A Security Proxy Based Protocol for Authenticating the Mobile IPv6 Binding Updates

Abstract. In this paper, we propose a security proxy based protocol for authenticating the binding updates in Mobile IP Version 6 environment, which combines the Deng-Zhou-Bao¡s protocol [2] with Aura¡s two hash-based CGA scheme [8] to avoid the use of trusted CAs. The two hash-based CGA scheme enables our protocol to achieve stronger security than other CGA-based protocols without a trusted CA, resulting in less cost of verifying the HA¡s public key than the one of the Deng-Zhou-Bao¡s protocol. The comparison of our protocol with other protocols such as the Deng-Zhou-Bao¡s protocol, CAM-DH and SUCV shows that our protocol can provide good performance and manageability in addition to stronger security than one hash-based CGA approaches..

Key Words: Mipv6 Binding Update Protocol, CGA, CAM-DH, Return Routability

1 Introduction

The route optimization operation in Mobile IP Version 6 (MIPv6) environment allows direct routing from any correspondent node (CN) to any mobile node (MN) [2]. But the route optimization requires that the MN constantly informs its CNs about its new care-of-address (CoA) by sending them binding update (BU) messages. Without a security solution, the route optimization functionality exposes the involved MNs and CNs but also all other nodes of the Internet to various security threats [1]. The essential requirement to address the security threats is for the CN to authenticate the MN sending the BU message. Only after successfully authenticating the MN, the CN has to update its binding cache entries. Unfortunately, it is so difficult to achieve strong authentication between two previously unknown nodes (MN and CN) where no global security infrastructure is available. Thus, the need has arisen for a security solution to enable sufficient authentication between the CN and the MN, excluding the use of traditional secret- or Public Key Infrastructure (PKI) based authentication infrastructures.

Several researches have been conducted to solve this security issue [2-7]. Recently, the Return Routability (RR) protocol has been accepted as the basic technique for securing the BUs. Nevertheless, the RR protocol has some potential drawbacks, both in terms of its security properties and also performance [2]. Unlike the RR protocol, the protocols such as CAM, CAM-DH, SUCV and ABKs have been proposed based on public key [2-6]. The public key based protocols attempted to associate the MN¡s address with its public key to avoid the use of additional security infrastructure such as PKI, by using the novel methods such as Cryptographically Generated Address (CGA) and identity-based cryptosystems.

Deng, Zhou and Bao proposed a public key based protocol [2]. Unlike other protocols, their protocol uses the public key certificates (PKC), issued for home links, containing home link subnet prefixes as subject names instead of the public keys bound with the MNs¡s HoAs. Therefore, their protocol with such PKCs can be much more traceable, manageable and scalable than the above public key based approaches. Moreover, it uses the home agents (HA) as trusted security proxies to off-load the public key cryptographic operations of the MNs to the HAs under the MIPv6¡s assumption that communication between the MNs and their HAs is protected with pre-established security association. In spite of the above strength, their protocol has a critical limitation. That is, it needs trusted Certification Authorities (CA) to issue the PKCs containing home link subnet prefixes as subject names for home links. Also, the verification of the PKCs is burden to the CNs.

In this paper, we propose a security proxy based protocol for authenticating the BUs, which combines the Deng-Zhou-Bao¡s protocol with Aura¡s two hash-based CGA scheme [8] to avoid the use of trusted CAs. That is, in our protocol, the HAs use the addresses derived from the their public keys via the CGA method instead of the PKCs issued by the trusted CAs. Like Deng-Zhou-Bao¡s protocol, our protocol uses the HAs as the trusted security proxies to minimize the expensive cryptographic operations in the MNs.

The rest of the paper is organized as follows. Section 2 reviews the Deng-Zhou-Bao¡s protocol. In section 3, we describe the two hash-based CGA scheme and propose a security proxy based protocol for securing the BUs. Section 4 analyzes the proposed protocol. Finally, section 5 draws some conclusions.

2 Review of Deng-Zhou-Bao¡s protocol

Deng, Zhou and Bao designed their protocol to possess the following features [2]. First, it performs one-way authenticated key-exchange between the MN and the CN where the MN authenticates itself to the CN and the exchanged session key is used to secure the BU messages from the MN to the CN. Second, it employs public key cryptosystems and is secure against powerful adversary who is able to launch both passive and active attacks. Third, it is easy to manage and scalable. Instead of issuing PKCs containing the MNs¡s HoAs as subject names for the MNs, their scheme issues PKCs containing home link subnet prefixes as subject names for home links. Fourth, no public key cryptographic operations are performed at the MNs. The HAs function as trusted security proxies for the MNs in the protocol. They testify the legitimacy of the MNs¡s HoAs, facilitate authentication of the MNs to the CNs, and establish shared secret session keys for them.

Notation is as follows.

h() : a cryptographic secure one-way hash function

prf(k, m) : a keyed pseudo random function ? often a keyed hash function. It accepts a secret key *k* and a message m, and generates a pseudo random output.

P_X/S_X : a public and private key pair of *X*.

$S_X(m)$: node *X*¡s digital signature on a message *m*.

m|*n* : concatenation of two messages *m* and *n*.

2.1 System Setup

A home link is associated with a public/private key pair P_H and S_H in a digital signature scheme. The private key S_H is kept by a HA in the home link. The home link obtains a PKC, $Cert_H = \{ HL, P_H, VI, SIG_{CA} \}$ from a *CA*, where *HL* is the home link subnet prefix, *VI* is the valid duration of the certificate, and SIG_{CA} is *CA*¡s signature on *HL*, P_H and *VI*. It is assumed that CNs can obtain *CA*¡s public key via various means. The protocol also uses the Diffie-Hellman key exchange algorithm to arrive at a mutual secret value between parties of the protocol. Let *p* and *g* be the public Diffie-Hellman parameters, where *p* is a large prime and *g* is a generator of the multiplicative group Zp*. To keep notations compact, $g^x \bmod p$ is written simply as g^x. It is assumed that the values of *p* and *g* are agreed upon before hand by all the parties concerned.

2.2 Protocol Operation

The protocol messages exchanged among a *MN*, its *HA* and its *CN* are shown in Fig. 1. In the protocol, the existence of and operations performed by the *HA* are transparent to both the *MN* and the *CN*. As far as the *MN* is concerned, it sends message *REQ* to and receives *REP* from its *CN*. Similarly, from the *CN*¡s point of view, it receives *COOKIE0*, *EXCH0* and *CONFIRM* from and sends *COOKIE1* and *EXCH1* to the *MN*. The use of cookies during the key exchange is a weak form of protection against an intruder who generates a series of request packets, each with a different spoofed source IP address and sends them to a protocol party. For each request, the protocol party will first validate cookies before performing computationally expensive public key cryptographic operations. If the authentication process is successful, the *CN* creates a cache entry for the *MN*¡ *HoA* and the session key K_{BU}, which will be used for authenticating binding update messages from MN. After that, the *MN* proceeds to send CN BU messages protected using K_{BU} as in the RR protocol.

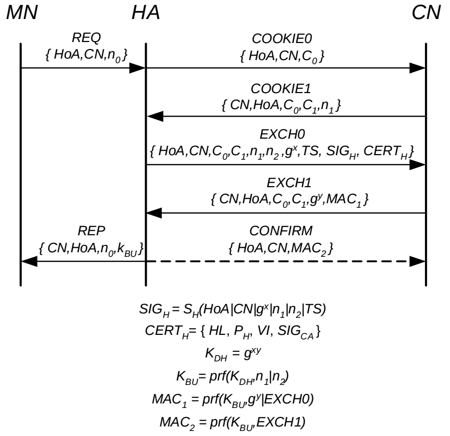

MN
HA
CN
REQ
$\{ HoA,CN,n_0 \}$
COOKIE0
$\{ HoA,CN,C_0 \}$
COOKIE1
$\{ CN,HoA,C_0,C_1,n_1 \}$
EXCH0
$\{ HoA,CN,C_0,C_1,n_1,n_2,g^x,TS, SIG_H, CERT_H \}$
EXCH1
$\{ CN,HoA,C_0,C_1,g^y,MAC_1 \}$
REP
$\{ CN,HoA,n_0,k_{BU} \}$
CONFIRM
$\{ HoA,CN,MAC_2 \}$
$SIG_H = S_H(HoA|CN|g^x|n_1|n_2|TS)$
$CERT_H = \{ HL, P_H, VI, SIG_{CA} \}$
$K_{DH} = g^{xy}$
$K_{BU} = prf(K_{DH},n_1|n_2)$
$MAC_1 = prf(K_{BU},g^y|EXCH0)$
$MAC_2 = prf(K_{BU},EXCH1)$

Fig. 1. Deng-Zhou-Bao¡s protocol

2.3 Weakness of the Deng-Zhou-Bao¡s protocol

Because of issuing PKCs containing home link subnet prefixes as subject names for home links, the Deng-Zhou-Bao¡s protocol is able to be much more manageable and scalable than other public key based approaches. Furthermore, with the PKCs, it can achieve a strong one-way authentication of the MN/HoA to the CN and allow the CN to securely share a secret session key with the MN.

Nevertheless, there is a critical limitation that the protocol should employ trusted CAs to issue the PKCs for home links. It is not feasible solution where no global CA is available. To protect against the man-in-the-middle attack, the CN should validate $Cert_H$¡ certificate path and revocation status in addition to the signature on $Cert_H$. Obviously, such validation is heavy burden to the CN.

Thus, the Deng-Zhou-Bao¡s protocol needs to be enhanced to avoid the use of trusted CAs and PKCs issued by them.

3 The Proposed Protocol

In this section, we propose a security proxy based protocol for authenticating the BUs, which combines the Deng-Zhou-Bao¡s protocol with Aura¡s two hash-based CGA method to avoid the use of trusted CAs. In our protocol, the HA uses the address derived from its public key via the CGA method instead of the PKC issued by a trusted CA.

3.1 Appliance of the Two Hash Based CGA Scheme

Recently, Aura proposed a new CGA scheme where two hash values are computed instead of one [8]. The first hash value (Hash1) is used to produce the interface identifier (i.e. rightmost 64 bits) of the address. The purpose of the second hash (Hash2) is to artificially increase that computational complexity of generating new addresses and, consequently, the cost of brute-force attacks. The CGA format is defined in [8].

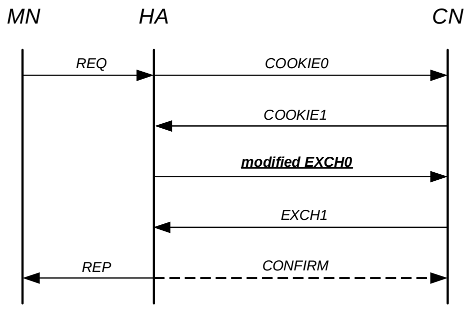
In our protocol, a home link is associated with a public/private key pair P_H and S_H in a digital signature scheme. A HA in the home link keeps the public/private key pair, and derives a CGA from the public key P_H.

Each CGA can be associated with a self-signed X.509 v3 certificate. The self-signed X.509 v3 certificate structure, its extension and two 128-bit hash values (Hash1 and Hash2) is defined in [8-9]. As an alternative to the certificate, an optimized parameter format can be used. The optimized format is simply the concatenation of the DER-encoded subjectPublicKeyInfo and CGAParameters data values.

The process of obtaining a new CGA is as follows.

1) Generate a public/private key pair P_H and S_H for a home link.
2) Generate a new CGA via the algorithm presented in [8].
3) Create and sign a self-signed X.509 v3 certificate, which contains an extension where the extnID has the value cgaExtnID, critical has the value false or true, and the extnValue contains the encoded CGAParameters data value. As an alternative to the certificate, an optimized parameter format can be created.

Like the Deng-Zhou-Bao¡s protocol, it is assumed that the public Diffie-Hellman parameters *p* and *g* are agreed upon before hand by all the parties.



modified EXCH0 = $\{$ *HoA,CN,*C_0*,*C_1*,*n_1*,*n_2*,*g^x*,TS,* SIG_H*,* $pkInfo_H\}$

$pkInfo_H$ *= Self-Signed* $Cert_H$ *or* OPF_H

OPF_H *= DER_Encode(H¡s subjectPublicKeyInfo) | H¡s CGAParameters*

Fig. 2. The Proposed Protocol

3.2 Protocol Operation

In our protocol, the *HA*s function as security proxies for the *MN*s. They testify the legitimacy of the MN¡s HoA, facilitate authentication of the MNs to the CNs, and establish shared secret session keys for them. For the appliance of the CGA, our protocol modifies the Deng-Zhou-Bao¡s one by replacing the $Cert_H$ of *EXCH0* with the self-signed X.509 v3 certificate or the optimized parameter format. Thus, when the *CN* receives the modified *EXCH0*, it should verify the *HA*¡s *CGA* using the self-signed X.509 v3 certificate or the optimized parameter format instead of $Cert_H$. The algorithm for verifying the *HA*¡s *CGA* is defined in [8].

In a case of using the self-signed X.509 v3 certificate, the CN should validate the signature on the certificate besides the HA¡s CGA. Our protocol is outlined in Fig. 2.

4. Analysis

Our protocol is analyzed in terms of security, performance and manageability. Then, it is compared with other protocols such as the Deng-Zhou-Bao¡s protocol, CAM-DH and SUCV.

4.1 Security

As computers become faster, the 64 bits of the interface identifier will not be sufficient to prevent attackers from searching for hash collisions. Our protocol uses the two hash-based CGA scheme to prevent such brute-force attacks. The scheme includes the routing prefix of the address in the input for the first hash value Hash1 and uses the second hash value Hash2 to increase the cost of brute-force attacks. During address generation, the input for Hash2 is modified by varying the value of modifier until the leftmost 12*Sec bits of Hash2 are zero. This increases the cost of address generation approximately by a factor of $2^{12*\mathrm{Sec}}$. It also increases the cost of brute-force attacks by the same factor (ie. from 2^{59} to $2^{59+12*\mathrm{Sec}}$). Thus, our protocol is more secure than other CGA based approaches such as CAM-DH and SUCV, which require the cost of brute-force attacks, $O(2^{62})$.

4.2 Performance

We evaluate the performance of our protocol in terms of the cost of verifying the HA¡s public key P_H and the public key cryptographic operations that the MN should perform. Fig. 3 shows the cost of verifying the HA¡s (or the MN¡s) public key. Our protocol needs $Cost_{Self\text{-}Signed\text{-}Cert}$ or $Cost_{OPF}$ to verify the HA¡s public key P_H, which are less than $Cost_{DZB.}$ Especially, because $Cost_{2Hash\text{-}CGA} \approx Cost_{1Hash\text{-}CGA,}$ our protocol with the optimized parameter format has almost the same cost as the cost of one hash-based approaches such as $Cost_{CAM\text{-}DH}$ and $Cost_{SUCV}$. From the viewpoint of the MN, the MN is allowed to perform no public key cryptographic operations. That is, the security proxy HA performs the expensive cryptographic operations on behalf of the MN. CAM-DH and SUCV provide the option to off-load the expensive cryptographic operation of the MN to its HA. But CAM-DH does not fully remove the expensive cryptographic operations from the MN and SUCV needs for the HA to manage the MN¡s private key.

<Notation>

$Cost_{Cert\text{-}Signature}$: the cost of verifying the signature on the certificate

$Cost_{Revocation\text{-}Status}$: the cost of checking the revocation status of the certificate

$Cost_{Cert\text{-}Path}$: the cost of verifying the certificate path

$Cost_{2Hash\text{-}CGA}$: the cost of verifying two hash-based CGA

$Cost_{1Hash\text{-}CGA}$: the cost of verifying one hash-based CGA

$Cost_{DZB}$: the cost that the Deng-Zhou-Bao's approach verifies P_H included in $Cert_H$

$Cost_{Self\text{-}Signed\text{-}Cert}$: the cost that our approach verifies P_H included in a *HA*'s self-signed certificate

$Cost_{OPF}$: the cost that our approach verifies P_H included in a *HA*'s optimized parameter format

$Cost_{CAM\text{-}DH}$: the cost that the CAM-DH verifies P_{MN}

$Cost_{SUCV}$: the cost that the SUCV verifies P_{MN}

<Cost>

$$Cost_{DZB} = Cost_{Cert\text{-}Signature} + Cost_{Revocation\text{-}Status} + Cost_{Cert\text{-}Path}$$
$$Cost_{Self\text{-}Signed\text{-}Cert} = Cost_{2Hash\text{-}CGA} + Cost_{Cert\text{-}Signature}$$
$$Cost_{OPF} = Cost_{2Hash\text{-}CGA}$$
$$Cost_{CAM\text{-}DH} = Cost_{1Hash\text{-}CGA}$$
$$Cost_{SUCV} = Cost_{1Hash\text{-}CGA}$$
$$Cost_{Revocation\text{-}Status} + Cost_{Cert\text{-}Path} > Cost_{Cert\text{-}Signature} > Cost_{2Hash\text{-}CGA} > Cost_{1Hash\text{-}CGA}$$
$$Cost_{SUCV} = Cost_{CAM\text{-}DH} < Cost_{OPF} < Cost_{Slef\text{-}Signed\text{-}Cert} < Cost_{DZB}$$

Fig. 3. The Cost of Verifying the HA¡s (or the MN¡s) Public Key

4.3 Manageability

Because our protocol needs no trusted CA and allows the HA, instead of the MN, to use the address derived from its public key, it is more manageable and scalable than other protocols.

The comparison of our protocol with other protocols such as the Deng-Zhou-Bao¡s protocol, CAM-DH and SUCV is summarized in Table 1.

As shown in Table 1, our protocol can provide good performance and manageability in addition to stronger security than one hash-based CGA protocols.

Table 1. The comparison of the proposed protocol with other protocols

	Ours	Deng-Zhou-Bao	CAM-DH	SUCV
1	X	O	X	X
2	two hash-based CGA	PKC	one hash- based CGA	one hash-based CGA
3	HA	HA	MN	MN
4	O($2^{59+12*Sec}$)	O(2^{128}) or O(2^{160})	O(2^{62})	O(2^{62})
5	$Cost_{Self\text{-}Signed\text{-}Cert}$ or $Cost_{OPF}$	$Cost_{DZB}$	$Cost_{CAM\text{-}DH}$	$Cost_{SUCV.}$
6	High	High	Low	Low
7	X	X	O	X
8	DH	DH	DH	DH
9	cookie	cookie	return routability	puzzle

1. Trusted CA
2. Mechanism binding the public key with its owner.
3. Node who generates and manages the private key/public key pair
4. Cost of brute force attacks
5. Cost of verifying the public key
6. Manageability and Scalability
7. Public key cryptographic operations the MN should perform
8. Method that generates and distributes a session key

5. Conclusion

In this paper, we propose a security proxy based protocol for authenticating the BUs, which combines the Deng-Zhou-Bao¡s protocol with Aura¡s two hash-based CGA scheme to avoid the use of trusted CAs. Because the two hash-based CGA scheme increases the cost of brute-force attacks by a factor of 2^{12*Sec} (ie. from 2^{59} to $2^{59+12*Sec}$), our protocol can achieve stronger security than other CGA-based protocols. Moreover, its cost of verifying the HA¡s public key is less than the one of the Deng-Zhou-Bao¡s protocol, and with the optimized parameter format, it can have almost the same cost as the one of one hash-based approaches. Also, the security proxy HA allows for the MN to perform no public key cryptographic operations. Because our protocol needs no trusted CA and allows the HA, instead of the MN, to uses the address derived from its public key via the CGA method, it is more manageable and scalable than other protocols.

The comparison of our protocol with other protocols such as the Deng-Zhou-Bao¡s protocol, CAM-DH and SUCV shows that our protocol can provide good performance and manageability in addition to stronger security than one hash-based CGA protocols.

References

[1] J. Arkko, "Security Framework for Mobile IPv6 Route Optimization," <draft-arkko-mipv6ro-secframework-00.txt>, Nov. 2001.

[2] R. Deng, J. Zhou, and F. Bao, "Defending Against Redirect attacks in Mobile IP," CCS¡02, Nov. 2002.

[3] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," ACM Computer Communications Review, April 2001.

[4] M. Roe, T. Aura, G. O'Shea, and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," <draft-roe-mobileip-updateauth-02.txt>, Feb. 2002.

[5] S. Okazaki, A. Desai, C. Gentry and et. el., "Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)," <draft-okazaki-mobileip-abk-01.txt>, Oct. 2002.

[6] G. Montenegro, C. Castelluccia, "SUCV Identifiers and Addresses," <draft-montenegro-sucv-02.txt>, Nov. 2001.

[7] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," <draft-ietf-mobileip-ipv6-24.txt>, Jun. 2003.

[8] T. Aura, "Cryptographically Generated Addresses (CGA), " <draft-aura-cga-00.txt>, Feb. 2003.

[9] R. Housley, W. Ford, T. Polk, and D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile," RFC 2459, Jan. 1999.