A PUBLIC-KEY BASED SECURE MOBILE IP[1]

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, and Isidro Castineyra

Abstract *The need for scalable key management support for Mobile IP – especially, the route-optimized Mobile IP – is well known. In this paper, we present the design and the first implementation of a public key management system that can be used with IETF Mobile IP. The system, called the Mobile IP Security (MoIPS) system, was built upon a DNS based X.509 Public Key Infrastructure with innovation in certificate and CRL dispatch as well as light-weight key generation. The system can be used to supply key parameters for authenticating Mobile IPv.4 location management messages and to establish IPSec tunnels for Mobile IP redirected packets. It can also be used to augment emerging firewall traversal techniques for Mobile IP. A FreeBSD UNIX prototype with core functionality was completed at the time this paper was published.*

1. INTRODUCTION

1.1 Review of Mobile IP Protocols

Mobile IP or IP mobility support [rfc2002] (abbr. MIP) is a protocol for passing IP datagrams between a *Mobile Node (MN)* and its *Corresponding Nodes (CNs)* as the Mobile Node changes it attachment point on the Internet. The protocol employs network layer agents to capture IP datagrams that are sent to the Mobile Node's *permanent IP address* in its *home subnet* and redirect these datagrams using IP-IP encapsulation [rfc2003] to a *Care-of IP Address (COA)* assigned temporarily to the Mobile Node while it is visiting a *foreign subnet.* The agents in the home subnet are known as the *Home Agent (HAs)* and the ones in the foreign subnet are known as the *Foreign Agents (FAs).* Together, these *mobility agents* track the movement of Mobile Nodes by passing *registration messages* among themselves and the Mobile Nodes. Based on the registration process, the Home Agents keep track of the locations of Mobile Nodes under their administration, and serve as the entry points to the *IP-IP packet redirection tunnels*. The Foreign Agents, however, may or may not be the exit points of these tunnels depending on the choice of Care-of Addresses: if the Care-of Address is the IP address of a network interface on a Foreign Agent then the Foreign Agent is a tunnel end-point and the Care-of Address is called *Foreign Agent-Care-of Address*; however, if the Care-of Address is a address assigned temporarily to a Mobile Node by DHCP or PPP then the Care-of Address is called *co-located Care-of Address* and the Foreign Agent serves only as a last-hop router and a Mobile IP administrator. In order to pass IP datagrams from the Mobile Nodes through the firewalls that surround a foreign subnet, *reverse tunnels* may be established from Care-of Address to the Home Agent [mip-tunnel-reverse] using IP-IP encapsulation. These tunnels are also managed by the Foreign Agents and the Home Agents via the registration process.

A more sophisticated version of Mobile IP, called *route-optimized Mobile IP* [mip-optim], was also proposed to the IETF Mobile IP working group. In that protocol, the Care-of-Address of a Mobile Node can also be disclosed to the Corresponding Nodes and a certain number of Foreign Agents, which have served the Mobile Node, using the *location binding update messages*. As a result, the Corresponding Nodes may tunnel their IP datagrams directly to the Mobile Node's Care-of Address, and the previous Foreign Agents may also *forward* IP datagrams destined to the Mobile Node to the current Care-of Address of the Mobile Node. These additional tunnels can help to shorten the transit time of redirected packets and reduce the number of packets dropped due to delivery failure. Consequently, they will improve the performance of Mobile IP, especially when it is used with a connection-oriented protocol such as TCP.

Figure 2-1 in the next page shows the message flow of both basic and route-optimized Mobile IP.

1.2 Mobile IP Security Requirements

While Mobile IP promises un-interrupted IP connectivity when the Mobile Nodes roam around in the Internet, it also increases the risk of causing remote redirection of internet traffic [bellovin-89] by simply introducing bogus registration and binding update messages. In addition, the presence of Mobile Nodes in their visiting networks may cause security concerns to both their home and foreign networks. Hence, the two goals of Mobile IP security protection are (1) to allow a Mobile Node to enjoy similar internet connectivity and safety when it visits a foreign network as it is in its home network and (2) to protect both the home and the foreign networks from passive and active attacks while the Mobile Node roams in the Internet.

Throughout the development of Mobile IP, the following security services have been considered useful for protecting a mobile internet:

- *data integrity*, *data origin authentication* and *anti-replay* protection of Mobile IP registration and location update messages,
- *access control* of the Mobile Nodes when they use resources on the visiting networks,
- *data integrity*, *data origin authentication* and *data confidentiality* protection of IP packet redirecting tunnels,
- *location privacy* of the Mobile Nodes and
- *anonymity* of the Mobile Nodes.

Among these services, the *first three* are essential to the secure operation of Mobile IP. The *Mobile IP Security (MoIPS) architecture* was developed to provide these services.

[1] This work reported in this paper was sponsored by Defense Advanced Research Project Agency (DARPA) and Air Force Material Command (AFMC) of the Department of Defense under contract number F19628-95-C-0150.

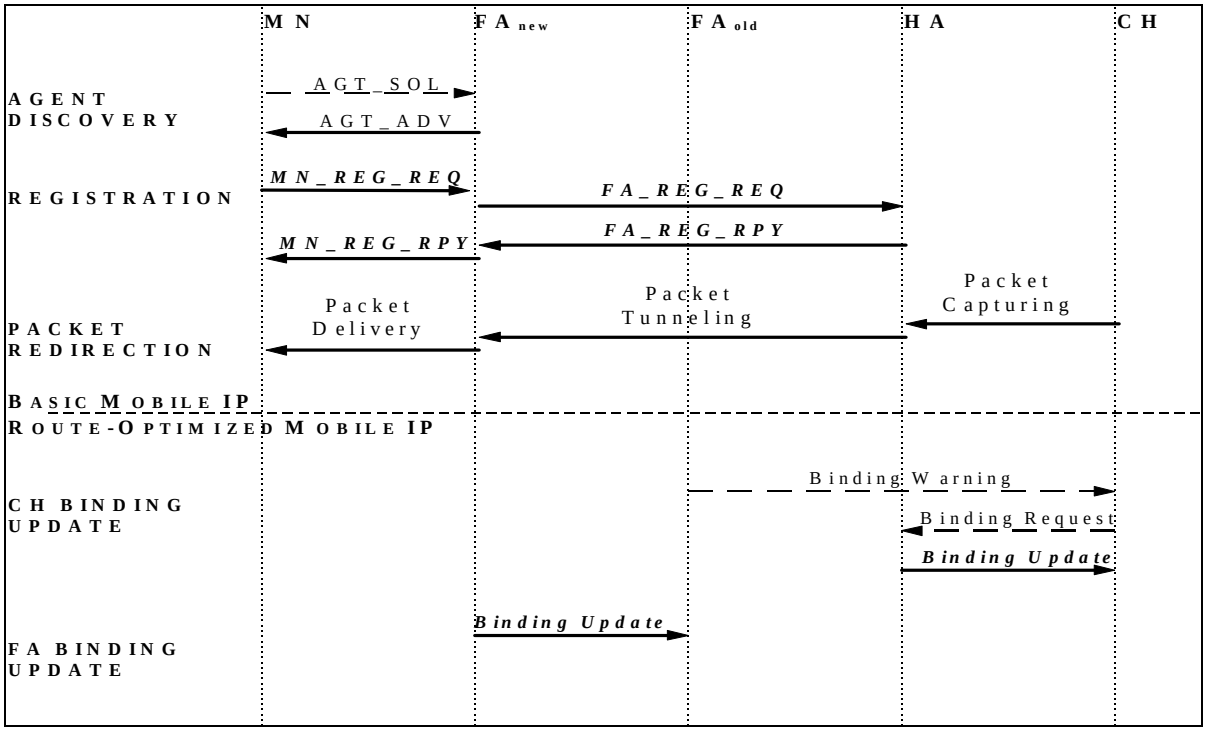

Figure 2-1. Message flow in Mobile IP protocols

1.3 Organization of the Paper

In the remaining *six* sections of this paper, we will discuss the design and implementation of MoIPS system. Section 2 offers a system overview which explains our approach to provide the three security services [Sect.2.1] and describes the public-key based MoIPS architecture. Sections 3–5 covers the three components of the system: the DNS-based X.509 public key infrastructure (PKI) in Sect.3, a lightweight key management scheme for Mobile IP control message authentication in Sect.4, and the IPSec protection of Mobile IP packet redirecting tunnels in Sect.5. The implementation of first MoIPS prototype will be briefly described in Section 6 before the conclusions are given in Section 7.

2. MoIPS System Overview

2.1 Security Services

As mentioned, the MoIPS system was developed to support three security services that are essential to the safe operation of Mobile IP. These services are (1) authentication of Mobile IP control messages for location update, (2) access control of Mobile Nodes to resources in the foreign networks, and (3) secure tunneling of redirected IP datagrams. In this section, we will examine the security needs of Mobile IP and explain our approach to address these needs.

2.1.1 Authentication of Location Updates

Among these Mobile IP messages shown in Figure 2-1, the *registration messages* in Basic Mobile IP and the *location binding update messages* in the Route-Optimized Mobile IP (all displayed in bold italics) carry the *location bindings* of mobile nodes, i.e. the associations between the permanent address and the current care-of-address of Mobile Nodes. By altering the location binding in these control messages or creating bogus messages or replaying pre-recorded messages, an adversary could redirect IP traffic for one node to another node.

In order to frustrate the remote traffic redirection attack mentioned above, registration and binding update messages must be protected with data integrity, origin authentication and anti-replay services. Each of these messages hence includes a 64-bit *identification* tag for detecting replays and one or more *authentication extensions* to provide message integrity and strong authentication using a hashed message authentication code (HMAC) [hmac-md5][hmac-sha1]. Although use of HMAC and an anti-replay tag addresses the security services cited above, the current Mobile IP lacks a *scaleable key management scheme* for dispatching cryptographic keys needed to support these services. In order to protect the registration messages, keys must be shared *at least* among Mobile Nodes and their Home Agents. In order to protect the binding update messages in the route-optimized Mobile IP, keys must be dispatched among MN-FA, FA-HA and MN-CN pairs.

2.1.2 Access Control of Mobile Nodes

For the purposes of network protection, accounting and resource management, it is desirable that the Foreign Agents (in cooperation with the Home Agents) can verify the identity of an Mobile Node before allowing it to complete its registration and establish an attachment point on the visiting subnets.

The access control procedure should be conducted by (1) verifying the *identity* of Mobile Node and (2) checking the *current status* of Mobile Node with a relevant authority, e.g. the Home Agent associated with the Mobile Node. This two-step procedure can ensure both the authenticity and the status of the

Mobile Node. In MoIPS, the identity and network affiliation of both end nodes (Mobile Nodes and Corresponding Nodes) and mobility agents (Foreign Agents and Home Agents) are enclosed in the public key certificates issued to these network entities. By exchanging these certificates and performing operations that demonstrate possession of the private keys corresponding to the public keys in the certificates, the end hosts can identify themselves not only to the mobility agents but also to one another.

The checking of Mobile Node status, on the other hand, can be conducted implicitly by exchanging *authenticated* registration requests and replies between Foreign Agents and Home Agents. By forwarding a registration request to a Home Agent, an Foreign Agent indicates that the Mobile Node has successfully passed its scrutiny. By returning a registration reply, the Home Agent then informs the Foreign Agent of its approval or rejection of the registration based on factors including Foreign Agent's identity and affiliation, Mobile Node's status, and Home Agent's own mobility control policy.

2.1.3 Secure Tunneling of Redirected IP Packets

The traffic to and from an Mobile Node while it is away from its home network generally will traverse the public Internet, as well as the visited foreign networks. The latter may entail the use of via wireless or other insecure communication media. Using these communication paths greatly increases the risks of passive intrusions such as eavesdropping and active attacks such as packet alteration, insertion or deletion. Consequently, both the foreign networks and the home network of the Mobile Node may require data integrity, data origin authentication and possibly confidentiality for the redirected packets.

In order for the home network to have the same level of trust and hence provide the same amount of connectivity to an Mobile Node when it roams among foreign networks as if it is residing at home, the home network will require secure traffic tunneling to and from the Mobile Node (or a trusted agent such as the Foreign Agent connected to the Mobile Node). Similarly, in order for the foreign network to pass traffic for the Mobile Node, the foreign network will require the traffic to be redirected by an authenticated and trusted entity in Mobile Node's home network such as the Home Agent that manages the Mobile Node. These secure tunnels can be implemented by using *IP security protocols (IPSec)* in *tunneling mode.* The protocols will transform each original IP datagram using authentication and encryption mechanisms negotiated by the communicating parties and then encapsulate the datagram in an IPSec header and an external IP header that specifies the end points of the IPSec tunnel. (Such services can be provided by using the Encapsulating Security Payload protocol, one of the two IPsec protocols defined for traffic security.)

The MoIPS architecture provides the requisite protection by incorporating an IPSec implementation and a key management module into the system. The two modules establish IPSec tunnels according to the instructions received from the Mobile IP module and obtain the public keys needed for establishing these services from a public key infrastructure incorporated into the architecture. IPsec makes use of the Internet Security Association and Key Management Protocol (ISAKMP) [isakmp] for automated key management.

2.2 Public-Key Based Architecture

The three security requirements discussed in the previous section demand the following three kinds of security support:

1. *a scalable key management infrastructure* capable of generating or dispatching *long-term key parameters* among any pairs (or even sets) of nodes attached to the global Internet — without this infrastructure, Route-Optimized Mobile IP cannot send authenticated binding updates to arbitrary Corresponding Nodes and secure tunnels between MN-CN and FA-HA will be difficult to establish;
2. *a rapid short-term key generation algorithm* for supplying the short-term keys needed for authenticating the Mobile IP registration and binding update messages — because Mobile Nodes can obtain network connectivity only after successfully completing registration and binding updates, it is essential to have a key generation algorithm that can supply fast changing keys with *no* additional message exchange;
3. *cooperation of Mobile IP and IPSec protocols* to enable Mobile Nodes, Foreign Agents and Home Agents to select the packet redirection tunnels they intend for IPSec protection and ISAKMP to negotiate the necessary security associations with minimal disruption of Mobile Node hand-offs.

In MoIPS architecture, we decided to use public key technology to meet the key management requirements. More specifically, we chose to develop a *public key infrastructure (PKI)* for managing X.509 v.3 *public key certificates* and the v.2 *certificate revocation lists (CRLs)* [pkix-ipki-1] that are issued to *Internet nodes* (instead of human subjects). We also chose to use the Internet *domain name system (DNS)* [rfc1034] as the primary certificate repository, supplemented occasionally with direct fetches of certificates and pushes of CRLs.

The main consideration motivating the use of PKI technology was *scalability*: in order to support global internet mobility, we require a technology that can establish shared secrets in real time among a large population of nodes spread among many network domains all over the world. A DNS-based PKI has clear advantage over a distributed system of key distribution centers (KDCs), such as a multi-realm Kerberos system. Using the DNS not only solves the potentially complicated *server discovery problem,* but use of certified long-term public keys also eliminates the need for real-time key dispatches by KDCs. Since public key certificates can be issued off-line, a (comparably-sized) certification authority (CA) can issue and manage a much larger number of certificates than the number of clients that can be served by a KDC.

Figure 2-2 illustrates the conceptual structure of MoIPS. Both Mobile IP (basic or route-optimized) and IPSec modules make use of a key management module and a cryptographic engine. The key management module, possibly running different

Error! Not a valid link.

Figure 2-2. MoIPS system block diagram

protocols for Mobile IP and IPSec, generates the short-term keys needed by the security services while the crypto-engine, implemented by software libraries or hardware tokens, performs the actual cryptographic (e.g., encryption and authentication) processing. Keys and other security parameters are kept in a protected database and passed only to the crypto-engine. Users of security service such as Mobile IP or IPSec make use of *security parameter indices (SPIs)* to refer to the different security settings. The key management module derives the short-term keys from the long-term public keys it obtains from the X.509 PKI. In order to obtain certified public keys, an X.509 certificate verifier was developed which can fetch certificates and CRLs via regular DNS lookup and / or receive them through direct exchanges using the *certificate discovery protocol (CDP)* [ipsec-cdp]. It then verifies the public-key signatures on these electronic documents following the trust hierarchy of the certification authorities. The verifier also maintains a cache of received and verified certificates and CRLs, to minimize number of fetches and signature verification operations required.

MoIPS supports multiple hierarchies of certification authorities (CAs), at the top level by cross-certificates. However, the MoIPS prototype does *not* include the implementation of CAs; instead, it uses the Certificate Management System developed by BBN and sold as a commercial product. The reason for this implementation decision was that future users of MoIPS may prefer to use CAs based on other commercial CA products or make use of commercial CA services.

Where feasible MoIPS makes use of emerging standard cryptographic application programming interfaces (CAPIs) to connect its different modules. For example, it uses the RSA CryptoKi CAPI as the interface between security service users and the crypto-engine; this interface enables MoIPS to use both the RSAREF crypto-library and the Fortezza crypto-token to perform the cryptographic operations. MoIPS also uses the PF_Key CAPI to support short-term key and security association management. PF_Key is the standard key management interface between IPSec and ISAKMP in the UNIX environment. However, due to the absence of a standard certificate management API, MoIPS developed its own simple interface (shown as Cert_API in Figure 2-2) to connect the certificate verifier with the key management module.

3. X.509 PUBLIC KEY INFRASTRUCTURE (PKI)

In this section, we will examine the core of the Mobile IP security architecture, i.e. a public key infrastructure that manages X.509 v.3 certificates and v.2 certificate revocation lists (CRLs) of the end nodes, and the mobility agents. The certificates and CRLs are distributed primarily as a new type of resource records X509CCRL in the domain name system. In specific cases [Section 3.8], they are also exchanged using certificate discovery protocol.

3.1 Reasons for Developing a DNS-Based PKI

We made a conscious decision in MoIPS to develop a X.509 PKI for Internet nodes and use DNS as the primary certificate dispatch mechanism. Several alternatives for public key management existed when we launched our project; among them, most promising was the *secure DNS (DNSSec)* activity [dns-secext] in the IETF. In the following, we give the tradeoff of advantages and cost of developing such an infrastructure.

Advantages of using X.509 v.3 Certificates Several important advantages of developing the PKI come from the use of X.509 v.3 certificates instead of bare public keys. The X.509 v.3 certificate profile includes many *extension fields* for carrying information other than key parameters. In particular, the following fields enable us to add valuable features to the PKI.

1. IssuerAltName [required, critical] enable the establishment of a CA hierarchy independent from the DNS zone structure. Whereas, the fields BasicConstraint and NameConstraint [required, critical] permit better control of CA authority in issuing certificates.
2. CertPolicy [optional, critical] allows the inclusion of policy specific information in the certificates in order to enforce Mobile IP access control policies.
3. KeyUsage [required, critical] specifies the intended use of the key parameters. The key identifiers, CAKeyID and SubjKeyID, [optional, non-critical] enable the certificate verifiers to distinguish the signing keys when multiple of them are in use during *key rollovers*. These fields help to enforce the correct use of keys.
4. By assigning status, required / optional and critical / non-critical, to each extension field, X.509 PKI enables detail verification policies to be specified for different kinds of public key certificates – e.g. the certificates issued for Mobile IP message authentication may have a profile different from those issued for IPSec protection.

All in all, X.509 v.3 certificates allows more information to be carried in the certificates and more ways to use this information to support security services.

Advantages of using Domain Name System The ubiquitous use of DNS over the Internet motivated both DNSSec and MoIPS PKI to use it as the certificate dispatch system. The choice is most appropriate for both DNSSec and MoIPS since they manage public keys assigned to network entities instead of human subjects. Moreover, these subjects are identified by domain names and/or IP address – both are information carried by DNS – and the communications among network entities are often established with DNS lookups; hence, DNS certificate fetches can easily be piggybacked onto these regular exchanges.

Costs of using a DNS-based X.509 PKI The use of any public key system entails a certain amount of overhead. In comparing X.509 to DNSSec, it is worth noting that X.509 certificates are larger than the KEY and the SIG records stored by DNSSec. However, to store the additional information carried in the X.509 extension fields used in MoIPS, additional DNS record types would have to be created, diminishing the apparent space advantage of DNSSec. In either case, retrieval of certificates (or multiple types of DNSSec records) will usually require TCP instead of UDP communication with DNS servers. The use of CRLs and certificates provides added flexibility for MoIPS, in contrast to the daily update of DNS records that DNSSec substitutes for certificate revocation. Given this difference in approach to revocation management, use of CRLs may result in fewer DNS fetches overall.

3.2 Certificate Types

Table 3-2. Profile of MoIPS CRLs[3]

Fields	Status	Values and Remarks
Version	*required*	= 2
SerialNumber	*required*	unique number per CA
Signature	*required*	= RSA (default)
Basic		
Validity	*required*	certificate valid period
SubjectName	*required*	= 0x00
SubjectPublicKeyInfo	*required*	DH public value (1024 bit) for end nodes RSA public key (1024 bit) for CAs
AuthorityKeyID	*optional / non-critical*	SHA-1 hash of CA public key
SubjectKeyID	*optional / non-critical (CA only)*	SHA-1 hash of subject public key
Revoked Certificates		Sequence of revoked certificates each with CRL Entry Extensions
UserCertificate	*required*	serial number of revoked certificate
RevocationDate	*required*	date and time of revocation (YYMMDDHHMMZ : GMT)
CRL Extensions		
Authority Key Identifier	*optional / non-critical*	SHA-1 hash of CA public key
Issuer Alt Name	*required / critical*	canonical domain name of CA
CRL Number	*optional / non-critical*	CRL serial number
Issue Distribution Point	*required / critical*	pointer to CRL distribution point in DNS

The X.509 PKI used with MoIPS manages *two* types of public key certificates.

Certificates for Mobile IP Control Message Authentication (MoIPS Certificates) These certificates bind the subject names of Mobile Nodes, Corresponding Nodes, Home Agents and Foreign Agents to Diffie-Helman (DH) public keys. The certificates also may carry optional information of host/agent types and their network affiliations. The DH public values are used to produce session keys necessary for authenticating Mobile IP registrations and location updates. The host/agent information may be used to exercise access control. The certificates are issued by the CAs that enforce Mobile IP security policy and should not be used by any application other than Mobile IP.

Certificates for IP Security Services (IPSec Certificates) These are public key certificates issued to support general *IP security services*, especially data origin authentication and confidentiality. These certificates may carry various public key parameters for different IPSec key management protocols including ISAKMP and SKIP. They are the same as other *IPSec certificates* issued to Internet nodes that support IP security services, and are certified by CAs that enforce IP security policy.

3.3 Certificate Entitlement and Policies

Policies of MoIPS Certificates All mobile IP aware hosts and mobility agents must have MoIPS certificates in order to authenticate their Mobile IP control messages. However, the certificates for Mobile Nodes and Corresponding Nodes may be issued under different policies than those for Foreign Agents and Home Agents. More specifically, *host certificates* must indicate the host type, *mobile* / *stationary*, and may optionally indicate the network domains (e.g. DNS zones) with which the hosts are affiliated. Under no circumstance should a host be marked as *both* mobile and stationary. On the other hand, *agent certificates* must indicate the agent type, *foreign* / *home*, and may indicate both the network domains the agents are affiliated with and the subnets that the agents are serving (e.g. by giving the subnet prefixes). A mobility agent can be marked as *both* a Foreign Agent and a Home Agent if the agent can provide both services.

Policies of IPSec Certificates All nodes intend to conduct secure IP communication should possess valid IPSec certificates. Although it is possible to establish IPSec tunnels using symmetric keys dispatched via Mobile IP control messages, the practice is not recommended for it bypasses proper setup of security associations. Also, because Mobile IP control message authentication and IP security protection are two *orthogonal* services, MoIPS Certificates should not be used to setup secure IP communication.

3.4 Subject Names

Two candidates of subject names, the *IP address* and the

[2] The *shaded rows* contain the extension fields of MoIPS certificates, and the *inverse colored rows* mark the fields not used in the certificates.

[3] The *shaded rows* contain the extension fields of MoIPS CRLs, and the *inverse colored rows* mark the fields not used in the CRLs.

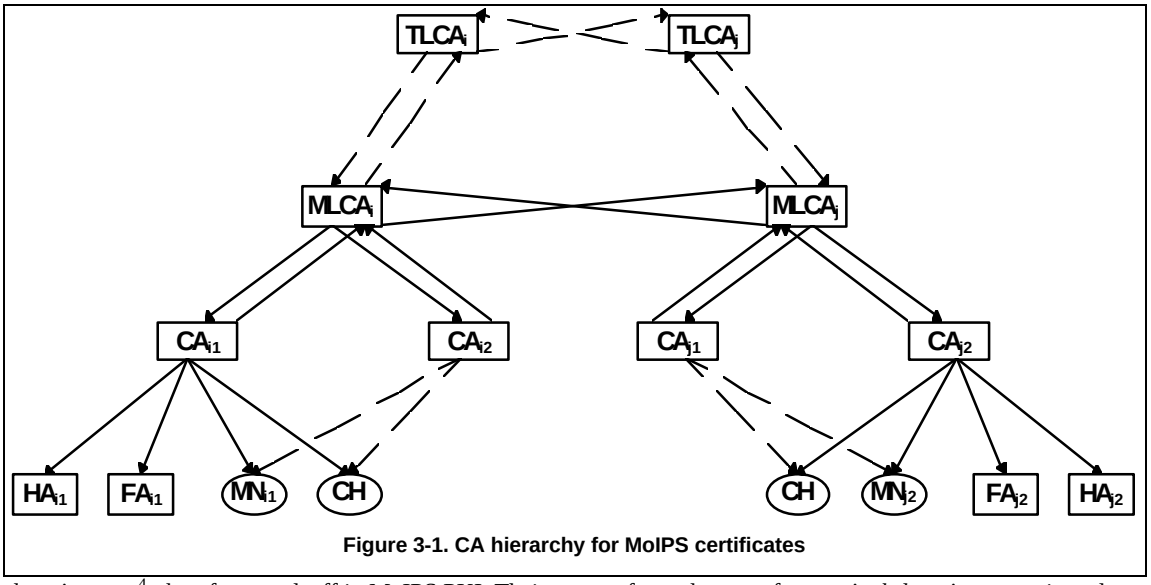

Figure 3-1. CA hierarchy for MoIPS certificates

canonical domain name[4], beg for a tradeoff in MoIPS PKI. Their preferences differ slightly depending whether the subject is an end node or a certification authority.

For Mobile Nodes, Corresponding Nodes, Foreign Agents and Home Agents, the choice is obvious: the *IP addresses* of Internet nodes / interfaces *must* be the subject name in the certificate because mobile IP protocol uses IP addresses as identifiers of Mobile IP entities. The use of IP addresses also has two other *advantages*: (1) it allows MoIPS certificates to be issued to interfaces rather than nodes on the Internet. This allows a multi-home node to have a certificate issued to each of its network interfaces when it functions as a Foreign Agent or a Home Agent. The configuration is particularly useful when the agent functions as a firewall or serves multiple subnets; (2) it simplifies the verification of NameConstraint: the lowest level CAs may own blocks of IP addresses and issue MoIPS certificates only to the mobility entities with IP addresses falling within the address ranges.

On the other hand, the use of IP addresses has two disadvantages: (1) the addresses may change over time and (2) they do not refer directly to distinct entries in the DNS. Consequently, the certificates must be revoked and re-issued whenever there is a change of IP address assigned to a node. Also, multiple certificates may be stored in one DNS entry and a *reverse domain name look-up* may be needed before searching the DNS directory for the certificates.

For CAs, *domain names* are the preferred subject names because the use of domain names will eliminate the *reverse DNS lookups* before fetching for a CA certificate, though it will introduce a heterogeneous naming scheme to the PKI. Owing to the fact that an Internet node may have multiple domain names, we also enforce the use of *canonical domain names* in order to specify a unique distribution point for every CA certificate. One can employ multiple SubjAltName fields in a certificate to store both the IP address and domain name of the entity in the same certificate.

3.5 MoIPS Certificate and CRL Profiles

MoIPS certificates conform to the profile of standard X.509 v.3 as specified in [pkix-ipki-1]. The IssuerUniqueID, SubjUniqueID, PublicKeyUsagePeriod and SubjDirAttributes fields are omitted, as suggested. Table 3-1 contains a summary of fields used in MoIPS certificates. The MoIPS CRLs also follow the standard format specified in [pkix-ipki-1]. Table 3-2 contains a summary of fields used in MoIPS CRLs.

3.6 Certificate Hierarchy

The MoIPS certification hierarchy takes the form of a multiple-tree structure [Figure 3-1]. Each tree starts with a top-level certification authority (TLCA) at the root, followed by arbitrary layers of middle-level CAs and ends with mobility aware hosts and agents at its leaves.

Each (lower-level) CA owns one or more contiguous blocks of IP addresses, and is responsible for issuing MoIPS certificates to the mobility aware hosts and agents with IP addresses falling within the range. In a fully developed hierarchy, different CAs may be dedicated to issue certificates only to the end nodes (Mobile Nodes and Corresponding Nodes) or the agents (Foreign Agents and Home Agents) under different security policies and manage different CRLs (shown in Figure 3-1 with dashed arrows).

CAs at adjacent levels are linked by *cross certificates* and so are the CAs at the roots of the trees. These cross certificates help to form the validation paths of the leave certificate. In order to manage the network of cross certification and control the number of certificates stored in each DNS entry, the structure must limit the number of trees as well as the number of descendants at every level of the hierarchy.

During initialization, every mobility aware entity (host or agent)

[4] A *canonical domain name* is the unique domain name that identifies the DNS entry of the Internet node. In order to support reverse DNS look-up — the conversion from IP addresses to domain names, DNS system requires a unique canonical name for every entry; additional names can be given to an entry as alias names.

is loaded with a *self-signed certificate*[5] of its CA via a safe channel supporting *peer-entity authentication*. When a mobility aware entity wants to obtain the public key of another entity, it shall obtain all the certificates along the verification path between its CA and the target entity. Using the public key contained in the self-signed certificate of its CA, the source entity can then verify all the certificates along the path and obtain the public key of the target entity.

3.7 DNS Based Certificate Dispatch

The X.509 certificate of a CA is stored as a new type of resource record, X509CCRL, in the DNS entry of the CA. Hence, the canonical domain name of the CA, which is also the subject name in its certificate, refers unambiguously to the certificate distribution point.

The X.509 certificates of mobility aware entities (both end hosts and mobility agents) also are stored as X509CCRL type resource records in their DNS entries. Since IP addresses are used as the subject names, a reverse DNS look-up must be used to get the entity's canonical domain name and find the certificate distribution point. If the entity has multiple IP addresses then its DNS entry may contain multiple certificate resource records, each maintains a X.509 certificate assigned to one of its IP addresses. A resolving mechanism must be built so that the module can retrieve the certificate correspond to a specific IP address.

The distribution points of CRLs can be stored in the DNS entries specifically appointed by the CAs. X.509 v3 certificates allow their CRLs to be stored in fragments at distribution points explicitly specified by the extension field CrlDistributionPoint. The DNS entries of network administration centers and/or DNS servers are ideal sites for maintaining the MoIPS CRLs. The multi-site distribution will be an ideal choice for a fully developed DNS-based PKI; however, for simplicity sake, the CRLs are kept in the DNS entries of the issuing CAs in the MoIPS prototype.

There are soft limits on the sizes and offsets of resource records in a DNS entry. To honor those limits, X509CCRL resource records should be stored at the end of a DNS entry without using pointer reference. The resource records may be *compressed* if the total size of a DNS entry exceeds 64K bytes or individual resource records can be shortened to be less than 500 bytes – the maximum length of an UDP fetch. Otherwise, TCP sessions must be established for fetches of X509CCRL.

3.8 Direct Certificate Exchanges

The X.509 certificates and CRLs also can be sent to the requesting entity using the IPSec certificate exchange protocol (CDP) [ipsec-cdp], since the communicating parties are able to establish real-time connections. However, the DNS system is favored because it provides a global distribution and caching mechanism.

Direct exchange of certificates and CRLs may be used to cope with particular incidents of *certificate or key revocation*. In order to shorten the wait time between the act of revocation and the publication of the next CRL, MoIPS PKI may mandate an immediate dispatch of a CRL and the new certificates by concerning Home Agents and Foreign Agents to all the Mobile Nodes with which they maintain active connections.

4. PROTECTION OF MOBILE IP CONTROL MESSAGES

The data origin authentication and anti-replay protection of Mobile IP control messages are performed in *four* steps:

1. *generation of replay protection identification numbers,*
2. *generation of short-term keys for data origin authentication,*
3. *production of message authentication tags based on short-term keys and message text.*
4. *verification of message authentication tags based on short-term keys and message text.*

Note that the generation of short-term keys is hidden behind the production and the verification of message authentication tags. These keys should not and need not be revealed to Mobile IP.

4.1 Zero-Message Key Generation

As stated in Section 2.2, the authentication service requires a rapid key generation algorithm to supply the necessary short-term keys. In this section, we describe such an algorithm for deriving short-term keys from the Diffie-Helman (DH) secrets shared between pairs of communicating parties. The algorithm requires Mobile IP to supply a transient value, and the *replay protection identification number* embedded in Mobile IP control messages is chosen to be the transient value.

4.1.1 Design Goals

The key generation algorithm was designed to satisfy the following *five* requirements:

1. *Usable by all Mobile IP nodes and agents* — unlike manual key installation, the algorithm can be used by Mobile Nodes, Corresponding Nodes, Home Agents and Foreign Agents to generate symmetric keys for message authentication *without scalability problems*.
2. *No modification of Mobile IP message and extension formats* — besides certificate fetches, the algorithm does *not* require any additional communication between the parties nor any modification to the format of Mobile IP control messages and message extensions.
3. *No use of encryption operations* — the algorithm avoids use of encryption operations, to minimize export control complexity.
4. *Strong protection of master keys* — the algorithm aims at making the discovery of the Diffie-Helman long-term shared secret, based on the knowledge of keys generated and replay protection numbers, as close as possible to random guesses.
5. *Low correlation with other Diffie-Helman based key*

[5] A *self-signed certificate* of a CA is a X.509 certificate signed by the CA using its own private key to binds its subject name with public key parameters and other relevant attributes. The certificate serves well as an end point of a verification path because (1) it does not refer to other signing authority and (2) it provides integrity protection (but not authentication) of the name-key binding.

generation — the algorithm was designed to be different from existing Diffie-Helman based key generation algorithms so that there is *no* significant or consistent correlation between the keys generated by these algorithms.

4.1.2 Computation Algorithm

For two communicating parties that share a DH secret, the algorithm generates short-term keys by feeding a folded version of the DH secret as the "key" and a finite repetition of the replay protection identification number as the "message" to an HMAC function. The output of the HMAC function is then used to authenticate a Mobile IP control message (which contains the replay protection number) by feeding it and the control message again into a HMAC function.

The algorithm can be divided into three steps: computation of long-term master key, preparation of transient values, and production of short-term keys.

Master Keys The algorithm begins by computing the symmetric secret S_{ij} based on the Diffie-Helman private values *i*, *j* and public values $g^i \bmod p$, $g^j \bmod p$ possessed by the two communicating parties:

$$S_{ij} = \left(g^i\right)^j \bmod p = \left(g^j\right)^i \bmod p .$$

The long symmetric secret S_{ij} is then "folded" by the following operation to produce the *long-term master key* K_{ij}: :

$$K_{ij} = \bigoplus_{}^{M} \left[S_{ij}\right]_{Lk} \qquad \text{with} \quad M = \left\lceil \frac{L\left(S_{ij}\right)}{Lk} \right\rceil .$$

The "folding" begins with the breaking down of S_{ij} (starting from its lowest order bits) into fragments of length *Lk* equal to that of the short-term keys to be generated. In case the last fragment is shorter than *Lk* then a fixed pattern of $55_{16} = 01010101_2$ will be padded repeatedly beyond the highest bit. After the fragmentation, a series of *exclusive OR operations* are performed iteratively to the fragments in ascending order starting with the one with lowest order bits. The long-term master key K_{ij} is yielded as the final result of the operations.

Transient Values A 512-bit transient value T_n is prepared by *eight* repeated concatenation of the 64-bit *replay protection identification number* R_n embedded in the Mobile IP control messages:

$$T_n = \left|^{8} R_n \right. .$$

The purpose of the repeated concatenation is to increase the length as well as the number of changing bits in the transient value to be fed into the HMAC function. This step is particularly important if R_n is derived from a timestamp with many slow changing bits. Nevertheless, the concatenation does *not* increase the total number of transient values and hence the total number of short-term keys which can be generated. If the replay protection numbers are 64 bits in length then a total of 2^{64} different keys can be generated for each pair of communicating parties that share a DH symmetric secret.

$$K_{auth} = HMAC\left(K_{ij}, T_n\right) = MD5\left(K_{ij} \oplus P_1 \mid MD5\left(K_{ij} \oplus P_2 \mid \right.\right.$$

Short-Term Keys Once the long-term master key K_{ij} and the transient value T_n are prepared, they are fed into the HMAC function for generating the short-term key K_{auth} . The *default* HMAC function, expressed below, uses MD5 as the base, one-way hash function:

where $P_1 = \left|^{48} 36_{16}\right.$ and $P_2 = \left|^{48} 48_{16}\right.$ are two constant padding *bored* with K_{ij}. If more protection is desired, the MD5 function used in the expression can be replaced by SHA-1 function, which is more suitable for pseudo-random number generation. Then, $P_1 = \left|^{64} 36_{16}\right.$ and $P_2 = \left|^{64} 5C_{16}\right.$ will be the two constant paddings. Note that the values of $K_{ij} \oplus P_1$ and $K_{ij} \oplus P_2$ can be pre-computed as suggested in [hmac-sha1].

4.1.3 Public Key Infrastructure Support

The algorithm needs the support of a PKI to issue an X.509v3 certificate (containing a *DH public value*) to every Mobile Node or Corresponding Node, and every Home Agent or Foreign Agent. All these certificates must contain the following DH parameters in an interoperable format:

dhKeyAgreement : DH algorithm type, iso/us/ rsadsi / pkcs

prime, p : prime modulus of exponentiation

base, g : base of exponentiation

privateValueLength : DH private value length

5. IPSEC PROTECTION OF PACKET REDIRECTION

Another function of the MoIPS architecture is to offer IPSec protection to IP datagrams redirected by Mobile IP. When implemented on selected packet tunnels, the IPSec data origin authentication and data confidentiality services enable the Mobile Nodes to enjoy the same network connectivity (with possible performance degradation) and communication privacy as when they were attached to their home networks. These services also augment the firewall traversal guidelines proposed by Gupta and Glass [mip-firewall-trav] to pass redirected datagrams through the firewalls defending both Mobile Node's home and visiting foreign networks.

5.1 Selective Use of MIP-IPSec Tunnels

Due to the different options existing in Mobile IP — particularly, the use of *reverse tunneling* and the choice between *co-located or foreign-agent care-of addresses* — IP tunnels can be established in different combinations of Mobile Nodes, Foreign Agents and Home Agents using full or minimal IP-IP encapsulations; any of these tunnels can be protected by IPSec protocol. Table 5-1 lists the possible tunnels[6] with C and ~C marking the use of co-located or Foreign Agent bounded Care-of Address, R and ~R marking the use / not use of reverse tunneling.

Notice that tunnels between the Corresponding Nodes and the mobility agents are not included among the choices. This is mainly due to the lack of mechanism in current Mobile IP for setting up these tunnels: for the sake of interoperability between Mobile IP and IP, the existence of Foreign Agents and Home Agents is hidden from the Corresponding Nodes, and no provision was made for these entities to communicate via Mobile IP control messages. Hence, although the Corresponding Nodes may learn the presence of Foreign Agents in route-optimized Mobile IP when they receive the Foreign Agent Care-of Address of Mobile Nodes, they must establish the IPSec tunnels by themselves without any assistance from Mobile IP. Moreover, the use of CN-FA tunnels may be less cost effective because they must be re-established frequently as Mobile Nodes roam in the foreign networks.

Among the possible IPSec tunnels, the MN-CN pair are end-to-end tunnels that may exist regardless of Mobile IP. We recommend using them whenever end-to-end security is needed. The remaining *three* pairs of tunnels, HA-FA, MN-HA and MN-FA, are introduced by Mobile IP packet redirection. Among them, the MN-HA tunnels are most useful while the MN-FA ones are the least. Their uses will be studied individually in the following paragraphs.

FA-HA Tunnels The MIP-IPSec tunnel going from a Home Agent to a Foreign Agent (and from a Foreign Agent to a Home Agent if reverse tunnel and Foreign Agent Care-of Address are used) are the easiest to establish. They can be implemented by simply adding IPSec protection to the existing Mobile IP tunnels.

When they are used to support data-origin authentication and confidentiality, these tunnels provide a *virtual private network (VPN)* connection between the *home network* and the *foreign network* currently visited by the Mobile Node. Such a connection may allow the Mobile Node to obtain the same connectivity as it is at home only if the Foreign Agent can strongly authenticate Mobile Node in either network or link layer. The more notable value of using the FA-HA tunnels arises perhaps from its use in firewall traversal. By configuring the firewalls in the foreign networks as Foreign Agents and setting up the FA-HA tunnels, we created authenticated communication paths through the firewalls. With the knowledge of Mobile Nodes, the firewalls, which assume the role of Foreign Agents, can easily screen the communication.

MN-HA Tunnels The MN-HA IPSec tunnels supporting data-origin authentication and confidentiality will be the most useful tunnels as they provide a secure communication path between a Mobile Node and its home network. The data-origin authentication (and integrity) will prevent spoofing, while data confidentiality will frustrate eavesdropping. By using the tunnels in both directions, an Mobile Node can have secure communication with its home network and enjoy the same connectivity as it has at home. Nonetheless, the tunnels do *not* provide all the protection required by the home network; in order to safeguard the home network, the Mobile Node must function as a firewall on the home network performing perimeter protection tasks specified by the network security policy.

The MN-HA tunnels are, however, more expensive to establish: since they are not a part of the packet redirection mechanism, they must be built separately using the procedure described in Section 5.2.

MN-FA Tunnels The MN-FA IPSec tunnels can be used in two ways if no link-layer protection has already provided the services: (1) data confidentiality for Mobile Node over the foreign network and (2) data origin authentication of MN-FA exchange. However, the MN-FA tunnels exist only if Mobile Node chooses to use an Foreign Agent Care-of Address and must be built by re-encapsulating the IP datagrams. Hence, these tunnels are expensive and should be replaced by MN-CN or MN-HA tunnels whenever possible.

Table 5-1. IPSec tunnels to be used with Mobile IP

	~C ~R	C ~R	~C R	C R
CH -> HA				
HA -> CH				
HA -> FA	🗐		🗐	
FA -> HA			🗐	
FA -> MN	🗐		🗐	
MN -> FA			🗐E	
HA -> MN	🗐	🗐	🗐	🗐
MN -> HA			🗐	🗐
CH -> FA				
FA -> CH				
CH -> MN	💻	💻	💻	💻
MN -> CH	💻	💻	💻	💻

[6] Table 5-1 notations: √ marks the packet redirecting tunnels, + marks the end-to-end tunnels between communicating hosts, E marks the tunnel which only exists when MN-FA encapsulation is used in reverse tunneling, and the dark shade marks an unintended use of the reverse tunneling flag to select an MN-HA tunnel with co-located COA although reverse tunneling is used primarily with FA bounded COA.

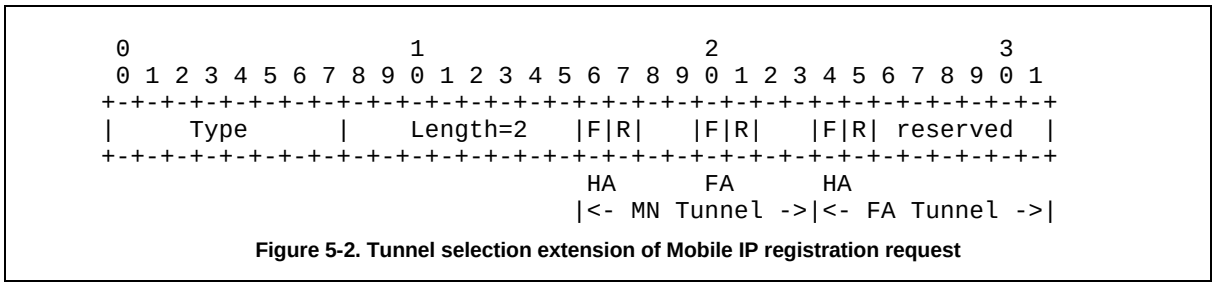

Figure 5-2. Tunnel selection extension of Mobile IP registration request

Tunnel Use in Firewall Traversal The MIP-IPSec tunnels studied in this section do *not* offer a complete solution to the firewall traversal problem encountered by packets redirected by Mobile IP; particularly, they cannot hide the unknown source or destination addresses caused by the use of private network addresses. Nevertheless, they can augment Gupta and Glass' guidelines in the following two ways:

1. With IPSec protection on Mobile IP redirected packets, firewalls which can parse Mobile IP and IPSec protocols may admit the protected packets with reduced risks.
2. By implementing the functions of both a firewall and a mobility agent, a network entity can provide thorough protection to its network by becoming an authenticated end-point of the redirected packets and the processor of these packets based on Mobile IP information it has.

In order to provide the second type of protection, a hierarchy of Foreign Agents must be built to implement multi-layers of firewalls surrounding a foreign network. Also, the Mobile Nodes must be assigned permanent IP addresses belonging to the *perimeter networks* enclosed by the firewalls. Both arrangements are technically feasible and may be regarded as the price for additional protection.

5.2 MIP-IPSec Tunnel Establishment

The establishment of MIP-IPSec tunnels takes two steps: (1) the mutual agreement among Mobile Nodes, Foreign Agents and Home Agents on the selection of tunnels and (2) the negotiation of necessary security associations using ISAKMP. After these steps, the involved entities may start to send IP-IP encapsulated datagrams protected by IPSec.

In this section, we will go through the tunnel selection process and comment briefly on the ISAKMP negotiation as well as the integration of IPSec with minimal IP-IP encapsulation.

5.2.1 Selection of IPSec Tunnels

The selection process aims at achieving an agreement among Mobile Nodes, Foreign Agents and Home Agents on the choices of tunnels which are protected with IPSec.

To reduce communication overhead, all exchanges will be conducted as extensions of Mobile IP control messages. As an example, Figure 5-2 shows the extension of registration request message. The extension contains flags indicating the end-point and the direction of tunnels requested by Mobile Nodes as well as Foreign Agents. By setting the corresponding flags, a Mobile Node can ask for IPSec tunnels setup in either one or both directions between MN-HA, MN-FA and FA-HA.

Error! Not a valid link.

Figure 5-3. Message exchanges for IPSec tunnel selection

Figure 5-3 displays the sequence of message exchange for conducting the tunnel selection. The sequence follows the basic steps of a Mobile IP registration with decisions concentrated at both Mobile Nodes and Home Agents:

1. A Mobile Node chooses the IPSec tunnels between itself and the Foreign Agent based on the exchange of agent solicitation and advertisement. It also chooses the MN-HA tunnels by referring to its security policy.
2. A Mobile Node records its choices in a tunnel selection extension and sends it along with a registration request. Upon reception, Foreign Agent inspects the extension and passes the message to the Home Agent.
3. After receiving the registration request, Home Agent checks the tunnel choices against its security policy and decides whether to reject any of the choices. It then sends the registration reply, which may contain zero or more error codes indicating its decisions.

Two types of error codes are needed for explaining the rejection of tunnel choices. One indicates a conflict between the tunnel choices and Mobile IP operating modes such as the selection of Care-of Address and reverse tunnels. The other indicates a mismatch between the tunnel choices and Home Agent security policy. In both cases, each error code is followed by an index code identifying the rejected tunnel.

5.2.2 Negotiation of Security Associations

The tunnel selection extension does not specify the IPSec security services and/or the security mechanisms to be used for protecting the Mobile IP tunnels. This is because all these choices shall be made by ISAKMP based on the domain of interpretation (DOI) and the protocol situations that govern the key management exchanges. A Mobile IP DOI will be developed in the near future to specify the security policy encoding of Mobile IP.

The introduction of ISAKMP negotiations inevitably complicates the packet redirection process because the negotiation of security associations may fail even *after* a successful Mobile IP registration. The failure of an ISAKMP negotiation does not block the packet redirecting tunnels, but it does mean the absence of IPSec protection. Error messages will be generated and logged in these cases.

6. PROTOTYPE IMPLEMENTATION

The project team delivered the first MoIPS prototype in August 1997. The prototype is marked by the following features:

- the capability of obtaining x.509 certificates and CRLs from DNS (possibly via a FA proxy), CDP and pre-installed files,

- the capability of verifying x.509 certificates and CRLs (including cross certificates) by following the multi-tree hierarchy shown in Figure 3-1,
- the ability of authenticating the registration messages of IETF Mobile IP using symmetric keys produced by the zero-message key generation scheme,
- the integration of MN-CN IPSec tunnels (in transport mode) with Mobile IP packet redirection – the use of only end-to-end IPSec with Mobile IP tunnels avoids temporarily the need of IPSec tunnel selection and special DOI.

In the following paragraphs, we describe briefly the main modules of this first prototype.

Mobile IP Module The MoIPS prototype was built upon an IETF RFC2002 compliant Mobile IP implementation developed by Prof. David Johnson's team in Carnegie-Mellon University [cmu-monarch]. The version currently used was v.1.0.2 upon FreeBSD v.2.2.1. The Mobile IP implementation was slightly modified in order to integrate with the zero-message key generation module.

Zero-Message Key Generation Module This module supplies the short-term symmetric keys necessary for authenticating the Mobile IP control messages. It implements the HMAC based key generation algorithm [Section 4.1] and offers two interface functions [Figure 6-4]. The function `MakeMasterKey` creates a master key of length `st_key_len` from a pair of Diffie-Halmen public and private keys, and the function `MakeShortTermKey` derives a short-term authentication key from `master_key` and the eight byte replay protection identifier `ident`.

IP Security and ISAKMP Key Management Modules The IPSec module is a FreeBSD port of NRL IPSec [v.α3] implementation from Portland State University Secure Mobile Networking Team [psu-smn]. This module also uses the `ipkey` utility in NRL IPSec for manual key input.

The ISAKMP module is a FreeBSD port of Cisco's ISAKMP / OAKLEY [v.α5] implementation. It uses a cryptographic library from Cylink Inc. and can conduct key negotiation only using manually inserted DSS keys. In the final release of the prototype, the ISAKMP module will be interfaced to the *certificate verifier* (CV) module so that it can obtain DSS keys from X.509 certificates stored in DNS entries.

X.509 Certificate Verifier The certificate verifier (CV) consists of a UNIX process daemon and an interface library. ISAKMP or ZmKeyGen modules are the clients of CV. They can obtain public keys, certificate fields or even complete certificates from CV by using the function calls in the interface library.

Whenever possible, the CV daemon responds to these requests based on information stored in its certificate database. If the requested information is not in the database then the daemon will take the following step in order: (1) obtains the certificates using the Certificate Fetcher, (2) verifies the certificates (also obtaining and verifying the certificates of CAs if necessary) and (3) caches the verified certificates in an internal database. The chains of certificates verified by CV are always ended with self-signed certificates.

Cryptographic Engine The MoIPS prototype uses RSAREF as the default cryptographic library, but chooses to interface with the library via the RSA PKCS#11 CryptoKi CAPI. This design decision allows the prototype to be compatible with other cryptographic processing support such as the Fortezza hardware tokens. The CryptoKi is a low-level session-oriented CAPI, which was thoroughly documented in [PKCS11] and [ZP96]. However, in order to hide a few low-level function calls from its clients, the MoIPS prototype implemented a small number of "wrapper" functions [moips-tech-rprt-6].

Currently, Mobile IP, CV and ZmKeyGen modules all use the CryptoKi CAPI. IPSec and ISAKMP modules, on the other hand, uses built-in cryptographic functions.

Certificate Fetcher and Foreign Agent Proxy The DNS Certificate Fetcher connects CV to the DNS daemon either directly or indirectly via the Foreign-Agent Proxy. In both cases, the two modules work together to provide the CV with X509CCRL resource records extracted from DNS entries.

Certificate Discovery Protocol Executive The CV module can use either DNS or CDP to fetch certificates and CRLs. In MoIPS, CDP was used to receive CRLs as they are pushed to the nodes in urgent cases.

7. CONCLUSIONS

In this paper, we describe the design and the first implementation of a public key management structure which satisfies the security requirements of Mobile IP for authenticated mobile node location updates and IPSec protected packet redirection. The system may have many promising applications including scaleable implementations of secure route-optimized Mobile IP and IPSec supported virtual private networking of Mobile IP traffic. The project shall be supplemented with future work on fast and hierarchical location management and efficient management of security associations based on security policies of network domains.

8. BIBLIOGRAPHY

[bellovin-89] S. M. Bellovin. "Security Problems in TCP /

```
u_char *MakeMasterKey(u_char *public,unsigned publen,
                      u_char *private, unsigned privlen,
                      u_char *p, unsigned plen,
                      unsigned st_key_len);

u_char *MakeShortTermKey(int alg,
                         u_char *master_key,
                         u_char *ident);
```

Figure 6-4. Interface functions to Zero-Message Key Generation module

IP Protocol Suite." *ACM Computer Communications Review*, 19(2), Mar. 89.

[cmu-monarch] D.B. Johnson. The CMU Monarch Project. `http://www.monarch.cs.cmu.edu/`

[dns-secext] D. E. Eastlake III, C. W. Kaufman. "Domain Name System Security Extensions." <*draft-ietf-dnssec-secext-06*>, IETF DNS Security Working Group, Oct. 95.

[hmac-md5] H. Krawczyk, M. Bellare, R. Canetti. "HMAC -MD5: Keyed-MD5 for Message Authentication". <*draft-ietf-ipsec-hmac-md5-03*>, IETF IP Security Working Group, Mar. 96.

[hmac-sha1] H. Krawczyk, M. Bellare, R. Canetti. "HMAC -SHA-1: Keyed-SHA-1 for Message Authentication". <*draft-ietf-ipsec-hmac-sha1-03*>, IETF IP Security Working Group, Mar. 96.

[isakmp] D. Maughan, M. Schertler, M. Schneider, J. Turner. "Internet Security Association & Key Management Protocol (ISAKMP)" <*draft-ietf-ipsec-isakmp-07*>, IPSec Working Group, Feb. 97

[mip-optim] D.B. Johnson, C. Perkins. "Route Optimization in MIP." <*draft-ietf-mobileip-optim-03*>, IETF Mobile IP Working Group, Nov. 95.

[mip-tunnel-reverse] G. Montenegro. "Reverse tunneling for Mobile IP". <*draft-ietf-mobileip-tunnel-reverse -02*>, IETF Mobile IP Working Group, Mar. 97.

[photuris] P. Karn, W. A. Simpson. "Photuris Session Key Management Protocol." <*draft-ietf-ipsec-photuris-08*>, IETF IP Security Working Group, Nov. 95.

[pkix-ipki-1] R. Housley, W. Ford, D. Solo. "Internet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile" <*draft-ietf-pkix-ipki-part1-02*>, IETF PKIX Working Group, Jun. 96.

[rfc1034] P. V. Mockapetris. "Domain Names: Concepts and facilities." *RFC1034*, Nov. 87.

[rfc1825] R. Atkinson. "Security Architecture for the Internet Protocol." *RFC1825*, IETF Network Working Group, Aug. 95.

[rfc2002] C. Perkins (ed.) "IP Mobility Support." *RFC2002, proposed standard.* IETF Mobile IP Working Group, Oct. 96.

[skip] A. Aziz. "Simple Key-Management for Internet Protocol (SKIP)." <*draft-ietf-ipsec-skip -06 >*, IETF IP Security Working Group, Nov. 95.

[ipsec-cdp] A. Aziz, T. Markson, H. Prafullchandra. "Certificate Discovery Protocol". <*draft-ietf-ipsec-skip -06 >*, IETF IPSec Working Group, Nov. 95.

[moips-tech-rprt-5] J. Zao, J. Gahm and M. Condell. "Quarterly Technical Report #5, Security Architecture for Global Host Mobility". BBN, Oct. 96.

[moips-tech-rprt-6] P. Helinek, N. Yuan, M. Condell and J. Zao. "Quarterly Technical Report #6, Security Architecture for Global Host Mobility". BBN Feb. 97.

[moips-zm-key-gen] J. Zao and S. Kent. "New Key Generation Algorithm for Mobile IP Control Message Authentication" *Sect.4, MoIPS Quarterly Technical Report #3, BBN Corp.* Apr. 96.

[psu-smn] J. McHugh and J. Binkley. The Portland State University Secure Mobile Networking Project. `http://www.cs.pdx.edu/research/SMN/.`