한국항행학회 논문지 제12권 제5호 2008년 10월

모바일 환경의 AAA 메커니즘에서 디바이스 인증 기술에 관한 연구

A Study on Device Authentication Technology in AAA Mechanism of Mobile Environment

박종혁*

Jong-Hyuk Park*

요 약

유무선 통합 환경의 도래와 모바일 디바이스의 대중화로 모바일 환경에서 디바이스를 이용한 다양한 서비스를 제공받고자 하는 수요가 급속도록 증가하고 있다. 그러나 모바일 환경에서는 유선 환경의 보안 위협사항 뿐만 아니라 무선 환경에서 나타날 수 있는 많은 위협에 노출되어 있다. 이러한 문제점에 따라 모바일 환경에서 디바이스를 이용해 서비스를 제공받는데 있어 안전하고 효율적인 보안 기술이 필요하다. 따라서 본 논문에서는 모바일 환경에서 안전한 서비스 제공을 위해 AAA (Authentication, Authorization, Accounting) 메커니즘에서 디바이스 인증 기술에 관한 연구를 진행한다.

Abstract

With the advancement of the mobile device and arrival of the integrated wired / wireless environments, the demand for services accessible by mobile devices is rapidly increasing. However, unlike existing wired networks, communication in wireless networks has many weaknesses. Therefore, research and development into an appropriate security technology has reached a critical stage, as combined wired/wireless environments emerge. Therefore, in this paper, we propose that device authentication technology in AAA (Authentication, Authorization, Accounting) mechanism of mobile environment for secure service offer.

Key words : Device, Mobile Network, Authentication, AAA

I. 서 론

유무선 통합 환경의 도래와 모바일 디바이스의 대중화로 인해 사용자들에게 다양한 서비스를 제공하게 될 것이며, 사용자들은 모바일 디바이스를 이용하여 이동하면서도 서비스를 지속받기를 원함에 따라 이에 대한 수요는 빠른 속도로 증가하고 있다. 차세대 이동통신의 국내 시장규모를 보면 서비스가 모바일 환경에서 디바이스를 이용한 서비스 이용은 유비쿼터스 환경의 중심 서비스로 발전할 것으로 예상되고 있다.

그러나 현재의 발전 예상과 다양한 서비스와는 반

* 경남대학교 컴퓨터공학부(Dept. of Computer Science and Engineering)
· 교신저자 (Corresponding Author) : 박종혁
· 투고일자 : 2008년 9월 2일
· 심사(수정)일자 : 2008년 9월 3일 (수정일자 : 2008년 9월 30일)
· 게재일자 : 2008년 10월 30일

대로 무선 환경이라는 특성으로 인해 기존의 유선망보다 다양한 위협사항 및 취약점을 가지고 있다. 즉 무선 환경에서 모바일 디바이스에 대한 도청, DoS (Denial of Service), Man-in-the-middle Attack, 디바이스 위장, 개인 프라이버시 침해 등의 다양한 위협에 노출되어 있으며, 또한 기존의 무선 환경에서 일어날 수 있는 다양한 위협을 그대로 가지고 있다. . 이러한 여러 취약점이 존재함에 따라 본 연구에서는 모바일 환경에서 안전하고 효율적인 서비스 제공을 위한 AAA [1],[3]-[6],[9],[10] 메커니즘에서 디바이스 인증 기술에 관한 연구를 진행한다. 본 논문의 구성은 다음과 같다. 2장에서는 보안 요구 사항에 대하여 기술하고 3장에서는 기존에 연구된 AAA 및 인증방식을 분석한다. 4장에서는 안전한 디바이스 인증 기술을 제안하고, 5장에서는 제안 방식을 분석하여 마지막으로 6장에서는 결론 및 향후 연구 방향으로 마치도록 한다.

Ⅱ. 보안 요구 사항

모바일 환경은 다양한 위협사항이 존재할 수 있기 때문에 그에 따른 보안 요구 사항을 만족해야 한다.

2-1 보안 위협 사항

모바일 환경에서 서비스를 제공받는데 있어 발생할 수 있는 보안 위협 사항은 다음과 같다.

- 개인정보 유출 : 제 3자의 불법적인 접근에 의한 개인정보 유출로 개인 식별 정보뿐만 아니라 결재 정보 등 가입자에게 금전적 손해를 입힐 수 있는 정보까지 유출될 가능성이 존재한다.
- 신분위장 : 안전하지 않은 통신로 상에서는 악의적인 제 3자가 정당한 가입자처럼 위장하여 인증을 받거나 서비스를 제공받을 수 있다. 이에 제 3자가 정당한 가입자처럼 접근하는 것에 대한 안전성을 제공해야한다.
- 세션 하이재킹 : 세션 하이재킹은 서버나 시스템에 대한 인증 절차를 건너뛸 수 있는 공격방법이다. 우선 공격자는 서비스 거부 공격과 같은 방법으로 사용자가 세션 연결을 유지할 수 없도록 한 후 서버로의 세션을 가로채 시스템에 로그온 하지 않고 접근 권한을 획득하게 된다. 하이재킹을 통해 세션을 훔치는 것뿐만 아니라 서버와 사용자가 주고받는 모든 정보를 도청할 수도 있다 [6].
- 데이터 도청 : 통신 채널에서 전송되는 데이터가 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다.

2-2 보안 요구 사항

서비스를 제공하는데 있어 기본적으로 만족시켜야 하는 보안 서비스는 다음과 같다.

- 기밀성 : 통신에 사용되는 데이터는 정당한 개체만이 확인할 수 있어야 한다. 데이터의 출처와 목적지, 횟수, 길이, 또는 통신 선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다. 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다.
- 무결성 : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다. 전송된 데이터의 무단 변경을 감지할 수 있게 하기 위해 전자 서명 등을 이용한다.
- 인증 : 인증 서비스는 통신이 기밀성을 갖도록 보증하는 것이 중요하다. 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어 : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다. 시스템에서는 운영체제의 접근 통제 기능을 사용하며 네트워크에서는 침입차단 시스템을 사용해서 접근 통제 수준을 높일 수 있다. 또한 서비스 이용에서

는 정당하지 않은 사용자는 서비스를 이용할 수 없다.

Ⅲ. 기존 연구

기존에 연구된 AAA 및 인증 방식의 개요에 대하여 알아보고 각 방식이 가지는 장/단점을 분석한다.

3-1 KERBEROS

가장 대표적인 티켓 방식으로 사용자에게 서비스를 안전하게 이용할 수 있도록 인증 서비스를 제공하는 있는 Kerberos [8] 가 있다. Kerberos는 중앙 집중식 인증 서버를 사용하고, 암호화 방식은 대칭키 암호화 방식을 사용하여 인증을 수행한다. 사용자가 서비스를 제공받기 위해서는 인증 서버에서 티켓-승인 티켓을 발급 받고, 티켓 발행 서버에서 서비스-승인 티켓을 발행 받아 서비스를 이용하게 된다. 각각의 Kerberos 구성요소에 접근하기 위해서는 사전에 약속된 패스워드를 기억하고 있어야 한다. 현재 Kerberos 프로토콜은 버전 4에서 버전 5까지 개발되었으며 이는 IETF (Internet Engineering Task Force) RFC 4120에 표준화 되어 있다. 이러한 Kerberos 프로토콜의 경우 패스워드의 취약점을 안고 있으며, 티켓 발행 서버가 세션키를 분배해주기 때문에 사용자와 서비스 제공 서버사이에 전송되는 메시지 정보를 알 수가 있어 익명성과 프라이버시를 제공하지 않는다. 또한 Kerberos 서버가 인증 서버와 티켓 발행 서버로 분리되어 있어 인증 요청 시 지연이 발생할 수 있는 문제점을 안고 있다.

3-2 익명성과 프라이버시 보장을 위한 인증방식

익명성과 프라이버시 보장을 위한 인증 방식에서는 인터넷을 통해 다양한 콘텐츠 서비스를 사용자가 편리하게 이용할 수 있도록 EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) 인증 방식과 SKKE (Symmetric-Key Key Establishment) 방식을 이용하여 보다 효율적인 인증 메커니즘을 설계하였다. 제안하는 메커니즘에서는 사용자가 인증서 방식을 통해 AAA 서버로부터 인증을 받으면 인증 서버와 가맹 관계에 있는 콘텐츠 제공자에는 별도의 로그인 과정 없이 서비스를 이용할 수 있는 SSO (Single Sign On) 서비스, 사용자 익명성 및 프라이버시를 제공한다. 사용자가 익명성을 필요로 하는 콘텐츠 서비스를 이용할 경우 사용자의 익명성을 보장 해주며 사용자와 콘텐츠 제공자가 안전하게 데이터를 전송하기 위해 사용 할 세션키를 인증 서버에게 노출시키지 않고 교환한다. 콘텐츠 제공자 마다 다른 세션키를 사용함으로서 사용자의 프라이버시를 보장해 준다 [7].

3-3 모바일 커머스 AAA 메커니즘

무선랜은 빠르게 차세대 모바일 통신에서 중요한 구성 요소가 되고 있다. 이러한 성공에도 불구하고 사용자의 프라이버시와 접근 제어, 인증과 같은 문제점은 과금의 문제점과 함께 부각되고 있다. 특히, 과금 분야에서 IP 기반의 패킷 과금에 관한 연구는 서비스 제공자에게 과금을 위한 고정된 합산 시스템 도입의 어려움을 가져오고 있다. 따라서 본 방식은 모바일 커머스와 검증 결과를 위해 국제 표준과 상호 운용성을 가지는 패킷 과금을 제안하였다 [2]. 그러나 과금 확인 및 Recharge를 위한 단계를 따로 거쳐야 하며, 홈 인증 서버와 Billing 서버로 집중되는 오버헤드가 증가되는 단점을 가지고 있다.

Ⅳ. AAA 메커니즘에서 디바이스 인증 기술

모바일 환경의 AAA 메커니즘에서 디바이스 인증 기술은 모바일 네트워크 환경에서 디바이스가 홈 인증 서버로부터 인증을 받고 인가 티켓을 발급받아 서비스에게 인가 티켓을 제시하고 서비스를 제공받을 수 있다. 또한 디바이스가 다른 사업자가 제공하는 서비스를 이용할 경우 외부 홈 도메인에 내부 홈 도메인에서 발급받은 인가 티켓을 제공하고 인증을 받고 서비스를 제공받을 수 있다.

4-1 시스템 계수

AAA 메커니즘에서 디바이스 인증 기술에서 사용되는 표기법은 다음과 같다.

- * : 각각의 개체 (D : 디바이스, $AAAH$: 홈 네트워크 인증 서버, $AAAL$: 외부 네트워크 인증 서버, SP : 서비스 서버)
- ID_* : *의 아이디
- PW_* : *의 패스워드
- CT : D와 $AAAH$ 간에 동기화되어 있는 카운터
- g : 곱셈군 Z_n^* 의 생성자
- $h(\ )$: 충돌성이 없는 안전한 일방향 해쉬 함수
- $E_*[\ ]$: *의 키로 암호화
- $Sign_*$: *의 개인키로 서명
- KS : D와 $AAAH$가 공유한 대칭키
- $Service-key$: $AAAH$와 SP가 공유한 서비스키
- KU_* : *의 ID 기반 공개키
- KR_* : *의 ID 기반 개인키

4-2 제안 프로토콜

제안 프로토콜은 모바일 네트워크에서 디바이스 인증 및 인가 티켓 발행 단계, 외부 네트워크에서 디바이스 인증 단계로 이루어지며, 디바이스와 홈 네트워크 인증 서버 간 공유한 대칭키는 사전에 분배되었다고 가정한다.

가. 디바이스 인증 및 인가 티켓 발행 단계

디바이스가 자신의 홈 네트워크 인증 서버에게 인증을 요청하면 인증 서버는 사용자 권한에 맞는 인가 티켓을 발행하고 서비스 서버에게 디바이스의 인가 티켓과 아이디를 브로드캐스팅한다. 디바이스는 서비스를 이용할 때 인가 티켓을 제시하고 서비스를 제공받는다.

① 디바이스는 디바이스의 일련번호, 대칭키와 카운터를 XOR 연산 후 해쉬 하여 패스워드를 생성하고 ID기반 개인키/공개키 쌍을 생성한다. 그리고 인증 요청을 위해 디바이스의 아이디, 홈 인증 서버의 아이디, 패스워드와 카운터를 대칭키로 암호화 하여 전송한다.

$$\begin{aligned} &PW = h(PIN \oplus KS \oplus CT) \\ &KU_D = ID_D \\ &KR_D = ID_D \cdot g^{PW} \\ &ID_D,\ ID_{AAAH},\ E_{KS}[PW,\ CT] \end{aligned} \tag{1}$$

② 홈 네트워크 인증 서버는 전송된 값과 데이터베이스에 저장되어 있는 값을 통해 패스워드를 생성하고 디바이스가 전송한 패스워드와 비교하여 인증한다. 인증이 완료되면 홈 네트워크 인증 서버의 ID 기반 개인키/공개키 쌍을 생성하고 인가 티켓을 생성한 후, 디바이스의 ID 기반 공개키로 암호화 하여 전송한다.

$$\begin{aligned} &PW' = h(PIN \oplus KS \oplus CT) \\ &KU_{AAAH} = ID_{AAAH} \\ &KR_{AAAH} = ID_{AAAH} \cdot g^{PW} \\ &Authorization\ Ticket = ID_D, ID_{AAAH} \\ &, Sign_{AAAH}[h(PW)] \\ &E_{KU_D}[Authorization\ Ticket] \end{aligned} \tag{2}$$

③ 디바이스는 전송된 티켓에 포함되어 있는 패스워드를 검증한다.

$$D_{KR_D}[E_{KU_D}[Authorization\ Ticket]] \tag{3}$$

④ 홈 네트워크 인증 서버는 서비스 서버들에게 사전에 공유한 서비스키로 디바이스의 아이디와 인가 티켓을 암호화하고 서명하여 브로드캐스팅 한다.

$$\begin{aligned} &E_{Service-key_{AAAH-SP}}[Sign_{AAAH}[ID_D, \\ &Asuthorization\ Ticket]] \end{aligned} \tag{4}$$

⑤ 디바이스는 서비스 서버에게 티켓을 제시하면 서비스 서버는 티켓을 검증한 후 디바이스에게 서비스를 제공한다.

나. 외부 네트워크에서 디바이스 인증 단계

이 단계에서는 디바이스가 다른 네트워크로 이동하여 모바일 서비스를 이용할 경우 외부 네트워크 인증 서버에게 홈 네트워크 인증 서버로부터 발급받은 인가 티켓을 제공하고 인증을 받고 서비스를 제공받을 수 있다.

① 디바이스는 외부 네트워크 인증 서버에게 홈 네트워크 인증 서버로부터 발급받은 인가 티켓을 홈 네트워크 인증 서버의 공개키로 암호화하여 아이디와 함께 전송한다.

$$ID_D, ID_{AAAH}, E_{KU_{AAAH}}[Authorization\ Ticket] \quad (1)$$

② 외부 네트워크 인증 서버는 홈 네트워크 인증 서버에게 디바이스로부터 전송받은 값을 전달하고, 홈 네트워크 인증 서버는 인가 티켓을 검증한 후, 서비스에 접근할 수 있는 인가 티켓을 서명한 후 외부 네트워크 인증 서버에게 전송한다. 외부 네트워크 인증 서버는 전송받은 티켓을 외부 서비스 서버에게 브로드캐스팅한다.

$$E_{KU_{AAAH}}[Authorization\ Ticket] \quad Sign_{AAAH}[Authorization\ Ticket] \quad E_{service-key_{AAAL-SP}}[Sign_{AAAL}[ID_D, Authorization\ Ticket]] \quad (2)$$

③ 디바이스는 외부 서비스 서버에게 티켓을 제시하면 스트리밍 서버는 티켓을 검증한 후 디바이스에게 서비스를 제공한다.

Ⅴ. 제안 방식의 분석

제안 방식을 앞에서 언급한 보안 요구 사항에 맞추어 분석하면 다음과 같다.

5-1 보안 위협 사항에 따른 분석

- 개인정보 유출 : 제 3자의 불법적인 접근 및 해킹에 의해 사용자의 개인정보가 유출될 수 있으며, 이에 따라 금전적 손해까지 피해를 입힐 수 있다. 따라서 개인정보 유출 방지를 위해 전송로상의 데이터는 암호화하여 전송하고, 인증 및 인가 정보를 티켓으로 구성하여 개인의 정보를 최소화하고자 하였다.
- 신분위장 : 제 3자가 정당한 사용자처럼 위장하여 불법적으로 접근하여 인증을 받거나 서비스를 이용할 수 있다. 따라서 제 3자가 정당한 가입자로 위장하는 것을 막기 위해 카운터 동기화 패스워드를 이용하며, ID 기반 공개키/개인키 쌍으로 암호화시키기 때문에 신분위장으로부터 보호할 수 있다.
- 세션 하이재킹 : 공격자는 통신로상의 세션을 가로채 정당한 절차 없이 접근권한을 획득할 수 있다. 또한 하이재킹을 통해 세션을 훔치는 것뿐만 아니라 서버와 사용자가 주고받는 모든 정보를 도청할 수도 있다. 따라서 카운터 기반 패스워드로 세션의 제한시간을 설정하였으며, 세션을 가로채더라도 인증 값을 알 수 없어 하이재킹으로부터 안전하다.
- 데이터 도청 : 통신 채널에서 전송되는 데이터가 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다. 비밀 값 구성 시 해쉬 값으로 데이터의 무결성 및 비밀 값을 유출할 수 없도록 하였다.

5-2 보안 요구 사항에 따른 분석

- 기밀성 : 통신에 사용되는 데이터는 정당한 개체만이 확인할 수 있어야 한다. 제안 방식은 디바이스와 홈 네트워크 인증 서버간 사전에 공유한 대칭키와 ID 기반 공개키/개인키 쌍으로 각 단계마다 암호화하여 전송하기 때문에 기밀성이 제공된다.
- 무결성 : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파

괴되지 않도록 해야 한다. 제안 방식은 해쉬 값을 이용하여 무결성을 보장한다.

- 인증 : 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다. 제안 방식은 카운터 동기화 패스워드를 사용하여 사용자를 인증하며, 인가 티켓을 검증함으로써 인증 서비스를 제공할 수 있다.
- 접근제어 : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다. 정당하게 인증을 받지 않은 디바이스는 인가 티켓을 발급받을 수 없기 때문에 외부 네트워크나 서비스를 제공받을 수 없다.

Ⅵ. 결 론

유무선 통합 환경의 도래와 모바일 디바이스의 대중화로 인해 사용자들에게 다양한 서비스를 제공하게 될 것이며, 사용자들은 모바일 디바이스를 이용하여 이동하면서도 서비스를 지속받기를 원함에 따라 이에 대한 수요는 빠른 속도로 증가하고 있다. 차세대 이동통신의 국내 시장규모를 보면 서비스가 모바일 환경에서 디바이스를 이용한 서비스 이용은 유비쿼터스 환경의 중심 서비스로 발전할 것으로 예상되고 있다. 그러나 현재의 발전 예상과 다양한 서비스와는 반대로 무선 환경이라는 특성으로 인해 기존의 유선망보다 다양한 위협사항 및 취약점을 가지고 있으며, 보안 기술 개발이 필요하다.

본 연구는 모바일 서비스 제공을 위한 AAA 메커니즘에서의 디바이스 인증 기술에 관한 연구를 진행하였으며, 모바일 디바이스를 이용하여 서비스를 제공받는데 있어 안전하고 효율적으로 서비스를 제공받을 수 있도록 하였다. 가입자 인증을 위해 카운터 기반 패스워드 및 인가 티켓 방식을 이용하였으며, 홈 네트워크에서 서비스를 제공받다가 외부 네트워크로 이동하더라도 인가 티켓을 이용하여 모바일 서비스를 지속적으로 제공받을 수 있다. 향후 AAA 표준과의 호환성을 제공할 수 있는 방안에 대한 모색 및 과금 서비스 제공을 위한 연구가 진행되어져야 한다.

감사의 글

이 논문(저서)은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2008-0174).

참 고 문 헌

[1] Bhrat Patel and Jon Crowcroft, “Ticket based service access for the mobile user,” *In Third annual ACM/IEEE internaional conference on Mobile computing and networking,* pp.223-233, 1997.

[2] Gwanyeon Kim, Chinu Lee, Sehyun Park, Ohyoung Song, and Byungho Jung, “A Study on Mobile Commerce AAA Mechanism for Wireless LAN,” *HSI 2003*, pp.719-724, 2002.

[3] Jung-Min Park, Eum-Hui Bae, Hye-Jin Pyeon, and Kijoon Chae, “A Ticket-Based AAA Security Mechanism in Mobile IP Network,” *ICCSA*, pp. 210-219, 2003.

[4] 김동현, “Mobile IP를 위한 티켓 기반 AAA 서비스에 대한 연구,” *연세대학교 대학원*, 2002.

[5] 김봉주, “차세대 인증 프로토콜 DIAMETER AAA 기술 동향,” *TTA 기술표준이슈*, 2001.

[6] 김현곤, 이병길, 최두호, 유상근, 김말희, 이해동, 유희종, “AAA 정보보호 기술 표준화 동향,” *전자통신동향분석*, 제20권, 제1호, 2005.

[7] 이동명, 최효민, 이옥연, “익명성과 프라이버시 보장을 위한 효율적인 인증 메커니즘 설계,” *한국정보처리학회 추계학술발표대회*, pp.941-944, 2005.

[8] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, “The Kerberos Network Authentication Service,” RFC 4120, 2005.

[9] John Vollbrecht, Pat calhoun, Stephen Farrell, Leon Gommans, George Gross, Betty de Bruihjn, Cess Laat, Matt Holdrege and David Spence, “AAA Authorization Framework,” RFC 2904, 2000.

[10] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “Diameter Base Protocol,” RFC 3588, 2003.

박 종 혁(朴鍾焃)

2001년 순천향대학교 공학사
2003년 고려대학교 공학석사
2007년 고려대학교 공학박사
2002년 한화 에스엔씨 기술연구소
2007년~현재 경남대학교 컴퓨터공학부 전임강사
관심분야 : AAA, 접근제어, 멀티미디어 보안 및 서비스, 유비쿼터스 컴퓨팅