An Unified Multiplex Communication Architecture for Simple Security Enhancements in IPv6 Communications

Kazuyuki NISHIDA
Osaka University
Osaka, Japan
k-nisida@ist.osaka-u.ac.jp

Shingo ATA
Osaka City University
Osaka, Japan
ata@info.eng.osaka-cu.ac.jp

Hiroshi KITAMURA
NEC Corporation
Tokyo, Japan
kitamura@da.jp.nec.com

Masayuki MURATA
Osaka University
Osaka, Japan
murata@ist.osaka-u.ac.jp

I. INTRODUCTION

Current IP communication style is not optimized and has various problems. Sufficient security considerations (including privacy protection) are not provided. Despite the "well-known port" method being known to be inappropriate from security standpoint, it continues to be used it. The conventional belief that one node owns one IP address and communication sessions are basically multiplexed at the transport layer is still held. We are moving to the IPv6 era in which it has become normal for one node to own multiple IP addresses. Therefore, it must be time to reconsider the current communication style and establish a new simple and security enhanced communication architecture.

We propose a new communication architecture called **Unified Multiplex**. It is designed to be coexisted with current communication style implementations. The proposed Unified Multiplex communication architecture can improve the current IP communication style drastically. We also intend to establish a new communication style and service providing methods that are suitable for the IPv6 era.

The architecture introduces new technologies, such as new address types called **EA (Ephemeral Address)** and **SSA (Specific Service Address)**. The EA is dedicated to a client session and is assigned when the session is started. (In the same way SSA is dedicated to a server session.) After the session is finished, it released. The EAs or SSAs that are dedicated to respective sessions and used as sessions' identifies. Since sessions can be multiplexed at the network layer only, in the architecture, transport layer "Port" information becomes less significant. Furthermore, the way of multiplexing and identifying the sessions becomes much simpler and securer than the current method.

We discuss problems on current communication style, which is now becoming legacy, and clarify requirements for a new architecture from practical viewpoints. We propose a new architecture that can solve the problems comprehensively. The design and implementation of the architecture and newly introduced technologies are discussed. Note here that the most important thing that settles results of this proposal is *how to coexist with current implementation and migrate to a new architecture*. A proposed new node should be able to communicate with existing nodes without changing the existing nodes. There are significant advantages when new Unified Multiplex communications are executed, and migration to new Unified communication world should be promoted. Although the architecture introduced new technologies, notions, and a new communication style, this has been achieved without modifying existing client and server applications. Only the OS kernel side modifications and improvements are necessary.

The proposed architecture has been implemented and its functions have been verified in experimental network.

II. PROBLEMS WITH CURRENT IP SESSIONS' MULTIPLEXING AND SERVICE PROVIDING METHODS

In RFC1078 [1], basic concepts of IP communication session multiplexing methods and service providing methods are described. (Hereafter, these will be referred to as "Legacy Multiplex.") Four types of information (source and destination IP addresses and port numbers) and protocol number (TCP or UDP) are used as a set for multiplexing and distinguishing IP sessions.

The concept of Legacy Multiplex was invented in the IPv4 era, when one node owned only a single IP address. In the IPv6 era, however, it has become very normal for one node to own multiple IPv6 addresses. Therefore, it is time to reevaluate the IP session multiplexing architecture in depth and innovate it.

The Legacy Multiplex has following two major problems.

First, in the Legacy Multiplex, intermediate nodes must deal with the transport layer information, because information needed to distinguish sessions is located at both network and transport layers. This makes operations on intermediate nodes complex and inefficient.

Second, the Legacy Multiplex uses "well-known" port numbers to connect a server for a target service. However, the port number information itself does NOT represent the essence of the provided service [2]. It is known that there is a service providing method that uses a different port number value from the "well-known" number on purpose. The concept of "well-known port" is based on an intrinsically good principle. i.e., there are not sufficient security considerations for privacy. In the "well-known port" method, servers let every clients know which types of services are provided on servers without any client identifications or security considerations. This means that attackers can easily obtain information on the servers they would like to crack. In order to solve these problems, several methods that extend or modify current systems are proposed in papers [3][4][5][6] etc. However, no clear conclusions are reached as of today.

III. PROPOSAL OF UNIFIED MULTIPLEX COMMUNICATION ARCHITECTURE AS A SOLUTION

In order to solve the above problems comprehensively, we propose a new communication architecture called Unified

Multiplex Communication Architecture and new communication styles.

Information to distinguish sessions should be minimum and closed in a single layer. Simple, minimum and efficient function implementations are desired. Also, new architecture should emphasize security and privacy protection methods. A proposed new node should be able to communicate with existing nodes without changing the existing nodes. There are significant advantages when new Unified Multiplex communications are executed, and migration to new Unified communication world should be promoted.

A. *Basic Design and Characteristics of Unified Multiplex Communication Architecture*

The basic concept of Unified Multiplex Communication Architecture is shown in Fig. 1. Multiplexing operations are implemented only at the network layer. Sessions can be distinguished by a set of the following only two types of information and protocol information (TCP or UDP).

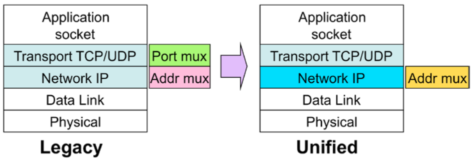

Fig.1 Basic concept of Unified Multiplex Architecture

In **Unified**, only IP "Address" information is used to distinguish IP sessions. It is not necessary for clients to obtain "Port" information any more to access services.

The important advantage of Unified Multiplex is that IP addresses are dedicated to sessions and many addresses are consumed. In the Legacy Multiplex, there are some security and privacy issues due to the usage of IP addresses which are identical during associate nodes are active [7][8][9]. On the other hand, in Unified Multiplex, IP addresses are valid only during the communication session is established, and immediately disposed after the session has been finished. This property significantly improves the security and privacy. For the third party, IP addresses are no longer the identifier of nodes because IP addresses will be varied according to the session even if the communication peers are the same. Moreover, any nodes cannot access to the node by using previously recorded IP addresses of the node.

A summary of how the proposed Unified Multiplex communication architecture improves in address usages, service providing methods, etc. is shown in Table 1.

Table 1. Comparison between Legacy and Unified

	Legacy	(Proposed) **Unified**
Number of Used Addresses	Use Only **One** Address (Basically)	Use **Multiple** Address
Information Dealing	General and **Share** Use **Same** Address	Specific and **Dedicated** Use **Different** Address
Service (on Servers)	Wait for **Anytime** (24 hour / 365days)	Wait for **Only** When Access Expected to Come
Information Fluidity	**Fixed** (Not Changed)	**Changed and Updated**

B. *Address Types used in Unified Communications*

There are two types of addresses in Unified communications. At client side, the **"Ephemeral Address" (EA)** is automatically selected and assigned by the OS when a session is actually started, and used for source address of the client in the session. After the session is finished, the address is automatically disposed. Since the address is used ephemerally (the existing life time is usually short), it becomes difficult for crackers to attack such sessions and the security protection mechanism is improved and privacy protection is enhanced.

At server side, the **"Specific Service Address" (SSA)** is used for a specific session in order to provide a specific service (e.g., client who can access the service is limited to the specified client only), NOT used to provide a usual generic service. Each specific session owns each "SSA (Specific Service Address)" exclusively. SSA information is never advertised to anonymous clients, i.e., only the client who has a right to access the service can obtain the SSA. A server does not need to utilize special techniques (such as packet filtering) to limit clients who can access the service. Only providing the service via the SSA is enough to limit the client. The IPv6 address space is huge, brute force type attack is thus realistically impossible. Several hundred billion years are needed to attack IPv6 address space (with one second per one address type attack to 64bit Interface ID space). Such a specific service/session enabled by the SSA can easily become secure. Many SSAs are consumed at a server that provides specific services. By consuming SSAs with this method, simple and strong security enhancements are brought to the architecture.

IV. IMPLEMENTATION RELATED ISSUES

The Unified Multiplex Architecture has been implemented under FreeBSD 6.2R, FreeBSD 8.0R, and its basic functions have been verified. We have also implemented EA functions in Linux operating system. The source codes for the Unified Multiplex Architecture implementations are not large roughly 5,000 line patches. Also, it has verified that standard applications (such as telnet/telnetd, ssh/sshd, apache, inetd, rsh/rshd, etc.) work without problems on the kernel where the Unified Multiplex communication architecture functions are implemented.

REFERENCES

[1] M. Lottor, "TCP Port Service Multiplexer (TCPMUX)," RFC1078 (Proposed Standard), November 1988

[2] "What if there were no well known numbers?" originally posted by J. Kristoff on IRTF end-to-end research group mailing list, August 2006 http://mailman.postel.org/pipermail/end2end-interest/2006-August/thread.html#6114

[3] Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)," RFC 2782, February 2000

[4] R. Srinivasan, "RPC: Remote Procedure Call Protocol Specification Version 2," RFC 1078, June 1995

[5] R. Srinivasan, "Binding Protocols for ONC RPC Version 2," RFC 1833, August 1995

[6] J. Touch, "A TCP Option for Port Names," Internet draft, draft-touch-tcp-portnames-00, work in progress, April 2006

[7] W. Haddad, et al, "Privacy for Mobile and Multi-homed Nodes: Problem Statement," Internet draft, draft-haddad-momipriv-problem-statement-03, work in progress, June 2006.

[8] Haddad, E. Nordmark, "Privacy Aspects Terminology," Internet draft draft-haddad-alien-privacy-terminology-05, work in progress, December 2008.

[9] T. Narten, R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," RFC 4941, September 2008