Smart App의 OTP를 이용한 컴퓨터 이중 잠금1)

김민지, 이덕규
서원대학교 정보보안학과
mj_0116@naver.com, deokgyulee@seowon.ac.kr

Double Locking a Computer using OTP from the Smart App

Min Ji Kim, Deok Gyu Lee
Dept of Information Security, Seowon University

요 약

기존의 컴퓨터 잠금에서는 비밀번호만 알게 되면 누구나 쉽게 컴퓨터를 사용할 수 있다는 보안 취약점이 있었다. 본 연구는 이를 보완하기 위해 OTP(One Time Password)를 이용한 컴퓨터 이중 잠금을 구현하였다. 어플리케이션과 클라이언트, 서버를 각각 개발한 후 서버와 어플리케이션 간 30초마다 생성되는 OTP의 생성 알고리즘을 연동시켜 놓았다. 클라이언트에서 잠금 화면이 출력되면 설정되어있던 비밀번호를 치고, 이후 OTP 입력창이 출력되면 OTP 어플리케이션을 확인하여 OTP 코드를 입력한다. 이러한 이중 잠금 방식은 해킹의 위험을 막을 수 있으며 안전성을 보장받을 수 있다.

1. 서론

제 4차 산업혁명으로 불리고 있는 현재 사회는 전자기기 없이는 생활하기 어려울 정도가 되었다. 전자기기의 사용도가 높아짐에 따라 해킹의 사례도 늘어나고 있기 때문에 보안의 중요성은 날이 갈수록 높아지고 있다. 그러나 컴퓨터 잠금 화면의 사용자 인증 방식은 비밀번호와 같은 단순한 인증 정보를 활용하기 때문에 보안에 취약하다는 문제를 가지고 있다. 사용자가 비밀번호를 외우기 쉬운 정보로 설정하거나, 고정된 비밀번호를 사용하기 때문에 공격자에 의해서 쉽게 추측될 수 있기 때문이다.[1] 따라서 기존 컴퓨터 잠금 방식에 OTP(One Time Password)를 접목시킨 이중 잠금으로 보안성을 높이는 방식을 생각하게 되었다. OTP(One Time Password)란 일회성으로 사용하는 비밀번호이다. 한 번 사용하고 난 OTP 코드는 재사용되지 않기 때문에 주로 높은 보안이 요구되는 은행에서 사용되고 있다[2]. OTP의 생성 방식으로는 질의-응답 방식과 시간 동기화 방식, 이벤트 동기화 방식, 조합 방식이 있다. 질의-응답(Challenge Response) 방식은 OTP 토큰과 OTP 인증 서버 간의 동기화 되는 기준 값이 없어, 인증 요청 시 사용자가 직접 임의의 난수 값을 OTP 토큰에 입력하여 OTP값을 생성하는 방식이다. 시간 동기화(Time-Synchronous) 방식은 OTP 토큰과 OTP 인증서버 간에 동기화된 시간 정보를 기준으로 특정 시간 간격마다 변하는 OTP를 생성하는 방식이다. 이벤트 동기화(Event-Synchronous) 방식은 OTP 토큰과 OTP 인증서버 간의 동기화된 인증 횟수(Counter) 값을 기준으로 사용자가 인증을 요청할 때마다 비밀번호를 생성하는 방식이다. 조합(Time Event Synchronous) 방식은 시간동기화와 이벤트 동기화 방식의 장점을 조합하여 구성한 OTP 생성 방식으로, 특정 시간 간격마다 비밀번호가 생성되며, 같은 시간 내에서 OTP 생성 요청이 다시 발생하면 인증 횟수를 증가시켜 새로운 비밀번호를 생성한다.[3] OTP는 인증 방식에 따라 OTP 토큰과 인증 서버 간의 암호 알고리즘과 시간정보, 인증횟수, Seed 값 등의 비밀정보를 동기화하고 해시 함수를 이용해 일회용 패스워드를 생성하기 때문에 재전송 공격에 안전하여 NIST(National Institute of Standards and Technology)에서 안전성이 높은 인증수단으로 가이드하고 있다.[4]

2. 기존방식 분석

기존의 OTP의 생성 매체인 전용 하드웨어 OTP 토큰은 OTP 자체를 생성할 수 있는 연산 기능, 암호 알고리즘 등이 내장되어 있다. OTP 생성 기능만을 지닌 전용 토큰이므로 추가 장비 필요 없이 사용이 가능하며 시스템 적용에 용이하다. 하지만 기존의 전용 하드웨어 OTP 토큰의 사용은 사용자가 별도로 단말기를 구입해야 하므로 구입비용에 대한 부담과 휴대하고 있어야 한다는 불편함이 있었다.[5]

1) 본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2019-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발)

(그림1) OTP단말기

또한 은행의 OTP 단말기는 통합되어 있는 경우가 많기 때문에 분실하게 될 경우 다방면의 위험이 존재했다. 만약 OTP 토큰을 분실 또는 도난당한다면 OTP 토큰을 취득한 사람은 OTP 토큰의 주인과 같은 OTP를 생성 할 수 있게 된다. 서버 측에서는 이 OTP가 인증자와 같은 것으로 인증이 되기 때문에 이는 곧 커다란 문제로 이어진다.[6]이러한 단점을 보완한 것이 바로 스마트 OTP 어플리케이션이다. 모바일 OTP는 OTP 생성 알고리즘이 소프트웨어 모듈로 휴대폰에 탑재된 형태로서, 별도의 OTP 기기를 구매하여 휴대하고 다닐 필요가 없다는 장점이 있다.[7] 또한 OTP 어플리케이션이 설치되어 있는 스마트 기기를 분실했다고 하더라도 백업과 복구가 간편하기 때문에 기존의 OTP 토큰보다 더 효율적이다.

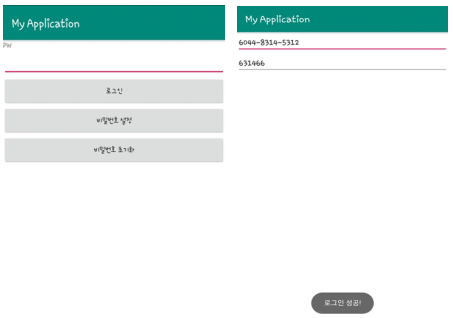
3. 제안방식

3.1. 이중 잠금에 대한 시스템

본 연구에서 사용된 OTP 생성 방식은 동기화 방식 중에서도 시간 동기화 방식이다. 30초마다 OTP 코드 값이 바뀔 수 있도록 설계를 하였으며, 시간 오차를 막기 위해 OTP의 생성 알고리즘을 OTP 어플과 서버 간에 연동시켜놓았다. OTP를 이용한 컴퓨터 이중 잠금 방식을 처음 실행하기에 앞서 사용자는 우선 사용자 등록을 해야 한다. 따라서 클라이언트를 처음 실행할 때 사용자 등록을 위한 일련번호 입력창이 나온다.

(그림2) 클라이언트 - 일련번호 입력창

사용자는 서버와 연동되어 있는 모바일 OTP 어플을 자신의 스마트 기기에 설치한 후 비밀번호를 설정한다. 설정한 비밀번호로 OTP 어플에 로그인할 경우, 일련번호 12자리와 OTP코드 6자리 값이 화면에 출력된다. 일련번호는 그 사람의 식별번호이기 때문에 다른 비밀번호로 로그인 시 다른 일련번호가 매칭이 된다. 사용자는 어플에서 비밀번호 설정 시 자동으로 생성되었던 자신의 일련번호를 확인한 후, 클라이언트의 일련번호 입력창에 입력하면 서버는 이를 해당 PC의 식별정보와 함께 파일로 저장해둔다. 따라서 이미 사용자 등록으로 일련번호를 입력해둔 PC에서는 다시 일련번호 입력창이 뜨지 않는다.



(그림3) OTP어플 - 일련번호와 OTP코드 창

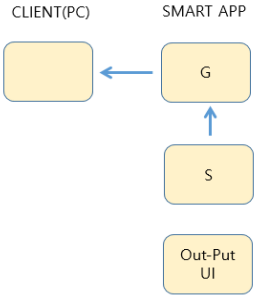
OTP 어플의 일련번호로 첫 등록을 하고 난 이후부터는 클라이언트 실행 시 바로 OTP 입력창이 뜨게 된다. OTP 어플 로그인 시 출력되는 OTP 코드 6자리 값을 클라이언트의 OTP 입력창에 입력하면 서버의 OTP 코드와 비교 후 동일한 OTP 코드로 판단 시 로그인에 성공하여 잠금이 풀리는 방식이다. OTP 코드는 30초마다 갱신되기 때문에 만약 클라이언트의 OTP 입력창에 코드를 입력 후 로그인 실패가 뜨게 되면 다시 어플의 OTP 코드를 재확인 후 입력해야 성공하게 된다.

(그림4) 클라이언트 - OTP코드 입력과 로그인 성공

3.2. OTP 코드 값 생성과 비교

본 연구에서 사용된 OTP 코드 값의 생성 방식은 사용자의 일련번호와 현재 시각을 각각 해시 값에 넣고 XOR 해서 시드(seed) 값으로 추출한다. OTP 코드 값은 30초마다 갱신되기 때문에 현재 시간이 30초 이상이면 비트를 반전시키는 방식을 사용하였다. 이렇게 구한 시드 값을 다시 해쉬한 다음 앞에서부터 48비트인 6자리만 추출한 후 10으로 나누어 OTP코드 값을 출력시켰다. OTP 코드 값 생성 방식은 어플과 서버를 동기화 시켰기 때문에 동일한 OTP 코드 값이 출력 된다. 본 연구에서 구현한 컴퓨터 이중 잠금 시스템의 동작 순서를 살펴보면 (그림5)와 같다. 우선 모바일 OTP 어플에서 S(시드값)으로 G(키 생성기)를 거쳐 OTP 코드 값이 생성되며, UI를 통해 화면에

출력이 된다. 사용자는 모바일 OTP 어플에 출력된 OTP 코드 값을 클라이언트의 OTP 입력창에 입력하고, 서버에서 생성된 OTP 코드와 사용자가 입력한 OTP 코드가 동일한 값인지 서버에서 비교 후 동일한 값일 경우 로그인에 성공한다.



(그림5) 시스템 동작 순서

4. 분석

OTP는 패스워드가 노출이 되더라도 스니핑이나 재연 공격을 방지할 수 있으며 서버에는 패스워드가 저장되지 않아 안전하다는 장점이 있다.[8] 하지만 OTP를 이용한 컴퓨터 이중 잠금 시스템을 공격자가 사용하게 된다면 무작위 대입 공격을 예상해볼 수가 있다. 따라서 공격자가 OTP 입력을 5회 이상 시도할 경우 무작위 대입 공격을 막기 위해 로그인이 차단되도록 구현하였다. 로그인이 차단된 상태에서는 Alt+F4를 통한 강제종료가 불가능하며, 작업관리자에서도 해당 시스템이 표시되지 않기 때문에 각종 시스템 공격으로부터 컴퓨터를 안전하게 사용 할 수 있다.

(그림6) 로그인 차단 화면

5. 결론

컴퓨터의 사용자가 증가할수록, 해킹의 사례도 증가하고 있다. 해킹을 막기 위한 다양한 방법들이 존재하지만 본 연구에서는 OTP 기반의 컴퓨터 이중 잠금을 이용해 보안이 한층 강화된 시스템을 구현하는 것에 성공하였다. 기존의 컴퓨터 잠금 화면 인증 방식인 PASSWORD 대신 OTP를 사용하게 되면 예측 불가능성, 재현 불가능성, 무작위성의 성질을 가지기 때문에 공격자로부터 해킹 위험성이 낮아 보안성이 뛰어나다는 장점을 갖고 있다. 또한 패스워드와 같은 인증 수단에 비해 OTP는 사전 공격이나 무차별 대입 공격 등에 대해 비교적 안전하고, 더 나아가 실제 시스템에 적용하게 될 경우 훨씬 뛰어난 보안성의 향상을 기대해 볼 수 있다. 본 연구에서 구현한 스마트 어플의 OTP를 활용한 컴퓨터 이중 잠금 방식은 기존에 찾아볼 수 없었던 새로운 컴퓨터 잠금 방식이며 많은 PC 사용자들이 해킹으로부터 안심하고 컴퓨터를 사용할 수 있을 것이다.

참고문헌

[1] 최동현 · 김승주 · 원동호, “일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향”, 한국정보보호학회지 v.17 no.3, pp12, 2007

[2] “일회용 비밀번호”, 『위키백과』 https://ko.wikipedia.org

[3] 정규환, “웹세션 환경에서 OTP를 이용한 사용자 인증 시스템의 설계“, 숭실대학교 정보과학대학원 정보보안학과 학위논문(석사), pp6-9, 2010

[4] 전진오, “웹 환경에서 세션 토큰을 이용한 OTP 인증”, 충북대학교 일반대학원 컴퓨터공학과 컴퓨터공학전공 학위논문(석사), pp5, 2018

[5] 김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 한국정보보호학회지 v.17 no.3, pp28, 2007

[6] 최종석 · 정민경 · 신승수, “모바일 기기를 이용한 OTP 인증”, 한국산학기술학회 추계 학술발표논문집, pp18, 2008

[7] 정윤수 · 한상호 · 신승수, “모바일 OTP 생성 모델에 관한 연구”, 디지털정책연구 v.10 no.2, pp185, 2012

[8] 신승수 · 한군희, “효율적인 OTP 기반의 인증 프로토콜”, 한국산학기술학회논문지 v.11 no.4, pp1305, 2010