Lessons Learned

Secure Management of IP Research

July 2002

Network Associates Laboratories

Introduction

IPsec, the Internet Protocol Security protocol [10] is an open standard created by the Internet Engineering Task Force (IETF) [7] to protect network traffic. IPsec is used to create secure connections (Security Associations or SA's) across networks. It provides various methods that enable authenticated, encrypted, and compressed traffic between networks and hosts. The Securely Managing High Grade High Speed IP Devices (SMIP) project is a research project aimed at creating a standardized method for providing the IPsec configuration information necessary to securely manage a network of IPsec nodes.

Because of the large scope of the IPsec protocol, the required configuration is complex. The SMIP project is researching a standardized method to securely transmit the needed IPsec configuration information out to IPsec nodes. SMIP consists of two major parts. The first part involves creating a standardized configuration method. This entails working within the IETF's IP Security Policy Working Group (IPSP WG) [8] to create a Management Information Base (MIB) [15], the IPsec Policy Configuration MIB [5], which uses SNMPv3 for secure communication.

The other major part of the project is the development of software that implements the IPsec Policy Configuration MIB on IPsec devices and provides a management interface for the configuration of the IPsec devices. Briefly, the management software uses a graphical front end to enter configuration information for the IPsec Policy. This front end communicates with a mid-level manager which in turn transmits the configuration information out to the network nodes by setting the appropriate values in the IPsec Policy Configuration MIB.

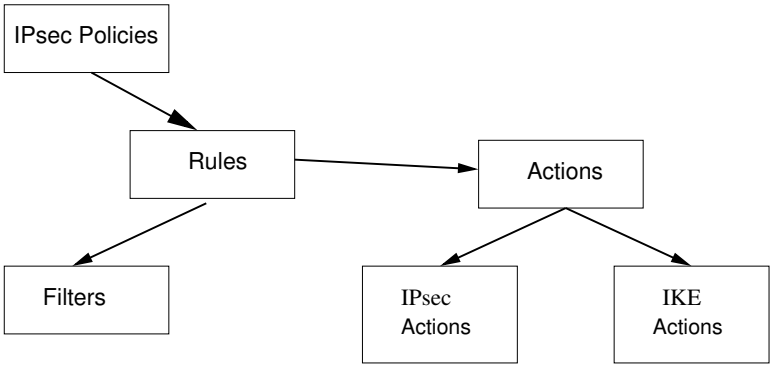

Figure 1: High Level IPsec Policy Configuration MIB View

IPsec Policy Configuration MIB

One of the goals of SMIP is to create a standardized method for configuring IPsec. To help create a standard method, the SMIP project is working within the IETF's IPsec Security Policy Working Group (IPSP WG). The IPSP WG's purpose is to develop a standardized IPsec configuration. Among the IPSP WG's goals is creating an abstract model for IPsec configuration and creating guidelines for configuring IPsec policy over protocols such as SNMP. This abstract model is currently an IETF internet-draft, the IPsec Configuration Policy Model [9]. The IPsec Configuration Policy Model is based on work by the Distributed Management Task Force (DMTF) [3]. The DMTF employs a large set of models for network management which the IPsec Configuration Policy Model references in its design.

Within the IPSP WG, the SMIP project is writing the IPsec Policy Configuration MIB to document guidelines for configuring IPsec Policy over SNMP. Figure 1 on page 2 is a simplified diagram of the MIB's design. Working within the standards process has had its advantages and disadvantages. One of the advantages is the level of interest. Attendance at IPSP Working Group meetings is high. Judging from this attendance, there is apparently a strong desire for standardized IPsec configuration. Two of the main disadvantages of a standards process, though, are the slow speed of the process and the constant change of the standard as it is developed.

Since the SMIP project started, the IPsec Configuration Policy Model has changed several times and the IPsec Policy Configuration MIB has changed to match it. One example of a change that affected the MIB is a change in the status of IKE. The Internet Key Exchange (IKE) protocol [6] is a fundamental part of IPsec. IKE is used to generate a shared key between two network nodes in order to establish a given authenticated or encrypted IPsec SA. After work on the Policy Configuration MIB had begun, the IETF decided that IKE is flawed and it has started working on a new protocol to replace IKE. This new protocol is currently referred to as Son of IKE (SOI) [12]. During one of the redesigns of the IPsec Policy Configuration MIB, therefore, one of the goals was a modularization and separation of the IKE functionality from the rest of the MIB to allow for the replacement of IKE with SOI in the future. Modularization also proved useful in dealing with MIB complexity.

Another obstacle to creating a working Policy Configuration MIB is the complexity of the protocols involved. IPsec and IKE are both complex protocols with a large number of configuration parameters. The IPsec Configuration Model is large and would be much larger if it did not reference many of the existing DMTF's models. In order to be effective, the Policy Configuration MIB has not only had to instantiate features of the IPsec Configuration Model, but also had to instantiate some of the features of the underlying DMTF models. The end result is a very large MIB. It has 28 tables and is the 2nd largest MIB currently in the IETF. To help combat size problems, a key part of the redesigns of the MIB has been modularization. Not only has IKE been separated in this fashion, but the basic parts of the model have been split into policies, filters, and actions in the MIB. This allows for easier handling of the complexity of IPsec and it allows for separate testing of the different parts of the MIB. An added advantage of the design is that it provides an architecture for the addition of new policy filters or actions in the future. Both IKE and IPsec actions can be replaceable with new actions. By creating extension tables, the MIB could even be used for network management needs other than IPsec such as flow control, generic firewall filtering, etc....

SMIP's work has also affected the IPsec Configuration Policy Model. In fact, several new features and changes to the Policy Configuration Model were direct results of the SMIP's development of the IPsec Policy Configuration MIB. An example of such a change to the model is the addition of compound actions. Initially, a rule in the IPsec Configuration Model could only have one action plus one fall-back action. The limits of this design became noticeable during MIB development and the model was changed to allow for a more complex sequence of actions to be initiated from a rule.

Difficulties in writing MIBs

The SMI [15] language is often unintuitive and few books or tutorials exist to teach it. This creates a paradox. Designing a good, efficient MIB requires first-hand experience designing MIB's. Fortunately, the IETF does have some working groups, the Evolution of SNMP (EOS) [4] and the Next Generation of Management Information Working Groups (SMING) [16] trying to improve the SNMP and SMI protocols respectively. New additions to these protocols may in the future make MIB writing easier.

[Unfortunately, both of these working groups have now been closed and no results have been produced.]

High Speed

Trying to handle a large number of packets through SMIP's IPsec filtering also affected the SMIP design. One of the key trade offs in packet handling for IPsec is between the Security Association Database (SADB) and the policies filters. The SADB is the database of the current SA's to and from a machine. The fastest way to handle a packet is to first check the SADB to see if an appropriate SA currently exists for that packet. If it does, send the packet through the existing SA. If an existing SA can

not be found, the policy filters would then be checked. Unfortunately, a receiving host using this method is placing more trust in the sending host. It assumes the traffic that the sending host transmits is correct. The receiver does not check those incoming packets against its policies. Additionally, especially with highly granular SA's, this method can cause a packet to be sent through an incorrect SA. For example, two SA's exist between the same two machines. One is for all IP traffic between the machines. The other SA is more granular and is just for SMTP (email) traffic. With the quicker, SADB first, method of checking a packet, email traffic could be sent incorrectly through a previously existing all-IP-traffic SA. A possibility for future research may be finding an efficient way to check that a packet correctly matches a policy after it matches with an SA in the SADB.

Granularity can also be an advantage to high speed IPsec processing. Although the current IPsec code in the SMIP project, plutoplus, does not support granularity beyond IP address, basing SA's on ports and services, could improve performance. Increased granularity of SA's can limit the more processor expensive SA's to the data traffic that requires them. Email could be sent over an AES encrypted SA, while web traffic is sent over an authentication only SA.

Policy filter ordering is another area that can directly affect efficient packet processing. Some filters, such as those based on IP headers, require little processing. Others, such as credential based filters, can require quite a bit of processing. By arranging filters in order from lower to higher processing requirements, overall packet processing can be increased. To allow for this type of ordering, the IPsec Configuration MIB has a priority number associated with a filter for rules that have multiple filters. Currently this ordering must be done by hand, but future additions could include wizard help in the SMIP GUI or even a filter optimization engine.

Software Development

Along with designing an IPsec Policy Configuration MIB, the SMIP project has been developing software to instantiate and use this MIB. The White Paper, *A Scalable IPsec Policy Configuration System* [11], describes some of the basic architecture of the SMIP software. A simple representation of the code's design is shown in Figure 2 on page 5. Using the SMIP code, a user can configure IPsec on remote network nodes with a web browser. The Web Server adds the configuration changes to a Database and notifies the mid-level Policy Management Engine via SNMPv3. The Policy Management Engine then processes the changes in the database and uses SNMPv3 to update the IPsec Policy Configuration MIB's on the remote IPsec Devices.

Several difficulties had to be dealt with during software development. Probably the largest difficulties are the size and the complexity of IPsec. Part of the solution to handling the configuration complexity has been to build on top of other tools. The client code (remote nodes) currently requires Linux, plutoplus for IPsec, cerebrus for IKE, iptables for filtering and net-snmp for SNMPv3 support. The mid-level manager uses Opensnmp for its SNMPv3 support and the database is MySQL. The top-level

manager uses Apache, Mod-Perl, SNMP Perl Modules and Database Perl Interfaces. Additionally, the use of these software packages by the SMIP project has ranged from difficult to easy as the software packages themselves vary in quality from beta to mature.

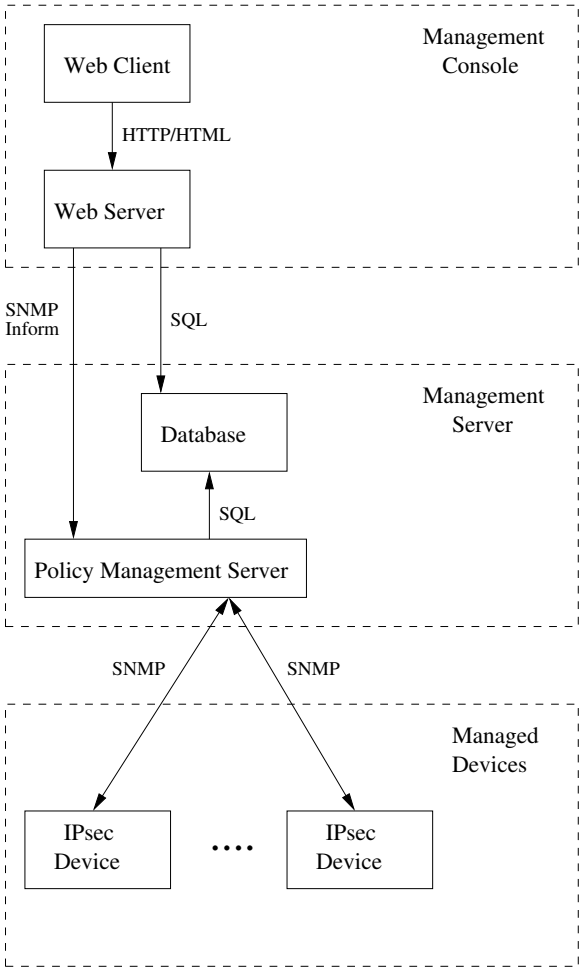

Figure 2: Top-Level SMIP Architecture

Even with the use of existing code, it has been necessary for the SMIP developers to add changes. For example, Plutoplus needed to be ported to the newest Linux 2.4 kernel. Net-snmp required a new agent API to support such a large MIB. Open-snmp required extensions to properly handle the SMI values for the mid-level manager's database access. The IPsec Policy Configuration MIB needed to be implemented in plutoplus. The software has also had to change in order to match the changes in the MIB design. Additional tables, table columns, and architecture changes have been added to the software as the MIB has changed.

Of course, while the changes to the model have affected software development, the reverse is also true. The software development implementing the IPsec Policy Configuration MIB has been invaluable to the MIB's development. The ultimate test of whether the MIB provides the pertinent information needed to create an IPsec SA between two machines is to actually build an SA based on the MIB's information. By implementing IPsec configuration based on the MIB, existing omissions in the MIB have been identified and corrected. A parameter added to the MIB and the model in order to indicate an SA's direction is one example of an important value originally missing both in the MIB and in the model, but found during implementation.

The user's graphical interface ran into the same size and complexity problems as the rest of the SMIP project. Trying to represent a large amount of data in an understandable form has proven difficult. Trying to make a complex configuration simple is equally hard.

Summary

The SMIP project is trying to develop a standardized method for configuring IPsec at remote network nodes. To do this, SMIP has been involved in the IETF's IPSP Working Group to help design a standardized configuration method, the IPsec Configuration Policy MIB. At the same time, the SMIP project has been trying to develop software that uses this MIB to configure IPsec at remote nodes using SNMPv3. Unfortunately, IPsec and IKE protocols are complex and require a large amount of configuration. Because of the size and complexity of IKE and IPsec, the software implementation has been a very important tool in testing and developing a practical, working MIB. Several optimizations having been made to the MIB and to the software design to more efficiently handle network packets, although future enhancement could be made to increase packet handling efficiency. While the standards process is slow, it has also been fruitful with much interest from the public. Using a standardized model has helped the SMIP project and the SMIP project has helped to evolve the standard model.

References

[1] R. Atkinson. IETF RFC 1825: Security architecture for the Internet Protocol, August 1995. Obsoleted by RFC2401 [10]. Status: PROPOSED STANDARD.

[2] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser. IETF RFC 1442: Structure of management information for version 2 of the Simple Network Management Protocol (SNMPv2), April 1993. Obsoleted by RFC1902 [17]. Status: PROPOSED STANDARD.

[3] DMTF. Distributed Management Task Force, Inc (DMTF). `http://www.dmtf.org/`.

[4] EOS Working Group. Evolution of SNMP Working Group. `http://www.ietf.org/html.charters/eos-charter.html`.

[5] W. Hardaker, M. Baer, R. Charlet, R. Story, and C. Wang. Ipsec policy configuration mib. Internet Draft, July 2002. http://www.ietf.org/internet-drafts/draft-ietf-ipsp-ipsec-conf-mib-04.txt.

[6] D. Harkins and D. Carrel. IETF RFC 2409: The Internet Key Exchange (IKE), November 1998. Status: PROPOSED STANDARD.

[7] IETF. The Internet Engineering Task Force. `http://www.ietf.org/`.

[8] IPSP Working Group. The IP Security Policy Working Group. `http://www.ietf.org/html.charters/ipsp-charter.html`.

[9] Jamie Jason, Lee Rafalow, and Eric Vyncke. IPsec Configuration Policy Model. Internet Draft, Feb 2002. http://www.ietf.org/internet-drafts/draft-ietf-ipsp-config-policy-model-05.txt.

[10] S. Kent and R. Atkinson. IETF RFC 2401: Security architecture for the Internet Protocol, November 1998. Obsoletes RFC1825 [1]. Status: PROPOSED STANDARD.

[11] NAI Labs. A Scalable IPsec Policy Configuration System. White Paper, November 2001.

[12] C. Madison. Son-of-IKE Requirements. Internet Draft, March 2002. http://www.ietf.org/internet-drafts/draft-ietf-ipsec-sonofike-rqts-00.txt.

[13] K. McCloghrie, D. Perkins, and J. Schoenwaelder. IETF RFC 2578, STD 58: Structure of Management Information Version 2 (SMIv2), April 1999. Status: STANDARD, `ftp://ftp.internic.net/rfc/rfc2578.txt`.

[14] K. McCloghrie, D. Perkins, and J. Schoenwaelder. IETF RFC 2579, STD 58: Textual Conventions for SMIv2, April 1999. Status: STANDARD, `ftp://ftp.internic.net/rfc/rfc2579.txt`.

[15] K. McCloghrie, D. Perkins, and J. Schoenwaelder. STD 58: Structure of Management Information version 2 (SMIv2), April 1999. See also RFC2578, RFC2579 [13, 14]. Obsoletes RFC1902 [17].

[16] SMING Working Group. Next Generation Structure of Management Information Working Group. `http://www.ietf.org/html.charters/sming-charter.html`.

[17] SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, and S. Waldbusser. IETF RFC 1902: Structure of management information for version 2 of the Simple Network Management Protocol (SNMPv2), January 1996. Obsoletes RFC1442 [2]. Status: DRAFT STANDARD.