Advances and Applications in Mathematical Sciences
Volume 20, Issue 2, December 2020, Pages 227-236

A REVIEW OF DIFFERENT VULNERABILITIES OF SECURITY IN A LAYERED NETWORK

PANKAJ KUMAR GUPTA, SHWETA MITTAL, PRAKHAR CONSUL and JITENDRA KUMAR JINDAL

Department of Computer Science
IIMT, Meerut, India
E-mail: Drpkg03@gmail.com

Research Scholar
TMU, Moradabad, India
E-mail: Shwetamittal79@gmail.com

Department of Electronics & Communication
DVSGI, Meerut, India
E-mail: Prakhar.consul@gmail.com

Department of Computer Science
IFTM, Moradabad, India
E-mail: Jindal_jk@hotmail.com

Abstract

The engendering of systems to a massive populace has upgraded the system's simple entry for a greater segment of programmers to abuse. More grounded security strategies, for example, Advanced Encryption Algorithms, proficient confirmation strategy and assurance top to bottom methodology are being utilized to manage these dangers. This paper gives a short review of different vulnerabilities related to every single layer of the OSI Model. Issues identified with the "eighth layer" have likewise been incorporated. The creator proposes to do execution investigation of the aggregate impact of utilizing security systems kept up at all layers of the system.

1. Introduction

Developing slips of digital security in military and non-military systems, an expanding danger of installed malware, digital assaults from negative component and countries has brought to fore the huge centrality of system

2010 Mathematics Subject Classification: 68P25, 68M12, 81P94.
Keywords: Vulnerabilities, Security, Layered Network.
Received May 25, 2020; Accepted August 5, 2020

security. At the same time, the engendering of systems to a massive population has wider ranging availability for a greater area of programmers to perform abusing activities, which is long lasting and being managed by more grounded security techniques and strategies for example propelled encryption calculations, effective validation procedures and insurance inside and outside methodology. Each system chairman guarantees about creating satisfactory safety efforts at the same point. In this perspective on the way that all framework chairman work in an outright manner and handle security arrangements and its suggestions at a few layers of OSI model, the extensive picture builds up a situation, where the source discovers his information crossing through a predetermined encryption process at every single stage/layer beginning from Application layer down to Physical layer and an unscrambling procedure at every single stage/layer at the goal end. This paper makes an intrigue to complete execution examination of the aggregate impact of implementing security components and systems at every single layers of the system for example OSI Layer Model.

2. Material and Methodology the Open Systems Interconnection (OSI) Model and Vulnerabilities

The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a hypothetical model that gives portrayal and institutionalization the verifiable elements of a correspondence framework by isolating it into reflection layers. The model is a production of the International Organization for Standardization (ISO). The model joins comparative correspondence capacities into one of seven intelligent layers. A layer benefits the layer above it and is adjusted by the layer beneath it. The applications and execution areas of OSI Model are wide to such an extent that OSI Layer Model characterizes the manner in which IT industry should edge and propose its systems administration conventions and rules. Right now, layer can banter with the layer above and underneath it.

Each layer is grown autonomously which permits adaptability and improvement in one layer to progress or headway immediately from some other layer. As data navigates each layer, indicated and significant data from that layer is connected-this system is normally known as

Encapsulation. Following is the concise diagram of different vulnerabilities associated with each layer.

2.1 Physical Layer Vulnerabilities:

These comprise of Disconnection of Physical Data Links, Dissemination of Power, Dissemination of Environmental Control, Keystroke and Other Input Logging, Physical Damage or Destruction of Data and Hardware, Physical Theft of Data and Hardware, Unauthorized changes to the utilitarian condition (including and excluding assets, information associations, separable media), Undetectable Interception of Data. The security issues end up being increasingly noticeable when the system depends on a remote media. A relatively predominant transmission at comparative frequencies can easily impact the nature of administration; if not completely discredit the support of the client. The likelihood of uninvolved, dormant and backhanded assaults on remote media is extremely high as it is progressively defenseless against block attempt.

2.2 Data Link Layer Vulnerabilities:

A gadget proceeding with its activity in indiscriminate mode and a bundle channel could be steady or harming instruments at OSI Layer two. Permitting stream examination, issue assurance and code troubleshooting can be valuable. Be that as it may, in inappropriate hands the capacity to duplicate datagram's represents a risk. A case of a layer two risk is Libpcap, a parcel limit driver that powers a NIC into salacious mode, permitting it to assimilate traffic fated to different machines. Different known dangers at layer 2 are:-

- Address Resolution Protocol (ARP) assault
- Content-Addressable Memory (CAM) table flood
- Media Access Control (MAC) Address Spoofing
- Private VLAN assault and DHCP starvation
- Spanning Tree Protocol Manipulation
- VLAN bouncing

2.3. Network Layer Vulnerabilities:

The system layer gives the deliberate and procedural methods for moving alterable length information groupings from a source/sender have on one system to a goal have on an alternate system (in spite of the information interface layer which associates sender and goal has inside the equivalent or comparable system), while keeping up the prominence of administration mentioned by the vehicle layer. The IP address permits a framework to reach the outside world and permits the outside world to contact the host. It is sensible to consider this limit to our framework defenseless. Coming up next are the key security dangers at the Network Layer related with the IP:- ICMP Attack, IP Spoofing, PING Flood (ICMP Flood), Ping of Death Attack, Routing (RIP) Attacks, Teardrop Attack and Packet Sniffing.

2.4. Transport Layer Vulnerabilities:

One way the Transport Layer guarantees that there is dependability and mistake checking is through the Transport Control Protocol (TCP) (Connection Oriented Communication System). Another convention utilized at Layer 4 is UDP (User Datagram Protocol) (Connection Less Communication System). Finding a framework on the Internet requires realizing the open IP address allotted to it. To focus on a particular application on a framework, a gatecrasher would need to realize the IP address to find and recognize the framework and the port number doled out to the application, combined as an attachment. A PC framework has 65535 ports. These ports can be additionally separated into three classes:

- Dynamic
- Enrolled
- Notable

This is the place Layer 4 security is utilized and actualized. Numerous applications utilize notable TCP and UDP ports. An aggressor will distinguish and gather data about a framework utilizing TCP and UDP. There are numerous manners by which TCP and UDP are utilized to enter, refuse any assistance, or output networks. The key security dangers related with transport layer are:

- TCP "SYN" Attack
- SSL Man-in -the-Center Attacks
- Land Attack
- TCP Connecting Hijacking
- UDP Flood Attack
- Port Output Attack

2.5. Session Layer Vulnerabilities:

The 'meeting' is set up utilizing the three-way handshaking mechanism for information correspondence. At the point when a customer builds up an association with a server, the customer sends a SYN demand; the server reacts with a SYN/ACK parcel and the customer approves the association with an ACK (affirmation) bundle. A TCP association can't be built up until these 3 stages have been finished. The vulnerabilities related with meeting layer are:

- DNS Poisoning
- SYN Attack
- SSH Downgrade Attack
- TCP Session Hijacking

2.6. Presentation Layer Vulnerabilities:

The introduction layer changes information into the structure that the application acknowledges. This layer designs and encodes information to be crossed over a system. It is some of the time called the punctuation layer. Encryption administrations are related with the Upper Layers of the OSI model, definitely and explicitly the Presentation Layer. When the information is gotten, what structure will it take? Encryption systems permit us to scramble the parcel substance, requiring an extraordinary code to unveil them. The more refined and convoluted, the encryption calculation, the harder it is to access the information. Clearly, this concentrated handling capacity could influence framework execution. Suitable arranging is fundamental and required to figure security needs and to keep up offset

between them with asset impediments. Vulnerabilities at this layer often begin from shortcomings or inadequacies in the execution of capacities upheld by the introduction layer. Proceeding on the topic of exploiting the first climate of inferred trust and basic usefulness that frameworks were (and keep on being) implicit, assailants gave unforeseen or illicit contribution to introduction layer offices, acquiring results that are undesired or not at all like what the first planners anticipated and proposed. A few strategies utilized are:-

- Attacking the NetBIOS
- Buffer Overflows
- Format String Vulnerabilities

2.7. Application Layer Vulnerabilities:

This OSI layer is closest to the end client or collector or goal framework/machine, which implies that both the OSI application layer and the client discuss legitimately with the product application. Application-layer works commonly incorporate deciding asset accessibility, distinguishing correspondence accomplices and synchronizing correspondence. While recognizing correspondence accomplices, the application layer decides the character and accessibility of correspondence accomplices for an application with information to transmit to a specific and explicit beneficiary/goal. The same the physical layer, the open-finished nature of the Application Layer joins numerous dangers together at its finish of the stack, some of which are as beneath:

- Access Attacks
- Authentication Attacks
- Backdoor Attacks
- Phishing Attacks

2.8. The Eighth layer-Human Layer and Vulnerabilities:

A general misjudging about the Open Systems Interconnection model is that it comprises of just seven layers. Nonetheless, there additionally exists an eighth layer above “Application” generally entitled as “Client” or “Human

Layer". This is additionally called the Neuman's Layer. This eighth layer must be advised and considered while investigating a system issue, the greatest number of times it can end up being all the more a typical reason than the physical layer. A blunder or a planned or ponder messing with any of the above layers by this eighth layer part can cause pulverization all through this system. Basic foundations for disappointments at the Eighth layer of the OSI model incorporate ID10T blunders and arrangement related issues. Seeing about how the eighth layer discusses straightforwardly with the application layer, an issue at the eighth layer can cause issues at different layers at different meticulousness relying upon arrange security and benefit settings. Many layer 8 blunders even reason disappointments at the physical layer, which is a genuinely regular event. Undoubtedly, the eighth layer can be as a rule exceptionally hard to investigate, yet whenever kept inside thought up and down the way toward investigating different layers, at that point a layer 8 issue may uncover itself to the troubleshooter without experiencing the entirety of the layers in the middle. Normal reasons for layer eight issues are:-. Users who accept they are adjusting a conclusive setting to make something "better" or "quicker" without the scarcest sign about what the setting really does, for example evolving TCP/IP settings, a client who unplugs a system link for "security" at that point can't interface the following day and a client who shows the "clicking disorder", which causes such a wide exhibit of issues that we cannot recognize, imprint and rundown on a bit of paper. It will be so devastating and tragic that either man or our executed security systems discover any space to manage such copying issues which at last results into devastation of correspondence medium for example organize.

3. Result and Tables Analysis and Methodology

3.1. Analysis: In perspective on the dangers located above, there exists a void in setting up a compacted model which likewise comprises of the 'eighth layer'. Further, no exploration exists on a total appraisal of the security arrangements actualized at singular levels. This paper thusly plans to produce an assessment basis which will in general clarify the security arrangements utilized and actualized at every single layer of the system. The creator is in this manner of the view that in any system the security

confirmation must be assessed dependent on a record that is a scientific capacity of individual layer security files.

3.2. Methodology: It is envisioned and recommended that each layer of the OSI model, including the Eighth Layer, must be surveyed for some random system. Contingent on the worth, prevalence and extent of security systems utilized and executed for that specific system, certain imprints will be granted to each layer. These future weighted against the risk affectability of that specific layer, inferring that for any trade off in that specific layer, what might be the effect of loss of data in that organize. When each layer has been evaluated or positioned and weighted, the individual layer esteems will be included and again standardized as a rate. This last rate will at long last be allotted a letter set evaluating, e.g.

- A is more than 90
- B is more than 80

This would be the last degree of the system under test. A case of 'Arrangement' layer table is given underneath.

S.No.	Parameter	Weightage
1	Execution of association in the yearly review of received digital security arrangement counting standard and most recent updates to programming applications Operating Systems their upgradation utilization of antivirus measures firewalls with powerful principles and other digital security foundation. This review ought to in a perfect world be directed by either an outside autonomous office with expertise in digital review or an in-house devoted segment implied for this reason as it were.	25
2	Disciplinary moves and remedial activities made for violations detailed in a year also on the digital review report.	15

3	Association proprietor has set out a security strategy or received a universal condition of workmanship arrangement.	10
4	Periodical testing (for example PT on approach least yearly) of clients in their comprehension of the set down strategy is being done.	10
5	Execution of clients in the PT on arrangement	10
6	Proportion of number of outside workers (without managerial control of associations System) who utilize the framework/system to the quantity of inner representatives who use the System/organize.	10
7	Number of outer reviews did by the association in five years	10
8	Proportion of number of outside workers	5
9	Proportion of number announced episodes to the quantity of framework clients in the association.	5

4. Conclusion

Late writing has demonstrated that the overall inclination is towards receiving an all encompassing way to deal with Network Security. In like manner broad and broad research is as of now in progress to investigate and display arranges streams. The present paper is relied upon to make another benchmark right now of system security measurements. While the users know about lists for (state) monetary adequacy of AAA CRISIL evaluating, there is no shortsighted reviewing for Information Security. This paper plots a procedure to accomplish the equivalent, by surveying People, Process and Technology and reviewing these parameters to show an oversimplified evaluating for the Information Network.

References

[1] S. P. NIST 800-55 (Revision 1).

[2] ISO / IEC 27004 and ISO / IEC 15939.

[3] Implementing a Network Security Metrics Program By Paul W Lowans GIAC available on 23 Sep 13 at urlhttp://www.giac.org/paper/gsec/1641/ implementing-network securitymetricsprograms/103004.

[4] Yan Huang and Yang, Research of Security Metric Architecture for Next Generation Network. Proceedings of IC-NIDC 2009.

[5] K. Scarfone and P. Mell, The common configuration scoring system (CCSS): Metrics for software security configuration vulnerabilities (Draft). Gaithersburg, MD: National Institute of Standards and Technology. Available at http://csrc.nist.gov/ publications/drafts/nistir- 7502/Draft-NISTIR-7502.pdf.

[6] M. Swanson, Security self-assessment guide for information technology systems. Gaithersburg, MD: National Institute of Standards and Technology. (2001).

[7] N. Seddigh, P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris and A. Hatfield, Current trends and advances in information assurance metrics. Proceedings of PST2004: The Second Annual Conference on Privacy, Security, and Trust. Fredericton, NB. (2004).