Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.115

전자금융사기 위험 분석과 대응방안에 관한 연구

정 대 용,[1,2†] 김 기 범,[1,3] 이 상 진[1‡]
[1]고려대학교 정보보호대학원, [2]경찰수사연수원, [3]경찰대학

A Study on Risk Analysis and Countermeasures of Electronic Financial Fraud

Dae Yong Jeong,[1,2†] Gibum Kim,[1,3] Sangjin Lee[1‡]
[1]Graduate School of Information Security, Korea University,
[2]Korean Police Investigation Academy, [3]Korean National Police University

요 약

전자금융사기의 수법이 계속 진화하고 있다. 이에 대응하기 위해 다양한 연구와 대응방안이 제시되었으나 근절하기 어려운 상황이다. 본 연구는 MS社의 Threat Risk Modeling 기법을 통해 전자금융사기의 위험을 분석하고 그 대응방안을 제시하기 위한 목적으로 수행되었다. 분석 결과 인증수단의 차이에도 불구하고 파밍의 위험이 높으며 추가적인 인증수단이나 기기보안 혹은 사용자 인증 기반의 보안체계 만으로는 공격을 예방하기 어렵다는 것을 확인하였다. 이에 따라 보안수단별 거래 한도의 재조정, 계좌인증 등 예방수단 및 추가적인 물리적 보안수단의 도입, 전자금융사기 예방 제도의 연계와 홍보 및 사용자 인식 개선을 통한 종합적인 전자금융사기 예방 정책의 수립 · 시행을 제안한다.

ABSTRACT

The methods of electronic financial fraud continue to evolve. Various research and countermeasures have been proposed to counter this problem, but it is difficult to eradicate it. The purpose of this study is to analyze the risk of electronic financial fraud through MS Threat Risk Modeling and to propose the countermeasures against the electronic financial fraud. As a result of the analysis, it is confirmed that despite the difference of authentication methods, there is a high risk of pharming, and it is difficult to prevent attack by using only additional authentication means, device security or user authentication based security system. Therefore, this study suggests the introduction of preventive measures such as readjustment of transaction limit by security means, account authentication, and additional physical security measures. It also suggests the establishment and implementation of a comprehensive electronic financial fraud prevention policy through linkage of electronic fraud prevention system and improvement of public relations and user awareness.

Keywords: Electronic Financial Fraud, Consumer Financial Information Security, Threat risk modeling, Threat modeling, Attack tree, STRIDE, DREAD

I. 서 론

컴퓨터와 네트워크의 발전 그리고 인터넷의 보급 확대에 따라 다양한 온라인 서비스가 제공되고 있다. 금융거래 분야에 있어서도 전자금융거래의 도입으로 번거롭게 영업점을 방문할 필요 없이 컴퓨터와 스마트폰을 이용하여 금융거래가 가능하게 되었고, 편리한 금융거래의 제공에 따라 많은 이용자들이 손쉽게 활용하고 있다.[1)]

Received(10. 20. 2016), Modified(01. 03. 2017), Accepted(01. 06. 2017)
† 주저자, dyjeong75@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

1) 2015년 만 12세 이상 인터넷 이용자의 인터넷 뱅킹 이

그러나 비대면 인증을 통한 전자금융거래의 취약점을 이용한 전자금융사기가 등장하게 되어 그 피해가 커져가고 있다. 이에 관계당국에서는 전자금융사기 예방서비스, 입금계좌지정서비스, 지연인출제도 및 지연이체제도 등 다양한 피해 예방 정책을 수립·시행하고 있다. 이러한 정책들이 어느 정도의 피해감소 효과를 거두었으나, 전자금융사기는 나날이 진화해 가고 있다.

전자금융거래의 침해는 직접적인 금전피해를 야기한다는 점에서 안정성이 담보되어야 한다. 이를 위해서는 전자금융 피해 분석을 통해 위협을 식별하고 이를 등급화하여 각각의 대응방안에 대한 우선순위를 부여하여 체계적인 대응방안을 모색할 필요가 있다.

본 연구에서는 전자금융사기를 통한 이체 위협을 먼저 확인하고 현재까지 알려진 위협에 대하여 MS社의 Threat Risk Modeling 기법을 적용하여 구조화된 방식으로 위험을 측정하여 문제점을 식별하고 현재의 피해 실태와의 비교를 통해 전자금융사기 피해 위험에 대한 대응방안을 도출하였다.

II. 이론적 배경

2.1 전자금융사기의 개념과 실태

2.1.1 용어의 정의

「전기통신금융사기 피해금 환급에 관한 특별법」에서는 전기통신을 이용하여 불특정 다수인을 기망(欺罔) · 공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함한다.

가. 자금을 송금 · 이체하도록 하는 행위

나. 개인정보를 알아내어 자금을 송금 · 이체하는 행위를 "전기통신금융사기"라고 정의(제2조 제2호)하고 있다.

"전자금융사기"라는 용어는 법률적 · 학술적으로 명확하게 정의되어 있지는 않으나, 일반적으로 전자금융거래의 취약점을 이용하여 피해금액을 이체시키는 신종 금융범죄수법인 피싱 · 파밍 · 메모리해킹 등을 통칭하는 용어로 사용된다[1].

전자금융거래에 대한 사기 수법은 ① 공격자가 피해자를 속여 스스로 정상적인 이체를 하게 하는 행위, ② 공격자가 피해자의 개인 · 금융정보를 알아내어 인증과정을 통과하고 자금을 직접 이체하는 행위, ③ 공격자가 악성코드를 이용하여 피해자의 정상적인 이체거래 요청 정보를 수정하여 공격자가 확보한 계좌로 이체되도록 하는 행위로 분류할 수 있다.

본 연구는 전자금융거래 시스템상의 이체거래 프로세스에 대한 위협을 모델링 기법을 통해 분석하는 것을 목적으로 하고 있어, 인증 프로세스의 취약점을 공격하는 방식의 피싱 · 파밍 기법(②번 유형)과 이용자 단말의 이체 처리과정에서 메모리상의 계좌정보를 수정하는 메모리해킹 기법(③번 유형)만을 분석대상으로 한다. ①번 유형은 "보이스 피싱", "메신저 피싱" 등으로 분류되는 수법으로, 피해자가 직접 인증과정을 거쳐 거래하는 행위이므로 전자금융거래 시스템에 대한 위협에 해당되지 않아 분석대상에서 제외하였다.

2.1.2 유형별 수법

2.1.2.1 피싱

피싱이란 피해자를 기망 또는 협박하여, 개인정보 및 금융거래 정보를 요구하거나, 피해자의 금전을 이체하도록 하는 수법을 말한다. 이는 전화, 메신저 등을 통해 피해자를 착오 빠트려 스스로 정상적인 이체거래를 하게 하는 방식과 피해자로부터 개인정보와 금융거래 정보를 취득하여 공격자가 직접 인증과정을 통과하여 금전을 이체하는 수법을 포함한다.

전자의 수법은 이체 거래 자체는 정상적인 것으로서 이체 거래 시스템에 대한 위협에 해당되지 않으나, 후자의 수법은 취득된 개인정보를 이용하여 거래 당사자의 신분을 속이는 수법(Spoofing)에 해당된다. 주로 전화나 문자메시지, 이메일 등을 통해 피해자를 기망하여 피싱사이트에 접속하게 한 후, 금융정보와 개인정보를 입력하게 하고 공격자가 이를 통해 인증과정을 통과하여 금전을 이체하는 수법이다.

2.1.2.2 파밍

피해자 PC에 악성프로그램에 감염시켜 정상적인 사이트 주소를 입력하더라도 가짜 사이트로 접속되도

용률은 52.5%(전년대비 2.7% 증가)이며, 최근 1개월 이내 이용한 경우는 44.0%이다.(한국인터넷진흥원, 2015년 인터넷이용실태조사)

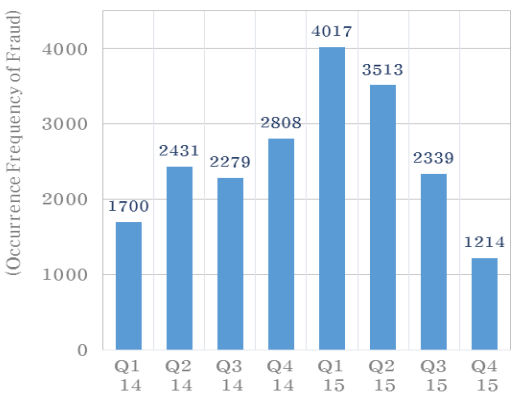
록 조작한 후 개인정보와 금융거래 정보의 입력을 요구한 후 이를 탈취하는 수법을 말한다. 범죄자는 이러한 정보를 이용하여 자신들이 확보한 계좌에 금전을 이체시켜 범행을 완료하게 된다. 최근에는 스미싱 기법 등을 이용하여 스마트폰에 금융앱 등을 가장한 악성프로그램을 설치하여 이를 통해 금융정보를 가로채는 수법을 사용하기도 하며[2], 피싱사이트를 통해서 정보를 탈취한 후 2Ch 인증을 통과하기 위해 QR코드 등을 이용하여 스마트폰을 해킹하는 수법[3], 실시간으로 채팅창을 통해 ARS 인증을 요구하는 수법[4] 등도 나타나고 있다.

2.1.2.3 메모리 해킹

피해자의 PC에 악성코드를 설치한 후 금융거래 과정에서 메모리상의 데이터를 모니터링하여 피해자가 정상적인 거래 요청과정에서 입력한 계좌번호나 이체금액을 변조한 후 금융기관에 전달하여 범죄자가 확보한 계좌로 지정된 금액을 이체시키는 방법을 말한다. 또한 피해자의 PC에 저장된 공인인증서를 복사하고 거래 과정에 입력한 공인인증서 비밀번호, 보안카드 번호 등 이체 정보를 알아낸 뒤, 거래 오류를 일으켜 거래를 중단시킨 후 범죄자가 확보한 공인인증서와 비밀번호, 보안카드번호를 이용하여 범행계좌로 이체시키는 등의 방법도 포함된다.

2.1.3 전자금융사기 발생 실태

경찰청 통계에 따르면 2014년부터 2015년까지 2



(Source: Korean National Police Agency, Rearranged by Author)

Fig. 1. Occurrence Frequency of Electronic Financial Frauds in 2014~2015

Table 1. Type and Occurrence Frequency of Electronic Financial Frauds in 2014~2015

(Source: Korean National Police Agency, Rearranged by Author)

	2014	2015	Sum	Ratio
Phishing	1,962	1,726	3,688	18.2%
Pharming	7,101	9,233	16,334	80.5%
Memory Hacking	155	124	125	1.4%
Sum	9,218	11,083	20,301	100%

년간 피싱, 파밍, 메모리해킹을 통한 전자금융사기는 모두 20,301건이 발생하였다. 연도별로는 2014년 총 9,218건, 2015년 총 11,083건으로 월 평균 약 845건에 해당된다. 특히 2015년 12월 기준으로 발생 총계는 전년 대비 1,865건(약 20.2%)이 증가하여 상승세를 보이고 있다. 분기별로는 그림 1과 같이 2105년 1분기에 최대 발생건수를 기록한 후 조금씩 감소되는 추세임을 확인할 수 있다.

유형별로는 표 1과 같이 파밍이 16,334건(80.5%)으로 대다수를 차지하고 있으며, 피싱이 3,654건(18.2%)이며, 메모리해킹은 277건(1.4%)으로 매우 적은 비중을 차지하고 있다.

2.2 위험분석의 개념과 방법

2.2.1 개념

위험이란 주어진 위협이 자산의 취약점을 악용하여 조직에 피해를 입힐 가능성을 의미한다[5]. 위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 그들이 어떠한 영향을 미치는 지를 분석해야 한다. 이는 주로 어떤 사건이 발생할 확률과 사건 발생시 비용을 곱하는 방식으로 추산하게 된다[6].

위험 분석은 위험의 크기를 측정하는 체계화된 절차로서 “자산의 취약성을 식별하고 존재하는 위협을 분석하여 이들의 발생가능성 및 위협이 영향을 미치는 손실 수준을 예측하여 위험의 내용과 수준을 결정하는 과정”을 말한다[7].

2.2.2 방법론

기존에 발표된 위험분석 방법론으로는 ISO/IEC TR 13335(GMITS), 영국 표준협회의 BSM7799, NSA의 IAM, NIST의 SP 800-30, 카네기멜론 대학의 OCTAVE, CRAMM, PRAM 등 다양하다

〔7〕. 시스템 평가 모델은 전문성을 가진 보안기술자가 시스템에 사용된 응용프로그램의 유형과 위험관리 도구의 적합성 등을 고려하여 적합한 평가 모델을 신중히 선택하여야 한다〔8〕. 전자금융사기의 공격은 주로 이체거래를 위한 사용자 인증절차에 집중되므로 시스템 전체의 분석보다는 인증과정의 분석을 위주로 한 간단하고 직관적인 모델링이 필요하다.

다양한 방법론 중에서 MS社의 Threat Risk Modeling 절차는 직관적이며 디자이너, 개발자, 코드 검수자와 품질 보증팀 등 다양한 구성원에게 채택되기 쉽다고 알려져 있다〔9〕. 따라서 본 연구에서는 위험분석을 위한 도구로서 MS社의 Threat Risk Modeling 기법을 사용한다.

2.3 선행연구 검토

피싱 · 파밍 · 메모리해킹 등 개별적인 공격을 통한 위협을 modeling하여 분석하거나 대응방안을 제시하는 연구는 아직 수행되지 않은 것으로 보인다. 다만, 전자금융사기 예방을 위한 연구와 Treat Risk modeling 등을 통한 시스템 분석과 대응에 대한 연구를 찾을 수 있다.

먼저 전자금융사기 예방을 위한 연구로서 개인·금융정보를 유출하는 수단인 피싱, 파밍사이트를 사전에 탐지하고 대응하는 사전 예방적 방안에 대한 연구〔10〕〔11〕와, 전자금융사기 예방서비스 등 다양한 예방정책의 보완과 연계를 통해 범죄를 예방하는 정책적 연구〔2〕, 전자금융거래 보안 통제사항에 대한 연구〔12〕 등이 있다.

위험에 대한 분석적 연구로서는 위협 모델링을 통해 스마트홈 서비스의 보안 위험을 분석한 연구〔13〕 지리 기상 정보 시스템(GWIS)에 대하여 STRIDE, DREAD 모델을 통해 위험을 분석한 연구〔8〕와 Attack tree를 이용하여 원격 의료시스템에서 발생할 수 있는 보안위험을 분석한 연구〔14〕가 있다.

기존의 연구들은 전자금융 침해에 대한 사전 예방이나 시스템 통제 강화를 통해 침해를 방지하는 것에 주안점을 두고 있거나, 시스템 자체의 분석을 통해 위험을 측정하는데 목적을 두고 수행되었으며, 특정한 공격기법의 실질적인 위협에 대한 심층적인 분석과 이를 통한 위험의 측정에 대한 연구는 미진하다고 보인다.

이에 본 연구는 전자금융사기 발생실태를 통한 실증적인 방법과 체계화된 Treat Risk modeling 방법론을 적용하여 이체거래 시스템의 프로세스와 위협을 구조화된 방식으로 분석하고, 각각의 위협에 대한 위험도를 수치적으로 제시하여 그 대응방안을 모색하였다는 점에서 기존의 연구와 차이점을 갖는다.

III. 전자금융사기 이체 위험분석

3.1 개념과 절차

Threat Risk Modeling은 안전한 웹 어플리케이션 개발과 올바른 통제수단의 결정 및 위협에 대한 효과적인 대응방안을 수립하는 필수적인 프로세스이다〔15〕. 세부적인 절차는 모두 5단계로 구성되어 있고 순서는 그림 2와 같다.

각 단계별로 ① Identify Security Objectives 단계에서는 보안의 객체(Objective) 즉, 시스템의 구성요소와 자산을 식별한다. ② Application Overview 단계에서는 식별된 보안 객체에 대하여 구성요소(Components), 데이터 흐름(Data flows), 신뢰 경계(Trust boundaries)를 식별하기 위해 DFD(Data Flow Diagram)를 작성한다. ③ Decompose Application 단계에서는 분석된 어플리케이션 구조를 통해 평가할 필요가 있는 보안에 영향을 미치는 요소들을 확인하고 분석한다. 구체적인 방법으로 STRIDE 기법을 통해 공격자의 입장에서 어떠한 방법으로 공격할 수 있는지 식별하는 단계이다. ④ Identify Threats 단계에서는 현재까지 알려진 다양한 위협을 기술하고, 이때, 구조화된 Attack Tree를 사용한다. ⑤ Identify Vulnerabilities 단계에서는 분석된 위협을 평가하

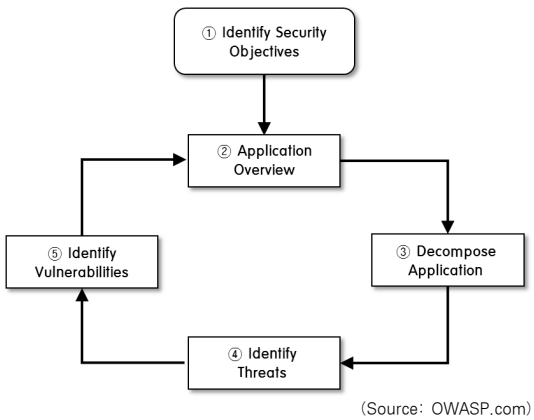


Fig. 2. Threat Risk modeling process

고 관련된 취약점을 검토한다. 확인된 위협과 취약점을 통해 위험을 측정하는 단계로서 DREAD 모델을 사용한다. 이를 통해 각각의 위협에 등급을 부여하고 이를 종합하여 위험을 측정한다[9].

3.2 1단계 - 구성요소와 자산의 식별

위험분석을 수행하는 첫 단계로서 구성요소와 자산을 식별한다. 이체과정의 구성요소로는 이용자(User), 이용기기(User PC or Smartphone), 이용 앱(Web browser, Mobile banking app), 인터넷(Internet, wireless), 네트워크 장비(Network equipment), 웹서버(Web sever), 인터넷뱅킹 서버(Internet banking server)를 식별할 수 있다.

자산(Asset)이란 조직 내의 가치를 가지고 있는 모든 것으로서 보호할 대상을 말한다. 전자금융거래에 있어 자산은 금융기관의 신뢰도, 개인정보 및 금융정보 등 다양할 수 있으나 전자금융사기는 피해자의 자금을 이체하는 것을 목적으로 하므로 이에 대해 지켜야할 자산은 피해자의 자금으로 볼 수 있다.

3.3 2단계 - DFD 작성

전자금융사기의 공격 대상인 자금의 이체 거래와 관련된 프로세스만을 간단히 도식화하면 그림 3과 같다. 이체거래는 사용자가 PC나 스마트폰 등 기기를 이용하여 원하는 계좌에 대한 계좌번호와 이체금액 등을 입력하고 보안카드나 OTP등 인증정보를 포함하여 이체를 요청하면 이체를 요청하면 웹서버를 경유하여 인터넷뱅킹 서버를 통해 이체과정이 진행된다.

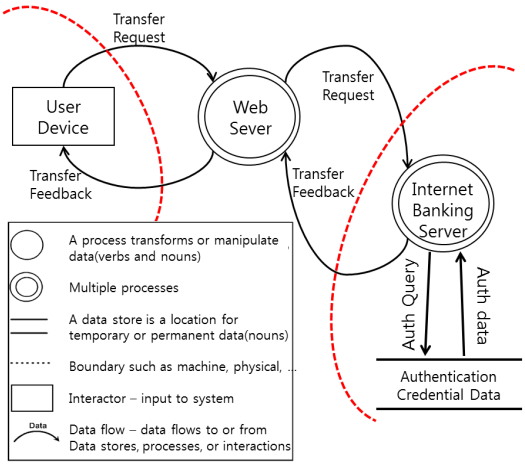


Fig. 3. Data Procedure of Electronic Financial Transaction

3.4 3단계 - 위협의 식별(STRIDE 모델)

3.4.1 STRIDE 모델

STRIDE 모델은 공격의 종류에 따라 알려진 위협의 특성에 대한 분류체계로서, S는 인증정보를 속이는 행위, T는 인가받지 않은 수정, R은 행위 부인, I는 정보 유출, D는 서비스의 거부, E는 부정한 권한의 상승을 나타낸다[16]. 전자금융거래 시스템에 STRIDE 모델을 적용하여 위협을 적용대상별로 분류하면 표 2와 같다.

Table 2. Apply STRIDE Model

(Source: MSDN.microsoft.com)

STRIDE Category	Threat target(s)
Spoofing identity	user, user device
Tampering with data	user device, internet, wireless network
Repudiation	user, user device
Information disclosure	internet, wireless, web sever
Denial of service	internet, wireless, web server
Elevation of privilege	user, device

3.4.2 전자금융사기 위협

전자금융사기는 범죄자가 확보한 계좌로 금전을 이체시키는 것으로 공격이 완성되는 범죄로서, 피싱 · 파밍의 경우 공인인증서와 비밀번호, 보안카드 비밀번호 또는 OTP가 필요하다. 공인인증서 재발급이나 다액이체의 경우 ARS인증을 통과하여야 하며 피싱 · 파밍사이트에서 실시간으로 승인을 요청하는 수법이 나타나고 있다[17]. 메모리해킹의 경우 사전에 악성코드를 설치하고 메모리를 모니터링하여 계좌번호와 이체금액을 변조하여야 하며, 거래 오류를 일으켜 보안카드번호 등을 탈취하는 수법의 경우 피싱 · 파밍과 마찬가지로 악성코드를 통해 공인인증서를 탈취하고 다른 정보도 입수하여야 한다.

따라서 전자금융사기는 유형별로 피싱 · 파밍의

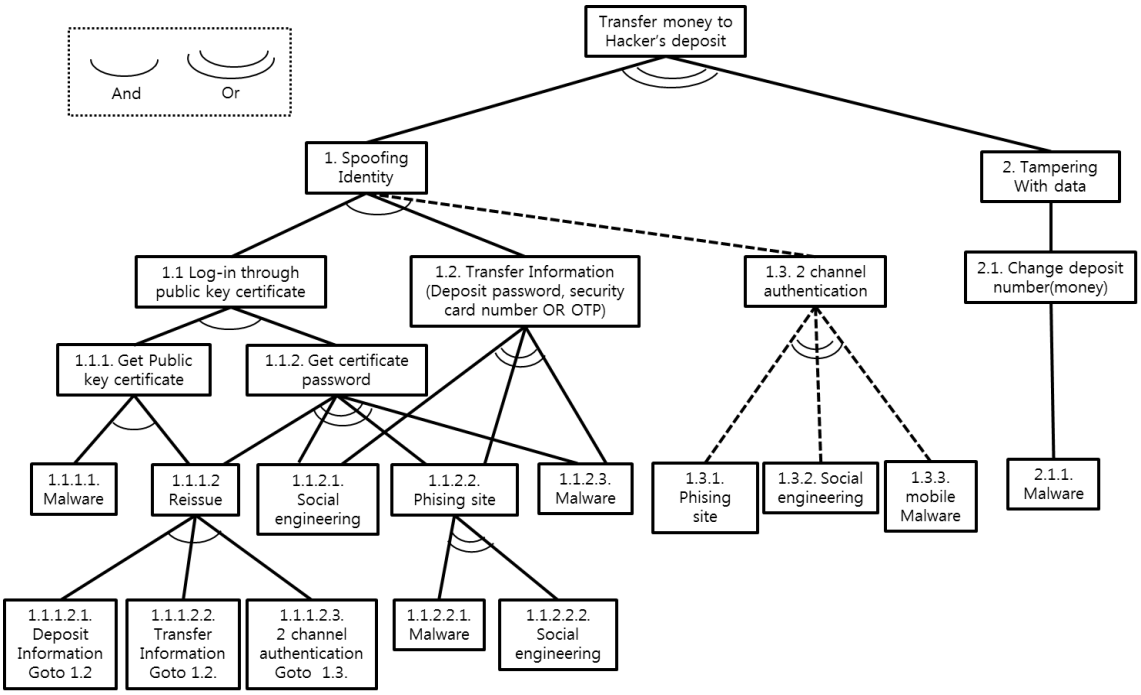


Fig. 4. Attack Tree of Electronic Financial Fraud

경우 인증정보를 이용하여 신원을 속이는 Spoofing Identify, 메모리 해킹은 전송되는 이체정보를 변조하는 Tampering with data로 특성을 식별할 수 있다.

3.5 4단계 - 위협의 구조화된 분석(Attack Tree)

Attack Tree[2][18]를 통하여 공격의 수단을 그림 4와 같이 단계별로 분석하였다. 분석 결과 신원을 속이기 위한 세부적인 방법으로 피해자 PC 등에 악성코드를 설치하여 공인인증서를 탈취하거나 탈취한 정보를 통해 재발행을 받는 방법이 있다. 공인인증서를 탈취한 경우 별도로 피싱사이트나 사회공학적 기법 혹은 악성코드 등을 이용하여 공인인증서 비밀번호를 취득한다. 계좌 비밀번호와 보안카드 번호, 혹은 OTP를 입수하기 위해서는 피싱사이트를 통하여 입력을 받거나 사회공학적 기법을 통해 피해자를 속여 비밀정보를 제공받는 방식이 사용될 수 있으며, 악성코드를 이용하여 정보를 입수할 수도 있다.

피싱사이트를 이용하여 피해자로 하여금 금융정보를 입력하도록 유도하기 위해서는 피해자의 PC에 악성코드를 이용하여 hosts파일을 변조하거나 DNS 설정 변경 또는 공유기 설정 변경을 통해 금융기관을 가장한 피싱사이트로 접속을 유도하는 파밍기법을 사용하거나 피해자에게 전화하여 수사기관이나 금융기관 직원을 사칭하는 등의 수법으로 피싱사이트에 접속하도록 유도하는 방법, SMS, 이메일, SNS 등을 통해 링크를 전송하여 피싱사이트에 접속하게 하는 등의 사회공학적 기법을 사용한다.

공인인증서 재발급이나 다액 이체를 위해서는 추가적으로 전자금융사기 예방서비스에 따라 2채널 인증을 통과하여 한다.[3] 2채널 인증방식에 대한 공격은 피싱사이트에서 실시간으로 피해자에게 입력을 요

2) Attack Tree는 B. Schneier에 의해 소개된 방법으로 다양한 공격 기법을 통해 시스템 보안을 향상시키는 방법이다. 공격에 사용되는 다양한 수단을 검토하여 체계적인 대응을 가능하게 한다.

3) 전자금융사기 예방서비스는 SMS를 통해 인증번호를 전송하고 이를 통해 인증하는 방식(SMS 인증)도 허용하고 있으나, 스마트폰이 해킹되는 경우에는 인증번호가 유출될 수 있어 취약하므로(정대용, 이경복, and 박태형. "전자금융사기 예방서비스의 개선방안에 관한 연구." 정보보호학회논문지 24.6 (2014): 1243-1261.) 대부분의 금융기관은 SMS 인증방식은 제한적으로만 허용하고 주로 ARS인증 방식을 이용하고 있다.

구하는 방식과 전화를 이용하여 피해자에게 입력하게 하는 방법, 혹은 스마트폰에 악성코드를 설치하여 정보를 탈취하는 방법이 가능하다.

전송되는 데이터를 변조하는 방식으로 컴퓨터에 설치된 악성코드를 통해 메모리상의 이체계좌번호와 이체금액을 모니터링한 후 해당 정보를 범죄자가 확보한 계좌번호와 다액으로 변조시키는 방법이 사용될 수 있다.

3.6 5단계 - 위험 측정(Dread 모델)

3.6.1 DREAD 모델[19]의 개념과 적용

확인된 위협에 대하여 DREAD 모델을 적용하여 위험의 정도를 측정한다. DREAD 모델은 각종 사이버공격에 대한 위험도를 측정하는 도구로서 각각의 항목에 대하여 시스템에 어떠한 영향을 미칠 수 있는지를 구조화된 방식으로 측정한다. 측정의 요소는 표 3과 같이 5가지 항목으로 구성되어 있으며 각 항목의 등급을 정량적으로 식별하기는 곤란하므로 추상화된 형태로 5점 척도나 3점 척도 등을 사용한다.

Attack Tree를 통한 위협분석결과 이체거래에 대한 전자금융사기는 공인인증서 및 비밀번호 취득, 이체 인증 정보 획득, 2채널 인증 통과 등 인증과정의 취약점을 이용하는 것으로 확인되었다. 이체거래를 위한 인증방식은 보안카드 또는 OTP를 이용한 인증방식에 따라 보안수준이 달라질 수 있으며 추가적인 2채널 인증의 적용여부에 따라 공격 수단이 달라질 수 있으며 위험도 다르게 나타날 수 있다.

따라서 DREAD 모델을 적용하여 위험의 수준을 측정하기 위해서는 각각의 인증방법과 추가 인증 적용 여부에 따라 공격의 유형을 분류한 후 유형별 위험도를 측정하여 보안수준에 따른 위험도를 평가하는 방법을 사용한다.

Table 3. DREAD Model (Source: MSDN.microsoft.com)

DREAD	Assessment
Damage potential	How great is the damage if the vulnerability is exploited?
Reproducibility	How easy is it to reproduce the attack?
Exploitability	How easy is it to launch an attack?
Affected users	As a rough percentage, how many users are affected?
Discoverability	How easy is it to find the vulnerability?

3.6.2 위험 측정 절차

DREAD 모델은 대상을 모델링하여 단순화하고 위험의 정도를 계량함에 있어 정성적인 방식으로 단순화하여 측정한다. 이에 따라 평가자의 전문적인 역량수준과 주관에 의해 결과가 좌우될 수 있다. 이러한 문제점을 보완하기 위해 관련 분야 전문가를 평가위원으로 구성하여 토론을 통해 위험 측정에 대한 기준을 결정하였다. 이후 결정된 기준에 따라 위원 각자의 개별 평가 후 이를 합산 후 각 항목의 평균값으로 위험의 수준을 확정하는 방식을 사용하였다.

평가위원은 전자금융사기의 프로세스를 이해하고 정보보호분야의 분석기법에 대한 전문지식을 갖춘 현직 경찰관으로 사이버수사, 디지털 포렌식, 경찰교육기관 관련분야 교수요원 등 10명으로 구성하여 평가를 수행하였다.[4)]

3.6.3 위험 측정 기준

항목별 위험 등급은 매우 높음(5), 높음(4), 중간(3), 낮음(2), 매우 낮음(1)로 구분하여 5단계로 수치화하였다. 등급이 높을수록 위험이 높은 것을 의미한다.

각 항목별로는 Damage potential 항목은 공격에 의해 발생될 수 있는 피해금액이 클수록 등급이 높은 것으로, Reproducibility 항목은 공격 기회가 주어지는 시간적 범위가 클수록 등급이 높은 것으로 기준을 설정하였다. Exploitability 항목은 공격 기법의 구현 난이도를 판단하여 구현이 쉬울수록 등급이 높은 것으로, Affected users 항목은 하나의 공격행위로 인하여 영향을 받는 이용자의 수가 많을수록 위험이 높은 것으로, 그리고 Discoverability 항목은 거래의 취약점과 이를 이용한 구체적인 공격방법을 찾아내는 것이 쉬울수록 등급이 높은 것으로 기준을 설정하였다.

4) 평가는 2016. 9. 27. 수행되었으며, 평가 위원은 사이버범죄수사(디지털 포렌식 포함) 경력 10년 이상이거나, 사이버범죄수사(디지털 포렌식 포함) 경력 5년 이상이고, 정보보호분야 석사 이상의 학위를 가진 자 중 전자금융사기 수사(관련 악성코드 분석) 경험이 있는 자로 구성하였다.

Table 4. Apply DREAD Model

Authentication methods	Attack	D	R	E	A	D	Total	AVG
Security card	Phishing	1.8	4.5	4.4	3.1	4.4	18.2	3.6
	Pharming	1.9	4.1	3.9	4.2	4.1	18.2	3.6
	Memory hacking	2.1	2.3	2.7	3.9	3.1	14.1	2.8
Security card + 2 Ch auth.	Phishing	2.9	2.9	3.1	2.5	4.0	15.4	3.1
	Pharming	3.0	3.0	3.0	3.9	3.5	16.4	3.3
	Memory hacking	3.2	1.6	2.0	3.6	2.6	13.0	2.6
OTP	Phishing	3.7	3.0	3.3	2.7	3.3	16.0	3.2
	Pharming	3.8	2.8	2.7	3.7	3.0	16.0	3.2
	Memory hacking	4.0	1.7	1.9	3.7	2.4	13.7	2.7
OTP + 2 Ch auth.	Phishing	4.4	2.0	2.3	2.1	2.5	13.3	2.7
	Pharming	4.5	1.8	2.1	3.2	2.5	14.1	2.8
	Memory hacking	4.8	1.4	1.4	3.1	2.0	12.7	2.5

IV. 위험 측정 결과 분석 및 검증

4.1 위험 측정 결과 및 분석

위험 측정 결과는 표 4와 같다. 인증수단별로는 보안 수준이 높다고 알려진 인증수단 즉 OTP를 이용한 인증과 2 Ch 인증을 함께 적용한 인증방식이 가장 위험이 낮고 보안카드만을 이용한 인증방식이 가장 위험도가 높다고 측정되었다.

공격기법별로는 각각의 인증수단의 차이에도 불구하고 피싱 · 파밍 공격의 위험이 메모리 해킹 공격의 위험보다 상대적으로 높은 수준이며, 특히 파밍 공격의 위험이 가장 높게 측정되었다.

측정 항목별로는 Damage potential 항목은 보안성이 높다고 알려진 인증방식을 사용하는 경우 오히려 위험도가 증가하는데, 이는 인증수단의 보안성에 따라 1일 혹은 1회 이체가능금액이 증가되므로[5] 위험도가 증가한다는 점이 반영된 것으로 분석된다.

Reproducibility 항목은 피싱 · 파밍이 메모리 해킹보다 높은 수준으로 측정되었고, 보안카드만 사용하는 경우 특히 높게 나타난다. 메모리해킹의 경우 이체순간에만 공격이 작동하므로 공격기회가 한정되므로 위험도가 낮고, OTP를 사용하거나, 2Ch 인증을 사용하는 OTP 유효시간과 2Ch 인증 입력 시간 제한으로 인하여 공격의 시간적 기회가 제한되기 때문으로 분석된다.

Exploitability 항목에서는 공격기법별로는 메모리해킹의 위험도가 가장 낮고, 피싱의 위험도가 가장 높게 측정되었다. 보안수단별로는 2Ch 인증을 사용하는 경우 위험도가 낮아지는 것으로 나타난다. 메모리 해킹은 메모리상의 이체정보를 변조하는 악성코드의 제작 난이도가 높아 구현가능성이 매우 낮고, 피싱사이트를 제작하고 피싱사이트로의 접근을 유도하는 악성코드를 사용하는 파밍 공격은 메모리해킹에 비해 구현가능성이 상대적으로 높으며, 전화 등을 이용한 피싱 공격은 피싱사이트 제작외에 별도의 악성코드 제작 등은 필요하지 않으므로 구현가능성이 매우 높다고 측정된 것으로 분석된다. 또한 보안수단으로 2Ch 인증을 추가로 사용하는 경우 스마트폰 해킹 혹은 사회공학적 기법을 사용하여 인증정보를 별도로 확보하여야 하므로 구현가능성이 낮아지는 것으로 분석된다.

Affected users 항목은 피싱의 위험도가 가장 낮게 측정되었고, 파밍과 메모리해킹은 상대적으로 높은 수준으로 측정되었다. 피싱은 전화 등을 이용한 사회공학적 기법으로 피해자를 기망하는 개별화된 공

5) 우리은행의 경우 보안등급을 1등급(OTP+공인인증서, HSM방식 공인인증서+보안카드, 2채널 인증+공인인증서+보안카드)과 2등급(보안카드+공인인증서)으로 2단계로 분류하며, 개인의 이체한도는 1등급은 1일·1회 이체한도는 각각 5억원 · 1억원까지 지정할 수 있고(단, 미지정시 1천만원 · 5백만원), 2등급은 각각 1천만원 · 5백만원이다. 또한 1등급의 경우 별도의 약정을 통해 이체한도를 초과하여 지정할 수도 있다.
〈우리은행 홈페이지: https://spot.wooribank.com/pot/Dream?withyou=CQIBG0022, 2016.4.29.〉

격의 형태가 주로 나타나고 있음에 반하여, 파밍과 메모리 해킹은 악성코드 배포 서버를 이용하거나 대량의 이메일 발송을 통해 다중에 대한 무차별적인 공격으로 다수의 사용자에게 영향을 미칠수 있다는 점에서 위험도가 높다고 분석된다.

Discoverability 항목의 위험도는 피싱이 가장 높고, 메모리해킹이 가장 낮게 측정되었다. 전자금융사기의 수법은 범죄 예방 홍보 등을 통하여 이미 잘 알려져 있다. 그러나 각 공격에 이용되는 기술적 취약점에 대하여는 수법에 따라 달리 평가될 수 있다. 먼저 피싱의 경우 피싱사이트 제작 외에 다른 시스템적인 취약점 확인이 불필요하므로 위험도가 매우 높으며, 파밍의 경우 악성코드 침투와 피싱사이트 유도를 위한 추가적인 시스템상의 취약점을 확인하므로 위험도가 상대적으로 낮으며, 메모리 해킹을 위한 거래과정의 메모리 분석과 변조에 관한 취약점 발견은 난이도가 높아 위험도는 가장 낮은 수준으로 평가되었다.

4.2 발생 실태와 비교 검증

위험 분석결과와 실제 전자금융사기 발생실태와 비교 검토를 통해 분석모델의 신뢰성을 검증하였다. 위험 분석 결과에서는 파밍의 위험도가 가장 높게 나타나고 피싱의 위험도는 파밍과 유사하거나 조금 낮은 수준이며, 메모리 해킹이 가장 낮은 위험도를 보이고 있다.

2014년부터 2015까지 2년간 발생한 전자금융사기 피해사례에서 피해총액은 약 1,390억원이며, 유형별로는 파밍이 81.4%인 1,118억원, 피싱이 18.4%인 255억원, 메모리해킹이 1.2%인 162억을 차지한다. 이를 위험 분석 결과와 비교하면 위험도가 높은 순위에 따라 피해발생 총액 순위가 같게 나타나고 있다. 그러나 위험도에서는 각각의 유형의 차이가 크지 않으나 실제 피해 발생 액수의 차이는 크게 나타난다는 것을 확인할 수 있다.

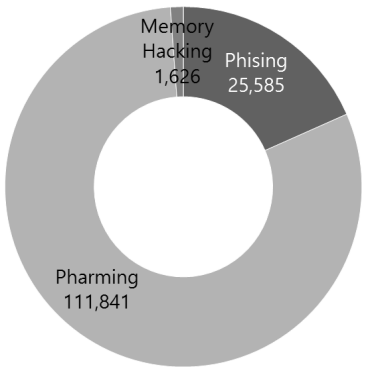


Fig. 5. Ratio of Attack damage(Million ₩)

위험도의 작은 차이에도 불구하고 피해액의 차이가 큰 것은 공격자들이 합리적 · 경험적으로 가장 효율적인 공격 방식을 우선 선택하기 때문인 것으로 추정할 수 있다.

4.3 연구모델의 한계

전자금융사기는 상황에 따라 매우 다양한 공격수법이 사용되므로 이를 모두 유형화하기는 어렵다. 본 연구는 전체적인 발생 현황을 중심으로 사례를 분류하고 대표적인 공격수법별 위협을 통해 위험을 추상화하여 측정하는데 중점을 두었기에 각각의 세부적 기법에 대한 기술적 분석이 부족하다는 한계를 갖는다. 또한, Threat Risk Modeling은 시스템의 전체적인 보안 위험을 분석하는 절차로서 전자금융사기와 같은 특정한 공격기법의 위험을 측정하는데 제한적이며, 각각의 위험도를 명확히 수치적으로 산정하기 어려워 위험도 측정이 객관적이지 못하다는 한계를 가진다. 이러한 한계를 보완하기 위해 Attack Tree를 이용하여 위협을 구조화된 형태로 분석하여 위협을 식별하였고, 위험 평가에 실제 사례를 경험한 전문가를 참여시켜 측정기준을 설정하고 이를 종합하는 방식으로 평가결과의 신뢰성 확보에 노력하였다.

4.4 문제점과 대응의 방향

4.4.1 추가인증수단의 낮은 위험예방효과

전자금융사기 위험은 상대적으로 보안수준이 높은 인증수단인 OTP · 2Ch 인증을 사용하는 경우에도 크게 낮아지지 않는다. 실제 피해 발생의 가능성은 낮아질 수 있으나 1일 이체 한도의 증가로 인하여 개별 피해자에게 큰 피해를 야기할 수 있다.

따라서, OTP · 2Ch 인증시 대폭 높아지는 이체 한도를 재검토하고, 보안수단별 거래한도 재조정을 통해 대량의 피해발생을 차단하여 전체적인 위험수준을 낮추는 것이 필요하다.

4.4.2 파밍 예방 미흡

파밍의 위험이 크고 실제 피해규모도 크다. 파밍은 악성코드를 유포하여 피해자의 기기를 침해하고, 이를 통해 피해자를 피싱사이트로 유도하여 금융 · 개인정보를 입수하는 방식을 사용한다. 추가적으로 OTP번호나, 2Ch 인증번호 등을 탈취하기 위한 사회공학적 기법이 활용되기도 한다.

파밍의 위험분석결과 및 발생상황으로 보아, 현재의 파밍용 악성코드 유포 탐지 및 차단을 위한 대응이 효과적으로 작동되지 않는 것으로 분석된다. 특히 이용자의 스마트폰 등에 대한 침해가 발생되는 경우 2Ch인증도 무력화될 수 있다.

따라서, 파밍 예방을 위하여 첫째, 기존의 악성코드 차단만이 아닌 악성코드로부터 보다 안전한 물리적 보안 매체를 적용하여 사용자 단의 보안을 강화하고, 둘째, 사용자 인증을 통과하거나 우회하는 경우 공격을 차단하기 위하여 서버 단에서 이상거래의 유무를 탐지하는 FDS 시스템의 효율적 활용이 필요하다.

4.4.3 사회공학적 기법에 대한 대응 미흡

공격 수단으로 사회공학적 기법이 폭넓게 사용되고 있어 PC · 스마트폰 등 기기에 대한 보안만으로는 공격자가 사용자의 개인 · 금융정보를 탈취하고 이를 통해 인증과정을 통과하는 것을 차단하는데 한계가 있다.

따라서 피싱사이트의 차단과 병행하여 사회공학적 해킹을 예방하기 위한 수단으로의 효과적인 예방홍보 정책이 필요하다. 다양한 공격수법에 대한 사용자 인식을 통해 개인 · 금융정보의 유출을 방지할 수 있다. 아울러, 이상거래탐지시스템도 효과적으로 활용될 수 있다.

또한, 이상의 대응방안을 효과적으로 시행하기 위해서는 금융거래의 보안을 위하여 기존에 시행되고 있는 정책을 연계 보완하고 새로운 제도를 도입하는 등 정책의 정비도 병행해야 할 것이다.

V. 전자금융사기 예방 정책 제안

5.1 보안수단별 거래 한도 재조정

각 금융기관은 사용자의 인증수단에 따라 보안등급을 부여하고 1일 · 1회 이체한도를 제한하고 있다. 그러나 OTP 등 상대적으로 강력한 인증수단을 사용하는 경우라 하여도 사회공학적 기법 등을 이용한 유효기간 내 재전송 공격 등을 통해 인증과정을 통과할 수 있다.[6] 그러므로 보안수준이 높은 인증수단을 사용한다 하여 피해 발생의 가능성은 낮아질 수 있으나, 피해발생시 피해규모가 커져 위험이 감소되지 않는다.

따라서 전자금융사기 위험을 감소시키기 위해서는 인증수단별로 지정된 보안등급에 따른 자금이체 한도의 차이를 낮출 필요가 있다. 특히 OTP를 사용하는 이용자는 보안카드를 사용하는 이용자에 비해 이체한도가 대폭 증가하게 되어 다액 피해 발생이 가능하므로 이에 대한 이체한도를 현재보다 낮게 재조정할 필요가 있다. 또한 개인의 이용패턴을 분석하여 다액 이체의 비중이 낮은 이용자의 경우 자동적으로 이체한도를 감액하는 방법도 고려할 수 있다.

아울러 스마트폰을 침해하는 파밍 공격의 경우 정보유출과 2Ch 인증이 한 기기에서 동시에 이루어질 수 있으므로 PC를 대상으로 한 공격에 비해 위험이 크다. 또한 스마트폰을 이용한 이체거래는 PC를 이용하는 거래에 비하여 1회 이체금액이 작다.[7] 따라서 PC와 스마트폰 이체거래의 한도액을 차별적으로 적용할 필요가 있다.

5.2 추가적인 물리적 보안 수단 도입

PC, 스마트폰 등을 이용한 기존의 인증방식은 해당 기기가 침해되면 공인인증서 및 각종 개인 · 금융정보의 유출을 통해 피해가 발생할 우려가 높다. 따라서 기기의 침해로부터 안전한 별도의 물리적 보안수단이 필요하다.

이러한 보안수단으로서 보안토큰(Hardware Security Module)을 이용할 수 있다. 보안토큰은 전자서명 생성키 등 비밀정보를 안전하게 저장 · 보관하기 위하여 키 생성 · 전자서명 생성 등이 기기 내부

6) 금융기관을 가장한 피싱사이트를 통해 금융정보를 탈취한 후, 채팅창을 열어 실시간으로 추가정보나 ARS 인증을 요구하는 수법이 등장하였다.
〈관련보도 : http://biz.chosun.com/site/data/html_dir/2014/03/19/2014031903316.html#csidxcbaecaeee44acd9a483571a9fa1d411〉

7) 전체 인터넷뱅킹 1회 이체 금액의 평균은 544만원이며, 스마트폰 기반 모바일뱅킹의 1회 이체금액의 평균은 82만원이다.〈보도자료, 한국은행, "2016년 2/4분기 국내 인터넷뱅킹서비스 이용현황", 2016. 8.〉

에서 처리되도록 구현된 하드웨어 기기로서 공인인증서의 유출을 방지할 수 있어[21] 전자금융사기 예방에 효과적이다.

공격자의 계좌로 이체를 차단하기 위한 수단으로 거래연동 OTP를 이용할 수 있다. 거래연동 OTP는 사용자가 PC에 입력한 계좌번호와 결제금액 등의 거래정보가 연동된 일회용 비밀번호를 생성하여, 거래정보가 변경된 경우 차단할 수 있다. 또한 거래연동 OTP는 표준 SSL/TLS를 이용하고 웹 표준에 기반한 서비스를 제공하므로 표준 브라우저 및 대부분의 플랫폼에서 별도의 프로그램이나 리더기없이 OTP 발생기만으로 거래서명 값을 발생할 수 있다는 특징을 가진다[21]. 이를 통해 OTP 값이 유출되거나 메모리 해킹을 통해 이체계좌번호가 변조되더라도 OTP 생성시 입력한 계좌가 아닌 다른 계좌로의 이체를 차단할 수 있어 전자금융사기를 예방할 수 있다.

5.3 사용자 인증을 탈피한 새로운 예방수단 활용

현재 공인인증서 이외에 금융권에서는 보안카드와 OTP를 추가인증 수단으로 사용하고 있고, ARS, SMS를 통한 2채널 인증을 병행하고 있다. 이러한 인증방식은 여러 번의 절차를 거치게 되므로 사용자의 편의를 저해하고 있음에도 결국 사용자 인증에만 기반하고 있어 위험을 방지하기 어려워 새로운 예방수단이 필요하다.

가장 우선적으로 고려되는 것은 이상거래탐지시스템(FDS)로서, 현재 대부분의 금융권에서는 도입하여 운영하고 있으나, 아직 운영 경험이 적고 필요한 데이터의 축적도 부족하여 충분한 피해 방지 효과를 기대하기 어렵다[20]. 꾸준한 연구 개발 및 운영경험의 축적을 통한 고도화가 필요하다.

또한 전자금융사기는 공격자가 자신들이 확보한 계좌로 피해금을 이체시키는 것을 목적으로 하므로 이체 실행단계에서 계좌를 인증하는 단계를 추가하여 이용자가 이체하고자 하는 계좌가 아닌 경우 이체를 차단할 수 있다. 이를 위해 이체 이력이 없는 새로운 계좌로 이체하는 경우 인증을 강화하거나 2채널 인증시 대상 계좌번호에 기반한 인증번호를 입력하게 하는 방법을 사용할 수 있다.

5.4 홍보 및 사용자 인식 개선

전자금융사기는 이용자 PC 혹은 스마트폰 등 거래 단말기에 대한 침입과정과 이용자에게 개인정보 · 금융정보를 입력하게 하는 과정에서 모두 이용자를 속이거나 혼란에 빠트려 정상적인 판단을 못하게 하는 사회공학적 공격수단을 활용하고 있다. 공격자의 해킹 기술뿐만 아니라 이용자의 심리적 허점을 노리는 공격 시나리오가 나날이 발전하고 있어 기존의 단말기 보안이나 시스템 보안, 인증체제의 개선 등 기술적 · 제도적 개선만으로는 예방에 한계가 있다.

따라서 전자금융사기를 예방하기 위하여 이용자에게 전자금융사기 예방 정보를 지속적으로 신속하게 전달하여야 한다. PC 및 스마트폰 보안 설정과 백신 및 보안 업데이트 설치 등 기본적인 단말기 보안 절차를 준수할 수 있도록 안내해야 하며, 공격용 악성코드나 기술 분석뿐만 아니라 피해자를 속이거나 혼란에 빠트리는 공격자의 시나리오를 분석하여 이에 대한 대응방안을 쉽게 정리하여 이용자가 이러한 수법에 빠져들지 않도록 사용자의 전자금융보안에 대한 인식을 개선해야 한다.

5.5 전자금융사기 예방제도의 체계적 연계

현재 전자금융사기 예방을 위한 제도로서 “전자금융사기 예방서비스”, “입금계좌 지정서비스”, “지연인출제도”, “지연이체제도”, “지급정지제도”, “비대면 인출제한제도” 등 다양한 예방정책이 시행되고 있다. 그러나 이러한 제도들은 세부적으로 목적은 다르나 전체적으로 모두 전자금융거래 사기 예방을 위한 목적을 가지고 도입되어 중요한 역할을 담당하고 있음에도 상호 연계와 통합적인 고려가 이루어지지 않은 채 개별적으로 시행되고 있어 이를 체계적으로 연계하여 사용자 인증부터 거래 완료시까지 각 단계별로 보안을 강화하고 종합적인 보안수준을 향상시켜야 할 필요가 있다[2].

예방 홍보에 있어서도 주의사항과 안내 문구를 보여주는 일방적인 방식으로는 효과를 달성하기 어렵다. 정책당국과 금융기관의 적극적인 협력과 이용자의 자발적 정책 참여를 통해 홍보효과를 제고하고 금융거래의 이용과정에서 자연스럽게 이용자 보안을 개선할 수 있도록 정책과 제도가 뒷받침되어야 할 것이다.

VI. 결 론

전자금융사기는 지속적으로 발생하고 있으며, 나날이 진화해가고 있다. 이러한 범죄에 대응하고 전자

금융보안을 향상시키기 위해 금융당국에서는 다양한 기술적 · 정책적 예방수단을 도입하여 시행하고 있으나 이를 근절하지는 못하고 있다.

이에 본 연구에서는 2014년, 2015년 2년간 국내 전자금융사기 발생 현황을 토대로 범죄의 유형과 수법을 분류하고 MS社의 Threat Risk Modeling 기법을 통해 전자금융거래의 자산을 식별하고, 구성요소를 목록화 한 후, STRIDE Model과 Attack Tree를 통해 위협을 체계화하고 DREAD Model을 통해 공격 수단별로 Risk를 측정하였다.

그 결과 인증수단의 차이에도 불구하고 파밍에 의한 피해발생 위험이 높으며, 추가적인 인증수단을 이용하거나 PC, 스마트폰 등의 기기 보안 강화만으로는 위험을 감소시키는데 한계가 있으며, 사용자 인증에 기반한 보안체계만으로는 공격을 차단할 수 없다는 것을 확인하였다.

이에 대응하기 위해서는 보안수단별 거래 한도를 재조정하고, 추가적인 물리적 보안 수단의 도입과 사용자 인증을 탈피한 새로운 예방수단의 활용, 홍보 및 사용자 인식 개선, 전자금융사기 예방 제도의 체계적인 연계를 통해 전체적인 금융보안수준을 향상시키는 것이 필요하다.

2016년 3월말 기준으로 17개 금융기관에 등록된 인터넷 뱅킹 등록 고객 수는 1억 1,977만 명을 넘어섰고, 일평균 이용 금액은 41조원이 넘게 되었다[22]. 이제 전자금융거래는 국민 경제활동의 기초로서 매우 중대한 역할을 하고 있으며, 전자금융거래의 안전과 원활한 이용은 반드시 선행되어야 할 문제이다. 따라서 금융보안 정책은 다양한 이론적 검토와 실질적인 검증을 통해 수립 시행되어야 하며, 항상 이용자의 관점에서 안정성과 편의성이 고려되어야 할 것이다.

References

[1] FSC(Financial Services Commission) and FSS(Financial Supervisory Service), "「Electronic Financial Fraud Prevention Service」 Test Operation-Enforcement of Identification Procedure on Replacement of Certificate and Electronic Transaction," Press Release, Sep. 14, 2012.

[2] Dae Yong Jeong, Kyung-bok Lee, and Tae Hyoung Park, "A Study on Improving the Electronic Financial Fraud Prevention Service," Journal of the Korea Institute of Information Security and Cryptology, 24(6), pp. 1243-1261, Dec. 2014.

[3] Ji Hwon Song, So Jun Ryu, "Malware evolution… Phising and Qshing Attack PC · Smartphone at same time," KISA Internet & Security Focus, pp. 36-54, Jul. 2014.

[4] Yonhap News, "ARS certification requirements in the chat window… appeared new financial fraud," http://www.yonhapnews.co.kr/economy/2014/03/20/0301000000AKR20140320180900002.HTML, Mar. 2014.

[5] ISO/IEC, "Standard 13335-1: Information technology - Security techniques - Management of information and communications technology security," Nov. 2004.

[6] Korea Information Security Agency, "Guide to Information Security Management System Risk Management," Nov. 2004.

[7] Cha Won Joo, "A Study on risk analysis and countermeasures of the type of cyber breaches to Public institutions," Master's Thesis, Korea University, Jun. 2013.

[8] Rao, K. Ram Mohan, and Durgesh Pant. "A threat risk modeling framework for Geospatial Weather Information System (GWIS): DREAD based study," International Journal of Advanced Computer Science and Applications 1(3), pp. 20-28, Sep. 2010.

[9] OWASP(The Open Web Application Security Project), "Threat Risk Modeling", Available : https://www.owasp.org/index.php/Threat_Risk_Modeling

[10] Joon ho Sa and Sangjin Lee, "Real-time Phishing Site Detection Method," Journal of The Korea Institute of Information Security and Cryptology, 22(4), pp.

819-825, Aug. 2012.
〔11〕 Ki-Hong Park, Jun-Hwan Lee and Han-Jin Cho, "Countermeasure against Social Technologic Attack using Privacy Input-Detection," The Journal of the Korea Contents Association, 12(5), pp. 32-39, May 2012.
〔12〕 Gangshin Lee, "A Study on Improving Security Controls in the Electronic Financial Transaction," Journal of the Korea Institute of Information Security and Cryptology, 25(4), pp. 881-888, Aug. 2015.
〔13〕 Kim Kyoung Gon. et al., "Using Threat Modeling for Risk Analysis of SmartHome," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp 378-379, Nov. 2015.
〔14〕 Dong-won Kim. et al. "Telemedicine Security Risk Evaluation Using Attack Tree," Journal of the Korea Institute of Information Security and Cryptology, 25(4), pp. 951-960, Aug. 2015.
〔15〕 Microsoft, "Threat Modeling Web Applications," Available : https://msdn.microsoft.com/library/ms978516.aspx
〔16〕 Microsoft, "The STRIDE Threat Model," available : https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
〔17〕 Woori bank, "ARS certified fraud through real-time chat window," Available : https://spot.wooribank.com/pot/Dream?withyou=CQSCT0116&ARTICLE_ID=15095&BOARD_ID=B00301&bbsMode=view
〔18〕 Schneier, Bruce, "Attack Trees," Dr. Dobb's Journal of Software Tools, 24(12), pp. 21-29, Dec. 1999.
〔19〕 Microsoft, "Threat Modeling," available : https://msdn.microsoft.com/en-us/library/ff648644.aspx.
〔20〕 Eui-soon Choi, Kyung-ho Lee, "A Study on Improvement of Effectiveness Using Anomaly Analysis rule modification in Electronic Finance Trading," Journal of the Korea Institute of Information Security and Cryptology, 25(3), pp. 615-625, Jun. 2015.
〔21〕 Financial Security Agency, "Research Report on the New Authentication Technologies for Electronic Financial Transaction," Financial Security Agency's Research Report. 2011-01, pp. 38-48, Mar. 2011.
〔22〕 The Bank of Korea "2016 1st Q, the domestic Internet banking service usage," Press Release, May 2016.

〈저자소개〉

정 대 용 (Dae Yong Jeong) 종신회원
1998년 2월: 경찰대학 법학과 학사 졸업
2010년 2월~2015년 1월: 충북지방경찰청 사이버범죄수사대장
2015년 2월: 고려대학교 정보보호대학원 공공보안정책학과 석사
2015년 2월~현재: 경찰수사연수원 보안·사이버수사학과장(교수)
2015년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 정보보호 정책 및 제도, 사이버범죄 예방, 디지털 포렌식

김 기 범 (GiBum Kim) 정회원
1997년 3월: 경찰대학 행정학과 학사 졸업
2008년 8월: 고려대학교 정보보호대학원 석사
2011년 8월 고려대학교 정보보호대학원 박사수료
2000년 1월~2004년 3월: 서울경찰청 사이버수사·포렌식팀장
2005년 2월~2013년 2월: 경찰청 사이버테러대응센터(현 사이버안전국) 정책기획 담당
2014년 2월~현재: 경찰대학 경찰학과 교수 및 국제사이버범죄연구센터장
〈관심분야〉 사이버범죄, 디지털포렌식, 정보보호, 디지털증거법

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2015년 1월~현재: 고려대학교 정보보호대학원 부원장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수