정 보 보 호 학 회 지
제23권 제6호, 2013. 12

전자금융거래 환경에서 보안카드 실수입력방지기법 적용을 통한 피싱/파밍 사고 방지 방안

박 진 규*, 이 정 호**

요 약

본 논문에서는 피싱, 파밍 등 전자금융 신종 사기 수법에 의한 사고 예방을 위하여, 모 시중은행의 전자금융거래 환경에서 약 3개월 동안의 자금이체 관련 로그를 기준으로 現 보안카드 인증 방식의 안전도를 분석하고, 개선할 수 있는 방안을 제안 한다. 제안 기법은 보안카드 지시번호의 배열 형식과 순서, 일부 보안카드 번호에 마스킹 적용 등을 통해 보안카드를 사용자마다 상이한 형식으로 발급하여, 사용자가 피싱 웹사이트 상 보안카드 번호 입력 화면과 본인이 가진 실물 보안카드가 크게 상이함을 스스로 인지하거나, 피싱 웹사이트 상 제시 화면에 따라 보안카드 번호의 입력 가능성을 낮추도록 하는 것이다. 이 기법은 저비용으로, 사용자의 추가 학습 노력을 최소화하면서도 사용자 부주의에 의한 보안카드 정보유출 위험을 감소시켜 전자금융거래의 안전성을 향상 시킬 수 있다.

Ⅰ. 서 론

금융거래에 있어서 비대면으로 전자적인 장치를 사용하는 전자금융거래 사용 비율은 매년 지속적으로 증가하고 있다. 특히 은행권역의 경우 2013년 3월 현재 전자금융거래가 전체 금융거래의 약 87%(거래건수 기준)를 초과하였으며, 전체 전자금융거래 중 약 45%를 PC를 이용한 인터넷뱅킹이 차지하고 있다[1].

그러나 비대면 전자적인 장치를 이용한 전자금융거래의 대중화의 부작용으로 피싱 및 파밍과 같은 신종 사이버 사기나 사용자 PC에 악성코드를 설치하여 금융정보를 유출하여 비정상 자금이체를 하는 금융사고 건수도 함께 증가하면서 사회적인 문제로 대두되고 있다[2]. 이에 따라 금융회사는 고객 주의 홍보를 강화하고, 기술적인 측면에서 자금이체를 수행하는 사용자에 대한 인증방식을 개선하거나 사용자 PC에 다양한 보안기술을 적용하는 등 사용자의 정보유출 방지와 추가 사고 예방에 노력하고 있다. 기술적인 측면에서의 구체적인 대응방법은 [표 1]과 같다.

또한, 금융감독당국도 소비자 보호를 강화하고자 전자금융거래법령과 전자금융 감독규정 개정 등을 통해 금융회사의 사용자 피해보상에 대한 법적, 금전적 책임을 확대하는 등 규제를 지속적으로 강화하고 있다[1].

그러나 전자금융사고 수법들은 갈수록 더욱 정교해짐에 반해 금융감독당국의 제도개선과 금융회사의 기술적인 대응은 현실적인 한계가 있기 때문에 전자금융거래

〔표 1〕 금융회사의 전자금융 사고 예방을 위한 주요 기술적인 대응 방법

구 분	주요 내용
(사전) 정보유출 방지	일회용비밀번호생성기(OTP) 사용 권장, 서버 인증 기법(예: 그래픽 인증) 추가 적용 등
(사후) 유출된 정보를 이용한 비정상 자금이체 방지	2채널 인증, 전자금융거래 PC 사전 지정 서비스 등

1) 부정한 방법으로 공인인증서를 만들어 사용자가 손해를 보면 금융기관이 책임을 져야 한다는 내용 등 해킹사고로 인한 이용자 피해에 대해 금융회사의 배상책임을 강화하는 전자금융거래법 개정안이 국회 본회의를 통과(2013.4.30)하고 2013.11월에 시행

* 우리은행 IT컴플라이언스부(jjpark@wooribank.com)
** 신한은행 정보보안실(guardian@shinhan.com)

사고의 최초 시발점인 사용자가 보유한 접근매체가 처음부터 유출되지 않도록 하는 방안이 더욱 중요해졌다.

이에 본 논문에서는 피싱, 파밍 등 전자금융 신종 사기 수법에 의한 사고 예방을 위하여, 모 시중은행의 전자금융거래 환경에서 약 3개월 동안의 자금이체 관련 로그를 기준으로 現 보안카드 인증 방식의 안전도를 분석하고, 보안카드 인증 방식을 개선할 수 있는 방안을 제안 한다. 단, 조사 대상기간에 해당하는 로그는 개인 사용자의 인터넷뱅킹서비스 이용에 따른 로그로 국한한다. 제안 기법은 보안카드 지시번호의 배열 형식과 순서, 일부 보안카드 번호에 마스킹 적용 등을 통해 보안카드를 사용자마다 상이한 형식으로 발급하여, 사용자가 피싱 웹사이트 상 보안카드 번호 입력 화면과 본인이 가진 실물 보안카드가 크게 상이함을 스스로 인지하거나, 피싱 웹사이트 상 제시 화면에 따라 보안카드 번호의 입력 가능성을 낮추도록 하는 것이다. 이 기법은 저비용으로, 사용자의 추가 학습 노력을 최소화하면서도 사용자 부주의에 의한 보안카드 정보유출 위험을 감소시켜 전자금융거래의 안전성을 향상 시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 현 시점의 전자금융거래 주요 인증수단 및 한계점에 대해 알아보고, 3장에서는 전자금융거래 자금 이체 시 인증 수단으로서 가장 많이 사용되는 보안카드의 안전도를 확인한다. 4장에서는 보안카드 인증 개선 방안을 제시하고, 5장에서는 제안 기법의 실효성을 확인한 후, 6장에서 마무리하고자 한다.

Ⅱ. 전자금융거래 주요 인증수단 및 한계점

전자금융거래[2]를 이용하는 사용자는 사전에 거래 금융회사를 방문하여 등록절차를 통해 비밀번호, 공인인증서 외에 추가로 보안카드 또는 일회용비밀번호생성기(OTP)를 발급받는다. 그리고 2013년 9월부터 전자금융사기 예방서비스 의무화 전면시행에 따라 1일 누적 기준 300만원 이상의 자금이체와 같이 주요한 거래의 경우에는 사전 등록된 PC를 사용하거나, 유/무선 전화를 활용한 사용자 인증 등 2채널 인증 수단을 추가하여 함께 사용하는 것이 의무화 적용되었다.[2]. 전자금융거래 시 사용할 수 있는 주요 사용자 인증 수단[3]은 [표 2]와 같다.

2) 본 논문에서 전자금융거래는 개인 사용자의 인터넷뱅킹에 한하여 설명함

〔표 2〕 전자금융거래에 이용되는 주요 인증 수단

구 분		설 명	비 고
비밀번호		로그인 비밀번호, 계좌 비밀번호, 이체 비밀번호 등	악성코드 또는 사용자 부주의에 의해 정보유출 가능
공인인증서		공인인증서 파일, 비밀번호	상동
일회용 비밀번호	보안카드	30~35개의 숫자로 구성	상동
	일회용비밀번호생성기	1회용 난수 6~8자리	유출 위험이 낮으나, 보안카드 대비 보급률이 낮음
2채널 인증		유/무선 전화를 통한 사용자 인증 등	전자금융사기 예방서비스 도입에 따라, 2013.9월에 의무화 적용

최근 금융감독당국과 경찰청 보도자료에 따르면, 전자금융거래의 보편화 및 사용량 증가와 함께, 이와 관련된 정보유출에 따른 사용자의 금전적 손실을 동반하는 금융사고도 증가하고 있다[3].

모 시중은행의 전자금융거래[4]에 가입한 약 1,190만명의 사용자 중 최근 3개월(2013.3~5월) 동안 전자금융거래를 위하여 1회 이상 접속한 실사용자 약 414만명을 대상으로 조사한 결과, 전용 일회용비밀번호생성기(OTP)를 사용하는 사용자는 약 10.7%를 차지하고, 일반 보안카드를 사용하는 사용자는 약 89.3%인 약 370만명을 차지한다. 자세한 내용은 [표 3]과 같다.

〔표 3〕 보안카드 및 일회용비밀번호생성기 보유 비율

구 분	사용자 수(명)	사용자 비율(%)
보안카드	3,697,189	89.33
일회용비밀번호 생성기	441,441	10.67
합 계	4,138,630	100

3) 전자금융거래법상에는 접근매체로 정의됨

4) 모 시중은행의 2013년 3월말 현재 개인 인터넷뱅킹 서비스 등록 사용자수는 약 1,190만명으로서 한국은행의 『2013년도 1/4분기 국내 인터넷뱅킹 서비스 이용 현황』에 따른 2013년 3월말 현재 인터넷뱅킹용 공인인증서(은행・신용카드・보험용, 범용) 건수 2,532만개 대비 약 47% 의 가입자 비율을 보유하고 있다. (한국은행 발표자료에서 동일 사용자에 대한 공인인증서 중복 발급 포함 시 모 은행의 가입자 비율은 더 증가됨)

본 논문에서는 전체 전자금융거래를 이용하는 사용자 대부분이 보유하고, 최근 발생한 금융사고의 핵심 공격 대상인 보안카드에 대해 피싱 및 파밍 공격에 한하여 설명하고자 한다.

일반적인 피싱 및 파밍과 같은 사이버 사기수법에 당하여 피싱 웹사이트에 접속한 사용자는 <그림 1>과 같이 보안카드 번호 입력을 요구받게 되고, 피의자는 입력된 보안카드 번호를 악용하여 비정상 자금이체를 수행한다. 이와 같은 전자금융사고는 일반적으로 일회용비밀번호생성기보다는 보안카드를 이용하는 사용자를 대상으로 하며, 사용자가 자신의 주요정보에 대한 유출 여부를 정확히 인지하지 못한 상태에서 스스로, 직접 유출하는 특성을 가지고 있다.

〈그림 1〉 피싱 웹사이트에서 보안카드 번호 등 주요정보 입력을 요구하는 화면

이처럼 피싱 웹사이트를 통해 보안카드 번호 등 주요정보가 유출되는 사고는 사회공학적인 공격으로 사용자의 부주의를 노린 방법이기에, 금융회사가 제공하는 보안 프로그램이나 기술적인 인증수단을 추가하는 방식으로 주요 정보의 유출을 사전에 막는 것은 한계가 있다. 다시 말하면, 현재 도입되어 운영되는 피싱 및 파밍 대응방안은 사용자의 편리성을 저해하면서 자발적인 학습을 지속적으로 요구하거나, 금융회사로 하여금 많은 추가 비용을 투자하게 했지만 실효성은 높지 않았다.[5] 그리고 2013년 9월에 의무화 이행된 전자금융 사기예방 서비스 또한 악성코드에 의해 유출 가능한 사용자 PC, 스마트폰 등 단말의 정보를 사용자 인증에 사용[6]한다는 측면에서 기술적인 한계가 있고, 2채널 인증도 주요 거래 시에만 적용되는 사후 통제이므로 사용자의 부주의에 의한 주요 정보 유출을 사전에 근본적으로 차단하는 것은 불가능하다.

Ⅲ. 現 보안카드 인증의 안전도 분석

전자금융거래에서 사용되는 일반적인 보안카드는 <그림 2>에서 보이는 바와 같이 단면에 4자리수의 30개(또는 35개)의 지시번호 별 4자리의 난수가 기재되고, 보안카드의 유일성을 보장하는 8자리(또는 10자리)의 일련번호가 있다. 다만, 본 논문에서 분석 자료로 사용한 보안카드는 30개의 지시번호를 가진다.

〈그림 2〉 모 시중은행 보안카드의 예

사용자의 계좌에서 비정상 자금이체 거래가 발생할 경우, 접근매체의 유출 경로에 따라 사용자와 금융회사의 관련 책임 및 보상이 결정된다. 그러므로 사용자가 스스로 주요 정보(접근매체)의 분실이나 피싱, 파밍에 의한 유출 등 과실을 인정하지 않을 경우, 금융회사에서는 정확한 사고 원인 파악 및 추가 사고 예방, 고객의 다른 과실 가능성 등을 고려하여, 먼저 사용자 단말 환경에서 신종 악성코드[7]에 의한 비밀번호와 보안카드

5) 금융감독원에서 2013년 7월 2일 보도한 『피싱(Phishing)사기에 의한 피해유형 분석 및 금융거래 시 유의사항』에 따르면, 2013.1월에서 5월 중에만 1,756건, 174억원의 피해가 경찰청에 신고, 집계될 정도로 다수가 발생하였음. 특히, 2012.10월~2013.5월 기간 중 발생한 11,439건의 피싱 사기로 인한 소비자의 피해 현황 및 사기의 유형 및 수법 분석 결과, 피싱 사기의 주요 경로는 피싱사이트와 파밍이 각각 31.4%(3,586건), 21.5%(2,463건)을 차지하여 보이스피싱(피해자의 창구, ATM기 유도 등)에 의한 피해 47.1%(5,390건)보다 더 높은 비중을 차지하고 있으며, 최근 들어 더욱 증가 추세에 있음

6) 뱅킹 PC 사전 지정 서비스

번호의 유출 가능성을 확인해야 한다.

보안카드 보유자의 경우, 금융회사에서 정상적인 전자금융 거래 중 악성코드와 관련된 주요정보 유출을 통한 비정상 자금 이체거래 여부를 확인하는 방법은 다음과 같다. 먼저 해당 사용자의 비정상 자금이체 발생 당시 및 그 이전 거래에서 사용된 PC 접속 주소, 보안카드 지시번호, 보안카드 일련번호 사용 내역 등을 확인하여 비정상 자금이체의 원인을 분석한다. 만약 비정상 자금이체 시점에 사용된 보안카드 지시번호가 과거의 거래[8]에서 한 번도 사용된 적이 없다면, 해당 보안카드 번호는 정상적인 전자금융 거래 중 사용자가 입력한 적이 없어 사용자 환경의 악성코드에 의한 유출 또한 기술적으로 불가능하므로 사용자의 보안카드 관리 부주의나 피싱, 파밍 등에 의한 사용자의 직접 입력으로 유출되었을 가능성이 매우 높다[9].

따라서 비정상 자금 이체 발생 시 사용된 보안카드 지시번호의 그전 거래에서 중복 사용 여부를 기준으로, 정상 거래 중 사용자 환경의 신종 악성코드와 관련된 사고 가능성 여부를 우선적으로 확인할 수 있다.

3.1 보안카드 사용 현황 및 안전도 분석

조사 대상기간 동안, 보안카드를 주요 거래 인증에 사용한 횟수 별 사용자 비율은 [표 4]와 같다. 참고로 개인 인터넷뱅킹 실사용자 3,697,189명([표 3] 참조) 중 조사 대상 기간 동안 보안카드를 1회 이상 이용한 사용자는 46.48%인 1,718,537명이다.

[표 4]에서 보는 바와 같이, 보안카드 지시번호 개수(30개 기준)보다 많은, 31회 이상 보안카드 사용 거래를 수행한 경우는 전체 거래의 38.82%에 해당하고, 해당 사용자는 135,848명으로 전체 사용자의 7.92%를 차지한다.

보안카드 인증 거래 반복에 따라 보안카드 지시번호가 중복 사용될 가능성의 경우, 보안카드 지시번호의 수가 S개이고, N번 정상 거래 후 다음 거래(N+1번째)에서 앞서 한 번이라도 사용된 보안카드 지시 번호가 다시 요구될 확률(P)은 다음과 같다.

$$P = \sum_{n=1}^{N} [(1-\frac{1}{S})^{n-1} \times \frac{1}{S}] \ , \qquad (N >= 1)$$

이를 보안카드 이용 빈도별 사용자 비율([표 4] 참조)에 가중하여 적용한 결과는 [표 5]와 같다. 참고로, 현행 인터넷뱅킹에서 보안카드가 사용되는 방식은 2개의 임의의 지시번호에 따라 4자리 보안카드 번호를 앞/뒤 2자리씩 분할하여 입력을 요하므로, 앞에서 설명한 확률은 반복확률($P \times P$)로 계산한다.

[표 5]에서 보이는 바와 같이, 보안카드는 사용 가능

〔표 4〕 보안카드 이용 빈도 별 사용자 비율

보안카드 이용 거래			사용자		
회수	비율	비율 (누적)	명	비율	비율 (누적)
1	1.32%	1.32%	264,476	15.39%	15.39%
2	1.89%	3.21%	190,201	11.07%	26.46%
3	2.26%	5.47%	151,370	8.81%	35.27%
4	2.43%	7.90%	122,255	7.11%	42.38%
5	2.47%	10.37%	99,173	5.77%	48.15%
6	2.49%	12.85%	83,311	4.85%	53.00%
7	2.46%	15.32%	70,776	4.12%	57.12%
8	2.47%	17.79%	62,123	3.61%	60.73%
9	2.44%	20.23%	54,528	3.17%	63.90%
10	2.46%	22.69%	49,450	2.88%	66.78%
11	2.42%	25.11%	44,234	2.57%	69.36%
12	2.40%	27.51%	40,271	2.34%	71.70%
13	2.39%	29.91%	37,022	2.15%	73.85%
14	2.34%	32.24%	33,537	1.95%	75.80%
15	2.30%	34.54%	30,784	1.79%	77.60%
16	2.23%	36.77%	27,960	1.63%	79.22%
17	2.19%	38.95%	25,849	1.50%	80.73%
18	2.14%	41.09%	23,849	1.39%	82.11%
19	2.06%	43.15%	21,842	1.27%	83.39%
20	1.99%	45.14%	19,954	1.16%	84.55%
21	1.90%	47.04%	18,187	1.06%	85.60%
22	1.83%	48.87%	16,710	0.97%	86.58%
23	1.77%	50.64%	15,513	0.90%	87.48%
24	1.70%	52.34%	14,236	0.83%	88.31%
25	1.64%	53.98%	13,188	0.77%	89.08%
26	1.57%	55.55%	12,107	0.70%	89.78%
27	1.50%	57.05%	11,182	0.65%	90.43%
28	1.43%	58.47%	10,232	0.60%	91.03%
29	1.38%	59.85%	9,569	0.56%	91.58%
30	1.31%	61.17%	8,800	0.51%	92.10%
31 이상	38.82%	100%	135,848	7.92%	100%
합계	100%	-	1,718,537	100%	-

7) 인터넷뱅킹 사용자용 보안프로그램을 우회하여, 공인인증서 파일과 인터넷뱅킹 거래 화면 캡쳐 및 사용자 입력 정보를 유출(키로킹)하는 악성코드 [4]

8) 사용자에게 보안카드 번호 입력이 요구된 정상 종료 거래와 비정상 종료 거래 전체

9) 은행 내부에서 사용자 인증정보(접근매체)는 유출되지 않았다고 가정함

〔표 5〕 보안카드 거래 회수 별 지시번호가 중복 이용될 확률

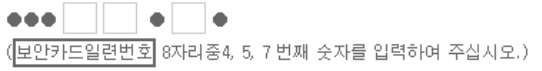
이용 회수(N)	사용자 수 비율(누적)	중복 발생 확률 ($P \times P$)
1	15.39%	0.11%
2	26.46%	0.43%
3	35.27%	0.94%
4	42.38%	1.61%
5	48.15%	2.43%
6	53.00%	3.39%
7	57.12%	4.46%
8	60.73%	5.64%
9	63.90%	6.91%
10	66.78%	8.27%
11	69.36%	9.69%
12	71.70%	11.17%
13	73.85%	12.70%
14	75.80%	14.28%
15	77.60%	15.89%
16	79.22%	17.53%
17	80.73%	19.19%
18	82.11%	20.86%
19	83.39%	22.55%
20	84.55%	24.24%
21	85.60%	25.94%
22	86.58%	27.63%
23	87.48%	29.32%
24	88.31%	31.00%
25	89.08%	32.66%
26	89.78%	34.32%
27	90.43%	35.95%
28	91.03%	37.57%
29	91.58%	39.17%
30	92.10%	40.75%
31 ~ 100	100%	42.30% ~ 93.37%

한 난수가 제한되어 있으므로 보안카드 사용을 반복할 경우, 다음 거래에서 앞서 사용된 보안카드 지시번호가 다시 사용될 가능성은 지속적으로 증가한다.

예를 들어, 보안카드를 6회 이용한 사용자의 경우 7회째에 앞서 사용된 보안카드 지시 번호가 중복해서 다시 제시될 확률은 3.39%에 해당한다. 다시 말하면, 해커가 사용자 PC에 악성코드를 설치하는 등 다양한 해킹방법을 이용하여 사용자 화면에 표시되는 보안카드 지시번호와 사용자가 입력하는 보안카드번호를 조사 대상기간인 3개월 동안 모두 모니터링 할 경우, 보안카드를 6회 이용한 적인 있는 사용자의 보안카드 번호를 다음 거래(7회째)에서 재사용하여 비정상 자금 이체 같은 사고를 일으킬 수 있는 최대 확률은 3.39% 이다.[10] 물론 이런 확률은 사용자의 정상적인 보안카드 사용 거래 시 해커가 해당 보안카드 지시번호 및 보안카드 번호 뿐만 아니라 공인인증서 파일과 공인인증서 비밀번호, 기타 비밀번호 등을 모두 유출해서 알고 있다는 가정에서 가능한 확률이다.[11]

3.2 보안카드 일련번호 사용 현황 및 안전도 분석

보안카드 일련번호는 대부분 8자리(일부 금융기관은 10자리)의 숫자로 구성되며, 일반적으로 보안카드의 유일성을 식별하기 위한 정보지만, 공인인증서의 부정 발급을 차단하기 위한 추가 인증수단으로서도 사용된다. 금융회사는 보안카드 일련번호 숫자 중 3개의 숫자를 임의로 선택하여 <그림 3>과 같이 제시하고, 정상 사용자가 이를 입력하도록 하는 방식으로 사용된다.



〈그림 3〉 공인인증서 재발급 시 보안카드 일련번호를 입력 받는 화면 예

보안카드 일련번호도 보안카드 번호처럼 반복하여 사용할 경우, 다음 거래에서 앞서 한 번이라도 사용한 적이 있는 순번의 번호가 모두 다시 요구될 가능성이 계속 증가하게 되며, 그만큼 공인인증서가 비정상적으로 발급될 가능성이 높아진다고 볼 수 있다. 다만, 본 논문에서 분석 자료로 사용한 보안카드 일련번호는 8자리를 가진다.

조사 대상 기간 동안 보안카드 일련번호를 입력하는 인증 거래의 이용 빈도 별 사용자 비율은 [표 6]과 같다. 참고로 보안카드 보유자 3,697,189명([표 3] 참조) 중 조사 대상 기간 동안 보안카드 일련번호를 1회 이상 이용한 사용자는 36.29%인 1,341,748명이다.

[표 6]에서 보이는 바와 같이, 보안카드 일련번호를 단 1회 이용한 사용자는 전체 1,341,748명 중 65.07%인 873,017명이다. 즉, 동일 조사에서 보안카드를 1회 이상 이용한 사용자 1,718,537명([표 4] 참조) 중

10) 보안카드 번호가 4자리 숫자로 구성됨에 따라 발생하는 임의추정가능확률(1/10,000)과 실제 온라인 거래에서 제공하는 연속적인 보안카드 입력 오류 최대 허용 회수(일반적으로 5회)는 없다고 가정함

11) 공인인증서 파일이 유출되지 않는 피싱, 파밍의 경우 해커의 공인인증서 재발급이 필요함

〔표 6〕 보안카드 일련번호 이용 빈도별 사용자 비율

보안카드 일련번호 이용 거래			사용자		
회수	비율	비율 (누적)	명	비율	비율 (누적)
1	36.75%	36.75%	873,017	65.07%	65.07%
2	20.23%	56.98%	240,316	17.91%	82.98%
3	12.74%	69.72%	100,906	7.52%	90.50%
4	9.02%	78.74%	53,549	3.99%	94.49%
5	6.49%	85.23%	30,842	2.30%	96.79%
6	4.38%	89.61%	17,345	1.29%	98.08%
7	2.76%	92.37%	9,368	0.70%	98.78%
8	1.85%	94.22%	5,496	0.41%	99.19%
9	1.25%	95.47%	3,296	0.25%	99.43%
10	0.91%	96.37%	2,152	0.16%	99.59%
11	0.67%	97.04%	1,447	0.11%	99.70%
12	0.47%	97.51%	932	0.07%	99.77%
13	0.37%	97.88%	675	0.05%	99.82%
14	0.29%	98.17%	484	0.04%	99.86%
15	0.21%	98.38%	338	0.03%	99.88%
16	0.19%	98.58%	286	0.02%	99.90%
17	0.15%	98.72%	206	0.02%	99.92%
18	0.13%	98.85%	169	0.01%	99.93%
19	0.10%	98.95%	122	0.01%	99.94%
20	0.11%	99.06%	128	0.01%	99.95%
21 이상	0.94%	100.00%	674	0.05%	100.00%
합계	100.00%	-	1,341,748	100.00%	-

50.80%는 공인인증서를 1회 재발급 받았다고 볼 수 있다.[12)]

보안카드 일련번호를 이용한 인증 거래를 반복할 경우, 앞서 한 번이라도 사용된 적이 있는 일련번호 순번이 다음 거래에서 모두 재사용될 확률(P)을, 모 시중은행에서 사용하는 것과 동일한 인증 로직을 구현하여 1백만명의 사용자를 가정하여 10회씩 반복 실행하여 구한 평균값은 [표 7]과 같다.

[표 7]에서 보는 바와 같이, 보안카드 일련번호를 이용한 사용자의 90.50%는 3회 이하로 보안카드 일련번호를 사용하였으며, 이 때 다음 거래에서 앞서 한 번이라도 사용된 순번이 모두 재사용될 확률은 39.58%이다.

다시 말하면, 사용자 주민번호, 비밀번호, 보안카드 번호 등이 모두 유출되었다고 가정할 때, 해커가 앞서와 동일한 방법으로 사용자 화면에 표시되는 보안카드 일련번호 입력 화면과 사용자가 입력하는 보안카드 일련번호를 조사 대상기간인 3개월 동안 모두 모니터링 할

12) 보안카드 일련번호를 사용하는 거래는 모두 공인인증서 발급 거래라고 가정함.

〔표 7〕 보안카드 일련번호 사용 회수 별 다음 거래 시 중복 제시 확률

보안카드 일련번호 인증 거래 회수	사용자 수 비율 (누적)	반복 확률(P)
1	65.07%	1.79%
2	82.98%	17.68%
3	90.50%	39.58%
4	94.49%	58.92%
5	96.79%	73.05%
6	98.08%	82.70%
7	98.78%	89.07%
8	99.19%	93.18%
9	99.43%	95.59%
10	99.59%	97.29%

경우, 보안카드 일련번호를 3회 이용한 적인 있는 사용자의 보안카드 일련번호를 다음 거래(4회째)에서 재사용하여 공인인증서를 부정하게 재발급 받을 수 있는 최대 확률은 39.58% 이다.[13)]

3.3 보안카드 재발급 현황

보안카드 번호와 보안카드 일련번호는 사용자가 보안카드를 재발급 받을 경우 모두 초기화되므로, 재발급 전에 유출된 값을 악용하는 것을 모두 막을 수 있다. 조사 대상 기간 동안 보안카드를 재발급한 현황은 [표 8]과 같다.

〔표 8〕 보안카드 재발급 회수별 사용자 비율

재발급 회수	사용자 수	비율
1	105,807	99.05%
2	1,008	0.94%
3	12	0.01%
합계	106,827	100.00%

실제 거래 로그 조사 대상 기간 동안, 보안카드를 1회 이상 재발급 받은 사용자는 106,827명으로 보안카드 1회 이상 사용자 약 172만명 대비 6.21%만이 재발급을 받았고, 보안카드 일련번호 1회 이상 사용자 약 134만명 대비 7.96%만이 재발급을 받았다.[14)] 그러므로 보안

13) 보안카드 일련번호 세자리 숫자를 임의로 입력 시 적중 확률(1/1,000)과 실제 온라인 거래에서 제공하는 연속적인 보안카드 일련번호 입력 오류 최대 허용 회수(일반적으로 5회)는 적용하지 않음

카드 실 사용자 중 주기적으로 보안카드를 재발급 받아 보안카드 정보의 유출에 따른 사고 위험을 제거하는 사용자는 많지 않음을 알 수 있다.

3.4 보안카드 인증 안전성 개선 방안 검토

보안카드 사용 거래의 반복에 따른 유출로 인한 사고 위험을 줄이기 위한 기술적인 방법으로 먼저 보안카드 지시번호와 보안카드 일련번호의 경우의 수를 증가시키는 방법을 고려할 수 있다. 예를 들어, 보안카드의 단면 또는 양면을 활용하여 보안카드 지시번호 수를 증가 시키면 중복 이용될 확률을 줄일 수 있는데, 30개에서 35개, 또는 40개로 늘릴 경우 중복 발생 확률은 [표 9]과 같다.

[표 9]에서 보이는 바와 같이, 보안카드를 6회 이용한 경우를 기준으로 보안카드 지시번호를 35개 또는 40개로 늘리면 동일한 지시번호가 다음 거래(7회째)에서 중복 이용될 확률이 3.39%에서 각각 2.55%와 1.99%로 감소하며, 30회를 이용한 경우는 40.75%에서 각각 33.74%와 28.31%로 감소하게 된다.

그러나 기술적인 방법으로 보안카드 지시번호의 수를 좀 더 늘리더라도, 반복 사용될 경우에는 그만큼 보안카드 정보 유출 가능성이 증가할 수밖에 없는 한계가 있으며, 그럼에도 불구하고 보안카드를 주기적으로 재발급 받는 실사용자의 비율이 높지 않음도 앞서 이미 확인 하였다. 또한 사용자가 보안카드 정보를 단 한 번만 정상적인 거래에서 입력했다고 하더라도, 해당 정보가 악성코드에 의해 유출되어 악용되었을 가능성이 전혀 없다고 할 수 없는 것이 앞서 기술적인 분석 결과에 따른 현실이므로[4], 실제로는 피싱, 파밍에 의해 모든 비밀번호와 보안카드 정보가 유출되어 발생된 비정상 자금 이체 사고의 경우에도 고객이 이를 부정할 경우, 수사권이 없는 금융회사에서 고객의 과실을 입증하기 어려운 문제가 있다. 따라서 금융회사에서는 사용자가 보안카드 번호를 실수로라도 유출하지 않도록 막을 수 있는 개선 방안을 수립하여 관련 피해 발생을 사전에 예방하는 것이 최선이다.

〔표 9〕 보안카드 지시번호의 수에 따라 지시번호가 중복 이용될 확률

정상 거래수 (N)	사용자 비율 (누적)	지시번호의 수에 따른 중복 발생 확률		
		30개	35개	40개
1	15.39%	0.11%	0.08%	0.06%
2	26.46%	0.43%	0.32%	0.24%
3	35.27%	0.94%	0.69%	0.53%
4	42.38%	1.61%	1.20%	0.93%
5	48.15%	2.43%	1.82%	1.41%
6	53.00%	3.39%	2.55%	1.99%
7	57.12%	4.46%	3.37%	2.64%
8	60.73%	5.64%	4.28%	3.36%
9	63.90%	6.91%	5.27%	4.15%
10	66.78%	8.27%	6.33%	5.00%
11	69.36%	9.69%	7.45%	5.91%
12	71.70%	11.17%	8.63%	6.86%
13	73.85%	12.70%	9.86%	7.87%
14	75.80%	14.28%	11.13%	8.91%
15	77.60%	15.89%	12.43%	9.98%
16	79.22%	17.53%	13.77%	11.09%
17	80.73%	19.19%	15.14%	12.23%
18	82.11%	20.86%	16.53%	13.40%
19	83.39%	22.55%	17.93%	14.58%
20	84.55%	24.24%	19.36%	15.79%
21	85.60%	25.94%	20.79%	17.01%
22	86.58%	27.63%	22.23%	18.24%
23	87.48%	29.32%	23.68%	19.48%
24	88.31%	31.00%	25.13%	20.74%
25	89.08%	32.66%	26.58%	21.99%
26	89.78%	34.32%	28.02%	23.26%
27	90.43%	35.95%	29.46%	24.52%
28	91.03%	37.57%	30.90%	25.79%
29	91.58%	39.17%	32.33%	27.05%
30	92.10%	40.75%	33.74%	28.31%
평균	-	17.89%	14.37%	11.78%

Ⅳ. 실수 입력 방지 기법을 적용한 보안카드 인증 개선 방안

본 논문에서는 피싱 웹사이트에 표시된 보안카드 입력 화면상의 지시번호 표기 방식 등이 금융회사가 사용자에게 제공하는 실제 보안카드의 표기 방식과 모두 동일하다는 점에 착안하여, 사용자마다 서로 상이한 형식의 보안카드를 발급함으로써 사용자가 스스로 피싱 웹

14) 분석 기간을 1년으로 확대해서 최근 1년간 보안카드 이용 사용자가 모두 최근 3개월 사용자와 중복 되고, 보안카드 재발급 사용자는 중복이 전혀 없다고 가정하면, 보안카드 재발급자 비율은 최대 6.21% * 3/12 = 24.84%임. 보안카드 사용 거래 분석 자료와 보안카드 재발급 거래 분석 자료를 비교하면, 보안카드 번호 사용자는 분석 기간 중 2회 이상 중복 사용 비율이 약 85%로 높은 반면에, 보안카드 재발급자는 중복 비율이 0.95%로 아주 낮으므로, 분석 기간을 1년 이상으로 확대하면, 보안카드 이용 사용자 중 보안카드 재발급자 비율은 약 15~20% 에 이를 것으로 추정됨

사이트에 접속했음을 쉽게 인지하거나, 피싱 웹사이트 화면상의 지시번호에 따라 사용자가 보유한 보안카드 번호를 정상적으로 입력할 수 없게 하는 실수방지기법(fool proof)을 적용한 보안카드 인증 개선방안을 제안한다. 실수 입력 방지 기법은 세부적으로 보안카드 지시번호의 배열형식 다양화, 보안카드 지시번호의 순서 차별화, 보안카드 번호 마스킹 방식으로 구성된다.

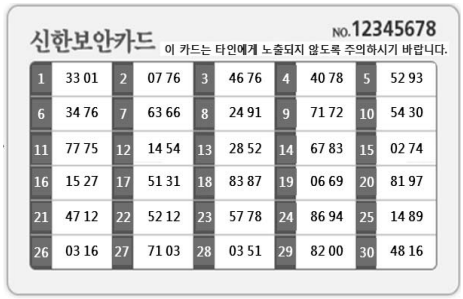
4.1 보안카드 지시번호의 배열 형식 다양화 방식

일반적으로 보안카드의 지시번호는 모든 사용자들에게 동일하게 정형화된 배열로 구성되어 있다. 예를 들어, 모 시중은행의 보안카드는 지시번호 30개가 6행 5열로 구성되고 지시번호는 좌측 상단을 기준으로 행이 먼저 변경된 후 열이 변경되는 방식으로 연속된 번호로 부여되어 있다.

〈그림 4〉 현재 사용되는 보안카드 지시번호의 배열형식

금융회사에서, 보안카드 지시번호 배열형식이 기존과 다른 방식인 (a)열우선, (b)회전, (c)회전 및 행열 수 변경 등으로 변경된 보안카드를 사용자에게 임의로 발급한다면, 피싱 웹사이트의 보안카드 지시번호 배열형식은 해커(피의자)가 직접 사용자의 보안카드 실물을 확인하지 않는 한 상이할 가능성이 높기 때문에, 피싱 사이트에 접속한 사용자가 보안카드 지시번호 배열방식의 상이함을 스스로 인지하여 보안카드 번호를 입력할 확률이 낮아진다.

이 방법은 물리적인 한계로 인하여, 보안카드 번호 배열 형식의 경우의 수가 제한적인 단점이 있으나, 현재의 단일 방식의 배열형식을 사용하는 경우에 비하여 피싱에 의해 보안카드 번호를 입력할 가능성을 최대 1/(배열형식의 수)까지 낮출 수 있다는 장점이 있다.



(a) 열우선으로 변경된 보안카드

(b) 회전 변경된 보안카드

(c) 회전 및 행렬수가 변경된 보안카드

〈그림 5~7〉 보안카드 지시번호의 배열형식을 다양화하는 방식 예시

4.2 보안카드 지시번호의 표기 순서 차별화 방식

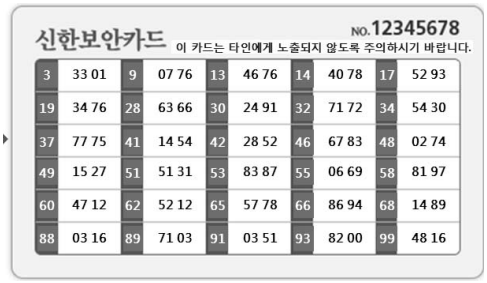
앞서 설명한 보안카드 지시번호의 배열형식 다양화 방식은 해커가 적어도 하나의 배열형식을 인지하여 피싱 웹페이지를 구성할 수 있기 때문에, 동일한 배열형식을 이용하는 사용자는 피싱 사고를 당할 가능성이 여전히 잔존한다.

이의 대응 방안으로서, 보안카드 지시번호를 구성하는 기존의 아라비아 숫자를 사용자의 사용 편의성이 저하되지 않는 수준에서 (a) 숫자와 문자 혼용(예: 1, A, 2, B,...), (b) 최초 시작번호 변경(예: 51~80), (c) 임의

배열(예: 3, 5, 9, ...) (d) 역순으로 배열(예: 99,98,97,...) 등의 방식을 혼용하여 사용자마다 차별화된 보안카드를 발급한다면, 피싱 웹사이트의 보안카드 지시번호 표기 순서는 해커가 직접 사용자의 보안카드 실물을 확인하지 않는 한 상이할 확률이 매우 높기 때문에, 사용자가 우연의 일치로 동일한 보안카드 지시번호의 배열을 가진 피싱 웹사이트에 접속하더라도 보안카드 지시번호의 상이함을 스스로 인지할 수 있을 뿐만 아니라, 피싱 웹사이트에서 제시한 보안카드 지시번호에 따라 사용자가 실제 보유한 보안카드 번호를 정상적으로 입력하는 것 자체가 기술적으로 불가능하거나 매우 어렵기 때문에, 보안카드 번호 유출에 따른 피해를 입을 확률이 그만큼 낮아진다.

이 방법은 보안카드 지시번호 위치를 인식하는 직관성이 일부 저하됨으로써 사용자에 따라 사용상 불편을 체감하는 정도가 기존 방식 대비 높다는 단점이 있으나, 물리적인 한계를 최대한 활용하여 보안카드 지시번호 순서를 다양화함으로써 피싱을 당하는 사용자가 보안카드 번호 입력 전에 이상 유무를 사전 판단하는 확률을 매우 높일 수 있다는 장점이 있다.

〈그림 8〉 현재 보안카드 번호 입력 화면 예시



〈그림 9〉 보안카드 지시번호의 표기 순서 임의 변경 예시

〈그림 10〉 변경된 보안카드 사용 시 보안카드 번호 입력 화면 예시

4.3 보안카드 번호 마스킹 방식

현재 숫자로만 구성된 보안카드 번호 중에서 일정한 개수의 임의의 번호를 선택하여 공백 또는 키보드로 입력이 불가능한, 사용자 별로 임의의 이미지로 마스킹하면, 보안카드 번호가 가지는 전체 경우의 수는 감소하는 단점이 있지만, 해커는 사용자마다 어떤 지시번호에 해당되는 보안카드 번호가 마스킹 되었는지를 사전에 알 수 없으므로, 보안카드 번호 전체를 입력 받는 피싱 웹사이트를 만들거나, 보이스 피싱을 통해 전체 보안카드 번호를 하나씩 물어보는 등의 행위를 할 때 사용자 스스로 현재 상태가 비정상적임을 인지할 수 있는 확률을 높일 수 있다.

〈그림 11〉 일부 보안카드 번호에 이미지 마스킹 적용 예시

Ⅴ. 제안기법의 비용 및 편익 분석

실수 입력 방지 기법으로 제안한 세 가지 방식의 장단점은 다음과 같으며, 금융회사에서는 발급 대상 사용자의 연령대나 거래 유형에 따라 세 가지 방식을 적절히 혼용하여 활용할 수 있다.

〔표 10〕 실수입력방지기법 세가지의 장단점

구 분	장 점	단 점
보안카드 지시번호의 배열형식 다양화	피싱에 의해 보안카드를 입력할 가능성을 최대 1/(배열형식의 수)까지 낮출 수 있음	물리적인 한계로 인하여 배열형식의 경우의 수가 제한적임
보안카드 지시번호의 표기 순서 차별화	피싱을 당하는 사용자가 보안카드 번호 입력 시 이상 유무를 판단하는 확률을 높일 수 있음	보안카드 지시번호를 인식하는 직관성이 낮음으로써 사용자에 따라 사용상 불편을 체감하는 정도가 기존 방식 대비 높음
보안카드 일부 번호 마스킹 적용	사용자 편의성 감소 최소화, 보이스 피싱을 통해 보안카드 번호를 하나씩 물어보는 경우에도 적용 가능	보안카드 번호가 가지는 경우의 수가 적어짐

제안 방식의 실효성 확인을 위하여 소요 비용 및 편익을 분석한 결과는 다음과 같다.

비용 측면의 경우, 사용자들의 보안카드를 신규/교체 발급 시만을 고려한다면 추가 비용은 발생하지 않는다.[15] 기존 실사용자들이 이미 보유하고 있는 보안카드를 모두 일괄 교체 발급한다고 가정할 때는 전체 은행에서 개선된 방식으로 보안카드 재발급을 위해 추가되는 비용을 다음과 같이 추정할 수 있다. 국내 인터넷뱅킹 서비스에 등록된 개인 사용자는 여러 은행에 중복 가입을 포함하여 약 8,419만명이며,[16] 그 중 최근 1년 간, 1회 이상 인터넷뱅킹을 이용한 사용자 비율(45.4%)를[17] 적용하면 인터넷뱅킹 실거래 사용자는 약 3,825만명으로 가정할 수 있다. 여기에 『[표 3]의 1회 이상 로그인한 사용자 중 보안카드와 OTP 사용자 비율』을 적용하여 그 중 보안카드 사용자가 90% 라고 가정할 때, 전체 보안카드 발급 개수는 약 3,443만개이므로 보안카드 한 개당 추가되는 비용을 금융기관의 도입 비용(130원)[18] 으로 가정하면 전체 은행에서 총 약 45억원의 1회성 비용이 소요된다.

편익 측면의 경우, 인터넷 피싱 및 파밍에 의한 사용자의 직접적인 피해 감소액을 편익으로 가정한 경우는 다음과 같다. 2013년 7월, 금융감독원의 보도 자료에 따르면, 2013년 1월에서 5월까지 경찰청에 신고 접수된 전체 피싱 사기의 총 피해규모는 1,756건에 174억원이며, 그 중 인터넷 피싱사이트나 파밍이 전체의 52.9%를 차지하고[19] 있다[3]. 이에 따라 인터넷뱅킹 피싱 및 파밍과 보이스피싱의 건 별 사용자 피해액이 동일하다고 가정할 경우, 인터넷 피싱 및 파밍의 사용자 금전 피해 규모를 1년으로 환산 시 약 2,229건, 220억원이 예상된다.

그러므로 본 논문에서 제시한 방안이 인터넷 피싱 및 파밍으로 인한 보안카드 번호 유출 및 이를 통한 불법 자금 이체를 20%만 줄일 수 있다고 가정해도, 1년간 약 44억원의 사용자의 직접적인 금전 피해를 감소시킬 수 있으며, 이는 전체 은행의 인터넷뱅킹 실거래 사용자에 대한 보안카드 교체 원가 비용(약 45억원)에 근접하므로 약 1년 만에 손익 분기점을 달성하게 된다. 그리고 인터넷 피싱 및 파밍 사고로 인한 피해자의 정신적인 고통과 기회비용 등 간접 피해액과 금융회사의 신뢰도 저하 및 감독기관과 정부의 행정력 소요 등 기타 사회적 비용 등을 감안할 때 비용, 편익 분석 면에서의 타당성이 더욱 증가 한다. 특히, 금융회사 입장에서는 신규 보안카드 발급부터 적용하면 추가 비용을 거의 들이지 않고서도 실효성을 장기적으로 거둘 수 있는 가장 효율적인 방법이 될 것으로 예상된다.

15) 금융회사의 서버 시스템에서 사용자 별 차별화된 보안카드 제시 화면과 보안카드 정보(DB) 관리를 위해 필요한 개발, 관리 비용은 금융회사마다 상이하므로 본 논문에서는 고려하지 않음.

16) 한국은행의 『2013년도 1/4분기 국내 인터넷뱅킹 서비스 이용 현황』에 따른 2013년 3월말 현재 기준[1]

17) 본 논문에서 참조한 모 시중은행 실거래 결과 분석 자료 기준

18) 5대 시중은행의 2013년도 보안카드 도입 단가 평균 기준

19) 2012년10월에서 2013.5월 기간 중 발생한 전체 피싱 사기 11,439건 중 사기범의 인터넷뱅킹 비율 기준

Ⅵ. 결 론

본 논문에서는 전자금융거래에서 보안카드를 사용하는 사용자들에게 피해를 주는 주요 사고 유형인 피싱 및 파밍의 대응 방법을 제시함으로서 소비자 보호를 강화하고, 전자금융거래 전반의 신뢰도를 제고하고자 했다.

일반 사회에 도둑이나 금융 사기가 있는 것처럼, 사이버 상의 전자금융거래도 처음 시작할 때부터 도청, 해킹 등 기술적인 공격의 시도가 있어 왔지만 감독기관과 금융기관에서 매번 시의 적절한 대책을 수립하여 비교적 큰 피해 없이 안정적으로 서비스를 제공해올 수 있었다. 그러나 최근 들어 신종 사기 수법인 피싱 및 파밍이 지속적으로 진화하면서 사용자가 피해를 당하지 않도록 근본적으로 해결 방안을 수립하는데 한계가 있어 왔다.

이는 피싱 및 파밍의 근간이 사회 공학적 공격 기법으로 사용자를 속이는 수법을 사용하기 때문이므로, 본 논문에서는 그 동안의 단순한, 사용자에 대한 사전 주의 홍보 강화나 불법 자금이체 방지를 위한 추가 인증을 강화하는 방식 같은 사후 통제의 한계점을 극복하기 위하여, 정상적인 사용자는 고의가 아니면 속기 어려운 수준의 대응 방안으로서 보안카드의 활용 방법을 개선한 실수 입력 방지 기법을 제안하고 비용 및 편익 분석을 통해 타당성을 검토 하였다.

새로운 해킹 수법들은 지속적으로 등장하고 있으며, 일반 비밀번호나 보안카드 번호 등 고정된 값은 기술적인 한계로 인해 결국은 유출이 가능하다고 가정하고 대응 방안을 계속 마련하는 것이 합리적이다. 하지만 좀 더 안전한 접근매체로서의 일회용비밀번호발생기의 보급률이 보안카드보다 훨씬 낮은 현실을 감안할 때, 금번 제시된 방안이 현실적으로 쉽게 적용 가능한 실효성 있는 방안이 될 수 있을 것으로 기대된다.

참고문헌

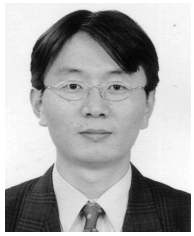
[1] 한국은행 보도자료, 2013년도 1/4분기 국내 인터넷뱅킹 서비스 이용 현황, 2013.5.16

[2] 금융감독원 보도자료, 전자금융사기 예방서비스 전면시행 가이드라인, 2013.5.15

[3] 금융감독원 보도자료, 피싱(Phishing)사기에 의한 피해유형 분석 및 금융거래 시 유의사항, 2013.7.2

[4] 김인석, “電子金融 事故有形 分析을 통한 情報保護 政策에 관한 硏究,” 논문, pp. 76-80, 2008.2

〈저자소개〉



박 진 규 (PARK JIN KYU)
1997년 2월 : 동국대학교 경영학과 졸업
2013년 현재 : 고려대학교 정보보호대학원 재학 중
1988년 2월 : 우리은행 전산부 입사
2002년 10월~현재 : 우리은행 IT컴플라이언스부(IT보안팀) 근무
<관심분야> 금융 정보보호

이 정 호 (LEE JUNG HO)
1994년 2월 : 경북대학교 전자공학과 졸업
2013년 2월 : 연세대학교 경영학 석사
2003년 8월~현재 : 신한은행 정보보안실 근무
<관심분야> 금융 정보보호