# 

# SW보안개론

## 1번 과제: 인터넷뱅킹, 백신SW, 방화벽 조사 정리

SW보안개론 2분반, 32170578, 김산

제출일 : 4월 02일

### 1. 인터넷 뱅킹의 보안 위협과 보안 기능

#### 인터넷 뱅킹 서비스 관련 사이버 위협

인터넷 뱅킹 서비스와 관련한 사이버 위협의 대표적인 예로 피싱, 웜과 트로이 목마와 같은 Malware를 이용한 공격, 그리고 DDOS공격이 있습니다.

**피싱(Phishing)**  
피싱은 개인정보(Private)과 낚시(fishing)의 합성어로 금융정보나 개인 식별 번호 등의 민감한 개인정보를 피해자를 속여 탈취한후 이를 악용하는 사기 수법을 말합니다.

피싱은 피해자를 속이거나 속이는 가해자의 능력에 의존하며, 스푸핑(spoofing)이라는 방식을 통해 이루어 집니다. 스푸핑은 합법적인 웹 사이트, 전자 메일 또는 엔티티 통신을 모방하여 피해자가 통신망 또는 웹 사이트를 신뢰할 수 있다고 믿도록 속입니다. 이렇게 피싱은 은행 고객을 속여 은행 계좌 정보, 사회 보장 번호, 신용카드 데이터, 비밀번호 또는 금융 개인 식별 번호(PIN)와 같은 민감한 정보를 공개하도록 하기 위해 정상적인 것 처럼 속이고 정보를 탈취, 악용합니다.

예를들어 공격자는 신뢰할수 있는 기관이나 잘 알려진 사이트로부터 발송된 것 처럼 보이는 이메일을 전송하여 수신자가 해당 사이트를 접속하도록 유도합니다. 이후 수신자가 해당 사이트를 이메일에 첨부된 다이렉트 링크를 통해 사이트에 접속하여 자신의 개인정보를 입력하게 되고 이를 통해 공격자는 피해자의 민감한 개인정보를 수집, 금융자산에 손해를 끼치는 등의 방식으로 악용합니다.

**멀웨어(Malware)**

멀웨어를 통한 공격의 대표적인 예로 웜(Worm)과 트로이목마(Trojan horses)를 통한 공격이 있습니다.

웜은 네트워크에 걸쳐 스스로 복제하여 악의적인 수행을 하는 프로그램 또는 알고리즘을 말합니다. 악의적인 행동이란 보통 컴퓨터의 시스템 자원을 소진하여 시스템을 종료하는 행동을 수행합니다.

반면, 트로이 목마의 경우 스스로 복제하지는 않지만 웜만큼 파괴적입니다. 트로이 목마는 과거 트로이 군이 커다란 나무 목마에 들어가 숨어있다가 트로이군을 공격한 트로이 전쟁 이야기에서 따온 이름으로 그 공격방식이 이야기와 유사합니다. 가장 교활한(insidious) 방식의 트로이 목마는 바이러스를 제거하는 소프트웨어를 가장하여 바이러스를 유입시키는 방식을 사용하는 유형입니다.

또다른 전형적인 유형은 시스템에 잠입하여 키보드 입력을 가로채(Interception) 공격자에게 전송하는 유형입니다.

이러한 웜과 트로이 목마를 통한 금융기관 공격 사례로 버그베어(Bugbear)가 있습니다. 버그베어는 네트워크를 통해 수많은 메일을 전송하는 웜으로 일련의 실행파일을 감염시켜 키로깅 작업을 수행하고 백도어를 가능하게 하며, 시스템의 백신 소프트웨어를 무력화 시킵니다. 이러한 기능들을 통해 버그베어는 민감한 banking정보를 수집하고, 코딩된 이메일 주소로 전송하여 유출시킵니다.

**DOS, DDOS(분산 서비스 거부 공격)**

서비스 거부 공격(DOS)은 뱅킹 트렌젝션이나 데이터에 대한 인터넷 접근을 제공하는 서버를 타겟(Target)으로 서버의 갑작스러운 종료(Screeching halt)를 유발시킵니다.

이렇게 뱅킹 서비스가 다운되면 금융기관의 서비스가 중지될 뿐만 아니라 공격자는 이러한 행위를 통한 명성(publicity)을 얻게 됩니다.

분산 서비스 거부공격(DDOS)은 서비스 거부 공격의 수정된 형태로 공격자는 여러대의 컴퓨터를 감염시켜 하나의 타겟에 대해 서비스 거부 공격을 수행하는 방식입니다.

이러한 서비스거부공격/분산서비스 거부공격은 웜과 같은 다른 형태의 공격방식에 비해 피해가 크지 않은 편입니다.

(Rolf OppligerRuedi, 2009) (BhasinMadan, 2007)

#### 인터넷 뱅킹에서 사용하고 있는 보안 기능

**암호화 기술을 통한 개인정보 보호**

최근들어 자주 사용되고있는 모바일 플렛폼에서의 인터넷 뱅킹은 더 복잡한 보안문제를 안고 있습니다. 모바일 뱅킹 서비스는 선이 없는(wireless)환경에서 이루어 지는데 기존의 암호화 기술이나 트렌젝션 레이어에 대한 기존의 보안 기술은 모바일 뱅킹에 대한 충분한 보호를 제공해주지 못합니다.

현대 암호화 기술들은 PC의 강력한 계산 능력과 저장 용량을 바탕으로 하기 때문에 모바일 서비스에서 적용하기에는 어려움이 있었습니다. 이러한 계산의 복잡성을 줄이는 동시에 높은 보안성을 제공하기 위해 최근의 모바일 디바이스는 대칭키 암호방식AES와 공개키 암호방식ECC라는 암호화 알고리즘을 사용하기 시작하였습니다.

무선으로 전송되는 데이터에 대해서는 AES방식을 통해 암호화 하고, 암호화 키로 ECC알고리즘을 사용하여 암호화 합니다.

현재 AEC와 ECC는 해커의 공격으로부터 데이터를 보호하기 위한 가장 강력한 암호화 방식입니다.

**전자서명**

전자서명은 데이터 인증(Authentication)과 부인방지(non-Authorization)에 중요한 역할을 합니다. 전자 서명은 메시지, 소프트웨어 또는 디지털 문서의 기밀성(Confidentiality)과 무결성(Integrity)을 확인하는 데 사용되는 수학적 기법으로 손으로 쓴 서명이나 도장의 역할을 하는 디지털 정보입니다. 현재 잘 알려진 전자 서명은RSA알고리즘과 ECC알고리즘을 사용하고 있습니다.

**WPKI(Wireless Public Key Infrastructure)**

WPKI는 무선환경에서 인증과 암호화를 제공하기 위해 개발된 기술로, SIM카드와 같은 모바일 보안 요소를 사용하여 공개 키 인프라 기능을 제공하는 기술입니다.

상대방에게 메시지를 전송하면 수신자 PKI의 공개키를 이용해 메시지를 암호화하여 전송하고 수신자는 자신의 개인키를 이용하여 복호화하여 데이터의 기밀성을 유지합니다.또 hash함수를 이용하여 전송된 데이터의 무결성을 보장하며, 개인키를 통해 암호화한 전자서명을 통해 인증과 부인방지를 제공합니다.

(Mobile Banking Information Security and Protection Methods, 2008)

### 2. 백신 SW들의 동작 원리 및 기능

#### 악성 프로그램들 중, Spyware, Trojan horse, Bot, Zombie

**Spyware**

스파이웨어는 해커가 광고주에게 판매하거나 사용자의 아이디, 비밀번호, 신용카드 번호 와 같은 개인정보를 도용하기위해 사용자의 컴퓨터 활동을 몰래 모니터링하고 추적하는 악성 소프트웨어입니다. 스파이웨어는 트로이 목마처럼 합법적인 프로그램이나 소프트웨어를 다운로드 한다고 생각하는 사용자들에 의해 설치됩니다.

스파이웨어의 또다른 변형으로 스케어웨어(scareware)와 랜섬웨어(ransomware)가 있습니다. 스케어웨어는 사용자에게 악성 소프트웨어를 구매하도록 유도하는 사회공학적 기법을 이용한 악성 소프트웨어이며, 랜섬웨어는 컴퓨터 시스템을 감염시켜 파일들에 대한 접근을 제한하고 몸값을 요구하는 악성 소프트웨어입니다. 이들은 대개 가짜 안티-바이러스, 안티-스파이웨어 광고의 형태로 나타납니다. 이들은 바이러스를 발견했다는 거짓 팝업을 출력하여 가격을 지불하면 이들을 스캔하여 제거하겠다고 거짓말합니다.

스케어웨어는 바이러스나 멀웨어에 관한 이메일이나 인터넷 검색에서 나타나기도 합니다.

**Trojan Horses**

트로이 목마는 웜이나 여타 바이러스와는 달리 스스로 복제하지 않고 다른 파일을 감염시켜 스스로 번식하지는 않지만, 일부 트로이 목마는 웜이나 바이러스를 옮기기도 합니다. 트로이 목마는 다른 프로그램이나 파일로 위장한 프로그램 코드입니다. 사용자들은 예쁜 화면보호기나 재미있는 게임처럼 매력적이고 그들이 생각하기에 합법적이라고 생각하는 프로그램을 실행하거나 설치하여 트로이 목마를 퍼뜨리게 됩니다. 이러한 프로그램들과 함께 트로이 목마는 문제를 일으키는 프로그램을 설치합니다. 몇몇은 윈도우 시작시 팝업을 출력하거나 홈페이지를 바꾸는 등의 큰 문제를 일으키지는 않지만 파일을 삭제하거나 키로거, 백도어를 인가되지 않은 방법으로 설치하여 정보를 훔치는 큰 문제를 야기하기도 합니다. 많은 트로이 목마는 사용자가 잘못된 링크나 스팸메일을 클릭함으로써 컴퓨터에 유입됩니다.

**Bot and Zombies**

봇(Bot)은 바이러스와 웜을 통해 컴퓨터에 설치됩니다. 봇은 사용자 몰래 컴퓨터를 원격으로 조작하여 작업을 수행할 수 있습니다. 봇은 사용자의 컴퓨터에 대한 백도어를 허용하여 제어 권한을 얻은 다음 컴퓨터를 좀비로 만듭니다. 이러한 좀비 컴퓨터들의 집합을 봇넷(Botnets)이라고 하며 엄청난양의 스팸과 악성프로그램, 패킷을 보내는데 주로 사용됩니다. 과거 크네버 봇넷(Knber botnet)은 2010년 동유럽의 범죄조직에 의해 조직되어 전세계 약 2,500개의 상업 및 정부 컴퓨터 시스템을 손상시켰고 이메일, 인터넷 뱅킹 사이트, 소셜네트워크 사이트에 접속하였습니다.

(Zombies, Trojan Horses and You, 2011).

최근 사물인터넷(IoT)은 여러 사물인터넷 관련 장치가 점점 늘어나기 시작하면서 악성행위자들이 사물인터넷의 다양한 위치와 방대한 양을 악용할 수 있는 주된 표적이 되었습니다. 악성행위자들은 이러한 사물인터넷을 통해 서비스 거부공격(DOS)부터 스팸 및 광고 사기에 이르기 까지 다양한 용도로 사용할 수 있는 봇넷을 모으는 것을 목표로 삼고 있습니다.

(The Mirai botnet and the IoT Zombie Armies, 2017)

#### 백신 SW의 악성 프로그램(malware)탐지 방법

악성 프로그램을 탐지하기 위해서는 먼저 악성프로그램에 대한 분석을 해야 합니다. 악성프로그램에 대해 분석하여 어떻게 악성 프로그램이 동작을 하고 어떤 목적으로 개발되었는지 파악함으로써 백신SW의 개발자들은 좀더 쉽게 방어 기능을 구현할 수 있습니다. 악성프로그램을 분석하는 기법은 시간과 분석 기법에 따라 크게 3가지로 나뉩니다.

**정적분석(Static Analysis)**

프로그램을 실행하지 않고 코드를 통해 프로그램을 분석하는 기법을 정적분석 또는 코드분석 이라고 합니다. 코드로부터 얻을 수 있는 정적 정보(Static information)를 통해 소프트웨어가 악의적인 코드를 포함하고 있는지 판단할 수 있습니다. 정적 분석 기법을 통해 소프트웨어는 도구를 통해 역공학(reversed engineered)되고 악의적인 코드가 어떻게 수행되는지 구조를 파악합니다. 역공학을 위한 도구에는 디버거(debugger), 디셈블러(dissembler), 디컴파일러(decompiler), 소스코드 분석기등이 있습니다. 그리고 정적분석을 위한 기법에는 파일 형식검사(File Format Inspection), 문자열 추출(String Extraction), 흔적 채취(Fingerprinting), 안티 바이러스 스캔(AV scanning), 디셈블리(Dissembly)가 있습니다.

**동적분석(Dynamic Analysis)**

동적분석은 소프트웨어의 함수호출, 제어흐름, 함수의 명령어 파라미터(Parameter)를 추적하여 이루어 집니다. 악의적인 코드는 악성 프로그램의 행동을 추적하기 위해 만들어진 가상의 환경에서 실행됩니다. 이러한 동적분석을 위한 도구에는 샌드박스(sandbox), 시뮬레이터, RegShot, Process Explorer와 같은 에뮬레이터가 있습니다. 동적분석기법은 감염된 소프트웨어가 가상환경에서 모니터링 목적으로 실행되므로 정적분석 기법보다 효과적인 방법입니다. 동적분석을 통해 더쉽게 많은 종류의 악성 소프트웨어를 탐지할 수 있지만, 악성 소프트웨어를 실행하기 위한 환경을 설계해야 하기 때문에 더 많은 시간이 소요됩니다.

**복합형(Hybrid)**

정적분석 기법과 동적분석 기법을 합친 방식으로 두가지 방식의 장점을 모두 활용할 수 있습니다. 먼저 소프트웨어 코드 분석을 통해 악의적인 특징을 확인하고 가상 환경에서 동작 시켜 어떻게 동작하는지 파악합니다.

|  |  |
| --- | --- |
| 정적분석(Static Analysis) | 동적분석(Dynamic Analysis) |
| 빠르고 안전하다 | 시간이 많이 소요되고 취약하다 |
| 다양한 방식의 악성 소프트웨어를 분석하기 좋다 | 다양한 방식의 악성 소프트웨어를 분석하기 어렵다. |
| 난독화되고 복잡한 형태의 악성 소프트웨어를 분석할 수 없다. |  |
|  |  |

#### 다음 두 가지 경우(①과 ②) 중에서 어떤 경우가 더 나쁜 상황인지? 그리고 그 이유를 같이 설명하시오.

1. 악성 프로그램을 정상 프로그램으로 탐지하는 경우
2. 정상 프로그램을 악성프로그램으로 탐지하는 경우

### 3. 방화벽(firewall)의 목적 및 기능 이해

#### 방화벽의 목적과 기능

#### DDoS 공격 원리

#### 방화벽을 적용하여 DDoS 공격방어 방법

#### 네트워크 방화벽과 백신 SW와의 차이점

# 인용 자료

BhasinMadan. (2007). Mitigating Cyber Threats To Banking Industry.

Mobile Banking Information Security and Protection Methods. (2008). International Conference on Computer Science and Software Engineering. IEEE.

Rolf OppligerRytz, Thomas HoldereggerRuedi. (2009). Internet Banking: Client-Side Attacks and Protection Mechanisms. IEEE.

The Mirai botnet and the IoT Zombie Armies. (2017). MILCOM. IEEE.

Zombies, Trojan Horses and You. (2011). “state legisla”, www.ncsl.org.