정 보 보 호 학 회 지
제23권 제6호, 2013. 12

메모리 해킹 공격에 강건한 사용자 인증수단 고찰

이 한 욱*, 신 휴 근**

요 약

최근 인터넷뱅킹 해킹 기술과 악성코드 배포 기술이 빠르게 진화하고 공격형태도 더 정교해짐에 따라 사용자 PC에 설치된 보안 도구만으로는 더 이상 전자금융 서비스의 안전성을 담보하기 어려워지고 있다. 이러한 상황에서 메모리 해킹 악성코드에 의한 불법 계좌이체 사고가 빈번하게 발생하여 사회적 이슈가 되고 있으며, 개정된 전자금융거래법에서는 고객의 PC가 해킹되었다고 하더라도 이로 인해 발생한 금융 사고에 대한 손해 배상을 금융회사가 우선 책임지게 되어 있어 대응이 필요한 시점이다. 본 논문은 기 발생한 메모리 해킹 악성코드에 의한 인터넷뱅킹 사고로부터 파생될 수 있는 공격유형을 도출하고 사용자 인증수단이 해당 공격유형에 어떤 취약점을 노출하는지 살펴봄으로써 사용자 PC에 메모리 해킹 악성코드가 감염되어 있다고 하더라도 안전하게 전자금융 서비스를 완료할 수 있는 사용자 인증수단을 고찰해 보고자 한다.

Ⅰ. 서 론

최근 정상적인 인터넷뱅킹 사이트에서 계좌이체를 위해 고객이 입력한 정보를 탈취하는 메모리 해킹 악성코드에 의한 인터넷뱅킹 사고가 빈번히 발생하고 있다. 악성코드의 배포 경로와 PC의 해킹 기술의 발전에 힘입어 악의의 공격자는 손쉽게 인터넷뱅킹 고객의 계좌비밀번호, 이체비밀번호, 보안카드 지시번호 및 하드디스크에 저장된 공인인증서를 탈취하여 불법 이체 거래를 수행할 수 있게 되었으나 이를 방지하기 위한 기술의 개발 및 적용은 더디다. 아울러, 개정된 전자금융거래법은 고객의 PC가 해킹되었다고 하더라도 이로 인해 발생한 금융 사고에 대한 손해배상을 금융회사가 책임지도록 하고 있어 전자금융 서비스 전반에 걸친 보안 대책이 필요한 시점이다.

오늘날의 PC에서 악성코드의 감염 경로를 완전히 차단하는 것은 사실상 불가능한 일이므로 고객 PC에 악성코드가 설치되어 있다고 하더라도 안전하게 전자금융 서비스를 제공할 수 있는 방법을 모색하는 것이 필요하다. 악성코드가 감염될 수 있다는 전제를 염두에 둔다면 PC 자체의 안전성을 강화하는 것에만 집중할 것이 아니라 PC 이외의 안전한 매체를 통하여 인터넷뱅킹 등 전자금융거래를 완결할 수 있는 수단을 찾아야 할 것이며 이러한 수단에는 OTP, 보안토큰 등의 사용자 인증수단이 있다.

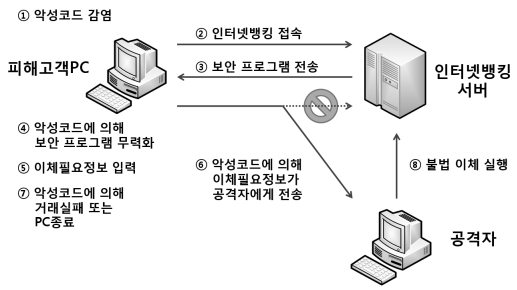
본 논문은 기 발생한 메모리 해킹 악성코드에 의한 인터넷뱅킹 사고유형 뿐 아니라 이로부터 파생될 수 있는 다양한 공격유형에 대해서도 안전하게 전자금융거래를 완결할 수 있는 사용자 인증수단에 대해 고찰하고자 한다.

Ⅱ. 인터넷뱅킹 사고내용

2.1 공격 세부절차

메모리 해킹 악성코드에 의한 인터넷뱅킹 사고(이하, 메모리해킹뱅킹사고)는 가짜 인터넷뱅킹 사이트로 유도하는 기존 파밍 공격과 달리 정상적인 인터넷뱅킹 사이트에서 계좌이체를 위해 보안카드 지시번호를 포함하여 고객이 입력한 정보(이하, 이체필요정보)를 가로챈 후 정상거래를 방해하면, 공격자는 이체필요정보를 악용하여 불법이체 공격을 수행한다. 그림 1은 메모리해킹뱅

* 금융결제원 정보보호기술팀 (hwlee@kftc.or.kr)
** 금융결제원 정보보호기술팀 (hkshin@kftc.or.kr)



〔그림 1〕 메모리해킹뱅킹사고 흐름도

킹사고의 전체 흐름을 보인다. 고객 PC가 악성코드에 감염되고(①), 피해고객이 정상적인 인터넷뱅킹을 수행하는 동안 이체필요정보를 입력하면(②~⑤), 악성코드가 이를 가로채서 공격자에게 전달하고 금융회사와의 정상거래를 방해한다(⑦~⑧). 공격자는 일정시간 경과 후, 피해고객이 입력한 이체필요정보를 이용하여 불법 이체를 실행한다(⑨).

2.2 공격 특징

메모리해킹뱅킹사고는 대부분의 인터넷뱅킹 이용고객이 유출되면 안전성을 완전히 상실하는 계좌비밀번호, 이체비밀번호, 보안카드, 하드디스크에 저장된 공인인증서만을 이용하고 있다는 점과 피싱 사이트 등을 통해 한꺼번에 지시번호 전부를 넘기는 비정상적인 경로를 제외하면 즉시 공격은 어려울 것이라 여겼던 보안카드 이용체계의 허점을 이용한다. 과거 이체 거래마다 임의의 보안카드 지시번호를 요청하던 방식은 공격자가 하나의 보안카드 지시번호만 알면 동일한 지시번호 요청이 발생할 때까지 반복시도를 통해 불법 이체를 완료할 수 있어, 2005년 금융감독원의 전자금융거래 보안 종합대책에 의해 '보안카드 비정상 오류 또는 종료 후 다음 거래 시 서비스 구분 없이 동일지시번호를 요구' 토록 변경하였다[1]. 하지만 메모리해킹뱅킹사고에서는 이를 역이용하여 피해고객이 입력한 보안카드 지시번호를 탈취한 뒤 고객이 이체거래를 완료하지 못하도록 방해하는 사이 탈취한 지시번호로 불법 이체를 수행하였다.

메모리해킹뱅킹사고를 유발한 악성코드는 기존의 악성코드와는 다른 방식으로 고객정보를 탈취하고 있다. 우선 기존의 일반적인 파밍 공격방법이 가짜 인터넷뱅킹 사이트로 유도하였던 것과는 달리 피해고객이 정상적인 인터넷뱅킹 사이트에 접속하였음에도 이체거래과정에 개입하여 고객의 입력 정보를 탈취하였다. 인터넷뱅킹 서비스에는 키보드보안(E2E 암호), 해킹차단기, 공인인증서, 온라인 백신 프로그램과 같은 보안 프로그램이 적용되어 있으나, 악성코드가 보안 프로그램의 메모리를 해킹하여 피해고객에게 보안 프로그램이 정상동작하는 것처럼 보이도록 하면서도 보안 프로그램이 제 역할을 다하지 못하도록 방해하는 방식으로 이를 가능하게 하였다. 그 결과 금융회사는 이체 거래가 중간에 정지되었지만 고객 PC의 보안 프로그램이 정상 동작하고 있었기 때문에 해킹 공격에 의한 것이라기보다는 고객 PC 또는 네트워크 장애에 의한 것으로 판단하기 쉽고, 또한 공격자에 의한 불법 이체 거래에 대해서는 이체에 필요한 모든 정보를 소지한 정상적인 고객에 의한 거래로 보이기 때문에 공격을 탐지하기 어려웠을 것으로 보인다.

마지막으로 메모리해킹뱅킹사고에서는 공격자가 보안카드 지시번호를 획득하고 일정시간 경과 후 불법 이체를 시도하는 공격 형태를 보이고 있으나 공격자의 의지에 따라 이체필요정보를 탈취한 즉시 공격하는 형태를 취하게 된다면 보안카드뿐 아니라 OTP를 이용하더라도 공격이 가능하게 될 것이다.

2.3 금융회사 조치사항

금융감독원은 소비자경보 2013-08호의 발령을 통해 인터넷뱅킹 시스템의 안전성을 확보하기 위하여 금융회사가 조치해야 할 사항을 발표하였다[2]. 이 조치사항은 단기적으로 가시적인 효과를 내기는 하였지만, 진화하고 있는 전자금융 공격방법에 적극적으로 대응하지 못하는 문제점을 지니고 있다.

- 비정상 종료 거래에 대해 본인확인 강화
- 악성코드 제거를 위한 백신프로그램 업데이트 및 배포
- 의심거래 발견 시 고객에게 SMS 통지 및 보안카드 재발급 유도
- 신종 전자금융사기로 인한 피해를 예방하기 위해 이메일, 팝업창 등을 통해 소비자 유의사항을 안내

악성코드의 감염 경로는 더욱 복잡하고 지능화되고 있고 백신 프로그램 등에 의한 악성코드의 탐지는 사후

처방에 지나지 않으므로 고객의 PC에 악성코드가 설치되지 않도록 방지하는 대책은 근본적으로 한계를 지닐 수밖에 없다.

Ⅲ. 메모리 해킹에 강건한 사용자 인증수단

이 장에서는 현재 인터넷뱅킹에 적용 중이거나 적용 가능한 사용자 인증수단을 거래내역의 확인 여부에 따라 분류하고, 메모리해킹뱅킹사고를 야기한 악성코드로부터 파생될 수 있는 인터넷뱅킹 공격유형을 도출한 뒤, 공격유형별로 사용자 인증수단의 취약점을 검토하여 메모리 해킹 공격에 강건한 사용자 인증수단을 도출하고자 한다.

3.1 사용자 인증수단의 분류

인터넷뱅킹에 적용 중이거나 적용 할 수 있는 사용자 인증수단은 거래내역 확인 가능 여부에 따라 표 1과 같이 분류할 수 있다. 최근 거래확인 대신 거래연동이란 용어를 많이 사용하고 있지만 공인인증 기반 기술의 경우 거래내역을 입력으로 하여 서로 다른 전자서명 값을 생성하므로 원칙적으로 거래연동 수단에 속하게 되므로 분류 기준이 불명확해 질 수 있다. 본 논문에서는 사용자 인증수단의 구분을 보다 엄밀하게 하기 위해 사용자가 적극적으로 개입하여 별도의 매체를 통해 거래내역을 입력하거나 확인할 수 있는 연동 수단을 거래확인 수단이라고 하겠다.

〔표 1〕 사용자 인증수단

구분	인증정보 전송방식	분류
거래확인 불가 사용자 인증수단	동일채널방식	고정 값
		보안카드
		공인인증서 (단순저장매체 저장)
		보안토큰
		단순 SMS인증
		OTP
	별도채널방식	단순 2채널인증
거래확인 가능 사용자 인증수단	동일채널방식	거래연동 SMS인증
		거래연동 OTP
		거래확인 보안토큰
	별도채널방식	거래연동 2채널인증

우선 거래내역을 확인할 수 없는 사용자 인증수단에는 고정 값, 보안카드, 단순저장매체에 저장된 공인인증서, 보안토큰, OTP, 단순 SMS인증 및 단순 2채널 인증 등이 있다. 고정 값은 계좌비밀번호, 계좌이체비밀번호, MAC 주소 등 매번 동일한 값으로 구성되어 일단 유출되면 안전성을 완전히 상실하는 수단을 의미한다. 보안토큰은 공인인증서 기반의 기술이나 단순저장매체에 저장된 공인인증서와 구별하여 비밀키가 외부로 유출되지 않도록 기기 내부에서 생성되고 거래별로 서로 다른 전자서명 값을 생성하도록 구현된 하드웨어를 말한다. 단순 2채널인증은 인터넷뱅킹이 실행되고 있는 채널(PC 등) 외의 다른 채널(유선전화, 스마트폰 등)로 인증 수행하는 것으로 “전화인증을 위해 5번을 입력해주세요” 또는 “홍길동 고객님께서 공인인증서 발급을 신청하셨습니다. 승인은 1번, 취소는 2번을 눌러주세요”의 예와 같이 거래내역이 포함되지 않는 경우를 말한다.

거래내역을 확인할 수 있는 사용자 인증수단에는 거래연동 SMS인증, 거래연동 OTP, 거래확인 보안토큰 및 거래연동 2채널인증 등이 있다. 거래연동 SMS인증은 문자메시지에 거래내역이 표시되는 SMS인증을 말하며, 거래연동 OTP는 OTP 기기에 부착된 숫자패드에 수신계좌번호, 거래금액 등 거래정보를 사용자가 직접 입력하여 OTP번호를 생성하는 수단을 말한다. 거래확인 보안토큰은 보안토큰 카드 또는 보안토큰 리더기에 보안토큰의 PIN입력을 위한 키패드가 부착되어 보안토큰 비밀번호가 외부로 유출되지 않으며 거래내역을 표시하는 액정이 부착되어 해당 거래내역에 대한 전자서명을 수행하는 수단으로 독일의 Secoder 표준에 따른 보안토큰 카드 및 리더기가 여기에 해당한다[3]. 그림 2는 상용되고 있는 거래연동 OTP와 거래확인 보안토큰의 예이다. 거래연동 2채널인증은 2채널인증의 방법 중 “홍길동 고객님, A은행 계좌에서 B은행 김철수님 계좌로 100만원이 이체됩니다. 승인하시려면 승인번호 4자리를 전화기에 입력하세요” 의 예와 같이 인터넷뱅킹이 실행되고 있는 채널 외의 다른 채널로 거래 내용을 확인하고 승인번호를 입력하여 인증 수행하는 것을 말한다.

3.2 공격자의 능력

메모리해킹뱅킹사고를 유발한 악성코드는 PC에 적용된 각종 보안 프로그램을 무력화하여 고객이 입력한

〔그림 2〕 카드형(左)/리더기형(中) 거래확인 보안토큰과 거래 연동 OTP(右)

각종 정보를 가로채고 거래가 완료되는 것을 방해한다. 이러한 악성코드로부터 파생될 수 있는 새로운 공격유형을 예측하고자 우리는 공격자가 정보접근 능력, 변조 능력, 실시간공격 능력 및 고객의 스마트폰 제어 능력의 네 가지 조합 가능한 능력을 지닐 수 있다고 가정하였다. 각각의 능력에 대해 살피보자.

정보접근 능력은 고객이 입력하거나 PC가 연산한 데이터에 접근할 수 능력을 말한다. 공격자가 배포한 악성코드가 고객의 감염된 PC의 각종 보안 프로그램을 무력화하고 고객의 각종 입력정보와 연산 결과를 가로채 공격자에게 전송함으로써 공격자는 해당 능력을 획득할 수 있다.

변조 능력은 고객이 입력하거나 PC가 연산한 데이터를 변조할 수 있는 능력을 말한다. 공격자가 배포한 악성코드가 공격자의 의도에 따라 사전에 지시된 형태로 고객의 각종 입력 정보와 연산 결과를 변조함으로써 공격자는 해당 능력을 획득할 수 있다.

실시간공격 능력은 고객의 이체필요정보 및 누적된 거래 정보를 바탕으로 공격자가 자신의 PC에서 실시간으로 불법이체를 수행할 수 있는 능력을 말한다. 공격자가 배포한 악성코드가 고객의 이체필요정보를 공격자에게 실시간으로 전송하므로 공격자는 자신에 의지에 따라 고객의 거래정보를 관리하고 고객의 입력을 실시간으로 모니터링하면서 불법이체를 수행할 수 있다. 아울러, 최근 해킹사고는 공격자가 공격대상을 장기간 관찰하여 정보를 수집한 뒤 공격을 시도하는 추세이므로 이 능력은 타당하다.

마지막으로 스마트폰 제어 능력은 고객의 스마트폰을 제어하는 능력이다. 고객의 PC를 감염시킨 악성코드가 유럽에서 발생한 Eurograbber 공격[4]에서처럼 인터넷뱅킹 사이트에서 정상적인 페이지를 가장하여 스마트폰에 특정 앱을 설치하도록 유도하여 고객에게 전송된 SMS를 가로채거나 착신 전환 등을 수행함으로써 공격자는 해당 능력을 획득할 수 있다.

3.3 공격유형별 사용자 인증수단의 안전성 분석

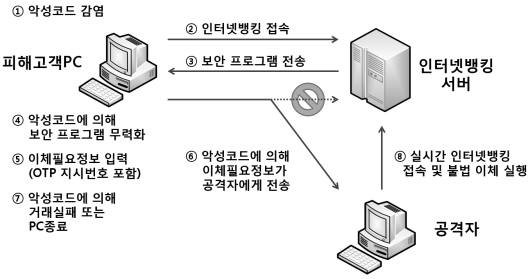
표 2와 같이 공격자가 획득한 능력에 따라 발생 가능한 인터넷뱅킹 공격 유형을 실시간 공격유형, 스마트폰 공격유형 및 변조 공격유형으로 분류하고 각각에 대해 살펴보고자 한다. 기존 사용자 인증수단 중 고정 값, 보안카드 및 단순저장매체에 저장된 공인인증서는 쉽게 탈취되어 재사용될 수 있기 때문에 대상에서 제외한다.

3.3.1 실시간 공격유형

실시간 공격유형은 고객이 악성코드에 감염된 PC에서 이체필요정보를 입력하면 악성코드가 이를 가로채 공격자에게 전송하고 피해고객의 정상적인 이체실행을 방해하는 중에 공격자가 실시간으로 불법이체를 수행하는 유형이다. 이 유형의 공격자는 고객 PC에 대한 정보접근 능력과 실시간 공격 능력을 지니고 있으며 실시간 공격이란 점을 제외하면 메모리해킹뱅킹사고의 공격과 유사하다. OTP 지시번호 또는 단순 SMS인증의 인증코드와 같이 일정한 시간 범위를 가지고 유효한 값이 변동되는 사용자 인증수단에 대해 효과적인 가로채기 공격이 가능하다. 악성코드가 감염된 PC에서 직접 불법 이체를 시도하는 것이 아니기 때문에 데이터를 변조할 필요 없이 입력 정보를 가로채거나 정상 사용자의 인증을 유도하는 방법으로 공격을 수행한다. 다만, 고객과 공격자의 거래내역이 서로 다르므로 거래내역을 확인할 수 있는 사용자 인증방법에 대해서는 공격자가 고객을 속이기가 쉽지 않고 인증 값을 가로채어 사용할

〔표 2〕 공격유형

공격유형	필요 공격자 능력			
	정보접근 능력	변조 능력	실시간공격 능력	스마트폰 제어 능력
실시간 공격유형	○		○	
스마트폰 공격유형	○			○
변조 공격유형	○	○		



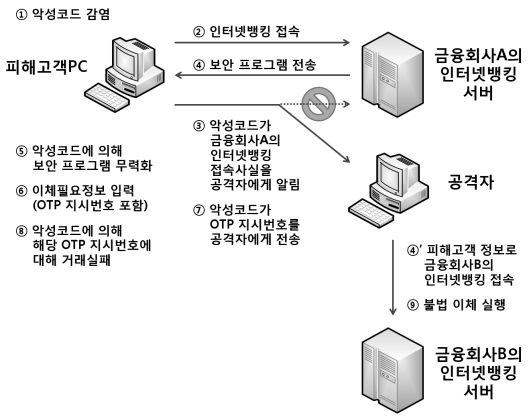
〔그림 3〕 실시간 공격유형의 OTP 동행공격의 예

경우 서버에서 쉽게 검증된다. 이 공격유형은 거래내역을 확인할 수 없는 모든 사용자 인증수단을 무력화할 수 있다.

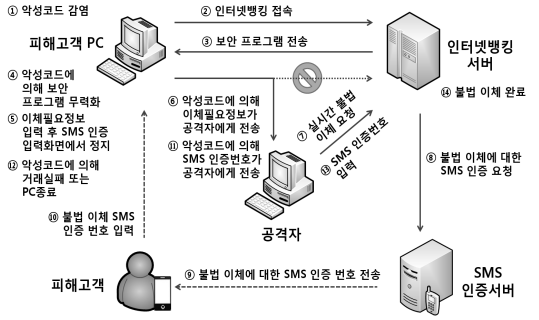
이 공격유형의 공격자는 가로채기를 이용한 OTP 동행 공격과 타행 공격, 단순 SMS인증 공격 및 인증유도를 통한 단순 2채널인증 공격을 수행할 수 있다. 각각의 공격에 대해 살펴보자.

우선 가로채기를 이용한 OTP 동행 공격은 그림 3에서 보는 바와 같이 악성코드가 OTP 지시번호를 가로채 공격자에게 전송하면(①~⑦), 공격자는 고객이 접속한 금융회사의 인터넷뱅킹에 실시간으로 접속하여 불법 이체를 수행한다(⑧). 이 경우 OTP 지시번호의 유효기간에 의해 공격 가능한 시간에 제한이 있지만 악성코드가 인터넷뱅킹 서버로의 접근을 차단하면서 다음 OTP번호를 요구하는 방식으로 공격시간을 늘일 수 있다. 메모리해킹뱅킹사고처럼 피해고객의 PC에서 지속적으로 이체거래를 실패하거나 PC가 종료되는 현상이 발생할 수 있다.

두 번째로 가로채기를 이용한 OTP 타행 공격은 악성



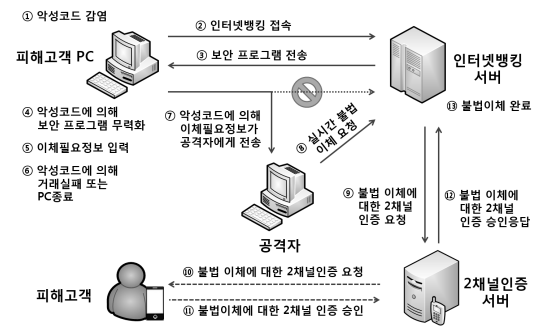
〔그림 4〕 실시간 공격유형의 OTP 타행공격의 예



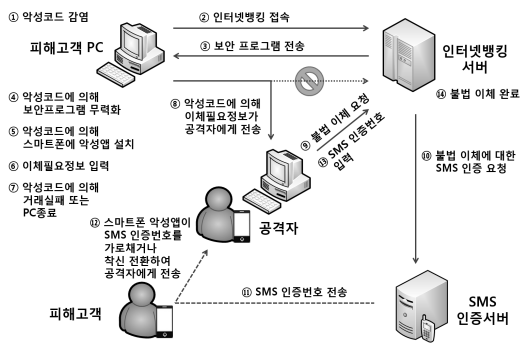
〔그림 5〕 실시간 공격유형의 단순 SMS인증 공격의 예

코드에 의해 금융거래 정보가 지속적으로 노출·수집되어 고객이 복수의 금융회사에서 OTP를 사용하는 것이 확인된 경우, 통합인증 방식 OTP의 허점을 이용하여 공격할 수 있다. 그림 4에서 악성코드가 OTP 지시번호를 가로채 공격자에게 전송하면(①~⑧), 공격자는 피해고객이 접속한 금융회사 외의 타 금융회사의 인터넷뱅킹에 실시간으로 접속하여 피해고객이 입력한 OTP 지시번호로 불법 이체를 수행한다(⑨). 악성코드가 첫 OTP 지시번호에 대해서만 거래를 방해하고 다음 OTP 지시번호에 대해서는 정상 거래가 이루어지도록 하면 앞의 동행공격의 예와는 달리 피해고객의 PC에서 지속적으로 이체거래를 실패하거나 PC가 종료되는 현상은 발생하지 않아 고객이 해킹 사실을 눈치 채기 어렵다.

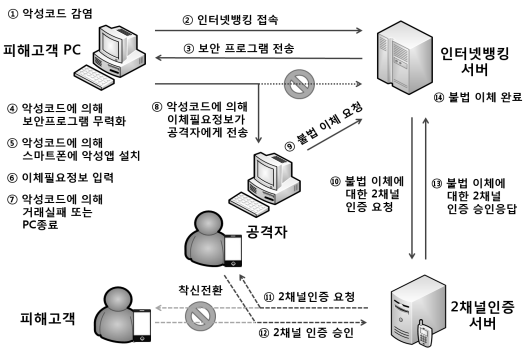
세 번째로 가로채기를 이용한 단순 SMS인증 공격은 공격자가 불법 이체를 수행하면 피해고객의 휴대전화로 SMS 인증코드가 전송되지만 피해고객이 거래 내역을 확인하지 못한다는 점에 착안한 공격방법이다. 그림 5에서 악성코드가 고객의 정상적인 계좌 이체를 방해하는 사이(①~⑥), 공격자가 불법 이체를 수행하여 인증번호를 전송하고(⑦~⑨), 고객이 이를 정상 이체에 대한



〔그림 6〕 실시간 공격유형의 단순 2채널인증 공격의 예



〔그림 7〕 스마트폰 공격유형의 단순 및 거래연동 SMS 인증 공격의 예



〔그림 8〕 스마트폰 공격유형의 단순 및 거래연동 2채널 인증 공격의 예

인증코드로 인식하여 입력하면(⑩), 악성코드가 가로채 공격자에게 전송한다(⑪). 동일 계정에 대한 인터넷뱅킹 동시접속이 제한되므로 메모리해킹뱅킹사고처럼 피해고객의 PC에서 지속적으로 이체거래를 실패하거나 PC가 종료되는 현상이 발생할 수 있다.

마지막으로 인증 유도를 통한 단순 2채널인증 공격은 공격자가 불법 이체를 수행하면 피해고객의 전화로 2채널인증 전화가 발신되지만 피해고객이 거래 내역을 확인하지 못한다는 점에 착안한 공격방법이다. 그림 6에서 악성코드가 피해고객의 정상적인 계좌 이체를 방해하는 사이(①~⑦), 공격자가 불법 이체를 수행하여 2채널인증 전화를 발신하게 하면(⑧~⑩), 피해고객이 이를 정상 이체에 대한 2채널인증으로 인식하고 승인하여(⑪) 불법 이체가 완료된다. 앞에서와 같이 피해고객의 PC에서 지속적으로 이체거래를 실패하거나 PC가 종료되는 현상이 발생할 수 있다.

3.3.2 스마트폰 공격유형

스마트폰 공격유형은 스마트폰을 이용하여 인증을 수행하는 고객의 PC와 스마트폰에 각각 설치된 악성코드와 악성앱이 고객의 이체필수정보와 인증정보를 가로채는 유형이다. 이 유형의 공격자는 고객 PC에 대한 정보접근 능력과 스마트폰 제어 능력을 지니고 있다. 안드로이드 계열과 같이 정식 앱스토어(마켓)가 아닌 인터넷에서 다운받은 파일로 앱을 설치할 수 있는 스마트폰에 대해 유효한 공격유형이며, 공격자가 앱스토어에 악성앱을 등록할 경우 보다 실효성 있는 공격을 수행할 수 있다. 대신, 피처폰이나 유선전화와 같이 외부 공격자의 통제가 어렵거나 불가능한 단말기는 공격 대상이 되기 어렵다. 피해고객의 스마트폰에 악성앱이 설치되면 공격자는 실시간으로 공격할 필요 없이 자신이 원하는 시간대에 공격을 수행할 수 있고 비활동 시간대인 심야에만 악성앱이 작동하도록 할 경우 피해고객이 악성앱의 존재를 눈치 채기 어려워진다. 동일 계정에 대한 인터넷뱅킹 동시접속이 제한되므로 메모리해킹뱅킹사고처럼 피해고객의 PC에서 지속적으로 이체거래를 실패하거나 PC가 종료되는 현상이 발생한다. 이 공격유형은 스마트폰을 통해 인증을 수행하는 모든 사용자 인증수단(단순 및 거래연동 SMS인증, 단순 및 거래연동 2채널인증)을 무력화할 수 있다.

이 공격유형의 공격자는 가로채기를 이용하여 단순 및 거래연동 SMS인증과 단순 및 거래연동 2채널인증 공격을 수행할 수 있다. 각각의 공격에 대해 살펴보자.

우선 단순 및 거래연동 SMS인증 공격은 그림 7과 같이 악성코드가 피해고객의 정상적인 계좌 이체를 방해하고(①~⑧), 이후 공격자가 불법이체를 수행하여 피해고객의 스마트폰으로 SMS 인증코드를 발송하게 하면(⑨~⑪), 고객의 스마트폰에 설치된 악성앱이 인증코드를 가로채거나 착신 전환을 통해 공격자에게 전송하여 불법 이체를 완료한다(⑫~⑭). 공격자가 실제 인증을 수행하므로 거래연동의 여부와 상관없이 공격이 이루어진다.

단순 및 거래연동 2채널인증 공격은 그림 8과 같이악성코드가 피해고객의 정상적인 계좌 이체를 방해하고(①~⑧), 이후 공격자가 불법이체를 수행하여 피해고객의 스마트폰으로 2채널인증 전화를 발신하게 하면(⑨~⑪), 고객의 스마트폰에 설치된 악성앱이 해당 전화를 공격자에게 착신 전환하여 불법 이체를 완료한다(⑫~⑭). 이 역시 공격자가 실제 인증을 수행하므로 거래연

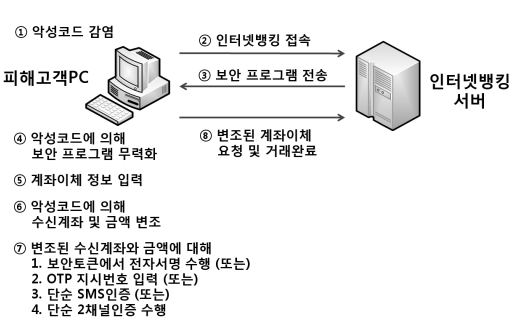
동의 여부와 상관없이 공격이 이루어진다.

3.3.3 변조 공격유형

변조 공격유형은 악성코드에 감염된 PC에서 고객이 계좌이체를 수행할 때, 악성코드가 수신계좌번호와 이체금액을 변조하여 불법이체를 완료하는 유형이다. 이 유형의 공격자는 고객 PC에 대한 정보접근 능력과 변조 능력을 지니고 있다.

변조 자체는 쉬운 기술이지만 인터넷뱅킹에서 변조 공격을 어렵게 만들기 위해 계좌이체 시 이체정보 입력 화면과 이체실행 화면을 분리하여 서버와 고객이 상호 교차 확인하고 키보드 보안 프로그램의 E2E 암호로 반복 확인하도록 하고 있어 변조 공격이 성공하기는 쉽지 않다. 일단 공격이 성공하면 피해고객의 PC 화면에는 정상적인 내용이 표시되므로 실제 이체가 완료되기 전에 악성코드의 감염사실이나 불법거래 사실을 전혀 인지하지 못하며 공격자의 개입 없이 악성코드에 의해서만 공격이 완료되므로 가장 진화된 형태의 공격유형이다.

이 유형의 공격에 대한 기본적인 대응방법은 고객이 인터넷뱅킹 외의 채널 또는 별도의 안전한 매체를 통해 거래내역을 입력하거나 확인하는 것으로 거래내역을 확인할 수 있는 사용자 인증수단이 이에 해당한다. 따라서 OTP, 보안토큰 등 거래내역을 확인할 수 없는 사용자 인증수단은 고객이 거래내역의 변조여부를 확인할 수 없기 때문에 변조 공격에 취약하다. 다만, 거래연동 OTP의 경우 이는 입력 정보가 숫자로 제한되어 계좌번호의 변조 여부의 확인이 완전하지 않을 수 있고 입력 숫자의 자릿수가 제한되어 금액의 일부만 입력하는 경우 이를 악용할 수 있어 제한된 안전성을 제공할 수 있다. 전자의 예로는 고객이 등록된 수신계좌로 이체할 때와 같이 계좌번호를 기억하지 못하거나 별도의 메모에 의존하지 않는 경우 계좌번호가 악성코드에 의해 변조되었다면 고객은 화면에 표기된 변조된 계좌번호를 입력할 수 있음을 들 수 있고, 후자의 예로는 금액의 처음 4자리만 입력할 경우 12,000원과 1,200,000원은 동일한 값을 입력하게 됨을 들 수 있다. 그림 9는 보안토큰, OTP, 단순 SMS인증 또는 단순 2채널인증에 대해 변조 공격유형의 예를 보여준다.



〔그림 9〕 변조 공격유형의 공격의 예

3.4 사용자 인증수단의 안전성 요약

거래내역을 확인할 수 없는 모든 사용자 인증수단은 이체내역이 변조되어도 피해고객 또는 서버가 검증할 수 없기 때문에 변조 공격유형에 취약하다. 단순 SMS 인증은 공격자가 실시간 불법이체 시 인증 유도를 하거나 스마트폰 악성앱 감염을 통해 가로챌 수 있어 실시간 공격유형 및 스마트폰 공격유형에 취약하며, 단순 2채널인증은 공격자가 실시간 불법이체 시 인증유도를 하거나 스마트폰 악성앱 감염을 통해 공격자의 전화로 착신 전환할 수 있어 실시간 공격유형 및 스마트폰 공격유형에 취약할 수 있다. OTP는 피해고객이 해당 값을 입력할 때 악성코드에 의해 유출되면 공격자가 유효한 시간범위 내에서 재사용할 수 있어 실시간 공격유형에 취약할 수 있다. 보안토큰은 비밀키가 외부로 노출되지 않아 공격자가 이를 획득할 수 없으므로 피해고객의 PC에서 불법 거래를 완료하지 않고 공격자의 PC에서 불법 이체를 수행하는 공격유형에 안전하다.

거래연동 SMS인증은 실시간 또는 변조 공격 시 피해고객이 위조 또는 변조사실을 확인할 수 있어 안전하지만, 스마트폰 악성앱 감염을 통해 SMS인증코드를 가로채거나 착신 전환으로 획득하는 스마트폰 공격유형에 취약할 수 있다. 거래연동 2채널인증은 실시간 또는 변조 공격에서는 피해고객이 위조 및 변조사실을 확인할 수 있어 안전하지만, 스마트폰 악성앱 감염을 통해 2채널인증 전화를 착신 전환하는 스마트폰 공격유형에 취약할 수 있다.거래연동 OTP는 실시간 및 스마트폰 공격유형에 안전하지만, 변조 공격유형에는 앞에서 언급한 바와 같이 입력 정보가 숫자로 제한되고 입력 자릿수에 제한이 있을 수 있어 완전하지 않은 안전성을 제공할 수 있다. 거래확인 보안토큰은 보안토큰과 같이 비밀키가 외부로 노출되지 않아 공격자가 이를 획득할 수

〔표 3〕 공격유형별 사용자 인증수단의 안전성

인증수단 구분		사고유형	실시간 공격유형	스마트폰 공격유형	변조 공격유형
거래내역을 확인할 수 없는 사용자 인증수단	단순 SMS인증	안전함	취약함	취약함	취약함
	단순 2채널인증	안전함	취약함	취약함	취약함
	OTP	안전함	취약함	안전함	취약함
	보안토큰	안전함	안전함	안전함	취약함
거래내역을 확인할 수 있는 사용자 인증수단	거래연동 SMS인증	안전함	안전함	취약함	안전함
	거래연동 2채널인증	안전함	안전함	취약함	안전함
	거래연동 OTP	안전함	안전함	안전함	제한적
	거래확인 보안토큰	안전함	안전함	안전함	안전함

없으므로 실시간 공격유형 및 스마트폰 공격유형에 안전하며 화면에 수신자의 이름, 은행명, 계좌번호 및 이체금액이 표시되므로 변조 공격이 발생하면 쉽게 육안으로 식별할 수 있다. 공격유형별 사용자 인증수단의 안전성을 정리하면 표 3과 같다.

3.5 사용자 인증수단 추가 고려사항

사용자 인증수단은 안전성이 가장 중요한 고려사항이겠지만 이 외에도 부인방지 기능, 편의성, 적용성 등 고려해야 할 사항이 있다.

부인방지는 거래 당사자 중 일방에 의해 해당 거래가 발생하였음을 부인하는 것을 방지하는 기술로 해당 거래 내역으로부터 당사자만이 해당 거래를 수행할 수 있었음을 누구나 검증할 수 있도록 증거를 남김으로써 거래의 완결성을 획득할 수 있다. 보안토큰과 거래확인 보안토큰을 포함하는 공인인증서 기반의 기술에는 기본적으로 부인방지의 기능이 부가되어 있다.

또한 아무리 사용자 인증수단의 안전성이 우수하다고 하더라도 사용자가 이용하기 불편하거나 업무에 적용하기 어려우면 외면 받을 수밖에 없으므로 이에 대한 고려가 필요하다.

Ⅳ. 결 론

메모리 해킹 공격과 이로부터 파생될 수 있는 공격유형에 강건한 사용자 인증수단은 기본적으로 실시간 공격, 스마트폰을 통한 인증에 대한 공격, 변조 공격에 취약성을 가지지 않아야 한다. 이를 만족하는 사용자 인증수단 중에서 거래내역표시 보안토큰은 고객의 PC가 악성코드에 감염되었다고 하더라도 안전하게 거래를 수행할 수 있어 이의 보급을 통해 전자금융의 안전성을 강화할 필요가 있다. 향후 전자금융의 안전성을 위협할 공격 방법은 메모리해킹뱅킹사고에서 사용된 악성코드를 기반으로 더욱 진화할 것이 자명한 일이므로, 신종 공격 방법에도 안전한 근본적인 대책 마련을 위해 지속적인 연구가 필요하다.

참고문헌

[1] 금융감독위원회, 금융감독원, “전자금융거래 안전성 강화 종합대책”, 2005.

[2] 금융감독원, “인터넷뱅킹 이용시 『신종 전자금융사기』에 주의하세요!!”, 2013.

[3] Zentraler Kreditausschuss, “Financial Transaction Services 3.0 Security – Alternative Sicherheitsverfahren”, 2013.

[4] E. Kalige and D. Burkey, “A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware”, 2012.

〈저 자 소 개〉

이 한 욱 (Hanwook Lee)
정회원

1996년 2월 : 경북대학교 컴퓨터공학과 학사
1998년 2월 : 포항공과대학교 전자계산학과 석사
2011년 9월~2013년 8월 : 성균관대학교 전기전자컴퓨터공학과 박사과정 수료
1998년 2월~현재 : 금융결제원 금융정보보호부 정보보호기술팀 차장
<관심분야> 암호, 인증, 정보보호

신 휴 근 (Hyu Keun Shin)
정회원

2002년 2월 : 아주대학교 정보및컴퓨터공학부 졸업
2004년 2월 : 아주대학교 정보통신대학원 석사
2004년 3월~현재 : 금융결제원 금융정보보호부 정보보호기술팀 과장
<관심분야> 침해사고분석, 보안관제기술