© 2015 IJSRSET | Volume 1 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Empirical Study of Various Security Mechanisms on Network

Bhart Bhushan
Village Gehli, PO Hamidpur, Tehsile Narnaul, Haryana, India

ABSTRACT

This paper expounds the Network Security issues which are becoming important as increasing demand of good quality communication. We are moving to digital information age so Information security is one of the critical component in ensuring secure communication and transaction i.e. m-commerce over the internet. There are various methods available and in use to provide security some of them are based on intrusion detection system (IDS) or authentication based methods i.e. passwords, biometric authentication. One of the most popular ways of ensuring security in the network is authentication. This paper analyse the various authentication techniques such as Token-based and Biometric-based and Knowledge-based and also gives a description of the architecture of Snort rule set which is a very popular digital signature and Intrusion Detection system on anomaly based. Furthermore, we also discuss the advantages of FPGA devices which are used in intrusion detection system implementation.

Keywords: Snort, Authentication, Denial of service, IDS, Passcode, Smart card, FPGA, RSA, Biometric

I. INTRODUCTION

This century is century of digital life. A large number of population becoming active user on the Internet for their entertainment, personal and professional work, this is the reason internet is growing very swiftly. AS the internet is growing, various threats such as fraud manipulation of information, Denial-of-Service (DOS) attacks and Trojan Horses to steal information also increasing very rapidly. So It becomes very important for us to take steps to protect our network from these threats so that our data or information and also to the resources of companies and government and personal resources by taking various security measures like IDS or authentication methods. Providing integrity, maintaining confidentiality, and ensuring the availability of correct information should be the primary objectives in network security. The main reason of these threats is internet characteristics of openness of the ignorance approach adopted by the internet users, obsolete technology and weak structure of the network. Often there are many network services that are enabled by default in a personal computer or a router. Many services among them may not be necessary and may be an attempt of intruder or attacker to steal our information. In this paper we will study about IDS. An intrusion detection system can be understand as the act of identifying and applying necessary actions against malicious activities targeted to network and resources such as data, memory, hardware. A network intrusion detection system is aimed to continuously scan the traffic passing the network and compare with a previously known set of malicious activities or look for statistical deviation of the system under surveillance from its normal behaviour. So it is good to disable these unnecessary services to protect them from hackers and intruder, More importantly, not only need to be careful regarding the security at each end of the network rather the concern should be on securing the entire network.

While developing a strategy to secure network, the following need to be considered: Access – Only authorized users are allowed to participate in communication over network, Authentication – it should be ensured that the users in the network are who they say they are. Actual transfer of information can happen only after the user has been authenticated and allowed to communicate to other systems in the network, Confidentiality – Data in the network remains inaccessible in any form to unauthorised user, Integrity – This is also to be ensured that the message has not been changed during transmission over the network.

II. SYSTEM AND NETWORK SECURITY AND IDS

As the vital information and online banking transactions activities occur over the network are increasing very rapidly, the malicious activities are also increasing. Intruder tries to break into network security to steal that information to perform various attacks. The Intrusion detection system (abbreviated as IDS) used in the network should be able to sense the suspicious activity and inform the user about this. A set of well defined rules eg. Snort and Bro are used to identify network suspicious events that are other than usual events.

The aim of new generation internet service providers is to provide a high speed error free communication keeping up with the demand of swiftly increasing data usage. Detailed packet inspection with regular string matching is a very common method of network intrusion detection. Implementation of Signature based network Intrusion Detection System (NIDS) requires to match a predefined pattern or predefined phrase that is already identified as harmful to the network. As the IDS should inspect the data packets at the rate of data connection, a very high performance is required for the IDS pattern matching scheme. Also the rule set should be regularly updated with the identification of new attacks. The hardware system used to implement IDS should have the mechanism of dynamic reprogramming. FPGA devices supports both of these features of high network traffic collection ability and dynamic reprogramming. So they are suitable devices for hardware implementation of IDS. But the high network traffic collection ability is not matched by the device frequency. So it becomes mandatory approach to implement parallelism in FPGA like multi core parallelization of microprocessors based IDS traffic analysis.

VARIOUS TYPES OF INTRUSION DETECTION SYSTEM

IDS can be classified into two main categories: analysis approach and placement of IDS. Analysis approach consists of misuse detection and anomaly detection. Various types of IDS are as follows

2.1 Host Based System

This type of IDS is available on each host that need filtration. These are able to detect whether an attempted attack is successful and can identify local attacks. It is possible to analyse the traffic and the effect of any attack can be analysed very accurately. Deployment and management of them is difficult if the numbers of hosts that are to be protected are large in number.

2.2 Anomaly Detection method

This method makes decisions based on normal network or system behaviour using statistical techniques.

This approach analyse network traffic and match it against an established baseline of normal traffic profile. The baseline characterizes normal behaviour for the network - such as used general protocols, the normal bandwidth usage. This method is able to identify new types of attacks which are till now unknown and unidentifiable by signature based IDS. But it may generate a large number of false positives; this is the main disadvantage of anomaly detection method. An anomaly detection method consists of two parts, the first part is termed as training phase the second phase is called anomaly detection, where the learned profile is applied to the current traffic to look for any deviations. The anomaly detection techniques are as follows: statistical methods, data-mining methods and machine learning based methods. In statistical methods it is assumed that a variation of the traffic in terms of volume of number of packets indicates attack, like bandwidth flooding attack. But if the attacker keeps traffic parameter bellow a certain level this method will not work. Incorrect combinations of port numbers and devices are indicators of attack. In this situation IDS should warn the administrator or user regarding detection suspicious or anomalous traffic. Based on placement in the network IDS can be classified as host based and network based systems.

2.3 Network Based System

It is a low cost deployment method of IDS. It scans the traffic on the network to which the hosts that are to be secured are connected. It is possible to identify attacks to and from multiple hosts on the network. This is a passive type of method in nature so it becomes easy to apply them to a pre- existing network without having large disruption. Network based system can be implemented either as an internal deployment mode or

can be used in early warning system. Difference between these two is given in below table.

Table1. Difference between Host-Based network system and Network-Based system

Network-Based IDS	**Host-Based IDS**
It detects attacks on network	It detects local attacks
Dependent on Bandwidth	Bandwidth independent
Independent of Host	Host dependent
Slow down the network that has IDS client installed	Slow down the hosts that have IDS client installed
Near real-time response	Response is received on a suspicious entry
Not suitable for encrypted network	Suitable for encrypted network
It is broad in scope	Its scope is narrow, monitors specific activities

2.4 Misuse Detection method

In this technique for some known misuses uses pattern matching algorithm to look into. It has a very low false positive rate (IDS generates warning when no attack has taken place). Because this method relies on comparing the incoming traffic with a known set of malicious patterns, so it is difficult to identify a new novel attack. Due to this reason, there is high false negative (Failure to detect an actual attack). The number of disallowed patterns now has reached the order of the thousands making the computation a more difficult task. Signature based Intrusion Detection System is a commercial success. Snort is one of the well defined rule set that uses protocol, signature and anomaly based detection methods.

2.5 Early Warning System IDS

It monitors all the data that is passing the network and IDS is implemented outside the firewall. Using this method, it is possible to identify attacks to and from multiple hosts. The deployment cost is less because this system has a single point of deployment and hence and it is also easy to configuring the system up to date and update the signatures. It can detects those malicious activities also that are blocked by firewall, this is shortcoming of this.

2.6 Internal Deployments IDS

IDS are implemented in such a way that it scans every network link through which the traffic is passing and provides extra protection. The IDS is deployed near the access router and near the network boundary. The data that is blocked by the Firewall is not handled by the IDS. But it is difficult to maintain and reconfigure the system with every rule set update because of the large number of hosts on network. Internal Deployments IDS is shown in below figure.

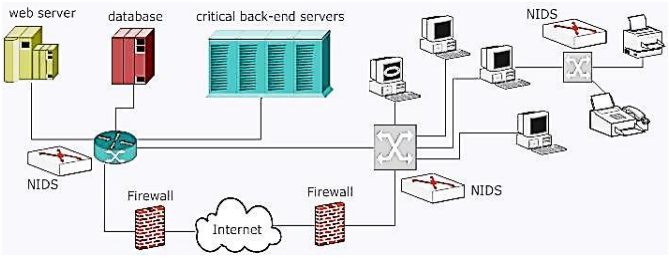

Figure 1. Internal Deployment Mode of IDS

Any ideal IDS should have the following desirable features:

System should be fault tolerant and run with the minimal human supervision, The IDS should not be susceptible to attacks from the intruder, and IDS should not interfere with the normal operation of the system. , It should be possible to reconfigure the IDS over time with the changing rules and security policies of the network. IDS should be portable to different machine architectures making it easy to implement. IDS should be general to detect various kinds of attacks and should have as smaller number of false positives as much possible.

III. INFORMATION SECURITY AND AUTHENTICATION

Information Security is a challenging issue in the field of networking. For ensuring security of information from hackers and intruder, authentication and IDS the major steps in network security. These are the concepts to protect information and data transmitted over wired as well as wireless networks. Authentication is one of the most effective techniques of ensuring that the person who is transmitting the information is whom he is claiming. So it is an act of detecting the actual identity of users, machines or any other network entity. Password is mostly used to verify someone's identity and next to password is biometric authentication in which fingerprints or iris of eye is scanned and matched with database. Different techniques can be used authenticate user or machines, to perform authentication between user and machine or machine and another machine too. In below table various types of attacks can cause harm during authentication is shown**.**

Table 2: Different types of attacks on data

Types of Attack	**Details of harm caused**
Insufficient authentication	Some websites don't authenticate much so hackers attack sensitive content. Some sort of mechanism should be there like captcha.
Unavailability of Firewall	To filter incoming and outgoing packets on a network, firewall is very necessary.
Brute force method of attacks	By attempting various try technique and error, hackers can guess username, password, ATM cards numbers, etc. This technique is highly popular.
Weak password Security	An untrusted Website may permit hackers and intruders to find a way to illegally obtain, change or recover another user's password, called as sniffing attacks
Shoulder surfing attacks	Hackers directly observe user while typing passwords or may obtain by hidden Cameras.

AUTHENTICATION TECHNIQUES

Following are the various authentication techniques are in use for the public network these days:

Biometric Based:

Biometric authentication is the process of verifying if a user is whom he is claiming to be, using biometrics i.e. finger print or iris of eyes of the user. Authentication based on Biometric can be classified into two categories: physiological and behavioural. In physiological authentication, faces, finger prints, hands, iris and retina follow. While in behavioural biometrics, signatures, voice prints and keystrokes are used. Biometric authentication is more secure as than password and token based techniques. Biometric authentication techniques are currently used in various organisations and government departments i.e. applying for a job, marking attendance on biometric machine etc. Iris and finger print biometric features gives higher performance than facial and hand features but device cost is more while cost of hand and facial recognition devices is moderate.

Password and pin based:

In an authentication technique, confidentiality and privacy can be ensured up to some extent. Users needs to remember secret text of alphanumeric and special characters called passwords. Passwords can be single words, numeric, phrases, any combination of these or a secret number. But in the authentication method, there is a problem that passwords can be easily guessed or randomly searched by the hackers or intruders. Both clear-text protocols such as MD5-based protocols like Challenge Handshake Protocol (CHAP) and Password Authentication Protocol (PAP) are used in Virtual Private Networks such as Point-to-Point Tunnelling Protocol (PPTP) make use of. Among them, the protocol MD5 should be preferred over PAP because of sniffing attacks. Simple text passwords must be avoided as far as possible.

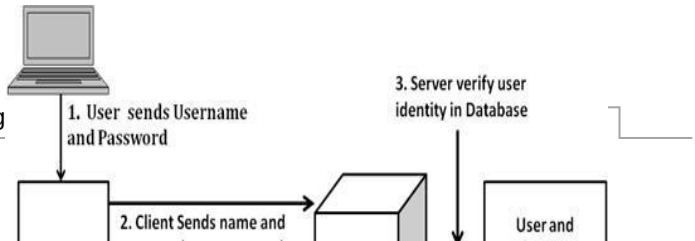

Figure 2. shows how authentication process is carried out with passwords.

C. Token based:

Token based technique is hardware based authentication method and so it is generally referred as object based technique. Physical keys to houses are matched with Tokens but in digital tokens many other elements are there to avail information safety. In computer network, security tokens are used. Tokens also have password so even if these are stolen by hackers, the hackers cannot modify the secret information. Bank cards i.e. debit card, credit card, smart cards and shopping cards are security token storage devices with passwords or pin code and pass codes. PIN codes similar to password except that pin codes are machine generated and stored. If wrong PIN or passwords are attempted more than specified attempts, the card is locked. There exist one time security tokens and smartcards as shown in Fig. 3.

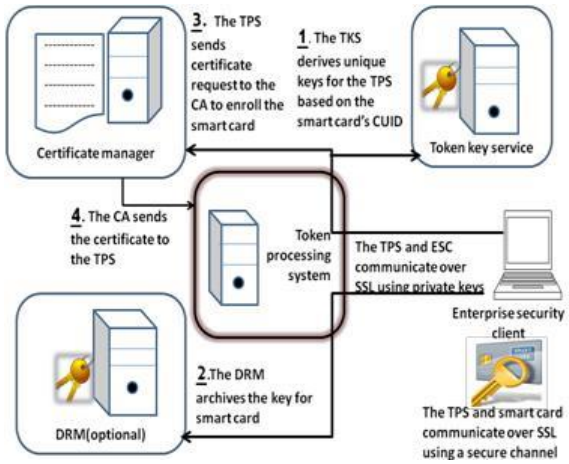

Figure 3. Token-based Authentication

One time password tokens:

One time password token are used in RSA algorithm of Ron Rivest, Adi Shamir and Leonard Adleman, it reduces the risk as compared to a simple text password as we may change our passwords according to our convenience after a specified interval of time. But secureID in RSA which is generated by some mathematical algorithms works in a better way as it changes every 60 seconds, and this information is only known to security server.

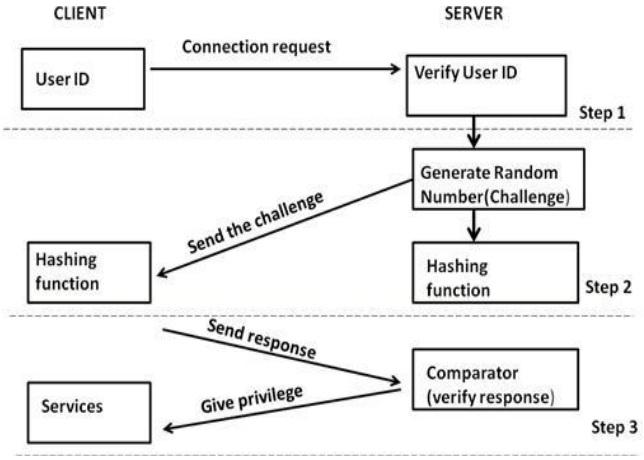

Figure 4. Mechanism for OTP method

A user logs on a private network, he enters his allotted ID and then the some random number displayed on the monitor. After encryption this information is transmitted to the security server. Any user authenticated only when the number that display on the screen matches the mathematical algorithm and the ID. One time password (OTP) can be used to make this scheme more effective. Above figure 4 shows the working that normally occurs during the process of OTP.

IV. DIFFERENCES OF STRENGTH OF AUTHENTICATION MECHANISM BASED ON PARAMETER

In the graph we can evaluate Procedural Strength, Discrimination Strength and Technical Strength. To compare the strength of above various authentication methods we will take the help of a graph.

In this graph weakness = 1/strength. Result of this, we get the following equation:

Binding Weakness = Discriminatory Weakness + Procedural Weakness + Technical Weakness

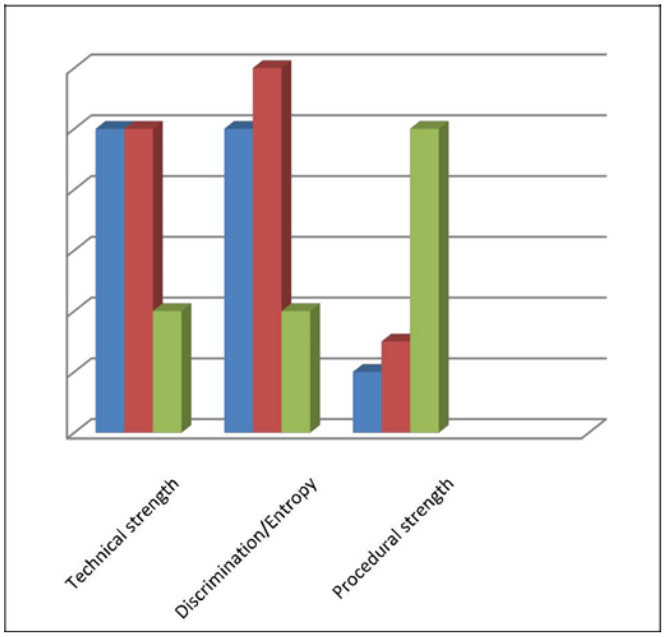

Figure 5. Authentication methods parameter Comparison

In above graph Password is shown in Blue, token in Red and Biometric in green. In the above graph, characteristics of the three different authentication mechanisms can be summarized including their hardware requirement, ease of operation, running cost, initial setup cost and vulnerability to attacks such as Denial-of-Service (DOS), procedural and technical strength. Token based authentications are significantly more robust against attacks because it uses twin password combination. In comparison to above two techniques, biometric cannot be easily stolen so it provides stronger protection but it is too expensive for personal use. Password based authentication is convenient and inexpensive technique, it provides high key space and hashing which protects from host attacks. So according to capacity and use people are free to choose the authentication technique as per their need and sensitivity of data and cost available.

AUTHENTICATION BASED ON COMBINATION OF MULTIPLE FACTOR

A combination of above techniques can be used to make network more secure. For network security, each authenticator result must be satisfied. As a Boolean AND operation is performed for each factor's authentication results, so all must be affirmative. Following combination can be used- Password and token based, Password plus biometric based, token and biometric based or even password token and biometric based. The combinations of biometric and passwords implementation are not so common because biometric usually includes sake for convenience. Combination of all three factors is required where there is a high need of security. Till now such a combination is not highly applied.

V. CONCLUSION

A number of security mechanisms are in use to ensure secure communication over network or internet. These security techniques include intrusion detection methods and various authentication techniques. In this paper we studied about various authentication techniques, among them be reached on conclusion that if you have to remember a single password, password based technique is best. But it is inefficient when we have to remember many passwords so we tend use easy to remember passwords. Against denial of service (DoS) attacks, token based techniques more suitable. A more secure technique, techniques biometric cannot be easily stolen so it provides stronger protection. Because a biometric can be easily copied by attackers so it is avoided to use a single factor authentication. To make protection against intrusion we can use intrusion detection schemes. The deep packet inspection is core component in IDS that match incoming traffic of packets with the known rules called signatures. Both in software or hardware implementation is the number and complexity of the rules/signatures that must be compared and verified against incoming traffic. To further improve security, we can use combination of above techniques. These techniques have their advantages and disadvantages. User on his/her requirement and suitability can choose from these techniques.

VI. REFERENCES

[1]. Jae-Jung Kim and Seng-Phil Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[2]. Anupriya Shrivastava et al, International Journal of Computer Science and Mobil Computing, Vol.3 Issue.6, June- 2014.

[3]. Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No: 04.
[4]. Przemyslaw Kazienko & Piotr Dorosz. Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). www.windowsecurity.com › Articles & Tutorials
[5]. Online]Available: http://www.authenticationworld.com/Token-Authentication.
[6]. The Snort Project, Snort User Manual 2.9.5,May 29, 2013, Copyright 1998-2003Martin Roesch, Copyright 2001-2003 Chris Green, Copyright 2003-2013 Sourcefire, Inc.
[7]. Online]Available:http://www.authenticationworld .com/Authentication-Biometrics.
[8]. Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.
[9]. Online]Available: http://www.duosecurity.com.
[10]. J. Moscola, J. Lockwood, R.P. Loui, and M. Pachos, "Implementation of a Content-Scanning Module for an Internet Firewall," Proc. of 11th IEEE Symp. on Field-Programmable Custom Computing Machines, FCCM 2003, pp. 31-38.
[11]. Online]Available:http://ids.nic.in/technical_letter/ TNL_JCES_JUL_2013/Advance%20Authenticati on%2 0Technique.pdf.
[12]. Stamati Gkarafli, Anastasios A. Economides, "Comparing the Proof by Knowledge Authentication Techniques", international Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2).
[13]. Roger Meyer, "Secure authentication on the internet"As the part of security reading room, SANS institute 2007.
[14]. R. Dhamija, and A. Perrig,"Deja Vu: "A User Study Using Images for Authentication", 9th USENIX Security Symposium, 2000.
[15]. R. Morris, K. Thompson, "Password security: A case history," Comm. ACM, Vol.22, no. 11, Nov. 1979, pp. 594-597.
[16]. B. L. Riddle, M. S. Miron, J. A. Semo, "Passwords in use in a university timesharing environment," Computers and Security, Vol. 8, no. 7, 1989, pp. 569-579.
[17]. S. M. Bellovin, M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," Proc. 1992 IEEE Computer Society Conference on Research in Security and Privacy, 1992, pp. 72-84.
[18]. Haq, I. U. and Yahya, K. M. "Heterogeneous Networks: Challenges and Future Requirements".
[19]. Srilatha Chebrolu, Ajith Abrahama,,*, Johnson P. Thomas, Feature deduction and ensemble design of intrusion detection systems, Elsevier Ltd. doi:10.1016/j.cose.2004.09.008
[20]. TSENG, Y.M., YANG, C.C. AND HAUR SU, J. "Authentication and Billing Protocols for the Integration of WLAN and 3G Networks", 2004.
[21]. Li, S., Zhou, J., Li, X. and Chen, K. "An Authentication Protocol for Pervasive Computing".
[22]. Misbahuddin, M., Premchand, P. and Govardhan, A. "A User Friendly Password Authenticated Key Agreement for Multi Server Environment", November 2009.
[23]. Sumanth Donthi Roger L. Haggard . A Survey of Dynamically Reconfigurable FPGA Devices. 0-7803-7697-8/03/2003 IEEE.
[24]. S. Sinha, F. Jahanian, J. Patel, "Wind: Workload-aware intrusion detection",Recent Advances in Intrusion Detection, Springer, pp. 290-310,2006.