MACsec(802.1ae)기반의 보안 VLAN 설계

이준원*, 박선호*, 김성민**, 소희정**, 금기호**, 정태명*
*성균관대학교 정보통신 공학부
**삼성 SDS
e-mail : junimirang@imtl.skku.ac.kr

Design of Secure VLAN on MACsec(802.1ae)

Jun-Won Lee*,Seon-Ho Park*,Seong-Min Kim**,Hee-Jung So**,
Ki-Ho Gum**,Tai-Myoung Cheong*
*Sungkyunkwan Univ
**cSamsung SDS

요 약

MACsec 프로토콜은 Layer2 통신에서 유용한 데이터 암호화 솔루션이다. 하지만 다른 네트워크상에 존재하는 호스트와의 암호화 통신을 위해서는 게이트웨이에서 복호화와 암호화 과정을 반복해야 하는 어려움이 있다. 본 논문은 다른 네트워크 상에 존재하는 호스트와 추가 VLAN을 구성하여 MACsec 통신이 별도 복호화와 암호화 과정을 반복하지 않고 수행될 수 있는 방안을 제시할 것이며, 이를 수행하기 위한 구체적인 시스템 설계와 부가적인 네트워크 구성에 대해 추가적으로 설명할 것이다.

1. 서론

네트워크 상의 각종 보안위협으로부터 조직의 내부 시스템을 보호하기 위한 다양한 솔루션들이 소개되고 적용되는 상황이다. MACsec 프로토콜은 LAN 상에서 호스트 간 통신 시 데이터를 안전하게 보호하기 위한 솔루션으로 각광받고 있다. 하지만 네트워크에 다수의 VLAN이 존재할 경우, 다른 VLAN상의 호스트와 통신을 위해 게이트웨이는 해당 프레임에 대해 복호화 및 암호화 과정을 제공해야 하므로, VLAN 간에 트래픽이 증가할수록 경유하게 되는 게이트웨이는 부하가 상승하여 전체 네트워크 속도 지연 및 어플리케이션 성능저하를 유발하게 된다. 전송 데이터 보안, 불필요한 사용자의 접근 차단, MAC flooding과 같은 보안공격 예방을 위해서도 VLAN 분리는 필수적으로 적용되어야 하므로 MACsec 적용에 한계가 발생할 수 있다. [6]

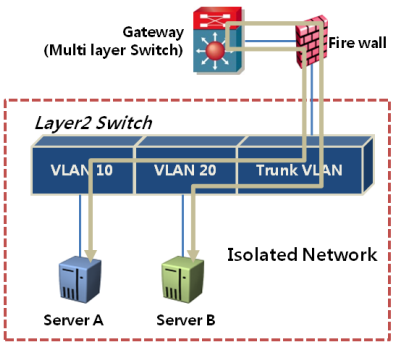
시스템의 특성과 제공하는 서비스에 따라 새로운 VLAN 도입 및 구성변경을 통해 개선을 할 수도 있지만 신규 비용 발생 및 시스템 설정 변경에 따른 많은 수고가 필요하며, 지속적으로 변경이 발생하는 시스템 환경에서는 이러한 대응은 매우 어려운 상황이다.

본 논문은 Port-Based Network Access Control (802.1X)[3]을 응용하여, MACsec 상에서 향상된 네트워크 성능을 제공하는 VLAN 모델을 제시하고자 한다. 2장에서는 일반적인 네트워크 구성 상에서의 취약점을 분석하고, 3장에서는 본 논문에서 핵심을 이루는 802.1X와 Radius(Remote Authentication Dial In User Service)에 대한 관련 기술을 이해하고, 4장에서는 Secure VLAN의 구성 및 프로토콜 설계방안을 제시한다. 5장에서는 이러한 구성 및 프로토콜 변경으로 예상되는 기대효과를 살펴보도록 하겠다.

2. 네트워크 취약점 분석

아래 그림. 1은 내부 시스템 중 별도의 보안 네트워크를 구성한 형태이다. 물리적으로 같은 Network에 존재하지만 VLAN이 분리되어 Server 간의 통신은 Gateway를 거쳐 이루어 진다. 이 경우 VLAN 간 통신은 Gateway 및 Firewall의 부하상승으로 이어지게 된다. 게다가 MACsec과 같은 2계층 보안이 추가된다면 이 프레임을 암호화 또는 복호화하는 과정을 Gateway가 수행해야 하므로 그 부하는 더욱 가중될 것이다.[2],[4] 이와 같이 다른 VLAN에 속해있는 호스트들 간에 MACsec을 적용하기 위해서는 이러한 부담이 남아있는 상황이다.

이러한 문제를 해결하기 위해서는 MACsec 프로토콜을 사용하는 프레임에 대해서는 다른 VLAN에 속해 있을지라도 2계층 상에서 통신이 이루어 질 수 있는 방안이 필요하다. 더불어 다른 IP대역에 속해있는 상대방 호스트와의 통신을 위해 ARP 운영방식에 있어서도 변경이 요구된다.



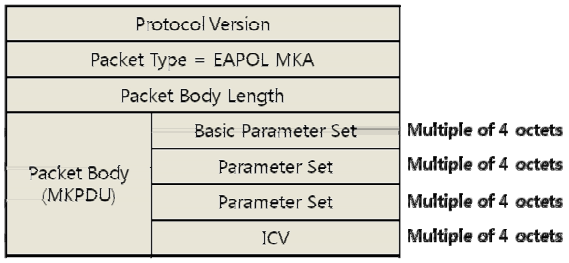
(그림 1) Isolated Network in LAN

3. 관련연구

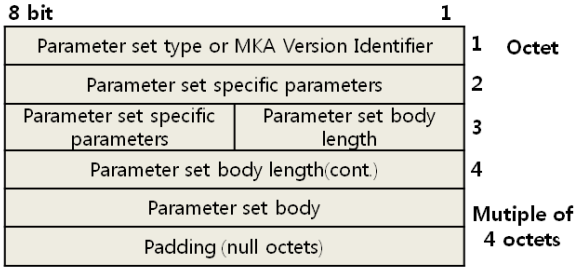
3.1. IEEE 802.1X (Port-Based Network Access Control)

802.1X[3]는 포트 기반의 네트워크 접근제어 표준이다. 본 논문에서 802.1X는 호스트의 log on/log off를 EAP 기능으로 관리하여 해당 정보를 CA-MS(Certificate Association Management Server)로 전달하는 역할과 2010년부터 추가로 정의된 MKA(MACsec Key Agreement) 프로토콜을 지원하기 위해 사용된다. [8]

802.1X는 인증을 요구하는 요청자(Supplicant), 실제적인 접근제어를 수행하는 인증자(Authenticator), 그리고 해당 요청자가 유효한지를 확인하는 인증서버(Authentication Server)로 구성되며, 인증절차는 EAP(Extensible Authentication Protocol)에 의해 상호인증으로 진행되는데 초기화(Initialization) → 시작(Initiation) → 중재(Negotiation) → 인증(Authentication) 의 순서이다. 특히 중재(Negotiation) 단계에서는 EPAOL-MKA의 패킷 형태로 주요한 MACsec Key 정보를 인증서버로부터 할당 받게 된다. 이때 전달되는 MKPDU(MKA Protocol Data Unit)은 그림 2의 형식을 갖는다. Parameter set은 MACsec peer유지 및 SAK 정의를 위해 사용되며, 그림 3과 같이 구성된다. [8]



(그림 2) EAPOL-MAK Packet Body



(그림 3) Parameter set encoding

인증서버에서는 접속하는 호스트 그룹에 따라 VLAN ID를 NAS(Network Access Server)에 할당하기도 하지만 본 논문에서 제시하는 보안VLAN은 다수의 VLAN을 사용하므로 별도 VLAN 할당을 하지 않는다. 단 호스트에 적용될 Default VLAN에 대한 정보가 EAPOL 프레임을 통해 전달될 수 있는 방안이 사전에 마련되어야 한다.

3.2. Radius (Remote Authentication Dial In User Service)

일반적으로 Radius 서버는 인증서버와 인증자간에 Radius-encapsulated EAP 패킷을 전달하는 역할 또는 인증서버로서의 역할을 수행하기도 한다.[1] 조직의 규모 및 서비스 형태에 따라 Radius 서버의 역할은 달라질 수 있지만 EAP동작 및 CA-MS와의 원활한 통신을 위해 랜구간에 적용하는 것이 바람직하다.

Radius 서버의 운용 전, EAPOL PDU가 Version 3 이상을 지원하는 가를 필히 확인해야 한다. Version 2 이하에서는 TLV(Type Length Value, a form of encoding)를 지원하지 않으므로, EAPOL-MKA관련 PDU를 전달할 수 없기 때문이다. [8]

4. 보안 VLAN 설계

현재 대부분의 VLAN 운영방식은 스위치에서 포트 별 VLAN ID를 부여하는 것이 일반적이다.[3] 이 경우 특정 포트에 단일 VLAN을 할당하므로 호스트는 한정된 VLAN 내 에서만 통신이 가능했다. 본 논문에서는 전송되는 프레임에 태깅되는 VLAN ID를 호스트가 속한 CA에 따라 추가로 할당하도록 한다. VLAN ID 수신 및 태깅은 MACsec어플리케이션 모듈에 추가되어 MACsec 프레임 전환과 동시에 이루어 진다. 또한 동일 VLAN 내에서 다른 IP 대역을 가진 호스트들이 통신할 수 있는 방안도 마련하도록 한다.

4.1 CA Management Server

CA-MS(CA Management Server)는 CA별 호스트의 정보를 지속적으로 업데이트하여 동일 CA에 해당하는 호스트에게 전달하는 기능을 수행한다. CA-MS가 인증서버로부터 전달받는 정보는 표1과 같다. 각각의 값은 EAPOL-MKA 파라미터 속성으로부터 승계하며, Member Identifier(96bit) [8] 로는 MAC address를 사용한다.

CKN	Member Identifier	Default VLAN	Update Type (Start/Logoff)

<표 1> Received DATA from Authentication Server

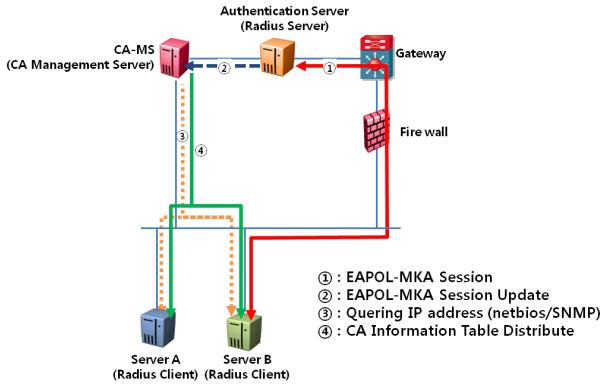
CA-MS는 표 1의 정보를 토대로 CA Information Table을 업데이트하고, Netbios 또는 SNMP를 통해 찾아온 호스트의 IP address를 추가하여, 표 2와 같은 테이블을 모든 VLAN에 MACsec 프레임으로 Broadcast한다. 이때 Broadcast로 해당 정보가 전달되더라도, MACsec에 참여하지 않는 호스트는 SAK를 갖지 않으므로 CA Information 정보를 안전하게 유지할 수 있다.

CKN	Member Identifier	Secure VLAN	IP address	TTL

<표 2> CA Information Table

그림 4는 EAPOL-MKA Session부터 CA Information

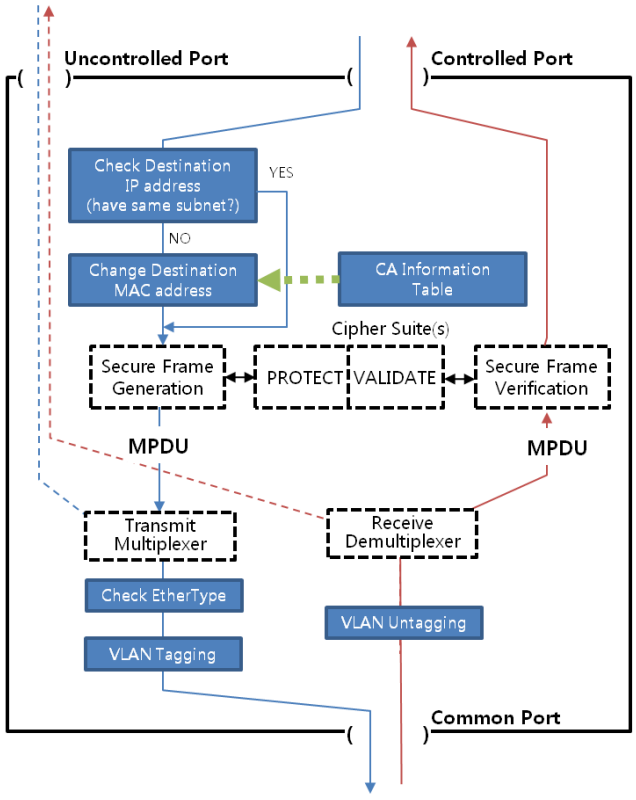
Table 업데이트까지 과정이다. 안정한 네트워크 운용을 위해 CA-MS 는 분리하며, 중간에 추가 방화벽을 설치할 수 있다. 이는 백도어로CA-MS접근하거나 상위 네트워크에 접근하는 것을 차단하기 위함이다.



(그림 4) CA Information Update Flow

4.2. VLAN tagging Method

MACsec에 참여하는 호스트들은 전달받은 CA Information Table을 토대로 VLAN Tagging을 실시하게 된다. VLAN 변경작업은 그림 5와 같이 MACsec의 SecY 프로세스[6]에서 수행된다. Tagging 되는 VLAN 정보는 인증서버로부터 수신한 Default VLAN ID와 CA-MS에서 수신한 Secure VLAN ID를 참고로 하게 된다.



(그림 5) SecY Process with Secure VLAN Module

SecY 프로세스를 살펴보면 VLAN tagging 작업에 앞서 프레임의 목적지 주소 변경작업을 수행하는데 이는 다른 서브넷에 존재하는 호스트에 접근할 경우 게이트웨이의 MAC 어드레스로 설정되기 때문이다. 이를 위해 CA Information Table이 일종의 ARP Table 역할을 수행하게 된다. Check Ether Type 모듈은 MACsec 적용 여부에 따라 다른 VLAN을 할당하는 역할을 수행한다.

5. 적용 후 기대효과

하드웨어적인 측면에서 기대효과를 살펴보면, IP cores 사의 MACsec 전용 프로세서(GCM1-128) [5]를 이용할 경우 500MHz 기준으로 최대 6.4Gbps 처리성능을 나타낸다.[9] 다른 VLAN 간에 업로드/다운로드 양방향으로 1Gbps 트래픽만 존재하더라도 상호 프레임 전달을 위한 복호화/암호화 수행으로 4Gbps 처리능력을 요구하게 된다. 하지만 Secure VLAN 적용 시 별도 복호화/암호화 과정을 요구하지 않으므로 62.5%의 전용 프로세서 자원을 절약하게 된다. 이뿐 아니라 Layer3 통신을 위해 게이트웨이로 향하는 트래픽을 Layer2구간에서 처리함으로써 방화벽 및 게이트웨이 자원을 절감하여 네트워크 성능향상을 기대할 수 있다.

보안적인 측면에서는 제한된 LAN상의 MACsec 프레임을 방화벽 하단에서 처리함으로써 Man-In-The-Middle Attack 등의 공격을 사전에 차단하게 된다.

6. 결론 및 향후 연구

본 논문에서 제시하는 Secure VLAN 솔루션은 일반적인 사용자 환경보다는 보안이 요구되는 데이터를 취급하는 데이터센터 네트워크에 적합하다. 따라서 클라우드 컴퓨팅 환경으로의 전환을 앞두고 있는 시점에서 매우 유용한 활용을 발견할 수 있다. 일례로 클라우드 컴퓨팅에서 통합 표준의 하나로 고려하는 PCI DSS(PCI Data Security Standard)는 취급하는 정보나 기능에 따라 시스템 및 네트워크의 분리를 요구하고 있지만 무조건적인 시스템 분리는 인프라 투자 및 관리비용 상승으로 이어지게 된다.[7] MACsec 기반의 Secure VLAN은 이러한 요구조건을 만족시키면서 기존 네트워크 인프라와 성능을 유지할 수 있는 적합한 솔루션으로 바라볼 수 있다.

나아가 현재 802.1X의 Tunnel속성으로는 제한되어 있는 NAS의 Trunk port 구현은 Secure VLAN의 원활한 구성을 위해 추가적으로 진행될 연구과제이다.

참고문헌

[1] Aboba, B. & Calhoun, P., RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP), RFC 3579, September 2003

[2] Altunbasak, H., Krasser, S., Owen, H., Grimminger, J., Huth, H. & Sokol, J., Securing Layer 2 in Local Area Networks, Networking-ICN 2005, Springer, 2005, pp. 699-706

[3] Congdon, P., Aboba, B., Smith, A., Zorn, G. & Roese, J., IEEE 802.1 X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, RFC3580, September, 2003

[4] Jun-Won, Lee., Secured Network Design for Hyper Market by applying MACsec(802.1AE) Protocol 2010

[5] McGrew, D. & Viega, J.,The Galois/Counter mode of operation (GCM), 2004

[6] Romanow, A., Media Access Control (MAC) Security, IEEE 802.1 AE, 2006

[7] Velte, T., Velte, A. & Elsenpeter, R.,Cloud computing: a practical approach, McGraw-Hill Osborne Media, 2009

[8] IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control, IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), 2010, pp. C1 -205

[9] IPCores AES-GCM MACsec (IEEE 802.1AE) and FC-SP Cores, IP Cores, Inc., 2010 http://www.ipcores.com/msp1_macsec_processor_ip_core.htm