Return Routability 프로토콜의 취약점 및 개선 방안*

장학범**, 강성용*, 최형기**
성균관대학교 정보통신공학부
e-mail: {hbjang, sykang, hkchoi}@ece.skku.ac.kr

Vulnerability of Return Routability Protocol and Improvement

Hak-Beom Jang**, Seong-Yong Kang*, Hyoung-Kee Choi**
*Dept. of Mobile Systems Engineering, Sunkyunkwan University
**Information and Communication Engineering, Sungkyunkwan University

요 약

기존의 모바일 IPv6에서 경로 최적화를 하기 위해 바인딩 업데이트를 할 때 RR 프로토콜을 사용한다. IPv6에서 바인딩 업데이트는 이동노드가 홈 네트워크에서 외부 네트워크로 이동했을 때 Home Agent와 Correspondent Node(CN)에게 전송하며 이 과정에서 몇 가지 취약점으 가지고 있다. HoIT와 CoIT 메시지는 서로 연관이 없으며 이동 단말과 HA사이에만 IPSec으로 보호된 터널이 존재하고 HA와 CN 사이에는 보호되지 않는다. 따라서 공격자는 CN과 가까이에 위치하여 자신의 CoA를 CN에게 CoIT를 보내 토큰을 받아서 CN과 바인딩 업데이트를 할 수 있다. 바인딩 업데이트가 끝나면 두 노드 사이는 정상적인 통신을 할 수 있고 공격자에 의해 위험에 노출 될 수 있다. 또한 CoIT 메시지를 보내면 CN에서는 토큰을 생성하게 되므로 공격자가 다수의 기기를 획득해 CN에게 계속 CoIT를 보내면 계속 토큰을 만들어야 하므로 다른 정상적인 노드의 통신을 방해할 수 있다. 따라서 이 논문에서는 이러한 RR프로토콜에 대한 문제점을 분석하고 이러한 문제점을 해결 할 수 있는 개선 방안을 논의 해 본다.

1. 서론

최근 스마트폰이나 PDA등 이동 단말이 발전하면서 이러한 단말기는 IP를 가지고 통신할 수 있게 된다. IP를 사용하는 기존의 컴퓨터같은 기기들은 고정된 IP를 가지게 되는데 IP 주소는 네트워크 링크에서 결정되므로 따라서 기존 네트워크에서 외부 네트워크로 이동할 때 IP주소가 변경되므로 따라서 TCP같은 상위 계층과 연결이 끊어지므로 끊임 없는 통신을 할 수 없게 된다. 따라서 이러한 이동성의 욕구를 충족시키기 위해 Mobile IP 프로토콜 기술이 등장하게 되었다. Mobile IP는 이동 사용자가 로밍 중에도 진행 중인 세션을 그대로 유지하게 하고 사용자와 네트워크간에 이동에도 사용에게는 서비스의 연속성을 제공하는 것이다. 현재 네트워크 상에서 IP 버전 4를 사용하므로 만약 Mobile IPv4에서 이러한 이동성을 제공하기 위해 Home Agent(HA)라는 특별한 라우터를 두어서 만약 이동 단말이 외부 네트워크로 간다면 그 단말은 HA에게 이동한 IP 주소를 통보하게 된다. 즉 CN이 MN과 통신을 하려고 할때 HA에 메시지를 보내면 HA가 MN의 이동여부를 판단해 MN이 존재하는 위치로 패킷을 보내주게 된다. 따라서 끊김 없는 통신이 가능하게 된다. 하지만 IP 버전4가 가지고 있는 IP 부족 때문에 IP 버전6가 제안되고 Mobile IP 또한 IP 버전6에서도 이동성을 지원하는 Mobile IPv6가 제안되었다. Mobile IPv6는 기존의 IPv4가 가지고 있는 Triangle Route 문제와 Ingress Filtering 문제를 해결하였고 IPv4에서 필요했던 Foreign Agent(FA)가 Mobile IPv6에서는 필요없게 되었다. Mobile IPv6에서는 이동 단말이 새로운 새로운 네트워크로 이동했을 때 Mobile IPv4와 같이 C처음 패킷은 HA를 통해서 외부 네트워크로 전송되어 바인딩 업데이트를 하게 된다. 이때 Mobile IPv6는 경로 최적화를 수행하기 위해 HA와도 바인딩 업데이트를 하지만 CN과도 바인딩 업데이트를 하게 된다. 이때 CN과 바인딩 갱신을 수행하기 위해 RR 과정을 통해서 안전한 통신을 할 수 있다. 하지만 기존의 RR 과정의 경우 몇 가지 취약점으 가지고 있다. HoIT와 CoIT 메시지는 서로 연관이 없으므로 공격자는 자신의 CoA를 CN에게 CoIT를 보내 토큰을 받아서 CN과 바인딩 업데이트를 할 수 있다. 바인딩 업데이트가 끝나면 두 노드 사이는 정상적인 통신을 할 수 있고 공격자에 의해 위험에 노

* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 기초연구사업임 (No.2011-0005037)

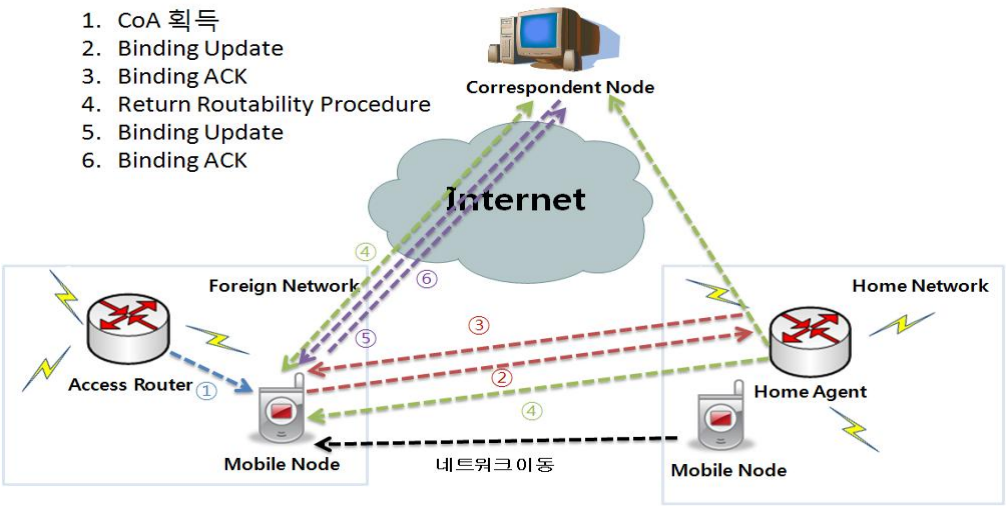

그림 1 Mobile IPv6의 동작 과정

출 될 수 있다. 또한 CoIT 메시지를 보내면 CN에서는 토큰을 생성하게 되므로 공격자가 다수의 기기를 획득해 CN에게 계속 CoIT를 보내면 계속 토큰을 만들어야 하므로 다른 정상적인 노드의 통신을 방해할 수 있다. 본 논문에서는 문제점을 해결하였고 새롭게 개선된 RR 과정을 제시한다.

2. 연구 배경

이동 단말은 CN과 연결을 맺고 통신을 수행한다. 통신 상대는 eh 다른 이동 단말일 수도 있고, 혹은 서버와 같이 이동성이 없는 단말일 수 도 있다. 그림 1과 같이 만약 단말이 외부 네트워크로 이동 했을 경우 CoA(Care-of Address)를 얻게 된다. 이 과정은 Router의 Router Advertisement 메시지에서 수행되며 단말이 이 메시지를 받으면 DHCP 방식으로 주소를 획득하거나 또는 Stateless Auto-configuration 방식으로 주소를 얻게 된다. CoA를 얻게 되면 이제 모바일 단말은 HA와 CN과 바인딩 업데이트를 하게 된다. 한편, 바인딩 업데이트를 위해 이동 단말은 통신 상대 CN에게 HoA 및 CoA를 모두 전송하여 알려준다. 메시지를 송신할 때 이동 단말과 통신상대 CN은 둘만의 비밀 값을 이용하여 바인딩 업데이트를 하므로 누구도 바인딩 업데이트 메시지를 생성할 수 없다. 그러나 이 과정에서 CN과 MN 사이에만 비밀 값을 이용해 바인딩 업데이트를 한다면 그 비밀 값은 크기가 작기 때문에 전수조사를 통해 짧은 시간 내에 찾아 낼 수 있다. 따라서 악의적인 목적을 가진 공격자는 MN이 송신한 바인딩 업데이트 메시지를 차단한 후, 이 비밀값을 찾아내어 바인딩 업데이트 메시지를 위조하여 송신함으로써 이동 단말 MN의 HoA를 다른 CoA와 연결시킬 수 있다. 만약 이동 단말 MN의 HoA가 공격자의 CoA와 연결된다면, 이후에 통신 상대 CN이 송신하는 모든 메시지를 CoA, 즉 공격자에게 송신되고, 공격자는 이 메시지들을 열람하거나, 이를 변조하여 MN에게 송신할 수 있다. 이러한 공격을 막기 위해 Mobile IPv6에서는 바인딩 업데이트 메시지는 서로 다른 2개의 경로를 통해서 CN에게 한번에 전송된다. 즉 이동 단말 MN은 통신 상대 CN에게 바인딩 업데이트 메시지를 송신하는 동시에, MN 자신의 홈 네트워크 HA를 통해서 CN에게 바인딩 업데이트 메시지를 송신한다. 이러한 Mobile IPv6에서 MN이 CN에게 보내는 바인딩 업데이트 메시지 인증하기 위해 사용하는 메커니즘이 Return Routability(RR)이다.

3. Return Routability

이 장에서는 Return Routability(RR) 과정에 대해서 설명해본다. Mobile IPv6에서는 기본적으로 MN이 HA를 거쳐서 터널을 통해 이동하는"Triangle Routing" 문제를 해결하게 된다. MN과 CN이 직접 통신해 Route Optimization을 할 수 있도록 하기 위해서는 MN 자신의 CoA를 CN에게 전송하여 바인딩 업데이트를 통해 이루어진다. 이때 사용하는 메커니즘이 RR 프로토콜이다. 기본적으로 RR프로토콜은 CN 입장에서 실제로 CoA에 존재하는 이동 단말이 있는지를 확인하는 작업이다. 그림 2와 같이 총 6개의 메시지가 사용된다 이중에서 5번째 메시지가 바인딩하는 메시지이다. 우선 CN은 HoTI(Home Test Init)와 CoTI를 서로 다른 경로를 통하여 CN에게 전송한다. 이동 단말은

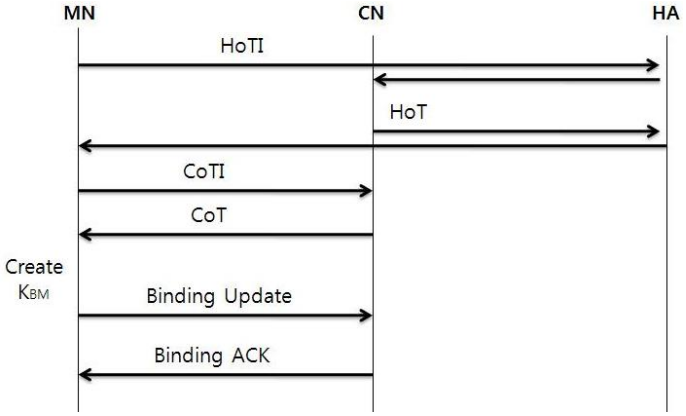

그림 2 Return Routability 메시지 교환 과정

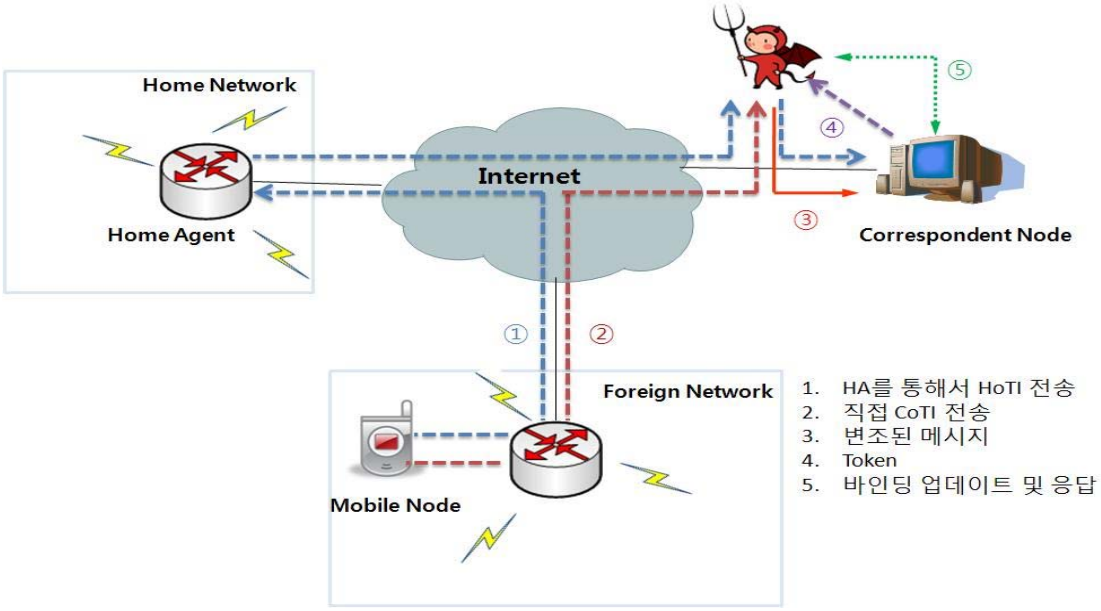

그림 3 Mobile IPv6 바인딩 업데이트 변조 공격

우선 먼저 Home Agent를 경유하여 CN에게 HoTI 메시지를 전송한다. HoTI 메시지는 CN에게 RR절차의 시작을 알리는 메시지이다. 이 HoTI에는 이동 단말의 Home address(HoA), 모바일 쿠키(MC1), HIC(Home Init Cokie)를 포함한다. 이때 이 경로의 경우 IPSec으로 보호된 터널을 통하여 전송되기 때문에 안전한 경로이다. HA에서 터널링을 통해 전송된 후 CN에게 다시 HoTI 값을 전송하게 된다. 그리고 단말은 다시 CN에게 직접 CoTI를 전송한다. CoTI 또한 이동 단말의 임시주소 CoA와 모바일 쿠키 값 (MC2) 및 이동 단말이 생성한 CIC(Care of Init Cokie)를 포함하여 전송하게 된다. HoTI와 CoTI를 받게 된다면 이제 CN에서 HA를 경유하거나 eh는 직접 MN에게 응답 메시지인 HoT(Home Test)와 CoT(Care of Test)메시지를 보내게 된다. 이 HoT 메시지는 이동 단말이 보낸 HIC값과 CN이 생성하는 nonce값 HNI(Home Nonce Index)와 HKT(Home Keygen token)을 포함하여 MN에게 전송한다. 이때 각 토큰은 HoA 혹은 CN의 비밀값 KCN 그리고 CN이 생성한 랜덤 nonce를 사용하여 해쉬함수를 생성한다. 이러한 랜덤값은 CN이 인덱스를 붙여서 저장하고 있으며, 이 인덱스 값은 HoT에 포함되어 있다. 인덱스 주소로 CN은 해당 토큰이 어떤 IP주소와 랜덤값을 사용하여 만들었는지를 알 수 있다. 마찬가지로 CoT 역시 동일한 요소들을 가지게 되고 직접 이동 단말으로 전송하게 된다. 이제 이동 단말은 두 경로로부터 받은 두 개의 토큰을 이용하여 Key를 만들게 된다. 따라서 이 key를 가지고 Binding Update 메시지의 MAC을 생성하게 된다. Binding Update 메시지에는 HoA와 CoA, sequence number, HNI, CNI 그리고 생선한 키로 MAC 암호화한 값이 포함된다. 이동 단말이 바인딩 업데이트 메시지를 보내게 되면, CN은 이것을 받아서 HNI와 CNI를 통해서 해당 랜덤 값 nonce를 얻고 HoA와 CoA를 가지고 각 두 개의 토큰을 생성하게 된다. 생성한 토큰으로 MAC으로 암호화된 값을 풀고 Binding Update 메시지를 확인하게 된다. sequence number는 Binding Update에 대한 Binding ACK 메시지의 일치성을 검증하기 위해서 포함된다. CN은 메시지를 검증하면 검증확인 응답으로 Binding ACK를 보내게 된다. 이 메시지 또한 토큰으로 생성한 key로 암호화 되어있으므로 MN이 ACK를 받게 된다면 서로 안전하게 Binding Update가 되었음을 알 수 있다. 이후 이동 단말은 CN과 직접 통신할 수 있게 된다. 이동 단말과 Home Agent 사이에는 IPSec ESP 터널에 의해 보호 되므로 공격자가 이들 사이에 메시지를 변조하기 위해서는 두 가지 경로에 대해서도 알고 있어야 한다. 따라서 이러한 RR 프로토콜은 보안강도가 향상된다.

4. Mobile IPv6 바인딩 업데이트 취약점

위에서 설명했듯이, Mobile IPv6에서는 이동 단말이 이동 단말과 바인딩 업데이트를 하기 위해서는 HA를 통한 경로와 직접 전송하는 경로를 통하여 이동 단말과 Binding Update를 취한다. 이때 HA를 통하는 경로는 이동 단말과 HA 구간이 IPSec으로 보호 받고 있지만, 이 구간 이외에는 보호 받지 못하고 있다. 따라서 위의 그림3과 같이 만약 공격자가 이동 단말과 HA사이 구간이 아닌 HA와 CN구간에서 CN과 가깝게 위치하고 있다면 CN에게 전달 되는 정보를 획득할 수 있다. 따라서 이 과정에서 암호화 되지 않은 이동 단말의 HoA를 전송해서 해당 토큰을 획득할 수 있다. 그림3과 같이 1번, 2번 메시지를 공격자가 가로채 공격자의 주소(CoA)가 적힌 위조된 3번 메시지를 보내게 되고 따라서 CN은 공격자에게 토큰을 주게 되고 공격자와 Binding Update를 하게 된다. 인증이

끝나게 되면 CN의 모든 메시지는 공격자와 통신을 하게 된다.

또한 DoS 공격에 취약하게 된다. CN은 메시지 HoTI나 CoTI를 받을 때 마다 랜덤 값 HNI와 토큰을 생성해서 유지하고 또한 해쉬 연산을 하게된다. 이때 공격자가 다수의 CoTI를 가지고 DoS 공격을 시도한다면 CN은 HNI와 토큰을 생성하므로 메모리를 소비하게 된다. 따라서 DoS 공격에 취약할 수 있다.

마지막으로 RR 프로토콜의 경우 각각 HoTI와 CoTI에 대해서 토큰을 생성하게 되는데 이 두 메시지의 경우 전혀 연관성이 없다. 따라서 두 개의 토큰은 서로 독립적으로 구성되므로 여러 가지 잠재적인 위험에 노출되어 있다.

5. 보안 대책에 관한 논의

본 논문에서는 기존의 RR프로토콜에 대한 취약점을 제시했고 보안 대책으로 다음과 같은 요구사항을 만족해야 한다.

첫 번째로 공격자가 CN 근처에서 CN으로 전송되는 패킷을 가로채 기존의 HoA 정보와 새롭게 공격자의 CoA를 가지고 Binding Update를 시도하고 있다. 이러한 공격은 HoA의 노출을 방지한다면 막을 수 있다. 따라서 HoA가 CN에게 안전하게 전달 될 수 있도록 보장되어야하고 혹시 패킷을 가로채더라도 패킷을 가지고 어떠한 정보도 알아 낼 수 없어야 한다. 두 번째로 기존의 RR과정에서는 CN이 생성하는 두 개의 토큰은 아무런 연관성을 가지지 않는다. 이러한 것은 다양한 공격의 주요한 원인이 되고 있다. 따라서 새롭게 두 토큰 사이의 연관성을 고려해야 한다. 셋 째로 각 서로 주고 받는 메시지에 대해서 인증이 필요하다. 현재 통신상대가 내가 원하는 통신상대인지를 알 수 있어야 한다. 따라서 이러한 인증을 통해서 DoS 공격을 방지할 수 있을 것이다.

6. 결론

본 논문에서는 Mobile IPv6의 Return Routability의 구성과 보안 구조에 대해서 분석하고 몇 가지 취약점을 발견하였다. 실제로 RR절차를 할 때 Binding Update의 취약점을 통해 공격자 이동 단말이 CN과 연결하여 통신할 수 있다는 것을 알 수 있고, 또한 두 토큰이 서로 연관성이 없으므로 다양한 공격의 원인이 되고 있다. 향후 연구로는 제안한 취약점에 대한 보안 대책을 생각해보고 취약점을 해결한 프로토콜을 제시하고자 한다.

참고문헌

[1] D.Johnson,c. Perkins, and J. Arkko, "Mobility Support in IPv6." RFC 3775, June 2004.

[2] C.Perken, "IP Mobility Support" RFC 2002, October, 1996.

[3] 신태일, 문영성, “Return Routability를 이용한 Fast Handovers for Mobile IPv6 인증 기법”, 2008

[4] 송세화, 최형기, 김정윤, “모바일 IPv6 바인딩 업데이트의 보안 향상 기법”, 2010

[5] Jie Li, H냐매-Hwa Chen, "Mobility Supprot for IP-Based Networks". 2005