OTP를 이용한 PC 인증 시스템의 설계1)

신동훈*, 이덕규*
*서원대학교 정보보안학과
e-mail:dhn96@naver.com, deokgyulee@seowon.ac.kr

Design of PC authentication system using OTP

Dong-Hoon Shin*, Deok-Gyu Lee*
*Dept. of Information Security, Seowon University

요 약

인터넷 이용률이 증가하고 정보통신 기술이 발달하면서 다양한 해킹 기법과 보안 기술이 등장하고 있다. 그러나 네트워크상의 보안이 잘 이뤄지더라도 PC의 보안이 잘 이뤄지지 않는다면 그것을 이용해 전달되는 데이터는 결코 안전하다고 할 수 없다. 이 논문에서는 PC의 사용자가 본인이 맞는지에 대한 인증에 주목하여 OTP를 이용한 PC 인증 시스템을 제안한다. OTP를 이용해 사용자를 인증하는 시스템을 설계 및 구현하고, 분석하여 최종적으로 시스템의 보안성을 확인한다.

1. 서론

현대 사회에서 개인과 인터넷은 밀접한 관계를 맺고 있다. 통계청에서 발표하는 인터넷이용실태조사에 따르면 인터넷 이용률은 지속적으로 증가하고 있으며, 2018년 기준 만 3세 이상 인구의 인터넷 이용률은 91.5%에 달한다.[1]

인터넷의 이용률 증가와 함께 정보통신 기술 또한 발달해왔다. 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.

본 논문에서는 사용자의 PC에 대한 보안 중, PC를 사용하는 자가 본인이 맞는지에 대한 인증에 주목하여 기존 ID/PW로만 이루어졌던 사용자 계정 보안에 OTP(One Time Password)를 접목한 인증 시스템을 제안한다. OTP는 무작위 패스워드를 이용하는 사용자 인증 방식으로, 특정한 방식에 따라 매번 패스워드가 변경되기 때문에 정적인 ID/PW 방식에 비해 비교적 안전하다.[2]

시스템은 사용자가 본인의 스마트폰을 이용해 PC에 사용자 본인임을 인증하고, 인증 실패 시 접근이 제한되도록 하는 것을 목표로 한다.

본 논문은 총 5장으로 되어 있다. 2장에서는 관련 연구로써 OTP 생성 방식을 기술하고 각 방식의 취약점에 대해서 분석한다. 3장에서는 PC 보안에 OTP를 접목한 시스템을 제안한다. 4장에서는 제안한 시스템을 구현하고 보안성을 확인한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

이 장에서는 OTP 생성 방식에 대해 기술하고, 각 방식의 장단점과 취약점에 대해 분석한다. 사용자를 인증하는 방식에는 크게 지식기반과 소유기반, 속성기반의 세 가지가 있다.[3][7] 지식기반은 사용자가 알고 있는 것을 이용하여 인증하는 방식으로 ID/PW 방식이 이에 해당한다. 소유기반은 사용자가 가지고 있는 것을 이용하여 인증하는 방식으로 대표적으로 SMS 인증이나 보안카드 등이 있다. 속성기반은 지문인식, 홍채인식 등 사용자의 고유한 속성을 이용하여 인증하는 방식이다. 이 중 OTP는 소유기반에 해당하는 인증 방식으로, 사용자가 인증을 요청할 때마다 새로운 패스워드를 생성한다.[6]

2.1 OTP 생성 방식

OTP는 서버와 OTP 토큰 간 동기화 여부에 따라 비동기(Asynchronous) 방식과 동기화(Synchronous) 방식으로 분류된다.[4][5] 이 중 비동기 방식은 서버와 OTP 토큰 간 동기화 없이 서버가 사용자에게 질의한 값을 사용자가 OTP 토큰에 입력하여 OTP를 생성하는 방식으로, 사용자가 매 인증 시마다 질의 값을 입력해야 하는 불편함이 존재하며 서버와 클라이언트 간 통신 횟수가 비교적 많이 요구되므로 부하가 발생할 위험이 있다.[2] 따라서 동기화 방식에 비해 자주 사용되지 않으므로 본 논문에서는 동기

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)

화 방식을 중심으로 기술한다.

동기화 방식에는 시간 동기화(Time-Synchronous) 방식과 이벤트 동기화(Event-Synchronous) 방식, 시간 이벤트 조합 방식(Time+Event-Synchronous)이 있다.[7]

2.1.1 시간 동기화 방식

시간 동기화 방식은 시간을 기준으로 하여 OTP를 생성하는 방식이다. 서버와 OTP 토큰 간 시간이 동기화 되어 있다는 전제 하에 동일한 OTP 생성 알고리즘에 입력 값으로 현재 시각을 사용하여 OTP를 생성한다.[5] 서버와 클라이언트 사이에 통신이 적게 요구되며, 특히 OTP 생성에 요구되는 값을 직접 주고받는 게 아니기 때문에 비동기화 방식에 비해 네트워크 부하가 적다는 장점이 있다.[2] 그러나 서버와 토큰 간 시간 동기화가 정확하게 이루어지지 않으면 OTP 생성 값이 달라진다는 단점이 있다.[6] 이를 보완하기 위해 시간 간격을 두어 OTP를 생성하는 방식이 주로 사용된다.

2.1.2 이벤트 동기화 방식

이벤트 동기화 방식은 서버와 OTP 토큰 사이에 동기화된 인증 횟수(Counter)를 기준으로 OTP를 생성하는 방식이다. 사용자의 인증 요청이 있을 때마다 서버와 OTP 토큰에서 카운터를 증가시켜가며, 이 카운터 값을 OTP 생성 알고리즘의 입력 값으로 사용한다.[5] 서버와 토큰 사이에 시간을 동기화시킬 필요가 없지만, 사용자가 OTP 토큰을 이용해 OTP를 생성하기만 하고 인증에 사용하지 않을 경우 서버와 토큰 간 카운터 값이 일치하지 않아 OTP 값이 달라진다는 단점이 있다.[6] 이를 보완하기 위해 카운터의 오차 범위 내에서는 인증을 허용하는 방법과, OTP 값을 연속해서 받아 값이 일치하는지 검증하는 방법을 주로 사용한다.

2.1.3 조합 방식

조합 방식은 시간 동기화 방식과 이벤트 동기화 방식을 결합한 형태의 방식이다. OTP를 생성할 때 시간 값과 카운터 값을 모두 사용하며, 동일한 시간 간격 내에 인증 요청이 다시 발생하더라도 매번 다른 OTP 값을 생성하기 때문에 안전성이 뛰어나다.[5]

3. PC 이중 잠금 시스템

이 장에서는 Windows 환경의 사용자 PC에서 기존 ID/PW 방식의 잠금 시스템에 OTP 인증 방식을 더해 안전성을 보완한 시스템을 설계한다. 이 시스템에서 사용자는 PC 잠금을 해제하기 위해 OTP 생성 알고리즘이 탑재된 모바일 어플리케이션을 이용하고, 만약 인증에 실패할 경우 PC 접근이 제한된다. 이를 통해 PC 내의 개인정보를 보호하고 보안성을 향상시킨다.

시스템은 초기 설정, 사용자 식별, OTP 값 생성, 검증 및 인증 단계로 구성된다. 각 단계의 세부 사항은 다음과 같다.

3.1 초기 설정

시스템 최초 사용시 서버와 사용자는 다음과 같은 과정을 통해 동일한 OTP 값 생성을 위한 초기 설정을 진행한다.

① 사용자는 모바일 어플리케이션을 실행하여 타인의 모바일 어플리케이션 접근을 방지하기 위한 비밀번호를 설정하고, 모바일 어플리케이션에서 임의로 생성한 12자리 일련번호를 클라이언트 프로그램을 통해 서버에 전송한다.

② 서버는 일련번호를 사용자의 PC 정보와 함께 저장한다.

3.2 사용자 식별

초기 설정이 완료되면 사용자 식별을 수행한다.

① PC에 사용자의 접근 시도가 감지되면 클라이언트는 서버에 접근 시도가 감지되었음을 알린다.

② 서버는 사용자의 PC 정보를 받아 일련번호가 매핑되어 있는지 확인한다. 이 때, 일련번호가 매핑되어 있지 않다면 클라이언트에 일련번호가 매핑되어 있지 않음을 알리고 초기 설정을 다시 진행한다.

③ 일련번호가 매핑되어 있으면 서버는 클라이언트에 인증 준비가 완료되었음을 알린다.

3.3 OTP 값 생성

사용자를 식별하고 인증 준비가 완료되면 서버와 모바일 어플리케이션에서 OTP 생성 알고리즘에 따라 OTP 값을 생성한다. 이 알고리즘은 시간 동기화 방식을 사용하며, SHA-256 해시 알고리즘을 이용한다.

<표 1> 용어 정의

용 어	정 의
SN	일련번호
T	현재 시각(yyMMddmm)
H(P)	P를 SHA-256로 해시
SEED	OTP 생성을 위한 시드 값
A⊕B	A와 B의 XOR 연산
E(P)	P의 첫 48비트 추출
a mod n	a를 n으로 모듈러 연산

① 일련번호와 현재 시각을 각각 SHA-256 해시 알고리즘을 사용하여 해시한다. 이 때, 현재 시각이 30초 이상이면 현재 시각의 비트를 반전하여 해시한다.

$H(SN),\ H(T)$

② 일련번호를 해시한 값 H(SN)과 현재 시각을 해시한 값 H(T)를 XOR 연산하여 SEED를 생성한다.

$SEED = H(SN) \oplus H(T)$

③ SEED를 SHA-256 해시 알고리즘으로 해시한다.

H(SEED)

④ SEED를 해시한 값 H(SEED)의 첫 48비트를 추출한 E(SEED)에 대해 10으로 모듈러 연산을 수행한다.

OTP = E(SEED) mod 10

3.4 검증 및 인증

OTP 값을 생성한 후에는 생성한 OTP 값을 이용하여 사용자 PC에 접근을 시도한 자가 사용자 본인이 맞는지 검증하는 과정을 수행하게 된다. OTP 값 검증에 성공하면 정당한 접근으로 판단하여 접근을 허가하고, 검증에 실패하면 비인가된 접근으로 판단하여 사용자의 접근을 제한하는 조치를 취한다.

① 사용자는 모바일 어플리케이션에서 3.3 단계에 따라 생성한 OTP 값을 클라이언트를 통해 서버에 전송한다.

② 서버는 사용자가 입력한 OTP 값을 받아 서버에서 생성한 OTP 값과 일치하는지 검증한다.

③ OTP 값이 일치할 경우 접근을 허가하고, 불일치할 경우 OTP 값을 다시 질의한다. OTP 값 질의는 최대 5회 실행되며, OTP 값이 5회 불일치하면 사용자의 접근을 제한한다.

4. 시스템의 구현 및 분석

이 장에서는 개인 PC 환경의 대부분을 점유하고 있는 Windows 환경에서 안드로이드OS를 사용하는 스마트폰을 이용해 실제로 시스템을 구현해보고, 시스템의 보안성을 평가한다. 구현 환경은 로컬 네트워크로 제한하여, 인증 서버에서 MAC 주소를 이용해 각 PC를 식별하고 필요시 접근을 통제할 수 있도록 한다.

4.1 서버

서버에서는 인증을 요청하는 각 사용자를 식별하고, 인증 및 후속 조치를 실시한다. 각 사용자 PC의 식별 정보와 일련번호를 DB로 저장 및 관리하여 PC별로 다른 OTP 값을 생성하고, 인증 실패 내역을 기록할 수 있도록 한다.

클라이언트로부터 전송받은 OTP 값의 검증을 서버에서 담당하며, 이 때 OTP 생명 주기가 거의 다했을 때 인증을 요청받았을 경우 서버에서 생성한 OTP 값과 사용자가 모바일 어플리케이션을 이용해 클라이언트에 입력한 OTP 값 사이에 오차가 발생할 수 있다. 이를 보완하기 위해 검증 최초 실패 시에는 OTP 값을 다시 입력받고, 인증 실패로 카운트하지 않는다.

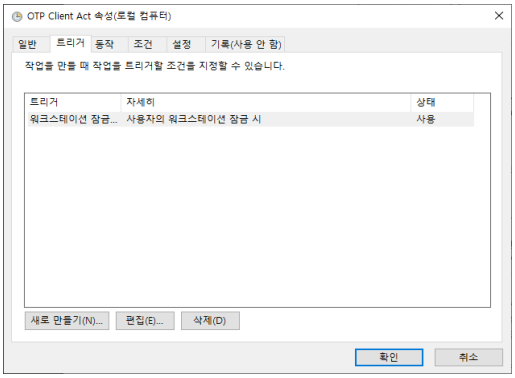
이외에 서버에서 DB에 저장된 PC 정보와 OTP 생성 알고리즘을 탈취당한다면 동일한 OTP 값을 생성할 수 있다는 단점이 존재하며, MITM(Man In The Middle) 공격에 의해 검증 과정을 우회할 수 있다는 취약점 역시 존재한다.

4.2 클라이언트

클라이언트는 사용자가 PC에 로그인할 때 처음 실행되며, 이후 윈도우 잠금이 해제될 때마다 실행되어 사용자 본인이 맞는지에 대한 인증을 수행하게 된다. 사용자는 작업 중 자리를 비울 때 윈도우를 잠금으로써 타인에 의한 의도치 않은 접근을 제한할 수 있다.

윈도우 환경에서 윈도우 잠금이 해제될 때마다 클라이언트가 실행되도록 구현하기 위해 윈도우에서 제공하는 작업 스케줄러를 사용한다. 그림 1과 같이 작업 스케줄러를 이용해 윈도우 잠금이 해제되면 클라이언트가 실행되도록 설정할 수 있다.

또한 클라이언트가 실행되는 중에는 클라이언트의 정상적인 동작을 방해하는 어떠한 키 입력도 있어서는 아니된다. 이를 방지하기 위해 클라이언트가 실행되는 중에는 동작에 방해를 줄 수 있는 커맨드 키 입력을 무시하도록 구현하였다.



<그림 1> 작업 스케줄러를 이용한 설정

4.3 모바일 어플리케이션

모바일 어플리케이션에서는 서버와 동일한 알고리즘을 사용하여 30초마다 변하는 OTP 값을 생성한다. 그러나 타인이 모바일 어플리케이션을 실행하여 OTP 값을 확인할 수 있다는 취약점이 존재한다.

이를 방지하기 위하여 모바일 어플리케이션 최초 실행 시 패스워드 설정 및 지문을 등록하고, 이후 실행 시마다 패스워드 혹은 지문을 이용해 어플리케이션에 로그인하도록 설정함으로써 사용자 본인만이 OTP 값을 확인할 수 있도록 한다.

4.4 분석

구현한 시스템은 PC를 사용하는 자가 본인이 맞는지에 대해 인증하려는 것을 목적으로 하였다. OTP는 사용자 본인만이 소유할 수 있으므로, OTP를 이용한 PC 인증 시스템은 PC를 이용하려는 사람이 사용자 본인임을 입증하는데 효과적이라 볼 수 있다. 또한 로컬 네트워크 내에서 시스템을 구성한다면 각 PC 이용자가 본인이 아니라고 판단될 경우 서버에서 PC 사용을 제한할 수 있어 보안적인 측면에서 효율적이다.

다만 OTP는 소유기반의 인증 방식이므로 사용자가 OTP를 분실하거나 탈취당한다면 보안성이 급격히 낮아질 위험이 있다. 따라서 사용자의 OTP 관리가 무엇보다도

중요하다.

5. 결론

본 논문에서는 위와 같이 OTP를 이용한 사용자 인증 시스템을 제안하고, Windows 환경에서의 구현을 통해 보안성을 확인하고 시스템에 대해 분석하였다. 지식기반의 ID/PW 방식에 소유기반의 OTP 방식을 결합한 인증 시스템은 기존 시스템에 비해 보안성 향상을 기대할 수 있다.

향후 과제로는 MITM 공격에 대비한 OTP 인증 모델의 연구가 이루어져야 할 것이다. 또한 OTP 인증 시간 내에 OTP 값을 입력하지 못해 인증에 실패할 경우의 보완점에 대한 개선 연구가 필요하다.

참고문헌

[1] 통계청 “인터넷이용실태조사”

[2] 김기영 “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”

[3] 신승수, 한군희 “OTP를 이용한 HMAC 기반의 3-Factor 인증”

[4] 신승수, 정윤수 “MAC Address와 OTP를 이용한 비인가 접근 거부 시스템”

[5] 김태형 “피싱방지 및 가용성개선을 위한 PKI기반의 모바일OTP 메커니즘 연구”

[6] 최동현, 김승주, 원동호 “일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향”

[7] 정윤수, 한상호, 신승수 “모바일 OTP 생성 모델에 관한 연구”