http://dx.doi.org/10.3745/KIPSTC.2011.18C.5.327

위치기반 Two-Factor L-OTP 프로토콜

서 화 정[†] · 김 호 원[††]

요 약

기존 휴대폰에 비해 강력한 연산능력을 가진 스마트폰의 출시 이후 개인 컴퓨터에서 제공되던 온라인 서비스의 영역이 점차 스마트폰으로 확산되고 있는 추세이다. 이러한 기술의 발전은 사용자에게 서비스제공의 시간 및 공간적 제한을 없애 주었지만, 악의적 공격에 쉽게 노출되는 보안상의 취약점을 가진다. 특히 금융권 서비스 이용 시 사용자의 비밀 정보가 교환되므로 더욱 주의를 기울여야 한다. 이러한 보안 문제를 해결하기 위해서는 하나의 세션에 하나의 비밀 키만을 사용하는 OTP(One Time Pad)가 권장되고 있다. 지금까지 스마트 폰에서의 OTP기법들은 기존 환경에 초점을 맞추어 제안 및 구현되어 왔다. 하지만 모바일 환경에서의 보안은 기존 시스템에 비해 공격에 취약할 뿐 아니라 자원적인 한계점을 가진다. 따라서 스마트폰에 적합한 새로운 개념의 OTP의 도입이 요구되어 진다.

본 논문에서는 시간동기화를 통한 T-OTP(Time One Time Pad) 기법과 위치기반 정보를 접목한 L-OTP(Location-OTP) 프로토콜을 제시한다. 제안된 방식은 스마트폰에서 사용자가 가지는 유일한 위치정보를 통해 OTP를 생성한다.

키워드 : OTP, 위치, 모바일

A Location based Two-Factor L-OTP Protocol

Seo, Hwa-Jeong[†] · Kim, Ho-Won[††]

ABSTRACT

After releasing the smart phone equipping the strong computational capability compared to traditional mobil phone, a field of services, which is available on the personal computers, is expanded to smart phone. The development of technology reduces the limited service utilization on time and space but it has a venerability exposing an information to malicious user. Especially we need to more attention when using the financial services which communicate the user's private information. To solve the security problem, OTP(One Time Pad), which uses a private key for a session, is recommended. OTP techniques in smart phone having focused on traditional environments have been proposed and implemented. However, security over mobile environments is more vulnerable to attack and has restriction on resources than traditional system. For this reason, definition of proper conceptual OTP on smart phone is required.

In the paper, we present the L-OTP(Location-OTP) protocol, using T-OTP(Time One Time Pad) technique with location information. Proposal generates the OTP using unique location information which is obtained in smart phone.

Keywords : OTP, Location, Mobil

1. 서 론

최근 불어 닥친 스마트폰의 돌풍으로 사람들은 언제 어디서나 인터넷에 접속하여 자신이 필요한 서비스를 제공받는 것이 현실화되었다. 이는 스마트 폰이 일반 폰보다 진보된 CPU능력, Wi-Fi 그리고 GPS와 같은 최신 기술을 내재하고 있으며 Open OS(Operation System)를 이용하여 누구나 제작 및 배포가 가능하기 때문이다[1]. 하지만 개방형 모바일 환경에서는 범용 OS를 채택하여 누구나 쉽게 개방된 개발 환경을 알 수 있으므로 모바일 공격의 규모 및 피해가 증가할 것으로 예상된다[2]. 따라서 모바일 상에서의 안전한 서비스 제공을 위해 금융권과 온라인 게임 사이트에서 특정 자원에 접근하는 사용자의 신원을 파악하는 것이 요구되어지고 있다. 이를 해결하기 위한 다양한 보안 기법 가운데 모바일 상에서 가장 활발히 연구되는 분야 중 하나는 OTP(One Time Password)를 이용한 사용자 인증 방법이다. OTP기법은 사용자에게 해당 세션에서만 사용가능한 비밀번호를 사용하여 사용자를 인증하는 보안 시스템이다. 해당 기법의 인증요소를 사용하는 방법의 수에 따라 구분하면 단일요소인증(1-Factor), 이중요소인증(2-Factor), 삼중요소인증(3-Factor)으로 구분된다. 이는 인증에 필요한 요소를 기

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2010-0026621).
† 준 회 원 : 부산대학교 컴퓨터공학과 석사과정
†† 정 회 원 : 부산대학교 정보컴퓨터공학부 조교수
논문접수 : 2011년 5월 24일
심사완료 : 2011년 7월 8일

존의 ID/Password방식을 벗어나 생체기반(홍채, 지문, 음성), 시간 그리고 카운터와 같은 정보를 조합하여 유일한 OTP를 생성해 내게 된다. 이와 같은 인증요소의 조합은 키의 값이 유일성을 가질수록 공격자에 의해 키의 생성이 어려우므로 권장된다.

본 논문에서는 GPS를 통한 위치정보를 이용하여 OTP생성에 필요한 인증요소를 제공하는 위치기반 OTP인 L-OTP(Location-OTP)를 제안한다. 논문의 구성은 다음과 같다. 2장에서는 OTP 기술과 위치정보에 대해 기술한다. 3장에서는 본 논문에서 제안하는 L-OTP 메커니즘 모델을 기술하고 4장에서는 제안 모델의 안전성 및 효율성을 분석한다. 5장에서는 구현결과를 보이며 마지막으로 6장에서는 본 논문에 대한 결론을 내린다.

2. 관련 연구

2.1 OTP 동기화 기술

서버와 OTP기기는 서로간의 동기화된 Seed값을 통해서 동일한 비밀값을 생성하는 기법이다. 따라서 동기를 맞추기 위해 다양한 방안이 사용되고 있다. OTP 동기화 기술은 시도 응답(Challenge response)방식, 시간 동기화(Time-Synchronous)방식 그리고 이벤트 동기화(Event-Synchronous)방식으로 크게 나누어 볼 수 있다. 현재 금융거래에서 사용되는 OTP 동기화 방식은 시간 동기화 방식을 사용하고 있으며 이에 대한 표준화작업이 진행 중에 있다[3].

2.1.1 시도 응답(Challenge-response)방식

인터넷 뱅킹 이용 시 사용하게 되는 보안 카드와 같이 사용자가 서버로부터 제시되는 시도값을 얻은 후 그 값을 특정한 알고리즘에 넣어 수행한 뒤 나오게 되는 값을 응답으로 서버에 입력하여 정당한 사용자인지 아닌지를 확인하는 기법이다.

2.1.2 시간 동기화(Time-Synchronous)방식

서버와 OTP단말기는 시간으로 서로 동기화되어 특정한 시간 간격에 따라 다른 OTP를 생성해 내는 방식이다. 이는 동기화된 시간을 짧게 잡을 경우 키 입력 시에 시간을 벗어나는 문제점과 반대로 시간을 너무 길게 잡을 경우 공격자가 OTP값을 알아챌 수 있는 가능성이 높아지는 단점이 있다. 또한 시간동기화를 위해 OTP단말기와 서버간의 시간동기화를 위한 추가적인 알고리즘이 필요하다.

2.1.3 이벤트 동기화(Event-Synchronous)방식

서버와 OTP단말기는 서로 간에 공유된 카운터를 유지하며 해당 값에 따라 OTP값을 생성하게 된다. OTP값이 생성되면 카운터가 증가하게 되고 이를 이용하여 새로운 카운터 값을 생성하게 된다. 하지만 해당 카운터값이 어긋나게 되는 경우 서버와 OTP단말기의 동기화가 다시 이루어 져야하는 단점이 있다.

2.2 위치 기반 정보

기존의 데스크 탑과 랩 탑 컴퓨터에서 서비스가 불가능했던 다양한 서비스들이 스마트 폰의 등장과 함께 가능해 지고 있다. 그 대표적인 예가 위치 기반 서비스이다. 스마트폰에 탑재된 GPS기능을 이용하여 사용자의 위치를 얻고 해당 위치정보를 기반으로 하여 사용자에게 특성화된 서비스 제공이 가능하다[4]. 예를들어 사용자 주위에 위치한 상점에 대한 정보를 얻고자 한다면 해당 GPS정보와 상점정보를 종합하여 해당 서비스 제공이 가능하다. 이러한 서비스의 제공은 정확한 위치정보를 기반으로 한다. 예전에는 빌딩안에 머무르게 될시 사용자의 위치정보를 얻는 것이 불가능했다. 하지만 GPS, Cell Tower 그리고 WPS(Wi-Fi Positioning System)정보를 조합하여 보다 정확한 위치정보 획득이 가능한 기법이 제안되고 있다.

2.2.1 GPS

궤도상에 배치된 인공위성으로부터의 수신되는 신호를 측정하여 지구상의 위치를 도출하는 방식이다. 하지만 실내, 건물 밀집지역과 같은 음영지역에서 신호감쇄로 인해 정확한 위치 인식이 불가능하다.

2.2.2 Cell Tower

CDMA, GSM/GPRS, WCDMA등과 같은 이동 통신망 기반으로 신호의 세기, 도달시간, 도달시간차, 입사각 등을 통해 사용자의 위치를 추적한다. 하지만 정확한 위치 인식을 위해 동기화 타이밍 유닛이 필요하다.

2.2.3 WPS(Wi-Fi Positioning System)

무선 LAN의 AP(Access Point)기기들로부터 수신되는 RF신호의 세기와 RF신호의 전달 지연을 이용한다. 이는 LAN장비의 정확한 위치정보가 필요하며 해당 장비가 고정되어 있어야 한다.

2.2.4 XPS

GPS, Cell Tower 그리고 WPS의 모든 정보를 이용하여 정확하고 신뢰성 높은 위치 정보를 제공한다[5]. 해당 기법은 실내의 위치 추적에도 용이하며 사전에 알려진 AP에 따른 위치 정보를 사용하여 위치를 측정함으로 성능과 정확도가 향상된다.

3. L-OTP(Location based One Time Password)

3.1 TOTP와 위치정보를 이용한 인증기법

본 논문에서 제시하게 될 OTP 알고리즘은 시간 동기화 기법인 TOTP를 통해 생성되는 비밀값과 위치정보값을 exclusive-or연산을 통해 OTP를 생성하는 기법이다. 해당 알고리즘은 OTP단말기와 인증서버가 동일한 시간으로 동기화가 되어 있어야 하며 사용자는 사전에 자신이 접속하게 될 위치에 대한 정보를 인증 서버에 저장해 두어야 한다.

3.2 제안 방식

본 장에서는 제안하는 알고리즘의 프로토콜과 사용되는 용어에 대해 상세히 알아보도록 한다.

3.2.1 용어 정의

<표 1>은 제안하는 알고리즘에서 사용되는 용어를 나타낸다.

(그림 1) 위치기반 OTP

〈표 1〉 용어 정의

기호	설명
ID	OTP가 가지는 Identification 값
K	인증서버와의 세션키 값
K_s	세션키 생성을 위한 임의의 난수
GPS	GPS정보
E_k	키 k로 암호화된 값
E_o	OTP의 공개키로 암호화된 값
C_s	위치 서버의 비밀키로 서명된 값
H_{GPS}	해시 연산된 GPS값
$H(\bullet)$	해시 연산

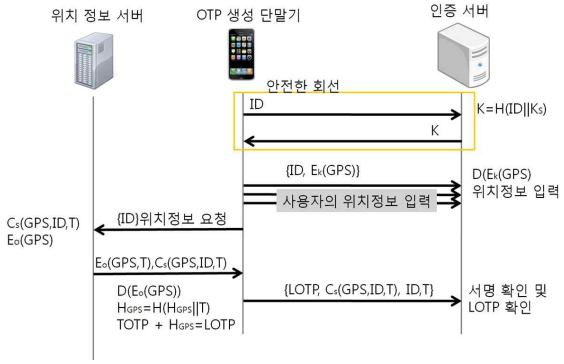
3.2.2 L-OTP 프로토콜

(그림 2)는 L-OTP의 전체 수행 프로토콜을 나타낸다. 처음에 생성 단말기는 안전한 회선을 통해 ID값을 인증 서버 쪽으로 전송하게 된다. 전송된 ID값은 서버에서 생성된 난수 K_s와 함께 해시연산을 수행하며 이를 통해 세션키값 K를 생성하게 된다. 사용자는 자신이 원하는 시기에 자신의 아이디와 자신의 비밀키로 암호화된 GPS정보를 인증 서버 쪽으로 전송하게 된다. 이를 통해 사용자는 자신이 OTP를 사용할 장소에 대한 GPS정보를 인증서버에 저장하게 된다.

OTP 생성단말기는 OTP생성이 필요한 시기에 자신의 GPS를 요청하게 된다. 이때 XPS서비스와 같이 위치정보를 저장하고 있는 위치정보 서버에서는 요청한 단말기에게 자신의 비밀키로 서명된 위치정보와 단말기의 공개키로 암호화된 위치정보 그리고 시간정보를 단말기에게 전송하게 된다.

단말기에서는 자신의 비밀키값을 통해 위치정보를 복호화하며 해당 위치정보에 매칭되는 해시위치정보와 시간정보를 해시연산하여 새로운 위치정보에 대한 해시값을 만들어 낸다. 이 값은 TOTP의 결과값과 exclusive-or연산을 하여 LOTP를 생성하게 된다.

생성된 LOTP, 서명된 위치정보, 단말기의 ID의 값 그리고 시간정보가 인증서버에게 전송되게 된다. 인증서버에서는 시간정보를 통해 해당 정보의 신선도를 확인한다. LOTP를 확인하기 위해 단말기와 동기화된 시간을 통해 TOTP를 생성하며 해당 값을 LOTP와 exclusive-or연산을 하여 해시된 위치정보를 만들어내게 된다. 이때 ID가 가지는 모든 위치정보에 대한 해시된 위치정보를 비교하여 동일한 값이 나온다면 위치정보 서버로부터 서명된 메시지를 인증한다. 만약 값이 제대로 나오지 않는다면 이는 잘못된 LOTP가 생성되었음을 의미한다.



(그림 2) 위치기반 OTP 프로토콜

<표 2>는 위치정보를 마스킹하기 위한 하나의 기법이다. 사용자가 접속하는 곳의 GPS 위치정보는 일정하여 공격자에 의해 쉽게 추측이 가능하다. 이를 방지하기 위해 위치정보와 위치정보의 생성 시간을 해시 연산함으로써 해시체인과 같이 계속해서 새로운 값을 암호화에 사용하게 된다.

〈표 2〉 GPS정보저장방식

첫 번째 라운드	두 번째 라운드	N번째 라운드
$H(GPS\|\|T) = H^1_{GPS}$	$H(H^1_{GPS}\|\|T) = H^2_{GPS}$	$H(H^{n-1}_{GPS}\|\|T) = H^n_{GPS}$

4. 안전도 및 성능 분석

4.1 보안성 요구조건

본장에서는 금융보안연구원에 의해 발행된 모바일 OTP 보안성 분석서의 요구조건에 따라 안전도를 확인해보도록 한다[6]. 보안 검토사항으로는 환경적 보안 요소와 기능적 보안 요소가 있다. 본 논문에서는 OTP의 기능적 요소에서 소프트웨어 구현시 안전성에 대해 검토해 보도록 하겠다. 즉 하드웨어적 그리고 제도적 관점에서의 보안은 안전하다고 가정한다.

4.1.1 OTP를 생성시 안전한 암호 알고리즘을 사용

해시알고리즘은 SHA224~512에 해당하는 알고리즘을 사용해야 한다. 현재 TOTP 표준에서는 SHA1, SHA256, SHA512까지 선택이 가능하다. 따라서 권고하는 보안을 만족한다.

4.1.2 암호화를 위한 세션키는 유추가 불가능한 값으로 사용

세션키 생성시 난수 생성 알고리즘을 이용하여 키를 생성하므로 생성키의 유일성을 보장해 주며 인증서버에서 일괄적으로 키를 생성하며 안전한 채널을 통해서 배포를 함으로 키에 대한 무결성 그리고 기밀성을 보장해 준다.

4.2 안전도 분석

안전성을 분석하기 위하여 기존에 나와 있는 공격에 취약성을 가지는 지 확인해 보도록 한다.

4.2.1 Password Guessing Attack

패스워드 추측공격이란 프로토콜에서 사용되는 비밀키 값을 공격자가 추측하여 대입해 보는 공격을 말한다. OTP 단말기와 인증서버는 서로 간에 안전한 채널을 통해 사전에 키를 공유하게 된다. 또한 해당 키는 난수값에 의해 생성이

됨으로 사용자들이 쉽게 선택하게 되는 자신의 특성(주민번호, 전화번호)을 유추한 공격에 강인하다.

OTP에 사용된 정보 또한 위치 서버에서 인증받은 위치정보와 수행횟수에 따라 변경되는 GPS 해시값은 공격자에 의해 유추가 불가능하다.

4.2.2 Stolen Verifier Attack

사용자인증에 사용되는 정보는 인증서버에 저장되어 공격자들의 공격대상이 된다. 본 논문에서 사용하는 위치정보의 경우 공격자가 해당 정보를 알게 된다고 하더라도 사용자의 단말기에서 생성되는 LOTP값을 생성해 내는 것이 불가능하다.

OTP 단말기는 위치정보서버와 비대칭키 방식의 정보교환이 이루어 진다. 즉 OTP단말기의 공개키로 암호화된 값으로 위치정보와 타임스탬프를 전송한다. 따라서 공격자는 위치정보생성에 사용되는 위치와 시간을 알 수 없으므로 인증 서버에서 얻은 정보를 통해 단말기의 LOTP와 위치서버의 서명값을 생성할 수 없다.

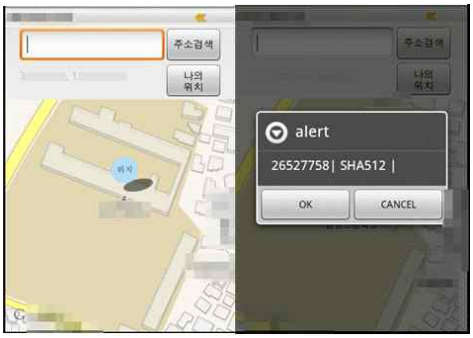
4.3 성능

제안된 프로토콜은 기존의 TOTP개념에 위치정보를 시간과 공간상으로 보다 안전하다. 유통되는 위치정보의 신뢰도를 높이기 위해 XPS의 위치정보서버에서 위치정보에 대한 서명을 수행하도록 제안하였다. 기존의 TOTP에 비해 메시지에 대한 서명과 검증 그리고 위치정보에 대한 암복호화 과정이 각각 한번씩 추가되었다.

5. 구현 결과

본 논문에서 제시하는 프로토콜은 안드로이드 OS 2.2상에서 구현해보았다. 프로토콜에 위치정보로 사용된 GPS정보는 위도와 경도에서 측정의 최소단위를 0.001로 하여 계산하였다. 여기서 위도는 1도당 약 110km 정도, 경도는 위도에 따라 1도당 0~110km정도의 차이가 나타났다. 따라서 위도와 경도의 0.001도 차이는 약 100m의 거리를 나타내게 된다. 또한 경도와 위도의 오차 범위를 생각하여 GPS결과값에 (+,-)0.001을 수행한 결과값을 사용하여 위치정보로 활용하였다. 본 알고리즘의 구현 실험은 한국 영토를 기준으로 수행해 보았다.

실험 시나리오는 사용자가 먼저 자신이 위치한 장소의 GPS정보를 인증서버에 저장하고 조건을 만족하는 위치에서 위치정보 서버에게 인증을 요청한다. 그 다음에 서명된 위치정보와 암호화된 GPS정보가 폰에 전송되게 된다. 복호화된 위치정보와 TOTP는 LOTP 생성에 사용된다. (그림 3)은 자신의 위치정보를 저장한 뒤 해당정보를 이용하여 LOTP를 생성하는 화면이다.



(A) (B)

(그림 3) (A)자신의 위치정보, (B)LOTP생성

6. 결 론

본 논문에서 제시하는 OTP 동기화 기법은 위치정보서버로부터 서명받은 사용자의 위치정보를 인증서버와 동기화된 시간 정보와 함께 조합하여 위치기반 OTP를 생성하게 된다. 제시된 방안은 위치기반 서비스의 발전과 맞물려 그 중요도가 높아지고 있는 위치정보를 이용한 새로운 개념의 OTP 동기화 기법이다. 이는 사용자가 지정된 위치에서만 서비스에 접근을 할 수 있도록 제한함으로써 보안관점에서 안전한 OTP관리 및 생성이 가능하다.

참 고 문 헌

[1] 제갈병직, "스마트폰 시장과 모바일OS 동향", Market Trends, Vol.36, 2010.
[2] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안 기술", 정보보호학회지, 제19권 5호, 2009. 12.
[3] IETF, "TOTP: Time-based One-Time Password Algorithm," 2010.
[4] K¨upper, A.: Location - .based Services -. Fundamentals and Operation. John Wiley & Sons, Chichester 2005.
[5] F Henry, R Henry, G Rooss, "Hybrid positioning system", 2006. 2.
[6] 금융보안연구원, "모바일OTP 보안성 분석서", 2011. 3.

서 화 정
e-mail : hwajeong@pusan.ac.kr
2010년 2월 부산대학교 정보컴퓨터공학과 (공학사)
2010년 2월~현 재 부산대학교 컴퓨터공학과 석사과정
관심분야 : 정보보안, RFID/USN, 암호 이론, VLSI 설계

김 호 원
e-mail : howonkim@pusan.ac.kr
1993년 2월 경북대학교 전자공학과 (공학사)
1995년 2월 포항공과대학교 전자전기공학과(공학석사)
1999년 2월 포항공과대학교 전자전기공학과(공학박사)
2008년 2월 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원/팀장
2008년 3월~현 재 부산대학교 정보컴퓨터공학부 조교수
관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안