이동 IPv6의 확장된 경로 최적화 프로토콜에 대한 형식화된 보안 분석

유일선* · 김흥준**

A Formal Security Analysis on the Enhanced Route Optimization Protocol for Mobile IPv6

Il-sun You* · Heung-jun Kim**

요 약

최근에 Mobile IPv6(MIPv6)의 경로 최적화 옵션을 보호하기 위한 표준안으로 ERO 프로토콜이 채택되었다. 이 프로토콜은 강력한 공개키 암호화 기법을 기반으로 기존의 RR 프로토콜을 개선하고 성능과 보안성을 최적화 하였다. 한편, ERO 프로토콜을 포함하여 다양한 MIPv6 보안 프로토콜들이 제안되었으나 이들에 대한 형식화된 보안 분석이 부족한 실정이다. 일부연구에서 형식화된 보안 분석이 시도되었으나 분석의 대상이 되었던 보안 프로토콜들은 초창기에 제안된 비교적 단순한 프로토콜들이었다. 본 논문에서는 MIPv6 보안 프로토콜들을 위한 형식화된 보안 분석의 기준을 제시하기 위해 BAN 논리를 채택하여 ERO 프로토콜의 유효성을 검증한다. 이를 위해 MIPv6 환경을 고려하여 이동노드의 *HoA*와 *CoA*에 대한 주소 테스트를 검증에 반영하도록 BAN 논리를 확장하였다. 본 논문에서 제시된 분석 방법은 향후 MIPv6 관련 보안 프로토콜의 형식화된 분석을 위해 유용하게 활용될 것으로 기대된다.

ABSTRACT

Recently, the ERO protocol has been adopted as a standard to protect the routing optimization mode introduced by MIPv6. This protocol uses the public key cryptography and the early binding update method to improve the Return Routeability protocol while optimizing both security and performance. On the other hand, though various security approaches including the ERO protocol have been proposed for MIPv6, they lack formal verification. Especially, to our best knowledge, there is no formal analysis on the ERO protocol. In order to provide a good example for formal analysis on MIPv6 security protocols, this paper verifies the correctness of the ERO protocol through BAN-logic. For this goal, BAN-logic is extended to consider the address tests on the mobile nodes's *CoA* and *HoA*. It is expected that the analysis presented in this paper will be useful for the formal verifications on the security protocols related to MIPv6.

키워드

Mobile IPv6, Enhanced Route Protocol, CGA, BAN-logic

* 한국성서대학교 정보과학부 조교수

** 진주산업대학교 컴퓨터공학부 부교수(교신저자)

접수일자 2009. 01. 19

Ⅰ. 서 론

정보통신의 발달과 모바일 컴퓨팅 기술의 확산으로 인해 컴퓨팅 장치들을 위한 이동성 지원이 매우 중요하게 인식되고 있다. MIPv6(Mobile IP Version 6)는 인터넷의 이동성 관리를 지원하기 위한 표준기술로서 향후 이동 인터넷 시대를 주도할 것으로 기대된다[1].

MIPv6는 이동노드(*MN*: Mobile Node)와 대응노드(*CN*: Corresponding Node) 사이의 직접 통신을 위해 경로 최적화 옵션(RO: Route Optimization Mode)을 소개하였고, 이를 보호하기 위해 Return Routeability(RR) 프로토콜을 제안하였다[1]. RR 프로토콜은 이동노드의 *HoA* (Home Address: 홈네트워크에서 할당되는 주소로 이동노드의 지속적인 식별을 위한 주소)와 *CoA* (Care-of Address: 외부네트워크에서 할당되는 주소로 이동노드의 라우팅을 위한 주소)에 테스트 패킷을 전송하여 수신 여부를 확인함으로써 이동노드가 실제로 해당 주소에 위치하는지를 검증하는 주소테스트 기법을 기반으로 설계되었다. 그러나 RR 프로토콜은 암호화 기법을 사용하지 않고 주소 테스트 기법에 의존하기 때문에 방향전환 공격 (Redirection Attack) 등과 같은 다양한 공격에 취약하고, 잦은 바인딩 갱신 (Binding Update)으로 인한 성능의 저하를 초래하는 심각한 문제를 갖고 있다[2]. 이러한 문제를 해결하기 위해 공개키 기반의 바인딩 갱신 보안 프로토콜이 제안되었다[2-6]. 특히, 2007년에 Arkko와 Vogt, Haddad가 제안한 Enhanced Route Optimization (ERO) 프로토콜은 Internet Engineering Task Force(IETF)에 의해 RR 프로토콜을 대체할 수 있는 표준안으로 채택되었다[6]. ERO 프로토콜은 Cryptographically Generated Addresses(CGA) 기법을 적용하여 광역의 보안 인프라가 불가능한 MIPv6 환경에서 공개키 암호화와 전자서명을 안전하게 사용할 수 있도록 설계되었고[7], 이른 바인딩 갱신 기법 (Early Binding Update)을 통해 효율성을 극대화 하였다.

한편, ERO 프로토콜을 포함하여 다양한 공개키 기반의 MIPv6 보안 프로토콜들이 제안되었으나 이들에 대한 체계적이고 형식화된 보안 분석이 부족한 실정이다. 비록 [3]과 [8]에서 BAN 논리(BAN logic)를 활용하여 형식화된 보안 분석을 시도하였으나 분석의 대상이 되었던 보안 프로토콜들은 초창기에 제안된 비교적 단순한 프로토콜들이었다[3][8][9]. 또한, 이들은 BAN 논리의 단순 적용으로 인해 이동노드의 *HoA*와 *CoA*에 대한 주소 테스트를 분석에 반영하지 못하였다.

본 논문에서는 MIPv6 보안 프로토콜들을 위한 형식화된 분석의 기준을 제시하기 위해 BAN 논리를 적용하여 최근에 표준으로 채택된 공개키 기반의 ERO 프로토콜에 대한 유효성 검증을 하고자 한다. 특히, MIPv6 환경을 고려하여 이동노드의 주소 테스트를 분석에 반영할 수 있도록 BAN 논리를 확장한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 ERO 프로토콜을 기술하고, Ⅲ장에서는 ERO 프로토콜의 형식화된 보안 분석을 한다. Ⅳ장에서 향후 연구 제시와 함께 결론을 맺는다.

Ⅱ. 확장된 경로 최적화 프로토콜

ERO 프로토콜은 첫 바인딩 갱신에서 공개키 암호화 기법을 활용하여 이동노드와 대응노드 사이에 강력한 장기비밀(long-term secret)을 교환하고, 이후의 과정에서 이 비밀을 바탕으로 보안성과 효율성을 극대화 하였다. 또한, 이른 바인딩 갱신 기법을 적용하여 바인딩 갱신 메시지 교환과 데이터 전송이 동시에 수행되도록 함으로써 바인딩 갱신 지연을 최소화 하였다.

ERO 프로토콜은 장기비밀을 교환하는 초기단계와 이후의 과정인 후속단계로 나눌 수 있으며, 본 장에서는 이 두 단계를 중심으로 ERO 프로토콜을 기술한다.

1. 기호

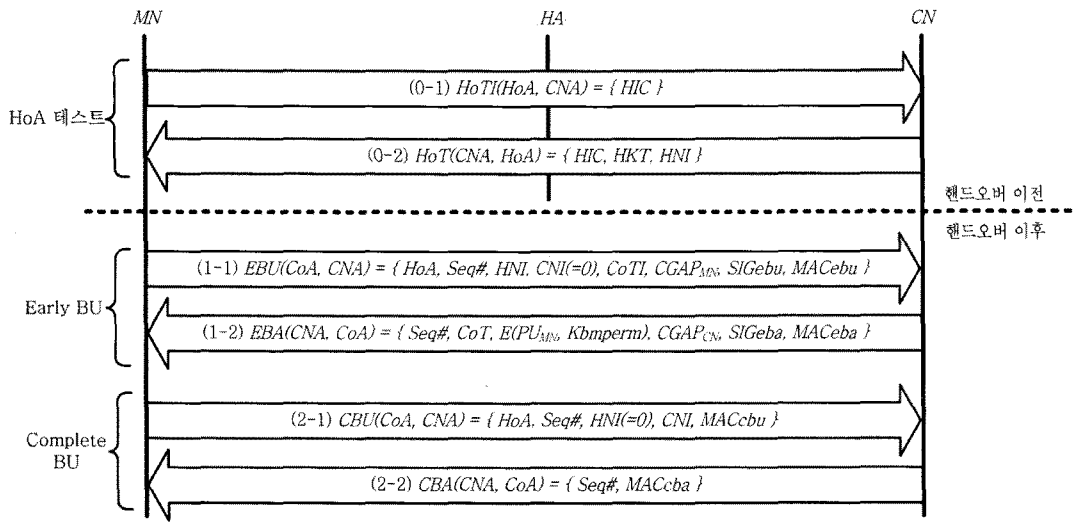
- *Msg(SA, DA):* 프로토콜 메시지를 나타내며 *Msg*는 메시지의 이름이고 *SA*는 메시지의 송신자 주소, *DA*는 수신자 주소를 나타냄
- *H(msg): msg*의 해쉬값을 계산하는 일방향 해쉬함수를 의미함
- *HMAC(k, msg):* 대칭키 k를 통해 msg의 HMAC 값을 계산하는 HMAC 함수를 의미함
- |: 메시지 결합 연산자, ^ : 배타적 논리합 연산자
- *MN:* 이동노드, HA: 홈에이전트, CN: 대응노드 (이후로부터 이 기호들을 주로 사용할 예정임)
- *CNA:* 대응노드의 주소, *HAA:* 홈에이전트의 주소
- *CNI:* Care-of nonce index, *HNI:* Home nonce index
- *CKT:* Care-of keygen token

- *HKT:* Home keygen token
- *CIC:* Care-of init cookie, *HIC:* Home init cookie
- *First(n,m):* 메시지 m의 첫 번째 n비트
- *PUX : X*의 공개키, *PRX : X*의 개인키
- *E(K, M):* 키 *K*로 메시지 *M*을 암호화 함
- *S(K, M):* 키 *K*로 메시지 *M*을 전자서명 함

2. 초기단계

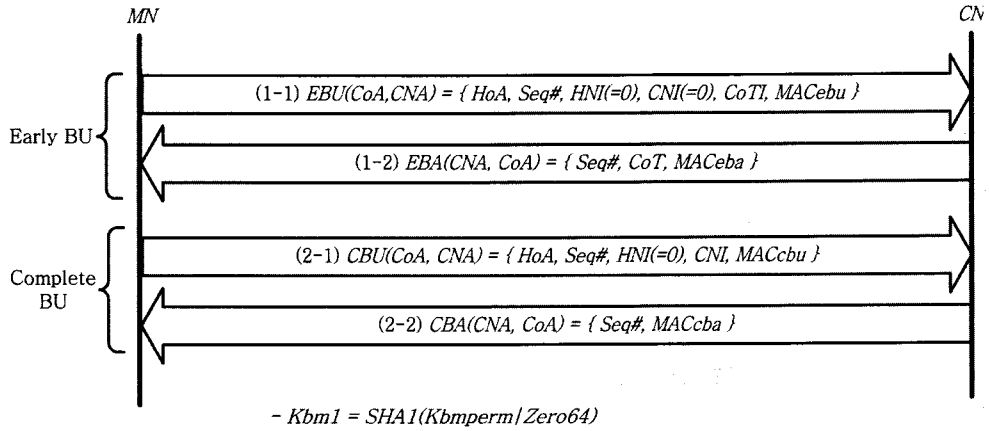
ERO 프로토콜의 초기단계는 그림 1과 같이 HoA 테스트와 Early BU, Complete BU 과정으로 구성되며, 주요 목적은 MN과 CN 사이의 장기비밀인 Kbmperm을 교환하는 것이다.

MN은 핸드오버(hand over) 이전에 CN과 HoTI와 HoT를 교환함으로써 HoA 테스트 과정을 수행한다. 이 과정은 MN이 HoA에 존재하는지를 확인하기 위한 주소 테스트 과정으로서 핸드오버 이전에 발생하기 때문에 바인딩 갱신 지연에 영향을 주지 않는다. 이 과정을 수행하면 MN은 HoT 메시지에 포함된 HKT를 획득한다. MN이 다른 네트워크로 핸드오버를 하게 되면 Early BU 과정을 수행한다. 특히, EBU 메시지는 MN의 전자서명과 함께 Kbm1(HKT로부터 파생됨)을 통해 계산된 MACebu를 포함하는데 이 값은 CN이 서비스 거부 공격에 취약하지 않도록 하고 MN이 HoA에 존재함을 확인시켜 주는 기능을 제공한다. 이 과정을 통해 MN과 CN은 장기비밀인 Kbmperm을 교환하며, 이른 바인딩 갱신 기법을 적용하여 MN이 CoA에 존재함이 검증되지 않았음에도 불



- *Kbmperm: 초기단계에서 교환되는 장기비밀 (long-term secret)*
- *CoTI = { CIC }, CoT = { CIC, CKT, CNI }*
- *Kbm1 = SHA1(HKT|Zero64), Zero64는 64비트의 0으로 이루어진 값*
- *MACebu = First(96, HMAC_SHA1(Kbm1, CNA|CoA|EBU))*
- *MACeba = First(96, HMAC_SHA1(Kbm1, CNA|CoA|EBA))*
- *$CGAP_X$: X*의 CGA 기법 적용을 위한 매개변수
- *SIGebu = $S(PR_{MN}$, CNA|CoA|EBU)*
  *EBU*는 *EBU* 메시지에서 *MACebu* 부분을 *0*으로 처리한 것을 의미
- *SIGeba = $S(PR_{CN}$, CNA|CoA|EBA)*
  EBA 는 *EBA* 메시지에서 *MACeba* 부분을 *0*으로 처리한 것을 의미
- *Kbm2: SHA1(CKT|Kbmperm)*
- *MACcbu: First(96, HMAC_SHA1(Kbm2, CNA|CoA|CBU))*
- *MACcba: First(96, HMAC_SHA1(Kbm2, CNA|CoA|CBA))*

그림 1. ERO 프로토콜의 초기단계
Fig. 1 The initial phase of the ERO protocol



- *Kbm1 = SHA1(Kbmperm|Zero64)*
- *MACebu = First(96, HMAC_SHA1(Kbm1, CNA|CoA|EBU))*
- *MACeba = First(96, HMAC_SHA1(Kbm1, CNA|CoA|EBA))*
- *Kbm2: SHA1(CKT|Kbmperm)*
- *MACcbu: First(96, HMAC_SHA1(Kbm2, CNA|CoA|CBU))*
- *MACcba: First(96, HMAC_SHA1(Kbm2, CNA|CoA|CBA))*

그림 2. ERO 프로토콜의 후속단계
Fig. 2 The subsequent phase of the ERO protocol

구하고 데이터를 전송한다. 즉 MN은 EBU 메시지를 송신하면서 데이터를 함께 송신하고 CN은 EBA 메시지를 송신하면서 데이터를 함께 송신한다.

MN이 EBA 메시지를 수신하면 메시지에 포함된 CKT와 Kbmperm를 통해 Kbm2를 생성한다. 이후에 MN은 Kbm2에 의해 준비된 CBU 메시지를 전송함으로써 Complete BU 과정을 시작한다. CN이 CBU 메시지를 Kbm2에 의해 검증할 수 있다면 CN은 MN이 실제로 CoA에 존재한다는 것을 신뢰할 수 있다. 이 시점부터 CN과 MN은 안전한 상태에서 데이터를 전송할 수 있다.

3. 후속단계

초기단계 이후에 MN은 Kbmperm의 수명이 다하기 전까지 오직 핸드오버가 발생할 때만 바인딩 갱신을 수행한다. 이처럼 초기단계이후에 Kbmperm를 바탕으로 수행되는 모든 바인딩 갱신 과정을 후속단계라 부른다. 후속단계는 그림 2와 같이 Early BU와 Complete BU로 구성된다. 후속단계는 초기단계에서 이미 MN의 HoA를 검증했기 때문에 HoA 테스트 과정을 생략하였다. 따라서 MN이 Early BU에서 Kbm1을 소유하고 있음이 증명된다면 CN은 MN의 HoA가 유효하다고 신뢰한다. 후속단계의 Early BU와 Complete BU는 공개키 암호화 혹은 전자서명 부분을 제외하고 초기단계와 유사하다. 즉 Early BU 과정에서 EBU와 EBA 메시지는 MN과 CN의 전자서명 대신에 Kbm1(Kbmperm로부터 파생됨)에 의해 계산된 MAC 값에 의해서 보호된다. 또한, Kbmperm의 교환과정이 생략된다. 따라서 후속단계에서는 Kbmperm을 바탕으로 공개키 연산 없이 경량의 연산들로 메시지를 보호하여 연산 오버헤드를 최적화하였다.

Ⅲ. 형식화된 보안 분석

본 장에서는 BAN 논리를 적용하여 ERO 프로토콜에 대한 유효성을 검증한다. 이를 위해 먼저 BAN 논리를 간략하게 소개한 후에 BAN 논리 기법에 따라 ERO 프로토콜의 초기단계와 후속단계를 검증하고 프로토콜의 보안성을 고찰한다. 특히, MN의 CoA와 HoA에 대한 주소 테스트를 분석과정에 반영하기 위해서 BAN 논리를 확장 적용한다.

1. BAN 논리

BAN 논리는 1989년에 Burrows와 Abadi 그리고 Needham에 의해서 제안되었다.

표1. BAN 논리의 기호
Table 1. Notations used in BAN-logic

기호	의미
$P \models X$	P는 X를 믿는다(believe).
$P \lhd X$	P는 X를 지금 보았다(see).
$P \vdash X$	P가 X를 언젠가 보냈다(once said).
$\#(P)$	P의 값이 최신이다(fresh).
$P \Longmapsto X$	P는 X에 대한 전권이 있다(jurisdiction).
$P \overset{K}{\longleftrightarrow} Q$	K는 P와 Q 사이에 공유된 안전한 키이다. (즉 P와 Q 에게만 알려진 키)
$\overset{K}{\rightarrow} P$	P와 K를 공개키로서 소유한다.
$P \overset{K}{\rightleftharpoons} Q$	K는 P와 Q 사이에 공유된 안전한 비밀이다. (즉 P와 Q 에게만 알려진 비밀)
$<X>_Y$	X는 비밀 Y 와 함께 조합되었다.

BAN 논리는 단순함과 견고함으로 인해 각종 보안 프로토콜의 형식화된 분석을 위해 가장 널리 사용되는 기법이 되었다[9]. 일반적으로 BAN 논리는 아래와 같은 프로토콜 검증절차를 갖는다.

① 프로토콜을 정규화(Idealized form) 함
② 프로토콜의 초기 상태에 대한 가정을 정의함
③ 의도하는 결과를 얻을 때까지 반복적으로 BAN 논리의 기본 공리들을 적용함.

BAN 논리에서 주로 사용되는 기호는 표 1과 같고, Message meaning 법칙(R1)과 Nonce Verification 법칙(R2), Jurisdiction 법칙(R3)과 같은 기본 공리는 (R1)-(R5)와 같다. 여기서 (R1)-(R3)은 Message meaning 법칙을 나타내고, (R4)는 Nonce verification 법칙, (R5)는 Jurisdiction 법칙을 나타낸다. 이외에도 자주 사용되는 공리는 (R6)-(R8)이다. BAN 논리에 대한 자세한 사항은 [9]를 참조하면 된다.

$$\frac{P \models \overset{K}{\leftrightarrow} Q,\ P \lhd \{X\}_K}{P \models Q \vdash X} \quad \text{(R0)}$$

$$\frac{P \models \overset{K}{\rightarrow} Q,\ P \lhd \{X\}_{K^{-1}}}{P \models Q \vdash X} \quad \text{(R2)}$$

$$\frac{P \models P \overset{K}{\rightleftharpoons} Q,\ P \lhd <X>_K}{P \models Q \vdash X} \quad \text{(R3)}$$

$$\frac{P \models \#\{X\},\ P \models Q \vdash X}{P \models Q \models X} \quad \text{(R4)}$$

$$\frac{P \models Q \Longmapsto X,\ P \models Q \models X}{P \models X} \quad \text{(R5)}$$

$$\frac{P \models \#(X)}{P \models \#(X, Y)} \quad \text{(R6)}$$

$$\frac{P \models (X, Y)}{P \models X} \quad \text{(R7)}$$

$$\frac{P \models Q \models (X, Y)}{P \models Q \models X} \quad \text{(R8)}$$

2. BAN 논리의 확장

기존의 BAN 논리에서는 MN이 BU 메시지를 통해 주장하는 위치에 실제로 존재하는지를 검증할 수 없다. 즉 MN의 주소를 테스트하기 위한 CoT나 HoT 메시지는 검증에 있어서 큰 영향을 끼치지 못한다. 본 논문에서는 MN의 주소 CoA나 HoA에 대한 테스트를 검증하기 위해서 특정노드가 특정주소에 존재함을 표현하는 기호 @를 추가하였다. 즉 MN이 Addr에 존재한다면 $MN@Addr$와 같이 표현할 수 있다.

3. 프로토콜 검증

본 절에서는 앞서 언급된 BAN 논리를 적용하여 ERO 프로토콜의 초기단계와 후속단계의 유효성을 검증한다. 이를 위해 초기단계와 후속단계는 BAN 논리의 절차에 따라 정규화 되고, 각 단계의 초기상태에 대한 가정이 정의된다. 이후에 BAN 논리의 기본 공리를 적용함으로써 형식화된 분석이 진행된다.

가. 초기단계

ERO 프로토콜의 초기단계는 다음과 같이 정규화 된다. 여기서 HoT와 HoTI는 이후의 BAN 논리 검증 절차에 영향을 끼치지 않기 때문에 생략하였다.

(1) $MN \rightarrow CN: \{H(EBU,\ MN@HoA)\}_{PR_{MN}}$
(2) $CN \rightarrow MN: \{H(EBA)\}_{PR_{CN}}$
$where\ EBA includes (CoT, \{Kbmperm\}_{PU_{MN}})$
(3) $MN \rightarrow CN: < CBU,\ MN@CoA) >_{Kbm2}$
(4) $CN \rightarrow MN: < CBA >_{Kbm2}$

단계 (1)을 보면 MN이 HoA에 존재하는 것을 의미하는 $MN@HoA$가 추가되었다. 즉 CN이 EBU 메시지에 첨부된 전자서명을 검증하는 과정에서 서비스 거부 공격을 예방하기 위해 추가된 MACebu는 HKT(MN의 HoA에서 수신함)에 의해 계산되기 때문에 전자서명이 유효하다는 의미는 EBU 메시지를 신뢰할 수 있을 뿐만 아니라 MN이 실제 HoA에 존재한다는 것을 나타낸다. 이와 유사하게, 단계 (3)에서는 MN이 CoA에 존재함을 의미하는 $MN@CoA$가 추가되었다. 즉, CBU를 보호하기 위해 추가된 MACcbu는 Kbmperm과 함께 CTK(MN이 CoA에서 수신함)로부터 파생된 Kbm2에 의해 계산되기 때문에 CBU가 유효하다는 것은 메시지 자체에 대한 신뢰성 이외에 MN이 CoA에 존재한다는 것을 암시한다.
초기단계에 대한 가정은 다음과 같다.

$(A1)\ MN \models \#(Seq)$

$(A2)\ MN \models CN \Rightarrow Kbmperm$

$(A3)\ MN \models \xrightarrow{PU_{CN}} CN$

$(A4)\ CN \models \#(Seq)$

$(A5)\ CN \models \xrightarrow{PU_{MN}} MN$

$(A6)\ CN \models MN \overset{Kbmperm}{\rightleftharpoons} CN$

엄밀히 말하자면 CGA에 의해 증명되는 MN의 PU_{MN}을 BAN 논리를 통해 증명할 수 없기 때문에 (A3)와 (A5)를 추가하였다. 초기단계는 앞서 주어진 정규화 형태와 가정을 바탕으로 다음과 같이 검증된다.

단계 (1)은 (A6)와 (R2)에 의해 식(1)과 같이 유도될 수 있다.

$$CN \models MN \vdash (EBU,\ MN@HoA) \quad (1)$$

여기서 EBU는 Seq#을 포함하기 때문에 (A4)와 (R6)에 의해서 식(2)를 구할 수 있다.

$$CN \models \#(EBU,\ MN@HoA) \quad (2)$$

식(1)과 식(2) 그리고 (R4)를 적용하면 식(3)을 유도할 수 있다.

$$CN \models MN \models (EBU,\ MN@HoA) \quad (3)$$

결과적으로 식(3)과 (R8)에 의해 식(4)와 식(5)를 얻을 수 있고 이들을 통해 CN은 EBU 메시지 자체와 MN이 HoA에 존재한다는 사실을 신뢰할 수 있다.

$$CN \models MN \models EBU \quad (4)$$
$$CN \models MN \models MN@HoA \quad (5)$$

단계 (2)는 단계 (1)과 유사하게 (A3)와 (R2), 그리고 (A1)과 (R6)을 차례로 적용한 후, (R4)를 적용하여 식(6)으로 유도될 수 있다.

$$MN \models CN \models EBA \quad (6)$$

또한, 식(6)과 (R8)에 의해 파생된 식(7)을 통해 식(8)을 유도할 수 있다.

$$MN \models CN \models \{MN \overset{Kbmperm}{\rightleftharpoons} CN\}_{PU_{MN}} \quad (7)$$

$$MN \models CN \models MN \overset{Kbmperm}{\rightleftharpoons} CN \quad (8)$$

결과적으로 식(8)에 (A2)와 (R5)를 적용하면 식(9)를 유도할 수 있다.

$$MN \models MN \overset{Kbmperm}{\rightleftharpoons} CN \quad (9)$$

식(9)를 통해서 MN은 Kbmperm이 오직 자신과 CN에게만 알려진 안전한 비밀이라는 것을 신뢰할 수 있으며 따라서 후속단계를 포함한 이후의 과정에서 더 이상 공개키 기반의 키 교환 없이 바인딩 갱신을 효과적으로 할 수 있는 근거를 확보하게 된다.

MN과 CN은 식(9)와 (A6)를 바탕으로 Kbmperm과 CKT에서 파생된 Kbm2를 안전한 비밀로서 신뢰할 수 있

다. 이를 바탕으로 단계 (3)은 (R3) 및 (A4)와 (R6), (R4)를 적용하여 식(10)과 같이 유도될 수 있다.

$$CN \models MN \models (CBU, MN@CoA) \quad (10)$$

따라서 (R8)에 의해 식(11)과 식(12)를 구할 수 있다.

$$CN \models MN \models CBU \quad (11)$$
$$CN \models MN \models MN@CoA \quad (12)$$

특히, 식(12)에 의해 CN은 MN이 CoA에 존재함을 신뢰할 수 있게 된다.

단계 (4)는 단계 (3)과 유사하게 (R3) 및 (A1)과 (R6), (R4)에 의해 식(13)과 같이 유도된다.

$$MN \models CN \models CBA \quad (13)$$

이제까지의 검증과정을 볼 때 CN의 입장에서는 식(4)와 식(11)을 통해 EBU와 CBU 메시지를 신뢰할 수 있고 또한 식(5)와 식(12)를 근거로 MN이 HoA와 CoA에 실제로 존재하는 것을 믿을 수 있다. 한편, MN의 입장에서는 식(6)와 식(13)을 통해 자신이 전송한 바인딩 갱신메시지가 CN에 의해 수락되었음을 확인 할 수 있고 아울러서 식(9)를 통해 Kbmperm이 이후의 과정에서 적용할 수 있는 안전한 비밀이라는 것을 신뢰할 수 있다. 이처럼 ERO의 초기단계는 BAN 논리에 의해 유효하다는 것을 증명할 수 있다.

나. 후속단계

ERO 프로토콜의 후속단계는 다음과 같이 정규화 될 수 있다.

$(1) MN \rightarrow CN: < EBU,\ MN@HoA >_{Kbm1}$
$(2) CN \rightarrow MN: < EBA >_{Kbm1}$
$\quad where\ EBA includes\ CoT$
$(3) MN \rightarrow CN: < CBU,\ MN@CoA) >_{Kbm2}$
$(4) CN \rightarrow MN: < CBA >_{Kbm2}$

특히, CN은 이미 초기단계에서 MN이 HoA에 존재하는 것을 검증했기 때문에 MN이 Kbm1을 안다고 증명할 수 있다면 MN이 주장하는 HoA를 신뢰할 수 있다. 따라서 단계 (1)에서 $MN@HoA$을 추가하였다.

후속단계에 대한 가정은 다음과 같다.

$(B1)\ MN \models \#(Seq)$
$(B2)\ MN \models MN \overset{Kbmperm}{\rightleftharpoons} CN$
$(B3)\ MN \models MN \overset{Kbm1}{\rightleftharpoons} CN$
$(B4)\ CN \models \#(Seq)$
$(B5)\ CN \models MN \overset{Kbmperm}{\rightleftharpoons} CN$
$(B6)\ CN \models MN \overset{Kbm1}{\rightleftharpoons} CN$
$(B7)\ CN \models CKT$

후속단계는 앞서 주어진 정규화된 형태와 가정을 갖고 다음과 같이 분석된다.

단계 (1)은 (B6)와 (R3) 그리고 (B4)와 (R6)를 적용한 후에 (R4)에 의해서 식(14)와 같이 유도될 수 있다.

$$CN \models MN \models (EBU, MN@HoA) \quad (14)$$

즉 CN은 식(14)에 의해서 EBU 메시지를 신뢰할 수 있을 뿐 아니라 MN이 HoA에 존재함을 믿을 수 있다. 그러나 이 시점에서 CN은 MN이 CoA에 존재함을 믿을 수 없다. 단계 (2)는 (B3)와 (R3) 그리고 (B1)과 (R6)의 적용후, (R4)에 의해서 식(15)와 같이 유도될 수 있다.

$$MN \models CN \models EBA \quad (15)$$

식(15)에 의해서 MN은 EBA 메시지를 신뢰하기 때문에 (R8)을 적용하여 EBA 메시지에 포함된 CKT를 신뢰할 수 있다. 또한 (B2)에 명시된 것처럼 MN은 초기단계에서 CN과 공유한 Kbmperm을 믿는다. 따라서 이들 두 값에 의해서 파생된 Kbm2에 대해 식(16)이 유도될 수 있고 이와 유사하게 (B7)과 (B5)에 의해서 식(17)이 유도될 수 있다.

$$MN \models MN \overset{Kbm2}{\rightleftharpoons} CN \quad (16)$$

$$CN \models MN \overset{Kbm2}{\rightleftharpoons} CN \quad (17)$$

단계 (3)은 식(17)과 (R3) 그리고 (B4)와 (R6)를 적용한 후에 (R4)를 적용하여 식(18)로 유도될 수 있다.

$$CN \models MN \models (CBU, MN@CoA) \quad (18)$$

식(18)에 의해 CN은 CBU 메시지의 유효성과 함께 MN이 실제로 CoA에 존재한다는 사실을 신뢰할 수 있다. 단계 (4)는 식(16)과 (R3) 그리고 (B1)과 (R6)의 적용 후, (R4)에 의해서 식(19)와 같이 유도될 수 있다.

$$MN \models CN \models CBA \quad (19)$$

이제까지의 검증과정을 종합해 보면 CN의 측면에서 식(14)와 식(18)을 통해 MN의 바인딩 갱신을 믿을 수 있고, MN의 측면에서는 식(15)와 식(19)를 통해 CN이 자신이 요청한 바인딩 갱신을 수용하였음을 믿을 수 있다. 따라서 ERO의 후속단계는 BAN 논리에 의해 유효하다고 볼 수 있다.

다. 성능과 보안성 사이의 상반된 관계

앞 절에서 언급된 것처럼 ERO 프로토콜은 BAN 논리 기반의 형식화된 분석을 통해 유효하다는 것이 검증되었다. 그러나 프로토콜이 유효한 시점에 주목할 필요가 있다. 즉 초기단계나 후속단계에서 실제로 CN이 MN의 바인딩 갱신을 신뢰할 수 있는 시점은 CBU 메시지를 받는 시점이다. 그러나 ERO 프로토콜은 성능의 극대화를 위해 바인딩 갱신과 데이터 전송을 동시에 수행하기 때문에 CN이 CBU 메시지를 받는 시점이 아닌 EBU 메시지를 받는 시점에서 데이터 송수신을 시작한다. 결국, CN은 식(3)과 식(14)에서 의미하는 MN의 HoA에 대한 믿음만을 갖기 때문에 CBU 메시지를 수신하기 전까지는 방향전환 공격 등에 취약할 수 있다.

본 절에서는 이러한 상황을 표 2에서 제시된 ERO 프로토콜의 시점기호를 활용하여 분석하고자 한다. MN이 CN에게 데이터를 전송하기 시작할 때까지 기다려야 하는 지연시간 $LSend(MN)$은 t1과 같고 CN으로부터 데이터를 수신할 때가지 기다려야 하는 지연시간 $LRecv(MN)$은 t3라고 할 수 있다. 그러나 CN이 MN의 데이터를 수신 하는 시점 t2 (이 시점은 EBU 메시지를 받는 시점과 같음)와 MN이 데이터를 수신하는 시점 t3에서 CN이 갖는 MN에 대한 신뢰는 $CN \models MN \models (EBU, MN@HoA)$와 같다. 즉 CN은 MN이 실제로 CoA에 존재하는지에 대한 확신 없이 데이터 송수신을 시작한다. 이러한 안전하지 않은 상태는 CN이 MN으로부터 CBU 메시지를 수신한 시점 t5까지 계속된다. 만일 보안을 강화하고 이른 바인딩 갱신 기법을 사용하지 않는다면 CN은 MN이 HoA와 CoA에서 실제 존재하는지를 확인하는 시점 t5에서 메시지의 송수신을 시작하기 때문에 $LSend(MN)$와 $LRecv(MN)$의 값은 각각 t4와 t6임을 알 수 있다. 즉 보안성을 강화한다면 $LSend(MN)$은 (t4-t1)시간, $LRecv(MN)$은 (t6-t3)시간 만큼 늘어나는 것을 알 수 있다. 이러한 특성은 ERO 프로토콜이 상황에 따라 보안과 성능사이의 균형을 이루도록 개선할 수 있는 여지를 남긴다.

표 2. ERO 프로토콜의 시점 기호
Table 2. Time notations of the ERO protocol

기호	의미
t1	MN이 EBU 메시지를 전송하기 시작한 시간
t2	CN이 EBU 메시지를 수신완료하고 EBA 메시지를 전송하기 시작한 시간
t3	MN이 EBA 메시지를 수신 완료한 시간
t4	MN이 CBU 메시지를 전송하기 시작한 시간
t5	CN이 CBU 메시지를 수신완료하고 CBA 메시지를 전송하기 시작한 시간
t6	MN이 CBA 메시지를 수신 완료한 시간

Ⅳ. 결 론

본 논문에서는 BAN 논리를 적용하여 ERO 프로토콜에 대한 형식화된 분석을 하였다. 형식화된 분석에 의하면 ERO 프로토콜의 초기단계와 후속단계가 유효하다는 것을 알 수 있었다. 그러나 이 프로토콜이 최종적으로 유효한 시점이 대응노드가 CBU 메시지를 받는 순간임에도 불구하고 그 이전에 이동노드의 CoA에 대한 신뢰 없이 데이터가 전송되는 문제점이 있다. 이는 핸드오버 지연을 최소하기 위해 이른 바인딩 갱신 기법을 적용하였기 때문에 발생한 문제로 전형적인 보안과 성능의 상반된 관계를 보여준다.

본 논문에서 제시된 분석방법은 다양한 MIPv6 관련 보안 프로토콜을 위한 형식화된 분석에 유용하게 활용될 것으로 기대된다. 향후연구로 ERO 프로토콜에서 이동노드의 주어진 상황에 따라 데이터 전송의 시점을 유연하게 조정하여 성능과 보안성의 합리적인 균형을 제공하는 방법에 대한 연구가 요구된다.

참고문헌

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

[2] R. Deng, J. Zhou, and F. Bao, "Defending Against Redirect attacks in Mobile IP," Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov., 2002

[3] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM Computer Communications Review*, Vol. 31, No. 2, April, 2001.

[4] Ilsun You, "Improving the Kang-Park's Protocol for Securing Binding Update in MIPv6," Journal of The Institue of Electronics Enginners of Korea, Vol. 44-TC, No. 10 pp.148-155, Oct., 2007

[5] Ilsun You and Sung Kyo Choi, "An Improvement of Mobile IPv6 Binding Update Protocol Using Address Based Keys," Journal of The Institue of Electronics Enginners of Korea, Vol. 42-CI, No. 5 pp.21-30, Sep., 2005

[6] J. Arkko, C. Vogt and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," *IETF RFC 4866*, May, 2007.

[7] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, March 2005

[8] J. Li , J. Huai, Q. Li and X. Li, "Towards Security Analysis to Binding Update Protocol in Mobile IPv6 with Formal Method," *Springer-Verlag LNCS*, Vol. 3794, pp. 1073-1080, December, 2005.

[9] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication," ACM Trans. Computer Systems, Vol. 1, pp. 18-36, 1990.

저자소개

유일선(Ilsun You)

1995년 단국대학교 전산통계학과 학사
1997년 단국대학교 전산통계학과 석사
2002년 단국대학교 전산통계학과 박사
2005년~현재 한국성서대학교 정보과학부 조교수
관심분야 : MIPv6, 인터넷 보안, 접근통제

김흥준(Heung-Jun Kim)

1989년 단국대학교 전자계산학과 졸업(학사)
1993년 단국대학교 대학원 전산통계학과 (석사)
1999년 단국대학교 대학원 전산통계학과 (박사)
1999년~현재 진주산업대학교 컴퓨터공학부 부교수
관심분야 : 컴퓨터구성, 모바일 네트워킹, P2P