한국통신학회논문지(J-KICS) '13-12 Vol.38B No.12
http://dx.doi.org/10.7840/kics.2013.38B.12.937

인터넷 익스플로러에서 사용자 정보 유출 가능성

이 상 호◆, 맹 영 재*, 양 대 헌**, 이 경 희°

Possibility of Disclosure of User Information in Internet Explorer

SangHo Lee◆, YoungJae Maeng*, DaeHun Nyang**, KyungHee Lee°

요 약

국내 인터넷 브라우저 시장 점유율 1위인 인터넷 익스플로러의 일부 버전에서 CORS(Cross-Origin Resource Sharing)를 이용한 사용자 정보의 유출이 가능함을 확인하였다. 이는 이전의 방법과는 달리 악성 프로그램 등의 설치 없이도 로그인한 계정의 정보를 유출할 수 있으며, 이를 이용하면 보안 프로그램의 영향을 받지 않고서도 SNS와 포털 사이트의 사용자 정보 혹은 계좌 정보나 카드 사용내역까지 얻을 수 있다. 인터넷 익스플로러 뿐만 아니라 일부 모바일 브라우저에서도 CORS를 이용한 공격이 가능함을 보였다. 이 논문에서는 인터넷 익스플로러로 접속한 은행사, 카드사, SNS, 포털 사이트를 대상으로 한 CORS를 이용한 공격으로 사용자 정보의 유출은 물론 2차 공격으로 이어질 수 있는 가능성과 개선방안을 살펴본다.

Key Words : Internet Explorer, CORS, User Information

ABSTRACT

Internet Explorer is the popular internet browser the most in domestic. In some version of Internet Explorer, user information could be leaked cause CORS(Cross-Origin Resource Sharing) Internet Explorer support. Different before, without setup a malicious program, attacker can get the user information even account information, credit card usage list and user information with SNS or internet portal site logged in regardless of secure program. Not only Internet Explorer but also mobile browser, it could be. In this paper, we make study of the potential disclosure of user information by attack using CORS, second attack and the way to improvement of vulnerability of CORS.

Ⅰ. 서 론

개인정보는 개인을 식별할 수 있는 정보이며, 이는 주민등록번호뿐만 아니라 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의거 이메일 또는 출신학교 역시 개인정보의 범주에 포함된다. 개인정보는 개인을 식별하는 정보이므로 유출시 명의 도용에 이어 2차, 3차 피해를 야기하며, 매년 이와 같

※ 본 연구는 인하대학교의 지원에 의하여 수행되었습니다.
◆ First Author : 인하대학교 컴퓨터정보공학부 정보보호 연구실, 181cm76kg245@gmail.com, 학생회원
° Corresponding Author : 수원대학교 전기공학과 부교수, khlee@suwon.ac.kr, 정회원
* 한국전자통신연구원 부설연구소 연구원, brendig@ensec.re.kr
** 인하대학교 컴퓨터정보공학부 부교수, nyang@inha.ac.kr, 정회원
논문번호 : KICS2013-10-428, 접수일자 : 2013년 10월 4일, 심사일자 : 2013년 11월 27일, 최종논문접수일자 : 2013년 12월 6일

은 사고로 인한 막대한 규모의 피해가 발생하고 있다[1]. 대표적인 예로 2011년 네이트 3500만 명, 2012년 KT 870만 명, 2013년 청와대 10만 명의 회원 정보 유출사건을 들 수 있으며, 이로 인한 흔한 피해로 스팸 메일과 스팸 문자를 꼽을 수 있다. 이메일 역시 법률에서 명시하고 있는 개인정보이며, 스팸 메일과 문자 역시 개인정보 유출에 따른 피해임이 분명하다. 이러한 기업 또는 단체의 고객정보 유출 사고의 경우 대량의 개인정보가 불법 유통의 과정을 거쳐 유포되는데 반해 특정 소수를 목표로 하는 공격의 경우 이를 통해 이득을 취하려는 공격자의 의도가 보다 더 명확하며 피해로 드러나는 시간이 더 짧다. 개인이 목표가 되는 공격의 대부분은 사용자 모르게 악성 프로그램을 설치하거나 혹은 사용자가 가짜 웹페이지에 접속하도록 하는 방법으로 PC 혹은 스마트 폰에 저장되어 있는 정보를 획득하였지만, 이 논문에서는 악성 프로그램의 설치 없이 인터넷 브라우저의 정책을 이용하여 사용자의 정보를 획득할 수 있는 가능성을 제시한다.

인터넷 익스플로러(이하 IE)의 일부 버전에서 XDR(XDomainRequest)과 XHR(XMLHttpRequest)에 대해 CORS(Cross-Origin Resource Sharing)를 지원하며, 이를 이용하면 사용자가 서버에 요청하는 정상적인 메시지와 같은 HTTP Request를 생성할 수 있다[2,3]. 생성된 HTTP Request를 서버에 요청하면 서버의 응답에서 공격자는 사용자가 로그인한 웹페이지의 사용자 정보를 획득할 수 있음을 실험을 통해 확인하였다.

이는 사용자 PC의 IE 뿐만이 아니라 스마트 폰의 모바일 브라우저를 통해서도 CORS를 이용해 정보를 획득할 수 있음을 확인하였다. 스마트 폰의 특성을 고려했을 때 스마트 폰이 공격의 대상이 될 경우 피해는 PC 못지않을 것이다.

국내 인터넷 브라우저의 IE 점유율은 2012년 12월 74.47%, 2013년 1월 기준 스마트폰 가입자는 3천3백만여 명에 달한다[4,5]. 따라서 국내 인터넷 브라우저 사용자 중 74.47%와 3천3백만 스마트폰 사용자는 CORS를 이용한 공격에서 자유롭지 못하다고 할 수 있으며, 이전에 비해 보다 더 간소한 방법으로 사용자 정보가 유출될 수 있다는 점은 치명적임에 틀림없다.

이 논문에서는 2장 IE에서 CORS를 이용한 공격이 가능한 원인을 살펴보고, 3장 CORS를 이용해 유출이 가능한 정보를 실험을 통해 확인한다. 4장에서는 개선 방안을 모색한다.

Ⅱ. IE의 위협모델

이 장에서는 IE의 CORS 정책을 살펴보고, 이 논문에서 고려하는 위협모델을 정의한다.

2.1. IE의 CORS 정책

XDR과 XHR은 서버와 클라이언트 간 HTTP, HTTPS 요청과 응답을 위해 제공되는 API이다. IE8, 9 버전에서는 XDR, IE10 버전에서는 XHR에 대해 CORS를 지원하고 있으며, IE에서 XDR 및 XDR 객체를 생성해 크로스 서버에 HTTP Request를 전송하면 서버는 사용자에 의한 정상적인 요청인지 공격자에 의한 요청인지 판단할 수 없다. 이 요청에 따른 서버의 응답에서 공격자는 의미있는 사용자 정보를 획득한다. 기타 인터넷 브라우저에서도 역시 CORS를 지원하지만 브라우저의 정책이나 보안 등급 등에 의해 공격자가 CORS를 이용한 사용자 정보의 획득에는 한계가 있다.

2.2. 위협모델 정의

이 논문에서 정의하고 있는 위협모델은 다음과 같다.

- CORS를 이용한 정보의 유출은 설치가 아닌 파일의 실행만으로 가능하며, IE에서 로그인된 웹페이지의 사용자 정보를 획득한다.
  CORS를 이용한 공격의 이점은 사용자의 PC에서 정보를 획득하기 위해 악성프로그램을 사용자 몰래 설치하는 이전의 공격과 달리 별도의 프로그램을 요구하지 않는다는 점이다. 일부 기관의 보안정책에는 악성 프로그램 또는 출처가 불분명한 프로그램의 설치를 허용하지 않지만 로컬에서 HTML 파일의 실행에는 제약을 두지 않는다.
- 공격자에 의해 전달된 HTML 파일의 실행은 보안 프로그램의 영향을 받지 않는다.
  사용자의 브라우저에서 CORS를 이용해 생성된 요청 메시지는 정상적인 요청 메시지와 다르지 않으며, 이는 사용자 PC의 안티 바이러스 및 개인정보보호 유출 방지 프로그램의 영향을 받지 않는다.
- 악성 HTML 파일의 요청에 따른 서버의 응답은 사용자의 브라우저에서 제공되는 스크립트에 의해 복호화 되며, 공격자는 평문의 정보를 획득할 수 있다.
  CORS를 이용한 사용자 정보 획득 공격 과정

을 그림 1에 도식화 하였다. 각각의 단계가 수행하는 작업은 다음과 같다.

- 공격자는 사용자가 로그인한 웹페이지에서 의미 있는 정보를 조회하는 스크립트를 전달한다. 일부 암호화되어 전달되는 경우 서비스 중인 웹페이지의 접속 시 제공되는 암·복호화 스크립트를 이용할 수 있다.
- 공격자가 전달한 스크립트는 사용자 PC의 브라우저에서 로그인한 웹페이지에 정보를 요청하는 정상적인 패킷을 생성하므로, 보안 프로그램에 영향을 받지 않는다.
- 서버는 정상적인 사용자의 요청에 응답한다.
- 일부 서버의 응답 역시 암호화 되어 사용자에게 전달되나 이는 사용자의 브라우저의 스크립트에 의해 자동으로 평문으로 복호화되며, 복호화된 평문의 정보는 공격자에게 전달된다. 공격자는 사용자 PC에서 전달된 내용 중 의미 있는 사용자 정보를 획득할 수 있다.

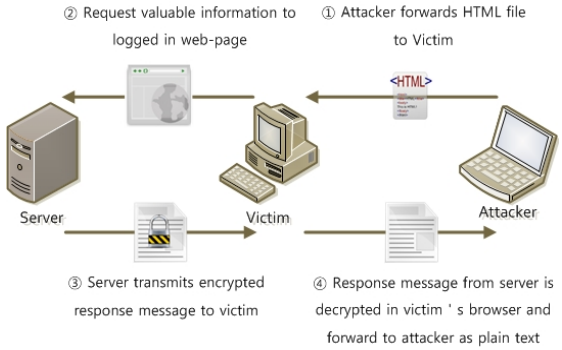

그림 1. CORS를 이용한 사용자 정보 획득 과정
Fig. 1. Process to get user information using CORS

2.3. 위협모델의 성공적 공격 방법

CORS 관련 보안 정책이 온라인 주소 상에서만 적용 가능하고, 로컬에서는 적용되지 않으므로 공격자는 사용자가 파일을 다운로드하여 실행하도록 해야 한다. 논문에서 고려하는 시나리오는 다음과 같다.

최근에 카드사는 사용자의 동의를 얻어 잔여 마일리지 안내 또는 카드 이용 명세서를 이메일을 통해 고객에게 제공한다. 정상적인 카드 이용 명세서의 경우 HTML 파일을 다운로드 한 후 로컬에서 실행하는 방법임을 착안하여 공격자는 CORS를 이용해 사용자 정보 획득을 목적으로 하는 악성 HTML 파일을 만들고, 카드결제 이용대금 명세서로 가장하여 사용자에게 전송한다. 사용자는 공격자로부터 정상적인 명세서로 위장한 메일을 수신하고 첨부파일을 다운로드하여 로컬에서 실행하면, HTML 파일은 사용자가 로그인한 웹페이지에서 의미 있는 정보를 조회하는 요청 메시지를 서버에 발신한다. 사용자의 요청에 따른 서버의 응답은 때에 따라서 암호화되어 전송되지만 사용자 브라우저의 스크립트에 의해 복호화 되며, 복호화된 사용자 정보는 공격자가 미리 설정해둔 서버에 수집된다. 공격자가 생성한 악성 HTML 파일은 사용자의 브라우저에서 서버에 정보를 요청하고 서버로부터의 응답을 다시 공격자에게 전달하는 일련의 과정을 자동화 하여 수행한다. 사용자는 이메일 주소, 휴대폰 번호부터 계좌 정보, 카드 사용내역에 이르기까지의 사용자 정보 유출을 눈치 챌 수 없다.

Ⅲ. CORS를 이용한 사용자 정보 유출

표 1. 각각의 웹페이지가 가지는 사용자 정보
Table 1. Web-pages with user information

	Information	Note
Bank	Account information	Xecure Web
Credit-card	Credit card payments list	Xecure Web
e-mail	Sent, received mail	
SNS	Blocked user list e-mail address	
Internet-shopping	Order history Change delivery address	
Mobile	Blocked user list	

CORS를 이용해 IE에서 로그인한 웹페이지의 정보 획득이 가능한지 표 1의 목록을 대상으로 실험하였다. 실험에는 그림 2와 같이 사용자, 공격자, 은행 서버와 공격자가 사용자의 정보를 얻기 위해 설정한 서버로 환경을 구성하였다. 각각은 네트워크를 통해 연결되어 있으며 서로 다른 망에 위치하고 있다. 공격자는 사용자 정보를 수집하는 서버를 외부에 설정함으로서 공격자와 사용자가 동일한 네트워크에 위치하는지 여부에 관계없이 사용자 정보를 수집하며 공격을 계속할 수 있다. 실험에 사용한 사용자의 IE의 버전은 각각 8.0.7601.17514, 9.0.8112.16421, 10.0.9200.16660IC 이다.

3.1. 은행 및 카드사

실험은 XecureWeb 암호화 방식을 사용하는 국

내 은행 네 곳, 국내에서 서비스 중인 외국계 은행 한 곳과 카드사 두 곳을 대상으로 진행하였다.

공격자가 사용자의 브라우저를 통해 로그인된 은행과 카드사의 웹페이지에서 사용자 정보를 획득하려 할 경우 서버와 클라이언트 간의 통신은 암호화를 통해 이루어지며 거래 시 설치되고 실행되는 키보드 보안, 공인인증서 보안을 위한 프로그램을 고려해야한다.

먼저 패킷 캡처 프로그램 Fiddler를 통해 실험에 대상이 되는 은행을 살펴보면, 다섯 곳 모두 계좌정보 조회를 위해 서버에 요청하는 메시지의 형태와 전송하는 데이터가 다름을 알 수 있다. 더불어 위 프로그램을 이용하면 웹페이지에 최초 접속 시 또는 로그인시 서버에서 데이터 암호화를 위해 제공하는 스크립트를 얻을 수 있다. XDR 및 XHR 객체를 이용하면 정상적인 계좌조회 요청과 같은 HTTP Request를 생성할 수 있으며, 이를 서버에서 제공하는 스크립트를 이용해 암호화할 수 있다. 이렇게 생성한 HTTP Request를 서버에 전송하면 서버는 수신한 HTTP Request가 사용자로 부터의 정상적인 요청인지 공격자에 의한 요청인지 구분할 수 없다. 서버로부터의 응답은 사용자의 웹브라우저 스크립트에 의해 복호화 되므로 공격자는 서버의 응답에서 의미 있는 사용자의 구체적인 정보(예금주, 계좌 번호, 잔액, 최종 거래일)를 획득할 수 있으며, 일부 은행에서는 사용자가 기업고객으로 등록되었을 경우 회사명, 사업자 등록 번호, 일일 거래 금액과 같은 추가적인 정보 또한 획득 할 수 있다. 더욱이 CORS를 이용한 공격은 로컬에서 발생한 정상적인 요청과 같으므로 금융사가 제공하는 보안 프로그램과 로컬에서 실행중인 보안 프로그램에 영향을 받지 않는다.

이를 은행이 아닌 카드사의 웹페이지에 적용시킬 경우 공격자는 사용자가 소지하고 있는 카드의 종류와 카드 사용 내역을 모두 볼 수 있다. 공격자가 카드사의 웹페이지를 통해서 획득 할 수 있는 정보는 카드의 사용 내역을 통해 경제적인 모든 활동을 조회 할 수 있다는 것과 더불어 위치정보 유출의 가능성을 가진다. 요즈음 발급되는 대부분의 신용카드와 체크카드에는 대중교통을 이용할 수 있는 교통카드 기능이 있으며, 카드사는 사용자가 이용한 대중교통의 내역만 따로 조회할 수 있는 서비스를 제공하고 있다. 그 내역에는 대중교통의 이용일자, 대중교통 수단, 승하차 역의 정보가 고스란히 남아 있어 피해자의 금전적인 활동 이외에도 이동경로 정보 획득을 통해 사용자의 위치정보를 짐작해 볼 수 있을 뿐만 아니라 사용자 정보의 유출로 인한 사생활 침해로도 이어질 수 있다.

3.2. 메일

CORS를 이용하면 서비스에 로그인된 사용자의 IE에서 송·수신한 메일을 조회할 수 있다. 메일 조회의 경우 서버와 사용자간의 패킷이 암호화 되지 않으므로 은행과 같이 별도의 암·복호화 스크립트가

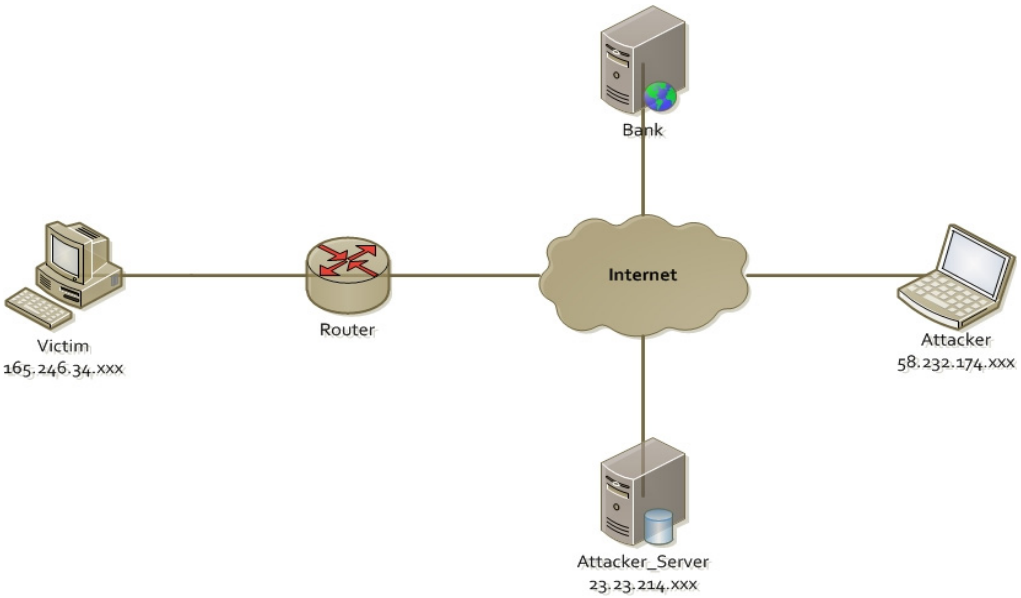

그림 2. 실험을 위해 구성한 네트워크 환경
Fig. 2. Test bed for experiment

불필요하며, 공격자가 메일의 내용을 획득함이 보다 수월하다. 실험에는 국내외 이메일 서비스를 제공하는 포털 사이트 각각 1곳을 대상으로 진행하였으며, 두 곳 모두 IE에 로그인된 웹페이지에서 이메일의 내용을 획득 할 수 있었다.

3.3. SNS

공격의 타깃을 SNS로 하였을 때, 공격자가 획득할 수 있는 사용자 정보는 두 가지를 생각해 볼 수 있다. 첫째, 사용자가 SNS상에서 차단하고 있는 사용자 목록과 둘째, 이메일 주소이다. 국내 서비스 중인 한 SNS에서는 설정을 통해 다른 사용자를 차단함으로서 더 이상 차단된 사용자와 커뮤니케이션을 하지 않도록 하는 기능을 제공한다. 이는 SNS의 성격상 설정한 사용자만 조회 할 수 있도록 해야 한다. 또 다른 SNS는 회원 가입 시 입력했던 이메일 주소를 아이디로 사용하며, 이 이메일 주소는 해당 SNS 정책상 비공개를 원칙으로 하고 있다. CORS를 이용하면 SNS 내 사용자가 설정한 또는 비공개로 설정된 정보를 얻을 수 있다.

3.4. 인터넷 쇼핑몰

국내의 한 포털 사이트는 23,000여개의 인터넷 쇼핑몰을 하나의 아이디로 통합 관리할 수 있는 서비스를 제공하고 있다. CORS를 이용하면 IE에서 로그인한 포털 사이트를 통해 사용자가 구매한 내역을 조회 할 수 있다. 더불어 단순히 구매 내역의 조회뿐만 아니라 정보의 변경도 가능해 CORS를 이용한 사용자 정보의 유출과 더불어 공격으로 인한 금전적인 피해가 일어날 가능성이 있다.

실험은 CORS를 이용하여 구매한 물품의 배송지 정보를 변경할 수 있음을 확인한다. 포털 사이트가 제휴하는 인터넷 쇼핑몰은 구매한 물품의 배송이 시작되기 전까지는 물품의 배송지 정보를 변경할 수 있다는 것을 알고 실험을 위해 판매중인 상품을 임의로 선택해 주문하였다. 먼저 공격자는 사용자의 구매 목록을 조회할 수 있다. 조회된 내용 중 상품이 배송 전 단계인 입금확인 중 또는 결제 완료인 단계의 상품만 추출한다. 공격자는 배송지 정보를 변경하기 위해 생성하는 HTTP Request는 단순히 변경될 배송지 정보만이 아니라 기타 상품에 대한 정보와 같이 일정한 형식을 갖추어 서버로 요청함을 패킷 캡처 프로그램 Fiddler를 통해 관찰 할 수 있다. 포털 사이트 역시 서버와의 통신이 암호화 되지 않으므로 서버가 요구하는 값을 조회를 통해 얻을 수 있으며, 이 값과 새로운 배송지 정보 값을 XDR, XHR 객체를 이용해 HTTP Request를 만들어 서버에 요청한다. 공격자는 전 과정을 자동으로 실행하는 HTML 파일을 만들고 정상적인 명세서로 위장하여 사용자에게 전달한다. 실행 결과 배송지 정보가 변경되었음을 알 수 있다.

3.5. 모바일 브라우저

앞의 실험은 사용자 PC의 IE를 대상으로 사용자 정보 획득을 목적으로 하는 공격이다. IE의 XDR 및 XHR 객체가 지원하는 CORS를 이용한 공격인데, 일부 모바일 브라우저에서도 위와 같은 공격이 가능함을 실험을 통해 알 수 있었다. 실험은 3.3절의 로그인된 SNS 계정에서 차단된 사용자 목록을 획득하는 공격과 같다. 실험은 안드로이드 마켓에서 천만회 이상의 다운로드가 된 모바일용 브라우저를 사용하였으며, 해당 모바일 브라우저는 web-kit 엔진을 사용하는 것으로 확인하였다. 실험에는 해당 SNS가 제공하는 전용 어플리케이션이 아닌 앞서 설명한 모바일 브라우저에서 로그인 하였다. 로그인한 계정에는 실험의 결과 확인을 위해 임의의 사용자를 미리 차단해 두었다. 이후에 정상적인 명세서로 위장한 HTML 파일을 공격자로부터 전달 받았다는 가정 하에 같은 모바일 브라우저에서 실행 하였다. 실험의 결과를 통해 해당 모바일 브라우저는 CORS를 지원하는 것을 알 수 있다.

이는 모바일 브라우저에서 로그인한 SNS만이 아닌 해당 모바일 브라우저를 통해 이루어지는 모든 활동에 대해서 공격이 가능함을 시사 하는 점에서 의미를 갖는다.

Ⅳ. CORS의 한계와 개선 방안

앞서 3장을 통해 CORS를 이용한 사용자 정보 수집이 가능함을 보였다. 이 장에서는 CORS를 이용한 공격의 한계와 개선 방안을 제시한다.

4.1. CORS를 이용한 사용자 정보 유출의 한계

앞의 CORS를 이용해 공격에 성공한 사례는 모두 서버에게 단순한 조회를 요구하는 경우였다. 대체로 단순 조회의 경우 서버는 이미 로그인된 사용자에게 추가적인 정보를 요구하지 않으며, 공격의 대상이 되었던 웹페이지 역시 로그인 상태에서는 사용자 신원 확인을 위한 추가적인 정보를 요구 하지 않았다는 점이 공격을 가능하게 하였다. 물품의

배송지 정보를 변경하였던 사례 역시 사용자가 로그인 되어있으면 사용자 인증을 별도로 거치지 않으며, 배송지 정보 변경 후에도 사용자의 메일이나 혹은 문자 알림과 같은 서비스가 제공되지 않기 때문에 사용자 스스로 확인하지 않는 한 쉽게 눈치 채지 못한다.

대부분의 IE에서 접속 가능한 모든 웹페이지가 CORS를 이용한 공격에 가능하지만, 항상 그렇지는 않다. 한 예로 요즈음 인터넷을 통해 등본 출력과 같은 민원을 처리할 수 있는 온라인 서비스가 제공되고 있다. 해당 사이트에 접속하여 로그인 후 문서 출력 혹은 정보 조회와 같은 민원을 요청하면 해당 사이트에서는 공인인증서를 통해 본인을 한 번 더 인증하는 절차를 거친다. 물론 민원을 요청하는 HTTP Request를 XDR 혹은 XHR 객체로 생성하여 서버에 요청할 수 는 있지만, 단순히 CORS를 지원하는 객체만으로는 서버가 요구하는 추가적인 본인인증에 답을 할 수 없다.

4.2. 개선 방안

3장의 실험과 CORS가 가지는 한계를 바탕으로 CORS에 의한 사용자 정보 유출 피해를 줄일 수 있는 정책을 이용하는 개선 방안을 제안한다. 첫째, 서버의 추가적인 사용자 정보 요구에는 공격자가 답할 수 없다는 점을 이용할 수 있다. 일부 민감한 개인정보의 경우, 사용자에게 추가적인 인증을 요구함으로써 CORS에 의한 사용자 정보 유출을 제한할 수 있다. 조회는 모든 사이트에서 빈번하게 일어나는 작업 중 하나이므로 매번 사용자에게 본인 인증을 요구하는 것 역시 발생하는 트랜잭션과 가용성을 고려해야 한다. 둘째, 서비스를 통해 변경사항에 대한 알림을 제공할 수 있다. 이로서 최소한 정상적인 사용자로 하여금 조회 또는 변경 사항에 대해 확인할 수 있게끔 할 수 있다. 셋째, 구글의 브라우저 크롬의 경우 CORS를 허용하지만 브라우저의 정책에 의해 공격을 성공 할 수 없다. 크롬 실행 시 웹 보안 비활성 옵션을 추가하여 실행함으로서 사용자 정보를 획득할 수 있지만 웹 보안 비활성 옵션을 추가하여 크롬이 실행하도록 하는 추가적인 스크립트 파일을 고려하면 공격자의 입장에서는 공격을 계속하기가 현실적으로 어렵고 까다로워진다. 이 점을 이용하면 CORS를 허용하되 기본적으로 비활성화 하여 잠재적인 피해의 규모를 줄일 수 있다. 한국인터넷진흥원의 '모바일 접속환경을 위한 웹사이트 침해예방 연구'[6]에서 자바 스크립트 코드에 대해 검증 절차의 마련을 CORS의 대응 방안으로 제시하였다. 하지만 이 연구에서와 같이 피해의 대상이 서버가 아닌 PC임을 고려하면 사용자가 스크립트 코드의 검증 후 실행하는 방법에 비해 조회 또는 변경 사항을 알리는 것이 클라이언트 사이드에서는 보다 현실적이며, 상기 정책의 활용으로 제한을 둠으로서 잠재적인 피해를 줄이는 것 또한 예방의 측면에서 의미를 가진다.

V. 결 론

개인적인 정보의 유출은 유출된 정보만으로도 치명적이지만 이를 이용하는 추가적인 공격의 가능성이 있다. 이는 피해자의 금전적인 부분 혹은 사생활과 직·간접적으로 연관되기 때문에 공격으로 인한 사용자 정보 유출의 피해 범위를 가늠할 수 없으며, 사용자 정보의 불법 유통과 유포 역시 무시할 수 없는 잠재적인 피해임에 틀림없다. 이전의 공격과 달리 이 논문에서는 IE의 정책을 이용하여 사용자 정보 유출을 HTML 파일 하나로 가능하게 했으며, 간단하지만 무시할 수 없는 결과를 낳는다. 더불어 공격이 불가능했던 웹페이지의 특징을 보면 추가적으로 사용자를 인증하려는 과정이 있었으며, 이는 공격을 계속 할 수 없었다는 점에서 의미를 갖는다. 뿐만 아니라 이 논문을 통해 CORS를 이용한 사용자 정보 유출의 피해를 예방하고 줄일 수 있도록 하는 개선 방안을 제안하였다. 이메일에서 개인 식별 코드까지의 어떠한 형태의 개인정보도 유출 후에는 악용의 소지가 있으며, CORS을 이용한 사용자 정보 유출 공격의 개선을 위한 적용방안의 필요성과 더불어 이를 보호하려는 개인 스스로의 노력 또한 절실하다.

References

[1] Korea Communications Commission, *The number of consultation about abused personal information(2013)*, retrieved Sep., 15, 2013, from http://www.index.go.kr/egams/stts/jsp/potal/stts/PO_STTS_IdxMain.jsp?idx_cd=1366&bbs=INDX_001&clas_div=A.

[2] J. Lam and J. B. Ullrich, *Cross Site Request Forgery: What Attackers Don't Want You to Know(2013)*, Retrieved Sep., 15, 2013, from

http://www.sans.org/reading-room/whitepapers/application/appsec-cross-site-request-forgery-attackers-33108.

[3] World Wide Web Consortium, *Cross-Origin Resource Sharing(2012)*, Retrieved Sep., 15, 2013, from http://www.w3.org/TR/2012/WD-cors-20120403/.

[4] StatCounter, *Top 5 Browsers in South Korea on Dec 2012(2013)*, Retrieved Sep., 15, 2013, from http://gs.statcounter.com/?chart_type=line&statType_hidden=browser&region=Worldwide&region_hidden=ww#browser-KR-monthly-201212-201212-bar.

[5] Korea Communications Commision, *Wired and wireless communication service subscriber statistics(2013)*, Retrieved Sep., 15, 2013, from http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=60400&dc=&boardId=1030&boardSeq=36008.

[6] KISA, *A Study on Prevention of Infringement of Web Sites for Mobile Access Environment(2010)*, Retrieved Sep., 15, 2013, from http://www.kisa.or.kr/public/library/reportView.jsp?regno=017161&pageIndex=13&searchType=&searchKeyword=.

이 상 호 (SangHo Lee)

2013년 2월 공주대학교 정보통신공학과 졸업

2013년 3월~현재 인하대학교 컴퓨터정보공학과 석사과정

<관심분야> 시스템 보안, 웹 보안

맹 영 재 (YoungJae Maeng)

2006년 8월 인하대학교 컴퓨터정보공학과 학사

2008년 8월 인하대학교 컴퓨터정보공학과 석사

2008년 9월 인하대학교 컴퓨터정보공학과 박사과정

2012년 4월~현재 한국전자통신연구원 부설연구소 연구원

<관심분야> 무선 센서 네트워크, 웹 보안, 사용자 인증, 금융 보안

양 대 헌 (DaeHun Nyang)

1994년 2월 한국과학기술원 과학기술 대학 전기 및 전자공학과 졸업

1996년 2월 연세대학교 컴퓨터과학과 석사

2000년 8월 연세대학교 컴퓨터과학과 박사

2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원

2003년 2월~현재 인하대학교 컴퓨터정보공학과 부교수

<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, 네트워크 보안

이 경 희 (KyungHee Lee)

1993년 2월 연세대학교 컴퓨터과학과 학사

1998년 8월 연세대학교 컴퓨터과학과 석사

2004년 2월 연세대학교 컴퓨터과학과 박사

1993년 1월~1996년 5월 LG 소프트(주) 연구원

2000년 12월~2005년 2월 한국전자통신연구원 선임연구원

2005년 3월~현재 수원대학교 전기공학과 부교수

<관심분야> 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식