인증 게이트웨이를 활용한 ESM 시스템의 개발

김재한°, 한기준, 백석철
건국대학교 컴퓨터공학과, ㈜하우리
{jhkim°, kjhan}@db.konkuk.ac.kr, scbaek86@hotmail.com

Development of an ESM System using Authentication Gateway

Jae-Han Kim°, Ki-Joon Han, Suk-Chul Baek
Department of Computer Science & Engineering, KonKuk University, HAURI Inc.

요 약

인터넷을 이용하는 인구가 늘어남에 따라 인터넷을 통해 제공되는 서비스도 점점 다양해지고 있다. 이로 인하여, 다양한 서비스를 제공하는 각종 서버들에 대한 보안 사고도 증가하고 있다. 그리고, 보안에 대한 관심과 필요성이 증가하면서 많은 보안 솔루션들이 개발되었으며, 다양한 보안 솔루션을 상호 연동함으로써 종합적인 보안 관리를 하기 위한 ESM 시스템이 제시 되었다. ESM 시스템은 보안 위협에 대해 빠른 판단, 대응, 그리고 원격지 네트워크에 대한 보안 관리를 가능하게 한다. 그러나, 원격지 네트워크에 대한 보안 관리는 인터넷을 거치기 때문에 많은 보안 위협에 직접적으로 노출될 수 있다. 이를 해결하기 위해서 ESM의 메인 시스템 부분이 인터넷과 직접 연결되지 않도록 하여 직접적인 보안 위협으로부터 보호하고, 타겟 시스템의 모니터링 정보가 유출, 위조, 변조되는 것을 방지하기 위해서 사용자의 접근을 인증해주는 인증 게이트웨이의 활용이 필요하다. 따라서, 본 논문에서는 ESM의 메인 시스템 부분에 인증을 거친 에이전트만이 접근할 수 있도록 하여 ESM 시스템의 에이전트로부터 오는 정보를 안전하게 받음으로써 원격지 네트워크상의 서버나 보안 솔루션에 대한 통합 보안 관리를 안전하게 수행할 수 있는 인증 게이트웨이를 활용한 ESM 시스템을 개발하였다. 본 논문의 ESM 시스템은 에이전트, 인증 게이트웨이, 매니저, CA 서버, 운용 소프트웨어로 구성되어 있다.

1. 서 론

오늘날 인터넷을 이용하는 인구가 꾸준히 늘어남에 따라 많은 사람의 요구를 충족시키기 위해 다양한 서비스가 제공되고 있다. 이러한 추세에 따라 서비스를 제공하는 서버들에 대한 각종 보안 사고 발생도 점차 증가하고 있는 상황이다[13, 14]. 이로 인하여, 보안에 대한 필요성과 관심이 높아지면서 침입 차단 시스템, 침입 탐지 시스템, 안티 바이러스 제품 등의 많은 보안 관련 솔루션들이 개발되고 있다. 하지만, 이러한 개별 보안 솔루션들만으로는 종합적인 보안 정책 수립이나 다양한 보안 위협에 대해 빠른 대처가 어렵기 때문에, 여러 보안 솔루션을 상호 연동함으로써 종합적인 보안 관리를 하기 위한 ESM(Enterprise Security Management) 시스템이 제시되었다[12].

ESM 시스템은 여러 보안 솔루션들에서 발생하는 다양한 보안 관련 이벤트들을 하나로 모아서 관리함으로써 종합적인 보안 정책을 수립하거나 빠른 판단을 할 수 있도록 해준다. ESM 시스템에 의한 보안 관리는 근거리 네트워크상의 서버나 보안 솔루션뿐만이 아니라 원격지 네트워크상의 서버나 보안 솔루션에 대해서도 보안 관리를 수행할 수 있다. 이 경우 관리의 대상이 원격지에 있기 때문에 관리에 필요한 정보가 인터넷을 경유하여 전달되게 된다. 인터넷과 같은 공용 네트워크는 항상 보안위협에 노출되어 있고 중요 접속 정보 등이 유출될 가능성이 있으며, 특히 ESM 시스템의 중요 부분이 인터넷에 무방비한 상태로 연결되어 있을 경우 공격의 주요 표적이 될 수 있다.

따라서, 원격지 네트워크에 대한 통합 보안 관리를 위해서는 보다 안전하고 신뢰할 수 있는 시스템을 갖춘 ESM 시스템이 필요하다. 이런 조건을 갖추기 위해서는 ESM 시스템의 중요 부분이 인터넷에 직접 연결되지 않도록 보호되어야 하며 타겟 시스템으로부터 클라이언트가 보내오는 모니터링 정보가 유출, 위조, 변조되지 않도록 해야 한다[1, 3].

본 논문에서는 인증 게이트웨이를 활용하여 ESM 시스템의 중요 부분을 인증을 거친 데이타만이 접근할 수 있도록 하여 인터넷을 통한 다양한 보안 위협으로부터 보호하고 PKI(Public Key Infrastructure)를 이용하여 ESM의 클라이언트로부터 오는 정보를 유출, 위조, 변조로부터 보호하여 안전하게 받을 수 있도록 하여 원격지 네트워크상의 서버나 보안 솔루션에 대한 통합 보안 관리를 보다 안전하게 수행할 수 있는 ESM 시스템을 개발하였다.

본 논문의 구성은 다음과 같다. 제 1 장의 서론에 이어 제 2 장에서는 관련 연구로써 ESM과 인증 게이트웨이에 대해 설명한다. 제 3 장에서는 인증 게이트웨이를 활용한 ESM 시스템의 개발에 대하여 설명한다. 마지막으로, 제 4 장에서는 결론과 향후 연구과제에 대해 언급한다.

2. 관련 연구

본 장에서는 관련 연구로써 ESM과 인증 게이트웨이에 대하여 설명한다.

2.1 ESM 시스템

ESM 시스템은 침입 차단 시스템, 침입 탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모아서 관리하는 통합 보안 관리 시스템이다. ESM 시스템은 다양한 보안 솔루션이나 일반 서버들을 모니터링 함으로써 종합적인 보안 정책 수립을 지원하거나 신속하고 효과적인 조치를 위해 각종 경보 기능을 제공한다. 근래에 ESM 시스템은 통합 보안 관리 수준에서 벗어나 시스템 자원 관리(SMM: System Material Management), 망 관 리 시스템(NMS: Network Management System)과 같은 기업 시스템의 자원 관리 분야까지

확대되고 있다.

ESM 시스템은 기업들이 서로 다른 기종의 보안 솔루션 설치에 따른 중복 투자 및 자원 낭비를 줄일 수 있으며, 각종 보안 솔루션 간에 상호 연동함으로써 통합 보안 관리를 통해 다양한 보안 위협에 대해 빠른 판단과 대응을 가능하게 한다. ESM 시스템은 일반적으로 보안 관리 대상 네트워크의 타겟 시스템에 탑재되는 에이전트, 수집된 정보를 관리하는 매니저, 운용 소프트웨어로 구성된다. 매니저는 에이전트에 의해 수집된 정보와 에이전트의 설정 정보 등의 ESM 시스템의 모든 정보가 모이는 곳이기 때문에 가장 중요한 부분이다.

2.2 인증 게이트웨이

인증 게이트웨이는 사용자가 네트워크에 접속하고자 할 경우 강제로 인증을 받게 함으로써 허용되지 않은 사용자의 네트워크 접근을 방지하는 게이트웨이이다[11]. 즉, 네트워크가 신뢰성 있는 사용자의 접근만을 허용하도록 하게 한다. 따라서, 인증 게이트웨이는 IP-Spoofing등을 이용한 불법적 접근을 방지할 수 있으며, 다른 보안 솔루션과 연동하여 보안 위협을 가할 수 있는 데이타를 동적으로 차단하는 등의 다양한 보안 솔루션에 활용 가능하다. 본 논문에서는 인증 게이트웨이의 이러한 기능을 이용하여 매니저가 인터넷에 바로 노출되지 않도록 매니저의 선단에 인증 게이트웨이를 배치하여 매니저가 인터넷상의 많은 보안 위협으로부터 보호될 수 있도록 하였다.

인증 게이트웨이의 인증은 LDAP, DB, user_auth, Kerberos, IP Address, SSH 등의 여러 가지 방법을 사용할 수 있다[11]. 본 논문의 인증 게이트웨이는 PKI 방식를 사용하여 인증한다. PKI 방식은 유일한 한 쌍의 공개키와 개인키를 가지고 있으며, 공개키로 암호화한 데이타는 개인키로만 풀리고 개인키로 암호화한 데이타는 공개키로만 풀리는 특징을 가지고 있다[2, 6, 7]. PKI는 사용자(User), 등록기관(RA, Registration Authority), 인증기관(CA; Certification Authority), 디렉토리 서버(DS; Directory Server)로 구성된다[2, 6].

본 논문에서는 CA 서버가 Trusted-Third Party에 위치했다고 가정하고 에이전트, 인증 게이트웨이, 그리고 매니저와 아무 제약없이 인증서 정보를 주고 받을 수 있게 하였다.

3. 인증 게이트웨이를 활용한 ESM 시스템의 개발

본 장에서는 인증 게이트웨이를 활용한 ESM 시스템의 개념적 흐름도를 통해 전체 시스템의 개념적 흐름을 살펴보고 전체 구조도을 통해 각 구성 요소의 모듈별 기능들을 설명한다.

3.1 시스템의 개념적 흐름

본 논문에서 제시하는 인증 게이트웨이를 활용한 ESM 시스템의 개념적 흐름도는 그림 1과 같다.

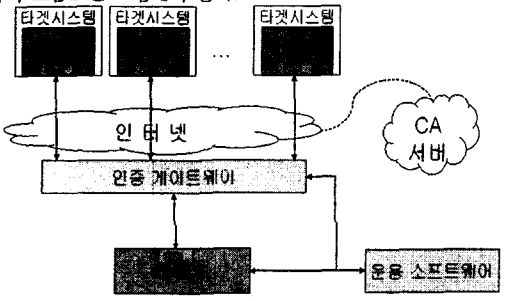

그림 1 시스템의 개념적 흐름도

본 논문의 ESM 시스템은 크게 에이전트, 매니저, 인증 게이트웨이, CA 서버, 운용 소프트웨어로 구성된다. 타겟 시스템은 에이전트가 설치된 침입 차단 시스템, 침입 탐지 시스템 등의 기존 보안 솔루션이나 일반적인 인터넷 서비스를 담당하는 서버를 의미한다. 에이전트는 타겟 시스템에 설치되어 수집한 정보를 매니저에 보내는 클라이언트를 뜻하며, 인증 게이트웨이는 에이전트에 대한 인증과 매니저를 보안 위협에 대해 보호하는 게이트웨이이다. 매니저는 에이전트에서 보내진 모니터링 정보를 정리하여 저장하거나 운용 소프트웨어로 보내는 서버이다. CA 서버는 인증 서버로서 공개키 인증서를 생성, 보관, 발급한다. 운용 소프트웨어는 전체 시스템을 운용하기 위한 소프트웨어이다. 전체 시스템의 흐름을 순서대로 살펴보면 다음과 같다.

① 에이전트가 타겟 시스템으로부터 모니터링 정보를 수집한다
② CA 서버로부터 인증서를 발급받고 수집된 정보와 함께 SSL이용해 매니저로 보낸다.
③ 수집된 정보는 인터넷을 거쳐 먼저 인증 게이트웨이에 도달된다. 인증 게이트웨이의 인증을 통과하면 매니저로 보내진다.
④ 매니저는 수집된 정보를 받고 정해진 분류 방법에 따라 매니저에 저장하거나 운용 소프트웨어로 보낸다.
⑤ 운용 소프트웨어는 정보를 받아 정해진 형식을 통해 리포팅하고 이를 토대로 보안 상황을 판단하여 대응한다.

본 논문의 ESM 시스템은 타겟 시스템의 에이전트에서 매니저로 인터넷을 통하여 정보를 전달한다. 이렇게 전송된 정보는 매니저에 도달하기 전에 인증 게이트웨이의 인증을 거치도록 되어 있다. 이것은 매니저가 ESM 시스템의 중요한 부분이므로 다양한 보안 위협으로부터 보호되어야 하기 때문이다. 만일 매니저가 인터넷에 무방비 상태로 노출되어 있다면 공격의 주요 표적이 되어 ESM 시스템뿐만 아니라 보안 관리 대상인 타겟 시스템에도 심각한 영향을 미치게 된다. 따라서, 인증 게이트웨이를 매니저의 선단에 위치시켜 인터넷을 통하여 들어올 수 있는 다양한 보안 위협으로부터 보호하여 원격지 네트워크상의 타겟 시스템에 대해서도 안정성과 신뢰성 있는 보안 관리가 가능하게 하였다.

3.2 시스템의 구조

본 논문에서 제시하는 인증 게이트웨이를 활용한 ESM 시스템의 전체 구조도는 그림 2와 같다.

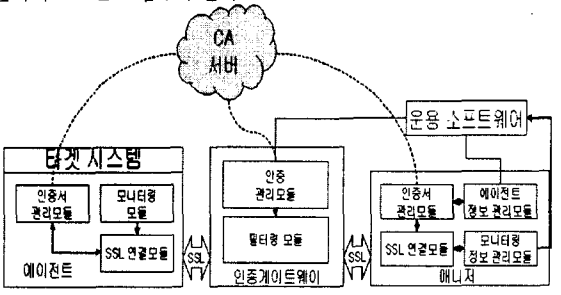

그림 2 시스템의 전체 구조도

인증 게이트웨이를 활용한 ESM 시스템의 주요 구성 요소는 에이전트, 인증 게이트웨이, 매니저, 운용 소프트웨어이고 부가적으로 CA 서버가 포함되어 있다. 에이전트는 타겟 시스템의 모니터링 정보를 수집하고, 인증 게이트웨이는 에이전트에 대한 인증과 매니저의 보호를 담당하는 게이트웨이이다. 매니저는 모니터링 정보와 에이전트 정보를 분류, 정리, 저장하거나 운용 소프트웨어로 보낸다. 운용 소프트웨어는 타겟 시스템에 대한 리포팅 기능과 ESM 시스템의 설정을 변경하는 기능을 가진 소프트웨어이다.

3.3 시스템의 주요 구성 요소

본 논문에서 제시한 인증 게이트웨이를 활용한 ESM 시스템의 주요 구성 요소와 각 구성 요소 별 세부 모듈에 대한 설명은 다음과 같다.

3.3.1 에이전트

에이전트는 보안 관리 대상 네트워크의 타겟 시스템에 탑재되어 시스템의 자원, 서비스 포트의 상태, 시스템 로그 정보를 수집하여 매니저에 전달한다. 타겟 시스템이 보안 솔루션인 경우, 보안 관련 이벤트 정보도 함께 수집한다. 에이전트는 인증서 관리 모듈, 모니터링 모듈, SSL 연결 모듈로 구성된다. 인증서 관리 모듈은 CA 서버로부터 인증서를 발급받고 SSL 연결 시 사용될 수 있도록 하는 기능을 담당한다. 모니터링 모듈은 타겟 시스템의 자원 사용 현황, 제공하는 서비스 종류별 정보, 시스템 로그 정보, 보안 관련 이벤트 정보 등을 수집하여 SSL 연결 모듈로 보내는 기능을 담당한다. SSL 연결 모듈은 인증서 관리 모듈에서 발급받은 인증서와 함께 모니터링 모듈에서 받은 정보를 SSL 연결을 통해 매니저에 전달하는 기능을 담당한다.

3.3.2 인증 게이트웨이

인증 게이트웨이는 현재 매니저의 관리 대상인 에이전트에 대한 인증 정보를 가지고 해당 에이전트로부터 오는 데이타만을 통과시키는 기능을 하여 매니저에 대한 다양한 보안 위협을 차단하고 불확실한 정보가 전달되지 않도록 한다. 인증 게이트웨이는 인증 관리 모듈과 필터링 모듈로 구성된다. 인증 관리 모듈은 에이전트를 포함한 모든 접근 시도에 대해 허용여부를 결정하는데 필요한 인증 정보를 관리하고, 이를 이용해 접근 허용 여부를 판단하는 기능을 담당한다. 인증 관리 모듈에서 에이전트를 인증하기 위해 인증 게이트웨이의 공개키 인증서를 확인하며 이를 위해 사용하는 인증 정보로 IP 주소와 인증 게이트웨이가 발급 받은 인증서 두 가지를 사용한다. 필터링 모듈은 인증 관리 모듈의 접근 허용 여부에 따라 접근을 차단하거나 통과 시키는 기능을 담당한다.

3.3.3 매니저

매니저는 여러 에이전트를 관리하며 에이전트로부터 전달받은 수집 정보를 분류 및 정리하여 직접 저장하거나 운용 소프트웨어로 보낸다. 매니저는 인증서 관리 모듈, 에이전트 정보 관리 모듈, 모니터링 정보 관리 모듈, SSL 연결 모듈로 구성된다. 인증서 관리 모듈은 에이전트로부터 전달받은 인증서를 CA 서버를 통해 받은 에이전트의 인증서와 비교하여 에이전트 정보 관리 모듈에서 관리하는 에이전트 정보와 비교하여 관리대상 에이전트가 맞는지를 확인하고 어떤 타겟 시스템에서 온 정보인지를 판별하는 기능을 담당한다. 에이전트 정보 관리 모듈은 관리대상 에이전트 정보의 리스트를 관리하는 기능을 담당한다. 에이전트 정보는 에이전트가 설치된 타겟 시스템의 IP 주소, 이름 정보, 모니터링 레벨 등이며 에이전트 정보 관리 모듈은 에이전트의 설정 정보도 함께 가지고 있다. 모니터링 정보 관리 모듈은 에이전트에서 수집하여 보낸 정보를 저장하고 운용 소프트웨어에 보내주는 정보 관리 기능을 담당한다. SSL 연결 모듈은 SSL 을 사용한 연결을 담당한다.

3.3.4 운용 소프트웨어

운용 소프트웨어는 리포팅 기능과 시스템 설정 기능을 가지고 있다. 리포팅 기능은 에이전트로부터 수집된 정보를 매니저가 분류하여 보내주면 정해진 형식에 따라 디스플레이하고, 이상 정보에 대해서는 특별한 표시를 하여 알려주는 기능이다. 시스템 설정 기능은 ESM 시스템의 모니터링 레벨 변경, 에이전트의 등록/삭제 등의 시스템 설정을 변경할 수 있는 기능이다.

4. 결론 및 향후 연구과제

인터넷이 대형화, 다양화 되면서 서비스 제공을 위한 서버가 증가하였고 이에 따른 보안사고가 많아지게 되었다. 이를 해결하기 위해 보안 솔루션이 점차 증가하였고 이들을 통합 관리하기 위한 ESM 시스템이 등장하게 되었다. ESM 시스템은 보안 위협에 대한 빠른 판단, 대처, 그리고 원격지 네트워크에 대한 보안 관리를 가능하게 한다. 그러나, 원격지 네트워크에 대한 보안 관리는 인터넷이라는 공용 네트워크를 통하기 때문에 ESM 시스템의 중요 부분이 보안 위협에 노출될 수 있으므로, 안전하고 신뢰성 있는 보안 관리가 이루어 질 수 없는 문제가 발생하였다. 따라서 본 논문에서는 인증된 사용자의 접근만을 허용하는 인증 게이트웨이를 활용한 ESM 시스템을 개발하였다. 본 논문의 ESM 시스템은 타겟 시스템의 모니터링 정보를 수집하는 에이전트, 에이전트에 대한 인증, 매니저의 보호를 담당하는 게이트웨이, 모니터링 정보와 에이전트 정보를 분류, 정리, 저장하는 매니저, 타겟 시스템에 대한 리포팅과 설정 변경을 할 수 있는 응용 소프트웨어로 구성되어 있다.

본 논문에서 제시한 ESM 시스템은 분산된 원격지 네트워크들에 대한 통합 보안 관리가 필요할 때 유용하게 활용될 수 있을 것이다. 향후에는 인증 게이트웨이에 IDS 기능 등을 추가하여 전체적인 시스템의 기능을 향상시키는 방법에 대한 연구가 필요하다.

참고문헌

[1] Amoroso, E. G., *Intrusion Detection*, Intrusion.Net Books, 1999.

[2] Fung, C. K. and Lee, M. C., " A *denial-of-service resistant* public-key authentication and key establishment protocol," 2002. *21st IEEE International, 2002*, pp. 171-178.

[3] Hunt, C., *TCP/IP Network Administration 2nd Edition*, O' Reilly & Associates Inc., 1999.

[4] Kawase, T., Watanabe, A. and Sasase, I., " Proposal of secure remote access using encryption," Global Telecommunications Conference, 1998, pp. 868-873.

[5] Menezes, J., et.al., *HANDBOOK of APPLIED CRYPTOGRAPHY*, CRC Press LLC, 1997.

[6] OpenCA PKI Development Project, http://www.openca.org/openca, 2003.

[7] OpenSSL: The Open Source toolkit for SSL/TLS, http://www.openssl.org, 2002.

[8] Stevens, W. R., *UNIX Network Programming Volume 1 2nd Edition*, Prentice Hall, 1998.

[9] Suzuki, S. and Nakada, K., " An authentication technique based on distributed security management for the global mobility network," IEEE Journal, 1997, pp. 1608-1617.

[10] Zhu, Y., Wang, B. and Chen, J., " Trusted third party based mutual authentication in UPT system," 1998. ICCT '98. 1998 International Conference, 1998, pp 5.

[11] Zorn, N., *Authentication Gateway HOWTO*, The Linux Documentation Project, 2002.

[12] Zwicky, E. D., et.al., *Building Internet Firewalls*, O' Reilly & Associates, 2000.

[13] 김도형, 김성준, 이원구, 이희규, 이재광, " 침입탐지형 로그 분석기의 설계 및 구현," 한국정보과학회 학술발표논문집 제29권 제1호, 2002, pp. 856-858.

[14] 김정원, 최종욱, 김상진, " 네트워크 침입탐지를 위한 인공면역 시스템의 동적 클론선택 연구," 한국정보과학회 학술발표논문집 제29권 제1호, 2002, pp. 847-849.