바이오메트릭 정보를 이용한 일회용 패스워드(B-OTP) 생성 기법 개발 및 응용

장원준, 이형우
한신대학교 컴퓨터공학부

Biometric One-Time Password Generation Mechanism and its Application on SIP Authentication

Won-Jun Jang, Hyung-Woo Lee
School of Computer Engineering, HanShin University

요 약 최근 인터넷 기반 서비스에서 사용자 인증 과정의 취약점을 이용한 공격이 급증하고 있다. 특히, 인터넷 뱅킹과 인터넷전화가 많이 보급됨에 따라 보안사고가 급증하고 있으며 공격자들의 공격 수법도 점차 지능화 되고 있다. 결국 인터넷뱅킹과 인터넷전화 등의 서비스에서 바이오메트릭 정보와 같이 사용자가 소유하고 있는 개인 고유 정보 등을 이용하여 보다 강화된 인증을 제공할 필요가 있다. 따라서 본 연구에서 제시하는 B-OTP 기술은 바이오메트릭 정보(Biometric Data)를 OTP 방식과 접목하는 기술로 기존 인터넷 서비스에서의 사용자 인증을 강화시킬 수 있는 방법이다. 사용자가 입력한 바이오메트릭 정보를 이용하여 생성된 B-OTP 값을 이용할 경우 인터넷뱅킹과 인터넷전화 서비스 등의 보안성을 높일 수 있을 것으로 기대된다.

Abstract Diverse kind of attack using the vulnerability of user authentication on Internet service is announced recently. Especially, security accidents on the Internet banking service and Internet telephony service(SIP) are increased rapidly. Attack skills are also evolved into intelligent mechanism. Therefore, more enhanced authentication mechanism is required on existing Internet banking and telephone services for preventing those kinds of attacks using personal identity information such as biometric data. In this research, the proposed B-OTP mechanism can be used to enhance security on a user authentication procedure by combining biometric data with existing OTP mechanism. As a result, the security on internet banking and Internet telephone service will be more improved by using proposed B-OTP mechanism.

• Key Words : 바이오메트릭 데이터, 바이오 일회용 패스워드, 인증, Biometric Data, B-OTP, Authentication,

1. 서론

최근 인터넷 뱅킹 및 인터넷전화 서비스 이용에서의 사용자 인증 취약점이 발견되고 있다. 특히 인터넷 뱅킹에서 사용하고 있는 보안카드 방식만으로는 효율적인 대응이 어렵게 되었으며 인터넷전화 서비스 역시 사용자 인증의 취약점을 이용한 공격이 가능하여 이에 대한 대응 방안이 필요하다.

인터넷 전화(VoIP : Voice Over Internet Protocol) [1] 서비스는 Internet Protocol망을 사용하여 음성 데이터를 전송하는 기술이다. 기존 VoIP 기술은 ITU-T

이 논문은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음 (KRF-2008-521-D00444).
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2010년 12월 12일 수정일 2010년 12월 24일 게재확정일 2010년 12월 28일

(International Telecommunication Union Telecommunication Standardization Sector)의 H.323 시그널 프로토콜을 사용한다. 하지만 H.323 프로토콜[2]은 LAN 환경에서 Multimedia 통신을 지원하기 위해 개발된 프로토콜로 확장 네트워크 구성과 대규모 사용자를 지원하는데 한계가 있으며, 서비스 구현이 복잡하고 호환성을 보장하지 못한다는 단점을 가지고 있다. 이러한 단점을 보완하기 위해 SIP(Session Initiation Protocal)[3]가 등장하였다. SIP 기반의 이러한 공격기법들은 공격자가 SIP 패킷에 대해 수정 및 삭제를 함으로써 이루어진다. 여기서 발생하는 문제점은 공격자가 패킷에 대하여 수정 및 삭제를 하여도 문제없이 통신이 된다는 점에 있다. 따라서 이러한 문제점을 해결하기 위해서는 SIP 프로토콜에서의 인증을 한층 더 강화하여 패킷에 대한 수정이나 삭제가 이루어지지 못하도록 각 Agent 간의 사용자 인증이 이루어져야 한다.

인터넷 뱅킹 서비스에서 사용하는 기존 OTP 방식은 OTP 토큰에 대한 실제 소유자에 대한 확인 과정을 제공되지 못하고 있다. OTP(One-Time Password) 토큰 발급시 비밀키 정보를 이용하여 패스워드를 생성하고 있으나, 실제 사용자에 대한 정보를 포함하고 있지 않아 제 3자에 의해 사용시 이를 확인할 수 있는 방법이 제공되지 못하고 있다. 또한 OTP 정보에 대해 MITM(Man in the Middle Attack) 공격이 가능하기 때문에 이를 능동적으로 보완할 수 있는 방법이 기술적으로 제시되어야 한다. 그리고, OTP 토큰에 대한 분실시 비동기화/동기화 방식 모두 분실/도난시 대응 방안을 제시하지 못하고 있다. OTP 토큰이 분실되었을 경우 원래 소유주에 대한 확인 과정이 전혀 제공되지 않고 있다. 결국 현재까지 제시된 OTP 방식은 단순히 일회용 패스워드를 생성하는 과정에만 목적을 두고 있을 뿐, OTP 기기 및 모듈에 대한 소유자 인증/확인 과정이 제공되지 못하고 있기 때문에 새로운 방식을 개발할 필요가 있다.

따라서 이에 대한 해결방안으로는 본 연구에서는 OTP 토큰 실제 소유자 인증을 위해 각 개인이 고유하게 소유한 바이오메트릭 정보로부터 OTP 값을 생성하여 인증에 활용하는 방식을 제시하고자 한다. 이와 같은 방식을 사용하게 되면 인터넷 뱅킹, 인터넷 전화 서비스 등에서 발생하는 인증 문제도 해결할 수 있으며, 스마트폰 등과 같은 정보기기를 이용한 OTP 기반 다중 인증에도 활용 가능하다는 장점이 있다. 본 논문에서는 기존 OTP 기술 및 SIP 서비스의 취약성에 대하여 분석하였으며, 바이오메트릭 정보와 OTP 기술을 접목한 B-OTP를 이용하여 이를 직접 SIP 보안 인증 시스템에 적용하였고 안정성을 분석하였다.

2. 기존 OTP 및 SIP 서비스 취약성

2.1 OTP 기술 분석

기존의 OTP(One-Time Password)[4] 기술은 일회용 패스워드를 생성하는 기술이다. OTP 생성기술은 크게 비동기화 방식과 동기화 방식으로 나눌 수 있다.

비동기화 OTP 방식[5]은 Challenge Response 방식으로 작동하는 것이며, 질의 값에 대한 응답 결과로 인증과정을 수행한다. 이 방식은 서버와의 동기화가 필요 없다. 그러나 질의 값이 반복될 경우, 공격자의 공격 성공 확률이 높아진다.

OTP 동기화 방식은 시간 동기화 방식의 경우 서버와 OTP 단말간의 동기화된 시간 정보를 기준으로 특정 시간 간격마다 패스워드를 생성하는 방식으로 MITM 공격에 취약하며, 재사용 시간의 제약이 있다는 문제점이 있다. 이벤트 동기화 방식의 경우는 서버와 OTP 단말간의 동일한 카운트 값을 기준으로 패스워드를 생성하는 방식으로 MITM 공격과 재전송 공격에 취약하며, 인증서버에서 카운터의 오차 범위 설정에 따라 성능 및 안정성에 많은 차이가 발생한다. 이벤트-시간 동기화 방식의 경우 시간 동기화 방식과 이벤트 동기화 방식의 장점을 조합한 방식으로 특정 시간 간격마다 패스워드가 생성되며, 같은 시간에서 재생성 시에는 카운트 값을 증가시켜 패스워드가 변하도록 하는 방식으로 MITM 공격에 취약하며, 인증 실패 및 인증 재 시도를 위해 기다려야하는 불편함이 있다.

OTP의 위협요소로 공격자의 목표는 서버를 속여 정당한 사용자로 위장(impersonation)하는 것이며, 공격 방법은 다음과 같다.

- 재전송(replay) 공격 : 도청(eavesdropping)으로 획득한 세션의 인증정보를 서버에게 재전송하는 공격 방법
- 사전(dictionary) 공격 : 사용자들은 외우기 쉬운 특정 개인 정보(기념일 등)을 PIN 번호로 사용하기 때문에, 공격자는 이를 이용하여 사전에 PIN번호를 추측하는 공격 방법

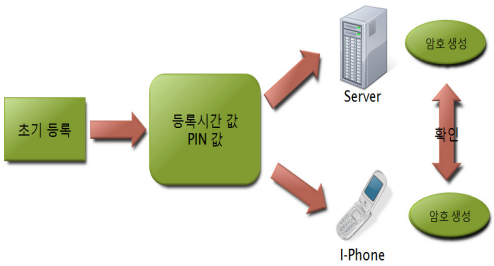
- 세션 하이재킹(hijacking) 공격 : 공격자가 정당한 사용자의 세션을 가로채는 공격 방법
- 비동기(de-synchronization) 공격 : 동기화 방식 OTP의 동기를 어긋나게 함으로써 정당한 사용자의 로그인을 방해하는 일종의 DoS 공격

2.2 기존 OTP 생성 방법 분석

OTP 생성의 기본적인 원리는 사용자가 OTP 생성매체를 통하여 사용자 고유의 비밀 키(PIN)값을 입력하게 되면 MD5나 MD4 같은 Hash함수를 통하여 암호화를 한 뒤 그것을 이용하여 OTP값을 생성하는 것이다. 이러한 알고리즘에 시간, 이벤트, 질의응답 같은 방식을 추가하여 매번 다른 OTP 값이 생성하도록 한다. 서버와 OTP 생성매체는 항상 동일한 알고리즘을 사용하여 OTP 값을 생성하여야 인증 시에 값이 불일치하여 인증이 실패하는 것을 막을 수 있다. 이와 같이 일 방향성 함수인 Hash 함수를 이용하였기 때문에 암호화된 OTP 값을 다시 원래의 값(PIN값+시간, 이벤트, 질의응답)을 알아내기가 힘들기 때문에 해커로부터 사용자의 정보를 노출당해도 쉽게 암호를 얻기 힘들다는 것이 장점이다.

[그림 1] OTP 생성 방식

OTP의 인증 절차는 사용자가 OTP를 사용하기 위하여 초기 등록을 하게 되면 OTP 서버는 PIN 값(랜덤한 4자리 값)을 사용자에게 전달한다. 전달한 뒤에 서버는 그 PIN 값과 사용자가 OTP를 등록한 시간 값 그리고 현재 시간 값을 사용하여 OTP 값을 생성하고 OTP 생성매체 또한 동일하게 OTP 값을 생성한다. 그런 뒤에 사용자가 OTP 생성매체에 출력되고 있는 OTP 값을 이용하여 서버에 인증 요청을 하게 되면 서버의 OTP 값과 사용자가 입력한 OTP 값을 비교하여 같으면 인증이 성공하게 된다.

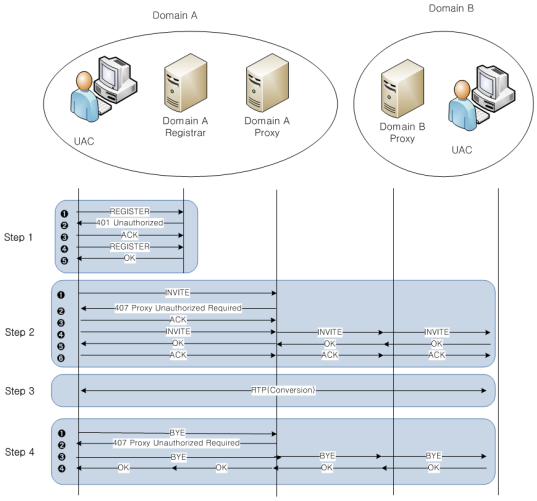


[그림 2] OTP 기반 인증

2.3 응용 서비스 분석 : 인터넷전화 서비스

인터넷전화 서비스를 위한 SIP 프로토콜 세션 설정 및 통신 과정은 사용자가 Proxy 서버에 등록하는 과정부터 시작된다. SIP Proxy 서버는 사용자로부터 호 연결 및 해제 요청을 대행해 주는 역할을 하며 Local Server와 Proxy Server는 물리적으로 동일한 서버에 동작을 한다.

각 사용자와 서버들은 서로의 위치를 알아내기 위해 DNS와 Location Server를 통해 서로의 정확한 위치 정보를 받게 된다. 이를 이용하여 각 사용자들은 처음 Invite를 하는 경우 Location Server를 통해 필요한 상대방의 위치정보를 획득하여 사용자들이 서로 호 설정을 할 수 있도록 도움을 준다.



[그림 3] SIP 등록 및 콜 인증

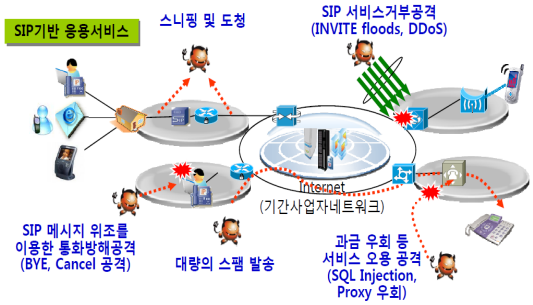
사용자 등록부터 통신을 해지하는 모든 과정은 다음과 같이 종류별로 4단계로 표현할 수 있다.

- 1단계 : 자신을 등록하는 Register 단계

- 2단계 : 다른 사용자와 통화를 하기 위해 Invite를 요청하는 단계와 부가적인 Ringing, Trying, OK, ACK 단계를 통해 호 설정을 하는 단계
- 3단계 : 호 설정 단계들이 마무리가 되면 RTP/RTCP 단계를 통해 사용자간 쌍방향 통신을 하는 단계
- 4단계 : RTP통신 단계를 종료시키고 다시 대기상태로 들어가는 Bye, OK 단계를 거쳐 사용자는 다시 대기 상태로 유지되는 단계

2.4 SIP 보안 취약점 분석

SIP 에서의 공격[6]은 IP 프로토콜 이용하기 때문에 IP프로토콜에서 나타났었던 위협들이 모두 취약점으로 나타나고 있다. SIP 에서의 SIP Message Flooding 공격은 Register Flooding 공격[7]과 Invite, RTP Flooding[7]이 대표적이다.



[그림 4] SIP 보안 취약점

Register Flooding 공격은 공격자의 반복적인 register를 통해 다른 사용자가 서버를 사용하지 못하게끔 과부하를 거는 공격의 형태로, 서버 flooding 공격이 있다. Invite, RTP Flooding 공격은 공격 대상은 SIP 서버, 소프트 스위치, 사용자 단말 및 소프트 폰이며 공격자는 많은 수의 유효한 INVITE 메시지 또는 음성 메시지를 보내어 시스템에 이에 대하여 응답 메시지를 준비하게 함으로써 해당 시스템의 CPU 및 메모리 자원을 고갈시키게 하며 시스템 자원의 고갈로 인하여 서비스의 이용 및 사용하고 있는 모든 사용자의 서비스 지연 또는 마비 현상이 발생한다.

SIP Parser 공격은 Malformed Message공격이 대표적이다. 이는 SIP 헤더와 바디 내용이 일반 문자로 되어 있다는 점을 이용하여 다른 문자들로 삽입, 변조 혹은 삭제하는 것이다. SIP Parser 공격은 정상적인 SIP 패킷에 영문, 공백, 특수기호, 숫자 등을 추가 시켜 SIP 프록시 서버와 사용자의 정상적인 서비스를 방해 한다. 또한 정상적인 호 설정 시 이를 임의로 수정하여 호 설정을 해지하는 DoS공격도 가능하다.

SIP Session Hijacking 공격은 정당한 사용자가 인증을 수행한 후 몰래 세션을 가로채는 보안 공격 기법을 말한다. 이는 주고 받는 모든 패킷들을 간접 모니터링하거나 직접 사용권한을 가로채어 중요자원에 접근하는 것 등을 할 수 있다.

SIP Spoofing 공격은 타인의 시스템 자원에 Access할 목적으로 인터넷 주소, 사용자 ID 등을 날조함으로써 정당한 사용자인 것처럼 보이게 한다거나 승인 받은 사용자인 체하여 시스템에 접근함으로써 추적을 피하는 고급 해킹 기법을 말한다. SIP 환경에서는 공격자는 MITM 공격을 통해 정당한 사용자와 서버사이에서 패킷을 가로채어 SIP 프락시 서버와 사용자들을 속여 악의적인 행위를 한다.

2.4 해결 방안

앞서 SIP 사용자 등록 및 인증, 보안 취약성에 대하여 분석을 하였다. 기존의 SIP 보안기술은 새로운 공격에 즉각 대응하지 못하며, 다양한 공격 도구들을 이용해 공격을 수행할 경우 SIP 보안 문제점이 그대로 노출되었다.

따라서 SIP 프로토콜에 대한 공격은 SIP 프록시 서버와 사용자간의 송수신 되는 메시지에 대한 공격을 통해 이루어지게 된다. 공격자는 SIP 프록시 서버에 송수신되는 SIP 세션 정보에 대한 스니핑과 스푸핑 공격, MITM 등을 수행 할 수 있기 때문에 이에 대한 대응 방안이 제시되어야 한다. 본 연구에서는 이러한 문제점들을 해결하고자 SIP에서 송수된 되는 메시지 및 사용자간의 인증을 강화하기 위하여 바이오메트릭 정보와 OTP 기술을 접목한 B-OTP 방식을 통신 간에 보안 향상을 위한 메커니즘으로 제시하고자 한다.

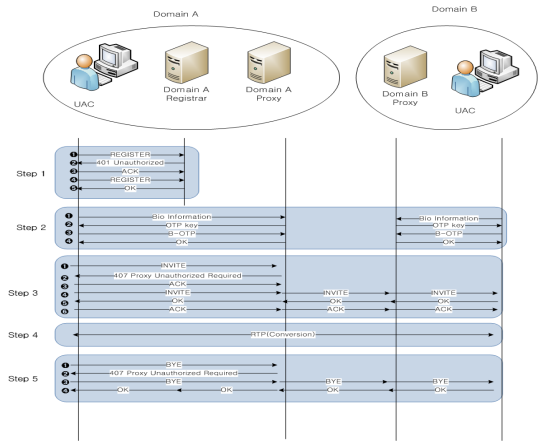
3. 제안하는 B-OTP 생성 기법 및 B-OTP 기반 SIP 인증 시스템 구조

3.1 SIP 등록 및 인증 전체 구조

기존의 SIP 등록 및 콜 인증에 B-OTP 과정을 추가함으로써 UAC 간의 인증이 강화된 통신을 할 수 있다. 본

연구에서 제안한 기법은 B-OTP 기술을 이용한 인증 강화 방식으로 이를 직접 인터넷전화 서비스에 적용하였다.

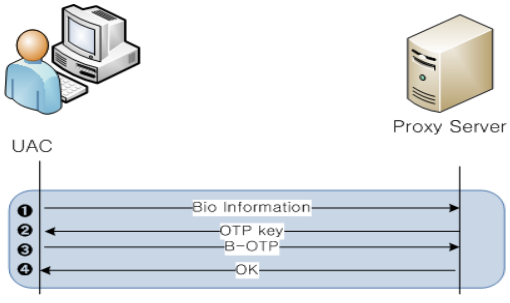
사용자는 최근 널리 보급되고 있는 스마트폰 등에 있는 카메라 장치/모듈을 이용하여 사진/이미지를 캡춰하게 되고 이를 이용하여 서버와의 B-OTP 정보를 생성하게 된다. 카메라 모듈을 통해 획득되는 정보는 각 개인마다 고유한 바이오메트릭 정보에 대한 것으로 예를들어 각 사용자의 얼굴 사진 등을 스마트폰을 이용하여 획득하고 이를 이용하여 B-OTP를 생성하게 된다. 생성된 B-OTP 정보를 이용항 인터넷전화와 같은 서비스에서의 보안성 강화 및 인증 취약점을 보완할 수 있는 방법으로 사용할 수 있게 된다. 본 연구에서 적용한 인터넷전화 서비스 기반 SIP 등록 및 B-OTP 기반 인증 시스템에 대한 전체적인 구조는 다음 그림과 같다.



[그림 5] B-OTP SIP 등록 및 인증 전체 구조

3.2 B-OTP 기반 사용자 인증 구조

구체적으로 B-OTP 인증을 위한 정보 생성 및 절차는 다음과 같다.



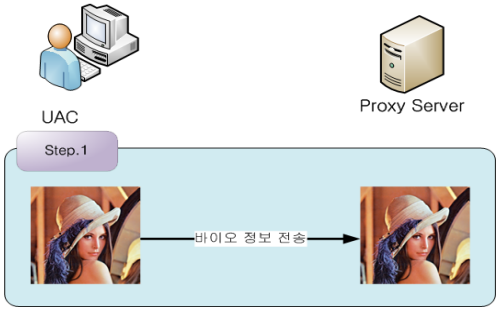
[그림 6] B-OTP 인증

UAC는 자신의 바이오 정보를 서버에게 보내며, 서버는 OTP Key값을 랜덤하게 생성하여 UAC에게 전송한다. UAC는 자신의 바이오 정보와 서버로부터 전송받은 OTP Key값으로부터 B-OTP를 생성한다. 이제 UAC는 생성한 B-OTP값을 다시 서버로 전송한다. 서버도 UAC에서의 B-OTP과정과 동일하게 B-OTP를 생성하며, UAC로부터 받은 B-OTP와 비교한다.

다음은 B-OTP 기반 사용자 인증구조의 세부 단계이다.

1단계, UAC는 바이오 정보를 Proxy 서버로 보내게 된다. 바이오 정보는 사용자 인증을 강화하기 위하여 자신의 얼굴을 이용한다. 이 후, 이 바이오 정보에서 B-OTP 값을 추출하게 됨으로 UAC와 Proxy서버는 바이오 정보를 임시로 보관한다.

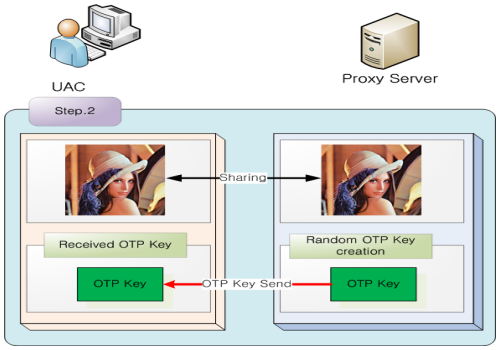
이때 사용되는 사용자의 얼굴 정보는 PC 또는 노트북, 스마트폰 등에 장착된 카메라 모듈 등을 이용하여 각 사용자의 얼굴 이미지 정보를 획득하게 된다. 하지만 본 연구에서 사용한 기법은 획득된 얼굴 이미지에서 얼굴 부위만을 추출/이용하는 것이 아니라, 각 사용자로부터 획득된 이미지를 전송하고 동시에 해당 이미지 내에 있는 랜덤 위치에 있는 이미지 픽셀 정보를 이용하여 B-OTP 정보를 생성하는 방식이다. 아래 그림과 같이 1단계 과정에서 UAC는 서버로 이미지 정보를 전송한다.



[그림 7] B-OTP 인증 1단계

2단계, Proxy 서버는 Random한 OTP Key를 생성한다. OTP Key는 10바이트의 크기로 되어 있으며, 생성된 OTP Key는 UAC로 전송한다. 이 OTP Key는 B-OTP를 추출하기 위한 키로 사용된다.

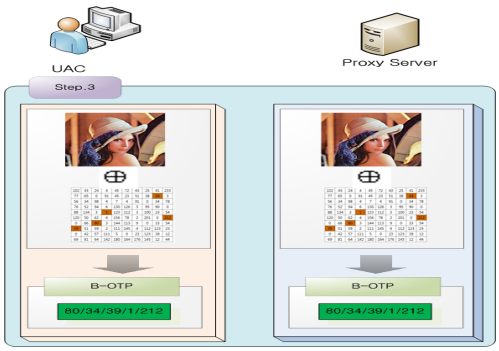
이때 사용하는 Random 함수는 암호학적으로 안전한 랜덤 함수를 사용하며 스마트폰의 키패드 자판에 대한하는 정보를 이용할 수 있도록 고안되었다.



[그림 8] B-OTP 인증 2단계

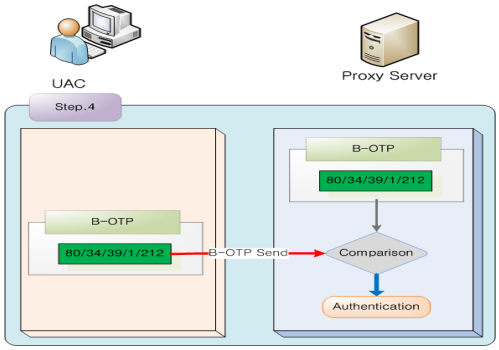
3단계, UAC는 Proxy 서버로부터 받은 Random한 OTP Key와 자신의 바이오 정보를 이용하여 B-OTP 값을 추출하게 된다. 이때, Proxy 서버 또한 UAC와 동일한 과정을 통하여 UAC의 바이오 정보와 생성한 Random OTP Key를 이용하여 B-OTP 값을 추출한다.

UAC는 Proxy Server로부터 받은 OTP Key 값을 이용하여 UAC의 카메라 모듈로부터 획득된 이미지에 대해 B-OTP를 생성하게 된다. OTP Key 값의 정보를 이용하여 이미지내 특정 위치에 대한 픽셀 값을 추출하고 이 정보를 이용하여 B-OTP 정보를 생성하게 된다.



[그림 9] B-OTP 인증 3단계

4단계, B-OTP 값을 추출한 UAC는 Proxy 서버로 B-OTP 값을 전송한다. Proxy 서버는 UAC로부터 전송받은 B-OTP 값과 전 단계에서 생성한 B -OTP 값을 비교한다.



[그림 10] B-OTP 인증 4단계

3.3 B-OTP 기반 OTP Key 구조

B-OTP 인증 과정에서 Proxy 서버가 UAC로 전송하는 OTP Key 생성 과정을 살펴보면 다음과 같다. Proxy 서버는 암호학적으로 안전한 랜덤 함수를 이용하여 매번 다른 배열에 해당하는 OTP Key 값을 생성하게 된다. 그 결과 예를들어 다음과 같은 OTP Key 값을 생성할 수 있다.

[표 1] OTP Key 생성 결과(예시)

원본 키	1	2	3	4	5	6	7	8	9	0
치환 키	2	6	8	1	0	7	3	4	9	5

위의 표에서 서버가 생성한 Random OTP Key값은 2681073495이다. 이 키 값은 UAC에게 보내지며, UAC는 10자리의 이 키를 2개씩 5묶음으로 나눠서 사용한다. 2개의 키는 바이오 정보의 위치 좌표 정보를 의미하며, 그 결과 5개의 위치 값이 나오게 된다. 위치 값을 이용하여 이미지로부터 B-OTP 값을 생성하게 된다.

3.4 B-OTP 위치 값 추출 알고리즘

앞에서 제시한 바와 같이 UAC에서 바이오 정보를 서버로 전송하면 서버는 Random OTP Key 값을 생성한다. 생성된 OTP Key는 UAC로 전송된다. UAC는 Key 값을 가지고 바이오 정보의 위치 값인 B-OTP 값을 추출한다.

다음의 사용자가 카메라 등을 이용하여 캡쳐한 얼굴 이미지에서 OTP Key 값에 해당하는 정보를 추출한 결과이다.

102	43	24	4	45	72	43	25	41	233
77	65	0	91	45	23	51	38	34	3
56	34	98	4	7	4	91	0	34	78
76	52	94	6	130	126	3	95	90	0
88	134	3	1	123	112	3	100	23	54
120	50	62	4	156	78	2	201	0	212
0	66	80	3	144	113	9	0	33	54
39	51	59	2	111	145	4	112	123	23
0	42	57	111	5	0	23	123	39	12
69	81	64	142	180	164	176	145	12	44

[그림 11] B-OTP 추출 알고리즘

이미지에서 B-OTP에 사용될 5개의 픽셀값이 추출되면 이에 대해 기존의 OTP 함수를 적용하여 최종적으로 B-OTP 값을 생성하게 된다.

예를들어 5개의 픽셀에 대한 값 P1 ~ P5에 대해서 전체 값들에 대해 합을 구하고 이를 MOD 연산을 취하여 생성된 값을 전송하는 구조로 알고리즘을 개발할 수 있다.

B-OTP 추출 알고리즘은 UAC와 Proxy 서버에서 수행된다. 1) Proxy 서버가 Random OTP Key 값을 UAC로 전송했을 경우 OTP Key를 저장하고, 2) UAC에서 생성된 B-OTP 값이 Proxy 서버로 송신된다면, Proxy 서버는 B-OTP 값을 검증 하기 위하여 UAC로부터 받은 이미지 정보와 Proxy 서버에서 생성한 Random OTP Key를 이용하여 B-OTP 생성 및 검증 과정을 수행하게 된다. 그 결과 동일한 B-OTP 값이 나오게 되면 인터넷뱅킹 또는 인터넷전화 서비스에 대한 사용자 인증 과정을 통과하게 되고 이후 서비스를 개시하게 된다.

4. 안정성 분석

4.1 메시지 변조 및 MITM 공격에 대한 대응

인터넷뱅킹에서 사용되는 OTP 토큰은 MITM 공격이 가능하다. 하지만 본 연구에서 사용하는 기법인 경우에는 매번 다른 이미지 정보를 UAC가 전송하게 되며 또한 Proxy 서버도 매번 다른 랜덤 OTP Key 값을 생성하여 전송하게 된다. 따라서 기존의 OTP 방식에서 문제가 되는 공격에 대해 보다 강화된 보안성을 제공할 수 있다.

또한 기존의 SIP 프로토콜의 패킷은 텍스트 형식이다. 이는 가장 큰 장점인 동시에 단점이 되어 공격에 쉽게 수정 및 삭제가 된다. 따라서 본 논문에서는 근본적인 INVITE 메시지 변조 및 수정에 대응하기 위하여 B-OTP 방식의 인증을 추가하였다. 메시지 변조는 공격자가 자신의 IP로 패킷을 돌리기 위해 필요한 정보를 수집하거나, 통신 중간에 통신을 끊는 상태정보를 수정 및 삽입하여 정상적인 서비스를 방해하는 것이다. 본 논문에서는 B-OTP 기술을 이용하여 메시지를 변조할 수 있는 INVITE에 대하여 사전에 바이오 정보를 가지고 인증을 함으로써 공격에 대하여 방지할 수 있다.

4.2 메시지 및 사용자 인증

인터넷뱅킹에서 사용하는 OTP 방식과 인터넷전화 기반 SIP 프로토콜에서의 사용자 인증은 필수적인 요소이다. 본 논문에서 제시한 B-OTP 방식 기반 SIP 서비스 구조는 사용자 인증을 강화시켜준다. 자신의 바이오메트릭 정보인 얼굴은 사용자 마다 다르기 때문에 B-OTP 과정을 통해 정상적인 사용자의 여부를 확인하여 효율적으로 인증하게 된다. 따라서 인터넷 기반 서비스에서의 사용자 인증성을 강화할 수 있다.

4.3 제안한 구조의 안정성 분석

정보에 대한 위협이란 허락되지 않은 접근, 수정, 노출, 훼손, 파괴 등이다. 본 논문에서는 기존 인터넷뱅킹에서 사용하는 OTP 방식을 개선하여 인터넷전화에서 사용하는 SIP 프로토콜에 적용하여 SIP 등록 및 인증을 강화하기 위한 구조를 제안하였다. 기밀성이란 허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 본 논문에서는 B-OTP 기반 SIP 통신 과정에서 바이오 정보를 이용한 인증과정을 추가하여 인가되지 않은 사용자의 접근이 불가능 하다. 따라서 인가되지 않은 사용자 또는 객체가 정보를 수정할 수 없도록 하는 무결성 또한 정상적인 사용자만이 접근이 가능함으로 보장된다. 가용성 보장 및 인증도 바이오 정보를 이용함으로 인해 통신 전 정상적인 사용자를 판별할 수 있으며, 따라서 UAC 간의 SIP 통신 사이에 접근이 가능하지 않다.

5. 결론

현재 인터넷 뱅킹에서 사용하고 있는 보안카드 방식만으로는 급증하고 있는 보안 사고에 효율적인 대응이 어렵게 되었으며 SIP 기반 인터넷전화 서비스 역시 사용자 인증의 취약점을 이용한 공격이 가능하여 이에 대한

대응 방안이 필요하다. 또한 SIP 기반 인터넷 전화는 급속도로 사용자가 증가하고 있는 추세이지만 사용자 인증에 대한 취약성을 악용한 공격 시나리오 등이 제시되고 있다.

IP 프로토콜 기반의 인터넷 전화 서비스는 기본적으로 IP망에서 발생 가능한 보안 위협이 내재되어 있다. 특히 공중전화망과 유무선 인터넷의 연동이 가능한 인터넷 전화 서비스의 피해 파급은 단일 망을 넘어서 통합망에 이르기까지 피해가 확산될 수 있으며 음성 패킷의 전달은 Agent 간 전화 서비스라는 점에서 통화 내용이 불법적으로 노출 되는 것을 방지해야 한다.

따라서 본 논문에서는 기존의 문제점들을 해결하기 위하여 UAC로부터 바이오메트릭 정보를 이미지 형태로 전송하고 Proxy 서버가 생성한 OTP Key 값을 이용하여 B-OTP 정보를 매번 다르게 생성하여 인증 과정에 적용하였다. 기존 SIP 등록 및 인증에서 사용자 인증이 강화된 바이오 정보를 이용한 단계를 추가함으로써 인터넷뱅킹, 인터넷전화 서비스에서 발견되는 인증 문제점을 개선할 수 있었다.

참 고 문 헌

[1] 한국전자통신연구원(ETRI), “VoIP 기술 및 시장 동향”, 기술평가팀 P.4-13, P.19-45, 2006

[2] http://www.voip-forum.or.kr, VoIP 국내표준, “H.323 기반 인터넷 텔레포니 단말”, 2005.12

[3] http://www.voip-forum.or.kr, VoIP 국내표준, “SIP 기반 인터넷 텔레포니 단말”, 2005.12

[4] 최동현, 김승주, 원동호, “일회용 패스워드(OTP: One-Time password)기술 분석 및 표준화 동향”, 한국정보보호학회지), Vol.17, No.3, pp12-17, 2007.

[5] 김기영, “일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰”, 한국정보보호학회지, Vo1.17, No.3, pp26-13, 2007

[6] Mark Collier, "VoIP Vulnerabilities Registration Hijacking", SecureLogix Corporation, P.1-4, 2005.1

[7] 김지훈, “VoIP 보안 위협”, ASEC, 2008

저 자 소 개

장 원 준 (Won-Jun Jang) [정회원]

- 2010년 2월 : 한신대학교 정보시스템공학과 졸업
- 2010년 2월 ~ 현재 : 한신대학교 일반대학원 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 스마트폰 보안

이 형 우 (Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 전산과학과 졸업
- 1996년 2월 : 고려대학교 일반대학원 전산과학과 석사
- 1999년 2월 : 고려대학교 일반대학원 전산과학과 박사
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 부교수

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 바이오정보보호