RGPVNOTES.IN

Program : **B.E**

Subject Name: **Information Security**

Subject Code: **IT-8001**

Semester: **8th**

Unit V: Web Issue

Problems related to web application security comes in many ways, most of the vulnerabilities start in the web application side, as developers we need to follow certain principles, test our code and learn as much as possible about the subject, as a foundation of web application security in order to know how to prevent issues to the most significant treats.

Web application security is defined as the methods, principles and implementation used to prevent and identify security threats. Security can be understood as an effective measure solution against threats. A threat is considered a malicious danger that can exploit vulnerabilities against our resources. In web application this security weakness is the result of poor coding, mistakes in the development and bad design techniques. However, in order to code our applications in a hack-resilient way, consider the following: -

- To have organizational Management.
- Use testing tools.
- Follow Methodologies for development.
- Use standards, policies.

Uniform Resource Locator/uniform resource identify

A URL (Uniform Resource Locator), as the name suggests, provides a way to locate a resource on the web, the hypertext system that operates over the internet.

- The URL contains the name of the protocol to be used to access the resource and a resource name.
- The first part of a URL identifies what protocol to use. The second part identifies the IP address or domain name where the resource is located.
- A URL is the most common type of Uniform Resource Identifier (URI).
- URIs are strings of characters used to identify a resource over a network.
- URL protocols include HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) for web resources, "mailto" for email addresses, "ftp" for files on a File Transfer Protocol (FTP) server, and telnet for a session to access remote computers.

A URL is mainly used to point to a webpage, a component of a webpage or a program on a website. The resource name consists of:

- A domain name identifying a server or the web service; and
- A program name or a path to the file on the server.
  Optionally, it can also specify:
- A network port to use in making the connection; or
- A specific reference point within a file -- a named anchor in an HTML (Hypertext Markup Language) file.

For example, http://www.ietf.org/rfc/rfc2396.htm specifies that:

- The resource is to be retrieved using the HTTP protocol (which powers the web) via a web browser;
- The resource is reached through the domain name system (DNS) name, which could be a single server, a load-balanced cluster of servers or a service running on a system with a different name); and
- The path to the specific resource is /rfc/rfc2396.htm.
  In the following example, the URL would retrieve the file at the point marked with the named anchor "index": http://www.ietf.org/rfc/rfc2396.htm#index

The following example -- https://delphicoracle.gr:45678/Prohesy?year=2020 -- specifies:

- Use of the encrypted (secure) version of HTTP: HTTPS;
- Use of a nonstandard port (45678) for the communication; and
- Invocation of a program, "Prohesy" with parameter "year" set to value "2020".

Finally, this example -- ftp://www.somecompany.com/whitepapers/widgets.ps -- specifies use of the FTP protocol to download a file.

HTTP

HTTP means Hypertext Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

- For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.
- The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed
- HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it.
- This is the main reason that it is difficult to implement Web sites that react intelligently to user input.
- This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

HTTP Error Messages:

- Errors on the Internet can be quite frustrating — especially if you do not know the difference between a 404 error and a 502 error. These error messages, also called HTTP status codes are response codes given by Web servers and help identify the cause of the problem.
- For example, "404 File Not Found" is a common HTTP status code. It means the Web server cannot find the file you requested. This means the webpage or other document you tried to load in your Web browser has either been moved or deleted, or you entered the wrong URL or document name.
- On a 404 error, for example, you could look at the URL to see if a word looks misspelled, then correct it and try it again.

Cookies

HTTP cookie, web cookie, or cookies have a series of text sent by a server to a web browser which will then send it back, without change to the server each time the browser accessing the web site.

- HTTP cookies are used for authenticating, tracking, and maintaining specific information from the user, such as user preferences or list their electronic shopping carts.
- Cookies are still stored in the computer can speed up access to the website in question. However, cookies can reduce computer's hard disk space and provide opportunities for spreading spyware through cookies to log onto the computer. This is what is feared.
- Cookies can also be a weakness for sites that require log-in access to the encrypted, because the Shared Computer, Cookies may be the main enemy of security, which allows us to get into other people's pages without entering any password, even if the password has been changed.
- Cookies are also often referred to as IP (Internet Protocol).

Web Security Problem

When deploying a Web service, you must think about how you will secure that service. Yes, even if you decide to open access to the service to everyone and anyone, you still must think about security — For example, protecting yourself against people seeking to deny access to your service. Security encompasses the following:

- Equipment deployment
- Authenticating users
- Guarding data so that users only see what they should see
- Tracking user activity

Any and all these items may be a part of your overall security plan. In this chapter, we will look at all of these items and show how you can use them to make your Web service more secure.

Equipment deployment

One of the easiest things to do to secure your corporate data is to use hardware in an intelligent way. When deploying a publicly accessible Web service, you will want to expose as little of your internal infrastructure as necessary. There are several things you will want to do:

- Put your database machines behind a firewall.
- Use hardware to protect your equipment. For example, rely on routers instead of software firewalls. Hardware is typically faster at routing and is easier to lockdown. The software firewall may have unknown interactions with which to deal.
- Make use of a demilitarized zone (DMZ). In other words, only put the machine serving the Web service on the public Internet.

The basic theme in equipment deployment, as you have just seen, is that you should strive to keep most of your machines behind some sort of protective firewall.

Penetration Test: A penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization. Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access to sensitive data.

Penetration Testing Follow These General Steps

1. Determination of scope
2. Targeted information gathering or reconnaissance
3. Exploit attempts for access and escalation
4. Sensitive data collection testing
5. Clean up and final reporting

Vulnerability Assessment: A vulnerability assessment is the process of identifying and quantifying security vulnerabilities in an environment. It is an in-depth evaluation of your information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

Vulnerability Assessments Follow These General Steps

1. Catalogue assets and resources in a system
2. Assign quantifiable value and importance to the resources
3. Identify the security vulnerabilities or potential threats to each resource
4. Mitigate or eliminate the most serious vulnerabilities for the most valuable resources

Firewalls- A firewall is a hardware or software system that prevents unauthorized access to or from a network.

- It can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.
- All data entering or leaving the intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.
- Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world.
- This helps prevent hackers from logging into machines on your network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside.
- Firewalls are essential since they provide a single block point, where security and auditing can be imposed.
- Firewalls provide an important logging and auditing function; often, they provide summaries to the administrator about what type/volume of traffic has been processed through it.

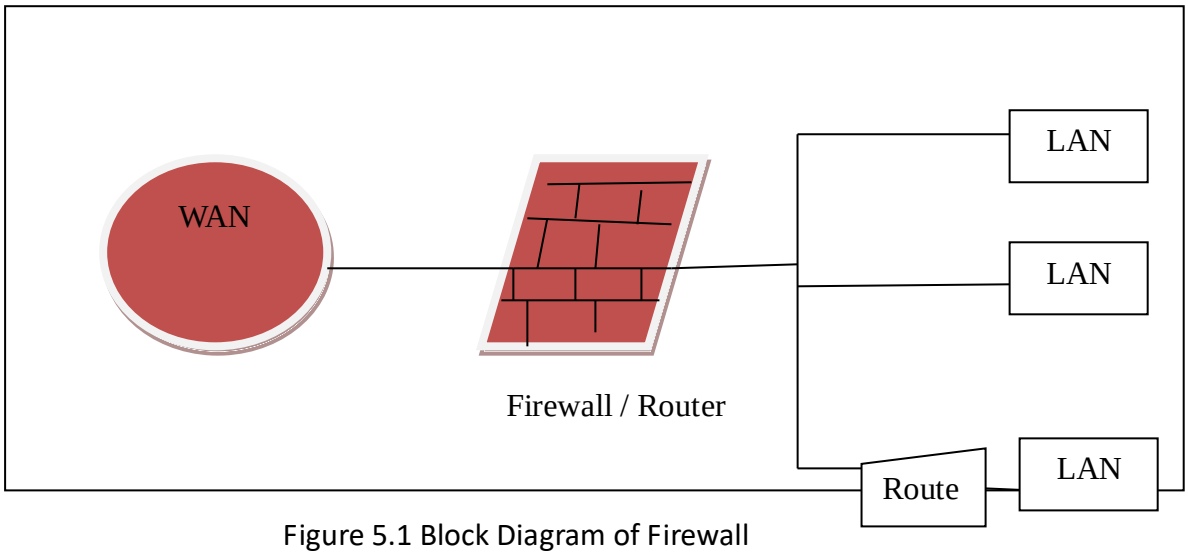

Figure 5.1 Block Diagram of Firewall

Firewall Policy

- A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies.
- Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances
- This risk analysis should be based on an evaluation of threats; vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if systems or data are compromised.
- Firewall policy should be documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise, or as the organization's needs regarding network applications change.

Access Control

An access control list can be used for many different purposes (such as filtering traffic on an interface or be used in a distribute list to filter routing updates or be used in a dialer list to identify interesting traffic or be used in Policy Based Routing to make a routing decision, and other purposes). I believe that your question relates to the function of filtering traffic on an interface). An access control list is an implementation of a type of logic that can selectively permit or deny certain packets to go through an interface.

Types of firewalls:

The National Institute of Standards and Technology (NIST) divide firewalls into three basic types:

- **Packet filters**
- **Stateful inspection**
- **Proxys**

These three categories, however, are not mutually exclusive, as most modern firewalls have a mix of abilities that may place them in more than one of the three.

- One way to compare firewalls is to look at the Transmission Control Protocol/Internet Protocol (TCP/IP) layers that each can examine.
- TCP/IP communications are composed of four layers; they work together to transfer data between hosts.
- When data transfers across networks, it travels from the highest layer through intermediate layers to the lowest layer; each layer adds more information.
- Then the lowest layer sends the accumulated data through the physical network; the data next moves upward, through the layers, to its destination.

- Simply put, the data a layer produces are encapsulated in a larger container by the layer below it.

Firewall implementation

The firewall remains a vital component in any network security architecture, and today's organizations have several types to choose from. It's essential that IT professionals identify the type of firewall that best suits the organization's network security needs

- Once selected, one of the key questions that shapes a protection strategy is "Where should the firewall be placed?" There are three common firewall topologies: the bastion host, screened subnet and dual-firewall architectures. Enterprise security depends on choosing the right firewall topology.
- The next decision to be made, after the topology chosen, is where to place individual firewall systems in it. At this point, there are several types to consider, such as bastion host, screened subnet and multi-homed firewalls.
- Remember that firewall configurations do change quickly and often, so it is difficult to keep on top of routine firewall maintenance tasks. Firewall activity, therefore, must be continuously audited to help keep the network secure from ever-evolving threats.

Packet filters

On the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion.

- In a software firewall, packet filtering is done by a program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing (called DROP) or allow it to pass (called ACCEPT).
- There are three ways in which a packet filter can be configured, once the set of filtering rules has been defined. In the first method, the filter accepts only those packets that it is certain are safe, dropping all others.
- This is the most secure mode, but it can cause inconvenience if legitimate packets are inadvertently dropped. In the second method, the filter drops only the packets that it is certain are unsafe, accepting all others.
- This mode is the least secure, but is causes less inconvenience, particularly in casual Web browsing. In the third method, if the filter encounters a packet for which its rules do not provide instructions, that packet can be quarantined, or the user can be specifically queried concerning what should be done with it.
- This can be inconvenient if it causes numerous dialog boxes to appear, for example, during Web browsing

Application level gateway

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

- Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.
- The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client's behalf.
- A computer's internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address.

Encrypted Tunnel

Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

- Tunneling is also known as port forwarding.
- In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport.
- As the packets move through the tunnel, they are encrypted, and another process called encapsulation occurs. The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending. The units look like public data, allowing them to be transmitted across the Internet.
- Encapsulation allows the packets to arrive at their proper destination. At the destination, de-capsulation and decryption occur.

There are various protocols that allow tunneling to occur, including:

- **Point-to-Point Tunneling Protocol (PPTP):** PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the "virtual" sense because it is being created in a tunneled environment.
- **Layer Two Tunneling Protocol (L2TP):** This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.

Security Architecture

Security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible.

In security architecture, the design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents. System architecture can be considered a design that includes a structure and addresses the connection between the components of that structure.

key attributes of security architecture are as follows:

- **Relationships and Dependencies**: Signifies the relationship between the various components inside IT architecture and the way in which they depend on each other.
- **Benefits:** The main advantage of security architecture is its standardization, which makes it affordable. Security architecture is cost-effective due to the re-use of controls described in the architecture.
- **Form:** Security architecture is associated with IT architecture; however, it may take a variety of forms. It generally includes a catalog of conventional controls in addition to relationship diagrams, principles, and so on.
- **Drivers:** Security controls are determined based on four factors:
    - Risk management
    - Benchmarking and good practice
    - Financial
    - Legal and regulatory

The key phases in the security architecture process are as follows:

- Architecture Risk Assessment: Evaluates the business influence of vital business assets, and the odds and effects of vulnerabilities and security threats.
- Security Architecture and Design: The design and architecture of security services, which facilitate business risk exposure objectives.

- Implementation: Security services and processes are implemented, operated and controlled. Assurance services are designed to ensure that the security policy and standards, security architecture decisions, and risk management are mirrored in the real runtime implementation.
- Operations and Monitoring: Day-to-day processes, such as threat and vulnerability management and threat management. Here, measures are taken to supervise and handle the operational state in addition to the depth and breadth of the systems security.

Intrusion Detection System.

- An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases, the IDS may also respond to anomalous or malicious traffic by acting such as blocking the user or source IP address from accessing the network.
- There is network based (NIDS) and host based (HIDS) intrusion detection systems.
- There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies.
- There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat

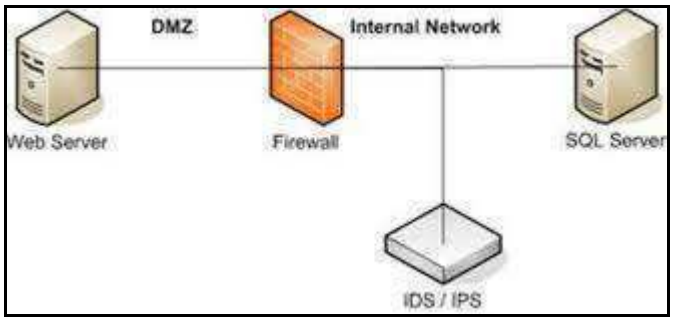

Figure 5.2 Block Diagram of IDS

Types of IDS:

NIDS

- Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- Ideally you would scan all inbound and outbound traffic; however, doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

- Host Intrusion Detection Systems are run on individual hosts or devices on the network.
- A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Signature Based

- A signature-based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based

- An IDS which is anomaly based will monitor network traffic and compare it against an established baseline.
- The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, then the baseline.

Passive IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to act to block the activity or respond in some way.

Reactive IDS

- Reactive IDS will not only detect suspicious or malicious traffic and alert the administrator but will take pre-defined proactive actions to respond to the threat.
- Typically this means blocking any further network traffic from the source IP address or user.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in