Information Security can be classified into two sections:

1. Information/ Information Seccurity
2. Information Security risks and management
3. **Information Security:**

CIA ->

Confidentiality: Information is kept private and secret

Integrity: Then sent information is not tempered.

Availability: Who can access

Contrability: Control over the information. Ex: Delete, archive etc.

Non-repudiation: People can not deny

Wannacry Ransomeware

OceanLotus

1. **Information Security risks:**  
   Physical, Netowork, System, information, Application, Managemnet, Others

Management Risks:

National, Enterprise, Management System

Current development of security management:

Information Security plan and strategies

Strengthening legislation

Standardization (ISO/IEC)

**\*\* Information Security Standardization**

ISMS -> Intenational Security Management Standardization

Plan -> Do -> Check -> Action

**1.3 Basic Network Concept**

Architecture of typical Campus network: Access Layer - > Aggregation Layer -> Core Layer -> Egress layer

OSI -> Open System Interconnect Standard model

TCP/IP MODEL

1. Network Access Layer
2. Internet Layer : ICMP, SNMP, (ARP, RARP)
3. Transport Layer (TCT : Connection oriented, UDP: Unreliable/Streaming/Skype)
4. Application Layer : HTTP/Telnet/Tftp/FTP/DNS

Full Data: (Eth)(IP)(TCP)(App)(User Data)

Network Layer Protocol:

ARP : Address Resolution Protocol. How A host gets the mac address of a desired host -> Operation type = request

Gratuitious ARP: Use to detect IP Address conflict. Confliction detected -> Temporary IP Address (APIPA -> Automatic private IP Address Assignment)

ICMP : Internet Control Message Protocol. (Transmit error, control, query ) (application - > ping, tracert)

Routing Protocol : OSPF, (SNMP -> Simple Network Management Protocol -> Mechanism to talk to NMS (Network Management System. Is a software can be installed on server. Example : eSight) ). MIB - > Management Information Base. =🡺 MIB-> Agent -> NMS through SNMP, UDP(Port -> 161 )

The eSight Network Traffic Analyzer(NTA)

No external hardware probe. Netflow, Netstream, sFlow protocol to analyze common IP Packets

NetStream - > Huawei patented to collect and distribute statistics about network traffic NDE(netstream data exporter) to NSC(Netstream Colector) to NDA(Netstream Data Analyzer)

Transport Layer Protocol:

TCP: (Transmission control protocol) (Connecting -> Three way handshake) (Disconnecting -> Four way handshake)

Application Layer Protocol:

DNS: From right to left ([www.ex.com](http://www.ex.com) -> com -> fist level. Ex-> second level) (Client -> Cache -> (Root, Top-level, Recursive))

FTP: (Two channels -> Control(port 21)/Data(port 20))

Two Modes(Active -> client Setups control connection and Server setups Data connection, Passive client setups both)

HTTP/(s) : Stateless Protocol. Address Resolution -> Hello msg -> Get Request -> Key Sharing -> Get response . (Request and response packet)

SMTP: (Simple Mail Transmit Protocol) How mail sent from client to server. MX record to get IP. Scan email

POP3 : Post Office protocol. How mail downloaded to server

IMAP : Internet mail access protocol. Receiving mail from sever to client

1.4 Common Network Devices

NGFW -> Next Generation Firewall. NIP -> Network Intrusion Prevention. DMZ -> exposed to the internet. Web/mail server…

Switch : Data link Layer. Forwarding -> (Flooding, Forwarding, Discarding(Source destination same, different vlan, policy violation, authentication failure))

Routers:

Firewall : Filtering DDos attach, Trojan horse attack, Checking authentication. Control the packet to permit or deny(to/from internet)

1989 Access Firewall: IP filtering firewall. But Sources IP could be faked.

<1994 proxy technology: Scanning before downloading page to Internet explorer. Very few applications that can understand proxy technology

1995 Session mechanism: Check if the same session for the both outgoing request and incoming response packet.

>1996: Dedicated all integrated filtering

2004: UTF(Unified Thread management) All in single appliance -> VPN Web filtering, mail filtering, bit of IPS, intrusion detection/prevention, entity of network translation and packet filtering

2005: Deep packet Inspection Technology(DPI) A lot different types of traffics through same HTTP Protocol

2009 Control based on user + application + content

Zones : Trust Zone(LAN), Untrust Zone(Internet), DMZ

Same physical interface cannot have the two security value

VRP: Versatile Routing Platform -> Operating System.

CLI -> Userview <> This symbol. Viewing files directories loading , saving configuration files

To System View -> “system-view” symbol -> []

Interfaceview - > “interface Gigabit 0/0/1” ip address, switch port, vlan configuration, port access type, trunk

Protocol View -> “ISPF 1” “RIP 1”

Configuration Interfaces:

Device Login System : Console, Telnet, SSH, Web

It is recommended to use SSH instead of Telnet because of missing auth

Telnet:

“stelnet server enable”

“service-manage enable”

“service-manage ssh permit”

=========================

system-view

rsa local-key-pair create

user-interface vty 0 4

protocol inbound all

authentication-mode aaa

aaa

manager-user username

service-type ssh

password cipher password

1.5 Common Information Security Threats

Stuxnet: Primary target SCADA system(controls everything within plants) Computer worm(multiplied from one machine to another)

Form of attacks largely unchanged : phishing, viruses, vulnerability

Security Threats Categories

1. Cyber
   1. DDos : 2016 USA almost paralyzed half system.

Mirai malware forced IOT devices to do attack.

* 1. Network Intrusion
  2. Scanning : Scan connected devicese through ICMP (ping), Then scan ports specially telnet
  3. Spoofing attack: Brute force password. Then take control and sniff

Defense:

Firewall, Anti-DDos

1. Application
   1. Os
   2. Viruses
   3. Phishing : Weibu worm attack
   4. Data breach
   5. Injection, XSS, Malicious Code, Data breach

Defense : Regular vulnerability checking, Patching

Awareness

Firewall waf antivirus

1. Data Transmission and Device
   1. Communication traffic hijack
   2. Man in the middle (ARP Spoofing)
   3. Unauthorized
   4. Weak protection

Defense : No PPTP. SSTP

1.6.1 Threat Defense and Information Security Development Trends

1. Security Awareness

2. O&M and management

3. Security products and tools

Wall of sheep ->

Gartner 10 security technologies:



Future development Trends:

SECaaS -> Security as Service, End point detection, Traffic control, Software defined security protection solution.

Huawei third generation sandbox -> deep neural network based security

3.1 Introduction To Firewall

Classification:

1. Packet Filtering
2. Proxy
3. Stateful Inspection : TCP/UDP Session checking

==

1. Layer 2 Firewall : stays transparent
2. Layer3 : Work as a router. Supports NAT(Network transalation,) UTM(Unified threat management)

Firewall security policy is a set of rules.

Principal of firewall forwarding:

Core techneology of packet filtering is ACL(Access Control List)

Quering and Creating Session

Session Table is created based on the first packet. The first packet goes following the rules.

“display firewall session table”

“display firewall session table verbose” (for in details)

Security Policy Matching Check :

Traffic -> Condition -> Action -> (Response , Profile)

Security policy configuration process :

Start - > (Create Zone) - > Configure Interfaces - > configure User and Authentication -> Configure Objects -> Create Profiles -> (Configure the Security Policy) -> (Save and Commit)

ASPF -> Application specific packet filtering -> Used for multichannel protocol filtering. Will monitor three way handshake. Incomplete connection will be rejected

Server Map Table Generated on four condition:

1. Forward traffic of multi channel protocol -> Multicahnnel protocol
2. Static entries henerated in case of NAT configured
3. Triplet Server map -> STUN Protocol
4. Dynamic -> NAT to PAT

Fragment cache function is used to cache fragment before the first fragments

“long-link” -> persistant session

3.2 NAT -> Network Address Translation

Translates private ipv4 address to public address

IPSec VPN encrypts info of the packet headers

Categories ->

1. Source NAT -> Address pool mode , Outbound interface address mode(Easy IP)
   1. Address pool mode (1) No port. Limited internal connection
   2. Address pool mode (1) port. internal connection -> Individual port
   3. Easy IP -> dynamic outgoing single IP. Port same as apm 2
2. Server mapping -> Static mapping (NAT server)
3. Intrazone NAT -> Twice NAT
4. NAT ALG -> Translation information in application layer data

3.3 Dual System hot standby

Redundancy deployment solution for Routers (VRRP -> Virtual router redundancy protocol)

To ensure switch over between VRRP lets introduce (VGMP -> VRRP Group Management Protocol)

HRP -> Huawei Redundancy protocol -> backs up dynamic status data. And some of the key configuration commands between the firewalls. Doesn’t backup IP. But session table dynamic black list etc.. shares backup data through the heartbit interfaces/ heartbit links. Shares HRP data packets

Heartbit interface has five states:

1. Invalid
2. Down
3. Peerdown
4. Ready
5. Running

Backup modes of hot standby:

1. Automatic
2. Manual Backup
3. Quick session backup
4. Automatic Sync of Fw configuration after restart

3.4 Authentication

User Classification:

1. Administrator -> Console, Telnet , SSH, FTP, Web
2. Internet access user
3. Remote access user

SSO -> Single Sign-on

AD SSO -> Receiving messages from the user pc

Portal Authentication for Internet access user:

1. Redirect Authentication
2. User-initiated authentication

Remote Access user authentication

1. SSL VPN
2. L2TP VPN
3. IPSec VPN
4. PPPoe

Possible firewall authentication are below:

1. Portal Authentication
2. Authentication Exemption
3. No Autnetication
4. SMS Authentication

3.4 User management and Authentication:

Authentication:

1. What I know: password
2. What I have: bank credit card, token card, smart card
3. What I am: biometric, dna

AAA Technology: Local Auth, Server Auth, No Auth

Third party authentication : LDAP, AD, RADIUS => Remote Access Dial in User Service. Client server based auth system, access remote access to server. Uses AAA, UDP

(Username & pass)( client) => USG => RADIUS SERVER

Acces Req(USG), Access accept(RADIUS Server), Accounting Req(USG), Accounting response(RADIUS), Accounting stop(USG), response(Radius)

HWTACAS(Third party auth) => Huawei Terminal Access Controller Access control system (older). Communication between User, USG, Server, Every message through USG

Comparison HWTACAS, RADIUS:

1. Port : uses TCP, UDP port 1812|1813 or 1645|1646
2. Encrypts everything except header, only encrypts password
3. Auth and authorization separate, Together
4. Applies to security control, accounting
5. Supports authorization of control commands,

LDAP: Lightweight Directory Access Protocol, open vendor-neitral industry standard protocol. Originated from X.500 (tree structure)

DIT -> Directory information tree (Collection of directory entries)

Entry

RDN -> Relative Distinguished Name -> a child entry

DN -> Distinguished Name -> Uniquely identified and entry

AAA Auth -> User auth -> user management

Firewall(USG) everything including binding and handling reply message

Auth classification: Local, Server, SSO, SMS

Authentication domain is environment for the user organizational structure => Microsoft Active Directory(AD)

Every user belong exactly on parent group

User Clasification : Administrator => Telnet, SSH, webftp, console,

Internet access user, Remote access user => Through VPN

Auth type => Local, Server, both

Authentication process :

SSO => single sign on => Kind of session. Use single sign on and access multiple services

AD SSO: Quering security logs from the AD Server, Receive message from user pc,

User, AD Server, AD Monitor and firewall all are connected through ha switch. Firewall process the final authentication process

User => AD Domain Controller => Monitor => Firewall

Portal Authentication for internet access user:

1. Redirect Auth : Redirect when user tries to access HTTP Service
2. User-initiated auth: proactively access auth web pages before accessing the contents

Remote access user:

1. SSL:
2. L2TP,
3. IPSec,
4. PPPoE

An authentication policy takes effect on the following authentication mode : Redirect, User initiated, Excemption, SSO

Policy: Firewall will check packets based on different param. Possible param: zone, address region. Possible actions: portal, excemption, no, SMS

RADIUS Server : 1812 for auth. Port 1813 for accouting

User information stored in csv or dbs

4.5: Intrusion Prevention:

Network Threats : Hacker intrusion(Unauthorized access, tempering, Damage), DDos(Access, damage), viruses and malware(access, tempering, damage)

DDos : Botnet => Syn Flag, UDP Flood, ICMP Flood, C&C attack(Control catch => keep searching), Smurf(not popular anymore. Broadcast ping)

Virus : spyware Trojan horse, worm

Intrustion detection(camera), Security hardening room, Security management center(Monitoring room), Door firewall, Access control system(card, fingerprint), Security Guard(Scanner, vulnerability search)

IPS:

1. Offline: port mirroring through switch
2. Inline: in serial to block realtime

IPS features: Realtime blocking, Zero configuration to go online, Service awareness, User defined rules, Self learning and adaptation

Computer Viruses and malicious code:

|  |  |  |  |
| --- | --- | --- | --- |
| Items | Virus | Worm | Trojan horses |
| Replication | Insert into host | Self | Not self replicate |
| Existence | Parasitic | Independent | Parasitic |
| Means of infection | Running on host | System vulnerability | Based on carries function |
| Infected target | Mostly local files | Other computers on the network | Zombie host |
| Triggering mechanism | Computer user | Programs | Remote control |
| Affected target | File system | Network, system performance | Information theft, dos |
| Prevention | Removing from host | Patching | Preventing implementation |

Antivirus technology:

1. Single device antivirus
2. Network

Sysinternal => To know more

Modes of gateway antivirus:

1. Proxy scanning mode: If virus detected throw to
2. Flow scanning mode: File signature are extracted. Based on stateful

Response action:

1. Alert
2. Block
3. Declare: email
4. Delete attachment: email

4.1 Encryption And Decryption Algorithm:

Development -> Scytale -> Cease cipher -> fense cipher-> cipher machine

Digital Envelope

Symmetry cryptography:

Stream : RC4

Block cipher : DES, 3DES, AES, IDEA, RC2, RC5, RC6, SM1, SM4

Asymmetry: DH, RSA, DSA

Hash Algo: MD5, SHA, SM3

DIGITal Certificate signedby trusted third party CA -> Certificate authority

Certificate type :

1. Self-signed certificate
2. CA Certificate
   1. Issuer -> CA
3. Local Certificate
4. Local Device certificate

Structure: version, serial number, algorithm, issuer, validity, subject name, subject public key info, extension, signature

Certificate Format :

PKCS#12 -> w/o private keys in binary format .PN12, .PFX

DER -> without private keys in binary .DER, .CER, .CRT

PEM -> w/o private keys in ASCII format .PEM .CER .CRT

PKI -> Public Key Infrastructure

PKI consists of -> End entity, CA(Certificate authority), RA(Resgistration authority), database

If RA Available -> RA, not available -> CA.

Revocation => when expired.

When password forgotten=> revoke + Issue new one

PKI lifecycle:

Application(EE) -> Issue (CA)-> Storrage (CA)-> download (EE)-> installation 🡪 Authentication -> renewal -> revocation

PKI generated pair of private and public key

Applications -> VPN, IPV6, HTTPS login, System login auth

PKI Authentication center(peering): Request CA Certificate, Return CA Certificate, install, Send public key and entity information, Issue local certificate after validation is passed, Install local Certificate, Verify peer local certificate

Use case: HTTPS, IPsec vpn, SSL Vpn(Client to site)

4.3 Application of cryptographic techniques:

PKI ensures the validity of a public key

1. Digital envelope
2. Digital Signature: Trust, Hash
3. Digital Certificate: Integrity, Non-repudiation

Application: VPN, ipv6, https login, system login authorization

Qos -> Quality of services.

Category of vpn:

1. Layer 2: PPTP , LTF, L2TP -> Not used now
2. L3 : GRE, IPSec
3. Transport layer: SSL VPN

Application:

1. Site to site: IPSEc, L2TP, L2TP over IPsec, GRE over IPSec, IPSec over GRE
2. Client to site: SSL, IPSec, L2TP, L2TP over IPSec

L2TP: Layer 2 tunneling protocol => user and enterprise server

1. NAS(Network access service) initiated VPN
2. Automatic dialing on the LAC(L2TP access conectrator): dialing
3. Client initiated VPN: Client on a trips. Access from phone pc. PPP + L2TP encapsulation.

|  |  |  |
| --- | --- | --- |
| Client | SCCRQ(Start control connection request) : LAC Chap Challenge => | LNS |
|  | SCCRP (Reply): LNS CHAP Response <= |  |
|  | Verification success => |  |
|  | SCCCN(Connection) LAC Chap response => |  |
|  | Verification succeeds <= |  |
|  | ICRQ => |  |
|  | ICRP <= |  |
|  | ICCN (PPP Negotiation parameter) => |  |
|  | Authentication success (PPP Connection establish. Get IP) <= |  |
|  | The user access internet resource ⬄ |  |

GRE => General routing encapsulation. Can transmit IPX, IP, Appletalk(heterogeneous network)

Security zones : untrust(5), trust(85), DMZ(50), local(100)

IPsec -> IP Security ESP|AH, Encryption -> DES, 3DES, AES, SM1/SM4, Authentication: MD5, SHA1-3

IPSec SA(Security Association).

Encapsulation in Transport mode:

Encapsuation in Tunnel Mode -> New IP Header is added outside for public routing

IKA SE -> Automatic key negotiation: UDP Port 500

IPSec sender -> IP Packet -> Encryption Algorithm -> Encrypted packet -> Authentication Algo(HMAC) ->

HTTP -> SSL -> TCP

SSL VPN Products:  
 SVN Security gateway, USG Series device

User authentication, File sharing, Web proxy, Port forwarding, Network extension

VPN Configuration:

LNS -> L2TP Network Server.

Configure LNS(Firewall) -> Enable L2TP -> Configure the VT interface(Set the IP, sepecify the address of service domain, Configure PPP Authentication, Add interfaces to security zone) -> Set the L2TP Parameter(peer name, tunnel auth, enable virtual forwarding) -> Configure the LNS authentication solution -> Configure the security policy ->

VPN Client -> Seco Client

GRE VPN Configuration procedure:

Configure the GRE Device -> Perform basic configuration(Set interface IP Addresses, add security zone) -> Set the tunnel interface(Set ip addresses, set the tunnel protocol, set source destination tunnel, add security zone) -> Configure route to the peer -> Configure the security policy ->

Point to Point IPSec VPN :

Configure point to point -> conf. route to the peer -> conf. intrazone security policy -> conf. IPSec/IKE Security proposal, Configure and apply IPSec policy ->

5.1 Security Operation:

Basic operation condition:

1. Business Continuity planning(BCP)
2. Physical security
3. Managing security operation
4. Incident prevention and reponse
5. Disaster recovery plan
6. Investigation and forensics

End point management -> Anti virus

CERT -> well known response team.

BCP Basic steps: Project scope and plan prepation -> business impact assessment (priority determination, risk identification, possibility assessment, impact assessment, resource priority)-> Continuity planning preparation(policy development, plan implementation, preparation and handling, training and education, planning approval) -> BCP documentation

Incident response management : detect -> respond -> mitigate -> report -> recover -> remeditate -> learn

Disaster recovery plan : implamentation recovery policy, execute the disaster recovery plan, test the plan

Investigation

Evidence:

1. Physical
2. Documentary: logs
3. Verbal

Investigation and forensics process : Incident confirmation -> Request for law enforcement -> Evidence collection and presentation -> In person communication -> Filing of law suits

5.2 Monitoring:

Logs -> Network device logs, operating system logs

Log analysis key point:

Who, When Where , How(wired, wireless, vpn), what(Action, device type, resource )

Event ID:

4624: login success

4625: Login failure

4634: Logout success

4672: login as admin

1: Kernl General

4616: Change system time

Log analysis tool: Log parser by Microsoft -> XML, CSV

Security assessment method: Security scan, manual audit, penetration test, Questionaries, Interview Survey.

Port scanning software : Superscan. Nmap. Sparta -> Vulnerabolity scanner.

Burp Suite uses to payloads to scan the vulnerability:

1. Client: XSS, HTTP Header injection, office redirection
2. Server: SQL Injection, command line injection and file search.

Manual Audit: No external software installed

Passive collection:

Packet capture(command, packet capture software(==debugging ospf event)), port mirroring, log

Wireshark: Port mirroring, capture and detect packet

Firewall log format: Binary, syslog, netflow, dataflow

Windowa systems log: System, application, security

5.3 Digital Forensics:

Characteristics of cybercrimes:  
 Professional means, Convert forms, Transactional, Huge potential damage, Many members and lowering ages, complex and diverse motifs

Motifs: Prestige, Trick, Political action, profit, Ignorance, Revenge

Digital evidence: Text, graphs, images, animation, audio, video

Sources of digital evidence: Comminucation, broadcasting tv, computer and network

Characteristics of digital evidence: Fabricated, Shapeless, dynamic and vivid, vulnerable and fragile, diverse, high-tech

Concept of forensics: confirming, protecting, extracting, archiving, presenting court digital evidence

Principal of digital forensics: Timeliness, Continuity, Legitimacy, Integrity, Comprehensiveness,

Process: Protect the scene, obtain evidence, preserve evidence, verify, analyze, trace, present

Software forensics tool

1. Thumbs plus: Image check
2. Hetman uneraser: anti-deletion
3. CD-R Diagonostics: CD-ROM Tool
4. Dtsearch: text search tool
5. SafeBackSnapBack, Ghost and DD: Driver image program
6. DiskScrub: Disk erasing tool
7. Encase
8. TCPdump, Wireshark, Sleuth kit, Argus, Sniffers => Packet analysis and forensics

Evidence preservation Technology: Encryption, Digital envelope and signature, Digital certificate, timestamp

Verify evidence: Relevance, objectivity, validity

Principal of verification: legitimacy, independence, supervision