情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

전자 금융 거래 환경의 인증 기술 동향 분석*

임 형 진*, 심 희 원**, 서 승 현***, 강 우 진****

요 약

인터넷의 보편화와 사용자 증가는 현실 생활들의 대부분에 활동을 인터넷에서 가능토록하고 있다. 특히, 인터넷 뱅킹은 자금이 전자적으로 이동하는 중요 행위로서, 지속적으로 증가하는 보안위협으로부터 대응하기 위해 수많은 인증방법이 고안되어 사용되고 있다. 인터넷 뱅킹의 전체적인 보안성을 향상하기 위해서 사용자 인증 방법으로부터, 안전한 전송방법에 이르기까지 다양한 보안 솔루션들이 종단간 유기적으로 구성되어 제공되고 있다. 본 논문에서는 이러한 기술들 중 국내외에서 사용되는 다양한 인증 기법들을 조사하여 분석하고, 지속적으로 증가하는 보안위협에 효과적으로 대응할 수 있는 대응 기술에 대한 사례를 제시한다.

I. 서 론

전 세계적으로 많은 은행들이 자신의 고객들에게 인터넷 뱅킹을 서비스하고 있다. 이러한 서비스들에서 다루어지는 정보에 대한 안전한 보호는 국가별로 서로 다른 기술 및 방식을 사용하여 제공하고 있다. 이처럼 인터넷 뱅킹의 보안성 향상을 위한 공통적인 기술은 존재하지 않지만, 전 세계적으로 개별 표준 및 기술에 의해 안전하게 유지되고 있다. PCI DSS(Payment Card Industry Data Security Standard)는 지불 결재를 위한 전 세계적인 표준으로 안전한 지불결재를 위한 요구사항을 정의하고 있으며[1], 인터넷 뱅킹 분야에서도 여러 정부에서는 자국에 사용될 가이드라인을 제시하고 있다. 미국의 경우 통화감독청(Office of the Comptroller of the Currency, OCC)에 의해 제시되는 인터넷 뱅킹 가이드라인[2], 미국 연방금융회사검사위원회(Federal Financial Institutions Examination Council, FFIEC)에 의해 제공되는 인터넷 뱅킹의 인증 시스템에 대한 가이드라인[3], 연방통상위원회(Federal Trade Commission, FTC)에 의해 제시되는 규정[4] 등이 존재한다.

국내에서는 금융감독원에 의해 1999년 최초로 인터넷 뱅킹 서비스에 대한 보안성 승인으로부터 시작하여, 2008년 현재까지 관련 기술이 비약적으로 발전해 왔다. 특히, 인터넷 뱅킹에 공인인증서를 적용하였으며, 이후 보안카드를 통해 본인만이 전자금융을 사용할 수 있도록 하는 보안책이 실시되어, 전자금융가입자의 인증이 매우 강력하게 되었다. 하지만 하드디스크 등에 저장되는 공인인증서를 타인이 사용할 수 있는 가능성이 제기되었으며, 이에 따라 전자금융 안정성 보안대책이 실시되었다[5].

사용자가 은행에 접속하여 안전한 금융거래를 수행하기까지는 사용자가 소지한 인증매체의 형태, 사용자의 컴퓨터, 전송 구간 등에 필요한 다양한 보안 요구사항들이 존재한다[6]. 이러한 보안 요구사항이 적정한 수준에 도달하기 위한 시발점으로서 안전한 사용자 인증 방안의 수립은 전체 보안 시스템의 안정성을 향상시키는데 중요한 역할을 한다[7]. 앞서 언급하였듯이 국내뿐만 아니라 해외에서도 다양한 인증 방식을 사용하여 인터넷뱅킹 즉 전자금융을 이용하는 고객의 정보와 자산을 보호하는 다양한 시도들이 존재하고 있다.

본 논문에서는 현재 국내외에서 사용되고 있는 다양

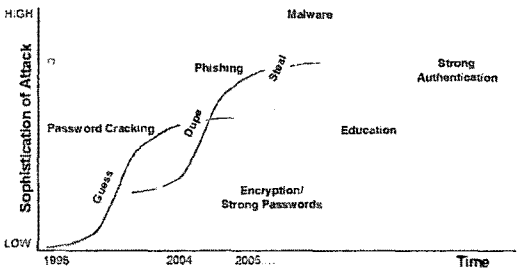
* 금융보안연구원 인증관리팀 (hjlim@fsa.or.kr)
** 금융보안연구원 인증관리팀 (hwshim@fsa.or.kr)
*** 금융보안연구원 인증관리팀 (seosh@fsa.or.kr)
**** 금융보안연구원 인증관리팀 (hanull@fsa.or.kr)

한 사용자 인증 방식에 대해 조사 분석하고자 한다. 2절에서는 사용자 인증 단계에서 나타날 수 있는 보안 취약성 및 가능한 보안 위협을 살펴본다. 3절에서는 현재 사용되고 있는 다양한 인증 기술들을 분류하고, 각 인증 방식의 특성을 살펴본다. 또한, 현재 사용되고 있는 다양한 인증 방식을 특성에 따라 분류한다. 4절과 5절에서는 인증 기술에 대한 비교 분석과 알려진 보안 취약성에 효과적으로 대응할 수 있는 대응 기법들을 살펴보고 6절에서 결론을 제시한다.

Ⅱ. 인증 기술에 대한 보안 위협

[그림 1]에서는 사용자 인증 기술에 대한 공격방식의 발전과 이에 대한 대응 기술의 진화과정을 나타내고 있다. 단순히 정당한 사용자인 것을 위장하기 위해 타인의 패스워드를 사용하는 것으로부터 네트워크 스니핑에 의한 패스워드 탈취, 메모리로부터 패스워드 탈취와 같은 정교한 공격에 이르기까지 공격기법의 다양화는 관련 인증 기술의 진화를 불러왔다[8-10].

[표 1]은 사용자 인증 단계에서의 다양한 공격방식



〔그림 1〕 정교한 공격방식의 증가와 관련 대응 기술[9]

〔표 1〕 인증 기술 공격 방식[12]

공격방식	내 용
사용자 위장 공격	사용자가 고의로 자신의 인증키나, 일련의 인증 이벤트들을 거부하도록 컴퓨팅 환경을 취약하게 만드는 공격방식에 해당
도청 공격	공격자가 인증 목적으로 사용하기 위해 인증 과정으로부터 인증키 값들과 같은 데이터 정보를 얻는 공격방식에 해당
내부자 공격	인증시스템 혹은 시스템 관리자가 고의로 인증 시스템을 취약하게 만들거나 관련 데이터나 인증키들을 탈취하는 공격방식에 해당
키로거 공격	사용자에 의해 타이핑하는 패스워드나 인증키 정보등을 탈취하기 위한 목적으로 사용자의 키스트로크를 캡쳐하는 악의적인 코드나 하드웨어 공격. 스크린 로거 공격(screen logger attacks)들은 스크린에 의존하는 보안기술을 사용하는 환경에서 키스트로크를 캡쳐하는 변종공격에 해당
악의적 코드 공격	공격은 일반적으로 사용자의 컴퓨팅 환경을 목표로 하며, 단순한 키로거로부터 사용자 컴퓨터의 제어권을 탈취하는 정교한 트로이안 목마 프로그램들과 같이 다양하다. 악의적인 코드 공격은 인증서버를 목표로 할 수도 있음
중간자 공격 (Man-in-the-middle attacks)	공격자가 인증절차 과정에서 인증서버와 사용자 사이에 끼어들어 사용자 대신 인증 서버로 인증을 시도하며, 사용자에게는 인증서버로서 위장하여 인증 데이터를 가로채는 공격 형태에 해당
패스워드 추측 공격	패스워드를 추측하기 위한 공격방식으로서 brute force, common password, dictionary 공격과 같은 다양한 변형들이 존재한다. 공격자는 특정 사용자의 패스워드를 추측하려고 시도할 수 있음
피싱 공격	공격자는 사용자의 패스워드나 다른 민감한 정보들을 노출할 수 있도록 사용자를 속이는 공격방식으로서 다른 통신채널, 위조된 웹 페이지, e메일을 사용하는 일종의 사회공학적 공격방식에 해당
재전송 공격	공격자가 성공적인 인증 데이터를 기록하고 인증서버로 거짓으로 인증을 시도하기 위해 이 정보를 재전송하는 공격 형태에 해당
세션탈취 공격	공격자는 성공적인 인증을 수행한 세션을 가로채(hijacks)는 공격 형태
훔쳐보기 공격 (Shoulder surfing attacks)	사용자가 패스워드를 입력할 때 은밀히 패스워드를 관찰하는 사회공학적 공격방식의 한 형태
사회공학적 공격	안전하지 않은 인증 프로토콜을 사용하는 사용자를 속임으로서 인증키와 관련 데이터를 얻는 것을 목표로 하는 공격이나, 악의적인 코드를 사용자의 컴퓨터에 삽입하는 공격형태에 해당 (한 예로 공격자는 사용자 정보를 캐내기 위해 헬프데스크 직원을 속이려 하는 시도 등)
검증자 위장 공격	공격자는 인증키와 관련 데이터를 얻기 위해 사용자에게 인증서버로 인식하고 동작 하도록 속이는 공격 형태로서 인증 서버로 사용자가 인증 정보를 입력하도록 유도하는 공격형태에 해당

들을 나타내고 있으며 여기서 기술되는 대부분의 공격 방식들은 공격자들이 구현하는데 충분히 쉽고 이미 존재하는 멀웨어(malware)에 의해 실행되는 것이 가능하다[11]. 여기에는 초기 등록과정에서의 공격과 인증키 관리에 대한 공격은 포함되지 않는다. 여기서 제시되는 공격 방식들이 모든 방식을 포함하지 않더라도 현재 인증 방식에 대한 가능한 공격들을 나타내고 있다. 특히 훔쳐보기(shoulder surfing) 공격은 사회 공학적 공격 방식에 해당하기 때문에 아래 나열되는 공격 방식들이 반드시 서로 각기 다른 방식에 해당하지 않는다.

최근의 정교한 공격은 사용자 컴퓨터에 사용자 정보를 탈취할 수 있는 악의적인 프로그램을 통해서 시도된다는 것이며, 원격에서 사용자의 컴퓨터로부터 정보를 탈취하는 것이 아니라 직접 사용자의 컴퓨터에 악의적인 프로그램을 구동시켜 실시간으로 사용자 입력 정보를 갈취 및 변경한다는 것이다. 이러한 공격은 [표 1]에서 나타내는 바와 같이 악의적 목적을 위해 다양한 공격 방식을 조합하여 최종 공격 목표를 성취해 낸다[8,12,13]. 예를 들어 사용자의 인증 정보를 탈취하기 위해서 사용자에게 전송된 e메일에 첨부된 악의적 파일을 이용해 해킹하고자하는 목적을 가진다면, 속임(deception), 이메일 첨부(email attachment), 다운로드 구동(drive-by downloads), 해킹(hacking), 키보드로깅(keyboard logging)과 같은 공격 방식들을 조합하여 사용자의 인증정보 탈취 및 거래 트랜잭션을 위변조할 수 있게 된다[6]. 그러므로 사용되는 인증 방식에 상관없이 멀웨어는 사용자나 은행이 알아채지 못하게 공격자의 계좌정보로 결재 트랜잭션을 변경할 수 있다. 비록 전자서명된 트랜잭션이라고 하더라도 멀웨어가 데이터 자체를 서명할 수 있어 여전히 취약점이 존재한다고 할 수 있다.

더욱이, 악의적 소프트웨어에 대한 대응을 위해 안티 멀웨어 솔루션들이 존재한다고 해도 전혀 감염되지 않는 시스템을 보장하는 것은 불가능하다.

Ⅲ. 사용자 인증 기술

3.1. 멀티팩터 인증

본 절에서는 멀티팩터 관점에서 사용자 인증기술을 살펴보고자 한다. 인증을 위해 사용되는 속성에 따라 인증 타입을 분류 할 수 있으며 이러한 타입의 조합 수

	속성예	사용례	분류
알고 있는 것 (Something Know)	패스워드 	PC, 네트워크 접속	타입1
지니고 있는 것 (SomethingOwned)	열쇠 	출입통제	타입2
신체의 일부 (Something Inherent)	지문 	플래쉬 메모리 접근제어	타입3

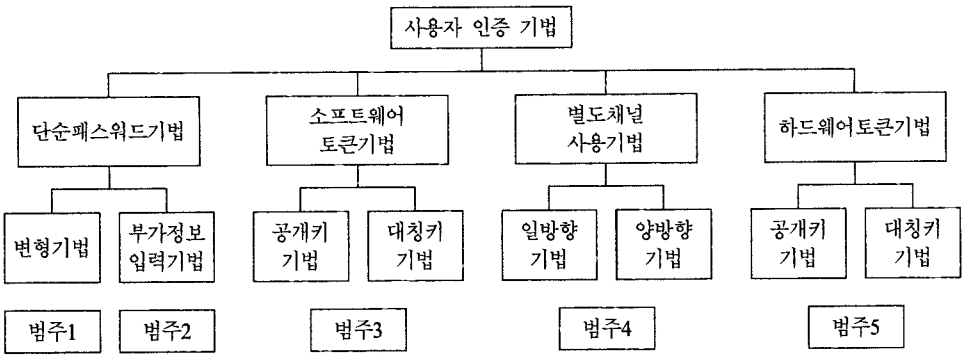
〔그림 2〕 인증 팩터 분류

준에 따라 멀티팩터 타입으로 정의할 수 있다. 인증 타입으로는 [그림 2]에서 나타나는 바와 같이 '알고 있는 것'(something known), '지니고 있는 것'(something owned), '신체의 일부'(something inherent)으로 분류된다[14]. 단순 인증 방식은 세 가지 형태중 하나의 특징을 가지는 방식을 사용하는 것을 의미한다. 그림 오른쪽에는 인증 수단에 따라 분류된 인증 방식의 타입을 나타내고 있으며, 각 타입의 특성은 독립적인 차별성을 갖는다.

일반적으로 같은 타입의 팩터는 본질적으로 공통적으로 취약한 부분을 가지고 있다. 따라서 같은 타입의 두 개 팩터의 사용은 같은 취약성을 공유하게 된다. 인증 방식의 다중 팩터 결합은 각 단일 인증 기법들 간의 장점을 결합한 것으로 좀 더 다양한 공격에 대응하여 강한 인증 타입을 구성할 수 있도록 한다. 일반적으로 이러한 인증 방식을 2팩터 인증 혹은 3팩터 인증이라 불리며, 이러한 인증 방식을 멀티팩터 인증이라고 칭한다. 2팩터 방식이란 서로 다른 타입의 인증 방식이 결합된 경우를 말하며, 일반적으로 사용되는 2 팩터 인증의 예는 알고 있는 속성으로서 PIN(Personal Information Number)과 지니고 있는 속성으로서 토큰을 함께 사용하는 것을 의미한다.

3.2. 사용자 인증 방식 분류

본 절에서는 인터넷 뱅킹에 사용되는 다양한 인증 기법들을 분류하고자한다. 전통적인 사용자 인증 방식으로 대부분의 컴퓨터 시스템에서는 사용자 인증 방식으로 ID/패스워드 방식을 사용한다. 단지 사용자만이 알고 있는 복잡한 값 및 문자의 조합 혹은 단어를 키보드를 사용하여 ID/패스워드 형태로 입력하고 서버에서



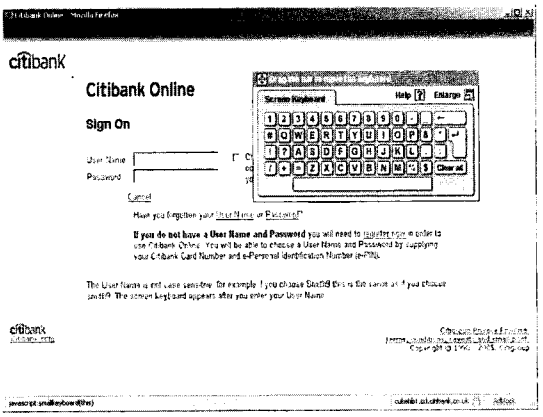
〔그림 3〕 인증 기법의 분류

이 값을 검증하는 방식이다. 그러나 단순한 피싱 공격이나 키로거에 취약하기 때문에, 기본적으로 단순 패스워드 방식을 중심으로 다양한 인증 방식들을 결합하거나 확장하여 사용할 수 있다. [그림 3]은 사용자 인증 기법을 5가지 범주로 분류하고 있으며, 이는 일반적이고 공통적으로 사용되는 기법들을 분류한 것이며, 이들에 기반한 다양한 변형들이 존재 할 수 있다. 범주1은 ID/패스워드의 방식을 변형하는 기법이며, 범주2는 ID/패스워드 이외에 부가정보를 입력하는 인증방식을 말한다. 범주 4는 인증 정보의 검증 및 전송을 위하여 별도의 통신채널을 활용하는 방식이며, 범주 3과 5는 암호 속성을 이용하여 인증 강도를 향상하는 방안에 해당한다. 다음 절에서 언급될 사용자 인증 기법의 5가지 분류 범주에 속하는 방식들은 다양한 변형과 혼합 방식이 존재한다.

3.2.1 아이디/패스워드 기법의 변형

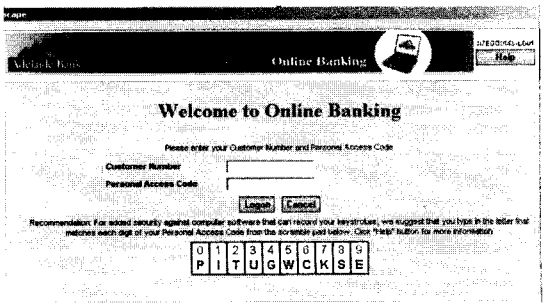
이 방식은 특정 기술이라기보다는 일반적인 패스워드 인증을 변형한 형태에 해당한다[15,16].

① 가상키패드(Virtual Keypads)
사용자는 그래픽 이미지로 표현되는 가상 키패드를 사용하여 요구되는 비밀값을 마우스로 클릭하여 입력하는 방식으로 일부 방식에서는 임의조합으로 구성된 키패드를 사용하는 경우도 있다. [그림 4]는 대표적인 사용례를 보여주고 있다. 특정 응용들에서는 패스워드를 구성하는 일부 문자들만 포함하도록 키패드를 구성하거나 문자 위치에 그래픽 아이콘을 보여주는 경우도 있다.



〔그림 4〕 가상 키보드 방식

② 스크램블패드(Scramble Pads)
[그림 5]에서는 로긴 화면에 문자들을 랜덤한 숫자들에 할당한 스크램블 패드를 보여주고 있다. 숫자 패스워드를 할당하기 보다는 스크램블 패드로부터 해당 문자를 입력한다. 은행의 웹서버에서는 이를 숫자 패스워드로 변환하여 단순 패스워드 방식처럼 검증한다. 사용자 ID(user name)도 같은 방식으로 입력될 수 있다.



〔그림 5〕 스크램블패드

③ 부분패스워드(Partial Password)

이 방식은 사용자가 기억하는 패스워드의 모든 정보를 입력하지 않고, 일부분을 입력하는 방법이다. 부분 패스워드 추출을 위한 별도의 지시번호를 서버로부터 챌린지 형태로 제시받거나, 기억하고 있는 PIN번호를 사용하여 제시되는 문자열 중 특정 문자를 입력하는 형태에 해당한다. 한 예로서 "자신의 패스워드 중 3번째, 6번째, 1번째 문자를 입력하시요"와 같은 일종의 챌리지 값에 대해서 자신이 알고 있는 패스워드의 해당 문자만을 입력하게 된다.

이 방식은 전체 패스워드가 키보드로 직접 입력되지 않기 때문에 단순한 스파이웨어(key loggers)나 피싱 공격에 덜 취약하다. 유럽의 일부 은행의 경우는 키로거 공격을 막기 위해 명시적으로 부분 패스워드 전송(partial password)방식을 구현하여 단순 패스워드 방식의 보안성향상을 고려하고 있다.

3.2.2 부가정보 요구 기법

이 범주에 포함되는 인증방식들은 ID/패스워드이외에 부가정보로서 특정 오브젝트(문자, 이미지등)를 사용자가 확인 후 인증하거나 로긴시 여러 질문들에 응답을 해야 로그인이 가능하다. 이 방식은 사전에 등록한 ID/패스워드를 입력하는 것이 아닌 사전에 협의된 질의문구나 특정 오브젝트를 확인하는 방식이다. 이러한 범주의 방식들은 사용자 전용의 이미지를 사용하거나 윈도우 패드락에 특정 이미지를 나타내는 방식이 있으며 사용자 인증방식에 사이트 인증을 부가하기 위해 사용한다[17,18].

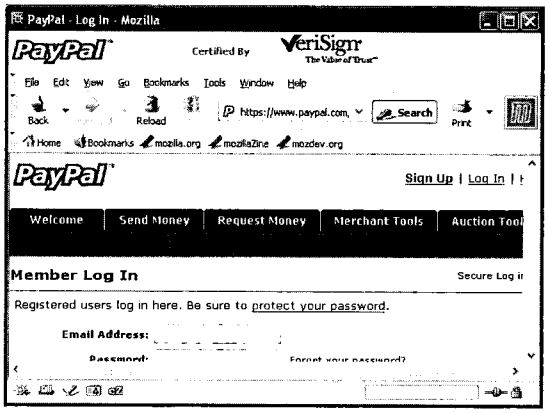
① 사전 등록된 질의응답방식

이 방식은 사용자가 사전에 등록된 질의/응답에 대하여 로그인시 질의 내용이 요구될 때 응답하는 방식으로 고정된 챌린지(challenge)/리스폰스(response) 형태의 인증방식에 해당한다. 이와 유사한 방식으로 은행에 이미 알려진 최근 거래 내역과 같은 사용자 정보를 이용하는 방식도 있으며 이는 텔레뱅킹시 신원을 검증하기 위해 사용자 정보를 확인하는 것과 동일한 방식이다. 이러한 인증 방식의 유사한 사례로서 인터넷 포탈 사이트에서 아이디 가입시 개인정보에 대한 질문을 선택하고 대답을 저장해두는 형태가 해당되며, 전화 고객센터에서 사용자 본인 확인수단으로 사용되는 경우도 있다.

② 패드락 및 트러스트바 사용 방식

이 방식은 브라우저가 방문 웹 사이트들의 히스토리를 유지하고 새로운 사이트로 방문하였을 경우 사용자에게 그래픽하게 알려주는 방식으로 Markham[21]등에 의해 제안된 방식으로 [그림 6.a]의 상단에 나타내고 있다. 새로운 방문 사이트 경우 그림에서와 같이 그래픽하게 표현해 준다. [그림 6.b]의 하단은 Amir Herzberg에 의해 제안된 웹사이트에 대한 정보를 비쥬얼하게 브라우저에서 보여주는 트러스트바라는 툴을 설치하여 사용할 수 있으며 사용자는 로그인시 이러한 정보를 확인한 후 거래를 실행할 수 있다[21]. 이 경우 트러스트바는 해당 웹사이트를 인증하는 인증권한 기관(Certification Authority, CA)의 로고와 해당 웹사이트의 로고를 나타내준다.

a. 윈도우 패드락 이용방식

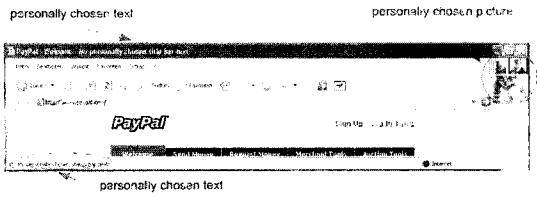


b. 트러스트 바 사용방식

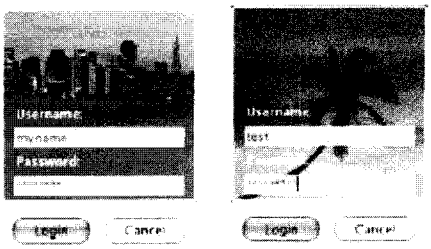
〔그림 6〕 특정 오브젝트 이용방식

③ 개인화 이미지 및 텍스트 사용 방식

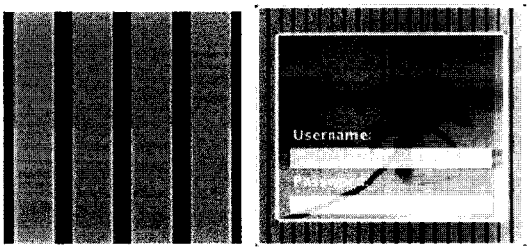
Tieyan Li는 [그림 7]와 같이 개인화된 이미지 및 텍스트를 적용한 브라우저를 이용해 서버 및 사용자를 인증하는 방안을 제안하고 있다[19]. [그림7.a] 경우는 개인이 선택한 텍스트와 이미지가



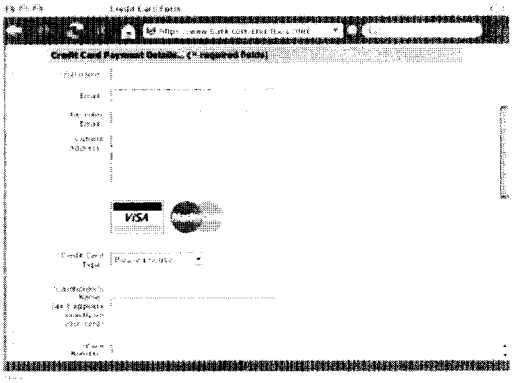
a. 개인화 이미지 및 텍스트 이용한 방식



b. 백그라운드 이미지를 사용하는 트러스트 윈도우



c. 해쉬 트러스트 윈도우와 이미지 사용방식



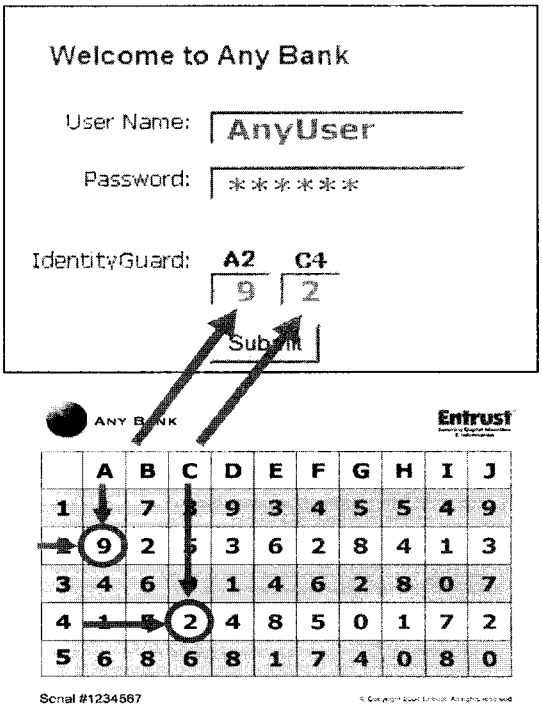
d. 인증된 웹사이트를 해쉬 트러스트 이미지로 표현하는 방식

〔그림 7〕 개인화 이미지 및 텍스트 활용방식

사용자의 브라우저에 나타나는 방식을 나타내고 있다. [그림 7.b]의 경우는 사용자가 선택한 특정 이미지가 로그인 박스에 나타나는 방식으로 스푸핑을 방지하고자 하는 목적으로 사용되고 있다[23]. [그림 7.c]의 경우는 사용자가 처음 로그인 시 랜덤하게 비쥬얼(visual) 해쉬가 생성되며 은행 거래시 서버로부터 전송되는 웹페이지에 계속 적용된다. [그림 7.d]는 이를 적용한 웹 화면을 나타내고 있다.

④ 그리드(Grid)카드 방식

[그림 8]에서 보여주는 바와 같이 사용자는 일련의 숫자가 기입된 카드형태의 토큰을 소지하고 매 거래시마다 순서대로 해당 숫자를 입력하는 방식이다. 국내에서는 보안카드라 명칭되며, 매 거래시 카드의 숫자를 조합하여 입력하는 방식이다. 상대적으로 적은 비용을 가지지만 보안카드로 생성할 수 있는 숫자 조합이 한정되어 있고, 분실 및 악의적 도용의 문제가 있다. 특히 국내에서 이 방식은 로긴시 사용자 인증 수단보다는 거래 인증 목적으로 사용된다.



〔그림 8〕 그리드(보안)카드 방식

3.2.3 소프트웨어 토큰 방식

이 범주의 인증 방식은 키의 암호 속성을 이용하여 사용자 인증을 수행하는 방법으로 사용자 컴퓨터에 특정 소프트웨어를 설치하여 사용한다. 일반적으로 소프트웨어 토큰이라고 칭하며 인증에 사용되는 키의 속성은 대칭키와 비대칭키 방식으로 구분된다.

① 대칭키 방식

이 방식은 통신하는 양자 간에 동일한 키를 분배하고 키로 암호화 또는 메시지 인증 코드(MAC) 연산을 수행하여 인증하는 방식이다. 대표적인 대칭키 인증 방식으로 원타임 패스워드(One Time Password, OTP)가 해당한다. OTP의 경우 전통적인 아이디/패스워드 방식의 고정된 패스워드를 분배된 키와 OTP생성 알고리즘을 사용하여 매번 바꾸어 인증정보의 가로챔 및 재사용 공격을 방지하고 있다[25].

소프트웨어 토큰 방식의 OTP는 사용자 컴퓨터 및 이동 단말(phone, PDA등)에 OTP 생성용 소프트웨어를 다운로드하여 사용하는 방식을 의미하며 하드웨어 토큰 방식과 기능은 동일하다. 사용자가 OTP기반의 인증을 하고자 할 때 설치된 OTP 소프트웨어로부터 생성된 비밀값을 이용해 웹브라우저에 입력한다. 사용자가 입력한 아이디/패스워드와 OTP가 인증 서버로 전달되며, 인증 서버는 OTP를 검증한다.

② 비대칭키(=공개키) 방식

비대칭키 기반의 사용자 인증은 통신하고자 하는 양측이 개인키와 공개키 쌍을 분배하고 자신의 개인키로 서명하여 전송하면 공개키로 전송 내용을 확인하는 형태로 사용된다. 대표적인 방식으로는 공인인증서 방식이 있으며, 국내의 경우 전자서명법에 의해 본인 확인 수단으로서의 법적 효력을 가진다[24].

또한 비대칭키는 전자서명을 통해 트랜잭션에 대한 인증에 사용될 수 있다. 사용자는 컴퓨터에 저장된 자신의 개인키를 이용하여 트랜잭션에 서명하고, 응답자(예; 은행서버)는 공개 디렉토리 등에 저장된 사용자의 인증서를 이용하여, 거래 내용에 대해 검증할 수 있기 때문에 안전하게 전자거래를 수행할 수 있다.

3.2.4 별도 채널 사용 방식

별도 채널 사용방식은 일반적으로 사용자가 유선 단말을 사용하여 웹브라우저 접속을 통해 인터넷 거래를 실행할 때 별도의 채널로서 다른 인터넷 응용 또는 유무선 전화를 통해 인증과정에 이용하는 방식에 해당한다.

① 일방향 방식

일방향 방식의 별도 채널 사용방식은 사용자가 인증을 위해 현재 연결된 채널에 아이디/패스워드를 입력하고 자신의 이동 통신 단말이나 다른 응용 프로그램으로 일회용 비밀번호를 문자메시지 형태로 수신한 후 브라우저에 입력하는 방식이다. 따라서 인증 서버로부터 일방향으로 인증 정보를 구성하는 데이터가 별도의 채널을 통해 사용자에게로 전송 되기만 한다. 일부 벤더들은 다음 로긴을 위해 일회용 비밀번호 값을 미리 전송하는 경우도 있다. 이러한 범주의 다른 형태로서 e메일에 의해 인증 확인 정보를 인증 요청자에게 전송하는 경우도 있으며 이들은 모두 인증을 위해 별도의 일방향 채널을 사용하는 방식에 해당한다.

② 양방향 방식

양방향 방식은 일방향 방식과 비교할 때 별도의 채널로 특정 비밀값을 수신만하기보다는 현재 거래 요청에 대한 내용을 확인 및 응답하는 방식을 주로 사용한다. 즉, 이동 전화 혹은 음성전화를 통해 사용자가 자신의 거래 내역을 확인후 그 결과를 응답해야 거래가 진행될 수 있다.

이 방식은 "click and ring"방식으로 불리며 거래 시도 후 응답이 즉각적으로 이루어져야 한다. 음성 전화망은 여러 인증방식들과 통합될 수 있다. 대부분의 공통적인 구현으로 SMS OTP와 병행하여 사용되기도 하며, 거래내역에 대한 확인이 자동화된 음성 메시지(voice call)를 통해 요구될 수 있다. 이 방식은 사용자가 거래 실행 전에 자신의 거래 내역을 전화를 통해 확인과정을 거친 후에라야 거래가 진행될 수 있다.

3.2.5 하드웨어 토큰 방식

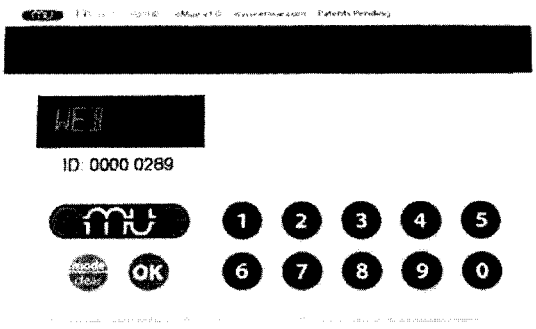
소프트웨어 토큰과 비교할 때 이 방식은 인증에 사

용되는 정보를 저장하는 별도의 장치를 사용하며 하드웨어 토큰 방식으로 분류한다. 이러한 토큰들은 정보를 저장할 수 있는 컴퓨터 칩을 내장하는 경우도 존재하며 기본적인 컴퓨터 기능을 수행할 수 있다. 일반적으로 스마트 카드나 USB형태의 토큰이 존재하며, 스마트 카드 형태의 경우는 신용 카드 크기의 장치를 의미한다. 이러한 하드웨어 토큰들은 민감한 데이터를 보호하기 위해 PIN에 의해 제어될 수 있으며, 특별히 스마트카드 형태의 장치들은 이 장치를 읽어 낼 수 있는 전용 리더기를 필요로 한다. 또한 사용되는 키 방식에 상관없이 토큰 자체에 디스플레이 기능과 키 패드를 포함하는 경우도 있다[12].

① 대칭키 방식

하드웨어 토큰 기반의 OTP 경우는 카드형 및 일반 토큰형 등 다양한 형태가 존재하며, 해당 토큰에서 OTP 값을 생성하며, 사용자는 이를 웹브라우저에 입력하여 사용하게 된다.

스마트 카드와 결합된 OTP토큰은 생성된 일회용 비밀 값을 디스플레이하는 소형 리더기와 함께 사용하는 방식이 존재하며, 최근에는 [그림 9]와 같이 카드 자체에 디스플레이 화면과 키패드를 내장한 토큰도 개발되고 있다.



[그림 9] 핀패드를 내장한 카드형 OTP토큰

② 비대칭키 방식

공개키 기반의 하드웨어 토큰 방식은 크게 소형 리더기를 요구하는 스마트카드 형태나 USB를 소유하고 결재시 전자서명에 이용할 수 있다. 국내 전자 금융 거래시 공인인증서 저장매체로서 보안하드웨어모듈(Hardware Security Module, HSM)을 거래등급 1등급으로 지정하고 있다. 공인인증서를 저장한 스마트 토큰이나 HSM방식은 PC에 저장된 공인인증서의 유출 가능성을 줄일 수 있어 소프트웨어 토큰 방식에 비해 더 안전하고, 이동성도 편리하다. 대부분의 공개키 방식의 하드웨어 토큰은 OTP 토큰에 비해 상대적으로 높은 비용이 요구된다.

Ⅳ. 사용자 인증 기술의 분석

4.1. 보안 위협에 대한 가정

올해 초 시만텍에서는 2팩터 인증을 사용하는 금융거래를 공격하여 정보를 갈취하는 새로운 형태의 멀웨어를 발견하였음을 발표하였다. 이 트로이안(Trojan) 멀웨어의 특징은 프로그램을 다운로드하는 Downloader. Silentbank를 사용자 PC로 설치하고 거래정보 탈취 및 변경을 시도하는 Trojan.Silentbank를 다시 다운로드하는 방식을 사용한다[26]. PC에 설치된 멀웨어는 사용자가 금융 거래를 하는 동안 사용자의 계좌를 공격자의 거래 계좌로 바꿔치기 하는 등 사용자의 컴퓨터에서 직접 정보를 탈취하고 정보수정을 할 수 있다. 가로채기 공격(Man-in-the-middle, MITM)의 경우 공격자와 뱅킹 사용자가 서로 다른 컴퓨터에 위치하게 되지만, 이 멀웨어는 사용자와 동일한 물리적 위치에 존재한다. 아직까지 이러한 공격으로 나타난 피해사례는 없지만, 보안 연구자들은 이 멀웨어의 출현과 함께 공격기술의 정교화 및 변종의 출현을 통해 이러한 공격이 현실화 될 것이라는 것을 예견하고 있다.

본 논문에서는 현재 이 멀웨어가 사용자의 컴퓨터에 설치되어 있으며 해커는 앞서 2절에서 언급하였던 보안위협들을 이용하여 로컬 및 원격 공격이 가능한 상황을 활용할 수 있다고 가정한다. 여기서 이러한 멀웨어 타입에 사용자의 컴퓨터가 감염되었다고 가정하는 것은 현재의 기술 및 상황에서 충분히 가능한 상황이다.

국내의 전자 금융거래 환경에서 가장 높은 보안성을 제공하는 3가지 방안으로 공인인증서와 결합하여 OTP, HSM 방식과 2채널(별도채널) 인증방식을 선택하고 있다. 이와 관련하여 김기영[30]은 OTP의 MITM 취약성을 언급하였으며, 최근의 오스트리아 Cert 컨퍼런스에서는 OTP를 포함한 2팩터 인증방식의 MITM 취약성을 경고하였다. 또한 [8,13,27,31]에서는 SMS기반 인증 방식, 이미지 기반인증방식, 공인인증서기반 인증

방식에 대한 논리적 공격이 가능함을 세부적인 시나리오를 통해 지적하고 있다. 본 논문에서는 지면의 제한으로 이상의 보고들에 대해 세부적으로 언급하지 않지만 기존 사용되는 인증방식들이 논리적으로 완전하지 않음이 제기되고 있다는 것을 언급한다. 따라서 이러한 공격이 가능한 상황을 가정하여 2절에서 언급한 인증 기술들의 장단점을 비교하고자 한다.

4.2. 인증 기술의 비교 분석

[표 2]에서는 [그림 3]의 범주에 따른 인증 기법들을 비교하고 있다[6,8,18,32]. 표의 세로축은 분류 범주에 따른 인증 기법들을 나타낸다. 가로축은 사용자 편의성에 영향을 미치는 요소와 대표적 보안 위협을 나타내고 있다. [표 2]의 가로축에서 사용자 편의성 범주의 멀티팩터 타입은 [그림 2]에서 기술하는 인증 타입을 의미한다. 멀티팩터 타입 'xy'에서 'x'와 'y'는 [그림 2]에서 정의하는 각 타입의 번호를 의미한다. 따라서 '타입 11'의 경우는 같은 '타입1'들이 결합된 인증 방식을 나타낸다. 사용자 불편은 사용자 인증 방식을 이용하는데 있어 조작, 교육 및 동작하는데 있어 복잡성을 의미하며, 설치 비용의 경우는 소프트웨어나 하드웨어의 설치 및 유지에 대한 복잡성을 의미한다. 사용자 부주의 경우는 해당 인증 방식을 사용 관리하는데 있어서 사용자에 의한 관리 소홀이나 부주의로 발생할 수 있는 보안 취약성 정도 혹은 오류발생 정도를 의미한다. 사용자 군은 해당 인증 기법이 범용 응용에 사용될 수 있는 정도를 나타내고 있다. 이동성의 경우는 해당 인증 기법이 휴대 편의성을 지원하는 정도를 나타내고 있다.

가로축의 비교 항목 중에서 보안성 범주에서는 보안 위협의 강도에 따라 스니핑으로 부터 보안 위협의 정도가 높은 항목인 MITM순으로 나열하였다.

[표 2]에서 기술되는 개별 인증 방식의 멀티팩터 중에서 같은 타입의 인증 방식들 간에 인증 강도의 차이가 나타난다. 따라서 같은 타입의 팩터들을 결합한 인증 방식은 특정 취약성에 대한 대응 방안으로서 의미가 있을 수 있다. 이는 단일 팩터의 취약성에 대해 또 다른 타입의 단일 팩터를 사용하여 대응하는 것이며, 팩터 자체의 제약성을 극복하는 대응방안이 되지 못한다. 또한, 서로 다른 팩터를 결합한 2팩터 방식이라고 하더라도 인증 강도 또는 구현 방식에 따라 차이가 날 수 있다. 예를 들어 단순 패스워드 방식과 결합한 보안카드방식과 PIN번호를 요구하는 OTP 장치는 모두 2팩터 인증 방식을 사용한다. 그러나 단순 패스워드 방

〔표 2〕 사용자 인증 기술의 비교

		멀티팩터 타입	사용자 편의성					보안위협			
			사용자 불편	설치 비용	사용자 부주의	사용자군	이동성	스니핑	키보드로깅 /화면캡처	피싱	MITM
범주 1	ID패스워드방식	1	낮음	낮음	낮음	높음	높음	X	X	X	X
	가상키패드	11	보통	낮음	높음	낮음	높음	○	△	X	X
	스크램블패드	11	보통	낮음	높음	낮음	높음	○	△	X	X
범주 2	사전질의응답방식	11	보통	보통	보통	보통	높음	X	○	X	X
	보안카드	12	보통	높음	보통	보통	높음	○	○	△	X
	이미지검증방식	11	보통	보통	보통	낮음	높음	○	X	△	X
범주 3	비대칭키방식	12	낮음	보통	낮음	높음	낮음	○	○	X	X
	대칭키 방식	12	보통	보통	낮음	보통	낮음	○	○	△[1]	X
범주 4	일방향방식	12	낮음	높음	보통	낮음	높음	○	○	X	X
	양방향 방식	12	보통	높음	보통	낮음	높음	○	○	X	X
범주 5	비대칭키 방식	12	보통	높음	낮음	낮음	높음	○	○	△[2]	X[3]
	대칭키 방식	12	보통	높음	낮음	높음	높음	○	○	△[1]	X[3]

[범례] ○ : 대응 가능, X: 대응 불가, △: 부분적으로 대응 가능하나 논리적인 취약성 존재함

1) 피싱 사이트에 입력된 OTP값은 일정시간 경과 후에는 사용할 수 없음

2) 피싱 사이트에서 해커가 필요한 전자 서명 값을 생성하여 원래 사이트에 사용하는 재사용 공격이 가능함

3) 현재 제시되는 구현 방식에서의 취약성을 의미하며, 암호속성 자체의 취약성을 의미하지 않음

식은 매체가 분리된 상태로 안전하게 입력되는 PIN이라기 보다 사용자의 PC에서 입력되는 패스워드를 사용하기 때문에 스파이웨어나 네트워크 스니퍼로부터 취약하다. 따라서 후자가 훨씬 강한 인증방식을 제공한다.

가상 키패드나 스크램블 패드 방식은 단순 스파이웨어(key loggers)에 대해 패스워드를 보호할 수 있지만, 마우스를 클릭할 때 화면 캡쳐를 하는 멀웨어에 취약하다. 또한 피싱 형태의 공격에 충분한 보호를 제공하지 못한다. 따라서 현실적으로 이를 보완하기 위한 더 강한 인증을 필요로 한다.

단순한 질문/응답 방식의 경우 비록 사전에 사용자가 이 항목을 설정했다고 하더라도 쉽게 추측되거나 노출될 수 있다. 예를 들어 "가장 존경하는 인물은?"과 같은 정보는 아이디 탈취 공격이나 사회 공학적 공격에 노출되기 쉽다. 따라서 이 방식은 주 인증 목적보다는 패스워드 등록 및 재설정시에 주로 사용되며, 단순 패스워드 방식과 같은 인증 방식에 부가적인 인증 방식으로 사용될 수 있다.

이미지 검증방식의 경우 사용자 인증 뿐 아니라 사전에 사용자가 설정한 이미지를 사용자가 확인함으로서 사이트인증 목적으로 사용될 수 있다. 따라서 주로 피싱의 대응 용도로서 사용되고 있으나 이전 절에서 언급하는 바와 같이 사용자 컴퓨터의 멀웨어가 이미지 정보와 사용자 비밀정보들을 수집하여 MITM공격하는 것이 가능하다[8].

공인인증서의 경우는 사용자의 컴퓨터에 사용자의 인증서가 위치하고 있기 때문에 악의적 탈취에 취약하며, 사용자의 이동성에 제약을 준다. 비록 공인인증서 탈취문제를 방지할 수 있는 HSM과 같은 보안 모듈에 저장된 방식이라 하더라도 사용자의 컴퓨터에 연결되어 사용될 경우는 멀웨어에 의해 해커가 HSM을 동작할 수 있는 취약점이 존재한다. 일부 스마트카드의 IC칩에 저장된 공인인증서 사용방식이 존재하나 범용의 리더기를 요구한다는 점에서 사용자 군에 제약성이 존재한다.

공인인증서와 마찬가지로 사용자 컴퓨터에 설치된 소프트웨어 기반 OTP는 이동성에 제약성을 가진다. OTP 소프트웨어 토큰의 경우는 소프트웨어의 취약점을 이용한 공격이 가능하므로, 토큰소지가 불가능할 경우 차선책으로 사용될 수 있다. 특히 이동단말과 결합한 소프트웨어 OTP는 전용 하드웨어 토큰의 보안성에 근접하며, 부가의 토큰 발급 및 소지가 필요 없기 때문에 낮은 비용과 높은 편의성을 제공한다. 또한 OTP 보안성 향상을 위해 로그인과 트랜잭션 처리 시점 사이에 여러 OTP값들을 요구하는 방식도 제기 되고 있지만 사용자 편의성과 OTP 동기화 문제 등의 제약성이 부가적으로 고려되어야 한다.

일방향 및 양방향의 별도채널 인증 방식의 경우 가장 큰 장점은 대부분의 사용자가 이미 이동 단말을 가지고 있으며 별도의 토큰을 사거나 추가할 필요가 없다는 것이다. 그러나 이동 단말의 번호가 공격자에게 알려질 경우 콜 포워딩(Call Forwarding)과 같은 리다이렉션 공격에 취약성이 존재하며, 사용자 편의성 관점에서 매 사용마다 요금이 부과되는 제약성이 존재한다. 따라서, 비용문제는 사용자 뿐만 아니라 금융기관에 부담으로 작용하게 된다. 별도 채널 활용 방식의 경우는 일반적으로 지리적으로 인구가 밀집되어 있고, 이동 통신 인프라가 잘 갖추어진 지역에서 기존 인증 방식을 강화하기 위한 용도로 사용된다.

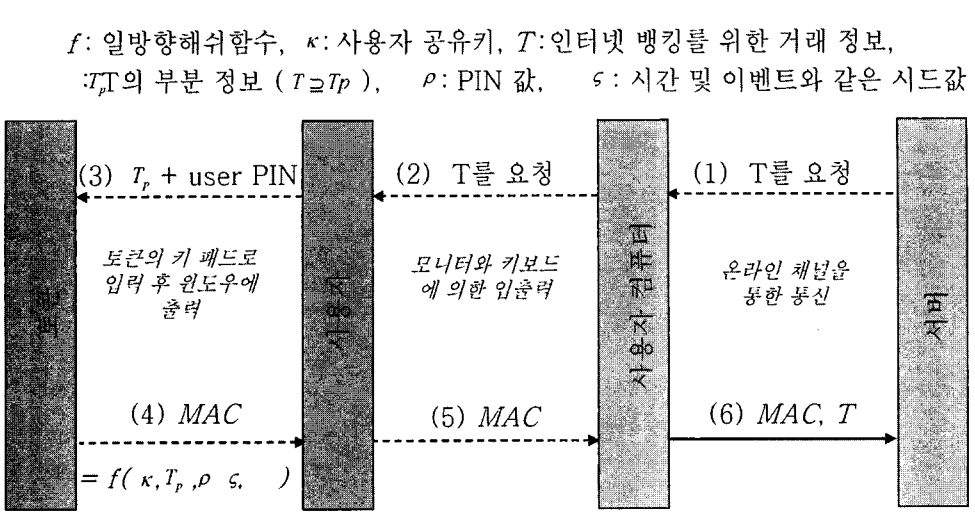
V. 취약성에 대한 기술적 대응 기법

[표 2]에서 살펴본 바와 같이 보안위협에 적극적으로 대처하기 위해 많은 인증기술들이 사용되어 왔으며, 각 범주별 인증기술들을 동시에 사용하는 방법으로 공격에 대응하여 왔다. 하지만, 정교한 공격방식이 꾸준히 증가되고 있으며, 최근 심각한 보안위협으로 등장한 피싱 및 MITM 공격에 완벽하게 대응하는 기술 및 사례는 아직까지 없다.

본 논문에서는 이러한 취약점을 감소 또는 완화하기 위한 방안으로서 보안매체를 활용한 강한 인증방식인 트랜잭션 검증 기법과 사용자 거래의 위험분석을 통해 인증을 보완하는 백엔드(back-end) 인증 기법을 소개한다.

5.1 트랜잭션 검증 기법

Beker, Henry J.등에 의해 watchword Protocol이 Thales사로부터 1989년도에 제안되었다[28,29]. 이 방식의 특징은 서버로부터 전송된 챌린지값을 별도의 분리된 토큰에서 서명하여 웹브라우저를 통해 응답하는 방식이다. 강한 인증성을 제공하는 요인은 챌린지/리스폰스 방식이라기보다는 별도의 분리된 보안매체에서 전송내용을 서명 한다는 것이다.

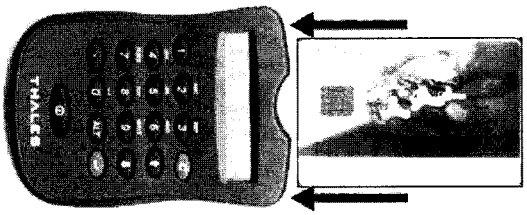


〔그림 10〕 트랜잭션 검증방식

이러한 접근으로부터 대칭키 기반의 OTP 토큰에서 거래정보를 기반으로 생성되는 맥(MAC)사용 방식이 제안 되고 있다. [그림 10]에 나타나는 바와 같이 사용자 토큰에 결재 정보에 관련된 정보를 입력하여 토큰의 비밀키를 이용하여 거래정보에 대한 맥을 생성한 후 브라우저에 입력하여 서버로 전송하는 것이다. 이 방식은 정교한 MITM 공격이 시도되더라도 성공할 수 없는 메커니즘을 가진다. 국내에서는 계좌연동 OTP등으로 명명되고 있지만 일반적인 명칭은 트랜잭션 검증 방식으로 통한다.

맥 기반 OTP는 매우 강한 인증성을 제공할 수 있지만, 사용자가 직접 많은 정보를 토큰에 입력해야하는 제약성을 가지고 있다. 이에 대한 대안으로 많은 정보들 중 일부를 랜덤하게 추출하여 입력하는 방식도 제시되고 있지만, 여전히 데이터 조합에 대한 복잡성을 내재하고 있다. 또한 이 방식의 가장 큰 제약은 OTP 맥이 단독으로 트랜잭션 인증 및 검증 목적으로 사용될 경우 금융거래시 요구되는 부인방지 기능을 제공하지 못한다는 근본적 제약을 가지고 있다. 그러나 국내에서는 OTP가 공인인증서와 함께 사용되기 때문에 이러한 문제에 대응할 수 있는 상황이다.

트랜잭션 검증 방식의 또 다른 대표적인 사례로서 유럽에서 추진 중인 스마트카드 기반의 공인인증서 방식을 예로 들 수 있다. 공격자가 사용자에게 보여지는 화면을 수정하여 송금 계좌를 자신의 것으로 교체하지 못하도록 웹 브라우저로부터 외부 카드리더로 전송된 화면에 보여지는 송금계좌번호를 스마트카드가 직접



〔그림 11〕 트랜잭션 서명에 사용되는 소형 리더 장치

서명한다. 이 방식의 제약은 [그림 11]과 같이 사용자가 소지한 스마트카드를 이용하여 서명할 수 있는 숫자 패드가 달린 사용자 입력 장치를 별도로 소지해야 하며 사용자가 직접 입력에 사용해야한다. 이 방식은 고객의 컴퓨터에 직접 연결되지 않고 별도의 토큰에서 거래 인증 및 서명 작업이 동작하기 때문에 기존 인증서가 가지고 있는 MITM 취약성 문제를 현저히 감소시킬 수 있다. 그러나 사용자 부주의에 의해 피싱 사이트에서 요구하는 트랜잭션에 서명할 수 있는 가능성이 존재한다. 더욱이, OTP 기반 트랜잭션 검증 방식과 같이 높은 보안성을 가지는 기술이라 하더라도 운영의 복잡성이 존재하여 사용자의 편의성이 저해될 수 있다.

5.2 백엔드 인증 기술

[표 2]에서 나타나는 대부분의 방식은 사용자의 컴퓨터에 설치된 보안 소프트웨어나 사용자가 소지한 토큰을 중심으로 동작하는 프런트 엔드(Front-end)인증 방식의 범주에 해당한다. 그러나 백엔드 인증 방식의

경우는 사용자의 금융 거래 내역을 실시간 분석을 통해 고객의 정보, 계좌, 트랜잭션을 보호하기위한 목적을 갖는다[33].

미국 FFIEC 가이드라인의 경우 2006년 말까지 OTP, 바이오 인증과 함께 백엔드 인증을 금융권에서 도입해야하는 대응 방안 중에 하나로 제시하였었다. 또한 2003년 제정된 미국의 공정정확신용거래법(FACTA)에서는 2008년 11월 1일부로 카드사 및 금융사들은 백엔드 인증을 적용하도록 하고 있다[34].

이 방식은 프런트엔드에서 적용된 인증기술들이 정교한 공격에 의해 무력화된 경우에도 사용자의 금융거래 패턴을 분석하고, 이상 거래를 탐지하여 이에 대응하는 효과적인 방안이다. 더욱이 백엔드 인증은, 해당 은행의 인증 서버에서 수행되기 때문에 사용자 및 사용자측 단말에 별도의 요구사항을 갖지 않는다. 백엔드 인증 서버는 사용자의 디바이스 정보 및 트랜잭션의 패턴을 취합하여 정상유무를 판별하며 이 과정에서 퍼지로직이나 확률·통계적인 분석 혹은 뉴럴 네트워크와 같은 데이터 마이닝 기술을 탐지모델로 사용하는 솔루션도 존재한다. 일반적으로 이러한 기술들은 이상 행동에 대한 임계치로서 위협스코어(risk score)를 정의하고 이를 초과하는 거래 트랜잭션에 대한 단계적인 대응 조치를 요구하게 된다. 이상 유무 감지시 2채널을 활용한 챌랜지/리스폰스를 시도하여 확인을 하거나 OTP를 사용한 추가적인 검증을 시도할 수 있다.

트랜잭션에 대한 모니터링은 모델이나 룰(rule) 혹은 이들 간의 결합을 통해 수행되며, 모니터링 대상은 웹, 전화, 자동화기기(Automated Teller Machine, ATM) 등 채널간, 응용간, 기관간에(bad IP나 블랙리스트 참조) 사용자 행동 및 트랜잭션을 모니터링 한다. 기본적으로 룰에 정의되지 않은 행동은 감지할 수 없으며, 기존 응용시스템들과 적절히 튜닝 되지 않으면 많은 긍정오류(false positive) 결과를 생성할 수 있다.

[표 3]에서는 현재 대표적인 글로벌 업체들의 백엔드 솔루션을 비교하고 있다. *탐지 방법*의 경우 각 솔루션들이 거래 트랜잭션의 이상 유무를 판별하는 방법을 의미한다. 개별 솔루션들은 주로 트랜잭션 패턴별, 거래 패턴별, 디바이스 정보별로 사용자 프로파일을 생성하여 분석하는 방법을 이용하고 있다. *탐지 모델*의 경우는 위협스코어를 산출해내기 위해 사용하는 접근 모델을 의미한다. *크로스채널 탐지*의 경우는 솔루션들이 인터넷 연결 뿐만이 아니라 ATM등 사용자 거래 트랜잭션이 발생하는 모든 채널에 대한 탐지 지원 여부를 나타낸다. *위치 정보*의 경우는 물리적 및 논리적인 위치 정보에 대한 이상 유무 탐지를 사용하는 여부를 나타내고 있다. 물리적인 위치 정보로는 사용자가 위치하는 국가, 도시,

〔표 3〕 백엔드 인증 솔루션 제품군

업체명 (제품명)	탐지방법	탐지모델	크로스 채널탐지	위치 정보이용	디바이스 정보사용	사용기관
Actimize[35] (FraudPrevention)	트랜잭션분석 및 사용자 프로파일 분석 혼용	룰기반 퍼지로직	사용	-	-	CheckFree, Well Fargo, Leumi bank, Bank of America 등
Cyota[36] (eVision)	트랜잭션분석 및 사용자 프로파일 분석 혼용	-	-	사용	사용	Bank of America, US bank, Royal bank 등
41st[37] (FraudNet)	사용자 프로파일 분석	룰기반비정상 행위탐지	-	사용	사용	-
Fair Isacs[38] (Blaze Advisor)	트랜잭션분석 및 사용자 프로파일 분석 혼용	룰기반통계적 확률	사용	-	-	Junifer bank, Royal bank
Quova[39] (GeoPoint)	트랜잭션분석 및 사용자 프로파일 분석 병행	룰기반비정상 행위탐지	사용	사용	-	Ever Bank, GlobalCollect, SafeCharge
Iovation[40] (Reputation Manager)	디바이스정보와 사용자 프로파일 패턴분석	룰기반비정상 행위탐지	-	사용	사용	UltimateBet, BoDog등 온라인 게임업체
Entrust[41] (Identity Guard)	트랜잭션분석 및 사용자 프로파일 분석병행	룰기반비정상 행위탐지	사용	사용	사용	US bank, Schufa, Commerce Bank, New Zealand bank 등
Digital Resolv[42] (Fraud Analyst)	사용자프로파일 및 트랜잭션 모니터링	룰기반비정상 행위탐지	사용	사용	사용	NetBank, America Online,Symantac 등

시간 등의 정보 등이 해당하며, 논리적인 정보로는 IP주소, 도메인, 라우팅 타입, ISP 정보 등의 정보가 해당된다. *디바이스 정보* 사용의 경우는 디바이스 쿠키, 브라우저 언어 및 버전, OS 버전 등의 정보를 통해 사용자 디바이스 프로파일 활용 유무을 나타내고 있다.

[표 3]에는 언급되지 않지만 벡엔드 인증 솔루션들은 구축방식에 따라 임베디드 모드, 모니터링 모드, 인라인 모드 3가지 형태로 기존 인터넷 뱅킹 시스템과 연동한다. 임베디드 모드의 경우 기존 웹서버에 프리프로세서(pre-processor)를 탑재하는 임베디드 형태의 통합 방식이며, 모니터링 모드는 패킷 스니핑 형태로 거래 트랜잭션을 모니터링 한다. 마지막으로 인라인 모드의 경우 모든 거래 트랜잭션이 해당 웹서버로 도달하기 전에 별도의 API를 거쳐 처리되는 모드에 해당하며, 솔루션들의 특성 및 기존 시스템 상황에 따라 유연하게 적용할 수 있도록 이상의 3가지 방법들을 결합하여 지원하고 있다.

벡엔드 인증 기술이 다른 인증기술과 혼용해서 사용될 경우 멀티팩터 관점에서 인증정보를 구성하는 요소가 한 개 이상임을 의미한다. 그러나 3팩터 이상의 인증 방식을 구성하는 팩터들은 직접적으로 인증정보를 구성하는 요소가 되지 않는다. 즉 [표 3]에서 살펴보았던 바와 같이 이러한 인증 정보는 행동(behavior)이나 위치(location)와 같은 정보로서 단지 더 신뢰성 있는 인증 결정을 주거나 침해의 가능성을 추출하는 용도로 사용되는 부가적인 정보형태를 가진다. 따라서 강한 인증을 구성한다 라기 보다는 효과적인 인증강도를 제공함을 의미한다.

이러한 솔루션들은 기본적으로 거래 정보 및 사용자 계좌 정보에 대해 이상 발견시 즉각 대응하기 위한 실시간 분석 방식을 사용하며, 사후 금융 사고에 대한 감사 목적의 분석기능을 지원하는 솔루션도 있다. 이 방식의 가장 큰 장점은 사용자의 편의성을 저해하지 않고, 정교한 공격들에 대응할 수 있는 방법을 제공한다는 것이다. 그러나 금융 기관 입장에서는 별도의 시스템 구축 및 유지 비용을 요구하며, 기존 시스템과의 연동 문제가 고려되어야 한다. 현 시점에서 업체별로 상이한 솔루션을 제시하고 있어 백엔드 인증 솔루션을 개발하는 업체들에서는 동일 사용자 거래 패턴의 이상 유무에 대해 솔루션 간에 이상 징후 정보를 공유할 수 있는 프로파일 규격의 표준화를 IETF에서 진행하고 있는 상태이다[34].

Ⅵ. 결 론

지금까지 알려진 보안 위협에 대한 가정을 기반으로 전자 금융거래 환경에서 사용되는 인증 기술의 장단점을 분석하였고 이에 대응할 수 있는 향상된 적용 방안을 살펴보았다. 또한 강한 인증 기법을 도입하기 위해 전체 금융 네트워크를 고려할 때 사용자 측의 프런트엔드와 은행 뱅킹 시스템쪽의 백엔드 관점에서 대응 기술을 고찰하였다. 본 논문에서는 대응 기술로서 전자금융거래 트랜잭션에 상당한 수준의 보안성을 제공할 수 있는 트랜잭션 검증 방식과 함께 트랜잭션 인증을 효과적으로 보완하는 백엔드(back-end) 인증 기법을 제시하였다.

우리는 진화하는 공격기술에 맞선 대응 기술을 설계할 때, 사용자 편의성 및 비용추가 대비 효과를 충분히 고려해야 할 것이다. 아무리 강력한 사용자 인증기법이라고 하더라도, 사용자에 번거로움을 야기한다면 편의성 측면에서 바람직하지 않으며 사용자의 선호도가 떨어질 수 밖에 없다. 이러한 관점에서 벡엔드 인증 기술은 사용자에게 불편을 야기하지 않으면서 기존 인증 시스템에 부가적인 보완책을 제시해준다는 측면에서 시사하는 바가 크다고 하겠다.

참고문헌

[1] Security Standards Council, "Payment Card Industry (PCI) Data Security Standard", http://www.pcisecuritystandards.org/, Sep. 2006.

[2] Office of the Comptroller of the Currency (OCC), http://www.occ.treas.gov/netbank/netbank.htm, "Electronic Banking Guidance".

[3] Federal Financial Institutions Examination Council, http://www.ffiec.gov, "FFIEC Guid ance on Electronic Financial Services and Consumer Compliance".

[4] Federal Trade Commission, http://www.ftc. gov/.

[5] 금융보안연구원 보안 기술팀, "전자금융 사고현황 및 방지대책 (안)", 2007. 03.

[6] George Tubin, "The Sky is Falling : The Need for Stronger Consumer Online Banking Authentication", Market Research Report, TowerGroup, Apr 2005.

[7] Richard E. Smith, "Authentication : From Passwords

to Public Keys", Addison Wesley, 2002.

[8] Candid W., "Phishing In The Middle of the stream"-Today's Threats to Online Banking", Symantec Security Response, 2006.

[9] Christian Ludl, Sean McAllister, Engin Kirda, and Christopher Kruegel, "On the Effectiveness of Techniques to Detect Phishing Sites", LNCS 4579, Springer, 2007.

[10] Rolf Oppliger, and Sebastian Gajek, "Effective Protection Against Phishing and Web Spoofing", LNCS 3677, Springer, 2005.

[11] State Services Commission, "Guidance on Multi-factor Authentication", http://www.e.govt.nz, 2006.

[12] Hole, J, K. J., and Moen. V, "Case Study : Online Banking Security", IEEE Security & Privacy, 2006.

[13] Hiltgen, A, Kramp, T. and Weigold, T., "Secure Internet Banking Authentication", IEEE Security & Privacy, 2006

[14] Committee on National Security Systems(CNSS) Instruction No. 4009, National Information Assurance (IA) Glossary, published by the United States Federal Government, Revised June, 2006.

[15] Roshen Chandran, "Partial Passwords and Keystroke Loggers", http://plynt.com/blog/2005/08/partial-passwords-and-keystrok/, 2005.

[16] Forrester Research, "ForrTel : Online Banking Customer Authentication : Review of Two-Factor Authentication Mechanisms In Use Today", 2005.

[17] Oppliger R. Gajek S., "Effective protection against phishing and web spoofing", 9th IFIP TC-11 Conference, 2005.

[18] Plosni K., Federrath H., Nowey T., "Protection Mechanisms Against Phishing Attacks", LNCS 3592, Springer, 2005.

[19] Tieyan Li, and Wu Yongdong, "Trust on Web Browser : Attack vs. Defense", International Conference on Applied Cryptography and Network Security (ACNS'03), 2003.

[20] Amir Herzberg, and Ahmad Jbara, "Security and Identification Indicators for Browsers against Spoofing and Phshing attacks", Cryptology ePrint Archive, 2006.

[21] Markham, G. "Phishing-Browser-based Defences", http://www.gerv.net/security/phishing-browser-defences.html, 2005.

[22] Rachna Dhamija, "The battle against phishing : Dynamic Security Skins", '05 : Proceedings of the 2005 symposium on Usable privacy and security (SOUPS), 2005.

[23] 금융감독원, http://www.fss.or.kr

[24] 최동현, 김승주, 원동호, "일회용 패스워드(OTP : One-Time Password) 기술 분석 및 표준화 동향", 정보보호학회 논문지 17권 제 3호, 2007. 06.

[25] ComputerWorld Security, "Another new Trojan intercepts online banking information" http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057240

[26] Candid W., "Threats to Online Banking", Symantec Security Response, 2005.

[27] URL, "Security Technologies : Authentication parts", www.isg.rhul.ac.uk/files/IY5522_2006-07_Lec_07.pdf.,

[28] Beker, Henry J., Halliden, Paul W., Friend, and John M. K., "US Patent 4890323-Data communication systems and methods", http://www.freepatentsonline.com/4890323.html.

[29] 김기영, "일회용 패스워드를 기반으로 한 인증시스템에 대한 고찰", 정보보호학회 논문지 제 17권 3호, 2007. 06.

[30] RSA, "RSA, Fighting Emerging Threats : How to Compat Man-In-The-Middle And Trojan Attacks", 2007.

[31] Verisign, "A Guide to Providing Proactive Protection to Consumer Online Transactions", Whitepaper, 2008.

[32] George Tubin, "Emergence of Risk-Based Authentication in Online Financial Services; You Can't Hide Your Lyin' IPs", TowerGroup Industry Report, May 2005.

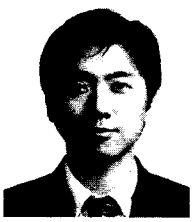
[33] United States federal law, "The Fair and Accurate Credit Transactions Act", 2003.

[34] David M'Raihi, Sharon Boeyen, Michael Grandcolas, and Siddharth Bajaj, "How to Share Transaction Fraud (Thraud) Report Data", IETF Internet draft(in progress), http://www.ietf.org/internet-drafts/draft-mraihi-inch-thraud-04.txt, Feb. 2008.
[35] Actimize, http://www.actimize.com/
[36] Cyota, http://www.rsa.com/
[37] 41st, http://the41stparameter.com
[38] Fair Isacs, http://www.fairisaac.com
[39] Quova, http://www.quova.com/
[40] Iovation, http://www.iovation.com/
[41] Entrust, http://www.entrust.com/
[42] Digital Resolv, http://www.digitalenvoy.net/

〈著者紹介〉

임 형 진 (Hyung-Jin Lim)
정회원

1998년 2월 : 한림대학교 컴퓨터공학과 졸업 (학사)
2001년 2월 : 성균관대학교 정보통신공학과 졸업 (석사)
2006년 8월 : 성균관대학교 컴퓨터공학과 졸업 (박사)
2007년 10월~현재 : 금융보안연구원 인증관리팀 선임연구원
<관심분야> 메쉬 네트워크, IP 기반 이동성(Netlmn, MEXT, AUTO CONF) 지원 기술, 네트워크 관리 및 보안, 키 협상 및 인증 프로토콜, 금융정보보호



심 희 원 (Hee-Won Shim)

1998년 2월 : 단국대학교 전자계산학과 졸업 (학사)
2000년 2월 : 홍익대학교 전자계산학과 졸업 (석사)
2000년 3월~2006년 11월 : 한국정보인증 선임연구원
2006년 12월~현재 : 금융보안연구원 인증관리팀 선임연구원
2008년 3월~현재 : 전남대학교 정보보호학과 박사과정
<관심분야> PKI, OTP, 네트워크 보안, 암호이론

서 승 현 (Seung-Hyun Seo)
종신회원

2000년 2월 : 이화여자대학교 수학과 졸업 (학사)
2002년 2월 : 이화여자대학교 컴퓨터학과 졸업 (석사)
2006년 2월 : 이화여자대학교 컴퓨터학과 졸업 (박사)
2006년 5월~2007년 11월 : 고려대학교 정보경영공학전문대학원 연구전임강사
2006년 12월~현재 : 금융보안연구원 인증관리팀 주임연구원
<관심분야> 암호이론, 네트워크보안, OTP

강 우 진 (Woo-Jin Kang)

1992년 2월 : 연세대학교 중어중문학과 졸업
1992년 2월~1998년 7월 : 조흥은행 전산부
1999년 4월~2003년 1월 : 투나인 정보기술 연구소장
2003년 4월~2006년 10월 : LG CNS 금융사업부 전자금융업무 BA
2006년 11월~현재 : 금융보안연구원 인증관리팀장
<관심분야> 소프트웨어공학, 보안감리, 금융정보보호