모바일 IPv6 바인딩 업데이트의 보안 향상 기법+

송세화○ 최형기
성균관대학교 정보통신공학부
dreaminsh@ece.skku.ac.kr, hkchoi@ece.skku.ac.kr

Secure Binding Update in Mobile IP version 6

Sehwa Song○ Hyoung-Kee Choi
School of Information and Communication Engineering, Sungkyunkwan University

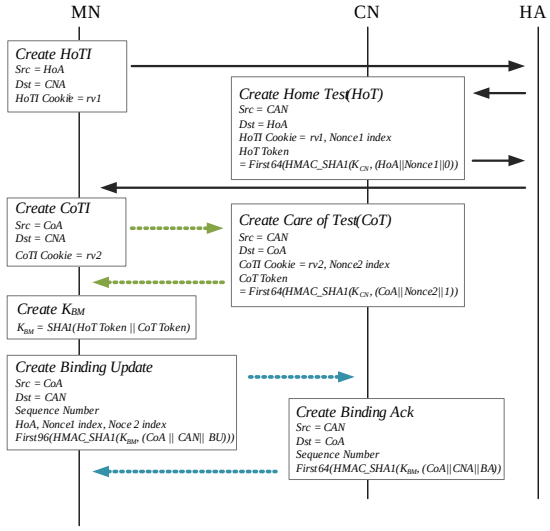
IP를 사용하는 무선단말의 보급이 활발해지고 있다 향후, 보다 많은 주소를 지원하기 위해 IPv6가 IPv4를 대체할 것으로 보인다[1]. IPv6는 무선단말이 가지는 mobility를 지원할 수 없다. IPv6에 mobility를 지원하기 위해 Mobile IPv6가 제안되었다[2]. 무선단말이 이동함에 따라 routing되는 경로가 길어지게 됨 Mobile IPv6는 무선단말이 이동하면서 바뀌는 IP를 통신상대방에 알려주는 Binding Update기능을 제공 통신상대방은 무선단말이 주장하는 새로운IP에 대해서 Return Routability방식을 통해 검증한다[3]. Return Routability는 공격자가 무선단말의 Home Agent와 통신상대방 사이에 있을 경우, 취약점이 존재한다. 이를 악용하여 공격자가 무선단말과 통신상대방의 세션을 뺏는 공격이 가능하다. 본 논문은 소인수분해 방식과 cookie를 사용하는 새로운 Binding Update방법을 제안 제안하는 방법을 통해, 취약점 해결과, 단말과 통신상대방의 연산량을 감소시키는 효과가 있다

Mobile IPv6의 Binding Update는 Home Agent와 Correspondent Node에게 수행되며, 본 논문에서는 Correspondent Node에의 Binding Update를 다룬다. MN은 CN과 HA를 거치지 않고 바로 통신하기 위해서 MN이 새롭게 할당받은 CoA를 Binding Update메시지를 사용하여 CN에 등록시켜야 한다. Binding Update는 MN이 이동하여 새로운 IP를 할당 받은 후, <그림 1>과 같이 6개의 메시지를 통해 이루어진다. Home Test Init(HoTI)메시지와 Care of Test Init(CoTI)메시지를 통해 MN은 CN에게 Binding Update에 사용할 키를 구성하는 토큰을 요청하고 CN은 Binding Update에 사용될 키를 이루는 토큰 두 개를 서로 다른 경로로 무선단말에게 전송한다 MN이 정상적이라면 HoT와 CoT메시지를 통해 토큰 2개를 확보할 수 있다. MN은 <그림 1>과 같이 토큰 2개를 사용하여 K_{bm}을 생성하고, K_{bm}을 통해 Binding Update에 대한 MAC을 만들어, Binding Update메시지를 CN에게 전송한다. CN은 Binding Update의 MAC을 토큰을 통해 확인하여 MN의 새로운 CoA가 정상임을 확인하고 향후 통신을 CoA를 통해 수행한다. 이 Binding Update방법은 3가지 원인에 의해 취약점이 존재한다 첫 번째는 토큰이 전달되는 구간 중에 HA와 MN사이만 IPSec[5]으로 보호될 뿐, 그 의외의 구간에서는 평문으로 전달된다 따라서, 악의적인 목적을 가진 단말의 경우 다른 단말의 HoT를 확보할 수 있다. 둘째, HoTI, CoTI를 받은 CN은 전송자가 자신과 통신중이었던 MN인지, 아니면, 다른 단말인지 확인할 수 없고 무조건 토큰 생성 후, HoT와 CoT를 MN에게 전송한다. 셋째, 토큰 생성시 두 개의 토큰이 아무런 연관성이 없다. 두 개의 토큰이 연결고리가 없어 오직Binding Udpate메시지에 같이 사용이 되면 인증하게 된다.

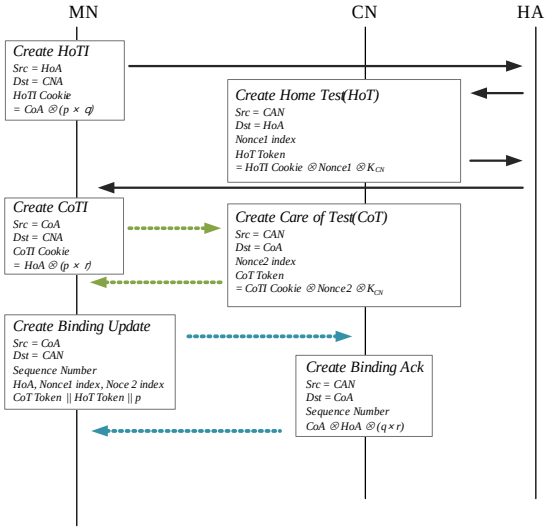
그래서, HA와 CN사이의 구간에 공격자가 MN에게 전송되는 HoT메시지를 탈취할 경우 Session Hijacking 공격이 가능하다[4]. 공격자는 자신의 IP주소로 CoTI메시지를 통해 Care of Keygen Token을 확보 후, 피해자가 되는 MN의 Home Keygen Token을 확보하여 Bindng Update를 시도할 수 있다.

본 논문에서는 큰 수의 소인수분해와Cookie를 사용하는 새로운 Binding Update를 제안한다. 이는 두 개의 토큰의 생성에 MN의 참여하게 되어 향후 Binding Update시 두 개의 토큰을 자신이 요청하여 생성하였음을 증명하게 된다 기존 MIPv6의 Binding Update와 메시지 수는 동일하나 <그림 2>와 같이

+ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028)



<그림 1> 기존 MIPv6 Binding Update



<그림 2> 제안하는 MIPv6 Binding Update

각 토큰를 구성하는 내용에 차이가 있다. 우선 MN은 HoTI, CoTI메시지를 전송하기 전에, 64bits 소수 p, q, r을 생성한다. HoTI와 CoTI메시지에 <그림 2>과 같이 HoTICookie 및 CoTICookie를 만들어 같이 보낸다. 이 때, 두 개의 Cookie는 p라는 공약수를 가지는 64bits 소수의 곱을 통해 연관성을 확보하게 된다. 또한, Cookie생성시 HoTICookie에는 CoA를 , CoTICookie에는 HoA를 사용하게 된다. CN은 HoTI 및 CoTI메시지를 받으면, <그림 2>과 같이 Home Keygen Token과 Care of Keygen Token을 생성하여 기존 방법과 동일한 경로로MN에게 전송한다. MN은 두 개의 토큰의 concatenation과 소수 p를 Binding Update메시지로 전송한다. MN은 binding update 메시지 전송할 때, p를 같이 보냄으로써 두 개의 토큰이 자신이 요청하여 생성한 것임을 증명한다Binding update메시지를 받은 CN은 두 개의 토큰에서 MN이 생성했던 두 개의 수를 추출해낸 후에, p로 MOD연산을 수행하여 0이 나오는지 확인하게 된다. 공격자는 2개의 소수의 합성 수에서 공약수를 뽑아내기가 어렵기 때문에 악의적인Binding Update를 수행하기 어렵다. 제안하는 방법은 기존에 비해 연산량이 상당히 적어지기 때문에CN입장에서 다수의 MN이 접속해 있는 경우에도 빠른 처리를 할 수 있다. 단, 기존에 비해, 약 20%정도 전송 Bit수가 증가하나, 이는 무선망의 Bandwidth가 증가하면 극복이 될 수 있다.

참고문헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December, 1998

[2] D. Johnson, C. Perkinsm, J. Arkko, "Mobility Support in IPv6", RFC 3775, June, 2004

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

[4] H. Fathi, et al., "Leakage-Resilient Security Architecture for Mobile IPv6 in Wiress Overlay Networks", IEEE journal on selected areas in communications, Vol.23 No.11, 2005

[5] S. Kant, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 1998, November , 1998