정 보 보 호 학 회 지
제25권 제6호, 2015. 12

온라인 본인확인수단 동향 분석

육 형 준*, 임 하 빈**, 이 경 률***, 임 강 빈****

요 약

과거 인터넷 뱅킹 서비스에서 클라이언트와 서버 채널 사이에 암호기술을 활용하여 안전한 채널을 구성함으로서 인증, 무결성, 부인방지, 암호화 등의 보안요건을 만족하였지만, 현재의 인터넷 뱅킹 서비스에서 제3자인 공격자는 수학적으로 안전성이 보장된 네트워크상의 보안채널을 공격하는 것이 아니라, 채널의 끝부분인 사용자의 전자적 장치나 금융기관의 웹 서버, 데이터베이스 서버, 어플리케이션 서버 등을 포함하는 인터넷 뱅킹 서버나 내부자에 의하여 내부 호스트에 대한 공격을 시도하는 추세이다. 따라서 이러한 위협에 대응하기 위하여 최근 금융기관에서는 접근 매체를 활용하여 거래를 요청하는 주체가 사용자 본인임을 확인하기 위한 다양한 수단을 도입하고 있으며, 이에 대하여 조사한 결과를 서술한다.

Ⅰ. 서 론

과거의 인터넷 뱅킹 서비스는 클라이언트와 서버 채널 사이, 즉, 사용자의 전자적 장치와 금융기관의 인터넷 뱅킹 서버 사이에 암호기술을 활용하여 안전한 채널을 구성함으로써 인증, 무결성, 부인방지, 암호화 등의 보안요건을 만족하여 전통적인 Yao-Dolev 위협모델[1]로부터 안전성을 보장하였다[2,3]. 하지만 현재의 인터넷 뱅킹 서비스에서의 제3자인 공격자는 수학적으로 안전성이 보장된 네트워크상의 보안채널을 공격하는 것이 아니라 채널의 끝부분인 단말, 즉, 사용자의 전자적 장치[4, 5]나 금융기관의 웹 서버, 데이터베이스 서버, 어플리케이션 서버 등을 포함하는 인터넷 뱅킹 서버나 내부자에 의하여 내부 호스트에 대한 공격을 시도하는 추세이다[6-12]. 따라서 이러한 위협에 대응하기 위하여 최근 금융기관에서는 접근매체를 활용하여 거래를 요청하는 주체가 사용자 본인임을 확인하기 위한 다양한 수단을 도입하고 있으며, 이를 온라인 본인확인수단으로 정의하여 각각의 방식으로 분류하여 각 방식에 대해여 조사한 결과를 토대로 서술한다.

Ⅱ. 온라인 본인확인수단 개요

온라인 본인확인수단 개요에서는 본인확인수단에 대한 정의를 서술하고 기존에 존재하는 본인확인수단을 분류하며, 국내에 적용된 본인확인수단의 현황을 파악한다.

2.1. 온라인 본인확인수단 정의

사용자 인증이란, 서비스 혹은 정보 등을 요청하는 주체가 사용자 본인임을 확인하고 이를 검증하는 것을 의미하며, 주체의 확인 및 검증을 위하여 제공되는 수단을 본인확인수단이라고 한다. 이러한 본인확인수단은 주체가 누구인지를 밝히는 식별(identification), 주체를 증명하는 인증(authentication), 주체에 대한 시스템 자원을 허가하는 권한부여(authentication) 단계로 이루어지며, 이는 서비스를 제공받기 위한 필수적인 요구조건이다[13,14].

인터넷 뱅킹 서비스에서의 온라인 본인확인수단은 서비스를 요청하는 주체의 신원 확인 기능과 송/수신자 간 전달되는 거래정보의 무결성을 보장하여 거래인증 기능을 지원한다[3, 15]. 추가적으로 거래내역의 무결성

본 연구는 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2015R1A6A3A01019717)
* 순천향대학교 정보보호학과 (goodyug@sch.ac.kr)
** 순천향대학교 정보보호학과 (habin103@sch.ac.kr)
*** 순천향대학교 보안안전융합기술사업화센터 (carpedm@sch.ac.kr)
**** 순천향대학교 정보보호학과 (yim@sch.ac.kr)

을 보장함으로써 부정거래를 방지하고, 거래에 참여하는 주체인 사용자와 금융기관의 거래사실에 대한 부인방지 기능을 제공한다. 즉, 인터넷 뱅킹 서비스에서의 온라인 본인확인수단은 사용자와 금융기관의 인증, 거래정보의 무결성 보장, 거래내역에 대한 부인방지 기능을 제공하며, 이러한 기능은 암호기술과 연동되어 거래에 참여한 주체가 아닌 제3자가 인터넷 뱅킹 서비스를 이용할 수 없도록 방지하는 역할을 한다.

2.2. 온라인 본인확인수단 분류

인터넷 뱅킹 서비스에서 본인확인수단은 수단을 활용하는 개수에 따라 단일요소 본인확인수단과 복합요소 본인확인수단으로 분류된다. 단일요소 본인확인수단은 한 가지 팩터만을 사용하여 본인임을 확인하는 것을 의미하며, 지식기반 본인확인수단(something you know), 소지기반 본인확인수단(something you have), 특징기반 본인확인수단(something you are), 행동기반 본인확인수단(something you do)[16], 소셜 네트워크기반 본인확인수단(somebody you are)[17]으로 분류된다. 복합요소 본인확인수단은 동일하지 않은 단일요소 본인확인수단을 결합하여 본인임을 확인하는 것을 의미하며, 멀티팩터 본인확인수단과 멀티채널 본인확인수단으로 분류된다. 이러한 분류는 심희원의 연구[3]를 참조하였으며, 해당 연구는 CA사의 인증기술 분석[16], 전자금융 인증기술 동향 분석[18], 인증기술의 공격기법 분석[19] 등의 연구결과를 참조하였다. 조사한 결과를 토대로 분류한 온라인 본인확인수단을 표 1에 나타내었다[20-22].

2.3. 국내 온라인 본인확인수단 보안등급

2008년 4월 발표된 보안등급별 이체한도 차등화 정책에 따르면, 전자금융거래의 안전성 강화를 위하여 거래수단별로 보안등급을 부여하고, 이에 따른 이체한도를 표 2와 같이 적용하였다[15]. 보안등급은 총 3개의 등급으로 분류되며, 기본적으로 일회용 비밀번호(보안카드 포함)나 공인인증서를 사용하여야 하며, OTP 생성기, 공인인증서, 하드웨어 보안토큰, 2채널 인증, 휴대폰 SMS(Short Message Service)의 조합에 따라 등급이 분류된다.

보안카드와 공인인증서를 이용하는 3등급의 경우 1회 이체한도는 1,000만원, 1일 이체한도는 5,000만원이며, OTP 생성기나 하드웨어 보안토큰 등을 이용하는 1

〔표 1〕 온라인 본인확인수단 분류

본인확인수단 분류		대표적인 본인확인수단 일례	
단일요소	지식기반	고정 비밀번호	· 단순 비밀번호 방식 · 그래픽 인증 방식 · 스크램블 패드 방식 · 부분 비밀번호 방식
		등록정보 질의응답	-
	소지기반	보안카드	-
		소프트웨어 보안토큰	· 공인인증서 방식
		스마트카드	-
		하드웨어 보안토큰	-
		OTP 생성기	· 질의-응답 방식 · 시간 동기화 방식 · 이벤트 동기화 방식 · 조합 방식
		거래연동 인증	· 거래서명 기술 · 거래연동 기술
	특징기반	바이오 인증 등	-
	행동기반	위험기반 인증	· 물리적인 위치정보 · 논리적인 위치정보 · 트랜잭션 정보
		휴먼인지 인증	· CAPTCHA
	소셜 네트워크 기반	증빙 시스템 등	-
복합요소	멀티팩터 기반	비밀번호+OTP 생성기 이용 PC 지정 등	-
	멀티채널 기반	전화 승인	· 인가코드 입력 방식 · 사실안내 방식 · 상세안내 방식

〔표 2〕 보안등급별 온라인 본인확인수단

본인확인수단	보안등급
OTP 생성기+공인인증서	1등급
하드웨어 보안토큰 방식 공인인증서+보안카드	
보안카드+공인인증서+2채널 인증	
보안카드+공인인증서+휴대폰 SMS(거래내역통보)	2등급
보안카드+공인인증서	3등급

등급의 경우 1회 이체한도는 1억원, 1일 이체한도는 5억원으로 높은 보안등급일수록 거래 가능한 액수가 증가한다. 게다가 기업이나 법인의 경우에는 1등급 보안 본인확인수단을 사용하여야 하는 대상으로 반드시 OTP 생성기를 사용하여야 하며, 개인은 보안 2등급이나 3등급의 본인확인수단을 사용할 수 있다[15].

Ⅲ. 온라인 본인확인수단 현황

온라인 본인확인수단 현황에서는 온라인 본인확인수단의 개요에서 분류한 본인확인수단에 대하여 각 수단별로 상세히 서술한다.

3.1. 단일요소 본인확인수단

단일요소 본인확인수단은 단일팩터만을 사용하여 본인임을 확인하는 것을 의미하며, 단일팩터는 사용자의 지식에 기반을 둔 '지식기반', 사용자가 소지하는 장치에 기반을 둔 '소지기반', 사용자 자체에 기반을 둔 '특성기반', 사용자의 행위에 기반을 둔 '행동기반', 사용자의 소셜 네트워크에 기반을 둔 '소셜 네트워크기반'으로 나누어진다.

3.1.1. 지식기반 본인확인수단

지식기반 본인확인수단은 사용자의 기억능력에 의존적인 수단으로 대부분의 시스템에서 본인확인수단으로 활용된다. 가장 대표적인 방법으로 아이디-비밀번호 기반이 있으며, 사용자가 설정한 임의의 아이디와 비밀번호를 등록한 후, 차후에 이를 검증하는 방식으로 활용된다. 이와 같은 방식은 관리가 편리하고 구축이 용이한 장점은 있지만, 사용자 기억능력의 한계로 인하여 비밀번호와 같이 민감한 정보를 생성하거나 변경하는데 어려움이 있어 보안성이 낮은 단점도 있다. 그러므로 현재 인터넷 뱅킹 서비스에서는 계좌이체와 같은 거래를 이용하는데 활용되지는 않고 로그인 시 사용자를 확인하는 수단으로 활용되며, 다른 본인확인수단과 결합되어 보안성을 높이는데 사용되기도 한다. 지식기반 본인확인수단은 고정 비밀번호 방식, 등록정보 질의응답 방식으로 분류된다.

3.1.1.1. 고정 비밀번호 방식

고정 비밀번호 방식은 사용자만이 아는 고정된 정보를 등록하고, 이후 이를 확인하는 과정에서 동일한 정보를 제공함으로써 본인임을 확인하는 방식이다. 가장 기본적인 고정 비밀번호 방식은 아이디-비밀번호 방식이 있으며, 이를 확장한 그래픽 인증 방식, 스크램블 패드 방식, 부분 비밀번호 방식이 있다. 이 방식은 사용자의 기억능력의 한계로 인하여 비밀번호를 복잡하게 생성하는데 어려움이 있고, 복잡한 비밀번호를 생성하더라도 제3자에 의하여 노출된 경우에는 안전성을 보장할 수 없어 강한 인증의 범주에 속하지는 않는다. 따라서 소지기반이나 특성기반 본인확인수단과 동시에 사용되는 멀티팩터 본인확인수단에 활용될 수 있는 가장 효과적인 본인확인수단이다[3].

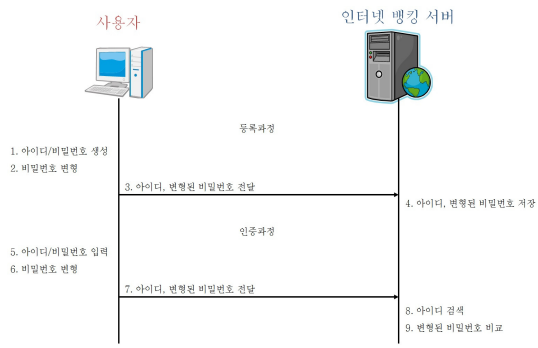
단순 비밀번호 방식은 상기했듯이 사용자가 키보드를 이용하여 설정한 고정된 비밀번호 정보를 검증함으로써 본인을 확인하는 방식이다. 일반적으로 이 방식은 등록과정과 인증과정으로 나누어지며, 이를 그림 1에 나타내었다.

Step 1. 아이디/비밀번호 생성: 사용자는 인터넷 뱅킹 서버에 등록하기 위하여 자신의 지식을 기반으로 문자나 숫자 등으로 구성된 아이디와 비밀번호를 키보드를 통하여 입력한다.

Step 2. 비밀번호 변형: 비밀번호 정보가 제3자에게 그대로 노출되는 것을 방지하기 위하여 해쉬와 같은 암호기술을 이용하여 변형한다.

Step 3. 아이디, 변형된 비밀번호 전달: 사용자의 아이디와 변형된 비밀번호를 인터넷 뱅킹 서버에 전달한다.

Step 4. 아이디, 변형된 비밀번호 저장: 인터넷 뱅킹 서버는 추후 사용자 인증에 사용될 아이디와 변형된 비밀번호를 데이터베이스와 같은 저장소에 저장한다.



〔그림 1〕 단순 비밀번호 방식의 등록 및 인증과정

인증과정은 다음과 같다.

Step 1. 아이디/비밀번호 입력: 사용자는 본인확인을 위하여 이전에 등록한 아이디와 비밀번호를 입력한다.

Step 2. 비밀번호 변형: 비밀번호 정보가 제3자에게 그대로 노출되는 것을 방지하기 위하여 해쉬와 같은 암호기술을 이용하여 변형한다.

Step 3. 아이디, 변형된 비밀번호 전달: 사용자의 아이디와 변형된 비밀번호를 인터넷 뱅킹 서버에 전달한다.

Step 4. 아이디 검색: 인터넷 뱅킹 서버는 수신한 아이디를 기반으로 데이터베이스와 같은 저장소에 저장된 아이디를 검색하여 올바른 비밀번호를 확보한다.

Step 5. 변형된 비밀번호 비교: 확보한 올바른 비밀번호와 사용자로부터 수신한 비밀번호를 비교함으로써 사용자를 검증한다.

단순 비밀번호 방식은 인증에 사용되는 가장 중요한 정보인 비밀번호가 키보드로부터 입력되는 방식인데, 키보드의 심각한 취약점이 드러남에 따라 새로운 인증 모델이 필요하게 되었고, 이에 포인팅 장치와 디스플레이 장치를 활용한 그래픽 인증 방식이 제안되었다. 그래픽 인증 방식은 이미지를 이용하여 비밀번호를 입력받는 방식이며, 디스플레이 장치에 특정 이미지를 출력하고 출력된 이미지 내에서 포인팅 장치의 클릭정보를 다수 입력받아 이를 비밀번호 형태로 구성하는 방식이다. 그래픽 인증 방식은 문자열을 이용한 방법, 변종 기호를 이용한 방법, 얼굴 그림을 이용한 방법, 영상 내의 관심점을 이용한 방법, 가상공간의 임의영역에서 회전 및 이동 가능한 객체를 이용한 방법, 회전 및 확대가 가능한 3D 객체를 이용한 방법 등이 있다[23].

문자열을 이용한 방법은 가장 단순한 방법이며, 문자열을 출력한 후 선택한 문자열을 비밀번호로 구성하는 방법이다.

변종 기호를 이용한 방법은 그림 2와 같이 특정한 기호나 그림들을 정방형으로 나열하고, 사용자가 특정 기호나 그림을 선택하면 선택된 순서나 조합을 기반으로 비밀번호를 구성하는 방법이다[23].

얼굴 그림을 이용한 방법은 그림 3과 같이 다양한 인종이나 사람의 얼굴이 출력되면, 사용자가 특정 얼굴을 선택하여 선택된 순서나 조합을 기반으로 비밀번호를 구성하는 방법이다[23].

영상 내의 관심점을 이용한 방법은 그림 4와 같이 임의의 영상이 출력되면, 사용자가 특정 영상을 선택하고 선택된 영상 내에 사용자가 관심이 있는 특징점을 순차적으로 선택하여 이를 기반으로 비밀번호를 구성하는 방법이다[23].

〔그림 2〕 변종 기호를 이용한 그래픽 인증방식 일례

〔그림 3〕 얼굴 그림을 이용한 그래픽 인증 방식 일례

가상공간의 임의영역에서 회전 및 이동 가능한 객체를 이용한 방법은 그림 5와 같으며, 특정한 모델, 예를 들어 집 내부나 도서관 내부, 차량 내부, 실험실, 연구소 등의 이미지가 출력되면, 사용자가 출력된 영상 중 특정 영역을 선택하고 선택된 영상을 회전 및 이동함으로써 다양한 정보를 선택할 수 있도록 구성하여, 이를 선택하는 순서나 선택된 특정 사물을 기반으로 비밀번호를 구성하는 방법이다[23].

회전 및 확대가 가능한 3D 객체를 이용한 방법은 그림 6과 같으며, 임의의 3D 객체, 예를 들어 지구본이 출력되면, 사용자가 지구본 내부의 나라를 순차적으로 입력하여 이를 기반으로 비밀번호를 구성하는 방법이다[23].

〔그림 4〕 영상 내의 관심점을 이용한 그래픽 인증 방식 일례

〔그림 5〕 가상공간의 임의영역에서 회전 및 이동 가능한 객체를 이용한 그래픽 인증 방식 일례

〔그림 6〕 회전 및 확대가 가능한 3D 객체를 이용한 그래픽 인증 방식 일례

인터넷 뱅킹에서의 그래픽 인증 방식은 계좌비밀번호 등을 입력하는데 활용되며, 출력된 가상의 키패드에 키보드를 이용하지 않고 마우스를 통하여 비밀번호를 입력함으로써 비밀정보를 보호한다. 출력되는 가상 키패드는 제3자에 의하여 마우스 입력 위치가 추적되어 비밀정보가 노출되는 것을 방지하기 위하여 서버에서 난수 생성기를 이용하여 사용자마다, 그리고 매번 다른 키패드를 생성한다. 이와 같은 방식을 통하여 키보드로부터 입력되는 정보를 가로채는 제3자의 공격에 대응하여 안전하게 비밀정보를 입력할 수 있고, 마우스의 좌표값 또는 좌표 값에 해당하는 난수 값만이 저장되므로 이를 탈취하여 비밀번호를 역으로 유추하는 것은 사실상 불가능하다.

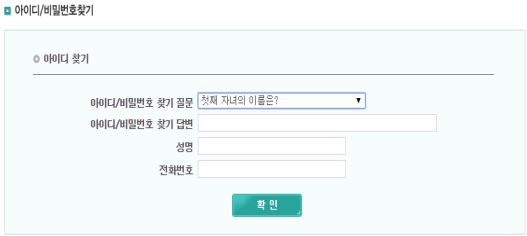
스크램블 패드 방식은 그림 7과 같이 문자를 랜덤한 숫자로 매핑한 스크램블 패드를 출력하여 아이디나 비밀번호 입력을 문자 대신 랜덤한 숫자로 입력하는 방식이다[24].

〔그림 7〕 스크램블 패드 방식 일례

부분 비밀번호 방식은 사용자가 비밀번호 전부를 입력하지 않고 특정 순서에 해당하는 문자를 입력하는 형태이다. 예를 들어 인터넷 뱅킹 서버가 비밀번호의 2번째, 7번째, 5번째 문자를 요구하면 사용자는 그에 해당하는 문자만 입력함으로써 인증하는 방식이다[18].

3.1.1.2. 등록정보 질의응답 방식

등록정보 질의응답 방식은 그림 8과 같이 비밀번호가 아닌 인터넷 뱅킹 서버에서 임의로 제공된 질문에 대한 응답을 등록하고, 인증 시 응답을 검증함으로써 본인임을 확인하는 방식이다[25]. 이 방식은 주로 다른 본인확인수단과 함께 사용되며, 비밀번호를 찾을 경우에 활용되기도 한다. 최근에는 사용자가 인터넷 뱅킹 서버에 이미지를 등록한 후, 서버가 등록한 이미지를 사용자에게 올바르게 제공하는지 확인함으로써 서버를 인증하기 위한 수단으로 제공되기도 한다. 이러한 방식을 개선하여 사용자 전용의 이미지를 사용하거나 윈도우 패드락에 특정 이미지를 출력하는 방식, 사이트 인증을 부가하기 위하여 사용되며[26,27], 대표적인 등록정보 질의응답 방식으로 Dynamic Skin[28], SiteKey[29], TrustBar[30] 등이 있다.



〔그림 8〕 사전 등록된 질의응답 방식 일례

3.1.2. 소지기반 본인확인수단

소지기반 본인확인수단은 사용자가 소지한 것에 의존적인 수단으로 전자금융에서 대부분의 본인확인수단으로 활용된다. 이와 같은 방식은 사용자가 소지한 것을 기반으로 본인을 확인하기 때문에 소지하지 않은 제3자는 검증받지 못하므로 높은 보안성을 제공하지만, 항상 휴대하여야 하는 단점도 있다. 소지기반 본인확인수단은 보안카드, 소프트웨어 보안토큰, 스마트카드, 하드웨어 보안토큰, OTP 생성기, 거래연동 인증 방식으로 분류된다.

3.1.2.1. 보안카드 방식

보안카드는 그리드카드(grid card), 안전카드, 시크릿카드 등으로 불리며, 30개 혹은 35개의 난수로 구성된 보안카드를 대면확인을 통하여 금융기관에서 직접 수령하는 것이 일반적이지만, 전자우편 또는 팩스 등으로도 배포할 수 있어 적용성이 우수하고 배포비용이 저렴한 장점이 있다. 본인확인을 위하여 금융기관에서 임의의 위치에 해당하는 숫자를 사용자에게 질의하면, 사용자는 보안카드를 참조하여 요청된 숫자를 응답하고 금융기관에서 이를 검증함으로써 본인임을 확인한다[31]. 과거에는 1개의 번호를 입력하는 방식으로 운용되었지만, (구)정보통신부, 금융감독위원회, 금융감독원, 산업자원부, (구)한국정보보호진흥원으로 구성된 관계부처에서 “전자거래 안전성 강화 종합대책”의 일환으로 그림 9와 같이 2개의 번호를 제시하여 특정 위치의 앞 두 자리, 특정 위치의 뒤 두 자리를 입력받는 방식으로 안전성을 강화하였다[32].

보안카드는 거래마다 매 번 다른 번호를 요구하므로 넓은 의미에서 OTP에 포함될 수 있으며, 30자리일 경우 870가지의 비밀번호, 35자리일 경우 1,190가지의 비밀번호를 생성할 수 있다. 하지만 금융회사별로 보안카드를 소지하여야 하는 불편함도 있으며, 일정횟수 이상 틀릴 경우 사용이 제한되어 금융기관을 직접 방문하여 사용제한을 해제하여야 하는 단점도 있다. 일반적으로 보안카드는 단독으로 사용되지 않고 본인확인수단보다 거래를 인증하는 목적으로 활용된다[18].

〔그림 9〕 보안카드 입력 방식 일례

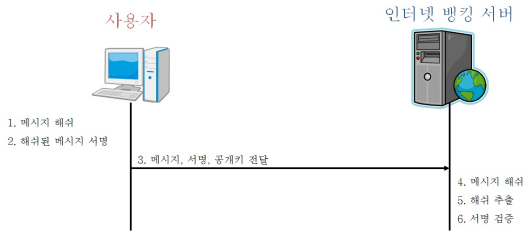
3.1.2.2. 소프트웨어 보안토큰 방식

소프트웨어 보안토큰 방식은 하드디스크나 메모리 등에 암호학적인 비밀키를 저장하고 이를 기반으로 암호연산을 이용하여 강한 인증정보를 생성하는 방식이다[3]. 소프트웨어 보안토큰의 대표적인 방식은 PKI(Public Key Infrastructure) 기반의 공인인증서가 있으며, 지식기반의 본인확인수단인 고정 비밀번호와 결합되어 멀티팩터 본인확인수단으로 주로 활용된다.

공인인증서는 1999년 전자서명법 제정에 의하여 등장한 공개키 기반의 암호기술이며, 2003년 6월부터 인터넷 뱅킹을 시작으로 전자금융거래에서 의무적으로 사용되었다. 이후 공인인증서는 전자금융감독규정 제3장 제7조에 따라 모든 전자금융거래에 있어 필수적으로 사용되면서[15] 인터넷 뱅킹, 증권거래, 정부민원, 조달업무, 병무행정 등에서 전반적으로 활용되고 있다. 이는 기존의 본인확인수단과는 달리 공인인증기관(CA, Certificate Authority), 공개키 암호 시스템 등 공인인증체계를 기반으로 전자서명을 생성하고 검증함으로써 무결성과 부인방지, 본인확인 등의 종합적인 보안기능을 제공한다[33, 34].

공인인증서는 X.509 기반이며, X.509는 X.500 디렉터리 서비스를 보충하기 위한 인증구조로서, X.509와 X.500 모두 ISO/ITU의 표준 X시리즈의 부분이다. X.500은 디렉토리 서비스를 제공하는 것이고, X.509는 이 서비스를 인증하기 위한 PKI 구조를 제공한다. X.509의 가장 오래된 제안으로 첫 번째 버전(C1)은 1998년에 만들어져 Visa와 MasterCard가 안전한 SET 표준으로 채용하였고, Entrust와 TimeStep과 같은 인트라넷을 지원하는 회사들에서도 활용되었다[35].

전자서명법 제2조 제7호와 제8호에 명시된 전자서명의 정의는 전자서명 생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보로서 공인인증기관이 발급하는 인증서를 말한다[36]. 기술적으로는 전자문서의 해쉬 값을 서명자의 개인키로 암호화한 데이터이고, 서명자의 공개키로 암호화된 데



〔그림 10〕 공인인증서를 이용한 전자서명 및 검증과정

이터를 복호하여 검증대상 전자문서의 해쉬 값과 비교함으로써 전자서명을 검증한다[37,38]. 이에 대한 과정을 그림 10에 나타내었다.

Step 1. 메시지 해쉬: 사용자는 거래정보와 같이 전달하고자 하는 메시지를 해쉬 알고리즘을 통하여 해쉬 값을 생성한다.

Step 2. 해쉬된 메시지 서명: 해쉬된 메시지를 공인인증서 암호를 입력하여 추출된 사용자 공인인증서의 개인키로 서명한다.

Step 3. 메시지, 서명, 공개키 전달: 사용자는 메시지와 서명, 사용자 공인인증서의 공개키를 인터넷 뱅킹 서버로 전달한다.

Step 4. 메시지 해쉬: 인터넷 뱅킹 서버는 전달받은 메시지를 검증하기 위하여 해쉬 알고리즘을 통하여 해쉬 값을 생성한다.

Step 5. 해쉬 추출: 사용자로부터 전달받은 공개키를 활용하여 서명된 메시지로부터 해쉬 값을 추출한다.

Step 6. 서명 검증: 인터넷 뱅킹 서버에서 생성한 해쉬 값과 전달받은 서명된 메시지로부터 추출한 해쉬 값을 비교함으로써 서명을 검증한다.

공인인증서는 전자서명 생성정보(개인키)가 가입자에게 유일하게 속한다는 사실을 확인하고 증명하는 전자적 정보이기 때문에 이를 통하여 사용자 본인임을 확인한다. 전자서명법에 따라 국가에서 지정한 공인인증기관에서 발행하며, 사용자 본인의 공개키, 일련번호, 이름, 유효기간 등의 정보를 포함한다. 공인인증서의 주요 구성요소를 표 3에 나타내었다[38].

공인인증서가 활성화됨에 따라 인터넷 뱅킹, 온라인 증권거래, 전자민원, 쇼핑몰, 주택청약 등 전자거래 전반에 본인 및 신원확인, 전자서명의 수단으로 활용하고 있으며, 금융분야에서 비금융분야로 점차 확대되고 있다. 그 사례를 살펴보면 2000년 전자입찰, 2001년~2005년에는 인터넷 뱅킹 및 증권업무, 2006년~2009년

〔표 3〕 공인인증서 주요 구성요소

주요 구성요소	설명
일련번호	공인인증서 일련번호
발행기관 식별명칭	공인인증기관 식별명칭
유효기간	공인인증서 유효기간 시작일과 만료일을 명시
소유자 식별명칭	공인인증서 소유자의 실명을 포함한 식별명칭
공개키	공인인증서 소유자의 공개키
공개키 사용목적	공개키의 사용목적을 명시(전자서명, 암호화 등)
인증서 정책	공인인증서 발행기관이 인증서를 발행하는데 적용한 인증서 정책과 인증업무 준칙을 명시
발행기관의 서명 값	위의 내용이 진실임을 증명할 공인인증기관의 전자서명 값

에는 주택청약 및 연말정산, 2010년 이후로는 인감대체 수단으로 이용되고 있다.

공인인증서를 이용하기 위해서는 공인인증기관으로부터 인증서를 발급받아야 하며, 전자서명을 수행하는 소프트웨어를 설치하여야 한다. 이를 공인인증서 가입자 설비 혹은 가입자 소프트웨어라 부른다. 가입자 소프트웨어는 웹 사이트에 접속할 경우 설치되거나 실행되며, 대부분 active-X 기반으로 구현된다.

3.1.2.3. 스마트카드 방식

스마트카드는 가로 85.6mm, 세로 54mm, 두께 0.76mm의 물리적 특성을 가지며, 내부에 마이크로프로세서, 카드 운영체제, 보안모듈, 메모리로 구성된 신용카드 크기의 플라스틱 카드를 의미한다[39, 40]. 스마트카드는 리더기와의 접촉 방식에 따라 ISO 7816 표준인 접촉식과 ISO 13338 표준인 비접촉식으로 분류되며, 현금카드나 신용카드 등의 기능을 포함하여 ATM (Automated Teller Machine) 기기 등에서 예금인출 등의 거래에 사용하는 범용적인 기술이다[41].

과거 스마트카드 기술은 계좌정보와 같은 비밀정보를 스마트카드 내의 메모리에 보관하고 PIN(Personal Identification Number)을 통한 접근제어를 제공하는 기술이 활용되었지만, 최근에는 Java Card나 Global Platform[42]과 같은 기술을 적용함으로써 연산기능을 지원하는 경우가 대부분이다. 이러한 기술을 지원함으

로써 스마트카드 내의 애플릿 등의 접근함수를 통하여 동작하고, 해당 함수를 통해서만 비밀정보에 접근할 수 있어 복제를 불가능하게 하고[3], 역공학과 같이 조작을 하는 공격을 불가능하게 한다.

이와 같은 장점에도 불구하고 별도의 리더기가 반드시 필요하므로 ATM 기기 등에서 한정적으로 사용되는 단점이 있지만, 스마트카드 기능을 제공하는 SIM (Subscriber Identification Module) 카드를 이용한 스마트폰에서의 인터넷 뱅킹 인증기술이나[43] 스마트폰의 NFC(Near Field Communication) 기술을 활용한 거래서명 기술이 연구되고 있다[44].

3.1.2.4. 하드웨어 보안토큰 방식

PC에 저장된 공인인증서의 유출문제를 해결하고자 “전자거래 안전성 강화 종합대책”에서 공인인증서를 하드웨어 보안토큰에 저장하도록 권고하였다. 하드웨어 보안토큰은 거래와 관련된 비밀정보를 안전하게 저장하고 관리하기 위하여 키와 전자서명과 같은 정보의 생성을 기기 내부에서 처리하도록 구현된 하드웨어 기기이며, 마이크로컨트롤러유닛(MCU, Micro Controller Unit), 운영체제, 보안모듈로 구성된다[45].

하드웨어 보안토큰은 표준설정, 제품인증 과정을 거쳐 2007년 11월에 국내에 출시되었으며, 2008년 초부터 국내 금융회사에 적용되기 시작하였다[46]. 스마트카드와는 다르게 별도의 리더기를 필요로 하지 않고 USB, 시리얼, 블루투스 등으로 컴퓨터와 연결되며, 거래와 관련된 정보는 토큰 내부에서 자체적으로 생성된 비밀키나 공인인증서의 개인키를 기반으로 암호화 혹은 서명되어 인터넷 뱅킹 서버에 안전하게 전달된다. 토큰 내부에 저장된 비밀키나 공인인증서의 개인키와 같은 비밀정보는 외부로 유출되거나 복제되지 않고 비밀정보를 기반으로 생성된 입력 값에 대한 출력 값만 전달되므로 높은 보안성을 제공한다. 게다가 지식기반 본인확인수단 중 하나인 고정 비밀번호를 함께 사용함으로써 보안성을 더욱 향상시키고, 고정 비밀번호의 설정 및 입력횟수를 제한하여 오류횟수가 초과할 경우 토큰을 사용할 수 없거나 초기화하는 기능도 제공하며, 반영구적으로 사용이 가능하다는 장점이 있다.

3.1.2.5. OTP 생성기 방식

금융감독원에서 2005년에 발표한 “전자금융 보안 종합 대책”에서 OTP 생성기를 제안하였고, 서울 상암동 DMC(Digital Media City)에 통합인증센터를 구축하여 2007년 6월 29일부터 9개 금융기관에서 인터넷 뱅킹 거래에 적용하였다.

OTP 생성기는 사용자가 본인을 확인할 때마다 매번 다른 비밀번호를 생성함으로써 고정 비밀번호가 가지는 한계를 보완하고자 제안된 방식이며, 하드웨어 OTP 생성기와 소프트웨어 OTP 생성기로 분류된다. 하드웨어 OTP 생성기는 OTP 생성기 내부에 대칭키 형태의 비밀정보가 안전하게 저장되고, 비밀정보를 기반으로 해쉬함수나 대칭키 알고리즘과 같은 OTP 생성 알고리즘을 통하여 생성된 31~64비트의 OTP 값을 OTP 값 추출 알고리즘(truncate 함수)을 통하여 6~8자리 숫자나 문자로 축약하여 LCD(Liquid Crystal Display)에 출력하면, 사용자가 이를 확인하여 입력하는 방식으로 이루어진다. 소프트웨어 OTP 생성기도 기본적인 개념은 하드웨어 OTP 생성기와 동일하지만, 별도의 기기를 소유하지 않고 소프트웨어 형태로 구성되어 사용자 PC에서 생성되는 방식이다.

OTP 생성기의 시초인 S/KEY 모델은 난수 r 값에 함수 f를 n+1번 수행하여 X_{n+1}을 구한 뒤, r과 X_{n+1}을 OTP 사용자와 검증자에게 전달하며, 검증 시 사용자가 X_n을 전달하면 서버가 이 값에 함수 f를 수행한 결과와 초기 값을 비교하여 올바른 경우 저장된 X_{n+1}을 X_n으로 갱신하는 방식이었다. 하지만 이와 같은 방법은 n 값을 재설정하여야 하는 문제점이 있어 이를 개선함으로써 현재의 OTP 생성기와 같은 형태가 되었다.

OTP 생성기는 현재 사용하는 비밀번호를 이용하여 다음에 사용될 비밀번호를 유추하는 것이 불가능하고, 오프라인 추측 공격과 사전 공격으로부터 안전성을 제공한다[15, 47]. 이와 같은 특성은 탈취된 비밀번호를 재사용하는 공격에 강인하며, PIN이나 지문인식 등을 함께 사용하여 투팩터 인증을 지원할 수 있어 기존의 비밀번호 방식에 비하여 더욱 안전하게 활용될 수 있다.

OTP 생성기에서 제공하는 투팩터 방식은 하드웨어 PIN 방식과 소프트웨어 PIN 방식이 있다. 하드웨어 PIN 방식은 OTP 생성기에 올바른 PIN 번호를 입력하여야 OTP 생성기가 활성화되기 때문에 PIN 번호를 아는 본인이 아니면 OTP 값을 생성할 수 없으므로 투팩터 인증을 제공한다. 소프트웨어 PIN 방식은 OTP 생성기에 대한 접근을 제어하는 하드웨어 PIN 방식과는 다르게, 사용자가 인증을 요청할 경우 소프트웨어 PIN 번호와 OTP 번호를 함께 전송함으로써 투팩터 인증을 제공한다. 이와 같은 투팩터 인증은 제3자가 단순히 기기만을 획득한 경우에는 PIN 번호를 모르기 때문에 OTP

생성기의 악용을 방지한다.

OTP 생성기의 종류로는 OTP 전용기기, 모바일 OTP, 카드형 OTP, 보이스 OTP 등의 매체가 있으며[48], OTP 값의 생성 방식에 따라 비동기화 방식과 동기화 방식으로 분류된다. 동기화 방식은 동기화 방법에 따라 시간 동기화 방식, 이벤트 동기화 방식, 조합 방식으로 분류된다[49-51].

비동기화 방식은 질의-응답(challenge-response) 방식이 대표적이며[52], OTP 생성기 도입 초기 금융권에서 주로 사용되었다. 이 방식은 클라이언트와 서버가 공유하는 비밀키를 기반으로 난수를 생성하여 질의한 결과에 대한 응답을 검증함으로써 사용자를 증명하는 방식이다. 세부과정을 살펴보면 클라이언트가 서버로 인증을 요청하면, 서버는 난수(질의 값)를 생성하여 클라이언트로 전송한다. 클라이언트에서 수신한 난수를 사용자가 OTP 생성기에 입력하면, OTP 생성기는 자신의 비밀키로 이를 암호화하여 응답 값을 출력한다. 사용자가 응답 값을 입력하여 서버로 전송하면, 서버는 자신의 비밀키로 암호화한 질의 값과 클라이언트로부터 수신한 응답 값을 비교하여 인증여부를 판단한다. 이 방식은 서버와의 동기화를 요구하지 않기 때문에 동기화에 필요한 부하를 줄일 수 있으며, 클라이언트와 서버가 상호인증을 수행한다는 장점이 있지만, 사용자가 직접 질의 값을 입력하여야 하고, 서버 측에서 질의 값을 관리하여야 하는 단점도 존재한다.

시간 동기화 방식은 서버와 OTP 생성기가 미리 동기화된 시간정보를 기반으로 특정 시간(일반적으로 1분)마다 OTP 값을 생성하는 방식이다. 이 방식은 사용자가 OTP 생성기에서 생성된 난수를 입력하여 서버로 전송하면 서버에서 이를 확인함으로써 사용자를 인증하기 때문에 중간자 공격 등의 공격에 의하여 OTP 값이 탈취되더라도 특정 시간 이내에 사용하여야만 공격이 성공하며, 특정 시간마다 OTP 값이 바뀌는 특성으로 인하여 탈취된 OTP 값을 재사용하는 공격에 강인한 장점이 있다. 하지만 OTP 값을 입력할 때 특정 시간이 지나면 OTP 값이 바뀌기 때문에 다시 입력하여야 하는 불편함이 있으며, 잘못 입력하였을 경우에도 특정 시간동안 기다려야 하는 단점이 있다.

이벤트 동기화 방식은 서버와 OTP 생성기가 동기화된 동일한 카운터 값을 공유한 후, 이를 통하여 비밀정보를 생성하는 방식이다. 이 방식은 해쉬체인을 이용하여 구성할 수 있으며, 최초 생성한 해쉬 값을 기반으로 해쉬체인을 생성한 후, 카운터 값에 해당하는 해쉬 값을 비교함으로써 인증을 수행한다. 따라서 한 번 생성된 OTP 값이 다시 생성될 때까지 변경되지 않는 특성이 있어 시간 동기화 방식이 가지는 특정 시간으로 인하여 발생하는 문제점을 보완하는 장점이 있지만, 사용자의 부주의나 악의적으로 여러 번 OTP 값을 생성시키면 서버와 OTP 생성기의 카운터 값이 동기화되지 않으므로 이를 보정하여야 하는 단점과 중간자 공격 등으로 OTP 값이 탈취될 경우 재사용이 가능한 문제점이 존재한다. 이러한 문제점을 보완하기 위하여 카운터의 오차범위(카운터~카운터+16)를 정하여 범위 내의 값일 경우나 연속된 두 번의 OTP 값이 일치하면 사용자를 올바르게 인증하는 세이프워드 OTP가 있다.

조합 방식은 시간 동기화 방식과 이벤트 동기화 방식의 장점을 조합한 방식으로 시간 동기화 중심의 조합 방식과 이벤트 동기화 중심의 조합 방식으로 분류된다. 시간 동기화 중심의 조합 방식은 특정 시간(24~32초)마다 OTP 값을 생성하며, 특정 시간 내에 다시 인증을 요청할 경우 카운터 값을 기반으로 OTP 값을 갱신하는 방식이다. 이 방식은 시간 동기화 방식이 가지는 특정 시간 내의 재사용 공격을 보완하는 장점이 있다. 이벤트 동기화 중심의 조합 방식은 특정 시간에 생성한 카운터 값을 기반으로 사용자가 인증을 요청할 때마다 OTP 값을 생성하는 방식이다. 이 방식 역시 이벤트 동기화 방식에서의 재사용 공격을 보완하는 장점이 있다[48, 53].

현재 OTP와 관련하여 국내/외에서 많은 표준이 정의되었다[53]. 일반적으로 OTP 생성기는 부인방지 기능을 제공하지는 않지만 신뢰기관이 보증하는 경우, ISO/IEC 13888-2[54] 표준을 준용하는 부인방지 기능을 제공할 수 있으며, PKI 인증서와 함께 사용하는 경우에도 부인방지 기능을 제공할 수 있다[55]. 최근에는 스마트폰의 USIM(Universal Subscriber Identification Module)을 활용한 USIM OTP[56]와 스마트카드와 스마트폰의 NFC 기능을 활용한 스마트 OTP, 거래정보와 연동하여 OTP 값을 생성하는 거래연동 OTP 등[57]이 연구되었다[58].

3.1.2.6. 거래연동 기술

거래연동 기술은 메모리 해킹과 같은 공격으로 거래정보를 위/변조하는 것을 방지하기 위하여 제안된 기술로 거래정보에 대한 서명을 생성하는 거래서명 기술과 거래정보와 연동된 정보를 생성함으로써 본인임을 확인하는 거래연동 기술로 분류된다.

거래서명 기술은 하드웨어 보안토큰과 같이 신뢰할 수 있는 장치에서 거래정보에 대한 서명을 생성하는 기

술이다. 기존의 본인확인수단은 사용자 PC에서 거래되는 환경으로 인하여 메모리 해킹과 같은 공격을 이용한 거래정보의 위/변조가 가능하므로 이를 보완하고자 제안된 기술로, 사용자가 서명을 생성하는 별도의 장치에 거래정보를 직접 입력하고 장치 내에 저장된 비밀정보를 기반으로 입력된 거래정보에 대한 서명을 생성하므로 거래정보에 대한 위/변조가 불가능한 특성이 있다. 이 기술은 거래정보를 입력하고 출력하여야 하므로 키패드와 같은 입력모듈과 LCD와 같은 출력모듈 등으로 구성되며, 영국을 포함한 유럽지역에서 사용되는 EMV(Euro, Mastercard, Visacard)의 CAP(Chip Authentication Protocol)[59]와 IBM의 ZTIC(Zone Trusted Information Channel)[60-62]이 대표적인 거래서명 장치이다. 거래서명 기술로는 SiB 거래서명 인증기술[4]과 MP-AUTH 거래서명 인증기술[63], NFC 거래서명 인증기술[64], MATS 거래서명 인증기술[3] 등이 있다.

SiB 거래서명 인증기술은 사용자의 PC가 안전하지 않으므로 인터넷 뱅킹 서버와의 통신을 위한 창구로 활용하고, 입력모듈이 부착된 별도의 장치를 통하여 계좌번호와 이체금액 등의 거래정보를 입력하면, 장치 내부의 스마트카드를 통하여 거래정보에 대한 서명을 생성하고 사용자 PC를 통하여 인터넷 뱅킹 서버로 전달하는 방식이다. 이 기술은 사용자 PC와 별도의 장치와의 통신채널이 필요한 공개키 방식과 단말기에서 출력된 서명정보를 사용자 PC에 입력함으로써 통신채널이 필요하지 않은 대칭키 방식으로 분류된다. 대칭키 방식은 EMV에 의하여 CAP 기술로 표준화되었고, 영국을 포함한 유럽에서만 3,000만 이상이 사용하며[65], 이를 활용하는 다양한 형태로 연구되었지만, 별도의 장치를 소지하여야 하는 불편함이 있다.

MP-AUTH 거래서명 인증기술은 SiB 거래서명 인증기술이 가지는 별도의 장치를 소지하여야 하는 문제점을 개선하기 위하여 휴대폰이나 스마트폰 등을 이용하여 거래정보를 사용자가 승인하는 공개키 방식의 거래서명 기술이며, 휴대폰을 활용한 다양한 방식의 거래서명 기술이 연구되었다[66, 67, 68, 69].

기존의 기술들은 은행이 사용자의 거래서명을 인증하는 기술을 제공하지만, 사용자가 은행으로부터 수신하는 거래정보를 검증할 수 없다는 문제점이 있다. 따라서 사용자와 은행이 상호인증을 제공하면서 부인방지 기능을 제공하는 MATS-1 기술과 MATS-2 기술이 연구되었으며, 부정거래를 차단하고 추적하는 기능을 제공한다[3].

거래서명 기술이 거래정보에 대한 서명을 생성하는 기술이라면, 거래연동 기술은 거래정보와 비밀정보가 연동된 정보를 생성함으로써 본인임을 확인하는 기술이다. 이 기술은 거래서명 기술로부터 개선되었으며, 2004년 영국 지불결제 연합(APACS, Association for Payment Clearing Service)에서 제안된 이후로 2006년 제안된 SiB 거래서명 인증기술과 CAP 기술을 참조하여 금융보안연구원에서 거래정보와 OTP 생성기를 결합시킨 거래연동 OTP 기술을 제안하였다[57]. 거래연동 OTP는 기존의 OTP 생성기에 거래정보를 입력하기 위한 숫자패드를 부착하여 거래정보의 일부와 생성된 OTP 값을 연동한 정보를 생성함으로써 거래정보를 위/변조하는 거래조작 공격에 효율적으로 대응이 가능하다.

그 밖에 거래연동 SMS 인증과 거래확인 보안토큰, 거래연동 2채널 인증 등이 연구되었다. 거래연동 SMS 인증은 문자메시지에 거래내역을 포함하여 SMS로 인증하는 방식이며, 거래확인 보안토큰은 하드웨어 보안토큰의 액정에 거래내역을 출력하여 인증하는 방식, 거래연동 2채널인증은 전화망을 이용하여 사용자가 거래내역을 확인하고 승인번호를 입력함으로써 인증하는 방식이다[70].

3.1.3. 특징기반 본인확인수단

특징기반 본인확인수단은 사용자 자체의 정보가 본인확인수단으로 활용된다. 사용자 자체의 정보란 사용자 신체의 일부분인 지문, 홍채, 정맥 등의 정보를 의미하며, 이러한 정보는 사용자마다 유일한 특징을 가지므로 복제가 거의 불가능하여 높은 보안성을 지원한다. 하지만 이러한 정보가 노출될 경우 유일성을 보장할 수 없고 신체를 활용한다는 부정적인 인식과 다른 본인확인수단들보다 높은 비용으로 인하여 인터넷 뱅킹 서비스에서는 적극적으로 활용되는 수단은 아니며, 대표적인 특징기반 본인확인수단으로 바이오 인증이 있다.

기존의 본인확인수단들은 대부분 사용자의 지식을 기반으로 비밀정보를 확인하고 이를 증명하는 과정으로 이루어져 있어 사용자 지식의 한계가 본인확인수단들의 한계와 밀접한 관계를 가진다. 이에 소지기반 본인확인수단들이 등장하였지만, 어느 정도 사용자의 지식을 요구하며, 소지한 기기의 비밀정보가 노출되거나 물리적인 복제 및 변경으로 인한 위험성도 존재한다. 이와 같은 문제점을 해결하고자 사용자가 가지는 고유의 정보를 기반으로 본인을 확인하는 바이오 인증이 등장하였다.

바이오 인증은 사용자 신체일부의 특징을 고유정보로 활용하여 이를 사전에 등록한 후, 검증 시 신체일부의 특징을 확인함으로써 본인을 확인하는 방식이다. 바이오 인증에서 사용되는 고유정보는 안면, 지문, 홍채, 정맥, 장문, 귀, 입술 등의 신체일부 그 자체를 이용한다. 따라서 이 방식은 사용자 신체가 반드시 필요하기 때문에 분실이나 변경의 위협으로부터 안전하게 보호되므로 보다 높은 보안성을 지원하지만[71], 신체를 확인하기 위한 별도의 단말 및 시스템을 구축하는데 많은 비용이 필요하며, 유출될 경우 심각한 결과를 가진다는 단점이 존재한다.

바이오 인증은 조달청의 나라장터 전자 입찰 시스템에서 대표적으로 활용되며, 소지기반의 하드웨어 보안토큰이나 OTP 생성기를 활성화하기 위하여 활용되기도 한다. 조달청의 나라장터 전자 입찰 시스템에서는 인증서를 대여하여 불법으로 대리 입찰하는 문제점을 보완하고자 지문 보안토큰을 도입하였으며, 사용자가 지문 보안토큰을 구매하여 신분증과 함께 등록기관에 제출하면, 등록기관은 지문 보안토큰에 주민등록번호 혹은 법인사업자등록번호와 3개의 손가락의 지문을 등록한다. 사용자는 이를 수령받아 주민등록번호 혹은 사업자등록번호와 지문인증을 통하여 공인인증서를 저장하고, 지문인증이 완료된 후에 저장된 공인인증서를 통하여 로그인 및 입찰에 참여하기 위한 서비스를 제공한다. 일반적으로 바이오 인증은 본인확인을 위한 수단으로 활용되므로 암호화나 무결성, 부인방지 등의 기능은 제공하지 않는다. 그러므로 보안토큰에 저장된 공인인증서에 대한 접근통제로 활용하고 공인인증서를 기반으로 거래정보의 암호화 및 전자서명 등을 수행함으로써 보안성을 향상시킨다.

그 외에 바이오 정보를 포함한 인증서에 대한 연구[72], 바이오 정보 데이터 교환 규격(CBEFF, Common Biometric Exchange Formats Framework)에서 바이오 정보를 포함하는 인증서에 대한 표준이 연구되었다[73].

3.1.4. 행동기반 본인확인수단

행동기반 본인확인수단은 사용자가 특정 행위를 할 때 나타나는 특성에 대한 정보를 검증하는 방식이며, 흔히 키보드를 입력하는 속도나 필체, 음성 등의 정보가 활용된다. 그리고 사용자가 인터넷 뱅킹 서비스를 할 때의 특성, 예를 들어 거래금액이나 시간 등의 패턴을 확인하는 위험기반 인증기술과 서비스를 요청하는 주체가 기계인지, 사람인지를 판단하는 휴먼인지 인증기술이 있다. 이와 같은 본인확인수단은 직접적으로 사용자를 인증하는 용도로 활용되지는 않지만, 위협을 탐지하거나 차단함으로써 보안성을 향상시키는 역할을 한다.

3.1.4.1. 위험기반 인증기술

위험기반 인증기술은 전통적으로 카드사에서 주로 이용되었으며, 사용자가 서비스를 이용하는 과정에서 나타나는 특징을 기반으로 본인임을 확인하는 방법이다. 지식기반과 소지기반, 특성기반의 본인확인수단은 사용자나 소지하는 장치를 기반으로 이루어지기 때문에 프런트-엔드 인증 방식이라 하며, 위험기반 인증기술은 거래내역 등의 정보를 실시간으로 분석하여 그 특성을 기반으로 이루어지기 때문에 백-엔드 인증 방식으로 분류된다. 미국 FFIEC(Federal Financial Institutions Examination Council) 가이드라인에서 2006년 말까지 금융기관에서 OTP 생성기, 바이오 인증과 더불어 백-엔드 인증기술을 도입하여야 할 것을 제시하였으며, 2003년 제정된 미국의 공정정확신용거래법(FACTA, Fair and Accurate Credit Transactions Act)에 따르면 2008년 11월 1일부로 카드사를 포함한 금융사들이 백-엔드 인증기술을 적용하였다고 한다.

이 기술에서 활용하는 정보로는 사용자의 국가, 도시, 시간 등의 물리적인 위치정보와 IP(Internet Protocol) 주소, 도메인, 라우팅 타입, ISP(Internet Service Provider) 정보 등의 논리적인 위치정보, 그리고 디바이스 쿠키, 브라우저 언어 및 버전, OS(Operating System) 버전 등의 디바이스 정보가 있으며, 이러한 정보를 활용하여 기존에 수집된 사용자의 정보와 다른 정보가 수집되거나 거래금액과 같은 트랜잭션과 관련된 정보가 수집되면 이를 탐지하여 서비스를 제한하는 기술이다. 이 방식은 정보를 수집한 후, 통계를 기반으로 이루어지기 때문에 퍼지로직이나 확률, 통계기반의 분석이나 뉴럴 네트워크와 같은 데이터 마이닝 기술을 탐지모델로 활용하지만, 오탐지나 미탐지와 같은 문제점으로 인하여 탐지가 될 경우, 보통 즉각적인 대응을 하는 것이 아니라 소지기반 본인확인수단의 OTP 생성기와 같이 다른 수단을 통하여 추가적으로 확인하는 단계를 거친다[18]. 국내에서는 이상거래 탐지기술로 불리며, 미국 VeriSign 사의 VIP(Verisign Identity Protection) 이상거래 탐지 서비스(Fraud Detection Service)가 있으며 HSBC 은행이 도입하였다[15].

3.1.4.2. 휴먼인지 인증기술

휴먼인지 인증기술은 인터넷 뱅킹 서비스에서의 취약점을 활용한 공격들이 사람이 아닌 자동화된 도구들에 의하여 발생한다는 사실에 기인하여 인터넷 뱅킹 서비스에 접속하는 주체가 사람임을 판단하는 인증기술이다. 대표적인 기술로는 사람만이 인식할 수 있는 문자를 일그러진 그림으로 출력하여 입력받는 CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart)[74]가 있다. 이 방식은 변조된 질의 값을 사용자가 쉽게 인지하기 어려워 DRM(Digital Rights Management)이나 문자서명 등의 기술과 함께 사용되어야 안전하다[75, 76, 77].

3.1.5. 소셜 네트워크기반 본인확인수단

소셜 네트워크기반 본인확인수단은 다른 본인확인수단과는 다르게 본인을 확인하는 것이 아닌 본인과 친분이 있는 사람을 인증함으로써 본인을 확인하는 방식이다. 이 방식은 본인을 직접 확인하지 않기 때문에 주된 본인확인수단을 사용하지 못하는 응급 상황에서 활용된다. 기존에는 이메일이나 등록정보 질의응답 방식, 고객센터를 통하여 응급 상황에 대처하였으나, 이메일은 보안성을 만족하기에는 불충분하고, 등록정보 질의응답 방식은 제3자가 응답을 유추할 수 있으며, 고객센터는 비용이 많이 필요하고 사회공학적 공격에 취약하다는 문제점이 존재한다. 이와 같은 문제점을 해결하고자 사용자와 친분이 있는 사람을 검증함으로써 본인을 확인하는 증빙 시스템(voucher system)이 연구되었다[78].

증빙 시스템은 질문자와 도움자로 구성되며, 질문자가 도움자에게 도움을 요청하면, 도움자는 자신을 인증함으로써 질문자를 인증하기 위한 증빙 코드(vouch code)를 수신하여 질문자에게 전달한다. 질문자는 도움자로부터 받은 증빙 코드를 통하여 본인임을 인증함으로써 임시 비밀번호를 발급받는 등의 방법으로 응급 상황에 대처한다.

3.2. 복합요소 본인확인수단

복합요소 본인확인수단은 단일요소 본인확인수단을 2가지 이상 복합적으로 사용하여 본인임을 확인하는 것을 의미하며, 단일팩터를 여러 가지 활용하는 '멀티팩터기반'과 통신채널을 여러 가지 활용하는 '멀티채널기반' 본인확인수단으로 나누어진다.

3.2.1. 멀티팩터기반 본인확인수단

멀티팩터기반 본인확인수단은 단일팩터 본인확인수단을 2가지 이상 복합적으로 사용하는 것으로, 예를 들어 지식기반의 고정 비밀번호를 활용하여 소지기반의 OTP 생성기 활성화하는 방식으로 단일요소 본인확인수단보다 강한 보안성을 제공하며[79], 동일한 방식의 단일팩터를 여러 가지 사용하는 경우, 예를 들어 지식기반의 고정 비밀번호와 지식기반의 등록정보 질의응답을 사용할 경우에는 멀티팩터기반 본인확인수단이라 할 수 없고, 하나의 팩터가 손상될 경우 다른 팩터에 영향을 주지 않도록 독립적이어야 한다. 이러한 이점으로 인하여 2005년 미국 FFIEC의 가이드라인에 의하여 금융권 도입을 권고하였으며[80, 81], 중국은 중국은행감독관리위원회(CBRC, China Banking Regulatory Commission)에서 발표한 "전자은행안전평가지침"에서 이중식별에 대한 언급이 있고[82], 유럽, 일본, 싱가포르, 한국 등의 국가에서도 권고하는 기술이다.

멀티팩터기반 본인확인수단과 관련된 많은 연구가 진행되고 있으며, 사용자가 인터넷 뱅킹 서버로 전송한 거래정보를 QR(Quick Response) 코드와 같은 2차원 바코드로 변환하여 사용자 PC에 출력하면, 이를 디코딩하여 사용자가 거래정보를 확인한 후, OTP 생성기를 통하여 OTP 값을 생성하는 기술[83], 위험기반 인증기술인 인터넷 프로토콜 주소 인증기술이나 지리적 주소 인증기술, 사용자가 이용하는 PC를 검증하는 이용 PC 지정 기술 등이 있다.

이 중 이용 PC 지정 기술을 상세히 살펴보면, 위험기반 인증기술의 일환으로 사용자가 인터넷 뱅킹 서비스에 접속하는 PC를 제한하고 접속하는 PC의 정보에 대한 일치여부를 판단하는 인증기술이다. 즉, 이용 PC 지정 기술은 사용자에 대한 인증뿐만 아니라 사용자가 접근 가능한 PC만이 특정 서비스를 이용할 수 있도록 디바이스를 인증하는 기술이다. 사용자가 인터넷 뱅킹 서비스와 같은 특정 서비스를 이용할 경우, 지식기반이나 소지기반 등의 1차적인 본인확인을 거친 후, 사용자 PC의 고유정보를 사전에 등록하며, 이후 서비스를 이용할 경우에는 고유정보를 가진 PC에서만 서비스를 제공하고 이외의 PC에 대해서는 서비스를 차단한다. 현재 은행 및 게임, 파일보안솔루션 등에서 이용 PC 지정 서비스를 제공한다.

이용 PC 지정 서비스의 동작과정을 자세히 살펴보면, 등록단계에서 사용자가 아이디-비밀번호, 공인인증서, 휴대폰 인증 등의 본인확인을 통하여 1차적인 본인

확인을 수행하고, 인증된 사용자가 사용하는 PC의 고유정보를 생성하여 서비스 제공자에게 전달한다. 서비스 제공자는 수신한 정보를 데이터베이스에 저장하여 서비스를 제공할 때 이를 검증하는 용도로 활용한다. 인증단계에서는 1차 본인확인을 거친 사용자가 자신의 PC를 검증하기 위하여 고유정보를 생성한 후, 이를 서비스 제공자에게 전달하면, 서비스 제공자는 데이터베이스에 저장된 고유정보와 전달받은 정보를 비교함으로써 본인임을 확인한다. 이는 등록된 PC가 아니면 서비스를 제공받지 못하므로 안전성을 보장한다[84].

3.2.2. 멀티채널기반 본인확인수단

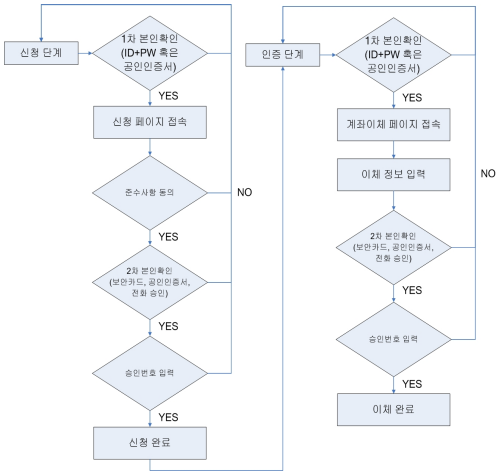
멀티채널기반 본인확인수단은 사용자의 전자적 장치와 인터넷 뱅킹 서버 사이의 통신채널을 두 가지 이상 활용하는 것으로, 일반적으로 유선망과 전화망을 이용하여 안전성을 지원한다[85]. 이는 다양한 형태로 활용될 수 있으며, 거래내역을 사용자 PC와 휴대폰으로 나누어 입력한 후, 서버에서 최종적으로 조합하는 방식이나 사용자 PC로부터 거래내역을 수신한 후, 휴대폰으로 인증번호를 전송하면, 사용자는 수신한 인증번호를 사용자 PC에 입력하여 서버로 전송하고 서버에서 전송한 인증번호와 수신한 인증번호를 비교하는 방식 등이 있다.

그 중 전화 승인을 상세히 살펴보면, 이용 PC 지정 서비스가 인터넷 뱅킹 서비스에서 이용하는 단말을 특정 기기로 제한하는 방안이라면, 전화 승인은 서비스를 이용할 때의 본인확인수단을 강화하는 방안이다. 기존의 본인확인수단들이 하나의 채널을 이용하여 인증함으로써 발생하는 문제점을 보완하기 위하여 분리된 채널을 이용하여 복수의 인증을 수행하며, 국내에서는 2007년에 도입하였고 이를 흔히 투채널 인증이라 불린다.

전화 승인이란, 사용자가 서비스를 이용하는 단말을 통하여 서비스에 필요한 정보를 서비스 제공자에게 전달하면, 서비스 제공자가 이를 확인한 후, 별도의 채널을 통하여 서비스 내역을 전달한다. 사용자는 수신한 서비스 내역을 확인하여 자신이 요청한 서비스 내역과 동일하다면 승인을 선택하고, 변경되었거나 서비스를 이용하지 않을 경우 취소를 선택하여 그 결과를 서비스 제공자에게 전달한다. 서비스 제공자는 별도의 채널을 통하여 수신한 서비스 이용결과를 확인하여 최종적으로 서비스를 인가한다. 즉, 최초 서비스를 이용할 때 대면 확인을 통하여 본인 명의의 전화번호를 등록하고, 차후 서비스 이용 시 등록된 전화번호를 통하여 사용자에게 서비스 이용에 대한 결정(승인 혹은 취소 등)을 입력받음으로써 서비스를 이용하는 주체가 사용자 본인임을 확인한다. 따라서 이와 같이 분리된 채널을 이용하여 복수의 인증을 하는 전화 승인을 통하여 사용자를 확인하면, 기존의 본인확인수단들에서 발생 가능한 보안위협으로부터 안전하게 보호된다. 이러한 장점에도 불구하고 통화 중이거나 통신장애 등의 문제가 발생하여 응답할 수 없는 경우에는 거래가 성립되지 않고, 통화에 시간이 많이 소모되므로 시스템에 과부하를 초래할 수 있는 단점이 존재한다.

일반적으로 전화 승인을 제공하는 방식은 인가코드 입력 방식과 사실안내 방식, 상세안내 방식이 있다. 인가코드 입력 방식 또한, 지정번호 입력 방식, 일회용 인증번호 입력 방식, 사용자 기억 인증번호 입력 방식으로 나누어진다. 지정번호 입력 방식은 고정된 번호를 입력하는 방식으로, 예를 들어 승인은 1번, 취소는 2번을 입력하는 방식이다. 일회용 인증번호 입력 방식은 고정된 번호가 아닌 안내에서 알려주는 일회용 번호를 입력하는 방식으로, 예를 들어 승인할 경우 39번, 취소할 경우 45번을 입력하라는 안내를 통하여 사용자가 승인을 결정하는 방식이다. 이 방식의 경우 매 승인마다 다른 입력번호를 요구하기 때문에 사용자가 직접 들어야만 정상적으로 입력이 가능하다는 장점이 있다. 사용자 기억 인증번호 입력 방식은 사전에 미리 사용자가 특정 번호, 즉, 승인번호를 등록하고 승인할 경우 승인번호를 입력함으로써 등록된 승인번호와 입력한 승인번호를 비교함으로써 승인여부를 판단한다. 사실안내 방식은 서비스를 요청하는 행위에 대한 사실만을 안내하는 방식으로 승인 및 취소 여부만을 판단한다. 예를 들어 계좌이체를 요청할 경우, 계좌이체 승인은 1번, 취소는 2번에 대한 입력을 받음으로써 승인여부를 판단한다. 상세안내 방식은 사실안내 방식보다 더 자세한 내역을 안내함으로써 사용자가 요청한 서비스 내역을 확인할 수 있도록 한다. 예를 들어 계좌 이체를 요청할 경우 A은행 a계좌에서, B은행 b계좌로, C금액이 이체된다는 안내와 함께 승인은 1번, 취소는 2번에 대한 입력을 받음으로써 승인여부를 판단한다. 상기 등록 및 인증 단계의 분석을 통하여 전화 승인의 등록 및 인증 과정의 흐름도를 그림 11에 나타내었다.

전화 승인에 사용되는 전화번호는 휴대 전화번호, 집 전화번호, 직장 전화번호 총 세 가지이다. 이 중 하나 혹은 둘 이상을 추가하려고 한다면 해당 번호를 추가한 후, 등록된 하나의 전화번호를 통하여 전화 승인이 이루어져야만 추가가 완료된다. 전화번호를 변경하는 경우



〔그림 11〕 전화 승인 등록 및 인증 단계 흐름도

도 이와 비슷하다. 변경을 원하는 전화번호를 선택하여 변경하면, 등록된 다른 전화번호를 통하여 전화 승인이 이루어져야만 변경이 완료된다. 만약 등록된 번호가 하나일 경우나 등록된 번호를 모두 변경하려고 한다면 영업점을 직접 방문하여야 한다.

전화 승인의 경우, 사용자가 서비스 해지를 원하면 영업점을 직접 방문하여 해지하여야 한다. 또한, 승인번호를 특정 횟수 이상 올바르게 입력하지 않았을 경우에도 영업점을 직접 방문하여 새로운 승인번호를 등록하여야 한다.

기타 멀티채널 인증방식으로 인증서를 이용한 투채널 인증방식, QR 코드 기반 투채널 인증방식, 멀티채널 기반의 일회용 가상 키패드, SMS 거래내역 통보 등이 있다. 인증서를 이용한 투채널 인증방식은 사용자가 PC를 통하여 거래정보를 인터넷 뱅킹 서버로 전송하고, 스마트폰과 같은 모바일 환경에서 인증서를 기반으로 승인한 정보를 서버에 전송하면, 서버는 수신한 두 정보를 비교함으로써 최종적으로 거래를 승인하며, 기존의 사용자가 보내는 정보를 금융기관만이 인증하는 단방향 거래인증 방식을 개선하여 금융기관에서 보내는 정보도 사용자가 인증하도록 양방향 인증을 제안함으로써 피싱에 안전하게 설계되었다[86]. QR 코드 기반 투채널 인증은 사용자가 PC에서 입력한 거래정보를 서버에서 QR 코드로 변환하여 웹 페이지에 출력하면, 사용자가 스마트폰으로 출력된 QR 코드를 디코딩하여 거래내역을 확인함으로써 최종 승인하는 방식이다[35, 39]. 멀티채널 기반의 일회용 가상 키패드는 하나의 채널에서 일회용 키패드를 출력하고, 다른 채널에서는 사용자로부터 출력된 일회용 키패드에 대한 값을 입력받는 방식이다[87]. SMS 거래내역 통보는 거래과정에 직접 참여하지는 않지만 거래가 승인되는 즉시 거래결과를 등록된 전화번호로 SMS를 발송함으로써 거래내역을 통지하는 방식이다.

Ⅳ. 결 론

본 논문에서는 인터넷 뱅킹 서비스에서 거래를 요청하는 주체가 사용자 본인임을 확인하기 위한 수단을 온라인 본인확인수단으로 정의하여 기존에 존재하는 각 수단을 조사하고 분류한 결과를 서술하였다. 온라인 뱅킹 서비스 뿐만 아니라 온라인을 통하여 다른 서비스를 제공하는 공급자의 입장에서 서비스를 요구하는 주체가 사용자 본인임을 확인하기 위한 수단을 참고하거나 새로운 온라인 본인확인수단을 제안할 경우, 기존 수단에 대한 참고 자료로써 활용 가치가 있을 것으로 기대된다.

향후 연구로는 본 논문에서 분류한 온라인 본인확인 수단의 각 방식을 기반으로 서비스 제공자가 더욱 안전하고 효과적으로 주체를 확인할 수 있도록 강화된 본인확인수단에 대한 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] D. Dolev and A. C. Yao, “On the Security of Public Key Protocols”, Proc. IEEE 22nd Ann. Sym. Foundations of Computer Science, IEEE CS Press, pp.350-357, 1981.

[2] 황부연, “MITB 공격에 안전한 투채널 기반 인터넷 뱅킹 시스템”, 고려대학교 정보보호대학원, 석사학위논문, 2012년 6월.

[3] 심희원, “온라인뱅킹의 확장된 상호인증 및 부인방지를 위한 거래서명 인증기술”, 전남대학교 대학원, 박사학위논문, 2011년 8월.

[4] A. Hiltgen, T. Kramp, and T. Weigold, “Secure Internet Banking Authentication”, J. IEEE Security & Privacy, 4(2), pp.21-29, 2006.

[5] R. Oppliger, R. Rytz, and T. Holderegger, “Internet Banking: Client-Side Attacks and Protection Mechanisms”, Computer, 42(6), pp.27-33, 2009.

[6] 송지훈, “내부정보유출 방지 솔루션 보안성 평가”, 대진대학교 대학원, 석사학위논문, 2009년 1월.

[7] 최옥현, “내부자에 의한 정보 유출 위협과 대응방안 수립에 관한 연구”, 한남대학교 경영산업대학원, 석사학위논문, 2009년 2월.

[8] 엄정호, 박선호, 정태명, “내부자의 불법적 정보 유출 차단을 위한 접근통제 모델 설계”, 한국정보보호학회 논문지, 20(5), pp.59-67, 2010년 10월.

[9] 차인환, “내부 정보보호를 위한 인원보안 관리방안 연구”, 한국전자통식학회 논문지, 3(4), pp.221-232, 2008년 12월.

[10] 송지훈, 이시진, 장항배, “내부정보유출 방지를 위한 데이터베이스 보안 솔루션 보안성 평가”, 한국정보기술학회 논문지, 7(3), pp.179-187, 2009년 6월.

[11] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, and L. Flynn, “Common Sense Guide to Mitigating Insider Threats (4th ed.)”, CERT Program, Software Engineering Institute, and Carnegie Mellon University, Dec. 2012.

[12] D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, “Common Sense Guide to Prevention and Detection of Insider Threats (3rd ed.)”, CERT Program, Software Engineering Institute, and Carnegie Mellon University, Jan. 2009.

[13] 이성운, 김현성, 유기영, “패스워드 기반의 효율적인 키 교환 프로토콜”, 한국정보과학회 논문지, 31(4), pp.347-352, 2004년 8월.

[14] 최은정, 김찬오, 송주석, “공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜”, 한국정보과학회 논문지, 30(1), pp.75-80, 2003년 2월.

[15] 금융보안연구원, “전자금융 新인증기술 연구보고서”, 2011년 3월.

[16] CA. corp., “Managing String Authentication: A Guide to Creating an Effective Management Syste”, 2007.

[17] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, “Forth-Factor Authentication: Somebody You Know”, Proc. 13th ACM Conference on Computer and Communications Security, pp.167-178, Oct. 2006.

[18] 임형진, 심희원, 서승현, 강우진, “전자 금융 거래 환경의 인증 기술 동향 분석”, 한국정보보호학회 학회지, 9(6), pp.73-79, 2008년 12월.

[19] P. Hanacek, K. Malinka, and J. Schafer, “e-Banking security – A comparative study”, IEEE Aerospace and Electronic Systems Magazine, 25(1), pp.29-34, Jan. 2010.

[20] 이형우, “안전한 로그인을 위한 소프트 보안카드 기반 다중 인증 시스템”, 한국콘텐츠학회 논문지, 9(3), pp.28-38, 2009년 3월.

[21] B. A. Forouzan, “Cryptography and Network Security”, Mc Graw Hill Higher Education, 2008.

[22] 맹영재, 신동오, 김성호, 양대헌, “전자금융거래에서의 문서변조 취약점 분석 및 대응방법 고찰”, 한국정보보호학회 논문지, 20(6), pp.17-27, 2010년 12월.

[23] 정태영, 이경률, 임강빈, “키보드해킹에 대비한 새로운 영상기반 패스워드”, 한국정보보호학회 학회지, 18(3), pp.41-47, 2008년 6월.

[24] Click Studios Blog, “PS5 Updata - ScramblePad Authentication”, http://clickstudios.wordpress.com/2011/01/24/ps5-update-scramblepad-authentication, Jan. 2011.

[25] 에너지관리공단, “그린홈”, http://greenhome.kemco.or.kr/index.do

[26] R. Oppliger and S. Gajek, “Effective Protection Against Phising and Web Spooping”, LNCS 3677, pp.32-41, 2005.

[27] K. Plossl, H. Federrath, and T. Nowey, “Protection Mechanisms Against Phising Attacks”, LNCS 3592, pp.20-29, 2005.

[28] B. Schneier and J. Kelsey, “Cryptographic Support for Secure Logs on Untrusted Machines”, Proc. the 7th USENIX Security Symposium, pp.53-62, Jan. 1998.

[29] C. Wuest, “”Phising In The Middle Of The Stream“-Today’s Threats To Online Banking”, Proc. 8th Association of anti Virus Asia Researchers Conference“, 200(6), Mar. 2005.

[30] A. Herzberg and A. Jbara, “Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks”, J. ACM

Transactions on Internet Technology, 8(4), Article No.16, Sep. 2008.

[31] 이원철, 이석래, 이재일, 김인석, “전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구”, 한국정보보호학회 학회지, 15(4), pp.43-48, 2005년 8월.

[32] 금융감독원, “전자거래 안전성 강화 종합대책”, 2005년 9월.

[33] S. Al-Riyami and K. Paterson, “Certificateless public key cryptography”, Proc. of Asiacrypt, LNCS 2894, pp.452-473, 2003.

[34] T. Elgamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, J. IEEE Transactions on Information Theory, IT-31(4), pp.469-472, 1985.

[35] 정상각, “전자금융거래에서의 QR CODE 기반 투-채널 인증기법의 제안”, 고려대학교 정보경영공학전문대학원, 석사학위논문, 2010년 12월.

[36] “전자서명법”, 법률 제10008호, 2010년 2월.

[37] ITU-T, “ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribution certificate frameworks”, Oct. 2012.

[38] 금융결제원, “전자금융거래시 공인인증서 의무사용 규제완화 관련 주요이슈 및 현황”, 2010년 7월.

[39] 이용재, “이중채널을 이용한 안전한 사용자 인증 및 전자금융거래시스템에 관한 연구”, 숭실대학교 대학원, 박사학위논문, 2011년 12월.

[40] 이형익, “부정이체 방지를 위한 실시간 IP 차단 시스템에 관한 연구”, 고려대학교 공학대학원, 석사학위논문, 2010년 8월.

[41] E, M. Hamann, H. Henn, T. Schack, and F. Seliger, “Securing e-business applications using smard cards”, IBM Systems Journal, 40(3), pp.635-647, Oct. 2001.

[42] GlobalPlatform Inc., “GlobalPlatform Card Specification version 2.2.1”, http://www.globalplatform.org/specificationscard.asp, Jan. 2011.

[43] L. Lunde, A. Wangensteen, “Using SIM for strong end-to-end Application Authentication”, Master of Science in Communication Technology, May 2006.

[44] D. A. Oritiz-Yepes, “Enhancing authentication in eBanking with NFC enabled mobile phones”, M. D. Thesis, Eindhoven University of Technology, Aug. 2008.

[45] 김지연, 권현조, 전길수, 임선간, 이재일, “HSM 제품 동향 및 안전성 분석”, 한국정보보호학회 학회지, 14(1), pp.76-90, 2004년 2월.

[46] 장윤근, “인터넷뱅킹 사용자 입력정보의 안전성 강화를 위한 대체방안에 대한 연구”, 동국대학교 국제정보대학원, 석사학위논문, 2009년 6월.

[47] N. Haller, C. Metz, P. Nesser, and M. Straw, “A One-Time Password System”, IFTF RFC 2289, 1998.

[48] 서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례”, 한국정보보호학회 학회지, 17(3), pp.18-25, 2007년 6월.

[49] P. Hoyer, “OTP and Challenge/Response algorithms for financial and e-goverment identity assurance: current landscape and trends”, Proc. ISSE Securing Electronic Business Processes, pp.281-290, 2009.

[50] N. M. Haller, “The S/KEY One-Time Password System”, Proc. Symposium on Network and Distributed Systems Security, pp.151-157, Feb. 1994.

[51] 최동현, 김승주, 원동호, “일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향”, 한국정보보호학회 학회지, 17(3), pp.12-17, 2007년 6월.

[52] D. M'Raihi, J. Rydell, S. Bajaj, S. Machani, and D. Naccache, “OCRA: OATH Challenge-Response Algorithm”, IETF RFC 6287, Jun. 2011.

[53] 송성현, 김근옥, “국내외 OTP 표준화 동향”, 한국정보보호학회 학회지, 22(2), pp.30-36, 2012년 4월.

[54] ISO/IEC 13888, “Information technology – Security techniques – Non-repudiation”, http://www.iso.org, 2009.

[55] 임형진, 이정근, 김문성, “안전한 인터넷 뱅킹을 위한 트랜잭션 서명기법에 관한 연구”, 한국인터넷정보학회 논문지, 9(6), pp.73-79, 2008년 12월.

[56] 금융보안연구원, “모바일 OTP 보안성 분석서”, 2009년 11월.

[57] 금융보안연구원, “거래연동 인증기술의 이해”, 이슈리포트, 2010(1), 2010년 11월.

[58] 금융보안연구원, “국내 금융OTP 이용 현황 및 동향”, 금융보안리포트, 2012(9), 2012년 12월.

[59] J. Tuliani, “Implementing CAP”, J. Card Technology Today, 18(10), pp.9, Oct. 2006.

[60] IBM ZTIC, “IBM Zone Trusted Information Channel”, http://www.zurich.ibm.com/ztic

[61] T. Weigold, T. Kramp, R. Hermann, F. Horing, P. Buhler, and M. Baentsch, “The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks”, LNCS 4968, pp.75-91, 2008.

[62] T. Weigold and A. Hiltgen, “Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services”, Proc. World Congress on Internet Security(WorldCIS), pp.125-132, 2011.

[63] X. Fang and J. Zhan, “Online Banking Authentication Using Mobile Phones”, Proc. 5th International Conference on Future Information Technology(FutureTech), pp.1-5, May 2010.

[64] D. A. Ortiz-Yepes, “Enhancing authentication in eBanking with NFC enabled mobile phones”, M. D. Thesis, Eindhoven University of Technology, Aug. 2008.

[65] O. Manahan, “Smart Card Talk”, http://www.smartcardalliance.org/pages/newsletter-201010-profile?issue=201010, 2014년 9월 열람.

[66] D. Scheuermann, “The smartcard as a mobile security device”, J. Electronics & Communication Engineering, 14(5), pp.205-210, Oct. 2002.

[67] F. Aloul, S. Zahidi, and W. El-hajj, “Two factor authentication using mobile phones”, Proc. IEEE/ACS International Conference on Computer Systems and Application(AICCSA), pp.641-644, May 2009.

[68] G. Starnberger, L. Froihofer, and K. M. Goeschka, “QR-TAN: Secure Mobile Transaction Authentication”, Proc. International Conference on Availability, Reliability and Security(ARES), pp.578-583, Mar. 2009.

[69] K. Fuglerud and O. Dale, “Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client”, J. IEEE Security & Privacy, 9(2), pp.27-34, Mar. 2011.

[70] 이한욱, 신휴근, “메모리 해킹 공격에 강건한 사용자 인증수단 고찰”, 한국정보보호학회 학회지, 23(6), pp.67-75, 2013년 12월.

[71] B. Hemery, J. Mahier, M. Pasquet, and C. Rosenberger, “Face Authentication for Banking”, Proc. 1st International Conference on Advances in Computer-Human Interaction(ACHI), pp.137-142, Feb. 2008.

[72] S. Santesson, Microsoft, M. Nystrom, RSA Security, T. Polk, and NIST, “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, RFC 3739, Mar. 2004.

[73] F. L. Podio, J. S. Dunn, L. Reinert, C. J. Tilton, B. Struif, F. Herr, J. Russell, M. P. Collier, M. Jerde, L. O'Gorman, and B. Wirtz, “Common Biometric Exchange Formats Framework”, NISTIR 6529-A, Apr. 2004.

[74] D. J. Steeves and M. W. Snyder, “Secure online transactions using a captcha image as a watermark”, U. S. Patent, US 11/157,336, Jun. 2005.

[75] F. Hartung and F. Ramme, “Digital rights management and watermarking of multimedia content for m-commerce applications”, IEEE Communications Magazine, 38(11), pp.78-84, Nov. 2000.

[76] A. Haouzia and R. Noumeir, “Methods for image authentication: a survey”, J. of Multimedia Tools and Applications, 39(1), pp.1-46, Aug. 2007.

[77] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, “Secure authentication using image processing and visual cryptography for banking applications”, Proc. 16th International Conference on Advanced Computing and Communications(ADCOM),

pp.65-72, 2008.

[78] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, “Fourth-Factor Authentication: Sombody You Know”, Proc. ACM conference on Computer and Communications Security (ACM CCS), pp.168-178, Oct. 2006.

[79] GPayments, “Two-Factor Authentication: An essential guide in the fight against Internet fraud”, http://www.gpayments.com/pdfs/WHITEPAPER_2FA-Fighting_Internet_Fraud.pdf, Feb. 2006.

[80] Federal Financial Institutions Examination Council (FFIEC), “Authentication in an Internet Banking Environment”, http://www.ffiec.govpdf/authentication_guidance.pdf, Oct. 2005.

[81] Financial Service Authority(FSA), “Countering Financial Crime Risks in Information Security”, Nov. 2004.

[82] 성재모, “국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응체계”, 전남대학교 대학원, 박사학위논문, 2011년 2월.

[83] 이영실, “2차원 바코드와 스트림 암호 기반의 모바일 OTP를 활용한 온라인 뱅킹용 인증 시스템”, 동서대학교 디자인 & IT 전문대학원, 석사학위논문, 2010년 8월.

[84] K. Lee and K. Yim, “A Guideline for the Fixed PC Solution”, Proc. International Conference on Smart Convergence Technologies and Applications(SCTA), pp.74-76, Aug. 2012.

[85] H. N. You, J. S. Lee, J. J. Kim, and M. S. Jun, “A study on the two-channel authentication method which provides two-way authentication in the Internet banking environment”, Proc. 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp.539-543, Nov. 2010.

[86] 유한나, “금융거래 시스템에서 모바일 인증서를 이용한 Two Channel 인증방식”, 숭실대학교 대학원, 석사학위논문, 2010년 6월.

[87] 박영록, 손진우, 신선호, 윤명근, “다중채널 기반의 안전한 금융거래 입력방식”, 한국정보보호학회 학회지, 23(1), pp.9-17, 2013년 2월.

〈저자소개〉

육 형 준 (Hyeungjun Yeuk)
학생회원

2010년 2월 : 동양대학교 전자유도기술학과(공학사)
2012년 8월 : 순천향대학교 정보보호학과(공학석사)
2013년 3월 ~ 현재 : 순천향대학교 정보보호학과 박사과정
관심분야 : 취약점 분석, 시스템 보안, 내부자 공격, 하드웨어 보안

임 하 빈 (Habin Yim)
학생회원

2012년 3월~2014년 2월 : 동신대학교 정보보안학과 학사과정
2014년 3월~현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 인터넷 뱅킹, 시스템 보안, 하드웨어 보안, 취약점 분석

이 경 률 (Kyungroul Lee)
정회원

2008년 8월 : 순천향대학교 정보보호학과(공학사)
2010년 8월 : 순천향대학교 정보보호학과(공학석사)
2015년 2월 : 순천향대학교 정보보호학과(공학박사)
2011년 5월~2011년 12월 : (미)퍼듀대학교 방문연구원
2015년 6월~현재 : 순천향대학교 박사후연구원
관심분야 : 취약점 분석, 시스템 보안, 하드웨어 보안, 인터넷 뱅킹, 사용자 인증, 디바이스 인증

임 강 빈 (Kangbin Yim)
종신회원

1992년 2월 : 아주대학교 전자공학과(공학사)
1994년 2월 : 아주대학교 전자공학과(공학석사)
2001년 2월 : 아주대학교 전자공학과(공학박사)
1999년 3월~2000년 2월 : (미)아리조나주립대학교 연구원
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
2009년 3월~현재 : 한국인터넷정보학회 이사
2010년 12월~2012년 2월 : (미)퍼듀대학교 객원교수
관심분야 : 취약점 분석, 내부자 공격, 보안 하드웨어 구조, 인증 프로토콜, 홈랜드 시큐리티