International Journal of Information Technology and Management

Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

NETWORK SECURITY USING FIREWALL AND CRYPTOGRAPHIC AUTHENTICATION

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

Network Security Using Firewall and Cryptographic Authentication

Anand Pandey

Assistant Professor, Dr. Bhim Rao Ambedkar University, Agra

Abstract – The network Security is the hottest topic in the current research scenario. The information security is really threatened by obnoxious users. With increasing vulnerabilities, caused by port scan attacks, replay attacks and predominantly IP Spoofing, targeting services, the network behavior is getting malevolent. But there is a lack of any clear threat model. The authors have endeavored to consider this problem in order to improve the network security and enhance secure shell daemon protection. A mechanism, QUICKKNOCK, improving upon the potentialities of technologies such as port knocking and SPA (Single Packet Authorization), using Firewall and Cryptography, has been proposed.

Keywords: QUICKKNOCK, SSH Daemon, Network Security, Port knock, Encryption algorithms, IP Spoofing, Symmetric Cryptography

----------X----------

INTRODUCTION

Security in communication is a crucial research area because of the complex technical nature involved in data transmission. The problem creeps in when the intention of the one of the users connecting with the network becomes bad .The increased vulnerabilities, cause replay attack dictionary attack , IP Spoofing and packet crafting etc. [1,2,3]. Security attack is an action which compromised the security of information owned by an organization. If a server runs on non-vulnerable software, a port scan is not a serious threat, but in case of non-patched and 0-day exploit software it becomes big threat. A popular method of protecting against such network attacks is the firewall, which simply blocks all connection attempts to “internal” network hosts from “external” ones. One class of proposed solutions to this problem is “port knocking” wherein a firewall is deployed to protect a server, but before allowing a client connection to a particular service, the client must transmit an authenticated knock. But the goal of a port knocking scheme to conceal the set of services running on a network host, through existing implementations have serious flaws[4, 5, 6].

Port knocking schemes generally use the port number within the TCP or UDP header to transmit information from the client to the server, whereas its successor Single packet authorization (SPA) scheme uses messages to be sent over any IP protocol; not just those that provide a port over which data is communicated. Improving upon Fwknop(Firewall Knock Operator) currently supports sending SPA messages over ICMP or TCP. The technique Port Knocking and SPA has been used interchangeably. The above issues has been addressed and tried to be sorted out with modified enhanced approach [7].

REVIEW OF LITERATURE:

In this paper, we have developed a formal security model QUICKKNOCK which captures above notion. A formal security model is critically important in order to be certain that a given protocol, even one that seems secure at a glance, is secure in true sense. Examples of such “apparently secure” protocols, developed without formally stated security goals, are numerous [8, 9, 10] and some of them have been in operation for years (and have even become industry standards). So much so all those protocols were originally designed for security, and even used well-known cryptographic primitives, but the protocols were not secure[1,14].

SINGLE PACKET AUTHORIZATION (SPA):

SPA is a method of limiting access to server and network resources by cryptographically authenticating legitimate users before any type of TCP/IP stack access is allowed. The predominant researcher Michael Rash has given authenticated and effective solution to this security issue using Fwknop [11]. Through which an authenticated single packet has been sent to access services(daemons) that resides on the servers with IP address range. The firewall is reconfigured in such a way that only authenticated packet from legitimate IP address is received by the server in a default-drop stance.

SYSTEM DESIGN:

In this section ,the new modified scheme QUICKKNOCK, has been introduced and implemented, displaying secure port knocking scheme, and discuss how this enhanced security model implementation averts number of limitations of previous systems which only attempt to authenticate the start of a connection [14, 15], but provides no guarantee that connections stay authentic. In other words, previous implementations does not protect against attacks such as connection hijacking, IP spoofing, packet crafting, client/server synchronization, and in distinguishability [11]. Next comes the analysis of number of possible attacks on these implementations. Finally, the results are graphically shown using Afterglow. QUICKKNOCK is designed to be an application-agnostic transport-level authentication layer. It prevents forgery and IP spoofing, packet crafting while hiding the presence of authentication scheme. The kernel hooks has been used to ensure that applications do not need to explicitly support the system in order to benefit from it.

PROTOCOL USED:

The QUICKKNOCK Pseudo Code is outlined. Which has addressed the vulnerabilities of previous Implementations? A QUICKKNOCK client starts a connection which is composed of a TCP SYN packet to a QUICKKNOCK-enabled server and steganographically embeds an authentication token into the packet. The embedding algorithm and resulting packet header structure has been described respectively. The server receives a SYN packet and extracts the authenticator. If verification is successful, the server allows the connection to continue, otherwise the packet is dropped. The client and server share a key, as well as a counter which is incremented for every client connection attempt. The counter prevents IP spoofing, packet crafting by ensuring that every SYN packet sent by the client is different from any packets sent previously, and is also used as the nonce required by the MAC function. The key, initial counter and resynchronization interval are exchanged out of band, since negotiation is impossible in case of single-way communication.

- **MAC:**

A Message Authentication Code (MAC) is a short piece of information, similar to a hash code. It provides both original authentication and integrity protection of a message .The use of keyed MAC is preferred to additional series of knocks , applying it to the source and destination (IP, port) tuples as well as the counter, so every connection attempt is guaranteed to contain a unique MAC. The algorithm Poly1305-AES is deployed, for MAC function since it is designed specifically to work on small bits of data such as network packets and is implemented in optimized assembly for a number of popular platforms. The connection counter serves as the nonce required by Poly1305-AES. Considering that AES is a pseudorandom permutation, an attacker should not be able to compose a valid MAC, or even identify one from random bits, for the next SYN packet without knowing the key, keeping in view its visibility to outer world. MACs are generated by block ciphers and use symmetric secret keys to ensure that only those who know the key can modify, or verify the message.

CONCLUSION:

The schemes used in the existing PK/SPA implementation were flawed and vulnerable to attacks such as IP spoofing , packet crafting , connection hijacking , DDoS, No guarantee of backward and forward secrecy since the same keys were used. In addition to this, other issues which are such as usability to differentiate between port scans and port knocks ignore IP address which have flooded firewall with bogus packets, code complexities for embedded port knocking techniques using symmetric and asymmetric ciphers, limited packet loss while authenticating packets. By utilizing only single packet as we have designed a more secure SPA based authentication scheme QUICKKNOCK which withstands some of these attacks. The current scheme is capable for recovery from packet loss while authenticating, differentiates port scans and port knocks. There is also an improvement avoiding code complexity in existing implementations for embedded port knocking techniques such as symmetric and asymmetric ciphers.

REFERENCES:

[1] Sebastian Janquier (2006) “An Analysis of Port Knocking and Single Packet Authorization”: Master’s Thesis University of London.

[2] Feng T., Wang S., Yuan Z.-T.UC secure network coding against pollution attacks(2012) Information Technology Journal, 11 (9), pp. 1175-1183.

[3] Bellovin, S.M.: Security problems in the TCP/IP protocol suite. SIGCOMM Comput.Com- mun.Rev. 19(2), 32–48 (1989).

[4] Barham, P., Hand, S., Isaacs, R., Jardetzky, P., Mortier, R., Roscoe, and T.: Techniques for lightweight concealment and authentication in IP networks. Technical Report IRB-TR-02-009, Intel Research Berkeley (July 2002).

[5] Rash Michael (2007) Available at Website http://www.cipherdyne.org/fwknop/docs/SPA .htm,

[6] Jaggi, S., Lang berg, M., Katti, S., Ho, T., Katabi, D., Medard, M., Effros, M.Resilient

network coding in the presence of byzantine adversaries (2008) IEEE Trans. Inform. Theory. 54, pp. 2596-2603.

[7] Kumar Rajesh, TalwarI. M, KumarKapil , " A Modified Approach to Analysis and Design of Port Knocking Technique", International Journal of Computational Intelligence and Information Security(September 2012) Vol. 3 (7), pp. (28-39)

[8] Fluhrer, S., Mantin, I., Shamir, A.: Attacks on RC4 and WEP. RSA Laboratories, Crypto-bytes 5(2) (2002)

[9] Bleichenbacher, D.: Chosen cipher text attacks against protocols based on the RSA encryption standard PKCS# 1.In: Krawczyk, H. (ed.) CRYPTO 1998LNCS, vol.1462, pp.1-12.Springer, Heidelberg (1998)

[10] Smits R., Jain D., Pidcock S., Goldberg I., Hengartner U. "Bridge SPA: Improving tor bridges with single packet authorization" (2011)Proceedings of the ACM Conference on Computer and Communications Security, pp. 93-101.

[11] M. Rash "Single Packet Authorization with fwknop" The USENIX Magazine, vol 31, no1, Feb 2006.pp63-69[Online] Available http://www.usenix.org/publications/login/2006 02/pdfs/rash.pdf.

[12] Agrawal S., Boneh, D. Homomorphic MAC's: MAC based integrity for network coding (2009) Applied Cryptography Network Security, 5536, pp.292-305.

[13] Murdoch, S.J., Lewis, and S.: Embedding covert channels into TCP/IP. In: Barni, M., Herrera- Joancomart´ı, J., Katzenbeisser, S., P´erez-Gonz´alez, F. (eds.) IH 2005. LNCS, vol. 3727, pp. 247–261. Springer, Heidelberg (2005)

[14] Eugene Y. Vasserman, NicholasHopper, JohnLaxson, and James Tyra "SILENTKNOCK: Practical, Provably Undetectable Authentication Vol.8, pp. 121-135 (2009).Available at http://sclab.cs.umn.edu/node/151

[15] Wang, Y.Insecure "Provably secure network coding" and homomorphic authentication schemes for network coding (2010) IACR Eprint Archive.