Autoritat de Certificació de la Comunitat Valenciana

GENERALITAT VALENCIANA

Seguridad de la información: CISSP

Valencia
16 de Enero de 2007

Conselleria d'Infraestructures i Transport
Generalitat Valenciana

Índice

- **(ISC)^2**
- **CISSP: los dominios.**
  - *Security Management Practices*
  - *Access Control*
  - *Security Models and Architecture*
  - *Physical Security*
  - *Telecommunications and Network Security*
  - *Cryptography*
  - *Business Continuity Plan*
  - *Law Investigations and Ethics*
  - *Application and system development*
  - *Operation security*

¿Qué es el (ISC)^2?

- **International Information Systems Security Certification Consortium**
  - CISSP: 5 años experiencia en algún dominio.
  - Systems Security Certified Practitioner (SSCP): Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators. 7 dominios y 1 año de experiencia.
  - Certification and Accreditation Professional (CAP): assess risk and establish security requirements. 2 años experiencia.

Dominio 1

GENERALITAT VALENCIANA

Security Management Practices

Security Management Practices

- **El enfonque de la seguridad debe ser 'Top-Down'**
- **Los controles se clasifican en:**
  - Administrative: policies, standars procedures and guidelines. Screening of personnel, awareness and training, and implementing change controls procedures.
  - Technical controls (logical): Implementing and maintaning access control mechanism, password and resource management, indentification and authentication methods, security devices and configuration of the infrastructure.
  - Physical Controls: controlling individual access into de facility and departaments, locking systems and removing unncesary floppy or CD-ROM drivers, protecting the perimeter of the facility, monitoring for intrusion, and enviromental controls.
- **Gestión del riesgo: Vulnerability, threat, risk, exposure, countermesaure or safeguard.**
  - Cost/ benefit comparasion. SLE, ALE, ARO
  - Quantitative VS Qualitative. And example of Qualitative: Delphi
  - Management risk: transfer, reduces, rejecting, accept.

Security Management Practices

- **Security policy:**
  - Bussines objectives.
  - A reference easily understood document for everyone.
  - Developed to integrate security into all business functions and process.
  - Including all legislation and regulation applicable to the company.
  - Others Policy documents: issue-specific policy, system-specific policy (sotware in PC, computers locked, Host Fws)
- **Types of policies:**
  - Regulatory: following standars set by specific industry regulatory.
  - Advisory: advise employers regardings the expected behavioral.
  - Informative: is an information not an enforcable policy. General information about patners, goals and mission.
- **Other documents:**
  - Standars (obligatory), baseline , guidelines (recomendation), procedures (step by step)

Security Management Practices

- **Due Care and Due diligence**
- **Information Classification:**
  - Military (TS, S, Confidencial, Sensitive but unclassified, Unclassified) VS Busines (Confidencial, Private, Sensitive, Public)
- **Data classification Procedures**
  - Define classification, criteria, owner, data custodian, security controls applied.. (Similar to LOPD / RD)
- **Classification controls:**
  - Access control, encryption, auditing, Separation of duties to access, reviews (classification), backup and recovery.
- **Layers of control (roles):**
  - Data owner, data custodian, system owner, security Administrator, Security Analyst, Application owner, supervisor, Change control Analyst, Data Analyst, Process Owner, Solution provider, User, Product line manage.
- **Hiring Practies: NDA.**

Security Management Practices

- **Employers controls:**
  - Rotation of duties
  - Mandatory vacations
  - Split Knowledge and dual control
- **Termination (contracts, employers..)**
  - Leave the facility with supervision
  - Surrender badges-ID, keys..
  - Users accounts and password must be deleted and changed.
  - An exite interview
- **Security Awareness Training:**
  - Types:Management, Staff, Technical.
  - Evaluating the program: questionaries, reduction of number incidents..

Dominio 2

GENERALITAT VALENCIANA

Access Control

Access Control (2)

- **Security Principles: C I A.**
- **Identification, Authentication, Authorization**
- **Identification:**
  - Unique ID : for accountability
  - Non descriptive of the user's position or role.
  - Not Shared with other users
  - A standard naming schema (easier)
- **Authentication:**
  - Something your are, you know, you have.
  - Strong authentication : Two Factor authentication.
- **Identity Management:**
  - Various types of users need different level of access.
  - Resources have different classification level
  - Diverse identity data must be kept on different types of users
  - The corporate environment is continually changing.

Access Control

- **Biometrics: (personal attribute or behavior)**
  - Error Types 1 and 2.
  - Palm Scan, Hand geometry, retina scan, Iris scan, Signature Dymanics, keyboard dynamics, voice Print, Facial Scan, Hand Topography.
- **Passwords:**
  - Weakest: guessed (birth..)
  - Passwords policy (lenght, time, not easy guess..)
  - Attacks:
    - Electronic Monitoring.
    - Access the password file.
    - Brute force attacks.
    - Dictionary attacks.
    - Social engineering
  - Limit numbers logins - > Clipping level
  - Cognitive passwords: fact-opinion-based information.
  - One-time passwords
    - Token device
    - Synchronous VS Asynchronous

Access Control

- Passphrase -> virtual password
- Memory card VS Smartcard

- **Authorization**
  - Roles: Security Administrador, System Administrator, operator..
  - Groups: UNIX concept of Groups.
  - Physical and logical: physical access to gain a shell.
  - Time of day: Deny access at of work time.
  - Transaction type: view your bank account but not allowed to tranfer money.
  - Problem: authorization creep.
- The **need to know concept** and **least privilege** concept.
- Single Sign-On:
  - Kerberos: Tickets grant access or not. KDC (Key Distribution Center) is the manager
  - SESAME. SSON designed in Europa
  - Security Domain.

Access Control

- **Access control model**
  - DAC (Discrectionary access control). Owner of the resource assing privelges (UNIX perm).
  - MAC (Mandatory access control). OS assigned the perms.
  - RBAC (Role-Based access control).
  - Concept of security label: Classification and category.
- **Access Control Techniques and Technologies**
  - Rule-Based access control:
    - If ... then...
  - Constrained User Interface: database views, shell with a few commands..
  - Content dependent
  - Context dependent.

Access Control

- **Access control matrix**:
  - Capabilites table: rows of the matrix. User perms to all the objects
  - ACL: columns of the matrix. Which users have access to and object

Access Matrix (cont.)

- A process may switch from a domain to another domain while it executes.
  - **Domains can be viewed as objects.**

domain \ object	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

Yair Amir Fall 00 / Lecture 9 9

Access Control

- **Centralized access control administration:** one entity is responsible for overseeing access to all corporate resources
  - **Radius and tacacs (TACACS+, XTACACS..). Diameter (mobile IP).**
- Decentralized access control administration: in a departament, area, office..
- **Access control layers**:
  - **Administrative control**:
    - Policy and procedures
    - Personnel controls (separation of duties, rotation of duties)
    - Supervisory structure (Supervisor response employer action)
    - Security-awareness training
    - Testing (testing procedures and security controls..)
  - **Physical controls**
    - Network segregation
    - Perimeter Security
    - Computer controls (locks CD-Roms, floppy, USB)
    - Data backups
    - Work area separation (level of access to different areas)
    - Cabling (STP vs UTP)

Access Control

- Technical controls
  - System Access (DAC, MAC, logins and passwords.)
  - Network architecture (DMZ)
  - Network Access (FWs, ACLs..)
  - Encryption and protocols
  - Control zone (avoid intercept emantion of signals)
  - Auditing

Access control types

- Preventive: administrive
  - Policies and procedures
  - Effective hiring practices
  - Pre-employer background checks
  - Controlled termination processes
  - Data classification and labeling
  - Security awareness
- Preventive: physical
  - Badges
  - Guards, dogs
  - Fences, locks, mantraps

Access Control

- Preventive: Techincal
  - Passwords, biometrics, smart cards
  - Encryption, call-back systems, database views, constrained user interfaces
  - Antivirus software, ACLs, firewalls, routers, clipping levels.

- **Accountability**
  - System-level events:
    - System performance, Logon attemps, logon ID, Date and time of each logon, Lockouts os users and terminals, user of administration utilities, devices used, funcionts performance, request to alter onfiguration files
  - Applicaation level events:
    - Error messages, files opened and closed, modifications os files, Security violations within applications
  - User level events:
    - Identification and authentication attemps, files and services and resources used, commands initiatded, security violations
- **Review of audit information:**
  - Audit reduction tool
  - Variance detection (history of logs)
  - Attack signature detection (IDS)

Access Control

- **Keystroke: records and record keystroke** (key-logger)
- **Protecting Auditing Data and log information** (only administration an security personnel)
- Access Control Practices:
  - Deny access to undefined and anonymous users
  - Limit and monitoring the usage of privilege accounts
  - Suspend or delay access after a number of attemps
  - Remove obsolete user accounts and not used accounts
  - Disable services and port unnecesary
  - Replace default password settings accounts
  - Enforce password rotation
  - Enforce password requeriments
  - Audit system and user events and actions and review periodically.
  - Object reuse
  - Tempest
    - White noise (interference)
    - Control zone (zone of emanations)

Access Control

- **Access control Monitoring**
  - IDS:
    - Network
    - Host
    - Signatures (knowledge)
    - Statistical anomaly-based IDS
      - Protocol anomaly based
      - Traffic anomaly based
    - Rule based:
      - if-- then..
      - Expert systems
  - **IPS: (Intrusion Prevention Systems)**
    - **Preventive control and detective control**
  - **Honeypot (and Honeynets)**
    - **Entincement (legal) VS entrapment (ilegal!!)**
  - **Sniffer (Hackers and network admin)**
- Thearts to Access Control:
  - **Brute force attacks**
  - **Spoofing logon**
  - **Phising attacks**

Dominio 3

GENERALITAT VALENCIANA

Security Models And Architecture

Security Models And Architecture

- **Computer Architecture**
  - CPU (ALU, CU), Register (PC, PSW), BUS (address, data)
  - SMP, MultiTrhead (thread VS Process), Multitasking, Multiprogramming.
- **Kernel mode VS user mode**
  - Process Isolation
  - Base register and limit register (Buffer Overflow)
- **All kinds of memory (RAM, ROM..)**
- **The conept o domain and execution domain**
- **CPU modes and protection rings**
  - Monolitic VS layered
  - Microkernel
- **Trusted Computing Base (TCB)**
  - Trusted path (secure comunication path betwen user and kernel)
  - Trusted shell (a Secure shell)
- **Security perimeter**
- **Reference monitor and security kernel**
- **Least privilege**
- **Security models**
  - State machine models
    - Bell-LaPadula (confidencial / MAC), Biba (integrity / DAC).
    - Clark Wilson: Constrained data items.

Security Models And Architecture

- **Covert Channel.**
  - Timing and storage
- **Security Modes of Operation**
  - Dedicated, System high-security model, Compartmented security mode, Multilevel Security mode
- **System Evaluation Methods**
  - TSEC == Orange Book
    - D,C1,C2,B1,B2,B3,A
  - ITSEC
  - Common Criteria
- **Certification and Accreditation**
- **Maintenance Hooks (Developers!!!)**
- **Buffer Overflow**
  - Bounds checking (good practice program!!)

Dominio 4

GENERALITAT VALENCIANA

Physical Security

Physical Security

- **Threads:**
  - Natural enviorenment threats: Floods, earthquaters, tornados..
  - Supply system threats: Power distibutions outages, communications interruptions..
  - Manmade threats: unautorizhed access (external and internal), explosions, damage by angry employers, employee errors and accidents
  - Politically motivated threats: terroris attackts, riots..
- **The first objective in Physical Security: Live safety.**
- **Issues with selecting a facility**
  - Visibility, Surrounding area and external entities, Accesibility, Natural disasters
- **Construction the facility**
  - Walls, doors, Ceilings, window, flooring, heating and ventilation and AC, Electric power supplies, water and gas lines, fire detection and suppression
- **EMI, RFI: noise**

Dominio 5

Telecommunications and network security

Telecommunications and network security

- **TCP/IP vs OSI**
- **Analog vs Digital**
- **Asynchornous vs Synchronous**
- **Network topology:**
  - Ring, bus, star, mesh
- **Ethernet, Tokenring, FDDI, CDDI..**
- **Coaxial VS UTP/STP**
- **Tranmision methods: unicast, multicast, broadcast**
- **Routing protocols: BGP, IGRP, OSPF..**
- **Firewalls**
  - Packet filter (ACLS)
  - Stateful Firewalls
  - Proxy firewalls
  - Application-level proxies.

Telecommunications and network security

- **Differents Fws architectures**
  - Screened host, screened subnet, bastion host..
- **Honeypot / Honeynet**
- **VPN (Virtual Private Network)**
  - Tunnel / Transport
  - IPSec (ESP and AH)
- **WLAN (WIFI):**
  - 802.1x