An Improved Address Ownership in Mobile IPv6

Min-Shiang Hwang[†] Cheng-Chi Lee[§, ¶] Song-Kong Chong[‡]

Department of Management Information Systems[†]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Graduate Institute of Networking and Communication Engineering[‡]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

Department of Computer Science[§]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Department of Computer & Communication Engineering[¶]
Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

May 21, 2008

An Improved Address Ownership in Mobile IPv6

Abstract

This paper proposes an improved address ownership scheme in Mobile IPv6 (MIPv6). The authors combine the idea of lossless compression with one-way hash function, and present a new method to protect the binding update in MIPv6 against redirect attacks.

Index Terms: Address ownership, IPv6, MIPv6, redirect attacks

1 Introduction

Attacks against Internet routing have received much attention in the IPv6 world. Mobile IPv6 (MIPv6) introduces new extensions to the IPv6 protocol, specifying routing support to permit an IPv6 node to move around the Internet using its permanent home address (HoA). In MIPv6, the home agent (HA) plays an important role in supporting node mobility. Through a home address (HoA) registered to the HA, a mobile node (MN) which is far away from its home network can use the binding update (BU) and binding acknowledgement (BA) messages exchanged between the MN and its HA, and between the MN and its correspond node (CN), to maintain reachability [5].

The binding update message contains the care-of-address (CoA) which is dynamically allocated on the foreign network in order to provide information about the MN's current point of attachment. Upon receiving the binding update message, the receiving ends (both HA and CN) update the current location of the MN to the new address CoA. The HA will intercept any packets destined for the HoA and tunnel them to the MN. The CN takes advantage of the binding update by sending future messages directly to the MN at its CoA. Since the binding update message is an extremely significant piece of information to be well protected, its origin should be authenticated in order to prevent redirect attacks [5, 10] from working.

In 2001, O'Shea and Roe first proposed a mechanism named CAM (Childproof Authentication for MIPv6) to secure the binding update (BU) against redirect attacks in MIPv6 [10]. The goal of CAM is to provide minimum protection to BU when IPSec AH is not available [10]. There are two advantages of CAM. First, the communicating parties do not require a shared secret. Second, the utilization of a certification authority or other security infrastructure is avoided. The idea of CAM has been later adopted by many researches as groundwork to develop various defense mechanisms upon, not only to be used in MIPv6 [3, 4, 6, 8], but also in IPv6 itself to work against denial-of-service attacks [1, 2, 9]. So far, the idea of CAM is still under discussion in the IETF Mobile IP Working Group.

In IPv6, a 128-bit IP address can be divided into a 64-bit subnet prefix (SP) and a 64-bit interface identifier. According to [10], 62 bits of the interface identifier can be used to store the cryptographic hash of a public key, and the other 2 bits are for EUI-64 global identifiers. The CAM performs as follows.

Protocol Operation: A mobile node MN self-generates a public/private key pair PK_M and SK_M. The MN's home address is denoted as $HoA = \{SP \| H_{62}(PK_M, i)\}$, where $H(\cdot)$ is a one-way hash function and $H_{62}(\cdot)$ represents only the leftmost 62 bits extracted to form the low order bits of an IPv6 address; i is a random number used to prevent birthday collisions herein. A BU message from the MN to its CN ($MN \rightarrow CN$) is given by $\{CoA, Add_C, HoA, PK_M, i, T_M, \{H(CoA, Add_C, HoA, T_M)\}sign_M\}$, where $\{\cdot\}sign_M$ is MN's signature signed with its private key SK_M, Add_C is CN's IP address, and, T_M is MN's time-stamp. Upon receiving the BU, the CN computes $H_{62}(PK_M, i)$, and compares it with the leftmost 62 of the low order bits of the HoA. If the HoA verification turns out positive, then CN takes the

PK_M to verify $\{H(CoA, Add_C, HoA, T_M)\}sign_M$. If positive, the CN accepts the BU. The later packets transmission will redirect to the MN's CoA. Since no one except the private key owner of the HoA can generate these verifiable information, the CN is convinced that the MN is the owner of the CoA.

Basically, 62 bits are too few to gain strong security and real protection against brute force attacks [1, 4, 9]. An attacker may search through a large number of public/private key pairs for collisions where there is the same HoA. Therefore, many improved mechanisms have been proposed to solve this problem [1, 2, 4, 6, 8, 9]. Among the proposed mechanisms, [1, 2, 9] focus on the security of IPv6 Neighbor or Router Discovery functions against denial-of-service attacks, ignoring the solution to the address ownership problem in MIPv6. The other mechanisms require more security infrastructures, e.g. CA or $IPSec$, to support their functionalities in protecting a BU in MIPv6 [4, 6, 8]. These mechanisms are complicated in computation. Here, to make a difference, we shall propose an efficient method to solve these problems.

In this letter, we present a novel method to improve the address ownership in MIPv6. The idea of a lossless compression algorithm [7] will be introduced first and then combined with a secure one-way hash function to complete our new method to protect the MIPv6 binding update against redirect attacks. The proposed method breaks the limit of the 62-bit cryptographic address in CAM. It reduces the complexity of the improved protocols ahead of it when protecting BU against redirect attacks. Moreover, the proposed method avoid the utilization of a CA and $IPSec$. It keeps the merit of [10]; that is, the communicating parties do not need a shared secret.

2 The Proposed Method

Let's use the same notations as above. An MN first selects a key pair PK_M/SK_M. Then, the MN computes $X = H(SP, PK_M, i)$. Given a public lossless compression algorithm LC which is one that guarantees its decompressed output is bit-for-bit identical to the original input. Suppose the original output K of $H(\cdot)$ is 128 bits. The MN computes the cryptographic address $Y = LC_{62}(X)$, where LC_{62} means given an appropriate input X, its compression output is 62 bits. Suppose the compression ratio CR (the size of uncompressed results divided by the size of compressed results) of LC is 0.25, and then the appropriate length of X that should be used in LC_{62} can be computed by using the following equation:

$$CR = \frac{X - 62}{K}.$$

In this case, the value of X is the leftmost 94 bits of $H(SP, PK_M, i)$. After computing the cryptographic address $Y = LC_{62}(X)$, the MN claims its home address $HoA = \{SP \| Y\}$. This HoA is publicly known. When the MN roams to another network, it will send a BU to its CN. Note that the BU is entirely the same with the original CAM:

$$BU = \{CoA, Add_C, HoA, PK_M, i, T_M, \{H(CoA, Add_C, HoA, T_M)\}sign_M\}.$$

When the CN receives the BU, it decompresses the Y from the HoA. In this case, the CN will obtain the original 94 bits again. Then, the CN computes $X' = H(SP, PK_M, i)$ and takes the leftmost 94 bits of X' to make a comparison with the decompressed data. If the comparison turns out positive, the CN continues its verification with $\{H(CoA, Add_C, HoA, T_M)\}sign_M$ by using the public key PK_M of the MN. A positive verification result gives the CN strong confidence that the MN in fact owns the claimed CoA and that there is nothing wrong with the BU.

In the proposed method, the complexity of the brute force attack is on the order of $O(2^{94-1})$. The CAM is only $O(2^{62-1})$. By including the MN's subnet prefix SP and a random number i in the hash calculation $H(SP, PK_M, i)$, we can avoid an attacker from searching each cryptographic address in the whole IPv6 networks by just building up *one* lookup table that contains many public/private key pairs [1]. Therefore, birthday attacks will take no effect. However, the random number i is still needed in the hash calculation. If it were given up, an attacker would be able to easily build up a lookup table aiming at a particular subnet, especially if the subnet is very valuable.

With no shared secret needed and no certification authority or other security infrastructure required in the proposed method, we keep the merit of CAM in the proposed method.

3 Analyses

In this section, we shall analyze the new method. According to Table 1, it is easy to discern that by taking in the idea of lossless compression, the proposed method increases the security of CAM substantially. If an attacker wishes to mount an impersonation attack, with the proposed method in the way, he/she must attempt 2^{94-1} tries to find a public key that will produce the same cryptographic address. If the attacker can compute 100 billion hashes per second, by using the CAM, he/she needs 266 days to find out a collision. However, facing the proposed method, the attacker will need 3 billion years.

The proposed method makes use of the cryptographic address Y of an MN's home address $HoA = \{SP \| Y\}$ as compressed data. Since the compression algorithm is publicly known, a CN can decompress it into some original data and make a verification. An attacker who wishes to mount a redirect attack will have as much trouble as shown in Table 1 shows.

4 Discussions and Conclusions

When an MN computes its cryptographic address $Y = LC_{62}(X)$, the compression ratio of a lossless compression algorithm LC may fluctuate as the value of X varies. Therefore, if the value of X cannot produce an appropriate

Table 1: Comparisons between the proposed method and CAM

Item	CAM[1]	Ours[2]
If an attacker able to compute		
1 million hashes/sec	73,118 years	314,038 billion years
1 billion hashes/sec	73 years	314 billion years
100 billion hashes/sec	266 days	3 billion years

[1] 62 bits a cryptographic address

[2] 94 bits a cryptographic address

length (62 bits) cryptographic address Y, the MN should select a new key pair PK'_M/SK'_M or just adjust the value of i. Then, the MN can compute a new $X = H(SP, PK_M, i)$ again to set up its HoA by following the steps described in Section 2. Note that the 0.25 compression ratio is just an example. The question of how to choose an efficient and secure compression algorithm is beyond the scope of this letter. However, if the chosen compression algorithm can provide a higher compression ratio, the proposed method can then provide stronger security protection.

Although an MN may need to put in some efforts when establishing an appropriate HoA, compared with the robustness provided in the binding update phase when roaming, the efforts that the MN invests in the HoA establishment are worth every while.

References

[1] Jari Arkko, Tuomas Aura, James Kempf, Vesa-Matti Mantyla, Pekka Nikander, and Michael Roe, "Securing IPv6 neighbor and router discovery," in *Proceedings of the ACM Workshop on Wireless Security*, pp. 77–86, Atlanta, Georgia, USA, 2002.

[2] T. Aura, "Cryptographically generated addresses (CGA)," *draft-ietf-send-cga-04 (work in progress)*, Dec. 2003.

[3] Ching-Wen Chen, Chou-Chen Yang, and Ming-Chin Chuang, "An efficient authentication scheme between manet and wlan on ipv6," *International*

Journal of Network Security, vol. 1, no. 1, pp. 12–21, 2005.

[4] Robert H. Deng, Jianying Zhou, and Feng Bao, "Defending against redirect attacks in mobile IP," in *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 59–67, Washington, DC, USA, 2002.

[5] S. M. Faccin and F. Le, "A secure and efficient solution to the ipv6 address ownership problem," in *4th International Workshop on Mobile and Wireless Communications Network*, pp. 162–166, Stockholm, Sweden, 2002.

[6] D. Johnson, C. Perkins, and A. Arkko, "Mobility support in IPv6," *RFC 3775, Requset for Comments*, Jun. 2004.

[7] A. Lempel and J. Ziv, "A universal algorithm for sequential data compression," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 337–343, 1977.

[8] Gabriel Montenegro and Claude Castelluccia, "Crypto-based identifiers (CBIDs): Concepts and applications," *ACM Transactions on Information and System Security*, vol. 7, pp. 97–127, Feb. 2004.

[9] Pekka Nikander, "Denial-of-service, address ownership, and early authentication in the IPv6 world," in *9th International Workshop on Security Protocols*, pp. 12–21, Cambridge, UK, 2001.

[10] Greg O'Shea and Michael Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM SIGCOMM Computer Communication Review*, vol. 31, pp. 4–8, Apr. 2001.