제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

모바일 금융 서비스를 위한 확장된 OTP 메커니즘

한창윤, 임나석, 최옥경, 홍만표
아주대학교 대학원 지식정보보안학과
e-mail : shadow115@ajou.ac.kr, nsleem@ajou.ac.kr, okchoi@ajou.ac.kr, mphong@ajou.ac.kr

Extended OTP Mechanism For Mobile Financial Services

Changyun Han*, Naseok Lim, Okkyung Choi, Manpyo Hong
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

스마트폰 보급의 확산으로 모바일 금융 서비스 이용자 수는 증가하고 모바일 금융 보안에 대한 중요성이 증가되고 있는 실정이지만 해마다 다양해지는 금융 공격에 대비하기는 결코 쉽지 않다. 최근 주로 사용되고 있는 금융 보안 인증 방식인 OTP(One-Time Password)는 세션 공격에 대한 보안 대비가 가능하지만 차별화된 OTP 생성 메커니즘을 적용하는 것이 힘든 단점이 있다. 본 연구에서는 이러한 기존 방식의 문제점을 해결하기 위해 확장된 OTP 메커니즘을 이용한 새로운 금융 보안 방식을 제안하고자 한다. 제안 방식은 센서 네트워크를 금융 보안 알고리즘에 적용시킨 위치 기반 동기화 방식의 OTP 생성 메커니즘으로서 다양한 금융 해킹과 공격 기법에 대비가 가능하다.

1. 서론

All IP 기반 이동통신 네트워크의 활성화로 인하여 모바일 단말기를 통한 금융결제 서비스의 사용이 증가한다. 모바일 금융서비스는 이동통신망과 유무선 통신망에 VoIP(Voice over Internet Protocol)와 IMS(IP Multimedia Subsystem)의 기술을 통하여 인터넷 뱅킹, 텔레 뱅킹, 각종 금융 결제가 가능하며, 공간과 시간의 제한을 받지 않는다. 하지만, 해마다 정교해지는 금융 공격에 의해 모바일 금융 보안이 큰 이슈가 된다.[1]

최근, 로컬 네트워크에서 활발히 사용하는 세션 인증 방식은 OTP이다. OTP는 해당 세션에서만 패스워드의 사용이 가능한 일회용 패스워드이다. 따라서 MITM(Man In The Middle)공격이나 재사용 공격에 의해 패스워드가 노출되어도 다음 세션에서 사용할 수 없기 때문에 세션 공격에 대한 보안이 가능하다. 현재 OTP는 다양한 금융서비스와 인터넷 결제 등에 활용된다. 그러나, 이동 통신 서비스는 모바일 단말기의 로밍이 자주 일어나고, 다중 회선을 사용하기 때문에 현재 OTP 생성 메커니즘을 적용하는 것은 여러 가지 문제가 있다.[2]

본 논문은 USN(Ubiquitous Sensor Network)을 이용하여 확장된 OTP 메커니즘 생성 방안을 제시한다.

먼저, 위치기반 OTP는 동기화 방식의 생성 메커니즘으로서, 센서 네트워크와 모바일 단말기의 위치를 통하여 OTP를 생성한다. 모바일 단말기에는 센서가 부착되어 있으며, 센서 노드들과 통신을 하며 세션마다 다른 OTP를 생성한다. OTP의 생성은 모바일 단말기의 위치 좌표 값을 이용하여 연산을 수행한다.

2장 기반 기술은 대표적인 보안 인증 방식인 OTP에 대해 살펴보고, 기존 OTP 메커니즘의 보완점을 살펴본다. 3장에서 위치를 통한 OTP 생성 알고리즘과 설계 및 구현 방식을 기술하고 마지막으로 4장에서 결론과 향후 연구방향을 제시하였다.

2. 기반 기술

OTP는 고정 패스워드의 유출에 의한 재사용 보안 취약성을 보완하기 위한 일회용 패스워드로 매번 다른 비밀번호로 사용자를 인증하는 일회용 비밀번호를 의미한다. 한번 사용했던 비밀번호로 다음에 사용될 비밀번호를 유추하는 것이 수학적으로 불가능하다. 모바일 OTP는 하드웨어 방식의 OTP발생기와 같은 전용장치를 이용하지 않고, 휴대폰 등의 이동장치에 설치된 OTP 모듈을 통해 생성되는 방식을 의미한다.[3]

OTP 생성 메커니즘은 사용자가 OTP를 패스워드로 사용하기 위해 가변적인 난수를 생성하는 방식을 의미한다. OTP 생성 메커니즘은 비 암호 모듈 방식, 별도 채널 이용방식, 암호 모듈 이용방식으로 나뉜다. 현재 상용화되어 사용하는 방식은 주로 암호 모듈 이용방식으로 공개된 표준 해쉬 알고리즘을 이용하여 OTP를 생성한다.

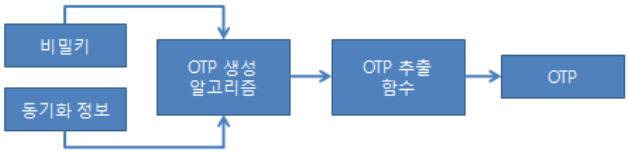

그림 1. OTP 생성 메커니즘

비밀키 : 모든 OTP에 유일하게 저장된 비밀 값으로 암호 알고리즘의 비밀키로 사용된다.
동기화 정보 : 비밀키와 같이 암호알고리즘에 입력되어 OTP값을 생성하는 중요 정보로, 매번 OTP 값을 변경시키는 정보.
OTP 생성 알고리즘 : OTP를 생성하는 알고리즘.
OTP 추출 함수 : OTP 생성 알고리즘을 통해 생성된 값을 6~8 자리 숫자로 변화하여 최종 OTP 값을 추출하는 함수.

OTP는 동기 정보에 따라 시간 동기화, 이벤트 동기화, 질의/응답 방식이 있다.

*시간 동기화 방식[4,5] : 서버와 OTP 장치 간에 동기화된 시간 정보를 기준으로 특정 시간간격 마다 OTP를 생성하는 방식이다. 특정 시간 간격마다 비밀 번호가 변하기 때문에 특정시간 간격 안에 입력을 못하면 비밀 번호가 바뀌어 다시 입력해야 하는 단점이 있다. 모바일은 이동성과 휴대성이 중요하므로 시간 간격을 길게 잡을 경우, 공격의 가능성이 커지게 된다.

*이벤트 동기화 방식[4,5] : 서버와 OTP 장치 간에 동일한 카운트 값을 기준으로 OTP를 생성하는 방식이다. 모바일 단말기에 이벤트 동기화 방식을 사용할 때, 여러 번 패스워드만 생성하고 해당 패스워드를 인증 값으로 사용하지 않으면, OTP 장치와 서버 간의 카운터 값이 달라져 OTP 장치를 다시 초기화해야 하는 단점이 있다.

*질의/응답 방식[4,5] : 어떤 단말기를 사용하든 사용자는 해당 질의 값을 입력하고, 그 결과로 얻은 응답 값을 다시 입력해야 한다. 따라서 사용자의 입력 내용이 많고 번거로움이 발생한다.

모바일 단말기는 이동성과 휴대성이 좋은 특징이 있다. 하지만 기존 동기화 방식을 사용하면 모바일 단말기 사용에 제약이 발생하며, 언급한 문제로 인하여 무결성과 가용성에 하자가 발생한다. 따라서, 센서의 위치를 이용하여 모바일 전용 OTP 메커니즘을 생성한다. 모바일 단말기는 삼변 측량을 통하여 센서 노드와의 거리를 알 수 있으며, 위치 좌표를 알 수 있다. 그리고 모바일 단말기의 고유 단말번호를 위치 좌표와 연산을 하여 암호 키를 생성한다. 단말기의 고유 번호를 연산에 사용하는 이유는 공격자가 동일한 위치에서 OTP를 생성할 경우 동일한 난수 값이 생성될 확률이 발생하기 때문이다. 생성한 암호 키는 hash 함수를 통하여 난수 값이 형성된다.

3. 확장된 OTP 생성 메커니즘

위치 기반 OTP 생성 메커니즘은 기존 동기화 방식과는 다르게 OTP의 위치를 암호 키로 사용한다. 지정 서버와 사용자는 미리 모바일 금융 서비스를 이용하게 될 장소를 공유한다. 모바일 금융 서비스를 이용하는 장소는 일정 하지 않으므로 사용 가능 지역을 적절한 곳에 지정한다. 서비스 가용 구역을 정하는 것은 정책적인 의미가 포함되므로 추가적인 토의가 필요하다.

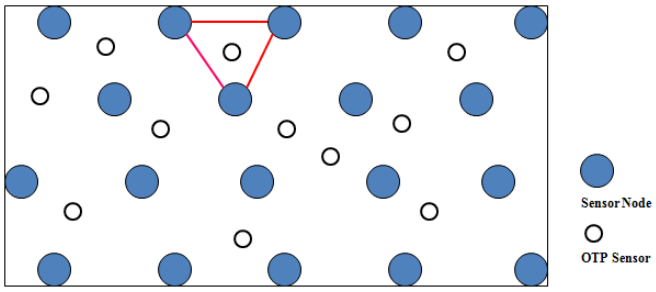

그림 2. 센서 노드와 OTP 위치

그림 2에서 센서 노드들은 지정된 곳에 위치한다. 밑줄이 그려진 삼각형 부분은 OTP 단말기가 위치한 장소이다. 사용자가 OTP를 생성할 경우 그림과 같이 OTP의 인접 지역에 위치한 센서 노드를 통하여 삼각형의 구역이 설정된다.[6] 센서 노드는 센서 네트워크의 게이트웨이에 위치 좌표가 저장된다. 만약 삼각형 지역이 미리 지정한 위치이고 이곳에서 모바일 서비스를 이용한다면, OTP 생성을 위한 첫 번째 채널이 형성된다.

OTP 단말기의 위치는 정확한 위치를 알아내기 위해 삼변측량을 사용한다. 센서 노드들은 자신의 좌표를 가지고 있으며, 주기적으로 다른 센서 노드들과 정보를 교환한다. OTP 센서는 모바일 단말기에 부착되어 있으며 센서 노드와 전파를 통하여 센서 노드의 단말기 간 거리를 구할 수 있다.[7]

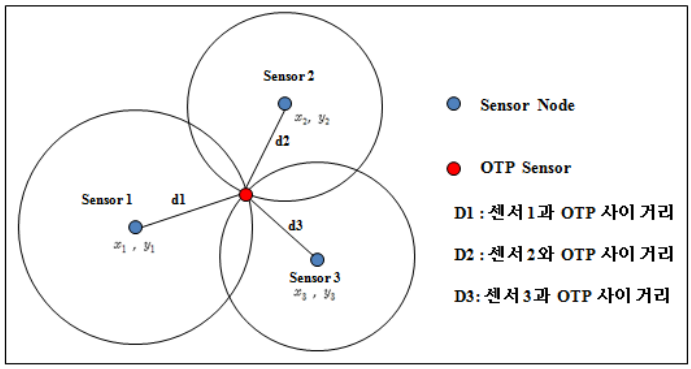

그림 3. OTP 알고리즘을 위한 구조도

단순한 위치 좌표 값을 OTP로 생성하게 되면 역 공학에 의해 추적이 가능하다. 따라서, 각 단말기들의 위치 좌표 값을 통하여 간단한 연산을 수행 한 후, 의미 있는 값들을 조합하여 OTP를 생성한다.

그림 3은 센서 노드와 OTP 센서들의 직경과 좌표 값이 나타나 있다. x_1 , x_2, x_3 과 y_1 , y_2 , y_3은 그림 3에서 삼각형을 이루는 센서 노드들의 좌표 값이다. 각 직경 중 가장 짧은 값으로 비밀 키 생성을 위한 첫 번째 암호 키로 사용한다. 각 센서 노드들의 좌표 값의 평균값을 만들어서 남은 암호화키를 생성한다. $x_s = (x_1 + x_2 + x_3)/3$ 과 $y_s = (y_1 + y_2 + y_3)/3$ 연산을 수행하여 평균 값 x_s 와 y_s을 생성한다. 두 값은 OTP를 위한 나머지 난수가 된다. $\{d_i , x_s, y_s\}$을 순차적으로 배열하여 암호화키가 생성된다. 하지만 위치 좌표와 사용자 지정 위치가 차이가 난다면 오차가 발생할 수 있다. 오차를 줄이기 위해 인식 거리 단위를 넓게 잡는다면 비슷한 위치에 OTP가 동일하게 생성이 될 수 있다. 따라서, 동일한 OTP 생성을 막기 위해 최종적으로 만들어진 암호 키에 단말기의 고유번호를 혼합한다. 위치 기반 OTP는 MITM이나 재사용 공격을 통하여 패스워드가 노출되었어도, 다른 위치에서 서비스를 이용 한다면 한번 발행된 OTP는 사용할 수 없게 된다. 외부로부터 공격을 당하는 것은 쉽지 않으며, 무결성과 기밀성, 가용성을 모두 만족하는 메커니즘이다.

4. 결론

본 논문은 기존 OTP 동기화 방식으로 사용되는 시각 동기화 방식, 이벤트 동기화 방식, 질의/응답 방식의 문제점을 보완한 모바일 단말기에 적합한 위치기반 OTP 생성 메커니즘을 제안하였다. 위치기반과 OTP를 주요 주제로 연구한 이유는 국내 금융보안의 기술적인 문제를 극복하기 위함이다.

USN을 이용한 위치 기반 OTP 생성 메커니즘은 금융보안과 센서 네트워크의 기술적 융합으로 국내 학회에서는 연구가 이루어지지 않은 분야이다. 정부의 U-City 사업과 관련해서 USN은 전국적으로 확대되어 교통, 유통, 환경 등 다양하게 응용되고 있지만 U-금융의 활용도는 기대에 미치지 못하고 연구가 미흡한 실정이다. 이에 기존 금융보안 기술과는 다른 새로운 접근 방법을 시도하여 OTP 메커니즘을 연구하였다. 향후 연구 방향으로 위치기반 OTP 메커니즘과 기존 동기화 방식 OTP 메커니즘의 결합 시도와 실험 평가를 연구할 계획이다.

참고문헌

[1] Oppliger R, Rytz R, Holdereger, T, "Internet Banking : Client-Side Attacks and Protection Mechanisms" IEEE Computer Society , 2009

[2] 최동현, 김승주, 원동호, "일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향", 성균관대학교 정보통신공학구 정보보호연구소 2007, 6

[3] 금융보안연구원 "모바일 OTP 보안 분석서 v2.0" 2011

[4] 한국정보통신기술협회 , "일회용 패스워드(OTP) 토큰 보안 요구 사항" TTAK.KO-12.0103, 2010

[5] 한국정보통신기술협회 , "일회용 패스워드(OTP) 인증 서비스를 위한 보증 레벨" TTAK.KO-12.0120

[6] Baoli Zhang, Fengqi Yu, "An Event-triggered Localization Algorithm for Mobile Wireless Sensor Networks" IEEE International Conference on Future Computer and Communication, 2010

[7] 김선관, 김태훈, 탁성우 "다중 무선센서 네트워크 환경에서 삼변측량 기법을 이용한 위치인식 방법들에 대한 비교평가", 2010