한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

Beacon을 이용한 위치기반 인증 시스템 설계

조해룡°, 이양규*, 최민*
°*충북대학교 정보통신공학부
e-mail:hrjo@cbnu.kr°, {yglee, mchoi}@cbnu.ac.kr*

Design of Location-Based Authentication System using Beacon

Hae-Ryong Jo°, Yang-Kyu Lee*, and Min Choi*
°*Dept. of Information and Communication Engineering, Chungbuk National University

● 요 약 ●

특정 인터넷 서비스는 그 성격에 따라 제한된 위치에서만 서비스를 제공하도록 설계한다. 이러한 시스템 구조에서 사용자의 위치정보는 서비스 접근을 통제하는 과정에서 핵심적으로 사용되며 LSB(Location Based Service), WPS(Wifi Positioning System)와 같은 기술로 제안되었다. 그러나 기존 인증 기법은 대상이 일정하지 않은 불특정 다수의 사용자가 접근하기에 적합하지 않고, 서비스 공급자의 무선 AP를 이용하기 때문에 과도한 서버 부하에 취약하다. 따라서 본 논문에서는 이러한 문제를 해결하기 위해서 Beacon을 이용한 위치기반 인증 시스템을 제안한다. Beacon이란 Bluetooth 기술을 기반으로 근거리 무선 통신 기기이다. 사용자가 서비스 접근 권한을 획득하기 위해 인증 서버에서 요구하는 인증 코드는 BLE(Bluetooth Low Energy)를 사용하는 Beacon이 브로드캐스팅한다. 즉, 사용자는 Beacon이 BLE로 브로드캐스팅한 데이터를 수신할 수 있는 물리적인 범위까지 접근해야 인증 절차를 수행할 수 있다.

키워드: 비콘(Beacon), 위치기반 서비스(LBS : Location Based Service), 인증(Authentication)

I. 서 론

인터넷 서비스는 지속적으로 다양화되었고, 보안 및 인증에 엄격한 몇몇 서비스는 그 특성에 따라 특정 물리적 위치에서만 제공되도록 설계되었다. 온라인으로만 제공되던 서비스를 물리적 공간에 제약을 두어 특정 장소에서만 이용 가능하도록 하는 서비스는 도서관, 쇼핑몰, 교육기관, 정부기관 등 다양한 곳에서 그 사례를 찾아볼 수 있다. 기존의 e-mail, 온라인 쇼핑, 디지털 콘텐츠 등 보편적인 인터넷 서비스에 적용된 ID(identification), password를 이용한 인증 절차는 유동적이고 불특정한 다수의 사용자를 대상으로 하기에 적합하지 않다. 이를 해결하기 위해 불특정 다수의 사용자가 이용하도록 인증된 디바이스 설치, 무선 AP를 이용한 WPS(Wifi Positioning System)를 대안 제안하였으나 공간, 예산, 서버 트래픽 등 한정된 자원으로 인한 현실적인 제약이 뒤따르고 있다. 우리는 정부기관의 정보제공, 도서관의 온라인 열람, 쇼핑몰의 할인쿠폰 발급과 같은 서비스를 이용하기 위해 오프라인 또는 온라인에서 일정 시간 대기하는 상황에 익숙하다. 이 문제는 서비스를 제공에 필수적인 인증 절차를 수행할 수 있는 사용자의 수가 크게 제한되어 있기 때문에 발생한다. 불필요하게 소요되는 시간, 인력과 같은 자원을 절약하기 위해서는 사용자가 급격하게 증가하는 상황에서도 개개인이 직접 인증 절차를 수행하여 서비스를 이용할 수 있어야 한다.

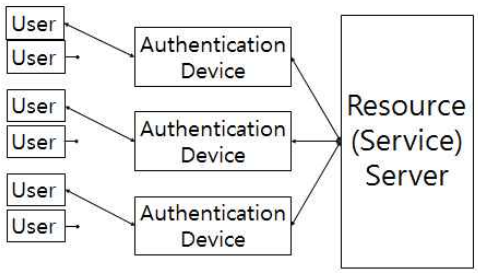

그림 1. 인증 처리 지연으로 인한 사용자 대기
Fig. 1. User waiting by the authentication processing delay

이러한 문제를 해결하기 위하여 본 논문에서는 BLE(Bluetooth Low Energy) 통신을 사용하는 디바이스, ‘Beacon’ 이용하여 인증 절차를 수행하는 위치기반 인증 시스템 설계에 대해 다루었다. 다양한 환경, 디바이스에서 응용할 수 있는 REST open API 웹 서비스를 기반으로 BLE 통신을 지원하는 스마트폰을 인증 디바이스로 사용하였다. 위치기반 인증 시스템은 Beacon이 BLE로 브로드캐스팅하는 인증코드를 사용자 개개인의 디바이스가 수신하고 유효성을 검사하여 인증 절차를 수행한다. 불특정 다수의 사용자 디바이스가 Beacon의 브로드캐스트 데이터를 수신할 수 있는 물리적 범위까지 접근해

있다면 그 모든 인원이 동시에 인증 절차를 진행하고 서비스를 이용할 수 있다. 본 연구에서는 도서관의 논문 열람 서비스를 예시 사례로 들어 Beacon 인증 시스템을 적용하였다. 기존의 경우 IP 또는 MAC address가 인증된 몇몇 디바이스를 이용해야 도서관에서 제공하는 논문을 열람할 수 있었다. 하지만 도서관 내부에 인증 코드를 브로드캐스팅하는 Beacon을 설치한다면, 이를 수신 받을 수 있는 모든 디바이스는 인증 절차를 수행하고 외부로부터 접근이 제한된 논문을 열람할 수 있는 접근코드를 얻을 수 있다. 특정 디바이스만 접근할 수 있도록 제한하지 않더라도 한정된 물리적 위치에서 더 많은 사용자에게 서비스를 제공할 수 있다. 접근코드는 OTP(One Time Password)로 사용되며, 제공하는 서비스의 특성에 따라 접근코드의 유효기간을 설정하여 서비스 이용시간을 통제할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 위치기반 인증에 대한 선행 연구와 본 연구에서 요구하는 Beacon에 대한 개념에 대해 알아본다. 3장에서는 본 논문에서 제안한 위치기반 인증 시스템의 구조와 설계, 구현 대해 다루고, 4장에서는 결론을 제시하였다.

II. 관련 연구

1. 관련연구

1.1 Location-Information 측위 기술 및 인증기법

기존의 위치정보(Location-Information) 측위 기술은 크게 2가지, 위성항법 시스템과 실내 무선 측위 기술로 분류할 수 있다. 사용자의 디바이스가 위성신호를 수신 받는 위성항법 시스템은 GPS, Galileo, GLONASS-K, COMPASS, QZSS 등이 있으나 실내와 같은 음영지역일 경우 정확한 측위가 불가능하다. 때문에 적외선, 초음파, UWB(Ultra Widebands), RF(Radio Frequency) 등의 무선 신호를 이용하여 RF Fingerpirnt 기법이나 삼각 측량 기법을 사용한다. 실내 무선 측위 기술에는 무선 AP를 이용한 WPS(Wifi Positioning System)가 대표적으로 사용되고 있다. WPS(Wifi Positioning System)는 무선 AP의 대역폭을 초과하는 사용자 접근이 발생할 경우 서비스 지연 및 이용불가 상황이 발생할 수 있다는 한계가 있다.

위치기반 인증기법은 특정 서비스에 접근하기 위한 인증 절차에서 사용자의 물리적 위치정보(Location-Information)를 활용한다. 기존의 인증 시스템에서 취약했던 네트워크 공격기법에 대한 보완으로 위치정보를 통한 인증을 일정 주기마다 갱신한다.

1.2 BLE(Bluetooth Low Energy) Beacon

Beacon이란 약속된 신호를 일정한 주기로 발생시켜 위치 및 방향 정보를 송신하는 장치를 의미한다. 사전적 의미로 신호등, 등대와 같은 무선 송신소로 사용되었으나 IoT(Internet of Things)에 대한 개념이 확립되고 관련 기술이 발전함에 따라 IT 분야에서는 Bluetooth 프로토콜을 기반으로 한 신호 발생기를 지칭하는 용어로 통용되었다. Bluetooth SIG가 2010년 6월에 채택한 Bluetooth 4.0은 저전력 동작, 무제한 동기화, 고속 전송, 기기 가용성 확대, 위치 식별 등의 기술이 구현되었고 이전까지 많은 제약이 있었던 Beacon에 대한 연구개발을 가속화할 수 있는 계기를 마련하였다. 이에 현재의 Beacon은 BLE 기반 신호 송신기술 및 기기를 나타내는 용어가 되었고, 2013년 Apple이 iBeacon이라는 통신 규격을 발표하여 상용화하였다.

III. 시스템 구조 및 설계

본 장에서는 Beacon을 이용한 위치기반 인증 시스템의 구조와 인증 절차의 처리 단계, 예시 모델로 도서관의 논문 열람 서비스의 인증 시스템을 제안한다.

1. 시스템 구조

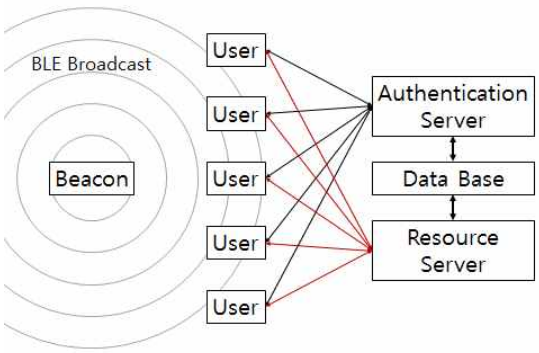

그림 2. Beacon을 이용한 위치기반 인증 시스템 구조
Fig. 2. Authentication system architecture using the beacon

그림 2는 Beacon을 이용한 위치기반 인증 시스템의 구조와 인증 절차의 처리 단계를 보여준다. Beacon을 이용한 위치기반 인증 시스템은 인증 코드를 브로드캐스팅하기 위한 Beacon, User, 인증 코드를 기반으로 보호된 자원에 접근하기 위한 Client, 보호된 자원을 제공하고 인증을 절차를 진행하여 접근 코드를 발급하는 인증 서버(Authentication Server), 접근 코드의 유효성을 검사하여 제한된 서비스를 제공하는 자원 서버(Resource Server)로 구성되어 있다. 특정 인터넷 서비스에 위치기반 인증 시스템을 적용하기 위해서는 서비스 접근을 허용하는 물리적 위치에 Beacon을 설치하여 브로드캐스팅 하도록 동작시켜야 한다. 사용자가 Beacon에 접근하여 개인 디바이스로 인증코드를 수신해야만 인증 절차를 수행할 수 있기 때문이다. 사용자의 디바이스는 Beacon의 브로드캐스트 데이터를 일방적으로 수신받기만 하여 인증 절차를 수행하려는 사용자가 급격히 증가하더라도 지연대기가 발생하지 않는다. 사용자는 서비스 공급자가 정의한 물리적 서비스 허용 위치에 근접해있다면 제한된 서비스를 이용하기 위해 인증 절차를 수행하고 서비스에 접근할 수 있다. 그 절차는 다음과 같다.

1) 사용자는 client를 통해 서비스(보호된 자원)를 이용하려고 한다.
2) client는 Beacon으로부터 수신 받은 인증코드(Auth_code)와 사용자를 식별하기 위한 user_email을 사용하여 authentication server에 서비스 접근을 위한 인증 절차를 요청한다.
3) authentication server는 client로부터 수신한 인증코드(Auth_code)의 유효성을 검사하고, 유효기간을 가진 접근코드(Access_code)를 발급하여 client에게 송신한다.

4) client는 authentication server로부터 접근코드(Access_code)를 발급받아 인증 절차를 완료한다.
5) 사용자는 resource server가 지원하는 서비스 접근 환경을 통해 접근코드(Access_code)를 입력하고 서비스 제공을 요청한다.
6) resource server는 사용자가 입력한 접근코드(Access_code)의 유효성을 검사하고, 서비스를 제공한다.

2. 인증 절차(Authentication Flow)

사용자는 client를 통해 authentication server로 서비스 접근 요청을 실시하고 user_email, 인증코드를 파라미터로 송신한다.

authentication server는 인증코드의 정합정도, 유효기간 등 유효성을 검사하여 유효하지 않은 경우 인증 불가 메시지를 반환한다. 인증코드가 유효한 경우 해당 email로 인증코드가 발급된 기록과 그 유효기간을 조회하여 유효성 검사를 실시한다. 해당 email로 발급되었고 유효기간이 남은 인증코드가 없는 경우 새로운 인증코드를 생성하여 발급한다.

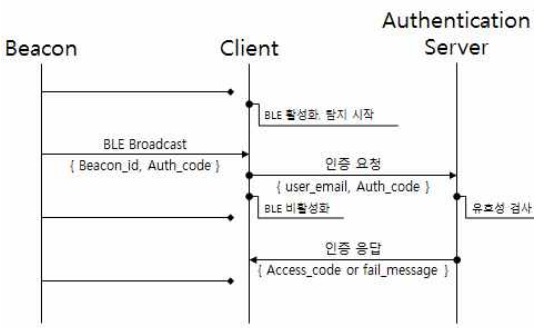

그림 3. 인증 절차
Fig. 3. Authentication Flow

3. 접근 절차(Authentication Flow)

사용자는 인증절차를 통해 발급받는 접근코드를 사용하여 web browser 등 resource server가 허용한 환경을 통해 서비스 제공 요청을 실시한다. resource server는 사용자로부터 수신한 접근코드의 정합정도, 유효기간 등 유효성을 검사하여 서비스 제공 여부를 판단한다.

4. 시스템 설계 – 논문 열람 서비스에 적용한 Beacon 인증 시스템

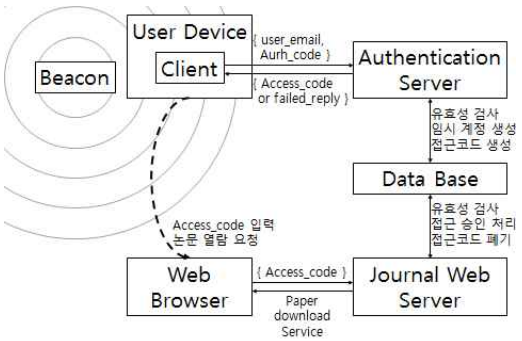

그림 4. 온라인 논문 열람 서비스의 인증 시스템 구조
Fig. 4. Authentication system architecture for the paper reading service

그림 4는 본 논문에서 제안한 Beacon 인증 시스템을 온라인 논문 열람 서비스에 적용한 예시 모델이다. 도서관과 같은 특정 장소에 Beacon을 설치하면, 인증 코드를 수신할 수 있는 범위까지 접근해야 논문 열람 서비스의 접근 권한을 획득할 수 있다. 도서관에서 제공하는 디바이스나 AP의 대역폭을 사용하지 않고도 인증 및 접근 절차를 진행하기 때문에 새로운 디바이스에 대한 높은 접근성과 사용자 증가에 대한 확장성을 확보하였다. 인증 절차를 완료하여 발급받은 접근코드의 유효기간을 짧게 설정할수록 해당 서비스의 보안성이 향상된다.

IV. 결 론

본 논문에서는 Beacon을 이용한 위치기반 인증 시스템을 제안하였다. 불특정 다수의 사용자가 개별적으로 위치기반 인증 절차를 수행할 수 있도록 BLE 통신 기반의 Beacon을 사용하였고, 기존 위치기반 인증 시스템의 한계였던 트래픽 부하를 해결하기 위해 인증 절차와 접근 절차를 분리하여 각기 다른 서버로 구성하였다. 불특정 다수의 사용자는 BLE 통신을 지원하는 다양한 개인 디바이스를 통해 인증코드를 수신 받아 인증 서버 서비스 접근코드를 요청한다. 인증 서버는 인증코드의 유효성을 검사하고 서비스 접근코드를 발급한다. 서비스 접근코드는 유효기간을 가지며 해당 기간을 초과하여 만료된 경우 다시 인증 절차를 수행하여야 한다. 서비스 접근코드의 유효기간이 짧을수록 접근 통제가 효과적으로 이루어진다. 또한 접근 코드는 유일성을 가지도록 생성하여 각기 다른 사용자가 동일한 접근코드를 발급받지 않도록 한다. 사용자는 자원 서버에 접근코드와 함께 서비스 제공 요청을 보내고, 자원 서버는 접근코드의 유효성을 검사하여 서비스를 제공, 사용된 접근코드를 폐기한다. 이처럼 브로드캐스팅을 통해 유효기간을 가진OTP(One Time Password)로 사용되는 접근코드를 발급하는 인증 시스템은 서비스 접근 인증에 대한 보안성과 새로운 사용자에 대한 확장성을 확보하였다.

Acknowledgement

본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0234798)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] Jung Min Choi, Kwantae Cho, Dong Hoon Lee, "Location-Based Authentication Mechanism for Server Access Control," Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 6, pp. 1271-1282, Dec. 2012.
[2] Sung-Je Kim, Yong-Hwan Cho, Tae-Woo Lee, "Accredited by the device identifier location-based security techniques", Journal of Korea Entertainment Industry Association, Vol. 8, No. 1, pp. 234-237, Nov. 2011.
[3] Dorothy E. Denning, Peter F. MacDoran, "Location-based

authentication: Grounding cyberspace for better security", Computer Fraud & Security of Elsevier Science Ltd (C), pp.12-16, Feb. 1996.

[4] Hyunsu Kim, Jimin Bae, Jihoon Choi, "Wireless LAN Based Indoor Positioning Using Received Signal Fingerprint and Propagation Prediction Model", The Journal of Korea Information and Communications Society, Vol. 38, No. 12, pp.1021-1029, Dec. 2013.

[5] Paramvir Bahl and Venkata N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System", INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol.2, pp.775-784, Mar 2000

[6] Azad Jiwa, Thomas Hardjono, Jennifer Seberry, "Beacons for authentication in distributed systems", Journal of Computer Security, 4, pp.81-96, 1996

[7] Cheolhoon Kim, Sungwon Lee, "A Research on Performance Improvement of iBeacon using Beacon Code Architecture Extension", Journal of Korea Information and Communications Society, June, 2014