Network Security - Authentication Methods and Firewall

Minal Dhankar*

Abstract

Nowadays computer security is becoming a major issue because we are moving to a digital world. The security of data is extreme important in ensuring safe transmission of information over the Internet. Authentication and firewalls are one of the most basic and commonly used techniques to ensure security in the network. A firewall is a device that prevents unauthorized access to a network and can be implemented in hardware or software or a combination of both. This paper presents various authentication techniques like Knowledge based, Token based, Biometric based and an analysis of Firewall Technology.

Keywords: Firewall Testing, Firewall Technology, Authentication, Biometric, Password, Security Tokens

Introduction

As the world is digitizing people are becoming more active on the Internet, but along with this awareness several security threats like viruses, Denial of service etc. have also increased tremendously. So, the most important issue in today world is to secure the network. Security network is important because we do not want any sensitive or confidential information to go outside the network. These threats can create serious damage to an individual's personal information and to the resources of a company or an organization. These threats are present mainly due to the ignorance of the user and poor technology and design of the network. These threats are also a result of the network services which are enabled by default into a computer and are used by the hackers for information gathering. The firewalls installed before are not suitable for the present computer threats and cannot prevent data against these threats. A firewall is a hardware or software system that prevents unauthorized access to or from a network and can be implemented in hardware and software or both. Firewall filters incoming and outgoing data packets as they come in and go outside of the network. The following are basic features of a secure network-

1) *Access:* Only authorized users are used to communicate to and from a particular network..
2) *Authentication:* This ensures that users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.
3) *Confidentiality*: Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.
4) *Integrity:* This ensures that the message has not been changed during transmission.

Data Security And Authentication

During the process of data communication there is always a threat of stealing of data by the hackers. So, to secure sensitive information, authentication is the key in network security. Authentication is the technique of ensuring the identity of user or any other entity involved in the network. Password is the most commonly used scheme for verifying the identity of a person. Attacks which can occur during authentication are given in Table I.

Authentication Methods

Following are the primary authentication techniques used in the public network these days:

Minal Dhankar*
Asst. Prof., Maharaja Surajmal Institute
(Affiliated to GGSIP University)
New Delhi, India

Table I: Attacks on Network Data

ATTACK	DESCRIPTION
Passive Attack	Monitors unencrypted traffic and looks for sensitive information
Active Attack	The attacker tries to bypass or break into secured systems
Distributed Attack	It introduces code such as Trojan horse to a trusted software
Insider Attack	It involves someone from the inside attacking the network.
Close-in Attack	This involves someone attempting to get physically close to data
Phishing Attack	The hacker creates a fake website that looks like an original website.
Hijack Attack	The hacker takes over a session between you and another person.
Spoof Attack	The hacker modifies the source address of the packets.

A. Password and pin based

Passwords and PINs are most commonly used authentication methods. These are known as Knowledge-based methods as users memorize their passwords. Passwords can be single words, numeric, phrases, any combination of these or personal identification number. For stronger protection, password should be longer. Plain passwords must be avoided as far as possible. In an authentication system, a strong password should be a combination of numbers, letters, special characters and mixed cases. In order to protect password during data transmission, the Transport Layer Security (TLS) or Secure Socket Layer (SSL) features, which can generate an encrypted channel for data exchange, should also be enabled for authentication systems. Cases have been reported of user ID's and passwords being stolen by fraudsters through phishing emails, fake websites, Trojan software and other malicious software. Since such attacks are focused on the end-user side, raising the awareness of user is very important so that they can protect their interests in their daily transactions. Unusual knowledge-based methods can also be adopted based on visual images (graphical password). One example is that a user is presented with a series of five randomly generated life-like faces and the user repeatedly picks out the faces from a series of grids filled with more faces. By picking the correct faces, the user has effectively typed in his password.

Fig.1 shows working of password based authentication technique. The user first enters a name and password. It is required that the Client application binds itself

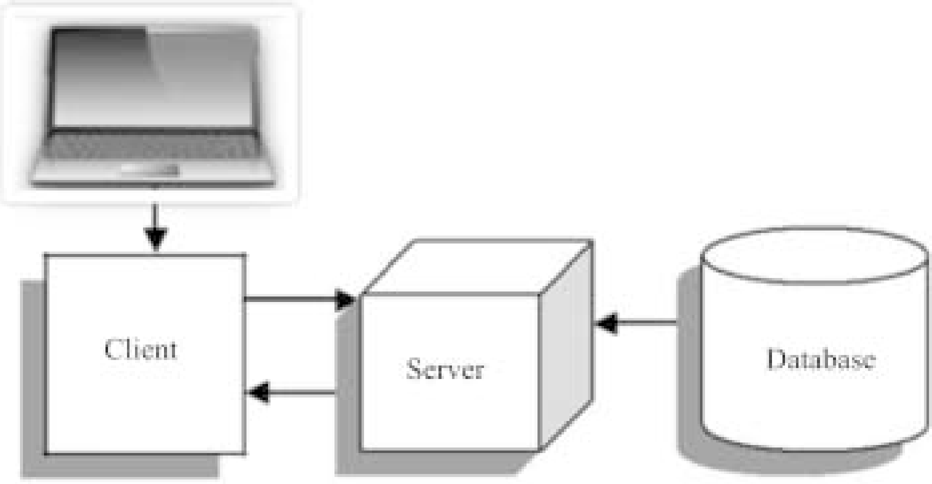

Fig.1 Server based authentication

to the Directory Server with a distinguished Name. The client uses the name entered by user to retrieve domain name. Next the client sends these credentials to the Directory Server. The server then verifies the password sent by the client by comparing it against the password stored in database. If it matches, the server accepts the credentials for authenticating the user identity. Then the server allows client so authorized to access the resources.

B. Token Based

This is a physical device that performs authentication and hence can be termed as object based. Tokens can be compared with physical keys to houses that are used as a token but in digital tokens many other factors are present to provide information safety. In digital world, security tokens are used. The general concept behind a token based authentication system is simple. Allow users to enter their username and password in order to obtain a token which allows them to fetch a specific resource-without using their username and password. Once their token has been obtained, the user can offer the token-which offers access to a specific resource for a time period-to the remote site. Tokens themselves have password so even if they are lost, the hackers cannot modify the vital information. Bank cards, smart cards are security token storage devices with passwords and pass codes. Pass codes are same as password except that the former are machine generated and stored. There exist one time security tokens and smartcards as. Analysis involves finding out the user expectations or needs regarding new or modified software. It involves frequent communication with the system user for requirement findings and specifying those requirements in the Software Requirement Specification document.

C. Biometric Based

Biometric authentication is the process of verifying if a user is whom he is claiming to be, using digitized biological signatures of the user. Biometric authentication can be classified into two groups: physiological and behavioral. In physiological authentication, faces, finger prints, hands, iris and retina follow. And in the case of behavioral, voice prints, signatures and keystrokes are used. This technique can term as ID based. This technique is safer as compared to password and token based techniques. Biometric authentication techniques are currently in operation in various enterprises. They are used for passports, visas, personal identification cards, accessing bank machines, doorway access control, and general computer desktop access

Working of Firewall in PC

There are various different methods firewalls use to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used in a number of ways to add protection to your home or business. Large organization or corporations often have very complex firewalls in place to secure their networks. On the other side, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidence data outside of the network. On the inbound side, firewalls can be programmed to stop access to certain websites like social networking sites.

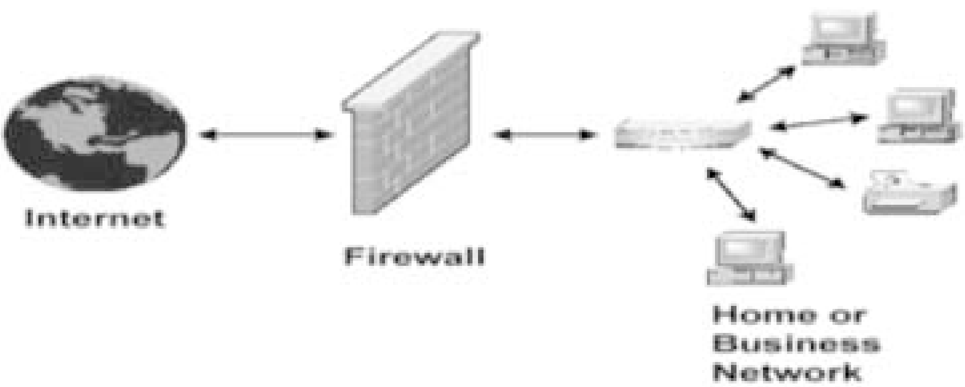

Fig. 2 Working of Firewall

Moreover, firewalls can prevent outside computers from accessing computers inside the network.

A company might choose to select a single computer on the network for file sharing and all other computers could be controlled. There is no limit to the variety of configurations that are possible when using firewalls.

For residence use, firewalls work much more basically. The main goal of a standalone firewall is to protect your personal computer and private network from various threads. Malware, malicious software, is the main threat to your home computer. Viruses are the first type of malware that comes to mind. A virus can be transmitted to your system through email or over the Internet and can quickly cause a lot of injure to your files.

There are two ways a Firewall can prevent this from occurrence. It can allow all interchange to pass through except data that meets a preset set of criteria.

Firewall uses the later way to prevent malware from installing on your computer. This free software firewall, from a global security solutions provider and certification power, uses the patent pending “Clean PC mode” to disallow any application from being installed on your computer unless it meets one of two criteria. Those criteria are as follow a) the user gives authorization for the installation and b) the application is on a widespread list of standard applications provided by this firewall. With this feature, you don’t have to worry about unauthorized programs installing on your computer without your awareness.

A. Firewall Technology Overview

A firewall works like a filter between your computer and the Internet. Firewalls can also do auditing. With firewall you can decide, data which can be accessed on your network and which should not. A firewall can look at a whole packet’s contents. There are various different types of firewall used to filter out information. Firewalls can be used in business and at homes too. In business firewalls can prevent employees from sending sensitive data outside the organization and can also be programmed to restrict access to certain websites. For home use the main goal of firewall is to protect your computer from malware or malicious software.

A.1 Packet Filters

The simplest form of firewall is packet filter. On the Internet, the aim of packet filtering is to allow or block packets based on source and destination addresses, ports, or protocols. A packet is sent from source to destination only if it is certified. A packet filter look at five things like the source and destination IP addresses, the source and destination ports, and the protocol such as UDP, TCP/IP, and so on. As packet filter deals with individual packets a decision is to be made for each and every packet, whether that particular packet can pass or should undergo some other action. Due to its simplicity and speed, a packet filter can be enabled on your routers, eliminating the need of a dedicated firewall. There are some problems with packet filters:

1. They generally do not have any idea about what is being sent in the packets.
2. They are not able to successfully handle protocols that rely on various dynamic conditions.

A.2. Application Gateways

An application gateway is also known as application proxy or application-level proxy such as an SMTP proxy that understand the SMTP protocol and it is a program that runs on a firewall system between two networks. An application gateway is one step farther than a packet filter as instead of simply checking the IP parameters, it actually looks at the application layer data. When a client program creates a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected .An application gateway check the data that is being sent and authenticate that the particular protocol is being used perfectly. Let's say we were creating an SMTP application gateway. It would need to keep track of the state of the link: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server. The application gateway must understand the protocol and process both sides of the conversation. As such, it is a much more CPU exhaustive process than a simple packet filter. However, this also lends it a larger element of security. You will not be able to run the earlier described SSH- over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Furthermore, because an application gateway understands the protocols in use, it is able to support difficult protocols such as FTP that create casual data channels for each file transfer. As it reads the FTP command channel, it will make out the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete. Often there is a protocol that is not directly understood by your application gateway but that must be allowed to traverse the firewall. SSH and HTTPS are two effortless examples. Because they are encrypted end to end, an application gateway cannot read the traffic actually being sent. In these cases, there is usually a way to configure your firewall to allow the appropriate packets to be sent without invasion by the firewall. It can be difficult to put together application gateways into your standard routing hardware due to the processing overhead [10]. Some newer high-end routers are able to function as application gateways, but you'll need plenty of CPU power for satisfactory presentation.

A.3. Stateful Inspection

In computing, a this firewall is a firewall that keeps track of the state of network associations (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to differentiate legal packets for different types of connections. Only packets matching is an active connection will be allowed by the firewall; others will be rejected it inspection, also referred to as Dynamic Packet Filtering, is a security feature. Check Point Software introduced this inspection in the use of its Firewall 1 in 1994, this firewall assessment takes the basic ethics of packet filtering and adds the concept, so that the Firewall considers the packets in the context of before packets. So for example, it records when it sees a packet in an internal table and in many execution will only allow TCP packets that match an existing conversation to be forwarded to the network. This has a number of advantages over simpler packet filtering: It is possible to build up firewall rules for protocols which cannot be correctly controlled by packet filtering. There is a risk that vulnerabilities in individual protocol decoders could permit an attacker to gain control over the firewall. This worry highlights the need to keep firewall software updated. Some of these firewalls also increase the possibility that personally hosts can be trick into solicit outside connections. This option can only be totally eliminated by auditing the host software. Some firewalls can be conquered in this way by simply screening a web page. More complete control of traffic is possible [6]. Equally, there are some disadvantages to this assessment solution, in that the execution is automatically more complex and therefore more likely to be errors. It also requires a device with more memory and a more influential CPU for a given traffic weight, as data has to be stored about each and every load flow seen over a period of time.

B. *Firewall Testing*

Firewalls plays important role in network protection and in many cases build the only line of security against the unidentified rival, systematic Firewall testing has been ignored over years. The reason for this lies in the missing of undependable, helpful and received testing methodologies. Efficiency testing is hard to do without particular tools, and even if you have particular tools, you may not get good results. Efficiency testing should focus on three areas: (1) intrusion prevention (2) antimalware (3) application identification. If you want to block peer-to-peer file sharing, open a few different Torrent clients and see what happens. Performance testing has to be completed by "pass/fail" indicators. For example, when the firewall starts to reject to open new sessions, the test should end as you have gone away from the limits. You should also set other limits, such as greatest latency time, to define when the firewall is not behaving sufficiently well. Do the same for applications such as webmail or face book, which both are the most important candidates for application identification and control. Don't try an automatic test tool, as the results are never as exact as the real application talking to real servers. This is especially correct of applications that are ambiguous, such as Bit Torrent and Skype, which can never be perfectly virtual in a test tool. Performance testing also usually requires particular tools, but has become so well- liked that there are open source alternative. When testing presentation remember to check your bad test against a null device a router or patch cable would work. This will tell you the maximum speed of your analysis bed. From there, keep in mind noted network tester David Newman's Laws of Testing: It must be repeatable, it must be worrying, and it must be significant. Take the device you're testing to its confines, even if you don't predict going that far. This will tell you where you will hit a wall in the upcoming and where you have sufficient headroom to grow. There are three general approaches to firewall testing:

1) Penetration testing
2) Testing of the firewall implementation
3) Testing of the firewall rules

The goal of penetration testing is to expose security flaw of a goal network by running attacks against it. Penetration testing includes information get-together, searching the network and attacking the target. The attacks are performed by running vulnerability testing tools, Saint that check the firewall for likely breaches of security to be exploited. If vulnerabilities are detected, they have to be permanent. Penetration testing is usually performed by the system administrators themselves or by a third party (e.g. hackers, security experts) that try to break into the computer system. The problem is that we have to be sure that we can trust the external experts. Penetration testing is a way to perform firewall testing but it is not the only one and it is not the way we precede.

Testing of the firewall working focuses on the firewall software. The examiner checks the firewall working for bugs. Different firewall commodities support different firewall

languages. Thus, firewall rules are vendor-exact. Consider a hardware firewall deploying vendor- exact firewall rules. The firewall execution testing approach evaluates if the firewall rules communicate to the action of the firewall. Firewal execution testing is primarily performed by the firewall vendors to increase the consistency of their products. Testing of the firewall rules confirmed whether the security policy is correctly executed by a set of firewall rules. A security plan is a

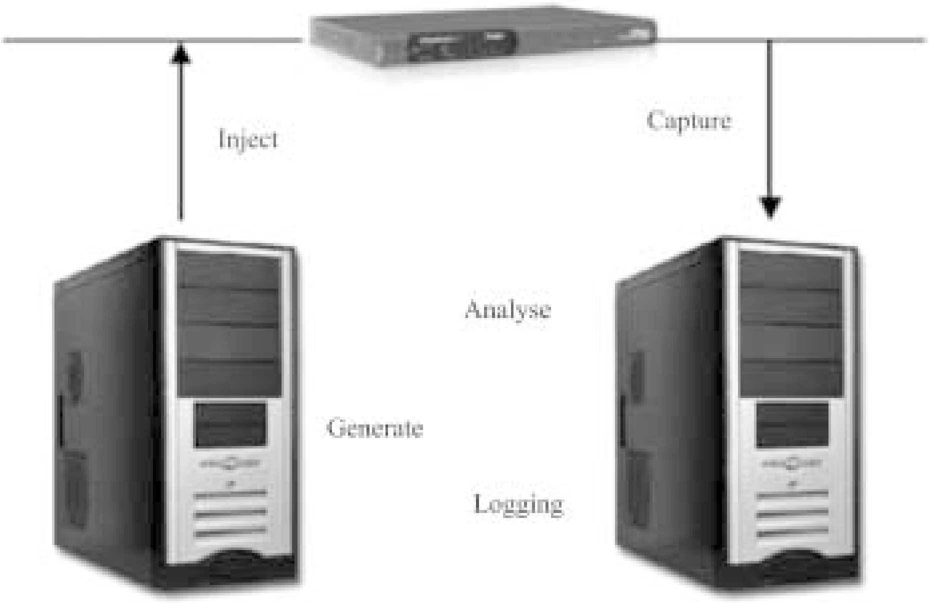

Figure 3: Testing of Firewall

document that sets the basic mandatory rules and morality on information security. Such a document should be plan in every company. The firewall rules are future to implement the directives in the security plan. Considering the test packet driven advance, firewall testing includes two phases: The identification of appropriate test cases that examine the behavior of the firewall and the practical performance of these tests.

Conclusion

Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. Password based technique is best if you have to remember a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember. Token based techniques provide added security against denial of service (DoS) attacks. In comparison to above two, techniques biometric cannot be easily stolen so it provides stronger protection. As signals, biometric can be easily copied by attackers so it should not be deployed in single factor mode. Furthermore we can choose a combination of above technique as discussed above. The firewall also has its own limitations All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor.

References

1. Lawrence O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.
2. Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No. 04.
3. [Online]Available:
   http://www. authenticationworld.com/Token-Authentication
4. [Online]Available:
   http://www.authenticationworld.com/Authentication-Biometrics.
5. Jae-Jung Kim and Seng-Phil Hong, "A Method of Risk Assessment for Multi-Factor Auhentication", Journal of Information Processing Systems, Vol. 7, No.1, March 2011.
6. Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRAN SACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.
7. [Online]Available:http://www.duosecurity.com.
8. [Online]Available:http://ids.nic.in/technical_letter TNL_JCES_JUL_2013/Advance%20Authenticatio N%20Technique.pdf.
9. Stamati Gkarafli, Anastasios A. Economides, "Comp Aring the Proof by Knowledge Authentication Techniques", International Journal of Computer Science and Security (IJSS), Volume(4): Issue (2).
10. Roger Meyer, "Secure authentication on the internet" As the part of security reading room, SANS institute 2007.
11. Canghong Zhang, based on network security firew All technology,Information technology, Chinese new Technology new product, 2009.
12. Rui Wang. Haibo Lin, Network security and firewall Technology, Tsinghua university publishing house, In 2000.
13. Kuang chu,network security and firewall technology, Chongqing university publishing house,2005.
14. S. Smith, E. Palmer, and S. Weingart, "Using a high-Performance, programmable secure coprocessor," in Proc. International Conference on Financial Crypt ography, Anguilla, British West Indies, 1998.