

2003

Securing Mobile IP Enabled Laptop

R. Wiangsripanawan
University of Wollongong

R. Safavi-Naini
University of Wollongong, rei@uow.edu.au

Willy Susilo
University of Wollongong, willy_susilo@uow.edu.au

Publication Details

This paper originally appeared as: Wiangsripanawan, R, Safavi-Naini, R & Susilo, W, Securing Mobile IP Enabled Laptop, The 11th IEEE International Conference on Networks, 28 September-1 October 2003, 693-698. Copyright IEEE 2003.

Securing Mobile IP Enabled Laptop

Abstract

Mobile IP (Internet Protocol) enables access to the Internet anywhere with one IP address, hence, providing the flexibility that is required by today's growing mobile work force. Deploying Mobile IP introduces new security threats that if not carefully addressed can have severe consequences for home organizations. IPSec is a commonly used protection mechanism that is employed in this context. IPSec requires a flexible key management scheme to provide cryptographic keys to communicating entities. A commonly used public key based key management system is SKIP (Simple Key-Management for Internet Protocols). In this paper we consider the scenario where a laptop that is enabled with secure Mobile IP connection using SKIP, is stolen and the aim is to protect the private key stored in the laptop. We propose a method of protecting the private key in which the secret stored in the laptop cannot be used to determine the private key. We also introduce a method of 'disabling' the stored secret such that even when the laptop is stolen, there is no need for changing the private key. An important property of our system is that it does not add extra messages to the existing SKIP implementation.

Disciplines

Physical Sciences and Mathematics

Publication Details

This paper originally appeared as: Wiangripanawan, R, Safavi-Naini, R & Susilo, W, Securing Mobile IP Enabled Laptop, The 11th IEEE International Conference on Networks, 28 September-1 October 2003, 693-698. Copyright IEEE 2003.

Securing Mobile IP Enabled Laptop

(Extended abstract)

Rungrat Wiangsripanawan, Rei Safavi-Naini and Willy Susilo
Centre for Communication Security
School of Information Technology and Computer Science
University of Wollongong, Australia
Email: {rw26, rei, wsusilo}@uow.edu.au

Abstract—Mobile IP (Internet Protocol) enables access to the Internet anywhere with one IP address, hence, providing the flexibility that is required by today's growing mobile work force. Deploying Mobile IP introduces new security threats that if not carefully addressed can have severe consequences for home organizations. IPSec is a commonly used protection mechanism that is employed in this context. IPSec requires a flexible key management scheme to provide cryptographic keys to communicating entities. A commonly used public key based key management system is SKIP (Simple Key-Management for Internet Protocols). In this paper we consider the scenario where a laptop that is enabled with secure Mobile IP connection using SKIP, is stolen and the aim is to protect the private key stored in the laptop. We propose a method of protecting the private key in which the secret stored in the laptop cannot be used to determine the private key. We also introduce a method of 'disabling' the stored secret such that even when the laptop is stolen, there is no need for changing the private key. An important property of our system is that it does not add extra messages to the existing SKIP implementation.

I. INTRODUCTION

Mobile IP [1] allows a mobile node to use the same IP address while roaming between networks. As the user changes its point of attachment to the network, the data packets are dynamically directed to the routers that are able to deliver the packets to the user. Mobile IP provides the seamless connectivity that is required by many applications, and can be used to enforce IP-based access control on nodes. In a Mobile IP system there are three main types of entities: Mobile Nodes, Foreign Agents and Home Agents. A mobile node must register with the home agent, which will store this information in a routing table, called a *binding table*, to route packets to the node.

Mobile IP may be deployed over Intranets, or over wide area networks and the Internet. If Mobile IP is used over an unprotected Intranet, data packets may pass through insecure links, where packet content might be eavesdropped or modified. When Mobile IP is used over wide area networks and the Internet, a new problem is the traversal of packets through the firewall. Packets require tunnelling at the mobile nodes and de-tunnelling at the home agent or the firewall. Security of these tunnels and ensuring that they are established between authenticated parties and their contacts are authentic is an important security issue. To provide security in Mobile IP, cryptographic mechanisms such as IPSec [3], [4] are used. A commonly used method for providing secure keys is SKIP (Simple Key-Management for Internet Protocol [5]).

An important advantage of using SKIP is that key information can be communicated *in-line*, that is as part of the IP packet. Under SKIP, a mobile node requires a pair of private and public keys. The private key is known only to the node, while the public key is public. A node uses its private key together with the public key of another node to calculate a common key with that node. A mobile node must be able to securely access its private key. One alternative is to use tamper-proof storage, such as a smart card, to store the key and require the device that implements Mobile IP to access the key through a secure reader. This method has the inconvenience and expense of requiring a reader device. Software smart cards [27] camouflage the key in the software and so can expend with the card reader at the cost of lower security.

A commonly used alternative is to store the key information on the device encrypted with a key which is derived from a password known to the user. This allows a legitimate user who knows the password to access the key. However, encrypting the key with a secret password leaves the system open to off-line password attack. In this paper we consider a stolen laptop that implements Mobile IP and our aim is to protect user's private key against this attack. We assume the laptop uses IPSec and SKIP, and show a method of securing SKIP private key such that a lost device does not compromise the key. An important property of our system is that the key information can be included in the SKIP header.

We also show how to 'disable' the secret stored on the laptop such that, without changing the private key, the stored secret in the stolen laptop become of no use to the adversary.

The rest of this paper is organized as follows. In section II, we give an overview of Mobile IP, its security and current protection mechanisms. In section III, we introduce the problem and show that the known solutions are inadequate. In section IV, we describe a solution. Section V concludes the paper.

II. PRELIMINARIES

Mobile IP [1] is a network layer protocol designed over the Internet Protocol (IP) to enable mobility; that is allowing a node to change its point of attachment to the network while maintaining its connection. A Mobile IP address has two parts: a *home address* that is used as the permanent IP address of the node, and a *care-of-address* that changes according to the mobile node location. The latter is used for routing purposes. Two *mobility agents*, called *home agent* and

foreign agent, are used to establish the association between the mobile node and a *correspondent node*, which is a node that wants to communicate with the mobile node. The correspondent node can be a fixed node or a mobile node. The two agents are routers on the home network, and foreign network, respectively.

To use the Mobile IP outside the home network, the mobile node obtains a care-of-address from the network that it is visiting and registers this address with its home agent. A care-of-address can be either the IP address of the foreign agent, or a temporary address assigned to the mobile node in the foreign network, for example through DHCP [6] or PPP [7]. The two care-of-addresses are called *foreign agent* and *collocated* care-of-address, respectively. The home agent updates the care-of-address of the mobile node in its binding table.

Packets from a correspondent node will be received by the home agent and tunneled to the registered care-of-address. The foreign agent then de-tunnels packets and sends them to the mobile node. *Tunnelling* encapsulates Mobile IP's packets. For example, in IP-within-IP [8] the original Mobile IP packet is treated as the payload, while the home agent and the care-of-address are used as the source and destination of the encapsulated packet. *Route optimization* [9] is provided in extensions of the basic protocol and allows the correspondent node to send packets directly to the mobile node rather than traversing through the home agent. This reduces the required bandwidth and is particularly efficient in cases that the mobile node is close to the correspondent node.

Mobile IP inherits IP security problems and introduces new security and privacy concerns.

A. Security Issues in Mobile IP

We focus on security issues that are specific to Mobile IP.

Mobile IP can be deployed over an Intranet, or over a wide area network and the Internet.

If Mobile IP is used in an Intranet environment, without connection to the Internet, confidentiality and authenticity of packets must be guaranteed. Otherwise, not only security of the data is lost but also integrity of connections will be endangered. For example, modification of registration requests by a malicious router, which reports its own address as the care-of address for the mobile node will divert traffic and result in all packets from a correspondent node being tunneled to the malicious node, hence a denial of service attack. Other attacks include *replay* of registration requests by a malicious node, and *stealing* established sessions [2]. Authentication is also required in route optimization and without it an adversary can create fraudulent binding update packets to redirect the traffic.

If Internet-wide mobility is considered, the problem of traversing the firewall needs to be addressed as well. Firewalls use *Ingress Filtering* [12] to filter inbound packets based on their source address and so will discard packets whose network address is the same as the home network. Packets sent by a mobile node when it is outside the home network

will appear as inbound traffic with the IP address of an internal node and will be blocked. To overcome this problem *Reverse Tunnelling* [13] is used. Mobile nodes' packets are sent to the home agent before being forwarded to the correspondent node. This uses a method similar to tunnelling [1] but in the reverse order. However, the firewall must be sure that the tunneled packets are from legitimate node [14].

In general Mobile IP packets although they have the IP address of the internal network, cannot be assumed to have the same level of protection as packets in the internal network, since the packets might come from a foreign network and traverse through the Internet. In all above cases cryptographic mechanisms are used for providing the secured packets.

B. Security Mechanisms in Mobile IP

Mobile IP provides authentication by including a cryptographic field in registration packets. The default authentication algorithm is HMAC-MD5 [1]. There are 3 kinds of authentication extensions: a mandatory extension between the mobile node and the home agents, and optional extensions between the mobile node and the foreign agent, and between the home agent and the foreign agent.

IPSec is used to establish a secure connection (tunnel) between a remote mobile node and the internal network [15]–[20]. A secure connection between a mobile node and a home network may be through one IPSec tunnel between the node and the firewall, or the home agent, or two IPSec tunnels between the mobile node and the Foreign Agent, and between the mobile nodes and the home agent. IPSec requires a scalable key management system. The two commonly used standards are ISAKMP [10] and SKIP [5]. Although the former is adopted by IETF as the mandatory key management standard (IKE [11]), it is a session oriented protocol and has the overhead of establishing a session. In this paper we consider SKIP a protocol that bundles the key information into the data packet and so does not have this overhead.

III. STOLEN LAPTOP PROBLEM

A. Motivation

A mobile node is typically a laptop or a handheld device, which can be easily stolen and so the secret key of the device must be carefully protected and deployed. For example, if a laptop connection to the home network is naively automated such that upon switching on the device, the authentication protocol is automatically executed, its confiscation by a malicious user will completely compromise the home network.

SKIP requires the mobile node to have a pair of public and private keys. A common way of protecting the private key is to use a password to encrypt it and store the encrypted form on the device. However, because the public key is known by everyone, an attacker can launch an *off-line password guessing* attack to find the private key. The attack can be described as follows.

Let $E_k()$ be a symmetric key encryption algorithm used to encrypt the private key, and let $D_k()$ denote the corresponding decryption algorithm. k is the common key used by the two

algorithms such that for a message x , we have $D_k(E_k(x)) = x$. Also, let $\mathcal{E}_{pk}()$ and $\mathcal{D}_{sk}()$ denote a public key encryption algorithm using the public key pk , and a decryption algorithm using the private key sk , where for a message x , $\mathcal{D}_{sk}(\mathcal{E}_{pk}(x)) = x$. In an off-line password (key) guessing attack, the attacker has $X = E_k(sk)$ and his aim is to find sk . For this, the attacker will try all possible passwords, k , one at a time, and for each password k , (i) finds $u = D_k(X)$; (ii) for a text x , checks $x \stackrel{?}{=} \mathcal{D}_u(\mathcal{E}_{pk}(x))$. If the equality holds, the attacker has found the private key; otherwise the next password is tried. The attack works because of the ‘verifiable texts’ that is generated through the decryption process.

We assume the SKIP protocol is used for IPSec and the setting is similar to [17], [18].

B. Related work

Perlman and Kaufman [24] proposed to download the private key from a protected server. Their protocol needs the server to be fully trusted and at least two messages to be exchanged.

To reduce trust on the server and also protect against possible server compromise, the use of multiple servers [25], [26] has been proposed. The private key is divided into shares and each share is stored in one of the servers. The adversary has to compromise all servers to be able to retrieve the private key. The increased security is at the cost of more computation and communication with servers and so is unacceptable for many applications.

Mackenzie and Reiter [28] proposed a method of protecting private keys in network enabled devices. Their system does not require a trusted server and has provable security. Their construction can be used with any public key encryption and signature scheme. They also proposed a second protocol that is specific to RSA signature and El Gamal encryption. This protocol allows *key disabling* which is particularly useful if the secret key has already been downloaded onto the device and the only way to protect against the misuse of the key when the laptop is stolen, is to disable the key. The main drawback of their schemes is the need for additional messages.

C. Our Contributions

We propose an extension of SKIP to provide security against the compromise of the mobile device, that allows secure connection from outside and inside of the home network. We propose two protocols: the *external* IPSec protocol, which is used when the laptop is outside the home network and the *internal* IPSec protocol which is used when the laptop is located inside the home network (see the proposed solution section for more detail). The internal protocol has the following properties: the server does not need to be trusted; no initialization per user is required; and public keys are truly public. The last point contrasts with [27] which, while having similar functionalities, required the device’s public key to be unknown by the device. The external protocol provides key disabling property whilst preserving confidentiality of the private key even if the laptop is stolen. The main advantage of

the proposal is that the required security does not need extra messages and the added security is obtained by extending the SKIP header.

IV. THE SCHEME

First we introduce notation and provide relevant background.

Notations

Let $E_k()$ and $D_k()$ denote encryption and decryption algorithms and k denote the secret key.

Let $C = E_k(M)$ denote the cryptogram corresponding to M . We use $C \leftarrow E_k(M)$ to denote that the result of encryption is assigned to the variable C . $D_k()$ takes a ciphertext C as input and outputs either a message M , if C is a valid encryption of M , or otherwise returns \perp , we let $\hat{M} := \{M, \perp\}$.

Let $G_{enc}()$, $\mathcal{E}_{pk}()$ and $\mathcal{D}_{sk}()$ denote the key generation, encryption and decryption algorithms of an asymmetric encryption system, respectively. $G_{enc}(\ell)$ takes a security parameter ℓ that determines the security level of the system, and outputs a public and private key pair (pk, sk) ; that is $(pk, sk) \leftarrow G_{enc}(\ell)$. $\mathcal{E}_{pk}()$ takes a public key (pk) and a message M as input and outputs the encrypted value C of M , that is $C \leftarrow \mathcal{E}_{pk}(M)$. $\mathcal{D}_{sk}()$ takes a ciphertext C and a secret key (sk) as input and outputs either a message M , if C is a valid encryption of M or returns \perp otherwise, $\hat{M} \leftarrow \mathcal{D}_{sk}(C)$ where $\hat{M} := \{M, \perp\}$.

Let $x \in_R S$ denote a value x , randomly takes from a set S . The ring of integers modulo a number n is denoted by Z_n , and its multiplicative group, which contains only the integers relatively prime to n is denoted, by Z_n^* .

Diffie-Hellman Key Agreement

The first practical key agreement was proposed by Diffie and Hellman [29]. The protocol allows two parties to establish a shared secret over an insecure channel without having a shared key in advance. The protocol is as follows. To obtain a common key, Alice and Bob agree on a prime p and a primitive element $g \in Z_p^*$. Each participant selects his/her own secret a and b , $a, b \in Z_{p-1}$. Then, Alice sends W_a to Bob and Bob sends W_b to Alice via an authenticated channel, where $W_a = g^a \pmod{p}$ and $W_b = g^b \pmod{p}$. Given W_a , it is assumed to be hard to find $a \in Z_{p-1}$. This is known as the discrete logarithm assumption [31]. Finally, Alice computes the shared key $K_{AB} = W_b^a = (g^b)^a \pmod{p}$. Bob can compute the same key $K_{AB} = W_a^b = (g^a)^b \pmod{p}$.

This protocol is vulnerable to a ‘‘man in the middle’’ attack [32]. To protect against this attack, the shared key must be authenticated. This can be achieved by incorporating public key cryptography [31].

Public-key Certificate System

A Public-key certificate system is a system which consists of the components necessary to securely distribute the public key [23]. Examples include secure DNS [21] and X.509 directory lookup [22].

Deploying SKIP in Mobile IP

Simple Key-Management for Internet Protocols (or SKIP, for short) [5] is based on Diffie-Hellman key exchange. Users' public keys, g^i, g^j , are authenticated through a public key certificate system. SKIP does not need extra messages. Cryptographic information is included as part of the SKIP header and sent along with the encrypted payload. The receiver uses the source IP address of the received packets to determine the sender's public key. SKIP allows the sender to specify alternative IP addresses. This is very useful for mobile nodes to specify their care-of-address.

To compute a session key when the network is protected by the firewall, the mobile node must obtain its private key together with the public key of the firewall. This session key will be used to encrypt the shared key which will be used for future communication. The firewall will calculate the same session key in a similar way, using the mobile node's public key.

Due to space limitations, more details about SKIP and its deployment with Mobile IP are omitted.

A. First Scenario: The External IPsec Connection

The purpose of this IPsec connection is to authenticate packets at the firewall while preserving their confidentiality.

A Simple but Insecure Scheme

Let i and π denote a laptop's private key and the user's password respectively. If $\theta \leftarrow E_\pi(i)$ is stored in the laptop, an adversary can perform an off-line dictionary attack as described in section III-A. That is, the adversary randomly chooses a password $\hat{\pi}$ from his dictionary list and uses it to decrypt θ . That is, $\hat{i} = D_{\hat{\pi}}(\theta)$. He can verify whether his guess is correct by verifying whether $g^{\hat{i}} \stackrel{?}{=} g^i \pmod{p}$, where g^i is publicly available in the PKI directory.

A Secure Scheme

The basic idea of our scheme is to divide the laptop's private key into 2 parts. One part is encrypted with the user's password and stored on the laptop, while the other is stored at the firewall. When a remote laptop is switched on, the user enters his password, which is used to decrypt and obtain the laptop's part of the private key. Then, the laptop computes the session key from this value and the firewall's public key.

The firewall needs to be assured that the user knows the correct password π . We use Schnorr's indirect proof of knowledge [30] techniques to show this knowledge. After successful verification, the firewall computes the session key from its private key, its stored private key part of this laptop and the laptop's public key.

The protocol has two phases: the initialization phase and the key generation phase.

1. Initialization Phase

First, the laptop's private key i and the user's password π are generated. Next, the private key i is split randomly into two parts, β and δ , where $\beta + \delta = i \pmod{q}$. δ is stored at the firewall, and the encrypted version of β , $\theta \leftarrow E_\pi(\beta)$, is

-
- p, q are prime
 $g \in Z_p^*$, where g is a primitive element
1. select $\pi \in_R Z_q$, where π denotes a user's password
 2. select $i \in_R Z_q$, where i denotes a laptop's private key
 3. select β and δ , where $\beta, \delta \in_R Z_q$, and $\beta + \delta = i \pmod{q}$
 4. compute: $\theta \leftarrow E_\pi(\beta)$

Laptop stores	Firewall stores
θ	δ

Protocol 1 : External IPsec Connection: Initialization Phase

stored in the laptop's hard disk. The user password π and the components of the private key (i, β, δ) must be erased from the volatile memory. This phase is illustrated in Protocol 1.

2. Key Generation Phase

Laptop	Firewall
1. user enters password $\hat{\pi}$, where $\hat{\pi} \in Z_q$	Store δ
2. select r and s , where $r, s \in_R Z_q$	
3. compute : $\hat{\beta} \leftarrow D_{\hat{\pi}}(\theta)$	
4. compute : $\gamma = r + \hat{\beta}s \pmod{q}$	
5. $\alpha = \langle g^\gamma, r, s \rangle$	
6. obtain the firewall's public key η_{FW} from PKI	
7. $K_{MN-FW} \leftarrow (\eta_{FW})^{\hat{\beta}} \pmod{p}$	
SKIP process continues here	
8. $\langle \alpha, SKIP \text{ header}, SKIP \text{ payload} \rangle$	
→	
	9. receive $\hat{\alpha} = \langle g^{\hat{\gamma}}, \hat{r}, \hat{s} \rangle$
	10. obtain the laptop's public key η_i from PKI
	11. compute $g^{\hat{\beta}} = \frac{\eta_i}{g^{\hat{s}}} \pmod{p}$
	12. abort if $g^{\hat{\gamma}} \neq g^{\hat{r}} \cdot (g^{\hat{\beta}})^{\hat{s}} \pmod{p}$
	13. $K_{MN-FW} \leftarrow (g^{\hat{\beta}})^{\hat{j}} \pmod{p}$, j denotes the firewall's private key
	14. IPsec connection starts here

Protocol 2: External IPsec Connection: Key Generation Phase

First, the user needs to enter his password π so that $\hat{\beta}$ can be found. Then, the mobile node finds α , where $\alpha \leftarrow \langle g^\gamma, r, s \rangle$. γ is computed as $r + \beta \cdot s \pmod{q}$, where r and s are random numbers. The session key is computed from $\hat{\beta}$ and the firewall public key η_{FW} . That is, $K_{MN-FW} \leftarrow (\eta_{FW})^{\hat{\beta}} \pmod{p}$, where $\eta_{FW} = g^j \pmod{p}$. α is sent together with the SKIP packet.

The firewall verifies the authenticity of π by incorporating Schnorr's indirect proof of knowledge as follows: the firewall computes $g^{\hat{\beta}}$ from $\eta_i / g^{\hat{s}} \pmod{p}$, where η_i is the laptop's public key and $\eta_i = g^i \pmod{p}$, and compares if $g^{\hat{\gamma}} \stackrel{?}{=} g^{\hat{r}} \cdot (g^{\hat{\beta}})^{\hat{s}} \pmod{p}$ holds.

If verification succeeds, the firewall will be convinced of the user's identity, and computes the session key using $g^{\hat{\beta}}$ together with its private key (j). That is, $K_{MN-FW} \leftarrow (g^{\hat{\beta}})^{\hat{j}} \pmod{p}$. Otherwise, it will send a message to inform the user that authentication has failed. If the firewall receives several

TABLE I
MAIN DIFFERENCES BETWEEN THE EXTERNAL AND INTERNAL IPSEC
CONNECTIONS

	External IPsec	Internal IPsec
Peer	the firewall	any node
Location	outside the organization network	fixed or mobile inside the organization network
Server	not required (firewall stores δ)	required
User Authentication	at the firewall	at the server

failed requests from the same user within a short time period, it will suspend the connection request from the user. This is important to prevent the online dictionary attack.

Key Disabling Feature

We note that the private key i is not disclosed even though the system is accessed by a valid user. We can obtain a *key disabling function*, as defined in [28]. This allows the owner of the laptop to reuse the same private and public key pair for a new device. To disable the secret of the laptop, a new breakdown of the private key i into two components $(\hat{\beta}, \hat{\delta})$ where $\hat{\beta} + \hat{\delta} = i \pmod{q}$ and $(\hat{\beta}, \hat{\delta}) \neq (\beta, \delta)$ will be used. The new components $(\hat{\beta}, \hat{\delta})$ result in valid operations using the same public key g^i .

B. Second Scenario: The Internal IPsec Connection

When the Mobile IP enabled laptop is used inside the home network, it can communicate with the other mobile nodes directly without going through the firewall. To preserve the confidentiality of the communication, we use secure IPsec communication with the same private key as in the previous protocol. However, we need to modify the protocol.

When the laptop uses the external IPsec connection, it communicates directly with the firewall which stores δ . Therefore, the session key can be computed with the partial secret key β only, without the need to reveal δ . This is because the firewall has knowledge of δ . The situation is different when the laptop is used within the home network and uses the internal IPsec connection to communicate with another mobile node without going through the firewall. Since the other mobile node M_n does not know δ_{laptop} , it cannot compute the session key. Similarly, the laptop does not know δ_{M_n} . To solve this problem, we introduce a server with a function similar to the firewall for nodes inside the network. The server will allow each node M_n to download its own δ_n . This method is used instead of allowing the mobile node M_n to download δ_{laptop} , to avoid a collusion attack between M_n and the adversary. Otherwise, M_n 's user can reveal δ_{laptop} to the adversary, which will later enable him to perform an off-line attack when the laptop is stolen and taken outside the network.

The differences between the external and internal IPsec connection are illustrated in Table I.

TABLE II
MAIN DIFFERENCES BETWEEN THE EXTERNAL AND INTERNAL
PROTOCOLS

	External	Internal
No. of message	≥ 1	≥ 2
Ticket	not compulsory	compulsory
Private key	part of the private key is required	complete private key is required
Key disabling feature	provided	not provided

We allow mobile nodes to download their own δ from the server and assume the server is trusted. If the server is untrusted, we can employ the *ticket* concept from [28]. That is a public key encryption scheme is deployed to encrypt δ to form a ticket. This ticket is stored at the laptop. The public key of the server is used as the encrypted key. Therefore, the server in this scenario does not store δ , rather, it obtains δ from the ticket sent by the laptop using its decryption key sk_{sur} .

We note that the private key i is revealed in the internal IPsec connection, and hence we cannot reuse the key. If the stolen laptop is detected, both of the laptop's public and private key pair must be changed before the new initialization. We also note that we can use the same approach used in the untrusted server scenario to avoid storing δ at the firewall, by encrypting δ with the firewall's public key and store it in the laptop's hard disk.

The protocol is divided into two phases: the initialization phase and the key generation phase which are illustrated as follows.

1. Initialization Phase

If the server is trusted, the initialization values for the laptop follow the same procedure as in the external protocol. The additional task is to store δ at the server as well as the firewall.

If the server is untrusted, the laptop is required to store a ticket for δ . The ticket is computed as $\tau_{sur} \leftarrow \mathcal{E}_{pk_{sur}}(\delta)$.

2. Key Generation Phase

First, the laptop requests the server for δ . If the untrusted server is deployed, the laptop is required to send the ticket. The server needs to verify the identity of the user. If the verification succeeds, δ is sent to the laptop in a secure form. Laptop can combine this information with its secret information β to find a common key with another mobile node. This phase is shown in Protocol 5 in the extended abstract.

The main differences between the external and internal protocol are listed in Table II.

C. Comparison of our scheme and the existing Mobile IP-SKIP scheme

In the following we compare the proposed solution with the scheme in [17]. Both schemes use SKIP and provide secure channels between mobile node and the firewall. The scheme

TABLE III
COMPARISON OF THE EXISTING SKIP-MOBILE IP AND OUR SCHEME

Property	Gupta et al. [17]	Our scheme
Security		
Auth. scheme	Use external device	Use password
Auth. place	At the smart card reader	At the firewall
Auth. method	Use PIN No. with a smart card	Use Schnorr's indirect proof
Key disabling feature	No	Yes (External)
General		
Extra device	Smart card reader	No
Number of protocols	1	2
Server needed	No	Yes for the internal protocol
Extra Storage		
Laptop	Not required	- Store part of private key θ - Store ticket (untrusted server) Store part of private key δ
Firewall	Not required	
Computation		
Laptop	1. Verification of Pin Number at the smart card reader 2. Process SKIP operations	1. Decrypt the stored value using password 2. Compute Verification value 3. Process SKIP operations
Firewall	3. Process SKIP operations	4. Derive δ 5. Perform Schnorr's indirect proof 6. Process SKIP operations

in [17] uses a smart card to store the private key and requires smart card readers. Our scheme requires a small amount of storage in the laptop's disk.

Table III shows the main differences between our scheme and that of [17].

V. CONCLUSION

We have given an overview of Mobile IP and its advantages, and reviewed security issues related to Mobile IP. We considered the case that a device that has stored the private key of a secure Mobile IP system is lost and protection must be provided against unauthorized access of the adversary through the stolen device. We proposed protocols that secure the Mobile IP enabled laptop to be used securely inside or outside the home network.

REFERENCES

[1] C. Perkins, "IP Mobility Support," RFC 3344 (obsolete RFC 3220), August 2002.
 [2] J.D. Solomon, "Mobile IP: The Internet Unplugged," Prentice Hall, New Jersey, 1998.
 [3] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, Nov 1998.

[4] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov 1998.
 [5] A. Aziz, T. Markson and H. Prafullchandra, "Simple Key-Management for Internet Protocol (SKIP)," Internet Draft, August 1996.
 [6] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, March 1997.
 [7] W. Simpson, "The Point-to-Point Protocol (PPP)," RFC 1661, July 1994.
 [8] C. Perkins, "IP Encapsulation within IP," RFC 2003, October 1996.
 [9] C. Perkins and D. Johnson, "Route Optimization in Mobile IP," Internet Draft, February 2000.
 [10] D. Maughan, M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, November 1998.
 [11] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, November 1998.
 [12] P. Ferguson, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827 (obsolete RFC 2267), May 2000.
 [13] G. Montenegro, "Reverse Tunneling for Mobile IP," RFC 2344, May 1998.
 [14] D.B.C Chapman, S. Cooper and E. Zwicky, "Building Internet Firewalls," 2nd, O'Reilly & Associates, 2000.
 [15] J.K. Zao and M. Condell, "Use of IPSec in Mobile IP," Internet Draft, November 1997.
 [16] J. Binkley and J. Richardson, "Security Consideration for Mobility and Firewalls," Internet Draft, November 1998.
 [17] V. Gupta and G. Montenegro, "Secure and Mobile Networking," Mobile Networks and Applications 3 (381-390), Baltzer Science Publishers BV, 1998.
 [18] G. Montenegro and V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP," RFC 2356, June 1998.
 [19] Y. Tsuda, M. Ishiyama, A. Fukumoto and A. Inoue, "Design and Implementation of Network CryptoGate: IP-layer Security and Mobility Support," IEEE, 1998.
 [20] T. Braun and M. Danzeisen, "Secure Mobile IP Communication," Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks (LCN'2001), Tampa, USA, Nov 15-16, 2001.
 [21] D. Eastlake and C. Kaufmann, "Domain name system security extensions", RFC 2065, January, 1997.
 [22] Public-Key Infrastructure (X.509) (pkix) working group Home Page, <http://www.ietf.org/html.charters/pkix-charter.html>.
 [23] C. Kaufman, R. Perlman and M. Speciner, "Network Security Private Communication in a PUBLIC World," Prentice Hall, New Jersey, 2002.
 [24] R. Perlman and C. Kaufman, "Secure Password-Based Protocol for Downloading a Private Key," ISOC NDSS Symposium, 1999.
 [25] David P. Jablon, "Password Authentication Using Multiple Servers," Integrity Sciences, Inc., LNCS 2020: Topics in Cryptology -CT-RSA 2001, April 8-12, 2001 Proceedings, pp. 344-360, 2001, Springer-Verlag.
 [26] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proceedings of the Fifth International Workshop on Enterprise Security, IEEE, 2000.
 [27] D.N. Hoover, B.N. Kausik, "Software smart cards via cryptographic camouflage," Proceedings of the IEEE Symposium on Security and Privacy, IEEE, 1999.
 [28] P. MacKenzie and M.K. Reiter, "Networked Cryptographic Devices Resilient to Capture," Bell Labs, Lucent Technologies, Proceedings of the IEEE Symposium on Security and Privacy, IEEE, 2001.
 [29] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Info Theory, 22(6):644-654, 1976.
 [30] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", Advances in Cryptology - Crypto '89, Lecture Notes in Computer Science 435, pp. 239 - 252, 1990.
 [31] A. Menezes, P.C. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1997.
 [32] D.R. Stinson, "Cryptography : theory and practice," 2nd, CRC Press, 2002.