Network Working Group
INTERNET-DRAFT
Category: Informational

T. Doty
Network Systems Corp.
A. Molitor
Network Systems Corp.
August 1996

Proposed Mechanism for Self-Labeling of Content

<draft-rfced-info-molitor-00.txt>

Status of this Memo

Introduction

The wide-spread availability of information on the Internet which is deemed by some to contain objectionable content has led to calls by governmental and other bodies for a mandatory content label. It is suggested that the existing IP Security Options might be used as a method for self regulation by individuals offering information to the Internet community. It is further suggested that the options would allow a content labeling analogous to that used by the Motion Picture Industry (G, PG, R, NC-17) and television broadcasters (Adult Situations, Violence, Nudity, etc.). Since these IP options are well understood by the technical community, such a mechanism of self-labeling would be compatible with existing, deployed internetworking equipment.

The naming of the various ratings and content categories is undeniably USA-centric, for which the authors apologize. We hope to define the terms sufficiently to make the meaning clear to the global readership.

Definitions

Herein the word 'provider' or 'content provider' refers to the originator of a datagram. The model here is a host providing information content via any of a variety of possible protocols, to users of the Internet at large, either for a fee, or not.

The word 'local authority' is meant relative to the recipient of a datagram, and is intended to mean an authority local to that recipient. The model here is the campus network administration, or an Internet Service Provider through which a customer of a content provider gains Internet access.

General Content Label

The Basic Security Option (BSO) [1] describes a mechanism for labeling information according to military classification level (Unclassified, Confidential, Secret, or Top Secret). It is proposed that this field be used to label information according to the appropriateness of the audience: G (General audience, including small children), PG (Parental Guidance suggested for non-adolescent children), R (Restricted to adults), or NC-17 (inappropriate for children under the age of maturity). Since IP is globally deployed, and since opinions of what is and is not appropriate do vary across the globe, it is worth pointing out that this re-interpretation of the BSO provides a mechanism for agents to attach that agent's rating. In essence, this permits an opinion of the probable content of the payload to be attached to the datagram, which the recipient may or may not choose to examine. It is therefore quite by design that some information about the rating authority be included with the rating information. The format of the Basic Security Option is shown in Figure 1. The Basic Security Option has an assigned value of 0x82 (decimal 130).

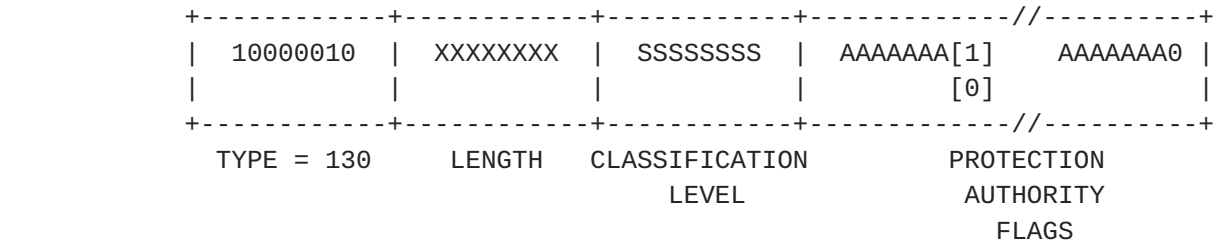

Figure 1. The Basic Security Option

To maximize the compatibility with existing deployed equipment, it is suggested that the same mappings be used that are currently defined for classification levels. The mappings defined in [1] are shown in Figure 2, along with the suggested new content labels. It is suggested that the obsolete mappings as specified in [2] be used for self rating, to avoid possible confusion with datagrams containing an actual security classification level.

Old Label	New Label	Value
Unclassified	G	0x55
Confidential	PG	0x7a
Secret	R	0xad
Top Secret	NC-17	0x3d

Figure 2. Specific Definitions for Label Values

[1] defined a Protection Authority Flag (PAF) that represented the classifying agency. It is suggested that this field be used to specify the identify of the rating agency that determined the content label. Currently, it is expected that most information labeled will be self-labeled (i.e. the content label will be assigned by the content provider); however, data could certainly be labeled by other agents, for example private companies who label data for a fee, or a local authority. It is suggested that two values be initially defined: 0 (labeled by the content provider) and 1 (labeled by a local authority).

It is surely very difficult to determine automatically the content of a datagram, for rating purposes. Thus, datagrams which are not explicitly labeled by the content provider can probably only be usefully be labeled based on the source IP address. However, this is still useful, since a local authority could potentially do the difficult work of mapping a large table of IP addresses into ratings at a location in the network where it can be most easily done. These ratings will then be carried with the packets, and can be very easily checked later, where the entire mapping table would be very inconvenient to manage.

Specific Content Label

The Extended Security Option (ESO) can be used to add additional content information. An ESO consists of a option code, 0x85, followed by a one octet length field, followed by a one octet 'source' ID, and lastly a bit field consisting of a variable number of octets, shown below as simply additional security information. More than one ESO

may be present in an IP header.

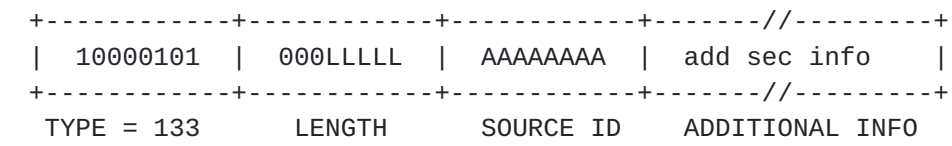

Figure 3. Extended Security Option

Widely available implementations of ESO processing software (DNSIX, see [3]) check ESOs found in datagrams arriving on an interface against a table of source IDs configured for that interface. The IDs found in the table identify whether to interpret ESOs with the indicated IDs as Network Layer ESOs (NLESOs), or Auxiliary ESOs (AESOs). This table of ESO source IDs and associated data is called an accreditation table, in the DNSIX documentation.

Every ESO found in a datagram must have a source ID found in the interface's table. For AESOs, this is sufficient, and the bit field present in the datagram option is ignored. For NLESOs, the interface's table has a pair of bit fields defined for each NLESO in the table, the so called maximum sensitivity and minimum sensitivity. In order for an NLESO present in the datagram to be valid, all bits set to 1 in the minimum sensitivity must be set to 1 in the datagram, and no bits which are not 1 in the maximum may be set to 1 in the datagram. Any DNSIX implementation must support bit fields up to 128 bits wide, so there is quite a lot of room for new content types.

We propose that the NLESO could be used to provide finer grained information about content potentially present in the datagram payload. In particular, the positions in the bit field may be used to represent various types of contents, and the source ID to represent the rating authority. Proposed assignments for source ID are limited to the content provider, whoever sent the datagram initially, and a general local authority, typically a rating authority located on the datagram recipient's network providing rating service directly to the recipient. This leaves a large set of other authorities.

Rating Authority	Source ID
Content Provider	0x01
Local Authority	0x02

Figure 4. Specific Definitions for Source IDs

For the two rating authorities defined above, the following bit values are defined, borrowing from the cable television industry in the USA:

Content Type	Bit Value
Language	0x80
Violence	0x40
Nudity	0x20
Adult Themes	0x01

Figure 5. Specific Definitions for Content Type Bits

Note that the intended semantics of an NLESO here are 'In the opinion of the rating authority indicated by the source ID, the payload of this packet may contain material of the indicated types which may be offensive to some.'

It is worth noting here that the BSO, as re-interpreted above, may well provide all the necessary information for a given recipient of datagrams.

Examples

A packet rated simply as PG-13, by the originator of the packet, would have a BSO of the form:

0x82 0x04 0x7a 0x00

A packet rated as R by the content provider, with additional information added by a local rating device indicating the possible presence of objectionable violent content would have a BSO:

0x82 0x04 0xad 0x00

and an NLESO of the form:

0x85 0x05 0x02 0x40 0x00

An end customer, wishing to restrict access to the most objectionable material would configure their attachment point to the network to be a multi-level interface accepting datagrams marked Unclassified (G, in the interpretation of this document) through Secret (R, in the interpretation of this document), but not Top Secret (NC-17, herein). In addition, the relevant interface would be configured to implicitly label unlabeled datagrams as, perhaps, Unclassified. Thus, only datagrams explicitly labeled as NC-17 would be rejected.

If a customer wished to accept G through R content, but wished in addition to reject packets which might contain, say, violent content, the following accreditation table on the attachment interface could be used.

Source ID	ESO Type	Min	Max
0x01	NLESO	0x00	0x40
0x02	NLESO	0x00	0x40

Figure 6. Sample Accreditation Table

Oddly enough, by specifying non-zero fields in the Min column, a customer could insist that any ESO-encoded rating must rate the content as having certain objectionable content. No packets without objectionable language, please. This last point truly illustrates that this is a labeling mechanism, not a device for censorship.

Interoperability and Deployment

Since IP options which are not understood by a host are ignored, this system of ratings is quite transparent to those not taking part in it.

Deployment must, by necessity of the culture of the Internet, be entirely voluntary. There are widely deployed DNSIX implementations available in network routers (several router vendors provide the capability, it is probably fair to say that the majority of deployed routers have at least limited DNSIX capability built in, but not enabled by the customer) and DNSIX implementations available for network hosts (Compartmented Mode Workstations offer the possibility of true mixed-content archive servers). Rating by providers would therefore typically be a matter of configuration of existing or widely available equipment. All that is required is the desire to provide rating information, and an agreed upon set of definitions. We hope that this document can serve for the latter.

Security Considerations

This memo raises no security issues, though it does re-use the IP Security Options.

References

[1] Kent, S. "U.S. Department of Defense Security Options for the Internet Protocol", RFC 1108, November 1991.

[2] St. Johns, M. "Draft revised IP security option", RFC 1038, January 1988.

[3] Defense Intelligence Agency, "DNSIX Detailed Design Specification Version 2.1", DDS-2600-5985-91, October 1991.

Authors' Addresses

Andrew Molitor
Network Systems Corp. MS 718
7625 Boone Ave. N
Brooklyn Park, MN, 55428

Ted Doty
Network Systems Corp.
7600 Boone Ave. N
Brooklyn Park, MN, 55428