Internet Architecture Board
Internet-Draft
Expires: February 12, 2004

M. St Johns, Ed.
G. Huston, Ed.
IAB

August 14, 2003

Considerations on the use of a Service Identifier in Packet Headers
draft-iab-service-id-considerations-02.txt

Status of this Memo

Copyright Notice

Abstract

This memo describes some considerations relating to the use of IP protocol number fields and payload protocol (e.g. TCP) port fields to identify particular services that may be associated with that port number or protocol number.

1. Introduction

This memo describes some considerations relating to the use of IP protocol number fields and payload protocol (e.g. TCP) port or service fields to identify particular services that may be associated with that port number or protocol number. It is a general statement regarding appropriate processing and use of service identifiers by

intermediate systems.

This memo points out that various measures by intermediate systems that are intended to filter or prevent the transmission of traffic based on the service identification within the traffic flow have limited effect, with a major side-effect of forcing the affected services to be redesigned using various forms of encapsulation or dynamic port negotiation in order to remove the fixed service identification from the IP packet headers. The IAB does not believe this serves the general interests of the Internet community related to the design of simple and reliable Internet applications. This memo suggests some thought be given to control mechanisms that do not rely on intermediary systems taking actions based on an assumed relationship between the service identifier in the packet and the actual service of which the packet is a part.

2. Service Identifiers

Although not necessarily by design, certain conventions have evolved with respect to the IP protocol suite relative to the identification of services within an IP traffic flow:

- Within the IP protocol suite, end point identifiers (e.g. TCP/ UDP/SCTP port numbers, IP protocol numbers) are designed to identify services to end points. In particular, TCP, UDP or SCTP (Stream Control Transmission Protocol) port numbers are intended to identify the source service location and the destination service entity to the destination end point.

- The IP [2] datagram header contains the source and destination address of the datagram as well as an indication of the upper-level protocol (ULP) carried within the datagram. If the ULP is either TCP [3], UDP [1], or SCTP [8] the payload will contain both source and destination port numbers which allows differentiation between services (e.g. TELNET, HTTP) and between multiple instances of the same service between the pair of hosts described by the source and destination address.

- By convention, for at least TCP and UDP, certain port numbers are used as rendezvous points and are considered "well known" on the source or destination side of the communication. Such rendezvous points are maintained in an IANA registry currently located at [11]. Specific registries for protocol and port numbers are at [12] and [13].

- Notwithstanding the "well-knownness" of any given port, port numbers are only guaranteed to be meaningful to the end systems. An intermediate system should generally not impute specific meaning to any given port number, unless specifically indicated by an end system (e.g. via the Resource Reservation Protocol (RSVP)[4]) or agreed to by convention among the end systems and one or more specific intermediate systems (e.g. firewall traversal for the IP Security Protocol (IPSEC)[5]).

- Some services make use of protocol interactions to dynamically allocate service identifiers (i.e. port numbers) to specific communications. One specific example of this is the Session Initiation Protocol (SIP)[9]. The implication of this is that intermediate systems cannot relate the service identifiers to the actual service unless they participate in the protocols which allocate the service identifiers, or are explicitly notified of the outcome of the allocation.

- Various products and service-related mechanisms deployed today take advantage of the fact that some service identifiers are relatively stable (and well known) to do various things (e.g. firewall filtering, QOS marking).

- Certain network operations, such as various forms of packet encapsulation (e.g. tunnelling) and encryption, can occlude this port number (or service identifier) while an IP packet is in transit within the network. For example, both the IPSEC Encapsulating Security Payload (ESP) [6] and Generic Routing Encapsulation (GRE) [7] both provide means for tunneling an IP datagram within another IP datagram. The service information becomes obscured and, in some instances, encrypted.

- Cooperating end systems may elect to use arbitrarily selected port numbers for any service. The port numbers used in such cases may be statically defined, through coordinated configuration of the cooperating end systems through use of a common application or operating system, or by dynamic selection as an outcome of a rendezvous protocol.

Intermediate system imposed service-based controls may block legitimate uses by subscribers. For example, some service providers are blocking port 25 (i.e. notionally SMTP) traffic for the stated purpose of trying to prevent SPAM, but which can also block legitimate email to the end user.

Attempts by intermediate systems to impose service-based controls on communications against the perceived interests of the end parties to the communication are often circumvented[10]. Services may be tunneled within other services, proxied by a collaborating external host (e.g. an anonymous redirector), or simply run over an alternate port (e.g. port 8080 vs port 80 for HTTP). Another means of circumvention is alteration of the service behaviour to use a dynamic port negotiation phase, in order to avoid use of a constant port address.

For the purposes of this memo a "party to a communication" is either the sender, receiver or an authorized agent of the sender or receiver in the path.

If intermediate systems take actions on behalf of one or more parties to the communication or affecting the communication, a good rule of thumb is they should only take actions that are beneficial to or approved by one or more of the parties, within the operational parameters of the service-specific protocol, or otherwise unlikely to lead to widespread evasion by the user community.

3. Ramifications

The IAB observes that having stable and globally meaningful service identifiers visible at points other than the end systems can be useful for the purposes of determining network behavior and network loading on a macro level. The IAB also observes that application protocols that include dynamic port negotiation for both ends of a connection tend to add to the complexity of the applications.

Dynamic port negotiation for a protocol may also limit or prohibit its use in situations where the service provider (e.g. ISP or employer) has instituted some form of service filtering through port blocking mechanisms.

From this perspective of network and application utility, it is preferable that no action or activity be undertaken by any agency, carrier, service provider or organization which would tend to cause end-users and protocol designers to generally obscure service identification information from the IP packet header.

Nothing in this statement should be construed as opposing encapsulation, application security, end-to-end encryption, or other processes beneficial or specifically desired by the end-users.

4. Security Considerations

This document is a general statement regarding appropriate processing

and use of service identifiers by intermediate systems. If enough agencies, carriers, service providers and organizations ignore the concerns voiced here, the utility of port and protocol numbers, general network analysis, end-user beneficial filtering (e.g. preventing DDOS attacks), and other common uses of these service identifiers might be adversely affected.

References

[1] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[2] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[3] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[4] Braden, B., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[6] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[7] Farinacci, D., Li, T., Hanks, S., Meyer, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[8] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[9] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[10] New York Times, "STUDENTS EVADE UNIVERSITY TACTICS TO PROTECT MEDIA FILES", 27th November 2002.

[11] IANA, "IANA Protocol Numbers and Assignment Services", May 2003, <http://www.iana.org/numbers.htm>.

[12] IANA, "IANA Protocol Number Registry", May 2003, <http://www.iana.org/assignments/protocol-numbers>.

[13] IANA, "IANA Port Number Registry", May 2003, <http://www.iana.org/assignments/port-numbers>.

Authors' Addresses

Mike St Johns
Internet Architecture Board

Geoff Huston
Internet Architecture Board

Appendix A. IAB Members

Internet Architecture Board Members at the time this document was completed were:

Bernard Aboba
Harald Alvestrand
Rob Austein
Leslie Daigle, Chair
Patrik Faltstrom
Sally Floyd
Jun-ichiro Itojun Hagino
Mark Handley
Geoff Huston
Charlie Kaufman
James Kempf
Eric Rescorla
Michael StJohns

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Acknowledgment

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