ENTERPRISE DIRECTORY SUPPORT FOR FUTURE SNMPV3 NETWORK MANAGEMENT APPLICATIONS

S. Omari[1]. R.Boutaba[2], O.Cherkaoui[3]

[1]Laboratoire PRiSM
Université de Versailles
45, avenue des Etats-Unies
78000 Versailles, France

[2]ECE Department
University of Toronto
10 king's college road
Toronto, On Canada, M5S 3G4

[3]Laboratoire d'informatique
Université UQAM
CP 8888, Succursale Centre-Ville
Montréal, Qc, Canada, H3C 3P8

Abstract

The work presented in this paper falls in the perspective to use management policies to configure the new SNMPv3 entities, to regulate SNMPv3 management exchanges and to customize security features according to th e enterprise needs. It particularly addresses the configuration of access control parameters to be implemented by SNMPv3 entities according to enterprise security policies. The overall process is supported by means of a directory service used as a repository for both SNMPv3 configuration parameters and security policies. The implemented directory information model complies with the DEN (Directory Enabled Networking) specification, which is gaining great acceptance into enterprises.

1. Introduction

Data security and maintaining system integrity are the primary concerns pointed out by corporations and individuals when connecting to the Internet. The newest version of the Internet management standard, SNMPv3, overcomes the weakness of the previous versions of the protocol by allowing authentication, privacy and access control to be performed during the exchange of messages between SNMPv3 entities (i.e., SNMPv3 managers and agents). This functionality is performed within the entity subsystems, more precisely by the security subsystem and the access control subsystem. The modular architecture of the entity, as defined by the IETF (Internet Engineering Task Force), allows these subsystems to implement different security models. The models currently defined with SNMPv3 management are: USM (User-based Security Model) [4]; and VACM (View-based Access Control Model) [3]. These additions allow the SNMPv3 management platform to claim reliability and hence readiness to be introduced into enterprise network management. However, the various SNMPv3 entities, within a given administrative domain, must be configured consistently so as to reflect and enforce the enterprise security policies. It is the role of the manager to configure the SNMPv3 entities and to initialize/modify the security parameters which shape the behavior of these entities with respect to security. In current practices, configuration information and security parameters/policies are maintained in distinct data stores, in multiple formats, and possibly by different managers. This may lead to inconsistent management decisions, which may lead, in turn, to the enforcement of conflicting security policies, and hence to the jeopardizing of the enterprise information security.

This paper aims at tackling this problem, that is to implement consistent models for security policies/parameters within a uniform, enterprise wide, logically centralized and physically distributed information store. In general, this approach will reduce the complexity of the task of managing large corporate networks. In particular, it will facilitate the proper configuration of SNMPv3 entities and ultimately its automation. Central to the proposed approach is a directory service used to store and access information about users, network devices, and applications including management applications. The adopted directory service allows various network applications and services to share information accessed through a uniform protocol, namely the Lightweight Directory Access Protocol (LDAP).

This paper emphasizes the use of a standard directory to store and access SNMPv3 security parameters used to configure and (re-)initialize SNMPv3 management entities. This is done in conjunction with the enterprise management policies, which are stored, themselves, in the directory. Security policies are hence controlled by accessing the directory in a centralized manner, this way preventing inconsistencies and conflicts. To promote interoperability between various management applications, SNMPv3 informational model is described according to the Directory Enabled Network (DEN) specification [1]. The DEN is an industry initiative standardized within the DMTF (Desktop Management Task Force) to provide a uniform model representing users, profiles, applications and network services within the directory through which management data from any source can be accessed in a common way. In this paper, we extend the DEN specifications to integrate the SNMPv3 information model.

0-7803-5796-5/99/$10.00 © 1999 IEEE

SNMPv3 persistent information is maintained in maintained by the directory service and can be shared/reused by a variety of authorized management applications and tools. Note that actual DEN specification already considers general and one purpose networking policies as a subject for modeling and storage within the directory service. This paper specifically targets enterprise security policies mapping into SNMPv3 security and access control subsystems [2]. More precisely, two policy types are considered here: Access control policies and their mapping into the VACM; and security policies and their mapping into the USM.

The automatic configuration of the SNMPv3 entities is implemented as a part of the ModularSNMPv3 project at University of Quebec At Montreal (UQAM), which essentially implements a working Modular SNMPv3 engine in Java.

This paper is organized as follows. Section 2 gives a overview of SNMP version 3 highlighting the security features, the subsystems of the SNMPv3 framework supporting these features, as well as the security models defined for these subsystems. Section 3 briefly describes the DEN specifications for enterprise network and systems management. Section 4 introduces our proposal for SNMPv3 directory-enabled management. Section 5 describes the implementation of the proposal. It describes the framework in which SNMPv3 directory-enabled management is implemented. Finally, section 6 concludes the paper.

2. SNMPv3 Management Framework

The new features of SNMPv3 include, authentication, privacy, authorization, access control and a new administrative framework based on naming of entities, policies, usernames, key management, and so on.

The SNMPv3 specifications are based on a modular architecture [5]. As depicted by Figure 1, the SNMP entity, either manager or agent, consists of an SNMP engine or several associated applications

The SNMPv3 engine consists of the dispatcher, the message processing subsystem, the security subsystem, and the access control subsystem. The dispatcher coordinates the communications between the various subsystems. The message processing subsystem prepares outgoing messages and extracts data from received messages. The security subsystem provides message security services such as integrity, authentication and privacy.

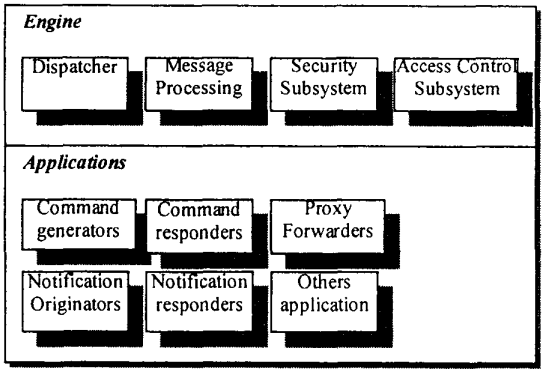

Figure 1: Architecture of SNMPv3 entities

The access control subsystem constitutes a decision making point to allow or not a specific type of access (e.g., read, write, notify) to a particular object instance. The User-based Security Model (USM), described in RFC2274 [4], is the standard security model currently used with SNMPv3. The View-Based Access Control Model (VACM), described in RFC2275 [3], is used within SNMPv3 access control subsystem. The different subsystems may support others models.

At the application level of the SNMPv3 entity, the various applications use the services provided by engine to accomplish specific tasks. Five dominant types of applications [6] can be enumerated: command generators; command responders; notification generators; notification receivers; and proxy forwarders.

The subsystems, models, and applications within an SNMP entity may need to retain their own sets of configuration information. Portions of the configuration information may be accessible as managed objects. The collection of these sets of information is referred to as an entity's Local Configuration Datastore (LCD).

In this section, we have described the new SNMP framework offering an extensible architecture composed of a set of subsystems. Each subsystem may implement different mechanisms and support multiple models. Security subsystems enforce security policies. Traditionally, security parameters are generally maintained in the MIBs encapsulated by the SNMP entities associated with the various network elements. This makes the maintenance of global security information difficult. Indeed, the various MIBs are distributed throughout the enterprise network and are more adapted for the storage of dynamic frequently changing information about the state of the devices. For persistent global management information

such as enterprise security policies, a more appropriate repository is required. A directory service, that provides a logically centralized physically distributed database for enterprise wide information and global management strategies, is a more natural alternative. In this perspective, the next sections respectively introduce directory services and their support for policy-driven management.

3. Directory services for network management

Directories are special databases that contain attribute-based information that are more descriptive than traditional relational databases. Directories are tuned to give quick-response to high-volume lookup or search operations. Each object is represented in the directory by a set of attributes. For instance, an user object is represented in the directory by attributes such as name, address telephone number and so on. The directory service can be considered as a replicated database which content is accessible through the Lightweight Directory Access Protocol (LDAP) [7].

Actual implementations of directory services support a wide scope of applications including electronic mail, printing services, and many others. The LDAP directory service has also been used as a support for the management of network equipment. It allows both network administrators and routers to store and retrieve network-related information from a single point. This allows a network administrator to manage a network more efficiently as compared to the case when persistent information such as configuration information is maintained in different databases at the levels of individual devices.

Sharing management knowledge between several and various management processes is another benefit of using a directory service. In order to permit a true exchange of network, system and service management data among heterogeneous management tools, a standard schema for describing these data is required. A recent initiative known as the DEN (Directory Enabled Network) standardized within the DMTF defines a set of abstract and concrete directory classes for modeling network elements, profiles, and services in such a way to guarantee interoperability. The considered classes concern high-level management information such as routing policies or quality of service (QoS) parameters. Based on the DEN specification, network resources can advertise themselves in the directory, discover other resources, and obtain further information about them, such as their actual configuration or a description of the services that they provide.

4. Directory-enabled SNMPv3 management

4.1. SNMPv3/DEN integrated schema and overall architecture

The integrated SNMPv3/DEN schema extends the DEN information model by adding classes that represent SNMPv3 entities. This integration facilitates the management of network devices offering SNMPv3 interfaces. The SNMPv3 classes stored in the directory are consumed by management entities directly or by network administrators through a management tool capable of parsing and displaying the specific schema structure.

The objective of the SNMPv3/DEN integration is two folds: First, to configure SNMP entities. Rather than making a connection to each device and performing a one-by-one configuration of SNMPv3 entities, the network manager only places the appropriate configuration attributes into the node's entry in the directory server. When a SNMPv3 device is initialized, its associated LDAP client queries the directory server and obtains its configuration details. Second, the use of the directory to manage at the application level, as opposed to the device level, security policies that applies to an aggregation of network devices. This way the directory server acts as a policy server, or a trader between management applications and the policy server if this later exist as a stand alone entity, accessed by the SNMPv3 entities through the associated LDAP clients to obtain access control and security policies to be enforced in the enterprise network.

The directory-based SNMPv3 management also allows :

- Enabling other applications to share information about SNMPv3 entities through the directory.
- LCD Configurations with consistent information. The configuration is applied uniformly across different SNMPv3 entities

The modularity of the SNMPv3 architecture allows to add and to remove, in a flexible way, applications into or from the SNMPv3 entity either playing the manager or the agent role. It allows add to easily incorporate a directory service client (LDAP client) into the entity application part (see figure1). This new application is launched when the SNMPv3 entity is started within a device. It requests the directory service server (LDAP server) for entity information such as entity configuration parameters or security policies.

Figure 2 shows the extension of the SNMPv3 entity architecture to include an LDAP client and thereby

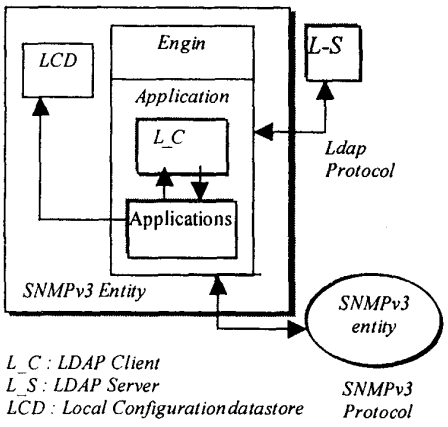

Figure 2: SNMPv3 entity architecture

integrate directory service support for SNMPv3-based management applications.

4.2. Authorization Policies

As stated previously, a second main advantage in using a directory service is to maintain enterprise management policies [8], and to promote their utilization to govern SNMPv3-based management.

In particular, the use of the directory-based policies enables:

- SNMPv3 security policies to be applied to the users profile that administer or use these entities. For example, the specification of the *username* into the USM model must be configured according to the user profile related to *username*.
- View-based access control policies and security policies to be controlled and managed by a centralized manner, and to be deployed and enforced.
- Policy centralization that allows the manager to detect easily the policies conflict [9]. Such conflicts must be resolved before populating the policy repository.

The new SNMPv3 security features should be regulated by enterprise security policies which are used to dictate the overall discipline and to control the overall network management activity. In particular, security policies will populate the directory, and retrieved at appropriate times to configure SNMPv3 entities and to drive their management behavior. This is done practically through a mapping of policy specification into SNMPv3 parameters [2].

The policy services are part of the Directory-enabled SNMPv3 Management applications. A policy server searches the relevant policies in the directory and sends them to the SNMPv3 entities. It provides the necessary consistency checks and conflict avoidance. For SNMPv3 entities that do not have such mapping application (typically SNMPv3 agent entities), they receive the configuration parameters from the SNMPv3 manager entity.

5. Implementation

The directory based SNMPv3 management is implemented within the ModularSNMPv3 project at UQAM [10]. Based on the most recent set of standards, a modular and secure network management system has been implemented to support SNMPv3 entities and protocol. A library of reusable classes of managed object are created to take advantage of the large set of already standardized managed objects in communication networks.

The implemented ModularSNMPv3 system allows dynamic binding and unbinding of the different modules at run time. It also allows to control the various modules constituting the SNMPv3 entity. All system is implemented in Java and has been demonstrated on-line on the Internet, by numerous users, and shown to perform adequately [http://www.teleinfo.uqam.ca/snmp]. We have extended this architecture with an LDAP client application, which is launched at the SNMPv3 initialization. This application retrieves the configuration parameters from the LDAP directory that has been populated by SNMPv3 specifications as part of our Directory-enabled SNMPv3 management application.

6. Conclusion

This paper shows the benefit of using a directory service to support SNMPv3 management applications and to promote interoperability between the various enterprise applications. It shows how the directory can be populated with enterprise wide information that is relevant to secure SNMPv3 management. In particular, the directory is used to store and access persistent SNMPv3 entities configuration information and enterprise security policies to be enforced by the SNMPv3 managers and agents. The implementation of security policies such as authorization policies is achieved through a mapping of policy specification to the appropriate security parameters of the SNMPv3 entities. This allows customizing the access control and security models (VACM and USM) implemented by the entities according to the enterprise-specific security requirements. Interoperability is achieved on one hand by using the standard widely accepted LDAP protocol for interacting with the directory service and on the other hand by adopting a common schema for

describing directory information. We have specified the SNMPv3 management entities using the DEN specifications by deriving SNMPv3 classes from the DEN classes hierarchy. To integrate directory service support for our SNMPv3 management system, we have implemented LDAP clients within the application layer of our SNMPv3 entities. This way, the configuration of an SNMPv3 engine is conducted through the associated LDAP client application by accessing and retrieving configuration information from a logically centralized LDAP server.

The major addition to SNMP-based management that is brought by the new version of the protocol (SNMPv3) is the security feature. Therefore, we have emphasized here the security issue by using the directory service to store and access enterprise wide security policies and to configure access control and security subsystems of the SNMPv3 management entities. A model for expressing and storing management policies is defined and its mapping into access control and security models of SNMPv3 entities (particularly VACM and USM) is provided. This will allow for enterprise policy-driven management and customized and flexible control of SNMPv3 management application. Indeed, in this approach, management policies such as security policies are not hard-coded into management applications, rather they are added, removed and modified easily by accessing the directory service. Also, this approach allows to better detect policy conflicts and ultimately prevent their occurrence.

As to the future, the development of a policy server is being undertaken to allow for automatic management of policies including their storage in the directory, the retrieval of policies from the directory and the provision of the necessary consistency checks and conflict avoidance. This development aims at integrating the COPS (Common Open Policy Service) protocol specification [11] for exchanging policies between the policy server and the SNMPv3 entities. Also planned is the development of demonstrator application of the directory-based and policy driven management to support differentiated services IP and ultimately provide IP-based enterprise Virtual Private Networks.

Bibliography

[1] Judd, Strassner, "Directory Enabled Networks - Information Model and Base Schema", Draft version 3.0c5, August 1998.

[2] Omari, Boutaba, Cherkaoui, "Policies for SNMPv3-based management", IEEE IM'99, Mai 1999.

[3] Wijnen, Presuhn, McCloghrie, "View-based Access Control Model for version 3 the Simple Network Management Protocol (SNMP)", RFC 2275, November1998.

[4] Blumenthal, Wijnen, "User-Based Security Model for version 3 of the Simple Network Management Protocol (SNMP)", RFC 2274, November 1998.

[5] Harrington, Presuhn, Wijnen, "An Architecture for describing SNMP Management Frameworks", RFC 2271, January 1998.

[6] Levi, Meyer, Stewart, "SNMPv3 Applications", RFC 2273, January 1998.

[7]Wahl, Coulbeck, Howles, Kille, "Lightweight Directory Access Protocol (v3): Attribute SyntaxDefinitions", RFC 2252, December 1997.

[8] Sloman, "Policy Driven Management for Distributed Systems", in Journal of Network and Systems Management, vol.2 part 4, 1994.

[9] Lupu, Sloman, "Conflict Analysis for Management Policies", IEEE IM'97.

[10] Cherkaoui, Saint Hillaire, Serhouchni, "Towards a modular and interoperable SNMPv3", IEEE NOMS'98.

[11] Boyle, Cohen, Durham, Herzog, Rajan, Sastry, "The COPS (Common Open Policy Service) Protocol ", Internet Draft. November 18, 1998