간편 결제 우회공격 기법 및 대응방안에 관한 연구

고준영, 강보선, 이근호
백석대학교
e-mail:jy_go@bu.ac.kr, masati@bu.ac.kr, root1004@bu.ac.kr

A Study of Easy Payment Evasion Techniques and Countermeasures

Jun-Young Go, Bo-Seon Kang, Keun-Ho Lee
Division of Information & Communication, Baekseok University

요 약

ActiveX가 법규제로 인해 없어지고 새로운 간편 결제 시스템이 출시되고 있다. 새롭게 도입되는 간편 결제 시스템의 경우 사용자가 한 번 내려 받으면 인터넷 익스플로러뿐만 아니라 사파리나 크롬 등 다른 브라우저를 사용 시 따로 보안프로그램을 내려 받지 않아도 된다고 한다. ActiveX대신 새로운 결제 시스템의 'exe'방식의 프로그램은 한 번 내려 받아 영구 사용할 수 있으며, 이러한 'exe' 프로그램은 인증우회가 가능하여 해커가 제3자의 금융정보를 가지게 된다면 간단한 우회를 통한 공격이 가능할 것으로 예측된다. 본 논문에서는 이러한 인증우회 공격에 관한 시나리오 및 'exe'프로그램 내부의 보안프로그램에서의 이상 징후 조기 탐지를 이용한 사전 예방기법을 제안한다.

1. 서론

온라인 쇼핑에서 빠르고 안전한 결제를 위해 보안프로그램 액티브X(Active-X)가 완전히 없어지고, 다음 달 부터 전자상거래에서 카드 결제시 보안프로그램이 필요 없는 간편결제 서비스가 새로 출시된다.

액티브X는 인터넷 익스플로러(IE)에서만 내려 받을 수 있는 보안프로그램으로, IE를 많이 사용하는 국내에서만 유독 표준화 돼어 대표적인 규제가 되어왔다. 하지만 최근 사용자가 늘어나고 있는 구글의 크롬이나 애플의 사파리 등 브라우저에서는 구동이 되지 않았으며, 설치를 요구하는 팝업창이 한꺼번에 여러 가지로 나와 사용자들의 불편함을 샀다. 반면 새로 출시되는 'exe' 방식의 프로그램은 한 번 내려 받으면 인터넷 익스플로러 외에 사파리나 크롬 등 다른 브라우저를 사용시 따로 보안프로그램을 내려 받지 않아도 된다. 따로 보안 프로그램을 받지 않아도 되는 장점이 있지만 'exe' 프로그램 하나에 보안모듈이 같이 포함되어 있어 'exe' 프로그램이 크랙되어 인증방식이 우회되면 사용자의 정보가 한번에 유출되는 취약점을 가지고 있다.

이와같이 액티브X가 사라지고 보안에 취약한 'exe' 프로그램이 배포되어 발생할수 있는 취약점에 관한 시나리오를 분석하여 그 대응책을 제안하고자 한다.

2. 관련연구

2.1 우회공격

우회공격에는 여러 가지 기법이 있지만 IDS에서 사용하고있는 스트링 패턴매칭 기법의 취약성을 이용하는 방법인 IDS에 관한 우회공격이 있고[1], 시스템이 네트워크 환경에 적용되어진 이후 지금까지 해킹에 대해서 비교적 안전하다고 생각된 방화벽에 관한 우회공격 기법이 있다[2]. 이와같이 보안도구에 대한 우회공격 기법이 일반적으로 알려져 있으나, 소프트웨어 상에서 간단한 크랙만으로 인증을 우회할 수 있다.

소프트웨어를 크랙하여 인증을 우회할수 있는 여러 가지 방법 중 OllyDbg를 사용하면 Code Window, Register Window, Dump Window, Stack Window를 기본적으로 확인하고 수정할수 있어서 크랙하여 인증을 우회하는데 많이 사용되고 있다.

2.2 빅데이터

액티브 X 가 사라지고 다양한 간편 결제 시스템이 다양하게 출시되고 상용화 된다면 그에 따른 대책방안을 일일이 세워두기 힘들게 된다. 인터넷 활성화에 따라 전자상거래를 이용하는 고객들의 정보량을 일반적인 탐지 시스템은 따라 잡기 힘들만큼 데이터의 량은 급증 하고 있

다.
그래서 빅데이터를 활용하는 방법으로 이상 징후를 탐지해야한다.

빅데이터를 분석하는 방법에는 다양한 플랫폼이 있는데 그중에서도 구글에서 2003년 발표한 하둡이라는 플랫폼이 존재 한다. 하둡은 대용량의 데이터를 처리하기 위해서 하둡분산파일시스템(HDFS, Hadoop Distributed File System)과 맵리듀스(MapReduce)를 이용하여 데이터를 처리한다[3]. 하둡파일분산시스템은 여러 형태의 대용량 데이터를 보다 안정적이고 빠르게 저장한다. 맵리듀스는 대용량 데이터를 보다 안정적이고 빠르게 병렬처리 한다. 이러한 구성을 하둡 생태계라고도 부르는데, 간편 결제 시스템에 대한 공격자들의 이상 징후를 데이터베이스화 하여 저장하고, 하둡 생태계를 잘 활용한다면 예전에는 보이지 않았던 사고패턴을 발견할 뿐 아니라 전자상거래에도 안전한 빅데이터 분석 플랫폼을 구축할 수 있을 것이다[4].

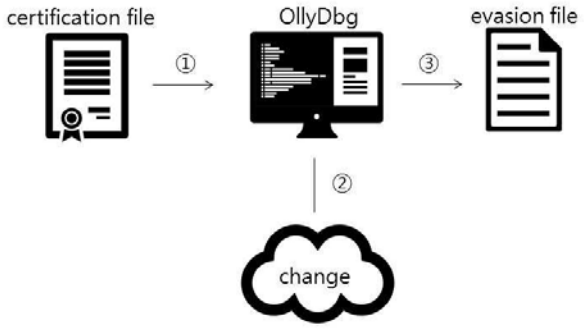
3. 인증우회공격 시나리오

해커는 액티브X가 없어지고 새로 출시되는 'exe'방식의 간편결제 시스템 프로그램을 OllyDbg툴로 크랙하여 인증우회를 하고 사전에 탈취한 피해자의 금융정보(신용카드)를 이용하여 간편결제 시스템을 악용하게 된다.

인증우회공격 시나리오를 분석하기 위하여 실제 해커 입장이 되어 테이블1의 환경으로 인증우회를 시도해 보았다.

<표 1> Scenario Environment

Crack Tool	OllyDbg110
Executable file	Visual Basic 2010Express



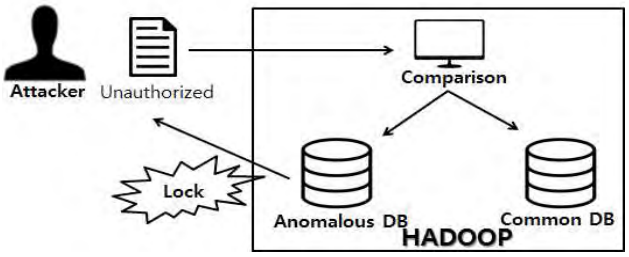
(그림 1) 'exe' 파일의 인증우회 시나리오

① 해커는 간편결제 'exe'파일을 OllyDbg툴로 실행을 한다.
② 크랙하려는 프로그램의 소스 코드에서 vbaStrCmp 즉, Visual Basic에서 사용하는 문자를 비교하는 함수를 nop로 바꿔준 후 Assemble를 활성화시킨다.
③ 인증을 우회하여 해커가 피해자의 권한을 획득한다.

가장 단순한 방법으로 내부에서 사용되는 문자열을 기준으로 검색을 하여 디스어셈블 된 코드가 보이는 곳에서 Search for -> All referenced text strings를 선택하여 문자열들만 추려서 확인을 시작한다. 디버깅을 시작하여 특이한 문자열을 발견하고, 여기서 특이한 무자열은 인증을 통과했을때의 문구를 나타낸다. 후에 call과 jnz가 어셈블리코드에 나타나고, jnz에서 실행이 되면 암호와 불일치했을 경우 실행될 화면이 표시가 된다. 그리고 call안에서 실행이 되어 암호와 다를 경우에도 암호를 맞췄을 경우와 같은 다음실행이 될 수 있게 할 수 있다는 것을 알 수 있을 것이다.

4. 대응방안

공격자가 OllyDbg 프로그램을 사용하여 파일 자체 내의 hex값이나 레지스트리 값을 변경하여 인증을 우회하여 간편 결제 시스템을 통과할 때 효율적으로 대응하기 위해서 빅데이터를 활용한 이상 징후 패턴 분석 기법을 제안하고자 한다.



(그림 2) 빅데이터를 활용한 대응방안

간편 결제 우회 공격에 대한 시나리오를 막는 대응 방안으로는 인증을 허가해줬을 때 데이터베이스에 인증 파일에 대한 정보를 수집하여 둔다. 이때 수집된 파일의 제어 정보에는 패킷의 길이와 프레임의 크기 등 데이터 링크 계층과 네트워크 계층에서 확인 할 수 있는 파일 정보를 저장한다. 이때 공격자가 인증을 우회하여 사용자의 정보 유출 및 결제를 시도 하는 순간 생겨난 패킷 및 로그를 빅데이터 플랫폼의 플럼, 카프카를 활용하여 결제 시 인증 파일에 대한 패턴을 추출한다. 그다음 맵리듀스의 빠른 속도를 이용하여 데이터 마트를 구성하여 기존에 저장해둔 파일과 비교를 한다. 그다음 일반적인 행동 패턴 데이터베이스와 이상 징후 패턴 데이터베이스를 구분하여 이상 징후 패턴 데이터베이스와 일치하는 공격일 경우 인증 파일을 다시 인증을 받도록 잠금 장치를 걸어버리면 인증 우회에 대한 대응 방안이 된다, 또한 간편 결제 시스템이 증가하는 시점 다양한 공격 시나리오들을 계속하여 저장하여 다양한 패턴의 공격까지 빅데이터를 활용하여 대비 할 수 있도록 한다.

5. 결론

이번에 새로 나올 간편결제 'exe'프로그램의 인증 방식은 어떠한 방법으로 나올지 아무도 모르고 있다. 그렇지만, 새로운 인증방법이 출시 될 때마다 해커들은 다양한 우회기법으로 크랙을 시도한다.

본 논문에서는 비교적 간단한 방법으로 'exe'파일을 만들어 인증우회를 시연하였고, 실제 출시 될 간편결제 'exe' 파일은 본 논문에서 크랙하여 인증을 우회한 exe 파일보다 암호화 기법이 몇 겹 있을것이라 예상이 된다. 하지만, 기존의 암호화 기법과 이미 인증 우회에 성공된 암호화 방법으로 출시가 되면 본 논문에서 보여준 방법과 더불어 쉽게 인증 우회를 할 수 있을 것이라 생각되지만, 오랜기간 사용하던 방법에서 새로운 방법이 출시되는 만큼 보안성이 뛰어난 간편결제 'exe' 파일이길 기대해 본다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)

참고문헌

[1] Jae-beom Park, Huy-kang Kim, Eu-jin Kim, "Design and implementation of the honeycomb structure visualization system for the effective security situational awareness of large-scale networks", JKIISC, Vol. 24, No. 6, pp. 1197-1213, 2014.

[2] Yang-min Lee, Mi-Yang Cha, Jae-kee Lee, "Development of Update Methods for Configuration Data of NETCONF Protocol considering Multiple Network Administrators", ISSN, Vol. 14, No. 5, pp. 27-38, 2013.

[3] Lee Hyeonjong, "Use of Big Data Hadoop platform", J-KICS , Vol. 29, No. 11, pp. 43-47, 2012.

[4] Song-young Kim, "A study on the security policy improvement using the big data", JKIISC, Vol. 23, No. 5, pp. 969-976, 2013.