Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 10, 2009

W. Haddad
E. Nordmark
Sun Microsystems, Inc.
F. Dupont
ISC
M. Bagnulo
Universidad Carlos III de Madrid
B. Patil
Nokia
H. Tschofenig
Nokia Siemens
March 9, 2009

Anonymous Layers Identifiers (ALIen): Threat Model for Mobile and Multihomed Nodes
draft-haddad-alien-threat-model-03

Status of this Memo

Copyright Notice

Abstract

This memo describes privacy threats related to the MAC and IP layers identifiers in a mobile and multi-homed environment.

Table of Contents

1. Introduction

The ALIen problem statement document [ALIen] introduced new attributes related to the privacy and described critical privacy issues related to providing these attributes on both the IP and MAC layers. In addition, ALIen highlighted the interdependency between privacy issues on the MAC and IP layers and the need to solve them all together.

This memo describes privacy threats and potential attacks related to the MAC and IP layers identifiers in a mobile and multi-homed environment.

2. Terminology

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 [RFC2119].

In addition, it would be useful to describe the following entities involved in defining threats against privacy:

Target

We use the term "target" to specify an entity who's privacy is threatened by an adversary/malicious node.

Adversary/Malicious Node

This term refers to the entity that is trying to violate the privacy of its target.

In addition, this draft uses the terminology described in [ALIen].

3. Threat Model Applied to Privacy

Before listing threats against privacy, we start by describing the privacy threat model, which will be applied on the MAC and IP layers in order to perform our analysis. The locations of adversaries violating privacy must be taken into account when analyzing different threats.

In a mobile environment, the three main threats against privacy are the following:

- Identifying
- Locating

- Tracing

In the ALIen context, a malicious node can identify its target via its device identifier(s), i.e., MAC address and/or its IPv6 address(es). Once the identification procedure is achieved, it becomes by itself a threat against privacy, since a malicious node located in one particular place will be able to claim with certain confidence that its target was present in the same place at a specific time, by just capturing its MAC address.

The next logic step after identifying a target is to locate it with maximum accuracy. The third step consists on tracing the target (possibly in real-time) while it is moving across the Internet.

Performing these three steps allow the malicious node to gradually increase its knowledge about its target by gathering more and more information about it. These information may allow, for example to build a profile of the target and then to launch specific attacks or to misuse the obtained information in other ways (e.g., marketing purposes, statistics, etc). Data gathered may include higher-layer identifiers (e.g., email addresses) or pseudonyms, location information, temporal information, mobility patterns, etc.

In order to access the MAC address of a targeted node in a WLAN, the malicious node needs to be either on the same link or within the distributed system (DS). However, in other scenarios, especially in the ongoing deployment of public outdoor WLAN technologies, more complex attacks involving multiple malicious nodes need to be considered.

Actually, taking a look at today's WLAN deployments in some cities like Chicago and New York [WIGLE] gives a clear picture of the high density of APs already deployed. These examples of today's WLAN

deployment lead to the following conclusions:

- the high density of APs deployed nowadays greatly extends the spatial and temporal coverage of the three main threats against privacy mentioned above.

- the MAC address is becoming easier to detect and thus is causing a growing privacy concern, in particular for mobility.

- o in some existing public areas covered by WLAN technologies, any efficient tracing of a designed target is greatly improved whenever multiple co-operative malicious nodes are deployed in different locations covered by WLAN technologies.

Based on the above, the suggested threat model when applied to the MAC layer should take into consideration the classic scenario, where one malicious node is collecting data on the link/DS and the scenario where many malicious nodes are deployed in different locations, within the WLAN covered area, and performing data collection while collaborating together for identifying, locating and tracking purposes.

4. Threat Model Applied to Privacy on the MAC Layer

We start our analyze by applying the threat model to the MAC layer.

4.1. Threats from Collecting Data

4.1.1. Discovering the Identity Presence

The WLAN technologies discloses the user's device identifier, i.e., the MAC address, in each data frame sent/received by the mobile node (MN) within the distribution system (DS) thus, making the device identifier readable/available to any malicious eavesdropper located on the link or in the same DS.

Based on this observation, collecting data on one particular link/DS, coupled with prior knowledge of the targeted node's MAC address allows the malicious node to check first if its target is located within the covered area or not.

An eavesdropper can perform data collecting via two ways. The first one is by positioning itself on the link/DS and sniffing packets exchanged between the MNs and the APs. The second way consists on deploying rogue access points in some particular areas. The ability to deploy rogue access points requires a missing security protection of the WLAN network.

In WLAN, the targeted MN does not even need to exchange data packets with another node, to disclose its MAC address to a malicious node eavesdropping on the same link than the MN. In fact, the target's MAC address appears in control messages exchanged between the MN and the AP(s) or between different MNs (adhoc mode).

In addition, identifying the target allows the malicious node to learn the target's IPv6 address and the data sequence number.

On the other side, a malicious node collecting data from one particular DS, may also try to conduct an active search for its target within the DS by trying to connect to the target, using the IPv6 address derived from the link local address, according to the stateless address configuration protocol defined in [STAT]. In such scenario, if the targeted node replies to the malicious node's request while being located within the same DS, then its presence will immediately be detected.

A malicious node may also choose and add new targets to its list, based on other criterias, which are learned from collecting data. For example, the frequency, timing and the presence duration of one particular node may encourage the malicious eavsedeopper to learn

more in order to gradually build a profile for that node.

4.1.2. Determining the Location

After identifying its target within a DS, a malicious node may attempt to determine its location. Such step can be performed by different means.

But it should be noted first, that discovering the target's presence on the MAC layer, implicitly maps its geographical location within a specific area. Depending on the network topology and the link layer technology, this area might be quite large or might have a fairly irregular shape. Hence, the malicious node may want to learn the most accurate location of its target.

It is also possible to determine the geographical location of the MN with a certain accuracy at the physical layer. This is done by identifying the Access Point (AP) to which, the MN is currently attached and then trying to determine the geographical location of the corresponding AP.

4.1.2.1. Tracing the Target

After identifying and locating its target, a malicious node located in a particular DS, can use data collecting to trace its target in real time within the entire ESS.

Tracing can be done either via the target's MAC address or its IPv6 address or via the data sequence number carried in each data frame or through combining them.

On the other side, these information allow the malicious node to break the unlinkability protection provided by changing the MAC address, e.g., during a L2 handoff, since it will always be possible to trace the MN by other tools than its MAC address.

4.1.2.2. Threats from Various Malicious Nodes

An efficient way to trace a target within an area covered by wireless link layer technologies is by deploying many malicious nodes within one specific area.

As it has been mentioned above, a malicious node located within a specific DS can trace its target only within the DS. However, there may be scenarios where tracing a particular target needs to go beyond one specific DS boundaries. In addition, the target MN's MAC address

may change many times before the MN leaves the DS. Consequently, even if the new DS is monitored by a malicious eavesdropper, it will

not be possible for him to identify the target anymore.

If the malicious nodes collaborate with each other, it would be possible to keep tracing the target within a specific region. In fact, the main goals behind collaborative tracing is to break the unlinkability protection when provided in an independent way at the MAC and IP layers. In fact, changing the MAC address alone while keeping using the same IP address will always make the target identifiable and traceable through different DSs.

Note that in addition to using the MAC and IP addresses, the sequence number can also be used for tracing purposes.

5. Threat Model Applied to Privacy on the IP Layer

Learning the target's IP address discloses the topological location, which may in turn reveal also geographical location information of the target. For example, location specific extensions to the DNS directory [LOC_DNS] can help to reveal further information about the geographical location of a particular IP address. Tools are also available, e.g., [HEO] that allows everyone to querry this information using a graphical interface. Note that the location information cannot be always correct, for example due to state entries in the DNS, NATed IP addresses, usage of tunnels (e.g., VPN, Mobile IP, etc.).

This information can be used to link the current target's location(s) to the regular one and provide the eavesdropper more information about its target's movements in real time.

5.1. Threats Against Privacy in Mobile IPv6 Protocol

In Mobile IPv6 protocol (described in [MIPv6]), threats against privacy can originate from the correspondent node (CN) and/or from a malicious node(s) located either between the MN and the CN or between the MN and its home agent (HA).

5.1.1. Quick Overview of MIPv6 Protocol

MIPv6 protocol allows a mobile node to switch between different networks, while keeping ongoing session(s) alive. For this purpose, MIPv6 offers two modes to handle the mobility problem. The first mode is the bidirectional tunnelling (BT) mode, which hides the MN's movements from the CN by sending all data packets through the MN's HA. Consequently, the BT mode provides a certain level of location

privacy by hiding the MN's current location from the CN.

The other mode is the route optimization (RO) mode, which allows the MN to keep exchanging data packets on the direct path with the CN, while moving outside its home network. For this purpose, the MN needs to update the CN with its current new location each time it switches to a new network. This is done by sending a binding update (BU) message to the CN to update its binding cache entry (BCE) with the MN's new location, i.e., care-of address (CoA). In addition, the RO mode requires the MN and the CN to insert the MN's home address (HoA) in each data packet exchanged between them.

5.1.2. Threats Related to MIPv6 BT Mode

As mentioned above, the BT mode keeps the CN totally unaware of the MN's movements across the Internet. However, the MN must update its

HA with its new current location each time it switches to a new network, in order to enable the HA to encapsulate data packets to its new location, i.e., new CoA.

In the BT mode, tracing the MN can either be done via the MAC address as described earlier, or by having a malicious node located somewhere between the MN and the HA, and looking into the inner data packet header.

On the other side, the MIPv6 protocol suggests that the tunnel between the MN and the HA can be protected with ESP protocol. In such case, the malicious node won't be able anymore to identify its target (when located between the MN and the HA) thus making the tracing impossible. However, tracing can always be possible at the MAC layer.

5.1.3. Threats Related to MIPv6 RO Mode

The MIPv6 RO mode and all new optimizations, e.g., [OMIPv6], [MIPSec], etc, requires that the MN sends a BU message to update the CN in order to announce its new current location after each IP handover, and to insert the MN's home address in each data packets sent to/from the MN.

Consequently, threats against MN's privacy can emanate from a

malicious CN, which starts by establishing a session with the target, i.e., by using its target's IPv6 HoA, sending it enough data packets and then waiting till its target switches to the RO mode.

But it should be noted that the MN may not decide to switch to the RO mode but keep using instead the BT mode, in order to avoid disclosing its current location to the CN.

On the other side, a malicious node may position itself somewhere on the direct path between the MN and the CN and learn the MN's current location from sniffing the BU message(s) and/or the data packets exchanged between the two entities.

Another possibility is to do the tracing on the MAC address. As mentioned above, this requires the malicious node to be located on the same link/DS than the MN.

The MIPv6 RO mode requires protecting all signalling messages exchanged between the MN and the HA by an ESP tunnel. In such case, a malicious node located between the MN and the HA cannot identify its target.

However, the IETF has recently adopted a new authentication protocol

for MIPv6 [MIPAuth], which allows securing the BU/BA signalling messages exchanged between the HA and the MN by using an authentication option carried in the BU/BA messages.

MIP6_AUTH protocol may have a serious impact on the MN's privacy, since it offers the malicious node a new location, i.e., the path between the targeted MN and its HA, to identify, locate and trace its target. This is in addition to positioning itself on the path between the targeted MN and the CN. It should be noted also that the path between the MN and the HA may be more interesting to use in order to break the MN's privacy, since the MN may try to hide its real identity (and consequently its location) from the CN, as proposed in [MIPLOP] while still using the real IPv6 home address to exchange signalling messages with its HA.

Furthermore, it would also be possible to learn the MN's pseudo-identifier(s) used in exchanging data packets and signalling messages between the MN and the CN on the direct path, by having two malicious

nodes located between the MN and the HA and between the MN and the CN and collaborating together.

6. Threat Model Applied to a Static Multi-homed Node

A multi-homed node can be described as being attached to more than one Internet Service Provider (ISP). Consequently, the multiple addresses available to a multi-homed node are pre-defined and known in advance in most of the cases.

The main goals behind providing the multi-homing feature are to allow the multi-homed node to use multiple attachments in parallel and the ability to switch between these different attachments during an ongoing session(s), e.g., in case of a failure.

For these purposes, the SHIM6 WG specified a proposal to address multi-homing issues, based on using the Hash Based Addresses (described in [HBA]) and the SHIM6 protocol (described in [SHIM6]).

The HBA technology offers a new mechanism to provide a secure binding between multiple addresses with different prefixes available to a host within a multihomed site. This is achieved by generating the interface identifiers of the addresses of a host as hashes of the available prefixes and a random number. Then, the multiple addresses are generated by prepending the different prefixes to the generated interface identifiers. The result is a set of addresses that are inherently bound. In addition, the HBA technology allows the CN to verify if two HBA addresses belong to the same HBA set.

The SHIM6 protocol aims to eliminate any impact on upper layer protocols by ensuring that they can keep operating unmodified in a multi-homed environment while still seeing a stable IPv6 address.

For a static multi-homed, the main privacy concern are the ability to identify the multi-homed node by an untrusted party and to discover its available addresses. The untrusted party can be the CN itself or a third party located somewhere between the multi-homed node and the CN.

6.1. Threats againt Privacy on the MAC Layer

A malicious node can identify the targeted multi-homed node via its MAC address. The ability to identify the target at the MAC layer allows the malicious node to learn part or all available locators used by the targeted node. However, it should be noted that for a static target, a successful identification of the MAC address may probably require more precise information concerning the geographical location of the target.

6.2. Threats against Privacy on the IP Layer

In a multi-homed environment, threats against privacy on the IP layer can emanate from the CN itself, in an attempt to learn part/all

multi-homed node's available locators.

For example, a malicious CN can use one pre-identified locator belonging to its target, to establish a session with the target. After that, the CN can try to push its target to switch (i.e., disclose) to new locator(s) by stopping replying to packets sent with the initial address, i.e., pretending a failure. In such scenario, and in order to avoid interrupting ongoing session, the targeted node may decide to switch to another (or more) locator(s), depending on the CN willingness to re-start sending packets to the new locator.

On the other side, an untrusted third party located near its target (e.g., based on prior knowledge of one of the target's locator) or one particular CN, can correlate between different locators used by the targeted node by eavesdropping on packets exchanged between the two entities.

Depending on the final solution adopted, the attacker can also sniff context establishment packets that will probably contain some or all the locators available to the multi-homed node.

7. Security Considerations

This document aims to formalize a privacy threat model for the MAC and IP layers and does not suggest any solutions to counter these threats. Based on that, the suggested threat model does not add nor amplify any existing attacks against the mobile or multi-homed node.

8. IANA Considerations

This document has no IANA considerations.

9. References

9.1. Normative References

[MIPAuth] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

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

[OMIPv6] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, May 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

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

9.2. Informative References

[ALIen] Haddad, W., Nordmark, E., Dupont, F., Bagnulo, M., and B. Patil, "Anonymous Layers Identifiers for Mobile and Multi-homed Nodes: Problem Statement", Internet Draft, draft-haddad-alien-problem-statement-02.txt, October 2007.

[HBA] Bagnulo, M., "Hash Based Addresses (HBA)", Internet Draft, draft-ietf-shim6-hba-05.txt, December 2007.

[HEO] "High Earth Orbit", February 2005.

[LOC_DNS] Davis, C., Vixie, P., Goodwin, T., and I. Dickinson, "A Means for Expressing Location Information in the Domain Name System", RFC 1876, January 1996.

[MIPLOP] Montenegro, G., Castelluccia, C., and F. Dupont, "A Simple Privacy Extension for Mobile IPv6", Mobile and Wireless Communication Networks", IEEE MCWN, October 2004.

[MIPSec] Dupont, F. and J-M. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", Internet Draft, draft-ietf-mip6-cn-ipsec-07.txt, Februray 2008.

[SHIM6] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", Internet Draft, draft-ietf-shim6-proto-10.txt, February 2008.

[WIGLE] "Wireless Geographic Logging Engine, http://wigle.net/gps/gps/Map/", 2006.

Authors' Addresses

Wassim Haddad
USA

Phone: +1 6462568041
Email: wmhaddad@gmail.com

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

Email: Erik.Nordmark@sun.com

Francis Dupont

ISC
Rennes
France

Email: Francis.Dupont@fdupont.fr

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

Email: Marcelo@it.uc3m.es

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, Tx 75039
USA

Email: Basavaraj.Patil@nsn.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Email: Hannes.Tschofenig@nsn.com