Network Service's Concealment through Port Knocking

Yousaf Bin Zikria, Syed Noor-ul-Hassan Shirazi, Khurram Murad, Nassar Ikram

Abstract—**An open door is a temptation for theft. In today's cyber space, novel ways of intruding into network compel security professionals to build supplementary security layers. The concept of obscuration and concealment for securing the servers from intruders is an ongoing debate. Different architectures are proposed in this regard. We are proposing a new architecture for securing network services through concealment using port knocking. In this way, we are accumulating another layer to existing security onion. Our architecture uses amalgamation of port knocking, VPN and PKI infrastructure to secure backend services like HTTPS, SSH, hence improving the security posture of the existing architectures.**

Index Terms— **Firewall, IPS, PKI, Port Knocking, VPN**

I. Introduction

NEW techniques of intruding and compromising the systems are on the rise which fuels the race between the attackers and network defenders. Both are trying to getting ahead of each other, network defenders are proposing innovative protection features and architectures to make their defense stronger and so are the attackers in creating new attacks. In today's world of vulnerability disclosure, exploit releases, worms, and script kiddies, and the use of internet at ease has become an increasingly hostile environment for businesses and home users alike. Advanced tools which are at anyone's disposal allow attackers to easily discover networked machines, enumerate ports and services running on them, and to ascertain whether or not those particular services are vulnerable to a particular exploit.[1,2]

Military and corporate networks are being targeted for past several years. Attackers are trying to steal information from military networks for their bad intents, establishment of cyber army's from different countries are another big concerns for all whereas intruders for the sake of financial gain can steal information and that can impact company's credibility and affect loss.

Foremost difficulty in protecting servers is that they are, for the most part, visible and happy to disclose information to anyone who asks. If an attacker finds a corporate FTP server, he can connect to it to know what version of FTP software is running if not hardened. He can then use this information to check whether or not that version of the software is vulnerable to a particular attack which would give him root access to the server machine or there exist another threat of zero day exploits. One simple way to protect is to turn off all unnecessary services. The notion of this gives life to port knocking and this is the key for our proposed architecture.

This paper is organized as follows. Section 2 gives preliminaries on port knocking, firewall, IPS, VPN and PKI which are critical part of our proposed architecture. Section 3 provides detail of proposed architecture. In section 4 we discuss defense in depth as a result of proposed architecture. Finally in section 5, we present our conclusion.

II. Preliminaries

The Port knocking is a method for transmitting information across closed ports, with the aim of authenticating users before giving them access to a protected service. The name "Port Knocking" originated with Martin Krzywinski in 2003[3] and refers to the concept of sending packets to predetermined network ports [4]. The basic idea was discussed as early as 2001, posted on a German Linux User Group mailing list [5].

Public key infrastructure is a security infrastructure that combines security mechanisms, policies, and directives into a system that is targeted for use across unsecured public networks (e.g., the Internet), where information is encrypted through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI is targeted toward legal, commercial, official, and confidential transactions, and includes cryptographic keys and a certificate management. PKI uses one or more trusted systems known as Certification Authorities (CA), which serve as trusted third parties for PKI. The PKI infrastructure is hierarchical, with issuing authorities, registration authorities, authentication authorities, and local registration authorities.

Virtual Private Network (VPN) is an encrypted network-to-network virtual tunnel that connects trusted endpoints. Both the VPN server and client must authenticate to each other. It connects two networks, like branch offices, or lone remote users to the office.

Firewall is a system that is the sole point of connectivity between the trusted and un-trusted parties.It provides access control by restricting which messages it will relay between the sites and the rest of the network.

Intrusion prevention system (IPS) is a security system that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

III. Proposed Architecture

In proposed architecture, we have added another security layers to the existing security onion. This will make tougher for the attacker to break into the systems those are built using existing technologies. The proposed architecture is shown in Fig. 1, consisting of three servers: green server, red server and PKI server. It has been tacit that servers are properly patched and no known vulnerabilities exist on servers.

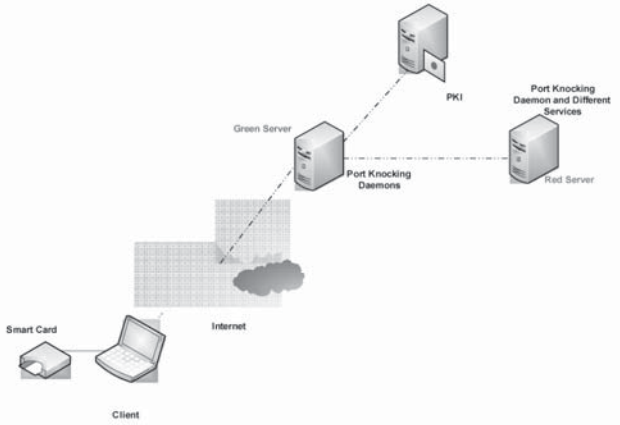

Fig. 1. Proposed Architecture

The green server plays very vital role in whole architecture. Firewall, IPS, VPN and port knocking daemon are also running on the same server. PKI server generates the certificates that clients will carry in smart card to get authenticated. Green server also serves as gateway for client to get authenticated using client's digital certificate with PKI, once a VPN tunnel is established between green server and client.

The services desired by clients is actually running on red server which is behind security layer of PKI and green server, Once client is authenticated and authorized by green server another port sequence will be sent to red server by green server to open required port for secure communication. Flexibility of client to use desired services is dependent on the fact that client can use internet at ease and has valid digital credentials and port knock sequence. Detail flow involved for secure communication is as follows:

i. Client initiates the connection by sending correct port knock sequence to green server.

ii. Green server in response open port which will be used to establish VPN tunnel between client and green server as shown in Fig. 2.

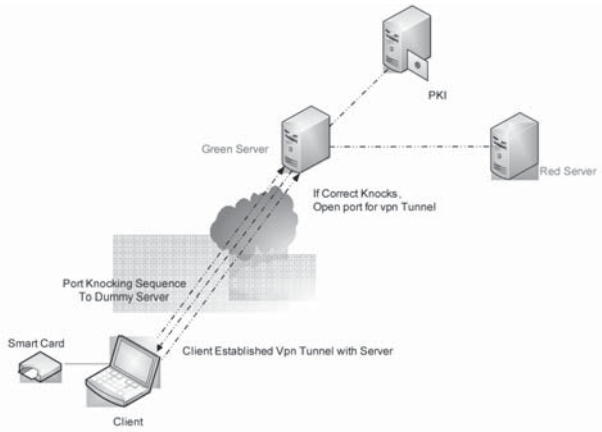

Fig. 2. Initial Establishment of client and green server

iii. After establishment of VPN tunnel, Client sends the smart card credentials via VPN tunnel to the green server which then authenticates the credentials with PKI as shown in Fig. 3. and triggers the second port knocking daemon which opens port for communication between client and red server.

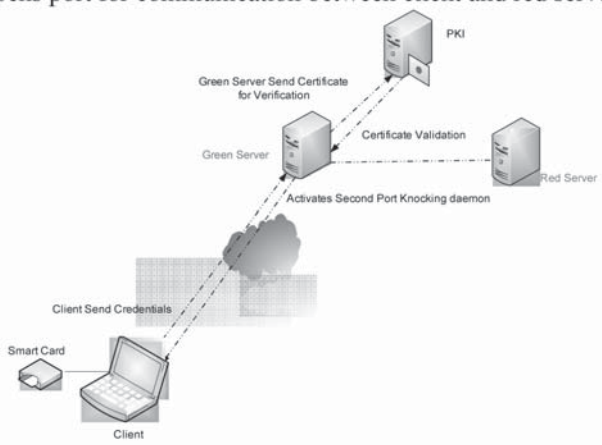

Fig. 3. Triggering second port knocking daemon.

iv. Client would request a service but this request would again be using port knock sequence for which port knocking daemon is triggered earlier. Client sends a new port knocking sequence over the VPN along with service request. Green server validates the port knocks and if it is in correct order send predetermined port knocking sequence over the VPN to the red server for required service. Server verifies the port knocking sequence and if correct opens the desired service for client and send the port number to the green server. Green server sends the IP and port number to the client for communication. Client established the VPN tunnel with server using the information provided and use the service as depicted in Fig. 4.

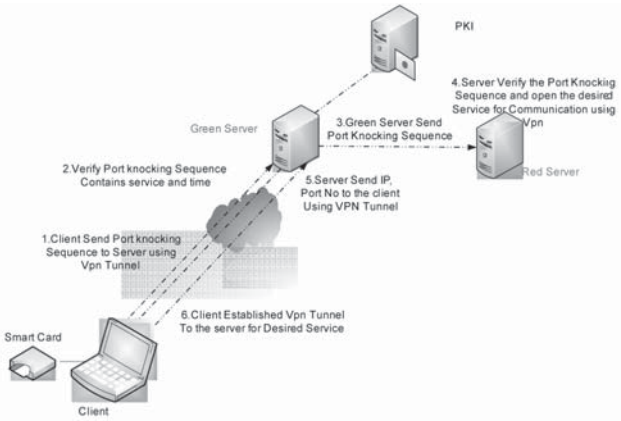

Fig. 4. Request for Service

v. Client sends closing port knocking sequence to the green server over the VPN. Green server verifies and sends port closing sequences to the server. It terminates every communication with the client and closes the port. Green server set sleep to the second port knocking daemon, close all the communication with this client and close the ports if no other client is connected. This is depicted in Fig. 5.

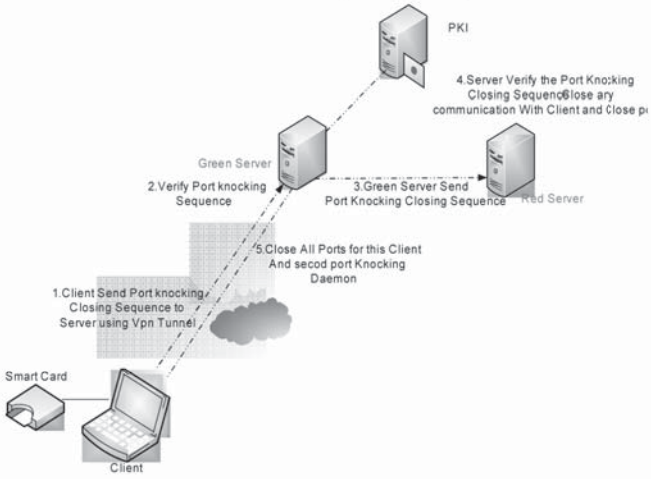

Fig. 5. Secure Termination

IV. Defense in Depth

Primary scan to the server reveals naught as it is a black hole. Attacker has to first overwhelm the initial port knocking daemon to ensue. If attacker finds vulnerability in port knocking or somehow gets the port knocking sequence by eavesdropping, he will replay those packets and scan again. At that moment IPS will sense the scan and instruct firewall to block this IP for any communications. Firewall and IPS are our first line of defense against the attackers. However, if the attacker defeats the IPS somehow, this requires port to establish the VPN tunnel with the server .This may not be achievable without having the valid credentials. The last security layer is the second port knocking sequence to the server without which the green server will not request the red server to open the desired service for the client. Our layered approach makes it virtually impossible for the intruder to break into the system.

V. Conclusion

We have proposed the new architecture by using Firewall, IPS, Port Knocking, VPN and PKI to provide defense in depth for our mission critical servers. Assorted exploits are kept in mind and we have tried to harden against all of these. Layered approach followed in the proposed solution results in fortifying the network so that mission critical services are offered risk free but this comes at the cost of additional hardware and processing delays; something affordable in view of criticality of services offered.

References

[1] Computer Emergency response Team Coordination center (CERT-CC) (2002), http://www.cert.org/archive/pdf/attack_trends.pdf
[2] Computer Emergency response Team (CERT) (2005), http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2005.pdf
[3] An Analysis of Port knocking and Single Packet Authorization by Sebastien Jeanquier.
[4] Krzywinski M. (2003) Port Knocking:Network Authentication Across Closed Ports. SysAdmin Magazine, pp 12:12-17
[5] Borss C. (2001) DROP/DENY vs. REJECT. Listserv post to Braun schweiger Linux User Group, https://www.lk.etc.tu-bs-de/lists/archiv/lug-bs/2001/msg05734.