이동단말을 위한 안전한 인증 알고리즘

고 훈°, 김선호, 신용태
대진대학교 컴퓨터공학과°, 동덕여자대학교 정보학부, 숭실대학교 컴퓨터학과
skoh21@daejin.ac.kr°, shkim98@dongduk.ac.kr, shin@comp.ssu.ac.kr

Secure Authentication Algorithm to Mobile Device

Hoon Ko°, Seonho Kim, Yongtae Shin
Dept. of Computing and Engineering , Daejin University°
Dept. of Information and Science, Dongduk Women's University
Dept. of Computing, Soongsil University

요 약

이동 환경에서 가장 심각한 정보 보호 위협 요소는 이동환경에서 Home Address Option(HAO)를 사용할 때 발생할 수 있는 공격을 어떻게 막을 것인가에 대한 것이고, 라우팅 헤더를 사용함으로써 발생할 수 있는 공격, 그리고 라우팅 헤더에 대한 공격, 바인딩 업데이트를 수행할 때 발생할 수 있는 공격으로부터 어떻게 방어할 것인가 이다. 이러한 위협들에 대해서 기밀성, 무결성 그리고 인증 서비스가 가장 중요한 정보보호 서비스 이다. 그중 인증은 신분 위장 및 재전송 위협으로부터 보호할 수 있으며 액세스 제어, 데이터 무결성, 기밀성, 부인봉쇄 들과 함께 연동 될 수 있다.

본 논문에서는 인증 기술을 이동단말에 적용하여 안전하고 빠른 인증처리를 위한 안전한 인증 알고리즘을 제안하고자 한다.

1. 서 론

인터넷의 정보보호 서비스는 기밀성, 무결성 그리고 인증 서비스 등이 있다. 그 중 인증은 신분 위장 및 재전송 위협으로부터 보호할 수 있으며 액세스 제어, 데이터 무결성, 기밀성, 부인봉쇄, 감사 서비스들과 함께 연동 될 수 있다.

인증 대상이 되는 것은 네트워크 사용자와 네트워크 장비, 그리고 컴퓨터에서 처리되고 있는 프로세스가 있다. 인증 과정에서 본인의 신분을 나타내고 본인임을 주장하는 주체를 신청자라 하고 이를 확인하는 주체를 검증자라고 한다. 인증은 신청자와 검증자 사이에 교환되는 정보에 의해서 수행된다.

이에 본 논문에서는 일방향 인증 기술을 이동단말에 적용하여 빠르고 안전한 인증처리를 진행 하고자 한다.

2. 관련연구

2.1 인증기술

인증이란 정보를 전송할 때 정보의 내용이 변조 또는 삭제되지 않았는지, 송·수신자가 정당한 사용자인지를 확인하는 방법이다.

인증의 종류는 메시지 인증과 사용자 인증으로 분류된다.

- 메시지 인증
  송·수신 되는 정보의 내용이 위·변조 또는 삭제되지 않았는지를 확인하는 방법
- 사용자 인증
  메시지의 생성, 전송, 수신, 이용, 저장 등 일련의 과정에 있는 주체가 정당한지를 확인하는 방법

2.2 일방향 인증

일반적으로 일방향 인증의 예는 다양하다. 즉 서버 접속 요구를 위한 Login 이나 전자 우편 등이 대표적인 예로 들 수가 있다. 이들은 사용자와 검증자가 동시에 메시지를 송·수신할 필요가 없다는 특징을 가지고 있다. 일방향 인증은 메시지의 의도된 수신자만이 그 메시지를 읽을 수 있다는 것을 보증한다.

그러나 재전송 공격에 대해서 취약하기 때문에 Time Stamp T를 삽입하는 것을 고려할 수도 있다.

[프로토콜]

① A는 Server S에게 다음의 메시지를 송신한다.
$ID_A \| ID_B \| N_1$

② S는 세션키와 A의 식별자를 B의 키로 암호화하여 B의 식별자, N1 및 세션키를 A의 비밀키로 암호화하여 A에게 전송한다.
$E_{K_B}[K_S \| ID_B \| N_1 \| E_{K_B}[K_S \| ID_A]]$

③ A는 수신된 정보를 복호화하여 검증한 후에, 다음의 정보를 B에게 전송한다.
$E_{K_B}[K_S \| ID_A] \| E_{K_S}(M)$

④ B는 수신된 정보의 복호화를 통해 KS를 확인한 다음 M을 확인함으로써 A를 인증하게 된다.

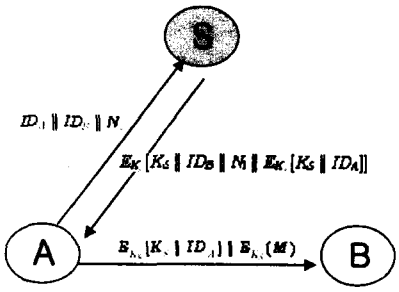

그림 1. 일방향 인증

3. 제안하는 인증 모델 및 분석

3.1 모델 설계

위에서 설명했듯이 기존 일방향 인증의 문제점은 재전송 공격에는 취약하다. 따라서 재전송 공격의 취약에 대한 문제점을 근본적으로 차단해야 한다. 그리고 서로 간에 정보를 전송할 때 사용되는 암호화 기법도 최근에는 암호화 하는데 소요되는 시간문제 때문에 인증을 위해서는 해쉬함수를 이용하는 방안이 강구되고 있다.

일단 재전송 공격을 근본적으로 차단하기 위해서는 A가 Server에게 전송하는 $ID_A \| ID_B \| N_1$ 정보를 암호화해서 전송해야 한다. 그리고 그 이후에 전송되는 메시지에 대해서는 해쉬함수를 이용하는 방법을 제안한다.

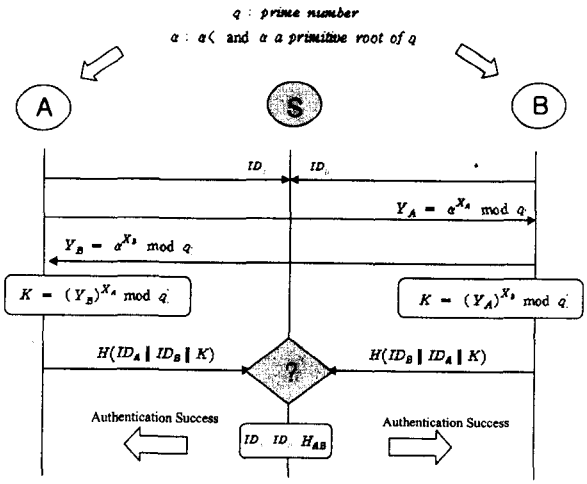

그림 2. 제안 모델

[기호설명]

- H : 해쉬함수에 의해서 처리
- ID_A : A 단말기의 개인 키
- ID_B : B 단말기의 개인 키
- H_{AB} : 단말기 A, B의 해쉬 값

그림 2는 제안하는 모델을 보여주고 있다.

Mobile Device A Side

Define :

q : *prime number*

α : $\alpha <$ and α *a primitive root of* q

ID_A *Send to S*

$Y_B = \alpha^{X_B} \bmod q$

$K = (Y_B)^{X_A} \bmod q$

$H(ID_A \| ID_B \| K)$

H Send to S

Mobile Device B Side

Define :

q : *prime number*

α : $\alpha <$ and α *a primitive root of* q

ID_B *Send to S*

$Y_A = \alpha^{X_A} \bmod q$

$K = (Y_A)^{X_B} \bmod q$

$H(ID_B \| ID_A \| K)$

H Send to S

Server Side

Receive ID_A, ID_B

Receive $H(ID_A \| ID_B \| K)$ *From A*

Receive $H(ID_B \| ID_A \| K)$ *From B*

if $(H(ID_A \| ID_B \| K) == H(ID_A \| ID_B \| K))$

then

Authentication Success

else

Authentication Fail

[단계설명]

[단계 1] 이동단말 A와 B는 서로 인증을 하기 전에 Server에게 개인의 ID 전달한다. 그리고 DH의 규칙에 맞게 K값을 생성한다. 이 K 값은 A와 B 이외에는 어느 누구도 알지 못한다. 따라서 A와 B의 ID는 공개되고 서로 간에 생성한 K는 비공개된다.

[단계 2] A와 B는 각각의 ID와 K값을 해쉬함수로 처리한 후 Server에게 전달한다.

[단계 3] Server는 A와 B로부터 해쉬값을 받게 된다. 그리고 그 값을 비교하게 된다.

[단계 4] 값이 같으면 서로에게 인증성공 메시지를 전송하고 같지 않으면 인증실패 메시지를 전송하게 된다.

3.2 모델 분석

이동단말과 Server의 역할을 살펴보면 이동단말은 DH 기법을 이용하여 K값을 생성한다. K값은 비공개이기 때문에 제3자가 알 수 없다. 즉 A와 B 서로만이 알고 있는 K값고 공개된 각각의 ID 값을 이용해서 해쉬함수로 처리 했다 하였을 경우, 이 값은 A와 B가 서로 비교를 해서 같음의 유무를 통해서 서로 간에 인증을 할 수 있다. 만약 제3자가 ID값은 변경해서 전송하면 Server는 이를 발견해서 무결성에 문제가 있음을 간파할 수 있다.

또한 굳이 Server에게 해쉬값을 전송한 이유는, Server는 이 값을 저장하고 있다가 차후에 제3자가 마치 A와 B인 것처럼 인증을 요청하였을 경우를 대비하기 위함이다. 이 경우 제3자는 K값을 알지 못하기 때문에 원래의 A와 B의 해쉬값과 다른 값을 Server에 전송해서 인증을 요청하기 때문에 Server는 이를 발견하여 처리할 수 있다.

4. 향후과제

지금까지 설명한 DH 키 교환 알고리즘을 이용하여 쌍방간에 인증을 위해서 사용한 모델이다. 본 모델에서 서버는 단순히 이동단말들이 처리해서 전송해오는 정보를 저장하여 비교하여 처리하는 역할을 담당한다. 따라서 서버의 부담은 그리 많지 않을 듯 하다. 향후 본 모델을 실험을 통하여 증명할 계획이다.

5. 참고문헌

[1] A. Al Jabri, Security of private-key encryption based on array codes, Electronics Letters 32(24)(1996) 2226~2227.

[2] Chang-Seop Park, Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems, ScienceDirect, October, 2003

[3] R.M. Campello de Souza, J. Campello de Souza, Array codes for private-key encryption, Electronics Letters 30(17)(1994) 1394~1396

[4] Thomas, R., H. Gilbert and G. Mazzioto: Influence of the mobile station on the pperformance of a radio mobile cellular network, Proc. 3rd Nordic

[5] R. Jain, T. Raleigh, C. Graff and M. Bereschinsky: Mobile Internet Access and QoS Guarntees using Mobile IP and RSVP with Location Registers, in Proc. ICC'98 Conf., pp.1690~1695, Altanta.

[6] D. Maughan, M. Schertler, M. Schneider, J. Turner. Internet Security Association and Key Management Protocol(ISAKMP), (I-D draft-ietf-ipsec-isakmp-07.txt), February 21. 1987