

Internet Engineering Task Force
Mobility and Multi-homing Privacy
Internet Draft
Expires July 2005

Wassim Haddad
Ericsson
Erik Nordmark
Sun Microsystems
Francis Dupont
Point6
Marcelo Bagnulo
UC3M
Soohong Daniel Park
Samsung Electronics
Basavaraj Patil
Nokia
February 2005

Privacy for Mobile and Multi-homed Nodes:
MoMiPriv Problem Statement
<[draft-haddad-momipriv-problem-statement-01](#)>

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Distribution of this memo is unlimited

Abstract

This memo describes the privacy in mobility and multi-homing problem statement.

Haddad et al.

Expires July 2005

[Page 1]

INTERNET-DRAFT

MoMiPriv Problem Statement

February 2005

Table of Contents

1.	Introduction.....	2
2.	Glossary.....	3
3.	Problem Statement.....	6
3.1.	Location Privacy vs. Privacy.....	6
3.2.	The MAC Layer Problem.....	8
3.3.	The IP Layer Problem.....	9
3.4.	The Interdependency Problem.....	11
4.	Security Considerations.....	11
5.	Acknowledgments.....	11
6.	References.....	12
7.	Authors' Addresses.....	13
	Intellectual Property Statement.....	15
	Disclaimer of Validity.....	15
	Copyright Statement.....	15

[1.](#) Introduction

In the near future, mobility and multi-homing functionalities will coexist in the majority of end hosts, such as terminals, PDAs, etc. For this purpose, Mobile IPv6 [[MIPv6](#)] protocol has been designed to provide a solution for the mobility at the network layer while Multi-homing is still an ongoing work.

MIPv6 does not provide any mechanism to protect the mobile node's privacy when moving across the Internet, while in the multi-homing area, the privacy may well be supported in any potential solution but may probably lack some features. This is mainly due to the fact that the privacy issues are not limited to the IP layer only.

This memo describes the privacy in mobility and multi-homing (momipriv) problem statement based on IPv6 only.

Haddad et al.

Expires July 2005

[Page 2]

INTERNET-DRAFT

MoMiPriv Problem Statement

February 2005

[2.](#) Glossary

Anonymity

Anonymity is a property of network security. An entity "A" in a system has anonymity if no other entity can identify "A", nor is there any link back to "A" that can be used, nor any way to verify that any two anonymous acts are performed by "A".

Anonymity ensures that a user may use a resource or service without disclosing the user's identity.

Anonymity in wireless networks means that neither the mobile node nor its system software shall by default expose any information, that allows any conclusions on the owner or current use of the node.

Consequently, in scenarios where a device and/or network identifiers are used (e.g., MAC address, IP address), neither the communication partner nor any outside attacker should be able to disclose any possible link between the respective identifier and the user's identity.

Pseudonymity

Pseudonymity is a weaker property related to anonymity. It means that one cannot identify an entity, but it may be possible to prove that two pseudonymous acts were performed by the same entity.

Pseudonymity ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

Consequently, a pseudonym is an identifier for a party to a transaction, which is not in the normal course of events, sufficient to associate the transaction with a particular user.

Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it.

Unlinkability

Two events are unlinkable if they are no more and no less related than they are related concerning the a-priori knowledge.

Unlinkability ensures that a user may make use of resources or services without others being able to link these two uses together.

Note that unlinkability is a sufficient condition of anonymity, but it is not a necessary condition.

Privacy

Privacy is a more general term than anonymity. Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.

In wireless telecommunications, privacy addresses especially the protection of the content as well as the context (e.g., time, location, type of service, ...) of a communication event.

Consequently, neither the mobile node nor its system software shall support the creation of user-related usage profiles. Such profiles basically comprise of a correlation of time and location of the node's use, as well as the type and details of the transaction performed.

Privacy can even be achieved by disconnectivity, i.e., not being connected to a network.

MAC Address

A MAC Address is a 48 bits unique value associated with a network adapter. The MAC address uniqueness is by default global. A MAC Address is also known as the device/hardware identifier.

Link

A communication facility or medium over which nodes can communicate at the link layer, such as an Ethernet (simple or bridged). A link is the layer immediately below IP.

IPv6 Address

An IP address is a unique 128-bit IP layer identifier for an interface or a set of interfaces attached to an IP network. An IPv6 address can be unicast, i.e., identifier for a single interface, or anycast, i.e., an identifier for a set

of interfaces, and a packet sent to an anycast address is delivered to only one interface, or multicast, i.e., an identifier for a set of interfaces and a packet sent to a multicast address is delivered to all these interfaces.

Interface Identifier

A number used to identify a node's interface on a link. The interface identifier is the remaining low-order bits in the node's IP address after the subnet prefix.

Basic Service Set (BSS)

A set of stations controlled by a single coordination function.

Extended Service Set (ESS)

A set of one or more interconnected basic service set (BSSs) and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs.

Distribution System (DS)

A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS).

For more literature about the Glossary content, please refer to [\[ANON\]](#), [\[ISO99\]](#), [\[Priv-NG\]](#), [\[Freedom\]](#) and [\[ANON-PRIV\]](#).

[3.](#) Problem Statement

The growing ability to trace a mobile node by an untrusted third party, especially in public access networks, is a direct and serious violation of the mobile user's privacy and can cause serious damage to its personal, social and professional life. Privacy becomes a real concern especially when the mobile node (MN) uses permanent device and/or network identifiers. Unfortunately, the privacy problem is not limited to a single layer and should not be solved independantly on one layer.

Protecting the user's privacy can be achieved, in many scenarios, by providing one or many of the privacy aspects defined above with regards to the mobile node's requirements and/or location. For this purpose, we try in the rest of this document to use the terms defined above, in order to highlight the issues in a more precise way.

It should be noted that this document focuses only on the privacy problem for a mobile and multi-homed node only and does not make any assumption regarding the privacy of a static node, e.g., static correspondent node (CN). In addition, this document assumes that the real IPv6 address is not hidden by default, i.e., any node is always reachable via its real IPv6 address.

The problem statement is divided into three problems. The first two problems are related to the identifiers associated with a mobile device, i.e., the MAC address and the IP address, and the third problem highlights their interdependency. But before delving into these problems, a quick overview on differences between location privacy and privacy is provided.

[3.1.](#) Location Privacy vs. Privacy

Before describing privacy problems related to the IP and the link layer, it seems useful to highlight the differences between the location privacy and privacy, in order to avoid a possible confusion later.

Location privacy is the ability to prevent other parties from learning one's current or past location [[LOPRIPEC](#)]. In order

to get such ability, the mobile node must conceal any relation between its location and the personal identifiable information. Note that in the momipriv context, the mobile node location refers normally to the topological location and not the

geographic one. The latter is provided by other means (e.g., GPS) than an IPv6 address. But it should be noted that it may possible sometimes to deduce the geographical location from the topological one.

However, concealing any relation between the location and the user's identifier(s) does not guarantee that the identifier(s) itself will not be disclosed, since it may be possible to hide the real location alone. But, having at least one user's identifier disclosed may be enough (e.g., if coupled with prior knowledge about few possible whereabouts) for other party to discover the user's current and/or previous location(s).

For example, in a context limited to IP and MAC layers, the only available identifiers and/or locators are the IP and MAC addresses, and only the IP address carries information, which can directly disclose the MN's location (note that mobile IPv6 discloses both the mobile node's home and current locations).

The MAC address alone does not provide any hint regarding the mobile node current/previous location. But if the other party has already established the link between the target and its MAC address and gained knowledge about some of the user's possible current/future whereabouts, then it will be possible to locate and even track the target.

On the other side, it should be noted that the two main privacy aspects, i.e., anonymity and pseudonymity, provide implicitly the location privacy feature by concealing the real user's identifiers regardless of his/her location(s). Actually, in both privacy aspects, real identifiers are replaced by static or dynamic ones, thus making the other party no more able to identify its target even at the correct location, i.e., any past/current location information becomes practically useless for locating and tracking purposes.

[3.2](#). The MAC Layer Problem

The first problem focus on the MAC layer and is raising growing concerns related to the user's privacy, especially with the massive ongoing indoor/outdoor deployment of WLAN technologies.

A mobile device attached to a particular link is uniquely identified on that link by its MAC address, i.e., the device identifier. In addition, the device identifier is disclosed in any packet sent by/to the MN when it reaches that particular link, thus making it a very efficient tool to trace a mobile user in a shared wireless medium access. Similar problems have caused bad press for cellular operators.

For example, a malicious node located in one distributed system (DS) can trace a mobile node via its device identifier while moving in the entire ESS, and learn enough information about the user's activities and whereabouts. Having these information available in the wrong hands, especially with the exact time when they occur, may have bad consequences on the user.

Another concern on the MAC layer, which can also be exploited by an eavesdropper to trace its victim, is the sequence number carried by the frame header. The sequence number is incremented by 1 for each data frame and allows the bad guy to trace its

targeted node, in addition to the MAC address.

In addition, the sequence number allows also the malicious node to keep tracing the MN, if/when the real MAC address is replaced by one or many pseudo-identifier(s) during an ongoing session [[WLAN-IID](#)].

In addition, it should be noted that even if the real MN's device identifier remains undisclosed during all the session(s), it may probably not be enough to provide the unlinkability protection on the MAC layer, between ongoing session(s).

Actually, in a scenario, where the malicious node is located on the link or in the distributed system, replacing the real MAC address with a static pseudo-identifier, i.e., to provide pseudonymity, or with temporary ones, i.e., to provide anonymity, it will always be possible to break the unlinkability protection provided by the MAC layer if the MN's IPv6 address remains unchanged.

Note that in such scenario, even a periodical change of the sequence number won't prevent the eavesdropper from correlating ongoing session(s), pseudo-identifiers and the mobile node.

However, it should be mentioned that replacing the real device identifier with static/dynamic pseudo-identifiers, in order to

provide anonymity/pseudonymity, during an ongoing session(s), raises another critical issue on the MAC layer level, which concerns the uniqueness of these new pseudo-identifier(s).

In fact, any temporary/static identifiers MUST be unique within the Extended Service Set (ESS) and the distributed system (DS).

[3.3](#). The IP Layer Problem

The second problem focus on the IP layer and analyzes the privacy problems related to IPv6 only.

A MN can configure its IPv6 address either from a DHCP server

or by itself. The latter scenario is called the stateless address autoconfiguration [[STAT](#)], and discloses the MN MAC address in the IPv6 address, thus enabling an eavesdropper to easily learn both addresses in this case.

In order to mitigate the privacy concerns raised from using the stateless address auto-configuration [[PRIV-STAT](#)], [PRIVACY] introduced a method allowing to periodically change the MN's interface identifier.

However, being limited to the interface identifier only, such change discloses the real network identifier, which in turn can reveal enough information about the topological location, the user or can even be the exact piece of information needed by the eavesdropper. Another limitation to its efficiency lays in the fact that such change cannot occur during an ongoing session.

While using only a different IPv6 address for each new session may prevent/mitigate the ability to trace a MN on the IP layer level, it remains always possible to trace it through its device identifier(s) on the MAC layer level, i.e., when a malicious node (or another one) is also attached to the same link/DS than its target. Consequently, it will be possible to learn all IPv6 addresses used by the MN by correlating different sessions, thus breaking any unlinkability protection provided at the IP layer.

MIPv6 allows an MN to move across the Internet while ensuring optimal routing (i.e., by using route optimization (RO)) mode and keeping ongoing session(s) alive. Although these two features make the RO mode protocol looks efficient, they disclose the MN's home IPv6 address and its current location, i.e., care-of address (CoA), in each data packet exchanged between the MN and the correspondent node (CN).

Furthermore, each time a MN switches to a new network, it has to send in clear a binding update (BU) message to the CN to

notify it about its new location.

Consequently, MIPv6 RO mode discloses to a malicious node located between the MN and the CN, all data required to identify, locate and trace in real time its mobile target, once it moves outside its home network(s) [Priv-NG].

MIPv6 defines another mode called the bidirectional tunneling (BT), which allows the MN to hide its movements and locations from the CN by sending all data packets through its HA (i.e., encapsulated). In such mode, the CN uses only the MN's home IPv6 address to communicate with the MN.

But if the CN initiates a session with a MN then it has to use the MN's home IPv6 address. In such scenario, if the MN wants to keep its movements hidden from the CN, then it has to switch to the bidirectional tunneling mode.

Consequently, all data packets sent/received by the MN are exchanged through the MN's HA and the MN needs to update only its HA with its location.

Although, the bi-directional tunneling mode allows hiding the MN's care-of address to the CN, it can disclose its real identity, i.e., IPv6 home address, and current location to a malicious node located between the HA and the MN (e.g., by looking to the data packets inner header), unless the HA-MN tunnel is protected by using ESP.

In addition to mobility, the multi-homing feature allows a mobile node to belong to different home networks and to switch between these home networks without interrupting ongoing session(s) [[MULTI](#)].

Although multi-homing can be considered as another aspect of mobility, switching between different home networks, in addition to moving between foreign networks, can disclose to a malicious node well located between the multi-homed MN and the CN, part or all of the MN's home IPv6 addresses, its device identifiers (e.g., when stateless address autoconfiguring is used) and its location(s). Such variety of identifiers can make the malicious eavesdropper's task easier.

For example, a malicious node located between the MN and the CN can start tracing its victim based on prior knowledge of one of its home address or MAC address, and by tracking the BU messages (e.g., the MN is using the RO mode).

After that, the malicious eavesdropper can correlate between different signaling messages and possibly data packets to expand

his knowledge to other victim's home/MAC addresses. Learning new identifiers offer the eavesdropper additional tools to detect and track future movements.

[3.4.](#) The Interdependency Problem

The MAC and IP layers problems described above highlight another concern that needs to be addressed in order to protect the MN's identifiers and/or hiding its locations: any change/update of the IP address and the pseudo-identifier must be performed in a synchronized way.

Otherwise, a change/update at the IP layer only, may allow the eavesdropper to keep tracing the MN via the device identifier and consequently to learn how/when the MN's identifiers are modified on the MAC layer, thus making such change(s) meaningless.

[4.](#) Security Considerations

This document is a problem statement, which describes privacy issues related to a mobile and multi-homed node, and does not introduce security considerations by itself.

However it should be noted that any potential solution for the momipriv problem, which allows using temporary device identifiers, dynamic pseudo-IP addresses and other parameters during an ongoing session should not allow a malicious eavesdropper to learn how nor when these identifiers are updated.

Any potential solution must protect against replaying messages using old identifiers and/or hijacking an ongoing session during an update of the identifiers.

Any potential solution should not allow exploiting any aspect of privacy, in order to gain access to networks.

[5.](#) Acknowledgements

Many Thanks to Hannes Tschofenig for his review and comments on the draft.

[6.](#) References

- [ANON] A. Pfitzmann et al. "Anonymity, Unobservability, Pseudonymity, and Identity Management - A Proposal for Terminology", Draft v0.21, September, 2004.
- [ANON-PRIV] M. Schmidt, "Subscriptionless Mobile Networking: Anonymity and Privacy Aspects within Personal Area Networks", IEEE WCNC 2002.
- [Freedom] A.F. Westin, "Privacy and Freedom", Atheneum Press, New York, USA, 1967.
- [ISO99] ISO IS 15408, 1999, <http://www.commoncriteria.org/>.
- [LOPRIPEC] A. Beresfold, F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2(1):46-55, 2003 IEEE.
- [MIPv6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.

[MULTI] N. Montavont, R. Wakikawa, T. Ernst, T. Noel, C. Ng, "Analysis of Multihoming in Mobile IPv6", [draft-montavont-mobileip-multihoming-pb-statement-03](#), January, 2005.

[PRIV-NG] A. Escudero-Pascual, "Privacy in the Next Generation Internet", December 2002.

[PRIV-STAT] S. Deering, B. Hinden, "Statement on IPv6 Address Privacy", <http://playground.sun.com/pub/ipng/html/specs/ipv6-address-privacy.html> November, 1999.

Haddad et al.

Expires July 2005

[Page 12]

INTERNET-DRAFT

MoMiPriv Problem Statement

February 2005

[Privacy] T. Narten, R. Draves, S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [draft-ietf-ipv6-privacy-addr-v2-02](#), December, 2004.

[STAT] S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [draft-ietf-ipv6-rfc2462bis-07](#), December, 2004.

[WLAN-IID] M. Gruteser, D. Grunwald, "Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis, September 2003", First ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, September 2003.

[6.](#) Authors' Addresses

Wassim Haddad
Ericsson Research

8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
Canada

Phone: +1 514 345 7900
E-Mail: Wassim.Haddad@ericsson.com

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Mountain View, CA
USA

Phone: +1 650 786 2921
Fax: +1 650 786 5896
E-Mail: Erik.Nordmark@sun.com

Francis Dupont
Point6
c/o GET/ENST Bretagne
Campus de Rennes

Haddad et al.

Expires July 2005

[Page 13]

INTERNET-DRAFT

MoMiPriv Problem Statement

February 2005

2, rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

E-Mail: Francis.Dupont@enst-bretagne.fr

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
E-Mail: Marcelo@it.uc3m.es

URI: <http://www.it.uc3m.es/marcelo>

Soohong Daniel Park
Samsung Electronics
Mobile Platform Laboratory, Samsung Electronics
416. Maetan-Dong, Yeongtong-Gu, Suwon
Korea

Phone: +81 31 200 4508
E-Mail: soohong.park@samsung.com

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 894-6709
E-Mail: Basavaraj.Patil@nokia.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any

license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.