MIP6 Working Group
INTERNET DRAFT
Informational
23 October 2006

Rajeev Koodli
Nokia Research Center

IP Address Location Privacy and Mobile IPv6: Problem Statement
draft-ietf-mip6-location-privacy-ps-04.txt

This document is a submission of the IETF MIP6 WG. Comments should be directed to the MIP6 WG mailing list, mip6@ietf.org.

Abstract

In this document, we discuss Location Privacy as applicable to Mobile IPv6. We document the concerns arising from revealing Home Address to an on-looker and from disclosing Care of Address to a correspondent.

Contents

1. Introduction

The problems of location privacy, and privacy when using IP for communication have become important. IP privacy is broadly concerned with protecting user communication from unwittingly revealing information that could be used to analyze and gather sensitive user data. Examples include gathering data at certain vantage points, collecting information related to specific traffic, and monitoring (perhaps) certain populations of users for activity during specific times of the day, etc. In this document, we refer to this as the "profiling" problem.

Location privacy is concerned with the problem of revealing roaming, which we define here as the process of a Mobile Node moving from one network to another with or without on-going sessions. A constant identifier with global scope can reveal roaming. Such a global scope identifier could be a device identifier or a user identifier. Often, a binding between these two identifiers is also available, e.g., through DNS. The location privacy problem is particularly applicable to Mobile IP where the Home Address on a visited network can reveal device roaming and, together with a user identifier (such as a SIP URI), can reveal user roaming. Even when the binding between a user identifier and the Home Address is unavailable, freely available tools on the Internet can map the Home Address to the owner of the Home Prefix, which can reveal that a user from a particular ISP has roamed. So, the location privacy problem is a subset of the profiling problem in which revealing a globally visible identifier compromises a user's location privacy. When location privacy is compromised, it could lead to more targetted profiling.

Furthermore, a user may not wish to reveal roaming to correspondent(s). In Mobile IP, this translates to the use of Care of Address. As with Home Address, the Care of Address can also reveal the topological location of the Mobile Node.

In this document, the concerns arising from the use of a globally visible identifier, such as a Home Address, when roaming are described. Similarly, the concerns from revealing a Care of Address to a correspondent are also outlined. The solutions to these problems are meant to be specified in a separate document.

This document is only concerned with IP Address Location Privacy in the context of Mobile IPv6. It does not address the overall privacy problem. For instance, it does not address privacy issues related to MAC addresses or the relationship of IP and MAC addresses [1].

2. Problem Definition

2.1. Disclosing the Care of Address to the Correspondent Node

When a Mobile IP MN roams from its home network to a visited network or from one visited network to another, use of Care of Address in communication with a correspondent reveals that the MN has roamed.

This assumes that the correspondent is able to associate the CoA to HoA, for instance by inspecting the Binding Cache Entry. The HoA itself is assumed to have been obtained by whatever means (e.g., through DNS lookup).

2.2. Revealing the Home Address to On-lookers

When a Mobile IP MN roams from its home network to a visited network or from one visited network to another, use of Home Address in communication reveals to an on-looker that the MN has roamed. When a binding of Home Address to a user identifier (such as a SIP URI or NAI) is available, the Home Address can be used to also determine that the user has roamed. This problem is independent of whether the MN uses Care of Address to communicate directly with the correspondent (i.e., uses route optimization), or the MN communicates via the Home Agent (i.e., uses reverse tunneling).

Location privacy may be compromised if an on-looker is present on the MN - HA path (when bidirectional tunneling is used), or when the on-looker is present on the MN and CN path (when route optimization is used).

2.3. Problem Scope

With existing Mobile IPv6 solutions, there is some protection against location privacy. If a Mobile Node uses reverse tunneling with ESP encryption, then the HoA is not revealed on the MN - HA path. So, eavesdroppers on the MN - HA path cannot determine roaming. They could, however, still profile fields in the ESP header; however, this problem is not specific to Mobile IPv6 location privacy.

When a MN uses reverse tunneling (regardless of ESP encryption), the correspondent does not have access to the CoA. Hence, it cannot determine that the MN has roamed.

Hence, the location privacy problem is particularly applicable when Mobile IPv6 route optimization is used or when reverse tunneling is used without protecting the inner IP packet containing the HoA.

3. Problem Illustration

This section is intended to provide an illustration of the problem defined in the previous section.

Consider a Mobile Node at its home network. Whenever it is involved in IP communication, its correspondents can see an IP address valid on the home network. Elaborating further, the users involved in peer - peer communication are likely to see a user-friendly identifier such as a SIP URI, and the communication end-points in the IP stack will see IP addresses. Users uninterested in or unaware of IP communication details will not see any difference when the MN acquires a new IP address. Of course any user can ``tcpdump'' or

``ethereal'' a session, capture IP packets and map the MN's IP address to an approximate geo-location. This mapping may reveal the "home location" of a user, but a correspondent cannot ascertain whether the user has actually roamed or not. Assessing the physical location based on IP addresses has some similarities to assessing the geographical location based on the area-code of a telephone number. The granularity of the physical area corresponding to an IP address can vary depending on how sophisticated the available tools are, how often an ISP conducts its network re-numbering, etc. And, an IP address cannot also guarantee that a peer is at a certain geographic area due to technologies such as VPN and tunneling.

When the MN roams to another network, the location privacy problem consists of two parts: revealing information to its correspondents and to on-lookers.

With its correspondents, the MN can either communicate directly or reverse tunnel its packets through the Home Agent. Using reverse tunneling does not reveal the new IP address of the MN, although end-to-end delay may vary depending on the particular scenario. With those correspondents with which it can disclose its new IP address ``on the wire'', the MN has the option of using route-optimized communication. The transport protocol still sees the Home Address with route optimization. Unless the correspondent runs some packet capturing utility, the user cannot see which mode (reverse tunneling or route optimization) is being used, but knows that it is communicating with the same peer whose URI it knows. This is similar to conversing with a roaming cellphone user whose phone number, like the URI, remains unchanged.

Regardless of whether the MN uses route optimization or reverse tunneling (without ESP encryption), its Home Address is revealed in data packets. When equipped with an ability to inspect packets ``on the wire'', an on-looker on the MN - HA path can determine that the MN has roamed and could possibly also determine that the user has roamed. This could compromise the location privacy even if the MN took steps to hide its roaming information from a correspondent.

The above description is valid regardless of whether a Home Address is statically allocated or is dynamically allocated. In either case, the mapping of IP address to geo-location will most likely yield results with the same level of granularity. With the freely available tools on the Internet, this granularity is the physical address of the ISP or the organization which registers ownership of

a prefix chunk. Since an ISP or an organization is not, rightly, required to provide a blue-print of its subnets, the granularity remains fairly coarse for a mobile wireless network. However, sophisticated attackers might be able to conduct site mapping and obtain more fine-grained subnet information.

A compromise in location privacy could lead to more targetted profiling of user data. An eavesdropper may specifically track the traffic containing the Home Address, and monitor the movement of the Mobile Node with changing Care of Address. The profiling problem is not specific to Mobile IPv6, but could be triggered by a compromise in location privacy due to revealing the Home Address.
A correspondent may take advantage of the knowledge that a user has roamed when Care of Address is revealed, and modulate actions based on such a knowledge. Such an information could cause concern to a mobile user especially when the correspondent turns out be untrustworthy.

Applying existing techniques to thwart profiling may have implications to Mobile IPv6 signaling performance. For instance, changing the Care of Address often would cause additional Return Routability and binding management signaling. And, changing the Home Address often has implications on IPsec security association management. Solutions should be careful in considering the cost of change of either CoA or HoA on signaling. For instance, changing the Care of Address often would cause additional Return Routability and binding management signaling. And, changing the Home Address often has implications on IPsec security association management. These issues need to be addressed in the solutions These issues should be addressed in the solutions.

When roaming, a MN may treat its home network nodes as any other correspondents. Reverse tunneling is perhaps sufficient for home network communication, since route-optimized communication will traverse the identical path. Hence, a MN can avoid revealing its Care of Address to its home network correspondents simply by using reverse tunneling. The Proxy Neighbor Advertisements from the Home Agent could serve as hints to the home network nodes that the Mobile Node is away. However, they won't be able to know the Mobile Node's current point of attachment unless the MN uses route optimization with them.

4. Conclusion

In this document, we have discussed the location privacy problem as applicable to Mobile IPv6. The problem can be summarized as follows: disclosing Care of Address to a correspondent and revealing Home Address to an on-looker can compromise the location privacy of a Mobile Node, and hence that of a user. We have seen that

bidirectional tunneling allows a MN to protect its CoA to the CN. And, ESP encryption of inner IP packet allows the MN to protect its HoA from the on-lookers on the MN - HA path.

However, with route optimization, the MN will reveal its CoA to the CN. Moreover, route optimization causes the HoA to be revealed to on-lookers in the data packets as well as in Mobile IPv6 signaling messages. The solutions to this problem are expected to be protocol specifications assuming the existing Mobile IPv6 functional entities, namely, the Mobile Node, its Home Agent and the Correspondent Node.

5. IANA Considerations

There are no IANA considerations introduced by this draft.

6. Security Considerations

This document discusses location privacy because of IP mobility. Solutions to provide location privacy, especially any signaling over the Internet, must be secure in order to be effective. Individual solutions must describe the security implications.

7. Acknowledgment

Thanks to James Kempf, Qiu Ying and Sam Xia for the review and feedback. Thanks to Jari Arkko and Kilian Weniger for the last call review and for suggesting improvements and text.

Informative References

[1] W. Haddad and et al. Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement (work in progress). Internet Draft, Internet Engineering Task Force, October 2004.

[2] J. Polk, J. Schnizlein, and M. Linsner. DHCP Option for Coordinate-based Location Configuration Information. Request for Comments 3825, Internet Engineering Task Force, July 2004.

8. Author's Address

Rajeev Koodli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043 USA
Phone: +1 650 625 2359
Fax: +1 650 625 2502
E-Mail: Rajeev.Koodli@nokia.com

A. Background

The location privacy topic is broad and often has different connotations. It also spans multiple layers in the OSI reference model. Besides, there are attributes beyond an IP address alone that can reveal hints about location. For instance, even if a correspondent is communicating with the same end-point it is used to, the ``time of the day'' attribute can reveal a hint to the user. Some roaming cellphone users may have noticed that their SMS messages carry a timestamp of their ``home network'' timezone (for location privacy or otherwise) which can reveal that the user is in a different timezone when messages are sent during ``normal'' time of the day. Furthermore, tools exist on the Internet which can map an IP address to the physical address of an ISP or the organization which owns the prefix chunk. Taking this to another step, with in-built GPS receivers on IP hosts, applications can be devised to map geo-locations to IP network information. Even without GPS receivers, geo-location can also be obtained in environments where [Geopriv] is supported, for instance as a DHCP option [2].

In summary, a user's physical location can be determined or guessed with some certainty and with varying levels of granularity by different means even though IP addresses themselves do not inherently provide any geo-location information. It is perhaps useful to bear this broad scope in mind as the problem of IP address location privacy in the presence of IP Mobility is addressed.

Intellectual Property Statement

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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.