

# Variable and Scalable Security: Protection of Location Information in Mobile IP

Andreas Fasbender, Dogan Kesdogan, Olaf Kubitz  
 Informatik 4 (Communication Systems), Aachen University of Technology  
 52056 Aachen, Germany, Phone: +49 (241) 80-21401, Fax: +49 (241) 8888-220  
 E-mail: {andreas,kesdogan,kubitz}@informatik.rwth-aachen.de

**Abstract**— The amount of mobile and nomadic computing is expected to increase dramatically in the near future. Hand in hand with this ubiquitous mobile computing security and privacy problems show up, which have not been dealt with sufficiently up to now. The main problems are traffic analysis and the easy access to location information, for example in the popular Internet just by looking at the address headers of messages. In this paper the need for security and privacy supporting networks is discussed.

We present the Non-Disclosure Method (NDM) as a way to provide the user with variable and scalable security and privacy. We exemplarily demonstrate the applicability of NDM in an existing network by presenting an upward compatible protocol extension to the Internet Protocol (IP), the Secure IP in IP Protocol. Its main design goal is the untraceability of network connections in mobile environments.

## I. INTRODUCTION

Today, the TCP/IP protocol suite provides little or almost no security to the user. All routers an IP datagram might pass as well as the communication channels have to be assumed to be trustworthy and resistant to malicious attacks. This assumption is made even harder because the route a packet is sent along is not controllable by the end user and may differ even for datagrams from the same source to the same destination.

Possible attacks against IP connections are for example destruction, collection and repetition of datagrams or the insertion of unauthorized messages. To guarantee a certain security level, Atkinson specified an Internet security architecture [1]. It may be implemented as an option to the IP protocol and provides message integrity, authentication and confidentiality. Message integrity ensures that the datagram is transmitted from source to destination without undetected alteration. Authentication ensures that the sender of the datagram is the one he claims to be. Confidentiality protects the transmitted data against unwanted access by third parties. To achieve these goals, two cryptographic security mechanisms may be used to support users

with their desired security level.

With the growing importance of tele- and data communications on the one hand and with increasing user expectations on the other networks must offer more and more services. An important evolution is the support of user mobility. Inspired by the success of mobile telephony people are now getting used to be able to communicate wherever they currently roam. Within the Internet society, a number of proposals for protocol extensions supporting station mobility have been suggested within the last few years [7]-[10],[15],[16]. To cope with the IP address concept, where a node address corresponds to a static point of network attachment, the Mobile IP draft standard [13] additionally uses a location-dependent temporary address. Upon registration with an agent located in a foreign network, mobile stations initiate a mobility binding between foreign and home network. A special agent in the home network intercepts all packets that are routed to the mobile node's home network via traditional routing mechanisms, encapsulates them into packets destined to the foreign agent and thereby redirects packets to the station's current location.

As shown above, privacy issues in the Internet are still left to the end user. Data privacy can be ensured by applying strong cryptographic procedures on an end-to-end basis. However, protection against traffic analysis is not handled appropriately. In mobile internetworks this problem experiences an even higher significance, since the current location of a mobile node can be easily retrieved just by looking at the address headers of the exchanged packets. Particularly registration requests can then be used to generate location profiles or to attain unauthorized service by running replay attacks. We think that confidential location management in Mobile IP is an important topic and therefore propose a method for protecting user privacy. This problem has already been discussed in the mobile telecommunication community [6].

## II. TRAFFIC ANALYSIS

A mainly unsolved security problem in packet-oriented networks is the analysis of network traffic flow for the purpose of deducing information that is useful to an unauthorized third party [1]. An important example of such information are the identities of the communication partners. In mobile environments protection against traffic analysis particularly means enabling location privacy, which up to now is not solved satisfactorily. By wire-tapping on network links or by an active attack against routers an intruder is able

The work of D. Kesdogan was supported by the Gottlieb Daimler- and Karl Benz-Foundation.

The work of O. Kubitz was supported by the Deutsche Forschungsgemeinschaft, Graduiertenkolleg 'Methods and tools of computer science and their application in technical systems', grant no. Sp 230/6-6.

to retrieve sender and recipient address from the message headers, which are usually transmitted in plain. The additional ease of eavesdropping on wireless links makes this problem even more important for mobile environments.

For traffic analysis there are a number of potential fields for the misuse of location information. For example, in networks for military or police use the knowledge about a communication between two parties is often as useful as the contents of the messages themselves. The same holds for business and private environments. Takeover negotiations between two companies may be disclosed for instance by unusually high data traffic, caused by audits or management meetings in one of the companies.

The IP Security Architecture RFC [1] explicitly states that protection from traffic analysis is not provided by the proposed security mechanisms. They suggest traditional methods like bulk link encryption and generating false traffic to hide the communication partners. The Mobile IP draft [13] specifies that protection from traffic analysis is an important topic. They propose link encryption and the establishment of bi-directional tunnels [11].

Link encryption transmits a message as ciphertext between source and destination. The message is deciphered and enciphered at the intermediate routers with link specific keys. At the routers the messages are processed as plaintext, where the data may be exposed to secrecy and authenticity threats [3]. Therefore, link encryption is not secure enough to prevent intruders from traffic analysis. Moreover, the encryption and decryption procedures impose delays at each intermediate router and do not allow the user to scale the level of security according to his demands.

Bi-directional tunnels can be used to establish a connection between networks [11], where the addresses of the communicating hosts are shielded from examination by intermediate routers, as original source and destination addresses are invisible or even enciphered. However, the traffic between the two corresponding networks (that provide the tunnel) is observable. This may give sufficient knowledge to an attacker, even if he does not know which nodes are communicating.

Chaum presented a method that allows messages to be sent anonymously through a so-called "mix" node [2]. There, a number of messages with equal length is collected from many distinct senders, repeats are discarded and their sequence is shuffled to obscure the flow through the network. A sender  $S$  first encrypts the message  $M$  with the public key of the receiver  $R$  (end-to-end encryption). Then, it encrypts this message plus the address of  $R$  using the public key of the mix (i.e. sort of link encryption). The message is sent to the mix, which decrypts the received message and forwards it to the recipient  $R$ . A single mix station can ensure the security of the messages. However, if the output of one mix is used as input of a second mix then both would have to conspire to trace any message. Thus, a cascade of mixes increases the security of the system and ensures untraceable traffic flow, provided that not all mixes are insecure or conspire. As we will show in section III, the mix

method imposes high delays on the messages and unscalable security to the user. Therefore we propose a new security architecture that provides scalable security and privacy in packet-oriented networks.

### III. THE NON-DISCLOSURE METHOD (NDM)

#### A. The Basic NDM Approach

For the proposed method we assume a number of independent "Security Agents" (SA) distributed over the whole network and possibly owned by different operators. Each agent  $SA_i$  possesses a pair of asymmetric cryptographic keys  $K_{SA_i}$  and  $K_{SA_i}^{-1}$ , a public and a private key, respectively. We assume a cryptographic system based on the RSA algorithm [3] for the rest of this paper.

Say a sender  $S$  wants to transmit a message  $M$  to a receiver  $R$  without disclosing his own location to  $R$  or any other attacker. This is especially interesting in systems where the address of  $S$  does not match with his real location (e.g. in Mobile IP as discussed in section I).  $S$  now selects a set of security agents ( $SA_1, \dots, SA_N$ ) and sends the message  $M$  over the following route from the sender to the receiver:  $S \rightarrow SA_1 \rightarrow SA_2 \rightarrow \dots \rightarrow SA_N \rightarrow R$ . This route is achieved by encapsulating the message  $N$  times by using the public keys  $K_{SA_1}, \dots, K_{SA_N}$  as follows:

$$M' = K_{SA_1}(SA_2, (K_{SA_2}(SA_3, (\dots (K_{SA_N}(R, M)) \dots))))$$

This resulting packet  $M'$  is sent to the first selected security agent  $SA_1$ , which decrypts the packet using its private key  $K_{SA_1}^{-1}$ , finding the next hop address  $SA_2$  as well as the encrypted message content  $K_{SA_2}(SA_3, (\dots (K_{SA_N}(R, M)) \dots))$ , and forwards this message to  $SA_2$ , and so on.

By this method, a security agent  $SA_i$  only knows the addresses of  $SA_{i-1}$  and  $SA_{i+1}$ , respectively. It does not know the addresses of the other security agents in the routing chain, leave alone the addresses of the sender or recipient. The last security agent  $SA_N$  finally receives the packet  $K_{SA_N}(R, M)$ , deciphers it with his private key  $K_{SA_N}^{-1}$  and delivers the original message  $M$  to the receiver  $R$ .

For an intruder observing the incoming and outgoing messages of a SA it might be possible to make suspicions of mappings between incoming and outgoing message by looking at the message length. By introducing a padding field of varying size this can be omitted: The  $SA_i$  may append a random number of arbitrary padding bytes to the end of the encrypted data and seals the whole data part including padding bytes using the public key of  $SA_{i+1}$ . By this datagram modification the new length hides the relation between incoming and outgoing IP messages. However, all messages observe a twofold encryption.

#### B. Comparison of NDM and Mix-Method

The main advantage of NDM lies in the rudimentary functionality of the involved security agents as compared to Chaum's mixes. However, a single mix, if it is trustworthy and implemented properly, provides sufficient user anonymity and data security, whereas only a cascade of SAs may achieve the same privacy level. Moreover, the anonymity

of a NDM-secured message stronger depends on the choice of the involved stations than the use of mixes does: The trustability of a given routing chain of SAs is mainly governed by the spatial distribution of the security agents, i.e. the protection of location information is attained by the choice of a (untraceable) communication path rather than a secure authorization center. With NDM the user has to be confident that an intruder is not able to simultaneously attack all SAs involved in the communication. If an attacker could listen on all incoming and outgoing links of a SA, not only the correspondences between message lengths of packets (as mentioned above) but also time instances of packet arrivals/departures and other traffic characteristics (like message frequencies) could reveal a sender/recipient combination and thus eliminate the use of the selected SA. Also, replay attacks could be used to confirm an accurate assumption about a communication relation between two peer entities.

While this already seems a rather costly procedure, the choice of a sufficient number of SAs, which are widely scattered in the network, possibly among different providers, almost certainly prevents a successful privacy intervention. Additionally making use of the described padding option, inserting dummy traffic into the packet streams and changing the visited SAs from time to time further decreases the likelihood of intrusions.

Concerning performance aspects of the described security architectures, NDM shows a better delay and throughput behaviour than the mix method. The latter imposes unacceptable delays on messages, since a sufficient number of items has to be collected in a mix to ensure unlinkability between of input and output sequences. This means, that either a large proportion (if not all) of the traffic has to be routed via the mix and thus has to be encrypted, or that a sufficient amount of false traffic has to be generated. The first solution would contradict the demand for personal scalability of the user's security level. Moreover, in both cases messages will observe much higher delays than necessary, and this already leaves out the detours to the mixes. Hence, the usefulness of the method in packet networks is restricted to non-real time messaging applications. For circuit switched networks there is already an extension of the mix method available, which supports real time applications [14].

NDM on the other hand enables a relatively fast packet processing in the visited agents, since messages are not first collected and then forwarded in a reordered sequence. However, the observed packet delays due to detours will be higher as compared to a single mix, depending on the number and distances of the visited SAs. Another paper on this topic provides a detailed analysis on the performance of NDM [5]. As is shown there, powerful protection against traffic analysis can be achieved with a tolerable packet delay overhead and thus support a wider range of applications than the mix method.

## IV. APPLICATION OF NDM TO MOBILE IP

### A. Secure IP in IP Protocol

The IETF internet draft IP Encapsulation within IP [12] specifies a method by which an IP datagram may be encapsulated (carried as payload) within another IP datagram. Encapsulation is suggested as a means to effect readdressing datagrams, particularly to support the Mobile IP specification. The process of encapsulation, sending and decapsulation is referred to as tunneling.

Mobile IP normally uses tunneling only to forward (redirect) a packet reaching the Home Agent (HA) but destined to a mobile node (MN) currently visiting a foreign network. The reverse direction does not use tunneling. This means that the source address is the IP address of the MN and not an address belonging to the foreign network the MN visits. The Mobile IP draft makes the assumption that IP datagrams are routed based on the destination address in the datagram header [13]. Nevertheless, because of security reasons firewall systems and routers often check the source field and reject invalid datagrams and thereby break the above assumption. This can be seen as an additional argument for the usage of Secure IP in IP encapsulation for Mobile IP. It provides tunneling in both directions between the home and foreign network.

To hide the location of a mobile node from the network the registration messages as well as all other packets between MN and HA sent over unsecured networks are tunneled using the Secure IP in IP protocol (SIP). Secure encapsulation using SIP may be performed by the MN itself, the Foreign Agent (FA) or any other node the MN is connected to over a secure communication link (e.g. protected by layer 2 encryption), hiding IP addresses from observers. In Mobile IP route optimization methods are proposed [8] in order to solve the problem of triangle-routing. The problem is that this method is making the current point of attachment of a mobile node even more public in the network. In terms of security concerns, this is not desired as it simplifies traffic analysis as well as location tracking.

### B. Secure IP in IP Protocol Encapsulation

Secure IP in IP is an encapsulation protocol based on the introduced Non Disclosure Method (NDM). Instead of tunneling a packet directly from one node to another (disclosing the endpoints of the tunnel and therefore the communicating hosts), several security agents (SA) in between are addressed, dividing the tunnel into independent subtunnels. A SA — only knowing the addresses of its predecessor and successor — is unable to disclose the entire tunnel's endpoints.

When encapsulating an IP datagram securely within an IP datagram the encapsulating node chooses a sequence of security agents ( $SA_1, \dots, SA_N$ ) the message has to pass (see figure 2). The addresses of the SAs are then successively encapsulated according to NDM as follows: A control bit Padding Valid (PV) and a Virtual Agent Identification (VAID) together with the datagram are encrypted using the public key of the last security agent  $SA_N$  in the

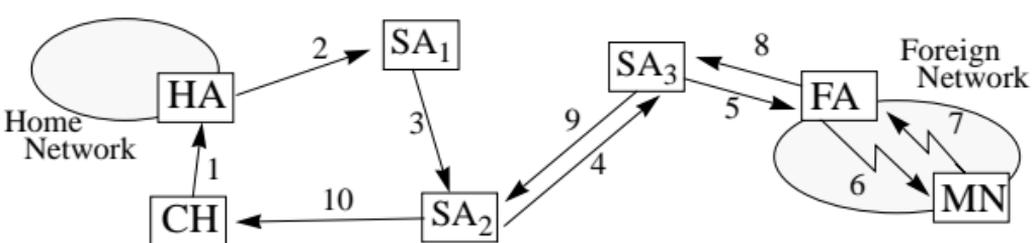


Figure 2: Example route from CH to MN

unchanged and helps the original sender to detect the original sender node as will be explained in section C.

The last security agent  $SA_N$  receiving the datagram strips the last encryption layer and finds the  $VAID_N$  field set to zero. Therefore, the bytes following  $VAID_N$  are seen as a normal IP datagram to the original destination network address that can be found in the encapsulated packet (IP address in the example of figure 1).

### ICMP Port Unreachable Error

The Internet protocol suite uses the ICMP to return error information like ICMP port unreachable errors (p.u.e.) to the sender of a packet, if errors have been detected. There are difficulties occur if port unreachable errors are generated while using Secure IP in IP encapsulation. Firstly, ICMP error messages would be returned only to the previous security agent, i.e. to the start of a tunnel part instead of to the start of the entire tunnel. Secondly, only the first few bytes of the undeliverable IP message are guaranteed to be returned in the ICMP error message.

To provide the sender of a Secure IP in IP message with an ICMP error message it must be successively propagated back to the start of the tunnel. Therefore, each security agent should store information about forwarded secure messages in a local cache database in order to "backward" return ICMP error messages to the previous security agent. A simple and efficient way to access this information is the

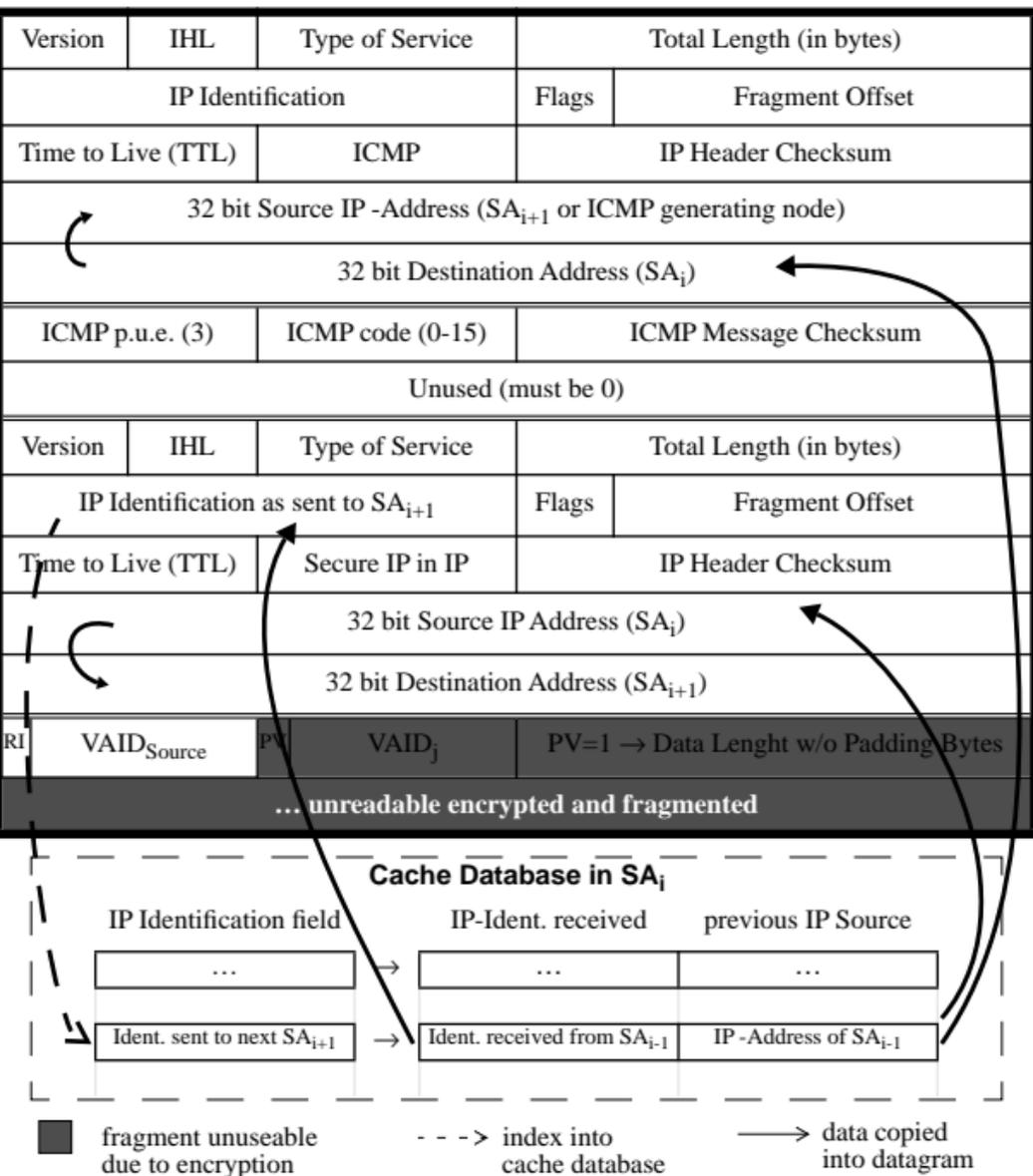


Figure 3: ICMP "backwarding"

ded in the returned ICMP message as an index to the cache database. The obtained information is inserted into the ICMP port unreachable error message and it is sent back to  $SA_{i-1}$ .

The control bit Return ICMP (RI) may be set by the encapsulating host in order to allow the return of ICMP error messages back to the sender. If RI is cleared (RI=0) ICMP error messages may not be returned and cache information