Access Controls

Mike Smith

26/04/10 - Rev.27

Threats

- Identity Theft
- Phishing
- Spoofing at logon
- Brute force attacks
  - Wardialing
- Dictionary Attack

Intrusion Detection Systems

- Signature Based
  - Pattern Matching
  - Requires continual update
  - Pattern & Stateful
- Anomaly Based
  - Can detect new attacks
  - Statistical, Protocol and Traffic
- Rule Based
  - Uses an Expert System
  - Cannot detect new attacks
- Network-Based - NIDS
  - NIC in promiscuous mode
- Host-Based - HIDS

Controls

- Administrative
  - Personnel Controls
  - Supervisory Structure
  - Security-Awareness Training
  - Testing
- Physical
  - Network Segregation
  - Perimeter Security
  - Computer Controls
  - Work Area Separation
  - Cabling
  - Control Zone
- Technical or Logical
  - System Access
  - Network Architecture
  - Network Access
  - Encryption and Protocols
  - Auditing
- Deterrent - Intended to discourage
- Preventative - prevent harmful occurrence
- Corrective - restore after harmful occurrence
- Recovery - Intended to bring controls back
- Detective - detect after harmful occurrence
- Compensating - Controls that provide for an alternative
- Directive - Mandatory controls, regulations or environment

Biometrics

- Acceptance
  - False Rejection Rate - FRR = Type I error
  - False Acceptance Rate - FAR = Type II error
  - Crossover Error Rate - CER = % when FRR = FAR
  - Privacy, Physical, Psychological
  - Time to authenticate is the main factor
- Fingerprints
- Retina Scans
- Iris Scans
- Facial Scans
- Palm Scans
- Hand Geometry
- Signature Dynamics
- Keyboard Dynamics
- Hand Topology

Three Factor Authentication

- 1 Something you know (password)
- 2 Something you have (token)
- 3 Something you are (biometric)
- Passwords
  - Static
  - Dynamic
- Tokens Smartcards
  - Static Password
  - Owner authenticates to token
  - Token authenticates to system
  - Dynamic Password
  - Synchronous
  - Asynchronous
  - Side-channel attacks

Accountability

- System-level events
- Application-level events
- User-level events

Access Control Models

- DAC - Data owners decide who has access to resources and ACLs are used to enforce security policy
- MAC - Operating systems enforce the system's security policy through the use of security or sensitivity labels
- RBAC - Access decisions are based on role
- Lattice based - provides least access privileges of the access pair - Greatest lower bound and Lowest upper bound

SSO

- Kerberos
  - Symmetric Key Encryption
  - KDC - Kerberos-trusted Key Distribution Center
  - TGS - Ticket Granting Service
  - AS - Authentication Server
  - KDC knows secret keys of client and server
  - KDC exchanges info with the client and server using symmetric keys
  - Using TGS grants temporary symmetric key
  - Client and server use temporary session key
  - Weaknesses
    - Replay is possible with time frame
    - TGS and Auth server are vulnerable as they know all
    - Initial exchange passed on password authentication
    - Keys are vulnerable
- SESAME
  - Needham-Schroeder Protocol
  - Supports MD5 and CRC32 Hashing

Access Control

- Centralized
  - RADIUS - incorporates an AS and dynamic password
  - TACACS - Terminal Access Controller Access Control System - for network applications - static password
  - TACACS+ - supports tokens
- CHAP - supports encryption
- Operate and maintain
- Monitor and evaluate

Application Security

Mike Smith

26/04/10 - Rev.12

Attacks

- Smurf (ICMP)
- Fraggle (UDP)
- SYN - TCP ACK
- DoS
- D-DoS
- Teardrop

Patch Management

1. Infrastructure
2. Research
3. Assess and Test
4. Mitigation - Rollback
5. Deployment - Rollout
6. Validation, Reporting and Logging

Malware

- Worm - replicates without a host
- Virus - needs an application
- Rootkit
- Botnets, RATs, Logic Bomb
- Trogan Horses
- Mobile Code / Java Applets / ActiveX Controls
- Insertion - Avoidance - Eradication - Replication - Trigger - Payload

Distributed Computing

- CORBA
- COM / DCOM - GUID
- SOAP
- EJB
- DCE - UUID

OLTP - ACID

- Atomicity - divide transactions into units of work
- Consistency - follow integrity policy
- Isolation - execute in isolation
- Durable - Once verified, committed on all systems

Capability Maturity Model - CMM I Regularly Drink My Orangejuice

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimizing

Database Models

- Relational
  - row = tuple
  - column = attribute
- Hierarchical
- Network
- Object Orientated
- Object Relational

DBMS

- Must implement access controls
- Caution against data inferencing
- Data definition language - DDL
- Data manipulation language - DML
- Query language - QL
- Report generator
- Views
- Aggregation - combining information
- Inference - deduce the full story

Interfaces

- Open Database Connectivity - ODBC
- Object Linking and Embedding - OLE DB
- Java Database Connectivity - JDBC

OOP

- Benefits of OOP
  - Modularity - Autonomous objects and cooperation through messages
  - Deferred Commitment - Internals of objects can be changed independently
  - Reusability - reuse objects from other programs
  - Naturalness - maps to business processes
- OOA - Process of classifying objects
- OOD - Create a representation of the real-world problem
- Polyinstantiation
  - Multiple copies from the same class
  - Government or military used to hide covert operations

SDLC

- I/LDAP/SDx2/II/OM/D
- Initiation
- Fuctional Design Analysis and Planning
- System Design
- Software Development
  - Verification - meets spec?
  - Validation - meets project goal?
- Installation/Implementation
- Operational/Maintenance
- Disposal

SDLC Methodologies

- Waterfall
- Spiral
- Joint Analysis Development - JAD
- Rapid Application Development - RAD
- Cleanroom
- Iterative
- Reuse
- Extreme

Business Continuity and Disaster Recovery

Mike Smith

26/04/10 - Rev.25

Other

- Personnel Safety is highest priority
- Software escrow used to protect investment in outsourced company
- Recovery
  - Salvage Team
  - Protect from looting

Backup

- Full, Differential, Incremental
- Disk duplexing
- Electronic Vaulting
- Tape Vaulting
- Insurance
- Service Bureaus

Testing and Revising the Plan

- At least once a year
- Checklist Test
- Structured Walk-Through Test
- Simulation Test
- Parallel Test
- Full-Interruption Test

Business Continuity Plan

- Initiation Phase
- Activation Phase
- Recovery Phase
- Reconstruction Phase
- Appendices

Maximum Tolerable Downtime - MTD

- Nonessential - 30 days
- Normal - 7 days
- Important - 72 hours
- Urgent - 24 hours
- Critical - Minutes to Hours

Business Continuity Steps

- NIST Continuity Planning Guide
- Understand the organization - Zachman Poster
- 1. Develop the continuity planning statement
- 2. Conduct the business impact analysis - BIA
- 3. Identify preventative controls
- 4. Develop recovery strategies
- 5. Develop the contingency plan
- 6. Test the plan and conduct training and exercises
- 7. Maintain the plan

BIA Steps

1. Select individuals to interview for data gathering
2. Create data-gathering techniques
3. Identify company's critical business functions
4. Identify resources these functions depend upon
5. Calculate how long these functions can survive without these resources
   - Maximum Tolerable Downtime - MTD
6. Identify vulnerabilities and threats to these functions
7. Calculate the risk for each different business function
8. Document findings and report to management

Facility Recovery

- Hot site
  - Fully configured
  - File and print services
  - Applications are installed
  - Workstations kept up to date
  - Available but expensive
  - Security must be duplicated
- Warm site
  - Facility with power and HVAC
  - File and print services may not have workstations
  - External communications should be installed
  - More time to get up and running but lower cost
- Cold site
  - Facility with power and HVAC
  - No computer hardware on site
  - Communications not ready
  - Least cost but false sense of security, most common
- Multiple Sites / Rolling hot site
- Reciprocal Agreements

Cryptography

Mike Smith

26/04/10 - Rev.31

IPSec

- **Authentication Header - AH** - used for authentication protocol
- **Encapsulating Security Payload - ESP** - used for authentication and encryption
- **Transport Mode** - payload of the message is protected
- **Tunnel Mode** - both payload and routing are protected
- **Security Association - SA** - Simplex, keeps record of parameters

Hashing

- Hash for message digest provides integrity
- HMAC - used with secret key to provide integrity and data origin authentication
- CBC-MAC - uses symmetric block algorithm, provides integrity and data origin authentication
- CMAC - same as CBC-MAC but uses complex logic
- MD2, MD4, MD5, SHA, HAVAL, Tiger

Asymmetric

- Also called Public Key Cryptography
- Each person has private and public key
- For Confidentiality - Sender encrypts with receivers public key - secure message format
- For Authentication - Sender encrypts with their private key - open message format

Strengths

- Better key distribution than symmetric
- Better scalability than symmetric
- Can provides authentication and nonrepudiation

Weaknesses

- Much slower than symmetric
- Mathematically intensive

Examples

- Rivest-Shamir-Adleman - RSA
- Elliptic Curve Cryptosystem - ECC
- Diffie-Hellman
- El Gamal
- Digital Signature Algorithm - DSA
- Merkle-Hellman Knapsack

Symmetric

- Also called secret keys
- For n people, requires n(n-1)/2 keys
- Same key to encrypt/decrypt at both ends
- Block and Stream types

Strengths

- Much faster than asymmetric
- Hard to break if using a large key size

Weaknesses

- Requires secure mechanism to deliver keys
- Each pair need a unique key
- Confidentiality, but not authenticity or nonrepudiation

Examples

- Data Encryption Standard - DES
  - Electronic Code Book - ECB
  - Cipher Block Chaining - CBC
  - Cipher Feedback - CFB
  - Output Feedback - OFB
  - Counter - CTR
- Triple-DES (3DES)
  - DES-EEE3
  - DES-EDE3
  - DES-EEE2
  - DES-EDE2
- Blowfish
- International Data Encryption Algorithm - IDEA
- RC4, RC5 and RC6
- Advanced Encryption Standard - AES
  - Rijndael

History

- 2000 BC Egypt - atbash - substitution
- 400 BC Sparta - scytale cipher - wooden rods
- 100 - 44 BC Caesar cipher
- 16th Century - Vigenere Polyalphabetic cipher
- 1917 - Gilbert Vernam - Vernam cipher - one-time pad
- 1920 - William Friedman - Father of Modern Cryptography
- WW II - German Enigma
- 1970 - Lucifer - IBM
- 1976 - DES

Services

- Confidentiality - cryptography protects confidentiality
- Integrity - cryptography helps with hashing algorithms and message digests
- Authentication - used for this too
- Authorization - upon proving identity can then have key to some resource
- Nonrepudiation - cannot deny sending message

Encryptions at various levels

- End-to-end encryption happens within the application
- SSL encryption takes place at the transport layer
- PPTP encryption takes place at the data link layer
- Link encryption takes place at the data link and physical layer

Cryptosystem

- Software
- Protocols
- Algorithms - Kerckhoffs' Principle - Publicly known
- Keys

Steganography

- Carrier - signal, data stream or file
- Stego-medium - medium in which hidden
- Payload - concealed information

Public Key Infrastructure

- Certificate Authority - CA
  - Takes liability for the authenticity of the individual
  - Binds the individuals identity to the public key
  - Requires cross certification with other CAs
  - Maintains Certificate Revocation Lists - CRLs
- Registration Authority - RA
  - Performs certificate registration duties
  - Broker between user and CA
- Certificate Repository, Certificate revocation system, OCSP
- Provides all services

Strong Cipher

- Confusion - carried out using substitution
- Diffusion - carried out using transposition

Information Security and Risk Management

Mike Smith

25/04/10 - Rev.20

Due ...

- **Diligence** - Do **Detect** - Steps to identify risks using best practices
- **Care** - Do **Correct** - Steps taken to correct identified risks to a minimum

Standards, Guidelines and Procedures

- Standards - Specify use of technology in a uniform way, compulsory
- Guidelines - similar to standards but not compulsory, more flexible
- Procedures - Detailed steps, required, lowest level
- Baselines - minimum standard and/or point in time

Risk Analysis

Steps

1. Assign Value to Assets
2. Estimate Potential Loss per Threat
3. Perform a Threat Analysis
4. Derive the Overall Annual Loss Potential per Threat
5. Reduce, Transfer, Avoid or Accept the Risk

- ALE = SLE x ARO = AV x EF x ARO
- Total Risk = threats x vulnerability x asset value
- Residual Risk = total risk x control gap

Delphi Technique

- Anonymous groupthink
- Subjective only

Qualitative

- Eliminates $ amounts for cost benefit
- Difficult to track
- Standards not available

Quantitative

- Major project
- Calculations are more complex
- Laborious
- More info gathering
- Standards not available

Fault Logic Tree Analysis

- False alarms
- Insufficient error handling
- Sequencing or order
- Incorrect timing outputs
- Valid but not expected outputs

Failure Modes and Effect Analysis - FMEA

- Block diagram of system or control
- Consider what happens if each block fails
- Tabulate failures and effects
- Correct the design
- Have engineers review

Controls

- Administrative - Policies & Procedures
- Technical /Logical - Restricted Access
- Physical - Locked doors
- Preventative - prevent harmful occurrence
- Detective - detect after harmful occurrence
- Corrective - restore after harmful occurrence

C.I.A

- Confidentiality - prevent disclosure of data
- Integrity - prevent modification of data
- Availability - ensure reliable timely access

Classification

- Government - Unclassified/Sensitive/Confidential/Secret/Top Secret
- Commercial - Public/Sensitive/Private/Confidential

Risk Analysis Terms

- Asset - resource, product, data
- Threat - action with a negative impact
- Vulnerability - absence of control
- Safeguard - control or countermeasure
- Exposure Factor (EF) = % of asset loss caused by threat
- Single Loss Expectancy (SLE) = Asset Value x Exposure Factor
- Annualized Rate of Occurrence (ARO) - represents estimated frequency in which threat will occur within one year
- Annualized Loss Expectancy (ALE) - annually expected financial loss: ALE = SLE x ARO

Security Frameworks

Control Objectives for Information and related Technology (CobiT)

- Plan & Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Committee of Sponsoring Organizations (COSO)

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

Standards

- BS7799
- ISO 17799
- ISO/IEC 27000

Security Program

- Plan and organize
- Implement
- Operate and maintain
- Monitor and evaluate

Legal, Regulations, Compliance and Investigations

Mike Smith

26/04/10 - Rev.25

Due ...

- **Diligence** - Do **Detect** - Steps to identify risks using best practices - investigated weaknesses
- **Care** - Do **Correct** - Steps taken to correct identified risks to a minimum - did all it could to prevent security breaches with proper controls and countermeasures

Evidence

- Best - primary, original, not oral
- Secondary - copies of documents and oral evidence
- Direct - does not need backup - witness account
- Conclusive - irrefutable
- Circumstantial - prove an intermediate fact
- Corroborative - supplementary
- Opinion - only the facts not opinions
- Hearsay - oral or written too far removed

Incident Response

Steps

1. Triage
2. Investigation
3. Containment
4. Analysis
5. Tracking
6. Recovery

Develop a Team

- Various BUs
- Virtual
- Permanent
- Hybrid
- CERT Mailing List
- CERT Documents

- Management decide on calling Cops

Computer Forensics

- International Organization on Computer Evidence - IOCE
- Scientific Working Group on Digital Evidence - SWDGE
- MOM - Motive, Opportunity and Means
- Locard's Principle of Exchange
- Identification - Preservation - Collection - Examination - Analysis - Presentation - Decision
- Primary / Working Image - First thing make a bit mirror copy
- Chain of Custody - Evidence labeled indicating who secured and validated it

Cybercrime

- Computer-assisted
- Computer-targeted
- Computer is incidental

OECD 7 Principles

- Collection should be limited and lawful
- Personal data should be complete and current
- Subjects should be notified of the reason for collection
- Disclosure only with consent
- Reasonable safeguards in place
- Practices and policies openly communicated
- Subjects should be able to find and correct personal info
- Organizations should be accountable

Types of Law

- Civil (Code) Law - continental Europe
- Common Law - England
  - Criminal - jail
  - Civil/tort - damages
- Customary Law
- Religious Law Systems
- Mixed Law Systems

Intellectual Property Law

- Trade Secret - important for company survival
- Copyright - protects the expression of the idea of the resource not the resource itself e.g. computer programs and manuals
- Trademark - word, name, symbol, sound, shape
- Patent - novel invention

Software

- Freeware
- Shareware or trialware
- Commercial
- Academic

Dealing with Privacy

- Government Regs - SOX, HIPPA, GLBA, BASEL
- Self-regulation - Payment Card Industry - PCI
- Individual user - Passwords, encryption, awareness

Telecommunications and Network Security

Mike Smith

26/04/10 - Rev.33

Wireless

- Spread spectrum - distributed across frequency range
- Frequency Hopping Spread Spectrum - FHSS - portion
- Direct Sequence Spread Spectrum - DSSS - all
- Need an Access Point - AP
- Hosts in group must use Service Set ID - SSID
- Authentication
  - Open System Authentication - OSA - in clear
  - Shared Key Authentication - SKA = WEP
  - Wired Equivalent Privacy - WEP - weak
  - Wi-Fi Protected Access - WPA, WPA2 - uses TKIP
- Best Practice
  - Enable 802.11i e.g. WPA
  - Change default SSID
  - Disable broadcast SSID
  - Add RADIUS or Kerberos
  - Put AP at centre of building and in DMZ
  - Implement VPN for wireless devices
  - Configure AP to allow only known MAC addresses
  - Disable DHCP
- Mobile Phones
  - WAP
  - i-Mode - Japan, Asia, Europe
  - Bluetooth - 802.15

OSI Model

- Australia Post Sucks It Never Delivers Parcels
- Application - FTP, TFTP, SNMP, SMTP, Telnet, HTTP
- Presentation - ASCII, EBCDIC, TIFF, JPEG, MPEG, MIDI
- Session - NFS, NetBIOS, SQL, RPC
- Transport - TCP, UDP, SSL/TLS, SPX
- Network - IP, ICMP, IGMP, RIP, OSPF, IPX
- Data Link - ARP, RARP, PPP, SLIP
- Physical - HSSI, X.21, EIA/TIA-232, EIA/TIA-449
- List of Protocols

TCP/IP

- Australian Trains Never Late
- Application
  - TCP - Stream
  - UDP - Message
- Transport
  - TCP - Segment
  - UDP - Packet
- Network - TCP and UDP Datagram
- Data Link - TCP and UDP Frame

WAN Technologies

- Channel Service Unit/Data Service Unit - CSU/DSU
- Switching
  - ISDN
    - BRI ISDN = 2 x B + 1 x D
    - PRI ISDN = 23 x B + 1 B
    - Broadband ISDN
  - Circuit
    - PSTN
  - Packet
    - X.25
    - Frame Relay
    - Cell - ATM
- Switched Multimegabit Data Service - SMDS
- Synchronous Data Link Control - SDLC
- High-level Data Link Control - HDLC
- High-Speed Serial Interface - HSSI
- SS7, VoIP, Session Initiation Protocol - SIP
- Tunneling Protocols
  - IPSec
  - PPP
  - PPTP
  - L2TP
- Authentication Protocols
  - Password Authentication Protocol - PAP - least secure
  - Challenge Handshake Authentication Protocol - CHAP
  - Extensible Authentication Protocol - EAP
  - RADIUS, Diameter, TACACS

Packets and Ports

- Well-known ports 0 - 1023
- TCP: Sequence and Acknowledgement numbers
- UDP: Source, Destination, Length, Checksum, Data
- 23 - Telnet
- 25 - SMTP
- 80 - HTTP
- 161, 162 - SNMP
- 20, 21 - FTP

IP Addressing

- IPv4 - 32 bits, IPv6 - 128 bits
- Class A: 0.0.0.0 - 127.255.255.255
- Class B: 128.0.0.0 - 191.255.255.255
- Class C: 192.0.0.0 - 223.255.255.255
- Class D - Multicast: 224.0.0.0 - 239.255.255.255
- Class E - Reserved: 240.0.0.0 - 255.255.255.255
- Subnetting

Network Devices

- Repeaters
  - Works at Physical Layer
  - Amplify signal
  - Clean up signal
  - Hub = multiport repeater
  - Hub also known as a concentrator
- Bridges
  - Works at Data Link Layer
  - Connect LAN segments
  - Filters based on MAC address
  - Retains same broadcast domain
  - Isolates collision domains
  - Can translate between protocols
- Routers
  - Works at Network Layer
  - Can connect different networks
  - Uses routing protocols: RIP, BGP, OSPF
  - Can filter based on IP address and protocols
- Switches
  - Combine functionality of a repeater and bridge
  - Can work at layer 3 and 4, can use tags = MPLS
  - Used to provide QoS
- Other: VLANs, Gateways, PBXs
- Firewalls
  - Packet Filtering & Dynamic Packet Filtering
  - Stateful
  - Proxy & Kernel Proxy
  - Dual-Homed
  - Screened Host & Screened Subnet

LAN Networking

- Ring, Bus, Star, Mesh Topology
- Ethernet - 10Base2, 10Base5, 10Base-T
- Fast Ethernet
- Token Ring
- FDDI

T- Carriers

- Fractional = 1/24th x T1, 1 voice channel, 0.06Mbps
- T1 = 24 voice channels, 1.544Mbps
- T2 = 4 x T1, 96 voice channels, 6.312Mbps
- T3 = 28 x T1, 672 voice channels, 44,736Mbps
- T4 = 168 x T1, 4032 voice channels, 274,760Mbps

Operations Security

Mike Smith

26/04/10 - Rev.26

Penetration Testing

1. Discovery - Footprinting and info gathering
2. Enumeration - port scans and resource identification
3. Vulnerability mapping - identify vulnerabilities
4. Exploitation - attempt to gain access
5. Report to management

Vulnerability Testing

- Personnel testing
- Physical testing
- System and network testing

E-mail

- POP
- SMTP
- IMAP - can leave on server
- Replaying - Often left enabled - SPAM redirection
- Fax - use an encryptor

Contingency

- Disk shadowing
- Redundant servers
- RAID, MAIT, RAIT
- Clustering
- Backups
- Dual backbones
- Direct Access Storage Device
- Redundant power
- Mesh network topology - not star

Controls

- Administrative
  - Separation of duties
  - Job rotation
  - Least privilege
  - Mandatory vacations
- Technical /Logic
  - Limit boot sequent
  - Harden Remote Access
- Physical - System Hardening

Change Control Process

1. Request for a change to take place
2. Approval of the change
3. Documentation of the change
4. Tested and presented
5. Implementation
6. Report change to management

Change Control Documentation

- New computers or applications installed
- Different configurations implemented
- New technologies integrated
- etc.

Media Controls

- Purging
- Zeroization
- Data remanence
- Degaussing generates a coercive magnetic force
- Physical destruction
- Care with object reuse

Failure Modes and Effect Analysis - FMEA

- Block diagram of system or control
- Consider what happens if each block fails
- Tabulate failures and effects
- Correct the design
- Have engineers review

Physical and Environmental Security

Mike Smith

26/04/10 - Rev.25

Fences

- 3 - 4 feet deter casual trespassers
- 6 - 7 feet too high to climb easily
- 8 feet - serious protection
- Gauges 11, 9, 6 lower number = thicker
- Mesh 2", 1", 3/8"

IDS

- Beams of light
- Sounds and vibration
- Motion
- Different types of field
- Electrical circuit

Gates

- Class I - Residential
- Class II - Commercial
- Class III - Industrial, e.g. Warehouse
- Class IV - Restricted, e.g. Prison

Fire

Detection

- Smoke activated
- Heat activated
- Plenum area - special cabling
- 4. Derive the Overall Annual Loss Potential per Threat
- 5. Reduce, Transfer, Avoid or Accept the Risk

Class

- A - Common combustibles - water or soda acid
- B - Liquids - CO2, soda acid or Halon
- C - Electrical - CO2 or Halon
- D - Combustable metals - total immersion
- K - Kitchens (commercial)

Suppression

- Fuel - Soda acid - removes fuel
- Oxygen - CO2 - Removes oxygen
- Temperature - Water - reduces temperature
- Chemical - Gas Halon or FM-200 - Interferes
- Wet pipe, dry pipe, preaction, deluge

Power

- Spike
- Surge
- Excess
- Fault
- Blackout
- Loss
- Sag/dip
- Brownout
- Degradation
- In-rush current

Locks

- Grade 1 - 3, Commercial, Heavy Duty, Residential
- Warded lock - Padlock
- Tumbler lock
- Combination lock
- Cipher lock

Threats

- Natural environmental
- Supply system
- Manmade
- Politically motivated

Defense in Layers

Deterrence

- Fences
- Warning signs
- Security guards
- Dogs

Delaying

- Locks
- Defense in depth measures
- Access Controls

Detection

- External intruder sensors
- Internal intruder sensors

Assessment

- Security guard procedures
- Communication structure

Response

- Response force
- Emergency procedures
- Police, Fire, Medical

Crime Prevention Through Environmental Design - CPTED

- Limited entry points
- Force guests to front desk
- Reduce entry points after hours
- Guard validates photo id
- Guest sign in
- Question Strangers

Windows

- Standard
- Tempered
- Acrylic
- Wired
- Laminated
- Solar Window Film
- Security Film

Static

- Antistatic flooring
- Ensure proper humidity 40 - 60%
- Proper grounding
- Avoid carpeting
- Antistatic bands when working on hardware
- Temperature 50 - 80 F (10 - 26 C)

Security Architecture and Design

Mike Smith

26/04/10 - Rev.28

Common Criteria

- Uses an Evaluation Assurance Level - EAL
- EAL1 - Functionally Tested
- EAL2 - Structurally Tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 - Semi-formally designed and tested
- EAL6 - Semi-formally verified design and tested
- EAL7 - Formally verified design and tested

ITSEC

- Evaluates on Functionality and Assurance
- Functionality rating F1 - F10
- Assurance rating E0 - E6

TCSEC Orange Book

- Trusted Computer Systems Evaluation Criteria - TCSEC
- A - Verified Protection
  - A1 - Verified Design
- B - Mandatory Protection
  - B1 - Labeled Security - Objects are classified
  - B2 - Structured Protection
  - B3 - Secure Domains
- C - Discretionary Protection
  - C1 - Discretionary Security
  - C2 - Controlled Access - reasonable commercial apps
- D - Minimal Security
  - Evaluated but fail

Issues

- Covert channels
- Race conditions
- Emanations
- Maintenance hooks
- Countermeasures
  - Reveal as little as possible
  - Limit access - need to know
  - Disable unused services and accounts
  - Use strong authentication

Terms

- Trusted Computer Base - TCB - the total combination of protection mechanisms within a computer system, including hardware, firmware and software to enforce security policy.
- Access Control - ability to permit or deny the use of an object by a subject
- Reference Monitor - system component that enforces access controls on an object
- Security Kernel - hardware, firmware and software that implement the reference monitor concept
  - Mediate all accesses
  - Be protected from modification
  - Be verified as correct

CPU Components

- Arithmetic Logic Unit - ALU - Performs computation
- Bus Interface Unit - BIU - I/O to CPU
- Control Unit - Coordinates other CPU components
- Floating Point Unit - FPU
- Memory Management Unit - MMU
- Pre-Fetch Unit
- Protection Test Unit

CPU States

- Operating (or Run)
- Problem (or Application)
- Supervisory - Privileged Instruction
- Wait

OS Terms

- Multiprogramming - can load more than one program in memory at one time
- Multitasking - can handle requests from several different processes loaded into memory at the same time
- Multithreading - can run multiple threads simultaneously
- Multiprocessing - has more than one CPU

Access Control Models

- Bell-LaPadula
  - 1973 - First formal confidentiality model
  - State-machine model
  - Simple security property - no read up
  - * property - no write down
  - Strong star property - subject's = object's clearance for RW
  - Discretionary property and trusted subject
- Biba
  - 1977 - First integrity lattice based model
  - Simple integrity property - no read down
  - * integrity property - no write up
- Clarke-Wilson
  - 1987 - commercial, e.g. banking
  - Unconstrained Data Item - UDI
  - Constrained Data Item - CDI
  - Integrity Verification Procedures - IVPs
  - Transformation Procedures - TPs
- Access Matrix
  - Object access rights to subjects
- Take Grant
  - Rights a subject can transfer to/from another subject or object
  - create, revoke, take, grant
- Information Flow Model
- Noninterference Model
- Brewer and Nash Model - dynamically changing access controls
- Graham-Denning Model - How subjects and objects should be created and deleted - access rights
- Confidentiality - Bell-LaPadula, Access Matrix and Take-Grant
- Integrity - Biba and Clarke-Wilson
- Three goals of integrity
  1. Prevent unauthorized modifications
  2. Prevent authorized users from improper modifications
  3. Maintain internal and external consistency - well-formed transaction