Proceedings of KFIS Spring Conference 2006 Vol. 16, No. 1.

모바일 노드에서의 ID기반의 AAA인증 프로토콜

Identity-based AAA Authentication Protocol in Mobile Node

조영복, 김동명,이상호

충북대학교 전자계산과
E-mail: bogi0118@netsec.cbnu.ac.kr
E-mail:singall@hanmail.net
E-mail:shlee@cbnu.ac.kr

요 약

인터넷의 발달과 사용자 증가로 인해 IETF는 다양한 네트워크와 프로토콜 상에서 안전하고 신뢰성 있는 사용자 인증을 위해 AAA를 제안하였다. 그러나 AAA의 최신 버전인 Diameter 표준의 인증 방식은 상호인증과 부인방지를 제공하지 않는다. 이러한 Diameter의 인증을 보완하기 위해 공개키를 이용한 AAA 인증 방식이 제안되었으나, 통신과 연산의 오버헤드로 인해 이동 노드에 적용이 어렵다. 이러한 단점을 극복한 ID 기반 AAA 인증 방식이 제안 되었으나 공모공격과 위장공격으로부터의 취약점을 가진다. 이 논문에서는 공모공격과 위장공격에 안전하고, 계산적·전력적 능력이 부족한 이동 노드의 연산량을 감소시키는 새로운 ID기반 AAA인증 방식을 제안한다. 제안한 방식의 검증을 위해 기존 방식을 비교 평가하여 암호학적인 안전성과 연산량의 효율성을 검증한다. 제안 방식은 이동 노드의 인증시 2개의 난수를 생성하여 안전성을 제공하며, Mobile 노드의 지수연산을 줄임으로 계산·전력적 측면에서 효율적이고 서버의 성능에 따라 인증 수행 시간을 감소 시켜 끊김 없는 서비스를 제공할 수 있는 장점을 갖는다.

Key Words : Diameter, ID-based Cryptography, AAA, Mobile IP

1. 서론

이동 인터넷을 통한 사용자의 서비스 이용 증가에 따라, 인터 도메인을 이용한 인터넷 서비스 사용에 관련된 보안과 과금에 대한 문제가 제기되었다. 이를 위해 IETF는 다양한 유무선 서비스에 대하여 인증, 권한 검증, 과금을 수행하는 AAA(Authentication, Authorization and Accounting) 표준을 제안하였다. ID 기반 암호는 공개키와 사용자의 ID를 일대일 맵핑을 통하여 공개키를 생성한다. ID 기반 암호를 이용할 경우, 사용자의 공개키는 사용자의 E-mail 주소, NAI(Network Access Ientifier)등이 사용될 수 있다. 결과적으로, 공개키와 관련된 CRL(Certificate Revocation List)을 획득하고, 확인하는 과정의 부하가 사라지게 되어 시스템과 CA간의 통신을 줄일 수 있는 장점을 갖게 된다. 이 논문에서는 ID 기반 암호를 이용하여, Mobile IP와 Diameter의 통합된 인증방식을 제안한다. 제안하는 방식은 D. Boneh와 D. Franklin의 Weil-pairing을 이용한 ID기반의 암호 방식을 이용한다. 제안하는 인증 방식은 공개키 기반 암호에 비해 계산적 부하와 통신량의 부하를 줄임으로 써 이동 노드에 적용이 용이하고, 기존에 요구되던 상호인증과 부인방지는 물론, Conspiracy Attack 과 Impersonation Attack에 대해 안전하다. 이 논문에서는 이동 인터넷의 발달로 인해 더욱 중요성이 부각되고 있는 AAA의 인증 방식을 보완하기 위해 제시되었던 기존 연구들의 문제점을 보완하며, 인증시 이동 노드의 계산적 부하를 줄일 수 있는 인증 방식을 제안하고자 한다. 연구를 위해 다음의 관련연구를 수행한다. 첫째, 인증 방식을 제안하기 위해 환경이 될 수 있는 AAA의 최신 버전인 Diameter에 대해 알아본다. 둘째, 관용키 기반의 인증 방식에 비해 공개키 기반의 인증이 갖는 장점을 유지하고, 공개키 기반을 이용한 이동 인터넷 환경에서의 단점을 보완하기 위해 ID 기반 암호에 대해 알아본다. 셋째, Diameter가 가지고 있던 알

려진 단점을 보완하였던 기존의 ID 기반 AAA 인증 방식을 분석한다. 논문의 구성은 제 1장 서론에 이어, 2장에서는 관련연구로서 ID 기반 암호와 Mobile IP 환경의 Diameter를 설명한다. 3장에서는 새로운 ID기반 AAA 인증 방식을 제안하고, 4장에서는 제안한 방식의 보안 요구사항과 기존 방식과의 비교를 통하여 평가한다. 5장에서는 결론을 도출한다.

2. 관련연구

AAA 프로토콜은 다중 네트워크와 플랫폼 상에서 인증, 권한 검증, 과금등의 기능들을 조정하는 프레임웍으로서 다음의 기능을 수행한다.
Mobile IP는 Mobile 노드가 홈망에서 타망으로의 이동시 사용자의 서비스를 끊임없이 받는 것이 가능하도록 하는 응용 서비스이다. Mobile IP환경에서 AAA를 이용한 사용자 등록 과정은 [그림2.1]와 같다

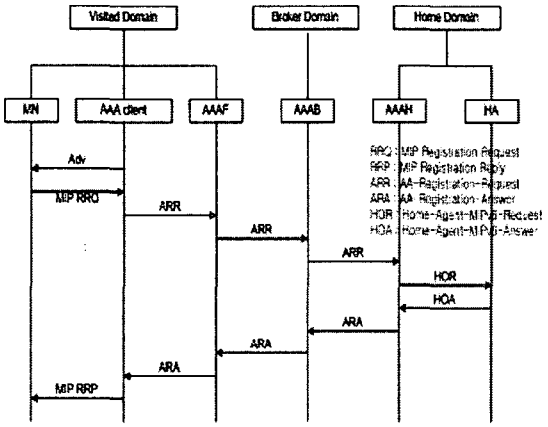

그림 2-1 Mobile IP를 지원하는 AAA의 인증 과정

2.1 ID 기반의 암호화

ID 기반 시스템은 거래를 원하는 상대방의 인터넷 도메인(Domain)의 주소(IP), E-mail 주소, 주민등록번호, 전화번호, 카드번호 등 사용자의 신분을 유일하게 확인할 수 있는 신분정보(Identity)만으로도 쉽게 상대방을 인증할 수 있고 이것을 바탕으로 공개키 기반의 전자서명과 키 분배를 사용자간에 독립적으로 할 수 있는 장점이 있다. D. Boneh와 D. Franklin이 Weil-pairing을 이용하여 새로운 ID 기반 암호를 제안하였다. 다음은 Weil-pairing과 같은 bilinear 함수를 적용한 초특이 타원곡선을 제외하고는 현재까지 알려진 GDH군은 존재하지 않는다.

- **Setup** :

$-H_1 : \{0,1\}^n \times G \rightarrow Z/p$, H_2 $\{0,1\}^n \rightarrow G$: 충돌 회피 함수

$-ID_B$: B의 ID

$-b(\in Z/p)$: 서명자 B의 마스터키

$-Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키

$-D_B = b \cdot H_2(ID_B) = bQ_B$

$-P_B = bP$: 공개키

- **Encrypt** :

① ID를 G상의 포인트 Q_{ID}로 변환한다.

② 랜덤 값 $\sigma \in \{0,1\}^n$를 생성하여 다음을 연산 $r = H_1(\sigma, M\})$

③ 다음을 계산하여 암호화

$$C = < rP, \sigma \oplus (g_{ID}^r), M \oplus G_1(\sigma) >$$

$g_{ID} = e(Q_{ID}, P_{pub}) \in F_{p2}$

- **Decrypt** :

① $C = < U, V, W >$라 하고 다음을 연산한다. $\sigma = V \oplus H(e(d_{ID}, U))$

② $M = W \oplus G_1(\sigma)$을 계산한다.

③ $r = H_1(\sigma, M)$을 계산하여 $U \neq rP$이면, 메시지를 거절하고 일치하면 암호문을 해독하게 된다. 다음은 차재춘과 천정희가 제안한 서명 방식이다.[Cheo02]

- **Sign** : 서명자 B는 난수 $r \in Z/p$를 선택하고, $U = rQ_B$, $h = H_1(M, U)$와 $V = (r+h)D_B$를 계산하여 $sig = (U, V)$를 메시지 M에 대한 서명으로 정의한다.

3. 제안 방법

이 논문에서는 AAA 환경에서의 새로운 ID 기반 인증 방식을 제안한다. 제안 방식은 2개의 랜덤 값을 생성하여, 이동 노드의 지수 연산 횟수를 감소시켜 계산적 부하를 줄이고, 생성된 2개의 랜덤 값을 이용하여 생성한 서명값으로 보안적 안전성을 확보한다. 제안은 Diameter 제공하는 EAP를 사용하여 인증을 수행하기 때문에, AAA 환경에서 추가적인 변환 없이 적용이 가능하다.

다음은 제안하는 ID 기반 AAA 인증 방식이 AAA 환경에서 작동 가능하기 위한 가정 사항이다.

① AAA 서버 간 교환 되는 메시지는 Diameter CMS 응용을 통해 기밀성과 무결성 보장.

② AAAH는 방문 도메인의 AAA client가 사용할 개인키를 생성은 SA가 설립후 생성하여 전달.
③ 이동 노드와 AAA 서버/클라이언트는 ID 기반 암호 연산의 수행이 가능.
④ AAAH 서버는 ID 기반 암호 시스템으로 개인키 생성 센터의 역할을 수행하여 이동 노드와 AAA client의 개인키를 생성하는 master key를 가짐.
⑤ 이 논문에서의 ID는 NAI를 사용.
⑥ HA는 개인키에 대응하는 NAI를 소유

Authentication Request 단계 :

① MN은 난수 $k_1, k_2 \in \{0,1\}^n$를 택하여 $M_{MN} = k_1 G,\ N_{MN} = k_2 G$를 계산한다.
② $\alpha_{MN} = x(M_{MN}), \beta_{MN} = x(N_{MN})$로 정의하고, $H(ID_{MN} \| ID_{Server} \| Time \| \beta_{MN}) = (a_{MN} + s_{MN}) \cdot \alpha_{MN} + k_1 \mu_{MN} mod q$를 만족하는 μ_{MN}을 구한다.
③ MN은 인증 서버에게 인증을 위해 $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$을 전송한다.

Authentication Respond 단계

인증 서버는 MN에게 받은 정보 $(r_{MN}, N_{MN}, \alpha_{MN}, \beta_{MN})$를 이용하여 다음을 계산한다

① $0<(r_{MN}, \alpha_{MN}, \beta_{MN})<p$ 와 $0<\mu_{MN}<q$ 를 확인한다.
② $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$의 정보를 이용하여 다음을 구성한다.
$r_{MN} H(ID_{MN}),\ M_{MN} = k_1 G,\ N_{MN} = k_2 G$
③ $V = r_{MN} P + R_{MN}$를 계산 후,
$H(ID_{MN} \mid ID_{Server} \mid Time \mid \beta_{MN}) G = \alpha_{MN} V + \mu_{MN} P_{MN}$를 검증하여 MN을 인증한다.

제안 방식의 인증은 Mobile IP의 등록과정과 연계되어 Diameter EAP 응용을 이용하여 인증이 수행되기 때문에 추가적인 Diameter의 변경 없이 적용이 가능하다. AAA 환경에서의 인증은 MN과 AAAH를 통해 이루어지고, Mobile IP와 관련하여 MN-FA-AAAH-HA의 통신이 이루어진다. AAA 환경에서의 모든 통신 메시지는 Diameter CMS Application을 통해 안전성을 제공 받기 때문에 AAA 인증 프로토콜은 AAA환경에서 인증 후에 안전한 통신을 위해 세션키가 생성되지 않는 특징을 갖는다. [그림 3.2]는 AAA 환경에서의 제안의 인증 과정을 나타낸다.

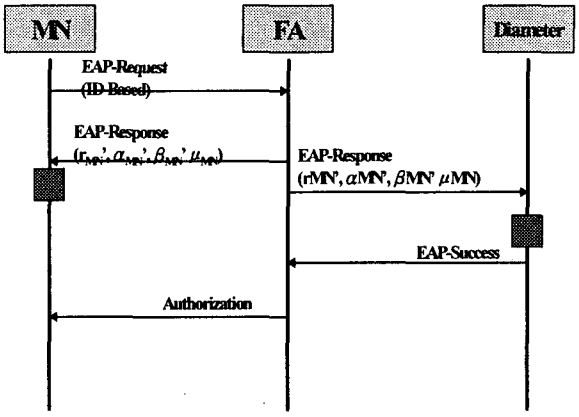

그림 3-2 제안 방식을 적용한 AAA 인증 과정

① 제안의 인증은 이동 노드가 FA의 EAP-Request 메시지를 수신하는 것으로 시작.
② 이동 노드는 방문 네트워크를 통해 인터넷에 접속 시, 2개의 난수, 자신의 ID, AAAH의 ID, Timestamp를 이용 인증 정보 $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$를 생성하고 EAP-Response 메시지에 포함해서 FA에게 전송..
③ FA는 EAP-Response 메시지를 수신 한 후, MN의 AAAH에게 EAP-Request 메시지를 전송한다. 이때, FA는 MN의 인증 정보인 $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$를 확인 할 수 없고, EAP-Response 메시지를 읽어 해당 AAAH에게 메시지를 전송한다.
④ AAAH는 이동 노드의 인증 정보 $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$를 확인하여 이동 노드를 인증한다. AAAH가 이동 노드 인증정보에 연산에 포함한 ID_{AAAH}의 정당한 소유자가 아니면 AAAH는 인증 정보를 확인할 수 없다. 이동 노드가 전송한 인증 정보에 포함된 ID_{MN}이 이동 노드의 인증 정보가 아니면 검증시 불가능 판정이 내려진다. MN이 정당한 사용자일 경우 AAAH는 MN에 관련된 Mobile IP 등록 과정을 진행한다. MN의 Mobile IP 등록 과정을 마친 후 EAP-Success 메시지를 FA에게 전송한다.
⑥ EAP-Success 메시지를 수신한 FA는 MN에게 네트워크 접근 권한 부여한다.

4. 평 가

이 절에서는 제안한 방식이 무선 환경에서 가능한 재사용 공격, 위장 공격, 공모공격, 알려지지 않은 키 공유 공격, KGC의 비밀키 노출에 대한 안전성을 검증한 후, 기존의 제안한 ID 기반 인증 방식과 비교 분석한다.

- 위장 공격 : 공격자는 (a_{MN}, s_{MN})의 값들을 획득해야 한다. 그러나 그것이 불가능하기 때문에 공격자는 임의의 $H(ID_{MN} \mid ID_{AAAH} \mid Time \mid \beta_{MN}')$를 생성하여 그것의 정당한 서명 값을 포함하여 $(r_{MN}', \mu_{MN}', \alpha_{MN}', \beta_{MN}')$값이 필요. 그러나 $(a_{MN} + s_{MN}) \cdot \alpha_{MN} + k_1 \mu_{MN} mod q$를 만족하지 못한다. 따라서 위장공격이 불가능하다.
- 공모 공격 : n명의 사용자들이 공모하여 KGC의 마스터키인 s_{KGC}를 알아내기 위해서는 자신들의 비밀 정보인 n개의 (r_A, s_A)를 가지고 연립방정식 $s_{A_i} = k_{a_i} + r_{a_i a_{KGC}} mod q (1 \leq i \leq n)$를 풀어야 한다. 그러나 모든 사용자에게 k_{A_i}는 비밀 정보이고 서로 다르게 주어지기 때문에 이 문제를 푸는 것은 불가능하다.
- KGC의 비밀 키 노출 : 제안한 스킴은 KGC의 비밀 정보가 노출되어도 MN의 인증 시 사용되는 비밀정보는 직접적으로 드러나지 않는다. 스킴에서 인증 시 서명 값을 생성하기 위해서는 MN만이 알고 있는 비밀 정보인 r_{MN}이 사용되는데 이것은 MN이 생성하는 것이기 때문에, 공격자가 s_A를 알더라도 인증 시 사용되는 고유한 r_{MN}값은 생성할 수 없다.

[표 4.1] 안전성 분석

	상호 인증	부인 방지	공모 공격	위장 공격	KGC의 S키노출
제안	Yes	Yes	Yes	Yes	Yes
기존 방식	Yes	Yes	No	No	No

Yes : 공격에 안전함 No: 공격에 안전하지 못함

제안하는 방식은 암호학적 연산 시 가장 많은 부하를 발생시키는 지수 연산의 횟수를 이동 노드에서는 줄이고 있다. 인증의 수행 시 2개의 랜덤 정수를 생성하고, 각 각의 서명 값을 인증에 사용한다. 제안은 이동 노드의 부하를 줄이기 위해 지수 연산을 AAAH서버의 인증 확인 과정에서 수행하도록 설계 하였다.

[표 4.2] 계산량 분석

		제안	기존 방식
통신 횟수(C)		2	2
랜덤 정수 생성횟수(R)	MN	2	1
	AAAH	0	0
지수연산(E)	MN	0	1
	AAAH	1	0
곱셈연산(M)	MN	2	3
	AAAH	2	2
해쉬 연산(H)	MN	1	3
	AAAH	2	3
노드별 수행시간	MN	2R+ 1E+ 2M+ 1H	1R+ 1E+ 3M+ 3H
	AAAH	2M+ 2H	2M+ 3H

5. 결 론

이동 통신의 발달과 사용자의 증가로 인하여, 여러 환경의 네트워크와 이종 기기간의 통신이 빈번하게 일어나고 있다. AAA의 최신 버전인 Diameter 표준이 상호인증과 부인방지를 제공하지 못하는 문제점과 PKI를 이용할 경우 이동 환경에 적용하기 어려운 단점을 보완하기 위해 ID 기반 AAA 인증 방식이 제안되었다. 기존 방식은 ID 기반 암호 방식과 제안한 서명 방식을 그대로 사용하여 공모 공격과 위장 공격에 안전하지 못했다. 또한 KGC의 Master key가 노출되면, 모든 사용자들의 개인키 생성이 가능해지는 단점을 가지고 있었다. 제안방식은 2개의 랜덤 값을 생성하여, 이동 노드의 지수 연산 횟수를 감소시켜 계산적 부하를 줄이고, 생성된 2개의 랜덤 값을 이용하여 생성한 서명 값으로 보안적 안전성을 확보한다. 제안은 Diameter 제공하는 EAP를 사용하여 인증을 수행하기 때문에, AAA 환경에서 추가적인 변환 없이 적용이 가능하다.

참고문헌

[1] Byung-Gil Lee, Hyun-Gon Kim; Concatenated Wireless Roaming Security Association and Authentication Protocol using ID-Based Cryptography Telecommunications, 2003. ICT 2003. 10th International Conference on , Volume: 1 , 23 Feb.-1 March 2003 Pages:597 - 603 vol.1

[2] Byung-Gil Lee, Doo-Ho Choi, Hyun-Gon Kim, "Mobile IP and WLAN with AAA Authentication Protocol using Identity-Based Cryptography" Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th I

EEE Semiannual , Volume: 3 , 22-25 April 2003 Pages:1507 - 1511 vol.3

[3] Kyungah Shim; "Efficient ID-based authent icated key agreement protocol based on W eil pairing "Electronics Letters ,Volume: 39 ,Issue: 8 ,17 April 2003 Pages:653 - 654

[4] J. C. Cha and J. H. Cheou "An Identity-Ba sed Signature from Gap Diffie-Hellman Gr oups," in Cryptology ePrint Archive, http:// eprint.iacr.or~2002/018/2002.

[5] Sufatrio, K. Y. Lam "Mobile IP Registrati on Protocol :A Security Attack and New S ecure Minimal Public-Key Based Authentic ation," in I-SPAN '99, June 1999.

[6] P.Calhoun, W.bully, S.Ferrel, "Diameter CM S Security Application", draft-ietf-aaa-dia meter-cms-sec-05.txt, IETF work in pregr ess, April, 2002

[7] A. Fiat and A. Shamir "How to prove yo urself: Practical solutions to identification and siganture problems," in Proc. Crypto '8 6, pp. 186-194 1986.

[8] D. Boneh and M. Franklin "Identity Based Encryption from the Weil Pairings,"in Proc. of Crypto 2001, LNCS vol. 2139, pp. 213-22 9,

[9] P.Calhoun, C.Perkins, "Diameter Mobile IPv 4 Application", IETF work inprogress 2002.

[10] Y. Zheng, "Digital signcryption or how to achieve cost(signature and encryption)<<co st(signature)+ cost(encryption)", Advances Cryptology-CRYPTO'97, LNCS 1294, Sprin ger-Verlag, pp. 165-179, 1997