2012 IACSIT Hong Kong Conferences
IPCSIT vol. 29 (2012) © (2012) IACSIT Press, Singapore

Simple and Secure Communication Enabled by Innovating Service Providing Styles by IPv6 Address

Shigeyoshi Shima[1 +] and Hiroshi kitamura[2]

[1] The University of Electro-Communications / Information-Technology Promotion Agency, JAPAN
[2] NEC Corporation / The University of Electro-Communications

Abstract. In the IPv4 era, nodes in private networks generally use local addresses. In the IPv6 era, global addresses can be allocated to all nodes because the IPv6 address space is so large (2^128). Global addresses are used for direct communication between nodes in the Internet. Direct communication is a simple and an ideal communication model because gateways which translate or relay communications between nodes are unnecessary. However, in direct communication, nodes might receive connection requests from undesirable nodes and might be directly attacked from unknown nodes. Current secure mechanisms against those threats are managed by administrator and are inconvenient for users with lack of knowledge about network and information security. We propose a simple secure communication mechanism with the potential for a security model based on wide address space. For our secure communication mechanism, we create a new type of service-specific address (SSA) and innovate in existing server address and service providing methods. Our secure communication mechanism has been designed and implemented.

Keywords: IPv6, multi-address, non-disclosure, secure communication, direct communication

1. Introduction

The IPv4 Addresses of the unallocated address pool administered by the IANA (Internet Assigned Numbers Authority) was exhausted on 3 February, 2011. The Internet will soon have to migrate to the IPv6 because of the IPv4 global address shortage for an increasing number of nodes.

In IPv4 networks, nodes in private networks are generally assigned a local address (IPv4 private address). Nodes in private networks must communicate with nodes in the Internet through address translation mechanisms such as NAT and cannot become servers. In IPv6 networks, all nodes can be assigned a global address because the IPv6 address space is so large (2^128). Thus, nodes in private networks can directly communicate with nodes in the Internet without using address translation mechanisms. Direct communication is a simple and an ideal communication model. Nodes can become not only clients (request/send) but also servers (response/receive). Thus, even home network users can provide services from nodes in home networks. Home network users can communicate without special functions from nodes in the Internet (e.g., smart phones) to nodes in private networks (e.g., home servers). It is expected that this freedom will lead to new services for home network users. However, nodes might receive undesirable packets (e.g., probing packets, DoS attack packets, etc.) because they receive packets at all times. Secure communication mechanisms against such threats have already been developed for IPv4 networks; e.g., Firewall and IPSec/IKE. However, these mechanisms have to be managed by an administrator and are inconvenient for home network users who may lack knowledge about network and information security. Thus, this limitation would likely interfere with the spread of new services. We propose IPv6 address non-disclosure security to prevent packets from undesirable users and unknown users in direct communication from reaching home network users.

[+] Corresponding author. Tel.: + 81-3-5978-7530; fax: +81-3-5978-7518.
E-mail address: s-shima@ipa.go.jp.

2. Current secure communication issue in IPv6 direct communication

IPv6 networks have secure communication mechanisms for preventing undesirable packets from reaching servers: Firewall and IPSec/IKE [1]. Note that NPTv6 [2] is not treated in this paper because nodes in private networks can not directly communicate with nodes in the Internet.

- Firewall

Firewall configurations require complex packet filtering policies, access controls, and so on.

- IPSec/IKE

IPSec/IKE configurations require a security policy (SP), security association (SA), cryptography algorithms, and authentication keys.

It is difficult for users who lack knowledge about network and information security to configure the security policies of secure communication mechanisms. Such mechanisms are usually managed by trained administrators [3] [4]. Moreover, home network users may be prone to making mistakes in configuring complex policies. That would leave them vulnerable to receiving packets from undesirable or unknown nodes.

3. Our secure communication mechanisms

There is an analogy between direct communication in an IP network and cellular phone network communication. In both communications, subscribers (nodes) directly communicate with other subscribers (nodes) and request (send) and respond (receive). Let us briefly consider the existing threats affecting direct communication and countermeasures of cellular phone subscribers. Threats include prank calls and telephone solicitation. Some simple countermeasures are as follows.

(1) A subscriber should not give undesirable and unknown subscribers their phone number. A subscriber tends to register others' phone numbers and owner information. S/he should answer the phone only after s/he has identified the caller on the cellular phone display.
(2) A subscriber often has his/her stored phone numbers organized for certain purposes or into groups.
(3) A subscriber turns on the phone power only when he or she wants to use it.
(4) A subscriber can change his/her phone number if s/he thinks an undesirable subscriber knows it.

We define countermeasure (1) as "non-disclosure model." A non-disclosure model can be used by subscribers without much security and network knowledge. Countermeasures (2), (3) and (4) avoid undesirable requests as much as possible. We decided to embody countermeasures (1), (2), (3), and (4) in our secure communication mechanism.

4. Security evaluation of non-disclosure model in IPv6 private networks

In the non-disclosure model, a phone number of a cellular phone network corresponds to an IP address of an IPv6 network (cellular phone measurement (1)). A threat in the non-disclosure model would be an IPv6 address of a node coming to be known by an undesirable user.

The IPv6 address is divided into two parts: the prefix and the interface ID. The interface ID does not affect the routing. Thus, the minimum network size is a 64-bit address space. We assume that a node searches the 64-bit address space. If the search time is one address per second, it will take more than 10 billion years to search all addresses [5]. Therefore, it is very difficult to search for accessible hosts by using a brute force address search in IPv6 networks. If an undesirable node cannot know an address of a node in an IPv6 network, the undesirable node will not even be aware of the existence of the node. Thus, the non-disclosure model is effective to avoid undesirable requests in IPv6 networks.

5. Specific Service Address (SSA) for new security mechanisms

We referred to cellular phone measurements and propose new address concept: Specific Service Address (SSA). We evolved the server address concept as follows.

(1) From static to dynamic (cellular phone measurement (4))

The server address in IPv4 is static and is used permanently once it has been allocated to a server. An undesirable node can continue to attack the server because the server cannot change its address.

In the new mechanism, a SSA is dynamically generated and is allocated to a specific service only while a server provides a client with the service. The SSA is not used permanently. The SSA is revoked by the server when the server finishes providing the client with the service. The revoked SSA cannot be reused by the original client or by any other client. Thus, even if the revoked SSA is leaked to an undesirable client, the undesirable client will not be able to connect to the server. However, if an undesirable client can predict the next SSA, it might be able to attack the server by using the predicted SSA. Therefore, the server must generate random SSAs. Secure SSAs can be generated by using address generation methods such as CGA [6] and HBA [7].

It is known that dynamic addresses protect sites from attack packets sent from undesirable nodes [8].

(2) From general/common to specific/dedicated (cellular phone measurement (2))

In the legacy system, a server provides clients with multiple services by using the single address allocated to the server. All clients access that one server address.

In the new system, multiple addresses, one for each service, are allocated to a single server. A client accesses an SSA for each service. Thus, the server can provide each client with a different service and can permit access only by the client node that requires a given SSA service.

(3) From at all the time to only as needed (cellular phone measurement (3))

In the legacy system a server address is allocated to a server when the server node starts up and is used indefinitely. Therefore, the server allows access from a client at any time. Similarly, the server allows attacks by an undesirable client at any time.

In the new system, whenever a server starts to provide a client with a service, an SSA will be allocated to that server node's service. When the server has finished providing that service, the SSA becomes invalid and is revoked. If an undesirable node knows the invalid SSA, the undesirable client will not be able to reuse the invalid SSA.

Secure communication mechanisms based on the dynamic address have already been proposed [9][10]. However, these mechanisms do not have the characteristics of (1) and (3). Thus, the chance of secure communication mechanism based on SSA receiving packets from undesirable nodes is less than in other secure communication mechanisms based on dynamic addresses.

The concept of server address is innovated from the left side (Legacy) to the right side (SSA) in Fig 1. SSA assumes a multi-address environment in the server. Different SSAs are allocated to each service in the server. Whenever a server provides a client with a service, an SSA is dynamically generated for each service by the server. Whenever the client uses the service, the client communicates with the server by using the SSA assigned to that service. When the server finishes providing the client with the service, the server revokes the SSA. The client cannot reuse the same SSA in the next communication.

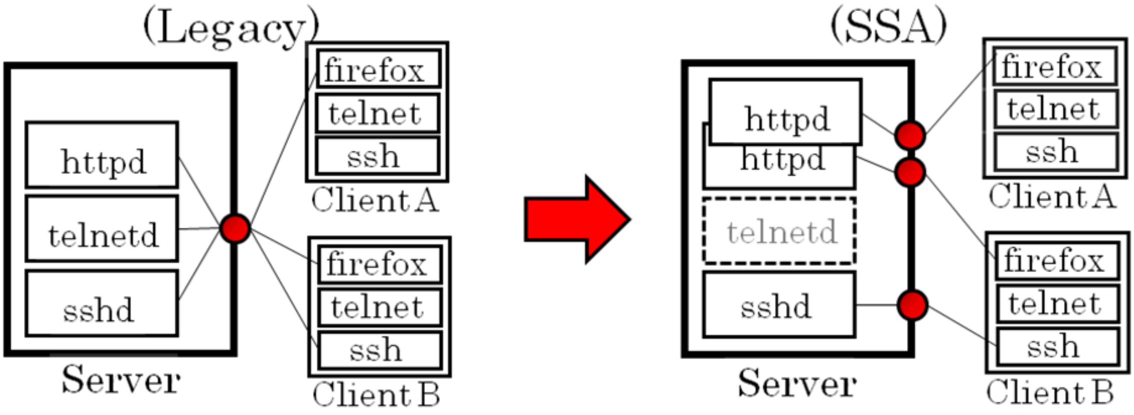

Fig. 1: Comparison of legacy and proposed server address characteristics

6. Requirements for our secure communication mechanism

Our secure communication mechanism has the following requirements.

(1) The configuration of the servers must be an SSA or a service name registration such as a phone number registration of a cellular phone. Most users can register phone numbers, owner information, and contacts lists. The service name is information for obtaining the SSA (e.g., www-abc.sample).
(2) New applications or agents must not be installed in the client.
(3) The configurations of client applications must not be changed.

7. Design and Implementation

We designed and implemented a prototype of our secure communication mechanism, called “IPv6 address non-disclosure security.” In the IPv6 address non-disclosure security, a client sends a service request to a server before the client node obtains an SSA from the server, because the SSA is dynamically generated by the server. Thus, the SSA must be propagated from the server to the client.

We chose the DNS protocol as the method by which a client obtains SSAs. Thus, a user does not need to add new applications or change the configuration of the client (Requirements (2) and (3)). We designed and implemented two modules to propagate SSAs.

- NOCA (Name Override Client Agent)

The NOCA exists between a client and a DNS Server, and it blocks and captures DNS queries. It checks whether the service name is contained in the service name list. The user registers the service name in the service name list (Requirement (1)).

We use "ipfilter" for blocking queries and "libpcap" for capturing them. We implemented functions to override DNS queries.

- Server agent

A server agent can generate an SSA and binds the SSA to a service process. We modified "inetd" for binding and unbinding SSAs.

The communication sequence of our prototype is shown in Fig. 2. The communication sequence from (1) to (7) in Fig. 2 is explained below.

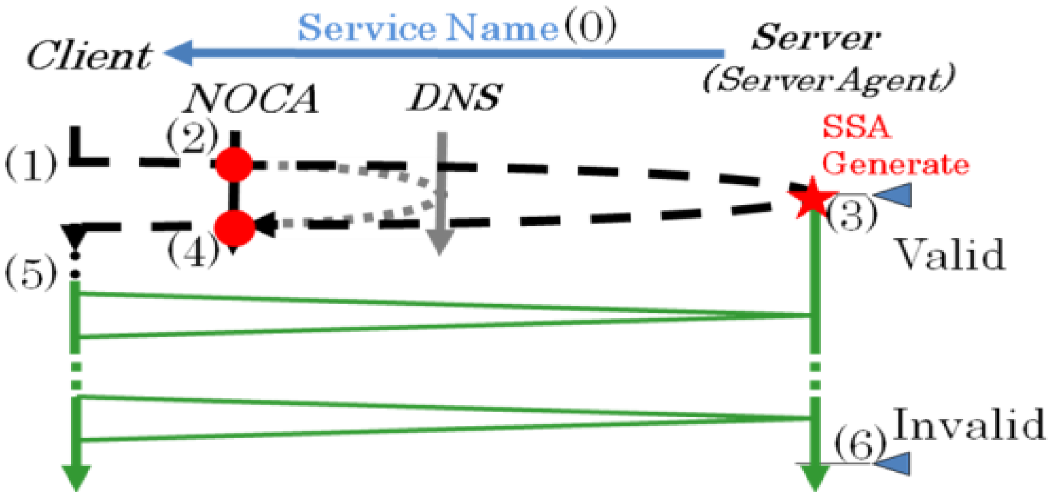

Fig. 2: Communication Sequence of our prototype

(1) The user of a server registers the service name on the service name list of a NOCA. The user of the server securely sends the service name to the client of the user (e.g., e-mail, telephone, etc.).
(2) The client resolves the service name (or a server name) by making a DNS query.
(3) The NOCA blocks and captures the DNS query. The NOCA checks whether the service name of the DNS query exists in the service name list. If the service name exists in the list, the NOCA sends an SSA request to the server. If the service name does not exist in it, the NOCA forwards the DNS query to the DNS server.

(4) The server agent receives the SSA request from the NOCA and starts to generate an SSA. The server agent randomly generates the Interface ID of the IPv6 address and generates an SSA from the IPv6 prefix of the server and the Interface ID. However, if the SSA and addresses of other nodes collide as a result of DAD [11], the server agent generates a new SSA. The server creates a service process (httpd) and allocates the SSA to the server process. The server sends the SSA to the NOCA.
(5) The NOCA creates a Reply packet for the DNS Query and sends the Reply packet to the client.
(6) The client sends a service request to the server of the SSA. The client (browser) accesses the server's service (httpd).
(7) When the server finishes providing services to the client, the server stops the service process (httpd) and revokes the SSA.

IPv6 address non-disclosure security is run on FreeBSD 5.4 and is written in about 6,000 lines of C language code (gcc). Thus, the development environment and software requirements of IPv6 address non-disclosure security are general in network systems.

8. Conclusion

This paper proposed IPv6 address non-disclosure security for users who lack knowledge about network and information security. We created a service-specific address (SSA) for the server from the existing server address and service providing methods. This new mechanism makes it very difficult for a node (server) to receive packets from undesirable nodes.

It is expected that IPv6 address non-disclosure security can be provided as a new security service by ISPs and that with it, home network users will be able to securely provide services to familiar people such as family, friends, etc. Note that if familiar people leak a service name to an undesirable user, that undesirable user can request services. However, this threat is not a serious issue in cellular phone networks.

Currently, the security service of our secure communication mechanism is restrictive because security service is provided by one NOCA. Thus, our next issue will be to improve the scalability of the SSA propagation method.

9. References

[1] M. Kaeo. IPv6 Security Technology Paper. *North American IPv6 Task Force (NAv6TF) Technology Report*. 2006.

[2] M. Wasserman, F. Baker. IPv6-to-IPv6 Network Prefix Translation. *RFC6296*. 2011.

[3] S. P. Maj, W. Makasiranondh, D. Veal. An Evaluation of Firewall Configuration Methods. *IJCSNS International of Computer Science and Network Security*. Vol10 No8. 2010.

[4] J. Touch, D. Black, Y. Wang. Problem and Applicability Statement for Better-Than-Nothing Security (BTNS). *RFC5387*. 2008.

[5] T. Chown. IPv6 Implications for Network Scanning. *RFC 5157*. 2008.

[6] T. Aura. Cryptographically Generated Addresses (CGA). *RFC 3972*. 2005.

[7] M. Bagnulo. Hash-Based Addresses (HBA). *RFC 5535*. 2009.

[8] J. Woodyatt, Ed. Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. *RFC6092*. 2011.

[9] A. Sakuai, T. Minohara, R. Sato, K. Mizutani. One-time receiver address in IPv6 for protecting Unlinkability. *Proc. 12th Annual Asian Computer Science Conference (Springer LNCS4846)*. 2007, PP.240-246.

[10] G.Van de Velde, T. Hain, R. Droms, et al. Local Network Protection for IPv6, *RFC4864*, 2007.

[11] N. Moore. Optimistic Duplicate Address (DAD for IPv6). *RFC 4429*. 2005.