Prof. N.R. Ganbote
New law college Ahmednagar

INTRODUCTION TO CYBER SECURITY / INFORMATION SECURITY

L.L.M. II YEAR SEMESTER IV MODULE 4 SYSTEM AND APPLICATION SECURITY.

CHAPTER : - I " SECURITY ARCHITECTURE AND MODELS "

1. Designing Secure Operating System

2. Controls to enforce security services.

3. Information Security Models .

CHAPTER :- II " SYSTEM SECURITY "

1. Desktop Security.

2. email security. PGP and SMME.

3. Web Security . web authentication.

4. SSL AND SET. Database security.

CHAPTER :- III " O.S. SECURITY "

1. O.S. Security Vulnerabilities , updates and patches.

2. O.S. integrity checks.

3. Anti – virus software.

4 Configuring the O.S. for security.

CHAPTER :- IV " WIRELES NETWORK AND SECURITY.

1. Components of wireless Networks

2. Security issues in wireless

NB :- 1 .This subject is for 25 marks and students are expected to understand basic concepts.

2. Examination Question Paper nature is of multiple choice. (MCQ)

CYBER AND INFORMATION SECURITY MODULE IV

- **SYSTEM AND APPLICATION SECURITY**

SYSTEM

1. A set of things working together as a part of the mechanism or an interconnecting networks e.g. Indian Railways [Hardware & Software].
2. A set of principles and procedure according to which something is done, an organized method e.g. a multi party system of the government.

APPLICATION

An application in computer is application program, is software computer program that runs on your computer. Web browser, email programs, word processors, games, and utilities like sort, so-sorts, spreadsheets, Data Base management, Power Point Presentation etc. are all application. The word application is used because each program as a specific application for the users.

SECURITY

Protection of the computer, its networks and various components from unauthorized access, misuse, and damage.

SECURITY ARCHITECTURE AND MODELS

Describes the components of the logical hardware operating system and software security components and how to implement that component to architect, build, evaluate the security of the computer- systems.

UNIX SYSTEM

/root directories
/ bin - essentials low level system utilities
/user- bin higher level system utilities and application programs – scosort latex.
/sbin super user system utilities.
/lib program libraries.
/user lib program libraries for high level user

/tmp temporary file storage space
/home home directories file

1. <u>Open and close system</u>
    a. Open
        i. Vendor Independent
        ii. Designed and written by outsider
        iii. Subject to review and evolution by outside parties not company insiders.
    b. Closed
        i. Vender Development
        ii. Not typically compatible with others system.

- ❖ Languages (Generation Languages)- *Gay lesbian*
    - ➢ 1GL machine languages
    - ➢ 2GL Assembly languages
    - ➢ 3GL FORTRON BASIC PL/1C etc
    - ➢ 4GL NATURAL, FOCUS, SQL.
    - ➢ 5GL pro logs LISP Other AI Languages
        - ▪ 1GL 10101
        - ▪ 2GL Assembly Languages
- ❖ FORTAN – Formula translation high level programming language.
- ❖ BASIC- Beginner All purpose Symbolic Instruction Code.
- ❖ COBAL – Common Business Oriental Languages.
- ❖ JAWA- Free Software from Sun Micro System.(Indoanasian Islands)
- ❖ FOCUS – Fundamental Operations and Concepts Underlying Schema EXTENDED FOR PC IN 1997 WWW

Computer Architecture
CPU Control Bus
Memory
Cache – Software that stores Data
RAM Random Access Memory
ROM Read Only Memory
DRM Dynamic Random Access Memory
CPU

- ✓ Instructions Cycle Fetch and Execute.
- ✓ Pipelining, CISC it is Router
- ✓ CISC Complex Instruction Set Computer
- ✓ RISC Reduced Instruction Set Computer – Router
- ✓ Multi Tasking
- ✓ Multi Processing
- ✓ Input Output programmed input output
- ✓ DMA Direct Memory Access
- ✓ Interrupts
    - ➢ Security Measures
        - rwe, r: Read; w: writes e: executes
          these are the permissions mapped and available to the users

CORE BANKING SYSTEM (CBS)

It is a SOFTWARE DEVELOP FOR core banking solution and centralized data management.
It includes the net Banking plus mobile banking
Software is developed TCS.(TATA CONSULTING SERVIVES)
UNIT BASED COMPUTER PLATFORM OPERATING SYSTEM.
OS SERVER
HP UNIX developed by FIB'S LAB GERMANY
APPLICATION SERVER : 2X 329000 SUPERDOM

- ❖ RDBMS Relational Database Management server.
- ❖ ORACLE COBOL
- ❖ DATABASAE 2X32 HP ITALIAN CORE.
- ❖ INTERGRITY SERVER

DESIGNING SECURE OPERATING SYSTEM

a) It may refer to security focus operating system.

b) Security evaluated operating system. That has achieved the certification from external auditing organisation. That is system audit.

c) Trusted operating system An os that provides sufficient support for multi level security an evidence of correctness to meet a particular set requirement.

d) Control to enforce security devices.

(1) Data and theft prevention

(2) Media Encryption.

(3) Detailed Forensics

(4) Malware protection

INFORMATION SECURITY MODELS

Types of Access Control

1. Discretionary Access Control (DAC) – data owners cancreate and modify matrix of subject / object relationships
(e.g., ACLs)
2. Mandatory Access Control (MAC) – “insecure”transactions prohibited regardless of DAC Cannot enforce MAC rules with DAC security kernel Someone with read access to a file can copy it and build a new “insecure” DAC matrix because he will be an owner of the new file.

- Access control list (ACL)
- Bell–LaPadula model
- Biba model
- Brewer and Nash model
- Capability-based security
- Clark-Wilson model
- Context-based access control (CBAC)
- Graham-Denning model
- Harrison-Ruzzo-Ullman (HRU)
- High-water mark (computer security)
- Lattice-based access control (LBAC)
- Mandatory access control (MAC)
- Multi-level security (MLS)
- Non-interference (security)
- Object-capability model
- Protection ring
- Role-based access control (RBAC)
- Take-grant protection model
- Discretionary access control

CHAPTER II- SYSTEM SECURITY

DESKTOP SECURITY

1) A personal computer designed for regular use at single location on or near desk or table.
2) Power supply plus motherboard CPU bus disk storage, floppy CD Drive tape drive keyboard, mouse, monitor, printer are component should be consider for desktop security.
3) It may be vertical horizontal
   WINDOWS DESKTOP SECURITY
   LINUX DESKTOP SECURITY
4) Assign a good and difficult password
5) Don’t your enable password option
6) If machine is crack lost change all password
7) Use and update antivirus regularly
   a) Set up automatic updating on regular basis
   b) Schedule virus scan automatically
8) Use good spy removal software
   a) Eg MS Anti spy or spy boat destroyer
   b) Sync, nul rem software
9) Take back up of registry eg run regetit
10) User personal firewall
    a) Norton Internet security
    b) Zone alarm
    c) Spygate personal firewall
11) Secure the cousole password permission network connection
12) Keep system up to date
13) Limit handling restricting services
14) Password protect screen saver to be use

15) Use Xlock and Xaut lock while away
16) Don’t normal log in as root in own machine
17) Machine should kept safe location
18) Set boot hierarchy
19) Restricted Remote Access
20) Set up an idle time out
21) Install tempwatch to delete the unused scrap file
22) Check Unwanted script in
    a) /root
    b) /local
    c) /var
    d) /spool.
    e) /inbox
    f) /mbox

Email Security

Threat to the security of emails itself

- ✓ Loss of confidentiality
- ✓ Loss of integrity
- ✓ Loss of data origin authentication
- ✓ Lack of non repudiation
- ✓ Loss of notification of receipt
- ✓ Denial of services
- ✓ Unauthorized access
- ✓ Disclosure of sensitive information
    a) Active content attack > clean up the servers
    b) Buffer over flow> fix the codes.
    c) Shell script all > scan before send the file
    d) Trojan horse attacks

e) Web bugs

Pretty good privacy (PGP)

All Ips are designed to facilities the secure and smooth flow of data transmission in networking s/m ME and PGP in networking are protocols use for the authentication of internet

- ✓ Widely use secure email software
- ✓ Available on several platform with sources code windows and Unix Linux
- ✓ Originally now free for the commercial used
- ✓ Not controlled by the standardized body
- ✓ Compressions by using zip
- ✓ Ready 64 conversions

Web Security

1. Almost everyone is relied on computer and internet.
2. Communications (e mails and cellphones)
3. Transportation (airplanes navigations)
4. Medicine
5. Shopping’s
6. Entertainments

Web security also known as the cyber security information by preventing detecting and responding to the attacks

i. Protecting yourself to recognized the risks and becomes familiar with the some of terminology associated with them

ii. Hackers:- people also seek to exploit weaknesses in software and computer system for their own use

iii. Virus: - it infects your computer before you something opening emails attachment to web pages.

iv. Worms: - worms and spreads without user intervention. Once the victims computer has been infected the worms will attempt to find and infect others computers.

v. Trojans Horse:- It is a program , software, that claims to be one thing while in fact doing something while in fact doing something else behind the screen.

Ransomware:

- A form of Trojans that has been around since 1989. It is known as the PC CYBORG Trojans.
- It infects the target computer by encrypting the owner's personal files.
- The victims is then contracted and offered a key to decrypt the files in exchange of cash
    - Key logger
        - Traditionally key loggers are software that monitors user activity such as keys typed using keyboard.
        - Modern key logger can
            - Record keystrokes on keyboard
            - Record movements and click
            - Record menus that are involved
            - Takes screenshots of the desktop at predefined interval such recorded data could be uploaded in real time when internet connection is available
                - Email attachment
                - IRC Channel
                - FTP
- Prevention
    - Use in anti spyware prevention
    - Firewall manual detection
    - Automatic form filler
- Firewalls
    - Mechanism that content the regulation and data filtering
    - Blocking unwanted traffic entering sub network
    - Preventing Sub network user of unauthorized material
- Aspect of Security

  - Privacy> Keeping your information private
  - Integrity> Knowing that your information not been changed
  - Authenticity> knowing who sent the information

- Malicious Websites
  - China – 67 %
  - USA – 15%
  - Russia – 4%
  - Malaysia- 2.2%
  - Korea – 2%
- Prevention measures
  - Use latest browser software
    - Internet Explorer version 7.1
    - Mozilla Firefox
    - Opera
  - 419 Nigerian Scams
    - An advance free fraud is a confidence trick that target is persuaded to advance sums of the money is a hope of realizing a very much larger gain. The 419 refer to the article Nigerian Criminal Code cheating dealing with the fraud.
- Phishing
  - Usually achieved by creating a website identical to a secure site
  - User is sent email requesting them to log in and provide a link to bogus sites
  - When user login password in stored and used to access the account by the hackers
  - Difficult to guard against particular is using Html Emails

- Authentication
    - It is the process in which the credential provided are compared to access files in a data base of the authorized user information on a local operating system or server. If the match process successful user id granted authorisation access.
    - Web Authentication
        - Authentication is a relatively very simple
        - User provide some sort of credential a password a smart card fingerprints digital certificates- which identifies that the user as the person who is authentication and authorised to access the system. There are many methods where the SSL and set methods are in the syllabus.
    - SSL (Secure Sockets Layers)
        - Protocol for the internet standards
        - Often use to access the websites
        - Using the combination of the public key technology and the secret key technology
        - It is supported by the major browsers
- Database Security
    - Data is the most valuable assets
        - Security of the data is great challenges
        - Privacy
        - Various security layers
        - Security can be breached at any time of those layer by any hackers
        - Three types of attacks
            - Intrudes
            - Insider
            - Administrators

- Default or weak password
- SQL injection structured query language
- Excessive user and group privileges
- Broken configuration management
- Buffer overflow
- Privileges escalation
- Denial of services
- Un-patched RDBMS
- Unencrypted Data
    - Steps
        - Isolate Sensitive Database
        - Eliminate vulnerabilities
- OS security Vulnerabilities
    - In computer security a vulnerabilities is a weakness which allows an attacks reduces system information assurance
        - Three element 1. System susceptibilities or flows
        - Attackers access to the flows
        - Attacker capabilities to exploit the flow
    - File and share permission that give up everything to anyone
    - Lack of personal file protection
    - Weak of personals file protection
    - Weak or nonexistence drive protection
    - No minimum security standards
    - Misusing the patches of windows and as well as third party software
    - Weak windows security policies
    - Unaccounted for systems running unknown and unmanaged services

  - Weak passwords
  - Device weakness

Operating system	Vulnerabilities
Apple OS	384
MS Windows Server	155
Ubuntu	152
MS Windows 8.1	151
MS Windows 10	53
Fedora Linux	38
Xen	34

- Updates and Patches
  - If your computer seems to be working fine, you may wonder why you should apply a patch
    - By not applying patch you might be leaving the door open for the malware to come in.
    - Malware exploits flows in the systems
    - Defect in client like web browser email program image viewers messaging software many allows malicious sites.
  - Top 10 safe computing tips
    - Patch patch patch
    - Install the protection software
    - Choose strong password
    - Backup
    - Control access to the machine
    - Use email and internet security
    - Use secure connection
    - Protect the sensitive's data.
    - Use desktop firewalls
    - Stay informed

- Protecting Data
    - Data security fundamentals
    - Plan ahead
    - Know what data you know
    - Scale down the data
    - Lock up

Software updates occasionally referred to as the patches are released for the variety of reasons

- Sometimes the patch will update the piece of the software to the latest version with new features in the software
- Sometime and update will improves an application stability
- Updates is issued to fix big or security hole in the program
- Security researchers have shown that installing system and software updates is the best defence against most common viruses and malware.

- **<u>O S Security checks</u>**

  Operating system security by Integrity checking and recovery using the write protected storage

    - ICAR system which protects the file system integrity and auto modified files
    - The system enables the files cryptographic hashes generation and verifications as well as configurations security constraints
    - All of the crucial data including ICAR system binaries file backup and hashes database are stored in a physical form write protected storage to eliminate the threat of unauthorized modification
    - A buffering mechanism was designed and implemented in the system to increase the operation performance.

- Additionally, the system supplies user tools for the cryptographic hash generation and the data base management of the system.
- The system is implementation as kernel extension compliant with the Linux security model

CHAPTER IV

Wireless Network & security component of wireless networks AP Access point

Wireless network use

- AP >Access Point
- WAP > Wireless Access point

  To provide a gateway to the wired network

  A wireless local area networks adaptors (WLAN) to provide link between a wirelesses client PC and the AP.

  Access Points (AP)

  - ➢ Connects to wired networks or directly to a cable/ DSL Model
  - ➢ Modem DSL Cable Modem
  - ➢ DSL provides wireless links to many wireless adapter
  - ➢ 32 or 64 wireless adapter to be connected simultaneously
  - ➢ Connection depends upon wireless bandwidth provided by the wireless adapter i.e. bps 54m/s or more.

- If only one wireless adapter is transferring data at a particular moment gets the full available bandwidth

- If several adapters are transferring data simultaneously the available band width is shared among them

- For excellent transmission using wired networking or 802.11 a wireless networking connection is recommended

Wireless Adapter

PCI – For the desktop system

Card Bus- For Notebooks

PCMCIA – People can’t memorizes computer Industry Acronyms Card Adapter

USB – for any system

Like Aps, PCI, and USB wireless are supplied a low gain, therefore Omni directional rubber duck antenna that can usually be replaced with an external high gain or unidirectional antenna

Dlink – Air plus Extreme DWL –G52Q which was typical PCI wireless adapter some adapter such as Proxim Orinoco cards include an external antenna port

Transmitter power, Receiver Sensitivity, and Antenna Considerations

The range of wireless connection an many factors

1. Its speed
2. Amount of interference
3. Obstruction in signal path
4. Types of antenna used
5. Powerful transmitters
6. Sensitive’s receivers

<u>Transmitter power</u>

It is stated in DBM and many range from o dbm

❖ Wireless devices may be fixed transmission power

- Set up transmission power dynamically under firewall control
- Or allow the transmission power depend upon the distance between the devices sensitivity of the receiver the data rate of the link
- The amount of the destruction is the signal path distance higher data rate transmission power

Receiver Sensitive

The flip side of the transmitter power is receiver sensitivity. All other things being equal, a more sensitive receiver can sustain a connection with a weaker signal than lower sensitivity. A sensitive is a very important as powerful transmitter because signal strength drop rapidly with the increasing signal from the transmitter and higher because of the data rate require strongly. It always recommended going for Dlink DWL 2100 AP which as excellent receiver sensitivity.

Antenna Considerations

The most mainstream wireless component is supplied with the standard rubber duck antenna is usually as Omni directional.

Types

- Antenna oriented vertically to maximize horizontal coverage's

- ❖ Antenna titled to provide additional vertical coverage at the expenses of horizontal coverage’s
- ❖ Antenna titled to provide additional front to rear vertical coverage at the expenses of horizontal and vertical right to left coverage
    - o The wireless environment
        - ▪ IT is to be appropriate
        - ▪ Appropriate networking
        - ▪ Hybrid network

Wireless Component

1. Provide temporary connection to an existing cable network
2. Help to provide backup to existing network
3. Provide some degree of portability
4. Extent network beyond the limit of physical connectivity

USES FOR WIRELESS NETWORK CONNECTIVITY

1. Useful for busy locations such as lobbies and reception area
2. User who are constantly on the move, such as doctors and nurses in hospitals
3. Isolated area and building
4. Department in which the physical setting changes frequently and unpredictable.
5. Structure such as historic buildings for which is greatest challenges.

- Types of wireless network
    - LAN
    - Extended LANS
    - Mobile computing

LAN –

- Extended LANS
- Use transmitters
- Receivers owned by the company
- In which the networks operator short distances

Mobile Computing- Used public carrier long distances company along with local telephone company and their public services to transmit and receive signals

LANS Wireless networks interface card with transceiver.

Access point

Transceiver sometimes called as Access point broadcast and receiver signal to and from the surrounding computer and passes the data packs and forth between cabled network and computers.

Wireless portable computer connecting to a cable networks access point wireless LAN us for the four techniques

1. Infrared Transmissions
2. Laser Transmissions
3. Narrow Band radio transmissions
4. Speedy Spectrums radio transmissions

Infrared Transmissions

- Infrared light beam to carry between the devices
- System need to generate strong signal broadcast at 110 MPS
- Line to sight networks
- Reflective Networks
- Broadband optical telepoints (High quality multimedia)

Laser Transmission

Laser beam for blocking transmission X rays

Narrow Band (Single Frequency) Radio Transmission

FCC- Federal Communication Commission

Spread Spectrum Radio Transmission

Point to point transmissions

Security Aspects

Division a verified protection

- Formal method are use to verified subjects and objects
- Are controlled is necessary discretionary and mandatory access controlled
- The design, development, implementation, documentation are locked as in a formal detailed way
- The way that the verified system was designed and developed is evaluated is a much more structured and stringent procedure

A1 Verified Design

- ❖ More stringent change configuration is put in place with the development of AI system and the overall design can be verified
- ❖ TCB The Trusted Computing Base specification and the security policy model
- ❖ In many cases, even the way that the system is delivered to the customers under security to ensure that there is no way of compromising the system before it reaches destination
- ❖ An Environment deals with top secret information and cannot adequately trust anyone using system without strict authentication, restricting and auditing.