Self-signed CGA방식에 기반을 둔 MIPv6 프로토콜에 대한 보안공격

김민경*, 강현선, 박창섭
단국대학교 전자계산학과
*e-mail: mashimaro@dankook.ac.kr

The security attack against the MIPv6 protocol which based on Self-signed CGA

Min-Kyoung Kim*, Hyun-Sun Kang, Chang-Seop Park
Dept of Computer Science, DanKook University

요 약

본 논문에서는 모바일 노드(mobile node, MN)와 대응노드(correspondent node, CN)사이의 바인딩 업데이트 (binding update, BU) 프로토콜에 대해 기존 프로토콜 및 BU메시지를 보호하기 위해 제안된 메커니즘에서 발견된 취약성과 결점을 살펴보고, 최근에 제안된 You-Cho의 프로토콜에 가할수 있는 보안공격에 대해 알아본다.

1. 서론

Mobile IPv6 (MIPv6)[1]는 모바일 노드(mobile node, MN)의 자유로운 이동성을 지원하기 위한 프로토콜(protocol)이다. 즉, MN이 인터넷상의 어느 한 점에서 다른 점으로의 이동시 전송계층 연결(transport connection)의 중단 없이 자유롭게 이동하기 위한 목적으로 제안되었다. MIPv6에서 MN에 대한 IPv6 주소는 MN의 홈 네트워크(home network)에서 정의된 고정된 주소인 HoA, MN이 외부 네트워크(foreign network)리 이동했을 경우, 외부 네트워크에 의해 동적으로 할당되는 CoA(care-of-address) 두 가지 형태로 정의된다. MN이 외부 네트워크로 이동했을 경우, HoA를 목적지로 하는 패킷을 계속적으로 전달받기 위해 MN은 HA(home agent)에게 BU메시지를 보냄으로써 새로운 CoA를 알리는 홈 등록(home registration)을 수행한다. HA는 성공적인 BU를 통해서 MN에 대한 HoA, CoA등의 바인딩 정보를 갱신하고, 이후 MN에게로 향하는 패킷을 MN에게 터널링(tunneling)한다. 만약 대응노드(correspondent node, CN)가 MN에게 패킷을 보내기를 원할 경우, CN은 MN의 현재 CoA를 모르기 때문에 먼저 MN의 HoA로 패킷을 전송한다. 그러면 MN의 HA는 새로운 CoA로 해당 패킷을 전달하고 MN은 CN에게 직접 응답한다.

그러나, 위의 삼각라우팅 문제(triangular routing problem)를 해결하기 위해 MIPv6에서 도입된 라우트 최적화 메커니즘(route optimization mechanism)을 사용할수 있다. MN으로부터 BU메시지를 수신후, CN은 MN의 HoA, CoA를 바인딩 캐쉬(binding cache)에 유지하고, MN으로 직접 패킷을 보낼수 있다. 만약 BU메시지가 전혀 인증되지 않는다면, 몇몇의 Redirect와 DoS(denial-of-service)공격이 가능하게 되며, 이외에도 인증되지 않은 BU메시지로 인해 발생할수 있는 몇몇의 잠재적인 공격[2,3,4]이 알려져 있다. 따라서 CN에게 송신되는 BU메시지는 반드시 보호되어야 한다.

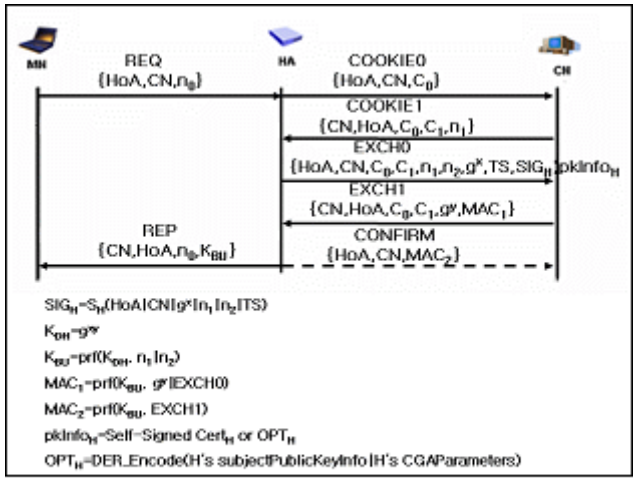
MN과 CN 사이의 안전한 BU 프로토콜의 핵심은 MN이 보낸 HoA, CoA를 CN이 확인하는 메커니즘(mechanism)이다. 그렇기 때문에, 안전한 BU 프로토콜을 위한 메커니즘은 다양한 유형의 공격에 대해 대응할 수 있도록 설계되어야 한다. 먼저, RR 프로시저(Return Routability procedure)[1]는 MN과 CN

이 사용하게 될 세션키를 HoA와 CoA 즉 각각 다른 두 경로로 보낸 키 재료를 이용하여 생성한 후, BU와 BA메시지에 대해 MAC을 이용한 인증된 Binding Update 과정을 수행한다. 그렇지만, 이 방식은 HoA와 CoA 사이의 바인딩이 제공되지 않으며, 처리를 위한 8개의 메시지 흐름은 효율성에서 문제가 있다. SUCV 프로토콜[5,9]은 CGA를 이용하고 더불어 Client Puzzle 개념[6]을 사용하여 CN에 대한 DOS공격에 대응하게 되며, Diffie-Hellman 방식에 의해 세션키를 설정하게 된다. 이 방식에서 MN은 CN이 보낸 Puzzle에 대해 Puzzle-Response를 계산한 후 Binding Update 과정을 수행하게 되는데, 이러한 계산은 하드웨어 제한적인 MN에게는 상당한 부담이며, 세션키 생성을 위한 Diffie-Hellman 방식이 인증이 안 되기 때문에 MITM(man-in-the-middle) Attack에도 노출되는 문제가 있다. 마지막으로 Security Proxy 기반 프로토콜[7]에서는 HA가 하드웨어 제한적인 MN을 대신하여 Security Proxy 기능을 하는 방식이다. 이 방식은 비록 다양한 공격에 안전할 수 있으나, 전 세계적인 PKI라는 보안 하부 구조(security infrastructrue)를 기반으로 한다는 점에서 현실성이 없다고 할 수 있다.

본 논문에서는 기존 BU 프로토콜과 그 프로토콜들의 문제점을 파악하고, 최근에 제안된 You-Cho의 바인딩 업데이트 프로토콜[8]에 대한 보안상의 취약점을 알아본다. 2장에서는 You-Cho의 바인딩 업데이트 프로토콜에 대한 개괄적인 소개, 3장에서는 [8]가 가지는 보안상의 결점과 가능한 보안공격을 알아본다. 마지막으로 4장의 결론으로 본 논문을 마치게 된다.

2. You-Cho의 바인딩 업데이트 프로토콜 [8](Binding Update Protocol)

(그림1) 은 Security Proxy 기반 프로토콜[7]에서 소개된 방식이 전 세계적인 PKI를 사용한다는 점에 대한 보완책으로 CGA를 사용하자는 방식이다. (그림1)의 프로토콜에서 MN의 HA는 MN의 공개키 계산의 부담을 덜어주기 위한 목적으로 보안 프록시(Security Proxy) 역할을 수행하며, CA에 의한 PKC(public key certificate)대신에 CGA방식으로 공개키를 유도한다. 또한, HA는 MN의 HoA를 증명하고, CN에게 MN의 인증을 쉽게 할 뿐만 아니라, MN과 CN의 BU(Binding Update)를 위한 K_{BU} (Binding Update Session Key)를 공유하도록 한다.



(그림1) You-Cho의 BU 프로토콜

· REQ : 먼저, MN은 HoA, CN, n_0로 구성된 메시지를 작성한다. HoA는 MN의 홈 네트워크(Home Network) 주소, CN은 CN의 주소, 그리고 n_0는 MN이 보낸 메시지를 확인하기위한 넌스(nonces)값이다. MN은 작성한 REQ 메시지를 HA에게 보낸다.

· COOKIE0 : HA는 MN과 CN사이의 K_{BU}의 공유를 위해 키 교환과정을 거치게 되는데, 이때 HA와 CN사이의 공격에서 보호하기 위해 C_i(COOKIE number, $i \geq 0$)을 COOKIE0 메시지에 포함시킨다. HA는 MN에게서 받은 HoA, CN에 C_0값을 포함하여 CN에게 보낸다.

· COOKIE1 : HA에게서 COOKIE0를 받은 CN은 n_1, C_1을 생성해서 HA에게 COOKIE1을 보낸다. COOKIE1에 포함된 목적지 주소는 MN의 HoA이다. 결과적으로 이 메시지는 MN의 홈 네트워크에게 배달되며, IPv6 Neighbor Discovery를 이용해서 HA에 의해 빼앗긴다.

· EXCH0 : COOKIE1 메시지를 받은 HA는 C_0를 확인하고, n_2를 생성한다.

그리고, 자신의 비밀값 x를 이용하여 D-H의 공개값 g^x를 계산하고, 홈 네트워크의 비밀키(S_H)를 이용하여 {HoA|CN|g^x|n_1|n_2|TS}을 서명한다. (TS는 타임스탬프를 의미한다) HA와 CN 사이의 authenticated D-H 키 합의를 위해 CGA-based 전자서명을 사용한다. 서명이 끝나면, HA는 CN에게 보낼 EXCH0 메시지를 생성한다. 이때, n_1과 n_2값을 서명에 포함시키는데, 그 이유는 예전 서명에 대한 응답을 카운팅 하고, 서명에 대한 공격을 막기 위해서이다.

· EXCH1 : EXCH0을 받은 후, CN은 쿠키값, 서명을 확인한다. 또한, 자가 서명 인증서(self-signed Certification)를 이용해서 HA의 CGA뿐만 아니라, 인증에 대한 서명까지도 확인한다.

EXCH0에 대한 확인이 끝나면 CN은 HA에게로부터 받은 g^x값과 자신의 y를 이용하여 K_{DH}값을 계산하고, 그것을 이용해 K_{BU}값을 얻는다.

또한 MAC_1 계산 값을 포함하여 HA에게 EXCH1 메시지를 보낸다.

· CONFIRM : EXCH1 메시지는 위에 설명했던 것처럼 HA에 의해 빼앗긴다. HA는 자신의 x값과 CN에게서 받은 g^y 를 이용해서 K_{DH}값을 계산하고, 그것을 이용해 K_{BU}값을 얻는다.

그리고, K_{BU}와 EXCH1을 이용해서 MAC_2값을 계산한 후, CN에게 CONFIRM 메시지를 보낸다. MAC_2값은 CN가 확인하고, 만약 그 값이 정당하다면, CN은 HoA에 대한 캐시 엔트리를 생성하고, K_{BU}값은 MN으로부터 온 BU메시지 인증 시 사용한다.

· REP : MAC_1의 인증을 마친 HA는 안전한 IPSec을 통해 REP 메시지를 보낸다.

이때 맨 처음 MN이 보냈던 REQ 메시지에 포함되었던 n_0를 함께 전송하게 되는데, 이것은 MN에게서 받은 메시지에 대한 응답임을 확인케 한다.

3. 보안공격

CGA를 기반으로 하는 프로토콜에 대해서는 여러 공격이 가능하다. 여러 공격이 가능한 이유는 CGA를 사용하면 누구나 공개키와 개인키를 생성할 수 있고, You-Cho의 프로토콜에서는 자신이 생성한 개인키로 서명을 하고, 자신의 공개키로 인증을 하는 Self-signed certificate를 이용한다는 점이다. 다음의 여러 공격에서 HA는 Self-signed된 디지털 서명을 기반으로 하는데, 이러한 서명은 누구나 생성할 수 있기 때문이다.

3.1 Redirect와 Flooding 공격

Redirect Attack은 공격자가 MN으로 향하는 메시지를 다른 노드로 redirect 하기 위한 목적으로 부당하게 다른 MN의 HoA를 사용하는 것이다. 공격자가 CN과 통신 중인 특정 MN의 HoA를 안다고 가정하자. 이때, 만약 공격자가 공격자의 CoA'와 MN의 HoA를 포함한 성공적인 BU 메시지를 CN에게 보낼 수 있다면, 공격자는 MN과 CN의 연결을 가로채기 할 수 있다. MN은 HoA, CN, n_0를 포함한 REQ 메시지를 HA에게 보낸다.

우선, 공격자는 MN의 HoA와 공격자의 CoA', n_0'를 포함한 REQ메시지를 HA에게 보낸다. HA는 공격자에게서 받은 메시지를 기반으로 CN과 BU에 사용할 키 설정과정을 거치게 된다.

공격자는 키 설정과정에서 CN과 정당한 K_{BU}를 공유하게 되며, 결국 이를 기반으로 Redirect 공격에 성공하게 된다. 위와 같은 방식으로, 네트워크 내의 임의의 호스트를 redirect 메시지로 flooding 공격도 가능하다.

3.2 Resource Exhaustion 공격

Resource Exhaustion공격은 공격대상 노드의 메모리와 계산 리소스를 고갈시키는 DoS 공격이다. 이 공격은 공격대상 노드에게 프로토콜이 실행되는 동안 계산 비용이 큰 공개키 계산이나 많은 상태를 생성하는 연속적인 메시지를 보냄으로써 flooding 공격을 성공시킬 수 있다. CN에 대한 Resource Exhaustion 공격은 다음과 같이 성공시킬 수 있다. 공격자는 임의의 REQ메시지를 생성하여 CN에게 연속적으로 보낸다. 연속적인 REQ메시지를 받은 CN은 불필요한 REQ메시지를 연속적으로 받음으로써, 원치 않는 키 교환과정을 수행하게 된다.

같은 방식으로, 공격자는 HA에 대한 Resource Exhaustion 공격을 성공 시킬 수도 있다.

3.3 가짜 HoAs를 이용한 공격

이 공격은 공격자가 가짜의 HoA를 위조하여, 위조된 BU 메시지를 CN에게 보내는 것이다. 공격자가 가짜의 IPv6 HoAs (HoA_1, HoA_2, …, HoA_m)와 임의의 CoAs (CoA_1, CoA_2, …, CoA_m)를 생성했다고 가정하자. 공격자는 자신이 생성한 가짜의 HoA와 CoA를 이용하여 CN과의 키 교환과정을 거칠 것이다.

그 과정에서 HA와 CN은 K_{BU}값을 공유하게 되고, HA는 그 K_{BU}값을 이용해서 CN에게 가짜 BU 메시지 (BU_1, BU_2, …, BU_m)를 생성해서 보낼 것이다. HA는 공격자에게서 온 HoA와 CoA를 인증할 방법이 없기 때문에, 그 값을 이용하여 CN에게 가짜 BU 메시지를 보내게 되고, 결과적으로 CN은 위조된 메시지를 연속적으로 수신하고 처리하게 됨으로써, CN의 바인딩 캐쉬는 불필요한 바인딩 정보로 채워질 것이다.

3.4 불필요한 BU 프로토콜 발생 공격

만약 MN/CN이 HA를 통해 올바른 REP/COMFIRM 메시지를 받는다면, MN은 자동적으로 CN에게 BU메시지를 보내게 될 것이다. 이러

한 속성을 이용하여, 공격자는 다수의 MN과 특정한 CN사이의 불필요한 BU프로토콜을 발생 시킬 수 있다. 공격자가 다수의 MN의 HoA, CoA와 HA를 알고 있다고 가정하자.

그렇다면, 공격자는 HA를 가장하여 특정 CN을 대상으로 한 많은 거짓 키 교환과정들을 거치게 되고, 그때 생성된 정당한 K_{BUS} (K_{BU1}, K_{BU2}, …, K_{BUm}) 값을 포함한 REP/COMFIRM 메시지가 MN과 CN에게 각각 보내진다.

그 후, CN은 상응하는 MN 혹은 HA와 몇몇의 불필요한 BU프로토콜을 수행하고, 바인딩 캐쉬에 많은 불필요한 바인딩 정보를 생성하여 저장 할 것이다.

4. 결론

본 논문에서는 최근에 제안된 [8]에 가능한 공격 시나리오를 유형별로 소개하였다. MN과 CN사이에 BU프로토콜이 작동하기 위해서는 그들 간에 서로를 인증해 줄 수 있는 메커니즘이 필요하다. 하지만 You-Cho가 제안한 프로토콜은 CN이 MN을 책임지고 인증할 수 없을 뿐 아니라 MN의 Security Proxy 역할을 하는 HA를 통한 다양한 공격들이 가능하다. 따라서, 차후에 본 논문에서 소개한 공격들에 대응할 수 있는 좀 더 안전하고, 효율적인 프로토콜이 제안되어야 한다.

참고문헌

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

[2] Aura, T., Roe, M. and Arkko, J., Security of Internet Location Management, In Proc. The 18th Annual Computer Security Applications Conference, Las Vegas, Dec. 2002.

[3] Aura, T., Mobile IP Security, Security Protocols: The 10th Int'l Workshop, Cambridge, U.K., Apr. 17-19, 2002, LNCS 2845, Springer Verlag, 2003.

[4] Nikander, P., Arkko, J. and Aura, T., Montenegro, G., Nordmark, E., Mobile IP version 6 Route Optimization Security Design Background, draft-ietf-mip6-ro-sec-02, Oct. 2004.

[5] O'Shea, G. and Roe, M., Child-proof Authentication for MIPv6 (CAM), ACM Computer Communications Review, 31 (2), July 2001.

[6] Aura, T., Nikander, P., and Leiwo, J., DoS-resistant Authentication with Clients Puzzles, Security Protocols: The 8th Int'l Workshop, Cambridge, U.K., Apr. 25-27 2000, LNCS 2133, Springer Verlag, 2001.

[7] Deng, R., Zhou, J., and Bao, F., Defending against Redirect Attacks in Mobile IP, In Proc. The 9thACM conference on Computer and communications security, Washington D.C., Nov 18-22, 2002.

[8] You, I. and Cho, K., A Security Proxy Based Protocol for Authenticating the Mobile IPv6 Binding Updates, Computational Science and Its Applications ICCSA 2004: International Conference, Assisi, Italy, May 14-17, 2004, LNCS 3043, Springer Verlag, 2004.

[9] Aura, T., Cryptographically Generated Addresses, RFC 3972, March 2005.