사용자 컴퓨터 환경에서 OTP를 활용한 컴퓨터 이중 잠금1)

신 선 경, 이 덕 규
서원대학교 정보보안학과

alsl9387@naver.com, deokgyulee@seowon.ac.kr

Double Lock up Computers Using OTP in User Computer Environment

Sun-Kyung,Shin, Deok Gyu Lee

Dept of Information Security Seo-won University

요 약

사용자의 PC에 대한 보안 중, PC를 사용하는 자가 본인이 맞는지에 대한 인증에 주목한다.
기존에 패스워드로만 이뤄졌던 사용자 계정 보안에 OTP(One-Time Password)를 접목 하는 프로젝트 설계 및 구현을 제안하고자 한다. 최근 인터넷과 같은 통신 기술 능력이 급속도로 발전함에 따라 많은 비즈니스들이 온라인을 통해서 이루어지고 있다. 이러한 환경에서 사용자 인증은 안전한 인터넷 사용을 위한 필수적인 요소이다. 따라서 일회용 패스워드의 기술과 필요성을 소개함으로 사용자 컴퓨터 환경에서 OTP를 활용한 컴퓨터 이중 잠금을 소개하고자 한다.

1. 서론

최근 인터넷과 같은 통신 기술 및 컴퓨터 계산 능력이 급속도로 발전함에 따라 많은 비즈니스들이 온라인을 통해서 이루어지고 있다. 이에 따라 지식 및 정보 등 다양한 분야에 있어 누구나 많은 혜택을 누릴 수 있게 되었다. 그러나 인터넷은 개방형 네트워크이기 때문에 공격자에 의한 시스템 침입, 도청 등과 같은 여러 가지 공격에 취약하다. 특히 기존에 오프라인 상에서 이루어지던 은행 거래와 상거래가 인터넷 뱅킹과 전자상거래와 같이 온라인상에서 이루어짐에 따라 전송되는 정보의 중요도가 높아지고 있으며, 만약 공격이 발생할 경우 그 피해수준 역시 높아지고 있다. 이러한 환경에서 사용자 인증은 안전한 인터넷 사용을 위한 필수적인 요소라고 할 수 있다. 사용자 인증이란, 어떤 사용자가 실제로 정당한 사용자인지를 판단하는 과정으로, 대표적인 방식으로 ID/Password가 있다. 하지만, ID/Password 인증방식은 password와 같은 단순한 인증 정보를 활용하기 때문에 네트워크 환경에서 커다란 문제점을 가지고 있다. 사용자가 아이디와 비밀번호를 외우기 쉬운 정보로 설정하거나, 고정된 비밀번호를 사용하기 때문에 공격자에 의해서 쉽게 추측될 수 있는 문제점이 있다. 또한 도청에 의해 쉽게 노출될 가능성이 높기 때문에 악의적인 공격자가 이를 이용하여 정당한 사용자로 위장할 수 있다.이러한 단점을 극복할 수 있는 인증기법이 매번 새로운 패스워드를 생성하는 일회용 패스워드 기술을 활용한 인증 방법이다. 이러한 일회용 패스워드는 국내에서 주로 인터넷 뱅킹에서 사용되어 왔으며, 최근에는 온라인 게임에 접속하거나 게임 아이템, 음악, 동영상을 구매할 경우에도 사용되고 있다. 이처럼 일회용 패스워드에 대한 수요가 늘어나고 있으며, 보다 다양한 분야에서 사용되고 있다. 따라서 이 프로젝트도 시대에 걸 맞춰 기존의 패스워드로만 이루어졌던 컴퓨터 보안에 OTP를 접목시킨 이중 보안을 통한 안정성 향상을 목표로 두고 연구하게 되었다.

2. OTP기술

사용자를 인증하는 방법에는 크게 세 가지가 있다. 첫째는 사용자가 알고 있는 것을 이용해서 인증하는 방법으로서 사용자가 특정 정보를 알고 있는지를 검증하는 방식이다. 대표적인 예로는 ID/Password 방식이 있다. 두 번째는 사용자의 특징을 이용해서 인증하는 방법으로 사용자가 가지는 지문, DNA 등을 검증하는 방식이다. 마지막으로 사용자가 ID카드, H/W토큰, S/W토큰 등을 소유하고 있는지를 검증하는 인증 방식이 있다. OTP는 이러한 세 가지 방법 중 마지막인 사용자가 가지고 있는 것을 이용한 인증방법으로 사용자가 인증을 받고자 할 때 매번 새로운 패스워드를 생성해주는 방식이다.

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)

2.1. OTP 기술의 필요성

해킹 기술의 다변화, 고도화 및 대중화로 ID/Password 인증방식의 안정성이 저하되고 있다. 이를 반영하듯, 피싱, 서버 해킹 및 악성 코드를 이용한 ID/Password 유출, 인터넷 뱅킹 해킹을 통한불법 인출 사건 및 온라인 게임 해킹을 통한 개인정보유출과 같은 피해 사례가 급증하고 있다. 또한 패스워드의 형태별 해독 시간이 짧기 때문에 인증방식으로 사용하기에는 매우 취약하다. 이러한 취약점을 보완하고자 password의 자리 수 제한, 특수 문자 사용 또는 주기적인 교체권고 등의 방법이 제안되고 있지만 이는 근본적인 해결책이 될 수 없다. 이러한 ID/Password 방식의 한계를 극복하기 위해서는 비밀번호의 개수를 굉장히 많이 늘리거나 매번 바뀌는 비밀번호를 생성해야한다. 여기서, 매번 바뀌는 비밀번호를 생성하는 방법이 OTP 기술이다.

3. 제안방식

1장에도 말했듯이, 인터넷이 발달하면서 다양한 네트워크 해킹 기법이 등장하고 있고, 그것을 방어하기 위한 보안 기술 또한 비약적인 발전을 이루었다. 하지만 네트워크상의 보안이 아무리 잘 이루어지더라도, 네트워크 통신의 시작과 끝에 위치한 PC의 보안이 제대로 이루어지지 않는다면 그것을 이용해 전달되는 데이터는 결코 안전하다고 할 수 없을 것이다. 사용자의 PC에 대한 보안 중, PC를 사용하는 자가 본인이 맞는지에 대한 인증에 주목하여 기존에 패스워드로만 이루어졌던 사용자 계정 보안에 OTP를 접목하는 연구를 기획하였다. 사용자가 본인의 스마트폰을 이용해 PC에 사용자 본인임을 인증하고, 인증 실패 시 접근이 제한되도록 하는 것을 목표로 한다. 이에 따라 사용자의 스마트폰과 OTP를 이용하여 사용자를 인증하고 PC에 대한 접근을 허가하도록 하는 방안을 제안한다.

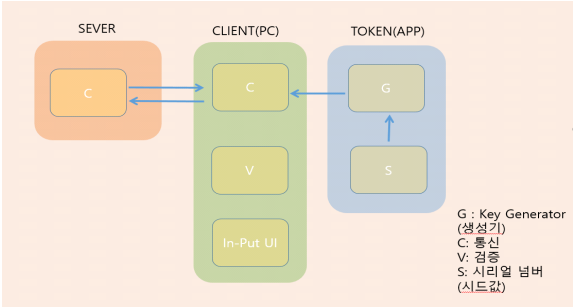
3.1.OTP 기술을 접목시킨 컴퓨터 보안

3.1.1 최초인증

처음 사용 시 사용자는 자신의 스마트폰에 OTP 어플리케이션을 실행하고, OTP 어플리케이션에 표시되는 일련번호와 자신의 비밀번호를 클라이언트 프로그램을 통해 서버에 전송한다.

3.1.2 OTP인증

최초인증이 완료되면, 사용자는 이후 PC를 사용하기 위해 서버에 OTP를 이용한 인증을 요청 할 수 있다.

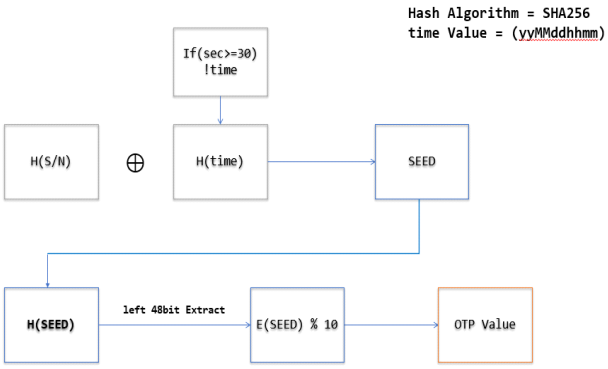


<그림 1> 제안방식 흐름도

3.2. 구현

APP과 서버는 SEED 값에서 랜덤으로 30초씩 동일한 NUMBER를 생성하고 있다. 사용자가 로그인을 할 때 앱에서 시리얼 넘버를 키 생성기에게 넘겨준다. 그리고 APP의 키 생성기가 PC 클라이언트에게 넘버값을 전해준다. 그리고 나서 클라이언트 통신은 1차 검증을 한 다음 서버 통신에게 암호화한 넘버값을 전송해주고, 넘버 값을 전송받은 서버는 토큰에서 키 생성기가 처음에 전송해준 넘버값과 기존에 서버에서 생성된 넘버값을 같은 값인지 검증해준다. 그 후 그 검증 값을 클라이언트에게 전해준다.

3.2.1 알고리즘



<그림 2> OTP 알고리즘

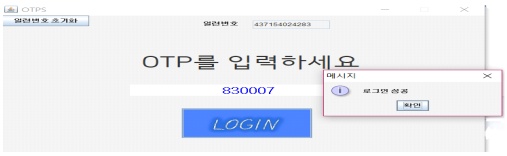
S/N: 일련번호
time: 현재시간(yyMMddhhmm)

먼저, 클라이언트의 S/N과 time을 불러와 각각 해시하여 256비트로 추출한다. 이 때, second가 30이상이면 time을 비트 반전하여 해시한다. 그리고 H(S/N)과 H(time)을 XOR하여 256비트의 SEED값을 구하고, SEED를 다시 해시하여 256비트의 H(SEED)를 구한 후 첫 48비트를 추출하여 E(SEED) 값을 구한다. 이렇게 구해진 E(SEED)를 10진수로 변환하기 위해 10으로 나눈 나머지 값을 구해 6자리의 OTP값을 생성하게 된다.

3.3. Client PC

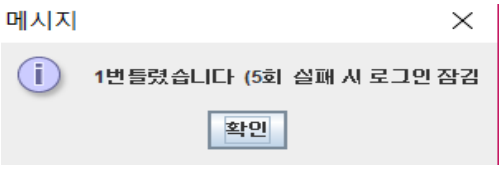
<그림 3> OTP창 활성화

APP이 로그인 시도를 하면 위 사진처럼 OTP 입력창이 활성화 된다. 클라이언트는 일련번호와 OTP 코드 입력창을 출력하고 OTP입력 값을 서버에게 전송한다. 또한 악의적인 공격을 대비해 사용자 본인임을 명확히 구분하기 위해 OTP코드 입력을 5회로 제한한다.



<그림 4> 로그인 성공창

일련번호와 올바른 OTP 코드를 입력할 시 로그인에 성공하게 되며, 만약 5회 로그인에 실패할 경우에는 무작위 대입 공격을 막기 위해 로그인이 차단되도록 구현 하였다.



<그림 5> 로그인 실패 시 창

4. 분석

4.1 취약점 분석

서버와 OTP 어플리케이션 간 시간 오차가 발생 할 경우 OTP 값이 달라질 수 있다. 따라서 서버에서 OTP 값을 두 개 생성한 후 클라이언트 프로그램에게 전달하여, 프로그램에서 서버와 OTP 어플리케이션 간 OTP값이 불일치 할 경우 서버로부터 전달받은 2번째 OTP값으로 재차 비교하는 방안을 고려해 볼 수 있다.

4.2 해결방안

OTP 전송 패킷을 가로채는 스니핑 공격이 발생 할 수 있기 때문에 서버와 이용자 간에 전송 되는 모든 패킷을 암호화함으로써 스니핑 공격을 예방 할 수 있다. OTP를 이용하는 인증 사이클은 기존 패스워드 등의 인증 수단에 비해 사전공격이나 무차별 대입 공격 등에 대해 비교적 안전하므로 실제로 시스템에 적용할 경우 보안성 향상을 기대 할 수 있다.

5. 결론

즉시 생성된 OTP코드를 비밀번호로 이용하므로 망각의 문제는 발생하지 않는다.

OTP는 ID/Password 인증방법을 대체하며 여러 분야로 사용이 확대되고 있다. 따라서 기존의 패스워드로만 이루어졌던 컴퓨터 보안에 OTP를 접목시킨 이중 보안을 통한 안정성 향상을 목표로 두고 비밀번호 노출 또는 망각의 문제를 해결하여 보안성을 강화 하였다.

본 논문에서 스마트폰 OTP 어플리케이션을 활용한 컴퓨터 이중 잠금에 대해서 서술 하였다.

참고문헌

[1] 최동현, 김승주, 원동호 (2007). “일회용 패스워드 기술 분석 및 표준화 동향”, 정보처리학회 논문지, 17(3), pp 12-17

[2] 황형진, 김권양, 하일규 (2017). “시간 동기 방식의 OTP를 이용한 디지털 도어락 시스템”. 한국정보통신학회 논문지. 21(5),1027-1034

[3] 숭실대학교 정보과학대학원 정 규 환 . 웹 세션 환경에서 OTP를 이용한 사용자 인증시스템 설계

[4] 최종석, 정민경, 신승수 (2008) . “모바일 기기를 이용한 OTP 인증 ”, 한국산학기술학회 추계 학술 발표 논문집

[5] 고려대학교 컴퓨터과학기술 대학원 ‘류연호‘ “OTP 개념을 이용한 사용자-인증 서버의 상호 인증 모델”

[6] 목원대학교 정보통신학과 ‘정윤수‘, 동명대학교 정보보호학과 ’한상호‘, 동명대학교 정보보호학과 ’신승수‘, “모바일 OTP 생성 모델에 관한 연구”