情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

권한인증서를 이용한 도메인간의 사용자 인증방안*

김 지 홍[1], 지 준 웅[1†‡], 김 창 규[2]
[1]세명대학교, [2]동의대학교

A User Authentication Method between Domains Using Privilege Certificates*

Ji-hong Kim[1], Jun-Woong Gi[1], Chang-Kyu Kim[2]
[1]Semyung University, [2]DongEui University

요 약

본 논문은 AAA 기반의 MIPv6 환경 하에서 노드가 이동함에 따라, 도메인간 사용자 인증에 관한 방법을 기술한다. 기존에는 MN이 도메인간 이동하는 경우, 방문도메인의 AAA 서버를 통해 홈도메인의 AAA 서버에서 사용자를 인증하는 방법이 제안되었으나, 본 논문에서는 도메인간의 권한인증서를 이용하여 방문도메인에서 사용자인증을 수행할 수 있는 방법을 제시한다.

ABSTRACT

In this paper, we design a user authentication method between domains when mobile node moves in AAA server based MIPv6 environment. Several papers proposed the user authentication method executing at AAA server in home domain via AAA server in visiting domain. In this paper we proposed the user authentication method using privilege certificates between domains.

Keywords : MIPv6, Privilege certificate, AAA server

Ⅰ. 서 론

노드가 이동하는 경우, 새로운 CoA(Care of Address) 주소를 발급받고, 이를 HA(Home Agent)와 CN (Corresponding Node) 에 알리기 위한 바인딩 과정을 거친다. MIPv6 표준에서는 HA와의 바인딩 과정은 Ipsec을 이용하여 보안하는 방안이 사용되고 있다. 즉, 노드가 이동한 후 HA로 BU(Binding Update)를 보낼 때, 이 BU 메시지가 진실한 MN(Mobile Node)으로 부터 생성된 것임을 보증해야 한다.

HA와의 바인딩 과정이 성공적으로 수행된 후에, 다시 CN과의 바인딩 과정이 수행된다. MIPv6 표준에서는 CN과의 바인딩 과정으로 RR 방식을 사용한다. RR 과정에서는 MN와 CN과의 경로, MN와 HA를 통한 CN과의 경로를 통한 바인딩 키 전달방법이 사용된다.

MIPv6에서 발생될 수 있는 보안위협은 크게 NDP (Neighbor Discovery Protocol) 프로토콜상의 보안 위협과 바인딩 과정에서의 보안위협으로 분류된다. NDP 프로토콜상의 보안위협[4]은 유, 무선 Ipv6 망에 모두 적용되는 위협으로서, 라우터 및 라우팅과 관련된 부분

접수일 : 2008년 7월 3일; 채택일 : 2008년 10월 7일
* 본 논문은 2007 학년도 세명대학교 교내 학술연구비 지원에 의해 수행된 연구임.
† ‡ 주저자, 교신저자 : gjwoong@empal.com

과 라우터와 무관한 인근 노드와 관련된 위협요소로 구분된다. 라우터와 관련된 보안위협은 허위 라우터에 의한 프리픽스, 라우팅 경로 정보 조작 등이 있으며, 기타 라우터와 무관한 인근 노드와 관련된 보안위협은 주로 DoS 공격에 의한 자동주소 설정 등의 과정을 정상적으로 동작할 수 없도록 하는 공격이 사용된다.

이와 같은 IP 구성의 문제점에 대하여 인프라구조 방식과 비인프라구조 방식에서의 접근방식이 제안되고 있다. 비인프라구조 방식으로 Mipv6 망의 근본적인 NDP 프로토콜의 문제점을 보완하기 위하여 SEND 방식[8]이 제안되었으며, 인프라구조 방식으로는 AAA 서버와 EAP 프로토콜을 이용한 방식[13,14,15]이 제안되었다.

비인프라구조 방식의 대표적인 SEND 방식은 NDP 방식에서의 대표적인 문제점인 노드의 진위성을 보장하기 위하여, 공개키를 기반으로 하여 생성된 암호학적 주소인 CGA 주소[7]와 디지털 서명방식이 사용된다. 도메인 내의 라우터들은 공개키 인증서를 사용하고, 노드들은 임의로 생성한 공개키와 보조 변수들을 이용하여 자신의 CoA 주소를 생성하고, 메시지의 마지막에 개인키를 이용한 서명문을 첨부함으로서, 진위의 노드임을 입증하는 방식이다. 이러한 방식은 계산량이 너무 많으며, 또한 라우터의 공개키를 검증하기 위하여 사용되는 교환메시지인 CPS/CPA 메시지에 대한 DoS 공격가능성이 높다는 점이 단점으로 지적된다.

인프라구조 방식에서 사용되는 AAA 서버 방식은 기존의 망 가입자들이 사용하고 있는 방식으로서, 가입자에게 부여한 ID와 패스워드에 해당되는 NAI(Network Access Identifier)를 사용하는 방식이다. MIPv6 사용자들은 이동 후에도 자신이 가입한 망사업자로부터 부여된 NAI를 이용하여 지속적으로 이동망을 사용할 수 있는 방법이다. AAA 서버를 이용한 부트스트랩 방법에는 Charles E.Perkins가 제안한 “Diameter Mobile IPv6 Application” 기술[13]과 Francis Dupont이 제안한 “AAA for Mobile IPv6” 기술[14], ETRI에서 개발한 6Msec 시스템 중 “AAA 인트라를 이용한 Mobile IPv6 Bootstrapping” 기술[15] 등이 있으며, 본 연구에서는 Perkins 제안방법을 분석하고, 효율성을 개선하기 위하여 SPKI 권한인증서를 도입하였다.

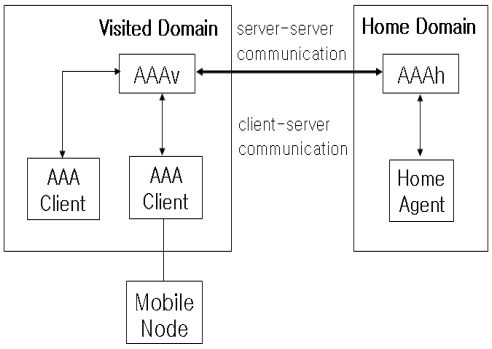
본 논문은 AAA 서버를 이용한 인프라구조에서 MN이 도메인간의 이동시, AAA 서버간의 권한인증서를 이용하여 응용계층의 서비스들이 지속적으로 제공될 수 있기 위한 방안으로서, 다음과 같이 구성된다. 2장에서는 기초이론으로서, 도메인간의 인증방식으로 Diameter 프로토콜을 이용한 Perkins 방식과 본 논문에서 도입할 권한인증서에 대하여 소개하고, 3장에서는 본 논문에서 제안하고 있는 방식에 대하여 설명하고, 4장에서는 제안방식과 기존방식에 대한 비교 및 장단점을 분석하고, 마지막으로 5장 결론으로 마무리한다.

Ⅱ. 기초 이론

2.1 MIPv6를 지원하는 Diameter 프로토콜

Charles E.Perkins가 제안한 “Diameter Mobile Ipv6 Application” 기술은 노드가 타 지역으로 로밍한 후에도 서비스를 지속적으로 제공받을 수 있게 하는 기술로서, 인증 메세지를 이용한 피기백 방식과 Diameter 프로토콜을 사용하고 있다.

MN이 홈 도메인에 등록된 상태에서 방문 도메인(visited domain)으로 이동하였을 경우에, MN는 타 도메인내의 액세스 라우터 혹은 Agent 기능을 하는 AAA 클라이언트에 접속하여, 자신의 NAI를 제시하고, 이를 인증 받는 구조이다. 이와 같은 구조에서 타 도메인의 AAAv 서버와 자신의 홈 도메인의 AAAh 서버간의 신뢰관계가 구축되고, 서버-서버 통신이 사용된다. 마찬가지로 AAA 클라이언트 혹은 HA는 AAA 인프라상의 계약관계가 성립된 상태에서 서버-클라이언트 통신이 사용된다. 이와 같은 Perkins가 사용한 모델은 [그림 1]과 같다.



[그림 1] Perkins의 기본모델

(기본 가정)

(1) MN은 AAA 인프라에 접속하기 위하여 NAI를

사용한다. 즉, MN의 Identifier가 MN-NAI인 경우에는 MN이 홈주소를 가지고 있다하더라도, AAA 인프라 구조에 접속하기 위해서는 MN-NAI를 사용하여야 한다. 만일 MN이 MN-NAI를 가지고 있지 않고, 단지 홈주소를 가지고 있는 경우, MN은 IPv6 홈 주소를 이용하여 AAA 기반구조에서 제공되는 인증/권한부여를 사용할 수 있도록 한다.

(2) MN과 AAAh는 장기간 사용가능한 키(long term Key)를 공유하고 있다.

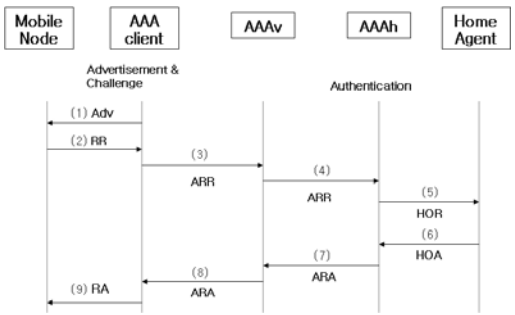
(3) AAAv와 AAAh 간의 통신로는 안전하다.

(프로토콜에서 사용되는 주요 AVP)

- MIP-Biniding-Update AVP(Attribute Value Pair) : MN 에서 HA로 전송된 MIP 바인딩 업데이트 메시지.
- MIP-Biniding-Acknowledgement AVP : HA에서 MN으로 전송된 MIP 바인딩 응답 메시지.
- Mobile-Node-Address AVP : IP 주소 형태이며, MN의 홈 주소.
- Home-Agent-Address AVP : IP 주소 형태이며, HA의 주소.
- MIPv6-Feature-Vector AVP : 홈도메인 내에서 동적 HA 할당 요구.
- Security Key AVP : AAA 서버들의 키분배 역할.

(기본 프로토콜)

기본 프로토콜은 홈도메인에서 동적으로 HA를 할당한 경우 혹은 사전에 설정된 HA를 이용하는 경우에 적용되는 절차는 [그림 2]와 같다.



[그림 2] 기본 모델에서의 메시지 흐름도

(1) MN이 새로운 도메인으로 이동하는 경우, 새로운 도메인에서 Adv 메시지로 부터 로컬 채린지(local challenge) 및 방문네트워크에 대한 기본정보를 받는다.

(2) MN은 CoA 주소를 발신지 주소로 하고, AAA 클라이언트 주소를 목적지로 하는 RR(Registration Request) 메세지를 생성한다. 또한 MN은 자신의 NAI와 호스트 채린지값을 생성하고, AAAh와의 공유키를 이용하여 MN 인증 데이타를 계산하여, AAA 클라이언트에게 전송한다. 만일 MN이 HA와 홈주소를 가지고 있지 않은 경우에는 홈주소를 할당해 주도록 요구할 수 있다. 동시에 자신의 CoA 주소에 대한 바인딩업데이트는 AAA 서버를 통해 HA로 전송된다.

(3) AAA 클라이언트는 MN로부터 수신된 인증요청 메세지에서 우선 로컬채린지 값을 체크하고, DAD (Duplicate Address Detection)를 체크하고, ARR (AA-Registration Request) 메세지를 생성한다. Diameter ARR 메시지에는 AAAh 서버로 전달될 정보가 포함된다.

(4) AAAh가 AAAv로부터 ARR 메시지를 수신하면, 먼저 AAAv는 적법한 AAA 클라이언트로부터 온 메시지인가를 체크한다. 그리고 MIP Feature Vector AVP를 체크하고, 이를 MN의 홈 AAA 서버로 전송한다.

(5) AAAv로부터 ARR 메시지를 수신하면, AAAh는 먼저 메시지가 적법한 AAAv로 부터 수신된 지를 체크한다. AAAh는 홈 체린지와 채택된 인증 알고리즘에 필요한 다른 정보들에 기초하여 네트워크 인증데이터를 계산한다.

(6) HA는 HOR(Home-Agent-MIPv6-Request)메시지를 수신하고, 먼저 Diameter 메시지를 처리한다. 수신된 메시지에 오류가 없는 경우에는 MIP-Binding-update AVP를 처리하고, 바인딩 응답 메세지를 계산한다. 또한 바인딩 정보는 바인딩 캐쉬에 저장하고, MN과의 보안연계를 위한 키를 계산한다. 마지막으로 MN으로 전송할 캡슐화된 바인딩 응답 메세지를 포함한 HOA(Home-Agent-MIPv6-Answer)메시지를 AAAh에게 전송한다.

만일 HA 할당을 요구하는 경우에는, AAAh 서

버는 적절한 HA를 할당하고, 이와 관련된 바인딩 업데이트 및 HA와 MN간에 사용될 보안 키 자재를 포함시킨다.

(7) AAAh는 MN에 의해 요청된 키와 관련된 키 재료를 계산하고, AAAv를 통하여 MN에게 전송한다. 즉, 만일 MN으로부터 요청된 메시지에 임베디드 바인딩업데이트 정보 혹은 동적 HA 할당 요청이 포함되어 있다면, AAAh는 MIP-Binding-acknowledgement AVP를 포함한 ARA(AA-Registration-Answer) 메시지를 AAAv에게 전송한다.

(8) AAA 클라이언트는 AAAv로 부터 ARA 메시지를 수신하면, MN에게 적합한 프로토콜로 메시지를 변환하여 RA (Registration Answer) 메시지를 보낸다.

(9) MN이 AAA 클라이언트로부터 RA 메시지를 받은 경우에, AAA 클라이언트로부터 수신된 인증 데이타를 이용하여 네트워크 인증하고, MN이 HA를 요청한 경우에는 홈 바인딩 응답메세지의 발신지 IP 주소로부터 HA 주소를 알아내고, 이를 저장한다.

“Diameter Mobile IPv6 Application” 기술의 특징은 AAA 메시지의 임베디드 데이터를 정의하여 MN의 AAA 인증과정에서 BU, Key 정보, 홈 주소할당, HA 할당 등의 MIPv6 설정기능의 상당부분을 처리할 수 있도록 한 것이다. 그러나 초기에 MN과 AAA 클라이언트간의 세션키가 설정되지 않은 상태에서 AAA 메시지에 BU를 피키백하는 경우, MN 및 HA의 정보가 노출될 수 있는 위험성이 있으며, 악의적인 공격자는 노출된 정보를 이용하여 분산 서비스 거부공격을 감행할 수 있는 위험성이 존재하는 문제점이 있다.

2.2 SPKI 인증서

SPKI(Simple PKI) 인증서[16]는 주로 접근통제를 위한 공개키 인증서를 정의하고 있으며, 개체의 이름 대신에 공개키의 광범위한 사용과 분배를 정의하고 있다. SPKI 인증서의 전체적인 개념은 공개키 암호 방식에 기반을 두고 있으며, 이 인증서를 통해 서로 다른 허가권을 자유롭게 정의할 수 있다.

SPKI 인증서에서 기본적으로 요구되는 사항은 발행의 자유, 권한 위임 가능, 허가권 정의와 분배의 자유, 명확한 유효기간, 공개키의 광범위한 사용 등으로 요약할 수 있으며, 권한인증서(Authorization Certificate)와 이름인증서(Name Certificate)로 구분된다. 이름인증서는 발급자 이름 영역내의 이름과 principal 또는 principal 그룹의 결합이며, 권한 인증서는 권한과 principal 또는 principal 그룹의 결합이다. 이름 인증서로는 SDSI(Simple Distributed Security Infrastructure) 이름인증서를 사용한다.

SPKI의 기본 인증서 형태는 권한인증서이다. 이 인증서는 한 principal에서 다른 principal로 어떤 특정 권한이나 허가를 전달하는 역할을 한다. 따라서 권한인증서는 권한을 생성하기 보다는 주로 권한을 위임 및 전달하는 역할을 한다. SPKI 권한인증서의 주요 5개 항목을 5-tuple이라고 부르며 자세한 내용은 다음과 같다.

① Issuer(발급자) : 인증서 발행자 또는 서명자의 공개키나 키의 해쉬값을 의미한다. 개인키는 인증서에 대한 서명에 이용된다.

② Subject(주체) : 인증서에 주어진 권한을 얻는 개체로서, 주체의 공개키나 키의 해쉬값을 사용한다.

③ Delegation(위임) : 위임 영역은 발급자가 주체에게 발행한 권한을 재 위임할 수 있는 권리를 주체에게 부여하는 영역으로, 부울 값으로 표현된다. 해당 인증서의 주체가 다른 주체에게 권한을 위임할 수 있도록 발급자가 허용하면, 부울 값은 “true”가 된다.

④ Authorization(허가) : 허가 영역은 접근 권한을 의미하며, 태그라고도 불린다. 발급자가 주체를 위해 인증서에 서명하면, 이것은 통상 주체가 가지게 될 권한을 정의하는 것이다. 권한은 인증서 발급자에 의해 자유롭게 정의될 수 있으며, 이 영역의 내용은 전적으로 어플리케이션에 달려 있다.

⑤ Validity Dates(유효기간) : 유효기간 영역은 발급자가 지정한 인증서의 유효기간을 정의하는데 사용된다. 이 영역의 형태는 not-before date와 not-after date를 사용한다.

이와 같이 5-tuple은 <I, S, D, A, V>로 표현된다.본 논문에서 사용하는 권한인증서는 SPKI 권한인증서의 형태를 사용한다.

인증서에는 공개키 기반구조에서 사용되는 공개키 인증서(PKC : Public Key Certificate), 권한인증서로서 사용자의 속성정보를 제공하는 속성인증서(AC : Attribute Certificate), 권한인증서로서 공개키에 의한 사용자의 속성정보를 제공하는 SPKI 인증서(SPKC Simple PKC)로 구분되며, [표 1]과 같이 세 가지 인증서가 비교된다.

[표 1] 인증서 비교

	공개키인증서	속성인증서	SPKI인증서
Name Space	Global	Global	Local
형식	이름 인증서	권한 인증서	권한인증서
권한	name → key	name → authorization	authorization → key
CA 구조	계층구조	이원화 계층	평등 구조
인증서 폐기 방법	CRL 사용	CRL 사용	짧은 유효기간 사용
유효기간	장기	단기	단기
인증서 표현 구문	ASN.1	ASN.1	S-expression

Ⅲ. 제안방식

제안방식은 기본적으로 Perkins의 기본모델을 근간으로 하고, AAAv 서버, AAAh 서버로부터 발급된 MN의 권한인증서를 적용하는 방식이다. 본 제안방식은 특정 타 도메인의 AAAv 서버가 자신이 속한 AAAh 서버에 특정권한을 위임하는 권한인증서를 발행하고, 다시 AAAh 서버는 자신의 도메인 가입자인 MN에게 타 도메인에 접속할 수 있는 권한인증서를 발행한다. 이때 MN은 방문도메인에 접속할 수 있는 권한인 NAI를 제시하여, AAAh 서버로부터 방문도메인에 접속할 수 있는 권한인증서 체인을 발급받는다.

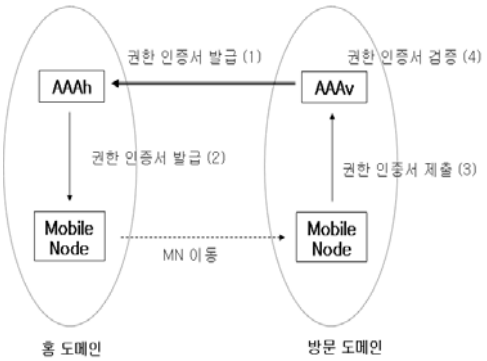
3.1 AAA 서버의 권한인증서 발행

도메인간의 계약관계에 의해 일정 권한을 타 도메인에게 위임하는 경우, 권한인증서를 발행한다. 즉, [그림 3]과 같이, 타 도메인 사용자들이 자신의 도메인에서 일정한 권한을 행사할 수 있도록 도메인 업체간의 권한위임이 우선된다. 도메인 업체는 다시 타 도메인 업체로부터 부여받은 권한을 이용하여, 자신의 도메인과 타도메인을 동시에 사용하기를 원하는 사용자에게 타 도메인에 접근할 수 있는 권한을 부여한다. 그리고 이와 같은 사용자 목록은 추후에 도메인간의 계약에 의해 정산한다.

MN은 그림 3과 같이 홈도메인의 AAAh 서버로부터 타도메인에 접근할 수 있는 권한인증서 체인을 발급받는다. 또한 MN은 HA에 접속하여 홈주소와 네트워크 접속에 필요한 정보를 할당받는다.

AAA 서버로부터 발급받은 권한인증서에는 해당 AAA 서버의 공개키, MN의 공개키, MN에게 발급된 권한사항(도메인별 접속권한)과 이에 대한 유효기간을 포함하며, 이러한 권한인증서의 무결성을 확인하기 위한 AAA 서버의 서명을 포함한다. 이때 MN이 발급받은 권한인증서는 타 도메인의 AAAv 서버가 발급한 권한인증서 <I_AAAv, S_AAAh, D1, A1, V1>와 자신의 도메인의 AAAh 서버가 발급한 권한인증서 <I_AAAh, S_HA1, D2, A2, V2> 체인이다. 여기서 D1은 타도메인에 권한을 위임하므로 True가 되며, D2는 더 이상 위임을 허용하지 않기 때문에 False가 된다.

3.2 권한인증서의 사용 및 검증



[그림 3] 권한인증서 사용

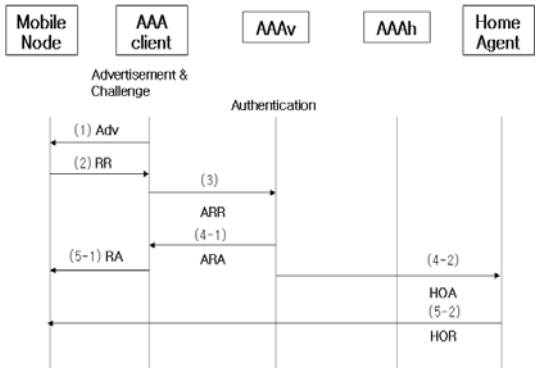
[그림 3]은 MN이 방문 도메인으로 이동한 경우, AAAv 서버가 AAAh 서버에게 발급한 권한인증서와 AAAv 서버가 MN에게 발급한 권한인증서를 AAAv 서버에 제출하여 권한인증서 체인을 검증하는 과정을 설명하였다.

<I_AAAv, S_AAAh, D1, A1, V1> + <I_AAAh, S_MN, D2, A2, V2> = <I_AAAv, S_MN, D2, A3, V3>

즉, 두 개의 권한인증서 체인은 AAAv 서버에서 AAAh 서버를 통해 S_MN에게 한정된 권한이 위임되었음을 알 수 있다. 여기서 A3는 A1 ∩ A2 이며, V3는 V1 ∩ V2 이다.

3.3 도메인간의 이동에 대한 Perkins 기본모델 적용

권한인증서를 이용한 모델은 기본적으로 AAAv 서버에서 사용자에 대한 인증이 가능하다. 그러므로 Perkins 방법의 기본모델에서 [그림 4]와 같이 AAAv 서버로부터 AAAh 서버로의 통신을 통한 사용자 검증과정이 생략되며, 단지 홈도메인에 있는 HA와 바인딩정보를 주고받는 형태로 구성될 수 있다.



[그림 4] Perkins 방법(기본모델)의 변형

(1) MN이 새로운 도메인으로 이동하는 경우 혹은 전원이 켜지는 경우로서, MN은 새로운 도메인에서 Adv 메시지로부터 다음과 같은 정보를 보관한다.
- 로컬 채린지(local challenge)
- 방문네트워크 ID(visited network ID)
- CoA를 계산하기 위한 정보

(2) MN은 다음과 같은 정보를 이용하여, CoA 주소를 발신지로 하고, AAA 클라이언트 주소를 목적지로 하는 메시지를 생성한다.
- MN의 권한인증서 체인으로서, AAAv 서버 및 AAAh 서버가 발행한 권한인증서를 포함한다. 또한 AAAv의 권한인증서의 권한필드에는 AAAv 도메인에 대한 접근권한을 포함한다.

또한 MN은 호스트 채린지값을 생성하고, AAAh와의 공유키를 이용하여 MN 인증 데이타를 계산하고, AAA 클라이언트에게 전송한다. 만일 MN이 HA와 홈주소를 가지고 있지 않은 경우에는, Perkins의 기본모델에서와 같이, AVP를 이용하여 AAAv 서버를 통해 요청하거나, 혹은 MIPv6에서 명시된 방법으로 홈도메인의 HA에게 직접 요구할 수 있다. CoA 주소에 대한 바인딩업데이트도 마찬가지 방법으로 전달될 수 있으며, [그림 4]의 경우에는 AAAv 서버를 통해 전달되는 방법을 도시하였다.

(3) AAA 클라이언트는 MN으로부터 수신된 인증요청 메세지에서 우선 로컬채린지 값을 체크한다. 체크에 성공하면 DAD 체크를 하고, Diameter ARR 메세지를 생성한다. Diameter ARR 메시지에는 다음과 같은 정보가 포함된다.
- MN의 권한인증서 체인
- 수신된 인증데이터로부터 추출된 상호인증을 위한 EAP AVP
- 만일 MIP 특성 데이터가 포함되어 있다면, MIPv6- Feature Vector AVP
- 바인딩 업데이트가 임베디드되어 있다면, MIP-Binding Update AVP
- 바인딩업데이트 메시지가 있다면, MIP-Home-Agent- Address AVP HA 주소는 임베디드된 홈 바인딩업데이트 정보의 목적지 주소로부터 추출된다.
- MN이 키 요구 데이터를 포함하고 있다면, Security Key AVP

(4) AAAv는 ARR 메시지를 수신하면, 먼저 적법한 AAA 클라이언트로부터 온 메시지인가를 체크한다. MN의 권한인증서 체인를 이용하여 MN의 네트워크 접근 권한을 확인한다.

(4-1) 적절한 권한이 설정되어 있는 경우에는 AAA 클라이언트에게 네트워크에 접속허가 메시지인 ARA 메세지를 보낸다. 이후, (5-1) 과정은 기본 모델

과 같다.

(4-2) MN의 권한이 적절한 경우에는 AAA Client로부터 전달된 MN의 바인딩 정보를 바로 홈도메인내의 HA에게 전송함으로서, 바인딩 과정이 수행된다. 이후, (5-2) 과정은 바인딩 응답과정이다.

마지막으로 MN은 AAAv 서버로부터 네트워크 접속권한 허가 정보와 홈도메인내의 HA로부터 바인딩 응답정보가 도착하면, MIPv6 표준에서 정의된 바와 같이 상대노드와 바인딩과정을 통하여 CN과의 통신을 유지할 수 있다.

Ⅳ. 본 제안의 장점

본 논문에서 제안된 방식을 이용하면 다음과 같은 장점이 있다.

4.1 공인인증서와 권한인증서의 사용 비교

기존의 공인인증서를 사용하는 방법에 비해 권한인증서를 사용하는 방법이 적합하다. 공인인증서를 사용하는 경우에는 신원확인과정을 거쳐, 인증기관으로부터 인증서를 발급받아야 하며, 또한 인증서를 사용할 때마다, 인증서 검증과정, CRL 조회과정을 거쳐야 한다. 반면에 본 논문에서 제안된 권한인증서를 이용하는 경우에는, AAAv 서버가 발행한 권한인증서와 AAAh 서버가 발행한 권한인증서 체인을 이용하여 검증과정이 간략히 될 수 있다. 그러므로 권한인증서를 이용함으로서 사용자 인증과정을 빠르게 할 수 있다. 또한 권한인증서는 5개의 주요 필드로 구성되어, 공인인증서에 비해 경량화되어 있기 때문에 MN의 성능에 지장을 주지 않으며 운영하기 쉽다.

즉, AAAh 서버를 통해서만, 사용자 인증이 가능했던 기존의 방식에 비해 본 제안방식은 권한인증서를 이용하여 방문 도메인에 위치한 AAAv 서버에서도 바로 사용자의 권한을 검증할 수 있도록 하였다.

4.2 권한인증서 사용의 장점

AAAv 서버가 발행한 권한인증서의 권한 필드에는 네트워크 접속 권한이 설정되어 있으며, AAAh 서버가 발행한 권한인증서에는 기본적으로 설정된 HA 주소와 홈 주소를 보관할 수 있으므로, Perkins 가 제안한 기본 모델의 경우에는 본 논문에서 제안한 권한인증서를 적용하면 성능이 크게 향상시킬 수 있다.

[그림 4]에서는 MN이 타 도메인으로 이동한 후, 최초의 인증과정에서 속도를 높이기 위하여 MN과의 바인딩과정을 포함하는 것으로 제안하였지만, 실제로 권한인증서 체인을 이용하여 네트워크 접속권한을 검증한 후, 즉, 사용자 인증과정을 마친 후에는, MN는 AAAv 서버 혹은 AAAh 서버와의 접속 과정을 거치지 않고 HA와의 바인딩과정, 홈주소 설정 및 HA 할당요구 등을 MN는 AAAh 서버가 발행한 권한인증서를 이용하여, HA와 직접 수행할 수 있다.

4.3 기타

Perkins의 기본모델은 1회의 라운드 트립으로 사용자 인증정보, 바인딩정보, HA 할당, 홈주소 설정 등을 구현할 수 있다고 하지만, 실제로는 각각의 과정에서 상당한 시간이 걸릴 수 있기 때문에, 전체적으로 1회의 라운트 트립시간이 상당히 지연될 수 있다. 또한 Perkins 모델의 경우, 라운드 트립시간은 8개의 단계로 구성되지만, 제안된 모델에서는 사용자 인증을 위하여 MN과 AAAv 서버간의 5개 단계와 동시에 바인딩정보 전달을 위한 2개 단계가 수행될 수 있도록 구성하였다.

기본적으로 Perkins가 제안한 기본모델은 1회의 라운드 트립으로 사용자 인증, 바인딩, 동적 HA 지정, 홈주소 설정, 암호화 정보 전달 등의 모든 기능을 수행할 수 있도록 하였으나, 이러한 방법은 실제로 구현하기에는 많은 어려움이 있으며, 또한 보안공격에 취약하다.

그러므로 MIPv6 표준에서 명시되지 않은 사용자 인증방법은 본 논문에서 제안된 방법을 적용하고, 기타 부분은 MIPv6 표준사항을 준수하는 방법이 좋을 것이다.

게다가, 권한인증서를 이용한 사용자 인증과정과 함께, 권한인증서를 이용한 MN과 HA간에 정의된 바인딩 과정, 동적 HA지정, 홈 주소 설정 등의 과정은 공개키 암호화방식을 적용하는 방법도 좋은 선택일 것이다.

Ⅴ. 결 론

본 논문에서는 AAAv 서버와 AAAh 서버가 발행한

권한인증서 체인을 이용하여, 홈도메인의 AAAh 서버 대신 이동망에서의 AAAv 서버에서 사용자 인증을 하도록 제안하였다. 그러나 만일 이동망의 AAA 클라이언트가 인증서 검증기능이 있다면, AAAv 서버까지 전달될 필요가 없으므로, [그림 7]에서의 (3)번 과정과 (4-1)번 과정이 생략될 수 있으므로, 성능이 보다 향상될 수 있다. 또한 이와 같이 권한인증서를 이용하여, 방문 도메인에서 사용자 인증이 완료되면, MN은 홈도메인의 AAAh 서버가 발행한 자신의 권한인증서의 공개키를 이용하여 암호화하여, 직접 HA와 바인딩 업데이트 등의 과정을 수행할 수 있다.

이와 같이 Perkins가 제안한 기술의 특징은 AAA 메시지의 임베이디드 데이터를 정의하여 MN의 AAA 인증과정에서 BU, Key 정보, 홈 주소할당, HA 할당 등의 MIPv6 설정기능의 상당부분을 처리할 수 있도록 한 것이다. 그러나 초기에 MN와 AAA 클라이언트간의 세션키가 설정되지 않은 상태에서 AAA 메시지에 BU를 피키백하는 경우, MN 및 HA의 정보가 노출될 수 있는 위험성이 있으며, 악의적인 공격자는 노출된 정보를 이용하여 분산 서비스 거부공격을 감행할 수 있는 위험성이 존재하는 문제점이 있다. 이러한 문제점을 해결하기 위한 방안으로 제안된 모델에서는 사용자 인증기능을 방문 도메인내에서 해결하고, 단지 MN와 HA간의 바인딩과정만은 별로도 진행될 수 있도록 분리시켰다. 또한 AAAv 서버를 중심으로 사용자 인증기능이 완료되며, 단지 바인딩 정보만을 홈 도메인으로 전송하도록 제안하였다.

참고문헌

[1] RFC 1883, Internet Protocol, Version 6 Specification, 12, 1998.

[2] RFC 2462, IPv6 Stateless Address Auto-configuration, 12, 1998.

[3] RFC 2461, Neighbor Discovery for IPv6, 12, 1998

[4] RFC 3756, Ipv6 ND Trust Models and Threats, 5, 2004.

[5] RFC 3775, Mobility Support in IPv6, 6, 2004

[6] RFC 3776, Using Ipsec to protect Mobile Ipv6 Signaling between MN and HA, 6, 2004.

[7] RFC 3972, CGA(Cryptographically Generated Address), 3, 2005.

[8] RFC 3971, SEcure Neighbor Discovery, 3, 2005

[9] RFC 3779, X.509 Extensions for IP Addresses and AS Identifier, 6, 2004.

[10] RFC 3281, An Internet Attributes Certificate Profile for Authorization, 4, 2002.

[11] draft-ietf-hip-base-03, Host Identity Protocol, June 23, 2005

[12] draft-ietf-hip-arch-03, Host Identity Protocol Architecture, August 1, 2005

[13] draft-le-aaa-diameter-mobileipv6-04.txt, Diameter Mobile IPv6 Application, 2001.

[14] draft-dupont-mipv6-aaa-01.txt, AAA for Mobile Ipv6, 2004.

[15] draft-mun-mip6-authhmip-movileipv6-00.txt, An Authentication Scheme using AAA in Herachical MIPv6, 2005.

[16] RFC 2692, “SPKI Requirements”, 1999.

<著 者 紹 介>

김 지 홍 (Ji Hong Kim) 종신회원
1982년 : 한양대학교 전자공학과(공학사,
1984년 : 한양대학교 전자통신공학(공학석사)
1996년 : 한양대학교 전자통신공학(공학박사)
1995. 2~현재 : 정보통신기술사
1991. 3~현재 : 세명대학교 정보보호학과 교수
<관심분야> 공개키기반구조, 접근제어, 네트워크보안

지 준 웅 (Chi Jun Woong) 정회원
1996년 : 상지대학교 자원공학과(공학사)
2001년 : 세명대학교 전기전자과(공학석사)
2008년 : 세명대학교 전기전자과(공학박사)
<관심분야> 정보보호, 시스템보안, 네트워크 보안

김 창 규 (Chang Kyu Kim) 종신회원
1981년 : 한양대하교 전자통신학과(공학사)
1984년 : 한양대학교 전자통신학과(공학석사)
1989년 : 한양대학교 전자통신학과(공학박사)
1988. 3~현재 : 동의대학교 정보통신공학과 교수
2006. 11~현재 : 동의대학교 공학교육혁신센터장
<관심분야> 정보보호, 이동통신