2005 International Conference on Wireless Networks, Communications and Mobile Computing

Improving the Security of SNMP in Wireless Networks

H. Otrok, A. Mourad, M. Debbabi and C. Assi

Computer Security Laboratory
Concordia Institute for Information Systems Engineering
Concordia University, Montreal (QC), Canada

Abstract— **Simple network management protocol (SNMP) is widely used for monitoring and managing computers and network devices on wired and wireless network. SNMPv1 and v2 do not provide security when managing agents. Three very important security features (authentication, encryption, access control) are added to SNMPv3 under the User-based Security Model (USM). Symmetric cryptography is used for encryption and one-way cryptography is used for authentication. The two keys used for encryption and authentication are derived from the shared password between the manager and agent. In this paper, we are addressing (1) the problem of one way authentication that leads to the man-in-the-middle attack and (2) the vulnerability pertaining to the password update method of SNMPv3. We propose to use certification authority for two-way authentication and Diffie-Hellman algorithm for key exchange to mitigate the impacts of these problems.**

Index Terms—**SNMPV3, Diffie-Hellman, Certification Authority.**

I. Introduction

SNMPv1 and v2 [10] are the two versions of SNMP that do not provide security. SNMPv3 is a secure network management protocol used for managing devices on wired and wireless network. It uses User-based Security Model (USM) to provide authentication, encryption and access control. Authentication is provided through implementing Hashed Message Authentication Code (HMAC) based on different one-way cryptography such as Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA). Advanced Encryption Standard (AES) is used for encryption. The two keys used for authentication and encryption are derived from the shared password between the manager and the agent. Moreover, access control is used to address who can access the network management components and what they can access. Wireless security management is the implementation of SNMP over wireless network. It is used by any manager that needs to manage access points and other devices on the wireless network. Several vulnerabilities and security threats were found in SNMP [4] and wireless network [6]. Man-in-the-middle attack (MITM) and updating the password for key freshness are two principal vulnerabilities found in wireless management security. The MITM attacker monitors transmissions between the manager and agent and retransmits and/or replay messages as the legitimate user. An attacker could also take his time to crack the admin password, without drawing attention to his activity, through preventing the device from sending traps[1] for failed authentication [4]. Once the admin password is discovered, the attacker will be able to manage and control all the devices that belong to the manager whose password has been cracked. Moreover, updating the password remotely by the manager becomes useless since the old password is now known by the attacker.

To prevent such attacks, certification authority is used to provide two ways authentication between manager and agent independent of the admin password. Moreover, Diffie-Hellman for secure key exchange method will be used to exchange symmetric keys between the manager and agent independently of admin password and to prevent MITM attack. With this model we will have three-way handshake between the certification authority, manager and agent, while in the classical model there is only two-way handshake between the manager and the agent. In USM model, username, password and access control are saved in the management information base (MIB) agent in the form of a table. We propose to change this table in the new model to contain the following information: username, public key and access control.

This paper is organized as follows: Section 2 presents the security of wireless networks. Section 3 describes the SNMPv3 Architecture. Section 4 describes the vulnerabilities and security threats of wireless network management. Section 5 describes the modified security architecture of SNMPv3. Section 6 describes the analysis of the modified architecture. A conclusion is drawn in Section 7.

II. Security of Wireless Networks

Wireless LAN (WLAN) standards are defined by the IEEE 802.11 working group. WLAN comes in three flavors: 802.11b, 802.11a and 802.11g. Wired Equivalency Privacy (WEP) protocol is used to prevent unauthorized users from connecting to the network and thereby accessing data and managing the network devices. WEP was designed to provide one way authentication, encryption and integrity of the data exchanged between the user and the access point. In [2], authors published a report identifying security weaknesses within the WEP algorithm. Based on their research, WEP was

E-mail: {h_otrok, mourad, debbabi, assi}@ciise.concordia.ca.

[1] A trap is unsolicited message sent by the agent to notify the manager of a significant event.

0-7803-9305-8/05/$20.00 ©2005 IEEE

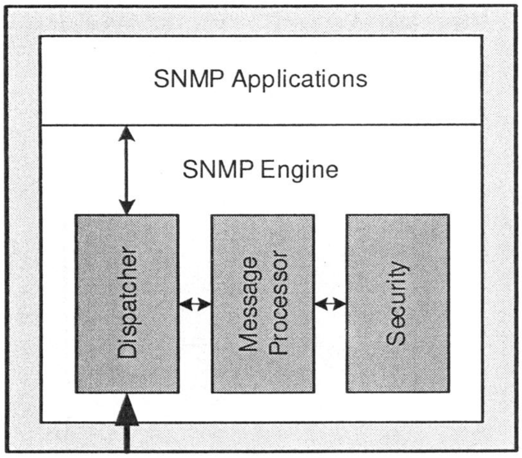

Fig.1. SNMP Manager

found to be insecure due to the improper implementation of the following algorithms:

1) The RC4 for encryption .
2) The cyclical redundancy check (CRC-32) checksum for data integrity.

Moreover, WEP is under the attack of the man-in-the-middle because the attacker can play the role of the access point and the user at the same time. In this case, the user will be connected to the attacker machine and the access point will respond to the user requests through the attacker machine without having any knowledge of the MITM. Wireless LAN hacking tools are widely available for free on the Internet, and new tools are introduced every week. Enhancement was done to address the issues of authentication and access control using IEEE 802.1X. The IEEE 802.1X defines Extensible Authentication Protocol (EAP) over LANs (EAPOL), which is used to authenticate clients as they join the network. The protocol IEEE 802.1X is also valunerable to MITM attack because it uses one way authentication between the user and the access point [8]. Therefore, WEP with IEEE 802.1X can provide partial security in wireless environment. For this reason, we suggest to enhance the security of SNMPv3 independently of the wireless security provided jointly by the WEP and the IEEE802.1X protocols.

III. SNMPV3 ARCHITECTURE

SNMP architecture went through two modifications. The first architecture of SNMP was known as SNMPv1. The latter was not able to provide the following: Manager-to-manager communication, retrieval of large volumes of data, management of large network and security for information retrieval and configuration. Those problems were solved by SNMPv2 except security, which was solved by SNMPv3. The SNMP architecture consists of two entity agents and managers. Agents are the software modules that reside in the managed devices to provide reporting and configuration services to managers. Each SNMP entity contains SNMP application and SNMP engine. The SNMP application uses the engine to exchange data and commands between managers and agents. Several modules are used within the engine. Dispatcher, message processing and security are the main modules found at both entities, manager and agent (Figure 1), while the access control module is found only at the agent entity (Figure 2). The dispatcher rule is to forward the messages received from the transport layer to the message processing module. The message processing module processes the message received according to the respective SNMP version. Then the message processing module forwards the message to the security module if the message belongs to SNMPv3. The security module in SNMPv3 is defined by the User-based Security Model (USM) [1]. The encryption and authentication are provided by the security module. Advanced Encryption Standard (AES) is the symmetric cryptography algorithm used for encryption. Authentication is performed using the Hashed Message Authentication Code (HMAC) based on two different one-way cryptography such as Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA). The symmetric keys used for encryption and authentication are derived from the manager's password stored at both entities. Key localization allows a manager to maintain only one password and it is enabled by hashing the generated key with the ID of each agent entity. This allows the manager to have different keys for different entities. When the key for an agent is compromised, the keys for other agents are not. Each agent keeps track of different users through an internal table in the MIB that contains the user name, password and access. The access control module is defined by the View-based Access Control Model (VACM) and it is used for addressing access rights issues.

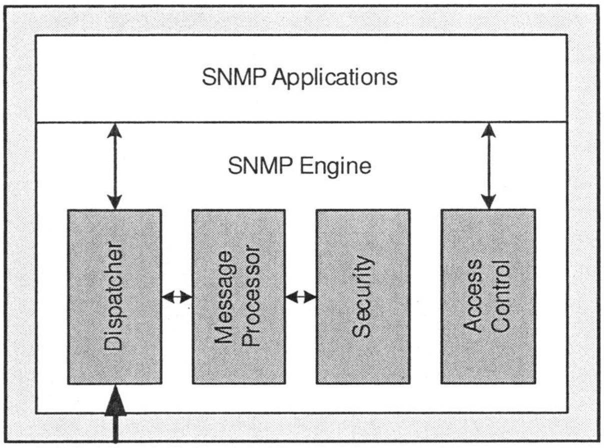

Fig.2. SNMP Agent

IV. VULNERABILITIES IN MANAGING WIRELESS NETWORKS

The goal of the security module provided by SNMPv3 is to prevent the following attacks:

1) Data modification: It is also known as the man-in-the-middle attack where the attacker can intercept messages and modify them.
2) Masquerade: An attacker claims to be someone else to get access to restricted management information.
3) Message modification: The attacker is able to delay messages, replay messages and reorder messages to enable unauthorized management operations.
4) Disclosure: The attacker can see confidential information.

Note that SNMPv3 is not intended to secure the following two threats:

1) Denial of service (DOS): The attacker is able to prevent the exchange of messages between the manager and the agent. The DOS attack probability in wireless network is much more than the wired network. Denial of service in wireless could be done through having same frequency value as the one used by the wireless network. For example, the IEEE 802.11 b frequency is 2.4 GHZ and the microwave oven frequency is also 2.4 GHZ. If you are using your wireless laptop and you turn on your microwave oven you will loose your wireless connection.
2) Traffic analysis: The attacker gains intelligence by monitoring the transmission of messages between the manager and agent. Currently there are free software provided for wireless to analyze the traffic between two parities such as Airmagnet [6].

Two vulnerabilities are discovered in the implementation of SNMPv3 over wireless networks.

1) The one way authentication used in SNMPv3 leads to the man-in-the-middle (MITM) attack as in the wireless network. The MITM can play a dual role: An agent and a manager. In this case, the manager will start managing the agent through the MITM. Moreover, the MITM may take the role of the agent; As a consequence, the manager, which is the non-authoritative entity, will try to synchronize its clock (SNMP engine time, SNMP engine boots) to that of the agent, which is the authoritative entity. This will render all the communication with the authentic device as unauthentic.
2) An attacker can take his time to crack the admin password, without drawing attention to his activity, through preventing the device from sending traps for failed authentication [4]. Once the admin password is discovered, the attacker will be able to manage all the devices that belong to the manager. In this case, updating the admin password will make no sense since the old password is already known by the attacker. The following is the password update algorithm used by SNMPv3 [10]:

Manager Entity:

1- Generate random

2- Compute: digest = Hash (Oldpassword || random)

3- Delta = digest XOR Newpassword

4- ProtocolKeyChange = (random || Delta)

Then it sends the message setRequest (protocolKeyChange) to the Receiver.

Agent Entity:

1- Compute digest = Hash(Oldpassword || random)

2- Compute Newpassword = digest XOR Delta

NOTE: digest XOR Delta = digest XOR (digest XOR Newpassword) = Newpassword

V. Modified Security Architecture

Our architecture is designed to provide two-way authentication between the manager and the agent using the certificate authority entity instead of the admin password, which provides one way authentication. Moreover, Diffie-Hellman method is used for symmetric key exchange instead of deriving the keys from the password. Finally, the MIB table of the agent, which contains the username, password and access, must be changed to username, public key and access, and the MIB table of the Manager, which contains username and password, must be changed to username and publickey.

A. Terminology and Notations

Notations used in this paper are defined as follows:

CA: The Certificate Authority is the entity that signs and issues the certificate for all entities. Moreover, it contains a table that lists all the managed devices by the manager.

ME	Manager Entity
AE	Agent Entity
ID_{ME}	ME's identity
ID_{AE}	AE's identity
$Sign_{ME}$	ME's signature
$Sign_{AE}$	AE's signature
$Cert_{ME}$	ME's certificate
$Cert_{AE}$	AE's certificate
K	Shared symmetric key
$m\ mod\ n$	Residue of m divided by n
$H()$	One-way hash function
P	Large prime number
Z_p^*	Multiplicative group of Zp
α	Generator in Z_p^*
$Time_{ME}$	Time stamp made by ME
$Time_{AE}$	Time stamp made by AE
$ME \longrightarrow AE$: M	ME sends the message M to the AE
$\Phi(n)$	The Euler function. It computes the order of the set. $\Phi(n) = p - 1$

B. Architecture

The modified security architecture consists of three entities CA, ME and AE. The CA signs the certification for both entities. The ME and AE need to register and get their public key certificates from CA [9]. So, an entity can easily authenticate another entity through this trust model. According to the modified architecture, when a manager needs to manage an agent, they use the following protocol to authenticate each other (Figure 3):

1) $ME \longrightarrow AE: \quad ID_{ME}, Cert_{ME}$
2) $AE \longrightarrow ME: \quad ID_{AE}, Cert_{AE}$

In step 1, ME sends its identity and certificate to the AE. AE verifies through CA whether or not the certificate is correct. If the certificate is correct, AE will authenticate ME.

In step 2, AE sends its identity and certificate to ME. The manager entity verifies through CA whether or not the certificate is correct. If the certificate is correct, ME will authenticate AE.

After the two-way authentication is completed, ME and AE will use the public cryptography Diffie-Hellman algorithm to

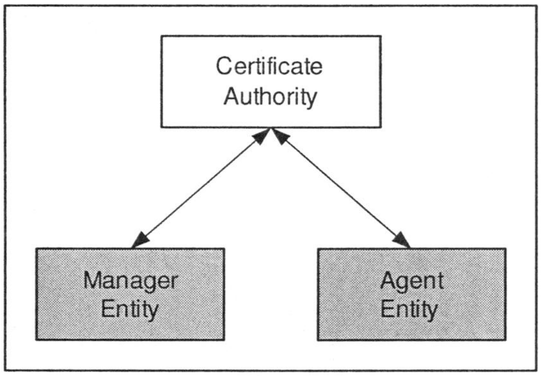

Fig.3. Two-Way Authentication

exchange the symmetric keys. They use the following key agreement protocol (Figure 4):

1) $ME \longrightarrow AE:$ ID_{ME},ID_{AE},$Time_{ME}$,α^a,α,p,$Sign_{ME}$
2) $AE \longrightarrow ME:$ $ID_{AE}, ID_{ME}, Time_{AE}, \alpha^b, Sign_{AE}$
3) $ME \longrightarrow AE:$ $ID_{ME}, ID_{AE}, Time_{ME}, Sign_{ME}$

In step1, ME chooses a large prime number p and a generator α of Z_p^*. It then chooses a private value a (where a is between $1 < a \leq \Phi(n)$) and computes α^a mod p. Finally, it computes its signature through computing the following:

$$Sign_{ME} = Sign_{ME}(H(ID_{ME}, ID_{AE}, Time_{ME}, \alpha^a, \alpha, p))$$

Then, ME sends the message to AE.

In step 2, AE receives the messages from ME. AE first verifies whether or not the messages $Time_{ME}$ and $Sign_{ME}$ are correct. If they are correct, then AE chooses a private value b (where b is between $1 < a \leq \Phi(n)$) and computes α^b mod p. Finally, it computes its signature as follows:

$$Sign_{AE} = Sign_{AE}(H(ID_{AE}, ID_{ME}, Time_{AE}, \alpha^b))$$

Then, AE sends the message to ME.

In Step 3, the ME verifies whether or not the messages: $Time_{AE}$, $Sign_{AE}$ are correct. If they are correct, then it computes the signature:

$$Sign_{ME} = Sign_{ME}(H(ID_{ME}, ID_{AE}, Time_{ME}, Time_{AE}, \alpha^b))$$

Then, ME sends the message to AE.

Finally, AE verifies whether or not the messages received from ME are correct. If correct, it means that ME and AE get the correct shared key K.

The key will be computed as follows:

$$\begin{aligned} K_{ME} &= (\alpha^a)^b modp \\ K_{AE} &= (\alpha^b)^a modp. \end{aligned}$$

Here is an example of the Diffie-Hellman Key Exchange algorithm [5]:

Example 1: - ME chooses p = 71
- ME chooses the generator α = 69
- ME private value a: a = 29
- Computing x= α^a = 61
- Public Key of ME is (x, α^a, p) = {61, 69, 71}
- AE private value b : b = 40

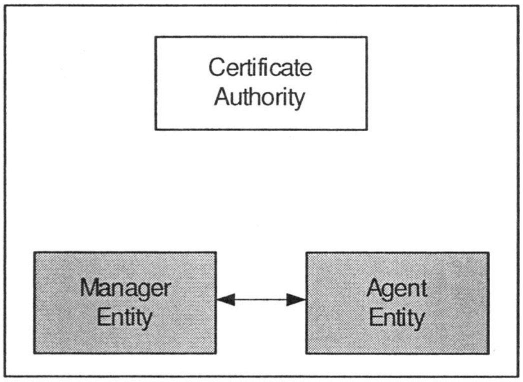

Fig.4. Secure Key Exchange

- Computing y= α^b = 32
- Public Key of AE is (y, α^b, p) ={32, 69, 71}
- Ka =32
- Kb =32

C. Modified Architecture Analysis

In the modified security architecture, if an attacker wants to apply a MITM attack, the receiver can easily discover it through the exchanged signatures. Moreover, the attacker cannot modify the message because of the use of time stamp and signatures in each step of the protocol. In addition to this, attacking Diffie-Hellman algorithm depends on the discrete logarithm problem, which usually needs too much time to be computed. For this reason, the manager is going to generate a new generator α, a new private value a and then it computes α^a to ensure the freshness of the new public key that will be sent to the agent. Finally, if the intruder changes the messages in the authentication phase, the receiver can discover that in the key exchange phase, since the receiver needs to verify the correctness of the following messages: identity and signature.

VI. Conclusion

The protocol SNMPv3 with its existing security is not sufficient for wireless network, where the intruder has many tools to analyze and crack password. The protocol SNMPv3 uses the admin password for one-way authentication and from this password the keys are derived. If an intruder is capable of knowing the password, the intruder can easily manage all the devices in the domain of the manager whose password has been cracked. In our new architecture, we presented two-way authentication independent of the admin password using the certification authority. The latter is the entity that signs and issues the certificate to both the manager and agent. Diffie-Hellman algorithm is used for secure key exchange between the manager and the agent. To ensure the security of Diffie-Hellman, time stamps and signatures are used in the key exchange protocol to prevent MITM attack. Finally, if an intruder wants to attack the Diffie-Hellman algorithm, the intruder needs to solve the discrete logarithm problem, which usually requires too much computation time.

REFERENCES

[1] U. Blumenthal and B. Wijnen, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, RFC 3414, December 2002.

[2] N. Borisov, I. Goldberg and D. Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*, 7^{th} Annual Conference on Mobile Computing and Networking, July 16-21, 2001.

[3] J. Case, R. Mundy, D. Partain and B. Stewart, *Introduction to Version 3 of the Internet-standard Network Management Framework*, RFC 2570, April 1999.

[4] P. Chatzimisios,*Security issues and vulnerabilities of the SNMP protocol*, IEEE Catalog Number: 04EX865, ISBN: 0-7803-8532-2.

[5] Internet Engineering Task Force (IETF) Working Group, *Diffie-Hellman Key Agreement Method*, RFC 2631, June 1999.

[6] M. Maxim and D. Pollino, *Wireless Security Book*, ISBN:0-07-222286-7.

[7] A. Menezes, P. Oorschot and S. Vanstone,*Handbook of applied Cryptography*, CRC Press, ISBN: 0-8493-8523-7, October 1996.

[8] A. Mishra and W. Arbaugh, *An Initial Security Analysis of the IEEE 802.1X Standard*, University of Maryland, 2002.

[9] R. Song and L. Korba, *Security Communication Architecture for Mobile Agents and E-commerce*, National Research Council Canada, 2003.

[10] W. B. Stallings, *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*, 3^{rd} Edition, Addison Wesley, 1999.