Network Working Group
Request for Comments: 1455

D. Eastlake, III
Digital Equipment Corporation

May 1993

Physical Link Security Type of Service

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. Discussion and suggestions for improvement are requested. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This RFC documents an experimental protocol providing a Type of Service (TOS) to request maximum physical link security. This is an addition to the types of service enumerated in RFC 1349: Type of Service in the Internet Protocol Suite. The new TOS requests the network to provide what protection it can against surreptitious observation by outside agents of traffic so labeled. The purpose is protection against traffic analysis and as an additional possible level of data confidentiality. This TOS is consistent with all other defined types of service for IP version 4 in that it is based on link level characteristics and will not provide any particular guaranteed level of service.

1. Nature of Requirement

This Internet Protocol addition addresses two potential security requirements: resistance to traffic analysis and confidentiality. These are described in the two subsections below followed by a discussion of why links have different levels of physical security so that it is meaningful to request that more secure links be used.

1.1 Traffic Analysis

At this time all Internet Protocol (IP) packets must have most of their header information, including the "from" and "to" addresses, in the clear. This is required for routers to properly handle the traffic even if a higher level protocol fully encrypts all bytes in the packet after the IP header. This renders even end-to-end encrypted IP packets subject to traffic analysis if the data stream can be observed. While traffic statistics are normally less sensitive than the data content of packets, in some cases activities of hosts or users are deducible from traffic information.

It is essential that routers have access to header information, so it is hard to protect traffic statistics from an adversary with inside access to the network. However, use of more secure physical links will make traffic observation by entities outside of the network more difficult thus improving protection from traffic analysis.

No doubt users would like to be able to request a guaranteed level of link security, just as they would like to be able to request a guaranteed bandwidth or delay through the network. However, such guarantees require a resource reservation and/or policy routing scheme and are beyond the scope of the current IP Type of Service facility.

Although the TOS field is provided in all current Internet packets and routing based on TOS is provided in routing protocols such as OSPF [See 5,6,7], there is no realistic chance that all of the Internet will implement this additional TOS any time in the foreseeable future. Nevertheless, users concerned about traffic analysis need to be able to request that the physical security of the links over which their packets will be pass be maximized in preference to other link characteristics. The proposed TOS provides this capability.

1.2 Confidentiality

Use of physical links with greater physical security provides a layer of protection for the confidentiality of the data in the packets as well as traffic analysis protection. If the content of the packets are otherwise protected by end-to-end encryption, using secure links makes it harder for an external adversary to obtain the encrypted data to attack. If the content of the packets is unencrypted plain text, secure links may provide the only protection of data confidentiality.

There are cases where end-to-end encryption can not be used. Examples include paths which incorporate links within nations which restrict encryption, such as France or Australia, and paths which incorporate an amateur radio link, where encryption is prohibited. In these cases, link security is generally the only type of confidentiality available. The proposed TOS will provide a way of requesting the best that the network can do for the security of such unencrypted data.

This TOS is required for improved confidentiality, especially in cases where encryption can not be used, despite the fact that it does not provide the guarantees that many users would like. See discussion at the end of the Traffic Analysis section above.

1.3 Link Physical Security Characteristics

Physical links, which are composed of lines and routers, differ widely in their susceptibility to surreptitious observation of the information flowing over them. For examples of line security see the following list:

1) Land line media is usually harder to intercept than radio broadcast media.

2) Between different radio broadcast media, spread spectrum or other low probability of intercept systems, are harder to intercept than normal broadcast systems. At the other extreme, systems with a large footprint on the earth, such as some satellite down links, may be particularly accessible.

3) Between land lines, point to point systems are generally harder to intercept than multi-point systems such as Ethernet or FDDI.

4) Fiber optic land lines are generally harder to intercept than metallic paths because fiber is harder to tap.

5) A secure land line, such as one in pressurized conduit with pressure alarms or one installed so as to be observable by guards, is harder to intercept than an unsecured land line.

6) An encrypted link would be preferable to an unencrypted link because, even if it was accessed, it would be much more difficult to obtain any useful information.

Routers also have different levels of security against interception depending on the physical security of the router site and the like.

The above comparisons show that there are significant real differences between the security of the physical links in use in the Internet. Choosing links where it is hard for an outside observer to observe the traffic improves confidentiality and protection against traffic analysis.

2. Protocol Specification

The value 15 decimal (F hex) in the four-bit Type of Service IP header field requests routing the packet to minimize the chance of surreptitious observation of its contents by agents external to the network. (This value is chosen to be at the maximum hamming distance from the existing other TOS values.)

3. Protocol Implementation

This TOS can be implemented in routing systems that offer TOS based routing (as can be done with OSPF, see RFCs 1245 through 1247) by assigning costs to links. Establishing the "cost" for different links for this TOS is a local policy function.

In principle services are incomparable when criterion such as those given in the Nature of Requirement section above conflict. For example, a choice between an encrypted broadcast system and an unencrypted fiber optic land line. In practice, link encryption would probably dominate all other forms of protection and physical security as mentioned in criterion 5 above would dominate other land line distinctions.

An example of "costs" at a hypothetical router could be as follows:

Cost	Type
1	Strong encryption with secure key distribution
2	Physically secure point-to-point line
6	Typical point-to-point line
8	Typical local multi-point media
12	Metropolitan area multi-point media
24	Local radio broadcast
32	Satellite link

Link costs should be chosen so as to be in the same ratio as the probability of interception. Thus the above example costs imply a local policy assumption that interception is 32 times more likely on a satellite link and associated router than on a strongly encrypted line and its associated router. It is not necessary to estimate the absolute probability of interception on any particular link. It is sufficient to estimate the ratio between interception probabilities on different links.

It should be noted that using costs such as the example given above could result in using many more links than if the default type of service were requested. For example, the use of over 50 highly secure links could be better than using two insecure links, such as an unencrypted satellite hop and radio link. However, if the costs have been properly set in proportion to the probability of interception, this larger number of links will be more secure than the shorter default routing. This consideration should make it clear why it is necessary to estimate router security as well as link security. An excessive cost ratio based solely on the security of a communications line could cause packets to go through many routers which were less secure than the lines in question. This necessity to take router characteristics into account is also present for all

other defined TOS values.

It should also be noted that routing algorithms typically compute the sum of the costs of the links. For this particular type of service, the product of the link probabilities of secure transmission would be more appropriate. However, the same problem is present for the high reliability TOS and the use of a sum is an adequate approximation for most uses as noted in RFC 1349.

References

[1] Postel, J., "Internet Protocol - DARPA Internet Program Protocol Specification", STD 5, RFC 791, DARPA, September 1981.

[2] Braden, R., Editor, "Requirements for Internet Hosts -- Communication Layers", STD 3, RFC 1122, IETF, October 1989.

[3] Braden, R., Editor, "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, IETF, October 1989.

[4] Almquist, P., "Type of Service in the Internet Protocol Suite", RFC 1349, Consultant, July 1992.

[5] Moy, J., Editor, "OSPF Protocol Analysis", RFC 1245, Proteon, Inc., July 1991.

[6] Moy, J., Editor, "Experience with the OSPF Protocol", RFC 1246, Proteon, Inc., July 1991.

[7] Moy, J., "OSPF Version 2", RFC 1247, Proteon, Inc., July 1991.

Security Considerations

The entirety of this memo concerns an Internet Protocol Type of Service to request maximum physical link security against surreptitious interception.

Author's Address

Donald E. Eastlake, III
Digital Equipment Corporation*
30 Porter Road, MS: LJO2/I4
Littleton, MA 01460

Phone: +1 508 486 2358 (w), +1 617 244 2679 (h)
Email: dee@ranger.enet.dec.com

*Company affiliation given for identification only. This document does not constitute a statement, official or otherwise, by Digital Equipment Corporation.