Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Analysis and Evaluation of a Need of Safeguard in Korean's Internet Banking Based on PDR Matrix

Geon Il Heo[1], **Chang Min Park**[2], **Huy Kang Kim**[*1]

[1]*Graduate School of Information Security, Korea University*

[2]*Information Security Center, Webcash*

ABSTRACT

Complaints among users have increased because of insufficient explanation about safeguard and forced use of safeguard. Someone has said that Internet banking safeguard(hereafter safeguard) is unnecessary because large-scale Internet banking fraud has happened continuously although financial companies have taken complaints among users lying down. But this is a misconception that people try to couple inconvenience caused by ActiveX with use of safeguard. We should judge necessity of respectively safeguard based on objective capacity and interrelation, as opposed to safeguard is unnecessary because of inconvenience. Therefore in this paper we analyzed and evaluated existing domestic safeguard's necessity based on PDR matrix namely, information security lifecycle which is classified Prevention, Detection, Response and six of Internet banking threats(account theft, public certificate snatch, malware infection, input data modification, input data snatch, phishing/pharming). This made us identify four overlapped sections and two empty sections of safeguard and know that all safeguards are certainly necessary except graphic authentication in P section of account theft and phishing/pharming, phishing prevention program in P section of phishing/pharming in case of overlapped section by evaluating their capacity. But we recognized a gap between the findings of our research and user's thought by surveying Internet banking users. So we proposed three ways to narrow the gap such as giving specific information regarding Internet banking threat and safeguard to user, giving information considered user's level to user, guaranteeing user's a choice regarding use of safeguard.

KEYWORDS: PDR matrix, Internet banking safeguards, Internet banking safeguards' capability evaluations

ARTICLE INFO: Received 23 March 2016, Revised 11 April 2016, Accepted 11 April 2016.

[*]Corresponding author is with the Graduate School of Information Security, Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, 02841, KOREA.

E-mail address: cenda@korea.ac.kr

1. 서 론

1990년대 초반, 미국의 컴퓨터 암호 기술 수출 규제로 인해 수출용 Internet Explorer의 암호화 수준이 40~56비트에 불과하여[1] 한국인터넷진흥원이 안전한 전자금융거래 환경 구축을 위해 독자적인 대칭키 암호 개발에 착수하였고 이윽고 1999년 2월, 128비트의 블록 암호 알고리즘 SEED가 완성되었다[2]. 하지만 SEED는 당시 국제 표준 암호 알고리즘이 아니었기 때문에 웹 브라우저에서 기본적으로 지원되지 않았고 SEED의 사용을 위해 별도의 plug-in을 개발해야 했다. 이에 따라 전체 웹 브라우저 중 당시 국내에서 압도적인 점유율을 보였던 Internet Explorer가 우선적으로 고려되었고 ActiveX를 통해 SEED의 사용이 가능해졌다. 이러한 전자상거래 기반 조성 아래 1999년 국내 최초의 인터넷뱅킹 서비스가 개시되었고, 2000년에는 대부분의 은행이 인터넷 뱅킹 서비스를 제공하였다[3]. 이렇게 조성된 국내 인터넷 뱅킹 환경은 1997년 9월 미국의 컴퓨터 암호 기술 수출 제한 정책이 해제된 이후에도 변화 없이 지속되었는데 이것은 결국 국내 인터넷 뱅킹 환경을 Internet Explorer와 ActiveX에 종속시켰다.

시간이 지날수록 Windows 및 Internet Explorer가 아닌 다른 OS, 다른 웹 브라우저에서의 인터넷 뱅킹 사용에 관한 요구가 증가하고, 은행마다 개별적으로 설치해야 하는 보안 프로그램, 그리고 여기서 파생되는 보안 프로그램 간의 충돌 문제 등으로 인해 사용자 불만은 점점 높아졌다. 이것은 2003년 프리뱅크 운동, 2009년 오픈뱅크 운동으로 가시화되었는데 이 운동은 특정 플랫폼에 의존하지 않는 인터넷 뱅킹 환경의 구현, 즉 이를 가능케 할 공인 인증서 사용의무 폐지, ActiveX를 이용한 보안 프로그램 설치 방식의 폐지에 관한 것이다[4]. 그러나 이러한 움직임은 안전한 인터넷 뱅킹 환경 구현 및 시스템 교체의 어려움이라는 표면적인 이유와 최선의 방법을 고민하는 것이 아닌 현행 관련 법규를 최소한으로 준수하려는 금융권의 수동적인 자세로 인해 정부와 금융권의 주목을 받지 못했다. 결국 이것은 사용자에게 “ActiveX=공인인증서” 또는 “ActiveX=보안 프로그램”이라는 매우 잘못된 고정관념을 심어주었다.

그러나 지난 2014년 초 일명 “천송이 코트” 사건을 시발점으로 핀테크(FinTech) 산업 육성 정책이 힘을 받게 되면서 국면이 급격히 전환되었다[5-6]. 전자금융거래법이 2014년 10월에 개정되어 2015년 4월부터 시행되었고 전자금융감독규정도 2015년 2월, 동년 3월, 두 차례에 걸쳐 개정되는 등 전자상거래 활성화를 위한 다양한 규제완화가 이루어졌고 이것은 인터넷 뱅킹에도 영향을 미쳤다[7-9]. 그리고 민간 및 공공기관을 대상으로 HTML5 기반의 non-ActiveX 환경 구축이 점차 진행되고 있으며[10], 마이크로소프트와 구글에서 각각 ActiveX 및 NPAPI의 지원 중단을 선언함에 따라 이것은 더욱 가속화되고 있다[11-12]. <표 1>은 전자금융감독규정 주요 개정 내용을 정리한 것이다[8-9].

표 1. 전자금융감독규정 주요 개정 내용
Table 1. The major revisions of Electronic Financial Supervision Rules

일 시	전자금융감독규정 주요 개정 내용	
2015.02	금융회사의 기술 자율성 제고	
		금융회사 등이 자율적으로 단말기 보호대책을 마련하도록 함
		공개용 웹서버 관리시 특정 인증수단의 사용 관련 조항을 삭제
		금융회사 등이 전자금융거래시 보안대책을 자율적으로 마련토록 함
		전자금융거래수단이 되는 매체와 거래인증수단이 되는 매체를 분리하도록 하는 조항을 삭제
2015.03	전자금융거래시 공인 인증서 사용의무 폐지	

안전한 인터넷 뱅킹 환경 구현이라는 명목 아래 절대 재고의 여지가 없을 것만 같았던 인터넷 뱅킹 safeguard들의 존재는 한 순간에 필수가 아닌 선택적인 존재로 바뀌었고, 국내 인터넷 뱅킹 환경은 non-ActiveX 환경으로의 신속한 변화를 요구받고 있다. 이로 인해 금융회사들은 safeguard를 EXE 파일로 묶어서 배포하는 임시방편을 취했고, ActiveX를 통해 구현했던 기존 safeguard들에 대해서는 non-ActiveX 기술로 재구현하거나 대체재를 검토하고 있다. safeguard 사용 유무에 대한 선택은 금융회사에게 일임되었음에도 불구하고 전자금융거래법 제9조에 따라 전자금융사고 발생 시 1차적 배상책임이 여전히 금융회사에 있기 때문에 금융회사는 기존 safeguard를 쉽게 포기하지 못하는 상황이고 새로운 safeguard의 도입에 있어서도 안정적인 운영을 보장할 수 없기 때문에 매우 보수적인 입장을 취하고 있다. 여기서 safeguard란 서버, 네트워크, 클라이언트 등 전 영역에 걸쳐 인터넷 뱅킹 보안을 위해 존재하는 모든 형태의 조치 수단을 가리킨다.

해외의 인터넷 뱅킹 환경을 가리키며 safeguard의 불필요성을 주장하는 이도 있지만 이것은 잘못된 주장이다. <그림 1>은 2012~2013년 주요 국가별 인터넷 뱅킹 피해 금액을 나타낸다[13-17]. 2012년 기준 영국의 피해 금액은 무려 우리나라의 약 3,332배이다. 해외의 인터넷 뱅킹은 우리나라보다 편리할지는 모르나 그것이 안전함을 보장하지는 않는다.

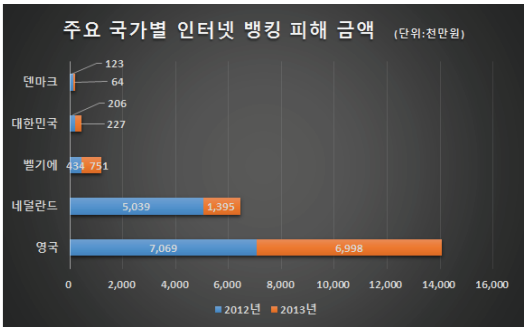

그림 1. 주요 국가별 인터넷 뱅킹 피해 금액
Figure 1. Damage to Internet banking by major country

과거에는 도입하기 급급했고 현재는 제거하기 급급한 국내 인터넷 뱅킹 safeguard의 필요성에 대한 면밀한 분석이 필요한 시점이 되었다. 그동안 국내 인터넷 뱅킹 safeguard는 그것을 설치하고 사용하는 과정에서 사용자들이 느끼는 불편함 내지 거부감, 그럼에도 반복되는 대규모 전자금융사고로 인해 본질적 역할은 무시된 채 그저 모든 전자금융사고의 원흉이자 불필요한 존재로만 인식되어 왔다. 단순히 불편해서 불필요하다는 식이 아닌 해당 인터넷 뱅킹 safeguard가 제공하는 객관적 성능과 상호간의 관계에 근거하여 그것의 필요성을 면밀히 판단하고 사용자가 실제로 인지하는 필요성과의 간극을 측정, 그리고 이것을 줄이기 위한 방법을 고민한다면 금융회사와 사용자 양측 입장에서 모두 합리적인 대안을 도출할 수 있다.

이에 따라 본 논문에서는 PDR matrix 관점에서 현존하는 국내 인터넷 뱅킹 safeguard의 필요성을 분석 및 평가한다.

2. 관련 연구

본 장에서는 본 연구에 앞서 기존의 정보보호 라이프 사이클, 인터넷 뱅킹 위협 및 safeguard 분류 현황, safeguard의 성능 평가, safeguard에 대한 사용자 의식 분석 방법에 대한 선행 연구를 분석한다.

2.1 정보보호 라이프 사이클

2000년 Bruce Schneier[18], 2001년 James LaPiedra는[19] 정보보호 라이프 사이클을 Prevention, Detection, Response, 이렇게 3가지 단계로 구분했고, 2014년 CBSS(Conference of State Bank Supervisor)에서 발간된 “A Resource Guide

표 2. 인터넷 뱅킹 위협 분류 관련 선행 연구
Table 2. The advanced research related to classification of Internet banking threat

연도	저자	분류 기준	위협	
2007	이상진 등	클라이언트	Input Validation, File System Manipulation, Process Manipulation, Cryptography, App Manipulation	
		서버	Parameter Manipulation, Sensitive Data, Session Management	
2009	김소이	클라이언트	악성코드를 활용한 사용자 접근매체의 제어, 비정상거래의 정상거래 오인을 통한 사기, 사용자 부주의, 물리적 카드 복제	
		네트워크	데이터 도청 및 변조. 네트워크 부하 초래 공격	
		서버	사용자 정보 탈취 공격, 공격을 통한 시스템 마비	
2010	한국정보통신 기술협회	-	평문구간 존재, COM 후킹 가능성, 이용한 정보 위·변조	
2011	이수미 등	이용자	이용자 부주의	
		전자적 장치	애플리케이션	App. 충돌, App. 위·변조, 역공학 공격
			웹 브라우저	웹 브라우저 위·변조, 피싱 및 파밍
			프로세스 메모리	메모리 해킹
			응용 및 커널 영역	키강제 입력, 키로깅
			입력장치	태핑, 스키밍
		네트워크	네트워크 구간	스크립트 삽입, 스니핑, 중간자 공격, 세션 훔치기 공격, 재전송 공격
			제휴 사업자 구간	내부정보유출, 분산 서비스 거부 공격
		금융기관	웹 서버	웹 해킹, 분산 서비스 거부 공격
			내부 시스템	내부 시스템 침투 공격, 내부자 정보 유출
			내부 네트워크 구간	스니핑

for BANK EXECUTIVES" 에서는 Identify, Protect, Detect, Respond, Recover, 이렇게 5가지 단계로 구분했다[20].

2.2 인터넷 뱅킹 위협 분류 현황

인터넷 뱅킹 위협 분류 관련 선행 연구는 <표 2>와 같다. 용어의 차이는 있지만 대부분 클라이언트, 네트워크, 서버 등 3개 구간으로 분류하여 위협을 정의했다.

2007년 이상진 등[21]은 클라이언트 사이드와 서버 사이드로 구분하여 간략하게 인터넷 뱅킹 위협을 분류했고, 2009년 김소이[22]는 클라이언트, 네트워크, 서버 구간으로 구분하여 보다 상세히 인터넷 뱅킹 위협을 분류했다. 2010년 한국정보통신기술협회(Telecommunications Technology Association, TTA)[23]는 구간의 구분 없이 평문구간 존재, COM 후킹 가능성, 이용한 정보 위·변조와 같이 3가지로 분류했고. 2011년 이수미 등[24]은 이용자, 전자적 장치, 네트워크, 금융기관으로 구분하여 가장 상세하게 각 구간별로 발생 가능한 인터넷 뱅킹 위협을 분류했다.

2.3 인터넷 뱅킹 safeguard 분류 현황

인터넷 뱅킹 safeguard 분류 관련 선행 연구로서 2009년 Laerte Peotta 등[25]은 디지털 인증서, OTP 토큰, OTP 카드, 브라우저 보호, 가상 키보드, 디바이스 등록, CAPTCHA, SMS, 디바이스 식별, Positive 식별, Pass-Pharse, 트랜잭션 모니터링 등 12가지로 분류했다. 2010년 한국정보통신기술협회[23]는 개인 침입차단 프로그램, 키보드해킹방지프로그램, 공인 인증서 관리프로그램, 암호화 프로그램 등 5가지로 분류했다.

2.4 성능 평가 방법론

국내의 경우 정보보호제품 도입 시 공식적인 기준으로서 성능보다는 CC 평가·인증, 보안적합성 검증 제도 등을 통한 보안성에 보다 중점을 두고 있고, 정보보호제품의 성능 평가에 관한 국내 표준은 아직 존재하지 않는다. 현재 한국인터넷진흥원에서 방화벽, 웹방화벽, 침입방지시스템, 차세대방화벽 4종을 대상으로 이를 수립 중이고 점차 정보보호제품 전반으로 평가 대상을 넓혀 가려는 계획을 가지고 있다[26].

대표적인 성능 평가 기관으로서 국내에는 한국정보통신기술협회가 있고[27], 국외에는 Tolly Group[28], NTSL[29], ICSA Labs[30], NSS Labs[31] 등이 있다. <표 3>과 같이 한국정보통신기술협회의 경우 RFC 2544[32], 3511[33]을 수용하여 개발한 국내 표준; 네트워크 보안 장비에 대한 성능 측정 방법 (TTAS_KO- 12_0044)[34]를 통해 침입차단시스템, 침입탐지시스템, 침입방지시스템과 같은 네트워크 보안 제품만을 대상으로 평가를 수행하며, 국외의 경우 기관에 따라 다소 다르지만 안티 바이러스, 안티 스파이웨어, 모바일 VPN(Virtual Private Network) 등 국내보다는 보다 다양한 정보보호제품을 대상으로 평가를 수행하고 있다. 주 평가 항목은 처리율(Throughput) 및 지연 시간(Latency)이며 이 2가지 항목이 여러 가지 상황에서 측정된다, 하지만 국내외 모두의 경우 평가 대상 제품에서 인터넷 뱅킹 safeguard는 존재하지 않았다.

2.5 인터넷 뱅킹 safeguard에 대한 사용자 의식 분석

인터넷 뱅킹 safeguard와 사용자 의식을 개별적으로 다룬 연구는 많지만 이 두 가지를 동시에 고려한 연구는 많지 않다. 2010년 김형식 등[35]은 국내 인터넷 뱅킹 safeguard의 메커니즘 및 한계를 설명하고 국내외 인터넷 뱅킹 경험자들을 대상으로 설문을 수행하여 비교적 간단하게 사용성 평가를 수행했다. 그리고 국내 인터넷 뱅킹 서비스의 보안성과 사용성을 향상시키기 위한 방안을 제시

표 3. 국내외 기관별 성능 평가 대상 및 공통 평가 항목

Table 3. The target of capacity evaluation and common evaluation item by domestic and foreign institution

기관	평가 대상	공통 평가 항목
한국정보통신기술협회	침입차단시스템, 침입탐지시스템, 침입방지시스템	처리율 (Throughput) 지연 시간 (Latency)
Tolly Group	침입차단시스템, 침입방지시스템	
NTSL	비공개	
ICSA Labs	안티 바이러스, 안티 스파이웨어, 스팸, PC 방화벽, 네트워크 방화벽, 침입방지시스템, 모바일 VPN 등	
NSS Labs	안티 바이러스, 브라우저, 호스트 침입 방지, 방화벽, 차세대 방화벽, IPS, UTM, 가상화, 취약점 평가	

했다. 동년 Catherine S. Weir 등[36]은 2차 패스워드, 토큰형 OTP, SMS OTP 등 3가지 인증 수단에 대한 사용성 평가를 수행했다. 사용성 평가를 위해 모의 환경을 구축하였고 실험자들로 직접 체험하게 한 뒤 설문, 인터뷰를 진행했다.

사용성 평각 방법론의 경우, 2002년 Genise 등[37]이 <표 4>와 같이 3가지 유형에 따라 총 6가지로 분류했다. 여기서 D는 Design, C는 Coding, T는 Testing, R은 Release의 약자이며 √는 평가 방법이 해당 단계에서 적용 가능함을 의미한다.

표 4. 사용성 평가 방법론
Table 4. The method of usability evaluation

Evaluation Type	Evaluation Method	Stage			
		D	C	T	R
Inspection	Cognitive walkthrough	√	√	√	√
	Pluralistic walkthrough	√			
Inquiry	Focus groups			√	√
	Interviews	√	√	√	√
Testing	Think aloud protocol	√	√	√	√
	Remote Usability testing	√	√	√	√

각 평가 방법에 대한 설명으로서 Cognitive walkthrough는 사용자가 아닌 평가자가 paper prototype 또는 working prototype을 통해 사용성을 논의하는 방식이고, Pluralistic walkthrough는 사용자, 개발자 등 관련된 모든 인원들이 모여 paper prototype을 통해 사용성을 검토하는 방식이다. 여기서 paper prototype이란 설계 모델로서 사용하기 위한 인터페이스를 손을 이용해 개략적으로 스케치한 것을 말하며, working prototype은 사용자가 제품 기능의 전체 또는 일부를 시험적으로 사용해 보기 위한 시제품을 말한다. Focus groups는 진행자가 사용자 그룹을 대상으로 사용에 대한 토론을 진행하는 방식이고 Interviews는 일반적인 설문을 의미한다. Think aloud protocol은 사전에 준비된 절차대로 사용자들이 제품을 사용하면서 사용성을 평가하는 방식이고 Remote Usability testing은 전자와 달리 사용자들이 자유롭게 제품을 사용하되 실험자가 해당 장소에는 위치하지 않고 사용자들의 행위를 기록하는 방식이다.

3. 방법론

3.1 PDR Matrix

인터넷 뱅킹 safeguard가 현존하는 관련 위협을 정보보호 라이프 사이클 전 영역 중에서 어느 정도 커버하고 있는지 명확히 식별하기 위해 본 논문에서는 PDR matrix를 제안한다. 가로축에는 정보보호 라이프 사이클이 위치하고 세로축에는 인터넷 뱅킹 위협이 위치한다. 그리고 두 축의 교점에 인터넷 뱅킹 safeguard가 위치한다.

P는 Prevention, D는 Detection, R은 Response를 의미한다. Prevention 영역에는 해당 위협의 발생을 무력화하기 위한 safeguard가, Detection 영역에는 해당 위협이 발생한 순간에 즉각적으로 해당 사실을 인지할 수 있게 하는 safeguard가, Response 영역에는 해당 위협 발생 시점으로부터 일정 시간이 흐른 뒤 사후 탐지를 가능하게 하는 safeguard가 위치한다.

분석 및 평가할 인터넷 뱅킹 safeguard 목록의 선정은 2015년 11월 24일 기준으로 국내 은행 인터넷 뱅킹 사이트 20곳을 직접 방문하여 safeguard의 도입 현황을 조사함으로써 이루어졌다. 조사 결과는 <표 5>와 같고 웹 언어 기반으로 구현된 것이 아닌 별도의 프로그램으로 설치되는 safeguard의 목록은 <표 6>과 같다.

인터넷 뱅킹 위협의 분류는 구간을 기준으로 했던 종래의 연구와 달리 <표 5>에 정리된 각각의

표 5. 국내 은행 인터넷 뱅킹 safeguard 도입 현황

Table 5. The current state of introduction domestic Internet banking safeguard

위협	Safeguard		일반은행													특수은행			비은행 금융기관			
			시중은행							지방은행												
			국민은행 [38]	SC은행 [39]	신한은행 [40]	외환은행 [41]	우리은행 [42]	하나은행 [43]	씨티은행 [44]	경남은행 [45]	광주은행 [46]	대구은행 [47]	부산은행 [48]	전북은행 [49]	제주은행 [50]	기업은행 [51]	농협 [52]	수협 [53]	산림조합 [54]	새마을금고 [55]	신협 [56]	우체국 [57]
계정 도용	패스워드 인증		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	보안카드 인증		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	OTP 인증	전용 H/W	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
		스마트기기																				
		IC칩	√		√					√				√								
	공인 인증서 인증		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	SMS 인증		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	ARS 인증		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	단말기 인증	PC	√			√	√								√		√	√	√	√	√	√
		스마트기기	√				√										√	√		√	√	
	예외 PC 로그인 알림				√								√									
	해외 IP 접속 차단		√	√	√		√	√						√		√	√			√		
공인 인증서 탈취	HSM	보안토큰	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√
		IC칩		√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√		√
		USIM			√								√				√					
악성 코드 감염	개인 방화벽		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	안티 바이러스 프로그램		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
입력 값 변조	시큐어 브라우저				√			√	√				√				√					
	거래연동 OTP		도 입 예 정																			
	입금계좌지정 서비스		√		√						√					√				√		
입력 값 탈취	키보드 보안 프로그램		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	가상 키보드		√	√	√	√	√	√	√												√	
	그래픽 인증				√		√						√								√	
피싱 / 파밍	피싱 방지 프로그램		√						√		√	√				√	√					√
	개인 URL																√					
	개인 이미지		√			√	√				√		√				√					
	EV SSL		√	√			√					√	√	√	√		√	√		√		
공통	SMS 알림		√	√	√	√	√	√	√				√				√	√	√	√	√	√

표 6. 인터넷 뱅킹 위협별 관련 safeguard의 제품 목록
Table 6. The product list of related safeguard by Internet banking threat

위협	Safeguard	회사명	제품명
악성코드 감염	개인 방화벽	안랩	AOS PC-FireWall[58]
		잉카인터넷	nProtect Netizen[59]
	안티 바이러스 프로그램	안랩	AOS AntiVirus/Spyware[58]
		잉카인터넷	nProtect Netizen[59]
공인 인증서 탈취	공인 인증서 보관	라온시큐어	USIM 스마트인증[60]
		위즈베라	세이프하드[61]
		미라지웍스	Sandbox[62]
		플라이하이	CPU 저장 기술(제품명:미정)[63]
입력 값 탈취	가상 키보드	NSHC	OPEN WEB nFilter[64]
	그래픽 인증	디지털존	GOTP[65]
		디멘터	Dementor_Web[66]
	키보드 보안 프로그램	라온시큐어	TouchEn Key[67]
		소프트캠프	Secure KeyStroke[68]
		안랩	AOS Anti-Keylogger[58]
입력 값 변조	시큐어 브라우저	안랩	AOS Secure Browser[58]
		위즈베라	NaRu[69]
		이니텍	INISAFE SandBox[70]
공통	FDS	인터리젠	iFDS[71]
		잉카인터넷	nProtect SecureLogMaster[72]
		KTB솔루션	KTBRealIP[73]

safeguard가 의도한 역할에 근거하여 분류했다. 이는 본 연구가 safeguard의 필요성 파악에 초점을 두었기 때문이다. 도출된 위협은 계정 도용, 공인 인증서 탈취, 악성코드 감염, 입력 값 변조, 입력 값 탈취, 피싱/파밍 등 총 6가지로서, 최종적인 인터넷 뱅킹 위협 및 관련 safeguard의 분류 결과는 <표 7>과 같다. <표 8>은 이를 토대로 작성된 PDR matrix 작성 예시이다. <표 8>의 sg.는 safeguard의 약자이다(이하 sg.).

표 8. PDR matrix 작성 예시
Table 8. The example of PDR matrix

	P	D	R
계정 도용		sg. 1	sg. 2
공인 인증서 탈취		sg. 3	
악성코드 감염	sg. 4		
입력 값 변조	sg. 5		
입력 값 탈취		sg. 6	
피싱/파밍	sg. 7		

3.2 성능 평가 방법론

특정 영역에 다수의 safeguard가 위치한 경우 각각의 필요성을 객관적으로 판단하기 위해 성능 평가가 필요하다. 처리율(Throughput)과 지연 시간(Latency)에 주로 중점을 두었던 종래의 사례와 달리 본 논문에서는 해당 safeguard가 수행해야 하는 본연의 역할 수행 여부에 초점을 맞춘다. 즉, 평가 항목으로서 해당 위협을 발생시키는 시나리오들을

표 7. 인터넷 뱅킹 위협별 관련 safeguard 분류
Table 7. The classification of related safeguard by Internet banking threat

위협	Safeguard
계정 도용	패스워드 인증, 보안카드 인증, OTP 인증, 공인 인증서 인증, 그래픽 인증, SMS 인증, ARS 인증, 단말기 인증, 예외 PC 로그인 알림, 해외 IP 접속 차단, SMS 알림
공인 인증서 탈취	HSM, SMS 알림
악성코드 감염	개인 방화벽, 안티 바이러스 프로그램
입력 값 변조	시큐어 브라우저, 거래연동 OTP, 입금계좌지정 서비스, SMS 알림
입력 값 탈취	키보드 보안 프로그램, 가상 키보드, 그래픽 인증, SMS 알림
피싱/파밍	피싱 방지 프로그램, 개인 URL, 개인 이미지, EV SSL, SMS 알림

얼마나 커버할 수 있는지, 다중 운영체제 및 다중 웹 브라우저를 지원하는지를 분석한다. <표 9>, <표 10>, <표 11>은 각각의 예시를 나타낸다. 위협 발생 시나리오 기반 성능 평가의 경우 그 결과를 O, △. X, -로 표기한다. O는 safeguard가 해당 시나리오로 인해 발생되는 위협을 완벽히 대응할 수 있는 경우, △는 인터넷 뱅킹 서비스 모듈에 safeguard 관련 모듈을 추가하는 과정 중에 발생하는 오류로 인해 우회할 수 있는 경우를 가리킨다. 예를 들어 패스워드 인증의 경우 일정 횟수의 로그인 실패 발생 시 다음 로그인 시도까지 강제적 대기시간을 할당하지 않으면 무작위 대입 또는 사전 대입 공격에 취약하다. 또는 대부분의 스마트폰 금융 앱 실행 전에 실행되는 안티 바이러스 프로그램의 경우 개발사의 API(Application Programming Interface) 사용 가이드를 정확히 준수하지 않은 경우 리버스 엔지니어링을 통해 안티 바이러스 프로그램을 실행하지 않은 채 금융 앱 실행이 가능하다. safeguard 자체 취약점으로 인한 경우는 모든 safeguard에 대한 취약점 분석이 필요함에 따라 본 연구의 범위를 벗어나므로 고려하지 않는다. X는 대응하지 못하는 경우를, -는 해당 시나리오 자체에 영향을 받지 않는 경우를 가리킨다. 다중 운영체제 및 다중 웹 브라우저 지원 유무의 경우 O, X로 표기한다.

표 9. 위협 발생 시나리오 기반 성능 평가 예시
Table 9. The example of capacity evaluation based threat occurrence scenario

	sg. 1	sg. 2	…	sg. n
scenario 1	△	X		X
scenario 2	X	-		X
…				
scenario n	O	△		-

표 10. 운영체제 기반 성능 평가 예시
Table 10. The example of capacity evaluation based operation system

	sg. 1	sg. 2	…	sg. n
Windows	O	O		X
Linux	X	X		O
MAC	O	X		X

표 11. 웹 브라우저 기반 성능 평가 예시
Table 11. The example of capacity evaluation based web browser

	sg. 1	sg. 2	…	sg. n
Internet Explorer	O	O		O
Chrome	O	O		X
Firefox	X	X		O
Opera	X	O		X
Edge	O	X		X

표 12. PDR matrix를 이용하여 나타낸 인터넷 뱅킹 safeguard 현황
Table 12. The current state of Internet banking safeguard described using PDR matrix

라이프 사이클 / 위협	Prevention	Detection	Response
계정 도용	패스워드 인증 보안카드 인증 OTP 인증 공인 인증서 인증 그래픽 인증 SMS 인증 ARS 인증 단말기 인증	예외 PC 로그인 알림 해외 IP 접속 차단	SMS 알림
공인 인증서 탈취	HSM	-	SMS 알림
악성코드 감염	개인 방화벽	개인 방화벽	안티 바이러스 프로그램
입력 값 변조	시큐어 브라우저	거래연동 OTP 입금계좌지정 서비스	SMS 알림
입력 값 탈취	키보드 보안 프로그램 가상 키보드 그래픽 인증	개인 방화벽	SMS 알림
피싱/파밍	피싱 방지 프로그램 개인 URL 개인 이미지 EV SSL	-	SMS 알림

3.3 설문 조사를 통한 사용자 의식 분석

3,1절과 3.2절의 방법론을 통해 도출된 결과와 실제 인터넷 뱅킹 사용자의 생각의 차이를 분석하기 위해 설문 조사를 실시한다. 설문 조사에 과한 자세한 내용은 4.7절을 참고하기 바란다.

4. 실험

본 장에서는 3장에서 제시한 방법론에 따라 PDR matrix에 인터넷 뱅킹 safeguard를 배치하고 각각의 필요성을 분석 및 평가한다.

4.1 중복 영역과 부재 영역 식별

<표 12>는 PDR matrix에 safeguard를 배치한 결과를 나타내고, <표 13>은 이에 근거하여 복수의 safeguard가 중복되어 존재하는 영역과 아예 존재하지 않는 영역을 정리하여 나타낸 것이다. 중복 영역은 총 다섯 개로서 P 영역에 세 개, D 영역에

표 13. safeguard의 중복 영역과 부재 영역
Table 13. safeguard의 중복 영역과 부재 영역

라이프 사이클 / 위협	중복			부재		
	P	D	R	P	D	R
계정 도용	√	√				
공인 인증서 탈취					√	
악성코드 감염						
입력 값 변조		√				
입력 값 탈취	√					
피싱/파밍	√				√	

두 개 존재했고, 부재 영역은 총 두 개로서 모두 D 영역에 존재했다.

4.2 PDR matrix의 각 영역별 safeguard 현황 분석

본 절에서는 각 위협별로 PDR matrix의 각각의 영역에 배치된 safeguard를 검토한다. P 영역과 D 영역에 위치하는 safeguard는 위협에 따라 모두 상이했지만 R 영역의 경우 악성코드 감염의 경우를 제외하고 모두 SMS 알림이 위치했다. 이는 해당 위협에 대한 직접적인 사후 대응용 safeguard가 존재하지 않고, 해당 위협 이후 발생한 추가 행위(계좌 이체, 공인 인증서 재발급, 비밀번호 변경 등)를 통해 인지하기 때문이다.

4.2.1 계정 도용

P 영역에는 패스워드 인증, 보안카드 인증, OTP(One Time Password) 인증, 공인 인증서 인증, 그래픽 인증, SMS(Short Message Service) 인증, ARS(Audio Response System) 인증, 단말기 인증 등이 위치했다. 패스워드 인증은 지식 기반의 가장 보편적인 인증 수단이고, 보안카드 인증과 OTP 인증은 소유 기반의 인증 수단으로서 보안카드보다는 OTP가 권장된다. 공인 인증서 인증도 소유 기반의 인증 수단이지만 HSM(Hardware Security Module)을 사용한다는 전제 하에 전자 서명을 통한 부인 방지 기능도 수행한다. 로그인 시에는 본인 식별을 목적으로, 계좌 이체와 같은 전자금융거래 시에는 전자 서명 목적으로 사용된다. 그래픽 인증은 마우스를 통해 사전에 등록된 이미지를 사전에 등록된 순서에 따라 선택함으로써 인증이 이루어진다. SMS 인증과 ARS 인증은 로그인 이후 계좌 이체 등 전자금융 거래 시 추가 인증 목적으로 사용된다. 단말기 인증은 사전에 등록된 단말기에서만 인터넷 뱅킹 서비스를 제공하는 것으로서, 등록되지 않은 단말기에서는 단순 조회와 같은 지극히 제한된 서비스만 이용 가능하다.

D 영역에는 예외 PC 로그인 알림, 해외 IP 접속 차단이 위치했다. P 영역의 단말기 인증을 사용할 경우 예외 PC 로그인 알림은 최적의 즉각 탐지 수단이 될 수 있다. 해외 IP 접속 차단은 이름처럼 해외에서 접속을 시도할 경우에만 차단하기 때문에 국내에서 계정 도용이 발생 시에는 즉각적인 탐지가 불가하다. 그리고 예외 PC 로그인 알림과 달리 SMS 발송은 하지 않고 접속만 차단한다. 대신 정상적인 접속 시 팝업 창을 통해 통보해주는 경우는 존재한다.

R 영역에는 SMS 알림이 위치했다. 단, 직접적인 사후 탐지가 아닌 계정 도용 이후 추가 행위를 통한 간접적인 사후 탐지이다. 공격자는 도용한 계정을 이용하여 공인 인증서 재발급, 계좌 이체 등의 행위를 할 수 있고 이러한 추가 행위는 SMS 알림을 통해 사용자가 알 수 있다. SMS 알림은 은행에 따라 다소 차이가 존재하는데 비밀번호 변경, 공인 인증서 재발급과 같이 빈도가 잦지 않고 필수적인 사항은 은행에서 사용자에게 자동적으로 통보하지만, 입출금 발생 시와 같이 빈도가 잦고 상대적으로 중요도가 떨어지는 경우는 사용자의 선택에 따라 SMS 알림 서비스를 제공한다. 이때 과금 부담은 사용자에게 있으며 과금 방식은 종량제와 정액제로 구분된다.

4.2.2 공인 인증서 탈취

P 영역에는 HSM이 위치했다. HSM은 보안 토큰, IC(Integrated Circuit Card) 카드, 스마트기기 USIM(Universal Subscriber Identity Module) 등 3가지의 형태로서 존재하고, MS CSP[74], PKCS#11[75],

PC/SC[76]와 같은 표준 API를 통해 특정 동작만 허용하기 때문에 HSM 내부에 저장된 공인 인증서 및 생성된 개인키의 외부 유출이 불가능하다. 사용 시에만 단말기에 연결하고 사용 후에는 단말기에서 제거하므로 같은 단말기를 사용하는 타인의 위협으로부터 안전을 보장받을 수 있다. 그리고 설령 HSM을 분실하더라도 일정 횟수 이상 PIN(Personal Identification Number) 번호 입력 오류가 발생할 경우 초기화 외엔 방법이 존재하지 않는다. HSM을 통해 공인 인증서의 부인방지 기능의 실질적 실현을 달성할 수 있고 패스워드 인증이라는 단순한 개인키 추출 과정의 안전성을 보장받을 수 있다.

D 영역에는 safeguard가 존재하지 않았다. 현재로서는 공인 인증서 탈취 발생 시 즉각적으로 알 수 있는 방법이 없다.

R 영역에는 계정 도용의 경우와 동일하게 SMS 알림이 위치했다. 역시 직접적인 사후 탐지가 아닌 간접적인 사후 탐지이다. 탈취한 공인 인증서와 패스워드를 사용한 계좌 이체 등의 추가 행위 발생 시 탐지할 수 있다.

4.2.3 악성코드 감염

P 영역과 D 영역에는 개인 방화벽이 위치했다. 인터넷 뱅킹 사용 시 제공되는 안티 바이러스 프로그램에는 상용 안티 바이러스 프로그램과 달리 실시간 감시 기능이 존재하지 않았고 사용자가 직접 실행하는 수동 검사 기능만 존재하였고 반면에 개인 방화벽에는 실시간 감시 기능이 존재했다. 개인 방화벽은 기본적인 방화벽 기능과 더불어 해킹 툴을 비롯한 외부와 의심스러운 통신을 시도하는 프로그램을 탐지하고, 해당 프로그램이 접근하는 IP 주소, Port 번호를 추출 및 차단하는 기능을 수행하기 위한 실시간 감시를 수행한다. 사실상 개인 방화벽이 안티 바이러스 프로그램의 역할을 수행하고 있다.

R 영역에는 안티 바이러스 프로그램이 위치했다. 수동 검사 기능을 통해 악성코드에 감염된 시스템을 치료할 수 있다. 의심 파일을 실행시키지 않은 채 signature 및 평판 정보 등으로만 탐지하기 때문에 false negative가 발생할 확률이 존재한다.

4.2.4 입력 값 변조

P 영역에는 시큐어 브라우저가 위치했다. 이것은 공격자의 디버깅, 리버스 엔지니어링 시도를 차단함으로써 메모리 해킹 등과 같은 MITB(Man In The Browser) 공격으로부터 인터넷 뱅킹 플랫폼인 웹 브라우저를 보호한다. MITB는 네트워크 구간에서 발생하는 MITM (Man In The Middle) 공격과 무관하다. 시큐어 브라우저는 독립적인 웹 브라우저 또는 기존 웹 브라우저의 모듈 등 두 가지의 형태로서 존재한다.

D 영역에는 거래연동 OTP, 입금계좌지정 서비스가 위치했다. 거래연동 OTP는 기존 OTP와 달리 이체할 계좌번호, 이체 금액 등의 거래 관련 정보를 기반으로 OTP를 생성하고 이를 기준으로 인터넷 뱅킹 사용 단말기에서 발생하는 메모리 변조를 탐지한다. 물리적으로 분리된 OTP 기기에서 거래 관련 정보를 입력하기 때문에 인터넷 뱅킹 사용 단말기에서 발생하는 그 어떠한 형태의 메모리 변조에도 대응할 수 있다. 국내의 경우 현재 도입을 위해 논의가 진행 중이다[77] 입금계좌지정 서비스는 사전에 등록된 계좌번호로만 이체를 허용하는 서비스이다.

R 영역에는 계속 동일하게 SMS 알림이 위치했다. SMS 알림을 통해 계좌 이체 발생 시 사후 탐지가 가능하다.

4.2.5 입력 값 탈취

P 영역에는 키보드 보안 프로그램과 가상 키보드, 그래픽 인증이 위치했다. 키보드 보안 프로그램은 별도의 다운로드를 통해 설치되며 키스트로크 발생 시 해당 키 값이 탈취되지 않도록 하거나 탈취되어도 공격자가 원래 값을 알기 어렵게 하기 위한 일련의 행위를 수행한다. 가상 키보드는 디스플레이 장치에 출력된 키보드 이미지를 마우스로 클릭함으로써 원하는 값을 입력한다. 그래픽 인증은 4.2.1절에서 설명했듯이 사전에 등록된 이미지 형태의 영어 알파벳 또는 숫자를 사전에 등록된 순서에 따라 마우스로 입력한다.

D 영역에는 개인 방화벽이 위치했다. 입력 값 탈취가 이루어진 후에는 이것을 공격자에게 전송하기 위해 FTP(File Transfer Protocol)를 이용한 파일 전송, 이메일 발송 등 다양한 방법을 통해 불특정 외부로의 네트워크 연결이 생성된다. 4.2.3절에서 설명했듯이 개인 방화벽은 의심스러운 트래픽을 발생시키는 프로그램을 탐지하고 해당 프로그램이 접근하는 IP 주소, Port 번호를 추출 및 차단한다.

R 영역에는 SMS 알림이 위치했다. 탈취된 정보를 바탕으로 계좌 이체 및 공인 인증서 재발급 등의 추가 행위 시 사후 대응이 가능하다.

4.2.6 피싱/파밍

피싱/파밍의 발생 기준은 위조된 사이트로의 단순 접속 여부가 아닌 위조된 사이트로의 접속 후 보안카드 번호와 같은 금융정보의 입력 여부이다.

이러한 기준 아래, P 영역에는 피싱 방지 프로그램, 개인 URL(Uniform Resource Locator), 개인 이미지, EV SSL(Extended Validation Secure Socket Layer)이 위치했다. 피싱 방지 프로그램은 black list를 통해 위조된 사이트로의 사용자 접근을 차단하는 프로그램이다. 개인 URL 서비스는 사용자가 지정한 문자열을 조합하여 인터넷 뱅킹 사이트의 도메인 주소를 재정의하는 것으로서 “공식 도메인 주소/개인 지정 문자열”의 형태를 띤다. 개인 이미지 서비스는 사용자가 지정한 특정 이미지가 인터넷 뱅킹 사이트 접속 시 화면에 나타나게 하는 것을 말한다. EV SSL은 기존 SSL의 주요 기능인 스니핑 방지, 데이터 변조 방지, 피싱/파밍 방지 중 피싱/파밍 방지를 가시적인 측면에서 강화한 것으로서, EV SSL을 적용한 구간의 경우 웹 브라우저 주소창이 녹색으로 표시되어 사용자의 식별력을 높여준다.

D 영역에는 어떠한 safeguard도 존재하지 않았다. 위조된 사이트에 금융정보를 입력한 후 공격자에게 유출될 때 즉각적으로 탐지하는 것은 거의 불가능하다.

R 영역에는 마찬가지로 SMS 알림이 위치했다. 이 경우도 간접적인 사후 탐지로서 훔친 금융정보를 이용하여 공인 인증서 재발급 및 계좌 이체 등의 추가행위 발생 시 탐지될 수 있다.

4.3 위협 간 연관 관계 분석

본 절에서는 4.4절의 중복 영역의 Safeguard 필요성 분석에 앞서 위협 간 연간 관계를 분석한다. <표 14>에서 볼 수 있듯이 6개의 위협 중 대다수인 공인 인증서 탈취, 입력 값 변조, 입력 값 탈취, 피싱/파밍은 악성코드 감염으로 인해 영향을 받게 되는 위협으로 나타났다. 현실적으로 어려운 얘기지만, 인터넷 뱅킹을 사용하는 개인 단말기의 악성코드 감염률을 획기적으로 줄이거나 인터넷 뱅킹 사용 시 일정 수준의 보안성이 보장된 전용 단말기를 사용한다면 나머지 위협으로 인한 영향을 크게 감소시킬 수 있다.

표 14. 위협 간 연관 관계
Table 14. Associative relations between threats

구분		후행 위협					
		악성코드 감염	계정 도용	피싱/파밍	공인 인증서 탈취	입력 값 변조	입력 값 탈취
선행 위협	악성코드 감염	–	√	√	√	√	√
	계정 도용	–	–	–	–	–	–
	피싱/파밍	–	√	–	–	–	–
	공인 인증서 탈취	–	√	–	–	–	–
	입력 값 변조	–	–	–	–	–	–
	입력 값 탈취	–	√	–	–	–	–

계정 도용은 악성코드 감염 이후 추가 행위인 공인 인증서 탈취, 입력 값 탈취, 피싱/파밍이 뒤따라야 했다. 결론적으로 악성코드 감염만 원천적으로 봉쇄할 수 있다면 대다수의 위협으로부터 자유로울 수 있다.

4.4 중복 영역의 safeguard 분석

본 절에서는 4.1절에서 언급된 것 중 다섯 개의 중복 영역에 대한 분석을 수행한다.

4.4.1 계정 도용의 P 영역

계정 도용의 P 영역은 8개의 safeguard로 구성되어 있고, 위협 발생 시나리오 대응 유무에 따라 이것들을 평가한 결과는 <표 15>이다. 패스워드 무작위 대입, 패스워드 사전 대입, 패스워드 도용, 보안카드 도용, OTP 탈취[78-79], 공인 인증서 도용, 그래픽 도용[80-81], 착신 전환[82], SMS 탈취[83], 단말기 인증 해지, 백도어를 통한 원격 접속 등의 시나리오를 통해 8개의 safeguard 모두 우회가 가능했고 이에 따라 특정 safeguard를 단독으로 선택하는 것은 불가능하다. multifactor 인증을 통해 공격자의 work factor를 높일 수 있는 방안을 고려해야 한다. 경우의 수는 크게 3가지로 나눌 수 있다.

첫 번째, 단말기 인증과 패스워드 인증, 공인 인증서의 결합이다. 4.3절에서 언급했듯이 대부분의 위협의 시발점이 악성코드 감염이기 때문에, 만약 인터넷 뱅킹을 사용하는 단말기의 악성코드 감염을 원천적으로 봉쇄한다면 단말기 인증과 기본적인 패스워드 인증만으로도 충분하다. 패스워드 인증은 동일 단말기를 사용하는 타인으로부터의 계정 도용을 막기 위함이다. 그리고 공인 인증서는 본인 인증이 아닌 부인 방지를 위해 사용된다.

두 번째, 단말기 인증과 HSM에 저장된 공인 인증서 인증, 거래연동 OTP 인증과의 결합이다. 첫 번째의 경우는 일정 수준의 보안성을 갖춘 인터넷 뱅킹 전용 단말기를 도입하지 않는 이상 아직은 현실적으로 실현되기 어렵다. 이에 따라 다양한 safeguard의 조합이 고려될 수 있는데 이 중 단말기 인증과 HSM 기반의 공인 인증서 인증, 거래연동 OTP 인증과의 결합이 가장 보안성이 높다. 아울러 HSM 기반의 공인 인증서는 부인 방지의 실현을 위해, 그리고 거래연동 OTP는 입력 값 변조의 탐지를 위해 반드시 사용되어야하기 때문에 이것들을 계정 도용의 예방을 위해 다시 사용하는 것은 비용 대비 효율 측면에서도 아주 좋다고 할 수 있다.

표 15. 시나리오 기반 계정 도용 safeguard 평가
Table 15. The evaluation of safeguards related to account theft based scenario

Safeguard / Scenario	패스워드 인증	보안카드 인증	OTP 인증	공인 인증서 인증	그래픽 인증	SMS 인증	ARS 인증	단말기 인증
패스워드 무작위 대입	△	-	-	-	-	-	-	-
패스워드 사전 대입	△	-	-	-	-	-	-	-
패스워드 도용	X	-	-	-	-	-	-	-
보안카드 도용	-	X	-	-	-	-	-	-
OTP 탈취	-	-	X	-	-	-	-	-
공인 인증서 도용	-	-	-	X	-	-	-	-
그래픽 도용	-	-	-	-	X	-	-	-
SMS 탈취	-	-	-	-	-	X	-	-
착신 전환	-	-	-	-	-	X	X	-
단말기 인증 해지	-	-	-	-	-	-	-	X
백도어를 통한 원격 접속	-	-	-	-	-	-	-	X

세 번째, HSM이 아닌 일반 저장매체에 저장된 공인 인증서와 OTP가 아닌 보안카드를 사용하는 사용자들을 위한 SMS 인증, ARS 인증, 그래픽 인증과의 자유로운 조합이다. HSM의 사용은 강제화 되었지만[84] 아직 그때까지 시일이 더 필요하고 거래연동 OTP도 아직 국내에 도입되지 않았다. 일반 OTP의 경우도 구매 비용이 높은 편이 아니지만 사용자가 선뜻 구매하려 하지 않는다. 이러한 사용자들은 SMS 인증, ARS 인증, 그래픽 인증 중 택일하게 하여 계정 도용의 발생 가능성을 낮춰야 한다.

그런데 이 조합은 2016년에 스마트 보안카드[85]가 예정대로 상용화될 경우 달라질 수 있다. 스마트 보안 카드는 스마트폰 앱을 이용해 OTP처럼 그때 그때 보안카드를 생성하는 방식으로서 현재 금융결제원과 은행권에 의해 공동 개발 중이다, 스마트 보안카드는 사용자에게 익숙한 보안카드 이미지를 그대로 활용하기 때문에 고객 저항이 거의 나타나지 않을 것이라 기대되므로 상용화 시 OTP 사용에 부담을 가지는 기존 보안카드 사용자들이 빠르게 스마트 보안카드로 흡수될 것이라 예상된다. 스마트 보안카드로 대체될 경우 은행의 보안카드 제작 비용이 사라지고 추가 인증이 필요하지 않아 SMS 발송 및 ARS 발신 비용도 절감할 수 있다.

하지만 가장 좋은 것은 금융회사에서 어떠한 하나의 최선의 조합을 선택하여 강요하는 것보다는 사용자가 보유하거나 선택한 safeguard에 따라 유연하게 다양한 인증 정책을 운용하는 것이다. 예를 들어 현재 우리나라의 경우 OTP 인증을 신청한 사용자는 보안카드를 이용한 인증이 불가능하다. OTP 기기를 다른 곳에 두고 오거나 은행 업무 시간이 아닐 때 OTP 기기가 망가졌을 경우 금융거래가 불가능하다. <표 16>은 트랜잭션 유형에 따른 8개의 safeguard의 조합 예시이다. 해당 예시는 전자금융거래 시 발생 가능한 트랜잭션을 로그인, 잔액 조회와 같은 단순 조회, 계좌 이체 등 세 가지로 구분하였고, 계좌 이체는 거래 금액에 따라 하, 중, 상, 최상 등 네 단계로 구분하였다. 계좌 이체의 등급을 구분하는 기준은 각각의 사용자의 예금 총액 및 평소 거래량에 따라 별도로 설정하는 것이 적합하므로 정의하지 않았다. 현재는 각 은행에서 고객이 사용하는 safeguard의 조합에 따라 등급별 이체한도를 제한하고 있지만 엄밀히 말해서 그

표 16. 트랜잭션 유형에 따른 계정 도용 P 영역의 safeguard 조합 예시
Table 16. The example of combination of safeguards related to account theft's prevention section by transaction type

<table>
<tr><td rowspan="3">트랜잭션</td><td rowspan="3">로그인,
잔액
조회</td><td rowspan="3">계좌이체</td><td colspan="4">계좌 이체 금액</td></tr>
<tr><td>하</td><td>중</td><td>상</td><td>최상</td></tr>
<tr><td colspan="4">구간별 금액 하한 및 상한 설정은 개인별 자산 규모 및 평소 거래 금액에 따라 설정</td></tr>
<tr><td rowspan="4">Safe
guard</td><td rowspan="4">패스
워드</td><td>보안카드,
HSM에 저장되지 않은
공인 인증서</td><td>conditional
possible_A</td><td colspan="3">unconditional impossible</td></tr>
<tr><td>보안카드,
HSM에 저장된
공인 인증서</td><td>unconditional
possible</td><td>conditional
possible_A</td><td colspan="2">unconditional
impossible</td></tr>
<tr><td>OTP,
HSM에 저장되지 않은
공인 인증서</td><td>unconditional
possible</td><td>conditional
possible_A</td><td colspan="2">unconditional
impossible</td></tr>
<tr><td>OTP,
HSM에 저장된
공인 인증서</td><td colspan="2">unconditional
possible</td><td>conditional
possible_A</td><td>conditional
possible_B</td></tr>
<tr><td>해석</td><td colspan="6">- conditional possible_A : 인증된 단말기일 경우 추가 인증 없이 계좌이체 가능
인증되지 않은 단말기일 경우 SMS 또는 ARS 또는 Graphic 인증 후 계좌이체 가능
- conditional possible_B : 거래연동 OTP일 경우 계좌이체 가능
- unconditional possible : 추가 인증 없이 계좌이체 가능
- unconditional impossible : 해당 범위에 속하는 금액에 대한 계좌이체는 불가능함</td></tr>
</table>

기준은 객관적일 수 없다. 3등급 범위에 속하는 금액이 누군가에겐 아무 것도 아닐 수 있겠지만 또 다른 누군가에겐 1등급 범위에 속하는 금액만큼 큰 것일 수 있다. 트랜잭션별 safeguard의 조합의 경우 로그인 또는 단순 조회 기능은 패스워드만으로 인증한다. 계좌 이체의 경우 보안카드인지 OTP인지, 그리고 공인 인증서가 저장된 곳이 HSM인지 아닌지에 따라 네 가지의 조합을 가진다. 각각의 조합은 추가 인증 없이 가능한 계좌 이체 금액의 구간이 다르고, 단말기 인증 또는 SMS/ARS/그래픽 인증 등의 추가 인증 또는 거래연동 OTP 사용 유무에 따라 상승될 수 있는 최대 이체 금액의 구간이 서로 다르다.

4.4.2 계정 도용의 D 영역

계정 도용의 D 영역은 2개의 safeguard로 구성되어 있다. 단말기 인증을 사용할 경우 예외 PC 로그인 알림이 해외 IP 접속 차단 기능을 포함하므로 예외 PC 로그인 알림만 사용하면 된다. 다만 단말기 인증을 사용하지 않을 경우 해외 IP 접속 차단이 유일한 대안이다.

4.4.3 입력 값 변조의 D 영역

입력 값 변조의 D 영역은 2개의 safeguard로 구성되어 있다. 거래연동 OTP가 아직 국내에 도입되지 않았기 때문에 현재로서는 입금계좌지정 서비스가 유일한 대안이다. 하지만 거래연동 OTP가 도입될 경우 최초에 구입 비용이 발생하지만 입금계좌지정 서비스처럼 사전 등록이 필요하지 않고 입금계좌번호뿐만 아니라 거래 금액의 변조까지 탐

지할 수 있으며 소유 기반의 multifactor 인증 효과도 있으므로 상대적으로 그 효과가 탁월하다.

4.4.4 입력 값 탈취의 P 영역

입력 값 탈취의 P 영역은 세 개의 safeguard로 구성되어 있고, 위협 발생 시나리오 대응 유무에 따라 이것들을 평가한 결과는 <표 17>이다. 입력 값 탈취와 관련된 시나리오는 하드웨어[86-87] 또는 소프트웨어[88] 형태의 키로거를 이용한 kernel level과 user level의 각 구간별 후킹, 그리고 화면 캡쳐이다. 키보드에서 발생하는 키스트로크를 보호하는 키보드 보안 프로그램은 이 시나리오에 모두 영향을 받으며 이 중 하드웨어 키로거는 대응이 불가했고 소프트웨어 키로거 및 화면 캡쳐 시도 시 무력화될 가능성이 존재했다. 마우스 입력 기반의 가상 키보드와 그래픽 인증은 태생적으로 키로거에 영향을 받지 않고 화면 캡쳐 시도에만 영향을 받는데 키보드 보안 프로그램과 마찬가지로 무력화될 가능성이 존재했다. 마우스 기반 입력 발생 시 해당 값의 탈취가 아닌 화면 캡쳐가 주를 이루는 이유는 각 문자열마다 자판이 존재하는 키보드와 달리 마우스는 어플리케이션의 정보와 결합하지 않는 한 좌클릭인지, 우클릭인지 또는 휠 버튼의 움직임인지 등에 대한 단편적인 사실밖에 알 수 없기 때문이다.

하드웨어 키로거는 키보드의 케이블과 본체의 PS/2(Personal System/2) 또는 USB(Universal Serial Bus) 포트 사이에 존재하는데 그 생김새가 마치 젠더와 매우 유사하여 자세히 살펴보지 않으며 식별하기 쉽지 않고 키스트로크가 물리적으로 시스템에 진입하기 이전에 가로채기 때문에 키보드 보안 프로그램이 대응할 수 없다. 하지만 하드웨어 키로거는 직접 설치해야 하는 어려움이 있고 휴대용 PC의 경우에는 내장된 키보드를 사용하기 때문에 외부 키보드를 연결하지 않는 한 하드웨어 키로거 사용 자체가 불가함에 따라 크게 문제가 되지 않는다. 키보드 보안 프로그램의 주요 대응 대상인 소프트웨어 키로거는 kernel level과 user level의 다양한 구간에서 후킹을 시도하는데 kernel level에서의 각 구간은 <표 17> 하단과 같이 인터페이스가 PS/2인지, USB인지, Bluetooth인지에 따라 달라진다. 키보드 보안 프로그램이 정상적으로 동작할 경우 설령 입력 값이 탈취되더라도 그 값은 평문이 아닌 암호문일 확률이 높기 때문에 크게 문제가 되지 않는다. 하지만 웹페이지에서 키보드 보안 프로그램을 호출하는 영역이나 그것의 주요 DLL(Dynamic-Link Library)이 변조될 경우 키보드 보안 프로그램을 무력화시킬 수 있다. 이러한 시도는 키보드 보안 프로그램의 취약점을 분석하는 것보다 상대적으로 훨씬 쉽기 때문에 공격자들이 선호하는 경향이 있다. 마지막으로 화면 캡쳐의 경우 가상 키보드 도입 초기에는 사용자의 편의성을 고려하여 클릭 시 화면에서도 그 변화를 동시에 나타내었고 마우스 포인터도 하나로만 나타내었기 때문에 사용자의 입력 값이 노출되는 사례가 존재했지만 현재는 사용자의 입력이 발생해도 화면에는 표시되지 않고 마우스 포인터도 최소 2개 이상으로 나타내며 원격 접속을 통한 인터넷 뱅킹을 제한함에 따라 화면 캡쳐를 통한 입력 값 탈취는 점점 어려워지고 있다. 하지만 가상 키보드나 그래픽 인증도 앞서 설명한 키보드 보안 프로그램의 사례와 같이 동일한 사유로 무력화될 수 있다.

다중 운영체제 및 웹 브라우저 지원 여부 관점에서 평가한 결과는 <표 18>, <표 19>로서 키보드 보안 프로그램은 Windows, Internet Explorer에서만 동작했으며 그 외의 운영체제나 웹 브라우저 환경에서는 가상 키보드나 그래픽 인증을 사용해야 했다.

그런데 가상 키보드 및 그래픽 인증은 거의 대부분의 운영체제와 웹 브라우저에서 작동되고 키

로거의 위협으로부터 완전히 배제되어 있음에도 불구하고 마우스 기반의 입력으로 인한 불편함 때문에 패스워드의 길이가 짧아지고 그 구성이 단순해져서 결과적으로 패스워드의 안전성이 낮아지는 경향이 있다. 이러한 문제는 가상 키보드보다 상대적으로 문자열 집합 크기가 작은 그래픽 인증에서 더 심각하게 나타난다. 반대로 키보드 보안 프로그램은 Windows의 Internet Explorer에서만 동작하고 별도의 프로그램을 통해 설치해야 하며, 복수의 개발사의 키보드 보안 프로그램이 설치되었을 경우 프로그램 실행 시 충돌이 발생하여 사용자에게 불편함을 가중시킬 수 있지만 키보드 입력의 이점이

표 17. 시나리오 기반 입력 값 탈취 safeguard 평가

Table 17. The evaluation of safeguards related to input data snatch based scenario

Scenario \ Safeguard		키보드 보안 프로그램	가상 키보드	그래픽 인증
Hardware Keylogger		X	-	-
Software Keylogger	User Level	△	-	-
	Kernel Level	△	-	-
Screen Capture		△	△	△

※ 입력 값 탈취 주요 발생 구간 및 방식
1) User Level : SubClassing, MessageHooking, API Hooking, BHO Disclosure, Screen Capture
2) Kernel Level :
- PS/2 : Port Scanning, IDT Hooking, H/W Breakpoint using Debug IDT Hooking, Filter and Service Callbank Hooking, VKD Hooking
- USB : USB Bus Drivers Hooking, USB Bus Drivers Upper Filter, USB Hub Drivers (or Usbccgp Drivers) Lower Filter, USB Hub Drivers (or Usbccgp Drivers) Hooking, USB Hub Drivers (or Usbccgp Drivers) Upper Filter, HIDUsb Drivers Lower Filter, HIDUsb Drivers Hooking, HIDUsb Drivers Upper Filter, VKD Hooking

표 18. 운영체제 기반 입력 값 탈취 safeguard 평가

Table 18. The evaluation of safeguards related to input data snatch based operation system

Scenario \ Safeguard	키보드 보안 프로그램	가상 키보드	그래픽 인증
Windows	O	O	O
Linux	X	O	O
Mac	X	O	O

표 19. 웹 브라우저 기반 입력 값 탈취 safeguard 평가

Table 19. The evaluation of safeguards related to input data snatch based web browser

Web Browser \ Safeguard	키보드 보안 프로그램	가상 키보드	그래픽 인증
Internet Explorer	O	O	O
Chrome	X	O	O
Firefox	X	O	O
Opera	X	O	O
Edge	X	O	O

있고 이것은 안전성 높은 패스워드의 수립을 가능하게 한다.

즉 다중 운영체제 및 웹 브라우저 지원을 위해 가상 키보드, 키보드 사용을 원하는 사용자들을 위해 키보드 보안 프로그램이 모두 제공되어야만 한다. 그래픽 인증의 경우 입력 값으로서 실제 암호가 아닌 이미지간의 상대 경로를 받아들이기 때문에 입력 값 탈취가 발생해도 무의미한 것이 장점이지만 이것은 가상 키보드도 가지고 있는 유사한 장점이고 화면 캡쳐 위협은 모두가 직면하고 있는 위협이므로 가상 키보드를 대체할 만한 특별한 부분이 존재하지 않는다.

4.4.5 피싱/파밍의 P 영역

피싱/파밍의 P 영역은 4개의 safeguard로 구성되어 있고, 시나리오 대응 유무에 따라 이것들을 평가한 결과는 <표 20>이다. 피싱/파밍과 관련된 모든 시나리오[89]가 사용자를 위조된 사이트로 유도하는데 초점이 맞춰져 있기 때문에 피싱 방지 프로그램을 제외한 나머지 3개의 safeguard는 모든 시나리오를 커버할 수 있다. 그리고 <표 21>의 경우 피싱 방지 프로그램은 알려진 위조된 사이트에 대해서는 접속 자체를 차단하기 때문에 사용자의 금융정보 입력 행위 자체가 발생할 수 없으나 알려지지 않은 신규 위조 사이트에 대해서는 어떠한 대응도 할 수 없다. 그러나 개인 URL, 개인 이미지, EV SSL은 알려진 또는 알려지지 않은 모든 위조 사이트에 대하여 사용자에게 식별력을 제공한다. 이에 따라 본 절에서는 개인 URL, 개인 이미지, EV SSL에 대해서만 고려한다.

개인 이미지는 2가지의 형태로 제공된다. 로그인 전에 확인하는 것, 로그인 이후에 확인하는 것이다. 대부분의 은행의 경우 로그인 이후에 사용자가 설정한 이미지를 표시함으로써 해당 사이트의 진위 여부를 판단하게 하였으나, 특정 은행의 경우 개인 URL의 입력을 통해 접속한 사이트에서 사용자가 설정한 개인 이미지를 표시함으로써 사이트의 진위 여부를 확인할 수 있게 하였다. 개인 URL과 개인 이미지를 개별적으로 제공하는 것보다는 위의 사례와 같이 개인 URL과 개인 이미지를 결합함으로써, 로그인을 하지 않은 채 접속한 인터넷 뱅킹 사이트의 진위 여부를 확인할 수 있게 하는 것이 좋은 방법이다. APT(Advanced Persistent Threat)가 아닌 불특정 다수를 대상으로 한 일반적인 공격이라 가정할 때, 공격자가 누군가를 특정하여 개인 URL과 개인 이미지를 모두 알아내고 그것을 바탕으로 위조된 사이트를 구축, 해당 사이트로 유도하기 위해 악성코드를 제작할 확률은 현실적으로 높지 않다.

EV SSL은 "웹 브라우저 주소창이 녹색이면 안전하다"는 식의 홍보가 많이 이루어지고 있는데 이것이 오히려 사용자를 위태롭게 할 수 있다. 공격자도 EV SSL을 신청하고 발급받을 수 있기 때문이다. 엄밀히 말하면 웹 브라우저 주소창의 색깔뿐만 아니라 접속한 사이트와 EV SSL 인증서가 발급된 대상이 일치하는지 반드시 확인해야 한다. 하지만 EV SSL은 DV(Domain Validation) SSL이나 OV(Organization Validation) SSL과 달리 신청 시 사업자 등록증과 신청자를 교차 확인하는 등 발급 절차가 까다롭고 발급 비용도 최소 60만원 이상에 육박하기 때문에[90] 공격자가 피싱/파밍을 위해 EV SSL을 구매할 확률은 사실상 높지 않다.

이러한 점들을 고려했을 때 개인 URL 및 개인 이미지의 조합과 EV SSL 중 택일함에 있어서 기준이 되는 것은 비용이다. SSL은 네트워크 구간의 암호화를 위해 반드시 사용해야 한다. 다만 피싱/파밍 방지를 위해 개인 URL과 개인 이미지의 조합을 사용할 것인지, 기존의 SSL을 EV SSL로 변경할 것인지에 대해서는 사용자의 선호도 파악과 같은 추

표 20. 시나리오 기반 피싱/파밍 safeguard 평가 (1)
Table 20. The evaluation of safeguards related to phishing/pharming based scenario (1)

Safeguard / Scenario	피싱 방지 프로그램	개인 URL	개인 이미지	EV SSL
hosts 변조	△	O	O	O
hosts.ics 변조	△	O	O	O
iframe 삽입	△	O	O	O
VPN 터널링	△	O	O	O
DNS 변조	△	O	O	O
메모리 변조	△	O	O	O
공유기 변조	△	O	O	O

표 21. 시나리오 기반 피싱/파밍 safeguard 평가 (2)
Table 21. The evaluation of safeguards related to phishing/pharming based scenario (2)

Safeguard / Scenario	피싱 방지 프로그램	개인 URL	개인 이미지	EV SSL
알려진 위조 사이트	O	O	O	O
알려지지 않은 위조 사이트	X	O	O	O

가적인 분석이 필요하다.

4.5 그 외 safeguard의 주요 이슈 고찰

본 절에서는 중복 영역에 속한 safeguard는 아니지만 회자됐던 주요 safeguard 이슈에 대해 분석한다.

4.5.1 공인 인증서 무용론

공인 인증서는 거래 당사자의 신원 확인, 거래 정보의 위·변조 방지, 거래 사실의 부인 방지 등을 목적으로 하는 PKI(Public Key Infrastructure) 기반의 전자금융거래용 인감증명서이다. 공인 인증서와 관련된 대부분의 전자금융사고는 공인 인증서 자체의 문제가 아닌 단순히 잘못된 보관 방식으로 인한 것임에도 불구하고, 대개의 사람들은 모든 문제의 원인이 공인 인증서 자체에 있는 것으로 잘못 인식하고 있고 이러한 악영향은 그 기반 기술인 PKI에까지 미쳤다. 그리고 이것은 ActiveX 폐지 정책과 FIDO(Fast IDentity Online)[91] 표준 확산과 맞물리면서 공인 인증서를 폐지하자는 여론의 형성으로 이어졌다.

하지만 잘못된 공인 인증서 보관 방식과 사용자의 사용성을 고려하지 않은 ActiveX 기반의 사용 환경이 문제일 뿐 공인 인증서와 그 기반 기술인 PKI에는 문제가 없다. 아울러 현재 확산 중인 FIDO 기반의 생체 인증 표준은 PKI와의 결합을 시도하고 있다[92]. 최근 모바일 결제 서비스 시장에서 열풍을 불러일으키고 있는 삼성페이, 애플페이 등이 단적인 예이다.

이러한 흐름에 맞춰 인터넷 뱅킹 서비스에서도 생체 인증이 검토 또는 도입 중에 있다. 모바일 뱅킹 시 공인 인증서를 사용하기 위해 입력하는 비밀번호를 지문으로 대체하는 것이 검토 또는 도입 중에 있고, 인터넷전문은행 및 일반 은행의 무인 스마트점포에서의 비대면 실명확인 수단 중 하나

로서 생체 인증이 권고되었다[93].

하지만 생체 인증의 도입이 궁극적으로 공인 인증서의 폐기를 목적으로 하는 것이 아니며 현재로서는 보안카드나 OTP와 같은 추가 인증수단으로서 활용하거나 단순 조회 또는 소액 이체와 같은 상대적으로 위험성이 낮은 거래에 한해서만 인증 수단 등으로 활용함으로써 생체 인증의 안정성을 검토해야 한다. 향후 공인 인증서의 사용성을 개선하고 생체 인증의 안전성을 검토하는 과정 속에서 사용자의 선호도에 따라 두 개 모두 양립하거나 한쪽으로 치우치는 형태를 띠게 될 것이다.

4.5.2 키보드 보안 프로그램 무용론

혹자는 OTP 인증을 사용하면 해당 값은 탈취해도 재사용이 불가능하기 때문에 키보드 보안 프로그램이 필요하지 않다고 주장한다. 하지만 이것은 잘못된 주장이다.

초기의 키보드 보안 프로그램은 아이디, 비밀번호, 계좌 비밀번호, 보안카드 번호, 인증서 비밀번호 등만 암호화했지만 지금은 메모리 변조 방지를 위해 거래정보(이체금액, 입금정보)까지 추가적으로 암호화하고 평문과 함께 금융회사로 전송된다.

4.5.3 개인 방화벽 무용론

또 어떤 혹자는 개인 방화벽은 인터넷 뱅킹 사용 중에만 동작하기 때문에, 인터넷 뱅킹이 완전히 종료된 후에 탈취한 정보를 공격자에게 보냄으로써 개인 방화벽을 우회할 수 있으므로 불필요하다 주장한다. 하지만 이것 역시 잘못된 주장이다.

모든 safeguard는 각각의 한계를 지니고 있고 그것을 보완하기 위해 다단계로 보안 체계를 구축한다. 개인 방화벽은 특정 프로그램에서 발생되는 의심스러운 인/아웃바운드 트래픽을 탐지하고 차단하는 것이 기본적인 역할이다. 위에서 언급된 특정 사례 하나만을 근거로 하여 개인 방화벽이 불필요하다고 주장하는 것은 매우 위험한 발상이다. 위와 같은 사례가 존재한다면 개인 방화벽 폐기에 관한 논의가 아닌 해당 부분을 보완하기 위한 논의가 이루어져야 한다. 그리고 설령 개인 방화벽이 종료된 후에 탈취된 정보가 유출되었다 하더라도 만약 키보드 보안 프로그램이나 가상 키보드와 같은 safeguard를 사용 중이라면 탈취된 값은 평문이 아닌 암호문일 확률이 높으므로 공격자에게 무의미하다. 물론 해당 암호문이 단순 치환문일 경우 상대적으로 복호화가 쉬울 수 있지만 이것은 치환주기를 단축시키거나 치환체계를 고도화할 문제이지 개인 방화벽의 역할과는 무관하다.

4.6 최종 분석 결과

4.2절의 PDR matrix에 따른 safeguard 배치 결과와 이 결과를 토대로 수행된 4.3절의 위협 간 연관관계 분석, 4.4절의 중복 영역의 safeguard 분석에 따른 각각의 인터넷 뱅킹 safeguard의 필요성 판정 결과는 <표 22>와 같다. 여기서 도입율은 <표 5>에 근거하여 작성되었다.

계정 도용의 경우 P 영역의 보안카드 인증, D 영역의 해외 IP 접속 차단을 제외하고 모든 safeguard가 반드시 필요하다고 판단되었다. 모든 safeguard의 도입율은 100%이나 사용자들의 선택은 자유롭지 못하기 때문에 이에 대한 개선이 필요하다.

악성코드 감염, 공인 인증서 탈취, 입력 값 변조의 경우 이와 관련된 모든 safeguard가 반드시 필요하다고 판단되었다. 조사된 금융기관들의 도입율도 100%였다. 입력 값 변조의 입금계좌지정 서비스는 거래연동 OTP가 도입되지 않은 지금은 필요하나 도입된 이후에는 필요하지 않다.

입력 값 탈취의 경우 P 영역의 그래픽 인증을 제외한 모든 safeguard가 반드시 필요하다고 판단되었다. 단, 시큐어 브라우저의 도입율이 20%에 불과하다.

표 22. safeguard 별 필요성 판정
Table 22. The judgement of necessity by safeguards

위협		Safeguard	판정	도입율
계정 도용	P	패스워드 인증	필수	100%
		보안카드 인증	선택	100%
		OTP 인증	필수	100%
		공인 인증서 인증	필수	100%
		그래픽 인증	선택	5%
		SMS 인증	필수	100%
		ARS 인증	필수	100%
		단말기 인증	필수	100%
	D	예외 PC 로그인 알림	필수	10%
		해외 IP 접속 차단	선택	45%
	R	SMS 알림	필수	100%
공인 인증서 탈취	P	HSM	필수	100%
	R	SMS 알림	필수	100%
악성 코드 감염	P	개인 방화벽	필수	100%
	D			
	R	안티 바이러스 프로그램	필수	100%
입력 값 변조	P	시큐어 브라우저	필수	20%
	D	거래연동 OTP	필수	0%
		입금계좌지정서비스	필수	25%
	R	SMS 알림	필수	100%
입력 값 탈취	P	키보드 보안 프로그램	필수	100%
		가상 키보드	필수	100%
		그래픽 인증	선택	5%
	D	개인 방화벽	필수	100%
	R	SMS 알림	필수	100%
피싱/ 파밍	P	피싱 방지 프로그램	선택	35%
		개인 URL & 개인 이미지	필수 택일	5%
				30%
		EV SSL		50%
	R	SMS 알림	필수	100%

피싱/파밍의 경우 P 영역의 피싱 방지 프로그램을 제외하고 모든 safeguard가 필수적으로 필요하다고 판단되었다. 단 개인 URL과 개인 이미지의 조합과 EV SSL 중에서 하나를 선택해야 한다. 이것은 4.7절에서 추가적으로 분석한다. 피싱/파밍과 관련된 safeguard의 도입율은 전반적으로 낮은 편인데, 피싱 방지 프로그램이 35%, 개인 URL이 5%, 개인 이미지가 30%, EV SSL이 50%를 차지했다.

4.7 설문 수행

본 절에서는 설문을 통해 인터넷 뱅킹 사용자가 <표 22>의 결과를 얼마나 수용하는지, 간극이 존재한다면 그 크기는 어느 정도인지, 이유는 무엇인지를 분석한다. 이를 위해 인터넷 뱅킹에 대한 기본 사항 및 인터넷 뱅킹의 위협과 safeguard에 대한 사용자 인지 정도를 사전 설문하고 뒤이어 본 내용인 safeguard의 필요성 및 문제점, 지불의사금액(Willingness To Pay, 이하 WTP)[94] 추정에 관해 설문한다. 그리고 개인 URL과 이미지의 조합과 EV SSL간의 선호도를 설문하며 마지막으로 설문 수행 내역에 대한 본인의 신뢰도를 설문한다.

설문은 약 2주일 동안 온라인상에서 진행되었으며 총 응답자는 160명(남자 84%, 여자 16% / IT 직군 61%, 非IT 직군 39%)이었고 이중 인터넷 뱅킹 사용 경험자는 143명이었다. 그리고 여기서 88명의 응답자가 2개 이상의 인터넷 뱅킹을 사용했다.

우선 사전 설문 항목의 경우, 인터넷 뱅킹이 안전하다고 생각한 응답자가 전체 중 17%, safeguard가 인터넷 뱅킹의 안전성에 영향을 미친다고 생각한 응답자 또한 26%로 나타나는 등 인터넷 뱅킹의 안전성 및 safeguard의 역할에 대한 신뢰도가 매우 저조하게 나타났다. 그리고 전체 응답자 중 32%가 safeguard와 ActiveX를 동일시하는 잘못된 이해를

가지고 있었다.

인터넷 뱅킹 위협의 사용자 인지 정도에 관한 설문의 경우, 대다수의 인터넷 뱅킹 위협을 들어봤거나 간단히 설명할 수 있는 것으로 나타났다. 악성코드 감염이 89%로 가장 높았고, 입력 값 변조는 상대적으로 낮은 62%였다. 그리고 safeguard의 사용자 인지 정도 및 필요성에 대한 설문 결과는 <표 23>과 같다.

표 23. safeguard 별 사용자 인지 정도 및 필요성
Table 23. Users'understanding and necessity by safeguards

위협		Safeguard	인지	필요성
계정 도용	P	패스워드 인증	84%	50%
		보안카드 인증	87%	36%
		OTP 인증	83%	63%
		공인 인증서 인증	90%	34%
		그래픽 인증	33%	8%
		SMS 인증	88%	35%
		ARS 인증	85%	28%
		단말기 인증	69%	30%
	D	예외 PC 로그인 알림	66%	67%
		해외 IP 접속 차단	71%	62%
	R	SMS 알림	83%	90%
공인 인증서 탈취	P	HSM	23%	59%
	R	SMS 알림	83%	87%
악성 코드 감염	P	개인 방화벽	68%	68%
	D			67%
	R	안티 바이러스 프로그램	71%	75%
입력 값 변조	P	시큐어 브라우저	50%	65%
	D	거래연동 OTP	42%	56%
		입금계좌지정서비스	57%	48%
	R	SMS 알림	83%	83%
입력 값 탈취	P	키보드 보안 프로그램	86%	48%
		가상 키보드	73%	44%
		그래픽 인증	33%	22%
	D	개인 방화벽	68%	34%
	R	SMS 알림	83%	78%
피싱/ 파밍	P	피싱 방지 프로그램	34%	44%
		개인 URL	31%	17%
		개인 이미지	24%	14%
		EV SSL	31%	25%
	R	SMS 알림	83%	80%

safeguard의 사용자 인지 정도는 거래연동 OTP(42%), HSM(23%)과 같은 신규 safeguard와 피싱 방지 프로그램(34%), 그래픽 인증(33%), 개인 URL(31%), EV SSL(31%), 개인 이미지(24%)와 같은 피싱/파밍 관련 safeguard를 제외하고 높게 나타났다. 즉, 나머지 safeguard들에 대해서는 응답자들이 들어봤거나 간단히 설명할 수 있는 것으로 나타났다. SMS 알림(평균 84%)은 위협과 관계없이 아주 높게 나타났고 공인 인증서 인증(90%), SMS 인증(88%), 보안카드 인증(87%), ARS 인증(85%), 패스워드 인증(84%), OTP 인증(83%) 등과 같은 계정 도용 관련 safeguard 및 키보드 보안 프로그램(86%), 가상 키보드(73%), 안티 바이러스 프로그램(71%), 개인 방화벽(68%), 입금계좌지정서비스(57%), 시큐어 브라우저(50%) 등과 같은 입력 값 변조/탈취 관련 safeguard에서 높게 나타났다. 그리고 응답자가 인터넷 뱅킹 위협 및 safeguard의 인지 정도에 관한 문항을 답하는데 있어 어려움을 겪은 경우, 그 이유 중의 하나로서 금융회사의 안내 부족이라는 것에 약 절반 이상(59%)이 동의했다.

인터넷 뱅킹 safeguard의 문제점에 관한 설문의 경우 safeguard에 대한 선택권이 없다고 생각한 응답자가 전체 중 67%, safeguard에 대한 금융회사의 구체적인 정보 제공이 부족하다고 생각한 응답자가 전체 중 70%, safeguard는 필요하지만 usability의 고려가 부족하다고 생각한 응답자가 전체 중 79%, safeguard의 필요성에 대한 금융회사의 캠페인이 부족하다고 생각한 응답자가 전체 중 74%로 나타났다. 필수적인 safeguard임에도 불구하고 사용자 입장에서 필요성이 낮다고 판단하게 된 이유

를 여기서 가늠해 볼 수 있다.

인터넷 뱅킹 safeguard의 WTP 추정에 관한 설문은 추가 인증 safeguard로 한정한 경우와 모든 safeguard를 포함한 경우로 구분하였다. 전자의 경우 구간형 질문 방식으로 WTP를 추정한 결과 5,000원 미만이 29%로서 가장 높았고 10,000원 미만이 20%로서 뒤를 이었다. 지불 의사가 없는 경우도 28%에 이르렀다. 나머지 금액 구간은 10% 미만으로서 매우 낮게 나타났다. 후자의 경우 개방형 질문 방식으로 WTP를 추정한 결과 각각 7,730원(0원 포함), 7,895원(0원 제외)으로 나타났다. 0원을 포함한 평균 금액은 지불 거부나 지불하지 않을 의사를 강하게 드러낸 응답자를 반영한 것으로서 지불 의사가 있는 응답자만 정리한 평균 금액보다 신뢰성이 높다.

개인 URL 및 개인 이미지와의 조합과 EV SSL 중 선호도를 파악하는 설문에서는 응답자 중 67%가 EV SSL을 선택했다. 웹 브라우저의 주소창이 녹색으로 강조되는 직관성에서 많은 호응을 얻은 것으로 추정된다.

마지막으로, 응답자의 40%가 자신이 설문한 결과를 신뢰하지 못하는 것으로 나타났다. 이것은 인터넷 뱅킹 safeguard에 대해 사용자들의 이해가 부족하여 설문 응답에 어려움을 겪었음을 의미한다.

5. 고찰

5.1 safeguard에 대한 사용자 안내 및 선택권 부족

4.7절에서의 설문 수행 결과, 인터넷 뱅킹 사용자들은 인터넷 뱅킹 위협 및 safeguard의 현황을 완전히 정확하게 알고 있지 못 했고 그에 따라 각 safeguard의 필요성 역시 제대로 판단하기 어려워 했다. 그리고 그에 대한 대표적인 원인으로는 인터넷 뱅킹 위협 및 safeguard에 대한 금융회사의 면밀한 안내 부족인 것으로 나타났다.

실제로 국내에서 인터넷 뱅킹 서비스를 제공하고 있는 20곳을 조사한 결과에서도 설문에서 지목되었던 원인과 관련된 내용들이 문제점으로 드러났다. 우선, <그림 2>에서와 같이 전체 중 불과 55%의 은행만이 메인 페이지에 보안센터 메뉴를 위치시켰다. 나머지 45%의 은행은 보안센터 메뉴가 특정 메뉴 하위에 존재하거나 보안 관련 정보가 여러 곳에 흩어져 있어서 해당 은행에서 제공되는 safeguard 목록 및 기능 등 관련 정보를 한눈에 파악하기 어려웠다.

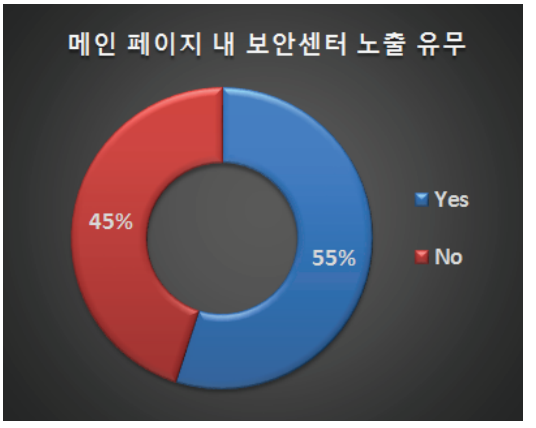

그림 2. 메인 페이지 내 보안센터 노출 유무

Figure 2. Whether security center is placed in main page or not

그리고 <그림 3>과 같이 전체 중 30%의 은행에서 safeguard 설치 관련 안내 페이지를 제공하지 않았다. 정보를 제공하는 70% 은행들도 페이지만 존재할 뿐 정작 사용자들에게 반드시 필요한 정보를 제대로 제공하지 못하는 등 유명무실한 경우가 많았다. 비교적 자세하게 안내된 곳이 일부 존재했으나 safeguard에 대한 안내, 인터넷 뱅킹 사용 시 유의사항, 개인정보보호 정책 등 다양한 항목들이

구분 없이 뒤섞여 있어 가독성이 매우 낮았고, 그 외 나머지 은행들은 각 safeguard에 대한 간략한 설명만이 존재할 뿐 역할, 한계, 미설치에 따른 위험 등 주요 항목들이 구체적으로 안내되지 않았다.

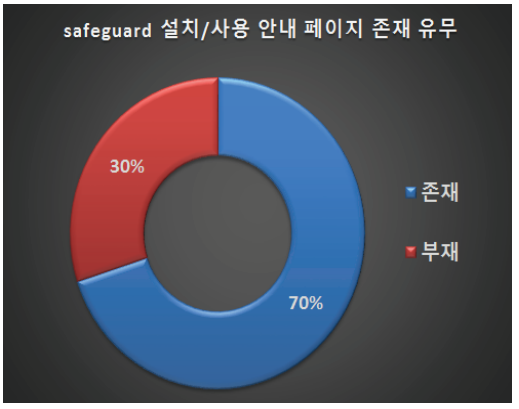

그림 3. safeguard 설치/사용 안내 페이지 존재 유무
Figure 3. Whether information pages related to safeguard's installation/use are existed or not

그리고 <그림 4>와 같이 전체 중 무려 40%의 은행들이 다중 OS/웹 브라우저 지원에 관한 안내 페이지가 존재하지 않았다.

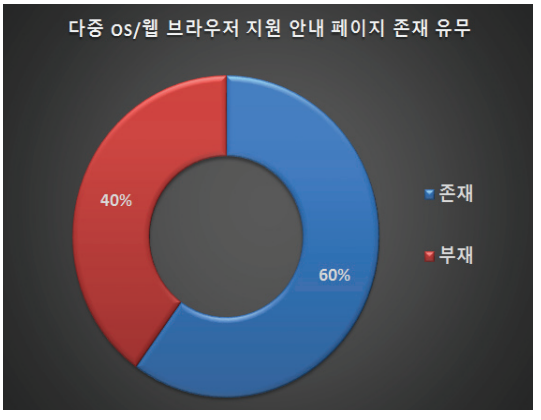

그림 4. 다중 OS/웹 브라우저 지원 안내 페이지 존재 유무
Figure 4. Whether information pages related to multiple OS/web browser support are existed or not

아울러 <그림 5>와 같이 전체 중 무려 95%의 은행이 인터넷 뱅킹 사용자의 동의 없이 safeguard의 설치 및 사용을 강제했다.

사용자 설문 결과 및 위의 조사 결과를 종합해 보았을 때, 인터넷 뱅킹 safeguard 사용과 관련된 주요 문제점은 사용자가 선택할 수 있는 부분이 거의 존재하지 않고, 강제로 설치 및 사용함에도 불구하도 해당 safeguard 역할, 한계, 미설치에 따른 위험 등 필수적인 정보를 알 수 없다는 점이었다. 아울러 이러한 간극을 해소하기 위한 금융회사의 노력도 매우 부족하다는 점이었다. 다음 5.2절에서는 이에 대한 대응방안을 제안한다.

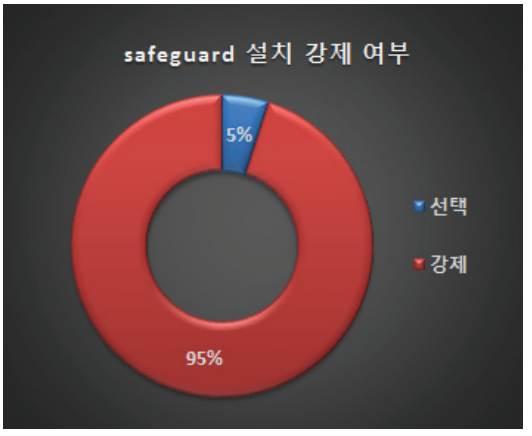

그림 5. safeguard 설치 및 사용 강제 여부
Figure 5. Whether it is forced to install/use safeguards or not

5.2 대응 방안

5.2.1 인터넷 뱅킹 위협 및 safeguard에 대한 구체적 안내

인터넷 뱅킹 위협과 그와 관련된 safeguard에 대한 구체적인 안내가 필요하다. 특히 safeguard의 경우 역할, 한계, 미설치 시 발생 가능한 위험 등이 구체적으로 안내되어야 하며 이러한 정보를 기

반으로 필수/선택적 safeguard로의 구분이 필요하다. 이를 통해 사용자들의 safeguard 선택을 도울 수 있고 경우에 따라 safeguard의 사용을 강제하더라도 수반되는 거부감을 줄일 수 있다. 이와 관련된 좋은 사례 2가지가 있다.

미국의 Bank of America의 경우 <그림 6>과 같이 Privacy & Security라는 단일 메뉴를 통해 Checking & Savings Security, Card & Debit Security, ATM Security, Online Banking Security, Mobile Banking Security, Email Fraud 등 인터넷 뱅킹을 포함한 모든 형태의 금융거래의 보안에 대해 다루고 있고 각 영역별로 How we protect you, What you can do, Types of fraud 등의 항목으로 구분하여 인터넷 뱅킹 위협 및 safeguard에 대한 정보를 일관성 있게 사용자에게 제공하고 있다[95].

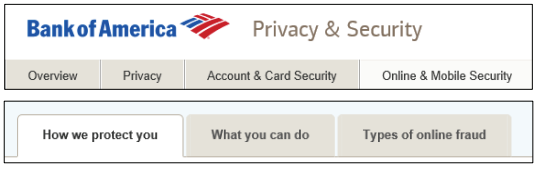

그림 6. Bank of America의 Privacy&Security 메뉴
Figure 6. Bank of America's Privacy&Security

그림 7. 대구은행의 safeguard 필수/선택 구분 사례
Figure 7. The example of the classification of safeguard by viewpoint of necessity and option in Daegu Bank

대구은행은 <그림 7>과 같이 safeguard를 필수/선택으로 구분하여 사용자에게 안내하고 있다[47]. 대구은행의 분류안의 옳고 그름을 떠나 이러한 안내는 주요 safeguard에 대한 사용자의 수용력을 높여주고 전반적인 거부감을 감소시킬 수 있다.

5.2.2 사용자 눈높이에 맞춘 안내

5.2.2절에서 제안한 내용을 실천함에 있어서 가장 중요한 것은 사용자의 눈높이를 고려하는 것이다. 아무리 자세히 설명되어 있다 하더라도 사용자가 그것을 이해하고 받아들이지 못한다면 아무 소용이 없다. 본 절에서는 다른 분야에서 사용자의 눈높이를 고려한 사례를 분석한다.

<그림 8>과 <그림 9>는 네이버에서 제작한 개인정보 취급방침의 Easy 버전[96] 및 인포그래픽 버전[97]이다. 개인정보 취급방침은 개인정보를 취급하는 기업이라면 의무적으로 게시해야 하는 것으로서, 해당 기업이 수집하는 개인정보의 항목, 목적, 보존 기간, 개인정보의 제3자 제공 및 위탁에 관한 내용, 개인정보의 기술적/관리적 보호 대책 등 다양한 내용들을 담고 있다. 하지만 그만큼 양이 방대하고 사용되는 용어도 익숙하지 않아 일반 사용자 입장에서는 읽고 이해하는 것이 쉽지 않다. 네이버에서는 이를 해소하기 위해 쉬운 말로 재해석한 Easy 버전, 그림으로 표현한 인포그래픽 버전을 각각 제작하여 사용자들에게 제공하였다. 단순히 개인정보 보호법을 준수하려는 수동적인 자세가 아닌 소비자가 개인정보 보호의 중요성을 인식하고 실천할 수 있도록 적극적인 자세로 개인정보 취급방침 제작에 임한 네이버의 사례는 인터넷 뱅킹 위협과 safeguard를 사용자에게 안내해야 할 금융권에서도 눈여겨봐야할 대목이다.

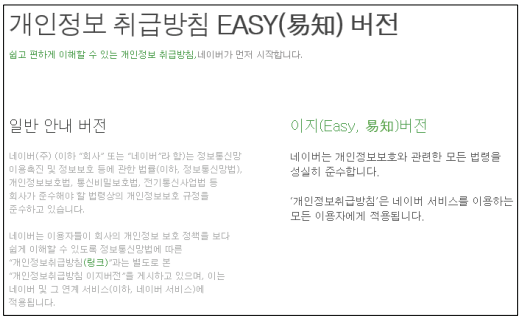

그림 8. 네이버의 개인정보 취급방침 Easy 버전
Figure 8. EASY version of Privacy policy in NAVER

그림 9. 네이버의 개인정보 취급방침 인포그래픽 버전
Figure 9. Infographic version of Privacy policy in NAVER

<그림 10>과 <그림 11>, <그림 12>는 디자인 사무소 PearsonLloyd가 A Better A&E(Accident and Emergency)라는 주제로 제안한 응급실 안내 패키지이다[98]. 2012년 영국의 NHS(National Health Service)는 응급실 내 폭력과 그로 인해 발생되는 막대한 각종 비용으로 인해 많은 부담을 안고 있었고 이를 줄이기 위해 원인 규명에 나섰다. 그 결과 응급실에 대한 명확하고 효율적인 정보와 안내가 부족한 가운데, 기약할 수 없는 대기 시간으로 인해 발생된 환자의 불만, 질병에 대한 불안 및 고통 등이 복합적으로 결합되면서 환자가 의료진에게 공격적인 성향을 띠게 하는 것으로 드러났다. A Better A&E는 <그림 10>의 Process Map을 통해 환자 본인이 Check in, Assessment, Treatment, Outcome 등 응급실 전체 진료 과정 중 어느 단계에 있는지 안내했고, <그림 11>과 같은 화면을 통해 응급실의 현재 혼잡도를 안내했다. 그리고 <그림 12>와 같이 Check in, A&E Waiting area, Assessment, X-Ray Seating area, Major injuries 등 각 상황별 주요 사항을 안내했다. 이렇게 함으로써 전체 중 75%의 환자가 대기시간 동안의 불만이 줄어들었다고 답했고 폭력 발생 빈도 또한 이전 대비 50%로 감소했다.

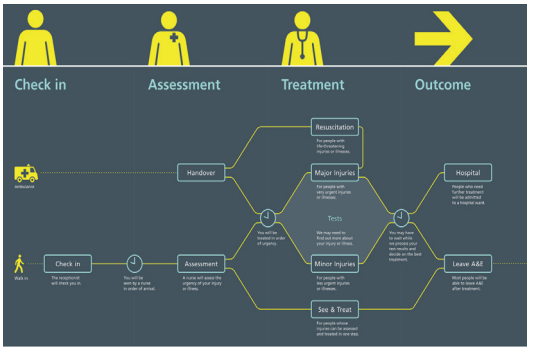

그림 10. 환자들의 이동을 도식화한 프로세스 맵
Figure 10. A process map which illustrates the patient journey

그림 11. 현재 대기시간을 나타내는 실시간 화면
Figure 11. Live information screens which display current waiting times for departments

그림 12. 각 구역마다 설치된 단계별 진료 행위 안내 판넬
Figure 12. Panels, installed throughout the department, which guide patients through each stage of their care

앞서 설명했듯이 인터넷 뱅킹 safeguard 사용에 있어서도 비슷한 문제가 존재한다. safeguard를 사용함으로써 어떤 효과를 보는지, 내 PC에는 어떠한 영향이 미치는지 정확한 정보를 알지 못한 상황에서 인터넷 뱅킹 웹페이지에 접속하자마자 강제로 자동적으로 설치되는 safeguard에 대해 사용자들의 불만이 매우 높다. 왜 일정 수준의 불편함을 감내하고 safeguard를 사용해야 하는지에 관한 보다 자세하고 친절한 안내가 수반된다면 사용자들의 불만은 크게 감소될 것이다.

5.2.3 인터넷 뱅킹 safeguard 선택권 제고

사용자의 눈높이에 맞춘 인터넷 뱅킹 위협 및 safeguard에 대한 안내, 그 다음으로 고려되어야 할 것은 인터넷 뱅킹 safeguard에 대한 사용자의 최종적 선택권 제고이다. 4.4.1절에서 언급했었던 인증 수단을 비롯한 모든 safeguard에 대하여 사용자의 선택권을 제고해야 한다. <그림 13>은 BNP PARIBAS Global Markets의 로그인 화면이다[99]. BNP PARIBAS는 프랑스의 대형 은행 그룹 중 하나로서 Global Markets는 주식, 채권, 선물과 같은 파생 상품을 매매하는 사이트이다. 이곳에서는 로그인 시 자체 패스워드 또는 Markit Hub[100]라는 사이트의 패스워드를 이용한 인증, 전화 인증, OTP 인증 등 네 가지의 인증 수단을 제공했으며 각각에 대해 Normal Security 또는 High Security로 보안성을 나타냈고 해당 인증 수단을 상징하는 그림을 사용함으로써 사용자의 선택을 도왔다.

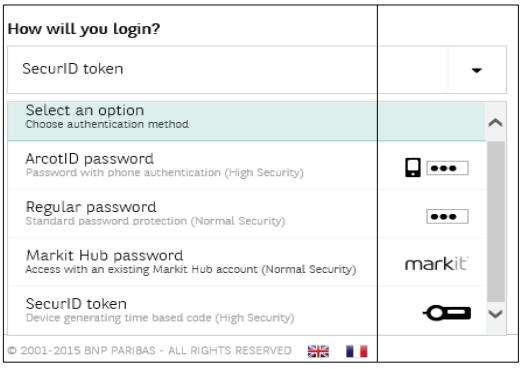

그림 13. BNP PARIBAS Global Markets 로그인 화면
Figure 13. BNP PARIBAS Global Markets' login user interface

6. 결 론

ActiveX 기반의 동작 방식 및 강제 설치로 인해 인터넷 뱅킹 safeguard에 대한 사용자의 불만이 나날이 높아져가는 가운데 대규모 전자금융사고는 끊임없이 발생하면서 인터넷 뱅킹 safeguard에 대한 무용성에 대한 주장이 계속 제기되어 왔다. 하지만 이것은 ActiveX로 인해 발생되는 불편함을 safeguard 사용에 관한 문제에 결부시킨 매우 잘못된 상황이다. 불편해서 불필요하다는 식이 아닌 각각의 인터넷 뱅킹 safeguard의 객관적인 성능과 상호간의 관계에 근거하여 그것의 필요성을 판단해야 한다. 그리고 해당 결과와 사용자가 실제로 인지하는 필요성과의 간극을 측정하고 간극을 줄이기 위한 방법을 고민해야 금융회사와 사용자 양측 입장에서 모두 합리적인 대안이 도출될 수 있다. 이에 따라 본 논문에서는 PDR matrix 즉,

Prevention, Detection, Response로 구분한 정보보호 라이프 사이클과 6개의 인터넷 뱅킹 위협(계정 도용, 공인 인증서 탈취, 악성코드 감염, 입력 값 변조, 입력 값 탈취, 피싱/파밍)을 기준으로 현존하는 국내 인터넷 뱅킹 safeguard의 필요성을 분석 및 평가하였다.

성능 평가는 복수의 safeguard가 존재하는 영역에 대해서만 수행하였고, 평가 기준으로서 관련 위협을 유발시키는 시나리오들에 대한 대응 여부, 다중 운영체제 및 다중 웹브라우저 지원 여부를 사용하였으며, 사용자가 가지는 간극과 그 원인을 분석하기 위한 방법으로서 설문조사 기법을 이용하였다.

우선 safeguard의 중복 영영과 부재 영역은 각각 4개, 2개가 존재하는 것으로 드러났다. 중복 영역은 계정 도용의 P 영역과 D 영역, 입력 값 탈취의 P 영역, 피싱/파밍의 P 영역이었으며, 부재 영역은 공인 인증서 탈취의 D 영역, 피싱/파밍의 D 영역이었다.

인터넷 뱅킹 위협별로 safeguard 현황을 살펴볼 경우 계정 도용의 경우 P 영역에 패스워드 인증, 보안카드 인증, OTP 인증, 공인 인증서 인증, 그래픽 인증, SMS 인증, ARS 인증, 단말기 인증이 존재했고, D 영역에는 예외 PC 로그인 알림, 해외 IP 접속 차단이, R 영역에는 SMS 알림이 존재했다. 공인 인증서 탈취의 경우 P 영역에 HSM, R 영역에 SMS 알림이 존재했으며 D 영역에는 존재하지 않았다. 악성코드 감염의 경우 P, D 영역에 공통적으로 개인 방화벽, R 영역에 안티 바이러스 프로그램이 존재했으며, 입력 값 변조의 경우 P 영역에 시큐어 브라우저, D 영역에 거래연동 OTP와 입금계좌지정 서비스, R 영역에 SMS 알림이 존재했다. 입력 값 탈취의 경우엔 P 영역에 키보드 보안 프로그램, 가상 키보드, 그래픽 인증, D 영역에 개인 방화벽, R 영역에 SMS 알림이 존재했다. 마지막으로 피싱/파밍의 경우 P 영역에 피싱 방지 프로그램, 개인 URL, 개인 이미지, EV SSL, R 영역에 SMS 알림이 존재했고, D 영역에는 존재하지 않았다.

인터넷 뱅킹 위협 간 연관 관계의 경우 시발점이 되는 위협은 악성코드 감염이었다. 악성코드 감염으로 인해 공인 인증서 탈취, 입력 값 변조, 입력 값 탈취, 피싱/파밍 등의 추가 위협에 사용자의 단말기가 영향을 받게 되고, 이 추가 위협들이 유효할 경우 궁극적으로 계정 도용의 위협에 노출되는 것으로 드러났다.

5개의 중복 영역에 대한 분석의 경우 우선 계정 도용의 P 영역은 총 3가지의 경우의 수가 존재했다. 첫 번째는 단말기 인증, 패스워드 인증, 공인 인증서 인증과의 결합, 두 번째는 단말기 인증, HSM에 저장된 공인 인증서 인증, 거래연동 OTP와의 결합, 세 번째는 HSM에 저장되지 않은 공인 인증서 인증, 보안카드 인증 그리고 그래픽 인증, SMS 인증, ARS 인증 중에서의 택일 결합이다. 현실적으로 두 번째 대안이 가장 안전하지만 비용과 사용성을 고려하고 다양한 선택권을 보장해야하므로 가장 안전한 특정 safeguard의 조합으로 인증하는 것보다는 사용자가 보유하거나 선택한 safeguard의 종류와 사용자의 요청(로그인, 잔액 조회, 계좌 이체 등)의 위험 정도에 따라 다양한 인증 정책을 운용하는 것이 효율적이라 판단되었다. 계정 도용의 D 영역은 단말기 인증을 사용할 경우 예외 PC 로그인 알림이 해외 IP 접속 차단 기능을 포함하므로 예외 PC 로그인 알림 기능만 필요함을 알 수 있었다. 그리고 입력 값 변조의 D 영역의 경우 현재는 입금계좌지정 서비스가 필요하나 훗날 거래연동 OTP가 도입될 경우 대체될 것으로 판단되었다. 입력 값 탈취의 P 영역의 경우 키보드 보안 프로그램은 입력의 편의성으로 인해, 가상 키보드는 다중 운영체제 및 다중 웹 브라우저 지원으로 인해 각각 필요하다고 판단되었지만 그래픽 인

증은 가상 키보드를 대체할만한 고유의 장점이 존재하지 않았다. 마지막으로 피싱/파망의 P 영역은 2가지의 경우의 수가 존재했다. 첫 번째로 개인 URL과 개인 이미지의 결합, 두 번째는 EV SSL이다. 2가지 경우 모두 우회 가능성이 존재하지만 실현 가능성이 현실적으로 매우 낮으므로 사용자의 선호도 분석에 따라 둘 중 택일이 필요하다고 판단되었다. 본 논문에서 수행된 설문에서는 전체 중 67%의 응답자가 EV SSL을 선호하는 것으로 나타났다.

결론적으로 계정 도용 및 입력 값 탈취의 P 영역의 그래픽 인증, 피싱/파밍 P 영역의 피싱 방지 프로그램을 제외하고 모두 필수적으로 필요하다고 판단되었다. 하지만 설문 결과 사용자들은 인터넷 뱅킹 위협 및 관련 safeguard 현황을 제대로 알고 있지 못 했고 그에 따라 각 safeguard의 필요성 역시 제대로 판단하기 어려워했다. 아울러 인터넷 뱅킹 위협 및 관련 safeguard에 대한 금융회사의 자세한 안내가 부족하다고 응답했다. 그래서 이에 대한 대응방안으로서 세 가지를 제시했다. 첫 번째는 인터넷 뱅킹 위협 및 safeguard에 대한 구체적인 안내로서 Bank of America와 대구은행의 사례를 분석하였다. 두 번째는 사용자의 눈높이에 맞춘 안내로서 네이버의 개인정보 취급방침 Easy 버전 및 인포그래픽 버전과 영국의 응급실 내 폭력 감소를 위한 디자인 관점에서의 개선 프로젝트를 분석했다. 해당 사례들 모두 엄밀히 인터넷 뱅킹과 분야가 일치하지는 않지만 “사용자 눈높이에서의 고려”라는 시발점이 동일하기 때문에 좋은 지침이 될 수 있다. 세 번째는 safeguard에 대한 사용자의 최종적 선택권 제고로서 BNP Paribas Global Market 사례를 분석하였다.

기존 연구의 한계는 현존하는 인터넷 뱅킹 위협이 무엇이고 각각에 대한 대응방안이 무엇인지 논해졌으나 Prevention, Detection, Response 등 정보보호 라이프 사이클 상에서 각각의 위협에 대처할 수 있는 safeguard가 구체적으로 무엇인지 분명하게 다뤄지지 않았다.

본 논문의 기여도는 인터넷 뱅킹 위협에 대응하는 여러 가지의 safeguard를 분석 및 평가함에 있어서 Prevention, Detection, Response 등의 정보보호 라이프 사이클 관점에서 바라본 최초의 시도였다는 점이며, 이를 통해 safeguard의 중복 영역과 부재 영역을 식별하였고 중복 영역의 경우 성능 평가를 통해 각각의 필요성을 분석하였다. 그리고 사용자에 대한 설문 조사를 통해 우리가 분석한 결과와 사용자가 가지고 있는 생각과의 간극을 측정하고 이 간극을 좁히기 위한 대안을 제시하였다.

아직 전체 은행 업무 중 제한적인 범위 내에서만 활용되고 있긴 하지만 신한은행의 정맥 인증[101], 기업은행의 홍채 인증[102], KEB하나은행의 지문 인증[103] 등 생체 인증이 점점 도입되고 있고, 비밀번호를 입력해야 IC 칩이 활성화되는 오프라인 부정 결제 방지를 위한 Chip Guard Display 카드[104], 스마트폰 앱을 통해 인터넷뱅킹, 스마트뱅킹, 텔레뱅킹, ATM 활성 유무를 설정하는 우리은행의 원터치 리모콘[105], 여기에 현금서비스 활성 유무 및 1회 사용금액과 1일 사용금액 설정, 가상카드번호 생성 기능까지 추가된 현대카드의 Lock & Limit 및 가상카드번호 서비스[106] 등 핀테크 활성화에 발맞춰 다양한 safeguard가 등장함에 따라 온/오프라인을 아우르는 관점에서 본 연구는 앞으로도 지속적으로 수행되어야 할 것으로 판단된다. 아울러 인터넷 뱅킹 safeguard의 성능 평가를 위한 기준 수립에 관한 연구 및 전자금융거래 시 safeguard를 위해 사용자가 얼마까지 지출할 용의가 있는지를 가리키는 즉, safeguard의 WTP에 대한 연구도 반드시 필요할 것으로 판단된다.

References

[1] C. A. Kim, *Change of the export regulation policy of the cryptographic product in United States*, Information Society Development, Vol. 224, No. 11-1, pp. 44-47, Jan. 1999.

[2] SEED, https://seed.kisa.or.kr/iwt/ko/sup/EgovSeedInfo.do, Sep. 2015.

[3] Korea Internet & Security Agency, *Internet 30th anniversary*, 2012 Korea Internet White Paper, Oct. 2014.

[4] J. K. Yoo, and S. J. Min, *Application of security technology for Internet banking compatibility*, Payment and Information Technology, Vol. 41, pp. 59-84, Jul. 2010.

[5] Joint ministries concerned, *Countermeasure for simplifying payment in e-commerce*, Jul. 2014.

[6] Financial Services Commission, *Action plan in 2015*, Jan. 2015.

[7] National Assembly, *Partial revision of Electronic Financial Transaction Act*, Jul. 2014.

[8] Financial Services Commission, *Notification 2015-3rd*, Feb. 2015.

[9] Financial Services Commission, *Notification 2015-7th*, Mar. 2015.

[10] Ministry of Science, *ICT and future planning, Countermeasure for improving use of ActiveX in private*, Apr. 2015.

[11] Microsoft, MBrowser: Microsoft Edge and Internet Explorer 11, https://technet.microsoft.com/en-us/library/mt156988(v=vs.85).aspx, Jan. 2015.

[12] The Final Countdown for NPAPI, http://blog.chromium.org/2014/11/the-final-countdown-for-npapi.html, Nov. 2014.

[13] Danish Bankers Association, http://www.finansraadet.dk/en/Facts-and-figures/Pages/Statistics-and-figures/Online-bank-hackings-–-Statistics.aspx, Sep. 2015.

[14] Telecommunication Financial Fraud Prevention Council, *Comprehensive countermeasure for preventing telecommunication financial fraud*, Dec. 2013.

[15] Safe internetbanking.be, https://www.safeinternetbanking.be/en/figures/cases-fraud, Sep. 2015.

[16] Dutch Basnking Association, http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html, Sep. 2015.

[17] Financial Fraud Auctoin UK, *Fraud the facts 2015*, 2015.

[18] Bruce Schneier, *The process of security*, Apr. 2000.

[19] James LaPiedra, *The information security process - prevention, Detection and response*, 2001.

[20] CBSS, *A Resource guide for BANK EXECUTIVES*, 2014.

[21] S-J. Lee, S-Y. Hwang, K-K. Kim, and S-K. Ryeo, *Internet banking service vulnerability analysis and security solution*, Journal of information and security, Vol. 7, No. 2, pp. 119-128, Jun. 2007.

[22] S. Y. Kim, *E-banking fraud's type and countermeasure*, Payment and Information Technology, Vol. 38, pp. 34-62, Oct. 2009.

[23] Telecommunications Technology Association, *Analysis and management of e-commerce service's threat*, Dec. 2011.

[24] S. M. Lee, and J. M. Seung, *Current status of e-commerce and classification of security threat in domestic*, Review of

The Korea Institute of Information Security & Cryptology, Vol. 21, No. 7, pp. 53-61, Nov. 2011.

[25] L. Peotta, M. D. Holtz, B. M. David, F. G. Deus, Rafael, and T. Sousa Jr., *A formal classification of internet banking attacks and vulnerabilities*, International Journal of Computer Science & Information Technology, Vol. 3, No. 1, pp. 186-197, Feb. 2011.

[26] Ministry of Science, ICT and Future Planning, We intend to increase information security industry in earnest as creative economy's blue ocean, http://www.msip.go.kr/web/msipContents/contents.do?mId=NzM=, Jun. 2015.

[27] Telecommunications Technology Association, http://www.tta.or.kr/index.jsp, Oct. 2015.

[28] The Tolly Group, http://www.tolly.com/Default.aspx, Oct. 2015.

[29] National Software Testing Laboratories, http://www.intertek.com/it/, Oct. 2015.

[30] ICSA Labs, https://www.icsalabs.com/, Oct. 2015.

[31] NSS Labs, https://www.nsslabs.com/, Oct. 2015.

[32] RFC 2544 - Benchmarking Methodology for Network Interconnect Devices, https://www.ietf.org/rfc/rfc2544.txt, Oct. 2015.

[33] RFC 3511 - Benchmarking Methodology for Firewall Performance, https://tools.ietf.org/html/rfc3511, Oct. 2015.

[34] Performance Measurement Methodologies for Network Security Devices(TTAS_KO-12_0044), http://www.tta.or.kr/data/weeklyNoticeView.jsp?pk_num=1876&nowSu=211&search=&data=&totalSu=1&ag_code=0000100004, Oct. 2015.

[35] H. S. Kim, J. H. Huh, and R. Anderson, *On the security of internet banking in South Korea*, Computing Science Group, Mar. 2010.

[36] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, *Usable security: User preferences for authentication methods in eBanking and the effects of experience*, Interacting with Computers, Vol. 22, No. 3, pp. 153-164, May. 2010.

[37] Genise, and Pauline, *Usability evaluation: methods and techniques: Version 2.0*, Aug. 2007.

[38] KB Kookmin Bank's Secrutiy Center, https://obank.kbstar.com/quics?page=osecure, Nov. 2015.

[39] Standard Chartered Bank's security program installation, https://open.standardchartered.co.kr/service/programInstall?P_name=IPInside&url=https%3A%2F%2Fopen.standardchartered.co.kr%2Flogin%2Findex%3FredirectURL%3D%2Fservice%2FH93301%3Fmenuid%3DOIB08060500000000, Nov. 2015.

[40] Shinhan Bank's Security Center, http://cs.shinhan.com/cs_index.jsp, Nov. 2015.

[41] KEB Bank's Security Center, http://www.keb.co.kr/, Nov. 2015.

[42] Woori Bank's Security Center, https://spot.wooribank.com/pot/Dream?withyou=CQSCT0001, Nov. 2015.

[43] Hana Bank's Security Center, http://www.hanabank.com/nhana/smartbk/smartbk06/smartbk061/CaCus000201/index.jsp, Nov. 2015.

[44] Citibank's Security Center, http://www.citibank.co.kr/, Nov. 2015.

[45] Kyongnam Bank's Security Center, http://www.knbank.co.kr/knbweb/knbweb.js

p?w2xPath=/xml/cust/security/SCN-HO-340 10100.xml, Nov. 2015.

[46] Kwangju Bank's Security Center, http://www.kjbank.com/banking/index.jsp, Nov. 2015.

[47] Daegu Bank's Security Service, https://www.dgb.co.kr/com_ebz_hlp_main.act, Nov. 2015.

[48] Busan Bank's Security Service, https://www.busanbank.co.kr/ib20/mnu/BHPCSC352000001, Nov. 2015.

[49] JB Bank's Security Center, https://www.jbbank.co.kr/, Nov. 2015.

[50] Jeju Bank's Security Center, https://www.e-jejubank.com/JeJuBankInfo.do, Nov. 2015.

[51] Industrial Bank of Korea's Security Center, http://www.ibk.co.kr/common/navigation.ibk?linkUrl=/financetech/efinance/safe/safe_main.jsp&pageId=SC00000000, Nov. 2015.

[52] NH Bank's Security Center, https://banking.nonghyup.com/so/jsp/initech/sandbox/index.jsp, Nov. 2015.

[53] Suhyup Bank's Security Service, https://www.suhyup-bank.com/, Nov. 2015.

[54] National Forestry Cooperatives Federation's Banking Security Center, http://banking.nfcf.or.kr/index.jsp, Nov. 2015.

[55] MG Community Credit Cooperatives' PC Security Service, http://www.nprotect.co.kr/service/kfcc/, Nov. 2015.

[56] National Credit Union Federation of Korea's Additional Service, https://openbank.cu.co.kr/, Nov. 2015.

[57] KoreaPostBank, http://www.epostbank.go.kr/, Nov. 2015.

[58] AhnLab Online Security 2.0, http://www.ahnlab.com/kr/site/product/productView.do?prodSeq=34, Nov. 2015.

[59] nProtect Netizen v5.5, http://www.nprotect.com/index.html, Nov. 2015.

[60] Raonsecure USIM Smart Authorization, http://www.usimcert.com/, Nov. 2015.

[61] Wizvera Safehard, https://www.safehard.co.kr/, Nov. 2015.

[62] Mirageworks' public certification protection technology based Sandbox, http://www.mirageworks.co.kr/Solutions/Certlocker.aspx, Nov. 2015.

[63] FlyHigh's public certification storage technology based CPU, https://www.facebook.com/myflyhigh/, Nov. 2015.

[64] OPEN WEB nFilter of NSHC, http://www.nshc.net/wp/portfolio-item/open-web-nfilter/, Nov. 2015.

[65] GOTP of DigitalZone, http://www.doculink.co.kr/service_03_GOTP.html, Nov. 2015.

[66] Dementor Web of Dementor, http://www.dementor.co.kr/, Nov. 2015.

[67] TouchEn key of Raonsecure, http://touchen.raonsecure.com/pc/pc_01.php, Nov. 2015.

[68] SecureKeyStroke of SoftCamp, http://www.softcamp.co.kr/sub/sub_2_7.php, Nov. 2015.

[69] NaRu of Wizvera, http://www.wizvera.com/naru.html, Nov. 2015.

[70] INISAFE Sandbox of INITECH, http://www.initech.com/www/html/inisafe/goMenu3_19_1.html, Nov. 2015.

[71] iFDS of INTEREZEN, http://www.interezen.co.kr/izh6/1_product/p_ipinside_ifds.jsp, Nov. 2015.

[72] nProtect SecuLogMaster of INCA Internet, http://www.nprotect.com/index.html, Nov. 2015.

[73] Real IP of KTB Solution,

http://www.ktbsol.co.kr/, Nov. 2015.

[74] Microsoft Cryptographic Service Providers, https://msdn.microsoft.com/ko-kr/library/windows/desktop/aa386983(v=vs.85).aspx, Jan. 2016.

[75] RSA Laboratories, PKCS #11: Cryptographic Token Interface Standard, http://germany.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm, Jan. 2016.

[76] PC/SC Workgroup, PC/SC Workgroup Specifications Overview, http://www.pcscworkgroup.com/specifications/overview.php, Jan. 2016.

[77] I. S. Kim, The time is for Transaction Singing OTP in July, http://www.etnews.com/20160125000271, Jan. 2016.

[78] GReAT, Use the force Luuuk, https://securelist.com/blog/incidents/63704/use-the-force-luuuk/, Jun. 2014.

[79] D. Venkatesan, Android.Bankosy: All ears on voice call-based 2FA, http://www.symantec.com/connect/blogs/androidbankosy-all-ears-voice-call-based-2fa, Jan. 2016.

[80] McAfee, *McAfee Labs Threat Advisory - PWS-Zbot*, Jun. 2014.

[81] Y. C. Lee, Virtual keyboard is bypassed RCS in 31 of 35 financial corporations, http://www.thescoop.co.kr/news/articleView.html?idxno=17500, Sep. 2015.

[82] S. H. Kwon, The attacker stole 26 million won from victim's account by applying call forwarding, http://www.yonhapnews.co.kr/bulletin/2015/02/23/0200000000AKR20150223017751060.HTML, Feb. 2015.

[83] E. S. Kang, SMS authorization code is abused in smishing, http://www.dt.co.kr/contents.html?article_no=2014030302010660800002, Mar, 2014.

[84] D. W. Kim, Bank's public certification must be stored in HSM, http://www.edaily.co.kr/news/NewsRead.edy?SCD=JA21&newsid=03112726609404344&DCD=A00102&OutLnkChk=Y, Jun. 2015.

[85] Y. G. Jung, *Recent trend and improvement of OTP authorization technology*, Payment and Information Technology, Vol. 61, pp. 30-69, Jul. 2015.

[86] A. Rosenan, and Z. Gutterman, *Protecting our keystrokes*, THE ISSA(Information Systems Security Association) JOURNAL, Apr. 2006.

[87] M. Seese, *Beating a keystroke logger on a public PC*, THE ISSA(Information Systems Security Association) JOURNAL, Mar. 2008.

[88] AhnLab, *White paper - AhnLab online security white paper ver. 1.0.1*, Nov. 2008.

[89] M. K. Gil, The finishing up of pharming technique for stealing financial information, http://www.dailysecu.com/news_view.php?article_id=8530, Jan. 2015.

[90] Comodo SSL, Kind and price of SSL Certification, https://www.comodossl.co.kr/products/ssl-certificate.aspx, Jan. 2016.

[91] FIDO Alliance, https://fidoalliance.org/, Jan. 2016.

[92] J. W. Lee, Combination public certification based PKI and biometric, http://www.dt.co.kr/contents.html?article_no=2015120702101560813001, Dec. 2015

[93] Financial Services Commission, *Regular press conference related financial reform*,

Dec. 2015.

[94] G. Lindsey, and G. Knaap, *Willingness to pay for urban greenway projects*, Journal of the American Planning Association, Vol. 65, No. 3, pp. 297-313, 1999.

[95] Bank of America, Online Banking Security from Bank of America, https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/online-banking-security.go, Feb. 2016.

[96] NAVER, Easy version of privacy policy, https://nid.naver.com/user2/privacycenter/info.nhn?m=viewTermOfUseSimple, Feb. 2016.

[97] NAVER, Infographic of privacy policy, https://nid.naver.com/user2/privacycenter/info.nhn?m=viewInfoGraphic, Feb. 2016.

[98] Frontier Economics, *Reducing violence and aggression in A&E: Through a better experience*, Nov. 2013.

[99] BNP PARIBAS Global Markets, https://ssoforms.bnpparibas.com/cib/LoginForm.aspx?TYPE=33554433&REALMOID=06-bbc8c69d-304f-1129-9ca2-839478260cb3&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=-SM-%2fpWHFX9njSKqw5b3ctc1hKiUwG%2bnmkBAvBQCyXpA2NKWJYgu3oEphfu5KWXqIAC1&TARGET=-SM-https%3a%2f%2fglobalmarkets%2ebnpparibas%2ecom%2fgmportal%2fprivate%2fhome, Feb. 2016.

[100] Markit Hub, https://www.hub.com/hub/?loginfailed=true, Feb. 2016.

[101] Shinhan Bank's Digital Kiosk, http://mbank.shinhan.com/pages/financialInfo/electronic_finance/Digital_Kiosk.jsp, Mar. 2016.

[102] Industrial Bank of Korea's Security Center Weekly Hot News, http://blog.ibk.co.kr/1827, Mar. 2016.

[103] Introduction to Institution of Smart OTP and Fingerprint Authorization Service, https://open.hanabank.com/contents/customer/news/1416933_93638.jsp?Ctype=B&cid=OpenB_main_Center&oid=1416933, Jun. 2016.

[104] Chip Guard OTP Display Card, http://www.surepassid.com/why-we-are-unique/multi-factor-authentication-mfa/otp-display-cards/, Mar. 2016.

[105] Woori Bank's one touch remote control, https://spib.wooribank.com/pib/Dream?withyou=PSBKM0147, Mar. 2016.

[106] Digital Hyundai Card, https://www.hyundaicard.com/cpl/en/CPLEN0501_01.hc, Mar. 2016.

PDR Matrix 관점에서의 국내 인터넷 뱅킹 Safeguard 필요성 분석 및 평가

허건일[1], 박창민[2], 김휘강[1]

[1] *고려대학교 정보보호대학원*

[2] *웹케시 정보보호센터*

요 약

인터넷 뱅킹 safeguard에 대한 자세한 안내 부족 및 강제적 사용으로 인해 사용자 불만이 나날이 높아져 가고 있다. 하지만 이러한 불만을 감수함에도 불구하고 대규모 전자금융사고가 끊임없이 발생함에 따라 safeguard 무용론에 대한 주장이 계속 제기되고 있다. 하지만 이것은 ActiveX로 인해 발생되는 불편함을 safeguard 사용에 관한 문제에 결부시킨 매우 잘못된 상황이다. 불편해서 불필요하다는 식이 아닌 각각의 인터넷 뱅킹 safeguard의 객관적인 성능과 상호간의 관계에 근거하여 그것의 필요성을 판단해야 한다. 이에 따라 본 논문에서는 PDR matrix 즉, Prevention, Detection, Response로 구분한 정보보호 라이프 사이클과 6개의 인터넷 뱅킹 위협(계정 도용, 공인 인증서 탈취, 악성코드 감염, 입력 값 변조, 입력 값 탈취, 피

싱/파밍)을 기준으로 현존하는 국내 인터넷 뱅킹 safeguard의 필요성을 분석 및 평가하였다. 이를 통해 4개의 중복 영역과 2개의 부재 영역을 식별하였고 중복 영역의 경우 관련 성능 평가를 통해 각각의 필요성을 분석한 결과 계정 도용 및 입력 값 탈취의 P 영역의 그래픽 인증, 피싱/파밍의 P 영역의 피싱 방지 프로그램을 제외한 모든 safeguard가 반드시 필요함을 알 수 있었다. 그러나 해당 결과를 바탕으로 한 사용자 설문 조사를 통해 본 연구 결과와 사용자의 생각 사이에 간극이 존재함을 알 수 있었고 이를 좁히기 위하여 인터넷 뱅킹 위협 및 safeguard에 대한 구체적인 안내, 사용자의 눈높이에 맞춘 안내, safeguard에 대한 사용자의 최종적 선택권 제고 등 세 가지의 대응방안을 제시했다.

Geon Il Heo received the bachelor's degree in the Department of Industry and Information System Engineering from Seoul National University of Science and Technology in 2012. He received the MS degree in the Department of Information Security from Korea University in 2016. From 2011 to 2012, he was a network security analyst at SK INFOSEC. He was a technical assistant in the Attached Institute of ETRI from 2013 to 2014. He has been a network security analyst at AhnLab since 2015. His current research interests include online game security, network forensic, data visualization.

E-mail address: aza837@korea.ac.kr

Chang Min Park received the bachelor's degree in the Department of Industry and Information System Engineering from Seoul National University of Science and Technology in 2013. He received the M.S. degree in the Department of Software Analysis & Design from Seoul National University of Science and Technology in 2015. He has been a security audit at Webcash since 2015. His current research interests include FinTech security, NFC security, privacy protection.

E-mail address: creative@webcash.co.kr

Huy Kang Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1998. He received the M.S. degree in Industrial & Systems Engineering from KAIST in 2000. He worked as Technical Director at NC soft from 2004 to 2010. He received the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2009. He is now an associate professor in School of Information Security at Korea University. His current research interests include Online game security, network security, network forensic, IDS, botnet detection.

E-mail address: cenda@korea.ac.kr