홈 네트워크를 위한 자동화된 사용자 인증 메커니즘

이창욱*, 이형수**, 장훈*, 김석윤*
*숭실대학교 컴퓨터학과
**전자부품연구원 지능형정보연구센터
e-mail:changuk@ssu.ac.kr
hslee@keti.re.kr
hoon@ssu.ac.kr
ksy@ssu.ac.kr

Automatic user authentication mechanism for home network

Changuk I*, Hyung Su Lee**, Hoon Chang*, Seok-Yoon Kim*
*Dept of Computer, Soongsil University
**Intelligent IT System Research Center, KETI

요 약

본 논문에서는 홈 네트워크 환경을 위하여 다양한 정보가전들에 서비스를 제공하고 운용하기 위해 OSGi 프레임워크를 이용하여 게이트웨이를 구성하였다. 홈 네트워크의 특성상 네트워크를 구성하는 정보가전들의 입력 수단에 대한 제약이 많고 자원이 한정적이다. 따라서 이러한 문제를 해결하기 위해 사용자에게 패스워드를 입력받지 않고 자동으로 인증 과정을 마치는 인증 메커니즘을 연구하였다. 패스워드를 입력받지 않음으로써 사용자 입력 대기 시간을 줄일 수 있고, 대칭키를 이용하여 암호화 과정의 연산량을 줄여 소규모로 구성되는 홈 네트워크 구조에 효율적으로 적용할 수 있었다.

키워드 : 홈 네트워크, OSGi, 사용자 인증 메커니즘

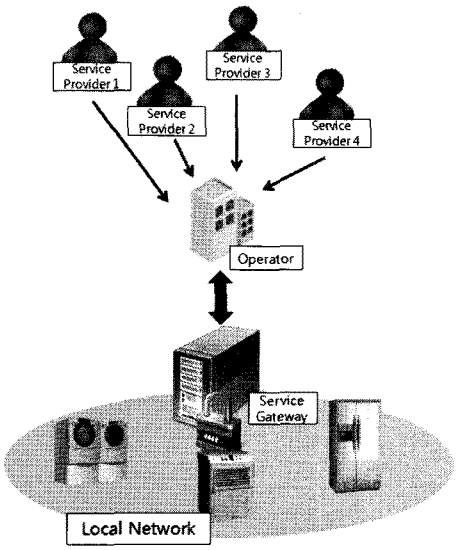
I. 서론

홈 네트워크는 가정의 다양한 장비들을 연결하여 서로 통신을 할 수 있게 하는 것으로 특성상 이기종의 다양한 정보가전들이 한정된 네트워크 자원을 이용한다. 본 논문에서는 이러한 이기종 디바이스들에 서비스를 전달하고 전달된 서비스를 운용하기 위하여 OSGi[1](Open Service Gateway Initiative) 개방형 스펙을 이용하여 게이트웨이를 구성하였다. OSGi 서비스 플랫폼 환경은 개방된 게이트웨이에 대한 보안 취약성이 발생하기 때문에 OSGi 환경에서는 인증 및 권한부여와 같은 보안 아키텍처의 구축이 필수적이다. 현재 학계에서는 OSGi 플랫폼 환경을 위한 향상된 보안 모델에 대한 연구가 진행중이다.[2] 그리고 OSGi 스펙에서는 아직까지 보안 아키텍처에 관한 구체적인 명세화가 없기 때문에 OSGi 환경을 위한 보안 아키텍처의 명세화가 필요하다.[3]

OSGi 플랫폼 환경의 특성상 사용자 인증 서버와 서비스를 제공하는 번들 서버(bundle server) 그리고 게이트웨이를 각각의 물리적인 장비로 나누는 것은 시스템 개발의 복잡성을 초래할 수 있고 시스템 구현 비용에 대한 부담이 증가하므로 이러한 기능들을 하나의 서비스 게이트웨이에 통합하여 구성하는 것이 바람직하다. 따라서 본 논문에서는 인증 서버와 번들 서버를 서비스 형태로 구현하여 서비스 게이트웨이에 배치하였다.

<그림 1>은 서비스 게이트웨이에 인증 서비스와 번들 서비스를 구현한 OSGi 서비스 플랫폼 기반의 홈 네트워크 구성도이다. 로컬 네트워크에는 다양한 이기종의 정보가전들로 이루어지며 서비스 게이트웨이에는 OSGi 프레임워크에 인증 서버와 번들 서버의 기능을 번들 서비스 형태로 구현하였다. 오퍼레이터는 서비스 게이트웨이의 요청을 받아 필요한 번들 서비스를 서비스 제공자에게 받아서 배포하는 것이다.

※ 지식경제부 지역산업기술개발사업의 "PAMP(Personal Area Media Platform)용 개인화 미디어 게이트웨이 시스템 기술개발" 지원을 받아 수행된 연구임.



〈그림 1〉 OSGi 서비스 플랫폼 기반의 홈 네트워크 구성도

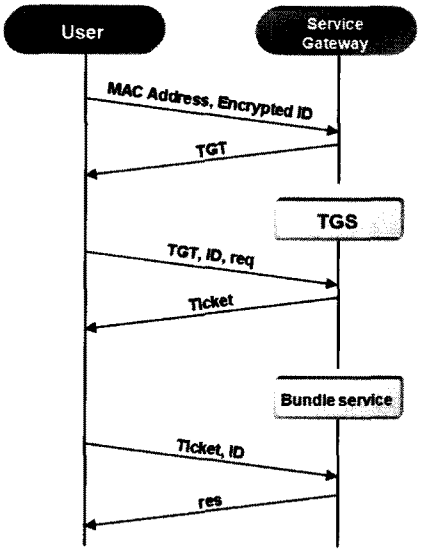
본 논문에서는 홈 네트워크를 위한 OSGi 서비스 플랫폼 기반의 자동화된 사용자 인증 메커니즘을 제안한다. OSGi 서비스 플랫폼은 일반적으로 소규모의 네트워크 구조로 구성되며 사용자의 디바이스에 문자 입력에 대한 제약이 따를 수 있다. 이러한 특성을 고려하여 기존의 패스워드 입력 방식이 아닌 사용자의 접속에 따라서 패스워드 입력 없이 인증 과정을 거치는 자동화된 사용자 인증 메커니즘을 제안한다.

II. 본론

일반적으로 기존의 사용자 인증 메커니즘은 사용자에게 식별자와 패스워드를 입력받아 인증 서버에 그 정보를 전달하여 정당한 사용자임을 판별하는 방식으로 구성된다. 그러나 홈 네트워크 환경에서의 정보가전과 같은 입력 수단이 제한적인 디바이스에서는 사용자가 접속을 원할 때마다 패스워드를 묻는 이러한 방식의 적용이 효율적이지 못하다.

본 논문에서는 자동화된 사용자 인증 메커니즘을 위하여 Kerberos 프로토콜[4]을 변형하여 적용하였다. Kerberos 프로토콜은 가장 기본적인 키(Key)를 이용한 암호화 방법으로써 인증(Authentication), 무결성(Identity), 데이터보안(Privacy)을 제공한다. Kerberos 프로토콜은 키를 배포하는 역할을 수행하는 KDC(Key Distribution Center)와 서비스를 제공받기 위한 티켓을 발행하는 TGS(Ticket Grating Service)로 구성되어 있다.

홈 네트워크 환경에서는 불특정다수가 접근하는 웹서버와 달리 정해진 수의 디바이스들과 한정적인 공간에서 서비스가 이루어진다. 이러한 환경에 맞추어 Kerberos 프로토콜의 KDC, TGS와 같은 서비스를 번들로 구현하여 하나의 서버에 기능을 통합하여 구현한다면 서버 구축의 효율성을 높일 수 있다. 따라서 본 논문에서는 전반적인 인증 서비스를 하나의 게이트웨이 서버에 번들 형태로 구성하여 OSGi 플랫폼 환경을 구축하였다.



〈그림 2〉 사용자 인증 메커니즘 순서도

〈그림 2〉는 본 논문에서 제안하는 Kerberos 프로토콜을 변형한 자동화된 사용자 인증 메커니즘의 순서도이다. 사용자 인증 메커니즘은 서비스 게이트웨이 인증 서비스의 사용자 인증 과정과 TGS의 서비스 티켓 발급 과정, 그리고 번들 서비스의 권한 부여 과정까지 총 3단계의 과정으로 이루어져 있다.

첫 번째는 사용자 인증 과정이다. 보안 메커니즘의 가장 기본이 되는 과정으로 사용자가 서비스 게이트웨이에 사용자 정보를 전송하고 서비스 게이트웨이는 이를 토대로 사용자에게 인증 여부를 결정하는 과정이다. Kerberos 프로토콜은 사용자의 패스워드를 비밀키로 이용하여 ID를 비밀키로 암호화 시켜서 서버에 전송하는 방식으로 구성된다. 그러나 본 논문에서는 자동화된 사용자 인증 메커니즘 구현을 위해서 패스워드 입력 방식을 채택하지 않았기 때문에 사용자 등록 과정에서 배포받은 대칭키를 이용하여 암호화한 식별자와 MAC Address를 서비스 게이트웨이로 전송하는 방식을 연구하였다.

두 번째는 서비스 티켓 발급 과정이다. 서비스 티켓 발급 과정은 사용자가 특정 서비스 이용에 필요한 티켓을 서버로부터 발급 받는 과정이다. 사용자가 특정 서비스에 접근하기 위하여 먼저 해당 번들 서비스에 접근할 수 있는 티켓을 발급받기 위한 작업을 거쳐야 한다.

세 번째는 서비스 권한 부여 과정이다. 서비스 권한 부여 과정은 사용자 인증이 완료되어 서버로부터 발급받은 티켓을 이용하여 원하는 특정 번들 서비스의 권한을 부여받는 과정이다.

〈표 1〉은 사용자 인증 메커니즘 프로토콜에 대한 명세이다. 사용자 인증 메커니즘 프로토콜에 대한 구체적인 내용은 아래와 같다.

〈표 1〉 사용자 인증 메커니즘 프로토콜

< 표기법 >	
ID_U	사용자 U의 식별자
K_X	X의 비밀키
$K_{X,Y}$	X와 Y의 세션키
$K_X\{M\}$	비밀키 K_X로 암호화된 M
T	TGS(Ticket Granting Service)
req	Service request message
BS	Bundle service
res	Response message
< 메시지 >	
① U → SG : MAC || $K_U\{ID_U\}$	
② SG → U : $K_{SG}\{TGT\}$ || $K_U\{K_{U,SG}\}$	
③ U → T : $K_{SG}\{TGT\}$ || $K_{U,SG}\{ID_U\}$ || req	
④ T → U : $K_{BS}\{Ticket\}$ || $K_{U,SG}\{K_{U,BS}\}$	
⑤ U → BS : $K_{BS}\{Ticket\}$ || $K_{U,BS}\{ID_U\}$	
⑥ BS → U : res	

1. 사용자 인증 요청 과정 (U → SG)

사용자가 서비스 게이트웨이에 접속하고 구성원의 권한을 획득하기 위해 서비스 게이트웨이의 인증 서비스에 인증 요청을 하는 과정이다. 일반적으로 사용하는 패스워드 입력 과정을 생략하고 사용자와 서비스 게이트웨이간에 미리 등록된 MAC address와 식별자, 대칭키를 이용하여 자동화된 인증 과정을 거친다. 안전한 인증을 위해 사용자의 MAC과 함께 사용자의 대칭키 KU를 이용하여 식별자를 암호화한 KU{IDU}를 서비스 게이트웨이에 전송한다.

2. 게이트웨이의 사용자 TGT 발급 (SG → U)

TGT란 티켓을 발행하는 TGS에 티켓 발행 요청을 하기 위한 티켓이다. 서버는 사용자로부터 받은 KU{IDU}를 서버가 가지고 있는 사용자의 MAC에 해당하는 대칭키를 이용하여 KU{IDU}를 복호화하고 복호화된 데이터가 서버가 저장하고 있는 ID와 일치할 시에 사용자에게 서버 자신의 비밀키 KSG로 암호화 된 KSG{TGT}를 발행한다. 그리고 TGS와의 통신 과정에서 사용하게 될 세션키를 발행하는데, 안전한 보안 과정을 위하여 사용자의 비밀키 KU로 암호화한 세션키 KU{KU,SG}를 사용자에게 전송한다.

3. 서비스 티켓 발급 요청 (U → T)

TGS란 서비스 제공을 받기 위한 티켓을 발행해주는 서비스이다. TGS는 인증 서버와 물리적으로 다른 위치에 있을 수도 있지만 본 논문에서는 서론에서 얘기한 OSGi 환경의 특성상 물리적으로 동일한 서버에 하나의 번들 형태로 구성하였다.

사용자는 티켓을 발급받기 위해 TGS에 서비스 게이트웨이로부터 받은 KSG{TGT}와 서비스 게이트웨이와의 세션키로 암호화된 사용자 식별자 KU,SG{IDU}, 그리고 티켓 발급 요청 메시지를 TGS에게 전송한다.

4. TGS의 사용자 티켓 발급 (T → U)

사용자에게 티켓 발급 요청을 받은 TGS는 자신의 비밀키로 KS{TGT}를 복호화하고 사용자와 서버의 세션키로 암호화된 사용자의 식별자 KU,SG{IDU}를 복호화하여 사용자의 신원을 확인하면 TGS의 비밀키로 암호화된 티켓 KBS{Ticket}을 사용자에게 발급하고 사용자의 세션키 KU,SG로 암호화한 TGS와의 세션키 KU,SG{KU,BS}를 사용자에게 전송한다.

5. 서비스 권한 부여 요청 (U → BS)

사용자는 원하는 번들을 이용하기 위해서 번들을 제공해주는 번들 서비스의 권한을 획득하여야 한다. 사용자는 권한 획득을 위한 TGS의 비밀키로 암호화된 서비스 티켓 KBS{Ticket}과 세션키로 암호화된 식별자 KU,BS{IDU}를 번들 서비스에 전송한다.

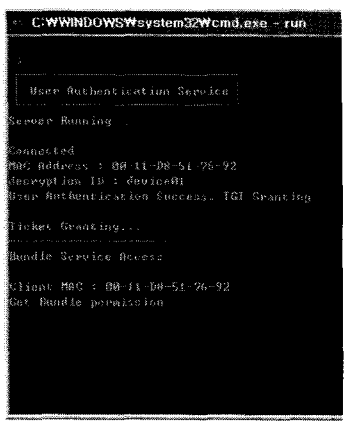
6. 번들 서비스의 사용자 권한 부여 (BS → U)

번들 서비스는 사용자로부터 전송받은 암호화된 티켓을 복호화하여 유효한 티켓인지 판별 후 사용자에게 서비스 자원에 대한 권한을 부여하고 응답메시지를 전송한다. 사용자는 응답메시지를 보고 권한을 부여 받았는지 확인할 수 있다. 사용자는 번들 서비스로부터 받은 권한으로 번들서비스의 자원에 접근할 수 있다.

III. 사용자 인증 메커니즘 구현

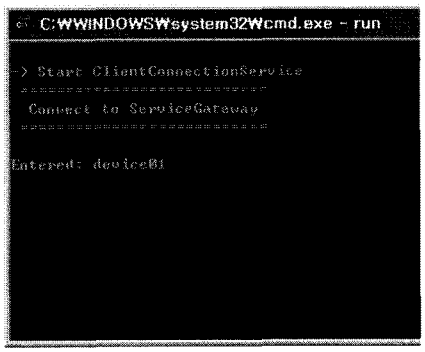
홈 네트워크를 위한 자동화된 사용자 인증 메커니즘은 클라이언트와 서비스 게이트웨이의 사용자 인증 서비스, 그리고 번들을 저장하고 사용자에게 제공해주는 번들 서비스로 이루어진다.

인증 메커니즘의 구현은 Windows XP 운영체제에서 JDK 1.5를 사용하였다. OSGi 프레임워크는 Apache사의 Felix 1.2.1을 사용하였으며 암호화 연산은 JCE의 암호화 라이브러리를 사용하였다.



〈그림 3〉 사용자 인증 서비스 실행 화면

〈그림 3〉은 서비스 게이트웨이에 설치되는 사용자 인증 서비스의 구동 화면이다. 클라이언트로부터 MAC 주소와 암호화된 식별자를 전송 받아 인증 과정을 수행하는 모습을 보여준다.



〈그림 4〉 사용자 접속 서비스 실행 화면

〈그림 4〉는 클라이언트에 설치되는 사용자 접속 서비스의 구동 화면이다. 서비스 게이트웨이에 접속하고 자신의 인증 정보를 전송하는 과정을 보여준다.

IV. 결론

본 논문에서는 홈 네트워크 환경을 위하여 OSGi 프레임 워크를 이용하여 자동화된 사용자 인증 메커니즘에 대해 연구하였다. 홈 네트워크에서는 정해진 소수의 사용자가 접속하며 디바이스들의 자원에 대한 제약이 많기 때문에 자원의 소모를 줄이는 것이 중요하다. 또한 사용자가 커뮤니티 그룹에 접속할 때 다양한 디바이스의 입력 장치에 대한 특성을 고려하여야 한다.

디바이스들의 제약사항을 고려하여 연산이 간단한 대칭키를 이용하여 효율성을 높이고 사용자의 식별자를 암호화하여 전송하는 방법을 사용하였다. 그로 인해 사용자의 패스워드 입력 과정을 생략할 수 있고, 로컬 네트워크에서 사용자의 접속만으로 인증과정을 거치는 자동화된 사용자 인증 메커니즘을 구현하였다. 자동화된 사용자 인증 메커니즘을 통하여 사용자 입력 대기 시간을 없애고 대칭키를 이용하여 암호화에 필요한 연산량을 줄일 수 있어서 홈 네트워크 환경에 효과가 있음을 보여주었다.

참고문헌

[1] OSGi Alliance, "OSGi Service Platform Release 4," http://www.osgi.org, 2007.

[2] Chi-Chih Huang, Pang-Chieh Wang, Ting-Wei Hou, "Advanced OSGi Security Layer," AINAW'07, Vol. 2, pp. 518-523, May. 2007.

[3] 박대하, 김영갑, 문창주, 백두권, "OSGi 서비스 플랫폼 환경을 위한 보안 아키텍처," 한국정보과학회, 제10권, 제3호, pp. 259-272, 2004년 6월.

[4] B. Clifford Neuman and Theodore Ts'o, "Kerberos: An Authentication Service for Computer Network," IEEE Communications Magazine, Vol. 32, No. 9, pp. 33-38, Sep. 1994.