Proposed Model for Secure SNMP Communication with Magic Square Method

Vinod Kumar Shukla
Research Scholar,
Mewar University
Chittorgarh, Rajasthan, India

Dr. Nitin Pandey
Amity Institute of Information Technology
Amity University, Noida, U.P, India

Dr. D. B. Ojha
Professor
Mewar University
Chittorgarh, Rajasthan, India

***Abstract*—We have proposed a model for securing the SNMP communication with help of dual encapsulation. Frist encapsulation is done with Magic square method and second with Ontology. SNMP has become a wide accepted protocol for network communication. In this paper it is proposed how the communication from SNMP manager to SNMP agent or vice versa can be more securely done.**

Keywords—SNMP; MIB; Magic Square; Ontology; Cryptography

1. INTRODUCTION

Network growth has given a new challenge to network security for its wide implementation. As the network is growing in size and number of network devices, the need for efficient management of network resources has emerged as alarming issue for network security. Network management is vital for optimized, controlled, and cost efficient utilization of network resources [1]. We can refer network security as group of policies and procedures implemented to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. Network security is required to all type of resources which operates on computer network.

2. SNMP

SNMP has become the standard for the exchange of network information. SNMP managed network devices work on concept of manager/agent that executes all the MIB objects that are relevant. The agent provides the information contained in the MIB to management applications when it is needed. SNMP polls for information gathered by a network agent. The agent collects data from the network device it is located on and stores it in the MIB. When polled, the agent will send the information back to the SNMP manager.

Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed forthe Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).

The basic communication architecture of SNMP is straightforward; there are three types of requests and one unsolicited information transmission.To get information from an SNMP device, a "manager" will send a "GetRequest" or "Get"NextRequest" to an "agent" and the requested information or an error message will be sent back in a "Response." If a manager wants to modify information on an agent, a "SetRequest" will be sent with a corresponding response to confirm or report an error. [2]

The unsolicited message form is called a "trap." This kind of message is usually sent by agents on start-up, on status change and in response to error conditions. [3]

When the SNMP manager requests the value of any object, it assembles a message with the OID, which is sent to the MIB for decoding. If the OID is listed within the MIB at that particular management station, a message is sent back to the manager including the value requested for that particular OID.[4]

OIDs or Object Identifiers uniquely identifies managed objects in a MIB hierarchy.

3. CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document [5].

Using generalization of 8X 8 magic square given by Deo Brat ojha and B L Kaul [6], encryption generates a key on the pattern of 8X8 magic square image.

A8X8 matrix filled with the integers in such a way that the sum of the numbers in each row, each column or diagonally also remain same, in which one integer use at once only. This scheme utilizes the Required Sum of Magic square [6, 7, 8, 9, 10,11] to generate an encryption key for the Scheme.

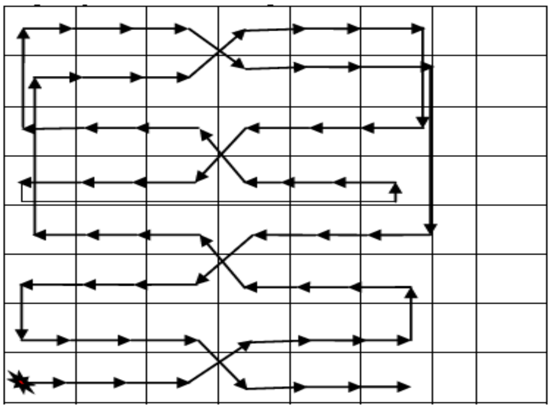

Fig. 1. Magic Square Generalized Figure

The concept utilizes the generalized form of a 8X8 matrix with the help of a special geometrical figure. With help of 8X8Magic Square, the process establishes a new platform to generate key and encrypt the data using our encryption scheme.

3.1 Process of Encryption and Decryption

In encryption phase, we take a message block and a new generated key $K_{new...i}$ implement encryption process as per traditional DES.In this process, we take a new key for every block of message. This new key $K_{new...i}$ is apply on each block of message M . In this new process , new key is also make 64 different key for every round of DES using shifting property as per traditional DES. For every block of message M , $K_{new...i}$ new makes a new key block for every round of DES to implement in the encryption process.

Decryption Process is the inverse step of encryption process. In decryption, we also use the same key which is used in encryption.

$$C_i = E_{K_{newi}}\{m_i\}\, and\ m_i = D_{K_{newi}}\{c_i\}$$

Where $1 \le i \le n.$

Cipher Text $C = C_1, C_2, C_3, \ldots\ \ldots\ldots\ldots\ C_n\ and$

Plain Text $M = m_1, m_2, m_3, \ldots\ \ldots\ldots\ldots\ m_n$

3.2 Sender Initial Phase

1. Sender chooses a required total sum S & difference d and send it to the receiver.
2. Then calculate the first no. using the formula 2a +7d = sum required, where a is first no. and d is difference.
3. Then calculate the sixty four $n_n = n_{n-1} + d$, where d chooses already.
4. Then arrange these sixty four numbers with the help of suggested geometrical figure.
5. Now Sender takes the centre no. and uses this rather than random no.

3.3 Receiver Initial Phase

1. Receiver receives required total sum S & difference d.
2. Then calculate the first no. using the formula 2a +7d = sum required, where a is first no. and d is difference.
3. Then calculate the sixty four numbers $n_n = n_{n-1} + d$, where d gets already.
4. Then arrange these sixty four numbers with the help of suggested geometrical figure.
5. Now receiver also takes the center no. and uses this rather than random no.

3.4 Key Generation Phase

$$F\{K, Center\ no.\} = K_{new\ i}$$

$$\underline{Function\ F}$$

3.5 Encryption & Decryption Phase

$$C_i = E_{K_{newi}}\{m_i\}\, and\ m_i = D_{K_{newi}}\{c_i\}$$

Where $1 \le i \le n.$

Cipher Text $C = C_1, C_2, C_3, \ldots\ \ldots\ldots\ldots\ C_n\ and$

Plain Text $M = m_1, m_2, m_3, \ldots\ \ldots\ldots\ldots\ m_n$

Both sender and receiver follow the process and generate separate key using generalized form of 8×8 a matrix with the help of a special geometrical. Every time when, required sum and difference are changed than new generated key also changed. Now, the sender use this newly generated key for encryption and the receiver uses this key for decryption. [12]

4. ONTOLOGY

An ontology is a representation or model of knowledge, a “formal, explicit specification of a shared conceptualization” according to (Gruber, 1993), and this means that however ‘shared’ it may be it is still extremely subjective, representing the time, place and cultural environment in which it is created.

Ontology refers to the interpretation of a group of ideas within a specific domain that defines the interrelationship between those ideas. Ontology can be used to study the existence of entities within a specific domain and sometimes can be used to identify the domain itself. [13]

The advantage of ontology is that it represents real world information in a manner that is machine process able. The reason ontologies are becoming popular is largely due to what they promise: a shared and common understanding of a domain that can be communicated between people and application systems. [14]

Onto-Agent is a proposed concept, in this paper, which will work on all the managed objects along with the manger. This will be responsible for the understanding ontology sent by all the other managed devices as well as manager. And this will also help to generate the ontology from the MIB OID values. [15]

5. PROPOSED MODEL

Our proposed model for transferring SNMP message between SNMP manager and SNMP agent work on the concept of dual encapsulation. In first phase of encapsulation the SNMP message is encrypted by Magic Square method and in second level of encapsulation the encrypted SNMP message is converted into related Ontology.

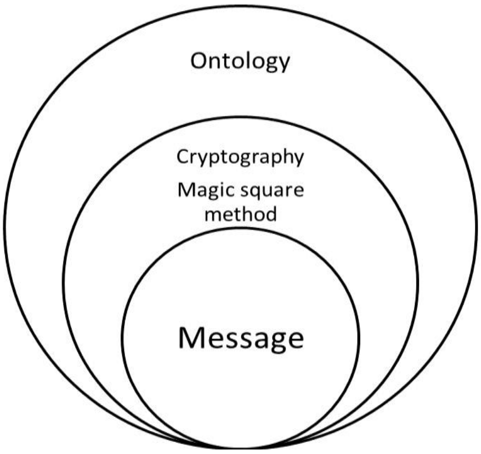

Fig. 2. Dual Encapsulation of Orginal SNMP message

In this paper our proposed system is for securing more to SNMP communication by using the concept of Magic square. Communication between SNMP manager and SNMP Agent is done by exchanging the MIB values. These MIB values are OID, which are unique. Our proposed model for SNMP manager and SNMP Agent can be graphically represented like following.

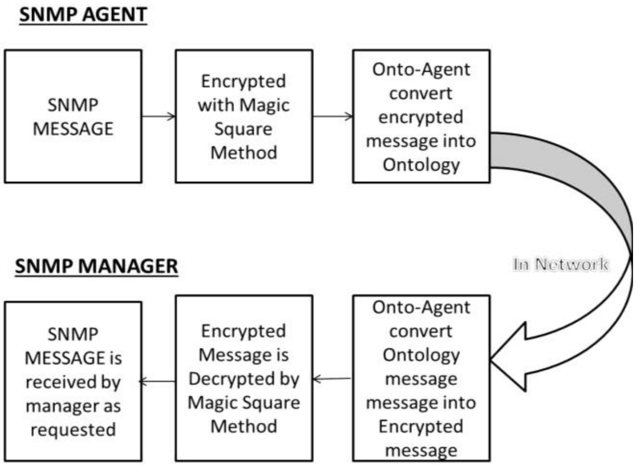
SNMP AGENT
SNMP MESSAGE
Encrypted with Magic Square Method
Onto-Agent convert encrypted message into Ontology
In Network
SNMP MANAGER
SNMP MESSAGE is received by manager as requested
Encrypted Message is Decrypted by Magic Square Method
Onto-Agent convert Ontology message message into Encrypted message

Fig. 3. Proposed Model for SNMP communication

5.1 SNMP Agent:

1. SNMP client communicates to Manager for requested values.
2. Before communicating values they are encrypted with help of Magic square encryption.
3. Encrypted values are then passed by Onto-Agent, which convert the entire massage into ontology with help of OWL-DL language.
4. This generated ontology is sent to SNMP manager.

5.2 SNMP Manager:

1. SNMP manager receives the Ontology of request data.
2. Onto-agent reads the ontology and convertsthe it from ontology to encrypted data.
3. Now with same technique message was encrypted (Magic square method) it is decrypted back.
4. And SNMP manager receives the requested OID values.

The above process of SNMP manager and SNMP agent can be applied vice versa for either side of communication.

6.CONCLUSION

The conclusion of the proposed model is to improve the communication between SNMP Manager and SNMP Agent for secure communication.

Scope of improvement is also very high as the process of Onto-Agent needs to be defined for automation as when different keys are generated how all the keys could be converted in to related ontology. We have suggested OWL-DL language, further can be tested and along with this in to different language.

7. REFERENCES

[1] Stallings, W. B., “SNMP, SNMPv2, SNMPv3 and RMON 1 and 2”, Third Edition, Addison, Wesley Longman Inc., Reading, Massachusetts, 1999.

[2] Vinod Kumar Shukla et al, “ONTOLOGICAL IDS MONITORING ON DEFINED ATTACK” International Journal of Science and Research, Volume 3, Issue 3, and March 2014.

[3] Network World, Resource Library, http://www.networkworld.com/details/748.html

[4]SNMP OID, http://www.dpstele.com/dpsnews/techinfo/snmp/snmp_oid.php

[5] Eli Biham, Adi Shamir, Differential Cryptanalysis of the Full 16-Round DES, Advances in Cryptology, proceedings of CRYPTO ’92, Lecture Notes in Computer Science 740, Springer, 1993.

[6] Deo Brat Ojha, B L Kaul, Generalization of 4×4 Magic Square, International Journal of Applied Engineering Research, Dindigul, Volume 1, No 3, 2010.

[7] Harold M. Stark. An introduction to number theory.MIT Press, Cambridge, Mass., 1978.

[8]. Joseph H. Silverman.The arithmetic of elliptic curves. Springer-Verlag, New York-Berlin, 1986.

[9]. Ezra Brown.Magic squares, finite planes, and points of inflection on elliptic curves. College Math. J., 32(4):260–267, 2001.

[10]. Agnew, Elizabeth H., “Two problems on magic squares,”Mathematics Magazine, 44 (1971),12–15.

[11]. Hanson, Klaus D.,“The magic square in Albrecht D¨urer’s“MelencoliaI”:Metaphysical symbol or mathematical pastime,” Renaissance and Modern Studies, 23 (1979), 5–24.

[12]Nitin Pandey et al, “SECURE COMMUNICATION SCHEME WITH MAGIC SQUARE” Journal of Global Research in Computer Science, 3 (12), December 2012, 12-14

[13]Computer Ontology, http://www.techopedia.com/definition/591/computer-ontology

[14]Ontologies Advantages, http://mecca.noc.uth.gr/ontologies_advantages.htm

[15] Vinod Kumar Shukla et al,” CONCEPTUAL ONTOLOGICAL MODEL FOR PRIVATE ENTERPRISE MIB UPDATE”” “Journal of Global Research in Computer Science”, Volume 5, Issue 3, March 2014

Mr. Vinod Kumar Shukla received the degree of MCA from U.P. Technical University in 2004, has total experience of nine years in teaching and training. He is currently pursuing PhD from Mewar University, Rajasthan, India in the area of Semantic web and Ontology

Dr. Nitin Pandey, is an Assistant Professor at Amity Institute of Information Technology, Amity University Uttar Pradesh. He has 10 year of experience His area of interest is Coding theory, Cryptography, Data Communication and Network Security. He is PhD in computer Science fromMewar University,Chittorgarh. He is the author and co-author of more than 10 publications in technical journals and conferences.

Dr. Deo Brat Ojha, Ph.D from Institute ofTechnology, Banaras Hindu University, Varanasi(U.P.),INDIA. His research field is OptimizationTechniques, Functional Analysis & Cryptography. Heis Professor at Mewar University,Chittorgarh,Rajasthan INDIA. He is the author/co-author of more than 250 publications in International/National journals and conferences.