Location Privacy in Mobile IPv6

Risto Mononen and Sandro Grech

Nokia Networks, PL/P.O.Box 301, 00045 Nokia Group,
02600 ESPOO, Finland

Abstract. The Mobile IPv6 protocol includes a route optimization mechanism that improves routing efficiency by informing correspondent nodes about the current care-of address of the mobile node. Mobile node physical location may be associated with its topologically correct IP address. Revealing the mobile node's care-of address can therefore be used to track the mobile with certain accuracy, which compromises the location privacy of the mobile node. We propose correspondent node authentication based on user-friendly identities towards the mobile node to facilitate the decision about whether or not a route optimization procedure should be initiated towards a given correspondent node.

1 Introduction

Location privacy is generally not considered to be a concern in the current fixed Internet since the binding between a user's identity and location is typically either missing or static. There are only limited cases where this does not hold. For example when using Internet banking services, the bank institution may be able to determine whether a user with known identity is logging in from his home, work or university, based on the user's IP address used when logging into the system.

In contrast, due to the inherent dynamic user location, location privacy has been included as one of the design criteria when developing cellular systems. The importance of this feature is reflected by a number of regulations governing the use of location information in various parts of the globe.

Both the Internet and cellular systems are undergoing fundamental technological changes which lead us to reconsider the issue of location privacy in future networks. One notable recent technological development is Mobile IPv6 [1]. Mobile IPv6 enables TCP/IP hosts to transit across IP networks while maintaining any active sessions running on top of IP. Mobile IPv6 includes a procedure to establish a direct shortest-path connection between the two communicating parties. This procedure, however, entails that the mobile host informs its location to the peer communicating entities. Before this procedure is completed, the mobile host's peers are unaware of the mobile host's location. All traffic is routed through the mobile host's home network where packets are redirected towards the mobile host's actual location. Consequently the routing efficiency and packet delay are not optimal.

Mononen R. and Grech S. (2004).
Location Privacy in Mobile IPv6.
In *Proceedings of the 3rd International Workshop on Wireless Information Systems*, pages 34-41
DOI: 10.5220/0002664700340041

We attempt to avoid revealing the mobile host's location to untrusted parties while maintaining an optimized direct route between communicating parties whenever possible. We propose that *the mobile node should strongly authenticate the correspondent node*, and match its identity with a binding update policy database to decide whether or not the mobile node's location should be revealed to the correspondent node.

The rest of the paper is organized as follows. Section 2 gives an overview of the Mobile IPv6 protocol. Section 3 reviews cellular and certificate based authentication technologies, which will form a building block for our proposed mechanism for location privacy in Mobile IPv6. The problem of location privacy is discussed in section 4, which also presents limitations related to location privacy in mobile networks where mobility is managed using Mobile IPv6. Our proposal to overcome this limitation based on correspondent node authentication is presented in section 5. Finally, a discussion with respect to other related work and final conclusions are given in sections 6 and 7, respectively.

2 Mobile IPv6 Overview

Mobile IPv6 solves the IPv6 host mobility problem by associating two IP addresses to each host – a static address for identification (known as *home IP address*), and a dynamic address (known as *care-of address*) used for maintaining reachability as the mobile node moves. The mobile node configures a new care-of address each time it becomes attached to a new network, such that the mobile node always has a topologically correct IP address that can be used for reaching the mobile node. At the same time, the higher layer protocols can keep using the mobile node's home address as a means of identification for the mobile node. The home address topologically corresponds to the mobile node's home network. The home network includes a router known as *home agent* (HA) which includes special functions related to mobility management, most notably the maintenance of soft states that map home addresses to care-of address. The mobile nodes are responsible for updating this state in the home agent. The procedure for doing this in Mobile IPv6 is known as *binding update procedure*. The home agent intercepts packets addressed to the mobile node's home address and diverts them towards the mobile node's care-of address as determined from the home agent's internal state. Outbound packets from the mobile node are delivered to their destination using standard IPv6 routing mechanisms or reverse-tunneled through the home agent.

In order to avoid inefficient routing paths which traverse the home agent in one or both directions, Mobile IPv6 includes the possibility of notifying the care-of address directly to the *correspondent node* such that, subsequently, traffic can be routed directly between the mobile and correspondent node, without traversing the home agent. This is enabled through a route optimization procedure, which essentially includes a binding update sequence from the mobile node to its correspondent node(s). A consequence of route optimization is the exposure of the mobile node's care-of address to its correspondent node. This raises some concerns related to location privacy of the mobile node, and will be analyzed further on in this paper.

3 Authentication

Authentication verifies a claimed identity of a principal. Verification is based on a *secret key that only the principal knows*. The authenticator does not necessarily know the secret key in question, but he must anyhow be able to check that the principal did know it. Symmetric and asymmetric key cryptography based verification schemes are outlined below. Cellular network authentication is given as an example of a symmetric key scheme. Public key certificate based authentication uses asymmetric keys. A memo by the Internet Architecture Board (IAB) [2] summarizes the basic authentication technologies.

3.1 Cellular authentication

A cellular access network authenticates the terminal when it first contacts the network at power-on. The process is almost invisible to the subscriber. Different 2nd and 3rd generation technologies (GSM, CDMA, UMTS) implement slightly different authentication procedures. The outline below is common to all of them.

Cellular network authentication is based on a *shared secret key* in the user's terminal (*user equipment, UE*) and a server (*authentication center, AuC*) in the home network [3]. The AuC generates a random challenge with the secret key and UE calculates response with the same key. The network verifies the response and authorizes the user. The air interface security keys are agreed during the authentication procedure as well.

GSM and 3rd generation terminals store the secret key on a *subscriber identity module* (SIM) smart card inside the UE. SIM never reveals the value of the key. It calculates the response only if the user gives the correct PIN code. The combination of SIM and PIN provides a strong two-factor authentication of the cellular subscribers and devices.

3.2 Certificate authentication

Public key certificate based authentication uses asymmetric key cryptography. In asymmetric key cryptography different keys are used for encryption and decryption. One of the keys is *public*, and associated with an identity in the certificate. The matching *private* key is stored securely in the UE just like the shared secret in the cellular authentication case. Any authenticator can generate a random challenge with the public key, and only the holder of the private key can calculate the correct response. *The certificate* binds the public key with an identity as mentioned above. This is essential in order to ensure that the public key really belongs to the claimed identity.

Certificates are related to two widely used IETF protocols to protect traffic confidentiality and integrity: *IPSec* [4] and *TLS* [5]. Both protocols authenticate the peer entity and establish session keys before encrypted communication can start. *IKE protocol* [6] authenticates the parties for IPSec sessions. TLS handshake protocol is

somewhat simpler and part of the TLS protocol [5]. Both protocols can use identity certificates for authentication.

4 Location Privacy

In the existing cellular networks an attacker may attempt to reveal a mobile user's location from several sources. Broadly the attack categories are:

1. Eavesdropping the user or signaling traffic in the air interface, transmission links or network elements,
2. Unauthorized location queries to the location services that the mobile network provides, and
3. Queries directly to the mobile device or the user.

Several standard data and signaling confidentiality measures are in place to mitigate the eavesdropping attacks (threat 1 above). Location information server requires always end user consent before responding to any location query (threat 2 above). The direct queries (threat 3 above) attempt a call to the victim and deduce the location from the response, e.g. kind of the "alerting" tone or language or IP source address of the "unreachable" response from the network. Typically only very coarse-grained location information can be deduced from the response – only the country can be deduced in the examples above. However, the Mobile IPv6 signaling combined with a "flat" routing hierarchy may reveal more location information to the attacker than is possible with the existing mobile data technologies.

There is a fundamental difference in circuit switching (including virtual circuits) and stateless packet forwarding technologies with regard to location data. The circuit switched voice and data is associated with a label that has only *local* significance and changes at each node. Examples are a PCM timeslot id, ATM virtual circuit id or MPLS label. Packet switched networks forward the messages based on *globally unique* identifier that does not change along the path – the IP destination address. The threat to location privacy stems from the topological correctness of this address, and its relation to the geographic location.

4.1 Location Privacy in Next Generation Mobile Networks

In the GPRS architecture, the GGSN tunnels subscriber traffic to and from the radio access network. The tunnel can be considered a form a circuit that has a role in GPRS mobility management and also hides the terminal location changes from the other Internet nodes beyond the GGSN "access router". A purely packet switched architecture does not deploy tunnels. WLAN access networks are more flat than GPRS since the access router typically resides low in the hierarchy. The subnet addresses of such routers reveal more granular location information to the communicating parties than GPRS subnets do.

Another issue is the trust model of the Internet. The well-known end-to-end argument [7] advocates that functions are better implemented in the application layer, unless they are absolutely necessary for all applications, or for the sake of

performance. End-to-end security means that hosts trust only each other in confidentiality and integrity protection, not the network. The approach is valid for *data* but not for *location confidentiality*. The network inevitably knows the mobile host address in order to route the packets to the correct destination. Almost always the network also knows the user identity. Therefore the network must be trusted for the location data.

The Mobile IPv6 route optimization procedure combined with routing topology information can be used to track down the mobile node's location and movement. Alternatively, a reverse DNS query on the IP address may already provide sufficient location awareness to the correspondent node. Topological information can be readily available in WLAN, for example, by driving around and keeping track of the mapping between allocated IP addresses and the corresponding geographical location.

In order to protect its location privacy, the mobile node can control the sending of the Binding Updates (BUs). The current specification [1] states: "*a mobile node may also choose to keep its topological location private from certain correspondent nodes, and thus need not initiate the correspondent registration*". However, the mobile node does not really have sufficient information for the decision on whether or not to initiate the correspondent binding procedure. An attempt to solve this issue is presented in the next section.

5 Mobile IPv6 Location Privacy Decisions based on Correspondent Node Authentication

We propose *correspondent node authentication* and *registration policy database* to control the correspondent registrations. The authentication verifies the peer identity. The policy states which individual identities or groups the binding updates will be sent to. The subchapters below analyze the possible solutions in more detail.

We assume two communicating users, Alice and Bob, establishing a communication channel. Alice is a mobile node and Bob is either mobile or fixed. In the analysis Alice is deciding whether or not to start the correspondent registration. Bob's identity is among the decision criteria. In general, the criteria should:

1. Be generally available to Alice,
2. Be reliable,
3. Be flexible with the mobile nodes that change IP addresses (mobile Bob),
4. Support understandable privacy policies (non-expert Alice defines the policy),
5. Assume minimal changes to the existing Internet practices and standards, and
6. Assume minimal trust on the network (end-to-end principle).

5.1 Why correspondent node authentication?

Alice and Bob know only each other's IP address when they establish a communication channel. Additionally Alice resolves Bob's DNS name to an IP address before initiating the connection. Thus Bob's DNS name is another identity that Alice may know. E-mail and SIP usernames are other possible choices. Alice

can use any of these identities among the criteria for the correspondent registration decision.

Bob's IP address must always be available to Alice to make communication possible in the first place. It is not reliable information since address spoofing is possible in the Internet. IP address based privacy policy is not flexible since Bob can get the address dynamically from DHCP. Mobile Bob will allocate a transient care-of address, which Alice definitely cannot use as an identity in the policy database. Understandability of IPv6 addresses in the policy database is poor. The addresses are expressed as hexadecimal number separated by colons, e.g. ab16:32:48:64:80:96:112:128 [3]. Network administrators can work with these addresses, but the common end-user configuring his personal preferences cannot.

Bob's DNS name is often, but not always, available to Alice. If Bob typically uses his terminal as a client only, e.g. for browsing web pages, there is no need for him to have a DNS name. If he has DNS name and allocates IP address dynamically from DHCP, the DNS address data must be updated accordingly. Attacks against the DNS servers and caches are possible in the Internet. Consequently, the data cannot be considered reliable. Flexible policies would be possible if the DNS updates became common, frequent and reliable enough. Understandable policies are the benefit of DNS names when compared with plain IPv6 addresses.

Bob's E-mail or SIP username is the most compelling alternative. The username can be made available to Alice with certificates in the IKEv2 initial exchanges. E-mail address is a standard subject name in [8]. The names are reliable since the trusted Certification Authority (CA) has signed them. Flexible and understandable policies are also supported. The username identifies a person and organization instead of a network interface, which is the scope of an IP address. After all, we want to authorize or deny the location information to humans and organizations, not to communication endpoints in the connectivity domain.

The example below shows a policy database Alice might have. The order of the rules is significant – the first matching name triggers the action:

1. Allow BU to <bob@isp.com> (trust Bob, send BU),
2. Deny BU to <eve@mywork.net> (don't reveal location to Bob's ex-wife, no BU),
3. Query BU to <*@mywork.com> (conditionally trust everyone in the company)
4. Deny BU to <*> (default rule, do not trust strangers)

Rule 3, in the above example, may trigger a prompt for end-user decision. Since the authenticated identity is in user-friendly format, the end user shall be capable of making a decision. Based on the end-user's decisions, the policy database may be dynamically updated with new entries.

The IP address, DNS name and username analysis above shows the strength of using *symbolic names* in defining the BU policy rather than plain IP addresses. However, DNS as a technology is not applicable due availability and reliability reasons. It would also bundle the otherwise independent Mobile IPv6 architecture to DNS in an undesirable way.

Both IP address and DNS name based identities rely on the consistent data and configuration in the network. In our proposal an actual IKEv2 challenge – response authentication protocol is run between the endpoints. This is in line with the Internet end-to-end model where the network is not trusted.

5.2 Trust relations

The signed certificates can be used for authentication without online connection to their signer, the CA. However, Alice must trust the CA who signed Bob's certificate, and vice versa. If the two do not use the same CA, there needs to be a chain of cross-certified CAs in place.

If Bob is running a fixed Internet web server, he is likely to have a certificate from a commercial CA like telecom operator. Bob may also be a mobile user, and typically the mobile users have not possessed certificates. Ongoing work in the 3GPP standardization may change this. [8] will specify a fluent way to issue certificates to mobile subscribers. If the majority of the Mobile IPv6 users in the future also have a cellular subscription, the subscriber certificates fit very well with the need to have client certificates for the IKEv2 authentication.

6 Related work

In the context of Mobile IPv6, location privacy mechanisms have been previously discussed in [9] and [10]. In [9], one or more additional layers of hierarchy are added as an extension to the basic Mobile IPv6 mobility management in order to improve its efficiency. Such a hierarchical approach reduces the exposure of location information to third parties. However, in practice, hierarchical mobility management only reduces the granularity of the location information, and this may not be sufficient for most practical location privacy requirements. [10] proposes a solution for location privacy in Mobile IPv6 which involves the introduction of a trusted *Information Translating Proxy* (ITP). ITP hides the location and identity information from other communication participants (including the HA, and access network) and attackers by translating those parameters. Consequently, all mobile node's traffic for which location privacy is required needs to traverse the ITP, effectively compromising the routing efficiency. Besides introducing a new network element, the mechanism requires a new protocol and modification to the Mobile IPv6 operation. Moreover it is unclear who would adopt the role of an ITP provider, in the presented model.

In comparison, in our proposal we assume a trust relationship between the mobile node and its home network, such that the mobile node's location can be safely revealed to its home agent. We re-use the existing TLS and IKE protocols in order to *validate whether a correspondent node is trusted or not*. We leverage the reverse tunneling mode of Mobile IPv6 in order to provide location privacy when the correspondent node is untrusted. Traffic encryption may be used to tackle location privacy from passive on-path eavesdroppers. This hides identity information that may be present in the payload of the packets bearing the mobile node's care-of address. Randomized interface identifiers as described in [11] can be applied when generating the care-of address, in order to avoid user profiling.

7 Conclusions

The current Mobile IPv6 specification does not address location privacy policies properly. Peer IP address and possibly DNS name are the only available identities the mobile node knows when deciding whether to reveal its IP address to a correspondent node, for route optimization purposes. We propose using application layer identities, such as e-mail and SIP usernames and realms, to allow flexible and understandable route optimization policies. End-to-end authentication between the Mobile IPv6 correspondent node and mobile node is strongly recommended to verify the identity that the peer is claiming. IKEv2 authentication has been used as an example of a possible certificate based challenge – response authentication protocol. TLS handshake protocol with client certificates and other possibilities should be studied as well. A benefit in IKEv2 usage is its ability to establish the generic IPSec protection for the rest of the communication between the mobile and correspondent node.

Lack of MN certificates and widespread PKI can be mentioned as shortcomings of the proposal. We believe that the ongoing 3GPP work for the subscriber certificates will bring their easy deployment into the mobile networks and changes the current situation. Several other applications would benefit from the certificates in addition to Mobile IPv6.

References

1. C. Perkins, et al.: “Mobility Support in IPv6”, Internet draft (work in progress), <draft-ietf-mobileip-ipv6-24>, June 2003
2. E. Rescorla: “A Survey of Authentication Mechanisms”, Internet draft (work in progress), <draft-iab-auth-mech-02.txt>, October 2003.
3. 3GPP TS 33.102: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture”.
4. S. Kent, R. Atkinson: “Security Architecture for the Internet Protocol”, RFC 2401, November 1998.
5. T. Dierks, C. Allen: “The TLS Protocol version 1.0”, RFC2246, January 1999.
6. D. Harkins, D. Carrel: “The Internet Key Exchange (IKE)”, RFC 2409, November 1998.
7. Saltzer, D. Reed, and D. Clark: “End-to-end arguments in system design”, ACM Trans. Computer System, November 1984.
8. 3GPP TS 33.221: “Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates”.
9. H. Soliman et al.: “Hierarchical Mobile IPv6 mobility management”, Internet draft (work in progress), <draft-ietf-mipshop-hmipv6-01.txt>, February 2004.
10. SuGil Choi, Kwangjo Kim and Byeonggon Kim, "Practical Solution for Location Privacy in Mobile IPv6", In Proc. of WISA2003, Aug. 25-27.
11. T. Narten et al.: “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, RFC 3041, January 2001.