

Requirements and Scenarios for a Voluntary Access Control System
<[draft-hardie-vac-req-01.txt](#)>

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Distribution of this memo is unlimited.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the "lid-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

Abstract

This document specifies the requirements and fundamental scenarios for a Voluntary Access Control system, based on the content rating of Internet resources and subsequent filtering of which resources may be accessed.

1. Introduction

The availability on the Internet of a variety resources, intended for many different audiences, causes concern to some members of the Internet community and to other members of the societies in which the Internet is found. This concern suggests the development of a method for creating and transmitting content information for Internet resources, so that users may create filters which eliminate material they would find offensive or inappropriate.

In this document, the requirements are set out for a voluntary access control system. It is presumed that such a system will be composed of several interlocking elements. One element of that system will be a label format for content information.

A second element will be a transport method or methods for supplying that content information. A third element will be a set of rules applied to the content information in order to filter access. Requirements for the third element are described in this document only functionally. Examples within this draft may refer to particular content ratings or rule sets, but these should not be taken as labels or rules which must be implemented for

conformance. A very small number of labels may be reserved by VAC authors, but it is the intent of the author of this draft that any system built according to the requirements described here be both extensible and entirely value-neutral.

1.1 Terminology

Interactive Internet Resources:

Internet resources in which a user chooses to participate in an interaction, with or without knowledge of the other participants. Examples include mailing lists to which users subscribe and chat systems such as IRC.

May:

This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option **MUST** be prepared to interoperate with another implementation which does include the option.

Must:

This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

Must not:

This phrase means that the definition is an absolute prohibition of the specification.

Should:

This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

Transaction:

A complete VAC action, consisting of a request from the client and a response from the server.

User-retrieved Internet Resources:

Internet resources or information collections made available by an information provider through protocols in which a user initiates the retrieval of items from the collection. Examples of user initiated processes include ftp, gopher, and http.

1.2 Scope

A VAC system must be able to handle labels applied to user-retrieved Internet Resources. A VAC system may choose to apply labels to Interactive Internet Resources.

2. Scenarios

2.1 An adult wishes to limit a child's access to the material on the Internet, eliminating all access to all material having certain characteristics.

2.2 Teachers wish to use structured browsing as a learning activity and would like to limit student access to Internet resources that have been identified as appropriate to particular topics.

2.3 A browser user wishes to reduce time wasted in exploring sites which are low-quality and would like to have prior knowledge of which sites have been designated as well-designed or interesting.

2.4 A trainer wishes to demonstrate the usefulness of the Internet to a group of novice users and would like to eliminate access to material having certain characteristics and to highlight material which has been designated as well-designed or interesting.

3. Scenario Implications

The scenarios listed above can be described as enabling a user to create virtual "blacklists", "whitelists", and "goldlists". In 2.1, the user wishes to create a virtual blacklist, eliminating all access to certain materials, but leaving open access to all other materials. In 2.2, the reverse occurs; the user wishes to designate certain materials as appropriate and eliminate access to all other

materials, thus creating a virtual whitelist. In 2.3, the user may access any material, but will prefer certain materials which have been placed on a virtual goldlist. In 2.4, a blacklist and goldlist are used in combination to create a particular view of Internet resources.

The goals of the four users in the scenarios above could be accomplished through actual lists. Goldlists (usually described as "cool sites" or "hot lists"), in particular, have been a part of the World Wide Web almost since its inception. Creating, maintaining, and transmitting these lists is, however, inefficient, and the lists easily become out of date. A Voluntary Access Control system can accomplish the same goals as each of these list types

through interaction of a rule set and a label.

4. Label format requirements

4.1 The label format must be unambiguous. Labels must always be made up of the same number of parts which occur in the same order.

4.2 Label format must be applicable at multiple levels of granularity. For user-retrieved internet resources, this means that the label format must support ratings for collections as well as resources.

4.3 Labels must be unordered. If a client wishes to request content information embodied in several labels, the order of the label request or label response must not affect the labels' interpretation.

4.4 Labels should be human-readable. In order to make goldlists possible and to allow the user to understand the cause of any blacklisting, the client must be able to display the label to a user for interpretation. This may be accomplished by transmitting a non-human readable short form if the server is certain that the client can translate it into a human readable form.

4.5 Labels should allow the easy application of rule sets. Where numeric label characteristics can be used, they should be preferred; where numeric ranges are used, a specific range order (ascending or descending) should be established as a default.

4.6 Labels should allow the application of complex rule sets. Non-numeric and non-range numeric labels must be allowed for label characteristics, in order to allow for the application of rule sets which cannot be easily written as numeric range boundaries.

4.7 Certain labels should be reserved to preserve interoperability among implementations. Labels for date-rated, rating-originator, and a request for all the ratings available for a particular document or resource are among those which should be standardized.

5. Transport requirements.

5.1 The VAC transport protocol must be lightweight. A successful VAC transaction should take place within a single network round trip.

5.2 The VAC transport protocol should allow for persistent connections. Since some clients will browse through pages at a rapid rate, polling the same set of servers each time, persistent connections will help improve performance.

5.3 In accordance with a layered network model, VAC should be implementable over a variety of connection schemes and underlying transport protocols; it is expected however, that it will initially

be transported over TCP.

5.4 The VAC transport protocol must support proxying.

5.5 Where proxies are used, VAC should distinguish between proxies which cache the ratings of other servers and proxies which themselves filter sites which may be accessed. Where proxies are used as filter points, progress messages should indicate clearly that the proxy has prevented access to a resource when such an event occurs.

6. Rule sets requirements

6.1 Rule set syntax must support statements of inclusion, exclusion, and display. To accomplish the goals set out in 2.1, for example, the rule set would exclude all sites which are labeled as having content the adult believes is inappropriate for that child. In 2.2, the rule set will include only sites which the teachers have labeled as appropriate to the lesson. In 2.3, the labels for particular sites or objects would be displayed along with the links to the objects, so that the user may choose those which appeal most. In 2.4, a rule of exclusion is applied prior to displaying labels for available objects. More complex rule sets are, of course, possible and encouraged.

7. Authentication requirements

7.1 VAC must support the authentication of the label server to the client. Given that ratings servers will likely be subject to attempts at spoofing, authentication of the server to the client is essential.

7.2 VAC should support the authentication of the client to the server. Since some ratings services will be commercial enterprises, client authentication should be supported.

7.3 VAC should be compatible with multiple mechanisms for authentication, in order to accommodate variable site policies and the vagaries of encryption regulations.

8. Intellectual property requirements

8.1 VAC may allow encryption of the rating. Since commercial enterprises will invest time and capital in the creation of labels, encryption may be necessary to protect this intellectual capital. When available, VAC should use Internet-standard methods for session encryption and authentication. Until such methods are standard, VAC may allow a client and server to encrypt the rating, using methods agreed on in out-of-band negotiations.

Acknowledgments

The author would like to acknowledge the useful discussions of members of the `vac-wg@naic.nasa.gov` mailing list and the attendees of the IETF "Read the Label" BOF at the Stockholm IETF.

Security Considerations

As noted in sections [7](#) and [8](#) above.

Author's Addresses

Edward Hardie -- `hardie@nasa.gov`
Network Applications and Information Center
NASA Ames Research Center
Mail Stop 204-14
Moffett Field, CA 94035-1000
Tel: 1.415.604.0134
Fax: 1.415.604.0978