u-City 네트워크 환경에 적합한 통합 인증 모델 설계

서장원*, 진광윤**, 최신형***
*동서울대학 컴퓨터소프트웨어과, **강원대학교 컴퓨터공학과,
***강원대학교 전기제어공학부
e-mail:jwsuh@dsc.ac.kr

The Design of Integrated Authentication Model adaptive for u-City Network

Jang-Won Suh*, Kwang-Youn Jin**, Sin-Hyeong Choi***
*Dept. of Computer Software, Dong Seoul College
**Dept. of Computer Engineering, Kangwon National University
***Division of Electrical & Control Engineering, Kangwon National University

요 약

u-City는 첨단 IT 기술을 도시에 적용하여 도시 내에서 발생하는 여러 가지 부작용들을 해결하고 시민들의 복지를 향상 시킬 수 있는 새로운 개념의 도시이다. 또한, u-City는 USN, BCN, IPv6, Wibro 등 네트워크 기술이 복합적으로 적용되어있고 모바일 폰, UMPC, PDA, PC 등 다양한 형태의 정보화 기기들을 통해 새로운 형태의 서비스를 이용할 수 있다. 본 논문에서는 다양한 정보화 단말이 무선 인프라를 이용하여 u-City 서비스에 접속하기 위한 통합 인증 모델을 제시한다.

1. 서론

컴퓨터를 비롯한 IT 관련기술의 발달로 인해 우리 생활에 많은 변화를 가져오고 있다. 과거 공상과학만화나 영화에서 볼 수 있었던 장면들이 현실적으로 가능하게 되었고, 이를 통해 가정에서 뿐만 아니라 직장에서의 생활이 상당히 편리하게 되었다. 이런 편리성에 대한 연구의 지속적인 발전으로 그 규모 및 범위 또한 확장되어가고 있다.

대표적인 예로서 많은 지자체들이 앞다투어 계획하고 실현하기 위해 준비 중인 u-City(ubiquitous City)가 있다[1].

u-City는 유비쿼터스 기술을 기반으로 하며, 여기에는 수많은 정보기기들을 연결하는 다양한 네트워크 기술이 필요하다. 다양한 기기들을 연결함으로 인해 발생할 수 있는 개인의 정보 및 도용 등의 문제를 해결하기 위해 이들 기기간의 보안은 필수적으로 해결되어야 한다. 이런 이유로 인해 u-City에는 uMC(ubiquitous Management Center)가 존재한다.

uMC는 u-City 내의 발생가능한 모든 서비스를 처리하도록 설계되어 있으며, 도시를 통제하는 중요한 기능을 수행함으로 내·외부의 악의적인 공격자로부터 해킹 및 서비스 공격 등의 목표가 될 경우 심각한 문제를 일으키게 된다. 특히, 모든 정보화 기기 및 주민들과 네트워크로 밀접히 연결되어 있기 때문에 네트워크 접근을 통한 서비스 거부 공격, 스니핑 공격, 변조 공격 등 보안 취약점은 더욱 커진다[2].

u-City의 경우 다양한 네트워크 기술이 존재함으로 인해 그 복잡성이 높고, 그에 따른 인증 및 접근 과정이 다양하므로 본 연구에서는 u-City의 핵심인 uMC 중심의 통합인증모델을 설계한다.

2. 구성요소

uMC 인증구성요소로는 사용자 단말, ER(Edge Router), Radius 서버, SSO 서버 등으로 구성된다.

사용자 단말은 접근 가능한 AP를 찾아 네트워크

에 연결하기 위한 암호화 처리 알고리즘을 가지고 있어야 한다. 또한, 가변 IP를 할당 받기 위한 DHCP 모듈, 공개키 암호화 기능, PIN Number 입력 기능, Hash 기능을 포함하고 있어야 한다.

사용자 단말의 암호화 모듈이 암호화를 수행하기 위한 처리 내용은 다음과 같다.

◦ 접속 가능한 네트워크를 찾기 위한 DHCP DISCOVER/DHCP OFFER 패킷을 브로드캐스트

◦ 공개키를 통한 SSO 서버로부터 전송된 인증 메시지 해독

◦ 사용자 PIN Number 입력 기능과 Hash 기능

◦ 상대방의 공개키를 이용한 데이터 암호화

ER은 기존 인증 방법에서는 존재하지 않던 부분으로 사용자 단말에서의 단말 고유 값을 입력 받아 인증 서버와 단말기의 접근 정보 및 서버의 정책을 결정하는 모듈이다. 이것은 암호화 기능은 없지만 IP Address 할당을 위한 DHCP 연결 기능과 Radius 서버 등을 연결하고, DHCP relay를 처리하는 기능을 가진다.

ER의 역할은 다음과 같다.

◦ 단말 정보를 통한 CLIPS 생성

◦ ACL 접근정보정책 및 패킷 제어 정책 반영

◦ DHCP Relay

◦ 최초 및 종료 시 접속 경로에 대한 Redirection

◦ 인증 후 접속 경로 설정 및 변경

Radius 서버는 CLIPS를 연결한 후 인증 정보를 확인하여 사용자의 정책을 추출하는 역할을 한다. 여기서, 단말 기반의 사용자 정책은 사용자 정책 DB와 단말 DB 정보를 통해 얻는다. Radius 서버의 역할은 다음과 같다.

◦ ER로부터 CLIPS 연결 처리

◦ 단말 정보로부터 정보를 추출하여 DB를 통한 사용자의 ACL 정책 정보를 추출하여 전달

SSO 서버 모듈은 사용자 인증을 최종적으로 승인하고 해당 사용자를 인증하는 서버이다. 인증 완료 후 u-City 내의 uMC 내부 모델에 인증 토큰을 할당하는 역할을 담당한다. SSO 서버의 역할은 다음과 같다.

◦ 사용자 기반의 세션키와 공개키를 암호화 하여 단말에 전달

◦ 사용자 PIN을 기반으로 한 단말기 상태 인증

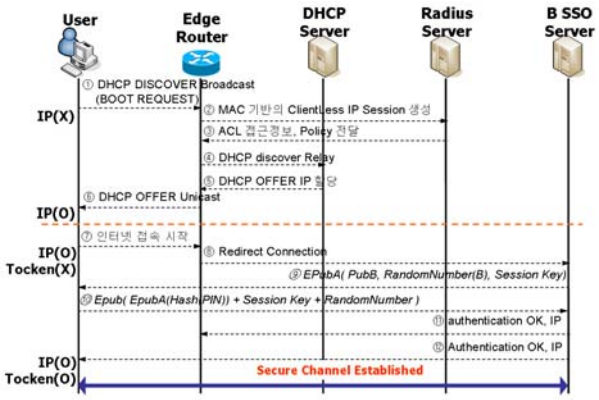
◦ 내부 사용자 접속을 위한 토큰 생성

◦ 사용자 인증 후 정책의 허용 여부를 Radius 서버와 ER에게 전달

u-City의 개발시 가장 중요한 구성요소인 uMC는 u-City의 핵심으로 기존 도시에서 기능을 나누어 관리하던 방식을 하나의 센터로 통합해 놓은 것으로 매우 복잡한 구조를 가지고 있다. 또한, 현재 구축되었거나 또는 구축 예정인 u-City의 특성이 모두 다르기 때문에 다양한 형태의 uMC가 존재할 수 있다. 본 연구에서는 uMC 구성요소 중 인증 부문만을 다룬다. 아울러, uMC 모듈은 기본적인 암호 모듈과 인증 모듈을 가지고 해당 시스템과 접속 시 암호화 구간을 통해 데이터를 처리한다. uMC가 인증을 위해 가지고 있어야할 DB의 종류로는 인증 DB와 사용자 DB가 있다.

3. 인증절차

망 접속시 인증을 위한 전체 인증 과정은 그림 1과 같다.



[그림 1] 망 접속시 인증 절차

사용자와 SSO 인증 서버 사이의 암호화 전송과 키 생성 및 교환 순서는 다음과 같다.

사용자는 IP 할당을 받은 후에 인터넷 및 사이트 접속을 시작하고 해당 트래픽은 Redirect 되어 인증 서버로 전송된다. 이때, 인증 서버는 사용자 단말의 주소로부터 단말기의 소유자 정보를 추출한 후, 해당 사용자의 공개키와 사용자 접근 정보를 추출한다. 그런 후에, 단말과 SSO 인증 서버간의 암호화

구간의 통신을 위한 Session Key를 생성하여 추출된 사용자의 공개키로 암호화 후 단말기로 전송한다. 전송된 패킷은 사용자가 개인키로 복호화한 후 Session Key와 Nunce 값, SSO 서버의 공개키 값을 추출하여 저장한다. 추출된 SSO 서버의 공개키 값으로 사용자로부터 직접 입력받은 PIN Number의 Hash 값과 Nunce 값을 포함하여 암호화 한다. 암호문은 SSO 서버로 전달되어 복호화 되고, 사용자 DB에서의 Password와 Hash 값을 검증함으로써 인증 여부가 확인된다.

인증이 완료된 사용자의 단말기는 다른 시스템의 별도 인증 절차 없이 사용되기 위해 인증 서버로부터 SSO 토큰을 생성 받아 Session Key로 암호화된 구간을 통해 안전하게 인증 정보를 전달 받게 된다.

단말기 및 사용자가 인증을 해결하지 못했을 경우 사용자의 모든 트래픽은 중단되고 패킷은 버려진다. 이와 반대로, 사용자가 인증을 풀었을 경우 Redirect 되었던 트래픽은 다시 전송되어 원활한 접속이 이루어진다.

네트워크에 처음 접속하는 단말은 네트워크를 인식하는 시점부터 IP가 할당되어 사용자 인증이 처리될 때까지 다음과 같은 인증 절차를 거친다.

① u-City 네트워크 영역에서 단말기를 동작시키면 네트워크에 접속하기 위해 단말은 DHCP DISCOVER 메시지를 전송한다.

② ER은 DHCP DISCOVER 패킷을 DHCP 서버로 전송하지 않고 보류한 상태로 CLIPS를 생성하여 인증 서버로 전송한다.

③ Radius 서버는 CLIPS를 통하여 전송된 MAC이 이미 등록되어 있는 사용자의 MAC 인지를 확인한다. 만일, 등록되어 있고 사용가능 하다면 IP를 할당한 뒤 정책을 적용하여 인증을 완료한 후에 접속을 허용한다.

④ 등록되어 있지 않다면, 차단 목록을 확인하고 공격자에 의한 차단 목록에 등록되어 있는지 확인한다. 만일, 확인 후 차단 목록에 등록되어 있다면 해당 단말기에서 발생하는 트래픽을 Drop 한다.

⑤ 공격자 목록에서 공격자로 확인되지 않으면, 신규 모드로 처리하여 사용자 등록을 실행하고 사용자의 공개키, 단말기, Password 등을 암호화하여 DB에 기록한다.

⑥ 신규로 접속시 망 인증 접속을 허가 받고 IP Address를 할당 받은 단말기는 네트워크를 통한 인터넷 접속을 시도한다.

⑦ 신규 등록 장비의 경우 MAC 등록을 처리하며, 신규 등록 장비가 아닌 경우 인증 처리를 위해 경로가 Redirect 처리되어 새로 인증을 실행한다. 이때, 인증 받은 장비는 사용자의 정책에 따라 인증을 수행한다.

⑧ 단말기 인증 및 사용자 인증이 완료된 상태에서 인터넷에 접속한다.

4. 결론

u-City는 첨단 IT 기술을 도시에 적용하여 도시 내에서 발생하는 여러 가지 부작용들을 해결하고 시민들의 복지를 향상 시킬 수 있는 새로운 개념의 도시이다. 본 연구에서는 다양한 정보화 단말이 무선 인프라를 이용하여 u-City 서비스에 접속하기 위한 인증 방법을 제안하고 그 절차를 서술하였다. 제안된 통합 인증 모델을 사용할 경우, 신규 사용자의 IP 할당과 이미 인증된 사용자의 빠른 서비스 접속이 가능하며, 공격자의 경우 차단 목록을 통해 관리됨으로 사전 차단이 가능하다.

참고문헌

[1] 황종성, "u-City의 개념과 구현 전략을 위한 이슈 분석", 정보과학회지, 제23권, Nov. 2005.

[2] 한국정보보호진흥원, "u-City 프라이버시 보호 방안 연구", 연구보고서, Dec. 2006.

[3] 안현섭, "u-City를 위한 통합 인증 시스템 모델", 고려대학교 컴퓨터정보통신대학원 석사학위논문, 2008.

[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", IEEE Security and Privacy Magazine, vol. 2, no. 3, pp.40-48, May-June 2004.

[5] Vladimir Brik, Jesse Stroik, Suman Banerjee: Debugging DHCP performance Internet Measurement Conference 2004 : 257-262.

[6] Groß, T. "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile", 19th Annual Computer Security Applications Conference, Las Vegas 2003.