다중 키 교환 알고리즘을 이용한 무선 보안 전송 기법

류동주* 김광현** 노봉남*

*전남대학교 정보보호협동과정

**광주대학교 정보통신학과

Wireless Security Transmission Using Algorithm of Multiple-Key Exchange

Dong-Ju, Ryu* Gwang-Hyun, Kim** Bong-Nam, Noh*

*Interdisciplinary Program of Information Security, Chonnam Univ.

**Dept. of Information & Communication, Gwangju Univ.

E-mail : ryu@gwangju.ac.kr

요 약

본 논문에서는 무선 네트워크 환경의 모바일 노드에서 전송되는 데이터의 기밀성 보장 및 안전한 전송을 위한 무선 기반의 네트워크 시험환경을 구축하고, 모바일 환경 중 IPv6에 기본으로 내장되어 있는IPSec을 이용한 효율적인 보안전송을 위한 IKEv2의 다중 키 교환 메카니즘에 관한 연구를 진행하였다.

무선망에서 모바일 노드의 핸드오프 패킷 전송 과정에서 끊김과 빈번하게 발생하는 키에 대한 재설정 및 재교환 문제를 해결하기 위해 하나의 단말에 여러 개의 키를 가지고 이동하는 기술을 연구하였다. 실험을 위해 사용된 키 교환 프로토콜은 MIPv6에서 기본적으로 탑재하고 양단간의 신뢰성 있는 암호화키의 관리와 분배를 위해 사용되는 IKEv2 프로토콜을 사용하였다. 본 논문에서는 SSFNet(Scalable Simulation Framework Network Models)이라는 네트워크 보안 시뮬레이터를 이용하여 IKEv2의 보안전송의 키 교환 지연 값을 비교 분석하여 성능을 측정하고 그에 따른 문제점과 개선 방안에 대해 연구하였다.

ABSTRACT

Constructed network test environment of wireless base for confidentiality guarantee of data and safe transmission that is transmited at Mobile node of Wireless Network environment in this paper. And, progressed research about IKEv2's Multiple-Key Exchange mechanism for efficient security transmission that use IPSec that is built-in to basis to IPv6 of Mobile environment. Have several key to single terminal to solve that is seam at hand off packet transmission process of Mobile Node in Wireless Network and Re-setting for Key and Re-exchange problem that happen frequently and studied technology that move. Key exchange protocol that is used for an experiment loads basically in MIPv6 and used IKEv2 protocol that is used for management and distribution of reliable encryption key between both end. Using network simulator of SSFNet(Scalable Simulation Framework Network Models) in this paper Key exchange delay value of IKEv2's security transmission analyzing comparison Performance measure and studied about problem and improvement way accordingly.

키워드

MIPv6, IPSec, IKEv2, Multiple-key, SSFNet, Fast-HandOff

I. 서 론

MIPv6의 이동성 지원과 관련한 프로토콜 표준화 방안은 보안성에 초점을 맞추어 진행되어지고 있다. 특히, 이동노드의 인증과 송수신되는 메시지는 현재 해킹의 기술력에 의해 거의 보호받지 못하고 있는 실정이다. 이 위협조건으로는 시그널링 메시지의 공격인 DoS(Denial-of Service)가 있으며, 또 다른 위협으로 Man-inthe-Middle 과 Hijacking 등이 있다. 현재 사용 중인 인터넷의 가장 큰 약점들이 새로운 NG기술로 전환되면서 많은 제안들이 봇물처럼 쏟아지고 있는 실정이다[1]. 이중 IP 기반의 보안 기술과 Transport 기반의 보안 기술이 주를 이루고 있으며 AAA(Authentication, Authoriza-tion, and Accounting) 인증 부분 역시 활발하게 논의되어지고 있다[2].

본 논문에서는 현재 Mobike(Mobile IKEv2) Working Group에서 논의 중인 노드 간 IKEv2를 이용한 인증 키 교환 방식을 조사하고, 이를 이용하여 다양한 인터페이스를 가진 노드에 이동성 제공을 위한 멀티 키를 사용, 인증부분과 빠른 핸드오프의

기능을 확인하고 효과적인 보안기술을 접목하고자 한다.

II. MIPv6의 보안 기술 동향

1. bootstrapping 과 IPSec의 연계

현재 MIPv6에서 보안을 위한 제안으로 Mobile IPv6 bootstrapping이 있다. Mobile IPv6 기본 스펙에서 규정된 IPv6 이동성에 관련된 메커니즘을 향상시키는 것으로,. Mobile IPv6 프로토콜의 deployment 용이성을 높이기 위하여, 이동노드와 홈 에이전트 사이의 IPsec SA 를 이동노드가 새로운 링크에 접근하여 부팅 시에 동적으로 설정하는 것이다. 기존 Mobile IPv6 기본 스펙에서는 이동노드와 홈 에이전트 사이의 BU(Binding Update) 메시지를 보호하는 것을 필수기능으로 규정하고 있으며, 이를 위하여 매뉴얼 SA 설정을 필수 기능으로 규정하고 있다[1][2][4]. 또한, 이동노드와 홈 에이전트 사이에 발생할 수 있는 재연 공격을 방지하기 위하여 IKEv1을 사용하도록 권고하고 있다. 그러나 SA설정과 IKEv1에서는 이동노드의 홈 주소와 홈 에이전트의 주소가 정적으로 설정되었다는 것을 가정하고 있으며, 이러한 점은 홈 에이전트가 위치하고 있는 도메인의 네트워크 주소 변경 및 홈 에이전트의 부하분산을 위한 동적 홈 에이전트 발견 및 동적 홈 프리픽스 발견 등의 메커니즘을 제공하는데 문제점을 초래한다. 이를 해결하기 위해서 제안된 것이 동적 bootstrapping이며 현재 활발히 논의 중에 있다. IKEv2는 위 과정 중 SA를 맺는 과정에서의 동적인 부분을 담당할 수 있도록 설계되어져 있다. 또 다른 논의 대상은 이동 노드의 홈 주소, 홈 에이전트 주소, 이동 노드와 홈 에이전트 간 보안 연관 설정 시 bootstrapping 절차를 수행하기 위한 새로운 AAA 응용 프로토콜의 필요성에 관한 논의가 진행되고 있다. 이 AAA 프로토콜에 의한 boots-trapping 인증 방식으로 EAP 프로토콜을 이용하고, 인증 과정 중에 발생하는 키를 이용하여 새로운 공유 비밀 키를 유도하고 이동 노드와 홈 에이전트에 분배함으로써, 두 노드 간 IKE(Internet Key Exchange)를 통한 IPsec 보안 연관 설정에 이용하도록 하는 논의가 진행 중에 있다[1][2][5].

또, Mobile IPv6의 bootstrapping과 관련하여 해결해야 하는 문제점들과 고려되어야 하는 사항들을 정의했으며, AAA프로토콜을 이용한 인증 과정과 Mobile IPv6 bootstrapping 절차를 어떻게 접목 시킬 것인가에 관한 논의가 진행되고 있다[6][7].

이동 노드와 홈 AAA서버간은 기존의 Diameter EAP 응용을 이용하고, 홈 AAA서버와 홈 에이전트 간에 새로운 프로토콜을 정의하려는 움직임이 있지만[8], 방문 망에서의 홈 에이전트 할당을 고려하지 않은 문제점이 지적되었다[9][10]. 또한 Mobile IPv6 bootstrapping 및 인증을 위한 이동 노드와 로컬 망에서의 AAA 클라이언트 간 통신 프로토콜 ICMPv6 (Internet Control Message Protocol for IPv6)와 PANA가 거론되고 있다[11][12][13].

2. MIPv6 보안 사항

① MN과 HA 간의 보안 전송

MN과 HA는 반드시 ESP(Encapsulating Security Payload)를 트랜스포트 모드(Transport Mode)에서 지원하여야 하며, non-NULL payload 인증 알고리즘을 사용하여 데이터 소스의 인증, connectionless 무결성 그리고 선택사양인 anti-replay 방지 등을 제공할 수 있어야 한다[1][3].

② MN과 CN 간의 BU 시그널링 메시지 보안

모바일 단말(MN)과 통신하는 Correspondent Node(CN)로 보내지는 BU시그널링 메시지를 보호하기 위해서는 위에서 언급한 IPsec SA 메커니즘이나 인증 구조기반(authentication infrastructure)이 MN과 CN 간에 필요치는 않다. 그 대신 RR (Return Routability)이라 불리는 절차를 이용하여 적법한 모바일 단말이 CN에게 BU 메시지를 보내고 있다는 것을 확인만 하면 된다.

③ Mobile Prefix Discovery 관련 보안

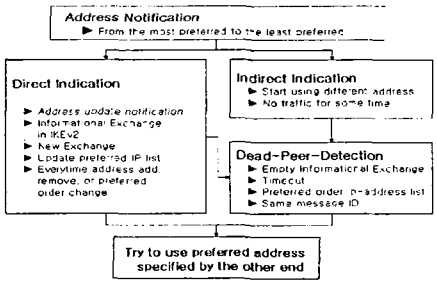
모바일 기기(MN)와 홈 에이전트(HA)는 IPsec 보안 제휴(Security Association) 메커니즘을 사용하여 이동 프리픽스(Mobile Prefix) solicitation과 advertisement의 시그널링 메시지를 보호하여야 한다. 또한 위에서 언급한 MN과 HA 간의 BU 시그널링 메시지 보안의 경우와 마찬가지로, 반드시 ESP (Encapsulating Security Payload)를 트랜스포트 모드(Transport Mode)에서 지원하여야 하며, non-NULL payload 인증 알고리즘을 사용하여 데이터 소스의 인증, connectionless 무결성(Integrity) 그리고 선택사양인 anti-replay 방지 등을 제공할 수 있어야한다[13][14].

3. IKEv2 프로토콜 기술 연구 동향

Mobike WG(Mobile IKE Working Group)은 한 호스트가 다수의 IP를 소유하는 경우나 IPSec환경에서 로밍이나 단말의 이동성으로 인해 IP 주소의 변경이 발생하는 경우, 이를 지원하기 위한 IKEv2 프로토콜을 확장하기 위해 구성되었다. Mobike는 다음 두 가지 경우를 지원, IKEv2를 확장하기 위한 IETF 워킹그룹이다[11][13].

- 한 호스트당 multiple IP 주소가 존재
- IPSec환경에서 로밍이나 Mobility로 인한 IP 주소 변경 발생

현재 Mobike에서 연구 진행하는 것은 NAT를 사용가능하게 하기 위한 방안에 대해서 초점이 맞추어져 있으며 무선 네트워크 설계 시 제안되어진 기본 설계는 VPN이다. 따라서 해당 노드와 서버간의 통신은 터널링 개념에서 시작된다. [그림 1]은 Mobike에 대한 기본적 구조 디자인이다[9][11].

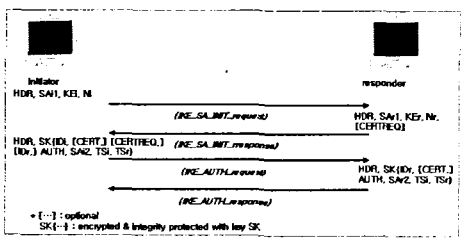


[그림 1] Mobike Design

4. IKEv2 프로토콜을 이용한 IPSec 동작원리

IKEv2 프로토콜은 기존의 IKEv1 프로토콜의 개념을 그대로 계승하면서 기능을 대폭 축약 설계한 것으로 기본 메시지 6개를 4개의 메시지 교환에 의해 통신쌍방의 인증된 보안 채널을 수립하였으며, 인증 방식도 4가지 방식에서 2가지(공개키, 사전공유 비밀키) 방식으로 줄였다. 또한 DoS(Denial of Service) 공격을 막기 위해 응답자로 하여금 쿠키로 응답하게 하여 합법적인 호스트에 대해서만 자원을 할당할 수 있게 한 키 관리 프로토콜이다[1][3].

IKEv2의 ID는 요청과 응답의 쌍으로 구성 되며 응답을 받지 못했을 때 요청 메시지는 재전송하거나 연결을 종료할 수 있다. 동작은 Initial Exchange 과정과 Subsequent Exchange 과정으로 이루어지며, 기본적으로 4개의 메시지 쌍으로 구성된다. Initial Exchange 과정은 IKE_SA_INIT와 IKE_AUTH으로 구성되는데, SA(Security Association) 설정이 끝나면, 상호 인증과 CHILD_ SA를 설정한다. [그림 2]는 Initial Exchange 설정 과정이다[8][9][11].

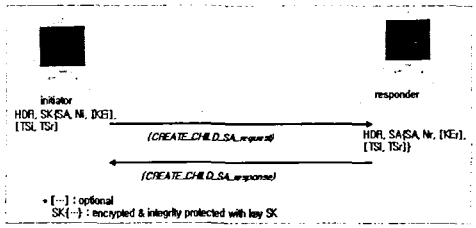


[그림 2] Initial Exchange 과정

[그림 3]은 Subsequent Exchange 과정을 표현한 것으로 IKEv1의 Phase 2에 해당하는 Subsequent Exchange는 2개의 메시지 쌍으로 구성되며, CREATH_CHILD_SA는 SA를 재설정할 때 사용된다. 이외에 Informational Exchange 과정은 프로토콜 수행 중에 발생한 오류 정보 및 이벤트 탄생 정보 등을 교환할 때 사용된다[8][9].

본 논문에서 사용된 키 교환 알고리즘은 다중 키이다. 이는 현재 Mobike에서 논의되기도 하지만 표준화되기 전까지 다양한 실험 환경을 구축하여 문제점을 사전 조사하여 실제 망에 구현 됐을 때를 대비하고자 한다.

따라서 실험환경에서 제시되는 기본적 알고리즘은 [그림 2]와 [그림 3]의 과정을 반복 수행하는 것이다.

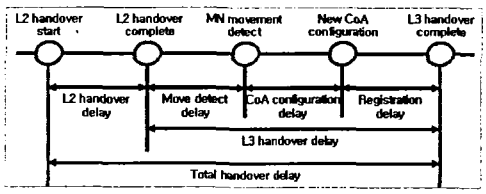


[그림 3] Subsequent Exchange 과정

III. 실 험 환 경

1. 고려 사항

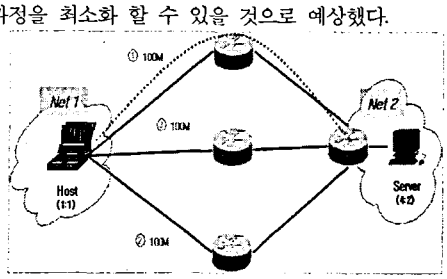
모바일 단말에서의 기본적 핸드오프에 대한 지연은 레이어2와 레이어3의 두 가지 형태에서 볼 수 있다. [그림 4]는 전체적 지연시간과의 관계를 보여주고 있다[15]. 본 논문에서는 멀티 키를 교환 했을 때의 지연시간을 측정하고 모바일 노드가 이를 수용하고 재 통신 하는데 걸리는 시간을 실험해 보았다.



[그림 4] MIPv6의 레이어별 지연

2. 실험 모델

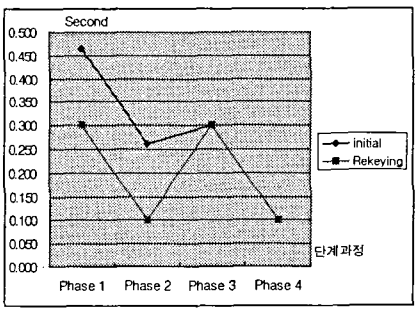
실험 환경을 위한 구성으로는 리눅스를 기반으로 구축되어져 있으며 자바를 이용한 시뮬레이션 네트워크인 SSFNET를 이용하였다. 또한 키의 측정치를 위하여 NIST(National Institute of Standards and Technology)의 NIIST(NIST IPSec and IKE Simulation Tool)를 이용하여 다중 키 관리와 교환에 대해 시뮬레이션 하였다[16][17]. 모바일 노드의 기본 전송은 100Mbps이고 하나의 SA를 가지는 것이 아닌 두 개 이상의 키를 사전 보유하게 설계하였다. 이렇게 수행하게 함으로써 핸드오프에서의 인증 과정을 최소화 할 수 있을 것으로 예상했다.



[그림 5]네트워크 실험환경 구성도

3. 실험 결과 및 분석

[그림 5]에서 실험 네트워크로 Net1의 모바일 노드가 Net2의 서버에 접속할 경우 기본 전송 단위는 IPSec 전송 초기 값 즉, SA 초기 설정 단계인 init 값을 전달하는 과정을 분석하였고, 두 번째 재전송 시 발생하는 재설정 키 즉, Re-Keying을 측정하였다. 마지막으로 평균값을 구하여 전체적인 지연 시간을 분석하여 보았다. 이를 위하여 각 노드 간 전송은 평균 20번 이상을 수행하여 결과를 살펴보았다. 각 경유 라우터의 번호가 있는데 1번 라우터가 단절 됐을 경우 라우터를 2번으로 교환하고, 다시 키를 생성해야만 계속적인 IPSec 전송이 가능하도록 설계하였다. [그림 6]에서 보면 처음 초기화 과정은 평균 20번 이상을 초기화 맺어질 때의 값인데 평균 값으로 약 0.46초이며 이를 재전송 즉 노드와 망 사이에서 재전송 하고 재설정 할 경우 약 0.3초의 평균값을 가졌다. 이를 보면 알 수 있듯이 재교환 값은 현재 가지고 있는 키의 값이 있으므로 빠르게 핸드오프를 할 수 있을 것으로 판단된다.



[그림 6] 실험 결과 분석표

IV. 결 론

본 논문에서는 IKEv2를 다중 키로 형성하여 통신하게 함으로써 핸드오프 시 발생하는 재전송과 재교환시 일어나는 시간적 차이를 극복하고자 하는 실험을 하였다. 실험 결과에서 보듯이 재설정 값이 초기화 보다 좀 더 빠른 것을 볼 수 있으며 이를 통해 상대적이기는 하지만 라우터의 단절은 핸드오프를 발생하는 과정으로 인식하고 재설정 및 키 재 생성을 하는 것을 보았다. 따라서 멀티플 인터페이스를 통해 교환해야 하는 이기종 레이어별 보안전송에 많은 활용이 가능할 것으로 보인다. 현재 수행중인 연구는 이를 좀 더 세부적인 핸드오프 과정과 보안 과정으로 분리하여 키 지연 시간과 이기종망간의 보안 전송 측정을 통하여 다양한 보안 전송 네트워크를 구현 할 예정이다.

참고문헌

[1] Arkko, et al. "Using IPsec to protect Mobile IPv6 signaling between mobile nodes and home agents,"RFC 3776

[2] A. Yegin, "AAA Mobile IPv6 Application Framework," INTERNET-DRAFT, draftyegin-mip6-aaa-fwk- 00.txt

[3] V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Archi tecture," draft-ietf-mip6-ikev2-ipsec-01.txt

[4] D.Johnson, C.Perkins, J.Arkko, "Mobility Support in IPv6", RFC3776

[5] A. Yegin, " Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP -based Network Access Authentication," [6]A. Yegin, "AAA Mobile IPv6 Application Framework," draft-yegin-mip6-aaafwk-01.txt

[7] H. Tschofenig and S. Thiruvengadam, "Bootstrapping Mobile IPv6 Using PANA" draft-tschofenig-mip6-boot strapping-pana-00.txt

[8] F. Dupont, "Address Management for IKE version2", draft-dupont-ikev2-addrmgmt-07.txt

[9] T. Kivinen, H. Tschofenig "Design of the MOBIKE Protocol", draft-ietf-mobike-design-03.txt

[10] AAA정보보호 기술 표준화 동향, 김현곤 외 6인 전자통신동향분석 제20권 제1호 2005년 2월

[11] Mobike WG, http://www.vpnc.org/

[12] Jee, J. Nah and K. Chung, "Diameter Mobile IPv6 Bootstrapping Application Using PANA,", draft-jee-mip6-bootstrap pana-00.txt

[13] 권혁찬외 2인, Mobile IPv6 표준화 및 기술동향 IITA, 주간기술동향, 2004.5

[14] 이병준, 이동성 지원을 위한 Mobile IPv6 관련 보안 이슈, TTA Journal No. 99

[15] 홍용근외 3인, Mobile IPv6에서 Fast Handover을 위한 IETF 기술동향, 전자통신동향분석 2005.

[16] NIIST, http://www.antd.nist.gov/niist

[17] SSFNet, http://www.ssfnet.org