

코드 난독화와 예측 불가능한 프로시저를 통한 자동화된 악성코드 방지 기법†

최진춘, 맹영재, 양대헌

인하대학교 정보보호연구실

Prevention Method of Malware using by Code Obfuscation and UnPredicatable Procedure

Jinchun Choi, YoungJae Maeng, DaeHun Nyang

Information Security Research Laboratory, INHA University

요 약

코드 난독화(Code Obfuscation) 기법은 프로그램의 저작권을 보호하거나, 역공학(Reverse Engineering) 등의 기법에 대응하는 방법중에 하나이다. 국내의 전자금융거래에 있어서, 악성코드가 설치된 컴퓨터에서 행해지는 MITB(Man-In-The-Browser) 공격에는 아직 취약한 상태이다. 이 논문에서는 코드 난독화를 이용해 MITB 공격에 대응하는 방법에 대해 제안한다.

I. 서론

최근에 국내 전자금융거래의 이용 현황은 꾸준한 증가세를 이어가고 있다. 한국은행이 발표한 2012년 국내 인터넷 뱅킹서비스 이용현황에 따르면 2012년 3월 말, 현재 19개 금융기관에 등록된 인터넷 뱅킹 이용 고객 수는 8,015만 명으로 전분기말(7,482만 명)에 비해 7.1% 증가하여, 꾸준한 증가세를 보여주고 있다. 또한 2012년 1/4분기 중 인터넷 뱅킹 이용건수 및 금액은 4,523만 건, 33조 1,814억 원으로 전년대비 각각 9.5% 및 0.5% 증가하였다.^[5]

이러한 전자금융거래에서는 사용자의 비밀과, 거래를 공격자로부터 보호하는 것이 중요한데, 이를 위한 각종 보안 프로토콜과 보안 프로그램

이 사용자를 보호함으로써 현재 전자금융거래가 가능하게 하고 있다.

하지만 현재 사용되고 있는 보안 프로그램들은 MITM(Man-In-The-Middle)의 일종인, 2007년 Philipp에 의해 이름 붙여진 공격인, MITB(Man-In-The-Browser) 공격에 대해서는 무방비 하다는 사실이 2010년 맹영재 등의 논문에서 실험으로 밝혀진 바 있다.^{[1][6]}

이 공격은 [그림 1]과 같이 사용자와 PC 사이에 보여지는 정보를 조작함으로써 발생하는 공격이다. 사용자에게는 정상적인 전자금융거래 과정이 수행되는 것처럼 보이지만, 실제로는 악성프로그램에 의해 변조된 문서의 내용이 보여지는 것이다.

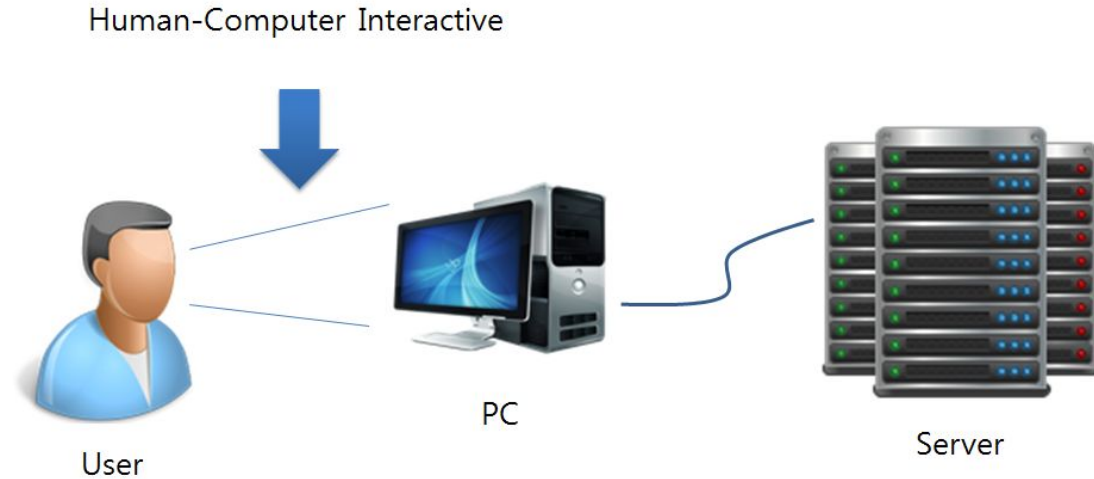
MITB 공격은 사용자의 컴퓨터에 악성 프로그램이 설치되었다는 가정 하에 가능한 공격이다. 이는 국내에서 ActiveX 또는 다양한 형태의 플러그인의 사용이 사용자들에게 프로그램

† 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었습니다(2012-0002146)

설치를 서비스를 제공받기 위한 하나의 절차로 인식되는 환경 속에서 악성 코드의 배포는 그만큼 쉬워졌다고 할 수 있다.

2.2 MITB 공격에 대응하는 기법

MITB 공격은 공격자에 의해 설치된 악성코드가 사용자의 컴퓨터에서 사용자의 눈을 속이



[그림 1] 사용자와 PC 간의 수행되는 HCI

이 논문에서는 국내 전자금융거래에서 발생할 수 있는 MITB 공격에 관련된 연구에 대한 논의와, 그에 대응하는 기존 기법에 대한 논의, 그리고 코드 난독화와 예측 불가능한 프로시저를 이용한 방법을 제안한다.

II. 관련 연구

2.1 코드 난독화

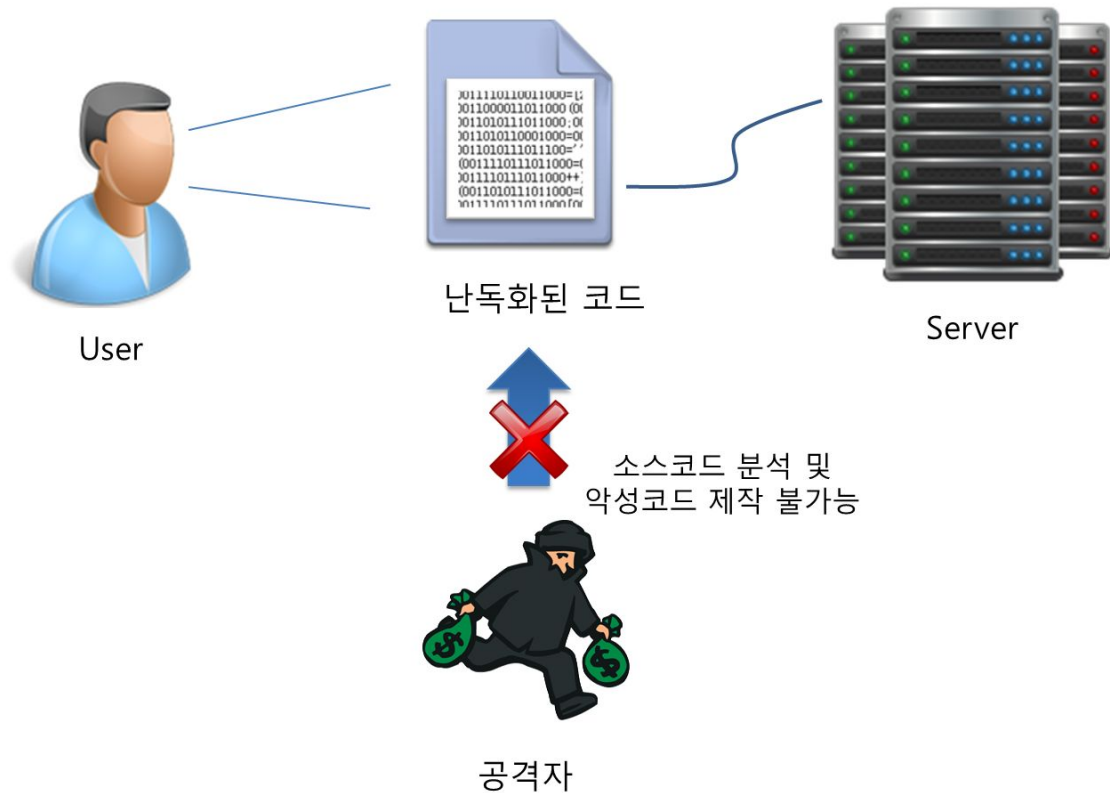
코드 난독화는 프로그램의 소스코드를 역공학을 이용하여 복제하거나, 임의로 변경하는 것으로부터 보호하기 위한 목적으로 사용한다.^[3] 또는 악성 프로그램이 Anti-Virus 프로그램의 검사를 피하기 위해 자신 스스로를 난독화 하는데에 사용되기도 한다. 일단 소스코드가 난독화 되면 사람의 눈으로는 프로그램의 구성이나 흐름이 거의 파악하기 힘들어진다. 하지만 코드 난독화로는 소스코드의 분석을 완전히 막을 수는 없다. 역공학이나 역난독화 등의 분석에 충분히 많은 시간을 투자한다면 어느 정도 수준까지는 프로그램 분석이 가능하다.^[7] 코드 난독화의 과정은 해당 프로그램의 Control-Flow와 Data-Flow를 각종 알고리즘을 통해 재배치하여 역난독화 도구나, 사람의 분석을 어렵게 만든다.

는 공격 방법이기 때문에, 사용자는 공격자가 보여주는 변조된 화면을 서버에서 보내준 정상적인 거래 화면으로 인식하고 전자금융거래를 진행하게 된다. 이러한 문서 변조방법이 가능한 것은 악성 프로그램의 동작이 전부 자동화 되어있기 때문인데, 이러한 공격 방법에 대응하는 기존의 노력들은 다음과 같은 것들이 있다.

먼저 추가적인 장치를 이용하는 방법이 있는데, ZTIC(Zone Trusted Information Channel)^[2] 같은 외부 디스플레이가 장착된 장치를 이용하여, 사용자의 거래 내용을 확인하고, 두 개의 버튼을 이용해 전자금융거래의 승인 여부를 사용자가 직접 결정하도록 되어있다. MITB 공격에 효과적으로 대응하지만, 이를 위한 추가적인 기기의 발급이 필요하다는 부담이 있다는 점이 있다.

또 다른 방법으로는 일반적으로 사용되는 캡차(CAPTCHA)가 아닌, 김성호 등의 논문에서 제안된 문맥기반의 캡차를 이용한 방법이 있다.^[4] 문맥기반의 캡차를 이용함으로써 이미지 프로세싱 기법이나, 인공지능 기법을 이용하여 캡차를 읽어내는 방법에 대응하여 서버와 사용자 간의 신뢰성 있는 보안 정보 전송이 가능하다.

앞서 말한바와 같이 역난독화는 충분한 시간을 투자 한다면 코드 분석은 가능하다. 하지만



[그림 2] 서버에서 난독화된 코드를 전송

III. 제안하는 기법

서버와 사용자 사이의 전자금융거래에서는 HTML 문서의 각 개체들에 DOM 형태로 접근하고, 각종 플러그인과 통신하여 문서를 구성할 때 JavaScript 를 사용한다. JavaScript 는 컴파일 되지 않고, 소스코드가 웹 브라우저 프로그램에 의해 번역되어 사용자에게 보여주는 형태이기 때문에, 소스코드의 내용이 그대로 노출되게 된다.

이 논문에서 제안하는 방법은 캡차를 사용하지 않고, MITB 공격에서 공격자가 자동화 된 악성 프로그램을 만들지 못하게끔, [그림 2] 와 같이 JavaScript 내용을 난독화한 후 전송하여 소스코드 분석을 힘들게 하는 방법이다. 만약 난독화 되지 않은 코드라면 공격자는 짧은 시간 안에 해당 소스코드를 분석하여, 그에 맞는 자동화 된 악성코드를 제작할 수 있을 것이다.

공격자가 매번 역난독화를 하여 자동화 된 악성코드를 제작해야 한다. 문서변조를 통한 공격 특성상 악성코드는 실시간으로 동작해야만 한다. 직접 역난독화 과정에 개입하는 매우 능숙한 공격자를 가정하더라도, 사용자들이 입는 피해는 완전히 자동화 된 악성코드가 다수의 사용자에게 설치되어 일어날 수 있는 것보다는 많이 감소하게 된다.

그리고, MITB 공격에 필요한 공격코드는 사용자의 전체적인 전자금융거래 과정을 자동화 하여 따라할 수 있어야 하는데, 일반적인 사용자에게 보여주는 거래 과정 화면을 보여주고, 만약 일반적인 사용자로 보이지 않는 이상행동들, 예를 들면 마우스 이동이나 키보드 입력 같은 이벤트가 사람의 입력과는 많은 차이가 있다고 판단이 되는 경우에는 일반 사용자에게는 보여주지 않았던 캡차 과정을 중간에 추가하여

자동화 된 악성코드의 수행을 무력화 하거나, 일반적인 사용자와는 다른 거래 과정 순서를 보여주게 되면, 미리 만들어진 자동화 된 악성코드는 해당 프로시저를 통과할 수 없게 된다.

IV. 기존 기법과의 비교

문서변조를 통한 자동화된 악성코드를 대응하기 위해 한 금융 사이트에서는 전자금융거래 페이지 내의 각 입력 폼의 변수 이름을 매번 로딩할 때 마다 랜덤한 문자열 값으로 바뀌어서 사용자에게 보여주는 것을 확인할 수 있었는데, 이는 입력 폼의 변수 이름을 직접 접근하는 방식이 아닌, 입력 페이지 코드소스 내의 입력 폼들의 배열순서 등을 이용하여 접근하면 입력 폼의 변수 이름과는 상관없이 해당 입력 폼에 접근이 가능하기 때문에 MITB 공격에는 효과적으로 대응할 수 없는 것을 확인할 수 있었다.

V. 결론

이 논문에서는 전자금융 거래 시 문서 변조를 하는 자동화된 악성 코드에 대응하는 방법으로, 코드 난독화를 이용한 방법과 공격자가 예측 할 수 없는 프로시저를 추가하는 방법을 제안하였다. 이것은 기존의 대응방법인 ZTIC 같은 외부 입력장치를 사용하는 방법이나, 사용자에게 추가적인 입력 프로세스를 요구하는 캡차 등의 방법보다 보다 사용자의 편의성을 고려한 MITB 공격에 대응하는 방법이라고 할 수 있다.

향후 효율적인 JavaScript 난독화 도구 개발과, 공격자가 예측하기 힘든 프로시저에 대한 연구가 더 진행된다면 자동화 된 악성코드를 이용하여 문서를 변조하는 MITB 공격에 좀 더 효율적으로 대응할 수 있을 것이다.

[참고문헌]

[1] 맹영재, 신동오, 김성호, 양대현, “전자금융 거래에서의 문서변조 취약점 분석 및 대응

방법 고찰,” 한국정보보호학회, 정보보호학회지, 제20권 제6호 2010,12, page(s) : 17-27

[2] ZTIC(Zone Trusted Information Channel), <http://www.zurich.ibm.com/ztic/>

[3] Code Obfuscation, http://en.wikipedia.org/wiki/Code_obfuscation

[4] 김성호, 강전일, 김기태, 양대현, “문맥 기반의 캡차를 이용한 신뢰성 있는 인터넷 계좌 이체 방법,” 한국정보보호학회 동계학술대회, 제19권 제2호, 2009, page(s): 319-323

[5] 한국은행, “2012년 1/4분기 국내 인터넷뱅킹서비스 이용현황,” <http://www.bok.or.kr/contents/total/ko/boardView.action?boardBean.sdt=&boardBean.edt=&boardBean.searchColumn=&boardBean.searchValue=&menuNaviId=559&boardBean.menuid=559&boardBean.brdid=89158&boardBean.rnum=11&boardBean.categorycd=0&boardBean.cPage=2>

[6] Gühring Philipp (2007). "Concepts against Man-in-the-Browser Attacks," <http://www.cacert.at/svn/sourcerer/CAcert/SecureClient.pdf>

[7] Udupa, S.K. “Deobfuscation: reverse engineering obfuscated code,” Reverse Engineering, 12th Working Conference on, 7-11 Nov. 2005