Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption

Martin Ehmke and Harri Forsgren
University of Helsinki, Finland
martin.ehmke@gmail.com; hforsgre@cs.helsinki.fi

Kaj Grahn and Jonny Karlsson
Arcada University of Applied Sciences, Helsinki, Finland
kaj.grahn@arcada.fi; jonny.karlsson@arcada.fi

Timo Karvi
University of Helsinki, Finland
karvi@cs.helsinki.fi

Göran Pulkkis
Arcada University of Applied Sciences, Helsinki, Finland
goran.pulkkis@arcada.fi

Abstract

Control signaling messages in Mobile IPv6 are mainly used to inform the home agent (HA) and the correspondent node (CN) about the mobile node's (MN's) new address when its network attachment point is changed. In order to prevent various security attacks, these messages must be protected. In the current standard, the control signaling messages between a HA and a MN are authenticated using IPSec, often with IKEv2 and X.509 certificates. Control signaling messages between a MN and a CN are currently protected by an effective but insecure protocol, known as Return Routability. Using IBE (Identity-Based Encryption) for authenticating control signaling messages requires more processing power but significant security enhancements are achieved. The current protocols for protecting control signaling messages are outlined in this paper. Proposed approaches for implementing IBE-authentication between a MN and a HA as well as between a MN and a CN are presented. Environments where the MN and the CN use the same Public Key Generator (PKG) as well as environments where they use different PKGs are taken into account. Finally, the performance of some proposed signaling protocols is estimated. An overview of IBE is given and the elements and operations needed to set up an IBE infrastructure are described in an appendix.

Keywords: mobile IPv6, mobile networking, network security, identity based encryption, elliptic curve cryptography, key agreement protocol, Internet Key Exchange protocol, EAP, routing.

Introduction

The number of devices connected to the Internet has grown rapidly during the last years. At the same time more and more computers have become portable and mobile. This has lead to an increased need for unique IP addresses as well as for the ability to move between

different network attachments while still maintaining the network connection.

Mobile IPv6 (MIPv6) is a protocol providing mobility features for IPv6 nodes (Johnson, Perkins, & Arkko, 2004). MIPv6 is estimated to be widely used in the future Internet. When moving to another network attachment point, a mobile node (MN) receives a new IP address from the local router. This new address has to be registered on the home router, known as home agent (HA), and also on the current communication partner, called correspondent node (CN), if route optimization is used.

These control signaling messages, called binding updates (BU), must be protected in order to prevent various attacks, such as man-in-the-middle and denial-of-service attacks (Boyd & Mathuria, 2003; Kempf, Arkko, & Nikander, 2004). In the current version of MIPv6, BUs between a MN and its HA are mainly protected using IPSec.

The possibilities to use identity-based encryption (IBE) for securing binding updates in the MIPv6 protocol are explored in this paper. IBE is a public key based cryptosystem where an arbitrary identity string can be used as a valid public key. Certificates and certificate revocation lists (CRL) are thus not needed and a user or client does not need to install certificates, verify certificates or perform searches in CRLs. These are significant advantages for mobile devices with limited bandwidth and low processing power. More details of IBE are provided in Appendix A and a list of abbreviations is in Appendix B.

In MIPv6 a security mechanism called Return Routability (RR) is specified for route optimization. RR is not based on public keys. Thus it can not be modified directly for IBE. However, certificate based protocols have been proposed instead of the RR protocol, and these protocols can be modified for IBE. Furthermore, there are IBE-based authenticated key agreement protocols which can be applied to secure the communication between a MN and a CN.

Binding Updates in Mobile IPv6

The MIPv6 protocol allows a MN to transparently maintain its network connection when the network attachment changes (Johnson, Perkins & Arkko, 2004). A MN is always reachable at its home address (HA), even if it is not physically located in its home network. When connected to a foreign network a MN receives a Care-of-Address (CoA) from the local router through stateless or stateful autoconfiguration. After receiving the CoA, the MN sends its current location information (CoA) in a binding update message (BU) to it's HA. After this process (called home registration) the HA can redirect and tunnel packets, directed to the MN's home address, to the MN's CoA. The process where a MN, located in a foreign network, is communicating with a CN (a stationary or mobile peer communicating with a MN) through the HA is called bidirectional tunneling. Bidirectional tunneling is used in the case the CN does not have a binding for the MN (registration in progress) or the CN does not support MIPv6.

Protection of Binding Updates between a MN and it's HA

The binding update signaling and other control messages between a home agent and its mobile node must be protected. MIPv6 specifies that an IPSec Encapsulating Security Payload (ESP) is used to secure home registration signals (BU and BA, Binding Acknowledgment), Return Routability messages (see next subsection), MIPv6 specific ICMPv6 messages, and payload packets.

The ESP header must have a non-null authentication transform for data origin authentication and connectionless integrity protection, and may optionally use anti-replay protection, if dynamic key exchange is used. Thus the defined security associations are based on the home address of the MN. In this case it is not necessary to change security associations in transport mode when the Care-of Address of the MN changes.

The use of ESP with binding update and ICMPv6 messages ensures that signaling and processing of the signaling is accepted only from authorized mobile hosts. Because the ESP authentication does not cover the MN's Care-of-Address, the binding update must have an alternate Care-of-Address option after the ESP header, containing the MN's care-of address.

All IPSec implementations must support both manual and automated key management. Manual techniques are feasible only in small environments. The default protocol for automated key management is IKEv2 (Kaufman, 2005). Besides the mutual authentication of communicating parties, it supports dynamic key management and negotiation of cryptographic algorithms. Authentication can be based on a shared secret, on X.509 certificates or on the Extensible Authentication Protocol (EAP).

An important part for IKEv2 security is based on the initial message exchange which consists of two message pairs, see Figure 1. The first pair, so-called IKE SA INIT, exchanges security parameters (HDR), supported algorithms (SA_{i1} and SA_{r1}), nonces (N_i and N_r), and Diffie-Hellman values (KE_i and KE_r). This pair creates so-called IKE SA. At this point each party can generate SKEYSEED, from which all the other keys are derived. Thus the key SK used in the second phase is derived from SKEYSEED.

The second pair sends the identities (ID_i and ID_r), authenticates them (*AUTH*) using either a shared secret key or the private key corresponding to the identity's X.509 certificate and finally sets up the SA pair (SA_{i2}, SA_{r2}). The symbols TS_i and TS_r are so called traffic selectors which are not essential in this context. The contents of the first message exchange are also verified during that authentication part. IKE thus prevents a man-in-the-middle attack on the Diffie-Hellman values. It is also impossible for an attacker to unnoticeable drop supported algorithms forcing the communication partners to fallback to weaker algorithms.

1. I → R: HDR, SA_{i1}, KE_i, N_i
2. R → I: HDR, SA_{r1}, KE_r, N_r, [*CERTREQ*]
3. I → R: HDR, E_{SK}{ID_i,[*CERT*,][*CERTREQ*,][ID_r,]*AUTH*,SA_{i2},TS_i,TS_r}
4. R → I: HDR, E_{SK}{ID_r,[*CERT*,]*AUTH*, SA_{r2},TS_i,TS_r}

Figure 1: IKE Initial Message Exchange: Initiator I communicates with responder R.

As shown in the Initial Message Exchange, the authentication payload *AUTH* is used to mutually authenticate the communicating parties. Depending on the chosen method, it carries a public key signature or a message authentication code (MAC). If any *CERT* payloads are provided, then the public key in the first *CERT* load must be used to verify the *AUTH* load. Obviously checking the validity of a signature can take some time, when there is a larger certificate chain to be checked and possibly certificate revocation lists also have to be consulted. If no *CERT* payloads are provided, then a MAC with a common shared key must be used for authentication.

More specifically, each party signs or MAC protects its first message to the other side, receives a nonce from the other side, and includes the results in the *AUTH* payload. This step is critical for the overall security of IKE. After all, the first two messages carry the algorithm proposals and Diffie-Hellman values. If integrity is not protected, an attacker could force the usage of weak algorithms or run a man-in-the-middle attack, respectively.

It is also possible to use *EAP* for authentication. If this is the case, the *AUTH* payload of the third message is left out as a signal to initiate the *EAP* authentication. Figure 2 shows the messages exchanged in *EAP* authentication. There may be 1−10 EAP-exchanges in the protocol. Success will end the EAP exchange (and, of course, an error). The used EAP method should provide a shared key and this key should be used in the authentication.

```
1.    I → R: HDR, SA_i1, KE_i, N_i
2.    R → I: HDR, SA_r1, KE_r, N_r, [CERTREQ]
3.    I → R: HDR, E_SK{ID_i,[CERTREQ,][ID_r,]SA_i2,TS_i,TS_r}
4.    R → I: HDR, E_SK{ID_r,[CERT,]AUTH,EAP}
5.    I → R: HDR, E_SK{EAP}
6.    R → I: HDR, E_SK{EAP}
.. ... ...
n.    R → I: HDR, E_SK{EAP(success)}
n+1.  I → R: HDR, E_SK{AUTH}
n+2.  R → I: HDR, E_SK{AUTH,SA_r2,TS_i,TS_r}
```

Figure 2. IKE Initial Message Exchange: Authentication using EAP (Kaufman, 2005).

Route Optimization

If the CN supports MIPv6, a more effective mobile routing technique called Route Optimization (RO) can be used. RO enables a MN and a CN to send packets directly to each other over the shortest route. Thus packets do not need to go through the HA. Before RO can be established, the MN must send a BU packet containing its CoA to the CN to inform about its current location. RO is efficient since triangular routing (bidirectional tunneling) is avoided. However, RO also causes new security risks, as described i.e. in (Nikander et al., 2005). It could, for example, be possible that a MN sends a false BU packet to the CN and redirects the communication stream to a desired location that can cause Denial-of-Service (DoS) attack. Therefore, authentication of BUs in RO is essential for maintaining security.

The situation between a MN and a CN is different compared to the situation between MN and it's HA. The CN may be any node. Thus there are no shared secrets or trusted certificates between the MN and the CN, which the MN is communicating with. That is why a so-called Return Routability procedure (RR) is applied. This is done in several steps:

1. A MN sends *home test init* (HoTi) and *care-of test init* (CoTi) to the CN. HoTi is sent through the HA and CoTi directly. Both contain a cookie and have the home address or the care-of address, respectively, as the source address.
2. On reception of either of the two messages HoTi or CoTi, the CN replies immediately with a *home test* (HoT) or *care-of test* (CoT) message. The replies are sent to the respective source address. Each of these replies contain the cookie retrieved from the corresponding init message, a nonce index and a keygen token, which is then later used for authentication of the binding updates.
3. When the MN has received HoT and CoT, the RR procedure is complete. MN is the only one being able to receive packets sent to both its home address and care-of-address. It can now calculate the binding key by hashing the two tokens. This key is used to create a Message Authentication Code (MAC) for Binding Updates. The created MAC can be verified by the CN.

The messages Home Test Init and Home Test are ESP protected. RR prevents simple third party attacks, but if the third party can take both HoTi and CoTi messages before they reach the correspondent node, attacks are possible. Moreover, a misbehaving mobile node can still make successful attacks in spite of the above measures. For example, a MN could include a fake care-of address in a binding update message to it's HA. The home agent is then used as an intermediate in a denial-of-service attack on the owner of the care-of address.

Mobile IP messages use a sequence number to protect against replay attacks and to ensure the correct ordering of the packets. The sequence numbers are tracked using a sliding window mechanism. For example, supposing a fixed window size of m packets and a situation where all packets with sequence numbers $< n$ have been acknowledged. The sender may then send out packets with sequence numbers $\{n, n+1,\ldots, n+m-1\}$ before receiving acknowledgment for the packet with sequence number n. When acknowledgment arrives from the receiver for the packet with the sequence number n, then the sequence number range (window) of unacknowledged packets slides to $\{n+1, n+2,\ldots, n+m\}$, and the sender is able to send out the packet with the sequence number $n + m$.

IBE Authentication in Mobile IPv6

Authentication of mobile nodes is essential in order to prevent possible attackers from spoofing the mobile node's identity. On the other hand, it is important for the mobile node to be sure about its communication partner. As seen before, identity-based authentication can ease the whole authentication process essentially. In this section, proposals for MIPv6 authentication based on IBE are presented.

First, IBE-authentication between a MN and a HA is considered. It is assumed that MN and HA establish IPSec SAs between each other and that IPSec uses the IKEv2 protocol. It is self evident that MN and its HA will use the same PKG, since they belong to the same organization. After this several possibilities to apply IBE-authentication between a MN and a CN are considered.

IBE Authentication between a Mobile Node and it's Home Agent

Mutual authentication between a MN and its HA is obligatory in MIPv6 and is normally done using IPSec and IKE. The authentication and session key generation is done with IKE. Currently, the normal way to do this is to use X.509 certificates in IKE. It is also possible that MN and HA already have a common shared secret. This can happen, for example, in WLAN environments, when MN moves to another WLAN that demands authentication.

If there are no shared secrets, it is natural to extend the IKEv2 authentication process to use identity-based authentication instead of authentication based on X.509 certificates. It is also natural to assume that both the MN and the HA use the same PKG. Depending on the relationship of these three entities, any of the trust levels I-III may be applied when the private keys are delivered.

When looking at IKE there are basically two ways of implementing IBE. The first method is to modify IKE's four-way handshake. The other method is to use EAP and create a new EAP authentication method based on IBE.

Modifying IKE

IBE may be applied in IKE by adding a third authentication method besides the existing shared-secret and X.509 authentication. Then IKE uses "IBE certificates" instead of X.509 certificates. Basically this IBE-based authentication works in the same way as X.509 authentication. Thus the peers are authenticated by signing the same block of data as in the X.509-based authentication, but using now an IBE-based signature, for example the previously introduced Hess signature. Now identities replace certificates and it is not necessary to check revocation lists.

A prototype implementation realizing this idea was done in (Ehmke, 2007). From a performance point-of-view it is obvious that there is no need anymore to transmit certificates or certificate requests, because the IKE identity can be used directly as the public key for authentication. Also expensive certificate-chain checking becomes superfluous. Moreover, it could be shown that

hardware accelerated IBE algorithms based on elliptic curve cryptography can be very efficient, especially on embedded devices.

Using EAP

If EAP is used, then Figure 2 shows the possible phases. EAP is recommended to be used with a method that establishes a shared key at the same time. This key should be used in the last two message exchanges that guarantee authentication.

One possibility is Chen's and Kudla's key agreement method using IBE (protocol 2' in (Chen & Kudla, 2003)). This protocol works without key escrow. Then the CERTREQ and CERT messages in steps 2, 3, 4 in Figure 2 are not needed. The resulting IKE Initial Message exchange is shown in Figure 3. In this case, both MN and HA have the same PKG, P is a public parameter of the PKG, and the random numbers a, b are chosen by the HA and the MN, respectively.

1. $MN \rightarrow HA$: HDR, SA_{MN1}, KE_{MN}, N_{MN}
2. $HA \rightarrow MN$: HDR, SA_{HA1}, KE_{HA}, N_{HA}
3. $MN \rightarrow HA$: HDR, $E_{SK}\{ID_{MN}, [ID_{HA},] SA_{MN2}, TS_{MN}, TS_{HA}\}$
4. $HA \rightarrow MN$: HDR, $E_{SK}\{ID_{HA}, AUTH, \text{EAP-CK-Req}(a \cdot P, a \cdot Q_{HA})\}$
5. $MN \rightarrow HA$: HDR, $E_{SK}\{\text{EAP-CK-Res}(b \cdot P, b \cdot Q_{MN})\}$
6. $HA \rightarrow MN$: HDR, $E_{SK}\{EAP(\text{success})\}$
7. $MN \rightarrow HA$: HDR, $E_{SK}\{AUTH\}$
8. $HA \rightarrow MN$: HDR, $E_{SK}\{AUTH, SA_{HA2}, TS_{MN}, TS_{HA}\}$

Figure 3. IKE Initial Message Exchange: Authentication using EAP with IBE.

The Chen-Kudla protocol generates a session key which is used only for authentication in the messages 7 and 8. The AUTH payloads must authenticate messages 3 and 4 and the authentication is based on MAC with the secret key generated by the EAP (Chen-Kudla) protocol.

IBE Authentication between a MN and a CN

Four approaches to adapt IBE authentication between a MN and a CN are presented. In the first approach the authentication is delegated to home agents. In the second approach, public elliptic curve infrastructure is used when a MN and a CN are communicating with each other. In the third approach an IBE based key agreement protocol proposed in (Kim, Lee, & Oh, 2005) is applied. In the fourth approach IBE is integrated with Cryptographically Generated Addresses (CGAs) (Cao et al., 2007). Since it is impossible to predict which CN will communicate with a MN it cannot be assumed that a MN and a CN use the same PKG. Multi-PKG based security solutions are therefore relevant.

Delegating Authentication to Home Agents

In (Bao et al., 2005) is introduced a protocol called Certificate-Based Binding Update Protocol (CBU) that is used to delegate the MN and CN authentications to Home Agents (HAs). Figure 4 shows the message exchange of the protocol.

In Figure 4, first an ESP protected request for shared secrets between the MN and the CN is sent by the MN to it's HA in the existing IPSec tunnel. HA and CN send cookies (CK-1, CK-2) to each other and validate the received cookies. This phase prevents triggering of computationally expensive cryptographic calculations in DoS attacks. HA and CN agree on shared secrets with a DH key agreement, in which the exchanged public DH keys are authenticated with PKI signatures certified by a common CA. An ESP protected reply including the agreed shared secrets is sent by the HA to the MN in the existing IPSec tunnel. Now Binding Update communication be-

tween the MN and the CN can start and it is authenticated by message authentication codes based on the agreed shared secrets.

The content of the messages is explained in the draft (Bao et al., 2005). The X.509 certificate based authentication and DH-key generation in steps 4-5 (see Figure 4) can be replaced with IBE-signatures and elliptic curve DH. Thus the signing is done by applying, for example, the IBE signature scheme in (Hess, 2002). In this case, the signed data (m in the chosen IBE signature scheme) is the same as in the original protocol. If the MN and CN use different IBE PKGs, then the public parameters of the signer must be sent along with the signature. This does not cause security risks, if the receiver knows the partner's PKG or is able to check that such a PKG exists.

1. $MN \rightarrow HA$: Req-secrets-MN-CN
2. $HA \rightarrow CN$: CK-1
3. $CN \rightarrow HA$: CK-2
4. $HA \rightarrow CN$: DH-parameters, sign
5. $CN \rightarrow HA$: DH-parameters, sign
6. $HA \rightarrow MN$: Reply-secrets
7. $MN \rightarrow CN$: $E_{KDH}\{BU\ message\}$

Figure 4. Delegating authentication to Home Agents.

Using a Public Elliptic Curve Infrastructure

The certificate-based technique proposed in (Hu, Zhou & Li, 2006) can be replaced by IBE-based signatures. In the original method, the participants are MN, CN and a common certificate authority CA. The method is shown in Figure 5.

1. $MN \rightarrow CA$: Request, T_1
2. $CA \rightarrow MN$: $D_{KprCA}\{K_{pbCN}, \text{Request}, T\}$
3. $MN \rightarrow CN$: $E_{KpbCN}\{MN, R\}$
4. $CN \rightarrow CA$: Request, T_2
5. $CA \rightarrow CN$: $D_{KprCA}\{K_{KpbMN}, \text{Request}, T_2\}$
6. $CN \rightarrow MN$: $E_{KpbMN}\{R_1, CK_2\}$
7. $MN \rightarrow CN$: $E_{KpbCN}\{D_{KprMN}\{CK_2, K_{SC}\}\}, E_{KSC}\{BU\ message\}$

Figure 5. Public key based authentication between a MN and a CN.

In Figure 5, T_1 and T_2 are timestamps, R_1 is a nonce, CK_2 a cookie, and K_{SC} is a common secret between MN and CN. This secret is generated by MN and it is delivered confidentially to CN in the protocol. The symbol E_{Kpb} means encryption with the public key K_{pb} and D_{Kpr} means the signature with the private key K_{pr}.

Now the certificate-based public key encryption and signatures can be replaced by IBE-based encryption and signatures. Then, the CA would be replaced by a PKG and the steps 1 and 2 as well as steps 4 and 5 in the original protocol would be unnecessary. NAIs (Network Access Identifiers) could be used as identities for all mobile nodes and in this case a MN can calculate the public key of a CN using the NAI of the CN. In addition to the NAI, the MN needs the public parameters of the CN's IBE system in order to be able to use the encryption with CN's public key. Both MN and CN must know the public parameters of each other's PKG. If MN and CN belong to the same PKG, then MN knows CN's and PKG's public parameters automatically and the protocol has only 3 phases. If the MN and CN have different PKGs, the MN must start the communication by sending a message to CN requesting for the public parameters of the CN and

its PKG. In the same message, MN can send the public parameters of its own IBE system to CN. In this case the protocol has 5 phases.

More precisely, the encryption E_{KpbCN} in step 3 is now done using IBE-based public key encryption and the signing with D_{KprMN} in step 7 is replaced with the IBE signature in (Hess, 2002). The encryption E_{SC} in step 7 is symmetric.

Using Multi-PKG Private Key Generation

A Multi-PKG key agreement protocol in (Kim, Lee, & Oh, 2005) is applied in the message exchange between a MN and a CN. Delivery of the public PKG parameters is added to the original protocol. The resulting signaling protocol is shown in Figure 6. It is assumed that MN uses PKG_1 and CN uses PKG_2.

In the protocol in Fig 6, after the first two messages, MN calculates the values

$$V_{MN}^{(1)} = a^{(1)}P^{(1)},\ a^{(1)} \in Z^*_{q(1)},\ \text{random}, \quad (1)$$

$$V_{MN}^{(2)} = a^{(2)}P^{(2)},\ a^{(2)} \in Z^*_{q(2)},\ \text{random}, \quad (2)$$

and CN calculates the values

$$V_{CN}^{(1)} = b^{(1)}P^{(1)},\ b^{(1)} \in Z^*_{q(1)},\ \text{random}, \quad (3)$$

$$V_{CN}^{(2)} = b^{(2)}P^{(2)},\ b^{(2)} \in Z^*_{q(2)},\ \text{random}. \quad (4)$$

After the fourth step, MN calculates the session key *SK* as follows:

$$K_{MC}^{(1)} = e^{(1)}(S_{MN}, V_{CN}^{(1)}), \quad (5)$$

$$K_{MC}^{(2)} = e^{(2)}(Q_{CN}, a^{(2)}P_{pub}^{(2)}), \quad (6)$$

$$SK = H(K_{MC}^{(1)} || a^{(1)}V_{CN}^{(1)} || K_{MC}^{(2)} || a^{(2)}V_{CN}^{(2)}). \quad (7)$$

CN calculates the same session key SK as follows:

$$K_{CM}^{(1)} = e^{(1)}(Q_{MN}, b^{(1)}P_{pub}^{(1)}), \quad (8)$$

$$K_{CM}^{(2)} = e^{(2)}(S_{CN}, V_{MN}^{(2)}), \quad (9)$$

$$SK = H(K_{CM}^{(1)} || b^{(1)}V_{MN}^{(1)} || K_{CM}^{(2)} || b^{(2)}V_{MN}^{(2)}). \quad (10)$$

The AUTH payloads in steps 5 and 6 in Figure 6 contain a MAC authentication, where the key *SK* is used. The last message 7, the binding update message, is encrypted using some symmetric encryption algorithm with the session key *SK*.

1. *MN* → *CN*: the public parameters of PKG_1
2. *CN* → *MN*: the public parameters of PKG_2
3. *MN* → *CN*: $V_{MN}^{(1)}$, $V_{MN}^{(2)}$
4. *CN* → *MN*: $V_{MN}^{(1)}$, $V_{MN}^{(2)}$
5. *MN* → *CN*: $AUTH_{MN}$
6. *CN* → *MN*: $AUTH_{CN}$
7. *MN* → *CN*: $E_{SK}\{BU\ message\}$

Figure 6. Authentication between a MN and a CN using a multi-PKG key agreement protocol in (Kim, Lee, & Oh, 2005).

Integration of IBE with Cryptographically Generated Addresses

The RR procedure for Route Optimization between a MN and a CN after a network attachment change for the MN is vulnerable to advanced eavesdropping attacks. Moreover, no ownership check of a MN Home Address is included in the RR procedure.

A recent IETF standard therefore specifies an enhanced Route Optimization protocol based on Cryptographically Generated MN Home Addresses as an optional alternative to the RR procedure (Arkko, Vogt, & Haddad, 2007). A Cryptographically Generated Address (CGA) is a 128 bit IPv6 address with a given 64 bit subnet prefix and a 64 bit interface identifier, which is derived from a hash of the public key of a MN (Aura, 2005). A CGA thus provides a strong cryptographic binding between the interface identifier of the CGA and the MN which owns the public key. With this binding the ownership of a MN Home Address can be proved without a PKI. A Home Address ownership proof is implemented in the Enhanced Route Optimization protocol by a BU message signed by the private key of the MN (Arkko, Vogt, & Haddad, 2007).

Authentication of a BU message with the CGA property of the Home Address of a MN does not suffer from the eavesdropping vulnerability of the RR procedure but is still vulnerable to unauthentic key attacks. An unauthentic public key can be used to generate a valid CGA address and the corresponding private key can be used to sign a fake BU message. A mechanism to solve this problem by integrating IBE with CGA is presented in (Cao et al., 2007). In the proposed scheme, MNs should first register an IBE-identity and get their public and private key pairs. The public key is then used to compute the CGA address, and the private key is used to sign.

The objective is to use the public and private IBE keys and then generate CGA addresses and signatures without paying additional computational cost of pairing. To address this issue an efficient IBE scheme called Combined Public Key (CKP) is deployed in (Cao et al., 2007). CKP is based on Elliptic Curve Cryptography (ECC). The ECC parameters are $T = \{a, b, G, n, P\}$, where a, b are parameters of elliptic curve $E : y^2 = x^3 + a \cdot x + b$ ($a, b \in F_p$), G is the base point and p is the order of prime field F_p. Let the private key of user A be an integer SK_A in F_p, then the public key of A is $SK_A \cdot G$, which is also a point on E.

In the scheme (Cao et al., 2007), two small size (m x n) matrixes, the Private/Secret Key Factor matrix (SKF) and the corresponding Public Key Factor matrix (PKF), compose a large number of private/public key pairs (m^n). The SKF matrix is composed of randomly chosen integers r_{ij} in F_p and the PKF matrix is composed of corresponding points $r_{ij} \cdot G$ on E. The chosen integers are generated by a PKG called Key Management Center (KMC) and kept secret until revocation. The user's private and public key pairs are obtained from a number of indexes based on the user ID. To obtain the indexes, a mapping algorithm F defined as a set of hash functions F_1, F_2,, …., F_n is deployed. Mathematically this can be written as $F(\text{user ID}) = (F_1(\text{user ID}) \bmod m, F_2(\text{user ID}) \bmod m, \ldots, F_n(\text{user ID}) \bmod m) = (i_1, i_2, \ldots, i_n)$, where $1 \le i_k \le m$.

Finally, the private key and the public key of user A are calculated from:

$$SK_A = (r_{i11} + r_{i22} + \ldots + r_{inn}) \bmod p \quad (11)$$

$$PK_A = (r_{i11} \cdot G + r_{i22} \cdot G + \ldots + r_{inn} \cdot G) \bmod p \quad (12)$$

Integrating IBC with CGA includes three main steps (Cao et al., 2007):

- ***IBC Setup***. The Combined Public Key cryptosystem for SKF/PKF matrixes is set up and registration from mobile nodes is received
- ***Key Extraction and Distribution***. The mobile node asks for an IBC identity from the Identity Management Centre and the public key factor matrix from the KMC is downloaded. The

mobile node then computes its own public key. The private key is distributed to the mobile node "out-of-band".

– ***IBC-CGA Address Generation.*** The final IPv6 address is generated using the procedure specified in (Aura, 2005).

Signing a message includes concatenating of the 120-bit type tag (type tag || message) and signing the concatenated message with the private key from the CPK as input. The validity of the original message with the signature and an IBE-CGA parameter data structure is checked by verifying the CGA address via the procedure specified in (Aura, 2005), concatenating the type tag, and the signature using the ECDSA algorithm with the public key as input.

The Mobile Node initiates a Correspondent Node registration for many reasons (Arkko, Vogt, & Haddad, 2007), i.e. the mobile node sends a Binding Update message to the correspondent node. The Binding Update message is authenticated in the following ways:

– If the MN´s home address is a CGA, but the mobile node does not have a permanent home keygen token, the MN authenticates the Binding Update message based on the CGA property of its home address

– If the MN´s home address is a CGA, and the mobile node has a permanent home keygen token, the MN authenticates the Binding Update message based on the CGA property by a proof of its knowledge of the permanent home keygen token

– If the MN´s home address is not a CGA, the MN authenticates the Binding Update message through a proof of reachability at its home address.

If the selected authentication method is related to CGA, the mobile node includes its CGA parameters and signature in the Binding Update message by adding one or more CGA Parameters options directly followed by a Signature option. The mobile node authenticates all subsequent Binding Update messages by a proof of its knowledge of the home key token obtained from the CN a Binding Acknowledgement message. This ensures that an attacker cannot downgrade the authentication method chosen by a MN. The type of home keygen token used by the mobile node depends on the authentication method. (Arkko, Vogt, & Haddad, 2007)

Performance Issues

RSA encryption and decryption are four to nine times faster than pairing based IBE encryption and decryption (Barreto et al., 2002; Scott, 2007). Thus the benefits of IBE methods are not based on the speed, but on the fact that it is not necessary to check the validity of certificates. This usually saves two steps in protocols, certificate chain validation and CRL checking. In most cases, it is better to save steps than processing time.

Binding Updates between a MN and it's HA

The number of steps in the protocols and the number of encryption, decryption and signature operations a MN must execute are considered. Possible authentication and integrity methods in the BU messages are not taken into account, since these methods are included in certificate based protocols as well as in IBE-based protocols and are usually based on symmetric encryption methods with a key that has been deduced from the session key.

The certificate based IKE takes 5 steps. (Compared to Figure 1, we add one step which starts the BU message.) There are 2 symmetric encryptions (one in the BU message), 1 decryption, 1 certificate-based signature and 1 signature verification. In addition, there is 1 certificate check (certificate chain and revocation list).

If IKE modified by with IBE is considered, then only the last two operations are left out. In the authentication, IBE-based methods are used. Thus signature operations are slower, but the overall performance is better than in the certificate based IKE.

On the other hand, IKE with EAP and IBE contains 9 steps (including the first BU message), 4 symmetric encryptions, 1 digital signature and 1 signature verification. Signatures may be based on MAC, but because of the number of messages exchanged the EAP version cannot compete with the modified IKE in speed. However, it may be applied, when an external authentication server is in use.

Binding Updates between a MN and a CN

Four protocols to secure the BU message from MN to CN,

- Delegation (Fig. 4)
- Public Key (Fig. 5)
- Key Agree (Fig. 6), and
- IBE&CGA,

have been presented. These protocols cannot compete in speed with the Return Routability procedure, but they are safer. That is why we compare the certificate based versions of Delegation and Public Key protocols with their IBE versions. Moreover, we compare the four IBE versions with each other.

When comparing certificate-based and IBE-based protocols, we only consider steps needed in the protocols. It is seen at once that the IBE-based versions of Delegation and Public Key save always two steps, in the Public Key protocol even four steps, if the public parameters of MN and CN are known to MN and CN. Thus the IBE versions are more efficient.

It is more interesting to compare the IBE versions with each other. In this case considered the number of

- pairings (#p),
- elliptic curve point multiplications (#m), and ‘
- finite field exponentiations (#e).

Symmetric encryption operations and hash operations are not taken into account, because these operations are very fast compared to elliptic curve operations. The numbers are seen in Figure 7.

In the Delegation protocol, MN does not make elliptic curve operations at all. That is why HA operations are counted in Figure 7 instead of MN operations. The elliptic curve operations in the IBE&CGA protocol are needed in the generation and verification of an ECDSA signature. It is seen that the IBE&CGA protocol is the most efficient, if we consider only elliptic curve operations. The three first protocols in Figure 7 have the same number of steps. If MN has very limited processing power, then the Delegation protocol maybe a good alternative.

Protocol	#p	#m	#e
Delegation	3	3	2
Public Key	4	6	1
Key Agree	2	3	
IBE&CGA		3	

Figure 7. The number of elliptic curve operations in different IBE secured binding update protocols.

Conclusions

Currently, IP Security Encapsulation Security Payload (IPSec ESP) in transport mode is the standardized method for securing BUs and other control messages sent in the home registration process. Mutual authentication, dynamic key management and negotiation of cryptographic algorithms are handled by the IKEv2 protocol. The authentication method is based on a shared secret, X.509 certificates or Extensible Authentication Protocol (EAP). This paper outlines how IBE can be applied by replacing X.509 certificate based authentication with IBE-based authentication in the four-way IKE handshake or by embedding an IBE based key agreement method in EAP.

In Route Optimization (RO), where control signals are sent between the MN and a CN, the situation is different. Since the CN could be any node, there are no shared secrets or trusted certificates between a MN and the CN it is communicating with. The Return Routability (RR) procedure, which has been standardized for securing control messages in RO, prevents simple third party attacks but can easily be broken if i.e. an attacker manages to lay his hands on the RR messages. Two proposals to replace the RR procedure with X.509 certificate based authentication have been made. In Certificate-Based Binding Update Protocol (CBU), (Bao et al., 2005), mutual authentication between a MN and a CN is delegated to the HA of the MN. Authentication is based on verification of PKI signatures on exchanged DH parameters. In the method proposed in (Kim, Lee & Oh, 2005) both the MN and the CN request authentication certificates from the same CA. This paper shows how X.509 certificate based authentication can be replaced with IBE authentication in both proposals by replacing PKI signatures with IBE signatures and PKI encryption with IBE encryption. A third IBE-based method presented in this paper for mutual authentication between a MN and a CN uses IBE-based key agreement in a multi-PKG environment. A fourth IBE based method integrates IBE with the use Cryptographically Generated Addresses for MN Home Addresses.

Performance measurements have shown that the computational costs are higher for pairing based cryptographic IBE operations in comparison with RSA/DSA/ECC-based cryptographic operations used in a PKI. However, since a public key operation in a X.509 certificate based PKI must verify a certificate chain and check the CRL of the issuing CA, pairing based IBE still provides a significant performance advantage compared to PKI. Performance estimations show that

- the IBE modified four-way IKE handshake clearly outperforms embedding of an IBE based key agreement method in EAP in mutual authentication between a MN and its HA,
- integration of IBE with the use Cryptographically Generated Addresses for MN Home Addresses leads to the most efficient IBE-based mutual authentication between a MN and a CN in a multi-PKG environment.

Security analyses of the used protocols have not been carried out, since all the used protocols are already analyzed protocols which have been adapted without compromising the uniqueness of initial random values or any other security assumptions.

References

Arkko J., Vogt, C., & Haddad, W. (2007). *Enhanced route optimization for Mobile IPv6*. IETF RFC 4866.

Aura, T. (2005). *Cryptographically generated addresses (CGA)*. IETF RFC 3972.

Bao, F., Deng, R., Qiu, Y., & Zhou, J. (2005). *Certificate-based binding update protocol (CBU)*. Expired IETF Internet Draft. Retrieved December 14th, 2008, from http://tools.ietf.org/id/draft-qiu-mip6-certificated-binding-update-03.txt

Barreto, P. S. L. M., Kim, H. Y., Lynn, B., & Scott, M. (2002). Efficient algorithms for pairing-based cryptosystems. In M. Yung (Ed.), *Advances in cryptology - Proceedings of CRYPTO 2002*, 354-368, Springer-Verlag, LNCS 2442.

Boyd, C., & Mathuria, A. (2003). *Protocols for authentication and key establishment*. Springer-Verlag

Cao, Z., Deng, H., Ma, Y., & Hu, P. (2007). Integrating identity based cryptography with cryptographically generated addresses in Mobile IPv6. In O. Gervasi & M. Cavrilova (Eds.) *ICCSA 2007*, LNCS 4706, Part II, Springer-Verlag, pp. 514-525.

Chen, L., & Kudla, C. (2003). Identity-based authentication key agreement protocols from pairings. *Proceedings of the 16th IEEE Computer Security Foundations Workshop - CSFW*, pp 219-233.

Ehmke, M. (2007). *Authentication methods for Mobile IPv6*. Master's thesis, University of Helsinki, Department of Computer Science.

Hess, F. (2002). Efficient identity based signature scheme based on pairings. *SAC 2002*, LNCS 2595 pp. 310–324.

Hu D., Zhou D., & Li P. (2006). PKI and secret key based mobile IP security. *Proceedings of the International Conference on Communications, Circuits and Systems, 3*, pp 1605–1609.

Johnson, D., Perkins, C., & Arkko, J. (2004). *Mobility support in IPv6*. IETF RFC 3775.

Kaufman, C. (2005). *Internet key exchange (IKEv2) Protocol*. RFC 4306.

Kempf, J., Arkko, J., & Nikander, P. (2004). Mobile IPv6 security. *Wireless Personal Communications, 29*, 389-414.

Kim, S., Lee, H., & Oh, H. (2005). Enhanced ID-based authenticated key agreement protocols for a multiple independent PKG environment. *ICICS 2005*, LNCS 3783, pp. 323–335.

Nikander, P., Arkko, J., Aura, T., Montenegro, G., & Nordmark, E. (2005). *Mobile IP version 6 route optimization security design background*. IETF RFC 4225.

Scott, M. (2007). Implementing cryptographic pairings. In T. Takagi, Tat. Okamoto, E. Okamoto, and Tak. Okamoto (Eds.), *Pairing-based cryptography: Proceedings of First International Conference, Pairing 2007*, Tokyo, Japan, Springer-Verlag, LNCS. 4575, pp. 177-196

Appendix A: Identity-Based Encryption (IBE)

Identity-based encryption (IBE) is a public-key cryptosystem which is simpler than certificate-based cryptosystems in the sense that an arbitrary identity string can be used as a valid public key. Thus there is no need for public key certificates and certificate management in IBE. The idea of IBE was introduced in (Shamir, 1984), but 17 years elapsed until the first practical IBE scheme based on pairing operations on discrete points on elliptic curves system was presented in (Boneh & Franklin, 2001).

Since then much research and development work has been devoted to IBE. A security flaw in the first practical IBE scheme has been removed (Galindo, 2005) and several variants of it have been proposed (Al-Riyami & Paterson, 2003; Boneh & Boyen, 2004; Gentry, 2003; Sahai & Waters, 2007). Also other practical IBE schemes have been proposed, for example a scheme based on quadratic residuosity (Cocks, 2001) and a Combined Public Key (CPK) scheme (Tang, Nan, & Chen, 2004). IBE based signature and key agreement schemes have been proposed (Barreto et al., 2002; Cha & Cheon, 2002; Chen, Cheng, & Smart, 2007; Chen & Kudla, 2003; Hess, 2002; Wang, 2005), standardization of IBE has started in IETF (Appenzeller, Martin, & Schertler, 2008; Boyen & Martin, 2007) and in IEEE ("IEEE," 2008), and IBE based security services have been integrated in commercial security products ("Voltage," 2008).

IBE Schemes

An IBE scheme for encryption and decryption consists of four algorithms (Boneh & Franklin, 2001):

- **Setup** – A private master key and public IBE parameters are generated by a Private Key Generation Authority (PKG)
- **Extract** – The private user key associated with an arbitrary public key string is generated with the master private key
- **Encrypt** with the public user key
- **Decrypt** with the associated private user key.

Secure private user key generation and distribution requires

- authentication of legitimate PKG users
- protected data communication between the PKG and authenticated users.

Setup and Extract

All algorithms depend on the chosen practical IBE scheme. For a pairing based IBE scheme it is in this paper assumed that there are n different public key generators (PKG), all with different public IBE parameters. The IBE parameters are chosen as follows:

- Each PKG_i has its own parameters $G_1^{(i)}$, $G_2^{(i)}$ and $e^{(i)}$, where $G_1^{(i)}$ is an additive group of order $q^{(i)}$, $G_2^{(i)}$ is a multiplicative group of order $q^{(i)}$, and $e^{(i)}$ is a non-degenerate bilinear pairing $G_1^{(i)} \times G_1^{(i)} -> G_2^{(i)}$. Bilinearity means that $e^{(i)}(a \cdot P, b \cdot P) = e^{(i)}(P,P)^{a \cdot b}$ for all $a,b \in Z_q(i)$ and for generators $P \in G_1^{(i)}$. Non-degeneracy means that $e^{(i)}(P,P) \neq 1$ for all generators P.
- Each PKG_i chooses a random generator $P^{(i)}$ of $G_1^{(i)}$ and cryptographic hash functions $H_1^{(i)}:\{0,1\}^* -> G_1^{(i)}$, $H_2^{(i)}:G_2^{(i)} -> \{0,1\}^k$, where k is the length of the partial session key. Partial session keys are used as the arguments in the hash functions.
- Each PKG_i chooses its secret master key $s^{(i)} \in Z^*_q(i)$ and computes its public key $P_{pub}^{(i)} = s^{(i)} \cdot P^{(i)}$.

Each PKG_i publishes all the domain parameters except the secret master key. A user with the identity ID under the PKG_i has a public key given by the formula $Q_{ID}^{(i)} = H_1^{(i)}(ID)$ and the PKG_i computes the private key as $S_{ID}^{(i)} = s^{(i)} \cdot Q_{ID}^{(i)}$. Furthermore, it is assumed that participants have agreed on a hash function H used in generating session keys.

Encrypt and Decrypt

If m is a message which is to be sent to identity A using PKG_1, the generator $P^{(1)}$ is a public parameter of PKG_1, and $P_{pub}^{(1)}$ is the public key of PKG_1, then m is encrypted by first choosing a

random integer r and then calculating the ciphertext (R, c) with $R = r \cdot P^{(1)}$, $S = e^{(1)}(P_{pub}{}^{(1)}, Q_A{}^{(1)})$, $c = m \text{ xor } H_2{}^{(1)}(r \cdot S)$. The ciphertext (R, c) is decrypted by first calculating the pairing $T=e^{(1)}(R,S_A{}^{(1)})$ and then $m = c \text{ xor } H_2{}^{(1)}(T)$. $S_A{}^{(1)}$ is the private key of receiver A.

IBE Based Digital Signatures

Many proposals for IBE based digital signatures have been made. The signature scheme proposed in (Hess, 2002) seems to be the best for the purposes in this paper, because it allows participants with different PKGs. This IBE signature scheme is based on pairing operations and uses the same setup and extract algorithms as the above described pairing based IBE scheme. The identity A uses PKG_1 and signs a message m. The identity B uses PKG_2 and verifies the signature. First A chooses an arbitrary point $P_A \epsilon G_1{}^{(1)}$. For each signature A picks a random number $t_A \in Z^*_q(1)$ and computes $r_A = e^{(1)}(P_A, P^{(1)})^{tA}$, $h_A = H_A(m||r_A)$, and $W_A = h_A \cdot S_A + t_A \cdot P_A$, where H_A is a hash function $H_A:\{0,1\}^* \times G_2{}^{(1)} -> Z^*_q(1)$. A's signature is now (W_A,h_A). B verifies the signature by computing $r_A=e^{(1)}(W_A,P^{(1)}) \cdot e^{(1)}(Q_A,-P_{pub}{}^{(1)})^{hA}$, and accepts the signature only if $h_A = H_A(m||r_A)$. Thus B needs the random generator $P^{(1)}$ of PKG_1, the public key $P_{pub}{}^{(1)}$ of PKG_1, the public key Q_A of A, the pairing operation $e^{(1)}$ of PKG_1, and the hash function H_A. A needs the corresponding data for B.

Private Key Delivery

First of all, every user must be registered beforehand by the PKG. A publicly available user registration database is maintained by the PKG and every time a user wants a private key the PKG checks the user credentials with the help of the database. The checks can be done with the help of elliptic curve cryptography, as Kumar, Shailaja, and Saxena (2006) have presented.

Next, the delivery of private keys depends on the connection between the PKG and a user. If a secure connection exists, then the private key can be submitted using this secure connection. If no secure connection exists, the blinding technique proposed in Kumar, Shailaja, and Saxena (2006) can be used.

In all the above methods the PKG knows the private keys of the users. This arrangement is called key escrow and it may be acceptable in some cases, but not in all. Key escrow can be avoided for example by using threshold techniques in distributed generation of private user keys with multiple PKGs (Boneh & Franklin, 2003).

In Girault (1991) three trust levels are defined for a trusted third party PKG, which generates private keys in IBE:

- *Level I*. The PKG knows or can easily compute the private keys of the users and can therefore impersonate any user at any time without being detected. The key escrow problem is thus unresolved on this trust level.
- *Level II*. The PKG does not know or cannot easily compute the private keys of users. However, the PKG can still impersonate a user by generating a false public key without being detected.
- *Level III*. The PKG does not know or cannot easily compute the private keys of the users. Moreover, there exists a proof method with which a false public key can be detected. Thus the PKG cannot impersonate a user by generating a false public key.

For role-based IBE security services in an organization trust level I is acceptable, if the organization acts as a PKG. Trust level I is even necessary for a role, which can be transferred from one person to another.

If users want to completely avoid the key escrow feature and achieve trust level III, it is possible to adopt a special private key issuing protocol as suggested in Kumar, Shailaja, and Saxena (2006). Then the PKG does not know or cannot easily compute the private keys of the users. Moreover, a proof method exists with which a false public key for a user can be detected. Thus the PKG cannot even impersonate a user by generating a false public key.

Issues in Applying IBE

If a protocol is based on public key encryption and digital signatures, then it may be modified in such a way that IBE encryption and IBE-based signatures are used instead of certificate-based encryption and signatures. The benefits of this approach are that it is no longer necessary to check certificates and certificate revocation lists.

There are also methods to agree directly on a common secret key with authentication at the same time. The simplest cases are those where the participants have the same PKG. One PKG is a realistic assumption, if communication takes place only between the members of the same organization. In a hierarchical IBE scheme the identities and the PKGs used by the identities are organized in a hierarchy tree (Gentry & Silverberg, 2002). A hierarchical IBE scheme is thus a generalization of IBE.

On the other hand, it is unrealistic to assume that a single trusted PKG or a single trusted PKG hierarchy is sufficient, if private keys must be issued to all entities in an entire nation or in the whole world. If there are many trusted authorities and many users using different PKGs or belonging to different PKG hierarchies, then the case, where users using different PKGs want to communicate with each other confidentially, must be considered. In this case each PKG has different public parameters and a different private master key.

The first IBE based key agreement protocols for multiple PKG environments, where every PKG has different public IBE parameters and different master keys, have recently been proposed in Kim, Lee, and Oh (2005).

References

Al-Riyami, S., & Paterson, K. (2003). Certificateless public key cryptography. *In Advances in Cryptology - Asiacrypt'03*, LNCS 2894, Springer-Verlag, pp. 452-473.

Appenzeller, G., Martin, L., & Schertler, M. (2008, October). *Identity-based encryption architecture and supporting data structures*. Retrieved December 14th, 2008, from http://www.ietf.org/internet-drafts/draft-ietf-smime-ibearch-09.txt

Barreto, P. S. L. M., Kim, H. Y., Lynn, B., & Scott, M. (2002). Efficient algorithms for pairing-based cryptosystems. In M. Yung (Ed.), *Advances in cryptology - Proceedings of CRYPTO 2002*, 354-368, Springer-Verlag, LNCS 2442.

Boneh, D., & Boyen, X. (2004). Efficient selective-ID secure identity based encryption without random oracles. In *Advances in Cryptology - Eurocrypt'04*, LNCS 3027, Springer-Verlag, pp. 223-238.

Boneh, D., & Franklin, M. (2001). *Identity-based encryption from the weil pairing*, In *Proceedings of Crypto 2001*, LNCS 2139, Springer-Verlag, pp. 213-29

Boneh, D., & Franklin, M. (2003). Identity-based encryption from weil paring. *SIAM J. of Computing, 32*(3), 586-615.

Boyen, X., & Martin, L. (2007). *Identity-based cryptography standard (IBCS) #1: Supersingular curve implementations of the BF and BB1 cryptosystems*. RFC 5091, IETF.

Cha, J. C., & Cheon, J. H. (2002). *An identity-based signature from gap Diffie-Hellman Groups*. Cryptology ePrint Archive. Retrieved December 14th, 2008, from http://eprint.iacr.org/2002/018

Chen, L., Cheng, Z., & Smart, N. (2007). Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4):213-241. Springer-Verlag, Berlin / Heidelberg.

Chen, L., & Kudla, C. (2003). Identity-based authentication key agreement protocols from pairings. *Proceedings of the 16th IEEE Computer Security Foundations Workshop - CSFW*, pp 219-233.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. *Eighth IMA International Conference on Cryptography and Coding*, Dec. 2001, Royal Agricultural College, Cirencester, UK.

Galindo, D. (2005). *Boneh-Franklin identity based encryption revisited*. Cryptology ePrint Archive, Report 2005/117. Retrieved December 14th, 2008, from http://eprint.iacr.org/2005/117

Gentry, C. (2003). Certificate-based encryption and the certificate revocation problem. In *Advances in Cryptology- Eurocrypt'03*, LNCS 547, Springer-Verlag, pp.272-293.

Gentry, C., & Silverberg, A. (2002). Hierarchical ID-based cryptography. In *Advances in Cryptology – ASIACRRYPT'02*, LNCS 2501, Springer-Verlag, pp. 548-566

Girault, M. (1991). Self-certified public keys. *EUROCRYPT 1991*, LNCS 547, Springer-Verlag, pp. 490-497

Hess, F. (2002). Efficient identity based signature scheme based on pairings. *SAC 2002*, LNCS 2595 pp. 310–324.

IEEE P1636.3™/D1. (2008, April). *Draft standard for identity-based public-key cryptography using pairings*. Retrieved December 14th, 2008, from http://grouper.ieee.org/groups/1363/IBC/material/P1363.3-D1-200805.pdf

Kim, S., Lee, H., & Oh, H. (2005). Enhanced ID-based authenticated key agreement protocols for a multiple independent PKG environment. *ICICS 2005*, LNCS 3783, pp. 323–335.

Kumar, K. P., Shailaja, G., & Saxena, A. (2006). *Secure and efficient threshold key issuing protocol for ID-based cryptosystems*. Cryptology ePrint Archive, Report 2006/245, Retrieved December 14th, 2008, from http://eprint.iacr.org/2006/245

Sahai, A., & Waters, B. (2007). *Fuzzy identity-based encryption*, E-print 2004/086. Retrieved March 11th, 2008, from http://eprint.iacr.org/2004/086.pdf

Shamir, S. (1984). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology Crypto'84*, LNCS 196, Springer Verlag, pp 47–53

Tang, W., Nan, X., & Chen, Z. (2004). Combined public key cryptosystem. In *Proceedings of International Conference on Software, Telecommunications and Computer Networks (SoftCOM'04)*. IEEE Comp-Soc., Los Alamitos

Voltage Security. (2008). Retrieved December 14th, 2008, from http://www.voltage.com

Wang, Y. (2005). *Efficient identity-based and authenticated key agreement protocol*. Cryptology ePrint Archive, Report 2005/108. Retrieved December 14th, 2008, from http://eprint.iacr.org/2005/108

Appendix B: List of Abbreviations

BU	Binding Update
CA	Certificate Authority
CBU	Certificate-based Binding Update Protocol
CGA	Cryptographically Generated Address
CPK	Combined Public Key
CoA	Care-of-Address
CRL	Certificate Revocation List
CN	Correspondent Node
CoT	Care-of Test

CoTi	CoT Init
DH	Diffie Hellman
DSA	Digital Signature Algorithm
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve DSA
ESP	Encapsulating Security Payload
HA	Home Agent
HoT	Home Test
HoTi	HoT Init
IBE	Identity-based Encryption
ICMPv6	Internet Control Message Protocol version 6
IKE	Internet Key Exchange
IKEv2	IKE version 2
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	IP Security
IPv6	IP version 6
KMC	Key Management Center
MAC	Message Authentication Code
MIPv6	Mobile IP version 6
MN	Mobile Node
NAI	Network Access Identifier
PKF	Public Key Factor
PKG	Public Key Generator
PKI	Public Key Infrastructure
RO	Route Optimization
RR	Return Routability
RSA	Rivest, Shamir, & Adleman
SA	Security Association
SKF	Secret Key Factor
WLAN	Wireless Local Area Network

Biographies

Martin Ehmke received his Master's degree in computer science from the University of Helsinki, Finland in 2008. He is currently working as a software developer.

Harri Forsgren received his Master of Science degree and is presently doing his PhD studies in computer science at the University of Helsinki, Finland. His research interests include cryptography, network security and formal methods.

Kaj J. Grahn received his doctoral degree at Helsinki University of Technology and is presently senior lecturer in telecommunications at Arcada University of Applied Sciences, Helsinki, Finland. His current research interests include security of wireless and mobile networks.

Jonny Karlsson received his Bachelor of Science degree in Information Technology and is since May 2002 research assistant and teacher at Arcada Unviersity of Applied Sciences, Helsinki, Finland. In January 2009 he started PhD studies in security of future networks at the Open University, Milton Keynes, UK. His current research interests include security of wireless and mobile networks.

Timo Karvi has studied first mathematics receiving a licentiate degree in 1993. After this, he changed to computer science and finished the doctoral degree in 2000. He is currently a lecturer in the computer science department of the Helsinki University. His research area is the verification of distributed systems, but he has also worked on computer security

Göran Pulkkis received in 1983 his doctoral degree at Helsinki University of Technology and is presently senior lecturer and researcher in computer science and engineering at Arcada University of Applied Sciences, Helsinki, Finland. His current research interests include network security and applied cryptography.