Network Working Group S. Jiang
Internet Draft X. Xu
Intended status: Informational D. Zhang
Expires: November 5, 2010 Huawei Technologies Co., Ltd
T. Chen
CNNIC
May 5, 2010

Hierarchical Host Identity Tag Architecture
draft-jiang-hiprg-hhit-arch-04.txt

Abstract

The current flat-structured Host Identity Tag architecture has various problems and limitation. Hence, a hierarchical HIT architecture that is compatible with the flat-structured HIT architecture is introduced in the document. This architecture and the process of HIT generation ensure the global uniqueness of HITs. This architecture also enables the multiple Host Identity Protocol administrative domains, solves the deployment problem of current flat-structured HIT architecture. It also enhances the scalability and resolution efficiency of the mapping system from HIT to IP or FQDN.

Table of Contents

1. Introduction

This document analyzes the problems and limitation of the current flat-structured Host Identity Tag (HIT, [RFC4423]) architecture in the Host Identity Protocol (HIP, [RFC5201]). The document specifies a hierarchical HIT architecture, which splits a HIT into two parts: a HIP Administrative Domain (AD) ID and a local host ID. The proposed hierarchical HIT architecture is also compatible with the flat-structured HIT architecture. The format of HIT and the detail process of HIT generation are defined. This architecture and the process of HIT generation ensure the global uniqueness of HITs. This architecture also enables the multiple HIP administrative domains, solves the deployment problem of current flat-structured HIT architecture. The aggregation of HITs in this architecture also enhances the scalability and resolution efficiency of the mapping system from HIT to IP or FQDN.

2. Analysis of the Current Flat-structured HIT Architecture

The HIT concept was defined in [RFC5201]: "... the Host Identity Tag (HIT), becomes the operational representation. It is 128 bits long and is used in the HIP payloads and to index the corresponding state in the end hosts."

In order to be able to represent hosts, the uniqueness of HITs is required in global scope. "In the HIP packets, the HITs identify the sender and recipient of a packet. Consequently, a HIT should be unique in the whole IP universe as long as it is being used." [RFC4423]

Although mathematically "the probability of HIT collision between two hosts is very low" [RFC5201], there is no mechanism to ensure that a HIT is global unique.

The current defined HIT is generated according to the ORCHID generation method described in [RFC4843]: "several possible methods ... to preserve a low enough probability of collisions". However, it cannot guarantee the global uniqueness of HITs. Furthermore, while the number of end devices continuously grows in the future, the possibility of HIT collision will increase rapidly. A technical mechanism is needed to ensure the global uniqueness of HITs, particularly with the consideration that collisions may happen. When such collision happens, more than one hosts will have the same HIT. Then, the HIT cannot uniquely identify a certain host.

Although there is a rough solution for how to distinguish duplicated HITs, it is far from a feasible or best solution.

[RFC4423] states "In the extremely rare case of a single HIT mapping to more than one Host Identity, the Host Identifiers (public keys) will make the final difference." It means the mapping system between HIP and IP must store or at least be aware of the Host Identifiers of all hosts. Given the facts that the Host Identifiers are quite large and may be in various lengths, the storage and management burden of the mapping system could be quite high. If there was a mechanism to ensure the global uniqueness of HITs, then, the mapping system would not have to be aware the Host Identifiers.

Furthermore, within the flat-structured HIT architecture, the robustness of resolution efficiency in the supporting mapping system is in a big question mark: a mapping server has to hold or at least to be able to access a large database that contains information on all HITs in the global scope. There more than a billion hosts now on the Internet and a global deployment of HIP would require an equal amount of HITs. In the future, there could be even billions of machines or even higher. The storage burden, maintenance consumption and synchronization updating are problems that are very difficult to solve. If the HITs were organized hierarchically, the mapping system could easily be organized hierarchically, even distributed.

One more disadvantage that the flat-structured HIT architecture is the difficulties for management. There is nothing common between HITs that were assigned by the same authority or that their represented hosts have the same properties. Hence, it is difficult to categorize HITs. Although this provides privacy to the end-hosts, the Access Control Lists (ACLs) would have to have a full list of HITs accessible to permitted services. Contrarily, the hierarchical HITs are more aggregatable. It makes HITs manageable. HITs can be grouped according to its belonging authority or domain. Each network operator just needs to manage and maintain HITs and their mapping information in a relatively small range.

According to the above analysis, it is natural to turn the flat HIT architecture into hierarchy. It can effectively reduce the global uniqueness requirement into much smaller scope uniqueness requirement. In another word, if a hierarchical HIT with a global unique AD ID is locally unique, it is guaranteed to be global unique. It can improve the resolution processing and enhance the scalability and resolution efficiency. Furthermore, it can optimize the management of both the host identity and the mapping database. Each administrative domain is responsible only for a part of the global HIT architecture. However, it is useful that the new

hierarchical HIT architecture is compatible with the flat HIT architecture for privacy purposes and other usage scenarios.

3. Hierarchical HIT Architecture

In this document, we introduce a two-level hierarchically structured HIT architecture. HIT is "128 bits long value and is used in the HIP payloads and to index the corresponding state in the end hosts." [RFC5201] "In the HIP packets, the HITs identify the sender and recipient of a packet." [RFC4423] HITs refer to nodes or virtual nodes. All nodes are required to have at least one HIT. A single node may also have multiple HITs. Applications on a same node may bind to different HITs.

In the hierarchical HIT namespace, a 128-bit HIT consists of two parts: an n-bit HIP AD ID and a (128-n)-bit local host ID. (n is a subject to be decided in the future.) It can represent maximum 2^n administrative domains and 2^(128-n) hosts within each administrative domain. The Administrative Domain ID has embedded organizational affiliation and global uniqueness. The local host ID is a hash over the AD ID and the public key of the ID owner.

```
|           n bits              |            128-n bits          |
+-------------------------------+--------------------------------+
|  HIP Administrative Domain ID |           local host ID        |
+-------------------------------+--------------------------------+
```

For the secure consideration, we recommend to assign more bits to the local host ID, which is a hash result, leaving less but enough bits for HIP Administrative Domain ID. The more the number of bits the local host ID is, the more secure it is against brute-force attacks. In the worst case, if the hash algorithm cannot be inverted, the expected number of iterations required for a brute force attack is O(2^(128-n)) in order to find a host identity that matches with a given local host ID. It should be noted that this draft does not take into account the ORCHID prefix defined in [RFC4843] for two reasons: firstly, ORCHID is only temporary assigned for experimental usage till 2014 only. The proposal design in the document is targeting to be used continuously after 2014. Secondly, the fixed 28-bit orchid prefix reduces the security properties massively and increase collusion possibility highly.

The HIP administrative domain, as its literal, is a logic region in which the HIs of all nodes are assigned by the same authority. Within a same HIP administrative domain, all the nodes should have the same HIP AD ID or the same leftmost certain bits. Furthermore, the authority may be organized internally hierarchically.

The HIP AD ID should be assigned by a global administrative organization with the principle that every HIP AD ID must be globally unique.

Consequentially, the HIP AD IDs may be organized hierarchically. For example, a big organization may obtain a block of HIP AD IDs with an assigned 16-bit prefix. It then can assign 24-bit HIP AD IDs to its sub-organizations. All these sub-organizations have the same leftmost 16-bit.

One promising allocation solution of HIP AD ID is following current routable IP address allocation system [RFC2050]. At first IANA allocates some HIP AD ID prefixes to RIR (Region Internet Registry) or NIR (National Internet Registry),then RIR or NIR sub-allocates the HIP AD ID prefix to LIR or backbone ISP that subdivides the tag prefix to middle or small ISP. Historical experience of routable IP address allocation indicates that the allocation system can ensure global uniqueness of HIP AD IDs.

One advantage of this solution is that the HHIT architecture can build distributed catalogue based on current IP address Internet Registry. Each level Internet Registry only needs to maintain its HHIT information. This catalogue is like current IP Whois Server operated by each IP address Internet Registry. But it should include many more attributes about a HHIT, such as organizational affiliation, geographical information, privacy protection rule etc. The catalogue should be independent of current IP Whois system and IP address Internet Registry should provide some mechanism to translate HHIT to its useful attributes on demand of various applications.

The local host IDs remains the original meaning of HIT - "a hashed encoding of the Host Identity". For each HIP administrative domain, it is mandatory to maintain the uniqueness of all local host IDs. It is guaranteed by the process of generating a HIT, see Section 5.

For resolution purposes, HITs are aggregatable with AD IDs of arbitrary bit-length, similar to IPv4 addresses under Classless Inter-Domain Routing [RFC4632].

3.1. Compatible flat-structured HITs

Obviously, not all hosts are willing to use hierarchical HITs in all scenarios for various reasons, such as privacy. Therefore, it is useful that the hierarchical HIT architecture keep compatible with the flat HIT architecture.

The flat HITs can be defined as a specific sub-set of the hierarchical HITs architecture. With the same reserved Flat HIT Tag (3 or 4 bits) at the beginning, for example, the left-most 3 bits is 000, the flat HITs can be used as defined in [RFC4423].

```
|                            128 bits                            |
+----------------------------------------------------------------+
|FHIT Tag|            Flat host identity tag                     |
+----------------------------------------------------------------+
```

3.2. HITs on nodes

HIP-enabled nodes may have considerable or little knowledge of the internal structure of hierarchical HITs, depending on the role the node plays (for instance, host versus mapping server). At a minimum, a node may consider pre-generated HITs have no internal structure:

```
|                            128 bits                            |
+----------------------------------------------------------------+
|                        host identity tag                       |
+----------------------------------------------------------------+
```

Only sophisticated hosts may additionally be aware of the type of their HITS and use the hierarchical structure of HITs to simplify the resolution procedure.

4. Generating a hierarchical HIT

The process of generating a new hierarchical HIT takes three input values: an n-bit HIP AD ID, a 2-bit collision count, (an example, it is a subject to be changed in the future.) the host identity (the public key of an asymmetric key pair). A hierarchical HIT should be generated as follows:

1. Set the 2-bit collision count to zero.

2. Concatenate from left to right the HIP AD ID, the collusion count, and the host identity. Execute the SHA-1 algorithm on the concatenation. Take the (128-2-n) leftmost bits of the SHA-1 hash value.

3. Concatenate from left to right the n-bit HIP AD ID, the 2-bit collision count and (128-2-n)-bit hash output to form a 128-bit HIT.

4. Perform duplicate detection within the HIP administrative domain scope. If a HIT collision is detected, increment the collision count by one and go back to step 2. However, after four collisions, stop and report the error. (Note: the duplicate detection mechanism is not discussed in this document. It may be broadcast or central registration.)

The design that includes the HIP AD ID in the hash input is mainly against the re-computation attack: create a database of HITs and matching public keys. With the design, an attacker must create a separate database for each HIP administrative domain.

The design reduces the number of bit of hash output 2 bits lower. It does reduce the safety. However, O(2^(128-2-n)) iterations is large enough to prevent brute-force attacks.

For security reason, the abovementioned SHA-1 hash algorithm may be replaced by any safer algorithm.

5. Requirements for modification on HIP

The usage of hierarchical HITs requires either a new version of HIP protocol or a new critical flag in the header of HIP control packets. The latter is considered easier and more fulfill.

6. Security Considerations

The most important security property of HIT is that it is self-certifying (i.e., given a HIT, it is computationally hard to find a Host Identity key that matches the HIT). Although this document limits the hash output to be (128-2-n)-bit long, it does not affect the self certifying security property.

7. IANA Considerations

This document defines a new namespace: HIP AD ID. It is an n-bit long value, which represents a globally unique HIP administrative domain. IANA may found an authority institute to manage the global assignment of HIP AD ID.

8. Acknowledgements

Useful comments were made by Miika Komu from HIIT, and other members of the IRTF HIPRG research group.

9. References

9.1. Normative References

[RFC2050] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg and J. Postel "Internet Registry IP Allocation Guidelines", RFC 2050, November 1996

[RFC4423] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.

[RFC5201] R. Moskowitz, et al., "Host Identity Protocol", RFC 5201, Oct 2007.

9.2. Informative References

[RFC4632] V. Fuller, T. Li, "Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", RFC4632, August 2006.

[RFC4843] P. Nikander, et al., "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", RFC 4843, April 2007.

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: shengjiang@huawei.com

Xiaohu Xu
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: xuxiaohu@huawei.com

Dacheng Zhang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Email: zhangdacheng@huawei.com

Tao Chen
CNNIC
No. 4, South 4th Street, Zhongguancun
Beijing 100190
P.R. China
Email: chentao@cnnic.cn