Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 15, 2011

W. Haddad
Ericsson
E. Nordmark
Oracle
F. Dupont
ISC
M. Bagnulo
UC3M
B. Patil
Nokia

November 11, 2010

Anonymous Layers Identifiers for Mobile and Multi-homed Nodes: Problem Statement
draft-haddad-alien-problem-statement-04

Abstract

This memo describes the anonymous layers identifiers in mobility and multi-homing problem statement.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on May 15, 2011.

Table of Contents

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 protocol (described in [MIPv6]) 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 anonymous layers identifiers (alien) in mobility and multi-homing problem statement.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [TERM].

3. Glossary

For privacy related terminology, please refer to [PRITERM].

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).

4. 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 alien problem statement is divided into four problems. The first two problems focus on the MAC and IP layers identifiers associated with a mobile device, i.e., MAC and IP addresses, and describe privacy issues resulting from using these identifiers in the context of a mobile and multi-homed environment. The third problem addresses privacy issues resulting from applying security mechanisms, e.g., IP Security (IPsec) and Securing Neighbor Discovery (SeND) while the fourth problem highlights the interdependency between the three problems, as being the main requirement to be considered when designing any potential solution.

But before delving into these problems, a quick overview on differences between location privacy and privacy is provided.

4.1. 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 alien 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 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.

4.2. 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 (SQN) carried by the frame header. The sequence number is incremented by one 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 ongoing 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 within 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).

4.3. 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 (described in [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, [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 parameters required to identify, locate and trace in real time its mobile target, once it moves outside its home network(s) (described first in [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 the IP Encapsulating Security Payload protocol (described in [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) (described in [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 offers the eavesdropper additional tools to detect and track future movements.

4.4. The Security Problem

4.4.1. The IPsec Problem

IP security (IPsec) protocol (described in [IPsec]) provides a set of security services at the IP layer. These security services are provided through the use of two traffic security protocols, i.e., namely the Authentication Header [AH] and ESP, and through the use of

cryptographic key management procedures and protocols, e.g., Internet Key Exchange protocol (described in [IKE]).

A main function of IKE protocol is to establish and maintain security associations (SAs) used by ESP and AH protocols. An SA is always identified by a static 32-bit parameter, i.e., Security Paramater Index (SPI), and possibly IP addresses.

Based on above, an IPsec SPI can be used to trace a particular MN from one place to another, even if its IP address may change (e.g., if [MobIKE] or [SCTP_IPsec] is used). Tracing remains possible even if care is taken to change the MAC address at the same time than the IP address.
Consequently, the IPsec SPI can be an efficient tool to break the unlinkability protection provided by a change(s) of the IP and MAC addresses (even if both addresses change at the same time), and also to learn and link the MN's new pseudo-IDs.

This is particularly problematic for the IKE SPIs, as there is no possibility for efficiently re-negotiating IKE shared secret(s), without revealing the previous SPIs in the process. Note that re-negotiating an IPsec SPI may be done within the protection of the IKE SA, hence hiding the change from eavesdroppers [EPSPR].

4.4.2. The Secure Neighbor Discovery (SeND) Problem

In order to protect against threats related to the IPv6 Neighbor Discovery protocol ([NDP]) as described in [NDPT], the IETF has standardized [SeND] protocol in order to specify security mechanisms for IPv6 ND protocol.

SEND protocol enables a secure neighbor cache discovery and construction by relying on the cryptographically generated addresses technology (described in [CGA]) to provide a proof of address ownership.

CGA technology consists on generating an RSA key pair and configuring an IPv6 address(es) from hashing the derived public key and other parameters. When using SEND protocol, the MN has to sign NDP messages with its CGA private key.

However, it is important to mention that generating an RSA key pair on small devices is a computationally expensive and lenghty procedure, i.e., power consumption is relatively high. Consequently, it is likely that such limitation may force the MN to use only one RSA key pair for a relatively long period of time, e.g., during an ongoing session. A more optimistic scenario would consist on precomputing few key pairs and using them in a random way.

As a result, hiding both the MN's IP and MAC addresses and periodically refreshing the SPI(s) (when they are used) and SQN(s) may not be enough to prevent the malicious eavesdropper from tracing the MN's movements by detecting ts CGA public key(s) sent during the Neighbor Discovery messages exchange, e.g., during a DAD procedure following an IP handoff. Note also that tracing the public key(s) can help the malicious node to link between different pseudo-identifiers at the MAC and IP levels.

4.5. 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 MAC pseudo-identifier, as well as all other static parameter must be performed in a synchronized way.

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

5. 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 alien 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 privacy aspect in order to gain access to networks.

6. Acknowledgements

Soohong Daniel Park and Hannes Tschofenig have contributed to this document. Many thanks to them.

7. References

7.1. Normative References

[TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, BCP , March 1997.

7.2. Informative References

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3792, March 2005.

[EPSPR] Arkko, J., Nikander, P., and M. Naslund, "Enhancing Privacy with Shared Pseudo Random Sequences", Security Proposals, 13rd International Workshop, Cambridge, April 2005.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[IKE] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[IPsec] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[LOPRIPEC] Beresfold, A. and F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2003.

[MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[MULTI] Montavont, N., Wakikawa, R., Ernst, T., Ng, C., and K. Kuladinithi, "Motivations and Scenarios for Using Multiple Interfaces and Global Addresses", Internet Draft, draft-ietf-monami6-multihoming-motivation-scenario-02.txt, July 2007.

[MobIKE] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[NDP] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[NDPT] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[PRITERM] Haddad, W. and E. Nordmark, "Privacy Terminology", Internet Draft, draft-haddad-alien-privacy-terminology-04.txt, June 2008.

[Priv-NG] Escudero-Pascual, A., "Privacy in the Next Generation Internet: Data Protection in the context of the European Union Policy", PhD Dissertation, December 2002.

[Privacy] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[SCTP_IPsec] Bellovin, S., Ioannidis, J., and A. Keromytis, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", RFC 3554, July 2003.

[STAT] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[SeND] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SeND)", RFC 3971, March 2005.

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

Authors' Addresses

Wassim Haddad
Ericsson
300 Holger Way
San Jose, CA 95134
USA

Phone: +1 646 2562030
Email: Wassim.Haddad@ericsson.com

Erik Nordmark
Oracle
17 Network Circle
Menlo Park, CA 94025
USA

Phone: +1 650 786 2921
Email: Erik.Nordmark@oracle.com

Francis Dupont
ISC
Rennes
Bretagne
France

Email: Francis.Dupont@fdupont.fr

Marcelo Bagnulo
UC3M
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
Spain

Phone: +31 91 6249500
Email: Marcelo@it.uc3m.es
URI: http://www.it.uc3m.es

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 8946709
Email: Basavaraj.Patil@nokia.com