MIPv6의 안전한 바인딩 갱신을 위한 프로토콜 비교 분석

원 유 석[†] · 조 경 산[††]

요 약

MIPv6에서는 경로 최적화를 위하여, 새로운 서브넷으로 이동한 MN(Mobile Node)은 CN(Correspondent Node)에게 자신의 HoA(Home Address)와 새로운 CoA(Care-of Address)와의 바인딩을 통고하는 바인딩 갱신 패킷을 전송해야 한다. 하지만, 안전하지 않은 바인딩 갱신은 오히려 침입자로 하여금 다양한 공격을 가능하게 한다. 이에 따라 안전한 바인딩 갱신을 위한 여러 프로토콜들이 제안되었다. 본 연구에서는 기존 프로토콜들을 비교하기 위해 공격에 대한 취약성을 포함한 보안 특성, 프로토콜의 관리 특성, 패킷 교환 횟수와 암호화 연산 시간의 성능 특성에 대한 비교 기준을 제시하였다. 또한, 제시된 기준에 따라 대표적인 4가지 바인딩 갱신 프로토콜들을 비교 분석하고, 안전한 바인딩 갱신을 위한 개선안을 제시하였다.

Comparison and Analysis of Protocols for the Secure Binding Updates in MIPv6

YouSeuk Won[†] · Kyungsan Cho[††]

ABSTRACT

For the route optimization in the MIPv6, MN (Mobile Node) sends CN (Correspondent Node) a binding update message to notify the binding of its HoA (Home Address) with its new CoA (Care-of Address). However, unauthenticated binding updates expose the involved MN and CN to various security attacks. Thus, protecting the binding update process becomes of paramount importance in the MIPv6, and several secure binding update protocols have been proposed. In this paper, we present the criterions for comparing the protocols's security including the vulnerability to the attacks, the manageability of protocol, and the performance of packet exchanges and cryptographic operations. Then, we analyze the four typical binding update protocols based on the presented criterions. In addition, we propose some improvement tips for secure binding updates.

키워드 : MIPv6, 안전한 바인딩 갱신(Secure Binding update), 보안성(Security), 프로토콜 성능(Protocol Performance)

1. 서 론

인터넷 기술의 빠른 발전과 무선통신 기술 및 단말기의 급속한 확산에 따라 무선 이동 인터넷 환경이 급진적으로 발전하고 있다.

인터넷 통신 프로토콜인 IP(Internet Protocol)에서는 호스트가 인터넷 서비스를 받기 위하여 접속되는 서브넷(subnet)을 고정적으로 지정하며, 호스트는 접속된 서브넷으로부터 유일한 IP 주소를 부여받는다. 따라서, 인터넷에서는 고정된 IP 주소로 패킷의 목적지 주소를 지정한다. 따라서, 이동 가능한 모바일 노드가 IP 주소를 변경하지 않고 이동하면 새로운 서브넷의 접속과 자료의 송수신이 불가능해진다. 이러한 문제를 해결하고 IP에서 호스트의 이동성을 제공하기 위해서 IETF(Internet Engineering Task Force)는 모바일 IP를 제안하였고, IP의 새로운 버전인 IPv6가 제안됨에 따라 새로운 모바일 IP 버전인 MIPv6가 제안되었다[2, 7]. 모바일 IP는 호스트가 다른 서브넷으로 이동하여도 인터넷을 통한 통신을 계속 허용하기 위해 2개의 주소 HoA(Home Address)와 CoA(Care-of Address)를 각각 연결 인식과 라우팅을 위해 사용한다.

MIPv6에서 이동성을 가진 모바일 호스트는 MN(Mobile Node)이라 하고, MN과 통신하려는 호스트는 CN(Correspondent Node)이라 하며, MN이 처음 위치한 홈 서브넷에 있는 라우터는 HA(Home Agent)라 한다. MIPv6에서는 MN이 새로운 서브넷으로 이동하여도 CN이 MN에게 직접 통신할 수 있는 경로 최적화(route optimization) 기능을 기본으로 제공하는데, 이를 위해서 MN은 자신의 이동을 CN에게 바인딩 갱신 패킷으로 통고해야한다. 하지만 안전하지 않은 바인딩 갱신은 오히려 공격자로 하여금 다양한 보안

† 준 회 원 : 단국대학교 대학원
†† 종신회원 : 단국대학교 정보컴퓨터학부 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 9월 9일

공격을 가능하게 한다. 따라서, 바인딩 갱신은 MIPv6의 기본 보안 요구를 만족시키기 위해 매우 중요하며, 이에 따라 안전한 바인딩 갱신을 위한 여러 프로토콜들이 IETF와 연구자들에 의해 제안되었다[1, 5-6, 8-9].

본 논문에서는 바인딩 갱신 프로토콜들을 비교할 수 있는 공격 유형과 보안, 프로토콜 관리 및 성능적 특성 기준을 제시하고, 동일한 기준에 따라 기존에 제안된 대표적인 4가지 바인딩 갱신 프로토콜들을 비교 분석한다. 또한, 각 프로토콜의 가능한 공격 유형에 대한 취약점과 개선안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 MIPv6의 기본 구조와 바인딩 갱신 과정을 설명하고, 3장에서 MIPv6의 바인딩 갱신을 위한 4개의 프로토콜을 설명한다. 4장에서는 가능한 공격의 유형을 분석하고 기존 프로토콜들의 보안성과 프로토콜 특성및 성능을 비교 제시한다. 5장에서 개선안을 제시하고, 6장의 결론으로 끝맺음한다.

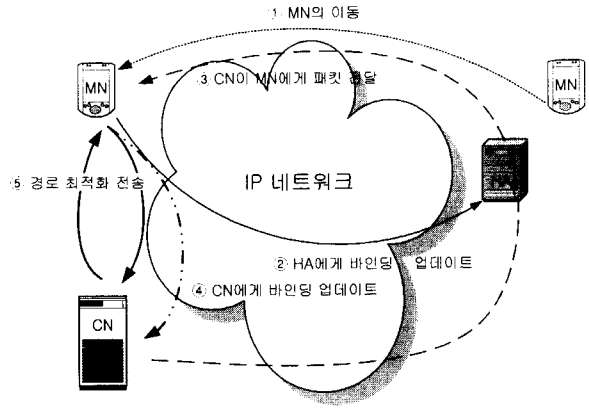
2. MIPv6의 구조 및 바인딩 갱신

모바일 IP에서 모바일 호스트는 HoA와 CoA의 두 개의 주소를 갖는다. HoA는 홈 서브넷에서 MN에게 부여된 IP 주소로 연결 인식을 위해 사용되며, MN은 어느 곳에 있더라도 항상 HoA에 의해 주소 지정될 수 있다. CoA는 MN이 이동된 서브넷에 연결되어 있는 동안 얻게되는 임시 주소로 라우팅을 위해 사용된다. MN이 가진 두 주소인 HoA와 CoA와의 연계를 바인딩이라 한다.

새로운 버전의 IPv6에 따라 등장한 새로운 모바일 IP 버전인 MIPv6은 MIPv4와 달리 경로 최적화를 기본으로 제공한다. MN의 이동을 지원하고 경로 최적화를 위해 HA와 CN은 MN의 HoA와 CoA의 바인딩을 저장하는 바인딩 캐쉬를 유지해야한다. 즉, MN은 CoA와 HoA의 바인딩을 생성하고, 안전한 IPsec을 갖는 터널을 통해 HA에게 바인딩 갱신을 통해 새로운 CoA를 등록한다. 또한, CN으로부터 HA를 경유한 패킷을 수신한 MN은 CN에게 자신의 새로운 CoA를 알리는 바인딩 갱신을 수행할 수 있다. 바인딩 갱신을 통해 CN은 MN의 새로운 CoA를 CN의 바인딩 캐쉬에 저장하고, MN에게 패킷을 전송할 때마다 해당 CoA에게 직접 그 패킷을 전송하는 경로 최적화를 사용한다[8].

Mobile IPv6에서 MN의 이동에 따른 바인딩 갱신 과정은 (그림 1)과 같다.

경로 최적화를 위한 CN으로의 바인딩 갱신은 패킷 전송의 효율성을 높이는 중요한 기능이므로, 바인딩 갱신 패킷은 안전하게 전송되어야 한다. MIPv6에서 MN과 HA사이에는 IPsec의 AH 또는 ESP을 통한 강력한 보안 연관을 갖도록 규정하고 있지만, MN과 CN 사이에는 보안 연관의 규정이 없으므로 CN으로의 보안에 취약할 수 있다. 따라서, 취약한 보안에 의한 다양한 공격에 대응하기 위하여, MN은 바인딩 갱신 패킷을 CN과 공유한 비밀 세션키로 암호화하거나 공개키 기반의 보안을 이용하여 전송할 수 있다.



(그림 1) Mobile IPv6에서 MN 이동 후 처리 과정

공유 세션키로 암호화하는 경우에는 바인딩 갱신 패킷을 전송하기 전에 MN과 CN에게 공유 세션키를 안전하게 분배해야 한다. 이러한 목적으로 네트워크 구조를 이용하는 RR 기법[8], 주소 기반의 공개키를 이용하는 ABK 기법[9], PKI 기반의 DH 키 교환을 이용하는 보안 프록시 기반 기법[6] 등이 제시되었다.

또한, 강한 보안성과 확장성을 가진 공개키로 바인딩 갱신 패킷을 보호하기 위해 전역 인터넷에서 유효한 CA의 필요 없이 주소로 MN의 공개키를 인증하는 CGA 기법도 제시되었다[5].

하지만, 기존의 바인딩 갱신 프로토콜의 연구는 프로토콜의 제안이거나 프로토콜들의 계통적인 소개[1] 또는 가능한 공격의 설명[4]이었으며, 동일한 기준으로 대표적인 프로토콜들을 비교 분석한 예는 없었다.

3. 안전한 바인딩 갱신을 위한 기존 프로토콜

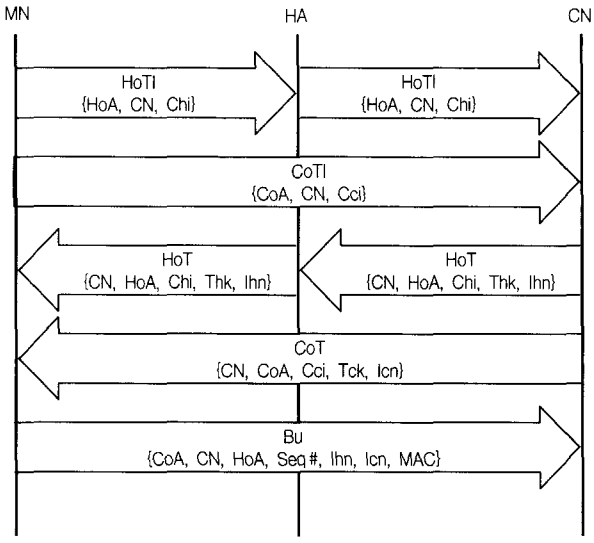
본 장에서는 최근에 바인딩 갱신의 보안을 위한 기본 프로토콜로 채택된 RR, RR의 보안되지 않은 제어 패킷의 취약성을 개선하기 위한 CGA, RR과 CGA의 보안 취약성을 개선하기 위한 보안 프록시 기반 기법, 키 크기에 대한 보안 취약성을 개선할 수 있는 ABK 등의 바인딩 갱신을 위해 제안된 대표적인 4가지 프로토콜들을 소개한다.

3.1 RR(Return Routability)

RR은 MN이 주장한 HoA와 CoA에서 패킷을 수신할 수 있는 가를 확인하여 MN을 인증하고 바인딩 갱신을 위한 공유 세션키를 생성하는 프로토콜이다[1, 7]. MN은 자신의 HoA와 CoA로 전송된 두 개의 패킷의 정보를 조합하여 공유 세션키를 생성하고, 이를 이용하여 바인딩 갱신 패킷을 암

호화하여 CN에게 전송한다.

3.1.1 프로토콜 수행 과정



Thk = HMAC_SHA1 (Kcn, (HoA, Nonce))
Tck = HMAC_SHA1 (Kcn, (CoA, Nonce))
Kbm = SHA1 (Thk | Tck)
MAC = prf (Kbm, (CoA | CN | BU))
Seq # = sequence number
Ihn = home Index of nonce
Icn = care-of Inex of nonce

(그림 2) RR 프로토콜의 수행 과정

3.1.2 프로토콜의 취약점

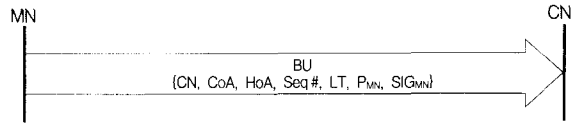
RR은 암호하 되지 않은 제어 패킷을 교환하므로 제어 패킷이 공격자에게 가로채어져 다양한 공격을 받기 쉽다는 보안적 문제를 가진다. 또한, 세션키 유효 기간이 수 초로 매우 짧아 MN이 새로운 서브넷으로 지속적으로 이동하는 경우에는 세션키의 유효 기간이 경과할 때마다 RR을 위한 패킷의 교환이 급증하는 성능적 문제가 있다.

3.2 CGA(Cryptographically Generated Addresses)

IPv6에서 128비트의 IP 주소는 서브넷 전치부 주소와 호스트의 인터페이스 식별자로 구성된다. CGA는 IP 주소(MN의 HoA)의 인터페이스 식별자를 그 노드의 공개키로부터 설정한다는 개념에 근거한다[3, 5]. CGA는 공개키의 해쉬 값을 IP 주소의 인터페이스 식별자로 지정하여 공개키를 검증할 수 있으므로, PKI 기반의 CA처럼 공개키에 대한 전역적 인증 구조는 필요없다.

MN은 디지털 서명을 위한 공개키/개인키를 HoA에 연관하여 생성하고, 자신의 개인키로 서명된 바인딩 갱신 패킷을 CN에게 전송한다. CN은 공개키를 MN의 HoA로부터 검증하고, 이를 이용하여 바인딩 갱신 정보를 수령한다. 따라서, RR과 같은 제어 패킷의 가로채기에 의한 보안 문제는 발생하지 않는다.

3.2.1 프로토콜 수행 과정



SIG_{MN} = S_{MN} (CoA | CN | HoA | Seq# | LT | P_{MN} | 128-n)
S_{MN} = private key
P_{MN} = public key (left-most (128-n)bit)

(그림 3) CGA 프로토콜의 수행 과정

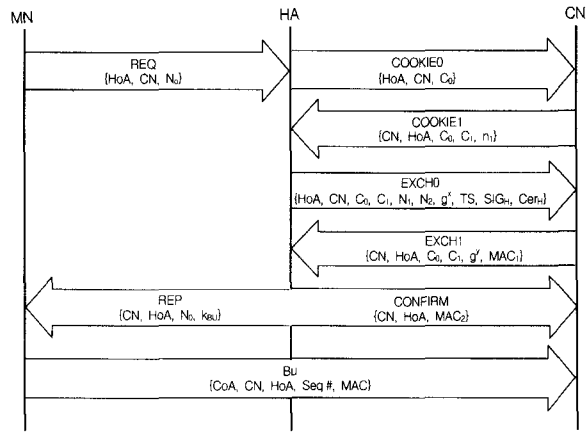
3.2.2 프로토콜의 취약점

공개키의 해쉬 값이 IP 주소의 인터페이스 식별자가 되므로 바인딩 갱신 패킷은 공개키를 소유한 MN으로부터 전송되었음을 확신할 수 있지만, IP 주소의 선택에는 제약이 있어서 프로토콜의 적용이 부적절한 경우가 있다. 또한, 새로운 서브넷으로 이동시마다 바인딩 갱신을 개인키로 서명하고 공개키로 서명을 검증해야하므로 연산의 과부하가 초래된다.

3.3 보안 프록시 기반 프로토콜

R. Deng등에 의해 제안된 이 프로토콜에서는, HA가 MN의 보안 프록시로 동작하여 과부하의 공개키 연산을 MN 대신 수행하고 CN과의 Diffie-Hellman 키 관리를 이용하여 세션키를 생성하여 MN에게 전달한다[6]. 세션키를 분배하는 공개키 생성 과정에서 성능과 신뢰할 수 있는 인증서의 구성에 중점을 두었다. MN의 여러 이동에 대해 비싼 공개키 암호화(서명, DH) 처리는 한번만 수행하고, 공유 세션키로 바인딩 갱신 패킷을 보호한다. 강력한 공개키 기법의 서명과 MAC 사용으로 외부 공격자의 가로채기에 의한 공격을 방지할 수 있다.

3.3.1 프로토콜 수행 과정



P_H/S_H = public/private key
SIG_H = S_H (HoA | CN | g^x | N_1 | N_2 | TS)
Cer_H = {HL, P_H, VI, SIG_{CA}}
k_{BU} = prf (k_{DH}, N_1| N_2)
Diffie-Hellman key k_{DH} = $(g^x)^y$
MAC_1 = prf (k_{BU}, g^y | EXCH0)
MAC_2 = prf (k_{BU}, EXCH1),
MAC = prf (k_{BU}, CoA | CN | HoA | Seq# LT)

(그림 4) 보안 프록시 기반 프로토콜의 수행 과정

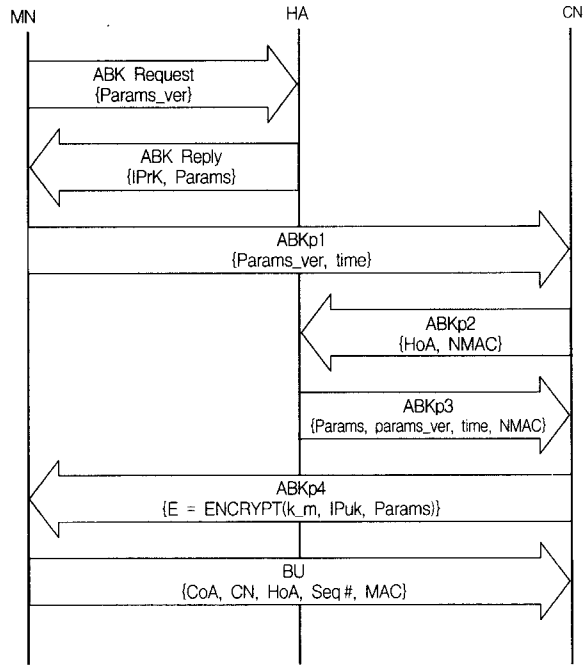
3.3.2 프로토콜 취약점

전체 인터넷을 통한 전역적인 CA를 필요로 하는 비현실적인 요소가 있으며, CA에 의한 인증 및 CRL 검증에 과도한 연산이 필요하다.

3.4 ABK(Address-based key)

주소 기반의 공개키를 생성하는 ABK에서 MN은 이동전에 한번만 공개키를 이용하여 세션키를 생성한 후에 공유 세션키로 바인딩 갱신 패킷을 암호화한다[3, 9]. HA는 신뢰성 있는 제삼자인 IPKG로 동작하여 자신의 홈 서브넷에 있는 모든 MN들의 개인키와 암호화 인수를 생성하여 각 MN에게 제공하고, CN에게는 암호화 인수를 제공한다. CN은 HA로부터 암호화 인수를 얻어 MN의 주소로부터 공개키를 생성하여 MN에게 세션키 정보를 암호하여 전송한다. 따라서, 공개키의 전송이나 인증서는 필요없다.

3.4.1 프로토콜 수행 과정



IPuK/IPrK = public/private key
IPuK = H (ID, time)
NMAC = MAC (SHA1 (HAA, N1), k_CN)
k_m = SHA1 (HoA, k_CN)
MAC = MAC (SHA1 (BU, k_r), k)
k = SHA1 (k_m | k_r)

(그림 5) ABK 프로토콜 수행 과정

3.4.2 프로토콜의 취약점

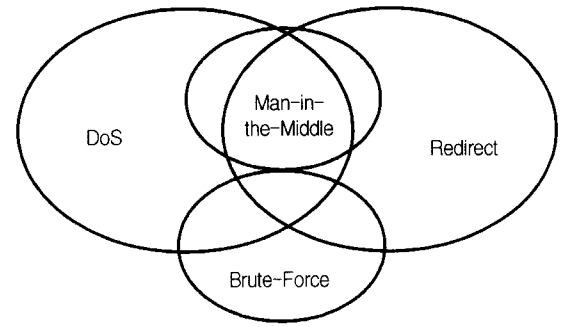
특별하게 처리하지 않으면, HoA의 인터페이스 식별자는 CoA의 인터페이스 식별자와 동일한 값을 갖는 전역적으로 유일한 주소를 가져야 한다는 제약이 있다.

4. 프로토콜들의 비교 분석

본 장에서는 바인딩 갱신에 대한 공격 유형을 분석하고, 보안성과 프로토콜 특성 및 성능의 비교를 위한 기준을 제시하고, 제시된 동일한 기준으로 3장에서 소개된 바인딩 갱신 프로토콜들을 비교한다.

4.1 바인딩 갱신에 대한 공격 유형 분석

MN과 CN 사이에는 정의된 보안 연관이 없으므로, 경로 최적화를 위한 바인딩 갱신 패킷에 적절한 보안 조치가 없다면 공격자들에게 다양한 공격의 기회를 제공할 수 있다. 본 절에서는 CN으로의 바인딩 갱신 과정에 가능한 공격의 유형을 제시한다. 각 공격의 유형은 독립적이지 않으며, 한 유형의 공격에 의해 다른 유형의 공격을 일으킬 수 있다. (그림 6)은 본 논문에서 고려한 공격 유형의 연관성을 보인다.



(그림 6) 공격 유형의 연관성

4.1.1 redirect(방향 전환) 공격

패킷을 실제 목적지가 아닌 다른 노드로 전송하도록 하는 공격이다. 예를 들면, 공격자가 바인딩 갱신에 필요한 정보를 가로채어 가짜 CoA를 갖는 위조된 바인딩 갱신 패킷을 CN에게 보내어 MN이 위조된 주소 CoA′로 이동한 것처럼 등록하고 CN이 이를 받아들이면, 그 이후에 CN이 MN에게 전송한 모든 패킷은 CoA′에 있는 호스트에게 전달된다. 또한, 바인딩 갱신 패킷의 재전송 공격은 이전의 CoA로 전송하도록 하는 redirect 공격이다. 만약 바인딩 갱신을 고의적으로 실패시키면 이전 MN의 CoA로 향하는 redirect 공격이 된다.

4.1.2 DoS(서비스 거부) 공격

공격을 받은 노드와 다른 노드(또는 모든 노드들) 사이의 통신을 불가능하도록 하는 공격이다. 예를 들면, 공격자가 자신이 등록된 CN(들)에게 새로운 위치 CoA′로 이동하였다고 통고하면, CN(들)은 새로운 주소 CoA′로 패킷을 전송한다. 이때, 만약 패킷이 비디오 파일 같은 대용량이라면, 새로운 주소 CoA′의 호스트는 감당할 수 없는 양의 정보를

수신하여 서비스 불능의 상태가 될 수 있다. 또한 존재하지 않는 주소로의 redirect 공격은 그 주소로의 통신이 불가능해지는 DoS 공격이다.

실제로 모든 패킷 전송은 패킷의 양 또는 수를 증가하면 다음과 같이 범람(flooding)에 의한 DoS 공격이 가능하다. 많은 MN을 통해 바인딩 갱신 패킷을 수신한 희생 CN은 바인딩 캐쉬의 과부하에 의해 불능상태가 될 수 있다. 또한, 많은 CN들로부터 위조 IP 패킷을 받은 MN은 CN들에게 불필요한 바인딩 갱신을 시도하게되어 불능 상태가 될 수 있다.

보안 체계에 대한 공격으로 불필요한 공개키 연산의 과도한 암호화 연산을 수행하도록 유도하는 DoS 공격도 가능하다. 복잡한 연산 이전에 약한 인증 적용으로 부적절한 바인딩 갱신을 방지할 수 있다.

Dos 공격으로 경로 최적화를 중단하면, 삼각 경로 사용으로 네트워크 통신량이 증가하게 되는데 이를 공격 목표로 하는 DoS 공격도 가능하다.

4.1.3 man-in-the-middle(중개인) 공격

제어 패킷이 평문으로 전송되거나 쉽게 가로채어진다면, 가로챈 패킷의 내용을 수정하여 전달하는 공격이다.

4.1.4 brute force(전사) 공격

암호화에 사용하는 키의 크기가 작으면 공격자는 가능한 모든 경우를 대입하여 암호화키를 생성할 수 있는 공격이다.

4.2 기존 프로토콜의 보안과 성능 비교 분석

3장에서 분석된 바인딩 갱신 프로토콜들을 동일한 기준에서 비교하기 위해 다음과 같은 보안 특성, 프로토콜 특성 및 성능에 대한 비교 기준을 설정하였다.

4.2.1 보안 특성

- 바인딩 갱신 패킷의 안전한 전송을 위한 암호화 방법
- 세션키 분배를 위한 암호화 방법
- 다양한 공격(redirect, DoS, man-in-the-middle, brute force 공격)에 대한 취약점

4.2.2 프로토콜 특성

- 신뢰할 수 있는 제삼자(TTP)의 필요성
- MN 노드의 인증
- 프로토콜 관리의 용의성 및 확장성

4.2.3 성능

- 패킷의 교환 횟수
- 프로토콜 전체의 암호화 연산 소요 시간
- MN의 암호화 연산 소요 시간

3장에서 소개된 바인딩 갱신 프로토콜들을 위의 기준에 의해 비교 분석한 결과는 <표 1>과 같다.

프로토콜의 성능은 패킷 교환 횟수(패킷 전송의 통신 시간을 반영)와 암호화 연산 시간으로 나누어 분석하였으며, 실제 적용되는 환경에 맞게 이 두 요소를 합하여야 전체 소요 시간이 구해진다.

RR은 공개키 연산을 사용하지 않으므로 암호화 연산 시간은 가장 작으며, CGA는 공개키로 바인딩 갱신 패킷을 보호하므로 암호화 연산 시간은 이동 횟수에 따라 크게 변화한다. 특히, 모바일 호스트의 특성에 맞추기 위해서는, <표 1>에서 제시된 MN의 암호화 연산 시간을 고려해야한다. 패킷 교환을 위한 전송 시간을 반영하는 교환된 패킷 수의 계산에서는 선택 사항인 바인딩 응낙 패킷과 패킷 요청 패킷은 제외하였다.

4.3 기존 프로토콜들의 공격 취약점 분석

본 절에서는 <표 1>에서 제시된 프로토콜들의 공격 취약점을 상세히 분석 제시한다.

4.3.1 RR

공격자가 CN과 HA(및 MN) 사이에 전송되는 평문의 HoT 및 CoT에서 정보를 가로채어 세션키를 생성하여, 위조된 바인딩 갱신 패킷을 통한 redirect 공격이 가능하다. 또한, 사악한 MN이 CN에게 희생 노드로 이동하였다고 거짓으로 바인딩 갱신을 하여 대용량 통신을 희생 네트워크로 이동시켜 범람에 의한 DoS 공격이 가능하다. 암호화되지 않은 제어 패킷에 대한 man-in-the-middle 공격도 가능하다.

4.3.2 CGA

공개키의 해쉬에 인터페이스 식별자의 62비트를 사용함으로 공개키에 대한 brute force 공격에 대해 보안이 취약하다.

MN의 인증이 없으므로 제 삼자가 공개키/개인키를 IP주소와 매치되도록 위조하여 바인딩 갱신에 대한 redirect 공격과 DoS 공격이 가능하다. 신뢰할 수 있는 제삼자가 없으므로 사악한 주소 소유자의 거짓 패킷에 의한 redirect 공격, DoS 공격이 가능하다. 또한, 공개키 연산의 서명/서명 검증 연산의 과부하에 의한 DoS 공격이 가능하다. 바인딩 갱신 패킷이 공개키로 보호되어 이동 노드에 대한 연산의 과부하가 발생하여 이로 인한 DoS 공격이 가능하다.

현재 사용되는 공개키와 주소의 관계를 변환하여, 공개키의 해쉬 값을 HoA의 인터페이스 식별자가 아닌 서브넷 전치부와 인터페이스 식별자를 혼합한 값으로 지정하거나 ABK와 같이 128비트의 IP 주소 모두를 공개키와 연계시키도록 하여 brute-force 공격을 완화시킬 수 있다.

〈표 1〉 바인딩 갱신 프로토콜들의 비교 분석

		RR	CGA	보안 프록시	ABK
바인딩 갱신의 암호화 및 연산		공유 세션키	주소 기반 공개키	공유 세션키	공유 세션키
		SHA-1 ×3 HMAC ×2	Sign × 1 verify × 1 SHA-1 × 1	SHA-1 × 2	MAC × 2 SHA-1 × 3
세션키 분배 방법 및 연산		프로토콜 기반	없 음	PKI 기반	ABK 공개키 기반
		SHA-1×3	없 음	SHA-1 ×2 HMAC ×4 DH agree ×2 DH gen ×1	MAC × 4 SHA-1 × 2 Encrypt × 1 Decrypt × 1
공격 취약성 [1]	Redirect	◉	◉	△	△
	DoS	◉	◉	△	△
	Brute-Force	X	◉	X	X
	Man-in-the-middle	◉	△	△	◉
TTP의 기능		없음	없음	보안 프록시	HA
MN의 인증		주소로 인증	공개키로 인증	프록시로 인증	공개키로 인증
관리의 용의성 및 확장성		우 수	보 통	우 수	취 약
교환 패킷 횟수 [2]		4 + n	n	7 + n	6 + n
전체 암호화 연산 시간(ms) [3]		0.00125 + 0.00337 × n	0 + 10.59015 × n	27.67958 + 0.00196 × n	10.59254 + 0.00196 × n
MN의 암호화 연산 시간(ms) [3]		0.00031 + 0.00106 × n	10.29 × n	0.00098 × n	0.30 + 0.00098 × n

1) 공격에 대한 취약점은 다음절에서 상세히 설명됨.
◉ : 공격에 취약함, △ : 공격이 가능함, X : 공격에 강함
2) MN이 n번 이동하는 경우
3) MN이 n번 이동하는 경우이며, [10]에서 제시된 RSA, SHA-1, SHA 1_HMAC 등의 연산 시간 자료를 적용하였음.

4.3.3 보안 프록시 기반 기법

사악한 MN이 시도하는 redirect공격과 이로 인한 DoS 공격이 가능하지만, 각 공격의 원인 제공자를 확인할 수 있다. 전체 인터넷에 유효한 전역적인 CA는 비현실적이므로, CGA와 같이 스스로 (예를 들면, 주소로부터 검증)공개키를 검증할 수 있는 방법이 요구된다.

4.3.4 ABK

암호 또는 서명되지 않은 제어 패킷에 대하여 man-in-the-middle 공격이 가능하다.

HA가 자신의 홈 서브넷에 있는 MN의 개인키/공개키를 생성하여 자신이 이를 사용하거나, 사악한 MN이 바인딩 갱신에 위조된 CoA를 사용하면 redirect 공격과 DoS 공격이 가능하다. 또한, HA에 대한 공격으로 암호 인수가 유실되면 피해가 발생한다. ABK 기법이 갖는(HoA의 인터페이스 식별자 = CoA의 인터페이스 식별자)의 제약으로 제삼자의 redirect 공격을 방지할 수 있다.

공개키 기반의 과도한 연산은 범람에 의한 DoS 공격이 가능하나, CN은 저장된 정보를 사용하고, HA는 자신의 도메인에 있지 않은 HoA를 포함한 패킷 거부를 거부하고, MN은 자신이 초기화한 응답만 접수하여 방지 할 수 있다.

5. 안전한 바인딩 갱신을 위한 개선 제안

4장의 분석으로부터 안전하고 효율적인 바인딩 갱신을 위해 다음과 같은 사항들이 프로토콜 설계에 고려되어야 한다.

첫째, 모든 바인딩 갱신은 CN이 MN으로 전송한 패킷에 대한 응답이다. 따라서, CN은 자신이 접속한 MN에 대한 일정 크기의 목록을 유지하고, 목록에 저장되지 않은 MN의 바인딩 갱신은 무시하고 또한 바인딩 갱신의 송신자가 자격이 있는 MN인지를 확인하여 공격자의 악의적인 redirect 및 DoS 공격을 방지할 수 있다.

둘째, CN의 바인딩 캐쉬에 대한 DoS 공격의 방지를 위해서는 CN의 바인딩 캐쉬 용량을 증가하고, 공격이 발견되면 MN 및 CN은 연관있는 노드사이에만 경로 최적화를 수행할 수 있도록 신뢰할 수 있는 상대방 목록을 유지한다.

또한, 프록시 기반의 기법에서와 같이 발생한 공격에 대하여는 공격 원인의 제공자(공격자)를 확인할 수 있도록 프로토콜 설계에 고려한다.

셋째, 불필요한 공개키 연산의 과도한 암호화 연산을 수행하도록 유도하는 DoS 공격은 복잡한 연산 이전에 약한 인증을 적용하여 방지할 수 있다. 이러한 유사한 방법이 CGA에 대해 시도되고 있다.

넷째, 세션키로 바인딩 갱신 패킷을 보호하는 경우에, RR을 제외한 프로토콜에서는 일단 세션키가 분배된 후에는 이를 악용하는 공격에 취약해진다. 따라서, 주기적으로 세션키를 검증할 필요가 있다.

다섯째, 공개키를 사용할 경우에는 MN의 부하를 줄이기 위해 HA를 보안 프록시로 사용할 수 있다. 또한, 전역 인터넷에서 공개키의 인증은 신뢰성 있는 CA의 사용을 피할 수 있도록 CGA나 ABK이 더욱 효율적이다.

여섯째, 본 논문에서는 바인딩 갱신 패킷의 전송까지만 다루었다. 만약 선택 사항인 바인딩 요청까지 고려한다면, CN이 먼저 바인딩 요청을 한 후에 MN이 바인딩 갱신을 하도록 하여 사악한 MN이나 외부 공격자의 위조 바인딩 갱신 패킷을 일부 방지할 수 있다. 이 경우에는 CN을 사칭한 공격에 대한 대비가 필요하다.

6. 결 론

MIPv6에서 MN이 새로운 서브넷으로 이동한 후에 수행하는 CN으로의 바인딩 갱신은 경로 최적화를 통한 패킷 전송의 효율성을 높이는 중요한 기능이다. IPsec을 통한 강력한 보안 연관을 갖는 MN과 HA 사이의 경로와 달리 MN과 CN 사이에는 보안 연관의 규정이 없으므로 보안에 취약할 수 있다. 따라서, 취약한 보안에 의한 다양한 공격에 대응하기 위하여 안전한 바인딩 갱신 기법들 - 네트워크 구조를 이용하는 RR 기법, 주소 기반의 공개키를 이용하는 ABS 기법, PKI 기반의 DH 키 교환을 하는 보안 프록시 기반 기법, 공개키 기반의 주소를 이용하여 바인딩 갱신 패킷을 보호하는 CGA 기법 등이 제안되었다.

하지만, 기존 연구에서는 여러 제안들의 소개와 제한된 비교만 제시되었고, 이 들을 동일한 기준에 의해 비교 분석하고 개선하려는 연구가 없었다. 본 연구에서는 바인딩 갱신을 위한 여러 프로토콜의 비교를 위해 공격의 유형에 대한 취약성 및 암호화 방법에 의한 보안 특성 비교, 신뢰할 수 있는 제삼자의 필요성과 MN의 인증과 같은 프로토콜 관리 특성 비교 및 패킷 교환 횟수 및 암호화 연산 시간 등의 성능 특성 비교를 위한 기준을 제시하고, 이에 따라 제안 프로토콜들을 비교하고 분석하였다. 분석 결과를 활용하면, 실제 바인딩 갱신이 적용되는 환경 특성에 적합한 프로토콜의 비교 및 선택이 가능하다.

또한 본 연구에서는 안전한 바인딩 갱신 프로토콜을 위한 제안도 제시하였다. CN은 자격 있는 MN으로부터의 바인딩 갱신만을 인증해야 하며, 공유 세션키로 바인딩 갱신을 보호할 경우에는 세션키 교환 이 후에 주기적으로 세션키를 갖는 MN을 검증하거나 바인딩 요청 패킷을 이용하는 방법이 권장된다. 공개키를 사용할 경우에는 MN의 부하를 줄이기 위해 HA를 보안 프록시로 사용할 수 있다. 전역 인터넷에서 공개키의 인증은 신뢰성 있는 CA의 사용을 피할 수 있는 자가 인증이 가능한 CGA 또는 ABK가 더욱 효율적이다. 또한, 발생되는 공격에 대하여는 공격자를 식별할 수 있는 방법을 추가하여 공격에 의한 피해를 줄일 필요가 있다.

본 연구에서는 성능의 분석을 위해 패킷 교환 횟수와 암호화 연산 시간의 두 항목을 제시하였고 [10]에서 제시된 자료를 해당 암호화 연산 시간 계산에 적용하였는데, 보다 정확한 분석을 위해 패킷 전송 과정을 포함한 통합 시뮬레이터의 개발이 향후 연구로 제시되었다. 본 연구의 결과는 바인딩 갱신 뿐 아니라 향후 MIPv6의 실용화 단계에서 인증과 정보 교환을 위한 다양한 응용에 활용할 수 있다.

참 고 문 헌

[1] 이광수, "MIPv6에서의 바인딩 갱신 인증", TTA 저널, 제 81호, pp.56-65, 2001.

[2] 조경산, 엄희용, "Mobile IPv6의 빠른 핸드오버 기법의 성능 개선", 한국시뮬레이션학회논문지, 제11권 제1호, pp.1-9, 2002.

[3] J. Arkko, et al., "Securing IPV6 Neighbor and Router Discovery," Proc. of WiSe '02, 2002.

[4] T. Aura, "MIPv6 BU Attacks and Defenses," draft-aura-mipv6-buattacks-01.txt, 2002.

[5] T. Aura, et al., "Cryptographically Generated Addresses (CGA)," draft-aura-cga-00.txt, 2003.

[6] R. Deng, et al., "Defending Against Attacks in Mobile IP," Proc. of ACM CCS '02, pp.59-67, 2002.

[7] D. Johnson and C. Perkins, "Mobility Support in IPv6," IETF, draft-mobileip-ipv6-16, 2002.

[8] T. Koskiahde, "Security in Mobile IPv6," Tampere University of Technology, 2002.

[9] S. Okazaki, et al., "Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)," draft-okazaki-mobileip-abk-01.txt, 2002.

[10] W. Dai, Crypto++ 4.0 Benchmarks, http://www.eskimo.com/~weidai/benchmarks.html, 2000.

원 유 석

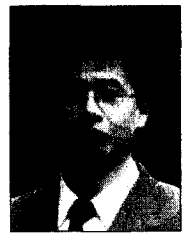
e-mail : server11@dankook.ac.kr

2000년 단국대학교 전산통계학과 학사

2002년 단국대학교 대학원 전산통계학과 이학석사

2002년~현재 단국대학교 대학원 박사과정

관심분야 : 네트워크 및 이동 통신 보안, 시뮬레이션, 에이전트



조 경 산

e-mail : kscho@dankook.ac.kr

1979년 서울대학교 전자공학과 학사

1981년 한국과학원 전기전자공학과 공학석사

1988년 Univ. of Texas at Austin 전기전산공학과 Ph.D.

1988년~1990년 삼성전자 컴퓨터부문 책임연구원, 실장

1990년~현재 단국대학교 정보컴퓨터학부 교수

관심분야 : 네트워크 시스템 및 이동 통신 보안, 웹 응용, 컴퓨터 시스템