HT-RR:CoTI와 직전 바인딩 정보를 이용한 바인딩 갱신 패킷의 인증 향상 기법

변경환*, 박민우**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 전기전자컴퓨터공학과
e-mail:momoida@skku.edu, mwpark@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

HT-RR:Procedure for Improving authentication by CoTI and Binding information

Kyung-Hwan Byun*, Min-Woo Park**, Tai-Myoung Chung*
*School of Information Communication Engineering, Sungkyunkwan University
**Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요 약

MIPv6(Mobile IPv6)는 이동노드(mobile node, MN)의 이동성(mobility)를 고려하여 만들어진 프로토콜로 이동노드와 상대노드(correspondent node, CN)간의 효율적인 통신을 위해 경로 최적화 기능을 제공하며, 이를 통해 두 노드가 홈 링크를 통하지 않고도 직접 통신할 수 있다. 이때 경로 최적화를 위해 바인딩 갱신(binding update)과정을 수행하며, MIPv6는 RR(return routability)를 통해 바인딩 갱신을 보호한다. 하지만 RR을 통한 바인딩 갱신은 거짓된 바인딩 갱신 공격에 취약하다. 본 논문에서는 RR과정의 취약점을 보완하는 HT-RR메커니즘을 제안한다.

1. 서론

기술의 발달로 인해 휴대용 장치의 기능이 보다 다양화되면서, 사용자들은 이동중에도 디바이스를 통해 다른 대상과 통신을 요구하게 되었다. 하지만 IP는 노드의 이동성을 고려하지 않고 설계된 프로토콜이므로, 노드의 주소가 동적으로 변할 경우 통신이 끊어져 모바일 노드에 적합하지 않다. MIPv6는 이러한 문제점을 보완하기 위해 등장하였다. MIPv6는 두 가지 방법을 통해 모바일 노드의 이동성을 지원한다. 첫 번째 방법은 양방향 터널(bidirectional tunneling)방식으로 MN과 CN간에 HA(Home Agent)를 거쳐 통신하게 된다. 두 번째 방법은 경로 최적화이다. 이 방법은 외부링크로 이동한 MN과 CN이 MN의 새로운 CoA(Care-of Address)를 통하여 직접 통신할 수 있도록 한다. 이를 위해 MN은 CN에게 새로운 CoA를 알리는 바인딩 갱신 과정을 수행해야 한다. 하지만 거짓된 바인딩 갱신 공격으로 서비스 거부(Dos, Denial-of-Service) 공격, 경로 변경(redirect) 공격, 이웃 폭격(neighbour bombing) 공격 등이 가능하다.

MIPv6는 바인딩 갱신 패킷을 암호화하기 위해 RR 과정을 사용하고 있다. 이 기법은 바인딩 갱신 패킷을 보호하기 위한 세션키를 얻기 위해 MN과 CN 사이에 메시지를 송수신한다. 하지만 RR과정은 세션키를 생성하기 위한 정보를 공개 채널을 통해 전달하는 문제점이 있다. 이로 인해 공격자가 HA와 CN사이의 링크에 존재하면 RR과정에서 사용되는 메시지의 정보를 가로채어 세션키를 생성할 수 있으며, 위조된 바인딩 갱신 패킷을 통해 서비스 거부 공격, 경로 변경 공격 등이 가능하다.

이런 문제점을 해결하기 위해 다양한 방법([4],[5],[6],[7])이 제시 되는데, 이 들은 모두 추가적인 IPsec이나 공개키를 사용한다. 하지만, IPsec이 장기간 연결 관계가 형성되는 MN과 HA 사이에서는 효율적일 수 있으나 단기간 연결 관계가 형성될 수 있는 MN과 CN간의 경우에는 비효율적일 수 있다. 또한 IPsec의 내부 키 교환 프로토콜인 IKE를 수행하는데 드는 연산량이 많기 때문에 저전력이며 한정된 계산량을 가진 통신 노드일 경우에는 자원 소모가 크다.

본 논문에서는 RR 과정중에서 가장 취약점인 HA와 CN 사이의 통신 경로 사이에 공격자가 존재하더라도 세션키 생성을 위한 정보를 얻을 수 없게 하여 바인딩 갱신 패킷의 무결성을 향상하는 HT-RR(Hidden Token Return Routability)방안을 제안한다. 본 논문에서 제안하는 바인딩 갱신 프로토콜은 IPsec이나 공개키 연산을 사용하지 않으며 기존의 RR과정에서 추가연산도 적기 때문에 CN이 저전력이며 한정된 계산량을 가진 통신 노드라 하더라도 자원소모가 적다.

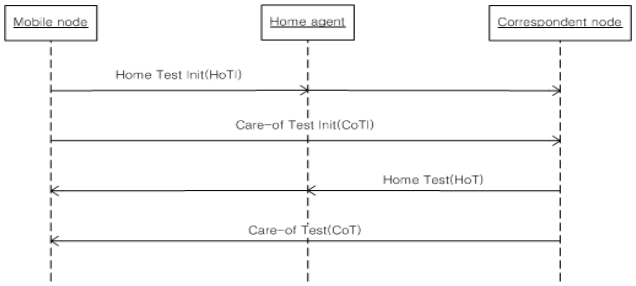
본 논문의 구성은 다음과 같다. 2장에서는 기존 바인딩 갱신 프로토콜에 대해서 살펴본다. 3장에서는 제안하는 프로토콜에 대해 자세히 기술하고, 4장에서는 제안하는 프로토콜의 안전성과 효율성을 살펴본다. 5장에서는 결론과 향후 연구방향을 제시한다.

2. 관련연구

이 장에서는 바인딩 갱신 프로토콜 중 표준으로 채택하고 있는 RR 과정과 보안상 문제점에 대해 구체적으로 살펴본다.

2.1 RR 과정

RR 기법은 MN이 CN에게 바인딩 갱신을 요청할 때 사용하도록 제안된 과정(procedure)이다. 이 기법은 CN이 MN의 바인딩 갱신 요청을 승인해주기 전에 이동노드의 HoA(Home Address)와 CoA를 사용하여 메시지를 수신할 수 있는지 확인할 수 있도록 해준다. 이 과정에서 MN과 CN 사이에 네 개의 패킷이 교환되는데 그 과정은 (그림 1)과 같다.



(그림 1) MN과 CN간의 패킷 교환 과정

MN은 CN에게 HoTI와 CoTI 패킷을 동시에 보내게 된다. HoTI는 소스 주소로 HoA를 사용하며 ESP 터널링 모드를 사용하여 HA를 거쳐 CN에 전달된다. 반면에 CoTI는 소스 주소로 CoA를 사용하며 HA를 거치지 않고 CN에게 전달된다. 그리고 HoTI에는 홈 이닛 쿠키(Home init Cookie,Cookie1)과 CoTI에는 케어 오브 이닛 쿠키(Care-of init Cookie,Cookie2)을 포함하고 있다. 이는 대응되는 회신 메시지를 식별하기 위해 사용된다. 이 두 메시지를 수신한 CN은 비밀키(Kcn)를 이용하여 HoT와 CoT에 포함할 토큰 홈 키젠 토큰(home keygen token, token1)과 케어 오브 키젠 토큰(Care-of keygen token, token2)을 생성한다. 그 과정은 (식 1)과 같다

token1 := HMAC(Kcn, HoA | nonce | 0) (식 1)

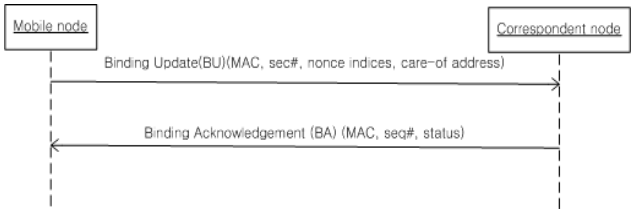
token2 := HMAC(Kcn, CoA | nonce | 1)

각각의 토큰은 HoTI와 CoTI의 응답 메시지 HoT와 CoT 메시지에 실어 송신한다. HoT와 CoT를 수신한 MN은 (식 2)와 같이 세션키(Kbm)를 생성한다.

K = SHA1(token1 | token2) (식 2)

2.2 바인딩 갱신 과정

RR과정 후에는 생성된 세션키를 이용하여 바인딩 갱신을 수행하며 그 과정은 (그림 2)와 같다.



(그림 2) MN과 CN간의 바인딩 갱신 과정

<표 1> 바인딩 갱신 패킷의 내용

Source Address = Care-of address
Destination Address = correspondent address
Parameters: Home address sequence number home nonce index Care-of nonce index binding authorization Data option

<표 1>은 바인딩 갱신 패킷의 내용을 나타낸다. 바인딩 패킷에는 CN에서 세션키를 생성하기 위한 값인 Home address, sequence number, home nonce index, Care-of nonce index 등이 포함된다. 그런데 CN은 서비스 거부 공격을 예방하기 위하여 RR과정 중에 MN의 정보를 저장하지 않는다. RR과정 이후에 MN은 세션키를 할당 받지만, CN은 보다 늦은 바인딩 갱신 과정 중에 세션키를 생성한다. 이는 CN이 바인딩 갱신 패킷을 통해 세션키를 생성하기 때문이다. 이 때 CN은 HoT와 CoT의 연관성을 고려하지 않는다. 따라서 다른 두 노드의 HoT와 CoT를 통해서도 세션키는 생성할 수 있으며 CN은 이 세션키를 정당한 것으로 인지한다.

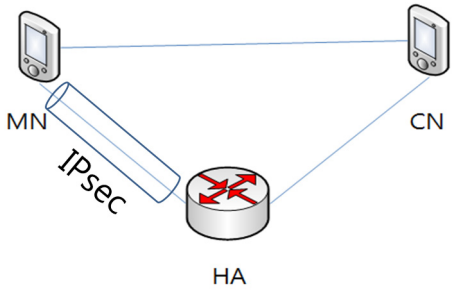
<표 2> CN이 바인딩 갱신 패킷을 수신시 확인사항

1	HoA의 Unicast 주소여부 확인
2	sequence number 확인
3	nonce indix mobility option 존재확인
4	binding authorization Data option 검증

바인딩 갱신 패킷을 수신한 CN은 <표 2>의 사항을 확인한다. 우선 HoA가 만약 유니캐스트 주소가 아니라면 해당 바인딩 갱신 패킷을 폐기한다. 두 번째로 순차번호(sequence number, seq#)의 정당성을 확인한다. 수신한 seq#이 직전에 수신한 값보다 크고 증가량이 32768보다 작아야 한다. 이를 만족하지 않으면 해당 바인딩 갱신 패킷 역시 폐기한다. 세 번째로 nonce indix mobility option의 존재여부를 확인한다. 네 번째로 binding authorization Data option을 검증한다. 이때 검증식은 (식 3)과 같으며, Kbm은 세션키, CoA는 care-of address, BU는 바인딩 갱신 패킷을 의미한다.

HMAC(Kbm, (CoA | correspondent | BU)) (식 3)

2.3 HA와 CN 사이의 채널에서의 공격



(그림 3) RR 과정에 이용되는 채널

RR 기법은 HA와 MN 사이의 채널은 IPsec 을 이용하여 보호하지만 MN과 CN사이의 채널과 HA와 CN사이의 채널은 보호하지 않는다. 그러므로 HoT와 CoT 메시지는 MN과 CN사이, HA와 CN사이의 공개채널에 노출되어 있다. 바인딩 과정은 세션키를 이용해 보호하는데 HoT가 노출될 경우 세션키를 조작할 수 있다. HA와 CN사이에 존재하여 HoT를 도청하는 공격자는 CN에게 CoTI메시지를 보내어 CoT값을 획득하고 이를 통해 조작된 세션키를 생성할 수 있다. 이때 세션키는 (식 4)와 같이 생성되며 CN은 이를 정당한 키로 받아들인다. 따라서 공격자는 조작된 세션키를 사용하여 거짓된 바인딩 갱신 공격을 할 수 있다.

$$K = SHA1(\ token1 \mid token2) \qquad (식\ 4)$$

CN은 <표 2>와 같이 검증을 수행하는데, 공격자에 의해 생성된 거짓된 바인딩 갱신 패킷은 seq#을 제외한 모든 값들이 만족한다. authorization Data option은 (식 3)과 같이 생성되며, 이 메시지는 세션키를 통해 인증이 이루어지는데 공격자는 조작된 세션키를 획득하였으므로 authorization Data option 역시 생성할 수 있다. seq#는 공격자가 예측 할 수 없지만 CN에서의 seq#검증은 잘못된 seq#의 사용을 검증하는 보안적인 기능이 아닌 과거의 바인딩 갱신 패킷을 배제하기 위한 기능으로 사용된다. 따라서 seq#는 직전에 사용된 seq#보다 크고 증가량이 32768보다 작기만 하면 되므로 seq# 역시 쉽게 통과할 수 있다. 따라서 공격자가 HoT만 획득하면 쉽게 거짓된 바인딩 갱신 패킷을 전송할 수 있다. 이를 통해 공격자는 기존의 MN과 CN의 통신을 끊을 수 있으며, 이를 활용하여 서비스 거부 공격을 감행 할 수 있다.

3. 본론

이 장에서는 바인딩 갱신 과정 중 HoT 내의 토큰값을 공개채널에서 직접적으로 노출시키지 않음으로써 HA와 CN간의 통신경로 사이에 악의적인 공격자가 존재하더라도 거짓된 바인딩 갱신 공격에 대해 안전한 HT-RR 프로토콜을 제안한다.

3.1 HT-RR 프로토콜

제안하는 HT-RR 과정은 두 가지 동작 과정으로 초기 HT-RR 과정과 차후 HT-RR 과정으로 나뉜다.

3.1.1 초기 HT-RR 과정

<표 3> 초기 HT-RR 과정 순서표

1	MN의 쿠키생성	CoA와 CoTI의 쿠키를 이용하여 Cookie1을 생성
2	MN의 HoTI와 CoTI 전송	RR 과정과 동일
3	CN의 HoTI와 CoTI 처리	두 메시지가 같은 MN으로부터 온 것인가의 확인 과정
4	CN의 HoT와 CoT의 생성	홈 키젠 토큰과 Cookie2를 배타적 논리합으로 히든 홈 키젠 토큰 생성
5	CN의 HoT와 CoT의 전송	RR 과정과 동일
6	MN의 HoT와 CoT 수신	수신된 두 메시지로부터 세션키 생성

<표 3>은 초기 HT-RR 과정의 순서를 나타낸다. HT-RR과정은 CN과 HA 사이에 공격자가 존재하여 HoT 메시지가 노출되더라도 해당 공격자가 홈 키젠 토큰을 알 수 없도록 하는 알고리즘이다. 초기 HT-RR의 CN은 CoTI의 Cookie2를 이용하여 HoT의 token1을 암호화한다. 따라서 공격자가 HoT를 도청해도 token1을 알지 못해 세션키를 얻지 못한다. HoT의 암호화를 위해 CN이 CoTI와 HoTI 메시지가 동일한 MN으로부터 왔음을 확인해야 한다. 이를 위해 <표 3>의 첫 번째 과정을 수행한다. 초기 HT-RR에서는 CoA와 Cookie2를 통해 Cookie1가 생성되며 그 과정은 (식 5)와 같다. Cookie2는 RR 과정과 동일하게 난수를 이용하여 생성한다.

$$Cookie1 := SHA1(Cookie2 \mid CoA\ )) \qquad (식\ 5)$$

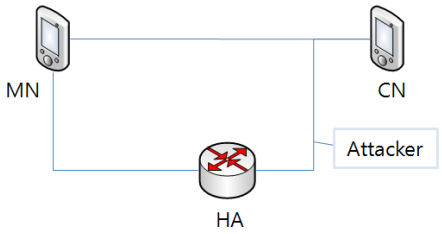
두 번째 과정은 생성한 HoTI와 CoTI을 CN에게 전송하는 과정이다. MN은 HoTI의 소스주소로 HoA를 사용하여 HA를 거쳐 CN에게 전달하며 CoTI는 소스주소로 CoA를 사용하여 CN에게 직접 전달한다. 이 과정은 기존의 RR과정과 동일하다. 세 번째 과정으로 CN은 수신한 HoTI와 CoTI가 동일한 MN으로부터 전송됨을 검증한다. CoTI를 수신하면 (식 5)을 통해 생성된 값과 HoTI의 Cookie1을 비교하여 두 메시지가 같은 노드로부터 송신되었음을 확인할 수 있다. RR에서는 CN이 DoS 공격으로부터 안전하도록 연결 상태 정보를 남기지 않는다. 하지만 HT-RR에서는 CoTI를 수신하면 Cookie1값을 계산하여 HoTI가 도달할 때까지 저장하고 있어야 한다. 이로 인해 추가적인 버퍼가 소모되며 그 크기는 (식 6)과 같다.

$$Buffer = \#CoTI * Cookie\ size \qquad (식\ 6)$$

여기서 Buffer는 CN의 추가적인 버퍼 소모량이며 #CoTI는 일정시간동안 수신한 CoTI의 수를 나타내고 Cookie size는 64bit이다. 네 번째 과정은 CN이 HoTI와 CoTI를 이용하여 토큰을 생성한다. 그 중 token1은 Cookie2와 배타적 논리합을 통해 히든 홈 키젠 토큰을 생성한다. 그리고 그 값을 홈 키젠 토큰을 대체하여 HoT 메시지에 담는다. 따라서 공개채널로 전달되는 HoT의 홈 키젠 토큰을

공격자가 알아볼 수 없다. 다섯 째 과정은 CN이 HoT메시지를 HoA로 전송하며 CoT메시지는 CoA로 전송한다. 이는 RR과정과 동일하다. 여섯 번째 과정은 MN이 HoT와 CoT를 수신하여 세션키를 생성하는 과정이다. MN은 Cookie2와 히든 홈 키젠 토큰을 배타적 논리합 연산을 이용하여 홈 키젠 토큰을 알아낼 수 있으며 이를 통해 정당한 세션키를 생성할 수 있다.

3.1.2 차후 HT-RR 과정



(그림 4) 이동 통신에 사용되는 채널

차후 HT-RR 과정은 홈 키젠 토큰을 암호화 하기위한 키 값으로 직전의 바인딩 갱신에 사용된 홈 토큰을 이용한다. 따라서 초기 HT-RR 과정에서 홈 키젠이 노출 안될 경우 CN과 같은 네트워크에 존재하는 공격자에 대해서도 거짓된 바인딩 갱신 공격에 안전하다. 이처럼 차후 HT-RR 과정은 누적된 값을 키값으로 사용함으로써 홈 키젠 토큰에 대한 안전성을 강화한다. 차후 HT-RR의 동작과정은 다음과 같다. i-1번째 바인딩 갱신시에 사용되었던 홈 키젠 토큰과 i번째 사용되는 홈 키젠 토큰을 배타적 논리합 연산을 하여 그 값을 CoT의 홈 키젠 토큰값을 대체한다.

hidden_home keygen token(i) = token1(i) ^ token1(i-1) (식 7)

4. 분석

4.1 안전성 분석

HT-RR 과정은 초기 HT-RR과정과 차후 HT-RR과정 두 과정으로 나뉘는데, 초기 HT-RR과정은 (그림 4)와 같은 위치에 존재하는 공격자로부터 안전한 바인딩 갱신을 제공한다. 초기 HT-RR과정은 세션키를 보호하기 위해 홈 키젠 토큰을 암호화 한다. 따라서 세션키를 가로채어 메시지의 경로 변경이나 이를 응용한 서비스 거부 공격은 불가능하다. 차후 HT-RR과정은 홈 키젠 토큰을 암호화 하기위해 직전에 사용한 홈 키젠 토큰을 사용한다. (그림 4)의 위치에 존재한 공격자에 대해서 초기 HT-RR과 같은 안전성을 제공하며, 초기 HT-RR과정이 안전하게 이루어질 경우 CN과 같은 네트워크에 존재하는 공격자에 대해서도 안전한 바인딩 갱신을 제공한다.

4.2 HT-RR의 오버헤드

<표 4 > RR 과정과 HT-RR과정의 효율성 비교

	RR과정의 연산량	초기 HT-RR과정	차후 HT-RR 과정
MN 계산	SHA-1	SHA-1*2	SHA-1
CN 계산	HMAC*2	HMAC*2 SHA-1	HMAC*2

연산량의 오버헤드는 초기 HT-RR 과정의 두 번의 SHA-1연산이 있으며, 공간의 오버헤드는 CN에서 HoTI와 CoTI의 연관성을 확인하기 위한 버퍼의 사용이 있다. 이때 버퍼 사용량은 (식 6)과 같다.

4. 결론

HT-RR 과정은 두 과정으로 나뉘는데 초기 HT-RR 과정은 Cookie2를 이용하여 token1을 암호화함으로써 공격자가 HA와 CN사이에 존재하더라도 세션키를 얻지 못하며, 차후 HT-RR과정은 직전의 바인딩 갱신 정보로 token1을 암호화하여 공격자가 CN과 같은 네트워크에 존재하더라도 세션키를 얻지 못한다. 그로 인해 HT-RR은 (그림 4)에 존재하는 공격자로부터 안전한 바인딩 갱신을 제공한다.

HT-RR는 CN과 같은 네트워크의 공격자가 초기 HT-RR과정부터 도청을 감행할 경우 거짓된 바인딩 갱신 공격에 대해 취약하며, 이를 보완하기 위한 연구를 수행해 나갈 것이다.

참고문헌

[1] D. Johnson. C. Perkins. J. Arkko. "Mobility Support in IPv6". IETF RFC 3775. Jun. 2004.

[2] P. Nikander. J. Arkko. T. Aura. G. Montenegro. E. Nordmark. "Mobile IP Version 6 Route Optimization Security Design Background". IETF RFC 4225. Dec. 2005.

[3] J. Arkko. V. Devarapalli. F. Dupont. "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents." IETF RFC 3776. Jun. 2004.

[4] G. O'shea. M. Roe. "Child-proof Authentication for MIPv6 (CAM)", *ACM Computer Communication Review*. Vol 31. No. 2. pp. 4-8. Jul. 2001.

[5] T. Aura. "Cryptographically Generated Addresses (CGA)." IETF RFC 3972. Mar. 2005.

[6] G. Montenegro. C. Castelluccia. "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address." *Proc. of the Network and Distributed System Security (NDSS 2002)*. Feb. 2002.

[7]구중두, 김상진, 오희국, "모바일 IPv6의 바인딩 갱신 기법에 관한 고찰", 한국정보보호학회 학회지, 제16권 1호, pp. 99-111, 2006년 2월.