# Security and Management in Network: Security of Network Management versus Management of Network Security (SNM Vs MNS)

**Arun Kumar Singh**
College of Computing and Informatics, Saudi Electronics University,
Abha City, Kingdom of Saudi Arabia (KSA)

ORCID ID: http://orcid.org/0000-0002-9974-4696

**Abstract:**
Everybody in the associated earth knows what a network is; it is a system of interrelated computers. A network management comprises of incremental hardware and software add-ons implemented among existing network components. The software used in accomplishing the network management tasks resides in the host computers and communications processors (e.g., front-end processors, terminal cluster controllers, bridges, routers). A network management is planned to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific points of each element and link known to the system. The effective elements of the network postulate regular feedback of status info to the network control center.

The elementary idea of networks is allowing people remote access to geographically aloof resources without having to be substantially present. It has also been deliberate to send data in return and forward, to stay linked. There are big networks and tiny networks, but size is immaterial in terms of significance of network security. The persistence of network security, quite simply, is to protect the network and its module parts from unlicensed approach and mistreatment. Networks are susceptible because of their inherent characteristic of facilitating remote access. For paradigm, if a hacker wanted to approach a computer not on a network, physical access would be vigorous. However, with networks in the picture, it is possible to side-step that particular security aspect. Therefore, it is vital for any network administrator, irrespective of the size and type of network, to implement stringent security policies to prevent probable sufferers.

In this paper, I present a common security Management Information Base (MIB) and discuss its application to representative security mechanisms, and a core set of security managed objects for use with the Simple Network Management Protocol (SNMP). Security applications are assessed for value of management via SNMP. A scenario of corporate firewalls illustrates concepts of security management correctness, sufficiency, and completeness. The main goal is to endorse a better thoughtful of the subjects and approaches to integrated, consistent security management.

**Keywords:**
*Network Management Security, Simple Network Management Protocol (SNMP), Management Information Base (MIB)*

## 1. Introduction

The persistence of network security is fundamentally to prevent loss, through mismanagement of data. There are a number of probable drawbacks that may arise if network security is not applied properly.

Some of these are:

- Contraventions of secrecy: Each business will identify with the need to keep certain critical information private from challenger eyes.
- Data demolition: Data is a very esteemed commodity for individuals and enterprises alike. It is a evidence to its importance when the proliferation of backup technology available today is considered. Demolition of data can severely cripple the sufferer concerned.
- Data handling: A system incident may be easily detectable, as some hackers tend to leave gestures of their execution. However, data handling is a more insidious threat than that. Data values can be changed and, while that may not appear to be a serious concern, the consequence becomes immediately apparent when financial information is in query.

During the twentieth era, the key technology has been information assembling, managing and circulation [1]. For the last ten years, many organizations have applied computer networks. Technological evolution is authorizing the distributed systems implementation based on client/server architecture coupled with proficiency and

Manuscript received May 5, 2017
Manuscript revised May 20, 2017

low costs [2]. PC´s and workstations interrelated are substituting mainframes. Networks and distributed processing systems are rising importance and, indeed, have become critical in the business world. Within a given organization, the trend is concerning larger, more complex networks supporting more applications and more users. As these networks grow in gradation, two facts become painfully apparent [3]:

- The network and its accompanying resources and distributed applications become crucial to the organization.
- More things can go incorrect, disabling the network, a slice of the network, or degrading performance to an intolerable level.

A requisite of efficient operation, free of faults, has shown with the importance of networks for the organizations [4]. The computer networks are compounded of dissimilar platforms of hardware and software: several protocols, resources and services. A large network cannot be put composed and managed by human effort alone. The complexity of such system requires automated network management tools to monitor and manage the resources application.

There are numerous definitions of network management. The ISO´s (International Organization for Standardization) one says that "Network Management has machineries to monitor, control and coordinate OSI (Open System Interconnection) environment´s resources for the information exchange among these resources". It involves the areas of:

- fault: The services that enable the detection, isolation, and correction of abnormal operation.
- configuration: The services that workout control over, identify, collect data from, and provide data.
- account: The services that enable charges to the recognised for the use of managed objects and costs to be identified for the use of those managed objects.
- performance: The services needed to evaluate the performance of managed objects and the usefulness of communication activities.
- security: The services that address those features of OSI security essential to operate OSI network management properly and to protect managed objects.

Common security solutions try to inaugurate perimeters or layers of guard to filter what data passes in or out. Multiple layers and access points make vigorous network security systems a natural example of distributed operations in both implementation and management aspects. The level of threat to the resources and data within a system makes effective management of security capabilities an important dispersed operations mission. Computer security has been of interest since the first multi-user systems. Only recently, since vital data and critical business functions moved onto networked systems, have network security mechanisms boomed. User prospects of system quality, privacy, performance, and reliability are increasing. The rapid arrangement of new security technology needs flexible, efficient management to help system operators from being amazed by configuration and monitoring overhead. The complexity and inter-reliant nature of network security requests an up-to-date system view and the capability to collect and correlate underlying event details. A security program depends on the correctness, completeness, and reliability of three related components – security procedure, implementation devices, and assurance dealings. Operational procedures and security techniques that counter security risks with controls and defensive measures. Security strategy has a direct impact on the rules and policing actions that ensure proper operation of the implementation mechanisms. Policy has an indirect influence on users; they see security applications and access services, not policies. The security policies of the organization determine the balance between users' ease of use and level of responsibility versus the amount of controls and countermeasures.

The goal of the security manager is to apply and impose consistent security policies across system boundaries and thru the organization. The challenges in achieving a functional security system are twin. First, a consistent and complete arrangement of the desired security policy must be defined, independent of the implementation. The second need is a unified scheme to impose the applicable security policies using existing tools, procedures, and mechanisms. The difficult task in achieving a "state of security" is not obtaining the necessary tools, but choosing and incorporating the right ones to provide an inclusive and reliable chain of security. I believe that the need for security management will proliferate, much as the growth of LANs created a demand for better network management solutions.

The quantity, variety, and complexity of security applications represent so many different functions and security states that incorporated management would be incredible without mapping attributes to a common management model. In this paper, I present a common security Management Information Base (MIB) and discuss its application to representative security mechanisms. The main goal is to endorse a better thoughtful of the issues and approaches to integrated, consistent security management.

## 2. Network Management Terminology

Network security management is defined just by flora a dispersed function. Applications that may apply security

management incorporate firewalls, databases, Email, teleconferencing, electronic commerce, intrusion detection, and access control applications. Security management faces the same security threats as other circulated applications. Synchronised management of security is not practicable without a secure management groundwork that defends in transit messages from amendment, spoofing, and replay. Although end system security is beyond the scope of this conversation, it is clear that key management, access control, and reliable implementation of management software are serious also. In its crudest form, security management could require human presence at every security device and manual assessment of all significant events. On the other hand, I believe that remote monitoring with computer assisted connection and management of system events is just as feasible for security management as it is for network management. [5, 6] In fact, it may be argued that detection of high-level attacks need the help of computer-assisted connection tools even more than network management systems. Some network management systems use remote style analysis and pattern recognition of management data to begin automated or suggested operator responses. Comparable possibilities for security are more a matter of market request and asset than technology limitation. Even a small network with uncertain security needs will soon face significant administrative overhead to configure and monitor firewalls, validation servers, secure Email servers, etc. Organizations are now coming to expect both privacy mechanisms and firewall protection, but aggressive pressures are driving administrators to reduce labour costs of network and system management through automation and association of management activities. The rapid deployment of security services in corporate and public networks reinforces the need for security management. Like other distributed applications, security management modules must speak a common language. Two standards-based management protocols have addressed security management slightly. SNMPv2 proposed many security enhancements over the existing SNMPv1, though the standards process warped under its own weight. SNMPv3 is emerging to syndicate the best aspects of SNMPv2 (RFC 1445-1452) with SNMPv2c (RFC1901-1907). Since SNMP is more pervasive than the ISO's Common Management Information Protocol (CMIP) standard, SNMPv3 is expected to be an important security management protocol.

I state security management as the "real-time monitoring and control of active security applications that apply one or more security facilities." The tenacity of security management is to safeguard that the security measures are operational, in equilibrium with current conditions, and compatible with the security policy. Not only must the services function properly and in a timely manner, they must counter existing threats to generate admissible sureness in the system dependability. One of the largest security drawbacks is to focus on certain security products or technologies without significant a balanced security policy and thereby attainment a false sense of security. Protection is only as strong as the weakest link. Pledge is the conventional term for methods that are applied to assess and safeguard a security system imposes and complies with intended security policies. One may use assurance tools before, during, or after security mechanism operations. Post-processing of security events predictably includes audit trail analysis and related off-line intrusion detection and trend analysis methods. Many Intrusion Detection System (IDS) applications began as post-processing functions due to limited processing and software capabilities, but most are drifting toward interactive, real-time operations [7]. Pre-operational analysis of security may involve extensive testing and the use of rigorous logical analysis referred to as formal methods. This approach is widely applied in critical aviation, nuclear power and medical systems, as well as security kernels, to enhance reliability [8]. The need for highly reliable security systems cannot be satisfied only through design and testing, especially since protection from malicious parties is a fundamental need1. Developers for critical systems have found that reliable systems must address:

- Fault prevention during design and development,
- Fault detection during operations and
- Fault recovery during abnormal or error states.

Network Management Security policy and security techniques have been foremost research matters for a long time, but relatively little work has been reported on management of circulated security applications. I present a core set of security managed objects for use with the Simple Network Management Protocol (SNMP). Security applications are assessed for value of management via SNMP. A scenario of corporate firewalls illustrates concepts of security management correctness, sufficiency, and completeness. Figure 1 express the basic components working in network security.

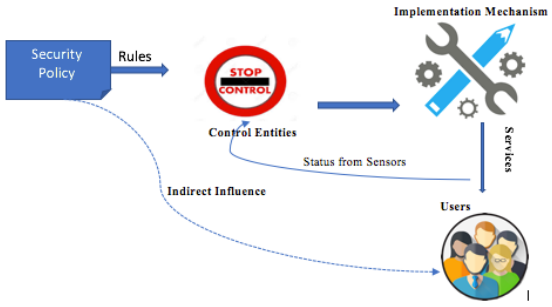


Fig. 1 Security Components

### 2.1 Management Information Base (MIB)

In purpose of the circulated nature of the managed resources, network management is a dispersed application based on perceptions like objects, agents, managers, management information base (MIB) and protocols.
Network devices, called objects, enclose info about themselves. For example, every device has been constituted with some assortment of limitations. A device has an existing status that indicates whether it is in vigorous running situation. Devices often keep internal facts that calculate incoming and outgoing traffic and various detected errors [9]. It is convenient to think of the alignment, status, and statistical info in a device as materializing a "database". In genuineness, info may be saved at a device as an amalgamation of switch settings, hardware counters, in-memory variables, in-memory tables, or files. This logical database of network management information is called a Management Information Base (MIB). Agent software is mounted in each device. An agent accepts incoming messages from a manager. These messages request reads or writes of the device's data. The agent carries out the request and sends back responses. An agent does not always have to wait to be asked for info. When a severe problem appears or a important event occurs, the agent sends a notification message called a trap to one or more managers. Manager software at a management station sends request messages (polling) to agents and receives responses and spontaneous trap messages from agents. What protocol carries this message? UDP is the preferred choice, but any transport protocol is adequate.
To a network management system, we need one or more applications that authorise an end user to control the manager software and view network information. To complete the Network Management, the ISO´s and ITU-T´s (International Telecommunication Union-Telecommunication Standardization Sector) standards are based on the CMIP (Common Management Information Protocol) protocol and the IAB´s (Internet Activity Board) are based on SNMP (Simple Network Management Protocol) protocol [10]. Because of the complication of OSI systems, CMIP is not very easy to be implemented. "Support for SNMP" actually is a shorthand for the fact that hubs, bridges, routers, multiplexors, switches, or whatever can be managed, adapt to the Internet-Standard Management Framework. This framework is easy to implement, is powerful, and opens up like a big umbrella to take more and more technologies under its protection.
Of the three central security principles (confidentiality, integrity and availability), integrity is the most serious to management operations. The authentication of users and the consistent delivery of the appropriate data are constant necessities. Whereas confidentiality of some data may be required, it is not a relentless driver. Accessibility of security management applications is also a slighter concern since many applications can remain to operate and maintain status info throughout gaps in communications. It may appear that a security management system that manages a trustworthy application should go through the same laborious testing and analysis as the primary security application. Rushby [11] indicates a security kernel must have access to and control over the vibrant security features of a system and must preserve secure attributes in spite of any possible sequence of operations. If the security management application imposes security, it and all related set-up would have to meet all security necessities of the central application (e.g., security kernel). I conclude that the tenacity of security management is not to impose security, but to manage security hazard by recognising and exposing status of important parameters. It is a means to gather status info and tune functioning parameters to meet current data safety needs. [12]

### 2.2 Simple Network Management Protocol (SNMP)

SNMP is described by the RFC1157 (May, 1990):

- Defines the messages that can be exchanged between a management station and a sytem to read or update variable values.
- Defines trap (alarm) messages that are sent by a system whose status is changing in a serious way.
- Deals with the nitty-gritty details of message formats and communications protocol specification.
- All sorts of equipment - bridges, repeaters, ASCII terminals.
- Many types of interface technology - Point-to-Point, DS1, DS3, X.25, Frame Relay, Ethernet, Token -Ring, FDDI, and others.
- Popular proprietary protocols such as DECnet, Phase IV, and Appletalk.

The easiness of version 1 of SNMP donated to its rapid completion and recognition. Nevertheless, version 1 had some severe deficiencies. There was no reliable method of authenticating the source of network management messages. There was no way to secure the contents of network messages from network eavesdroppers. In April of 1993, SNMP version 2 was put onto the standards path. Version 2 addressed the authentication and security of management messages. It also controlled useful protocol enhancements and improved the administrative framework for the maturing protocol suite. But version 2 has been criticized because of its complexity: it uses far superior system resources than version 1.
The SNMP community has used an evolutionary methodology to standardize what information should be kept in a device's MIB:

- Express groups of clearly useful parameters.

- After several months of field experience, fine-tune these groups. Throw away parameters that are not useful. Add new ones that are needed.
- Set up committees of industry experts to define MIB variables for special technologies, such as bridges or Token-Ring interfaces.
- Add vendor-specific allowances that cover special features of a vendor's stuffs.

To get this level of springiness, management info is structured as a tree, so that new branches can develop wherever they are needed. SNMP was originally developed to satisfy an instantaneous requirement to manage TCP/IP communications on the Internet. The first MIB, now called MIB-I, concentrated on information specific to TCP/IP. Sample variables from the originals MIB included:

- A system description
- The number of networking interfaces
- The IP address associated with each network interface
- Counts of the numbers of incoming and outgoing datagrams
- A table of information about active TCP connections

After positioning in the field, the basic definitions were clarified and many new definitions were added. The results were published in RFC1213: MIB-II. MIB-II has proved to be a robust basis for TCP/IP Management.

### 2.3 Integrated Security Management

Arrangement of operative security management needs three basic management components – applications, infrastructure, and agents. I focus on the issues of adapting the predominant management status and control mechanisms (management infrastructure and agents) to accommodate security management needs. The basic management infrastructure must provide suitable mechanisms for the following factors to maintain secure management of applications:

- confidentiality and integrity
- data transport
- common data encoding
- liveness3

These capabilities may or may not be available from existing network management systems. The use of standard protocols such as SNMPv3 along with recognized security mechanisms for authentication, access control, integrity and privacy ensures no weak security links. In addition, the management platform itself needs protection through good system and physical security.

It is broadly settled that alliance and integration of management functions is essential to keep costs down and allow small network operations staffs to extend their scope of control. It is also clear that moves toward centralized management can lead to single points of failure and functioning problems. A recent trend within the network management industry is the deployment of dispersed management systems that can helpfully share info and apply control functions. Many security applications may benefit from consolidated, cooperative management, especially those that are active and widely replicated across multiple sites.

Table 1. Security Applications (L=Low (1), M=Medium (2), H=High (3))

| Application | Proli-feration | Research Value | Real-Time Management | Total |
|---|---|---|---|---|
| Security Firewall | H | H | H | 9 |
| S-HTTP | L | H | H | 7 |
| Secure DNS | L | M | M | 5 |
| Secure Email | M | H | M | 7 |
| Kerberos | M | M | M | 6 |
| Intrusion Detection System (IDS) | M | H | H | 8 |
| Secure Audit Trail | M | M | L | 5 |
| Secure Multicast | L | M | M | 7 |
| System Security | H | H | L | 7 |

Numerous security applications are likely candidates for incorporated management using standard protocols. Table 1 above shows our assessment of the relative suitability of some possible applications. We used three subjective factors to assess each application for integration with a security management system. Proliferation rates how widespread the application is, research value assesses the importance of the application technology, and real-time management indicates the usefulness of interactive management in the application domain. For example, due to the rapid deployment and variety of vendor offerings, network security firewalls show great promise for management by standard protocols.

## 4. Network Management Application Scenario

When numerous similar manageable devices or submissions are in a common management domain, a common management application may be measured. I am presenting an example application with one Network Management Station (NMS) to manage a group of network security firewalls.

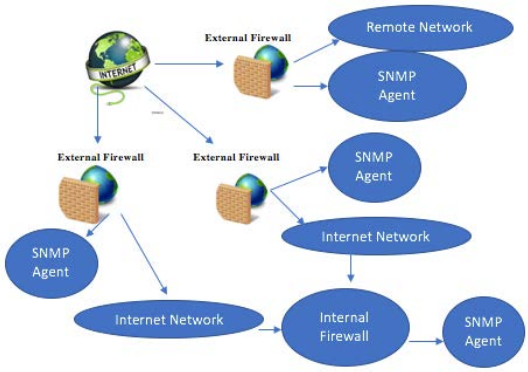


Fig. 2 Management of Internal and External Firewall

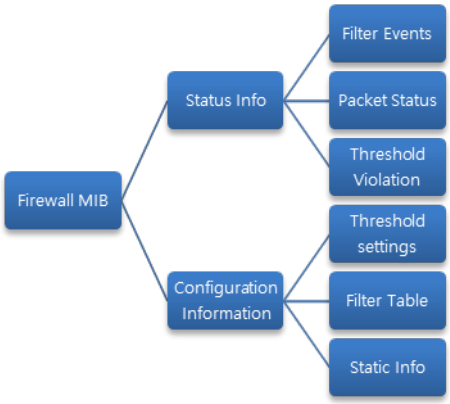


Fig. 3 Firewall MIB

Saudi Electronic University (SEU) has several externally linked LANs that require new firewalls and some that need firewalls between divisions. SEU has remote offices that connect via the Internet as in Figure 2. While most firewalls would be managed from an NMS inside the firewall, external management of firewalls is essential for organizations that want central administration. This can be challenging, since SNMP uses the User Datagram Protocol UDP service and management competences would be delayed if UDP access though the firewall is restricted. SEU managers want to use an existing network management platform to monitor the new firewalls. To do so, an upgrade from SNMPv1 to SNMPv3 will support data reliability and secrecy. Typically, the events of interest for a firewall will be the number of incoming packets that are dropped due to packet-filter restrictions. If a large number of drops occur in rapid sequence, a significant security event may be happening. Instead, if a high percentage of packets in an interval (say 60% in a 35-second interval) are overruled, there may be cause for concern. Both of these events could trigger a trap event to the NMS to alert an operator for further calculation. The NMS may raise or lesser the security monitoring posture based on the recent pattern of alerts, external information, or system security policy. If a reoccurring security alert is being produced from the same source, the manager may want to set the filtering action as “log packet” or “log header” for later review rather than just diving it. Such a management response may provide needed evidence to trace burglars. Care is needed to keep flooding attacks from overflowing storage areas, however. Recording packet drops requires the NMS operator to SET the packet-filtering rule that is accompanying with the alert. This may be done by doing a GET and searching through the packet-filter table for the rule, or the original alert may show the associated rule in the trap message. To change the configuration of the packet filtering table, the “action” column must allow read/write access.

Alternative method to assess the configuration and competence of a packet-filtering firewall is through summary variables such as the TopTenRuleHits, TopTenSrcIPAddrand TopTenDroppedPktSrcIPAddr similar to the Remote Monitoring (RMON) MIB (RFC1757/ 2021). In this method, the most important rules and problems can be closely judged and the effect of changes can be understood. Specific rules may be changed and turned on or off as conditions command. Perhaps, better functioning can be accomplished if rules that are fired most are reorganised in the filtering table. Packet-filter tables and application proxies only allow approved traffic to pass through. Changes to the firewall formation may result from reaction to status info or from external needs. New applications may be opened for use on a proxy server, or a security trigger could shutdown hazardous applications or positions. Therefore, application and packet-filtering tables may function like a router that permits traffic to flow onward toward its destination. Figure 3 shows high-level firewall MIB definition groups that may be retrieved from a standard NMS platform. The processes to make an update are as follows. If a firewall is operational and a new proxy application is to be added, the management station would update the application table by introducing a SET operation on the appropriate row values. Certain columns such as source and destination addresses would be mandatory parts of the table information. If a need for application access is temporary (i.e. user needs access while on travel), the management application could set a timed trigger to remove the access automatically.

The extension of the Internet and the number of delicate functions that require strong security prefigure a growth in demand for security management potentials. As electronic commerce, secure messaging and firewall applications and management applications will be needed to limit administrative loads while also allowing greater flexibility and control of security operations. Before an effective security management capability can be developed and

demonstrated, there are a few fundamentals. First, a secure management infrastructure must be in place. SNMPv3 is poised as the secure successor to SNMPv1. Next, a security MIB must be defined to allow SET/GET operations on essential values for the security application to be managed. This is a combative and problematic step because of the need to map terms and status parameters from many different vendor applications and features to a small set of commonly defined values. The core MIB can be extensive to define configuration and status parameters for security applications and vendor features in the same manner as other MIBs. The foundational work of defining a common core of security management substructure, attributes and MIB definitions will allow evolution to the next phase of capability development, that is, better relationship of management events with security difficulties. The modification of agent modules and security management applications to effectively access a common set of security values will open new management features. Then, pioneering use of security management views and collaboration with other management and security information across the network can uncheck new power for security management.

## 5. Basic 10 Ideas, anyone can help anyone to keep networks safe: [13]

1. **Communications** – A rigorous security policy is only as good as the people who must follow to it. In that regard, it is key to educate your users on how their activities may influence the network.
2. **Virus Management** – Viruses and other malware can source a wide range of complications, from slowing or crippling network activity to theft. So, virus-detection and spyware software must be installed and updated regularly.
3. **Patch Management** – Hackers habitually use known software security holes to misuse networks. Therefore, a key component of your protection should involve an automated patch solution.
4. **Encryption** – In the event that your network is cooperated, encrypting your data will store it in an unreadable format. This is predominantly useful for mobile devices.
5. **Physical Security** – Don't oversee the importance of restricting access to your servers or data center. This can be done with appropriate access control hardware and software.
6. **Passwords** - Dictionary attacks are another tool in the hacker cache. Corporate password policy should require strong passwords (a combination of letters, numbers and special characters) and influence periodic password changes.
7. **Vulnerability Scanning** – A vulnerability scanning tool will evaluate any weaknesses within your network and offer suggesting and cures to help address the issues.
8. **Spam Filtering** – Spam now accounts for a substantial portion of corporate email. These messages appeal users to click on links proposed to swipe sensitive info.
9. **Event Logs** – Logs are an elemental tool in uncovering potential attacks. But volume can quickly make this task uncontrollable, so employ the use of log management software to help avoid an attack before it happens.
10. **Backup and Disaster Recovery** – In the consequence of network failure, you'll want to restore operations as rapidly as possible. Backups, with a solid off-site storage strategy can do just that. Network security can seem like a discouraging task. However, today's environment demands our watchfulness. These best practices will help safeguard the safety and obtainability of your networks.

## 6 Conclusion

A network management is a collection of tools for network monitoring and regulator that is incorporated in the following senses:

- A single operator interface with a powerful but user-friendly set of commands for accomplishment most or all network management tasks.
- A minimal amount of dispersed equipment. That is, most of the hardware and software required for network management is integrated into the existing user equipment.

Networks and spread managing systems are of serious and rising prominence in enterprises of all categories. The movement is toward larger, more complex networks supporting more applications and more users. As these networks grow in measure, two specifics become painfully evident: The network and its allied resources and spread applications become indispensable to the organization, and More things can go incorrect, disabling the network or a portion of the network or degrading performance to an intolerable level. A large network cannot be put together and managed by human effort alone. The complexity of such a system directives the use of automated network management tools.

The extension of the Internet and the number of delicate functions that require strong security prefigure a growth in demand for security management potentials. As electronic commerce, secure messaging and firewall applications and

management applications will be needed to limit administrative loads while also allowing greater flexibility and control of security operations. Before an effective security management capability can be developed and demonstrated, there are a few fundamentals. First, a secure management infrastructure must be in place. SNMPv3 is poised as the secure successor to SNMPv1. Next, a security MIB must be defined to allow SET/GET operations on essential values for the security application to be managed. This is a combative and problematic step because of the need to map terms and status parameters from many different vendor applications and features to a small set of commonly defined values. The core MIB can be extensive to define configuration and status parameters for security applications and vendor features in the same manner as other MIBs. The foundational work of defining a common core of security management substructure, attributes and MIB definitions will allow evolution to the next phase of capability development, that is, better relationship of management events with security difficulties. The modification of agent modules and security management applications to effectively access a common set of security values will open new management features. Then, pioneering use of security management views and collaboration with other management and security information across the network can uncheck new power for security management.

## References:


[1] Tanembaum, Andrew S., Computer Netwoks, Prentice Hall International Inc., USA, 1989.

[2] Duarte, Fátima de Lima Procópio Duarte, Simulação e Análise do Benchmark TPC-C, Dissertação de Mestrado apresentada ao Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, Brasil, Janeiro de 1996.

[3] Stallings, Willian, SNMP SNMPv2 and RMON, Addison-Wesley Publishing Company, 1996

[4] Teixeira, Suzana de Queiroz Ramos e Oliveira, Mauro, Disponibilização do Conhecimento no Gerenciamento de Redes de Computadores, artigo, Brasil, XXIII Seminário Integrado de Hardware e Software, Agosto 1996.

[5] Marshall T. Rose, The Simple Book: An Introduction to Management of TCP/IP-based Internets, Prentice Hall Series in Innovative Technology, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.

[6] William Stallings, SNMP, SNMPv2 and CMIP: the Practical Guide to Network Management Standards, Addison-Wesley, 1993.

[7] Gregory B. White, Eric A. Fisch and Udo W. Pooch, “Cooperating Security Managers: A Peer- Based Intrusion Detection System”, IEEE Network, pp. 20-23, January/February 1996.

[8] John Rushby, "Critical System Properties: Survey and Taxonomy", Reliability Engineering and System Safety, 43(2): 189-219, 1994.

[9] Feit, Dr. Sidnie, SNMP - A Guide to Network Management, McGrawHill, 1995

[10] Case, J., Fedor, M. Schoffstall, M. Davin, J., Network Management Protocol-SNMP, May 1990.

[11] John Rushby, "Kernels for Safety?", Safe and Secure Computing Systems, pp. 210-220, Blackwell Scientific Publications, 1989.

[12] John Rushby, "Kernels for Safety?", Safe and Secure Computing Systems, pp. 210-220, Blackwell Scientific Publications, 1989.

[13] Post was provided by Veronica Henry of GFI Software Ltd.


**Author:**

Dr. Arun Kumar Singh is working as an Asst. Professor in the College of Computing and Informatics (Saudi Electronics University, KSA). He received Ph.D. in CS/IT under the guidance of Dr. Neelam Srivastava (IET Lucknow) and Dr. R. P. Agarwal (IIT Roorkee), M.Tech. (IT-WCC) degree in 2005 from IIIT-Allahabad under the guidance of Prof. M. Radha Krishnan and B.E. (ECE) degree in 2002 from Dr. B. R. Ambedkar University, Agra, India. His research interests are Big Data, Network Management, Wireless networking, Social Networking and Mobile computing.