IPSec에서 키 복구 기술을 적용한 효율적인 연결 관리 메커니즘

김 정 범[†] · 이 윤 정[†] · 박 남 섭[†] · 김 태 윤[††]

요 약

최근 리눅스에 대한 사용이 빠른 속도로 증가하고 있다. 하지만 리눅스의 오픈 소스 정책에 따른 리눅스 보안의 필요성이 대두되어 리눅스 기반의 효과적인 암호 개발이 급속히 확산되고 있다. 하지만 암호는 본래 가지고 있는 키 관리의 어려움 때문에 여러 가지 문제가 발생할 수 있다. 이러한 암호의 사용이 야기하는 역기능을 해소하고 순기능을 지향하기 위해 키 복구에 대한 연구가 활발히 진행되고 있으며, 지금까지 많은 키 복구 기술들이 제시되어왔다. 본 논문에서는 IPSec(IP Security) protocol로 구현된 VPN(Virtual Private Network) 환경 하에서 종단간에 연결이 끊어졌을 경우 이에 따른 연결 재 설정에서의 시간적 소모를 줄이기 위한 방안으로 키 복구 기술을 이용한 메커니즘을 제안한다. 즉 제안한 KRFSH(Key Recovery Field Storage Header)라는 새로운 메커니즘은 VPN에서 SG와 호스트 사이의 터널 형성을 위한 세션 정보를 잃어버렸을 경우를 대비해서 세션 정보를 미리 저장해두고, 필요할 때 복구 할 수 있다. 이러한 메커니즘을 리눅스상의 IPSec 프로그램인 FreeS/WAN에 탑재함으로써, 위에서 언급한 VPN의 문제점을 해결한다.

Efficient Session Management mechanism applied Key Recovery technique in IPSec

Jeong-Beom Kim[†] · Yun-Jung Rhee[†] · Nam-Sup Park[†] · Tai-Yun Kim[††]

ABSTRACT

Recently the use of Linux OS is increasing to tremendous figures. But due to the fact that Linux is distributed on an open-source policy, the need of security is an upcoming question which leads to widespread development of security on a Linux based environment. Cryptography, however, can cause various problems because of difficulty of key management. A lot of researchers have been concentrating on the key recovery technique to eliminate the reverse effect of using these kinds of security and to promote positive aspects of using it. In this thesis I am suggesting an mechanism based on the key recovery technique, as a method to save time in recovery and resetting a disconnection between two end-users through IPSec (IP Security) protocols in a VPN (Virtual Private Network) environment. The main idea of the newly suggested mechanism, KRFSH (Key Recovery Field Storage Header), is to store the information of the session in advance for the case of losing the session information essential to establish a tunnel connection between a SG and a host in the VPN environment, and so if necessary to use the pre-stored information for recovery. This mechanism is loaded on the IPSec based FreeS/WAN program (Linux environment), and so the VPN problem mentioned above is resolved.

키워드 : IPSec, SG, Tunnel, Recovery, 키 복구

1. 서 론

전 세계의 컴퓨터들이 네트워크로 연결되면서 해킹이나 바이러스와 같은 침해 사고들이 빈번하게 발생하여 많은 피해가 발생하고 있다. 이에 따라 시스템의 안전에 대한 인식도 증가하여 시스템 환경에서 보안 기능을 추가하려는 노력도 증가하여 왔다. 이러한 시스템들 중 Linux가 무료로 보급되면서 리눅스의 취약성을 이용한 해킹 사례가 빈번하게 보고되고 있는 실정이다. 리눅스는 소스 코드의 공개와 관련 문서의 풍부한 제공으로 쉽게 수정이 가능하여 많은 사람들의 사용이 확산되고 있다. 이러한 리눅스 시스템을 가지고 사람들의 재택 근무가 활발해지고 기업 외부와도 네트워크 구성이 필요하게 되는 등의 기업 네트워크가 점차 확대되어 감에 따라 막대한 시설 투자가 필요하게 되었다. 네트워크의 확대와 함께 네트워크에 연결된 서로간에 안전한 통신을 하기 위해 사용해 오던 전용망에 투자해야 하는 비용과 그에

† 준 회 원 : 고려대학교 대학원 컴퓨터학과
†† 종신회원 : 고려대학교 컴퓨터학과 교수
논문접수 : 2001년 8월 17일, 심사완료 : 2001년 11월 16일

따른 운영과 관리가 커다란 문제가 되고 있다.

VPN(Virtual Private Network)[1]이란 이런 문제들의 해결을 위한 방안으로, 기업의 네트워크를 구성할 때 전용 임대회선을 사용하는 것이 아니라 공용망인 인터넷망을 이용하는 연결망이다. VPN은 터널링이라는 기법을 사용하여 일대일 연결과 같은 터널을 형성하며 데이터 패킷들은 터널을 통해 안전하게 전달된다. 이러한 터널링을 구현하는 기술로는 PPTP(Point to Point Tunneling Protocol), VTP (Virtual Tunneling Protocol), L2F(Layer 2 Forwarding Protocol), L2TP(Layer 2 Tunneling Protocol), IPSec(IP Security Protocol)[2] 등이 있다. 본 논문에서는 이러한 터널링 기법 중 IPSec으로 구현된 VPN의 환경을 기반으로 연구한다.

IETF(Internet Engineering Task Force)에 의해서 IP 계층 보안을 위한 개방 구조로 설계된 IPSec은 네트워크 계층의 보안에 대해서 안정적이고 영구적인 기초를 제공한다. IPSec은 오늘날의 암호화 알고리즘을 수용할 수 있을 뿐만 아니라 새로운 알고리즘을 수용할 수 있다.

이러한 암호의 사용은 정보의 누출 및 오용을 방지하고 상대의 신원 확인을 가능하게 함으로써 온라인 상에서의 전자상거래나 전자 계약을 가능하게 하는 등 많은 장점을 가지고 있다. 그러나 암호는 본래 가지고 있는 키 관리의 어려움 때문에 많은 문제가 발생할 수 있다. 이러한 점을 해결하기 위해 제시된 방안은 키 복구 기반 방식이다.

기존의 IPSec에서는 터널이 중단되었을 경우 다시 세션 키를 위해 재협상을 하여 터널을 복구해야 한다. 하지만 많은 호스트와 연결된 SG(Security Gateway)에서는 세션 복구를 해주는데 많은 시간이 소모된다. 이러한 문제를 해결하기 위한 방안으로는 SG에 키 복구 방식을 이용한 메커니즘을 기반으로, 세션 재연결시 저장된 키 복구를 이용하여 세션 키를 복구 해줌으로써 호스트와 SG 간에 재협상 과정을 생략하였다. 이러한 재협상에 따른 시간적 소모를 줄이므로 세션 복구에 따르는 전체 시간을 줄일 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 암호 키 기반 관리 구조와 IPSec 기반의 VPN 구조에 대해 분석한다. 3장에서는 키 복구 메커니즘을 제안하며 이를 기반으로 기존 IPSec 기반 VPN 구조에 대한 SG를 확장한다. 4장에서는 제안한 메커니즘의 성능을 분석한다. 5장에서는 결론 및 향후 연구 과제를 제시한다.

2. 관련 연구

2.1 암호 키 기반 관리 구조

암호 키 기반 관리 구조는 일반적으로 암호문의 소유자가 아닐지라도 사전에 약속된 어떤 특정한 조건하에서 허가된 사용자에게 복호를 가능하게 하는 시스템으로 정의할 수 있다. 암호 키 기반 관리 구조가 키의 분실이나 손실로 접근할 수 없는 경우와 국가가 범죄 수사 등의 적법한 이유로 키에 접근할 필요가 있을 경우, 암호가 오용됨으로써 발생할 수 있는 잠재적인 이유들을 방지하기 위하여 필요하다.

현재까지 제안된 암호 키 관리 방식은 크게 위탁 방식[3, 4]과 TTP(Trusted Third Party) 방식[5, 6], 캡슐화 방식[7, 8]으로 나눌 수 있다.

위탁방식은 암호문 복호화를 위한 키 또는 키의 조각들을 신뢰하는 기관에 위탁하고 필요시에 그 정보들을 얻어내어 키를 복구해내는 방식으로 유사시에 확실한 키 복구가 가능하다는 장점이 있다. 반면에 이 방식에서 위탁되는 키나 키 조각들은 사용자들의 비밀키와 관련된 것들이므로 사용자의 프라이버시 보호를 위해서는 위탁기관의 신뢰성이 절대적으로 보장되어야 하는 문제가 있다. 이를 위한 방안으로 비밀 분산 방식(Secret sharing scheme)[9]이 주로 사용되고 있다. 또한 사용자의 키가 복구되었을 경우 키의 사용기간을 제한하는 것과 위탁되는 정보가 유효한 것인가를 확인하는 것도 해결해야 할 문제이다.

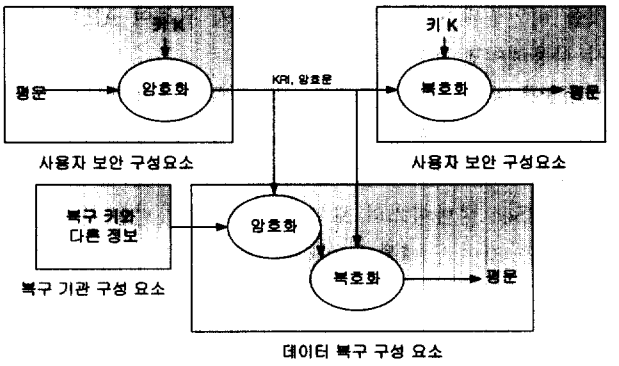
TTP 방식은 신뢰할 수 있는 제 3자인 TTP가 복구를 요청하는 사용자의 비밀키를 생성하고 사용자에게 분배하는 방식으로 실제적인 키 위탁은 일어나지 않으나 사용자가 오래 보존해야 하는 키를 TTP가 직접 보관하고 있으므로 위탁된다고도 할 수 있다. 이 방식에서 TTP는 사용자의 비밀키를 생성·분배하므로 신뢰성 보장이 절대적으로 중요하다. 이 방식의 장점은 TTP가 사용자들의 비밀키를 모두 가지고 있으므로 필요시에 TTP에 의한 키 복구가 확실히 보장되며 TTP 사이의 키 생성 방식을 통일하면 국가간 호환이 용이하다는 것이다. 반면에 많은 TTP가 필요하며 TTP와 사용자 그리고 TTP와 TTP 사이의 병목현상이 심하다는 단점이 있다.

캡슐화 방식은 생성되는 각각의 암호문에 대해 키 복구 정보를 생성하여 암호문과 함께 전송 또는 저장하는 방식으로 복구되는 키는 키 위탁 방식과는 달리 세션 키이다. 이 방식에서는 복구되는 키가 세션 키이므로 감청 기관의 복구능력을 제한할 수 있어 키 위탁 방식보다는 사용자의 프라이버시 보호에 유리하며 기존 프로토콜의 확장 필드를 이용하여 간단하게 사용할 수 있다는 이점이 있다. 그러나 키 복구에 필요한 정보를 사용자들이 생성하므로 조작이나 변조를 통해 키 복구 능력을 악용 할 수 있다는 문제가 있다.

(그림 1)은 캡슐화 방식의 키 복구를 사용하여 암호 통신을 하는 두 사용자 단말 장치 사이의 상호 작용을 나타내

고 있다.

이 방식에서는 먼저 목적키를 복구 가능하게 하기 위해서 사용자 단말 장치 내의 키 복구 정보 생성 기능은 목적키에 대응하는 키 복구 정보(KRI : Key Recovery Information)를 생성하여 캡슐화 한 후, 상대편 사용자 단말 장치로 암호문과 함께 전송한다.



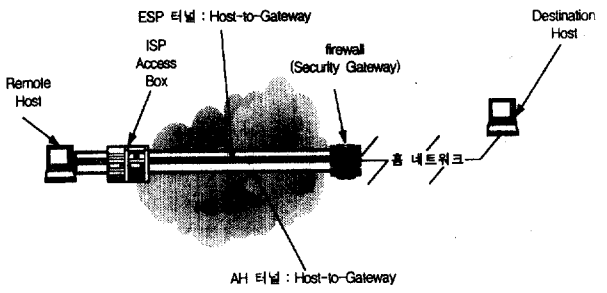
(그림 1) 키 복구 구조

본 논문에서 제안한 메커니즘은 이러한 암호 키 관리 방식 중 캡슐화 방식을 기반으로 제안한다.

2.2 IPSec 기반의 VPN 구조

통신 모델에서 IP 계층은 종단간의 보안을 제공 할 수 있는 가장 낮은 계층이다. 네트워크 계층 보안 프로토콜은 모든 상위층의 어플리케이션들을 수정하지 않고 IP 데이터그램을 통해서 운반되는 모든 상위층의 어플리케이션 데이터에 대해서 포괄적인 보안을 제공한다. 이러한 이유로 많은 VPN 장비는 IPSec으로 구현되어 있다.

본 논문에서는 원격 접근, 즉 Host-to-Gateway VPN 환경을 기반으로 한다. (그림 2)는 Host-to-Gateway VPN의 예이다.



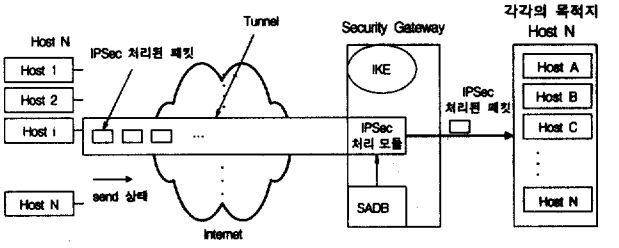
(그림 2) Host-to-Gateway VPN의 예

(그림 2)는 원격 호스트, 다이얼-업 링크, ISP(Internet Service Provider) 접근 Box, 인터넷, 방화벽 그리고 사설망에 있는 목적지 호스트를 포함한 공동의 원격 접근 설정을 설명하고 있다.

원격 사용자는 ISP가 요구하는 절차와 프로토콜을 사용해서 지역 ISP에게 연결 요청을 한다. ISP들은 원격 호스트들이 PPP(Peer-to-Peer Protocol)를 사용하고 계정 이름과 패스워드로 그 자신을 확인하는 것을 요구하여 호스트에 대한 인증 절차를 요구한 후, 동적으로 IP 주소를 할당받는다.

원격 호스트의 트래픽은 SG에서 인증, 복호화 되고 원격 호스트는 그들의 종단과 함께 요구된 SA 설정을 해야 한다. 동적으로 할당된 IP 주소는 미리 알 수 없기 때문에 방화벽 또는 원격 호스트들에게 패킷을 보낼 때 사용되는 목적지 호스트에 대한 SA를 미리 설정해 두는 것이 불가능하다. ISAKMP(Internet Security Association Key Management Protocol)는 이를 위해 SA를 만들기 위한 모든 암호화 키의 초기 생성, 그리고 이들 키들에 대해 계속적인 갱신을 하기 위한 표준화 된 방법을 제공한다.

이러한 Host-to-Gateway VPN은 세션 복구에 따른 시간이 너무 오래 걸린다는 문제가 있다. (그림 3)과 (그림 4)는 기존의 VPN의 세션 복구 문제점을 보여주고 있다. (그림 3)은 호스트가 안정된 네트워크 환경 속에서 IPSec 터널을 이용하여 보안 처리된 패킷을 순조롭게 보내는 것을 나타낸 것이다.

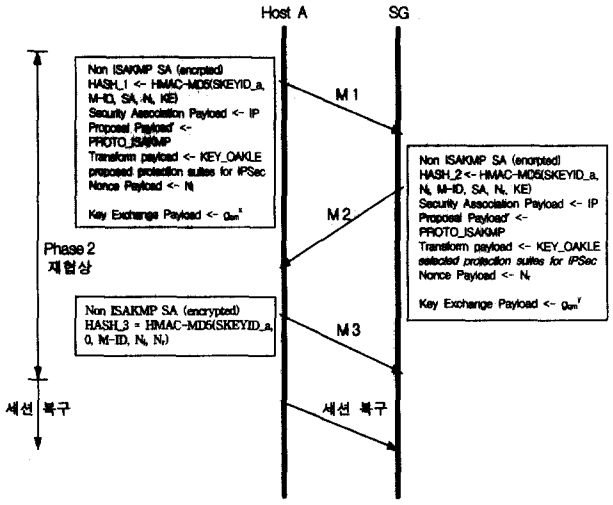


(그림 3) 기존의 IPSec으로 구현한 Host-to-Gateway VPN

이때 네트워크 상태의 불안정 등의 이유로 호스트와 SG 사이의 터널 연결은 모두 해체된 경우에 터널연결이 모두 중단된다. (그림 4)는 네트워크 상태가 원상태로 복구된 경우 재동작한 SG의 세션 처리를 나타낸다.

(그림 4)의 SG는 각 호스트에 대한 세션 정보가 순간 소실되었기 때문에 각 터널에 대한 정보를 알 수 없다. SG는 세션 정보를 모르는 호스트들에 대해서 다시 재접속을 요청하고 요청하기 이전에 키 협상 프로토콜인 ISAKMP의 Phase2 과정의 재시도를 통한 새로운 세션 정보를 서로 공유하게 된다

(그림 4)에서 보여주는 일련의 작업들은 여러 개의 호스트가 연결되어 있는 현 네트워크 상황에 적합하지 못하다. 이러한 문제점을 해결하기 위한 방안으로 본 논문에서는 키 복구 개념을 도입한 IPSec을 위한 새로운 SG를 제안한다.



(그림 4) 세션 재복구 시

3. 키 복구 메커니즘 기반의 SG 확장구조

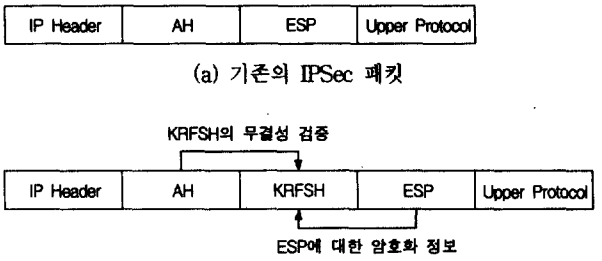
본 논문에서는 호스트가 SG에게 ESP에 대한 복호화하기 위한 키 복구 정보가 담긴 헤더를 추가하여 패킷을 보냄으로써 SG는 이 패킷의 무결성을 검증한 후 정당하면 SG내에 저장한다. 세션이 임의적으로 중단된 경우 SG내에 저장된 키 복구 정보를 이용하여 세션 복구를 하는 메커니즘을 제안한다. 이 과정으로 인해 메시지 3개로 구성된 키 협상 과정을 제외시킬 수 있어 시간적 소모를 줄일 수 있다.

3.1 제안된 메커니즘을 위한 프로토콜

2장에서 기술한 VPN에서의 SG 문제점을 해결하기 위한 해결책으로써 세션 정보를 저장해두었다가 세션 연결이 중단된 경우 세션 복구를 위해 세션 키를 재발급 받기 위해서 키 협상을 재시도하는 것이 아니라, 각 Host가 미리 자신의 세션 정보를 SG에 저장시켜두고서 만일의 사태에 저장된 키 정보를 이용하여 세션을 복구한다. 그렇게 함으로써 세션 복구에 걸리는 지연 시간을 줄이고자 한다. 이러한 메커니즘을 위해 Host의 세션 정보를 IP packet에 삽입하여 SG에게 전송하기 위한 방법으로 Key Recovery Alliance에서 제안한 단지 IPSec에서의 키 복구 메커니즘인 KRH(Key Recovery Header)[11]를 SG 확장 메커니즘에 맞게 형식을 변형하여 새로운 KRFSH(Key Recovery Field Storage Header)를 제안한다.

이러한 KRFSH는 키 복구 데이터를 IP 페이로드에 삽입하여 전송하므로 네트워크 하부조직의 변경을 요구하지 않는다. 즉 KRFSH를 사용하지 않는 시스템은 KRFSH를 무시한다. 이러한 KRFSH의 위치는 (그림 5)와 같이 End-to-End와 AH(Authentication Header)[12] 뒤, 그리고 ESP(Encapsulation Security Payload)[13]와 트랜스포트 헤더 전에 위치시킨다. 이러한 KRFSH는 키 복구를 수행하기 위해 덧붙여진 KRB(Key Recovery Block)[14, 15]를 네트워크를 통해서 전송하고, 수신할 수 있게 한다. 즉 KRFSH는 암호화되어진 부분인 ESP 부분에 대한 SA(Security Association)의 정보를 담고 있으므로 KRFSH는 ESP와 항상 함께 결합하여 사용하고 ESP 헤더를 포함하고 있지 않는 데이터그램에서는 전송할 수 없다. 이것을 비인증된 변형으로부터 보호하기 위하여 AH를 반드시 사용해야만 한다.

ESP를 위한 SA를 확립한 엔티티들은 KRFSH에 대한 SA 역시 확립해야만 한다. SA 확립이란 KRFSH가 모든 IPSec 패킷의 부분으로 덧붙여져서 전송되는 것이 아니라 IPSec 디바이스의 로컬 정책에 따라 전송 빈도수가 정해지는 것이기 때문에 이러한 정책에 대한 SA 확립을 말한다.



(a) 기존의 IPSec 패킷

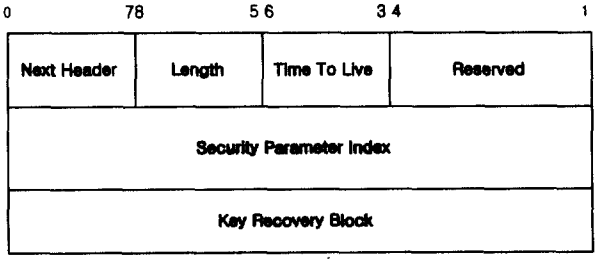
(b) 기존 IPSec 패킷 vs. 확장 패킷

(그림 5) 기존 IPSec 패킷 vs. 확장 패킷

제안한 헤더의 동작 원리는 다음과 같다.

- 송신자가 KRFSH를 포함하는 패킷을 보내기 위한 KRFSH의 인증 데이터를 산출하여 전송한다.
- 수신자는 인증 데이터를 받고 KRFSH의 인증 데이터를 검사한다.
- KRFSH를 받은 IPSec 엔티티는 KRFSH의 무결성을 검증하여 무결성에 오류가 있다면 타당한 KRFSH가 도착할 때까지 IPSec 패킷을 폐기한다.

(그림 6)은 KRFSH의 구조를 나타낸다.



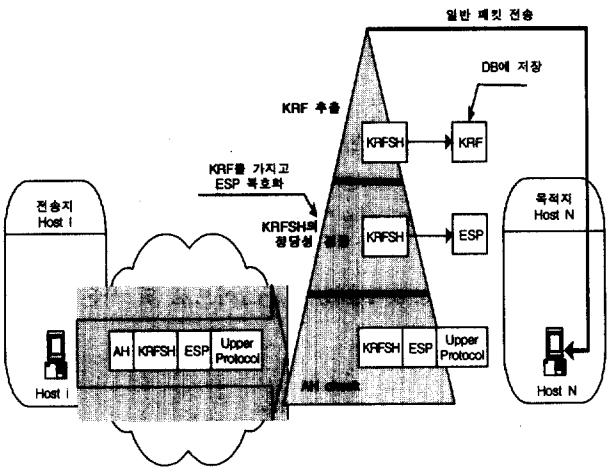
(그림 6) KRFSH의 구조

(그림 6)에서 Next Header 필드는 KRFSH 뒤에 오는 페이로드를 지칭하며 Length 필드는 32 비트 워드 단위인 Key Recovery Block 필드의 길이를 나타낸다. TTL(Time to live) 필드는 KRFS(KRF Storage) Database에 저장 만료 시간을 가리킨다. Reserved 필드는 차후에 쓰일 예약된 필드이고, SPI 부분은 이런 데이터그램을 SA에서 식별할 수 있는 32 비트의 의미-랜덤 값이다. 이 필드가 0인 경우에는 'KRFSH를 위한 SA가 존재하지 않는다'라는 것을 나타낸다. KRB 필드에는 KRF(Key Recovery Field)가 들어 있으며 KRB는 이 필드의 식별을 위한 블록이다. KRB 안에는 KRF가 삽입되어 있으며 이 KRF 안에는 수신자의 공개키와 세션 키를 대칭키 암호 알고리즘을 이용하여 만들어진 암호화 된 키가 들어있다.

3.2 제안한 SG 확장 메커니즘

KRFSH의 주요 목적은 이 헤더 내부에 키 복구 정보를 들여놓음으로써, 이 헤더를 삽입한 패킷이 호스트에서 SG로 전송되어질 때, SG에서는 이 정보를 저장해둠으로써 네트워크 상태의 불안정으로 인한 상황 속에서 세션이 끊어졌을 경우에 저장된 각 호스트에 대한 세션 정보를 해당 호스트에게 보냄으로써 일방적인 세션 복구가 이루어진다.

이러한 키 복구 기술을 탑재한 SG를 이용한 IPSec 터널링 VPN의 세션에 이상이 없을 시에 동작원리는 (그림 8)과 같다.

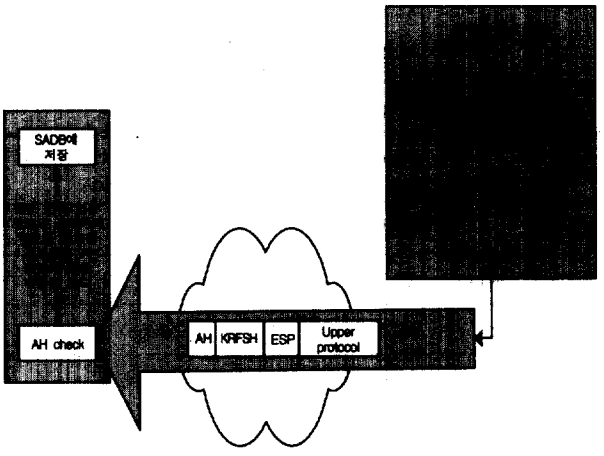


(그림 7) 제안한 SG 확장 메커니즘

(그림 8)에서 호스트가 KRFSH를 보내는 IP 패킷에 첨가해서 보내게 되면 TTL이 만료될 때까지 KRFSH 속의 KRB 안에 있는 KRF를 소스 주소와 함께 저장 해 놓는다.

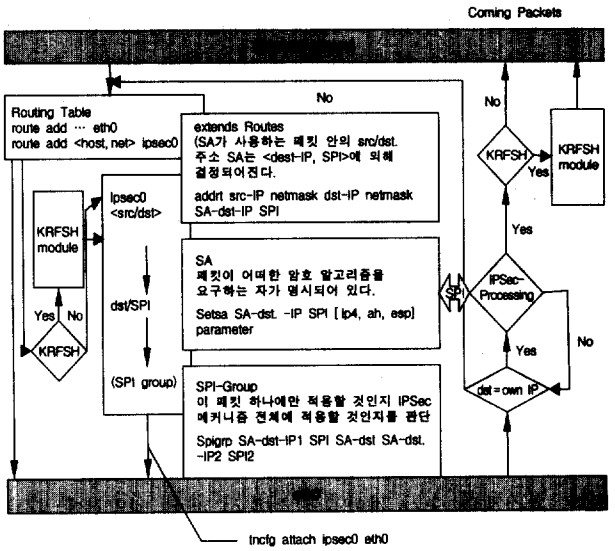
SG와 연결이 해제된 경우가 발생했을 때 제안한 SG를 가진 IPSec 터널에서의 세션 재연결 절차는 (그림 9)와 같다.

(그림 9)는 보낸 패킷에 포함된 KRFS안에 있는 세션 정보를 바탕으로 각 호스트에 대한 세션을 복구 해 주는 것을 보여준다. 호스트는 TTL이 만료될 때까지 KRFSH 속의 세션 정보를 포함하는 KRF를 소스주소와 함께 임시 저장 해 놓는다. 사고가 일어났을 경우, 저장되어 있는 세션 정보를 가지고 각각의 호스트의 세션 정보에 맞게 AH + KRFSH + ESP 형식으로 전송하게 된다. 그러면 호스트에서는 KRFSH속에 있는 세션 정보에 맞게 연결을 다시 복구한다.



(그림 8) 제안한 세션 복구 처리 메커니즘

이렇게 함으로써 각 호스트와 SG 사이에서 세션 재복구를 위한 메시지 3개로 구성된 재협상 과정을 생략 할 수 있어서 전체적인 시간 지연의 문제도 해결할 수 있다. 이러한 SG 내에서의 키 복구 메커니즘을 탑재한 내부 구성도는 다음과 같다.



(그림 9) 제안한 메커니즘의 내부 구성도

4. 성능 평가 및 분석

4.1 성능 평가

본 논문에서 제안하는 사용자의 신뢰성 확보를 위한 키 복구 기반의 IPSec 방식은 Linux의 보안 방식인 FreeS/WAN 1.8[16] IPSec을 수정하여 구현하였으며, 실험 환경의 구성을 위해 SG와 원격 호스트로 구성하였다. 사용한 암호화 방식은 AH는 MD5, ESP는 DES-CBC 알고리즘을 사용하였다. 두 시스템의 사양은 <표 1>과 같다.

〈표 1〉 시스템 및 운영체제의 S/W 사양

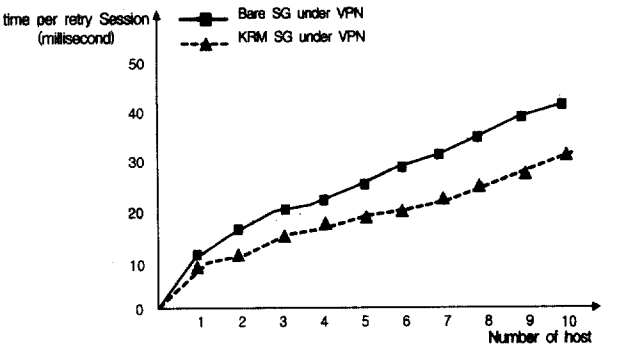
	Security Gateway	Host
CPU	Intel Pentium III 500Mhz	Intel Pentium III 500Mhz
RAM	128M	64M
Kernerl Version	2.2.12-20	2.2.5-15
AH	MD5	MD5
ESP	DES-CBC	DES-CBC

실험에 대한 세부 사항과 수행 시나리오는 다음과 같다.

- SG를 위한 키 복구 메커니즘은 재연결 속도 향상만을 기대한 실험이므로 수신측의 패킷 손실을 고려하지 않고 최소화하였다.
- SG 시스템이 서비스하는 호스트가 다수임을 가정하여 10개의 원격 접속 호스트가 SG 시스템에 접속하는 것으로 구성하였다.
- 제안한 메커니즘을 SG에 탑재하지 않은 경우 세션 복구 시간과 탑재했을 때의 세션 복구 시간을 측정하여 비교·분석한다

실험에 대한 (그림 10)의 그래프는 키 복구 없이 사용자의 수를 하나씩 증가시키고 SG의 강제적으로 재부팅 한 후 호스트와의 재연결 시간을 측정하여서 나타낸 그래프와 키 복구 기능이 있는 KRFSH 모듈을 SG에 탑재시 SG를 앞에서와 마찬가지로 재부팅하고 나서 호스트의 재연결 시간을 측정하여서 그래프로 나타낸 것이다.

(그림 10)의 그래프는 제안한 메커니즘을 탑재한 SG가 일반적인 SG보다 세션 관리의 성능 향상이 있음을 알 수 있다. 호스트의 수가 많아짐에 따라서 세션 재연결에 따른 제안 메커니즘을 탑재한 SG의 성능 향상이 약 27%로서 월등함을 알 수 있다. 또한 키 복구 방식 중 캡슐화 방식이므로 인증 데이터가 정당한 신뢰할 수 있는 제3자는 세션에 대해 복호가 가능하다. 그리고 복호가 가능한 것은 한 세션에 대해서이기 때문에 제3자, 즉 감청기관의 복구 능력을 제한할 수 있어 사용자의 프라이버시 보호에 유리함을 알 수 있다.



(그림 10) 세션 관리의 시간 비교 그래프

4.2 제안된 메커니즘의 성능 분석

먼저 호스트 A가 n개의 호스트와 연결되어 있다고 가정한다. Phase1 과정에서 소비되는 시간을 t_{p1}, Phase2 과정에서 소비되는 시간을 t_{p2}, 각각의 호스트의 시스템 내부의 프로세싱 시간을 t_{proc}라고 하고, 프레임 하나를 전송하는데 걸리는 시간을 t_{frame}, 각각의 호스트에서 i개의 데이터 프레임을 보내다가 세션이 중단되었을 경우 세션 복구 처리에 걸리는 총 시간 지연 T은 다음과 같다.

$$T = n \times \left(t_{p1} + 2t_{p2} + t_{proc} + \sum_{a=1}^{i} i t_{frame} \right)$$

$$= n \times \left(t_{p1} + 2t_{p2} + t_{proc} + \frac{a(a+1)}{2} t_{frame} \right)$$

여기서, $n>0$, $t_{p1}>0$, $t_{p2}>0$, $t_{proc} \ll 1$이므로 위 식은 아래의 식 (1)과 같다.

$$T = n \times \left(t_{p1} + 2t_{p2} + \frac{a(a+1)}{2} t_{frame} \right) \quad (1)$$

반면에 (그림 9)와 같은 VPN에서 걸리는 지연 시간은 세션에 대한 협상이 없으므로 총 지연시간 T'은

$$T' = n \times \left(t_{p1} + t_{p2} + a t_{frame} \right) \quad (2)$$

이다.

따라서 키 복구 기반이 있는 경우가 없는 경우보다 세션 재 연결에 따른 예측할 수 있는 총 시간 절약 Δ은 다음과 같다.

$$\therefore \Delta = T - T' = n \times \left(t_{p2} + \frac{a^2 + a - 1}{2} t_{comp} \right) \quad (3)$$

위의 식 (3) 에서와 같이, 정수배 만큼의 시간을 절약할 수 있다.

5. 결론 및 향후 연구과제

암호의 급속한 사용은 일상 생활에 있어서 많은 편리함을 제공하게 되었지만 범죄 집단에 의한 암호의 악용과 키의 분실 및 손상에 따른 암호문의 복호 불가와 같은 부작용 또한 크게 대두되고 있다. 이러한 암호의 부작용에 대한 여러 가지 대처 방안들 중에서 현재 세계 각국에서는 키 복구에 대한 연구가 활발히 진행되고 있다. 본 논문에서는 암호화 된 세션 연결이 끊어졌을 때의 문제에 대한 해결책으로서 SG를 위한 키 복구 메커니즘을 제안한다.

본 논문은 IPSec으로 설계된 Host-to-Gateway VPN에서 SG가 작동 불능 상태에서 재동작할 때 끊어진 세션에 대해 재협상을 하여 세션키를 얻는 데 따르는 시간적 소모와 암호의 악용을 해결하기 위해서 여러 가지 키 복구 시스템 중에서 대표적인 캡슐화 방식인 KRFSH를 제안하여 세션 정보를 저장함으로써 SG의 재동작에 의한 세션 복구를 재협상이 없이 복구 가능하도록 하였으며, 이에 따른 시간적 소모도 해결하여 좀 더 효율적임을 보였다.

향후 연구 과제로는 무선에서 사용자의 세션 키를 안전하게 복구할 수 있는 키 복구 시스템과 이러한 키 복구 시스템을 이용한 VPN 설계이다.

참 고 문 헌

[1] Dave Kosiur, "Building and Managing Virtual Private Networks?," John Wiley & Sons, 1998.

[2] Atkinson, R., "Security Architecture for the Internet Protocol," RFC 2401, NRL, November, 1998.

[3] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," the 2nd ACM Conference on computer and Communications Security, pp.59-67, 1994.

[4] Yair Frankel and Moti Yung, "Escrow Encryption System Visited : Attacks. Analysis and Designs," Crypto'95. Springer-Verlag. Lecture Notes in Computer Science. LNCS 963. pp.223-235, 1995.

[5] Ross Anderson and Micheal Roe, "The GCHQ Protocol and its Problems," Eurocrypt'97. Springer-Verlag, Lecture Notes in Computer Science, LNCS 1233, pp.134-148, 1997.

[6] Adi Shamir, "Partial key escrow : A new approach to software key escrow," Key Escrow conference, 1995.

[7] S. J. Kim, I. S. Lee, M. Mambo and S. J. Park, "On the Difficulty of Key Recovery System," Proc. of ISW'99 Information Security Workshop. Springer-Verlag, 1999.

[8] Brigit Pfizmann and Micheal Waidner, "How to Break Fraud Detectable Key Recovery," ACM Operating Systems Review 32, 1998.

[9] Adi Shamir, "Partial key escrow : A new approach to software key escrow," Key escrow conference, 1995.

[10] D. Maughan, M. Schertler, M. Schneider, J. Tunner, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, NRL, November, 1998.

[11] Tom Markham, Charles Williams. Key Recovery Header for IPSec, Computer & Security, Vol.19, 2000.

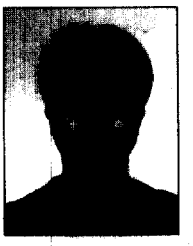
[12] Atkinson, R., "IP Authentication Header," RFC 2402, NRL, November, 1998.

[13] Atkinson, R., "IP Encapsulation Security Payload," RFC 2406, NRL, November, 1998.

[14] Sabari Gupta, A Common Key Recovery Block Format : promoting Interoperability between dissimilar key recovery schemes, KRA white-paper, 1998.

[15] Michael J.Markowitz and roge S.Schlafly, Key Recovery in SecretAgent Digital Signiture draft 5, June, 1997.

[16] FreeS/WAN, http : //www.freeswan.org/freeswan_trees/freeswan-1.8/doc/index.html.



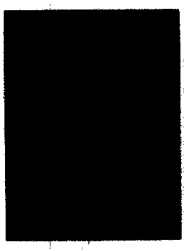
김 정 범

e-mail : qston@netlab.korea.ac.kr

2000년 고려대학교 정보공학과 학사.

2000년~현재 고려대학교 컴퓨터학과 석사과정 재학

관심분야 : IPSec, Ad-hoc Network, Key Recovery



이 윤 정

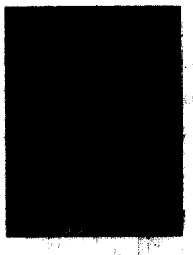
e-mail : genuine@netlab.korea.ac.kr

1993년 숙명여자대학교 전산학과 학사

1998년 숙명여자대학교 전산학과 석사

2000년~현재 고려대학교 컴퓨터학과 박사과정 재학

관심분야 : 컴퓨터 네트워크, 네트워크 보안, 이동통신 등



박 남 섭

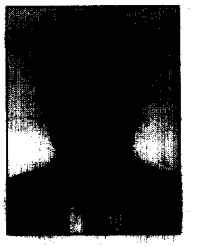
e-mail : nspark@korea.ac.kr

1998년 부산외국어대학교 컴퓨터공학과 학사

2000년 부산외국어대학교 컴퓨터공학과 석사

2000년~현재 고려대학교 컴퓨터학과 박사과정 재학

관심분야 : 네트워크 보안, 결함 허용 시스템, 네트워크 모니터링 등



김 태 윤

e-mail : tykim@netlab.korea.ac.kr

1981년 고려대학교 산업공학과 학사

1983년 미국 Wayne State University 전산과학과 석사

1987년 미국 Auburn University 전산과학과 박사

1988년~현재 고려대학교 컴퓨터학과 교수

관심분야 : 전자상거래, 컴퓨터 네트워크, EDI, 이동통신, 멀티미디어 등