인터넷 뱅킹 서비스 취약점 분석 및 보안대책*

이상진** · 황소연*** · 김경곤**** · 여성구*****

요 약

1999년 인터넷 뱅킹 서비스가 국내에 처음 도입된 이후 다수의 사용자들에게 인터넷 뱅킹 서비스는 없어서는 안 될 중요한 서비스로 자리 매김하게 되었다. 인터넷 사용자에게 편리함을 제공하는 것은 물론 은행 업무의 효율성을 가져다준 인터넷 뱅킹은 그 중요성이 더욱더 커져갈 것이다. 이로 인해 인터넷 뱅킹을 악용하는 사례가 발생하고 있으며, 특히 컴퓨터 해킹을 통해서 불법적 계좌 이체를 하거나 사용자 정보를 도용하는 등 그 피해의 유형 및 규모가 점점 증가하고 있는 추세이다. 본 논문은 인터넷 뱅킹 서비스를 구성하고 있는 전체적인 요소들(Components)을 분석하고 서비스 흐름(Service Flow)에 따른 해킹 위협을 구조적으로 분석한다. 이를 통하여 현 인터넷 뱅킹 서비스의 근본적인 문제점을 지적하고 인터넷 뱅킹 서비스의 해킹 위협을 최소화하기 위한 방안을 제시하고자 한다.

Internet Banking Service Vulnerability Analysis and Security Solution

Sang Jin Lee** · So Yeon Hwang*** · Kyung Kon Kim**** · Sung Koo Ryeo*****

ABSTRACT

Since the internet banking service was introduced to Korea in 1999, the service has placed itself as an indispensable service to most users. The internet banking, which provides convenience for internet users as well as efficiency for banks, is expected to increase its importance more and to play a bigger role as a passage of funds. Meanwhile, numerous accounts as to the misusage of the internet banking service have been reported and the types and size of damages, especially making illegal money transfers and embezzling user information through computer hacking, tend to increase continuously. This paper points out fundamental problems of the current internet banking service by analyzing the all components of the internet banking service and fitting the results of structural analysis of hacking threats in accordance with service flow. This paper also attempts to propose the means to minimize the hacking threats of the internet banking service.

Key words : Internet Banking, Internet Banking Service Flow, Hacking

---

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2006-(C1090-0603-0025)).

** 고려대학교 교수

*** 고려대학교 정보경영공학전문대학원

**** SK인포섹 전임 컨설턴트

***** (주)안철수연구소 전임컨설턴트

1. 서 론

20세기 인류의 눈부신 발전에 지대한 영향을 미친 기술 중에 하나는 바로 인터넷의 등장이다. 인터넷의 등장으로 인해서 지구촌은 하나가 될 수 있는 터전을 마련했으며, 각종 오프라인에서 행해지던 커뮤니케이션, 정보의 교류와 축적 등이 인터넷이라는 기술 혁신으로 인해 집안 또는 세계의 반대편에서 가능하게 되었다. 이러한 새로운 흐름과 함께 물질적인 교류가 이루어지던 화폐 역시 전자 화폐가 등장하게 되었고 1999년에 인터넷 뱅킹이라는 온라인 은행 서비스가 등장하게 된 이후 현재까지 그 이용률은 증대되고 있으며, 중요도 역시 지속적으로 증가하고 있다.

인터넷을 통한 은행업무가 활발해짐에 따라 안전한 서비스 제공을 위한 노력과 더불어 알려지지 않은 보안 위협이 꾸준히 증가하고 있다. 악의적인 사용자에 의한 인터넷 뱅킹 시스템의 해킹은 흥미 그 이상의 금전적 가치를 제공하고 있기 때문에 이에 대한 공격 기술들은 나날이 발전하고 있다. 각 금융권의 인터넷 뱅킹 시스템을 직접 해킹하여 뱅킹 사용자들의 로그인 정보 및 금융거래 정보를 빼내는 것은 지금 현재로는 아주 힘든 일이 아닐 수 없다. 현재 금융권의 네트워크 구성은 1차, 2차, 3차 방화벽으로 구성되어 있으며 각 망별 보안 수준들이 강화되어 있기 때문에 시스템에 대한 직접적인 공격시도는 거의 불가능하다.

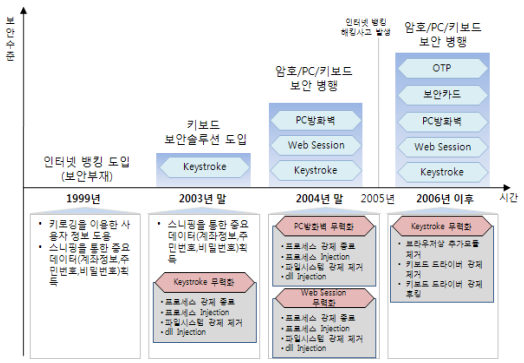
따라서 침입자 입장에서는 이 방법보다는 손쉽게 해킹할 수 있는 방법들은 생각해 내었다. 그 방법은 인터넷 뱅킹 시스템을 직접 해킹하는 것이 아니라 인터넷 뱅킹 시스템을 사용하는 이용자의 PC를 해킹하는 것이다. 대표적인 방법은 키 로거(Key Logger)를 이용하는 것인데 이는 인터넷 뱅킹 사용자들의 키보드 입력 값들을 저장하여 로그인 정보 및 뱅킹 거래 정보들을 빼내는 것이다. 이와 같이 해킹 방식이 증가함에 따라 이를 보완하기 위하여 키보드 보안 솔루션 및 웹 세션 암호화 솔루션 등이 등장하기 시작하였다. 이로 인해 금융거래 시스템의 보안 수준은 점점 증대되고 있는 상황이고 많은 보완이 이루어졌지만 체계적인 취약점 분석 및 대책은 미흡한 상황이며, 이로 인한 해킹 사고는 지속적으로 발생하고 있다.

본 논문에서는 인터넷 뱅킹 시스템의 서비스 흐름을 정의하고 각 흐름별 해킹 위협들을 도출하여 문제점을 고찰하고 보안대책을 제시하고자 한다.

2. 인터넷 뱅킹 보안 시스템 현황

2.1 인터넷 뱅킹 보안 수준에 따른 공격 수준

'인터넷 뱅킹의 연도별 보안 솔루션 도입 현황 및 공격흐름'은 (그림 1)과 같다. 1999년 국내 최초 인터넷 뱅킹이 도입되는 시점은 서비스의 효용성 측면에 대한 부분만 부각됨에 따라 보안적인 요소에 대한 고려가 미흡하여 인터넷뱅킹의 악용을 방지하는 보안 솔루션은 도입되지 않은 상태로 뱅킹 서비스가 이루어졌으며, 이에 따른 보안의 위협 요소를 감안하여 2003년 말 최초로 '키보드 보안 솔루션'을 도입하여 뱅킹 시스템의 보안 수준을 강화하였다.



(그림 1) 인터넷 뱅킹의 연도별 보안 솔루션 도입 현황 및 공격흐름

2004년 말에는 키보드 보안 솔루션뿐만 아니라

웹 세션을 암호화 하여 전송하는 'Web Session Security 솔루션', 뱅킹 사용자의 PC에 악성 코드 및 바이러스가 감염되는 것을 막기 위한 'PC보안 솔루션'이 병행되어 도입되었다. 2005년 말에 인터넷 뱅킹 해킹 사고가 처음으로 발생하였는데, 키보드 보안 솔루션을 무력화시킨 후 키 로깅(Key Logging)을 하여 계좌 비밀번호 및 기타 정보를 획득함으로써 불법적인 이득을 취했다[1].

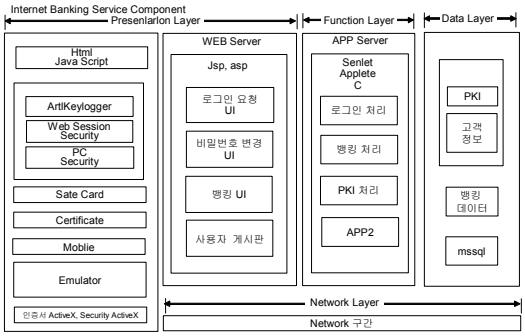
이후 보안 솔루션의 보안 강화에 더더욱 초점이 맞추어졌으며 현재에 이르기까지 보안카드 입력 방법 변경, 키보드 보안 솔루션 강화, OTP도입 등이 이루어졌다.

(그림 1)과 같이 연도별 보안 솔루션의 도입 현황을 기준으로 각 수준별로 발생할 수 있는 해킹 위협이 어떤 것들이 있는지 분석하여 보았다. (그림 1)을 참조하면 보안 솔루션이 존재하지 않는 상태인 1단계에서는 특별한 해킹 기법을 사용하지 않고, 키 로깅(Key Logging)을 통한 사용자 정보 도용이나 스니핑(Sniffing)을 통한 사용자의 중요 정보 획득이 쉽게 가능하다. 키보드 보안 솔루션이 존재하는 2단계에서는 초급 수준의 해킹을 통하여 키보드 보안 솔루션을 무력화 할 수 있으며 사용자 정보 도용이 가능하다. 3단계의 Web Session Security, PC 보안 솔루션, 키보드 보안 솔루션의 도입이 되어 있는 상태에서는 초급과 중급 수준의 키보드 보안 솔루션 무력화 기법과, Web Session Security 솔루션 무력화 기법 등의 방법으로 역시 사용자 정보의 도용이 가능하다.

그 다음 4단계는 현재의 인터넷 뱅킹 사용 수준으로 고급수준의 키보드 보안 솔루션 무력화 기법 및 기타 방법을 이용하여 사용자 정보 도용이 가능하다. 무력화 기법에 대한 구체적인 내용은 '3. 인터넷 뱅킹 취약점 분석'에서 알아보도록 하겠다.

2.2 인터넷 뱅킹 서비스 구성요소

인터넷 뱅킹 서비스의 구성 요소는 크게 Presentation Layer, Function Layer, Data Layer라는 3계층(Layer)으로 구성할 수 있다. Presentation Layer는 인터넷 뱅킹 사용자의 웹 브라우저를 통해서 외향적으로 보이는 뱅킹 사용자단의 PC와 웹서버에서 제공되는 웹 브라우저 상의 뱅킹 서비스를 위한 화면이 포함되어 있다. Function Layer는 실제 뱅킹 서비스를 하는데 있어 중요 로직이 되는 부분으로 사용자가 뱅킹 서비스에 대한 요청 시 이를 처리하는 부분이다. Data Layer는 실제 사용자의 신상 정보, 계좌정보, 뱅킹 데이터 등이 저장되는 부분을 말한다. Network Layer는 뱅킹 사용자가 입력한 데이터를 웹서버, APP서버, 데이터베이스 서버를 통하여 전송되는 일련의 과정들을 말한다.

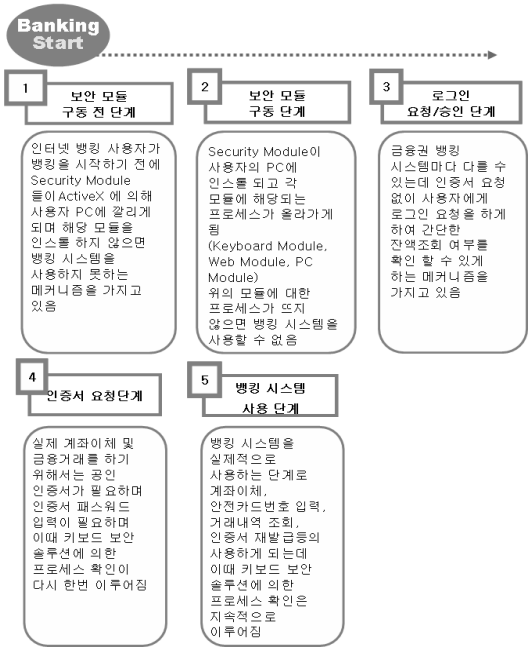


(그림 2) 인터넷 뱅킹 서비스 구성요소

2.3 인터넷 뱅킹 보안 서비스 프로세스

인터넷 뱅킹 서비스의 구성 요소와 함께 인터넷 뱅킹을 사용하는 사용자의 단계별 프로세스를 살펴보면 인터넷 뱅킹을 시작하기 위하여 웹 브라우저를 열면 1단계로 보안 모듈들이 사용자 PC에 깔리게 되며, 2단계로 보안 모듈들이 사용자 PC에서 실행이 된다. 3단계로 로그인 요청/승인을 하게 되는데 보안 솔루션의 프로세스들이 제대로 활성화 되어 있지 않으면 인증서 기반의 로그인 요청을 허용하지 않는 프로세스를 가지고 있으며, 4단계 5단계 또한 보안 솔루션에 대한 실시간 Alive Checking을

통하여 파일 시스템 및 프로세스를 점검한다.



(그림 3) 인터넷 뱅킹 서비스 단계별 프로세스

2.4 인터넷 뱅킹 보안 서비스 현황 및 문제점

인터넷 뱅킹 서비스를 사용함에 있어 '보안 솔루션들의 개별화', '보안 솔루션의 부분 적용', '보안 솔루션을 위한 솔루션', '사고 발생 후 조치'라는 총 4가지의 현황 및 문제점을 제시하고자 한다. 각각의 항목에 대한 내용은 다음과 같다.

2.4.1 보안 솔루션들의 개별화

현재 등장한 보안 솔루션들은 키보드 보안 제품, Web Session Security 솔루션, 스파이웨어 탐지/제거 제품, 개인 방화벽 제품 등 다수가 존재하고 있다. 동일한 카테고리를 담당하고 있는 보안 솔루션에서 보호 가능한 영역이 벤더별로 상이함은 물론 다른 카테고리의 보안 솔루션과의 상호 의존성이 존재하고 있지 않다. 이로 인해 보호 가능한 영역의 누락이 생기거나 연동되는 부분에서의 결함으로 인해 보안 솔루션에 치명적인 문제점이 발생하게 된다. 예를 들어, 통합된 보안을 제공하는 환경에서 상호 의존성을 검증하지 않을 경우 다른 영역을 담당하고 있는 제품이 제 기능을 충실히 수행하고 있는지를 확인하지 않기 때문에 자신의 기능에만 충실하게 된다. 그렇기 때문에 통합된 보안을 제공하는 영역에서 한 개의 카테고리가 누락됨으로 인해 사용자 PC에 대한 보안은 무효화 될 수 있다.

2.4.2 보안 솔루션의 부분 적용

인터넷 뱅킹에서 제공하는 서비스를 보호하기 위해 사용되는 보안 솔루션에 대한 적용이 일부분에 그치는 경우가 일반적이므로 프로세스 단계에 따른 Security Hole이 존재한다. 예를 들어 인터넷 뱅킹 프로세스 단계 중 로그인 단계에서는 Web Session Security 솔루션의 프로세스가 적용하고 있어 사용자의 주요 정보에 대한 획득이 초급 수준의 해커에 의해서는 어려운 상태이나 계좌 이체 단계에서는 Web Session Security 솔루션의 프로세스가 적용되어 있지 않아(암호화 모듈이 적용되어 있지 않아)인터넷 뱅킹 정보의 획득이 가능한 경우가 있다.

2.4.3 보안 솔루션을 위한 솔루션

뱅킹 시스템에서 제공되는 보안 솔루션을 우회할 수 있는 기법들이 다양하게 존재한다. 예를 들어 키보드 보안 솔루션을 사용자의 PC에서 구동함에 있어 프로세스 및 파일 시스템에 대한 무결성을 검증하지 않은 상태에서 실행된다면 악의적인 사용자는 Process Injection과 같은 다양한 기법들을 이용하여 정상적인 보안 프로그램을 해커에 의해 제작된 프로그램으로 변경하여 보안 기능을 무력화 할 수 있게 된다. 이러한 문제는 보안 솔루션을 위한 또 다른 보안대책을 요구하는 상황을 초래하게 된다.

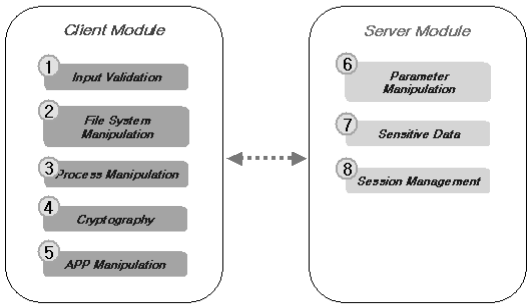
2.4.4 사고 발생 후 조치

이미 여러 어플리케이션의 보안 사고를 통해서 알 수 있듯이 사고 발생 후 보안 대책을 적용하였음에도 불구하고 또 다른 문제점이 지속적으로 발생하게 된다. 이는 사전 조치에 초점이 맞추어져 있기 보다는 사고가 발생한 문제에 대해서 임기응변식으로 대응하기 때문이다. 일반적으로 솔루션에 보안 문제가 발생하는 이유는 잘못된 설계 또는 특정 함수의 잘못된 구현 등으로 인해서 발생하게 된다. 하지만 보안 솔루션의 재설계 또는 전체 함수의 변경 등과 같이 근본적인 문제를 해결해야 함에도 불구하고 서비스의 정상화가 우선순위를 차지하기 때문에 문제가 발생한 특정 부분만을 수정하게 되며, 근본적인 문제 해결은 등한시 된다.

3. 인터넷 뱅킹 취약점 분석

3.1 인터넷 뱅킹 서비스 공격 분류

인터넷 뱅킹 위협 분석을 위한 공격 분류(Attack Category)는 크게 Client Module과 Server Module로 분류 할 수 있다. Client Module은 클라이언트 PC에서 발생하는 해킹에 대한 공격 분류를 말하며 Server Module은 뱅킹 서버 단에서 발생하는 해킹에 대한 공격 분류를 말한다.



(그림 4) 인터넷 뱅킹 서비스 단계별 프로세스

Client Module에서의 공격 분류는 5개, Server Module에서의 공격 분류는 3개로 총 8개의 항목을 도출할 수 있다.

3.1.1 Input Validation

인터넷 뱅킹을 위하여 사용자 PC에 깔려 있는 프로그램에 대하여 버퍼 오버플로우 공격과 같은 악의적인 입력 오류를 이용하여 사용자 PC를 점령할 수 있다. 이를 통해 사용자 PC에 악의적인 프로그램을 설치하여 사용자 도용을 시도할 수 있다[2].

3.1.2 File System Manipulation

인터넷 뱅킹 사용자의 PC에 깔려 있는 프로그램의 파일시스템을 조작하여 보안 모듈을 우회할 수 있으며. 이를 통한 사용자 계좌 정보 획득 및 중요 정보 획득이 가능하다.

3.1.3 Process Manipulation

인터넷 뱅킹 사용자의 PC에 깔려 있는 프로그램의 프로세스 조작을 통하여 보안 모듈을 우회할 수 있으며, 이를 통한 사용자 계좌 정보 획득 및 중요 정보 획득이 가능하다.

3.1.4 Cryptography

강력한 암호 선택 및 구현, 관리를 통해 중요 데이터가 유출 및 변조되지 않게 하기 위한 보안 구성요소이다. 암호화에 해당되는 보안 모듈의 부적절한 함수의 사용 및 복호화 함수 노출로 인하여 암호화를 무력화 시킬 수 있는 가능성이 존재한다[3].

3.1.5 APP Manipulation

인터넷 뱅킹 사용을 위하여 사용자 PC에 관련 어플리케이션이 설치되며 Reverse Engineering 기법을 통하여 보안 인증 모듈 우회 및 민감한 정보

에 대한 노출 가능성이 존재한다.

3.1.6 Parameter Manipulation

인터넷 뱅킹을 사용하는 단계에서 데이터 상의 파라미터(Parameter) 값을 변경한 후 전송하면 악의적인 제 3자에 의한 계좌정보 열람 및 잔액정보 열람 등의 행동을 취할 수 있다[3].

3.1.7 Sensitive Data

인터넷 뱅킹 서비스를 제공하는데 있어 사용자의 신상 정보 또는 계좌정보 및 비밀번호 등이 노출되는 경우가 있으며 이를 활용한 악의적인 행동이 취해질 수 있다. 민감한 정보의 노출을 발생시키는 모든 요소를 본 항목으로 볼 수 있다[3].

3.1.8 Session Management

사용자와 웹 어플리케이션 통신 시 사용자 정보 확인 및 현금 이체 등과 같은 중요 기능의 실행 전 사용자의 재확인 실시, 일정시간 동안 사용자 요청(Request)이 없을 때, 세션(Session)의 종료 등 사용자 세션 관리(User Session Management)가 이루어져야 한다. 세션 관리가 취약할 경우 공격자에 의한 Session Hijacking, Session Reply, Man In the Middle 등의 공격으로 합법적인 사용자로서의 권한상승을 통한 시스템 침해가 가능하다[3].

3.2 인터넷 뱅킹 서비스 위협 요소

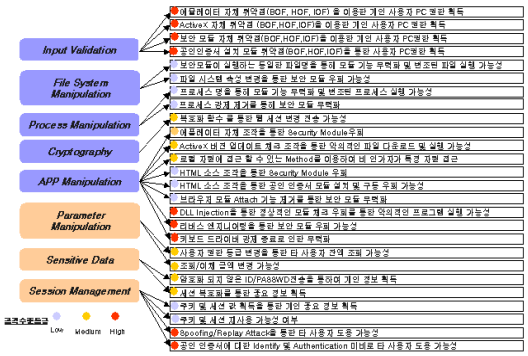
(그림 4)를 참조하여 인터넷 뱅킹에 대한 공격 유형을 Client Module과 Server Module을 대상으로 분류하였으며 공격 수준 등급을 Low(초급), Medium(중급), High(고급)으로 구분하여 총 28개의 공격 가능성을 (그림 5)와 같이 도출하였다. Low 수준은 해킹에 대한 기본 지식 없이도 쉽게 공격이 가능한 수준을 말하며, Medium 수준은 해킹에 대한 기본지식과 함께 Reverse Engineering의 기본 지식이 있어야 가능하며, High 수준은 실제 공격코드(Exploit Code)작성이 가능하고 Reverse Engineering 기법에도 능한 해커에 의해서 공격이 가능한 수준을 말한다.

공격 수준별로 공격 유형에 대해 분류를 하면 아래와 같다.

Low 수준의 공격에는 파일명과 파일 시스템 속성 변경을 이용한 File Manipulation, 프로세스명 위조와 강제 제거를 통한 Process Manipulation, HTML 소스 수정과 브라우저 모듈 Attach 기능 제거를 통한 App Manipulation, 쿠키 및 세션에 대한 획득과 재사용을 통한 Session Management의 공격 분류가 속한다.

Medium 수준의 공격에는 클라이언트에 존재하는 복호화 함수를 이용한 Cryptography, 애플리케이션 자체 조작과 ActiveX 업데이트 기능 조작, 비정상적인 Method 조작을 이용한 Parameter Manipulation, 비암호화된 통신과 세션 복호화를 통한 Sensitive Data의 공격 분류가 속한다.

High 수준의 공격에는 에뮬레이터, ActiveX, 보안 모듈, 공인 인증서 설치 모듈의 취약점을 이용한 Input Validation, DLL Injection과 Reverse Engineering 그리고 키보드 드라이버 강제 종료를 통한 App Manipulation, Spoofing/Replay Attack과 공인 인증서의 인증 부족을 이용한 Session Manipulation의 공격 분류가 속한다[4].



(그림 5) 공격 분류(Attack Category) 별 공격 가능성

〈표 1〉 공격 분류에 따른 보안 대책

공격 분류	원인	위협요소	보안대책
Input Validation	프로그램 개발시 보안적인 요소를 고려 하지 않음 (Buffer Overflow, Heap Overflow, Integer verflow)	보안모듈 자체 취약점을 통한 사용자 PC 권한 획득 후 악의적인 프로그램 설치(키로거, 웹 스니퍼)	보안요소를 고려한 개발 적용
File System Manipulation	파일 시스템 무결성 점검 미흡	보안 모듈 무력화(키로깅/스니퍼를 통한 계좌정보 획득)	파일 시스템의 파일 속성 및 무결성 점검 루틴 추가 (해쉬 값 비교 루틴)
Process System Manipulation	프로세스 무결성 점검 미흡		보안모듈 프로세스 무결성 점검 루틴 추가
Crypto-graphy	Web Session Security보안 솔루션 복호화 루틴 노출		사용자단 PC에 서버에서 Response된 데이터에 대한 캐싱 제거
APP Manipulation	바이너리 미보호 (안티 디버깅 루틴 부재)	Reverse Engineering 기법을 통한 보안모듈 우회/중요정보 획득/복호화루틴 파악	클라이언트 사용자에게 제공하는 바이너리에 대하여 안티 디버깅 루틴 추가
Parameter Manipulation	사용자 세션 관리 미흡	사용자 도용/타 사용자 계좌정보 조회	사용자 세션 관리 강화
Sensitive Data	클라이언트 사용자단에 사용자 중요정보가 Html 데이터 형태로 캐싱 사용자 중요 정보에 대한 암호화 전송 미흡	사용자 단 Html 캐싱 데이터 스니핑을 통한 계좌정보 획득/계좌정보 변조 전송	사용자단 PC에 서버에서 Response된 데이터에 대한 캐싱 제거 보안 루션의 방역 적용
Session Manage-ment	사용자 세션 관리 미흡	사용자 도용/타 사용자 계좌정보 조회	사용자 세션 관리 강화

4. 인터넷 뱅킹 보안대책

위의 인터넷 뱅킹 아키텍처 부분에서 여러 가지의 공격 위협들을 분류하였으며 이러한 공격 가능성들을 나열 하였는데 이에 대한 해킹 가능성을 최소화하기 위해서는 어떠한 방법들이 선행되어야 하는지를 알아보도록 하고, 향후 어떤 과제들을 고민해야 하는지에 대하여 기술하고자 한다.

총 8개의 공격 분류에서 도출된 보안 위협 원인을 분석하여 5가지의 위험요소를 찾아낼 수 있었다. 이를 바탕으로 총 7가지의 보안 대책을 <표 1>과 같이 도출해낼 수 있다.

4.1 보안요소를 고려한 개발 적용

보안모듈 바이너리에서는 Buffer Overflow[10], Format String Bug, DoS(Denial of Service)를 고려하여 입력 값에 대한 “경계 점검 루틴(Boundary Check Routine)”의 추가와 한계(Perimeter) 도달 시 Fail Over 기능이 필요하다. ActiveX의 경우 Buffer Overflow, 로컬 자원 접근, 업데이트 조작의 보안 요소를 고려하여 “경계 점검 루틴”을 비롯하여 보안에 취약한 메서드(Method) 사용 자제와 무결성 점검 등이 적용되어야 한다.

4.2 안티 디버깅 루틴 추가

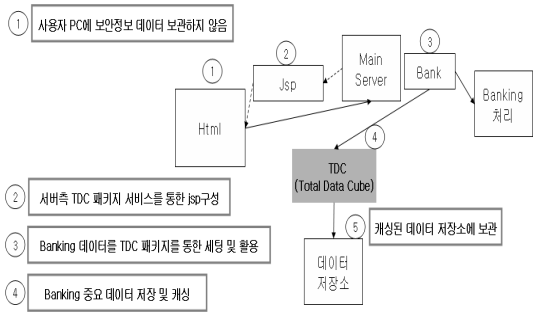
역공학 기법(Reverse Engineering)[9]을 차단하기 위해서는 “Packing 사용”, “코드의 암호화”, “실시간 디버깅 점검”방법을 이용할 수 있다.

4.3 사용자 PC에 주요 데이터 캐싱 금지

사용자의 중요 정보(비밀번호, 계좌번호)가 노출됨에 있어 서버의 Response 데이터에 대하여 Html 형태로 클라이언트에게 보여지는 것이 근본적인 문제가 되므로 이를 해결하는 방식으로 TDC (Total Data Cube) 방식을 이용한 보안대책을 엘엔제

이시스템(주) 업체에서 제시하였다[5].

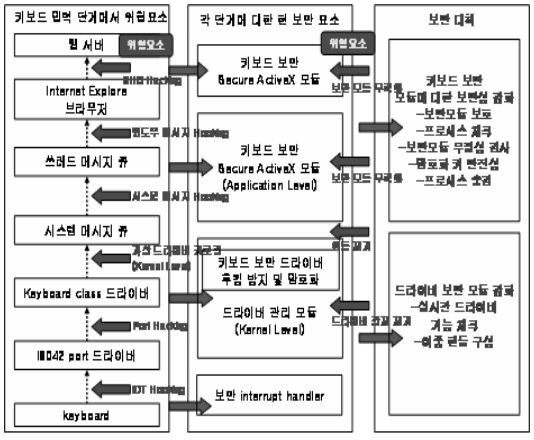
TDC 보안 솔루션은 Html로 클라이언트에 캐싱되는 민감한 정보에 대하여 서버 단에서 제공하는 TDC(Total Data Cube)에 의해 데이터 저장소에 저장되고, 서버 단에서 전송되는 민감한 정보는 클라이언트에 저장하지 않고 데이터 저장소에서 직접적으로 가져다 씀으로써 클라이언트에 제공하게 되는 민감한 정보의 노출을 방지할 수 있다.



(그림 6) TDC를 활용한 클라이언트 데이터 숨김

4.4 키보드 보안 솔루션

키보드 보안 솔루션을 해킹하기 위한 여러 가지 방법들이 있고 이 기법은 고난위의 역공학 기법이 사용된다. 아래의 보안 대책은 인터넷 뱅킹 시스템을 사용함에 있어 가장 중요한 요소로 자리 잡고 있는 키보드 보안 솔루션의 동작 방식에 따른 각 단계별 위협 요소를 정의하고 이를 해결하기 위한 방안을 정리해 보았다. (그림 7)에서 보안대책 중 Application Level에서 사용할 수 있는 해킹 방법은 Kernel Level에서 사용하는 해킹 기법에 비하여 쉽고 간단하다. 키보드 보안 솔루션들은 좀 더 강화된 구현 방식인 드라이버 보안 모듈 강화를 위한 실시간 드라이버 기능 점검, 이중 핸들 구성을 고려하고 있지만 Application Level에서의 기능 점검을 하고 있지 않는 경우가 다수 존재하여 이에 대한 무력화가 가능한 상태이다.



(그림 7) 키보드 보안 솔루션의 위협요소 별 보안대책

5. 결론 및 향후 연구과제

본 논문에서는 각종 보안 솔루션이 도입되어 있는 '인터넷 뱅킹 시스템'의 현황과 뱅킹 서비스의 컴포넌트를 기반으로 발생할 수 있는 취약점을 서버와 클라이언트로 구분하여 공격 수준별로 분석하고 이에 대한 보안대책을 제시하였다. 이는 체계적으로 인터넷 뱅킹의 기술적 취약점을 세분화하고 흐름화하여 분석하였다는 점에서 매우 의미있는 연구라고 생각한다. 그렇지만 인터넷 뱅킹 취약점 분석 아키텍처에 인터넷 뱅킹시 발생 할 수 있는 모든 위협들을 담기는 역부족이다. 본 연구 자료가 이와 유사한 서비스 흐름을 갖고 있는 웹 서비스의 보안 취약점을 도출하고 접근하는데 있어서 참고가 되었으면 한다. 또한 보다 심도 있는 인터넷 뱅킹 취약점 분석을 위해서는 운영체제의 커널 수준(Level)까지 확장한 연구가 있어야 할 것이다.

안전한 인터넷 뱅킹 서비스를 제공하기 위해서는 아직까지 수행해야 할 과제가 많이 남아 있다. 위의 아키텍처를 기반으로 하여 금융권 사이트들에 대한 공식적인 점검을 수행해본 결과 여전히

많은 문제점들을 드러내고 있는 것으로 판단된다. 보다 안정화된 뱅킹 서비스를 위해서는 다음과 같은 과제들이 고려되어야 할 것이다.

첫째, 보안 솔루션의 단일화를 추진해야 한다.

현재의 뱅킹 시스템은 키보드 보안 솔루션, PC 보안 솔루션, Web Session Security 보안 솔루션이 제각기 따로 동작한다. 이로 인하여 발생할 수 있는 문제점은 앞의 개요 부분에서도 언급을 하였지만 하나의 보안 솔루션이 문제가 발생했을 경우 다른 보안 솔루션의 기능까지 무력화 시킬 수 있다. 현 금융권에서 각 보안 솔루션들에 대한 단일화 움직임이 보이지만 단일화 함에 있어서도 각각의 보안 기능들을 신중하게 고려하여 적용되어야 할 것이다.

둘째, 보안 솔루션 적용 시 보안 솔루션의 기능적인 측면과 더불어 뱅킹 엔진과 연동상의 보안 적정성을 평가해야 한다.

인터넷 해킹의 발생 가능성을 최소화하기 위한 여러 가지 보안 솔루션들이 도입되어 있는 상태이고 각각의 기능적인 측면을 테스트하였을 때 각 기능은 훌륭하였다. 하지만 무력화 발생 가능성에 대한 부분을 고려하지 않고 있다. 즉, 뱅킹 엔진과 보안 솔루션간의 연동상의 보안 적정성 평가가 이루어지지 않고 각각의 기능적인 부분에만 치중 되어 있는 것이 현실이다. 향후 보안 솔루션의 도입 시 이에 대한 적정성 평가 프로세스를 통하여 보다 강화된 인터넷 뱅킹 서비스가 제공되어야 할 것이다.

셋째, OTP(One-Time Password) 방식의 필수 전향을 고려해야 한다.

각 은행권에서 OTP 방식을 이미 도입하였고 사용 중에 있다. 하지만 문제점은 비용 부분과 기존에 이미 Safe Card 방식을 사용하고 있는 고객들이 대부분이므로 이에 대한 강제 적용이 어려운 것이 현실이다. 향후 OTP 방식으로의 필수 전향을 고려하여 인터넷 뱅킹 서비스를 사용한다면 한층 강화된 서비스 운영이 가능 할 것으로 보인다.

참 고 문 헌

[1] 머니 투데이, “인터넷 뱅킹 첫 해킹 보안카드도 뚫려”, 2005.

[2] James C. Foster, Vitaly Osipov, and Nish Bhalla, Buffer Overflow Attacks, 2005.

[3] The Open Web Application Security Project (www.owasp.org).

[4] The Code Project(http://www.codeproject.com/dll/DLL_Injection_tutorial.asp).

[5] http://www.lnjsystem.co.kr/solution/solution_03_01.asp.

[6] Greg Hoglund and Gary McGraw, Exploiting Software : How to Break Code, Addison-Wesley, 2004.

[7] Mark Curphe and Joel Scambray, Improving Web Application Security, Microsoft Press, 2003.

[8] Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, and Riley Hassell, The Shellcoder’s Handbook, Wiley Publishing, 2004.

[9] Eldad Eilam, Reverse Engineering, WILEY, 2005.

[10] James C. Foster, Vitaly Osipov, Nish Bhalla, Buffer Overflow Attacks, 2005.

이 상 진

1994년 고려대학교 수학과 박사
1989년~1999년 한국전자통신 연구원 선임연구원
1999년~현재 고려대학교 교수

황 소 연

현재 고려대학교 정보경영공학 전문대학원

김 경 곤

숭실대학교 컴퓨터학부
현재 SK인포섹 전임 컨설턴트

여 성 구

울산대학교 경영학과
현재 (주)안철수연구소 전임 컨설턴트