SNMPv3 네트워크 관리메시지 보호를 지원하는 Diffie-Hellman 키 분배 방안

황일선* 박병연* 김동균* 김보문** 이명훈** 조인준**

*한국과학기술정보연구원 **배재대학교 컴퓨터공학과

Diffie-Hellman Key Distribute Scheme Supporting SNMPv3 USM for Protection of SNMP Messages

Il-sun Hwang*, Byung-yeon Park*, Dong-kun Kim*,

Bo-moon Kim**, Myung-hun Lee** In-june Cho**

*Korea Institute of Science and Technology Information

**Department of Computer Engineering Paichai Univ.

요 약

현재 IETF RFC 3414에서 제안한 SNMP 메시지 인증 및 기밀성 서비스용 키 분배 방식은 관리자의 패스워드를 기반으로 국지 키를 생성하는 알고리즘을 사용한다. 이는 관리자의 패스워드 노출 방지를 위해 관리자가 지리적으로 분산된 SNMP 관리객체(Managed Agent)를 순회하면서 설치해야 한다는 문제점과 또한 관리객체에 SNMP 메시지를 전송되는 시점에서 국지 키가 계산되어 SNMP 메시지의 전송지연 문제점을 내포하고 있다.

본 논문에서는 누구나 관리객체 설치가 가능하고 SNMP 메시지 전송지연을 제거할 수 있도록 SNMPv3 USM에 Diffie-Hellman 키 분배 방식을 적용하는 방안을 제안하였다. 제안된 방식은 RFC 3414와 동일한 수준에서 SNMP 메시지 인증 및 기밀성 서비스를 제공한다.

I. 서론

최근 인터넷 사용자의 급격한 증가와 초고속 인터넷 망의 구축, 그리고 여러 다양한 네트워크 응용 개발 등으로 인하여 네트워크 트래픽이 급격히 증가되고 네트워크를 관리하고 보호하려는 다양한 서비스들이 중요한 이슈로 떠올랐다.

인터넷 기반에서 망관리 프로토콜인 SNMPv3 USM(User-based Security Model)은 IETF RFC 3414으로 제정되었고[1], 현재 사용되고 있는 해쉬 알고리즘(Hash(MD5, SHA-1))과 암호화 알고리즘(CBC-DES)을 프레임 워크에 삽입[2]하여 보다 안전한 SNMP 메시지 전송을 할 수 있도록 하였다. 하지만 키 분배 방식에 있어서 관리자 패스워드를 기반으로 국지키(Localized Key)[3]를 생성하여 인증 및 기밀성 서비스를 제공한다. 이는 SNMP 관리객체(Managed Agent) 설치시 관리자의 패스워드가 필요하기 때문에 관리자가 직접 모든 관리객체를 설치해야 한다는 문제점을 내포하고 있다. 또한 SNMP관리주체가 관리객체에 SNMP 메시지를 보내는 시점에서 인증(AuthKey) 키 및 기밀(PrivKey)키를 계산하여 분배 받기 때문에 SNMP메시지 전송지연 현상을 야기한다.

본 논문에서는 이러한 문제점 해결을 위해 SNMP메시지 인증 및 기밀성 서비스용 키 분배를 관리자 키를 기반으로 한 국지키 분배방식에서 Diffie-Hellman 키 분배방식[4]으로 대체하는 방안을 제안하였다.

II. SNMPv3 USM에서 SNMP메시지 인증 및 기밀성 서비스용 키 분배 방식(RFC 3414)

USM에서 사용 중인 국지 키 방식은 관리 객체(Managed Agent) 설치 시 관리자가 자신의 패스워드를 국지 키 생성 알고리즘에 입력하여 인증키(AuthKey)와 기밀키(PrivKey)를 분배 받는다. 그림 1)은 SNMP 관리주체(메니저)와 SNMP 관리객체(에이전트)가 동일한 인증(AuthKey)키 및 기밀(PrivKey)키 분배 방법을 설명하고 있다.

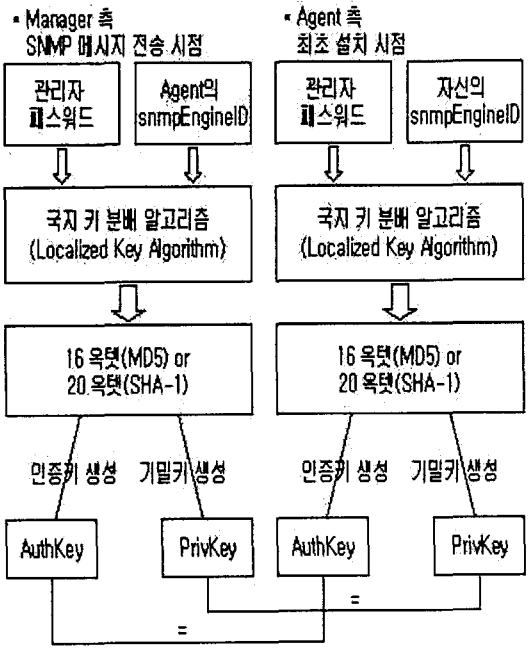

그림 1 : USM에서 인증 및 기밀키 생성

1. SNMP메니저에서 인증(AuthKey)키 및 기밀(PrivKey)키 분배 방법

그림 1)에서 보듯이 SNMP메니저와 에이전트간에 전송되는 SNMP메시지 보호를 위한 인증(AuthKey)키 및 기밀(PrivKey)키는 SNMP메니저가 SNMP메시지를 관리객체에 보내는 시점에서 이루어진다. 즉, 국지키 분배 알고리즘에 관리자의 패스워드와 보내고자하는 관리객체의 SNMP엔진 식별자인 snmpEngineID를 입력하여 16옥텟/20옥텟 스트링을 얻고 이를 가공하여 인증(AuthKey)키 및 기밀(PrivKey)키를 분배 받는 방식이다.

2. SNMP에이전트에서 인증(AuthKey)키 및 기밀(PrivKey)키 분배 방법

그림 1)에서 본바와 같이 에이전트와 메니저간에 전송되는 SNMP메시지 보호를 위해 인증(AuthKey)키 및 기밀(PrivKey)키 분배는 SNMP 관리객체 설치시점에서 이루어진다. 즉, SNMP 메니저가 직접 관리객체(에이전트)에 자신의 패스워드와 관리객체의 SNMP엔진 식별자인 snmpEngineID를 국지키 분배알고리즘에 입력한다. 국지키 분배 알고리즘은 16옥텟/20옥텟 스트링을 출력하고 이를 가공하여 인증(AuthKey)키 및 기밀(PrivKey)키를 분배 받는 방식이다.

3. SNMPv3 키 분배 분석 및 문제점

상기의 1항과 2항을 통해서 SNMP메니저와 에이전트들 간에는 서로 다른 인증(AuthKey)키 및 기밀(PrivKey)키 쌍을 분배받게 된다. 이는 SNMP 메니저의 패스워드가 기밀하다는 전제를 기반으로 한 것이다. 이러한 키분배 방식의 특징은 SNMP 메니저가 별도의 인증키 및 기밀키를 저장하여 유지하지 않고 관리객체에 SNMP메시지를 보내는 시점에서 해당 키를 계산한다는 점이다.

하지만 이러한 방식의 키 분배는 다음과 같은 문제점을 내포한다. 첫째, SNMP 메니저의 패스워드 기밀성 유지를 위해 SNMP 메니저가 직접 관리객체(에이전트)를 설치해야 한다. 이는 통신장비 설치를 SNMP 메니저에 의존해야 한다는 문제점을 야기한다. 둘째, SNMP 메니저가 SNMP메시지를 보내는 시점에서 인증(AuthKey)키 및 기밀(PrivKey)키가 계산되어 SNMP메시지 전송지연을 야기한다.

다음 장에서 이러한 문제점 해결을 위해 Diffie-Hellman 키 분배 방식을 제안한다.

III. SNMPv3 USM에서 Diffie-Hellman 키 분배방식 적용 방안 제안

앞서 언급한 문제점들을 해결하기 위하여 Diffie-Hellman 키 분배방식을 인증 및 기밀키 분배과정에 적용하는 방안을 제안한다.

1. Diffie-Hellman 키 분배방식 적용절차

SNMP 메니저와 에이전트간에 Diffie-Hellman 기밀키 분배는 에이전트 설치시점에서 그림 2)와 같은 절차에 의해 이루어진다.

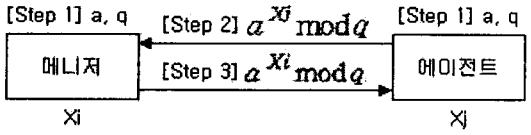

그림 2 : Diffie-Hellman 키 생성 방법

[Step 1] a, q를 메니저와 에이전트에 공개(q는 소수 a는 q보다 작은 정수)

[Step 2] 에이전트 :

- Xj(임의 랜덤 값) 선택
- $(a)^{Xj} \bmod q$ 값 계산
- 계산 된 $(a)^{Xj} \bmod q$를 메니저에 전송

[Step 3] 메니저 :

- Xi(임의 랜덤 값) 선택
- $(a)^{Xi} \bmod q$ 값 계산
- 계산 된 $(a)^{Xi} \bmod q$를 에이전트에 전송

[Step 4] 에이전트 : $(a^{Xi})^{Xj} \bmod q$ 값을 계산하여 Diffie-Hellman 기밀키 생성①

메니저 : $(a^{Xj})^{Xi} \bmod q$ 값을 계산하여 Diffie-Hellman 기밀키 생성…②

[Step 4]의 ①과 ②에서 계산된 기밀키는 SNMP 메니저와 에이전트간의 인증 및 기밀키를 생성에 사용된다. 이와 관련된 구체적인 절차는 그림 3)과 같다. 그림 3)에서 보듯이 SNMP 메니저는 에이전트가 설치되는 시점에서 SNMP메시지 보호를 위한 인증(AuthKey)키 및 기밀(PrivKey) 키를 생성한다. 즉, 기존의 국지키 분배 알고리즘에 관리자의 패스워드가 사용되는 대신에 Diffie-Hellman 키 교환 알고리즘을 통해 분배된 기밀키(즉, Step 4의 ①과 ②)를 사용한다. 이후의 단계로 메니저와 에인전트가 최종적인 인증 및 기밀키를 생성하는 방법은 RFC3414에서 제시한 절차와 동일하다.

이렇게 생성된 인증 및 기밀키는 메니저와 에이전트의 비휘발성 저장매체에 각각 저장되어 SNMP 메시지 보호에 직접 사용된다.

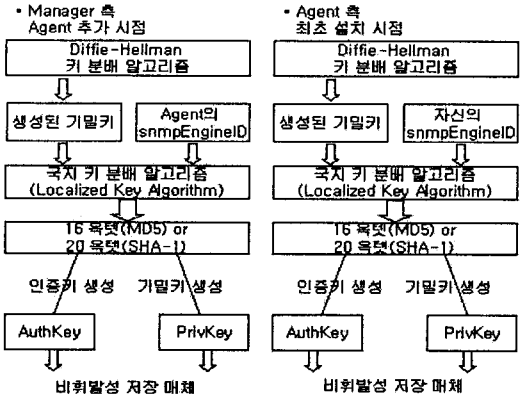

그림 3 : Diffie-Hellman을 적용한 USM

2. RFC3414방안과 비교

제안방안과 RFC 3414방안의 근본적인 차이점은 다음과 같다. 첫째, 인증 및 기밀키 생성과정에 SNMP메니저의 패스워드 사용을 Diffie-Hellman 기밀키로 변경한 점을 들 수 있다. 둘째, 관리대상이 되는 SNMP 에이전트 설치시점에 SNMP메니저와 설치 에이전트간에 사용될 인증 및 기밀키 분배가 완성되어 비휘발성 저장매체에 저장된다. 이는 RFC3414에서 SNMP메시지 전송시점에 인증 및 기밀키가 계산된 것과는 다르다.

상기와 같은 특징을 가진 제안방안을 통해서 기존의 RFC3414에서 제시한 방안이 가지고 있는 두 가지에 문제점(즉, ① 에이전트 설치시 SNMP 메니저에 의존문제. ② SNMP메시지 전송지연 문제)을 해결할 수 있다. 첫째, Diffie-Hellman 키 분배방식을 사용함에 따라 SNMP메니저의 패스워드를 알지 못하는 네트워크 관계자가 SNMP에이전트를 설치할 수 있다. 이로서 SNMP 관리자의 패스워드 노출 때문에 관리자만이 SNMP에이전트를 설치해야 하는 문제점을 해결하였다. 둘째, SNMP 에이전트 설치시점에 생성된 인증 및 기밀키를 비휘발성 저장매체에 저장하여 이를 SNMP 메시지 전송시점에 직접 사용함으로써 인증 및 기밀키 계산에 소요되는 만큼의 SNMP메시지 전송지연 현상을 제거하였다.

3. 제안방안의 보안성 분석 및 평가

제안방안에서 적용한 Diffie-Hellman 알고리즘은 MITM(Man-In-The-Middle)공격에 취약하다. 이러한 취약점은 키를 분배받는 양자의 관계에 따라 보안취약성 정도가 좌우된다. SNMP에서 관리

주체인 메니저와 관리대상인 에이전트들간의 관계는 특정 관리도메인을 중심으로 형성된다. 이는 불특정 대상을 중심으로 이루어지는 환경에서 Diffie-Hellman키 분배환경과는 다르다. 따라서 본 논문에서 SNMP메니저는 미리 알고 있는 SNMP 에이전트를 설치하는 시점에서 Diffie-Hellman 키를 분배받고 이를 SNMP엔진ID와 결합하여 인증 및 기밀키를 생성하기 때문에 MITM공격을 설치 시점으로 제한한다. 또한 인증 및 기밀키에 SNMP엔진 ID요소가 반영되기 때문에 불법적인 SNMP에이전트와 인증 및 기밀키 분배가 원천적으로 차단된다.

다음으로 SNMP메시지 보호를 위한 인증 및 기밀키를 미리 저장하는 방식에 대한 평가이다. RFC3414에서 SNMP에이전트는 자신이 설치되는 시점에 이들 키를 저장한다. 반면에 SNMP메니저는 SNMP메시지를 보내는 시점에 보내고자 하는 SNMP에이전트의 인증 및 기밀키를 계산에 의해 생성한다. 따라서 SNMP메니저는 각 에이전트에 대해 이들 키를 저장하지 않는다. 하지만 본 논문에서 제안방안에서 SNMP 에이전트가 이들 키의 저장방식은 RFC3414와 동일하다. 하지만 SNMP 메니저에서는 이들 키를 저장하기 때문에 RFC 3414와 다르다. 이는 SNMP메니저 시스템에서 사용자 식별 및 인증체제를 구축에 필요한 패스워드 보호 수준에서 이들 키들이 보호되어야 함을 전제로 한다. 해커와 같은 공격자로부터 보다 안전하게 이들 키의 보호를 위해서는 Secure OS와 같은 추가적인 보안설비가 필요하다.

Ⅳ. 결론

본 논문에서는 현재 IETF RFC 3414 USM에서 키 교환방식인 국지 키 교환방식의 문제점을 도출하고 이들을 해결할 수 있는 새로운 방안을 제안하였다.

제안방안에서는 SNMP메니저와 에이전트간에 인증 및 기밀키 분배과정에 Diffe-Hellman 키 분배 알고리즘을 도입하여 SNMP에이전트 설치자를 SNMP 메니저로부터 불특정 네트워크관계자로 확대하였고 SNMP에이전트 설치시점에 인증 및 기밀키를 분배받아 SNMP메니저 시스템에 저장하여 SNMP메시지 전송지연 현상을 제거하였다. 이럼에도 불구하고 RFC3414와 동일한 수준에서 SNMP메시지 보호서비스를 제공한다.

참고문헌

[1] Blumenthal, U. and B. Wijnen, "User-Based Security Model(USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[2] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[3] U. Blumenthal, N. C. Hien, B. Wijnen "Key Derivation for Network Management Applications" IEEE Network Magazine, April/May issue, 1997.

[4] R. Housley, RTFM Inc. "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999