glass Type
- Ceiling
  - Combustibility
  - Fire Rating

  - Load and Weight
  - Drop Ceiling

- Windows
  - Traslucent or Opaque Requirement
  - Shatterproof
  - Placement
  - Accessibility to Intruders

- Flooring
  - Combustibility
  - Fire Rating
  - Load and Weiring
  - Raised Flooring (flottante)
  - Nonconducting Surface

10.2.3 Facility Management

10.2.3.1 Facility Components

Internal Partitions: suddivione in aree del fabbricato, in modo da separare in base alle destinazioni d'uso. E' importante che la separazione sia anche nel controsoffitto e sotto al pavimento flottante

Data Center Location: devono essere posizionati al centro ed in un piano intermedio, in modo da evitare allagamenti (piani inferiori) e la facile propagazione del fuoco (piani superiori).

10.2.3.2 Computer and Equipment Rooms

L'ambiente deve essere confortevole per gli apparati, non più anche per gli uomini:

temperature: 70 - 74 Fareneight

umidity: 45 - 60%

fire suppresion: Halon (o sostitutivo)

access doors: una sola, due porte di uscita di emrgenza allarmate

flooring: anti-static

grounding: messa a terra di tutto l'edificio a norma (pozzetto di rame, etc)

carpeting: no o anti-static se proprio necessario

10.2.4 Personnel Controls

10.2.4.1 Pre-employment Screening

- Check References, Precedent Employments, Education
- Character Evaluation
- Background Investigation
- Drug Test

10.2.4.2 Employee Maintenance

- Job Rotation
- Duty Separation
- Periodic Review
- Security Clearance Reevaluation
- Supervisor Updates and Reccomendations

10.2.4.3 Post-Employment

- Friendly Termination
- Exit Interview
- Account Locking or Removal
- Changing Password
- Facility Escorting Removal

10.2.5 Training

10.2.6 Emergency Response and Procedures

Tali procedure sono necessarie per trattare casi di incendio, bombe, tornado, tempeste, civil unrest. DUrante ognuno di questi eventi determinate persone devono assumersi specifiche responsabilità e portare avanti i loro compiti. Allo scopo occorre prestare attenzione a:

- Evacuation Procedures
- System Shutdown
- Training and Drills
- Integration with Disaster Plans
- Accesible Documented Specific Emergency Procedures
- Periodic Equipment Test

10.3 Technical Controls

10.3.1 Access Controls

10.3.1.1 Personnel Access Control

Le persone devono essere correttamente identificate prima di permetterne l'accesso fisico.

PiggyBack: accesso non autorizzato di un individuo che sfrutta le credenziali o i diritti di accesso di un altro. Tipicamente si verifica qualora un individuo segue una persona correttamente autorizzata

La sicurezza dell'edificio può andare in contrasto, a volte, con la sicurezza delle persone. Occorre prendere una decisione su quale delle seguenti strategie adottare:

Fail-Safe: sicuro in caso di rotture ⇒in caso di mancanza di corrente le porte vengono sbloccate, in modo che le persone possano fuoriuscire

Fail-Secure: sicuro in caso di intrusioni ⇒in caso di mancanza di corrente le porte vengono bloccate in modo che nessuno possa entrare

10.3.1.2 Card Badge

Magnetic Card: memory card o smart card

Wireless Proximity Readers: due tipi principali

User Activated: l'utente appoggia la carta sul lettore

System Sensing: riconosce automaticamente la presenza di un determinato oggetto in un certo raggio d'azione, senza necessità di azione da parte dell'utente

Transponders: la carta è un sistema radio rice-trasmittente con batteria propria. Funziona con un codice di accesso

Passive Devices: dispositivo magnetico che reagisce al campo creato dal lettore. Non richiede batteria

Field Powered Devices: dispositivo elettro-magnetico. Richiede batteria

10.3.2 Intrusion Detection

Tipi di tecnologie da usare per rilevare la presenza di intrusi

Proximity Detection System: rileva le variazioni di capacitanza emettendo un campo magnetico

Photoelectric (PhotoMetric) System: determina il cambiamento di luminosità

Wave Pattern: genera un pattern predefinito di onde e si allarma qualora esso ritorni disturbato

[**Passive**] **InfraRed System:** identifica i cambiamenti delle oonde derivanti dall'irraggiamento, rilevando i cambiamenti repentini di calore

Acoustic-Seismic Detection System: determina il cambiamento di livello di rumore dell'ambiente circostante

10.3.3 Alarms

10.3.4 Monitoring (CCTV)

10.3.5 Heating, Ventilation, Air Conditioning (HVAC)

Positive Air Pressure: pressione maggiore di quella esistente esternamente, in modo tale che l'aria (ed anche le fiamme) tendano ad andare fuori

Protected Intake Vents:

Closed Loop Recirculation: aria reusata dopo averla filtrata

Dedicated Power Lines:

Emergency Shutoff Valves and Switches: per chiudere i flussi di water, gas, steam (vapore) in caso di rotture etc.

Positive Drain: il contenuto delle condotte (water, gas, steam) fluisce verso l'esterno

Placement:

Damaging Temperature

- 100° F Magnetic
- 175° F Electronic Systems
- 350° Paper Product

10.3.6 Power Supply

10.3.6.1 Power Protection

UPS: Uninterrupted Power Supply

On-Line: UPS sempre in carica posto fr aAC e apparati

Stand-By: in presenza di un power failure, il sistema commuta sull'alimentazione a batteria

Backup Supply: fonte di corrente alternativa (Genratore Autogeno o seconda linea)

10.3.6.2 Electrical Power Distrurbs

EMI: Electro-Magnetic Interference (e.g. light, electrical motor)

RFI: Radio Frequency Interference (e.g. Fluorescent light, cables)

Definitions

(Transient) Noise: interferenza EMI o RFI che causa fluttuazioni di corrente

Inrush Current: scarica di corrente necessaria all'aumentare della potenza richiesta

Ground: camminamnto verso il terreno per scaricare la potenza in eccesso

Clean Power: potenza che non fluttua

Ci possono essere delle fluttuazioni di voltaggio

Power Excess

Surge: alto voltaggio prolungato. Occorre installare dei surge protector, in modo cda non bruciare gli alimentatori

Spike: alto voltaggio momentaneo

Power Loss

BlackOut: mancanza di corrente prolungata

Fault: mancanza temporanea di corrente

Power Degradation

SAG/DIP: basso voltaggio momentaneo

BrownOut: basso voltaggio prolungato (e.g. una fase mancante)

10.3.7 Fire

10.3.7.1 Placement of Sensors and Detection

Plenum Area: zona in cui sono presenti cavi e fili (controsoffitti, intercapedini, pavimenti flottanti)

I sensori devono essere posti:

- sospesi al soffitto (generalmente il fuoco va verso l'alto)
- sotto i paviementi flottanti (in quanto i cavi possono far partire un fuoco sugli apparati elettrici)
- nei condotti aerei (poichè trasportano aria)

10.3.7.2 Placement of Sprinklers

Gli estintori devono essere posti a non più di 50 piedi dai quadri elettrici

10.3.7.3 Fire Protection

Shutdown System: sistema che sospende l'erogazione di corrente

Warning Sound Signal: segnale sonoro che indica il pericolo e che può fornire ausilio nella ricerca di una via d'uscita

Overrire Button: pulsante di disattivazione dell'allarme nel caso la situazione rientri sotto controllo

10.3.7.4 Type of Detection

Red Pull Boxes: pulsante a muro da attivare a mano

Smoke Activated: utilizzano electric devices (optical detector) che consentono una rilevazione rapida. Misura l'alterazione del raggio di luce inviato: qualora si dovesse frapporre del fumo la quantità di luce verrebbe a diminuire

Heat Activated: misurazione della temperatura. I device possono essere puntuali o a cavo. Esistono due modalità di funzionamento:

- Rate of Rise Temperature Sensor
- Fixed Temperature Sensor

Flame Activated: rileva la pulsazione delle fiamme o le radiazioni infrarosse emesse. Costano molto di più ma forniscono una rilevazione più pronta

Automatic Dialup Alarm: sistema che provvede a chiamare i vigili del fuoco

10.3.7.5 Type of Suppression

Fire Class

Fire Class	Fire Type	Elements	Suppression Method
A	Common Combustibles	Wood, Paper, Laminates	Water, Soda Acid
B	Liquid	Petroleum Products and Coolants	Halon, CO_2, Soda Acid
C	Electrical	Electrical Equipment ad Wires	Halon,CO_2
D	Combustible Metals	Magnesium, Sodium, Potassium	Dry Powder

Suppression Method

Combustion Elements	Suppression Method	Suppression Working
Fuel	Soda Acid	Removes Fuel
Oxygen	CO_2	Removes Oxygen
Temperature	Water	Reduces Temperature
Chemical	Halon	Interferes with chemical reaction

Halon Il gas halon interferisce con il processo di combustione degli elementi diminuendo il fuoco. Non causa danni agli apparati di elaborazione però genera i seguenti problemi:

- contribuisce al buco dell'ozono
- dannoso per le persone se presente in quantità maggiori del 10%

per questi motivi la EPA ha approvato i seguenti sostitutivi:

- FM-200
- NAF-S-III
- CEA-410

- FE-13
- Water
- Inergen
- Argon
- Argonite

Water Sprinkler Un sistema antiincendio basato sull'acqua costa molto meno di quelli basati su Halon e suoi sostituti.

Wet_Pipe closed head system): le tubature contengono sempre l'acqua. Attivato da sensori di temperatura. Da non usare in paesi in cui l'acqua può ghiacciare

Dry Pipe: le tubature non contengono acqua, ma vengono riempite da una valvola apposita all'ocorrere di un allarme generando, quindi, una sorta di delay. Attivato da sensori di temperatura. Sequenza:

1. Sensore attivato
2. l'acqua fluisce nei tubi
3. l'allarme antincendio suona
4. la corrente viene staccata
5. l'acqua fluisce dagli sprinklers

Preaction: sistema misto, in cui l'acqua viene rilasciata dagli sprinkler solo dopo che un apposito sigillo si sia fuso. In tale modo è possibile evitare l'uso di acqua in caso di incendi domabili in altro modo

Deluge: sistema analogo al dry, con la differenza di non avere saracinesche anche sugli sprinkler, in modo da offrire meno resistenza all'acqua e aumentare la portata

10.3.8 Backups

I supporti fisici dei salvataggi dati devono essere posti in appositi armadi ignifughi.

10.4 Physical Controls

Perimeter Control: prima linea di difesa. Vi sono due modi fondamentali di funzionamento:

Closed Facility: tutte le porte chiuse, meccanismi di monitoring accesi ed in posizioni strategiche

Facility on Operation: più complicato poichè occorre distinguere gli individui autorizzati da quelli non autorizzati

10.4.1 Fencing

"First Line of Defence". Efficace barriera fisica. Funziona come deterrente e misura preventiva. Costosa, inestetica. Si classifica in base all'altezza:

3-4 Feet: deterrente per trasgressori casuali

6-7 Feet: non scalabile facilmente

8 Feet + Barbed Wire: protezione seria

Un tipo completo di barriera perimetrale è il:

PIDAS: Perimeter Intrusion Detection and Assessment System è un tipo di recinto che presenta sensori sui cavi e alla base, sensori di vibrazione che fanno partire un allarme

10.4.2 Gates

ManTrap: stanzino con due porte e una finestra di ispezione. Elimina il pericolo di piggyback

TurnStile: tornello?

10.4.3 Bollards

Colonnine luminose poste per individuare eventuali veicoli in movimento

10.4.4 Locks

Controllo d'accesso più economico. Deterrente semi-serio:

- scoraggia gli intrusi non esperti
- ritarda gli intrusi esperti

Padlock: catena per recinto

Preset Lock: per le porte (key-and-knob, Mortise, rim)

Cipher (Programmable) Lock: utilizzano una tastiera, dovendogli fornire una combinazione ed a volte anche una swipe card. Costano più degli altri. Le opzioni solitamente disponibili sono:

Door Delay: allarme che scatta in seguito al prolungarsi nel tempo dell'apertura di una porta (e.g. il ceddino di Network)

Key-Changement: codice modificabile

Key-Override: codice di accesso passpartout (con allarme collegato)

Master-Keying: chiave da supervisore

Hostage Alarm: combinazione da usarsi in caso di presa di ostaggi o minaccia

Device Lock: per impedire il furto dei dispositivi (e.g. computer). Tipici device lock:

Switch Control: copre gli interruttori on/off

Slot Lock: device assicurato tramite cavo, passante per uno slot spurio, alla scrivania o simile

Port Control: blocco dell'accesso al disco o a porte seriali, parallele non utilizzate

Peripheral Switch Control: interruttore fra tastiera e computer

Cable Trap: previene la rimozione di dispositivi I/O facendo passare i cavi attraverso unità di blocco apposite

10.4.5 Lighting

Lighting è un controllo fisico che funziona in modo preventivo e come deterrente per gli intrusi nei parcheggi, entrate e sezioni critiche. Deve essere scelto con cura: la mancanza di una adeguata illuminazione pone in pericolo i dipendenti che potrebbero rivalersi sull'azienda.
Il NIST ha stabilito l'illuminazione per la protezione perimetrale delle aree critiche che deve essere fornita da ogni lampada:

- eight feet high
- two foot-candles

I tipi di illuminazione che si possono installare sono:

SearchLight:

StreetLight: illuminazione dei viali

FloodLight: illuminazione da stadio

Fresnel Unit: proiettori ad alta intensità (e.g. nelle carceri, film con Bruce Willis)

10.4.6 Surveillance

Dogs: molto buoni come misura preventiva e deterrente. Economici (non vanno in vacanza). Non distinguono un utente autorizzato da uno non autorizzato

Patrol Force (Guard): molto buoni. Sanno prendere decisioni in situazioni non convenzionali

10.4.7 Facility Construction Materials