한국컴퓨터정보학회 동계학술대회 논문집 제19권 제1호 (2011. 1)

HTTP 프락시를 활용한 인증정보 전달 안전성 분석

김문선°, 안경진*, 이형효*
°*원광대학교 정보전자상거래학부
e-mail: {kjahn}@wku.ac.kr

Security Analysis of Authentication Information in Transit using HTTP Proxy

Moon-Sun Kim°, Kyung-Jin Ahn*, Hyung-Hyo Lee*
°*Div. of Information and e-Commerce, Wonkwang University

● 요 약 ●

국내 주요 포탈사이트들은 SSL 보안프로토콜을 통해 ID/PW 방식의 사용자 인증정보를 전달하게 된다. 본 논문에서는 설정된 SSL 채널을 통해 전달되는 웹 브라우저와 포털 사이트 간 인증정보를 HTTP 프락시인 Paros를 이용하여 안전성을 분석한다.

키워드: Authentication Information, SSL, Man-in-the-Middle Attack, HTTP Proxy

I. 서 론

현재 대부분의 웹 사이트가 ID/PW 기반의 인증 수행을 하고 있다. 하지만 ID/PW가 보호되지 않은 상태에서 전달되는 경우 스니핑 위협으로부터 취약하고 신원 도용으로 연결될 수 있다[2]. 최근 국내 주요 포털사이트에서 ID/PW 인증정보의 안전한 전달을 위해 SSL 프로토콜을 이용한 보안접속 기능을 제공 중이다.

II. 관련 기술

2.1 SSL(Secure Socket Layer)

SSL(Secure Socket Layer)은 넷스케이프사가 개발했으며, 대칭키 암호시스템을 이용하여 중요 정보를 암호화함으로써 안전한 통신서비스를 제공한다. SSL은 응용계층과 전송계층 사이트에서 동작하며, 데이터에 대한 암호기능 외에 데이터의 무결성 보호와 출처인증, 서버와 클라이언트 인증 서비스를 제공한다[2].

그림 1. SSL의 동작위치

2.2 HTTP 프락시: Paros

프락시 서버는 PC 사용자와 인터넷 사이에서 중개자 역할을 수행하는 서버로서, 보안이나 관리적 차원의 규제 그리고 캐시 서비스 등을 제공한다. 프락시 서버는 기업의 네트워크를 외부 네트워크로부터 분리시켜주는 게이트웨이 서버, 그리고 기업의 네트워크를 외부의 침입으로부터 보호하는 방화벽 서버 등과 관련이 있거나, 또는 그 일부가 된다.

Paros는 Java기반이고, 프락시로서 작동함으로써 서버와 클라이언트 간 HTTP 및 HTTPS 데이터, 쿠키, 폼필드 등이 인터셉트되고 수정될 수 있도록 되어있다[4]. 또한, Scanner, Filter, Trapping HTTP requests and response, Other functions 들을 제공해 줌으로써 웹 사이트 구조분석 및 취약점 체크, 테스트 등이 가능하다.

III. Paros를 이용한 인증정보 취약점 점검

3.1 Paros 동작환경 설정

웹 클라이언트와 서버 사이에 HTTP 프락시 연결 설정은 [인터넷 옵션]-[연결]-[LAN 설정]에서 프락시 연결에 체크 해주고, 프락시 서버가 작동하는 IP주소와 포트번호를 입력한다.

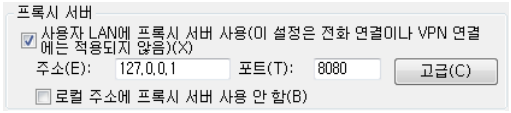

그림 2. 프락시 서버 연결 설정

HTTP 헤더에는 User Agent, 또는 User Agent String이라는 것을 가지고 있다. 이것은 웹 페이지에 접속했을 때 서버에게 웹 브라우저의 종류와 버전, OS 등을 알려주는 역할을 한다.

Paros는 기본적으로 User-Agent 헤더 안에 프락시 서버로 연결되는 서버에게 자신의 동작 정보를 서버에게 알려주고 있다. 최근 대부분의 포털사이트는 Paros와 같은 프락시 서버를 공격을 위한 도구로 분류하여 프락시로 접속하는 모든 연결에 대해서 차단한다.

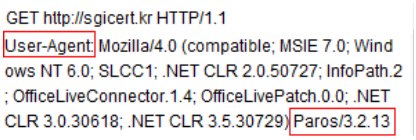

그림 3. Paros의 User-Agent 헤더

그러므로 naver나 daum과 같은 국내 유명 포털사이트는 프락시 서버로의 접속을 막고 있기 때문에 Paros 속성에 "-nouseragent" 옵션을 추가 해주어 자신의 동작여부를 숨겨 접속할 수 있다.

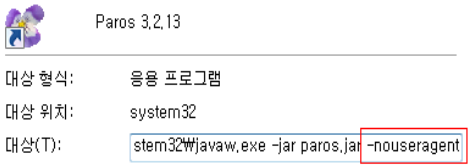

그림 4. Paros -nouseragent 옵션

최근 보안 사고가 급증하고 개인정보의 가치가 중요하게 인식되면서 많은 웹 사이트에서는 웹 서비스를 받기 위해 수행되는 인증 수단으로 널리 사용 중인 ID/PW 기반의 인증 방식에서 인증정보의 안전한 전달 위해 SSL 프로토콜을 이용하여 보안서비스를 제공해주고 있다.

그림 5와 같이 웹브라우저에서 프락시를 경유하여 서버에 접속하게 되면, 웹브라우저-프락시, 프락시-웹 서버 간의 SSL 채널이 2개가 생성되며 둘 간의 모든 정보를 중간에 위치한 프락시 서버를 경유하여 전송되기 때문에 ID/PW 인증정보가 유출 될 수 있다.

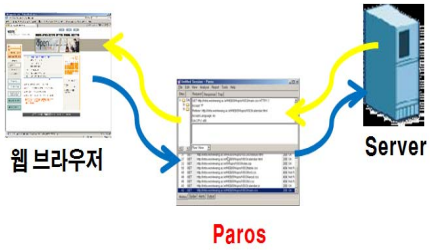

그림 5. Paros 동작 구조

웹브라우저-프락시, SSL연결 시 사용자가 사용하고 있는 웹브라우저는 프락시가 보낸 인증서가 검증과정 중 검증이 되지 않기 때문에 아래와 같은 인증서의 오류를 알려주어 사용자로 하여금 해당 서버에 접속 유무를 물어보게 된다. 이 경고를 무시하고 사용자가 해당 접속을 계속 진행한다면 사용자의 인증정보가 프락시로 전달된다.

그림 6. 보안 인증서 오류

3.2 국내외 주요 포털사이트 대상 실험

SSL 프로토콜 이외의 ID/PW의 인증정보가 암호화되지 않고 전송되는 사이트들은 국내 포털 daum과 외국 메일서비스 gmail, 국내 유명 게임사이트 피망과 최근 사용자가 급증하는 외국 SNS 사이트 twitter를 확인해 보았다.

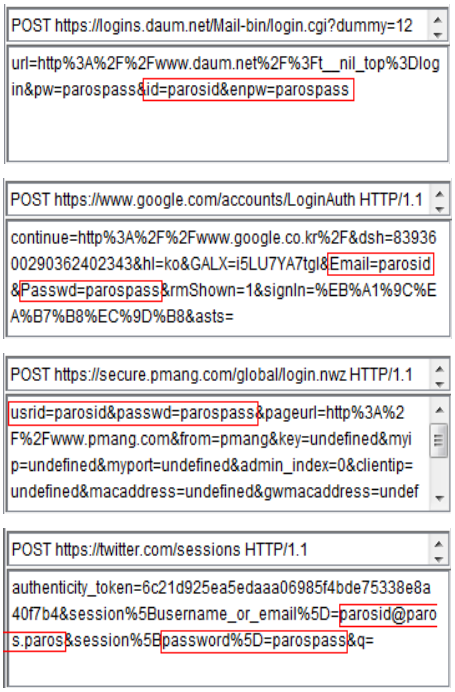

그림 7. 노출된 ID/PW 인증 정보

그림 7과 같이 암호화 되지 않은 ID/PW 정보는 프락시를 통해 서버에 전송된다. 결과적으로 중간에 있는 프락시 서버는 사용자의 인증정보를 알 수 있다. 이와 반대로 국내 포털사이트 naver와

cyworld의 인증정보를 보면, ID/PW 정보가 별도로 암호화되어 전송되기 때문에 사용자가 인증서 오류 경고를 무시해도 중간에 있는 프락시 서버는 사용자의 인증정보를 알 수 없다.

그림 8. 암호화된 ID/PW 인증 정보

인증정보가 안전하게 전달되는 경우는 SSL 채널을 통과하기 전 naver와 cyworld의 경우는 ASP를 이용하여 응용계층에서 서버의 특정키로 암호화하여 전송하기 때문에 ID/PW 인증 정보를 프락시 서버에서는 알 수 없다. 또한 ActiveX를 이용하여 특정 보안 프로그램을 작동시켜 ID/PW 인증정보를 암호화 할 수 있다.

3.3 ASP를 통한 ID/PW 암호화

ASP(Active Server Page)는 마이크로소프트사에서 개발한 서버 측의 스크립팅 환경이다[3]. 브라우저가 웹 서버에서 ASP 파일을 요청하면 서버는 프로세서를 호출하고, 프로세서는 요청된 파일을 읽고 스크립트 명령을 실행하여 결과를 웹페이지 형태로 브라우저에 전송한다.

예) ASP를 통한 naver 로그인

```
Set WSoc = Server.CreateObject("WinisSocket.Soc")
'오브젝트를 생성한다.
WSoc.CodeInput("코드번호")
'발급 받은 코드번호를 등록한다.
WSoc.HeaderAdd ("Referer")
'헤더 등록.
WSoc.ParamAdd ("enctp"),("2")
'네이버에서 로그인시 필요로 하는 값.
WSoc.ParamAdd ("encpw"),("")
'네이버에서 로그인시 필요로 하는 값.
WSoc.ParamAdd ("svctype"),("0")
'네이버에서 로그인시 필요로 하는 값.
WSoc.ParamAdd ("postDataKey"),("")
'네이버에서 로그인시 필요로 하는 값.
WSoc.ParamAdd ("saveID"),("")
'네이버에서 로그인시 필요로 하는값.
WSoc.ParamAdd ("id"),("아이디")
'네이버에서 아이디.
WSoc.ParamAdd ("pw"),("비밀번호")
'네이버에서 비밀번호.
```

naver는 정해진 하나의 키 값으로 로그인을 시도하는 사용자에게 키 값을 전송해주고, 키를 전달 받은 클라이언트는 서버가 전해준 키 값으로 ID/PW 인증정보를 암호화하여 전송한다. 이로 인해 프락시 서버에서는 사용자가 입력한 ID/PW 인증정보는 볼 수 없고 브라우저에 의해 암호화된 값만 볼 수 있다.

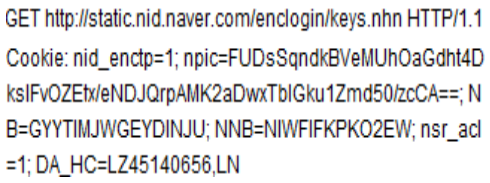

그림 9. naver의 암호화 키

본 논문에서 제안하는 알고리즘들은 1차 연구 방향으로서 센서들의 특성상 단방향 탐색방법에 대해 살펴본다. 일반적으로 단방향 탐색방법은 시작노드에서 목표노드 방향으로만 탐색을 수행하는 방법이다. 그 외 탐색방법으로 양방향 탐색방법으로서 시작노드와 목표노드 양쪽에서 반대편 노드로 탐색을 동시에 수행하는 방법이 있다. 본 연구에서 제안하는 알고리즘SNSP(Sensor Network Shortest Path)은 다음과 같다.

초기 step, round 값은 0이며, 시작노드를 중심으로 이웃한 노드까지의 비용을 초기화 값으로 설정하며, 그 이외의 노드는 ∞로 초기화 한다.

1) 시작노드를 이용한 DFS로, 시작노드에서 목표노드로 stack을 이용하여 탐색한다.
2) round가 1이면 시작노드의 이웃노드들의 비용으로 초기화하며, 그 이외의 노드는 ∞로 설정한다. round가 1이 아니면 시작노드의 이웃노드들의 비용을 이전 비용에 추가한다.
3) round는 시작 할 때마다 1씩 증가한다.
4) 현재 노드가 목표노드가 아니면 현재노드를 중심으로 최소 비용의 이웃 노드를 선택하여 비용을 측정하여 이전 비용을 추가한다. 이때 이전노드에서 이웃노드의 비용이 더 적으면 적은 해당 노드 비용으로 대체한다. 이웃노드가 아닌 노드들에 대해서는 이전비용으로 초기화한다.
5) 지나간 노드 집합가운데 목표노드까지의 비용이 존재한경우 이웃노드값보다 비용이 작으면 그것을 최단거리로 선택하며, 없으면 다음 단계를 실행한다.
6) 목표노드가 도달하면 지금까지의 비용을 5)부터 실행하며, 그렇지 않으면 3)부터 수행한다.

Ⅳ. 결 론

본 논문에서는 HTTP 프락시인 Paros를 이용하여 설정된 SSL 채널을 통해 전달되는 웹 브라우저와 국내외 주요 포털 사이트 간 인증정보의 안전성을 분석하였다. 물론 웹 브라우저 사용자가 인

증서 오류 화면에서 계속 진행을 하지 않으면 ID/PW 인증 정보에 대한 스니핑은 불가능하지만 ID/PW 인증 정보를 암호화하여 전송하게 되면 스니핑을 하더라도 암호화된 값만 보이기 때문에 안전하게 인증 정보를 전송할 수 있고 인증 정보가 유출될 위험은 줄어든다. 인터넷을 사용하는 대부분의 사용자들은 보안에 대한 지식이 부족한 현실을 고려할 때 국내 웹 서비스 제공 사이트들에서 인증정보 보호를 위한 추가적인 보안대책이 요구된다.

참고문헌

[1] 정보보안 개론과 실습 - 인터넷 해킹과 보안, 양대일, 김경곤 공저

[2] 정보보안 개론과 실습 - 네트워크 해킹과 보안, 양대일, 김경곤 공저

[3] http://winis.co.kr

[4] Paros User Guide for Paros http://www.parosproxy.org/