International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

A Review of the Adoption of IPSEC Concept in Securing Web Servers

[1]AMADI E.C., [2]ADJOGBE O. F., [3]NNONYELU H.U., [4]BENAFE C.

[1-4]Department of Information Management Technology, Federal university of Technology, Owerri, Imo State, Nigeria

ec.amadi@gmail.com

Abstract

This paper presents an in depth view of the adoption of internet protocol security (IPsec) in the management of web servers in the areas of security challenges. This concept has grown over the years due to the necessity and need to secure daily, the online resources we share and retrieve. The performance of different Web server architectures is evaluated in the context of a single implementation in order to quantify the impact of a server's concurrency architecture on its performance. This research presents a detailed information model about Internet Protocol Security (IPsec) policy designed to facilitate agreement about the content and semantics of IPsec policy, and enable derivations of task-specific representations of IPsec policy such as storage schema, distribution representations, and policy specification languages used to configure IPsec enabled endpoints. The information model described in this research explains the configuration parameters defined by IPsec.

Keywords—HTTP, Server, WWW, Web server, IPsec

I. Introduction

With the widespread in the use of the World Wide Web (WWW), webservers are expected to keep up with the ever increasing demand of users. The performance of Web servers plays a vital role in meeting the needs of large and growing users of the Web. A high performing Web server reduce the hardware cost of meeting a given service demand and provide the flexibility to change hardware platforms and operating systems based on cost, availability, or performance considerations. Web servers rely on caching of frequently requested Web content in main memory to achieve throughput rates of thousands of requests per second, despite the long latency of disk operations. Since the data set size of Web workloads typically exceed the capacity of a server's main memory, a high performing Web server must be structured such that it can overlap the serving of requests for cached content with concurrent disk operations.

II. Definition of Terms

Hypertext transfer protocol: it is an application protocol for the distribution of hypermedia and text information system. It is the foundation of data communication for the world wide web (www)

Server: A server is a computer program or a device that provides functionality for other programs or devices called clients. Servers can provide various functionalities often called services, such as sharing of data or resources among multiple clients or performing computations for client

World Wide Web (www): It is an information space where documents and other web resources are identified by a uniform resource locator (URL) interlinked by hypertext links and can be accessed by users.

Web server: A web server is a computer system that process request through hypertext transfer protocol (HTTP), the basic protocol used to distribute information on the World Wide Web (www). A web server can also be referred to as a system or specifically to the software that accepts and supervises the hypertext transfer protocol (HTTP) requests.

IPsec: The IPsec protocol suit is used to provide Privacy and Authentication services at the IP layer by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between nodes at the beginning of the session and negotiation of cryptographic keys to be used during the session.

III. Internet Protocol Security (IPsec) Performance

Performance analysis of IPsec protocol has been extensively studied, for instance research by Shue et al (2007) and Zoltan (2006). Due to the complex nature of the protocol, existing research on IPSec performance includes a wide range of diverse implementations in terms of protocol particularities (e.g. encryption algorithms, key management protocols) and technology contexts (e.g. wire line and wireless links, video applications, and voice applications). Nevertheless, the common factor when analyzing IPsec performance concentrates in two basic aspects: space complexity and time complexity. Work by Barbieri et al (2002) measured the overall effects of encryption and decryption operations on throughput. By analyzing the performance of voice traffic transmitted over IPsec, their results show that IPsec causes a significant reduction in the expected bandwidth evidencing the cryptographic engine as the bottleneck for voice traffic.

A different approach by Hadjichrstofi et. al. (2003) focus on the overheads imposed by IPsec when transferring different file sizes by means of different protocols in both wire line and wireless scenarios. Two important findings are distinguished; first, file size has a significant impact in terms of time complexity being small file sizes the reason for longer transfer time values; secondly, computational capabilities are also related to time complexity in the sense that faster processors achieved better results. Data length impact is also studied by Mujinga et al (2006) and concludes that for smaller data packets IPsec overhead impact is higher in comparison to larger data packets. In regards to the impact of processing capabilities, Ronan et al (2004) also determined that as processing capabilities increase the overall performance increase as well. Therefore, it should be possible to improve the overall performance by means of hardware cryptographic accelerators. Despite most of these works perform small-scale Emulations their contributions also apply when implementing IPsec in large scale environments. Of particular interest for this work is performance of IPsec in large scale networks. Research by Okhee (2003) measures the impact of different IPsec configurations in large scale networks. Obtained data offers a baseline framework for comparison with current speed connection values and current workload data for large scale networks. Nevertheless, his work offers a comprehensive framework for test modeling.

IV. IPsec Suite Architecture

The Internet Protocol Security (IPsec) functionality is based on two main aspects, namely:

a. A protocol to exchange security parameters (IKE) and
b. IP header extensions to carry the cryptographic information (AH/ESP)

The IPsec operates as follows; to create a cryptographically protected connection between two end-points, a session key must be established between an initiator and a responder side by means of the Internet Key Exchange Protocol (IKE). IKE protocol aims for end-points to exchange security parameters or proposals each of them support including: the type of service that is Authentication Header (AH) or Encapsulation Header (ESP); and the type of operation mode: Tunnel mode or Transport mode. Once both entities agree on the security features, they establish an active IPsec connection for the secured data.

V. IPsec as a standard for webserver networks

The main advantage of IPsec over other security protocols resides on its characteristic of transparent implementation for end users since it does not require any modification at the application level. This means that IPsec is capable to protect any protocol residing above IP regardless the underlying medium supporting IP. This characteristic is of special interest given the introduction of heterogeneous environment enabled by an all-IP approach. IPsec protocol suite robustness offers comprehensive security solutions. Diverse configuration settings enable different possibilities for security schemes. In order to implement a common solution that enables interoperability.

VI. Operation Modes in Internet Protocol Security (IPsec)

Configuration of IPsec services can be implemented either as a combination of both services or only one single service. Once the desired security level is selected, the actual transport of the data takes place according to the following connection modes.

a. Transport Mode

In transport mode, the original IP packet is segmented to allocate IPsec information between the IP header and the remainder of the data packet. Figure 2 represents the application of transport mode for both types of services. As the same figure shows, Transport mode protects the entire data packet. Because of this, transport mode is more suitable for end-to-end communications.

b. Tunnel Mode

In comparison with transport mode, Tunnel mode does not alter the original packet. In the contrary, it only adds a new IP header and IPsec information portions at the beginning of the IP packet. Therefore, tunnel mode is more suitable for connection between two networks or security gateways.

VII. IPSec Services

IPsec offers two types of services to secure a connection; they include authentication header (AH) and encapsulation service payload ESP. These services are IP headers to specify the cryptographic parameters they support. The selection of a service is according to the end user needs.

a. Authentication Header (AH)

IPsec uses Authentication header to provide connectionless integrity, data origin authentication and an optional anti-replay service for IP datagrams. This consists of the authentication data which is a variable length field that contains the integrity check value for this packet. The algorithms employed for integrity check value calculation are specified by a security association of IPsec. For point-to-point communication keyed message authentication codes based on symmetric encryption algorithms (e.g. DES, Rijndael) or on one way hash functions are used. For multicast communication one way hash algorithms combined with asymmetric signature algorithms are utilized. Hashed based message authentication code has been the mandatory-to implement media access control for IPsec. Hash message authentication code based on secure hash algorithm has been recommended for message authentication in several network security protocols. The key reasons behind this are the free availability, flexibility of changing the hash function and reasonable speed, among others. The media access control based on the block ciphers such as CBC-MAC-DES was generally considered slow due to the complexity of the encryption process. As well, since DES has been shown to be not secure enough against the growing computing power it is not recommended any more. However, after selecting the AES encryption algorithm, this situation merits re-evaluation as Rijndael shows good performance in both hardware and software and it has better security features than DES.

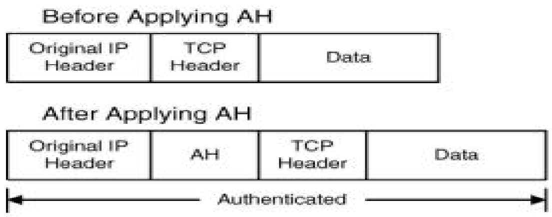

Figure 1 authentication header.

Authentication Header (AH) service provides integrity protection, authentication of origin and anti-replay attacks. AH does not offer encryption services to the payload portion of the packet. Nevertheless, implementation of AH header might be suitable in scenarios where cryptography exportation restrictions exist.

b. Encapsulation Service Payload (ESP)

In contrast to AH, Encapsulation Service Payload (ESP) not only provides integrity protection, optional authentication and anti-replay attacks services but also confidentiality by means of encryption. All services offered by ESP are configurable meaning that offered services can be activated or deactivated. A configuration mode of interest is ESP “Null Encryption” mode for which case confidentiality services are not offered. Under this configuration, ESP header has the same functionality as AH offering only integrity protection.

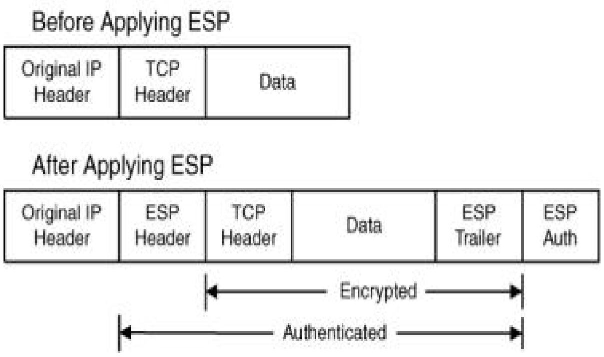

Figure 2. Encapsulated security payload.

VIII. Internet Protocol Security (IPsec) Adoption for the Webserver

After a considerable research work on the review of the adoption of IPsec for securing the webserver, we provides the various concepts of this technology (IPsec) to provides security services for IP traffic by allowing a host to set up a secure IP channel with any peer it wishes to connect to. The host can choose different services depending on the level of security required. The services provided by IPsec are based on two protocols: an authentication protocol (AH) and a combined encryption and authentication protocol (ESP). The first protocol provides services such as connectionless integrity and sender authentication, while the second protocol is in charge of guaranteeing confidentiality among other services. In order to execute any of these algorithms both the peers have to have previously agreed on pairs of secret keys. Such an agreement is performed by the IPsec key management module implementing the ISAKMP/Oakley protocol. Such a module mutually authenticates the peers, then it negotiates the symmetric keys they need to exchange messages and the cryptographic algorithms they will use. IPsec encodes the information needed to perform AH and ESP services in two additional packet headers called AH and ESP headers, respectively. IPsec may operate in two different ways, depending upon whether the secure communication is between two endpoints directly connected (in which case it operates in transport mode) or between two intermediate gateways to which the two endpoints are connected via a clear, i.e., unencrypted, channel (in which case IPsec operates in tunnel mode). For voice applications the following considerations apply: confidentiality is essential, authentication “in band” is expensive, session endpoints usually are not the cryptographic endpoints. Therefore, the best choice to secure voice traffic is to use the ESP header in tunnel mode.

IX. Conclusion

Today the Internet has virtually become the way of doing business as it offers a powerful ubiquitous medium of commerce and enables greater connectivity of disparate groups throughout the world. However this medium has its inherent risks. Loss of privacy, loss of data integrity, identifies spoofing and denial of service is some of the major threats in the Internet. Internet Protocol Security (IPSEC) addresses some of these issues by providing security services such as confidentiality, data integrity and authentication. The cryptographic algorithms

employed in these services must be able to handle packets which may vary in size over a large range. The size of the message has a significant impact on the performance of such algorithms. In particular, the message authentication algorithms process messages partitioned into blocks. Hence the messages have to be prepared by padding the required amount of zero bits to get an integer number of blocks. This process becomes a considerable overhead when the short messages are more dominant in the message stream.

REFERENCES

Chi-fu kuo and yung-feg Lu (2016) “The Performance Evaluation of a Dynamic

Configuration Method over IPSEC”

Department of Computer Science and Engineering.

Dustdar S. ,Schreiner .W (2005) “A survey on web services composition” International Journal of Web and Grid Services.

Faculty of Information and Natural Sciences

Gabriela Limon Garcia (2008) “IPsec performance analysis for large-scale Radio Access Networks” HELSINKI UNIVERSITY OF TECHNOLOGY

J. Jason, L. Rafalow and E. Vyncke (2003)“IPsec Configuration Policy Information Model”

Janaka Deepakumara, Howard M. Heys and R. Venkatesan “Performance Comparison of Message Authentication Code (MAC) Algorithms for the Internet Protocol Security (IPSEC).”

Janaka Deepakumara, Howard M. Heys and R. Venkatesan” Performance Comparison of Message Authentication Code (MAC) Algorithms for the Internet Protocol Security (IPSEC)”

Ji-Hoon JEONG, Geon-Woo KIM, So-Hee PARK and Sung-Won SOHN “Design and Implementation of the Ipsec-based Security System”

Luis Felipe Cabrera, Christopher Kurt and Don Box (2007) “An Introduction to the Web Services Architecture and Its Specifications”

Mohit Aron and Peter Druschel “TCP Implementation Enhancements for Improving Webserver Performance” TR99-335 Department of Computer Science

Niels Ferguson and Bruce Schneier "A Cryptographic Evaluation of IPsec" Counterpane Internet Security, Inc.

Rice University Houston, TX 77005

Roberto Barbieri, Danilo Bruschi and Emilia Rosti" Voice over IPsec: Analysis and Solutions" Andy Ozment Stuart E. Schechter (2006) "Bootstrapping the Adoption of Internet Security Protocols"

Stefano Lucetti "Automatic IPsec Security Association Negotiation in Mobile-Oriented IPv6 networks" Technical Report No. T2.1_05_PI_R01

Vivek S. Pai, Peter Druschel, and Willy Zwaenepoel (1999)" An Efficient and Portable Web Server"

World Wide Web timeline, pews Research center. 11 march 2014.