情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

서버 접근 통제를 위한 위치기반 인증 기법*

최 정 민,† 조 관 태, 이 동 훈‡
고려대학교 정보보호대학원

Location-Based Authentication Mechanism for Server Access Control*

Jung Min Choi,† Kwantae Cho, Dong Hoon Lee‡
Graduate School for Information Security, Korea University

요 약

최근 기업의 기밀정보 및 개인정보의 대량 유출에 따른 보안사고가 지속적으로 발생하고 있다. 이에 내부 정보 유출 방지를 위한 인증 강화와 접근통제 관련 보안 기술이 주목받고 있다. 특히 사용자의 현재 위치정보를 인증 요소로 활용하는 위치기반인증은 접근을 시도하는 사용자의 물리적 통제와 더욱 강력한 인증을 제공하고 내부 정보 유출 경로를 원천적으로 차단할 수 있다는 장점을 가지고 있어 다양한 형태로 제안되고 있다. 그러나 위치정보는 또 하나의 개인 식별 정보로써 인증 수행 시 안전하게 처리되어야 하며, 사용자 위치정보의 특성을 이용하여 유연한 물리적 통제를 수행할 수 있어야 한다.

본 논문에서 제안한 위치기반 인증 기법은 기존 관련 위치기반인증 프로토콜과 비교하여 위치정보 처리 과정의 안정성을 높이고, 최종 사용자 인증에 일회용 패스워드를 사용하여 사용자 인증을 강화한다. 제안된 기법은 내부 정보 유출 방지를 위해 인증 수행과 함께 사용자의 물리적 접근 통제의 개념을 접목시켜 기존 연구보다 높은 보안성을 제공함과 동시에 낮은 통신비용을 보장한다.

ABSTRACT

Recently, security incidents occur continuously, resulting in the leakages of a large amount of the company's confidential and private information. For these reasons, the security technologies such as the authentication and the access control in order to prevent the information leakage are attracting attention. In particular, location-based authentication that utilizes the user's current location information which is used an authentication factor. And it provides more powerful authentication by controlling the users who attempt to access and blocks internal information leakage path. However, location information must be handled safely since it is the personal information. The location based authentication scheme proposed in this paper enhances the stability of the process location information compared with existing relevant location-based authentication protocol. Also it strengthens the end-user authentication by using one-time password. In addition, the proposed scheme provides authentication to prevent information leakage and employs the concept of the user's physical access control. Resultingly, the proposed scheme can provide higher security than the previous studies, while guarantee to low communication cost.

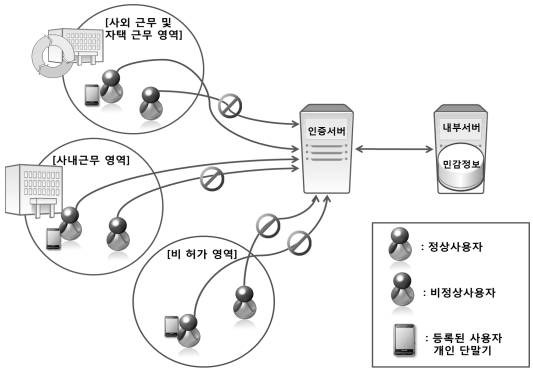
Keywords: Access Control, Location-Based Authentication

접수일(2012년 9월 6일), 수정일(2012년 10월 25일), 게재확정일(2012년12월 3일)
* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음.

† 주저자, choi87@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

내부 정보 유출이란 개인 및 기업의 정보를 특정 내부 정보 주체의 동의 없이 유출하는 행위를 말한다. 최근 기업 내부 서버와 데이터베이스의 내부 정보 유출 사건으로 기업과 개인의 피해 사례가 속출하고 있다[1]. 이러한 보안 피해 사례는 고도화된 해킹 기술에 의한 인증 도용이나 접근 통제의 부재에 따른 접근 권한 우회가 주원인이 되어 발생한다. 이에 전반적인 정보보호와 내부 정보 유출 방지를 실현하기 위해서는 안전한 사용자 인증과 접근통제가 동시에 이루어져야 한다. 최근, 사용자 인증 강화와 접근통제 솔루션 도입에 대한 기업들의 관심이 높아지고 있다[2]. 원천적으로 내부 정보 유출 사고를 방지하기 위해서는 일시적인 보안 솔루션 도입이 아닌 물리적, 관리적, 기술적 접근 통제를 모두 고려해야 한다. 특히 사용자의 물리적 위치의 개념을 포함한 인증 수행 및 내부 시스템 접근 통제는 기존의 사용자 인증을 통한 논리적 접근 통제 보안의 결함인 기존 인증 방식의 취약점을 이용한 접근 권한 우회를 완화 시킬 수 있다[3]. 이러한 사용자의 물리적 통제를 효과적으로 수행하기 위하여 여러 위치기반 인증 기법들이 연구되어져 왔다. 최근 국내에서는 안랩이 사용자의 물리적 위치를 이용한 사용자 인증 특허를 발표하였다[4]. 국외에서는 1996년 Dorothy E. Denning이 최초로 Location-Based Information이라는 사용자의 물리적 위치정보를 이용한 인증 개념을 제안하였다[5]. 이후 사용자의 물리적인 위치정보 인증 요소로 활용한 STAT1이 제안되었다[6]. 사용자의 시간정보와 위치정보를 접근통제에 적용한 연구로는 GEO-RBAC가 있으며[7], 특정 서비스와 위치정보를 연계하여 POS 결제 수행을 위해 사용자의 위치정보를 활용하는 LRAP가 기존에 제안되었다[8]. 현재 위치정보 측위 기술, 인증 처리 과정, 접근 통제에 사용자의 물리적 위치정보를 활용한 다양한 연구가 진행 중이며 기존 연구들은 대부분 인증에 사용되는 개인위치정보의 노출과 위·변조에 대해서는 보장하고 있지 않고, 인증과 함께 데이터 접근성을 보장하는 세부적인 접근통제 설정을 제안하고 있지 않다. 본 논문은 내부정보 유출 방지를 목표로 사용자의 작업환경을 제한함으로써 물리적인 접근통제를 보장하는 내부 서버 접근 통제를 위한 위치기반 인증 기법을 제안한다. [그림 1]은 제안하는 위치기반 인증 기법을 나타낸다. 정상 사용자는 외근을 나가거나 자택 근무 시 사내 중요 정보에 대한 조회만 가능



[그림 1] 내부 서버 접근 통제를 위한 위치기반 인증 모식도

하게 하거나 삭제는 불가능 하게 하는 접근 권한을 설정하여 통제를 수행 할 수 있다. 이외 정상 사용자의 비허가 지역에서 사내 중요 정보로 접근을 차단하며 비정상 사용자의 접근을 차단한다. 사용자는 인가된 물리적 환경에서 작업 수행을 위한 접근 권한 획득을 위해 미리 등록된 모바일 단말기를 이용하여 인증을 수행한다. 작업이 이루어지는 PC는 해당 위치에 기 설정 되어있는 공용PC 및 사용자 개인 소지 이동형 PC로 모바일 장치로 전송되는 Ticket을 이용하여 PC 인증을 수행한다. 제안하는 위치기반인증 기법은 개인의 물리적 위치정보를 인증식별자로 사용하여 안전한 물리적 작업환경을 확보하고 내부 시스템 접근을 시도하는 사용자 행위를 제한함과 동시에 안전한 데이터 이동 경로를 확보함으로써 내부정보 유출의 원인 요소를 제거하고자 하였다. 또한 인증에 사용되는 위치정보는 다른 개인정보와 결합되는 경우 개인 식별 정보로써 악용될 수 있으므로 개인정보보호의 대상이 된다. 이에 인증에 사용되는 위치정보를 인증서버의 공개키로 안전하게 처리한다. 그리고 사용자 인증 강화를 위해 투 채널 인증을 도입한다. 마지막으로 STAT1과의 비교 분석을 통하여, 제안된 기법이 STAT1과의 비교 분석을 통하여 제안된 기법이 더욱 안전함을 보였다.

논문의 구성은 다음과 같다. 2장에서는 위치기반인증 수행을 위해 필요한 위치정보 측위 기술과 접근통제 개념과 관련 선행 연구를 알아본다. 3장에서는 관련 연구로부터 필요한 보안 요구사항을 명시하였으며 4장에서는 본 논문에서 제안한 위치정보 처리 단계와 위치기반인증 시스템 모델과 프로토콜을 소개한다. 5장에서는 관련연구를 기준으로 안전성 분석과 효율성 분석한 결과를 보이고 마지막으로 6장에서는 결론을 내린다.

II. 관련 연구

2.1 위치정보(Location-Information) 측위 기술

위치 정보(Location-information)의 획득은 다양한 측위 기술을 통해 가능하다. 일반적으로 GPS, Galileo와 같이 사용자는 모바일 장치를 통하여 수신된 위성신호만 이용하는 위성단독 방법이 있으며 GPS를 이용해 얻어지는 위치정보의 정확도를 높이기 위해 A-GPS나 DGPS와 같은 기술이 현재 상용 서비스되어 제공되고 있다[9]. 그러나 실내나 건물이 밀집한 음영지역의 경우 GPS기반 위치 측위에 필요한 위성 신호 수신율이 급격히 저하되는 문제가 발생하기 때문에 정확한 사용자 위치 측위가 불가능 하다[10][11]. 이를 보완하기 위해 다양한 무선 실내 측위 기술이 제안되고 있다. 실내 측위를 위해 사용되는 신호 종류에는 적외선, 초음파, UWB(Ultra Wide bands), RF(Radio Frequency)등 있으며 현재 가장 주목받는 기술은 실내 무선 신호를 이용한 측위 방법이다[10][11]. 무선 신호를 이용한 측위 방법은 RF Fingerpirnt 기법과 삼각 측량 기법이 있다. 이 중 WPS(Wifi Positioning System)에서 사용되는 RF Fingerprint는 단말에서 측정한 RF전파 특성 정보와 기 구축한 DB의 정합 정도를 판단하여 가장 적합하게 정합되는 격자를 측위 결과로 선택하는 방식이다. 이러한 무선 측위 기술은 기존 무선 네트워크나 센서 망 또는 ad hoc 네트워크를 이용하여 구현된다는 장점이 있다[10].

2.2 접근통제(Access Control)

접근 통제는 불법적인 자원의 사용, 수정, 삭제와 불법적인 명령어 실행을 포함한 모든 허가되지 않은 접근을 방어하는데 목적이 있다. 즉 접근 통제는 정보자산의 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 권한 부여를 위한 정책 및 기술이 된다. 일반적으로 접근 통제는 사용자 신분의 인증을 기준으로 인증되기 전 까지 접근은 수행 될 수 없으나, 인증 수행 후 각 시스템 자원에 대한 사용자 요청을 보안 정책이 적용된 접근 통제 절차에 따라 접근 권한을 부여 받는다. 접근 통제는 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고, 어떤 조건하에 접근하는지가 결정되며 결정을 위한 요인은 접근 통제 정책에 반영되고, 접근 요청은 접근 정책을 시행하는 접근 통제 매커니즘에 의해 시행된다. 특히 본 논문에서 제안하는 위치기반 인증에 따른 접근 통제는 CBC(Context-Based Control)로 분류 될 수 있다. 위치기반 인증 접근 통제는 사용자의 현재 위치라는 외부적인 요소에 의존하여 객체의 접근을 제어하는 정책으로 신분-기반 또는 규칙-기반 정책들에 추가될 수 있다. CBC 도입 시 접근 통제 메커니즘, 인증 메커니즘, 또는 물리적 보안 대책에 대한 취약점을 보완할 수 있다[12].

2.3 위치기반인증(Location-Based Authentication)

인증은 개인의 신분을 확인하고 진위를 결정하는 과정이다. 이것은 네트워크에 대한 접근, 자원 및 서비스를 제어하기 위해 반드시 필요하다. 그러나 기존에 사용하고 있는 인증 메커니즘은 재생공격, 중간자 공격, 피싱과 같은 많은 공격기법에 의해 취약한 상태이다. 이러한 문제를 재정비하기 위해 강력한 인증을 제공하는 새로운 수단이 필요하다. 기존의 인증 방식에 위치정보(Location information)를 결합한 위치기반인증은 사용자의 물리적 위치를 실시간으로 확인한 후 인증을 수행한다[6][8]. 사용자 위치정보를 인증에 활용하는 인증 메커니즘은 기존 보안 메커니즘과 통합되어 물리적 접근제어의 효율성을 함께 제공한다. 또한 짧은 주기로 실시간 생성되는 위치정보를 이용하기 때문에 인증정보 재생성 불가 및 사용자의 지속적인 정상적인 연결을 탐지 할 수 있다. 이것은 공격자가 중간에 시스템과 사용자의 연결을 가로채는 것이 불가능함을 의미한다[13].

2.4 위치기반 인증 선행 연구

위치기반인증은 위치정보를 수신하는 단말기, 인증을 수행하는 서버, 인증을 요청하는 사용자로 구성된다. 사용자는 위치정보 수신기를 이용하여 위치 정보를 획득한다. 이후 인증을 위해 사용자는 수신한 위치정보를 서버에 전송한다. 서버는 사용자가 전송한 정보와 기존에 저장된 위치정보를 비교하여 인증을 수행한다. 위치기반인증은 위치정보를 수집하는 측위 방식과 인증 과정 시 위치정보 처리 방식에 따라 다르다. 위치기반 인증은 Two-Factor인증으로 피싱이나, 신원도용과 같은 인증관련 보안 사고를 방지 할 수 있다. LRAP는 서비스 제공자가 생성한 OTC (One-time code)를 위치정보로 암호화 한다. 사용

자가 결제 시 해당 위치에 존재하고, 자신이 소지한 모바일 장치를 이용하여 현재 위치정보를 수신 받으면, OTC를 복호화 하여 획득한 후 POS 결제를 수행한다[8]. STAT1는 인증 서버에 등록된 사용자의 모바일 장치가 수신하는 위치정보를 인증 요소로 하여 보호되어야 할 서버로 접근 통제를 수행하는 위치기반 인증 기법 중 하나이다. STAT1은 사용자의 인증 단말기(모바일 장치), 사용자 PC, 위치기반 인증을 수행하는 AAA서버, 보호되는 서버로 구성되어 있다. 인증 단말기와 PC는 UBS로 연결한다. 각 사용자의 인증 단말기와 인증 서버는 해시 함수를 제외한 공개키 기반의 서명을 통해 인증을 수행한다. 그 과정은 다음 순서를 따른다.

1) 사용자는 사용자 PC로 보호되는 서버에 요청을 수행한다.
2) 보호되는 서버는 요청메시지를 인증서버에 리다이렉팅한다.
3) 인증서버는 사용자 PC를 통해 인증 단말기로 위치정보를 요청한다. 이때 인증서버는 자신의 개인키로 암호화 한 요청 메시지와 요청 메시지 원본을 전달한다.
4) 인증 단말기는 인증서버의 공개키로 메시지를 검증하여 서버인증을 수행한다.
5) 이후 인증 단말기는 자신의 개인키로 암호화한 위치정보와 위치정보 원본을 전송한다.
6) 서버는 인증 단말기의 공개키를 이용하여 수신된 메시지를 검증하고 인증을 수행한다.
7) 최종 사용자 작업 환경이 이루어지는 PC와 보호되는 서버의 통신 연결을 위해 마지막 인증 결과를 사용자PC에 반영하고, 인증이 성공하였을 경우 서비스 전용 터널 연결을 수행한다.

기존 연구[6]은 인증에 사용되는 위치정보는 민감정보로 반드시 안전하게 처리 되어야 함을 언급하고 있다. 이에 인증서버와 인증 단말기의 상호 인증을 수행하고자 해시 함수를 제외한 공개키 기반의 서명을 응용한 프로토콜을 제안하였다. 그러나 모바일 장치의 개인키로 서명되어 인증 서버로 전송되는 위치정보는 완전한 기밀성을 제공하지 않으므로 전송 도중 위치정보가 노출될 가능성이 있다고 할 수 있다. 공격자가 특정 사용자의 정상 연결을 탐지하고 그 때마다 지속적으로 전송되는 위치정보의 패턴을 알게 되었을 경우 해당 위치정보가 특정 사용자의 인증요소로 사용됨을 파악할 수 있다. 또한 STAT1에서 인증 단말기가 위치 정보를 수신 후 개인키로 서명하기 전 그대로 노출되는 구간이 존재한다. 이 때 정상 사용자가 단말기의 위치정보를 조작하여 인증 시도 시 접근 권한을 획득 할 수 있다.

III. 보안 요구사항

기존 연구[14]는 전자 인증 단계에서 발생 가능한

〔표 1〕 보안 요구사항

보안 사항	요구사항
위치 정보 신뢰성	① 인증요소로 사용되는 위치정보는 신뢰 할 수 있는 정보여야 한다. 위치 측위 시 제 3자로부터 위·변조된 신호를 반영한 위치정보가 생성되지 않아야 하고 전송 도중 변조되지 않아야 한다. 또한 사용자가 모바일 장치로부터 위치 정보를 수신 했을 시 모바일 단말기에서 위치정보의 위·변조를 방지하여 위치정보 신뢰성을 보장한다.
인증 요소 기밀성	② 인증요소로 사용되는 위치정보는 다른 정보와 결합 했을 때 개인을 식별할 수 있는 정보가 된다. 따라서 인증에 사용되는 위치기반인증정보는 사용자와 정보 시스템 사이에 공유되는 비밀정보로 모바일 장치에서 인증 서버로 전송될 때 제 3자에게 유출되지 않아야 한다. 또한 인증정보 재사용 및 추측을 방지하기 위해서도 인증요소는 기밀성이 보장 되어야 한다.
인증 요소 무결성	③ 모바일 장치에서 생성되어 전송되는 모든 인증 요소들은 인증 서버로 전송 시 중간에 변조되지 않아야 한다. 또한 인증 서버는 공격자가 정당한 위치정보를 획득하여 인증을 시도하는 것인지 검증할 수 있어야 한다.
인증 도입 시 가용성	④ 새로운 인증 도입 시, 인증에 사용되는 기기(인증 수단)의 보급률과 인증 과정에 필요한 정보처리 기술은 기존 시스템에 장애를 발생시키지 않으며 기존 시스템과 동일한 가용성을 유지해야 한다.
접근 통제	⑤ 기존의 신분-기반 또는 규칙-기반 정책들에 사용자의 현재 위치, 지정된 시간 등 신분을 확인하는 접근통제 설정을 통해 물리적 보안 대책을 보완해야 한다.
	⑥ 접근 통제는 사용자의 안전하고 유연한 정보 자산의 접근을 최대한 고려하여 정보 자산 이용에 효율성을 보장해야 한다.
	⑦ 데이터 접근 하는 사용자는 인증 완료 후에도 지속적으로 접근 관리가 필요하다. 사용자가 이동형 디바이스로 작업하여 인증 수행 후 허가된 물리적 위치를 벗어나 데이터에 지속적으로 접근하는 것을 방지해야 한다.

위협에 대해 ITU-T 개체 보증 인증 프레임 워크와 NIST 전자 인증 가이드라인을 기반으로 도출하고, 보안 위협을 기반으로 '전자인증 보안 요구사항'을 추출하였다. 본 논문은 '전자인증 보안 요구사항'을 근거로 제안하는 위치기반 인증의 특성을 반영한 〔표 1〕을 보안 요구사항으로 한다.

IV. 서버 접근 통제를 위한 위치기반 인증

본 장에서는 기존 관련연구의 문제점을 개선하고 사용자 접근 통제를 보장하는 실내 위치정보 처리 단계와 서버 접근 통제를 위한 위치기반 인증 기법을 제안한다.

4.1 용어 정의

〔표 2〕 프로토콜 용어 정의

용어	정의
MD	사용자 모바일 장치(Mobile Device)
UT	사용자 단말(유선 연결 된 사용자 PC)
AS	인증 처리 서버(Authentication Server)
OBS	실제 데이터를 저장하고 있는 Object Server
R_i	AP_i와 Location Server간 동기화 되어 생성되는 임의의 난수
M	인증 요청 메시지
ID_i	사용자 로그인 아이디
PW_i	모바일 장치에서 위치기반 인증 어플리케이션 실행 시 요구되는 사용자 패스워드
TS_{MD}	모바일 장치 Time stamp
L_i	모바일 장치에 수신되는 사용자 위치정보
$IMEI$	인증서버에 등록된 사용자 모바일 장치 고유 번호
LT	인증서버에 전송되는 위치기반 인증 정보
C	LT의 해시 값
SC	C를 모바일 장치 개인키로 서명한 값
ELT	LT를 서버의 공개키로 암호화 한 값
ETK	$Ticket$을 K로 암호화 한 값
$Ticket$	UT에서 OBS로 접근하기 위해 AS와 최종인증에 사용되는 일회용 패스워드
P	OBS의 데이터 접근 권한 레벨
K_{M_PR}	서명을 위한 모바일 장치 개인키
K_{M_PB}	서명 검증을 위한 모바일 장치 공개키
K_{A_PR}	인증정보 복호화를 위한 서버 개인키
K_{A_PB}	인증정보 암호화를 위한 서버 공개키
K_{A_O}	인증서버와 Object Server의 비밀키
K_{L_A}	Location Server와 인증서버의 비밀키
K	$Ticket$ 을 암/복호화하기 위한 대칭키

4.2 위치정보 처리 단계

4.2.1 실내 위치 측위 방법

본 논문에서는 정보 접근 작업 환경이 주로 실내에서 이루어지는 점을 감안하여 실내 측위를 위해 실내 AP와 모바일 단말기 사이의 신호 세기와 전파 특성을 이용하여 측위 하는 RF Fingerprint 방식을 채택한다. RF Fingerprint 방식은 위치를 결정하는 Location Server에 신호세기(RSS)와, AP의 SSID, BSSID등으로 구성된 데이터를 수집하여 수집된 정보들의 평균값을 활용하여 비교 연산(패턴매칭) 후 위치를 결정하는 방식이다〔15〕. RF Fingerprint 방식은 Location Server가 미리 DB를 구축에 상당한 노력이 필요 하지만, 노이즈를 포함한 환경 정보를 활용하기 때문에 비교적 정확한 위치정보 결과를 제공한다〔11〕. 이 외에도 효율적인 실내 측위 기법이 존재한다면 RF Fingerprint 기법을 대체할 수 있다.

4.2.2 위치정보 처리 단계 위협

위치정보 처리 단계에서는 위치정보 신뢰성을 보장하기 위해 위치 정보 정확성과 함께 위치 정보의 안정성을 고려해야 한다. 위치 정보 정확성은 위치 측위 시 수집 되는 데이터가 신뢰 할 수 있는 데이터임을 보장하고 수집 도중 위·변조 불가능함을 의미한다. 만약 위치정보 정확성이 보장 되지 않을 경우 다음과 같은 위협이 존재한다. 첫 번째로 사용자의 위치를 측위를 수행하는 Location Server는 공격자가 Rogue AP를 이용하여 가짜 신호를 송출하는 경우 가짜 신호 데이터를 측위에 사용하기 때문에 실제 사용자의 위치가 아닌 다른 위치정보를 생성 할 수 있다〔16〕. 위치정보의 안전성은 Location Server에서 측위 대상으로 위치정보 전송과정과 위치정보 자체의 위·변조 불가능함을 의미한다. 위치 정보 안전성은 다음과 같은 위협에 따라 판단된다. 첫 번째로 무선 네트워크 기반 환경에서 사용자의 모바일 단말기에 수신되는 위치정보는 전송 도중 제 3자에 의해 노출되지 않아야 하며 위조나 변조할 수 없어야 한다. 만일 중간에 공격자가 위치 정보를 획득 하거나 획득한 정보를 위·변조 할 경우 정상 사용자인 것처럼 접근을 시도하거나, 정상 사용자의 접근을 방해 할 수 있다. 두 번째는 정상 사용자가 모바일 단말기 자체에 수신되는 위치정보를

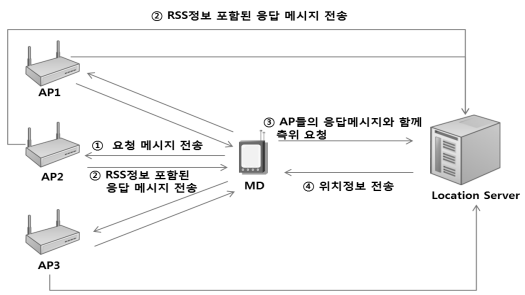
위·변조하는 것이다. 이것은 위치정보로 결정되는 접근 권한을 정상 사용자가 우회하는 원인이 될 수 있다.

4.2.3 제안하는 위치정보 처리 시스템

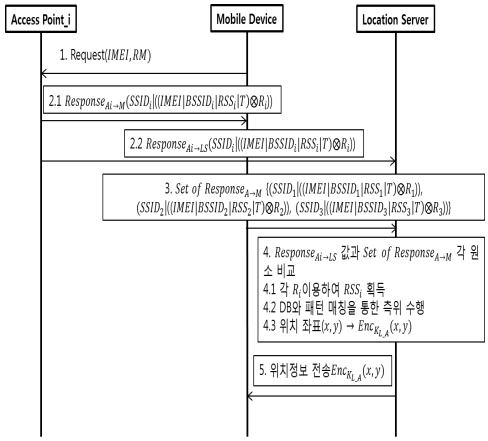
본 논문에서 제안하는 위치정보 처리 시스템은 RF Fingerprint 방식에 위치정보 신뢰성을 보장하고자 한다. 기존에 상용화 된 RF Fingerprint 방식을 활용하는 Skyhook localization process[16][17]에 전송되는 정보들에 임의의 난수를 XOR하는 단계를 추가 하였다. 이는 동일한 PN Generator(임의 난수 생성기)를 갖고 있지 않은 다른 노드들은 전송되는 정보를 중간에 가로챈다 하더라도 데이터를 복원할 수 없고 데이터를 위·변조 할 수 없음을 의미한다. 또한 AP_i가 생성하는 응답 메시지를 모바일 장치뿐만 아니라 Location Server에 동시에 전송하게 하여 수신된 데이터 값을 비교하여 모바일 장치에서 신호가 변조되어 전송되었는가를 판단할 수 있게 추가 하였다. 결과적으로 위치 결정을 위한 정보(응답메시지) 전송 도중 발생할 수 있는 위·변조에 대한 저항성을 높였다. 마지막으로 모바일 단말에 수신되는 위치정보는 인증서버와 Location Server의 비밀키로 암호화 된 값이기 때문에 정상 사용자가 접근 권한 우회를 위해 위치정보 자체를 열람하여 수정하는 행위를 불가능하게 한다. 참여 노드들은 다음과 같은 사항을 만족한다.

① MD(Mobile Device): 사용자가 소지하는 모바일 장치로 측위 대상이 된다. 주변 AP 장치에 위치 측위 요청 메시지를 브로드 캐스트 한다. Location Server와 DSSS기법을 적용한 무선 통신 수행한다고 가정한다.

② AP_i(Access Point_i): MD로부터 RSS를 측정한 후 RSS 정보 포함한 응답 메시지를 생성한다. 이때 AP_i는 Location Server와 각각 동기식 PN



〔그림 2〕 제안하는 위치정보 처리 단계 프로세스



〔그림 3〕 제안하는 위치정보 처리 프로토콜

Generator를 포함하고 있다.

③ Location Server(측위 서버): Location Server는 각 MD와 데이터 신호 안전성을 보장하기 위해 DSSS방식의 무선 통신 수행한다고 가정한다. 수집 데이터 안전성을 위해 각 AP_i와 동기화 된 PN Generator를 탑재하고 있다. 그리고 위치 측위에 사용될 각 AP와 좌표 정보로 이루어진 DB를 구축하고 있다. 마지막으로 사용자 MD에 위치 정보 전송 전 최종 위치정보를 암호화하기 위해 인증서버와 Location Server 간에 공유된 비밀키를 가지고 있다. 〔그림 2〕는 위치정보 처리 프로세스 과정을 나타내고 있다.

4.2.4 제안하는 위치정보 처리단계 상세 프로토콜

1) $MD \rightarrow AP\_i$: MD는 요청 메시지를 주변 AP_i에 전송한다.

2) AP_i 응답 메시지 생성 및 전송

① AP_i는 $Response_{A_i\to M}(IMEI|BSSID_i|RSS_i|T)$ 생성 후 LS와 동기식으로 생성되는 임의의 난수 R_i와 XOR연산한 결과에 $SSID_i$를 접합시킨 응답메시지 $Response_{A_i\to M}(SSID_i|((IMEI|BSSID_i|RSS_i|T)\otimes R_i))$를 MD에 전송한다.

② $Response_{A_i\to LS}(SSID_i|((IMEI|BSSID_i|RSS_i|T)\otimes R_i))$ 값을 각 AP_i가 Location Server에 전송한다.

3) $MD \rightarrow LS$: MD는 주변 AP_i로부터 수집한 응답 메시지를 모아서 LS에 $Set\,of\,Response_{A\to M}$를 보낸다.

4) Location Server는 MD로부터 수신한 $Set\ of\ Response_{A \rightarrow M}$와 AP_i로부터 수신한 $Response_{A_i \rightarrow LS}(IMEI|BSSID_i|RSS_i|T) \otimes R_i$의 원소를 각 비교한다. MD로부터 수신한 데이터와 AP_i로부터 수신한 데이터가 같다면, MD의 위치측위를 위해 R_i를 이용하여 $Response$메시지의 원본을 구한다. 그중 $BSSID_i$와 RSS_i, 값을 기존에 구축된 DB 비교를 수행하여 MD의 좌표값 (x,y)를 결정한다. 좌표값은 LS와 AS의 비밀키로 암호화 한 $Enc_{K_{L\_A}}(x,y)$ 값이 된다.

5) Location Server는 이전 단계에서 수신한 $Response$메시지의 $IMEI$를 참조하여 $Enc_{K_{L_A}}(x,y)$값을 MD로 전송한다. MD는 이후에 인증이 필요할 시 $Enc_{K_{L_A}}(x,y)$을 그대로 이용하여 인증을 시도한다.

4.3 제안하는 위치기반 인증 기법

4.3.1 시스템 모델

사용자 접근 환경의 물리적 통제를 위한 위치기반 인증 프로세스는 다음과 같은 시스템 모델을 갖춘다.

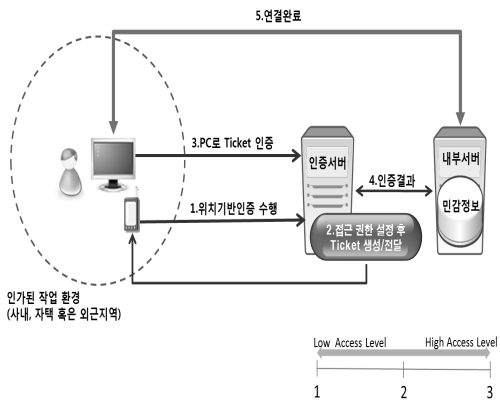
① 모바일 장치(Mobile Device): 사용자는 위치기반 인증을 수행하기 위해 모바일 장치를 사용자 PC와 USB 연결한다. 위치기반 인증에 사용되는 모바일 장치는 사용자가 소지하고 있는 개인 모바일 장치이다. 위치정보는 Location Server로부터 수시한다. 모바일 장치는 미리 인증서버에 등록되며 기기 등록정보로 $IMEI$를 사용한다. 사용자는 미리 설정한 패스워드를 입력해야 모바일 장치의 안전한 플랫폼에 접근 가능하며 모바일 장치의 위치기반 인증 프로세스를 실행할 수 있다. 모바일 장치의 위치기반 인증 프로세스는 위치정보 수신, 인증 요청 메시지 생성, 위치기반 인증정보 생성 및 암호화와 Ticket Display기능 등을 포함하고 있다.

② 사용자 단말(User Terminal, PC): 사용자 단말은 실제 데이터에 접근하여 작업이 이루어지는 PC이다. 사내 PC 뿐만 아니라 외근 시 사용되는 공용 PC 및 개인용 PC 모두 포함이 된다. 데이터에 접근하기 위해 사용자는 모바일 장치에서 Ticket을 확인한 뒤 PC에 Ticket값을 입력하여 인증서버에 최종 인증을 수행한다. 이때 사용자 단말과 인증서버는 안전한 SSL/TLS 통신을 수행한다고 가정하며 Ticket 값을 이용한 최종 인증 후 Object Server와 사용자 단말은 SSL/TLS 통신을 수행한다.

③ 인증 서버(Authentication Server) : 인증서버는 등록된 모바일 장치의 $IMEI$, 접근이 허가된 PC의 물리적인 위치정보, 접근 권한 레벨, 모바일 장치의 인증서(서명을 검증하기 위한 공개키 포함)를 이용하여 인증 및 접근 통제를 수행 한다. 이 때 참조되는 등록정보는 보안 관리자에 의해 관리되며 관리자 이외의 접근은 허용하지 않고 인증 및 접근 통제를 위한 등록 정보의 등록, 수정, 삭제할 경우 사용자의 동의를 얻는다. 인증 서버는 모바일 장치로부터 암호화된 위치정보를 수신하고 인증단계를 거쳐 접근을 요청한 사용자의 물리적 위치가 서버에 등록된 인가된 위치임을 확인한 뒤 서버는 해당 접근 권한 레벨을 설정한다. 〔그림 4〕에서 알 수 있듯이 OBS 접근을 위해 인증을 시도하는 위치에 따라 한 명의 사용자에게 다양한 접근권한 레벨을 부여할 수 있다. 사용자 위치에 따른 접근 권한 설정은 관리자가 접근통제 정책을 어떤 방식으로 설정하느냐에 따라서 다양하게 설정 가능하다. 〔그림 4〕에서 Access Level은 1~3으로 분류되고 있다. Access Level 1은 데이터를 열람하여 조회할 수 있는 접근권한이고, Access Level 2는 데이터 열람 조회 및 수정의 접근권한이다. Access

ID_i	$IMEI$	Location Information	DN's Certificate [Public key]	Access Level
Korea12	1158315	(x1, y1)	1158315_Certificate	2
Korea12	1158315	(x2, y2)	1158315_Certificate	1
Korea12	1158315	(x3, y3)	1158315_Certificate	3
Ieee312	1336544	(x4, y4)	1336544_Certificate	1
Ieee312	1336544	(x5, y5)	1336544_Certificate	3
Ieee312	1336544	(x2, y2)	1336544_Certificate	2
werdf223	1445369	(x1, y1)	1445369_Certificate	1
⋮	⋮	⋮	⋮	⋮

〔그림 4〕 인증서버 등록정보



〔그림 5〕 제안하는 위치기반 인증 시나리오

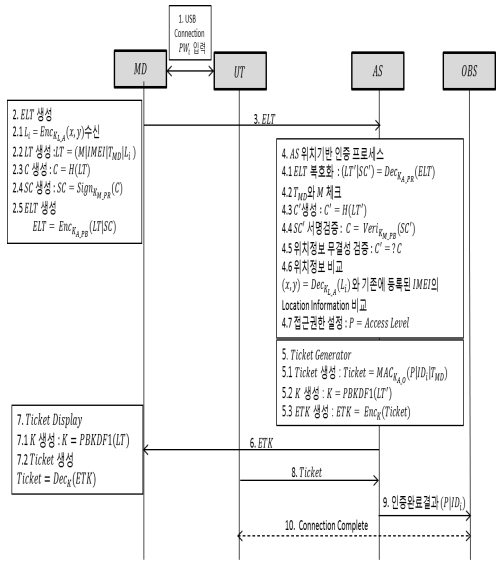
Level 3일 때는 데이터 열람 조회, 수정, 삭제의 권한을 할당 하며, 인증 서버는 권한 할당 완료 후 Ticket을 생성한다. 서버에서 생성된 Ticket은 키로 암호화 되어 모바일 장치로 전송된다. 이후 사용자의 위치정보를 실시간으로 확인한 뒤 접근통제를 수행한다.

4.3.2 위치기반 인증 시나리오

사용자는 인가된 작업 환경에서 인증 서버에 미리 등록 된 모바일 장치를 이용하여 인증을 시도한다. 사용자는 모바일 장치가 Location Server로부터 수신한 위치정보를 이용하여 위치기반 인증을 수행한다. 인증 서버는 사용자의 위치를 확인하고 해당 접근 권한을 할당한 뒤 Ticket을 생성하여 모바일 장치로 전송한다. 사용자는 모바일 장치에 수신된 Ticket을 확인한 뒤 PC로 Ticket을 이용한 인증을 수행한다. 인증 서버는 최종 Ticket 인증 수행 후 인증 결과를 내부 서버(OBS)에 전달하고 사용자 PC와 내부 서버는 통신 연결을 완료 한다.

4.3.3 제안하는 위치기반 인증 프로토콜 상세

1) $MD \leftrightarrow UT$: 사용자가 소지하고 있는 MD와 실제 데이터에 접근하는 사용자 PC(UT)는 USB포트로 유선 연결 된다. 유선 연결 이후 사용자 PC와 모바일 장치는 상호 장치 인식을 하고 사용자가 모바일 장치에 기존에 설정한 패스워드(PW_i)를 입력하면 로그인을 위한 위치기반 인증 프로세스가 실행된다.



〔그림 6〕 제안하는 위치기반 인증 프로토콜

2) MD의 위치기반 인증 정보(ELT) 생성 : 모바일 장치는 위치정보를 수신하고 서버에 전송할 위치기반 인증 정보(ELT)를 생성한다.

① L_i 수신 : 모바일 장치는 인증 서버(AS)에 전송하기 위한 위치정보를 LS로부터 수신한다.

② LT 생성 : 인증요청 메시지, 미리 등록된 모바일 장치 고유 번호, 모바일 장치 타임 스템프, 위치정보로 구성된다.

③ C 생성 : LT의 해시 값을 생성한다.

④ SC 생성 : C를 모바일 장치의 개인키로 서명한다.

⑤ ELT생성 : 모바일 장치는 LT와 SC를 AS의 공개키로 암호화 하여 ELT를 생성한다.

3) $MD \rightarrow AS$: MD는 AS로 ELT를 전송한다.

4) AS 위치기반 인증 프로세스 실행 : ELT를 수신한 AS는 인증 프로세스를 실행한다.

① AS는 개인키로 ELT를 복호화 하여 LT'과SC'을 얻는다.

② T_{MD}와 인증 요청 메시지 M을 체크한다.

③ 복호화 하여 얻은 LT'의 해시 값 C'을 생성한다.

④ 복호화 하여 얻은 SC'을 모바일 장치의 공개키로 서명검증 하여 C를 얻는다.

⑤ 전달받은 위치기반인증정보가 중간에 변조되지 않았음을 검증한다.

⑥ 위치정보 비교 : $(x,y) = Dec_{K_{L\_A}}(L_i)$ 와 기존 AS에 등록되어 있는 $IMEI$의 위치정보(Location Information)을 비교한다. (x,y)가 $IMEI$의 위치정보 허용 오차범위 안에 있다는 것이 확인 되면 다음 단계로 넘어간다. 그렇지 않은 경우 인증 요청을 거부한다.

⑦ $P = Access\ Level$: 등록정보를 참조하여 사용자 위치 정보에 따른 사용자 접근 권한을 설정한다.

5) AS의 Ticket Generator 실행 : 사용자 단말에서 최종 로그인시 필요한 Ticket를 생성한다.

①Ticket생성 : MAC을 이용하여 Ticket를 생성한다. 입력값은 위치정보 확인 후 할당 되는 P, 사용자 식별 ID, 모바일 장치의 타임 스템프 T_{MD}이며 사용되는 키는 AS와 OBS의 비밀키 K_{A_O}이다.

②$Ticket$을 암호화하기 위한 키 K를 생성한다. K

는 모바일 장치로부터 전달받은 LT'을 입력값으로 PBKDF1[18]을 이용하여 생성한다.

③ $Ticket$을 K로 암호화 하여 ETK를 생성한다.

6) $AS \rightarrow MD$: 인증서버는 ETK를 모바일 장치에 전송한다.

7) MD에서 Ticket Display : 모바일 장치는 전달받은 ETK를 복호화 하여 Ticket을 얻는다.

① $Ticket$을 복호화하기 위한 키 K를 생성한다. K는 모바일 장치가 인증을 위해 생성한 LT를 이용하여 생성한다.

② ETK를 K를 이용하여 복호화 한다.

8) $UT \rightarrow AS$: 사용자는 모바일 장치가 생성하는 Ticket를 확인, 사용자 작업 환경인 UT 로그인 창에 Ticket를 입력, 전송하여 최종 인증 수행 요청한다.

9) $AS \rightarrow OBS$: 최종 사용자 접근을 위한 Ticket 인증 결과인 사용자 ID_i와 상위 위치기반 인증 수행 후 할당 받은 접근 권한 P가 결합하여 전달한다.

10) $UT \leftrightarrow OBS$: Ticket이용한 최종 인증 완료 후, 사용자는 할당받은 접근 권한 P에 따른 실제 데이터 접근 실행한다. MD와 AS는 주기적으로 위치정보를 확인한다. (2~4 과정을 수행한다.) 만약 사용자 데이터 접근 실행 도중 해당 위치를 벗어난 경우 OBS로 접근을 종료(접근 권한 회수)한다.

V. 분석

5.1 안전성 분석

제안된 위치기반 인증의 안전성 분석은 보안 요구사항을 기준으로 STAT1과 비교하여 분석한다.

① 위치정보 신뢰성 : 본 논문에서 제안하는 위치정보 처리 단계에서는 위치측위 시 수집되는 데이터를 R_i와 XOR연산하여 위·변조를 방지하여 정확성을 보장하였다. 모바일 단말기 자체가 수신하는 위치정보는 AS와 LS의 비밀키 K_{L_A}로 암호화 된 값으로 수신 중 위·변조를 방지하고 정상 사용자의 위치정보 변조 시도를 방지하여 안전성을 보장하였다.

② 인증 요소 기밀성 : 기존에 제안된 STAT1의 경우 서버 인증을 통해 모바일 장치의 개인키로 서명되어 전송되는 위치정보가 안전하다고 주장한다. 그러나 만약 공격자가 전송되는 위치정보를 중간에서 가로챌 경우 개인정보 유출의 문제가 있으며 공격자가 정당한 사용자로 인증 우회를 위해 획득한 위치정보를 조작하여 인증서버에 전달 할 수 있다. 본 논문에서 제안하는 위치기반 인증기법은 식별정보와 결합한 위치 인증 정보를 서버의 공개키 K_{A_PB}로 암호화 하여 ELT 형태로 전송된다. 따라서 인증서버로 전송 도중에 노출 되지 않으며 개인정보보호를 보장한다. 사용자 단말에서 최종인증을 수행하기 위해 사용되는 일회용 패스워드인 Ticket값은 AS에서 비밀 공유키로 암호화 되어 ETK로 전송되기 때문에 공격자의 Ticket 재사용 공격을 막을 수 있다.

③ 인증 요소 무결성 : 모바일 장치에서 인증을 위해 생성되는 위치정보와 기타 사용자 식별 정보들은 모바일 장치의 개인키로 서명되어 $SC = Sign_{K_{M\_PR}}(C)$ 형태로 전송되고 인증 서버는 해당 모바일 장치의 공개키로 서명 검증 $C = Veri_{K_{M\_PB}}(SC')$ 과정을 수행함으로 전송 도중에 변조되지 않았음을 보장할 수 있다.

④ 인증 도입 시 가용성 : 최근 무선 인터넷 및 이동통신 기술의 발달과 위치 정보를 수신할 수 있는 기능이 탑재된 스마트 폰 및 모바일 장치의 급속한 확산으로 인해 사용자에게 따로 인증을 위한 기기 지급 비용이 필요하지 않으며, 기존 시스템 도입에 적합성을 보장한다.

⑤ 접근 통제 : 본 논문에서 제안하는 위치기반 인증은 사용자의 현재 위치정보에 따른 인증 수행으로 사용자는 서버에 등록된 인가된 위치에서만 정보 접근 및 작업이 가능하다. 이는 물리적 통제로 이어지며 정보자산 유출 방지를 위한 물리적 보안 대책이 될 수 있다. 위치기반 인증을 접근통제와 함께 연계시켜 설정할 경우 유연한 접근통제를 구현할 수 있다. 한 사용자는 인증을 수행하는 위치에 따라서 접근권한 레벨을 다양하게 부여 받을 수 있다. 인증 완료 후 인증서버는 모바일 장치의 지속적으로 주기적인 위치확인을 통해 실시간으로 사용자의 접근 권한을 회수 할 수 있다.

〔표 3〕 안전성 분석 비교

보안요구사항 / 프로토콜	위치정보 신뢰성	인증요소 기밀성	인증요소 무결성	인증 도입 가용성	접근 통제
STAT1	×	×	○	○	×
제안하는 프로토콜	○	○	○	○	○

〔표 4〕 제안하는 프로토콜과 STAT1 성능 비교

효율성분석 항목 / 프로토콜		연산 비용				통신비용
		공개키 연산 횟수		대칭키 연산 횟수 (P)	해시 연산 횟수 (H)	데이터 전송 횟수
		암/복호 (E/D)	서명/검증 (S/V)			
STAT1	모바일 장치	1S+1V		0	0	5
	사용자 PC	0		0	0	
	인증 서버	1S+1V		0	0	
	보호 대상 서버	0		0	0	
제안하는 프로토콜	모바일 장치	1E+1S		1P	1H	4
	사용자 PC	0		0	0	
	인증 서버	1D+1V		2P	2H	
	보호 대상 서버	0		0	0	

5.2 효율성 분석

기존 관련 연구인 STAT1과 본 논문에서 제안한 위치기반 인증 프로토콜을 비교하여 효율성을 분석한다. 〔표 4〕는 제안한 위치기반 인증 프로토콜과 STAT1의 연산비용과 통신비용을 비교한 것이다.

5.2.1 연산비용 비교

연산 비용은 공개키 연산, 대칭키 연산, 해시 연산의 횟수와 각 연산 시간을 기준으로 비교한다. 공개키 연산은 공개키 암·복호화와 서명과 서명검증에 따라 다른 연산 시간을 반영한다. 기존 STAT1 프로토콜은 모바일 장치와 인증서버에서 각 서명과 서명검증을 수행한다. 최종 연산은 2(1S+1V)로 실행 될 것이다. 제안된 프로토콜은 기존 STAT1 프로토콜과 비교 하였을 때 사용자 단말에서 일회용 패스워드를 이용한 최종 인증을 추가하여 Ticket생성을 위한 *MAC* 연산과 대칭키 연산의 수가 증가 되었다. *MAC* 연산 시간은 해시 연산 시간과 서로 큰 차이가 없기 때문에 해시 연산 횟수에 포함시킨다. 제안된 위치기반 인증 최종 연산은 1E+1S+1D+1V+3P+3H로 실행된다. 제안된 위치기반 인증 프로토콜은 STAT1 프로토콜과 비교 하였을 때 연산 수행 시간이 가장 긴 공개키 연산 횟수는 같고, 대칭키 연산 2회, 해시 연산 3회가 증가 하였다. 제안된 기법이 STAT1에 비하여 경미한 연산 수행 시간 증가가 예상 되지만, 〔표 4〕와 같이 STAT1보다 높은 안전성을 보장하기 때문에, 경미한 연산 수행 증가는 충분히 감안할 수 있다고 판단된다.

5.2.2 통신비용 비교

통신비용은 프로토콜에 참여하는 노드들의 데이터 전송 횟수를 기준으로 하여 비교한다. STAT1은 최종 사용자 PC인증을 포함하고 있지 않지만, 제안하는 위치기반 인증 프로토콜은 최종 사용자 PC에서 일회용 패스워드를 이용한 투 채널 인증을 제공함으로써 통신비용을 최소화하였다. 결과적으로 제안된 위치기반 인증 기법은 STAT1에 비하여 데이터 전송 횟수를 감소시켰다.

VI. 결론

본 논문에서는 접근 통제를 위한 사용자의 위치정보를 이용한 위치기반 인증을 제안하였다. 사용자의 위치정보를 인증요소로 이용함으로써, 물리적 접근 통제를 수행하며 최종 사용자 인증에 일회용 패스워드인 Ticket을 사용하여 인증을 강화하였다. 최종적으로는 사용자 단말과 데이터 서버와의 안전한 데이터 이동 경로를 확보하여 정보 유출 사고를 방지한다. 그리고 인증에 사용되는 사용자 위치정보를 안전하게 처리함으로써 기존에 제안된 STAT1 인증 프로토콜이 가지는 보안 취약점을 해결하고 보다 높은 효율성을 보장하는 프로토콜을 제안하였다. 위치기반인증 수행을 위해 반드시 필요한 사용자 위치정보는 다양한 측위기술을 이용해 생성 가능하다. 하지만 아직까지 사용자 위치정보가 인증을 위한 식별정보로 사용되기 위해서는 정확도가 다소 떨어지는 편이다. 그러나 사용자 위치정보의 오차범위를 줄이고 정확도를 높이기 위한 측위기술이 계속적으로 발전하고 있으며, 위치정보수신 기능을 탑재한 개인 모바일 장치의 확산에 따라 앞으로

는 정확한 위치정보를 누구나 사용할 수 있을 것으로 예상된다. 따라서 제안한 위치기반 인증 프로토콜은 측위기술의 발달에 따라 기존 시스템에 유용하게 적용될 수 있을 것으로 기대된다.

참고문헌

〔1〕 etnews.com, "내부 정보 유출 막아라, 기업들의 해결책은?," http://www.etnews.com/news/etc/2510410_1624.html, 2011년 9월.

〔2〕 DATANET, 보안담당자, "개인정보·내부정보 유출 걱정," http://www.datanet.co.kr/news/articleView.html?idxno=60710, 2012년 5월.

〔3〕 Andre van Cleeff, Wolter Pieters, Roel Wieringa, "Benefits of Location-Based Access Control : A Literature Study," 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, pp. 739-746, Dec. 2010.

〔4〕 ZDNET Korea, "안랩, 위치정보 활용 사용자 인증기술 특허," http://www.zdnet.co.kr/news/news_view.asp?artice_id=20120725111954&type=xml, 2012년 7월.

〔5〕 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.

〔6〕 David Jaros, "New Location-based Authentication Techniques in the Access Managemet," IEEE Computer society, pp. 426-430, Sept. 2010.

〔7〕 Elisa Bertino, Barbara Catania, Maria Suisa Damiani, "Geo-RBAC : A spatially Aware RBAC," SACMAT'05 Proceedings of the tenth ACM symposium on Access control models and technologies, pp.29-37, June. 2005.

〔8〕 Diana Berbecaru, "LRAP : A Location-Based Remote Client Authentication Protocol for Mobile Environments," 19th International Euromicro on Parallel, Distributed and Network-Based Processing of IEEE computer society, pp. 141-145, Feb. 2011.

〔9〕 진희채, 남광우, "위치 측위 방식과 위치기반 서비스 분석," 한국통신학회지(정보와 통신), 25(7), pp.24-33, 2008년 6월.

〔10〕 김정태, "무선 측위 기술 조사 및 분석," 대전자공학회논문지, 48(2), pp.72-78, 2011년 2월.

〔11〕 임유진, 박재성, 안상현, "실내 위치 측위 시스템을 위한 기하학적 접근 기법," 대한전자공학회논문지, 45(12), pp.97-104, 2008년 12월

〔12〕 김기현, "접근통제 기술 개요," 한국정보보호센터, 2001년 6월.

〔13〕 박세현, "위치기반 서비스에 적합한 전자서명 인증 기술 연구," 한국인터넷진흥원, 2003년 12월.

〔14〕 염흥열, 조효제, 이동희 "전자인증 수단 이용기반 확대를 위한 안전성 기준 연구," 한국인터넷진흥원, 2011년 12월.

〔15〕 김재훈, 강석연, "WPS측위 편차폭을 줄이기 위한 확률적 접근," 한국통신학회논문지, 37(7), pp.586-594, 2012년 7월.

〔16〕 Nills Ole Tippenhauer, Kasper Bonne Rasmussen, "Attacks on Public WLAN-based Positioning Systems," MobiSys '09 Proceedings of the 7th international conference on Mobile systems, applications, and services, pp.29-44, Jun. 2009.

〔17〕 Markus G.Kuhn, "Signal Authentication in Trusted Satellite Navigation Receivers," Towards Hardware-Intrinsic Security : Foundations and Practice, pp.331-348, Nov. 2010.

〔18〕 RSA Laboratories, "PKCS#5 v2.1: Password-Based Cryptography Standard," Octorber May, 2006.

〈著者紹介〉

최 정 민 (Jung Min Choi) 학생회원
2011년 2월: 서울여자대학교 정보보호학과 졸업
2011년 2월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 접근통제, 사용자 인증

조 관 태 (Cho, Kwantae) 학생회원
2005년 2월: 고려대학교 컴퓨터학과(학사)
2005년 3월~2008년 2월: 고려대학교 정보보호대학원(공학석사)
2008년 3월~현재 : 고려대학교 정보보호대학원 박사과정
〈관심분야〉 WSN 보안, 기기간 보안 통신, 차량간 보안 통신, 키 교환

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학석사)
1992년 5월: Oklahoma University 전산학 대학원(공학박사)
1992년 8월: 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술