© 2014 IJIRT | Volume 1 Issue 5 | ISSN: 2349-6002

NETWORK SECURITY IN OSI MODEL

Himanshi Grover
Dronacharya College of engineering
Farrukhnager, Gurgaon, India

Devesh Agrawal
Dronacharya College of engineering
Farrukhnagar, Gurgaon, India

Introduction

OSI (open system interconnection) is reference model for how messages should be transmitted between any two points in a telecommunication network. The OSI reference model defines a seven layers of functions that take place at each end of communication. It is an ISO standard for worldwide communications that defines a networking framework for implement protocols in seven layers.

The main benefits of OSI model include the following:

- Helps user understand the big picture of networking
- Helps user understand how hardware and software elements function together
- Makes troubleshooting easier by separating networks into manageable pieces
- Helps user understand new technologies as they are developed
- Aids in interpreting vendor explanations of product functionality

"In OSI model control is passed from one layer to the other starting at application layer in one station, proceeding to the bottom layer over the channel to next station and back up the hierarchy" i.e. starting at the top layer information is passed to the lower layer until it reaches to the bottom. Once the information reaches to the bottom, which just happens to be the physical medium the information makes its way to destination. When the information reaches the destination it travels up each layer until it reaches the appropriate level for translation. For example an e-mail starts at the application layer or the source and makes its way down the stack, across the wire, up the stack to the destination's application layer. Within the source computer control is passed from one layer to the next. Data travels down the source computer's hierarchy and then up the destination computer's hierarchy. Notice there is no way of skipping a layer, and that the process is a mirror with the next computer.

Each layer can communicate with only the layer above and below it from the above figure it becomes clear that the physical layer can communicate with the data link layer and the medium itself (there is no lower layer for the physical layer)

Each layer is developed independently this allows flexibility and allows development in one layer to progress without delays from other layers. As information passes through each layer relevant information to that layer is attached. This process is commonly known as encapsulation. This encapsulation is how each layer can communicate with its relevant layer at the destination.

Layer one: the physical layer

The physical layer is responsible for the physical communication between end stations. It is concerned with actual encoding and transmission of data in electromechanical terms of voltage and wavelength. The physical layer is critical to data communications it is also the most vulnerable and changeable, not depending upon

the logic and organisation of the electronic world, but on the vagaries of physics.

"It is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in case of digital equipment this possibly constitutes a problem, because remote reconstruction of signals inside the equipment may enable reconstruction of data the equipment is processing".

Physical layer vulnerabilities

- Loss of power
- Loss of environmental control
- Physical theft of data and hardware
- Physical damage or destruction of data and hardware
- Unauthorized changes to the functional environment
- Disconnection of physical links
- Undetectable interception of data
- Key stroke and other input logging

Physical layer controls

- Locked parameters and enclosures
- Electronic look mechanisms for logging and detailed authorizations
- Video and audio surveillance
- PIN and password secured locks
- Biometric authentication systems
- Data storage cryptography
- Electromagnetic shielding

Layer two: data link layer

The data link layer is concerned with the logical elements of transmission between two directly connected stations, it deals with the issue of local topology were many stations may share a common local media. This is the layer where data packets are prepared for transmission by physical layer, the data link layer is realm of MAC addresses and VLANs as well as WAN protocols such as frame relay and ATM. Switch issues such as broadcast and collision domains are the layer 2 concern. It is also realm of wireless protocols such as 802.11 wireless networking.

Layer two switches are also vulnerable to attacks on their virtual separation of segments known as VLANs. Recent vulnerabilities have been found on cisco's automatic configuration of VLAN trunks, allowing hosts that can send 802.11 trunking protocol signalling (an ability that is becoming more and more common in modern operating system and NIC drivers) to negotiate access to multiple VLANs. Cisco provides configurations to disable this behaviour, but the default behaviour is to allow automatic VLAN configuration.

As a newly emergent battleground the threat tend to outweigh the controls on the link layer, with the only strong tools being manual MAC filtering to enforce an explicit layer two policy, and strong network design to minimize exposure from the outset. The inherent design of most layer two communication imposes a layer of involuntary trust.

Link layer vulnerabilities

- MAC address spoofing (station claims the identity of another)
- VLAN circumvention (station may force direct communication with other stations by passing logical controls such as subnets and firewalls)
- Spanning tree error may be accidentally or purposefully introduced, causing the layer two environment to transmit packets in infinite loops.
- In wireless media situations, layer two protocols may allow free connections to the network by unauthorized entities or weak authentication and encryption may allow a false sense of security.
- Switches may force to flood traffic to all VLAN ports rather than selectively forwarding to appropriate ports, allowing interception of data by any device connected to a VLAN.

Link layer controls

● MAC address filtering- identifying stations by address and cross referencing physical port or logical access.

● Do not use VLANs to enforce secure designs, layer of trust should be physically isolated from one another with policy engines such as firewalls between.

● Wireless applications must be carefully evaluated for unauthorized access exposure. Built in encryption, authentication and MAC filtering, may be applied to secure networks.

Layer three- network layer

The network layer is concerned with global topology of the internet work. It is used to determine what path a packet would need to take to reach a final destination over multiple possible data links and paths over numerous intermediate hosts. This layer typically uses constructs such as IP addresses to identify nodes and routing tables to identify overall paths through the network and the more immediate next hop that a packet may be forwarded to. Protocols such as ARP facilitate that process, giving layer two mapping to layer three addresses, and telling layer three what link-layer path should be taken to follow its routing table's indication of appropriate path. In the opposite direction protocols such as IP will identify their higher level layer four transmission protocol such as TCP or UDP in order to direct layer four as how the incoming data should be handled.

Layer three is the last layer that has a rough physical correspondence to the real world. A given host will typically have a single layer three address or single layer three address per interface. Layer three addressing is also used by application to identify resources, using DNS resolution to map a hostname to an address or group of addresses. Layer three protocols often have mechanisms for broadcast or multicast of data to multiple machines in finite or arbitrary scopes.

In filling these many roles, a variety means for attack at layer three become exposed, in the realm of routing, especially public routing situations such as over the internet, most routing protocols have only an elementary level of security two peers may exchange routing information securely but they have no means to validate routes that may have propagated from untrusted parts of network. Attackers can steal the entire network ranges with the right resources allowing further attacks at layer three or above. Techniques have also been developed to abuse broadcast mechanisms, amplifying data into crushing streams of packets that can paralyze a host, often using untraceable spoofed addressing against unsecured third party machines which are turned into unwitting tools for abuse.

The ubiquitous control for layer three is the firewall- when correctly configured it will let only the necessary traffic pass through its boundaries. Encryption and authentication technologies such as IPSEC can be used to more reliably identify the source of IP communications. Routers must have strict policies regarding their exchange of routes and use of reliable means of authentication and communication with their peers.

Network layer vulnerabilities

● Route spoofing –propagation of false network topology.

● IP address spoofing – false source addressing on malicious packets

● Identity and resource ID vulnerability – reliance on identity to vulnerable resources and peers can be brittle and vulnerable.

Network layer controls

● Route policy controls - use strict anti-spoofing and route filters at network edges

● Firewalls with strong filter and anti-spoof policy

● ARP broadcast monitoring software

● Implementations that minimize the ability to abuse protocol features such as broadcast

Layer four – transport layer

The transport layer is concerned with the transmission of data streams into the lower layers of model , taking data streams from above and packaging them for transport, and with the reassembly and passing of incoming data packets back into a coherent stream for the upper layers of the model. Transport protocols may be designed for

high reliability and use mechanisms to ensure data arrives complete at its destination, such as the TCP protocol, or protocols may choose to reduce overhead and simply depend upon the best efforts of lower layers to deliver the data and protocols of upper layer to ensure success to the levels they require such as with the UDP protocol. Transport protocol may implement flow control, quality of service and other data stream controls to meet their transmission needs.

The transport layer is first purely logical layer in the model. It is the primary point where multiple data conversations from or to a single host are multiplexed. Some transport protocols such as TCP and UDP use the concept of port numbers to allow multiple simultaneous conversations between numerous destinations to individual local protocols or applications.

Some of the key vulnerabilities found at the transport layer came from poor handling of undefined conditions. Many transport protocols seem to have been implemented under the belief that they would be dealing with the well behaved communication from both the upper and lower levels -a false assumption in the hostile world of global public internet this means the protocols are subjected to unexpected or deliberately perverse input or handling exploiting the more obscure protocol details and so called impossible conditions and as a result often have unexpected behaviour.

Another vulnerability lies in the use and reuse of ports for multiple functions. This is found quite often in windows arena,where differing functions such as file and print sharing, remote administration, LAN messaging, RPC functions and a myriad and other applications all use a handful of UDP and TCP ports. This overuse of ports make restriction of access at layer four by firewall difficult. If any of the functions are needed, then the firewall ports are opened and in theory most if not all functions that use those ports could flow through unchecked. Most transmission protocols were built with an emphasis on utility and performance. As such they usually do not implement strong controls to validate the source of transmission, or that a packet is a legitimate part of a data conversation. This leads the ability to forge packets that can interrupt and redirect the flow of transmission. Some protocols such as UDP can be travially spoofed and fooled due to a complete lack of sequencing or state at layer four.other protocols such as TCP are more difficult due to their more extensive flow control and integrity checking.

Stronger mechanisms are possible in layer four implementations to make session hijacking more difficult as well. Recent improvements in TCP sequence number assignment based on random number generation rather than arbitrary and predictable sequences have made the blind takeover of TCP sessions much more difficult. The cisco PIX firewall provides a randomized TCP sequence number to traffic it passes as part of its NAT based adaptive security algorithm (ASA) fixing the problem for TCP implementations which are still non random and predictable.

Transport layer vulnerabilities

- Mishandeling of undefined, poorly defined, or illegal conditions

- Differences in transport protocol implementations allow fingerprinting and other enumeration of host information

- Overloading of transport layer mechanisms such as port numbers limit, the ability to effectively filter and quality traffics.

Transport layer controls

- Strict firewall rules limiting access to specific transmission protocols and sub protocol information such as TCP/UDP port number or ICMP type.

- Stateful inspection at firewall layer, preventing out of state packets, illegal flags and other phony packet profiles from entering the perimeter.

- Stronger transmission and layer session identification mechanism to prevent the attack and takeover of communications.

Layer five: Session layer

the session layer is concerned with the organization of data communications into logical flaws .it takes the higher layer requests to send data and organizes the initiation and cessation of communication with the far end host. The session layer also deals with higher order flow control from an application perspective just as the transport layer may control transmission from a network-

oriented perspective and limit the flow to match the available network capacity, the session layer may control the flow up through to the application layer and limit the rate the data enters or leaves that realm based on arbitrary or dynamic limits.

Functions of session layer include

- Virtual connection between application entities
- Synchronization of data flow
- Creation of dialog units
- Connection perimeter negotiations
- Acknowledgments of data received during a session
- Retransmission of data if it is not received by a device

As the session layer deals with the creation and controls of access the higher level applications, the issue of authorization and access is a natural weakness in this layer. Many session layer protocols lack strong protection for their authorization facilities. Protocols such as standard telnet and FTP pass usernames and passwords in the clear, allowing any layer to beneath them to intercept their credentials. Protocols with stronger protection of passwords such as the microsoft implementation of CIFS (common internet file system, used by MS for file and printer sharing) often fall prey to cryptographic or implementation weaknesses in the handling of passwords and authentication.

Secure channels of user and session authentication are essential to private communications. Cryptography technology allows for both the reliable identification of remote parties and the means for protecting the exchange of data from prying eyes. Passwords and other user credentials should be passed and stored in encrypted form to prevent interception or theft. User accounts should have expiration dates based on both usage and fixed time, requiring the update of credentials and reauthorization of access. Session identification may need to be based on a cryptography technology in order to protect sensitive communications in real-time environments.

To prevent brute-force or focused guessing of session credentials, failed attempts can be properly logged and limited to a fixed amount of failures before an account or service is logged out. This approach is a two-edged sword in that legitimate users may be locked out by illicit access attempts either inadvertently or as the basis for a denial-of-service attack. A safer possible approach is to limit connection attempts on a time basis such as only once every 30 seconds, or temporary lockout on failure with a brief enough duration that legitimate user access will recover in practical amount of time, but a brute force attack would be rendered impractical.

Session layer vulnerabilities

- Weak or nonexistent authentication mechanisms.
- Passing of session credentials such as user ID and passwords in the clear allowing intercept and unauthorized use.
- Session identification may be subject to spoofing and hijack.
- Leakage of information based on failed authentication attempts.

Session layer controls

- Encrypted password exchange and storage.
- Accounts have specific expirations for credentials and authorization.
- Protect session identification information via random cryptographic means.
- Limit failed session attempts via timing mechanism, not lockout.

Layer six: presentation layer

The presentation layer deals with the organization of data passed from the application layer into the network. This layer allows for the standardization of the data and the communication of data between dissimilar hosts such as platforms with different binary numbers representation schemes or character sets (for example: ASCII vs UNICODE) presentation protocols typicallly relay upon a standardized data format for use on the network and various conversion schemes to convert from standard format into and out of specific local format. The

presentation layer can also control network layer enhancements such as compression or encryption.

Functions of presentation layer include:

- encryption and decryption of message for security.
- Compression and expansion of a message so that it travels efficiently
- graphics formatting
- content translation
- system specific translation

Vulnerabilities at this layer often originate from weaknesses or shortcomings in the implementations of presentation layer functions. Continuing on the theme of taking advantage of original atmosphere of implicit trust and simple functionality that systems were built in, attackers feed unexpected or illegal input into presentation layer facilities. A recently recognized weakness known as format string vulnerability can also be classified in the presentation layer. Format string vulnerability takes the advantage of applications that use user-supplied information for the basis of input int I/O libraries in such a way that the user supplied data stream could control how the data is transmitted, formatted, or stored in a process of transmission. This occurs due to either direct or indirect use of the user input in the format portions of routines used to process the data.

Cryptographic presentation services can fall prey to weaknesses in their implementation or fundamental design. Many secure web servers use SSL have had subtle bugs in the underlying cryptography of the SSL implementation turn into either theoretical or practical security exploits.

Controls at presentation layer will typically take the form of cautious and untrusting coding practices when using routines and facilities for network and other inter process communication. User and peer input should always be highly suspect, weather the input is received from a remote station or a local user. Cryptography is a fast moving target, and technology and hardware capabilities advance constantly. The cryptographic strength of data protection services in the presentation layer should be selected carefully and reviewed periodically. Many cryptographic protocols have been found to have subtle flaws well after being declared secure, so a process of periodic re-evaluation of crypto solutions is also vital.

Presentation layer vulnerabilities

- Poor handling of unexpected input can lead to application crash or surrender of control to execute arbitrary instructions.
- Unintentional or ill advised use of extremely supplied input in control contexts may allow remote manipulation or information leakage.
- Cryptographic flaws may be exploited to circumvent privacy protections .

Presentation layer controls

- careful specification and checking of received input incoming into applications or library functions.
- Careful and continuous review of cryptography solutions to ensure current security versus know and emerging threats.

Layer seven: Application layer

The application layer deals with high level functions of programs that may utilize the network. occupying the top end of the stack the application layer is the most open ended of all of the layers. User oriented protocols such as naming (DNS, WINS), file transfer (FTP, HTTP), messaging (SMTP, TOC/OSCAR (used by AIM))and access (Telnet, RDP)all fall within the application layer in a more strict interpretation that views even a higher level function as outside the model completely.

Application layer provides the interface for the end user operating a device connected to a network. One of the prime threats at the application layer is the poor or non existent security design of basic function of an application. Some applications may insecurely handle sensitive information by placing it in publically accessible files or encoding it in hidden areas which are trivially displayed such as in html code of web form. The TFTP protocol is extensively used for booting of diskless workstations and network device management, but does not require any sort of username or password authentication to use its file access ability, giving an

intruder possible access to configuration and access information without challenge other than the need to guess file names.

Applications often grant excessive access to resources, allowing unprivileged users excessive access or or imposing inadequate control to prevent the corruption or loss of data.users may provide unexpected input to the application environment,which if not handled properly could lead to crashes or other unexpected behaviour. A malicious user may be able to use bugs and program flaws to attack and gain access to resources or data.

Some of the most prevalent controls at application layer relate to strong design practices in application design and implementation. Applications should make use of secure facilities available to them at lower network layers, carefully check incoming and outgoing data, and assume that communications can and will be subject to attack, requiring the use of strong authentication and encryption to validate and protect data as it travel across the network. Application should implement their own security controls, allowing for fine grained control of privilege to access resources and data, ideally using a mechanism that is straight forward and strikes a balance between usability and effectiveness. On the hardware front intrusion detection systems (IDS) can observe data traffic for known profiles of network activity that can indicate probes for vulnerable applications as well as detecting the presence of undesirable application traffic.

Application layer vulnerabilities

- open design issues allow free use of application resources by intended parties.

- Backdoors and application designs flaws bypass standard security controls.

- Program logic flaws may be accidently or purposely used to crash programs or cause undesired behaviour.

Application layer controls

- Controls must be detailed and flexible but also straight forward to prevent complexity issues from masking policy and implementation weakness standards, testing and review of application code and functionality, a baseline is used to measure application implementation and recommend improvements.

- Some host based firewall systems can regulate traffic by application, preventing unauthorized use of network.

Extending the model: the infosec nine layer model

The seven-layer model is more then enough for network purposes, but when used in the context of information security there are concepts that need organisation that sit outside of the conventional network model. Placing **the user at layer eight** may at first seem counterintuitive-the natural assumption would be that the user would sit at the top of the stack, controlling all that lies below.the experienced information security knows however that a user actions should always be guided by well organized and carefully developed policies.

In keeping with the layer model approach, we can look at the ideal security policy as also being independent of layers below:

your policy should apply across all platforms and applications independent of the specifies of the application and apply and fit with all classes of users, from the anonymous internet user up to the most trusted administrators and officers of the company.

A problem with applying the policy layer at level nine is that it implies control over the user layer that then independently operates within the framework of other layers.layer nine is generally referred as “blinders” layer this layer applies to organisational managers who have already decided, usually with little or no current information, to dictate a previously selected network plans. Proper controls should be implemented to secure these layers.

Conclusions:

We have covered a lot of security implementations in the seven layer model. In the security context the nine layer model can be applied to access both strengths and weaknesses. Just as individual layer examinations gave example of both controls and vulnerabilities . A point of interest that the ISO group developing the OSI model also developed a security model to complement a network interconnect model. this model is orthogonal to the seven layers of the OSI model, however specifying security services and mechanisms such as access control, authentication, data integrity and encryption as mapping

three dimensionally against the OSI network model. ISO leaves the service and mechanism interaction to the implementor, inviting the pick and choose approach that lacks coherence.

In the practical world of networking and security there is a tendency to gravitate to things that work best. most information security practitioners already applies the concepts of model and its terminology is embedded in the industry that surrounds the network and security hardware and software.

References

[1] http://www.infocellar.com/networks/osi-model.htm

[2] http://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377

[3] http://www.giac.org/paper/gsec/3908/layered-security-model-osi-information-security/106272

[4] http://en.wikipedia.org/wiki/OSI_model

[5] http://support.microsoft.com/kb/103884

[6] http://pages.uoregon.edu/joe/nitrd/up-and-down-the-osi-model.html