韓國 컴퓨터情報學會 2006동계학술발표논문집&학회지
第14卷 第2號, 2006. 12.

Tokenless OTP를 활용한 인증 모델

김 기 환*, 박 대 우*

The Authentication Model which Utilized Tokenless OTP

Ki-Hwan Kim*, Dea-Woo Park*

요 약

유비쿼터스 컴퓨팅 시대의 업무를 위하여 인터넷을 통한 원격 접속이 필요하고, 입력되는 ID와 패스워드에 대한 기밀성, 무결성의 네트워크 보안을 위하여 OTP를 적용하고 있다. 현재의 OTP는 Token이라는 하드웨어를 보유하고 있어야 하며, 보안에서도 취약점이 있다. 본 논문에서는 OTP 네트워크에 스니핑 도구를 설치하고, Cain을 이용하여 ARP Cache poisoning 공격을 시행하여 사용자 암호에 대하여 스니핑으로 취약점을 확인한다. 새로운 보안 방안으로 Tokenless OTP를 적용할 수 있는 새로운 시스템을 제안하고, 기밀성과 무결성을 보장하고자 한다. 외부에서 원격 접속 시 Tokenless OTP를 활용하여 접근제어를 위한 테스트를 하고, 접속에서 인증시스템과 연동하여 접속제어를 할 수 있었다. 만약 인증과정에서 해킹을 당해도 사용자만이 알고 있는 핀 번호 없이는 접속이 불가능 하다는 것이 확인되었다. 이 결과 Tokenless OTP를 적용할 시에 패스워드의 유출 및 오용과 해킹에 대한 방어가 되어 보안성을 강화하고, 안전성을 높이는 보안 시스템으로 평가 되었다.

Abstract

Is need Remote Access through internet for business of Ubiquitous Computing age, and apply OTP for confidentiality about inputed ID and Password, network security of integrity. Current OTP must be possessing hardware of Token, and there is limitation in security. Install a Snooping tool to OTP network in this treatise, and because using Cain, enforce ARP Cache poisoning attack and confirm limitation by Snooping about user password .Wish to propose new system that can apply Tokenless OTP by new security way, and secure confidentiality and integrity.Do test for access control inflecting Tokenless OTP at Remote Access from outside, and could worm and do interface control with certification system in hundred. Even if encounter hacking at certification process, thing that connection is impossible without pin number that only user knows confirmed. Because becoming defense about outward flow and misuse and hacking of password when apply this result Tokenless OTP, solidify security, and evaluated by security system that heighten safety.

▸ Keyword : Authentication, OTP, Tokenless OTP, Ubiquitous Security

• 제1저자 : 김기환, 교신저자 : 박대우(prof1@paran.com)
* 숭실대학교 정보과학대학원 정보보안학과

Ⅰ. 서 론

최근 컴퓨팅과 네트워크 기술의 발전으로 장소와 시간과 기기에 제한을 받지 않고, 인터넷만 접속이 되어있다면 언제든지 업무를 볼 수 있게 되었다. 〈그림 1〉은 유비쿼터스 컴퓨팅 시대(Age of Ubiquitous Computing)로의 업무가 진행되고 있음을 보여 주고 있다.

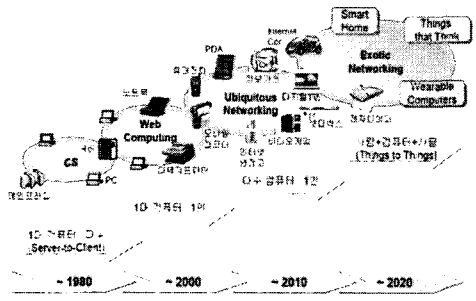


그림 1. 유비쿼터스 컴퓨팅 환경으로의 전환
Fig 1. Conversion toward a Ubiquitous Computing Environment.

유비쿼터스란, 물이나 공기처럼 시공을 초월해 '언제 어디에나 존재 한다'는 뜻의 라틴어(語)로, 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경을 말한다.

유비쿼터스 컴퓨팅 시대가 이루어지기 위해서는 BcN (Broband Convergence Network), 와이브로(WiBro)[1], 기술의 일반화와 함께, RFID 기기의 저가격화 등을 통한 IPv6의 단말주소를 갖는 정보기술의 고도화가 전제되어야 한다.

유비쿼터스 컴퓨팅 시대의 네트워크 접속 시에는 입력되는 ID와 패스워드에 대한 기밀성, 무결성 부문에 대한 네트워크 보안 문제가 대두되고 있다. 즉, 해커가 네트워크 취약점을 공격하여, 단말 상태에서 네트워크를 통하여 전달되는 패킷을 불법으로 수집하고 조합하면 스니핑(Sniffing)이 가능하다[2]. 스니핑을 한 후, 해커는 접근이 용이한 PC나 노트북 등의 개인 단말기를 악성코드나 바이러스를 사용하거나, 해커가 직접 해킹한 데이터 패킷을 이용하여 단말기나 네트워크에 공격을 할 수 있는 취약점이 존재한다.

또한 작은 규모의 LAN 환경에서의 리피터나 유선 무선의 허브에서의 스니핑이 가능하다. 이런 경우 패킷 스니핑 도구를 이용하면 데이터 등 정보를 복원 할 수 있을 정도의 스니핑의 취약점이 존재한다.

또한 원격지에서 인터넷망을 통해서 대상 네트워크의 인트라넷 서버 등의 전산자원의 서비스를 이용할 때에 중간에 라우터와 부속 디바이스에 관한 스니핑 공격도 가능하다.

2003년에 은행 현금카드 비밀번호 유출 사고나 폰뱅킹 인출 사고를 비롯해 2005년 6월에 있었던 인터넷뱅킹 예금 인출 사건은 전자금융 거래 시 본인 확인 장치에 대한 문제가 지속적으로 발생했다는 증거이다. 이에 대한 대책 방안의 하나로써 OTP(One Time Password)[3]가 필요하다.

이러한 문제점을 해결하기 위해, 최근에는 인터넷을 이용하여 언제 어디서나 별도의 소프트웨어 설치 없이 웹브라우저만으로 원격 네트워크의 전산자원에 접근 할 수 있는 방안이 강구되고 있다. 이 방안에다가 보안성을 지원하는 SL VPN(Secure Sockets Layer Virtual Private Network)이 네트워크를 통해 구현 되고 있다. 이 경우에 원격 네트워크에서 SSL VPN으로의 접속 시에 암호에 대한 보완을 위하여 OTP를 적용하고 있다.

그러나 현재의 OTP는 반드시 Token이라는 별도의 하드웨어를 보유하고 있어야하는 취약점 및 불편함이 있었다. 따라서 Token이 없이도 OTP를 적용할 수 있는 새로운 방안에 대한 연구가 필요하다.

본 논문에서는 원격 네트워크 접속 시에 사용자 이름과 패스워드가 스니핑 될 수 있는 가에 대한 취약성을 분석하고, 테스트 환경에서 테스트를 통해 스니핑이 되어 자료가 해킹이 됨을 확인한다.

스니핑 후에 원격 접속 시에 사용자 이름과 암호만을 이용한 방법, Token을 활용한 OTP방법, Token을 사용하지 않는 Tokenless OTP방법 등으로 테스트를 실시하고 각각의 방안에 대한 보안 방안들을 제시하고, 테스트에서 적용해 본다.

그리고 각각의 방안으로 원격 접속 방법에 대한 기밀성, 신뢰성, 가용성, 무결성 등 주요 보안기능의 관점에서 보안을 강화 시킬 수 있는 방안들을 제시하고 증명하여, 원격 접속 시에 정보보호를 이룩할 수 있도록 하는데, 본 논문의 목적이 있다.

Ⅱ. 관련 연구

컴퓨터 네트워크 환경에서 로그인시 사용하는 인증의 의미와 종류와 방식의 설명 및 OTP를 활용한 인증방식 및 종류에 대한 관련 연구를 한다.

2.1. 인증

1) 인증의 정의

인증(Authentication)이란 시스템 또는 네트워크에 액세스 하고자 하는 사용자를 확인하는 과정을 말한다. 즉, 원격접속 환경에서의 인증이란 허용된 사용자인지 인증 절차를 확인하는 것이다. 따라서 인증 절차는 컴퓨터나 네트워크와 같은 주요 전산 자산을 보호하는데 있어서 정보보안의 가장 기초적이면서도 필수적인 과정이다.[4]

컴퓨터 네트워크 및 SSL VPN 시스템에서 가장 일반적으로 사용되는 인증 절차는 로그온 ID인, 사용자 이름 및 로그온 암호를 확인하는 것이다. 사용자이름 및 암호가 정확하면 정당한 사용자 인 것으로 간주되어 사용자에 해당하는 합당한 권한을 부여 받게 된다. 그러나 이 방식의 취약점은 쉽게 암호의 도난, 부주의로 인한 노출 및 분실의 위험이 크다는 것이다. 중요 회사 정보 조회 또는 전자상거래, 금융 거래와 같은 중요한 거래에 있어서 이러한 일들이 발생하면 문제가 된다. 따라서 안전한 인증을 위하여 <표1>과 같은 다양한 인증방법의 특징 비교[5]를 보여주고 있다.

표 1. 다양한 인증방법 간 특징 비교
Table 1. Characteristics comparison between various authentication ways.

인증 방법	보안 수준	편리성
Username / Password	낮다 키보드 스파이웨어에 취약	사용이 간편 암호 기억 어려움 분실 시 복구가 어려움
복잡한 질의응답	Username/Password 보다 우수, 키보드 스파이웨어에 취약	여러 가지 질문에 대한 답변 (예: 소중한 것, 부모님 이름 등) 암호를 기억하기 좋다.
하드웨어 Token(OTP, USB등)	높음 Token의 존재 여부가 중요	Token을 필히 휴대 분실, 도난 및 파손우려
생체 인식	높음 유일한 식별자	지문, 홍채 등 신체적 특징 스캐닝
스마트카드	높음	인식기가 부착된 곳에서만 가능
PKI기반의 전자서명	높음	설치된 이후 이용 간편

2) 이중 요소 인증(Two-Factor Authentication)

이중 요소 인증이란? 2가지 인증 방법을 조합 적용하는 안전성을 향상시키는 인증을 말한다. 즉, 인증은 다음과 같은 3가지 요소로 구분할 수 있다. 바로 자신이 알고 있는 것(패스워드, PIN 등), 자신이 소유한 것(스마트카드, Token, 키 등), 자신 그 자체(지문 등 생체 정보)이다. 이들 중 하나의 요소만 이용하는 사용자 이름 및 암호만 사용하는 단일 인증은 보안에 취약한 편이다. 패스워드 등 자신이 아는 정보만을 사용할 경우 분실 여부를 인지하기 어려우며, Token, 키 등 자신이 소유한 것만을 사용할 경우 분실 시 습득자의 즉각적인 사용이 가능하다. 따라서 이러한 단일 인증의 보안 취약성을 보강하기 위하여 이들 중 서로 다른 2개의 인증을 조합하여 채택한 방식이 이중 요소 인증이다. 예를 들어 은행의 현금 자동 인출기(ATM)처럼 카드와 개인 식별번호(PIN)를 조합하여 사용함으로써 보안성을 높일 수 있다. 일반적으로 암호와 같이 인증을 위해 한 가지 요소에만 의존하는 방식을 약한 인증이라고 하고, 한번의 인증을 위해 독립적인 수단 2가지를 사용하는 인증을 이중요소 인증 이라고 하며 강한 인증이라고 불린다.[5]

이중 요소 인증의 가장 보편적인 방법은 "알고 있는 것(Something you know)"과 "지니고 있는 것(Something you have)"을 동시에 사용하는 것이다. 신용카드 또는 현금인출용 카드가 이중요소 인증 방식의 대표적인 예라고 할 수 있다. 즉 카드 자체는 물리적으로 사용자가 소유하고 있는 것이고, 이 카드에 대응되는 암호는 사용자가 알고 있는 것이다. 이 두 요소가 동시에 제시되어야만 인증 과정을 통과할 수 있다. 이중요소 인증 방식은 원격접속 및 온라인 ID 도용피해를 현격하게 줄여주고 있다. 왜냐하면 해킹을 하여도 암호만 도용하고 카드 없이는 필요한 정보나 시스템에 접근할 수 없기 때문이다. <표2>는 다중 인증에 사용되는 요소[5]들을 보여 주고 있다.

표 2. 다중 인증에 사용되는 요소
Table 2. Multi-Factor Authentication

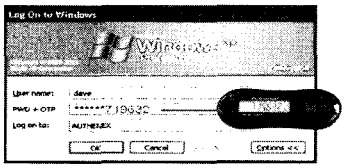
Factor 구분	사용 예
알고 있는 것(Something you know)	암호, PIN
지니고 있는 것(Something you have)	하드웨어Token, 핀번호, 신용카드, 핸드폰
신체의 일부(Something you are)	지문, 음성, 맥박, 홍채 등

이중요소 인증기술이 기존방식에 비해 안전성이 높아지긴 했으나 보편적인 용도로 확산되기에는 장애 요소가 있다. 사용자들이 새로운 물건 하나를 더 지니고 다니는 것에 대해 불편해 하기 때문이다. 또한 솔루션이 각각의 다른 기술을 채택하고 있을 뿐만 아니라, 특허로 보호 받고 있는 경우가 많아 솔루션 간에 호환성이 떨어지는 것도 보급 확대의 걸림돌이 되고 있다.

2.2. OTP

1) OTP 인증의 의미

OTP는 일회용 비밀번호 인증이다. 한 번 사용된 암호는 두 번 다시 사용하지 않는 매번 새로운 암호를 이용하여 인증하는 방식이다. 따라서 암호를 스니핑 당했다 하더라도 다음번에 재사용이 불가능하기 때문에 암호의 보안 취약성을 줄일 수 있다. 일회용 비밀번호는 이중요소 인증 방식의 한 가지 유형이라고 볼 수 있다.



〈그림2〉 Token OTP를 이용한 인증 예
Fig. 2. The authentication that used token OTP

〈그림 2〉 Token OTP를 이용한 인증[6]이다. 이 경우 일정시간마다 전용 단말기 등에 새로운 비밀번호가 생성되어 시스템에 접근할 때마다 새로운 비밀번호를 입력해야 하기 때문에 해킹이나 사용자의 관리소홀 등으로 비밀번호가 노출되는 것을 방지할 수 있다. 30개~100개의 정해진 범위에서 비밀번호를 입력하는 기존의 인쇄된 보안카드에 비해 OTP는 사용자 비밀번호가 노출되더라도 새로 생성된 비밀번호를 입력해야 하기 때문에 상대적으로 강력한 보안성을 제공할 수 있다.

2) OTP 알고리즘

대부분의 모든 OTP 생성 알고리즘은 수학적으로 일방향 함수(One-way Function f())에 기반을 두고 있다. 일방향 함수란 해쉬 함이며, 출력 값으로부터 입력 값을 유추해 낼 수 없는 특징을 가지고 있다.

거의 모든 유닉스(UNIX) 운영체제에 구현되어 있는 S/Key 시스템(RFC1760)이 그 예이며, 이 시스템은 다음과 같은 절차를 통해서 수행된다.[7]

a) 서버는 비밀 값 w를 1번, …, n번 해시 하여 n개의 비밀번호들을 얻고 w는 삭제한다.

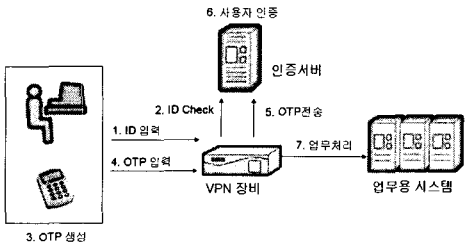
b) 생성된 n개의 비밀번호를 사용자에게 역순으로 출력해서 준다. 서버는 n번 해시한 값만을 남기고 모두 지운다.

c) 사용자는 출력된 순서대로 비밀번호를 제시한다.(즉, w를 n-1번 해시 한 값, n-2번 해시 한 값, …)

d) 서버는 사용자가 제시한 값을 한 번 해시하여 가지고 있는 값과 비교한다. 일치하면 수신한 값을 저장하고 이전 값은 삭제한다. 그리고 사용자를 인증한다.

이 절차를 통해 알 수 있는 것처럼, 특정 시점에서 사용자가 전송한 비밀번호를 알고 있다고 하더라도 다음에 전송할 비밀번호는 유추할 수 없다. 왜냐하면 다음에 전송될 비밀번호는 w를 한 번 덜 해시 한 값인 데, 해시 함수의 특성상 출력 값을 통해 입력 값을 유추할 수 없기 때문이다. 현재 운용되고 있는 OTP 알고리즘들은 S/Key보다 상당히 더 복잡하게 구현되어 있다.

〈그림 3〉은 동기화방식의 인증 절차를 보여주고 있는 것이다.



〈그림 3〉 동기화 방식의 OTP 인증 절차 (VPN 로그온)
Fig. 3. OTP authentication procedures of a synchronization method.(VPN Logon)

현재 사용되고 있는 OTP 솔루션들은 〈표3〉과 같이 서버와 클라이언트간의 암호 동기화 방식에 따라 다음과 같이 구분 할 수 있다.

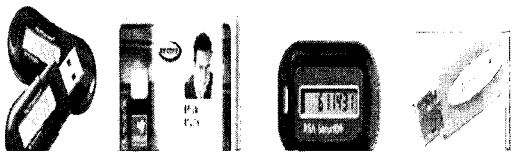
표 3. OTP 생성 방식 간 특징 비교
Table 3. Characteristics comparison between OTP generation methods.

OTP 생성	입력 값	장점	단점
시간 동기화 방식	시간 자동입력	서버의 질의 값을 입력할 필요가 없어 사용이 간편하고 호환성이 높음	OTP디바이스와 서버간의 시간 동기화 필요, 시간 간격이 길면 보안성이 떨어지고, 시간 간격이 낮으면 입력 오류 시 이용자 대기시간이 길어 불편
이벤트 동기화 방식	OTP 생성 횟수 자동 입력	시간 동기화 방식에 비해 전력소모 적어 배터리 수명이 길다	OTP Token과 서버 간 OTP생성 횟수 동기화에 대한 고려가 필요
질의 응답 방식	인증서버로부터 받은 임의의 난수	구현이 간편, 서버와 OTPToken간 동기화 불필요	질의 값 입력에 따른 불편함. 동일한 질의 값 반복 생성 방지장치 필요
혼합 방식	시간과 OTP 생성 횟수	시간 동기화에 비해 시간 간격을 길게 가져 갈 수 있음	같은 시간 간격 내에서 OTP 생성 횟수 동기화 장치 필요

3) 다양한 OTP 디바이스

사용자가 OTP를 이용하기 위해서는 OTP를 생성할 수 있는 전용 단말기와 같은 매체를 소유해야 한다. OTP를 생성하는 장치에는 〈그림 4〉와 같이 OTP 생성 전용장치인 전용단말기(Token), 휴대 전화나 PDA등에 OTP 생성 프로그램을 설치하는 모바일 OTP, 스마트카드 나 USB 등과 같은 다른 인증수단과 결합된 형태 등 매우 다양하게 장치들이 있다. 이외에도 전용 단말기는 휴대에 따른 불편함 때문에 Tokenless OTP솔루션을 제시한다.

강력한 인증 수단의 필요성에 높아짐에 따라 OTP 솔루션이 가장 적합한 대안으로 인식되고 있으나, 과다한 초기도입 비용, 배포 및 유지보수와 같은 지속적인 관리 부담, 일정 기간 경과 후의 라이센스 및 디바이스 교체에 따른 유비보수 비용, 휴대의 불편함에 따른 사용자의 이용 기피 등 OTP 활용을 위해서 개선하기 위한 지속적인 노력이 필요하다.



〈그림4〉 다양한 OTP 디바이스
Fig. 4. Various OTP devices

모바일 OTP(Mobile OTP)는 휴대전화에 탑재 가능한 일회용 비밀번호 생성 SW로 공개키 기반(PKI) 솔루션으로 OTP SW가 매번 다른 비밀번호를 생성해 주기 때문에 강력한 보안성을 제공받을 수 있다. 휴대전화에 OTP SW를 탑재함으로써 휴대전화 사용자는 언제 어디서든 사용자 인증을 할 수 있다는 장점이 있다.

2.3. 스니핑을 위한 공격 툴

1) Cain & Abel[8]

Cain & Abel은 네트워크 패킷을 스니핑 하여 여러 가지 다양한 시스코 암호, 라우팅 프로토콜 해시, VNC 암호, RADIUS 쉐어드 시크리트(RADIUS Shared Secrets), MS SQL 서버 2000 그리고 MySQL 암호를 해독할 수 있다.

그리고 IKE 미리 공유된 키까지 해독하고 IKE를 사용하여 비밀 키를 교환 및 업 데이트하는 IPSec VPN에 침입하며, 사전대입이나 무차별대입을 통한 크랙기능을 제공한다. 스크램블된 비밀번호를 해제하고 캐시에 저장된 비밀번호를 추출한다.

2) Ethereal[9]

네트워크 인터페이스로부터 활동 중인 패킷 데이터를 Ethereal로 캡처하여 캡처된 패킷 데이터를 열고 저장한다. 캡처된 많은 다른 캡처 프로그램들로부터 패킷 데이터를 인포트하고, 익스 포트를 한다. Ethereal은 공격 툴 기능과 함께 네트워크의 모니터링 툴이라고도 할 수 있다.

2.4. 패킷과 네트워크 모니터링 툴

1) NTOP[10]

네트워크 세그먼트에 현재 실시간으로 흐르는 트래픽상의 모든 세션과 현황 통계를 제공하고 가상 LAN이나 OSPF등 현황을 파악하며, 네트워크 내에서 인터넷공유 등 인가되지 않은 라우팅 기능을 하는 PC나 장비를 찾아낼 수도 있다. 또한 스니핑을 위한 인터페이스(Promiscuous Mode)를 감지해 관리자가 쉽게 보안 취약점에 대하여 대응할 수 있게 해준다.

III. 원격접속 시 로그인 접속에 대한 공격

외부에서 내부의 전산자원을 이용하기 위하여 원격 접속 시에 일회용 암호를 사용하지 않고, 사용자이름과 암호만을 사용하여 내부 네트워크인 LAN과 원격지의 WAN 구간에서의 로그인 접속에 대한 공격에 대한 테스트를 실시한다.

원격 접속 시 로그인 접속에 대한 근거자료로는 CERT에서의 취약성 공고 자료를 조사하였으며, 이 자료를 근거로 하여 취약성을 공격하고 분석하여 공격을 통한 결과를 나타낸다.

3.1. 일반 네트워크 구간의 스니핑 공격

외부에서 인터넷 네트워크를 통해서 원격 접속을 시도하는 단말기에 연결된 네트워크인 LAN구간에서 원격접속 서비스에 대한 취약점을 발견한다. 공격은 외부 네트워크의 로컬망 내 호스트에 스니핑 도구를 설치하고, ARP Cache poisoning을 시행[11]하여, LAN에서 발생하는 패킷을 스니핑 한 후 툴을 통해 원격 접속 시 필요한 사용자 암호에 대하여 스니핑을 실시한다.

1) 스니핑 테스트 PC 사양

인터넷 네트워크를 통해서 원격 접속 시에 스니핑 테스트를 위한 실험장비의 사양은 표 4.와 같다.

표 4 . 테스트 PC 사양
Table 4. Test System Specification.

PC	항 목	사 양
TEST PC(공격자)	하드웨어 사양(H/W)	Intel Pentium2.661Ghz CPU, 512M RAM, 80G HDD
	운영체제(OS)	Linux RedHat 9.0(OS),
	요구 소프트웨어(S/W)	Cain & Abel v2.9.
사용자 PC	하드웨어 사양(H/W)	Intel Pentium2.661Ghz CPU, 512M RAM, 80G HDD
	운영체제(OS)	Windows XP Professional (SP2),
	요구 소프트웨어(S/W)	원격 접속 프로그램

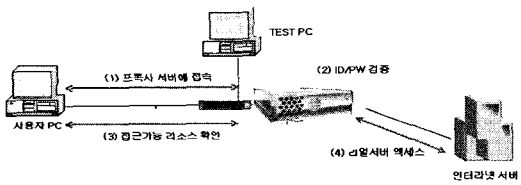


그림 5. 원격 로그인 접속 시 LAN에서 원격제어를 통한 스니핑
Fig. 5. Sniffing through remote controls at LAN in case of the access that is a remote log.

2) 테스트 네트워크 구성도

일반 네트워크의 시스템 환경 구성은 〈그림 5〉와 같다.

3) 공격 Tool

Cain & Abel은 패킷 스니핑과 패스워드 크래킹 등 다양한 기능이 포함된 통합 해킹 툴로서 스위칭 환경에서의 스니핑 및 각종 프로토콜에 대한 디코드가 가능하다.

4) 공격

a) 내부망의 사용자 PC를 공격하여 패킷을 스니핑 할 수 있는 Cain & Abel 프로그램을 설치하여 실행한다.
b) 스니핑 하려는 사용자 PC의 IP를 선택한 후 ARP Cache Poisoning을 실행한다.
c) 테스트 PC는 사용자 PC에게 Gateway Mac주소라는 정보를 포함한 ARP Reply를 전송한다. Gateway에게는 사용자 PC Mac주소라는 정보를 포함한 ARP Reply를 전송한다.
d) 사용자 PC는 수신한 ARP Reply 정보를 이용하여 자신의 Mac Table에 있는 Gateway의 Mac정보를 변경, Gateway는 수신한 ARP Reply정보를 이용하여 자신의 Mac Table에 있는 사용자 PC의 Mac정보를 변경한다.
e) 사용자 PC를 이용하여 통화할 때 변경된 Gateway의 Mac주소로 패킷을 전송한다.
f) 사용자 PC의 패킷을 스니핑 한 TEST PC는 올바른 Gateway로 패킷을 Forwarding, Gateway는 Proxy Server로 패킷을 전송한다.
g) 패킷을 받은 Proxy Server는 Gateway로 응답 패킷을 전송한다.
h) Gateway는 Proxy Server의 응답 패킷을 사용자PC 로 전송할 때 변경된 사용자 PC의 Mac주소로 전송한다.
i) Gateway에서 사용자 PC으로 전송되는 패킷을 스니핑한 TEST PC는 패킷을 사용자PC으로 Forwarding한다.
j) 이 공격 과정을 통하여 TEST PC는 패킷을 사용자 PC에서 Proxy Server로 전송되는 사용자 PC의 사용자이름 및 암호 그리고, 모든 정보 데이터를 스니핑 할 수 있다.

5) 공격 결과

LAN 구간에서 사용자 PC가 로그인 접속 시 사용하는 사용자이름과 암호에 대하여 공격을 통하여 정보를 입수 할 수 있었다.

공격 결과로 LAN 구간에서 취약점이 발견되고, 사용자의 이름과 암호가 알려져서 본인의 개인정보 및 PC정보의 유출뿐만 아니라 원격접속대상의 침투까지 가능하여 전산자원 및 정보의 불법적인 사용에 대하여 피해를 야기할 수 있다.[12]

3.2. Token OTP 사용 시에 스니핑 공격

원격 접속 서비스 시 필요한 사용자 이름 과 암호를 입수하여 원격접속 대상 네트워크에 침입하여 인트라넷 서버까지도 공격이 가능하였다.

이러한 취약점에 대해 〈그림 6〉과 같이 OTP서버를 도입하면 사용자 PC가 해킹을 당하여, 사용자 이름은 알 수 있어도 일회용 암호를 알 수가 없어서 원격접속대상 네트워크 및 서버를 접속할 수 없다. 따라서 인트라넷 서버 등의 보호가 가능한 보안환경이 구축 될 수 있다. [13]

1) 테스트 PC 사양

Token OTP를 활용하여 인터넷 네트워크를 통해서 원격

접속 시에 스니핑 테스트를 위한 실험 장비의 사양은 〈표 5〉와 같다.

표 5. 테스트 PC 사양
Table 5.Test System Specification

PC	항 목	사 양
Token OTP 인증 서버	하드웨어 사양(H/W)	Intel Pentium 1 Ghz CPU, 256M RAM, 50G HDD
	운영체제(OS)	Windows2000, 20003 Server LINUX
	유저 리포지토리	MS AD, LDAP, XML, SQL
	요구 소프트웨어(S/W)	Java J2SE Developers Kit v5 Jakarta Tomcat v5
TEST PC (공격자)	하드웨어 사양(H/W)	Intel Pentium 2.66 Ghz CPU, 512M RAM, 80G HDD
	운영체제(OS)	Linux RedHat 9.0(OS),
	요구 소프트웨어(S/W)	Cain & Abel v2.9.
사용자 PC	하드웨어 사양(H/W)	Intel Pentium 2.66Ghz CPU, 512M RAM, 80G HDD Token(OTP)
	운영체제(OS)	Windows XP Professional (SP2),
	요구 소프트웨어(S/W)	원격 접속 프로그램

2) 테스트 네트워크 구성도

Token OTP 테스트를 위한 실험 네트워크 구성도는 〈그림 6〉과 같다.

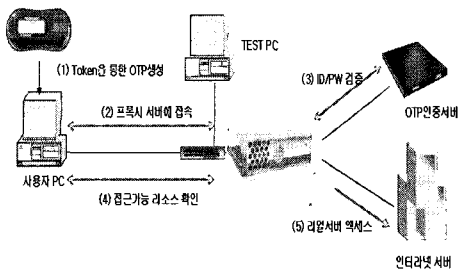


그림 6. TokenOTP 를 사용한 원격 로그인 접속
Fig. 6. Token OTP Server Network

3) 공격 Tool

❖ Cain & Abel

4) 공격

a) 공격자는 Promiscuous mode를 통해 모든 패킷을 잡아들여서, 공격자가 원하는 ID와 Password 등의 정보를 해킹[11]한 후 사용자 PC의 사용자 이름 및 일회성 암호를 원하는 목적지(TEST PC)로 전송한다.

b) PC 해킹 후 , 공격자는 사용자 이름 및 일회성 암호를 이용하여 대상 네트워크의 인트라넷 서버로의 접속이 일부 가능하여 정보조회 및 등록정보를 변조하여 원하는 목적지로 전송이 가능하다.

5) 공격 결과

위의 공격은 실험실 안에서 내부네트워크 구간에서 테스트를 하였다. 만약 실제 해킹이 수행되면, 사용자 이름 및 일회용 암호를 입수하여 원격 접속 후 대상 네트워크의 전산자원, 정보 전송자와 수신자 모두의 개인정보 및 정보의 불법적인 사용에 대한 대규모의 피해를 야기 시킬 수 있다.

3.3. Token OTP 적용의 취약점

원격 접속인증 시에 전용 단말기인 Token을 사용하는 일회용 암호는 다음과 같은 취약점을 가지고 있다.

a) 사용자 PC가 해킹을 당했을 경우 원격 접속 시 사용자의 이름과 일회용암호가 알려져서, 본인의 개인정보 및 PC 정보의 유출뿐만 아니라 원격 접속대상의 침투까지 가능하다.

b) 로그인 접속 시에 반드시 클라이언트용 전용 단말기를 휴대하여 일회용 암호를 추출 후 입력해야한다.

c) Token을 항상 갖고 다녀야하므로 분실의 우려 및 휴대의 불편함이 있다.

d) Token에 들어있는 배터리의 수명이 제한이 있으므로 배터리 수명에 따라 교체에 대한 번거로움과 투자비용이 추가된다.

e) Token을 배포 및 교체, 비용 부문에서 관리자의 업무가 가중된다.

IV. 원격 접속에서의 Tokenless OTP 적용

4.1. Tokenless OTP 적용 설계

원격 접속 시 보안강화를 위한 일회용 암호 전용단말기를 쓰지 않고도 그 이상의 효과를 볼 수 있는 솔루션에 대

하여 〈그림 10〉과 같이 구현해 보았다.

1) Tokenless OTP의 동작 원리

〈그림 7〉에서 개인별로 PIN을 부여하여 인증 요청 시마다 10개의 숫자 열이 제공되어 PIN과 10개의 숫자를 이용해 일회용 암호추출이 되는 것이 동작의 원리[13]이다.

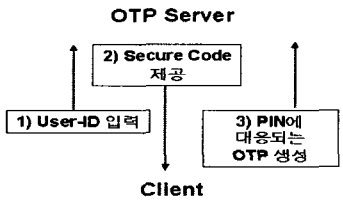


그림 7.Tokenless OTP 동작원리
Fig 7. Tokenless OTP action principle

2) Tokenless OTP 추출 과정

a) 개인별로 고유의 핀 번호 부여 (예:1369)

b) 원격으로 인트라넷 서버 접속 시 〈그림 8〉과 같이 사용자 인증 화면에서 사용자이름을 입력하면 화면 하단에 보안 스트링이 생성되어 나타난다. 입력 시마다 10개의 숫자 열 을 생성하여 로그인 화면에 나타낸다.

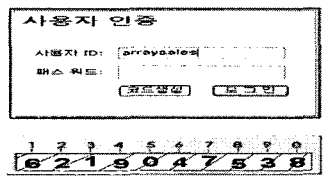


그림 8. 보안 스트링 생성[13]
Fig 8. Security String

숫자를 하나하나 취합하면 일회 암호(예: 4163)와 기존에 사용자에게 알려준 정적암호(예: Test)와 일회용 암호(예:4163)를 합쳐서 암호(Test+4163)를 입력한다.

c) 〈그림 9〉처럼 미리 사용자에게 부여해준 핀 번호(예: 6319인 경우)에 대응되는 숫자를 하나하나 취합하면 일회 암호(예: 4163)와 기존에 사용자에게 알려준 정적 암호(예: Test)와 일회용 암호(예:4163)를 합쳐서 암호(Test+4163)를 입력한다.

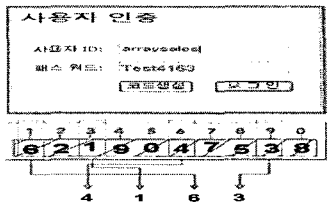


그림 9. 일회용암호 추출
Fig 9. OneTime Password

4.2. Tokenless OTP 적용 테스트

1) 테스트 PC 사양

Tokenless OTP를 활용하여 인터넷 네트워크를 통해서 원격 접속 시에 스니핑 테스트를 위한 시험장비의 사양은 〈표 6〉과 같다.

표 6. 테스트 PC 사양
Table 6.Test System Specification.

PC	항 목	사 양
Tokenless OTP 인증서버	하드웨어 사양(H/W)	Intel Pentium 1 Ghz CPU, 256M RAM, 50G HDD
	운영체제(OS)	Windows2000, 20003 Server LINUX
	유저 리포지토리	MS AD, LDAP, XML, SQL
	요구 소프트웨어(S/W)	Java J2SE Developers Kit v5 Jakarta Tomcat v5
TEST PC(공격자)	하드웨어 사양(H/W)	Intel Pentium 2.66 Ghz CPU, 512M RAM, 80G HDD
	운영체제(OS)	Linux RedHat 9.0(OS),
	요구 소프트웨어(S/W)	Cain & Abel v2.9.
사용자 PC	하드웨어 사양(H/W)	Intel Pentium 2.66 Ghz CPU, 512M RAM, 80G HDD
	운영체제(OS)	Windows XP Professional (SP2),
	요구 소프트웨어(S/W)	원격접속,.Tokenless OTP

2) 테스트 네트워크 구성도

Tokenless OTP 적용을 위한 테스트 네트워크의 구성은 〈그림 10〉과 같다.

3) 공격 Tool

❖ Cain & Abel

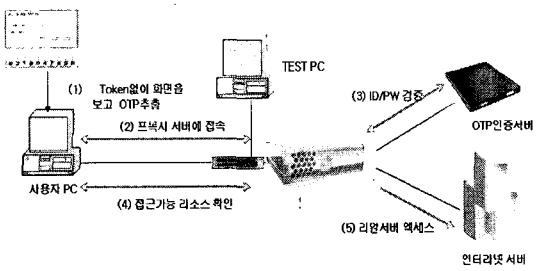


그림 10 . Tokenless OTP를 사용한 원격 로그인
Fig. 10. Tokenless OTP Server Network

4) 공격

a) 사용자 PC 해킹 후 , 공격자는 사용자이름 및 보안 스트림을 원하는 목적지(TEST PC)로 전송한다.

b) 사용자 PC 해킹 후, 공격자는 사용자 이름 및 보안 스트림을 캡쳐할 수 있으나, 사용자만이 알고 있는 핀 번호를 모르면 암호 추출을 할 수 없어서 대상 네트워크의 인트라넷 서버로 접속자체가 안되어 정보 조회 및 등록정보를 변조하여 원하는 목적지로 전송이 불가능하다.

5) 공격 결과

위의 공격은 테스트 룸 안에서 내부네트워크 구간에서 테스트를 한 결과, Token이 없이도 암호에 대한 추출을 방지 할 수 있어서, 원격 접속 후 대상 네트워크의 전산자원, 정보전송자와 수신자 모두의 개인정보 및 정보의 불법적인 사용에 대한 보안을 할 수 있었다.

표 7 원격접속시 인증 방안과 보안 기능
table.7. Authentication plan and security capability in case of remote access.

보안 가능	사용자이름, 암호	Token OTP	Tokenless OTP
기밀성	사용자 이름 및 암호 스니핑 가능	일회용 패스워드 스니핑 가능	암호화 후 보안 스트링 스니핑 내용 판독 불능
신뢰성	스니핑 가능성으로 신뢰성 훼손	일회에 한하여 패스워드 스니핑 가능	매회신규 보안스트림 생성 및 핀 번호 비교
가용성	LAN, WAN 구간의 단말기와 라우터	접근 제어와 인증 및 네트워크 모니터링 탐지 대응	패스워드의 핀 번호 추출로 스니핑 예방
무결성	무결성 보장이 안됨	메시지 다이제스트 해시 함수 MD5, SHA-1	무결성 보장, 스니핑 예방
부인봉쇄	사용자 이름 및 암호로 부인봉쇄	개인별 고유의 단말기로 부인봉쇄	개인 고유의 핀 번호로 부인봉쇄

〈표 7〉에서와 같이 Tokenless OTP에 적용 시 에는 보안스트링을 캡쳐 하더라도 암호화 및 사용자만이 아는 핀 번호 추출에 의해서만 암호를 생성하므로 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄[13]가 입증 되었다.

V. 결론

본 논문은 원격 접속 서비스 시 사용하는 사용자이름과 암호만을 사용하는 경우와 Token을 사용하여 인증하는 OTP 및 Token을 사용하지 않는 Tokenless OTP 시스템을 구성하여 사용자 PC 및 원격 접속대상에 대한 스니핑 테스트를 하였다.

3가지 경우에 대한 스니핑 테스트를 한 결과, 사용자 이름과 암호만을 사용하여 일반 네트워크에서의 원격접속을 하는 경우에 스니핑이 성공되었다. 따라서 대상 네트워크에 대한 원격 접속 시 에는 사용자이름과 암호만을 사용해서는 스니핑 공격에 대하여 취약점이 있다는 것을 밝혀낼 수 있었다

사용자 이름과 암호만을 가지고 대상 전산자원에 접근할 경우에 생기는 기밀성, 가용성, 무결성 의 3가지 보안 목표에 위배되는 문제에 대하여 Token을 사용한 OTP 와 Token없이 사용하는 Tokenless OTP를 제안 하였으며, 스니핑 보안 방안을 적용하는 테스트는 Ethereal에서 패킷의 분석으로 확인하였다.

대상 네트워크에 대한 원격 접속 시 Token OTP를 활용하여 접속하는 경우에 접근제어와 인증 및 네트워크 모니터링 탐지에 대한 대응은 할 수 있었다. 하지만 사용자 PC자체에 대한 해킹을 통하여 ID 및 일회용 패스워드에 대한 정보가 유출되어 일회성이긴 하지만, 일시적 접근을 허용하는 취약점이 발견 되었다. 또한, Token OTP 적용 시에 Token의 휴대 및 관리에 대한 불편함으로 인증에 대한 부문이 소홀해 질 수 있는 사회공학적인 보안에 대한 문제도 가지고 있었다.

최종적으로 Tokenless OTP를 적용하여 원격 접속 시에 사용자 이름과 보안스트링이 스니핑이 되어도 사용자가 아닐 경우에는 보안 스트링의 내용판독 및 핀 번호를 이용한 패스워드 추출이 불가능 하여 원격접속에 대한 기밀성, 신뢰성, 무결성이 보장되어 보안을 이룩할 수 있었다.

따라서 일반 네트워크 및 인터넷에서의 원격 접속 시에

는 Tokenless OTP를 함께 적용하여 시스템을 구성하는 것이 접속 시, 인증에 대한 보안취약점을 해결 할 수 있는 방안으로 입증이 될 수 있었다.

향후 연구 되어야 할 과제로는, 암호화와 접근제어 및 인증과 무결성 검증의 방법을 더 강화하기 위하여 사용자 핸드폰에 SMS[14]를 통하여 보안스트링을 보내는 방안에 대한 테스트 방안과 알려지지 않는 새로운 공격에 대하여 보안 대응이 될 수 있는 방안에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] 와이브로 보안기술 해설서. 한국정보보호진흥원. 2006.8.

[2] 박대우, " VoIP 서비스의 도청 공격과 보안에 관한 연구."한국컴퓨터정보학회논문지, 제11권 제2호, 2006. 5. 31.

[3] 송유진, 이동혁. "OTP 기반의 웹서비스 인증 메커니즘 설계 및 구현 ." 한국전자거래학회지, 제10권 제2호, 2003.

[4] Jalil Feghhi & P. Williams, Digital Certifi -cates: Applied Internet Security, Addison-Wesley, 1999.

[5] "OTP솔루션." NetworkTimes. 2006.10.

[6] "Token OTP." http://www.autehnex.com. 2003.3.

[7] 박중길, 김영진, 김영길, 백규태, 백기영, 류재철. "S/KEY를 개선한 일회용 패스워드 매커니즘 개발." 통신정보보호논문지. 제9권 제2호 ,pp28-32, 1999. 6.

[8] Cain & Abel v2.9. Cain &Abel, http://www.oxid.it/cain.html. 2006.11.

[9] Ethereal-network protocol analyzer Version 0.99.0, Ethereal. http://www.ethereal.com/, 2006.11.

[10] NTOP. http://www.ntop.org/download.html. 2006. 11.

[11] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[12] W. Stallings. "Cryptography and Network Security, Principles and Practice". Third Edition, Prentice-Hall, October 2005.

[13] Security String 과 Tokenless OTP. http://www.swivelsecure.com/?page=whitepapers/ 2006. 11.

[14] 김우경, 이경헌. "SMS와 OTP개념을 이용한 사용자 인증." 한국정보과학회논문집, 제31권 제2호, 2004.

저 자 소 개

김 기 환

1989년 안양 과학 대학 전자공학과 졸업

2003년 (주)테라 네트워크 기술 사업부 부장

2003년 한국 산업기술원, 지방정보화재단 네트워크 강사

2004년 한국방송대 경영학과 졸업 (경영학사)

2005년 숭실대학교 정보과학 대학원 정보보안학과 (석사과정)

2006년 (주)N&I KOREA 시스템사업부 기술영업이사

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, 디지털 포렌식, RFID, SSLVPN, OTP, DRM

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직 캐슬 정보통신 연구소 소장, 부사장

2004년 숭실 대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality