Network Working Group
Request for Comments: 1414

M. St. Johns
US Department of Defense
M. Rose
Dover Beach Consulting, Inc.

February 1993

Identification MIB

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. 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 memo defines a MIB for use with identifying the users associated with TCP connections. It provides functionality approximately equivalent to that provided by the protocol defined in RFC 1413 [1]. This document is a product of the TCP Client Identity Protocol Working Group of the Internet Engineering Task Force (IETF).

Table of Contents

1. The Network Management Framework

The Internet-standard Network Management Framework consists of three components. They are:

STD 16/RFC 1155 [2] which defines the SMI, the mechanisms used for describing and naming objects for the purpose of management. STD 16/RFC 1212 [3] defines a more concise description mechanism, which is wholly consistent with the SMI.

STD 17/RFC 1213 [4] which defines MIB-II, the core set of managed objects for the Internet suite of protocols.

STD 15/RFC 1157 [5] which defines the SNMP, the protocol used for network access to managed objects.

The Framework permits new objects to be defined for the purpose of experimentation and evaluation.

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Within a given MIB module, objects are defined using RFC 1212's OBJECT-TYPE macro. At a minimum, each object has a name, a syntax, an access-level, and an implementation-status.

The name is an object identifier, an administratively assigned name, which specifies an object type. The object type together with an object instance serves to uniquely identify a specific instantiation of the object. For human convenience, we often use a textual string, termed the object descriptor, to also refer to the object type.

The syntax of an object type defines the abstract data structure corresponding to that object type. The ASN.1 [6] language is used for this purpose. However, RFC 1155 purposely restricts the ASN.1 constructs which may be used. These restrictions are explicitly made for simplicity.

The access-level of an object type defines whether it makes "protocol sense" to read and/or write the value of an instance of the object type. (This access-level is independent of any administrative authorization policy.)

The implementation-status of an object type indicates whether the object is mandatory, optional, obsolete, or deprecated.

2. Identification MIB

The Identification MIB defines a uniform set of objects useful for identifying users associated with TCP connections. End-systems which support TCP may, at their option, implement this MIB. However, administrators should read Section 4 ("Security Considerations") before enabling these MIB objects.

3. Definitions

```
        RFC1414-MIB DEFINITIONS ::= BEGIN

        IMPORTS
            OBJECT-TYPE
                FROM RFC-1212
            tcpConnLocalAddress, tcpConnLocalPort,
            tcpConnRemAddress, tcpConnRemPort
                    FROM RFC1213-MIB;


        ident   OBJECT IDENTIFIER ::= { mib-2 24 }


        -- conformance groups

        identInfo       OBJECT IDENTIFIER ::= { ident 1 }


        -- textual conventions

        -- none

        -- the ident information system group
        --
        -- implementation of this group is mandatory

        identTable OBJECT-TYPE
                SYNTAX  SEQUENCE OF IdentEntry
                ACCESS  not-accessible
                STATUS  mandatory
                DESCRIPTION
                    "A table containing user information for TCP
                    connections.

                    Note that this table contains entries for all TCP
                    connections on a managed system.  The
                    corresponding instance of tcpConnState (defined in
                    MIB-II) indicates the state of a particular
```

```
                connection."
            ::= { identInfo 1 }

        identEntry OBJECT-TYPE
                SYNTAX  IdentEntry
                ACCESS  not-accessible
                STATUS  mandatory
                DESCRIPTION
                    "User information about a particular TCP
                    connection."
                INDEX   { tcpConnLocalAddress, tcpConnLocalPort,
                          tcpConnRemAddress, tcpConnRemPort }
                ::= { identTable 1 }

        IdentEntry ::=
            SEQUENCE {
                identStatus     INTEGER,
                identOpSys      OCTET STRING,
                identCharset    OCTET STRING,
                identUserid     OCTET STRING,
                identMisc       OCTET STRING
            }

        identStatus OBJECT-TYPE
                SYNTAX  INTEGER {
                            noError(1),
                            unknownError(2)
                        }
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                    "Indicates whether user information for the
                    associated TCP connection can be determined.  A
                    value of 'noError(1)' indicates that user
                    information is available.  A value of
                    'unknownError(2)' indicates that user information
                    is not available."
                ::= { identEntry 1 }

        identOpSys OBJECT-TYPE
                SYNTAX  OCTET STRING (SIZE(0..40))
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                    "Indicates the type of operating system in use.
                    In addition to identifying an operating system,
                    each assignment made for this purpose also
                    (implicitly) identifies the textual format and
```

```
                maximum size of the corresponding identUserid and
                identMisc objects.

                The legal values for the 'indentOpSys' strings
                are those listed in the SYSTEM NAMES section of
                the most recent edition of the ASSIGNED NUMBERS
                RFC [8]."
            ::= { identEntry 2 }


        identCharset OBJECT-TYPE
                SYNTAX  OCTET STRING (SIZE(0..40))
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                    "Indicates the repertoire of the corresponding
                    identUserid and identMisc objects.

                    The legal values for the 'identCharset' strings
                    are those listed in the CHARACTER SET section of
                    the most recent edition of the ASSIGNED NUMBERS
                    RFC [8]."
                ::= { identEntry 3 }

        identUserid OBJECT-TYPE
                SYNTAX  OCTET STRING (SIZE (0..255))
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                    "Indicates the user's identity.  Interpretation of
                    this object requires examination of the
                    corresponding value of the identOpSys and
                    identCharset objects."
                ::= { identEntry 4 }

        identMisc OBJECT-TYPE
                SYNTAX  OCTET STRING (SIZE (0..255))
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                    "Indicates miscellaneous information about the
                    user.  Interpretation of this object requires
                    examination of the corresponding value of the
                    identOpSys and identCharset objects."
                ::= { identEntry 5 }


        END
```

4. Security Considerations

The information available through this MIB is at most as trustworthy as the host providing it OR the organization operating the host. For example, a PC in an open lab has few if any controls on it to prevent a user from having an SNMP query return any identifier the user wants. Likewise, if the host has been compromised the information returned may be completely erroneous and misleading.

This portion of the MIB space should only be used to gain hints as to who "owns" a particular TCP connection -- information returned should NOT be considered authoritative for at least the reasons described above. At best, this MIB provides some additional auditing information with respect to TCP connections. At worse it can provide misleading, incorrect or maliciously incorrect information.

The use of the information contained in this MIB for other than auditing or normal network management functions is strongly discouraged. Specifically, using information from this MIB space to make access control decisions - either as the primary method (i.e., no other checks) or as an adjunct to other methods may result in a weakening of normal system security.

This MIB provides access to information about users, entities, objects or processes which some systems might normally consider private. The information accessible through this MIB is a rough analog of the CallerID services provided by some phone companies and many of the same privacy consideration and arguments that apply to CallerID service apply to this MIB space. If you wouldn't run a "finger" server [7] due to privacy considerations, you might not want to provide access to this MIB space on a general basis. Access to this portion of the MIB tree may be controlled under the normal methods available through SNMP agent implementations.

7. References

[1] St. Johns, M., "Identification Protocol", RFC 1413, US Department of Defense, February 1993.

[2] Rose M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based internets", STD 16, RFC 1155, Performance Systems International, Hughes LAN Systems, May 1990.

[3] Rose, M., and K. McCloghrie, Editors, "Concise MIB Definitions", STD 16, RFC 1212, Performance Systems International, Hughes LAN Systems, March 1991.

[4] McCloghrie K., and M. Rose, Editors, "Management Information Base for Network Management of TCP/IP-based internets", STD 17, RFC 1213, Performance Systems International, March 1991.

[5] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, RFC 1157, SNMP Research, Performance Systems International, Performance Systems International, MIT Laboratory for Computer Science, May 1990.

[6] Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), International Organization for Standardization, International Standard 8824, December 1987.

[7] Zimmerman, D., "The Finger User Information Protocol", RFC 1288, Center for Discrete Mathematics and Theoretical Computer Science, December 1991.

[8] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.

8. Authors' Addresses

Michael C. St. Johns
U.S. Department of Defense
DARPA/CSTO
3701 N. Fairfax Dr
Arlington, VA 22203

Phone: (703) 696-2271
EMail: stjohns@DARPA.MIL

Marshall T. Rose
Dover Beach Consulting, Inc.
420 Whisman Court
Mountain View, CA 94043-2186

Phone: (415) 968-1052
EMail: mrose@dbc.mtview.ca.us