2012 Third International Conference on Intelligent Systems Modelling and Simulation

Overview of Mobile IPv6 Security

Amirhossein Moravejosharieh
Department of Computer system and technology
University of Malaya
Kuala Lumpur, Malaysia
Amirhosein.moravej@ siswa.um.edu.my

Hero Modares
Department of Computer system and technology
University of Malaya
Kuala Lumpur, Malaysia
hero.modares@ siswa.um.edu.my

Rosli Salleh
Department of Computer system and technology
University of Malaya
Kuala Lumpur, Malaysia
rosli_salleh@um.edu.my

Abstract— **Mobile IP enables a mobile node to be recognized via a single IP address even though the node may travel from one network to another. Despite reposition between different networks, connectivity at different positions is attained continuously with no user intervention. Mobile IP grants connectivity to nodes everywhere, whether within home networks or away from home. General improvement in MIPv6 may offer enhanced security; however, there are areas still prone to attacks. Security solutions for the mobile IP protocol are still in progress. IP Security (IPsec) in the IPv6 protocol can secure Mobile IPv6 more than IPv4. IPsec presents security services for the application and transportation layer protocols of the TCP/IP stack. However, there are several unsolved concerns and problems with Mobile IPv6 in most cases which justifies development of new methods to provide acceptable level of security. This article focuses on how IPsec works, Mobile IPv6 security, potential threats and security considerations.**

Keywords- Internet Protocol security (IPsec); Mobile IPv6 security; potential threats in MIPv6 and security considerations.

I. Introduction

There are various implementations presented for Mobile IPv6. Some have been successful, while other concepts such as security bandwidth consumption and seamless handover are still concerns that researchers are trying to improve [1]. Communication privacy is a basic necessity of each user in public communication. A summary of necessary security issues includes how sender and receiver authenticate each other before creating any connection (addressing as trust), how communication between senders and receivers is protected against eavesdropping and tampering (addressing as confidentiality), and how authenticated users follow private communication (addressing as authorization). On the other hand, secure communication over the internet is essential for important applications such as banking, purchasing, making payments, virtual private network (VPN) and so on. Security includes peer authentication, and is encouraged by authorization to make use of resources, secret key and exchanges, and private communication using algorithms. Security can be provided either at the IP layer or transport layer. For example, Secure Socket Layer (SSL) is used to make a secure http which is visible as an https on a web page. The VPN applications for roaming users are based either on IP Security or SSL, which are both enough to provide the minimum security functions necessary. IP mobility is concerned with IP layer security so in this paper the focus is on preparing a summary of IP Security (IPsec). Authentication, integrity, confidentiality and access control can be achieved using IPsec in the network [2-5].

II. Background

Mobile IPv6 is a standard that offers a way for mobile nodes (MN) to preserve connectivity while they travel across different areas. All mobile nodes (MNs) have a home network with a permanent home IP address. In addition, each home network includes a home agent (HA) in charge of tracking MNs as they move in different networks. The time a MN leaves a home network and move to the neighbor network, obtaining a new IP address, is called a care-of address (CoA). The MN is required to register this address (CoA) with its HA through a binding update which defends its authenticity and integrity and is issued over an IPSec. Thus, even as the MN moves to a foreign network, a correspondent node (CN) can maintain communication with the MN using indirect routing made of packets being relayed by the HA. To decrease overhead at the border router, routing optimization is used. Routing optimization offers a way for the MN and CN to forward packets to each other directly without sending from the HA. If there is no security mechanism, the CN does not know which MN sent the BU. The BU is not actually secret but it needs to be sent from a legitimate MN. The integrity and authenticity of this binding update cannot be secured via IPSec as it cannot be assumed that a common public key survives between the two nodes. [6-8].

III. How IPsec Works

IPSec uses packet cryptography and filtering, with cryptography helping to achieve user data confidentiality, authentication and integrity. These are components which together with their interrelationships include the logical architecture of IPSec. In this section the fundamental components of IPSec architecture are briefly explained. IPSec architecture can be classified into three main areas:

- Security Associations (SA)
- SA and key management support
- Algorithms and methods

A. Security Associations

Security Associations are a number of keys that define the security services and an agreeable policy, and are used to defend communications between IPSec peers. Security Associations (SA) is a one-way connection that offers security

978-0-7695-4668-1/12 $26.00 © 2012 IEEE
DOI 10.1109/ISMS.2012.9

services. For each IPSec session two SAs are needed; for instance, if Authentication Header (AH) and Encapsulating (ESP) are both used between two peers in IPSec, then four SAs are needed. Security Association database (SAD) and Security Policy database (SPD) are two databases used in SAs. The SAD is used to keep the information about each SA after SA is established; then the SPD stores the policy requisites or security necessities for each SA to be established. Fig.1 illustrates SA, SAD and SPD architecture [9].

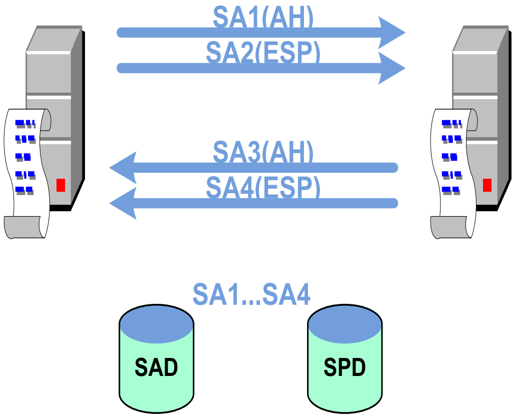

Figure 1. SA, SPD, and SAD Architecture.

B. *SA and Key Management*

The Internet Security Association and Key Management Protocol (ISAKMP) specify the framework for key exchange and authentication by preparing a way for establishing, negotiating, deleting, and changing SAs. IPSec needs support for both automatic and manual management of SAs and keys. Internet Key Exchange (IKE) is the key management protocol for IPSec. IKE includes the SKEME keying techniques protocol and the Oakley key exchange protocol. Fig.2 illustrates the architecture of SKEME, Oakley, IKE and ISAKMP protocol. In addition, IKE protocol is used to make a secure virtual private network (VPN) and network access or a remote host. Based on the IKE protocol, public-key, digital signature and pre-shared key are three authentication method categories in IPSec. Fig.3 illustrates IKE architecture and authentication methods [9, 10].

Three IETF standards are offered using IKE to create secure connection between peers:

- Kerberos v5.0 authentication.
- Public/Private Key signatures using Certification authority (CA) congruous with some systems such as Entrust, Netscape and VeriSign.
- Pre-shared key (password).

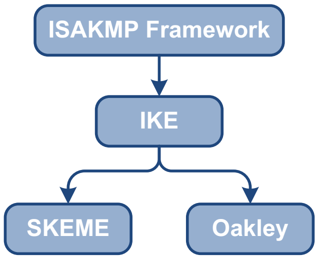

Figure 2. ISAKMP, IKE, Oakley, and SKEME Protocol Architecture.

The Diffie-Hellman key exchange algorithm is used to generate a unique, shared, secret key in Oakley protocol. This key is then used to generate keying material for encryption or authentication. For instance, DES encryption algorithm uses a shared secret key and the Diffie-Hellman key exchange can use one of a number of groups that define prime number key sizes in the key exchange process. Fig.3 illustrates the well-known Diffie-Hellman key exchange groups, Diffie-Hellman algorithm and Oakley protocol [9].

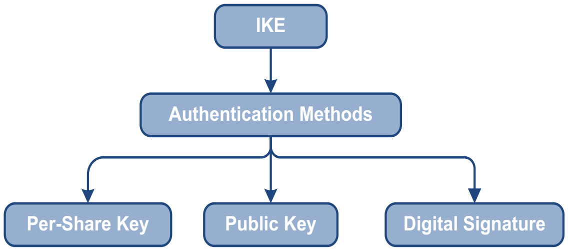

Figure 3. IKE Protocol and Authentication Methods Architecture.

C. *Algorithms and Methods*

Authentication Header (AH) and Encapsulating Security Payload (ESP) are two protocols used to make a secure IP layer in IPSec. Therefore, security services in SA are prepared using these protocols. The security protocol (AH or ESP), Security Parameters Index (SPI), and IP destination address are three requirements needed to identify the SA. Authentication Header (AH) and Encapsulating Security Payload (ESP) use Hash Message Authentication Code - MD5 and HMAC-SHA-1 in authentication or hash algorithms, and ESP uses DES and 3DES encryption algorithms.

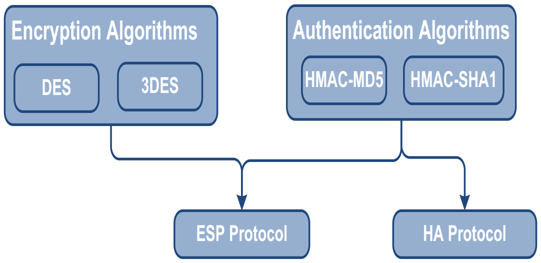

Figure 4. IPSec Algorithms and Protocols for Encryption and Authentication.

Fig.4 illustrates the IPSec Algorithms and Protocols for Encryption and Authentication [9].

IV. Security Analysis in MIPV6

The basic objective of developing Mobile IPv6 is security against some different types of attacks such as denial of service (DoS), connection hijacking, man-in-the-middle and impersonation. The security objective is to safely create routing changes because all threats are reasoned by the changed routing used to allow mobility in the network. There are several threat categories for Mobile IPv6 security, some of which are listed below:

- Threats against binding update (BU) to HA.
- Threats against route optimization with CN.
- Threats where the tunnels between HA and MN are attacked.
- Threats where Mobile IPv6 Routing Header is used to return traffic from other nodes.

Threats against BU and route optimization pertain to binding message authentication. Trust and authentication communication are needed between MN and HA because MN agrees to use the HA services so the relationship must be secured in advance. However, there is no prior relationship between CN and MN, but there are methods to authenticate binding messages between CN and MN. For instance, public key authentication can be used to achieve this aim. If a malicious node forwards a packet to the HA with source address set to an MN's address, then HA forwards the packet using MN's source address which is already set by the malicious node, so DoS attacks can occur. However, if HA uses a verifying algorithm to verify the BU message then HA can prevent DoS attacks in this case. To avoid such threat a new routing header can be used to prevent the incorrect routing header from making twisted firewall rules and getting a constrained address [11].

V. Proposed Security Solution

By the time a BU message is completed, the CN will start to send normal traffic to the MN using new CoA. After a reasonable amount of time, for example 10 seconds, CN with a new nonce sends a Binding Update Verification (BUV) to the MN which should reply with an verification acknowledgement message within 10 seconds; if the MN does not reply with this message in 10 seconds the connection between MN and CN is terminated. This concept can be used to minimize damage in the case of a bombing attack where the attacker sends all the packets to the MN. On the other hand, Cryptography Generated Address (CGA) can be used to make spoofing attacks more difficult. Also, the message can be signed by the sender's private key. Since the attacker needs public and private keys it is difficult to perform a redirection attack [6, 12, 13]. Table I [14] shows the threats and possible solutions for each.

TABLE I. Tread and possible solution [14].

Tread	***Possible Solution***	***Abbr.***
Man-in-the-Middle	Authentication of Control Message	MITM
Eavesdropping	Line Encryption	S
Manipulation of Binding Cache (DoS)	Authentication of Control Message	DoS
ICMP Attack	Access Lists for ICMP Requests on Router	DoS
Unauthorized Access	User Authentication, Access Lists	UZ
Session Stealing	Authentification of Control Message	MN-SS , CN-SS

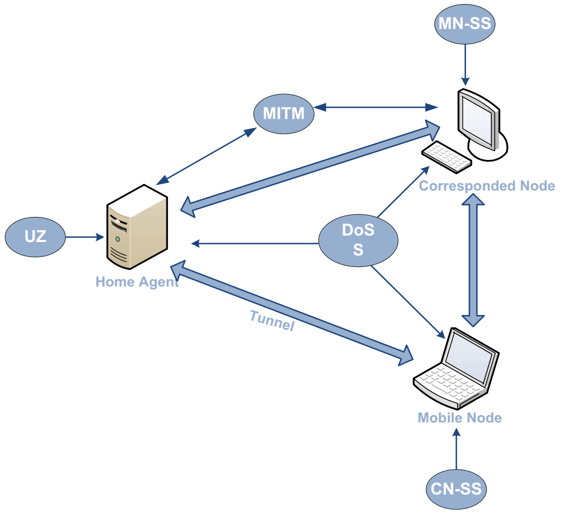

Figure 5. Tread

VI. Conclusion

The mobile IPv6 requirement is still incomplete, with some essential practical issues. The most important concern is protocol security, since without a suitable security solution; the protocol has no opportunity to be admitted and does not work at all. At present, in transport mode, IP Security Encapsulation Security Payload (ESP) is the standardized method for BU protection and also for making a secure connection to control messages sent in the home registration method. Some advantages that IPSec has over SSL/TLS are that it can perform independent of IP address, can encrypt any protocol and can also encrypt packets which consist of IP header. However, IPSec is very complicated, with various ways to configure it.

Dynamic key management, mutual authentication and negotiation of cryptographic algorithms can be controlled by IKE protocol. In addition, the authentication method which is one of the main ways for creating safe communication between peers can be based on a shared secret, Extensible Authentication Protocol (EAP) or X.509 certificates.

REFERENCES

[1] A. Moravejosharieh, R. Salleh, and H. Modares. "A Novel Approach For Efficient Resource Consumption In GPS-Based Mobile IPv6 Wireless LAN." Third International Conference on Computaional Intelligence Modelling and Simulation. Langkawi, Malaysia: IEEE, 20-22 September 2011.

[2] Y. C. Chen, and F. C. Yang. "An Efficient MIPv6 Return Routability Scheme Based on Geometric Computing." World Academy of Science, Engineering and Technology, 2009.

[3] W. Werapun, and A. Unakul. "Secure Mobile IPv6 Binding Updates with Identity-based Signature." international conference on Electronics Packaging, Jan 2004.

[4] R. Kandikattu, and L. Jacob. "Comparative Analysis of Different Cryptosystems for Hierarchical Mobile IPv6-based Wireless Mesh Network." International Journal of Network Security, Vol.10, No.3, PP.190-203, May 2010.

[5] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng. "Routing optimization security in mobile IPv6." Computer Networks - Elsevier, 2005.

[6] A. Encarnacao, and G. Bayer, "Mobile IPv6 Binding Update - Return Routability Procedure." 2008.

[7] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6." IETF draft, June 2004.

[8] W. Simpson, "IPng Mobility Considerations, RFC 1688." 1994.

[9] Windows Server TechCenter. Microsoft|TechNet. March 28, 2003. http://technet.microsoft.com/en-us/library/cc759130%28WS.10%29.aspx.

[10] OZEKI MESSAGE SERVER - Product Guide. "VPN configuration." OZEKI Evolving Capabilities . http://www.ozeki.hu/index.php?owpn=590.

[11] T. Koskiahde, "Security in Mobile IPv6." Apr, 2002: 1-14.

[12] The Government of the Hong Kong Special Administrative Region. "IPv6 SECURITY." May 2011.

[13] T. Scheffler, "Security Achitectures for Mobile IPv6." Euro6IX/6NET Workshop. Limerick, Ireland, 2002.

[14] M. Ehmke et al.,"Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption." Issues in Informing Science and Information Technology, 2009.