A Modified Hybrid Port Knocking Technique for Host Authentication: A Review

Ms. Pratiksha R. Yewale
Department of Computer Engineering.(CE)
SIPNA COET Amravati, India
pratikshayewale@gmail.com

Mr. Vishwas T. Gaikwad
Associate professor at SIPNA COET Amravati,
India
vtgaikwad@rediffmail.com

Mr. Harshal N.Datir
Assistant Professor at
SIPNA COET Amravati,
India

Abstract- The main objective is to develop and assess the performance of a replacement PK technique, which may avert all kinds of port attacks and meets all network security necessities. Port knock is a crucial conception to secure services provided by the servers. By a predefined port knock sequence server establish whether or not the request could be a legitimate request for a service. The new technique utilizes three acknowledge ideas, these are: port-knocking (PK), steganography, and mutual authentication, therefore, it's mentioned because the hybrid port-knocking (HPK) technique. It are often used for host authentication to form native services invisible from port scanning, give an additional layer of security. During this paper presents analyzing the network security concept of Port knock and assess their quality as firewall authentication mechanisms for gap network ports or activity bound actions on servers. This paper is developing and evaluating the performance of a replacement proposed modified hybrid port knock (MHPK) technique with proposed encryption/decryption technique. The planned technique is to stop completely different –different kinds of port attack and fulfill the complete security demand for network. Planned technique is that the combination of 4 ideas, this are port knocks (PK), symmetric key encryption/decryption, steganography and mutual authentication. Primarily it's the improved modification of hybrid port knocking therefore; it's observed because the modified hybrid port-knocking (MHPK) technique.

Keywords- *Port Knocking, Security, Steganography, Cryptography, Firewall*

*****

I. INTRODUCTION

The Internet will be seen as an enormous network of nodes connected along to produce completely different services. The question that comes is the way to access the servers within the network. This drawback has been self-addressed by following approaches: One will be by employing a firewall, which might management the traffic based on IP addresses. And another will be by victimization additional custom devices like Intrusion Detection and bar Systems. The when putt such efforts towards securing the network, cases of network-attacks area unit usually reportable. In general, the primary step of any attacker is information gathering, within which the attacker tries to search out the entire details of the victim system or net-work just like the services running, ports opened, version variety of some specific software’s etc. within the second step, attackers attempt to ascertain each the present and zero-day vulnerabilities within the version of services, and will exploit those vulnerabilities to cause breach of confidentiality, integrity or availableness problems. The primary line of defense against any attack is system's firewall. The firewall is used to limit the resources of any network connections. A firewall works on predefined set of rules in keeping with that it accepts or rejects any packet. These rules could also be based mostly upon the IP addresses or another characteristic. .To avoid the such issues port knock technique is use, Port knock may be a quite security mechanism put in over firewall of secure computer systems. PK close all ports of the system on that it's enforced, it additionally works on the principle of least privileged because it blocks all the unauthorized users initially and that we will say that there's a comprehensible improvement within the security thereto of a system with no port knock mechanism. Port knock [3] is acceptable for users who need access to servers that aren't publically accessible. Port knock refers to a technique of communication between two computers, sometimes a client and a server, within which the knowledge is encoded and probably encrypted in to a sequence of port numbers. This sequence is termed as knock sequence. The server will keep all its ports closed however open it on demand if users have genuine themselves by providing a selected knock sequence (a type of password). Initially all the ports on the server square measure closed for public communication and therefore the server is watching all the makes an attempt to attach to the services. Port knock is that the protected services don't need any modification. Port knock is simple to line up and presents no performance problems once addressing a modest range of incoming connections. Cryptography has the power to supply variety of services that aid us in protective our data in varied ways in which because it is distributed across networks or hold on on physical media. Confidentiality may be a crucial element of network communications once non-public data is being hold on or transmitted. The use of encryption has allowed us to protect such information and prevent it being disclosed to unauthorized parties. Similarly, knowledge integrity ensures that our data is not modified in transit, which we are able to trust that the knowledge received is as supposed. The marginally additional up to date field of public key cryptography has the additional ability of providing non repudiation whereby it is established that a personal did so send a particular piece of data. Cryptography has established to be very vital in authentication protocols, because it is critical sure enough items of data to be shielded from unauthorized modification so as to end in victorious authentication. In this paper we explain the concept of hybrid port knocking and modified hybrid port knocking techniques.

II. Port Knocking

A. Ports

Those unaccustomed to host-based networking typically have hassle coming back to terms with the notion of a port on a computer. Within the simplest of terms a port may be a virtual door (represented by a 16-bit integer) that permits the compute to stay track of that items of information is destined that application or service. Networking (transport layer) protocols like TCP (Transmission management Protocol) and UDP (User Datagram Protocol) each use the thought of a port once sending packets to and from networked hosts. The port number (when used) is enclosed in networking packets

B. Port knocking

Port knock may be a variety of host-to-host communication within which info flows across closed port. It is additionally known as Spread-Spectrum TCP technique. There are varied variants of the port knock methodology – information could also be encoded into a port sequence or a packet-payload. In general, data are transmitted to closed ports and received by an observance daemon that intercepts the knowledge while not causing a receipt to the sender. It is a technique of communication between two computers that is in between client and server within which info is encoded, and presumably encrypted, into a sequence of port numbers. This sequence is termed the knock. Initially, the server presents no open ports to the general public and is observance all affiliation makes an attempt. The client initiates affiliation makes an attempt to the server by causing SYN packets to the ports per the knock. This method of knock is offers port knock its name. The server offers no response to the client throughout the knock part, it as “silently" processes the port sequence. once the server decodes a sound knock it triggers a server-side method.

Example of port knocking:

As a simple example of port knocking, a server would close all ports and log requests to a specific port range; either TCP or UDP ports can be used. If a client transmits packets to a specific sequence of server ports (for instance, 1145, 1087, 1172, 1244, and 1031, in that order), then the server would perform some action (such as opening the SSH port to the client host). Here, the port sequence is a shared secret between the user and the server; knowledge of the secret implies that the user is authorized to access the protected service.

C. Type of Port Knocking

There are the two types of port knocking. one is Cryptographic port knocking and another one-time port knocking.

1. Cryptographic port knocking:

The particular method is to compute a ***MAC or hash*** include some value that is known to the server, such as a nonce (a value that is used no more than once for a given purpose) or timestamp, in the plaintext; on receipt, a server would decrypt the message and verify that the expected value is present.

2. One –time port knocking:

The most secure category of existing port knocking systems consists of that use one-time passwords (OTP) or timestamps. Due to the one-time nature of the authentication messages generated by these systems, they are resistant to replay attacks and, when properly implemented, give no information about any master keys in use.

D. Advantage and Disadvantage

The advantages of the port knocking technique are
Follow: [1]

1. Virtually not possible to see whether or not port knockings enforced on the server machine or not.
2. Detection by sniffing is much tough.
3. it's a firewall based mostly methodology for user authentication for non-common services.
4. Establishes connections to the hosts with no open ports by the subversive use of closed ports.
5. Edges from access management provided by IDS and firewalls.

Disadvantage of Port Knocking

A. Lack of association between authentication and connection

An attacker may hijack a in successful authentication by blocking any transmissions from a client when it authenticates. This drawback is very severe within the presence of NAT; to a server that has obtained the public IP address of a client, all hosts that share the client’s public address look alike.

B. Susceptibility to Denial-of-service Attacks

There are several possible denial-of-service attacks against port knocking servers. Mattock pointed out that an attacker could prevent a client from authenticating by sending packets with the client’s source address to random ports on the server while the client is trying to authenticate. Manzanares suggested that an attacker could affect a resource-consumption attack against a known port knocking server by sending packets with random forged source addresses to random ports.

E. Problems Associated with PK Techniques:

In order to extend network security, it's generally desirable to permit access to open ports on a firewall solely to approved external hosts (users) and gift closed ports to any or all others. the foremost obvious way to limit access to open port is to want users to authenticate themselves before granting them access open port is to require users to authenticate themselves before granting them access. There are number of techniques that are developed by several researchers to create port authentication, such as: PK, single packet authentication (SPA), or use a light-weight concealmentprotocol.The investigations on the performance of those techniques in avoiding all possible type of port attacks (e.g., 0-dayattacks, TCP-replay attacks, dictionary-based attacks, and brute-force attacks) have incontestable that most of those techniques suffer from either one or a lot of the following problems:

- 0-day attacks.
- The sequence replay attack.
- Minimal data transmission rate.
- Knock sequences and port scans.
- Knock sequence busting with spoofed packets.
- Failure if a client is behind a NATed network.
- Failure if packets are received/delivered in out of Order.
- A lack of association between authentication and connections being opened

III. Problems in existing port knocking systems:

Existing port knocking authentication Systems, the following three major problems present in most or all of them:

1. Out-of-order packet delivery:

Port-knock sequences typically contain 64 to 160 bits, and are usually sent at 8 bits per packet. Proper decoding of port-knock sequences by most servers is dependent on the order of arrival. According to Bennett al. [6], on certain busy Internet backbone routers, the probability of out-of-order delivery of at least one packet out of a burst of 20 can be greater than 90%.2 Of the port knocking systems

2. Network Address Translators (NATs).

If traffic from a shopper passes through a NAT [8] on the way to a server, and therefore the client's (private) IP address is encoded within the authentication token, then the authentication exchange, if prospering, can lead to the correct port being opened to the wrong client address. If the general public IP address is encoded within the token, then the port are opened to all or any hosts sharing the same public address. If the client's address is not encoded within the token the least bit, then the general public address from the packet headers would possible be used, resulting in identical drawback. No systems that we tend to found totally self-addressed this issue.

3. Lack of association between authentication and connection.

In no system that we found is there a logical association between the authentication sequence and the connection that is created after a port is opened. It is possible for an attacker to hijack a successful authentication by blocking further transmissions from a client and assuming its identity to a server after authentication has completed, but before a connection has been opened.

IV. HYBRID PROT KNOCKING TECHNIQUE

They developed their models making an attempt to avoid all attainable types of port attacks that will threat network security. The description of a brand new PK technique which will be used for economical, reliable, and efficient host authentication, known as the hybrid PK (HPK) technique. There are seven steps in HPK Technique. That are Traffic monitor, Traffic capturing, Traffic capturing, client authenticating, Server authentications, Proving the identity of the client, Port closing etc

1. Traffic Monitoring:

It is first steps of Hybrid port knocking in which a PK server is put in behind the network Firewall or entranceway and observation and checking traffic arrived to firewall.

2. Traffic capturing

In this step, the PK server captures only the traffic holding a payload (image) for further processing.

3. Image processing

In this step, the PK server extracts the payload (image) from the received packet. The payload is meant to cover some data using Steganography which will be used prove the knocking identity and request. If the payload, contains encrypted data, that is demand to encryption/decryption rule to access supposed data

4. Client authenticating

Client authenticating is four steps in HPK technique. During this step, when the PK server makes certain that the payload or image was carrying associate degree encrypted request, it has to certify that it's act with the correct client, thus it takes a random range and encrypts it using the client GnuPG public key and sends it as a payload to the client

5. Server authentications

In this step, the client now receives the packet carrying the encrypted payload, extracts it and decrypts it using the servers GnuPG public key. Then the client sends the random number as a payload back to the PK server to ensure its identity.

6. Proving the identity of the client

The PK server is still in the monitoring/sniffing state and receives the reply from the client to its random number check. The server extracts the payload and checks if the received message holds the same number as the one randomly generated and sent to the client.

7. Port closing

Finally, in this step, after the task is completed, either the client informs the PK server to close the port, or the PK server decides to close the opened port.

V. PROPOSED TECHNIQUE

Proposed Architecture**:** The HPK technique defines in [4] consists of seven main steps. Here proposed MHPK technique consists of only four main steps which are define in figure 1

1. Packet Capturing and Packet De-multiplexing
2. Authentication
3. Confidentiality
4. Port Closing

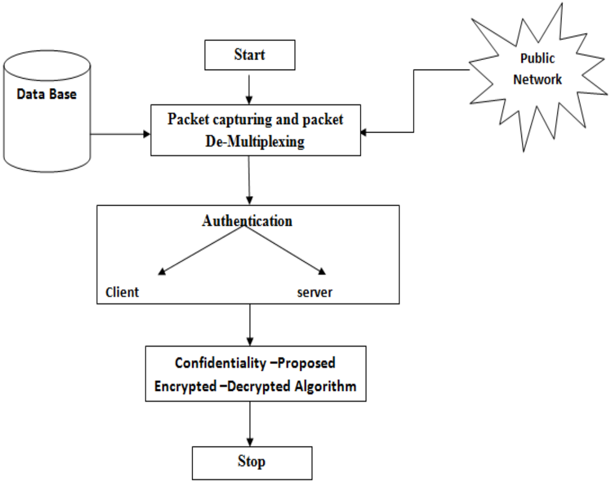
Start
Public
Network
Data Base
Packet capturing and packet
De-Multiplexing
Authentication
Client
server
Confidentiality –Proposed
Encrypted –Decrypted Algorithm
Stop

Fig.1 Block diagram of Proposed Technique

A. Modified Hybrid Port Knocking Technique:

The proposed technique is use for design port knock and port knocks system with high security. It is avert different-different form of port attacks and fulfill the whole security demand for network. Proposed technique is that the combination of four ideas, these are port knock (PK), symmetric key encryption/decryption, steganography and mutual authentication. During this model combine two t different Technique that are port knock and Cryptography. Proposed idea are going to be extremely secured and economical therefore this proposed technique can called “Modified Hybrid Port-Knocking (MHPK)” technique. Port knock system use a cryptographically-secure challenge response authentication system that accounts for out-of order packet delivery and part addresses the complications caused by NATs. [3] The MHPK technique consists of 9 main steps are as follows

1. Traffic monitoring

In this step, a PK server is installed behind the network firewall, as shown in Fig. 2, monitoring and checking traffic arrived to firewall or gateway

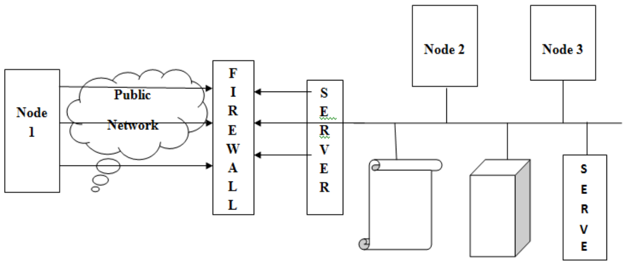

Fig 2. Traffic Monitoring

2. Traffic capturing and analyzing:

In this step, the PK server captures only the traffic holding a payload (image) for further processing, as shown in Fig. 3. In this figure, for example, only Traffic #3 is captured for further processing because it contains an image

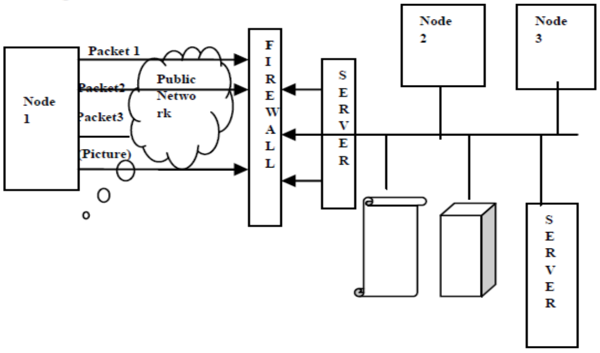

Fig 3 . Traffic Caputuring

3. Image processes and Cryptography Functioning

In this step, the PK server extracts the payload (image) from the received packet. The payload is supposed to hide some information using Steganography that can be used to prove the knockers identity and request. If the payload, contains encrypted information, which is demand to encryption/decryption algorithm to access intended information, see figure (4).

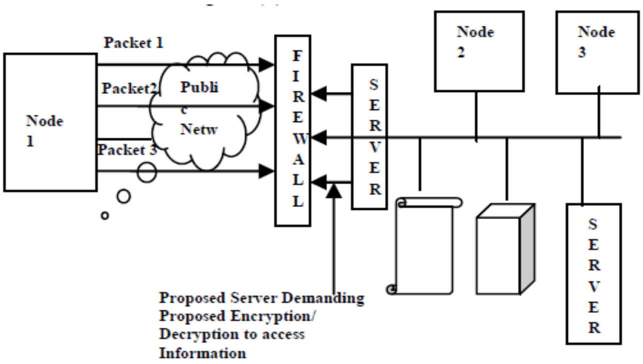

Fig 4. PK server deamanding encryption / decryption algorithm to access Information

4. Client authenticating

After the PK server makes sure that the payload was carrying an encrypted request, it needs to make sure that it is communicating with the correct client, so it takes a random number and encrypts it using the clients GnuPG public key and sends it as a payload to the client.

5. Server authentications

The client now receives the packet carrying the encrypted payload, extracts it and decrypts it using the servers GnuPG public key. Then the client sends the random number as a payload back to the PK server to ensure its identity.

6. Proving the identity of the client

The PK server remains within the monitoring/sniffing state and receives the reply from the client to its random number check. The server extracts the payload and checks if the received message holds a similar range because the one every which way generated and sent to the client.

7. Key Exchanging

After checking legitimacy between client and server key exchange step can follow. During this step client and Server changed radically symmetrical key through GNUPG public key technique.

8. Proposed Encryption/Decryption

After key exchanging between client and server. Server referred to as encryption/decryption method to access correct encrypted information from payload of the image. If the message is known then the PK server executes the opening/closing of the requested port on the firewall, or executes the remote command supported the client's request. If the payload, contains supposed info, that is either to demand the firewall to open/close a port for the consumer as shown in Fig. 5, or execute a command remotely on the acceptable server as shown in Fig. 6. Otherwise, if the result of the image process fails to reveal valid authentication parameters, the PK server blocks the information IP of the supply that sent the knocks and therefore the payload or image.

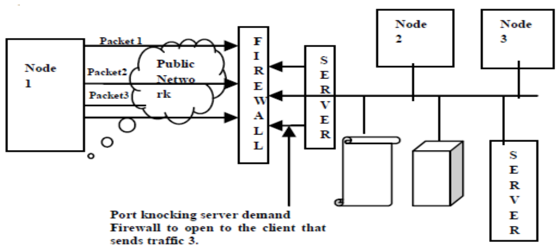
Packet 1
Packet2
Packet3
Node 1
Public Network
FIREWALL
SERVER
Node 2
Node 3
SERVER
Port knocking server demand Firewall to open to the client that sends traffic 3.

Fig 5. PK server demanding Firwall open /close port

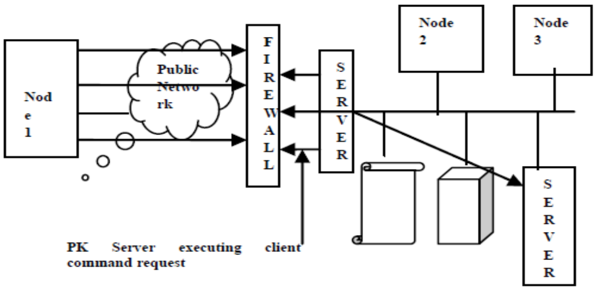

Fig 6. PK server executing client command request

9. Port closing

Finally, during this step, once the task is completed, either the client informs the PK server to shut the port, or the PK server decides to shut the opened port once fixed silent amount there on open port as shown in fig 6.

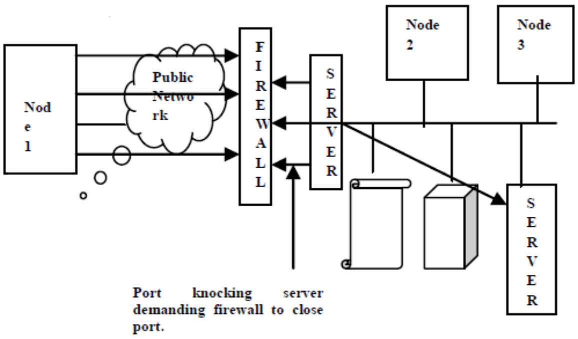

Fig 7. Port closing

The difference between existing and proposed port knocking technique is the encryption/decryption algorithm used by proposed technique to provide strong authorization. Proposed modified hybrid port knocking technique is just like existing port knocking technique but number of steps has shuffled up and down and added two more steps. These two steps are key exchanging and proposed encryption/decryption which is described above. Due to this encryption/decryption step proposed port knocking technique produced more good results.

CONCLUSION

Port knocking is used to prevent all possible port attack that may threat network security. It is also used to secure service provided by server. Port knocking can be used to construct authentication systems on firewalls with the goal of only allowing authorized users access to open ports. The conclusions of this proposed work are as follows, with the help of HPK and MHPK technique. The MHPK technique can be easily implemented in Java/.Net Technology and HPK technique can be easily implemented on any GNU/Linux firewall box. The both technique is much more secure than the traditional PK and the single packet authentication techniques. The communication protocol used is a simple secure encryption scheme that uses GnuPG keys with Cryptography and Steganography construction are both in HPK and MHPK technique. The HPK technique is immune to a TCP replay Attack, because it uses cryptography and Steganography within the TCP payload, and mutual authentication to authenticate both parties together. In other, MHPK technique is prevent different type of attack, because it uses cryptography to authorization and integrity, and Steganography for confidential and reduce packet capturing overhead, and mutual authentication to authenticate.

REFERENCES

[1] B. Rudis. The Enemy Within: Firewalls and Backdoors. Securities focus, June 2003. Available at http://www.symantec.com/connect/articles/enemy - Within firewalls-and-backdoors. Access Date 16-07-2010.

[2] W. Sonnenreich and T. Yates. Building Linux and OpenBSD Firewalls, Wiley, New York, 2000.

[3] A. Tongaonkar, A. Tongaonkar, N. Inamdar, and R. Sekar. Inferring Higher Level Policies from Firewall Rules Proceedings of 21st Large Installation System Administration Conference (LISA '07), USENIX Association, pp. 17-26, Dallas, USA, November 2007.

[4] J. Song, H. Takakura, and Y. Kwon, a Generalized Feature Extraction Scheme to Detect 0-Day Attacks Via IDS Alerts Proceedings of the 2008 International Symposium on Applications and the Internet - Volume 00, IEEE Computer Society Washington, DC, USA, 2008

[5] Ali Hussein, 2010, "A Hybrid Port-Knocking Technique for Host Authentication", Ph.D. Thesis, University of Banking and Financial Sciences.

[6] Python Programming Language http://www.python.org

[7] Traian Popeea, Vladimir Olteanu, Laura Gheorghe, Răzvan Rughiniș “Extension of a port knocking Client-server architecture with NTP synchronization” IEEE 2011

[8] Dr. Hussein Al-Bahadili and Dr. Ali H. Hadi “Network Security Using Hybrid Port Knocking” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, Aug

[9] Di Gioia P., “Behind Closed Doors: An Evaluation of Port Knocking Authentication’. Donald Bren School of Information and Computer Sciences, University of California, Irvine 2004.

[10] Dr. Hussein Al-Bahadili and Dr. Ali H. Hadi “Network Security Using Hybrid Port Knocking” IJCSNS International Journal of Computer Science And Network Security, VOL.10 No.8, August 2010.