연구논문 정보화정책 제24권 제2호, 2017년 여름호, pp.20~42

인터넷 뱅킹 서비스에서의 보안위협 분류 및 분석*

이 경 률**, 이 선 영***, 임 강 빈****

요 약 본 논문은 인터넷 뱅킹 서비스의 안전성을 평가하기 위한 보안위협을 분류하고 보안 요구사항을 제안하는데 그 목적이 있다. 분류한 보안위협은 기존에 발생하였던, 그리고 발생이 가능한 보안위협을 기반으로 분석하였으며, 이를 통하여 보안 요구사항을 제안하기 위한 기반을 다질 것으로 사료된다. 보안위협 도출을 위하여 인터넷 뱅킹 서비스의 구조를 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하였으며, 각 구간에서 발생하는 보안위협을 도출하였다. 특히, 사용자 구간이 상대적으로 취약하기 때문에 전체 서비스의 안전성을 확보하기 어려운 상황이므로 이를 중점적으로 분석하였다. 분석한 보안위협을 토대로 안전한 인터넷 뱅킹 서비스를 구성할 수 있을 것으로 예상된다.

주제어: 인터넷 뱅킹, 보안 위협, 보안 요구사항, 공격 기술

Analysis and Classification of Security Threats based on the Internet Banking Service

Lee, Kyung-Roul, Lee, Sun-Young, Yim, Kang-Bin

Abstract In this paper, we focus on classification of security threats and definitions of security requirements for Internet banking service. Threats are classified based on the past and potential incidents, based upon which we will be able to propose security requirements. In order to identify security threats, the structure of the Internet banking service is classified into three sections – the financial institutions, the network, and the user-terminal – and we defined arising threats for each section. We focused the analysis especially on the user-terminal section, which is relatively vulnerable, causing difficulties in securing stability of the service as a whole. The analyzed security threats are expected to serve the foundation for safe configuration of various Internet banking services.

Keywords: internet banking, security threats, security requirement, attack technique

2017년 4월 10일 접수, 2017년 5월 15일 심사, 2017년 5월 30일 게재확정
* 본 논문은 박사학위 논문으로부터 근거한 논문임
** 순천향대학교 연구교수(carpedm@sch.ac.kr)
*** 순천향대학교 교수(sunlee@sch.ac.kr)
**** 순천향대학교 교수(yim@sch.ac.kr)

Ⅰ. 서론

인터넷을 통한 금융업무가 가능해지면서 사용자들은 공간의 제약을 받지 않고 손쉽게 은행업무가 가능하게 되었다. 하지만 이러한 이점에도 불구하고 2005년 5월, 인터넷 뱅킹 서비스에서의 해킹사건이 최초로 발생하였다. 이에 금융기관에서는 외부로부터의 위협에 대응하기 위하여 사용자 구간과 네트워크 구간, 금융기관 구간에 다양한 보안기술을 적용하였지만, 악의적인 공격자에 의한 사고사례가 지속적으로 발생하는 실정이다(이태헌, 2016). 이러한 사고가 발생하는 원인은 각 구간에 보안기술을 적용하더라도 그 환경이 가지는 취약점으로 인하여 발생하는 문제점이 대부분이어서 일부 구간에 보안위협과 보안 요구사항을 정의함으로써 근본적으로 발생하는 문제점을 해결하고자 하였다(강성구 · 서정택, 2012; 이형찬 외, 2011; 김종기 · 전진환, 2006; 조강유 외, 2013; 홍석원 외, 2012). 하지만 이러한 지표들이 전 구간에 걸쳐 전반적으로 포괄하는 보안위협에 대하여 정의되지 않은 실정이므로 근본적인 문제점을 보완하기 위해서는 기술적인 조사가 선행되어야 하며, 그 결과를 기반으로 보안 요구사항을 정의함으로써 안전성을 확보하기 위한 연구가 필요하다. 따라서 본 논문에서는 인터넷 뱅킹 서비스의 전반적인 구조를 분석하고, 구조에 따른 영역별 보안위협을 도출함으로써 보안 요구사항을 정의하기 위한 선행 연구를 진행하였다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서 인터넷 뱅킹 서비스를 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하고 각 구간에서 발생하는 보안위협을 분류하며, 제Ⅲ장에서는 금융기관 구간에서 발생 가능한 보안위협을 정의한다. 제Ⅳ장에서는 네트워크 구간에서 발생 가능한 보안위협을 정의하며, 제Ⅴ장에

〈표 1〉 인터넷 뱅킹 서비스에서의 보안위협 분류

<table>
<tr><th>구간</th><th colspan="3">보안위협</th></tr>
<tr><td rowspan="3">금융기관
구간</td><td>내부 시스템</td><td colspan="2">• 웹 서버에서의 보안위협
• 분산 서비스 거부 공격에 의한 보안위협</td></tr>
<tr><td>내부망</td><td colspan="2">• 내부 네트워크 구간 도청에 의한 보안위협
• 내부 네트워크 시스템 침투 공격에 의한 보안위협</td></tr>
<tr><td>내부 이용자</td><td colspan="2">• 내부자에 의한 보안위협
• 내부자에 의한 정보유출</td></tr>
<tr><td>네트워크
구간</td><td colspan="3">• 도청에 의한 보안위협
• 세션 탈취에 의한 보안위협
• 재전송 공격에 의한 보안위협
• 중간자 공격에 의한 보안위협
• 스크립트 삽입에 의한 보안위협</td></tr>
<tr><td rowspan="7">사용자
구간</td><td rowspan="2">자산
(기술적 보안위협)</td><td colspan="2">하드웨어</td></tr>
<tr><td>소프트웨어</td><td>• 시스템 소프트웨어
• 응용 소프트웨어</td></tr>
<tr><td rowspan="5">업무 프로세스
(관리 및 구조적
보안위협)</td><td rowspan="3">서비스 구현/
설정 단계
(관리적 보안위협)</td><td>• 개발자 (구현 관점)</td></tr>
<tr><td>• 관리자 (설정 및 관리 관점)</td></tr>
<tr><td>• 이용자 (행동학적 관점)</td></tr>
<tr><td rowspan="3">서비스
이용 단계
(구조적 보안위협)</td><td>• 플랫폼 (플랫폼 관점)</td></tr>
<tr><td>• 보안 프로그램 (방어자 관점)</td></tr>
<tr><td>• 사용자 이용 (거래 및 인증 관점)</td></tr>
</table>

서는 사용자 구간에서 발생 가능한 보안위협을 정의한다. 대부분의 공격이 사용자 구간에서 발생하므로 사용자 구간을 집중적으로 분석하며, 사용자 구간을 관리적 보안위협과 구조적 보안위협, 기술적 보안위협으로 분류하여 각 관점에서의 보안위협을 상세히 서술한다. 마지막으로 제Ⅵ장에서 결론을 도출함으로써 본 논문을 마무리한다.

Ⅱ. 보안위협 분류

인터넷 뱅킹 서비스에서 기본적인 안전성을 제공하고 있음에도 불구하고 해킹사고가 발생하였으며, 이러한 사고가 발생하는 원인을 규명하기 위하여 인터넷 뱅킹 서비스에 존재하는 보안위협에 대하여 조사한 결과를 서술하고자 한다. 즉, 인터넷 뱅킹 서비스의 전 구간인 금융기관 구간과 네트워크 구간, 사용자 구간에서 다양하게 사고가 발생하는 이유는 각 구간이 가지는 취약점에 의한 보안위협이 존재하기 때문이므로 이에 대하여 상세히 서술하고자 한다. 인터넷 뱅킹 서비스의 구성은 (금융보안연구원, 2010a)에 근거하여 금융기관 구간, 네트워크 구간, 사용자 구간으로 분류하였다. 따라서 인터넷 뱅킹 서비스가 가지는 보안위협은 금융기관 구간, 네트워크 구간, 사용자 구간에서의 보안위협으로 분류할 수 있으며, 본 논문의 범위는 사용자 구간에 초점을 맞추었으므로 금융기관 구간과 네트워크 구간의 보안위협은 간략히 살펴보고자 한다. 이에 대한 분류를 〈표 1〉에 나타내었다.

Ⅲ. 금융기관 구간에서의 보안위협 분류

금융기관에서의 보안위협은 내부 시스템에서의 보안위협, 내부망에서의 보안위협, 내부 이용자에서의 보안위협으로 분류된다.

내부 시스템에서의 보안위협은 웹 서버에서의 보안위협, 분산서비스 거부 공격에 의한 보안위협으로 분류되며, 웹 서버에서의 보안위협은 웹 페이지가 가지는 취약점으로 인하여 금융기관 외부에서 내부의 시스템에 정상적으로 접속하여 사용자 이름, 주민등록번호와 같은 개인정보가 유출되는 위협이다(이수미 · 성재모, 2011). 분산 서비스 거부 공격(DDoS, Distributed Denial of Service)에 의한 보안위협은 웹 서버의 자원을 할당하는 요청을 다량으로 전송하여 자원을 고갈시켜 사용자가 인터넷 뱅킹 서비스를 정상적으로 이용하지 못하도록 장애를 발생시키는 공격이다. 이와 같은 공격은 공격을 명령하는 명령 제어 서버(C&C server, Command and Control server)가 존재하여 악성코드에 감염된 피해자 PC에 공격을 시도하는 명령을 전송함으로써 피해자 PC에서 특정 웹 서버에 집중적으로 패킷을 전송하는 것이 일반적이었으나, 최근에는 명령 제어 서버가 존재하지 않고 특정 날짜에 공격을 시도하는 방식과 같이 변형된 공격방법도 존재한다. 이와 같은 공격에 대응하기 위한 많은 연구가 진행 중에 있으나 근본적으로 차단하기에는 한계가 있으며, 실제로 사이버 전쟁으로 발전된 사례도 존재한다(이수미 · 성재모, 2011; 심희원, 2011; 성재모, 2011; 조혜숙 외, 2010).

내부망에서의 보안위협은 내부 네트워크 구간 도청에 의한 보안위협, 내부 네트워크 시스템 침투 공격에 의한 보안위협으로 분류된다. 내부 네트워크 구간 도청에 의한 보안위협은 내부자에 의하여 내부 네트워크 상에서 전송되는 트래픽을 도청하거나 가로채어 이를 악용하는 보안위협이다(이수미 · 성재모, 2011). 내부 시스템 침투 공격에 의한 보안위협은 금융기관 내부의 취약한 시스템을 공격자가 악성코드로 감염시켜 외부에서 내부로 침투하는 공격이며, 대표적인 공격으로 APT(Advanced Persistent Threat) 공격이 있다. 이와 같은 공격은 사전에 내부 시스템의 환경을 분석하여 오랜 기간 공격에 필요한 정보를 수집하여 내부의 기밀정보를 유출시키는 것과 같은 다양한 피해가 발생할 수 있으며, 금융권을 중심으로 점차 증가하는 추세이다(이수미 · 성재모, 2011).

내부 이용자에 의한 보안위협은 내부자에 의한 보안

위협, 내부자에 의한 정보유출로 분류된다. 내부자에 의한 보안위협은 내부 네트워크 구간 도청, 내부 시스템 침투 공격, 내부자에 의한 정보유출로 분류된다. 내부자에 의한 정보유출은 금융기관 내부에 저장된 사용자의 계좌번호, 계좌비밀번호와 같은 개인정보나 이러한 정보를 암/복호하기 위한 암/복호키가 내부자에 의하여 USB 메모리와 같은 저장장치나 출력된 문서 형태로 외부로 유출되는 보안위협이다(이수미 · 성재모, 2011; 성재모, 2011; 백명한, 1998).

Ⅳ. 네트워크 구간에서의 보안위협 분류

네트워크 구간에서의 보안위협은 도청에 의한 보안위협, 세션 탈취에 의한 보안위협, 재전송 공격에 의한 보안위협, 중간자 공격에 의한 보안위협, 스크립트 삽입에 의한 보안위협으로 분류된다.

도청에 의한 보안위협은 네트워크상에서 전송되는 패킷을 인가되지 않은 제3자가 접근할 수 있도록 랜 포트나 액세스 포인트(AP, Access Point)에 스니퍼를 설치하여 탈취한 패킷을 악용하는 것이 일반적이며, 더욱 진화된 형태로 Paros, Burp suite 등과 같은 웹 프락시 도구를 악용하는 형태가 많이 사용되는 추세이다. 이와 같은 보안위협의 경우에는 사용자의 전자적 장치와 금융기관의 웹 서버 사이에 수학적 도구를 활용하여 보안채널을 구성함으로써 직접적인 피해가 발생할 가능성은 크지 않지만, 무선 네트워크의 사용이 확대되면서 물리적인 공격이나 인증 프로토콜의 취약점과 같은 문제점으로 인하여 내부로 침투가 가능한 보안위협이 존재한다(이수미 · 성재모, 2011; 심희원, 2011; 성재모, 2011; 조혜숙 외, 2010; 이형익, 2010).

세션 탈취에 의한 보안위협은 인터넷 뱅킹 서버가 접속된 사용자를 구분하기 위하여 발급한 세션 아이디를 탈취하여 본인확인을 우회함으로써 정상적으로 조회와 같은 서비스를 이용하는 보안위협이다(이수미 · 성재모, 2011; 성재모, 2011).

재전송 공격에 의한 보안위협은 도청을 통하여 탈취한 인증과 관련된 패킷을 재전송함으로써 인가되지 않은 제3자가 정상적으로 서비스를 이용하는 보안위협으로, 사용자 인증정보의 평문을 확보하지 못하더라도 암호문을 재전송함으로써 본인확인의 우회가 가능하다(이수미 · 성재모, 2011; 성재모, 2011).

중간자 공격에 의한 보안위협은 공격자가 ARP (Address Resolution Protocol) 스푸핑과 같은 방법으로 MAC 주소를 변경함으로써 사용자가 인터넷 뱅킹 서버로 전송하는 패킷은 공격자에게 전송되고, 인터넷 뱅킹 서버가 사용자에게 전송하는 패킷은 공격자에게 전송되어 암호화된 패킷을 복호화하여 인증정보와 같은 비밀정보를 탈취하거나 거래정보를 위/변조하는 보안위협이다(이수미 · 성재모, 2011; 성재모, 2011).

스크립트 삽입에 의한 보안위협은 웹 페이지가 자바 스크립트로 구성되었기 때문에 발생하는 문제점으로, 인터넷 뱅킹 서버에서 제공하는 웹 페이지는 금융정보를 입력하는 필드만을 부분적으로 암호화하므로 스크립트 코드를 추가할 수 있다. 이와 같은 문제점으로 인하여 공격자에게 전송하는 스크립트 코드를 삽입함으로써 인터넷 뱅킹 서버로 전송하는 비밀정보를 탈취하는 보안위협이다(이수미 · 성재모, 2011; 성재모, 2011).

Ⅴ. 사용자 구간에서의 보안위협 분류

상기 금융기관과 네트워크 구간에서의 보안위협은 내부자에 의한 보안위협을 제외하고는 폐쇄적인 특징과 수학적 도구를 활용함으로써 안전성이 보장되어 공격자로 하여금 공격이 불가능하거나 공격 의지를 상실하게 한다. 이와 같은 안전성은 암/복호나 전자서명 및 검증 알고리즘에 사용되는 비밀키의 길이에 비례하며, Kerckhoff의 원칙에 따르면 알고리즘이 공개되더라도 비밀키를 알 수 없다면 안전성이 보장된다. 컴퓨터의 성능이 향상됨에 따라 비밀키의 무차별 대입 공

격에 취약하므로 요구되는 비밀키의 길이도 증가하며, BSI(Federal Office for Information Security), NIST(National Institute of Standards and Technology), ANSSI(French Network and Information Security Agency), Lestra 등과 같은 기관에서 연도별로 권장하는 최소한의 비밀키 길이를 발표하였으며, 대칭키 알고리즘의 키 길이를 〈표 2〉, 비대칭키 알고리즘의 키 길이를 〈표 3〉, 해쉬 알고리즘 및 그 크기를 〈표 4〉에 나타내었다(이재식, 2013).

이와 같은 이유로 공격자는 금융기관과 네트워크 구간보다 상대적으로 취약한 사용자 구간을 공격 대상으로 선택하는 추세이고, 사용자 구간에서의 보안위협은 공격자의 능력에 의존적이며, 공격자의 능력은 정보접근 능력, 변조 능력, 실시간 공격 능력 및 스마트폰 제어 능력으로 분류할 수 있다. 정보접근 능력은 사용자가 입력하는 아이디, 비밀번호, 계좌번호, 계좌비밀번호와 같은 비밀정보에 공격자가 접근할 수 있는 능력을 의미하고, 변조 능력은 입력된 비밀정보를 공격자가 원하는 정보로 변조하는 능력을 의미하며, 실시간 공격 능력은 입력된 비밀정보를 공격자에게 실시간으로 전송하여 악의적인 행위를 하는 능력, 스마트폰 제어 능력은 유럽에서 발생한 Eurograbber 공격(Kalige & Burkey, 2012)과 같이 악성 앱으로 인하여 SMS를 가로채거나 착신전환 등을 활용하여 악의적인 행위를 하는 능력을 의미한다. 각 능력을 토대로 발생 가능한 공격을 살펴보면 다음과 같다(이한욱 · 신휴근, 2013).

〈표 2〉 연도별 권장되는 대칭키 알고리즘의 키 길이(bit)

연도	BSI	NIST	FNISA	Lenstra
2009년까지	–	80	80	74
2010년까지	–	80	80	75
2012년까지	–	112	100	76
2020년까지	–	112	100	82

〈표 3〉 연도별 권장되는 비대칭키 알고리즘의 키 길이(bit)

연도		BSI	NIST	FNISA	Lenstra
2009년까지	최소	1536	1024	1536	1114
	권장	2048	–	–	–
2010년까지	최소	1728	1024	1536	1152
	권장	2048	–	–	–
2012년까지	최소	1976	2048	2048	1229
	권장	2048	–	–	–
2020년까지	최소	2048	2048	4096	1568

〈표 4〉 연도별 권장되는 해쉬 알고리즘 및 크기(bit)

연도	알고리즘 종류	BSI	NIST	Lenstra
2009년까지	–	80	148	160
2010년까지	–	224	150	160
2012년까지	SHA224, SHA256, SHA384, SHA512	224	152	256
2020년까지	–	224	163	256

〈표 5〉 정보접근 능력이 없는 공격자의 공격 성공 확률

본인확인수단		무차별 대입 공격 성공 확률
3등급	1. 공인인증서 2. 보안카드	$(1/10^4)\times100\%$
1등급	1. 공인인증서 2. OTP 생성기	$(1/10^6)\times100\%$
1등급	1. 하드웨어 보안토큰 2. 보안카드	$(1/2^{2048})\times100\%$
1등급	1. 보안카드 2. 공인인증서 3. 이중채널	$(1/2^{32})\times100\%$

정보접근 능력을 가진 공격자는 비밀번호와 같은 비밀정보에 대한 접근 능력이 있으며, 사용자의 전자적 장치 중 디스플레이 장치나 키보드와 같은 자원에 대한 접근 능력이 있을 수 있다. 정보접근 능력이 없는 공격자의 경우, 본인확인수단별로 무차별 대입 공격을 시도할 때의 공격 성공 확률이 〈표 5〉와 같이 매우 낮으므로 악성코드 등을 활용하여 비밀정보나 자원에 대한 접근을 획득함으로써 공격 성공 확률을 높일 수 있다. 표에서의 공격 성공 확률은 공인인증서가 쉽게 노출되므로 공격자가 접근 가능한 것으로 가정되었다(조창현, 2010).

공인인증서와 보안카드를 사용하는 경우에는 보안카드가 4자리로 입력하므로 $(1/10^4)\times100\%$의 공격 성공 확률을 가지고, OTP 생성기와 보안카드를 사용하는 경우에는 OTP 값이 6자리이므로 $(1/10^6)\times100\%$의 공격 성공 확률을 가지며, 하드웨어 보안토큰과 보안카드를 사용하는 경우에는 하드웨어 보안토큰 내에 저장된 공인인증서를 탈취할 수 없으므로, 공인인증서를 생성하는데 필요한 키인 $(1/2^{2048})\times100\%$의 공격 성공 확률이 매우 낮으므로 보안카드의 공격 성공 확률은 무시되었다. 이중채널을 이용하는 경우에는 전화망에 접근하는 확률을 계산하는 것이 수치적으로 한계가 있으므로 ESN(Electronic Serial Number)을 복제하는 확률로 대체되었으며, ESN이 32비트이므로 $(1/2^{32})\times100\%$의 공격 성공 확률을 가진다. 하지만 공격자가 보안카드, OTP 값, 하드웨어 보안토큰, 전화망에 접근이 가능한 경우에는 기존의 모든 본인확인수단에 대한 공격이 100% 확률로 성공이 가능하므로 이와 같은 능력을 갖추기 위한 다양한 공격을 시도한다(조창현, 2010; 유한나 외, 2011).

변조 능력을 가진 공격자는 사용자가 계좌이체와 같은 서비스를 이용할 경우, 사용자가 입력하는 계좌번호가 아닌 공격자가 원하는 계좌번호로 변조함으로써 불법이체를 시도한다. 현재 대부분 인터넷 뱅킹 서비스에서의 본인확인수단과 보안기술이 거래내역을 확인할 수 없는 구조이므로 메모리 해킹과 같은 공격기술을 활용하는 공격자에게 위협이 노출되는 문제점이 있으며, 거래내역을 확인하는 수단에서도 일부 문제점이 존재한다(이한욱 · 신휴근, 2013).

실시간 공격 능력을 가진 공격자는 사용자가 계좌이체와 같은 서비스를 이용할 경우, 이를 탈취하여 사용자의 이체를 잠시 중단시키거나 방해하고, 탈취한 이체정보를 이용하여 실시간으로 불법이체를 시도한다. 이와 같은 공격은 실시간이라는 점을 제외하면 메모리 해킹과 유사하지만, OTP 생성기나 보안카드의 경우에는 일정 시간동안 동일한 값으로도 정상적인 처리가 가능한 문제점으로 인하여 발생하며, 탈취한 정상적인 사용자의 인증정보를 활용하므로 탐지하거나 무력화하기에는 한계가 있다. 하지만 거래내역을 확인할 수 있는 본인확인수단의 경우에는 거래정보와 연관된 인

증정보가 생성되므로 이를 탈취하더라도 거래정보를 수정할 수 없으므로 불법이체가 불가능하지만, 거래내역을 확인할 수 없는 모든 본인확인수단에서 공격이 가능하다(이한욱 · 신휴근, 2013).

스마트폰 제어 능력을 가진 공격자는 멀티채널기반의 본인확인수단을 이용할 경우, 승인번호와 같은 SMS나 ARS와 같은 전화 승인이 요청되면, 사용자 스마트폰에 설치된 악의적인 앱을 통하여 SMS를 가로채거나 착신전환과 같은 악의적인 행위를 기반으로 불법이체를 시도한다. 이와 같은 공격은 동일 계정에 다중 사용자가 동시에 접근하는 것을 제한하기 때문에 사용자가 주로 이용하지 않는 심야 시간에 공격을 시도할 수 있으며, 모든 본인확인수단에서 공격이 가능하다(이한욱 · 신휴근, 2013).

상기와 같은 능력을 가지는 공격자에 의한 보안위협의 안전성을 평가하기 위하여 고전적인 Yao-Dolev 위험모델이 주로 사용되었으나(Dolev & Yao, 1983), 이는 공개키 프로토콜의 안전성 평가 기준인 인증, 무결성, 기밀성, 부인방지를 토대로 클라이언트와 서버 간 통신채널의 안전성을 중점적으로 평가함으로써 현재 사용자 구간의 위협을 고려하지 않았다. 따라서 통신채널뿐만 아니라 사용자 구간과 같은 채널의 말단에 대한 안전성 평가가 요구되었고, 이에 2006년 인터넷 뱅킹 서비스의 안전성 평가를 위한 새로운 위험모델이 제안되었으며(Hiltgen, et al,, 2006), 제안된 모델은 인터넷 뱅킹 서비스에 대한 공격을 오프라인 정보추출 공격, 온라인 채널탈취 공격, 거래조작 공격으로 분류하였다. 오프라인 정보추출 공격은 악성코드나 프로토콜과 같은 논리적인 취약점과 사용자의 부주의와 같은 관리적인 취약점으로 인하여 사용자의 비밀정보를 수

〈표 6〉 공격모델에 따른 세부적인 공격기술 일례

공격모델			세부적인 공격기술 일례
오프라인 공격	논리적 오류 기반	추측 공격	• 온라인/오프라인 추측 공격 • 오프라인 크래킹
		도청 공격	• 수동적 정보도청 • 감시
		재사용 공격	• 비밀정보 또는 인증정보 재사용
	관리적 부주의 기반	도난	• 정보 도난 • 단말기 도난
		복제	• 악성코드에 의한 정보 복제 • 단말기 복제 • 부채널 공격에 의한 비밀정보 복제
		위장 공격	• 서버 위장 공격 • 피싱 공격 • 파밍 공격 • 사회공학적 기법 • 사용자 부주의에 의한 기만 공격
온라인 공격	세션 탈취 공격		• 사용자 세션 탈취 및 가로채기
	중간자 공격		• 중간자 공격
거래조작 공격	메모리 변조 공격		• 브라우저 중간자 공격
	복합 조작 공격		• 메모리 변조+재사용 공격 등을 혼합한 복합 조작 공격
서비스 신뢰 공격	서비스 거부 공격		• 서비스 거부 공격 • 분산 서비스 거부 공격
	거래 부인		• 송/수신자 거래 부인

집하고 이를 차후에 악의적으로 활용하는 공격으로 정의하였고, 온라인 채널탈취 공격은 네트워크 구간에 침입하여 사용자의 비밀정보를 가로채거나 변조하는 공격으로 정의하였으며, 거래조작 공격은 거래정보를 공격자가 의도한 대로 조작하는 공격으로 정의하였다. 여기에 추가적으로 서비스 거부 공격과 같이 인터넷 뱅킹 서비스의 신뢰에 대한 공격을 추가한 연구가 진행되었으며, 상기 공격모델에 대한 세부적인 기술을 〈표 6〉에 나타내었다(심희원, 2011).

상기의 오프라인 및 온라인 공격과 같은 공격모델은 공격하는 방식에 따라 분류하였지만, 공격방식과 위협은 서로 상관관계가 부족하므로 본 논문에서는 이러한 공격모델을 참고하여 공격방법을 중점으로 관리적 보안위협, 구조적 보안위협, 기술적 보안위협으로 분류하였다. 분류의 기준은 (장상수, 2015)에서 위협 식별의 분류가 업무프로세스, 자산임에 근거하였으며, 분류한 사용자 구간에서의 보안위협을 〈표 7〉에 나타내었다.

〈표 7〉 사용자 구간에서의 보안위협 분류

대분류	소분류	보안위협 상세					
자산 (기술적 보안 위협)	하드웨어	복제	부채널 공격	PS/2 키보드	USB 키보드		
		디스플레이 장치	터치패드	보안 USB	임베디드 시스템		
	소프트웨어	시스템 소프트웨어	시스템 소프트웨어인 운영체제 및 커널은 응용 프로그램에서의 보안위협과 비슷하므로 응용 프로그램에서의 보안위협 참조				
		응용 소프트웨어 응용	세션 탈취	중간자 공격	재전송 공격	위장	인젝션
			역공학	후킹	메모리 해킹	종단 간 암호화	ActiveX
			MITB 공격	플래시	암호 라이브러리		
업무 프로세스	서비스 구현/설정 단계 (관리적 보안위협)	개발자 (구현 관점)	연속 인증시도	잔여정보	평문정보 저장	취약한 인증 및 세션	
			방화벽 시스템의 결함	URL 접속제한 실패	검증되지 않은 리다이렉트와 포워드		
		관리자 (설정 및 관리 관점)	보안 설정상의 오류	암호기능 관리 오류	제로데이 공격	허술한 감사 추적	감사정보 파괴
			세션관리 미숙	저장 데이터 훼손	전송계층에 대한 불충분한 보호	방화벽 시스템 관리자의 관리 미숙	
		이용자 (행동학적 관점)	사용자 부주의	사고 발생 후 조치			
	서비스 이용 단계 (구조적 보안위협)	플랫폼 (플랫폼 관점)	특권수준	입력 유효성 공격	파일 시스템 조작	프로세스 조작	어플리케이션 조작
			매개변수 조작	전송 데이터 훼손	악성코드	안전하지 않은 직접 객체 참조	
		보안 프로그램 (방어자 관점)	보안 프로그램의 부분적용	보안 프로그램의 개별화	보안 프로그램 무력화	서비스 구조의 문제점	
			암호기능 무력화	보안 프로그램의 의존적 운영	보안 프로그램을 위한 프로그램의 부재		
		사용자 이용 (거래 및 인증 관점)	거래 관점	거래부인	거래방해	거래정보 위/변조	민감한 정보
			인증 관점	인증수단의 문제점	훔쳐보기	도난	
				가짜 SSL 인증서	추측 공격	무차별 대입공격	

1. 자산에서의 보안위협(기술적 보안위협)

자산에서의 보안위협(기술적 보안위협)은 사용자의 전자적 장치 중 키보드나 마우스, 출력장치와 같은 하드웨어에서의 보안위협과 설치된 운영체제나 커널에서의 보안위협, 그리고 보안 프로그램이나 암호 라이브러리와 같은 응용 프로그램에서의 보안위협을 의미하며, 하드웨어에서의 보안위협, 소프트웨어에서의 보안위협으로 분류된다.

1) 하드웨어에서의 보안위협

하드웨어에서의 보안위협은 스마트카드의 복제와 같은 문제점이나 OTP 생성기와 하드웨어 보안토큰과 같은 하드웨어 장치가 부채널 공격에 의하여 비밀정보가 노출되는 문제점, 키보드와 같은 입력장치나 보안 USB와 같은 저장장치와 같이 사용자의 전자적 장치에 연결된 하드웨어 장치의 취약점으로 인하여 발생하는 보안위협을 의미하며, 복제, 부채널 공격, PS/2 키보드, USB 키보드, 가상 키보드, 보안 USB, 임베디드 시스템에서의 보안위협으로 분류된다.

복제에 의한 보안위협은 스키머라는 복제장비를 이용하여 마그네틱 카드방식인 신용카드를 복제하거나 안전성이 보장된 IC(Integrated Circuit)칩 카드 내에 저장된 카드정보의 유출, 혹은 하드디스크에 저장된 비밀번호 파일이나 공인인증서 파일, 보안카드 복사본을 복제하거나 일반적으로 복제가 불가능하다고 알려진 하드웨어 보안토큰의 복제로 인하여 발생하는 취약점이다. 이와 같은 취약점으로 인하여 지식기반이나 소지기반의 본인확인수단의 안전성을 확보하지 못하는 보안위협이 존재한다(심희원, 2011; 이형익, 2010).

부채널 공격에 의한 보안위협은 암호 알고리즘이나 비밀키가 외부로 유출되지 않는 스마트카드나 하드웨어 보안토큰과 같은 하드웨어 장치가 동작할 때의 전기 소모량이나 전자 신호량, 열, 소요시간과 같은 부가적인 정보를 이용하는 전력차 분석이나 전자기 분석, 혹은 오류를 주입하는 오류 주입공격으로 암호 알고리즘이나 비밀키가 유출되는 보안위협이다(심희원, 2011; 성재모, 2011; 김창균 · 박일환, 2008).

PS/2 키보드에서의 보안위협은 입력장치 중 하나인 PS/2 키보드를 통하여 입력되는 정보가 노출됨으로써 발생하는 취약점이다. 기존의 PS/2 키보드에서 발생하는 취약점은 하드웨어나 커널에서 발생하는 취약점보다 응용 프로그램에서 발생하는 취약점이 대다수이며, 하드웨어와 커널 및 운영체제, 응용 프로그램에서의 보안위협으로 분류된다.

하드웨어에서의 PS/2 키보드 보안위협은 PS/2 인터페이스의 입/출력 포트 주소인 0x60과 0x64 포트를 감시하여 입력되는 키보드 정보를 탈취함으로써 발생하는 취약점이다. 이와 같은 취약점이 발생하는 원인은 입/출력 포트에 저장된 데이터가 키보드를 입력하기 전이나 다른 데이터로 갱신되기 전까지 그대로 유지되기 때문이며, 이를 제어하기 위한 기능을 제공하지 않기 때문에 발생한다(이재식, 2013; 이원철 외, 2005; 장우석 외, 2005; 금융보안연구원, 2007b; 이재익, 2008; 강신범 · 정현철, 2005).

커널 및 운영체제에서의 PS/2 키보드 보안위협은 인터럽트를 처리하는 테이블을 후킹하거나 대체하는 공격, 키보드 인터럽트를 처리하는 핸들러를 후킹하거나 대체하는 공격, 키보드 드라이버를 후킹하는 공격, 필터 드라이버를 삽입하는 공격으로 분류된다.

키보드가 입력되면 키보드에 해당하는 인터럽트가 발생하며, 인터럽트 디스크립터 테이블(IDT, Interrupt Descriptor Table)의 키보드 인터럽트에 해당하는 테이블을 참조하여 인터럽트 서비스 루틴(ISR, Interrupt Service Routine)을 호출함으로써 키보드 데이터를 처리한다. 따라서 키보드 인터럽트 테이블 후킹 및 대체 공격은 인터럽트 디스크립터 테이블을 공격자가 준비한 테이블로 대체하거나 후킹하여 키보드 데이터를 탈취하는 공격기술이다(이재식, 2013; 이재익, 2008).

키보드 인터럽트 핸들러 후킹 및 대체 공격은 키보드로부터 입력된 데이터를 처리하기 위하여 준비된 인터럽트 서비스 루틴과 같은 인터럽트 핸들러를 공격자

가 준비한 핸들러로 대체하거나 후킹함으로써 운영체제보다 우선순위를 선점하여 키보드 데이터를 탈취하는 공격기술이다(이원철 외, 2005; 장윤근, 2009; 맹영재 외, 2010).

키보드 드라이버 후킹 및 대체 공격은 PS/2 인터페이스를 가지는 키보드나 마우스로부터 입력되는 데이터를 처리하기 위하여 운영체제에서 동작 중인 키보드 드라이버를 공격자가 준비한 드라이버로 대체하거나 후킹함으로써 운영체제보다 우선순위를 선점하여 키보드 데이터를 탈취하는 공격기술이다(이재식, 2013; 이원철 외, 2005; 장우석 외, 2005; 금융보안연구원, 2007b; 강신범 · 정현철, 2005; 장윤근, 2009; 맹영재 외, 2010).

운영체제에서 동작하는 드라이버는 응용 프로그램에 전달하기 위하여 단계적으로 구성되며, 이와 같은 구조를 통하여 추가적인 기능을 삽입하는 것이 가능하다. 따라서 필터 드라이버 삽입 및 후킹 공격은 이와 같은 기능을 공격자가 악용함으로써 상위계층으로 전달하는 정보를 탈취하는 상위 필터 드라이버나 하위계층으로부터 전달되는 정보를 탈취하는 하위 필터 드라이버를 설치함으로써 키보드 데이터를 탈취하는 공격기술이다(금융보안연구원, 2007b; 이재익, 2008; 강신범 · 정현철, 2005).

응용 프로그램에서의 PS/2 키보드 보안위협은 키보드 메시지를 후킹하거나 악의적인 DLL의 삽입, API (Application Programming Interface) 후킹과 같은 공격으로 분류된다.

메시지 후킹 공격은 키보드가 입력될 때나 웹 브라우저와 같은 응용 프로그램에 키보드 데이터를 전달하기 위하여 발생하는 메시지인 WM_GETTEXT를 후킹하여 키보드 데이터를 탈취하거나 SetWindowsHook 함수와같이이벤트를가로채는WH_CALLWNDPROC, WH_CBT, WH_GETMESSAGE, WH_KEYBOARD, WH_KEYBOARD_LL, WM_GETTEXT를 활용하여 후킹 프로시저를 설치함으로써 키보드 데이터를 탈취하는 공격기술이다. 실제로 이와 같은 기술을 활용하여 키보드 보안 프로그램에 의하여 변형된 키보드 데이터의 패턴을 분석함으로써 정상적인 키보드 데이터를 역추적하는 연구가 진행되었다(이재익, 2008; 강신범 · 정현철, 2005).

DLL 인젝션 공격은 악의적인 기능을 수행하는 DLL을 로드하거나 대체하도록 구성하여 웹 브라우저와 같은 응용 프로그램에 전달되는 키보드 데이터를 탈취하는 공격기술이다(이재식, 2013; 맹영재 외, 2010).

DMA(Dynamic Memory Allocation) 후킹 공격은 프로그램이 실행되면서 할당하는 가상 메모리 공간인 DMA가 외부에서 접근이 가능한 취약점으로 인하여 웹 브라우저나 키보드 보안 프로그램에 존재하는 키보드 데이터를 탈취하는 공격기술이다(이재식, 2013).

API 후킹 공격은 텍스트 컨트롤에 저장된 문자열을 복사하는 GetWindowText 함수와 같이 키보드 데이터를 처리하는 API 함수를 후킹함으로써 키보드 데이터를 탈취하는 공격기술이다(이재식, 2013).

클래스 후킹 공격은 종속클래스나 슈퍼클래스와 같은 윈도우 메시지를 처리하는 클래스를 후킹함으로써 키보드 데이터를 탈취하는 공격기술이다(이원철 외, 2005; 장우석 외, 2005; 이재익, 2008).

기타 공격 기술로 웹 브라우저에서 거래정보를 입력받고 전송하는데 활용되는 MSHTML, KEYPRESS, CHANGE, SUBMIT의 취약점을 통하여 키보드 데이터를 탈취하는 공격기술이 연구되었다(이원철 외, 2005; 장우석 외, 2005).

보안 USB에서의 보안위협은 저장장치 중 하나인 보안 USB에 저장된 공인인증서나 보안카드와 같은 소지기반의 본인확인수단과 관련된 비밀정보가 노출됨으로써 발생하는 취약점이다. 보안 USB에서의 기존 보안위협은 사용자 인증을 우회하도록 운영체제나 관리 프로그램의 환경이나 설정을 변경함으로써 보안 USB 내에 저장된 비밀정보에 접근하는 취약점이며, VMWare 환경, 실행 프로세스 강제 종료, 시작 프로그램에서의 삭제, 안전모드 폴더 삭제, PC 부팅 시간차, 안전모드

부팅, 공유폴더 접근, 하드웨어 직접 접근에 의한 보안위협이 존재한다.

VMWare 환경에서의 보안위협은 VMWare가 설치된 환경에서 보안 USB 저장장치가 정상적으로 동작하지 않아 인증이 자동으로 우회되는 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

실행 프로세스 강제종료에 의한 보안위협은 보안 USB의 사용자 인증이나 암/복호와 같은 보안기능을 제공하기 위하여 설치되는 관리 프로그램을 강제로 종료시킴으로써 보안기능이 무력화되는 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

시작 프로그램에서의 삭제에 의한 보안위협은 관리 프로그램이 부팅 시 자동으로 실행되지 않도록 시작 프로그램에서 삭제함으로써 보안기능이 무력화되는 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

안전모드 폴더 삭제에 의한 보안위협은 시스템을 안전모드로 부팅한 후, 보안 USB 제품과 관련된 폴더를 변경하거나 삭제하여 다음 부팅 시 제품에서 제공하는 기능을 정상적으로 동작되지 않도록 무력화하는 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

PC 부팅 시간차에 의한 보안위협은 PC가 부팅될 경우, 관리 프로그램이 실행되기 전에 보안 USB를 삽입함으로써 내부에 저장된 데이터에 접근이 가능한 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

안전모드 부팅에 의한 보안위협은 관리 프로그램이 실행되지 않는 안전모드로 부팅함으로써 내부에 저장된 데이터에 접근이 가능한 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

공유폴더 접근에 의한 보안위협은 보안 USB 내의 폴더를 공유하도록 설정함으로써 외부의 다른 PC에서 내부에 공유된 폴더로 접근이 가능한 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

하드웨어 직접 접근에 의한 보안위협은 하드웨어를 제어하는 프로그램을 통하여 보안 USB 내부에 직접 접근함으로써 발생하는 취약점이다(이형익, 2010; 금융보안연구원, 2010b).

2) 소프트웨어에서의 보안위협

소프트웨어에서의 보안위협은 운영체제 및 커널에서의 보안위협, 응용 프로그램에서의 보안위협으로 분류된다.

(1) 운영체제 및 커널에서의 보안위협

운영체제 및 커널에서의 보안위협은 종단 간 암호화에 적용된 키보드 보안 프로그램과 PKI 응용 프로그램의 연동과정에서 발생하는 취약점이나 역공학, 후킹, 메모리 해킹과 같이 커널이나 운영체제의 취약점으로 인하여 발생하는 보안위협을 의미하며, 대부분 응용 프로그램에서의 보안위협과 비슷하므로 생략한다.

(2) 응용 프로그램에서의 보안위협

응용 프로그램에서의 보안위협은 인터넷 익스플로러가 가지는 취약점이나 암호기능을 제공하는 암호 라이브러리, 혹은 웹 서비스가 가지는 취약점으로 인하여 거래정보나 비밀번호의 노출 및 불법이체가 발생하는 보안위협을 의미하며, 세션 탈취, 중간자 공격, 재전송 공격, 위장, 인젝션, 역공학, 후킹, 메모리 해킹, 종단 간 암호화, activeX, MITB(Man-In-The-Browser) 공격, 플래시, 암호 라이브러리에 의한 보안위협으로 분류된다.

세션 탈취에 의한 보안위협은 네트워크 구간에서의 보안위협이지만, 사용자 구간에서의 보안위협에도 속하며, 서버와 클라이언트 사이에 맺어진 세션을 탈취하여 전송되는 정보를 분석함으로써 비밀정보를 획득하거나 서버나 클라이언트로 위장함으로써 접근권한의 탈취가 가능한 보안위협이다(심희원, 2011; 조혜숙 외, 2010; 이재식, 2013).

중간자 공격에 의한 보안위협은 공격자가 서버와 클라이언트 사이에 위치하여 전송되는 정보의 도청이 가능할 뿐만 아니라 조작이 가능한 보안위협이다. 이와 같은 보안위협은 상호인증을 제공함으로써 대응이 가능하므로(Opplinger, et al., 2009) 대부분 서버 인증은 제공하지만, 사용자 인증을 제공하지 않거나 TLS의

취약점으로 인한 보안위협이 존재한다(심희원, 2011; Asokan, et al., 2005; Callegati, et al., 2003).

재전송 공격에 의한 보안위협은 인증정보나 인증정보를 생성하는 과정에서의 중간 값 등을 재전송하여 인증을 우회함으로써 발생하는 취약점이다. 도청 공격의 경우에는 인증정보와 같은 비밀정보를 획득하여야 하지만, 재전송 공격은 프로토콜 내의 일부정보만으로도 그 목적을 달성할 수 있어 모든 인증기술에서 공통적으로 발생 가능한 보안위협이다(심희원, 2011; 조혜숙 외, 2010; 이재식, 2013).

위장에 의한 보안위협은 인터넷 뱅킹 서비스에 관여하는 개체인 사용자나 서버를 위장함으로써 인증정보와 같은 비밀정보를 탈취하는 보안위협이다. 서버에게 사용자로 위장하는 공격은 사용자를 인증하는 본인확인수단의 취약점을 활용하는 방식이므로 강인한 본인확인수단을 적용할 경우에는 위장에 의한 보안위협은 감소하지만, 사용자에게 서버로 위장하는 공격은 본인확인수단의 취약점을 활용할 뿐만 아니라 피싱이나 파밍과 같이 사용자를 속이거나 사회공학적인 방법을 함께 활용할 경우에는 대응하기가 어려워 매우 심각하다(Knight, 2005; Larcom & Elbirt, 2006). 이와 같은 보안위협은 금융기관을 사칭하는 이메일을 발송하여 비밀정보를 입력하도록 하거나 DNS(Domain Name System/Server) 주소를 변조함으로써 자동으로 공격자가 제공하는 사이트로 접속하는 방법, 혹은 친구나 가족과 같이 친분이 있거나 은행직원과 같이 신뢰된 사람으로 위장하여 사용자 스스로 비밀정보를 제공하는 방법을 활용하며, 대표적인 공격으로 피싱과 파밍이 있다(심희원, 2011; 조혜숙 외, 2010).

피싱은 금융기관과 같이 신뢰할 수 있는 기관을 사칭하여 공격자의 웹 서버로 접속하는 링크가 포함된 이메일을 발송하고, 링크를 통하여 공격자의 웹 서버로 접속하는 사용자 PC에 악성코드를 설치하거나 금융기관에서 제공하는 사이트와 비슷하게 구성하여 인증정보와 같은 비밀정보를 탈취하는 공격이다. 이와 같은 공격이 가능한 이유는 사용자가 직관적으로 탐지하기 어렵도록 비슷한 주소를 이용하거나 웹 브라우저나 outlook 프로그램의 취약점을 기반으로 공격자의 주소를 금융기관의 주소로 변경하는 것과 같은 방법을 활용하기 때문이다. 이러한 피싱 사이트는 금융 사이트의 메인화면을 이미지로 저장하여 링크를 추가하는 방식인 캡처 이미지 사용방식, iframe 태그를 활용하여 금융 사이트 메인화면을 삽입하고 특정 부분에 비밀정보를 요구하도록 링크를 삽입하는 iframe 태그를 이용한 방식, 금융 사이트의 소스를 복사하고 이를 수정하는 방식, 신뢰할 수 있는 기관을 사칭한 팝업을 출력하는 방식, 자동화 도구를 이용한 방식으로 구축된다. 피싱은 초기에 이메일을 불특정 다수에게 전송하는 방식이었으나 타인의 메신저 아이디를 도용하여 지인인 것처럼 속이거나 악성코드와 결합한 메신저 피싱, 진짜 트위터와 비슷하게 구현한 가짜 트위터를 개설하여 인증정보를 탈취하는 트위터 피싱, 스마트폰의 분실 및 도난으로 새로운 계정을 생성할 때 이전 계정을 삭제하지 않음으로써 지인을 사칭하는 카카오톡 피싱으로 발전하였다(이수미 · 성재모, 2011; 성재모, 2011; 이형익, 2010; 이재식, 2013; 금융보안연구원, 2007a; 장우석 외, 2005; 강신범 · 정현철, 2005; 금융보안연구원, 2010b; 정순채, 2012; 금융보안연구원, 2011; 금융보안연구원, 2012).

파밍은 DNS 주소나 프락시 서버의 주소, 호스트파일의 변조에 의하여 정상적인 금융기관의 웹 사이트에 접속하더라도 강제로 공격자가 구축한 가짜 사이트로 접속되도록 유도함으로써 비밀정보를 탈취하는 공격이다. 파밍의 경우에는 피싱과는 다르게 웹 브라우저에 표시되는 주소도 정상적으로 표시되므로 사용자가 대응하기에는 매우 어렵다(이수미 · 성재모, 2011; 성재모, 2011; 이형익, 2010; 이재식, 2013; 금융보안연구원, 2007a; 금융보안연구원, 2012).

인젝션에 의한 보안위협은 악의적인 행위를 하는 DLL이나 스크립트를 삽입함으로써 비밀정보를 탈취하거나 메모리 해킹과 같은 거래내역을 조작하는 공격이 가능한 보안위협이다(조혜숙 외, 2010; 장윤근,

2009).

역공학에 의한 보안위협은 배포된 프로그램의 설계 사상이나 지식을 추출하여 취약점을 분석함으로써 암호키를 탈취하거나 유출이 가능한 보안위협을 의미한다. 이와 같은 보안위협은 PC 뿐만 아니라 스마트폰에서도 적용되는 보안위협으로 아이폰 앱의 동작을 분석하여 jailbreak를 탐지하는 기능을 우회하는 공격으로 활용이 가능하다(이수미 · 성재모, 2011; 성재모, 2011).

후킹에 의한 보안위협은 프로그램이나 운영체제가 실행하는 코드의 특정 부분을 제어하는 기술인 후킹을 활용하여 메시지나 함수의 수행을 정상적인 동작이 아닌 공격자가 원하는 행위를 수행하도록 제어함으로써 비밀정보를 탈취하거나 거래내역을 조작하는 공격이 가능한 보안위협이다. 사실 후킹은 API 함수 호출을 제어하여 리소스 누출과 같은 문제점을 발견하는 API 함수 감시, 운영체제나 프로그램의 동작과정을 분석하기 위한 디버깅과 역공학, 기존의 기능을 확장시킬 수 있는 긍정적인 목적으로 제공되었지만, 이를 공격자가 활용하면서 악의적인 목적을 달성하는 부정적인 측면이 존재한다. 일반적으로 후킹은 악의적인 목적을 가진 DLL을 레지스트리에 등록하거나 윈도우즈 후킹, CreateRemoteThread 함수를 활용하여 다른 프로세스로 침투시킨 후, 윈도우즈 프로시저를 새롭게 구현하여 변경이 가능한 윈도우즈 서브클래싱, 정상적인 DLL을 악의적인 DLL로 대체하는 Proxy DLL, 악의적인 함수로 분기하는 코드 덮어쓰기와 IAT(Import Address Table) 변경을 통하여 시스템 메시지나 스레드 메시지를 후킹하여 메시지가 전송될 때 정보의 탈취 및 전송의 방해, activeX 기술의 기반기술인 객체간 데이터 전송을 위한 프로그램 모델, 즉, COM(Component Object Model)을 후킹하여 activeX로 전송되는 정보를 탈취하거나 위/변조가 가능하다(이재식, 2013; 장윤근, 2009).

메모리 해킹에 의한 보안위협은 인증정보나 거래정보를 포함하는 비밀정보가 웹 브라우저나 키보드 보안 및 종단 간 암호화를 지원하는 프로그램의 메모리에 반드시 로드되어야 하는 특징으로 인하여 발생하는 취약점으로, 공격자가 메모리에 로드된 비밀정보를 탈취하거나 위/변조함으로써 불법이체가 가능한 보안위협이다. 이와 같은 보안위협이 더욱 심각한 이유는 피싱이나 파밍과 같이 가짜 웹 사이트에서 발생하는 것이 아니라 정상적인 금융기관의 웹 사이트에 접속하더라도 발생하며, 실시간으로 공격이 가능할 뿐만 아니라 보안카드나 OTP 생성기와 같이 강인한 본인확인수단을 활용하더라도 무력화되기 때문이다(강병탁, 2016; 이수미 · 성재모, 2011; 성재모, 2011; 이재식, 2013; 이한욱 · 신휴근, 2013; 황소연, 2008; 이재익, 2008; 장윤근, 2009; 금융보안연구원, 2014).

종단 간 암호화에서의 보안위협은 키보드 보안 프로그램과 PKI 응용 프로그램이 동작 중이더라도 보호하지 못하는 구간이 존재함으로써 발생하는 보안위협이다. 이와 같은 보안위협은 WM_GETTEXT와 같은 질의 메시지를 전송하여 웹 브라우저에 입력된 정보를 외부에서 수신하거나, 공개된 BHO(Browser Helper Object)나 DOM(Document Object Model) 객체를 통하여 입력된 데이터나 속성, 이벤트와 같은 다양한 요소가 외부에서 접근이 가능함으로써 발생한다. 특히, 키보드 보안 프로그램과 PKI 응용 프로그램의 연동을 위하여 내부에서 암/복호를 수행하기 때문에 평문구간이 존재하고, activeX 기반으로 구성된 IUnknown 속성을 가진 데이터 처리함수로 인하여 외부에서 접근이 가능한 문제점, 모듈 간 데이터를 암/복호하는 키가 고정된 정보로 사용됨으로써 암호문에 대한 평문공격이 가능한 문제점, 안전하지 않은 키를 사용함으로써 키를 유추할 수 있는 문제점, 모듈의 신뢰성을 검증하지 않음으로써 입력되는 정보가 악의적인 모듈로 전송되는 문제점이 있다(성재모, 2011; 조창현, 2010; 김영환 외, 2006; 금융보안연구원, 2007b; 한국정보통신기술협회, 2011).

ActiveX에서의 보안위협은 인터넷 뱅킹 서비스에서 제공하는 보안 프로그램이 activeX 기반으로 구성됨으로써 발생하는 보안위협이다. ActiveX는 개발과

사용이 편리한 이점을 제공하지만, 악의적인 행위를 수행하는 설치파일을 다운로드하도록 조작하거나 사용자 PC에 접근이 가능한 취약한 함수를 사용함으로써 악성코드 배포, 윈도우즈 비디오 스트리밍 취약점과 같은 자체적인 취약점, 구현상의 취약점, IUnknown 함수 후킹이나 XMLHTTP 함수 후킹과 같은 COM 후킹의 취약점으로 인하여 보안위협이 발생한다(황소연, 2008; 이재익, 2008; 박성용·문종섭, 2009).

MITB 공격에 의한 보안위협은 웹 브라우저 중간자 공격이라 불리는 웹 페이지를 조작하여 인증정보나 거래정보를 포함하는 비밀정보를 탈취하거나 위/변조하는 보안위협이다. 이와 같은 보안위협이 발생하는 이유는 로그인이나 이체화면이 보안성을 제공하지 않는 HTML(HyperText Markup Language)로 구성되어 네트워크 구간에서 암호화를 적용하더라도 웹 브라우저에 출력될 때에는 원문으로 복호되기 때문에 외부에서 수정이 가능하다. 이와 같은 문제점으로 인하여 DOM 개체를 삽입하여 이체계좌번호나 금액에 해당하는 HTML 문서를 공격자가 원하는 정보로 직접 수정하거나 공격자가 제작한 악의적인 문서로 덮어씌워 사용자를 속이는 행위가 가능하다. 더욱 심각한 문제점은 보안카드나 OTP 생성기와 같은 보안성이 높은 본인확인수단을 활용하더라도 이러한 정보가 사용자에 의하여 입력되기 때문에 거래정보를 확인할 수 없는 모든 본인확인수단이 무력화된다(이수미·성재모, 2011; 성재모, 2011; 이재익, 2008; 맹영재 외, 2010).

플래시에서의 보안위협은 HTML과 같이 기존의 정적이고 수동적인 웹에서의 환경에 보안기능과 연동이 가능한 플래시 기술(FLASH 혹은 FLEX 기술)을 적용함으로써 발생하는 보안위협이다. 이와 같은 보안위협은 플래시를 디컴파일하거나 디스어셈블이 가능하고 취약점을 분석하는 스캐너에 의하여 소스코드에 하드코딩된 민감한 정보나 설정파일과 같은 중요파일이 노출되거나, 동작과정을 분석함으로써 악의적인 기능을 삽입하여 재배포하는 취약점으로 인하여 발생된다(금융보안연구원, 2009).

암호 라이브러리에서의 보안위협은 인증정보나 거래정보와 같은 비밀정보를 보호하기 위하여 활용되는 해쉬나 암/복호 알고리즘과 같이 암호기능을 제공하는 라이브러리에서 후킹과 같은 공격에 의하여 비밀정보나 키가 노출되는 보안위협이다.

2. 업무 프로세스에서의 보안위협

업무 프로세스에서의 보안위협은 서비스 구현/설정 단계에서의 보안위협(관리적 보안위협), 서비스 이용 단계에서의 보안위협(구조적 보안위협)으로 분류된다.

1) 서비스 구현/설정 단계에서의 보안위협(관리적 보안위협)

서비스 구현/설정 단계에서의 보안위협(관리적 보안위협)은 보안 프로그램의 관리자나 개발자에 의하여 취약한 보안 기능을 사용하거나 구현상의 실수로 인하여 발생하는 보안위협이나 사용자가 자신의 전자적 장치에 대한 설정이나 보안 업데이트를 하지 않거나 비밀번호 및 공인인증서와 같은 비밀정보가 공개된 장소에 노출되어 쉽게 유출되는 것과 같은 사용자의 부주의로 인하여 발생하는 보안위협을 의미하며, 개발자(구현 관점)에서의 보안위협, 관리자 (설정 및 관리 관점)에서의 보안위협, 이용자(행동학적 관점)에서의 보안위협으로 분류된다.

(1) 개발자(구현 관점)에서의 보안위협

개발자(구현 관점)에서의 보안위협은 보안 프로그램 개발자의 실수, 혹은 미숙하거나 잘못된 구현으로 인하여 발생하는 보안위협을 의미하며, 연속 인증시도, 잔여정보, 평문정보 저장, 취약한 인증 및 세션, 방화벽 시스템의 결함, URL(Uniform Resource Locator) 접속제한 실패, 검증되지 않은 리다이렉트와 포워드에 의한 보안위협으로 분류된다.

연속 인증시도에 의한 보안위협은 비밀번호나 암호문, 혹은 해쉬 값에 대한 평문을 복구하기 위하여 복호

키나 평문을 무차별적으로 대입하는 공격이다. 이와 같은 공격은 암호 알고리즘과 키의 복잡도에 따라 공격 성공률이 결정된다. 비밀번호의 경우에는 영문과 숫자, 그리고 특수문자의 조합으로 구성되므로 비밀번호가 n자리를 가진다면 $1/(26+10+33)^n \times 100\%$의 공격 성공 확률을 가지며, 복호키나 해쉬 값의 경우에는 n비트를 가진다면 $1/2^n \times 100\%$의 공격 성공 확률을 가진다. 즉, 비밀번호가 10자리일 경우에는 $1/69^{10} \times 100\%$, 키 길이가 2048비트일 경우에는 $1/2^{2048} \times 100\%$, 해쉬 값의 길이가 256비트일 경우에는 $1/2^{256} \times 100\%$의 공격 성공 확률을 가진다는 의미이다. MD5(Message Digest algorithm 5) 알고리즘을 통하여 생성된 해쉬 값의 경우에는 인텔 2.66GHz의 사양을 가지는 보급형 PC에서 약 1천만번 연산을 수행하는데 2.8초가 소요되어 초당 3,571,428.6번의 연산이 가능하므로 약 219시간 내에 평문을 구할 수 있다. 소문자와 숫자 8자리로 구성된 비밀번호의 경우에는 9일이 소요되고, 특수문자를 포함할 경우에는 1,665일, 대문자를 포함할 경우에는 21,500일이 소요된다. 비밀번호를 10자리로 늘린다면 숫자와 소문자로만 구성하여도 11,849일이 소요되지만 6자리로 구성할 경우에는 소문자와 대문자, 숫자, 특수문자를 모두 사용하여도 3일 15시간이 소요될 만큼 무차별 대입 공격에 취약하다(조혜숙 외, 2010; 이재식, 2013; 이영실, 2010; 이정호, 2008; 신동휘, 2007).

잔여정보에 의한 보안위협은 할당된 비밀정보의 사용이 완료된 후에도 해제하지 않아 공격자나 인가된 사용자가 이를 획득하여 악용하는 취약점이다. 이와 같은 취약점으로 인하여 비밀정보가 노출되거나 탈취되어 악의적인 행위가 가능한 취약점이다(조혜숙 외, 2010).

평문정보 저장에 의한 보안위협은 암호화나 해쉬연산과 같이 평문을 추출할 수 없도록 변형시켜 저장되어야 하는 암/복호키나 비밀번호 등과 같은 비밀정보를 평문으로 저장함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 비밀정보가 노출되어 본인확인수단을 우회하거나 불법이체가 가능한 보안위협이 존재한다(조혜숙 외, 2010).

취약한 인증 및 세션에 의한 보안위협은 구현상의 취약점으로 인하여 인증이나 세션을 우회하거나 권한을 탈취함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 권한이 없는 공격자가 서비스를 정상적으로 이용하여 악의적인 행위가 가능한 보안위협이 존재한다(조혜숙 외, 2010).

방화벽 시스템이 결함을 가질 경우에는 외부에서 침입이 가능하거나 내부에서 외부로 정보를 유출하는 것이 가능하다. 이러한 결함은 제품 자체가 취약점을 가지거나 설치 중 혹은 외부 공격자에 의하여 발생할 수 있다. 이와 같은 취약점으로 인하여 권한이 없는 공격자가 사용자의 전자적 장치에 접근하거나 비밀정보의 유출이 가능한 보안위협이 존재한다(백명한, 1998).

URL 접속제한 실패에 의한 보안위협은 구현이나 설정 시, URL 접속권한이나 제한을 점검하지 않음으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 악의적인 사이트로 접속하여 악성코드를 설치하는 것과 같은 보안위협이 존재한다(조혜숙 외, 2010).

검증되지 않은 리다이렉트와 포워드에 의한 보안위협은 피싱 사이트와 같은 악의적인 사이트로 리다이렉트하거나 포워드하는 것을 점검하지 않음으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 악의적인 사이트에 접속하여 악성코드를 설치하는 것과 같은 보안위협이 존재한다(조혜숙 외, 2010).

(2) 관리자(설정 및 관리 관점)에서의 보안위협

관리자(설정 및 관리 관점)에서의 보안위협은 보안 프로그램의 관리자나 개발자의 미숙한 관리나 설정으로 인하여 발생하는 보안위협을 의미하며, 보안 설정상의 오류, 암호기능 관리 오류, 제로데이 공격, 허술한 감사추적, 감사정보 파괴, 세션관리 미숙, 저장 데이터 훼손, 전송계층에 대한 불충분한 보호, 방화벽 시스템 관리자의 관리 미숙에 의한 보안위협으로 분류된다.

보안 설정상의 오류에 의한 보안위협은 사용자나 보안 프로그램 관리자가 보안 설정을 하지 않거나 오류로 인하여 설정되지 않음으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 권한이 없는 공격자에 의한 비밀번호와 같은 비밀정보가 노출되는 보안위협이 존재한다(조혜숙 외, 2010).

암호기능 관리 오류에 의한 보안위협은 보안 프로그램 관리자의 부적절한 관리나 구현으로 인하여 취약점이 존재하는 알고리즘을 사용하거나 암호기능을 잘못 설정하는 등으로 인하여 발생하는 취약점이다. 이와 같은 취약점으로 인하여 암/복호키와 같은 비밀정보가 노출되는 보안위협이 존재한다(조혜숙 외, 2010).

대부분의 단말에 설치되는 운영체제는 알려지지 않은 취약점을 가지고 이를 보완하기 위하여 보안 업데이트를 실시하는데, 업데이트가 완료되지 않은 단말은 취약점을 가지므로 공격자에 의한 제로데이 공격으로 권한을 탈취하는 것과 같은 보안위협이 존재한다(이재식, 2013).

허술한 감사 추적에 의한 보안위협은 공격자가 침입한 흔적이 기록된 감사 데이터를 분석하는 도구가 불충분하거나 올바르게 기록되지 않음으로써 침입 흔적이나 추적이 불가능하여 발생하는 취약점이다(백명한, 1998).

감사정보 파괴에 의한 보안위협은 공격자를 추적하기 위하여 기록된 감사정보가 공격자에 의하여 수정되거나 삭제되어 침입 흔적이나 추적이 불가능함으로써 발생하는 취약점이다(백명한, 1998).

세션관리 미숙에 의한 보안위협은 사용자가 인터넷 뱅킹 서비스와 연결된 세션을 계좌조회나 이체와 같은 거래를 실시하기 전, 세션이 올바르게 관리되는지 확인하지 않거나 일정시간 동안 요청이 없을 경우에도 세션을 종료하지 않음으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 세션 탈취나 중간자 공격과 같은 공격을 시도함으로써 사용자를 도용하여 불법적인 행위가 가능한 보안위협이다(이상진 외, 2007; 황소연, 2008).

저장 데이터 훼손에 의한 보안위협은 사용자의 전자적 장치에 저장된 데이터를 위/변조하거나 삭제하는 등의 행위로 인하여 발생하는 취약점이다. 이와 같은 취약점으로 인하여 예를 들면, 공인인증서를 다시 발급받도록 유도하여 이를 탈취하는 것과 같은 불법적인 행위가 가능한 보안위협이다(조혜숙 외, 2010).

전송계층에 대한 불충분한 보호에 의한 보안위협은 보안채널을 구성하지 않아 네트워크상에 데이터가 평문으로 전송되거나 보안성이 상대적으로 약한 알고리즘을 사용하여 비밀정보가 노출됨으로써 발생하는 취약점이다(조혜숙 외, 2010).

방화벽 시스템 관리자의 관리 미숙에 의한 보안위협은 방화벽의 접근제어 규칙이나 감사정보의 모니터링, 로깅정보 등이 관리자의 부주의나 관리 미숙으로 인하여 부적절하게 사용됨으로써 발생하는 취약점이다(백명한, 1998).

(3) 이용자(행동학적 관점)에서의 보안위협

이용자(행동학적 관점)에서의 보안위협은 보안 프로그램 관리자나 개발자가 알려진 취약점에 근본적인 대응을 하지 않거나 사용자가 비밀번호를 공개된 장소에 노출시키는 것과 같은 취약점으로 인하여 발생하는 보안위협을 의미하며, 사용자 부주의, 사고 발생 후 조치에 의한 보안위협으로 분류된다.

사용자 부주의에 의한 보안위협은 사용자가 주의를 기울이지 않고 확연히 구분이 가능한 상황에서 악성코드를 설치하거나 보안카드나 공인인증서와 같이 유출되지 않아야 하는 비밀정보를 타인과 공유하거나 하드디스크나 이메일, 혹은 웹하드와 같이 보안이 취약한 장소에 저장하는 행위, 그리고 보안카드나 OTP 생성기와 같은 소지기반 본인확인수단을 분실하거나 보안 프로그램의 미설치, 비밀번호를 메모하는 것과 같은 행위로 인하여 발생하는 취약점이다. 이와 같은 취약점으로 인하여 공격자는 상대적으로 공격이 쉬운 웹사이트나 웹 메일 등을 공격하여 비밀정보를 탈취함으로써 정상적인 사용자로 위장하는 것과 같은 불법적인

행위가 가능한 보안위협이다(이수미 · 성재모, 2011; 성재모, 2011; 이형익, 2010).

사고 발생 후 조치에 의한 보안위협은 보안 프로그램의 잘못된 설계나 구현 등이 가지는 취약점으로 인하여 발생한 사고를 대응함에 있어 근본적으로 발생하는 취약점을 완전히 보완하지 않고 서비스를 빠른 시일 내에 정상화하기 위하여 취약점을 부분적으로 해결함으로써 발생하는 보안위협이다(이상진 외, 2007; 황소연, 2008).

2) 서비스 이용 단계에서의 보안위협(구조적 보안위협)

서비스 이용 단계에서의 보안위협(구조적 보안위협)은 사용자의 전자적 장치인 플랫폼의 특권수준 등으로 인하여 발생하는 보안위협이나 거래부인, 위조와 같이 거래 자체의 문제점으로 인하여 발생하는 보안위협, 본인확인수단을 이용한 사용자 인증의 구조적인 문제점으로 인하여 발생하는 보안위협, 보안 프로그램의 구성이나 구조적인 문제점으로 인하여 발생하는 보안위협을 의미하며, 플랫폼(플랫폼 관점)에서의 보안위협, 보안 프로그램(방어자 관점)에서의 보안위협, 사용자 이용(거래 및 인증 관점)에서의 보안위협으로 분류된다.

(1) 플랫폼(플랫폼 관점)에서의 보안위협

플랫폼(플랫폼 관점)에서의 보안위협은 링0나 링3와 같은 특권수준이 가지는 한계점으로 인하여 발생하는 보안위협을 의미하며, 특권수준, 입력 유효성 공격, 파일 시스템 조작, 프로세스 조작, 어플리케이션 조작, 매개변수 조작, 전송 데이터 훼손, 악성코드, 안전하지 않은 직접 객체 참조에 의한 보안위협으로 분류된다.

사용자의 전자적 장치에서 중앙처리장치(CPU, Central Processing Unit)가 준비한 링0, 링1, 링2, 링3인 4가지의 특권수준을 운영체제에서 모두 활용하지 않고 링0와 링3만으로 구성함으로써 발생하는 취약점이다. 즉, 악의적인 목적을 가진 프로그램이 특권수준이 낮은 링3의 특권수준을 가진다면 특권수준이 높은 링0에서 대응이 가능하지만, 운영체제와 동일한 링0의 특권수준을 가진다면 이를 대응하기에는 한계가 있다. 이와 같은 취약점으로 인하여 키보드와 같은 하드웨어 장치로부터 전송되는 비밀번호 등의 비밀정보를 탈취하는 것과 같은 악의적인 행위가 가능한 보안위협이다.

입력 유효성 공격에 의한 보안위협은 버퍼 오버플로우와 같은 공격으로 사용자의 전자적 장치에 대한 권한을 탈취하거나 프로그램에 혼돈을 유발함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 사용자의 전자적 장치가 공격자에게 장악되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

파일 시스템 조작에 의한 보안위협은 보안 프로그램이 설치된 파일 시스템을 조작하여 보안 기능을 우회함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 보안 프로그램이 정상적으로 동작하지 않아 사용자의 인증정보나 계좌정보 등의 비밀정보가 노출되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

프로세스 조작에 의한 보안위협은 보안 프로그램의 프로세스를 조작하여 보안 기능을 우회함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 보안 프로그램이 정상적으로 동작하지 않아 사용자의 인증정보나 계좌정보 등의 비밀정보가 노출되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

어플리케이션 조작에 의한 보안위협은 역공학 기술을 활용하여 보안 프로그램의 구성이나 구조, 동작과정 등을 분석하여 보안 기능을 우회하거나 무력화시킴으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 보안 프로그램이 정상적으로 동작하지 않아 사용자의 인증정보나 계좌정보 등의 비밀정보가 노출되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

매개변수 조작에 의한 보안위협은 인터넷 뱅킹 서버에 요청할 때 입력되는 매개변수에 질의문이나 특수문

자로 구성된 공격코드를 삽입하여 전송함으로써 발생하는 취약점이다. 매개변수가 조작된 요청은 방화벽과 같은 보안 프로그램에 탐지될 수 있으므로 매개변수의 순서를 재배치하거나 인코딩, 혹은 매개변수의 삽입이나 삭제, 변경 등의 방법을 조합함으로써 쉽게 탐지되지 않으며, 감사정보를 확인하여도 공격을 탐지하는 것이 매우 어려운 문제점이 있다(이상진 외, 2007; 황소연, 2008; 박재철, 2008).

전송 데이터 훼손에 의한 보안위협은 네트워크로 전송하는 데이터를 훼손하여 정상적으로 서비스를 이용하지 못하도록 오류를 발생시키는 보안위협이다(조혜숙 외, 2010).

무엇보다 근본적인 문제점은 사용자의 전자적 장치에 자의든 타의든 악성코드가 설치되는 구조를 가지기 때문에 보안위협이 발생한다. 악성코드는 비밀정보를 탈취하거나 시스템을 파괴하는 것과 같은 행위를 수행하는 프로그램이나 매크로, 스크립트와 같은 파일을 이메일 첨부파일이나 P2P(Peer-To-Peer) 사이트 등에서 다운로드하거나 로컬 및 원격 삽입 파일(LFI/RFI, Local/Remote File Inclusion)에 취약한 코드로 인하여 삽입되어 시스템이 공격자에게 장악됨으로써 발생하는 보안위협이다(조혜숙 외, 2010; 이형익, 2010; 박재철, 2008; 금융보안연구원, 2007a).

안전하지 않은 직접 객체 참조에 의한 보안위협은 보안 프로그램의 파일이나 디렉터리, 데이터베이스 기록, 키와 같이 내부에 구현된 객체에 대한 참조가 URI(Uniform Resource Identifier)나 폼 매개변수에 노출됨으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 보호되어야 하는 비밀정보가 제3자로부터의 접근을 통제하지 못하여 탈취되는 보안위협이다(조혜숙 외, 2010; 박재철, 2008).

(2) 보안 프로그램(방어자 관점)에서의 보안위협

보안 프로그램(방어자 관점)에서의 보안위협은 사용자의 전자적 장치나 인증수단의 안전성을 확보하기 위하여 설치되는 보안 프로그램이 개별적으로 구현되는 구조적인 문제점이나 이를 보호하는 프로그램의 부재 등의 취약점으로 인하여 발생하는 보안위협을 의미하며, 보안 프로그램의 부분적용, 보안 프로그램의 개별화, 보안 프로그램 무력화, 서비스 구조의 문제점, 암호기능 무력화, 보안 프로그램의 의존적 운영, 보안 프로그램을 위한 프로그램의 부재에 의한 보안위협으로 분류된다.

보안 프로그램의 부분적용에 의한 보안위협은 인터넷 뱅킹 서비스의 전 단계에 걸쳐 적용되어야 할 보안기능이 프로세스 단계에 부분적으로 적용됨으로써 발생하는 취약점이다. 예를 들어 로그인 단계에는 PKI 응용 프로그램이 동작하여 안전성을 확보하지만, 계좌이체 단계에서 적용되지 않아 비밀번호가 노출되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

보안 프로그램의 개별화에 의한 보안위협은 안전성을 보장하기 위하여 적용된 키보드 보안 프로그램과 PKI 응용 프로그램, 해킹 방지 프로그램 등과 같은 보안 프로그램이 제조사마다 상이하게 구현되어 상호간에 연동이 제한되며, 이로 인하여 보호되지 않는 구간이 발생하거나 연동되는 부분의 결함에 의하여 발생하는 보안위협이다(이상진 외, 2007; 황소연, 2008).

보안 프로그램 무력화에 의한 보안위협은 설치된 보안 프로그램이 동작되지 않도록 추가기능 관리항목을 통하여 사용을 중지하거나 역공학을 통하여 보안 프로그램의 동작여부를 확인하는 코드를 nop와 같은 의미가 없는 명령어로 대체하거나 jmp 명령어로 우회하도록 수정하는 방법, 혹은 보안 프로그램이 가지는 자체적인 취약점을 통하여 보안 프로그램을 무력화함으로써 발생하는 보안위협이다(황소연, 2008).

서비스 구조의 문제점에 의한 보안위협은 서비스를 제공하는 구간 중 하나라도 취약점이 발생하는 경우에는 서비스 전체가 위협에 노출되는 문제점이다. 이는 공격자가 취약한 부분만을 공격하므로 서비스 전체가 보안위협이 존재하는 결과를 초래한다(이재식, 2013).

암호기능 무력화에 의한 보안위협은 보안 프로그램

의 구성상 암호화된 데이터를 복호화하기 위한 복호모듈이 존재하는데, 공격자가 이를 악용하여 암호문을 복호모듈에 강제로 삽입하여 평문을 추출함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 암호기능이 무력화되어 비밀정보가 노출되는 것과 같은 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

보안 프로그램의 의존적 운영에 의한 보안위협은 인터넷 뱅킹 서비스의 안전성이 사용자의 전자적 장치에 설치된 보안 프로그램에 의존적이기 때문에 발생하는 문제점, 예를 들어, 거래정보가 연동되지 않는 구조로 인하여 사용자나 금융기관에서 위/변조와 같은 악의적인 행위를 확인할 수 없는 문제점이 발생하는 취약점이다. 이와 같은 취약점으로 인하여 메모리 해킹과 같은 불법이체가 가능한 보안위협이 존재한다(황소연, 2008).

인터넷 뱅킹 서비스에서의 안전성은 설치되는 보안 프로그램에 의존적이기 때문에 보안 프로그램을 위한 프로그램의 부재에 의한 보안위협은 프로세스 인젝션이나 DLL(Dynamic Linking Library) 인젝션과 같은 공격으로 보안 프로그램을 무력화함으로써 발생하는 취약점이다. 이는 보안 프로그램 자체를 보호하기 위한 프로그램이 존재하지 않기 때문에 발생하는 문제점이며, 이로 인하여 사용자의 전자적 장치가 공격자에게 장악될 경우에는 안전성을 확보할 수 없는 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

(3) 사용자 이용(거래 관점)에서의 보안위협

사용자 이용(거래 관점)에서의 보안위협은 사용자가 서비스를 이용하는 단계인 거래 관점에서의 보안위협, 인증 관점에서의 보안위협으로 분류된다.

거래 관점에서의 보안위협은 사용자나 금융기관에서 승인된 거래를 부인하거나 제3자에 의하여 거래를 방해하거나 거래정보를 위조하는 등의 문제점으로 인하여 발생하는 보안위협을 의미하며, 거래부인, 거래방해, 거래정보 위/변조, 민감한 정보에 의한 보안위협으로 분류된다.

거래부인에 의한 보안위협은 사용자나 금융기관에서 승인한 거래사실을 부인하는 것을 입증하지 못함으로써 발생하는 취약점이다. 금융기관은 사용자가 승인한 거래를 부정할 경우, 사용자가 보상을 목적으로 의도한 것인지, 공격자에 의하여 부정적으로 요청된 것인지 검증하기 어려우며, 사용자는 금융기관에서 부정적으로 승인된 거래를 검증하기 어렵다. 이와 같은 취약점이 발생하게 된 원인은 거래내역이 금융기관에만 저장되기 때문이며(Schneier & Kelsey, 1998), 이를 보완하기 위하여 Bank ID 기반의 거래부인 방지기술이 연구되었으나, 이 역시 Bank ID 서버가 사용자를 대신하여 서명을 수행하므로 공정하지 않은 방법이다(Hole, et al., 2006; Hole, et al., 2009). 따라서 이와 같은 취약점으로 인하여 거래부인을 방지하지 못함으로써 부정이체가 가능한 보안위협이 존재한다(심희원, 2011).

거래방해에 의한 보안위협은 사용자의 전자적 장치를 파괴하거나 네트워크를 절단하는 등의 방법으로 서비스를 이용할 수 없도록 방해하는 보안위협이다(백명한, 1998).

거래정보 위/변조에 의한 보안위협은 사용자가 요청하는 거래내역이 제3자에 의하여 위/변조됨으로써 불법이체가 발생하는 보안위협이다(조혜숙 외, 2010; 백명한, 1998).

민감한 정보에 의한 보안위협은 인터넷 뱅킹 서비스의 구조적인 특성상 인증정보나 계좌정보와 같은 비밀정보가 반드시 필요하지만, 이를 완벽하게 보호하기에는 한계가 있으므로 유출에 의하여 발생되는 보안위협이 존재한다(이상진 외, 2007; 황소연, 2008).

인증 관점에서의 보안위협은 본인확인수단 중 보안카드나 OTP 생성기와 같이 소지기반의 본인확인수단을 도난당하거나 고정 비밀번호와 같이 지식기반의 본인확인수단을 훔쳐보는 것과 같은 취약점으로 인하여 발생하는 보안위협을 의미하며, 인증수단의 문제점, 훔쳐보기, 도난, 가짜 SSL 인증서, 추측공격, 무차별 대입 공격에 의한 보안위협으로 분류된다.

비밀번호와 같은 지식기반의 본인확인수단의 경우, 한 번 노출되면 안전성을 보장할 수 없고, 보안카드나 OTP 생성기와 같은 소지기반 본인확인수단의 경우에는 분실이나 복제 등으로 인하여 안전성을 보장할 수 없으며, 바이오 인증과 같은 특징기반 본인확인수단의 경우에는 안전한 인증채널을 구성하기 어려운 문제점이 존재한다. 또한, 본인확인수단이 안전하더라도 중간자 공격이나 메모리해킹과 같은 공격으로 거래내역의 조작이 가능한 보안위협이 존재한다(이재식, 2013).

훔쳐보기에 의한 보안위협은 비밀번호와 같은 지식기반의 본인확인수단을 활용할 경우, 어깨너머공격과 같이 입력정보를 훔쳐봄으로써 비밀정보를 탈취하는 취약점이다. 이와 같은 취약점으로 인하여 카드나 통장을 획득하여 금전을 출금하는 보안위협이 존재한다(김영환 외, 2006).

도난에 의한 보안위협은 보안카드, 하드웨어 보안토큰, OTP 생성기와 같은 소기기반의 본인확인수단을 탈취함으로써 발생하는 취약점이다. 이와 같은 취약점으로 인하여 소지기반의 본인확인수단을 발급받지 않은 공격자가 정상적인 사용자로 위장되는 보안위협이 존재한다(심희원, 2011).

가짜 SSL 인증서에 의한 보안위협은 인터넷 뱅킹 서버에서 발급한 SSL 인증서가 아닌 공격자가 발급한 SSL 인증서를 이용하여 네트워크로 암호화되어 전송되는 데이터의 평문을 획득함으로써 발생하는 보안위협이다. 이와 같은 위협이 발생하는 원인은 일부 인증기관에서 발급한 인증서가 상대적으로 취약한 MD5 알고리즘을 사용하기 때문에 MD5의 취약점과 인증기관 목록을 기반으로 가짜 인증서의 생성이 가능하기 때문이다(이재식, 2013).

추측공격에 의한 보안위협은 전송되는 메시지나 인증정보, 비밀정보가 일부분을 통하여 전체 정보의 추측이 가능함으로써 발생하는 취약점이다. 일반적으로 이러한 공격은 비밀정보로부터 인증정보를 생성하는 과정에서 중간 값을 획득함으로써 완전한 인증정보나 비밀정보를 유추하는 방식으로 동작하며, 이와 같은 취약점으로 인하여 비밀정보가 유출되어 인증을 우회하는 것과 같은 보안위협이 존재한다(심희원, 2011).

무차별 대입 공격에 의한 보안위협은 구현 관점에서의 보안위협 중 연속 인증시도와 비슷하지만, 인증 횟수제한에 의하여 대응이 가능한 연속 인증시도와는 다르게 무차별 대입 공격은 횟수제한이 없어 전자적 장치의 성능과 키의 길이에 의존적인 공격 성공 확률을 가진다.

Ⅵ. 결론 및 시사점

1. 결론

온라인을 통하여 공간에 구애받지 않고 금융거래가 가능한 여건이 마련되었다. 이를 통하여 재화의 교환이 증가하여 국가 경제의 발전을 기대할 수 있었지만, 보안 취약점으로 인하여 사고가 지속적으로 발생함으로써 신뢰성을 보장하지 못하는 문제점이 존재한다. 따라서 인터넷 뱅킹 서비스를 중심으로 발생 가능한 보안 취약점을 분석함으로써 보안 위협을 도출하는 연구가 필요하며, 이를 통하여 보안 요구사항을 정의하기 위한 연구가 선행되어야 한다. 이에 본 논문에서는 인터넷 뱅킹 서비스의 전반적인 구조를 분석하여 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하였으며, 구조에 따른 영역별 보안위협을 도출함으로써 보안 요구사항을 정의하기 위한 선행 연구를 진행하였다. 특히, 사용자 구간이 상대적으로 취약하기 때문에 전체 서비스의 안전성을 확보하기 어려운 상황이므로 이를 중점적으로 분석하였다. 분석한 보안위협을 토대로 안전한 인터넷 뱅킹 서비스를 구성하기 위한 기초를 다질 것으로 예상된다.

2. 시사점

본 논문에서는 인터넷 뱅킹 서비스를 중심으로 발생 가능한 보안위협을 금융기관 구간, 네트워크 구간, 사

용자 구간으로 분류하여, 각 구간에서 발생 가능한 세부적인 보안위협을 도출하였다. 이를 자세히 살펴보면, 금융기관 구간에서는 6가지의 보안위협으로 분류되었고, 네트워크 구간에서는 5가지 보안위협으로 분류되었으며, 사용자 구간에서는 3가지의 대분류를 기반으로 10가지의 소분류, 그리고 소분류를 기반으로 65가지의 보안위협으로 분류되었다. 사용자 구간에서의 보안위협이 금융기관 구간 및 네트워크 구간에서의 보안위협보다 월등히 많음을 확인할 수 있는데, 공격자의 입장에서는 상대적으로 침입이 어려운 금융기관 구간 및 네트워크 구간보다 사용자 구간에서의 침입을 많이 시도하는 것으로 사료된다. 따라서 사용자 구간에서의 보안위협에 대응하기 위한 다양한 보안기술이 적용되어야 할 것으로 판단된다.

특히, 기술적으로 하드웨어, 운영체제 및 커널, 응용 프로그램 계층에서 발생하는 보안위협들 중 응용 프로그램 계층에서의 보안위협이 상대적으로 많은 결과가 도출되었는데, 이 역시 공격자의 입장에서는 공격을 위한 별도의 하드웨어 모듈을 구매하지 않으면서 상대적으로 접근이 용이하기 때문에 다양한 공격에 노출되는 것으로 판단된다. 하지만 방어자 입장에서는 응용 프로그램 계층에서의 위협을 낱낱이 해결할 경우에는 많은 인력 및 비용이 소모되는 결과가 초래되기 때문에 낮은 수준인 운영체제, 특히, 하드웨어 계층에서의 보안 기술을 도입하여야 할 것이다. 그 이유는 응용 프로그램 계층에서의 기능 및 동작은 하드웨어 계층으로부터 전달되거나 처리되는 과정으로부터 기인하기 때문에 낮은 계층인 하드웨어 계층에서 철저히 보안성을 확보한다면 상위 계층인 운영체제 및 커널 계층, 응용 프로그램 계층에서의 보안위협을 방지하는 것이 가능하다. 따라서 향후 새로운 기술을 도입하거나 기존의 기술을 보완하는 경우에는 설계 단계부터 이러한 문제점을 인지하고 보안성을 향상시키기 위하여 노력하여야 한다. 특히, 기존의 OTP, 전화 승인, 거래연동장치 등 별도의 하드웨어를 통하여 더욱 안전한 서비스를 제공하지만, 이러한 하드웨어로부터 생성되는 OTP값, 인증번호 등의 정보를 키보드에 입력하도록 구성되어 정보가 노출되는 문제점이 존재한다. 따라서 현재의 문제점을 보완하고 거래 및 인증정보를 안전하게 보호하기 위하여 정보가 노출되지 않도록 하드웨어부터, 혹은 하드웨어를 활용하여 서버로 안전하게 전달하기 위한 정책이 요구되며, 이러한 방안을 도입하는 경우에는 개발 단계부터 운용 단계까지 발생하는 보안위협에 대응하기 위한 정책이 마련되어야 할 것으로 사료된다.

향후 연구로는 도출된 보안위협을 기반으로 안전성을 확보하기 위한 보안 요구사항을 도출하는 연구가 진행되어야 하며, 이러한 요구사항을 토대로 안전성을 평가하기 위한 지표 및 평가방법에 대한 연구가 진행되어야 한다. 연구에 대한 결과는 인터넷 뱅킹 서비스를 포함한 전자상거래를 지원하는 모든 시스템의 안전성을 보장할 것으로 기대된다.

■ 참고문헌

강병탁 (2016). 「MITM 공격을 이용한 OTP 적용환경의 취약점 연구」. 고려대학교 정보보호대학원 석사학위논문.

강성구 · 서정택 (2012). “전기자동차 충전 인프라에서의 보안위협 및 보안요구사항 분석.” 「한국정보보호학회 학회지」, 22(5): 1027-1037.

강신범 · 정현철 (2005). “인터넷 뱅킹 해킹 유형과 대응 기술.” 「한국정보보호학회 학회지」, 15(4): 29-38.

금융보안연구원 (2007a). 「전자금융 이용자 보안가이드」. 서울: 금융보안연구원.

금융보안연구원 (2007b). 「종단간(End-to-End) 암호화 적용 가이드」. 서울: 금융보안연구원.

금융보안연구원 (2009). 「FLEX 기반 전자금융서비스 보안 기술 분석 보고서」. 서울: 금융보안연구원.

금융보안연구원 (2010a). 「금융부문 스마트폰 보안 가이드」. 서울: 금융보안연구원.

금융보안연구원 (2010b). 「정보유출 위협 및 대응방안 연구 보고서」. 서울: 금융보안연구원.

금융보안연구원 (2011). 「국내 피싱사이트 주요특징 및 대응

방안」. 2011(20). 서울: 금융보안연구원.
금융보안연구원 (2012). 「피싱사이트의 진화와 탐지」. 2012(6). 서울: 금융보안연구원.
금융보안연구원 (2014). 「전자금융환경의 거래서명 인증기술 동향 및 도입 시 고려사항」. 2014(2). 서울: 금융보안연구원.
김영환 · 김성진 · 이영록 · 노봉남 (2006). "인터넷뱅킹 클라이언트 보안 강화를 위한 새로운 마우스 이용 비밀번호 입력 기술." 「한국정보과학회 학술발표논문집」, 33(2C): 606-611.
김종기 · 전진환 (2006). "컴퓨터 바이러스 통제를 위한 보안행위의도 모형." 「정보화정책」, 13(3): 174-196.
김창균 · 박일환 (2008). "금융IC카드에 대한 부채널분석공격 취약성 분석." 「한국정보보호학회 논문지」, 18(1): 31-39.
맹영재 · 신동오 · 김성호 · 양대헌 · 이문규 (2010). "국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석." 「Internet and Information Security」, 1(2): 101-108.
박성용 · 문종섭 (2009). "보안 인증을 통한 ActiveX Control 보안 관리 모델에 관한 연구.", 「한국정보보호학회 논문지」, 19(6): 113-119.
박재철 (2008). "인터넷 뱅킹 보안을 위한 웹 공격의 탐지 및 분류." 「한국정보보호학회 학회지」, 18(5): 62-72.
백명한 (1998). 「인터넷 뱅킹 구축을 위한 보안 기술에 관한 연구」. 한양대학교 산업대학원 석사학위논문.
성재모 (2011). 「국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응체계」. 전남대학교 대학원 박사학위논문.
신동휘 · 최윤성 · 박상준 · 김승주 · 원동호 (2007). "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석." 「한국정보보호학회 논문지」, 17(2): 67-80.
심희원 (2011). 「온라인뱅킹의 확장된 상호인증 및 부인방지를 위한 거래서명 인증기술」. 전남대학교 대학원 박사학위논문.
유한나 · 이재식 · 김정재 · 박재표 · 전문석 (2011). "인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식." 「한국통신학회 논문지」, 36(8): 939-946.
이상진 · 황소연 · 김경곤 · 여성구 (2007). "인터넷 뱅킹 서비스 취약점 분석 및 보안대책." 「정보 · 보안논문지」, 7(2): 119-128.
이수미 · 성재모 (2011). "국내 전자금융 현황 및 보안위협 분류." 「한국정보보호학회 학회지」, 21(7): 53-61.
이영실 (2010). 「2차원 바코드와 스트림 암호 기반의 모바일 OTP를 활용한 온라인 뱅킹용 인증 시스템」. 동서대학교 디자인 & IT 전문대학원 석사학위논문.
이원철 · 이석래 · 이재일 · 김인석 (2005). "전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구." 「한국정보보호학회 학회지」, 15(4): 43-48.
이재식 (2013). 「안전한 인터넷 뱅킹 서비스 제공 모델 및 인증 기법 설계」. 숭실대학교 대학원 박사학위 논문.
이재익 (2008). 「전자금융거래 보안강화를 위한 종단간 암호화와 고려사항」. 성균관대학교 정보통신대학원 석사학위논문.
이정호 (2008). "전자금융 침해사고 예방 및 대응 강화 방안." 「한국정보보호학회 학회지」, 18(5): 1-20.
이태헌 (2016). "텍스트 마이닝을 이용한 정보보호인식 분석 및 강화 방안 모색." 「정보화정책」, 23(4): 76-94.
이한욱 · 신휴근 (2013). "메모리 해킹 공격에 강건한 사용자 인증수단 고찰." 「한국정보보호학회 학회지」, 23(6): 67-75.
이형익 (2010). 「부정이체 방지를 위한 실시간 IP 차단 시스템에 관한 연구」. 고려대학교 공학대학원 석사학위논문.
이형찬 · 이정현 · 손기욱 (2011). "스마트워크 보안 위협과 대책." 한국정보보호학회 학회지」, 21(3): 12-21.
장상수 (2015). "정보보호총론." 「정보보호 위험관리(Information Security Risk Management」, 403-437. 파주: 생능출판사.
장우석 · 이광우 · 최동현 · 정학 · 이병희 · 최윤성 · 김승주 · 원동호 (2005). "인터넷 뱅킹 보안." 「대한전자공학회 학회지」, 32(11): 37-50.
장윤근 (2009). 「인터넷뱅킹 사용자 입력정보의 안전성 강화를 위한 대체방안에 대한 연구」. 동국대학교 국제정보대학원 석사학위논문.
조강유 · 민상식 · 성재모 (2013). "전자금융 보안위협 관련 대응기술 연구 추진 방안." 「한국정보보호학회 학회지」, 23(6): 49-53.
조혜숙 · 김승주 · 원동호 (2010). "인터넷 뱅킹 시스템 관련 표준 분석 및 보호프로파일 개발에 관한 연구." 「한국정보처리학회 논문지」, 17-C(3): 223-232.
조창현 (2010). 「보안성이 강화된 인터넷 뱅킹 환경을 위한 이동통신 이중채널 인증 기법에 관한 연구」. 숭실대

학교 대학원 박사학위논문.
정순채 (2012).「전자금융사기 등 정보통신망 이용 금융사기 대응방안 고찰」. 경희대학교 국제법무대학원 석사학위논문.
한국정보통신기술협회 (2011).「전자금융서비스 위협 분석 및 관리 방안」, 기술보고서 TTAR-12.0008. 경기도 성남시: 한국정보통신기술협회.
홍석원 · 이명호 · 이철환 (2012). "한국형 스마트 그리드에서의 보안 위협 및 보안 요구사항."「정보과학학회 학회지」, 30(1): 66-74.
황소연 (2008).「인터넷 뱅킹 서비스 취약점 분석 및 보안대책」. 고려대학교 정보경영공학전문대학원 석사학위논문.
Asokan, N., Niemi, V. & Nyberg, K. (2005). "Man-in-the-Middle in Tunnelled Authentication Protocols." *LNCS* 3364: 28-41.
Callegati, F., Cerroni, W. & Ramilli, M. (2009). "Man-in-the-Middle Attack to the HTTP Protocol." *Journal of the IEEE Security & Privacy*, 7(1): 78-81.
Dolev, D. & Yao, A. C. (1981). "On the Security of Public Key Protocols." *Proceeding of the IEEE Ann. Sym. Foundations of Computer Science*, 350-357.
Hiltgen, A., Kramp, T. & Weigold, T. (2006). "Secure Internet Banking Authentication." *Journal of the IEEE Security & Privacy*, 4(2): 21-29.
Hole, K. J., Moen, V. & Tjostheim, T. (2006). "Case study: online banking security." *IEEE Security & Privacy*, 4(2): 14-20.
Hole, K. J., Klingsheim, A. N., Netland, L. H., Espelid, Y., Tjostheim, T. & Moen, V. (2009). "Risk Assessment of a National Security Infrastructure." *IEEE Security & Privacy*, 7(1): 34-41.
Kalige, E. & Burkey, D. (2012). "A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware." http://www.naavi.org/cl_editorial_12/Eurograbber_White_Paper.pdf. (Retrieved on Apr. 6, 2017).
Knight, W. (2005). "Caught in the net [Internet and e-mail security issues]." *IEEE Review*, 51(7): 26-30.
Larcom, G. & Elbirt, A. J. (2006). "Gone phishing." *IEEE Technology and Society Magazine*, 25(3): 52-55.
Opplinger, R., Rytz, R. & Holderegger, T. (2009). "Internet Banking: Client-Side Attacks and Protection Mechanism." *Journal of the IEEE Computer*, 42(6): 27-33.
Schneier, B. & Kelsey, J. (1998). "Cryptographic Support for Secure Logs on Untrusted Machines." *Proceedings of the USENIX Security Symposium*: 53-62.