Distributed Mobility Management [dmm]
Internet-Draft
Expires: April 30, 2015

C. Perkins
Futurewei
V. Devarapalli
Vasona Networks

October 27, 2014

MN Identifier Types for RFC 4283 Mobile Node Identifier Option
draft-perkins-dmm-4283mnids-01.txt

Abstract

Additional Identifier Types are proposed for use with the Mobile Node Identifier Option for MIPv6 (RFC 4283).

Table of Contents

1. Introduction

The Mobile Node Identifier Option for MIPv6 [RFC4283] has proved to be a popular design tool for providing identifiers for mobile nodes during authentication procedures with AAA protocols such as Diameter [RFC3588]. To date, only a single type of identifier has been specified, namely the MN NAI. Other types of identifiers are in common use, and even referenced in RFC 4283. In this document, we propose adding some basic types that are commonly in use in various telecommunications standards, including the IMSI, P-TMSI, IMEI, GUTI, and IEEE MAC-layer addresses. In addition, we include the IPv6 address itself as a legitimate mobile node identifier.

2. New Mobile Node Identifier Types

The following types of identifiers are commonly used to identify mobile nodes. For each type, references are provided with full details on the format of the type of identifer.

EPC supports several encoding systems or schemes including

- o RFID-GID (Global Identifier),
- o RFID-SGTIN (Serialized Global Trade Item Number),
- o RFID-SSCC (Serial Shipping Container),
- o RFID-GLN (Global Location Number),
- o RFID-GRAI (Global Returnable Asset Identifier),
- o RFID-DOD (Department of Defense) and
- o RFID-GIAI (Global Individual Asset Identifier).

For each RFID scheme except GID, there are two variations: a 64-bit scheme (for example, GLN-64) and a 96-bit scheme (GLN-96). GID has only a 96-bit scheme. Within each scheme, an EPC identifier can be represented in a binary form or other forms such as URI.

The following list includes the above RFID types as well as various other common identifiers and several different types of DUIDs.

- o IPv6 Address [RFC2373]
- o IMSI [ThreeGPP-IDS]
- o P-TMSI [ThreeGPP-IDS]
- o GUTI [ThreeGPP-IDS]
- o EUI-48 address [IEEE802]
- o EUI-64 address [IEEE802]
- o DUID-LLT [RFC3315]
- o DUID-EN [RFC3315]
- o DUID-LL [RFC3315]
- o DUID-UUID [RFC6355]
- o 12-15 reserved
- o 16 reserved
- o RFID-SGTIN-64 [EPC-Tag-Data]
- o RFID-SSCC-64 [EPC-Tag-Data]
- o RFID-GLN-64 [EPC-Tag-Data]
- o RFID-GRAI-64 [EPC-Tag-Data]
- o RFID-DOD-64 [RFID-DoD-96]
- o RFID-GIAI-64 [EPC-Tag-Data]
- o 23 reserved
- o RFID-GID-96 [EPC-Tag-Data]
- o RFID-SGTIN-96 [EPC-Tag-Data]
- o RFID-SSCC-96 [EPC-Tag-Data]
- o RFID-GLN-96 [EPC-Tag-Data]
- o RFID-GRAI-96 [EPC-Tag-Data]
- o RFID-DOD-96 [RFID-DoD-96]
- o RFID-GIAI-96 [EPC-Tag-Data]
- o 31 reserved
- o RFID-GID-URI [EPC-Tag-Data]
- o RFID-SGTIN-URI [EPC-Tag-Data]
- o RFID-SSCC-URI [EPC-Tag-Data]
- o RFID-GLN-URI [EPC-Tag-Data]
- o RFID-GRAI-URI [EPC-Tag-Data]
- o RFID-DOD-URI [RFID-DoD-96]
- o RFID-GIAI-URI [EPC-Tag-Data]
- o 39-255 reserved

3. Security Considerations

This document does not introduce any security mechanisms, and does not have any impact on existing security mechanisms. Insofar as the selection of a security association may be dependent on the exact form of a mobile node identifier, additional specification may be necessary when the new identifier types are employed with the general AAA mechanisms for mobile node authorizations.

Some identifiers (e.g., IMSI) are considered to be private information. If used in the MNID extension as defined in this document, the packet including the MNID extension should be encrypted so that personal information or trackable identifiers would not be inadvertently disclosed to passive observers. Moreover, MNIDs containing sensitive identifiers might only be used for signaling during initial network entry. Subsequent binding update exchanges would then rely on a temporary identifier allocated during the initial network entry.

4. IANA Considerations

The new mobile node identifier types defined in the document should be assigned values from the "Mobile Node Identifier Option Subtypes" registry. The following values should be assigned.

New Mobile Node Identifier Types

Identifier Type	Identifier Type Number
IPv6 Address	2
IMSI	3
P-TMSI	4
EUI-48 address	5
EUI-64 address	6
GUTI	7
DUID-LLT	8
DUID-EN	9
DUID-LL	10
DUID-UUID	11
	12-15 reserved
	16 reserved
RFID-SGTIN-64	17
RFID-SSCC-64	18
RFID-GLN-64	19
RFID-GRAI-64	20
RFID-DOD-64	21
RFID-GIAI-64	22
	23 reserved
RFID-GID-96	24
RFID-SGTIN-96	25
RFID-SSCC-96	26
RFID-GLN-96	27
RFID-GRAI-96	28
RFID-DOD-96	29
RFID-GIAI-96	30
	31 reserved
RFID-GID-URI	32
RFID-SGTIN-URI	33
RFID-SSCC-URI	34
RFID-GLN-URI	35
RFID-GRAI-URI	36
RFID-DOD-URI	37
RFID-GIAI-URI	38
	39-255 reserved

Table 1

See Section 2 for details about the identifer types.

5. References

5.1. Normative References

[RFC2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, August 2011.

5.2. Informative References

[EPC-Tag-Data] EPCglobal Inc., , "EPC(TM) Generation 1 Tag Data Standards Version 1.1 Rev.1.27 http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_1_rev_1_27-standard-20050510.pdf", January 2005.

[IEEE802] IEEE, , "IEEE Std 802: IEEE Standards for Local and Metropolitan Networks: Overview and Architecture", 2001.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFID-DoD-96] Department of Defense, , "United States Department of Defense Suppliers Passive RFID Information Guide (Version 15.0)", January 2010.

[ThreeGPP-IDS]
3rd Generation Partnership Project, , "3GPP Technical Specification 23.003 V8.4.0: Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 8)", March 2009.

Authors' Addresses

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-4586
Email: charliep@computer.org

Vijay Devarapalli
Vasona Networks
2900 Lakeside Drive, Suite 180
Santa Clara, CA 95054
USA

Cisco Networks
October 26, 2014

Privacy considerations for DMM
draft-perkins-dmm-privacy-00.txt

Abstract

Recent events have emphasized the importance of privacy in protocol design. This document describes ways in which DMM protocol designs and DMM networks can reduce certain threats to privacy.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

There have been many recent disclosures about breaches of privacy, and the all-too-frequent news stories about identity theft, credit card services infiltrated, and other serious threats. An extensive IAB discussion about the nature of such breaches is available [RFC6462].

Within the IETF, there has been a greatly increased awareness of how to mitigate these threats by improved protocol design [RFC6973]. One major danger is the dissemination of long-lived identifiers as part of protocol transactions. When a long-lived identifier can be observed in such transactions with disparate applications and servers, a history can be constructed about the person associated with that long-lived identier. Remarkably accurate predications can then be made about the future behavior of that person -- a clear threat to privacy. Notably, such predictions are not at all illegal, and yet most people would consider the ability to make such predictions as an unwanted outcome of using IETF protocols. Similarly, knowledge about the recent history of a person as inferred by tracking a long-lived identifier can provide strong hints about how to analyze the earlier actions (including personal interactions) of that person.

This document details the mechanisms as currently understood within mobility management protocols in order to better avoid perpetuating potential threats to privacy within DMM. As a general rule, trackable information in protocol messages should be avoided as much as possible [RFC4882].

The following mechanisms are discussed.

- o Recommend implementation of pseudo-home address feature [RFC5726].
- o Source IPv6 address for data packets could be used only for the lifetime of the application used for that address
- o MPTCP may be useful for additional protection against traffic analysis
- o MNID may contain confidential information. Packets in which the MNID extension contains a confidential identifer should be encrypted.
- o MAC randomization, recent Apple announcement

2. Pseudo-home Address

Recommend consideration of using the pseudo-home address feature from RFC 5726[RFC5726]. This has the effect of reducing or eliminating the ability to track the movement events related to a mobile node, which otherwise might be visible to snooping devices located anywhere between the mobile node and home agent.

3. Source IPv6 Address Utilization

Source IPv6 address for data packets could be used only for the lifetime of the application used for that address. For this purpose, each new address can be generated as detailed in [RFC4941].

4. MPTCP

MPTCP [RFC6824] can be used for additional protection against traffic analysis. This can be done by spreading traffic over several associated TCP endpoints, either randomly, or as chosen to emulate traffic patterns for unrelated applications.

5. MNID

MNID [RFC4283] may contain confidential information. Control packets in which the MNID extension contains a confidential identifer should be encrypted. Alternatively, the MN-ID could be generated based on CUI (Chargeable user identity), or some other temporary identifier. In that way, the access network would never have access to the real MN-ID.

6. MAC Randomization

While not under the jurisdiction of the IETF, MAC addresses are often included within IETF protocols. For the purposes of better protecting privacy, there has been much recent discussion about randomization of MAC addresses. As one example, see the recent announcement about Randomized Wi-Fi addresses by Apple Computers [apple-privacy].

Various protocols derived from Mobile IP are designed using certain assumptions related to the use of same MAC address. For example, LMA looks up a MN session using the MN's MAC address. This breaks when the MAC address changes. It is recommended that mobility management protocols reduce or eliminate dependence on MAC addresses. Some specific suggestions include the following:

- o Require the MN to present a new MAC address in each access attach.
- o Allow MN to present multiple MAC addresses during a single attach.
- o Handover keys and other key material should be able to deal with MAC address changes.

7. Non-issues

There are many cases where nonces or cookies are used for temporary use during control signal sequences -- for instance nonces as used with Mobile IP route optimization [RFC6275]. Insofar as these fields are used only temporarily, they are not often useful for tracking user movements. Even so, when the same value is used for a request and returned in a response, a small bit of information is leaked about the status of a protocol transaction. This may not be important, but if so can be averted by encryption.

8. Security Considerations

This document is entirely concerned with raising important security considerations, but does not specify any new protocol that may affect existing security designs.

9. IANA Considerations

This document does not suggest any IANA actions.

10. References

10.1. Normative References

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[RFC4882] Koodli, R., "IP Address Location Privacy and Mobile IPv6: Problem Statement", RFC 4882, May 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC5726] Qiu, Y., Zhao, F., and R. Koodli, "Mobile IPv6 Location Privacy Solutions", RFC 5726, February 2010.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6462] Cooper, A., "Report from the Internet Privacy Workshop", RFC 6462, January 2012.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

10.2. Informative References

[apple-privacy]
Apple Computer, , "Randomized Wi-Fi Addresses", 2014, <https://www.apple.com/privacy/privacy-built-in/>.

Authors' Addresses

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-4586
Email: charliep@computer.org

Sri Gundavelli
Cisco Networks
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com