AAA시스템의 티켓을 이용한 모바일 노드의 안전한 바인딩 업데이트에 관한 연구

강서일*, 이임영

순천향대학교 컴퓨터학부

A Study on Secure Binding Update of Mobile Node Using a Ticket in AAA system

Seo-Il Kang*, Im-Yeong Lee

Division of Computer, SoonchunHyang University.

요 약

유비쿼터스 사회가 다가옴으로써 많은 모바일 단말기를 사용자들이 이용하게 될 것이다. 이러한 환경에서는 모바일 단말기에 IPv6의 주소가 할당될 것이고, 외부로 이동한 단말기가 지속적인 서비스를 제공 받기 위해서 홈 네크워크에 자신의 이동 IP 주소를 바인딩 업데이트를 통해서 제공할 것이다. 그러나 공개되어 있는 네트워크에서 바인딩 업데이트의 수정을 통해서 서비스를 받지 못하게 하거나 DoS공격을 받을 수 있게 할 수 있다. 그러므로 본 제안 방식에서는 AAA시스템을 통해 티켓을 발급 받은 사용자가 안전하게 바인딩 업데이트를 할 수 있는 방안에 대하여 제시한다. 홈 네트워크의 AAA 서버가 티켓을 발급하고 외부 네트워크를 통해서 접근하는 모바일 노드의 바인딩 업데이트의 정보를 인증하여 안전한 서비스를 제공받도록 한다.

I. 서론

유비쿼터스 환경에서는 많은 사용자들이 모바일 단말기를 활용하게 된다. 현재의 IPv4의 주소는 모든 모바일 단말기에 주소를 부여할 수 있도록 충분하지 않다. 그러므로 IPv6의 주소 체계를 이용하게 될 것이며, 이와 같은 환경에서는 이동성을 제공하기 위해서 자신의 홈 네트워크의 이동한 외부 IP주소를 알리게 될 것이다. 그 과정을 보면 모바일 노드는 자신의 홈네트워크에서 CN(Correspondent Node)으로부터 데이터를 제공받으며 외부 네트워크로 이동하면 외부 네트워크은 이동한 모바일 노드에 CoA(care of address)를 할당한다. 그럼 모바일 노드는 할당 받은 CoA를 BU(Binding Update)를 통해서 CoA를 HA(home agent)와 CN에 알린다. 그리고 나서 CN 및 HA는 CoA로 바인딩 캐시를 갱신 후 모바일 노드에 바인딩 업데이트 확인 메시지를 보냄으로써 동작이 완료되게 된다. 이러한 일련의 동작을 통해서 외부에 이동한 모바일 노드에 지속적인 서비스를 제공할 수 있다. 본 논문에서는 바인딩 업데이트 메시지와 CoA가 조작되는 경우의 취약점을 확인하고 모바일 노드가 안전한게 바인딩 업데이트를 할 수 있는 방안을 제시한다. 2장에서는 보안 사항에 대하여 알아보고, 3장에서는 기존의 연구에 대하여 조사를 하고 4장에서 제안 방식을 설명한다. 그리고 5장에서는 제안 방식을 분석하며 6장에서 결론 및 향후 연구에 대하여 논의한다.

II. 보안 요구 사항

모바일 노드의 이동에 따른 주소 변경은 필수적이며, 바인딩 업데이트에서 메시지가 조작하여 공격할 수 있는 사항에 대하여 알아본다.

바인딩 업데이트의 메시지를 조작하여 CoA를 변경하면 다음과 같은 공격이 가능할 것으로 사료된다.

- 서비스거부 공격 : 바인딩 업데이트의 메시지를 변경하여 단말기 노드에 임의 모든 메시지를 전송하도록 한다.
- CoA의 조작 : HA와 CN에 잘못된 CoA를 가지도록하여 정보의 전송을 막을 수 있다.
- BA(Binding Acknowledgement)의 전송 : 공격자가 BA를 먼저 모바일 노드에 전송하여

BU의 메시지 전송을 차단한다.

이와 같은 공격은 메시지의 인증을 통해서 차단할 수 있다. 그러므로 본 제안 방식에서는 BU의 메시지의 인증 및 CoA를 검증할 수 있는 방안을 제시한다. 그러나 인증 메시지는 다음과 같은 보안 요구 사항을 만족해야 한다.

- 수정 및 조작 : 메시지를 수정 및 조작한 경우 알 수 있어야 한다.
- 임의 생성 : 메시지를 임의 생성하여 전송할 수 없어야 한다.

Ⅲ. 기존 연구

기존의 티켓을 이용하여 인증을 제공하는 방식에 대하여 연구를 한다. 다음의 연구 내용은모바일 노드의 외부 네트워크에서 홈 서버의 인증 및 인가를 제공하는 방식이다.

3.1 모바일 네트워크에서 티켓 기반의 AAA시스템

모바일 네트워크에서는 모바일 단말기가 이동하더라도 서비스를 제공하기 위해서 홈 네트워크의 홈 에이전트에 이동 네트워크 IP를 등록하여 서비스를 지속적으로 제공한다[2]. 이러한 경우 모바일 단말기에 대한 인증은 홈 인증 서버에서 제공하며, 이동에 따른 IP를 업데이트 하는 방안이 제시되어져 있다. 또한 홈 인증 서버에 매번 접근하기에 어렵기 때문에 중계 인증 서버를 제공하여 인증에 있어 효율성을 제공한다. 모바일 네트워크에서의 티켓 방식은 단말기의 식별자, 서비스 주소, 티켓의 유효 시간, 비밀 공유키를 포함하여 티켓을 구성하고 중계 서버에 제공함으로서 기존의 방식 보다 효율성을 제공할 수 있는 방안을 제시하고 있다. 또한 티켓은 외부 인증 서버가 사용하기 때문에 중계 서버까지의 오버헤드를 제공하지 않는다. 하지만 키 협상이나 보안 설정 방안은 기존의 방식을 그대로 활용하기 때문에 티켓을 제공하더라도 인가만 제공할 뿐 인증을 제공할 수는 없다. 그러므로 중계 서버 및 홈 인증 서버의 인증 단계가 필요하게 된다.

3.2 티켓을 이용한 AAA 시스템

티켓을 이용한 AAA시스템은 사용자가 홈 인증 서버에 자신의 정보를 등록하고, 홈 인증서버가 발급하는 티켓을 가지고 AP에 접근하여 사용한다. 티켓의 구성은 공개키 함수와 해쉬 함수를 이용하는 것으로써 디바이스의 인증을 제공하고 제공된 디바이스는 외부 네트워크의 AP로부터 티켓을 받아 검증하고 서비스를 제공받는다[1]. 각 단계는 인증, 인가, 키 등록 단계로 이루어져 있으며, 인증 이후 인가에서 티켓을 발급하도록 제안되어 있다. 다음은 각 단계에 대한 설명이다.

1) 인증 단계

디바이스는 자신의 아이디와 인증서를 서버의 공개키로 암호화 하여 다음과 같은 메시지를 제공한다.

$$Dev -> AS : UID, P_u, Certificate,$$
$$E_{as}(UID, sreq, h(\eta), nonce, Sign_u)$$

2) 인가 및 티켓 발행

서버는 무선 통신 관리자한테 디바이스의 아이디와 난수의 해쉬 값을 제공하면, 무선 통신 관리자는 티켓을 생성하여 각각의 AP로 전송한다. AP는 티켓의 메시지 내용을 브로드 캐스트하여 사용자의 단말기가 접근하였는지를 확인한다.

$$AS -> BM : UID, sreq, h(\eta)$$
$$BM -> PA_i : TK_r$$
$$PA_i\ broadcasts : TK_r$$

$$TK_r = D_{bm}(UID, ID_{channels}, h(\eta), T_1)$$

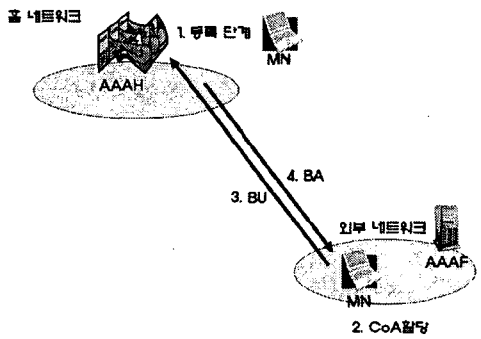
3) 키 등록 및 디바이스의 접근

사용자의 디바이스는 브로드 캐스트된 메시지의 내용을 확인하여 서비스를 제공 받기 위하여 자신이 가지고 있는 난수를 확인할 수 있도록 한다. 이때 난수가 틀리면 서비스를 제공 받지 못하게 된다. 이후 안전한 통신을 위해 키를 갱신하여 두 번째 티켓을 생성하게 된다. 연산은 다음과 같이 이루어진다.

$$PA_i\ broadcasts : P_{PA}, certificate$$
$$Dev -> PA_i : E_{PA_i}(UID, \eta, TK_r, nonce)$$
$$PA_i\ broadcasts : UID, ID_{channels}, TK_m, Sign_{PA_i}$$
$$TK_m = (k', T')$$

Ⅳ. 제안 방식

제안 방식은 모바일 노드의 홈 인증 서버의 등록 단계, 외부 네트워크에서의 CoA를 바인딩 업데이트 하는 단계, BA를 확인하는 단계로 이루어진다.



[그림 1] 제안 방식의 전체 흐름도

4.1 시스템 계수

본 제안 방식은 다음과 같은 시스템 계수를 활용한다.

- ID_* : 각각의 개체 아이디(*는 각각의 개체, MN : 모바일 노드, AAAH : 홈 인증 서버, AAAF : 외부 인증 서버)
- R_* : *가 생성하는 랜덤 수
- SK_* : *가 이용하는 세션키
- h() : 충돌성이 없는 안전한 일방향 해쉬 함수
- CoA : AAAF로부터 할당되는 IP
- S_No : 일련 번호

4.2 등록 단계

사용자는 AAAH에 자신의 모바일 단말기를 등록한다. 이때 모바일 단말기의 아이디(ID_{MN})와 세션키($SK_{MN-AAAF}$)를 생성하여 서로 비밀리에 공유하게 된다. 그리고 랜덤수(R_{MN})를 AAAH에 등록한다. AAAH는 티켓을 생성하여 모바일 단말기에 제공한다. 티켓을 다음과 같이 구성되어 진다.

$$Ticket = ID_{AAAH}, Sig_{AAAH}\mathrm{h}(\mathrm{ID_{MN}}||\mathrm{S\_No})$$

등록이 완료되면 모바일 단말기는 다음과 같은 정보를 획득하여 저장한다.

$$SK_{MN-AAAF}, Ticket, R_{MN}, S\_\mathrm{NO}$$

4.3 외부 네트워크의 이동

모바일 노드는 외부 네트워크에 이동하여 CoA를 할당 받기를 요구한다. 그럼 임시적으로 AAAF는 MN에 CoA를 할당하고 티켓을 전송 받는다. AAAF는 티켓을 가지고 AAAH의 서명을 확인한다. 이때 모바일 노드는 자신의 아이디와 S_NO를 제공하여 자신이 티켓의 정당한 소유자를 것을 검증할 수 있게 한다. 티켓의 정당한 소유자라는 것을 확인한 이후 CoA를 홈네트워크에 바인딩 업데이트 할 수 있게 한다. 바인딩 업데이트는 다음과 같이 이루어진다.

Step 1. 모바일 노드는 AAAH에 다음의 메시지를 전송한다.

$$ID_{MN}, E_{SK_{MN-AAAH}}[h(ID_{MN}||R_{MN}||CoA), CoA]$$

Step 2. AAAH는 외부 네트워크를 통해서 전송된 메시지를 받아 복호화하고 CoA를 검증한다.

$$h(ID_{MN}||R_{MN}||CoA) \stackrel{?}{=} h'(ID_{MN}||R_{MN}||CoA)$$

Step 3. Step2에서 검증되면 AAAH는 CoA를 등록하여 서비스를 제공할 수 있도록 한다.

4.4 AAAH의 세션키 갱신 및 티켓 재발급

AAAH는 바인딩 업데이트가 끝났다는 메시지와 동시에 티켓을 재발급하여 활용 할 수 있게 한다. 이때 초기에 등록한 모바일 노드의 난수가 없으므로 AAAH는 난수를 생성하여 제공한다. 순서는 다음과 같다.

Step 1. AAAH는 세션키를 다음과 같이 갱신하고 난수를 생성한다. 그리고 티켓을 재발급한다.

$$\neq wSK_{MN-AAAH} = SK_{MN-AAAH} \oplus R_{MN}$$
$$R_{AAAH}, \neq wS_{NO}$$
$$\neq wTicket = ID_{AAAH}Sig_{AAAH}[h(ID_{MN}|| \neq wS\_\mathrm{NO})]$$

Step 2. AAAH는 새로운 세션키로 각각의 데이터를 암호화하여 전송한다.

$$ID_{AAAH}, E_{\neq wSK_{MN-AAAH}}[Ticket, R_{AAAH}, \neq wS\_\mathrm{NO}]$$

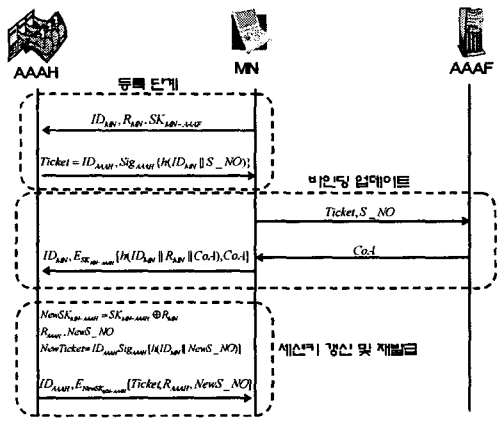
Step 3. 모바일 노드는 자신의 가지고 있는 난수로 새로운 세션키를 생성하여 전송되어져 온 메시지를 복호화하여 Ticket을 검증한다. 이후에는 새로운 티켓과 랜

덤수를 이용하여 다른 외부 네트워크로 이동하더라도 안전하게 바인딩 업데이트를 할 수 있다.

V. 제안 방식 분석

제안 방식을 2장에서 언급한 보안 요구 사항으로 분석하면 다음과 같다.

- 서비스 거부 공격, CoA조작, BA조작 : 메시지를 조작하기 위해서는 해쉬값으로 제공되는 값($h(ID_{MN}||R_{MN}||CoA)$)을 변경하여야 한다. 또한 세션키($SK_{MN-AAAF}$)를 알아야만 통신을 할 수 있다. 그러므로 바인딩 업데이트 메시지는 안전하다.
- 수정 및 조작 : 메시지를 수정하려면 AAAH의 서명을 위조할 수 있어야 한다. 이는 개인키를 알아내는 것으로 어렵다. 또한 난수(R_*)를 생성 삽입하여 각각의 메시지는 한번밖에 못 사용한다. 그러므로 임의 수정 및 조작을 할 수 없다.
- 임의 생성 : 메시지를 임의로 생성하려면 생성 인자를 모두 위조해야 한다. 임의 랜덤수를 생성할 수 있고 아이디는 공개되어 있다고 하나 CoA를 변경하면 데이터의 임의 생성을 알 수 있게 된다. 그러므로 바인딩의 업데이트는 안전하게 이루어진다.
- 사용자 인증 : 외부 네트워크에서 사용자 인증에 Ticket를 이용하여 홈 인증 서버의 인증을 받은 것을 검증 할 수 있다.



[그림 2] 단계의 흐름도

VI. 결론 및 향후 연구

본 제안 방식은 모바일 노드의 이동에 따른 CoA를 안전하게 갱신하는 방안을 제시하였다. 기존의 IPv6에서는 IPsec을 지원하나 보안 협상 및 이동성에 따른 잦은 CoA를 빠르게 지원하기 어렵다. 하지만 본 제안 방식에서는 사전 등록을 통해서 티켓으로 사용자의 인증을 제공하고 대칭키만을 이용하기 때문에 안전하게 보안을 제공할 수 있다. 또한 해쉬와 인증서버의 공개키를 이용하여 티켓을 제공하고 메시지의 무결성을 제공하여 5장에서 분석한 것처럼 보안 요구 사항을 만족시키고 있다. 향후 사용자가 많은 모바일 디바이스를 등록하는 경우 제안방식에서는 AAAH의 연산의 증가할 수 있다. 이러한 증가는 외부에 나가있는 모바일 노드가 이동에서도 안전한 인증을 제공 받기 위해서다. 그러나 이러한 방식은 홈 인증 서버의 오버헤드가 증가할 수 있으므로 홈 인증 서버의 오버헤드를 줄이는 방안이 필요하다. 또한 키 사용에 따른 관리적인 측면도 필요성이 증가하게 될 것이다.

[참고문헌]

[1] Yihong Zhou, Dapeng Wu and Scott M. Nettles, " On the Architecture of Authentication, Authorization, and Accounting for Real-Time Secondary Market Services," International Journal of Wireless and mobile computing, Jan, 2005

[2] Jung-Min Park, Eun-Hui Bae, Hye-Jin Pyeon, Kijoon Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network," ICCSA2003,pp.210-219

[3] 이효성, 김기천, 김인수 "Mobile 환경에서의 AAA 지역 등록 인증 개선 방안", 한국정보처리학회 2004년 추계학술대회, pp1267-1270

[4] 진봉재, 허의남, 문영성, "IEEE802.11 무선랜 기반의 Mobile IPv6 AAA환경세서 핸드오버 최적화 방안 연구", 한국정보처리학회 2004년 추계학술대회, pp1201-1204

[5] "AAA Authorization Application Examples", RFC 2905

[6] "AAA Authorization Framework", RFC 2904

[7] "Remote Authentication dial In User Service(RADIUS)", RFC 2865