프린터 관리 시스템의 취약점 분석

지우중, 이경문, 이병천

중부대학교 정보보호학과

Security Vulnerability of Printer Management System

Woojoong Ji, Kyungmoon Lee, Byoungcheon Lee

Department of Information Security, Joongbu University.

요 약

디지털화가 가속되면서 학교나 도서관 등 공공기관에서 디지털 정보의 이용이 높아지고 있으며 프린트 서비스의 요구도 점점 증대하고 있다. 함께 사용하는 공공 PC에서의 프린터 사용료에 대한 과금은 관리자에게 꽤나 까다로운 일인데 이러한 까다로운 과금 업무를 자동화할 수 있도록 하는 프린트 관리 솔루션이 개발되어 현재 널리 사용되고 있다. 하지만 서비스 개발자 및 프린터 관리 솔루션 개발자들의 보안개발에 대한 인식은 아직 취약한 부분이 많이 있는 것으로 보인다.

이 논문에서는 현재 공공기관에서 사용되고 있는 프린터 관리 서비스의 취약성을 분석하였다. 로그인과 프린터 과금 금액 등 중요한 정보를 전송하는 경우 HTTPS 등의 보안통신을 적용해야 하지만 HTTP 평문통신을 사용하여 도청공격에 취약하며, 수신하는 정보가 실제 상대방에서 전송되어온 것인지에 대한 인증 및 검증이 필요한데 이런 과정을 생략함으로써 프록시를 이용한 변조공격이 가능함을 확인하였다. 아울러 우리나라의 취약점 신고 포상제도가 널리 취약점을 찾아내고 빠르게 개선하려고 하는 본래의 목적에 적합하지 못하다고 생각하여 이를 개선할 수 있는 방안을 제시하였다.

I. 서론

최근 공공 도서관에서는 도서관 보상금 제도[1,2,3]를 도입하여 시행하고 있는데 도서관의 소장자료 중 디지털 형태로 구매할 수 없는 자료를 출판년도와 무관하게 디지털화하고 발행 후 5년이 지난 자료는 도서관간에 전송하여 볼 수 있게 하되, 이용에 대하여 도서관이 소정의 보상금을 지불하도록 하는 제도이다. 서비스에 활용되는 수많은 저작물들에 대해 보상금을 지급하여 저작물을 적법하게 활용할 수 있도록 함으로써 이용자들이 저작권법을 지키도록 함과 동시에 자료 사용의 편의성을 도모하기 위한 시스템이다. 이 제도를 적용하기 위해 도서관은 저작물을 프린트하는 경우 사용내용에 대한 적절한 과금 시스템을 준비하여야 한다.

또한 공공장소에서 사용하는 프린터 자체의 관리도 매우 까다로운 일인데 소모품 관리, 프린터 정비, 사용내역 관리, 복사 및 인쇄 사용량에 대한 과금 등이 필요하다. 이러한 까다로운 프린터 관리 업무를 자동화할 수 있는 솔루션들이 개발되어 사용되고 있는데, 그 중 S사의 제품은 대학교 대략 40곳, 공공도서관 40여곳 등에서 사용되고 있다. 이 시스템에서는 사용자들이 계정을 생성하고 돈을 예치한 다음 프린트한 페이지의 수만큼 금액이 차감되는데 특별한 하드웨어 장치의 도입이 필요없이 네트워크 연결만 되면, 장소에 상관없이 프린트가 가능하다는 장점이 있다.

우리는 S사의 프린터 관리 시스템을 패킷분석, 중간자공격 등 네트워크 공격 기법을 이용하여 분석한 결과 보안통신을 사용하지 않아 로그인, 과금 등의 중요 정보가 쉽게 도청되는 취약점이 있으며, 전송되는 정보에 인증이 제공되지 않아 공격자가 프록시 중간자공격으로 데이터를 쉽게 변조할 수 있음을 확인하였다. 공격자가 남의 로그인 정보를 취득하면 남의 계정으로 프린터 서비스를 이용할 수 있고, 과금 데이터를 변조할 수 있게 되면 돈을 지불하지 않고 프린터 서비스를 이용하거나 충전 금액을 공격자가 임의로 변조하는 것도 가능하게 될 것이다.

II. 프록시를 이용한 중간자 공격

HTTP 프로토콜을 사용하면 서버와 클라이언트 사이에 데이터가 평문으로 전송되기 때문에 공격자가 중간에 패킷을 가로챈 다음 악의적인 행동을 할 수 있다. 먼저 본 논문에서 사용되는 공격기법과 용어들에 대해 설명하고자 한다.

2.1 도청 공격

가장 먼저 이루어져야 할 공격은 통신 내용을 도청할 수 있는 스니핑인데 이것은 네트워크를 통해 오고가는 패킷들을 제 3자가 동의 없이 패킷을 가로채서 보는 것을 말한다. 스니핑을 위해서는 통신 패킷이 공격자를 거쳐가도록 해야 하는데 본 논문에서는 ARP 스푸핑을 이용한다.

스푸핑이란, 악의적인 공격자가 자신의 신분을 속이는 것을 말한다. 스푸핑의 기법에는 ARP 스푸핑, IP 스푸핑, 쿠키 스푸핑, DNS 스푸핑 등의 기법들이 존재한다. 공격자는 ARP 스푸핑을 통해 공격 대상의 ARP 테이블을 변조시켜 그 컴퓨터의 모든 네트워크 패킷은 공격자의 컴퓨터를 거쳐가게 되고 공격자는 해당 패킷에 대해서 정상적으로 처리해 줌으로써 공격 대상 사용자는 아무런 의심없이 네트워크 통신을 계속 사용하게 된다.

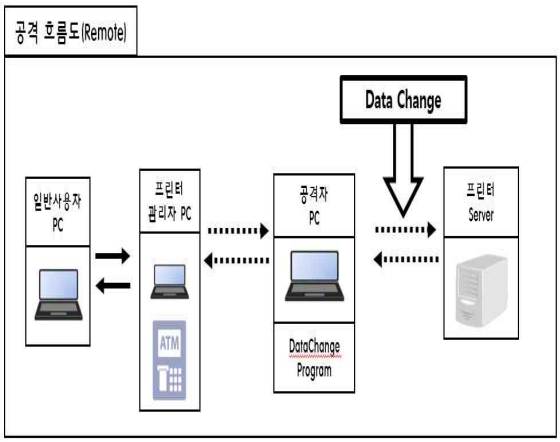
2.2 HTTP 중간자 공격

중간자 공격[4]이란 서버와 클라이언트 사이의 중간에 프록시 서버를 운영하면서 서버와 클라이언트 사이에서 HTTP 통신을 맺어 통신을 중개하면서 사용자의 프린터 과금 정보를 서버에 그대로 전달하도록 하는 공격 기법으로 사용자가 프린터를 사용하기 위해 지불한 금액 정보를 탈취할 수 있는 방법이다. 해당 취약점을 적용하기 위해 직접 프로그램을 구현하였으며 여기에서는 이것을 이용하여 HTTP 프록시 공격을 수행하는 사례를 보인다.

2.3 공격 시나리오

공격자가 운영하는 HTTP 프록시는 서버와 클라이언트 사이의 HTTP 통신을 중개하는 역할을 한다. [그림 1]에 전체적인 공격 시나리오를 도시하였다.

공격자가 ARP 스푸핑을 이용하여 프린터 관리 PC를 감염시킨다. 공격이 수행되면 공공기관에서 운영되는 프린터 관리 PC는 공격자의 PC를 거쳐서 프린터 서버로 통신을 하게 된다. 그 다음 프록시를 동작시키고 사용자가 프린터를 하기 위해 금액을 지불할 때까지 대기한다. 대기하고 있던 프록시에서 해당 사용자가 프린터를 이용하기 위한 금액을 지불하는 데이터가 거치게 될 때 해당 금액을 변조하여 실제 프린터 서버로 전송하게 된다. 만일 서버에서 클라이언트의 신분을 확인하고 통신데이터에 대한 인증을 검증한다면 이런 공격을 찾아내어 에러메시지를 내고 중단시킬 수 있겠지만 서버에서는 이러한 검증 시스템이 구현되지 않아 이런 중간자 공격은 훌륭하게 동작하게 된다.



[그림 1] 프록시를 이용한 공격

III. 프린터 관리 서비스 공격 사례

3.1 ID/Password의 노출 사례

일반적으로 ID/Password의 로그인 정보는 정보 노출을 방지하기 위해 HTTPS 프로토콜로 보내는 것이 일반적이다. 하지만 테스트중인 프린터 관리 서비스에서는 HTTPS 보안통신을 적용하지 않아 로그인 정보, 프린터 업무에 대한 정보, 금액 정보 등 모든 데이터가 HTTP 프로토콜로 서버와 데이터를 주고받는다. 그렇게 되면 프록시를 이용한 중간자 공격으로 통신 내용을 쉽게 도청할 수 있다.

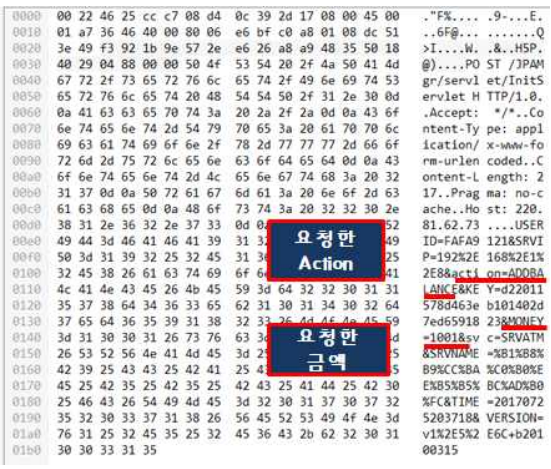
```
POST /JPAMgr/servlet/InitServlet HTTP/1.1
Host: 220.81.62.73:7070
Connection: keep-alive
Content-Length: 51
Cache-Control: max-age=0
Origin: http://220.81.62.73:7070
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Referer: http://220.81.62.73:7070/JPAMgr/servlet/InitServlet
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: JSESSIONID=B5A3BCD69A129712C0FA7FDFBA8946BC

svc=LOGIN&loginId=fafa9121&passwd=        &x=4&y=12HTTP/1.1 200 OK
```

[그림 2] 프린터 서비스 로그인 정보 도청

3.2 과금 금액 노출 및 변조 사례

사용자가 프린터 관리 서비스에 로그인하게 되면 현재 사용자 계정의 충전 금액이 서버로부터 전송되어온다. 사용자가 ATM 기기를 이용하여 금액을 충전하게 되면 충전금액을 포함하는 평문의 데이터가 프린터 관리 PC에서 서버로 전송된다. 사용자가 프린트 작업을 수행하는 경우 현재의 충전금액에서 사용량을 차감하고 남은 충전금액을 서버로 전송하게 된다. 이러한 모든 통신과정이 평문상태로 전송되며 서버에서는 검증을 하지 않고 그대로 받아들이기 때문에 공격자가 마음대로 데이터를 변조할 수 있다.

(a) 사용자의 금액 충전



(b) 공격자에 의한 충전금액 변조

[그림 3] 프린터 관리 시스템의 금액 변조

[그림 3]은 사용자가 금액 충전시 공격자 PC에서 데이터를 원하는 금액으로 변조하여 프린터 서버로 전송하는 사례를 보여준다. 서버는 데이터의 인증성 여부를 검증하지 않고 그대로 받아들이기 때문에 사용자 계정에는 변조된 금액이 충전되는 것을 확인할 수 있다.

3.3 취약점 개선 방안

여기에서 확인된 취약점은 네트워크 기반의 클라이언트/서버 환경의 서비스에서 가장 기본적인 보안 대책인 HTTPS 통신을 사용하지 않는 것과 서버가 인가된 클라이언트에서 보내온 데이터인지 확인하지 않는 문제점 때문에 발생한다고 볼 수 있다.

이를 해결하기 위해서는 서버에 인증서를 설치하고 HTTPS 보안통신을 사용하도록 서버를 구성해야 할 것이다. 서버가 프린터 관리 PC를 인증하기 위해서는 프린터 관리 PC를 서버에 초기 등록시 인증서를 발급하여 장착하도록 하고 인증서로 서명된 통신만을 받아들이도록 운영해야 한다. 또한 프린터 관리 PC의 시스템보안, 해킹대응을 위해 인증서의 저장 및 서명작업은 하드웨어보안모듈을 이용하도록 구성할 수 있을 것이다.

IV. 취약점 신고 결과

이러한 취약점을 확인한 후 해당 취약점이 업체에 피드백되고 빠르게 개선하도록 하기 위해 KISA[5]에 취약점 제보를 하였다. KISA에서는 신규 취약점을 빠르게 발굴하고 개선해나갈 수 있도록 하기 위해 취약점 신고포상제[6]를 실시하고 있는 것으로 알고 있다. 그러나 취약점 담당자로부터 받은 응답은 “실제 서비스 중인 웹사이트나 시스템(서버, 네트워크, 보안장비 등)에 특정 데이터를 전송하여 영향을 줄 우려가 있는 서비스 취약점”은 평가 및 포상 대상에서 제외된다는 것이었다.

[한국인터넷진흥원-안내] 공동인쇄구역 취약점 분석(17-550)

보낸사람 ☆업무용(취약점신고)<vuln@krcert.or.kr>

받는사람 < @naver.com>

안녕하세요. 한국인터넷진흥원 취약점 담당자입니다.

신고해주신 " 취약점 분석"은 아래와 같은 사유로
평가 대상에서 제외되었음을 알려드립니다.
* 실제 서비스 중인 웹사이트나 시스템(서버, 네트워크, 보안장비 등)에 특정 데이터를 전송하여 영향을 줄 우려가 있는 서비스 취약점은 평가 및 포상 대상에서 제외

앞으로도 적극적인 신규 취약점 발굴 및 신고활동 부탁드립니다. 감사합니다.

기타 문의사항이 있으시면 연락주시기 바랍니다.(분석가 :

감사합니다.

[그림 4] KISA 취약점 포상 제외 사항

실제 서비스 중인 웹사이트나 시스템에 특정 데이터를 전송하여 영향을 줄 수 있다는 것 자체가 취약점이 있다는 것인데 이를 포상금을 떠나 취약점으로 신고받지 않고 평가대상에서 제외된다는 것은 애초의 취약점 신고포상제의 취지와 맞는지 고려해보아

야 한다.

애초에 버그바운티(Bug Bounty) 제도란 소프트웨어 또는 웹 서비스의 취약점을 찾아낸 사람에게 포상금을 지급하는 제도로서 신고포상제 운영이 자체 발굴보다 보안 연구비를 절감하고 대량의 취약점을 발견하는데 효율적이기 때문에 많은 기업들이 운영하고 있다. 외국에서는 기업의 서비스나 제품 등을 해킹해 취약점을 발견한 화이트해커에게 포상금을 지급하는 버그바운티 제도를 통해 빠르게 보안 패치를 적용하고 있다.

하지만 국내에서는 2012년 이 제도를 도입했지만 취약점을 밝히는 것을 꺼려하는 기업 문화와 보안 불감증, 보안 취약점이 발견된다면 부정적인 이미지로 비춰질 것을 우려된다는 등의 이유로 포상금도 적고 신고 건수도 저조한 상태이다. 공공기관인 KISA가 취약점 신고포상제를 시행한다면 이 제도에 부정적인 기업입장을 우선시하기보다는 취약점을 빠르게 발굴해내고 기업에서도 빠르게 보안패치를 해나갈 수 있도록 압박하는 애초의 목적에 맞게 운영했으면 하는 바람이다.

V. 결론

우리가 일상적으로 사용하는 많은 서비스, 어플리케이션, 솔루션 등이 아직까지 보안 프로토콜인 SSL/TLS, HTTPS를 적용하지 않고 운영되는 경우가 많으며, 클라이언트/서버 환경에서 인가된 클라이언트가 보내는 데이터인지를 서버에서 확인하지 않는 등 취약한 방법으로 운영되는 사례가 많다는 것을 확인하였다. 서비스, 어플리케이션, 솔루션 개발자들뿐만 아니라 이러한 제품을 취급하는 회사들은 이러한 취약성들에 대해 인식하고 보안기술을 적절히 활용하여 신뢰성 있는 제품을 구현하려는 노력이 필요하다고 생각된다. 공공기관인 KISA가 운영하는 취약점 신고포상제는 이 제도에 부정적인 기업입장을 우선시하기보다는 취약점을 빠르게 발굴해내고 기업에서도 빠르게 보안패치를 해나갈 수 있도록 압박하는 애초의 목적에 맞게 운영했으면 하는 바람이다.

[참고문헌]

[1] 저작권법, 법률 제14634호

[2] 이영아, “개정 저작권법상 도서관 보상금 제도”, 문화관광부

[3] 정경희. "도서관보상금제도의 운영성과에 대한 분석." 한국문헌정보학회지, 49.4 (2015.11): 265-288.

[4] Man-in-the-middle attack, https://www.owasp.org/index.php/Man-in-the-middle_attack

[5] KISA 한국인터넷진흥원, https://www.kisa.or.kr

[6] 한국인터넷진흥원, S/W 신규 취약점 신고포상제 운영 안내서