네트워크 보안을 위한 도메인 방식의 키 관리 시스템

이 광 재*, 김 정 선
한국항공대학교 항공전자공학과

A Key Management System for Network Security Using Domain Names

Kwang-Jae Lee*, Jung-sun Kim
Dept. of Avionics, HanKuk Aviation University

요 약

네트워크의 보안문제는 트래픽의 증가요인의 하나로 작용한다. 본 논문에서 키 분배와 인증 문제를 해결하면서 트래픽을 증가를 억제할 수 있는 키 관리 시스템을 제안하였다. 인터넷의 도메인 방식을 이용한 제안된 키 관리 시스템은, 기존의 키 관리 시스템인 중앙집중형 키 관리 및 분산형 키 관리 시스템의 문제점을 개선할 수 있을 뿐 아니라 이들 시스템과 혼용하여 사용할 수 있을 것으로 판단된다. 키의 인증기관은 각각의 도메인에 존재하는 키 분배 센터 내에 분산시켜 상위 도메인으로부터 인증을 받게 되므로 인증 수준을 다중으로 할 수 있으며 단일화 된 인증기관의 위험을 해결할 수 있다.

I. 서론

정보화의 기반 구조로서의 컴퓨터 네트워크는 지역망, 공중망 등의 구분 없이 인터넷으로 상호 연결되어 지속적으로 팽창하고 있으며 최근 들어 ATM(Asynchronous Transfer Mode)과 같은 초고속 전송기술이 개발되면서 더욱 가속되고 있다. 특히 대부분의 컴퓨터가 GUI(Graphic User Interface)와 같은 사용자 인터페이스를 운영체제에 기본으로 채택하고 있고 문자데이터 뿐 아니라 음성, 영상 등의 멀티미디어 서비스와 전자우편, 인터넷을 통한 전자상거래가 추진되는 등 공간을 초월한 다양한 서비스가 빠르고 정확하며 쉽게 사용할 수 있게 됨에 따라 네트워크의 접속에 따른 트래픽이 급격히 증가하고 있다.[1]

그러나 디지털 정보의 교환을 위해 멀티미디어 데이터가 네트워크 상에서 이동할 때 사용자와 정보, 그리고 시스템 자원들이 외부에 노출됨에 따라 정보의 가로채기, 위조 변조 및 통신을 방해하는 공격으로 인하여 피해가 증가하는 등, 그 역기능 또한 심각한 상황에 이르고 있다.

이러한 문제를 해결하기 위한 대응 및 예방차원에서 여러 가지 알고리즘 및 보안기술을 이용한 정보보호 기술들이 활발히 개발되고 있으며 정보의 암호화가 그 해결방안으로 이용되고 있다.

관용적인 암호화방법이나 공개키 암호화방법의 특성과 성능은 차이가 있으나 두 방법 모두 암호화 키를 사용한다. 암호화 시스템에서 키의 크기는 알고리즘과 암호화 수준에 따라 가변 되고 키를 생성하는 과정에서 컴퓨터 시스템의 계산량 증가를 가져올 뿐 아니라 공개키를 요구하고 분배하는 과정과 사용될 키에 대한 인증의 요구는 부가적인 트래픽이 되어 전체적으로 네트워크의 성능을 저하시키는 요인으로 작용한다. 초고속 통신망의 구축이 대안 일 수 있으나 멀티미디어 등의 데이터 처리를 위한 대역의 제한은 병행되므로 망 전체에 미치는 영향은 비례하게 된다.

따라서 네트워크의 부하를 줄이면서 신뢰성 확보를 위한 키 관리가 절실히 요구되고 있으며 네트워크 암호화 알고리즘의 개선을 통한 방법과 키 관리 방법을 통해서 이와 같은 문제들을 해결하고 있다.

본문에서는 기존의 키 관리 시스템을 구분하여 각각의 문제점을 살펴보고 기존의 키 관리시스템과 호환성를 가지면서 키 관리 트래픽을 크게 감소시키고, 키의 분배와 동시에 인증의 문제를 해결하므로 네트워크의 성능을 개선할 수 있는 도메인 방식의 계층적 키 관리 시스템을 제안하였다.

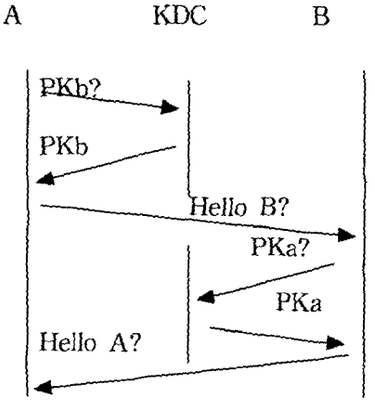
II 기존의 키 관리 시스템

비밀키 암호화 방식과 공개키 암호화 방식을 이용한 안전성 및 신뢰성의 확보는 암호화 키의 생성, 분배 및 관리에 크게 의존한다. 비밀키 방식은 필요한 키의 수는 적으나 비밀키를 네트워크를 통해 전달해야하므로 전송 중에 노출될 위험이 있고, 디지털 서명과 같은 서비스가 불가능하므로 특수한 분야를 제외하고는 현재 거의 사용되고 있지 않다. 이러한 비밀키 전송의 취약점을 보완한 공개키 방식은 암호화 과정에서 공개키를 사용하고, 복호화 과정의 비밀키를 사용하므로 비밀키가 노출되었다 해도 수학적으로 연관된 공개키를 무효화하여 보안문제를 해결할 수 있어 보안시스템의 기반구조 기술로 자리하고 있다.

현재 사용되고 있는 공개키 관리 시스템은 키가 저장된 공간의 위치에 따라 집중형 키 관리 시스템(CKMS, Centralized Key Management System)과 분산형 키 관리 시스템(DKMS, Distributed Key Management System)으로 구분할 수 있다.

1) 집중형 키 관리 시스템(CKMS)

네트워크의 특정 노드(node), 또는 키 서버(key server)가 키 분배 센터(KDC, Key Distribution Center)가 되어 네트워크에 등록된 모든 사용자의 공개키를 관리하는 시스템으로 송신자(A)가 상대방



<그림1> 집중형 키 관리 시스템

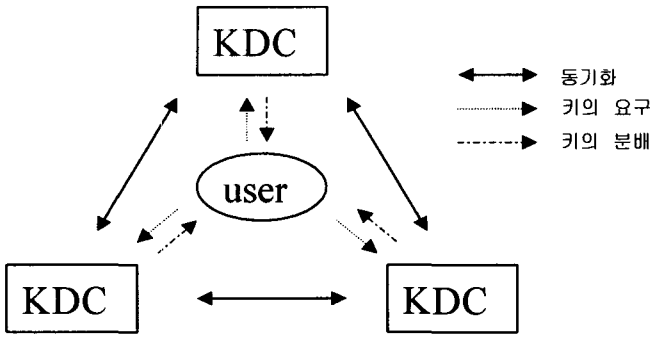
(B)의 공개키 PK_b를 획득한 후, 암호화하여 데이터를 전송하면 B는 자신의 비밀키 SK_b로 이를 복호화
하는 방식이다. KDC는 모든 사용자의 키 요구에 대한 수신자가 되며 사용자가 네트워크에 액세스 할 때마다 상대방의 키를 요구하므로 네트워크 트래픽이 키 서버에 집중되고 이에 따라 병목현상이 발생할 수 있다.

소규모 네트워크에서 하나의 키 서버로 모든 사용자 키를 관리할 수 있는 장점이 있으나 상대적으로 키 데이터의 파괴, 또는 공격 대상이 단일화되는 약점을 가지게 된다. 더구나 KDC의 관리자에 대한 신뢰성 여부가 네트워크의 신뢰성과 보안구조 전체에 큰 영향을 끼치게 되므로 일반적으로는 공신력이 있는 국가 기관이나 인증된 기관에서 관리하는 시스템 방식이다. <그림1>은 키의 집중관리 시스템에서 KDC를 통하여 정보를 교환하는 절차이다.

2) 분산형 키 관리 시스템(DKMS)

분산형 키 관리 시스템은 보다 큰 네트워크에서 복수의 KDC를 갖는 시스템으로 한 KDC는 다른 KDC의 공개키 디렉토리로부터 복사 본을 작성한 후 이를 관리하게 된다. 그리고 이들 KDC는 상호간 통신을 위한 동기를 유지하면서 사용자의 요구에 따라 키를

분배하게 된다. <그림2>는 분산형 키 관리 시스템에서의 발생하는 상호동작을 보여준다.



<그림2> 분산형 키 관리 시스템

그러나 동기를 유지하는 키 관리 시스템은 네트워크 트래픽이 증가할수록 복잡도가 지수적으로 증가하게 되어 네트워크의 관리 자체가 어렵게 될 가능성이 있고 복사된 키를 사용하므로 키의 적법성을 확인하기가 힘들어 진다. 즉 키의 인증을 검사하지 않으므로 신뢰성에 문제가 있을 수 있다. 다른 분산형 키 관리 방법은 KDC를 사용하지 않고 필요시에만 키 사용자가 키를 직접 요구하는 세션을 형성한 후 키를 교환하는 방법[2]이 있으나 획득된 키가 정당한지를 사용자가 검사할 수 없으므로 신뢰성 문제는 여전히 남게 된다.

III 계층적 키 관리 시스템의 제안

앞에서 살펴본 바와 같이 공개키의 관리 방법에는 집중형 키 관리 시스템과 분산형 키 관리 시스템이 있으나 네트워크 트래픽에 미치는 영향이 크고 키의 전송 중에 발생하는 키의 인증, 키의 무결성, 그리고 키의 유효성 등에 대한 문제 때문에 사용자가 요구하는 보안 수준에는 제한적일 수밖에 없다.

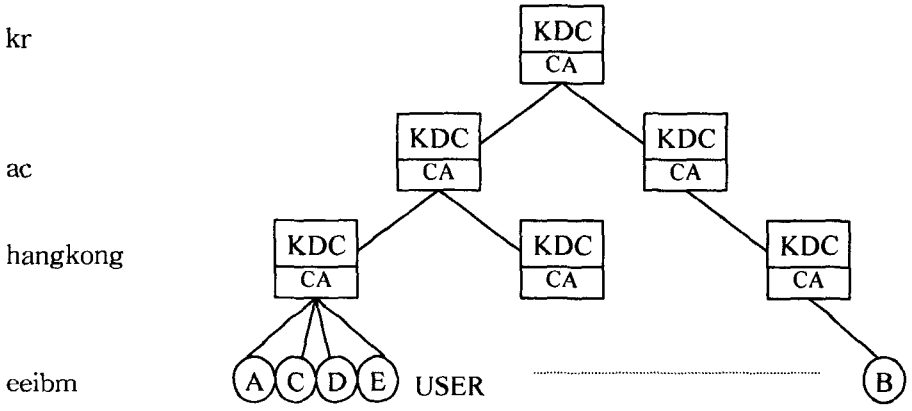
지속적으로 인터넷의 확장이 이루어지고 전자상거래가 활성화되고 있으며 멀티미디어 데이터의 교환이 일상화되면서 보다 쉽고, 빠르며, 높은 안전성이 요구되고 있다. 전체 네트워크에 큰 트래픽을 발생하지 않으면서 네트워크의 신뢰성을 향상시킬 수 있는 인터넷 도메인 방식의 계층적 키 관리 시스템을 제안한다.

1. 구성

이 시스템은 키 서버 또는 KDC가 독립적으로 운영되면서 사용자의 공개키를 인증해 주는 키의 인증기관(CA, Certification Authority)의 기능을 가지며 <그림3>과 같이 인터넷의 IP(Internet Protocol) 주소에 준한 도메인(Domain)형식을 갖는다. 도메인 이름이

eeibm.hangkong.ac.kr 인 경우 최상위 KDC는 kr, 그 하위의 KDC들 중 하나가 ac, 같은 방법으로 hangkong이라는 이름의 KDC와 사용자 시스템은 eeibm의 이름을 갖는다.

이와 같이 네트워크에 분산되어 있는 도메인 서버를 이용하여 계층적으로 KDC를 구성하면 대규모의 네트워크에서도 적은 레벨의 수로 계층화가 이루어지며 분산 시스템에서 요구되는 동기화를 취하지 않아도 된다. 따라서 키의 변경 시에도 update는 상위 KDC에서만 신속하게 이루어 질 수 있으므로 키 관리가 능동적으로 이루어 질 수 있다. 공개키 제반의 문제점은 KDC 내에 CA를 설치하고 인증서(certificate)를 발행함으로서 해결할 수 있다.



<그림3> 도메인 형식의 계층적 키 관리 시스템

2. 인증서의 발행

인증서는 CA가 공개키와 함께 사용자의 이름(ID, Identification)을 CA의 비밀키로 서명하여 발행하며 공개키를 얻을 때 CA의 공개키로 확인한다. 네트워크 내에서 각각의 객체인 사용자의 이름은 X.500 프로토콜의 명명방식에 준 한다. X.509에 준한 인증서의 생성 과정은 다음과 같다.[6]

1) 사용자 A는 자신의 공개키 PKa 와 자신의 사용자 이름 IDa를 CA에게 전송한다.
2) CA는 A의 공개 키 정보를 검사한 후 의 KDC의 정보를 부가하고 A의 공개키 정보에 서명한다.
   인증서의 형식은 <표1>과 같다.
3) CA는 A의 공개키 인증서 CERTa를 A에게 전송한다.
4) A는 CA의 공개키 PKca를 사용하여 인증서의 정확성을 검사한다.
5) A의 공개키는 인증서로서 분배되고 CA의 공개키를 액세스 할 수 있는 모든 사용자에 의해 이용 가능하게 된다.

CERTa={SN, AL, IDca, IDa, PKa, Ta, Dca(h(SN, AL, IDca, IDa, PKa, Ta))}	
SN : 인증서 일련 번호	PKa : 사용자 A의 공개키
AL : 서명에 이용한 알고리즘	Ta : 인증서 유효기간
IDca : CA의 이름	Dca( ) : CA의 디지털 서명
IDa : 사용자 A의 이름	h( ) : 일방향 해쉬 함수

<표1> 인증서의 형식

이와 같은 공개키 인증 시스템에서 CA가 A를 위한 비대칭 키의 쌍을 키 생성기(Key Generator)에게 의존한다면 A의 공개키와 비밀키가 키 생성키로부터 A에게 전송되므로 외부에 노출될 수 있다. 이 경우 전송과정의 안전성은 절대적으로 보장되어야 한다.

3. 기능

각 계층의 KDC는 모두 CA를 가지며 네트워크의 무결성과 키를 유지, 관리한다. CA의 기능을 요약하면 다음과 같다.

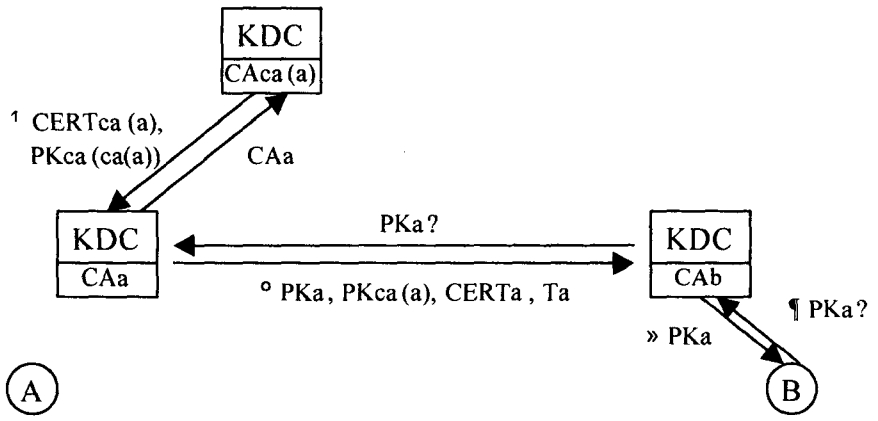
1) 사용자의 공개키 인증서를 발행하고 필요에 따라 취소한다.
2) 사용자에게 자신의 공개키와 상위 기관의 공개키를 전달한다
3) 등록기관의 요청에 의해 인증서를 발행하고 되돌린다.
4) 상호 인증서를 발행한다
5) 인증서와 그 소유자 정보를 관리하는 데이터베이스를 관리한다.
6) 인증서, 인증서 취소목록, 감사 파일을 보관한다.

CA는 자신의 키를 상위 계층에 있는 KDC의 디렉토리에 발행 즉시 등록하는데 이미 발행된 키라면 KDC 내의 CA에 의해 인증되며 이 경우 공개키는 사용자에게 보여지지 않는다. 키가 요구되는 경우는 사용자 A가 상대 원격 시스템의 하부 구조에 있는 한 사용자 B와 데이터 전송을 위해 공개키가 필요한 경우이며 각자의 공개키를 전송하기 위한 링크가 KDC간 형성된다. 이때 A는 B의 KDC에 대하여 A의 키를 보내고 키의 유효기간인 Timestamp를 설정하는 A의 KDC와 링크가 설정된다. 이 과정을 요약하면 다음과 같으며 <그림4>와 같이 나타낼 수 있다.

1) B는 B의 KDC에 대해 A의 공개키 PKa를 요청한다.
2) B의 KDC는 A의 KDC에 대해 A의 공개키 PKa를 요청한다.

3) B의 요청을 수락한 A의 KDC는 B의 KDC에게 다음을 전송한다. (각 KDC간 링크구성)
   : PKa, PKa의 CERTa, CA(A의 상위 KDC의 CA)의 공개키 PKca, 유효기간 (Timestamp)
4) B의 KDC는 B에게 A의 공개키 PKa를 전송한다.
5) A의 공개키 PKa를 받은 B는 이를 이용하여 메시지를 암호화하고 A에게 전송한다.

계층적 키 관리 시스템은 기존의 단순 KDC에 의한 키 분배와 공개키 암호에 의한 키 분배의 약점을 해결하기 위한 방안으로 각각의 특성을 혼합한 형태이다. 이와 같은 키 관리 시스템에서는 각각의 KDC가 CA를 운영해야 하며 그 CA는 전적으로 신뢰할 수 있어야 한다. 신뢰할 수 없는 CA는 KDC 내의 사용자들에게 부정한 키를 보낼 수 있으며 이를 방지하기 위해서는 각각의 사용자는 자신이 속한 KDC를 인증할 수 있는 공개키(PKca)가 필요하며 상대방 사용자가 속한 KDC의 공개키에 대한 인증도 요구된다. KDC 내의 CA를 신뢰할 수 있다면 사용자가 KCD에 직접 접근하는 것을 막을 수 있고 인증에 대한 검사가 필요 없으므로 네트워크 트래픽을 감소시킬 수 있다.



<그림4> 계층적 키 관리 시스템의 키 분배와 인증구조

IV. 결론

인터넷과 같은 대규모 네트워크에서 요구되는 보안문제를 해결할 수 있으며 키의 요구, 분배, 인증에 따른 네트워크의 트래픽을 크게 감소시킬 수 있는 도메인 개념의 계층적 키 관리 시스템을 제안하였다. 기존의 키 분배 및 인증 시스템과 비교하여 네트워크 객체들 간 상호작용의 고립을 피할 수 있으며, 신뢰할 수 있는 CA를 KDC내에 설계하여

인증 경로의 탐색을 간단히 하고, 인증의 필요 과정을 줄여, 네트워크 트래픽을 감소시킬 수 있도록 하였다. 각각의 KDC는 상위 KDC를 통하여 다시 키의 분배와 인증을 실시하므로 지속적으로 확장되고 있는 인터넷의 계층적 구조에 유연하게 대응할 수 있으며 사용자들에게 투명하면서도 보다 강화된 인증 수준을 제공할 수 있다.

제안된 시스템은 전체 네트워크의 지역성 및 신뢰성에 따라 키 인증의 과정을 축소하여 네트워크 트래픽을 조정할 수 있으나 폭주하는 트래픽에 대응하기 위해서는 동일키에 대한 중복된 인증의 요구를 회피할 수 있는 방법의 개선이 필요하다. 또한 적절한 네트워크의 모델을 설정하고 트래픽의 감소를 정량적으로 해석하는 연구가 지속되어야할 것이다.

참고문헌

[1] Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim, Ritchey, William Steen,"Internet Security Professional Reference"New Riders Publishing,1996

[2] Chu-Hsing Lin,"Dynamic key management schemes for access control in a hierarchy" Computer Communications, V.20 N15, Dec., 1997

[3] Varadharajan V, Calvelli C,"Key Management for a secure LAN-SMDS Network", Computer Communications, V.19 N.9-10, Sept., 1996

[4] Michael Gehrke, Thomas Hetschold, "Management of public key certification infrastructre - Experiences from the DeTeBerkom project BMSec", Computer Network & ISDN Systems, V.28 N.14 Nov.,1996

[5] Thomas Hardjono, Tetsuya Chikaraishi, Tadashi Ohta,"An Approach to Key Management and inter-Domain Authentication in the Telecommunications Management Network", IEEE Proceedings of the Globecom'93-Volume1, Nov., 1993

[6] ISO/CCITT, ISO9594-8/X.509. The Directory Authentication Framework, December 1993.