Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.655

공공기관 프린터 관리 시스템의 취약점 분석*

지 우 중,[1†] 이 경 문,[2] 이 병 천[2‡]
[1]성균관대학교, [2]중부대학교

Vulnerability Analysis of Printer Management System in Public Institutions

Woojoong Ji,[1†] Kyungmoon Lee,[2] Byoungcheon Lee[2‡]
[1]Department of Computer Science and Engineering, Sungkyunkwan University, Republic of Korea
[2]Department of Information Security, Joongbu University, Republic of Korea

요 약

디지털화가 가속되면서 학교나 도서관 등 공공기관에서 디지털 정보의 이용이 증가하고 있으며 프린트 서비스의 요구도 점점 증가하고 있다. 많은 서비스 가운데 공공 PC에서 프린트 서비스를 이용할 시 사용료를 지불하도록 해야 하는데 관리자에게는 꽤나 까다로운 업무이다. 이러한 까다로운 업무를 자동화할 수 있도록 하는 프린트 관리 시스템이 개발되어 현재 널리 사용되고 있다. 이 논문에서는 현재 공공기관의 공공PC에서 사용되고 있는 프린터 관리 시스템의 취약성을 분석하였는데 공공 PC 관리자 및 프린터 관리 솔루션 개발자들의 보안의식과 보안개발에 대한 인식은 아직 많은 부분이 부족한 것으로 보인다.

ABSTRACT

As digitalization accelerates, the use of digital information is increasing in public institutions such as schools and libraries, and the demand for print services is also increasing. Among many services, printing service on public PCs should charge fee to printer users, but it is a very difficult task for administrators. Print management solutions have been developed and are now widely used to automate these demanding tasks. In this paper, we analyze the vulnerability of printer management solutions used in public institutions. However, the security awareness of public PC administrators and printer management solution developers seem to be lacking.

Keywords: arp spoofing, mitm, printer vulnerability analysis, print spooling, meta data

I. 서 론

최근 공공 도서관에서는 도서관보상금제도[1,2,3]를 시행하고 있는데 이것은 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 제도이다. 이 제도를 적용하기 위해 공공기관 및 도서관에서 저작물을 프린트하는 경우 이에 대한 적절한 보상금 지불 시스템을 준비하여 저작권법을 지키도록 하여야 한다.

Received(03. 14. 2018), Modified(06. 04. 2018), Accepted(06. 11. 2018)
* 본 논문은 2017년도 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, woojoong@skku.edu
‡ 교신저자, sultan@joongbu.ac.kr(Corresponding author)

또한 공공장소에서 사용하는 프린터 자체의 관리도 매우 까다로운 일이다. 예를 들어 소모품 관리, 프린터 정비, 사용내역 관리, 복사 및 인쇄 사용량에 대한 과금 등 까다로운 프린터 관리 업무를 자동화할 필요가 있는데 이런 기능을 가진 많은 솔루션들이 개발되어 사용되고 있다. 또한 각 회사의 솔루션에서는 보상금제도 및 프린터 관리 서비스 이외의 다양한 서비스들을 제공하고 있다. 각 솔루션에서는 사용자들이 계정을 생성하고 돈을 예치한 다음 프린트한 페이지의 수만큼 금액이 차감 되고 특별한 하드웨어 장치의 도입이 필요 없이 네트워크에만 연결이 되면, 장소에 상관없이 프린트가 가능하다는 장점이 있다.

우리는 J사, P사의 프린터 관리 솔루션에 대해 패킷분석, 중간자공격, 메타 데이터 추출 등 다양한 공격 기법을 이용하여 분석하고 프린터 서비스 이외의 다른 서비스에 대해서도 공격과 분석을 진행했다. 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 있으며 프린트를 이용할 시 해당 프린터에게 스풀링을 하고 남은 스풀링 파일 정보를 쉽게 획득할 수 있음을 확인하였다. 또한 이러한 취약점을 이용해 공격자가 타인의 로그인 정보를 취득하면 타인의 계정으로 프린터 서비스를 이용 할 수 있고 과금 데이터까지 변조할 수 있어 돈을 지불하지 않고 프린터 서비스를 이용할 수가 있다.

II. 배경지식

본 장에서는 공공기관에서 사용되는 공공PC에서 사용되는 프린터 관리 솔루션의 취약점과 프린트 이외의 공공장소나 여러 사람들이 이용할 수 있는 다양한 서비스를 제공하는 솔루션에 대해 분석하기 위해 ARP SPOOFING, 중간자 공격기법, 프린터 SPOOLING에 대해서 간단하게 소개하고자 한다.

2.1 ARP SPOOFING

프린터 관리 솔루션에 대해 네트워크 환경에서 분석하기 위해서 가장 먼저 이루어져야 할 공격은 통신 내용을 도청할 수 있어야 한다. 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 스푸핑 기법[4]을 이용하였다.

공격자는 Fig. 1과 같은 ARP 스푸핑 공격을 통해 공격 대상의 ARP 테이블을 변조시켜 그 컴퓨터의 모든 네트워크 패킷은 공격자의 컴퓨터를 거쳐가게 하고 공격자는 해당 패킷에 대해서 정상적으로 처리해 줌으로써 공격 대상 사용자는 아무런 의심없이 네트워크 통신을 계속 사용하게 된다.

Fig. 1. ARP spoofing packet flow

2.2 중간자 공격 (MITM)

중간자(Man-in-the-middle, MITM) 공격[5,6]은 ARP 및 DNS 프로토콜의 정상적인 동작과 흐름을 악의적으로 수정하여 이루어진다. ARP 스푸핑, DNS 스푸핑 등으로 인해 감염된 클라이언트는 정상적으로 서버와 클라이언트가 통신하고 있는 것처럼 보이나 악의적인 공격자는 서버와 클라이언트 사이에 존재하면서 악의적인 행동을 하게 된다.

프린터 관리 솔루션의 각각의 제조사들은 프린터 관리와 사용자의 정보 등을 관리하기 위해 공공PC에서 사용되는 프린트에 관한 모든 정보는 프린터 관리 서버에 전송하도록 하고 있다. 이때 악의적인 공격자는 서버와 클라이언트 사이에서 HTTP/SSL 통신을 맺어 통신을 중개하면서 사용자의 프린터 과금 정보, 사용자의 개인정보 등을 탈취 및 변조가 가능하게 된다. 본 논문에서는 자체 제작한 프로그램을 이용하여 Fig. 2와 같이 HTTP 중간자 공격을 수행하는 사례를 보인다.

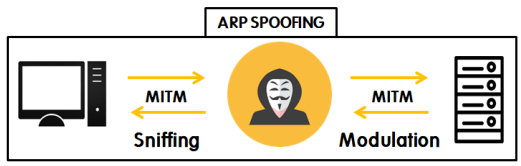


Fig. 2. MITM attack based on ARP spoofing

2.3 프린트 SPOOLING

스풀링(spooling)이란 컴퓨터 시스템에서 중앙처리장치와 입출력장치가 독립적으로 동작하도록 함으로써 중앙처리장치에 비해 주변장치의 처리속도가 느려서 발생하는 대기시간을 줄이기 위해 고안된 기법이다. 스풀링을 적용하는 가장 대표적인 곳은 프린터 출력 작업이다. CPU가 프린터 출력을 직접 제어한다면 프린터의 인쇄 작업이 끝날 때까지 다른 일을 하지 못하게 된다. 실제로 소요시간의 대부분은 CPU가 프린터의 응답을 기다리는 시간이기 때문에 CPU 사용효율이 매우 낮다. 이러한 문제점을 해결하기 위해 프린터에 프린트할 데이터를 일괄 전송하는 스풀링이 활용된다.

스풀러란, 프린터 자체적으로 버퍼를 가지고 있지만 버퍼의 용량이 작고 프린터 작업 속도가 느리기 때문에 인쇄 데이터를 호스트 컴퓨터의 디스크 버퍼에 스풀 시키는 소프트웨어를 말한다. 특정 문서나 페이지를 인쇄하기 위해 인쇄버튼을 누르면, 우선 문서나 사진이 프린트 설정에 맞게 변환되어 프린터로 전송된다. 하지만 프린터가 현재 다른 작업을 처리하느라 바쁜 상황인지 알 수 없기 때문에 우선 프린트 작업을 지시한 호스트 컴퓨터에 임시적으로 스풀 데이터를 생성한다. 이렇게 생성된 스풀 데이터는 차례로 프린터로 전송된다.

이때 스풀 데이터는 파일 형태로 저장되게 되는데 스풀 데이터가 저장되는 경로는 프린터 제조사, 설정에 따라 다르지만 가장 일반적으로는 Fig. 3과 같이 지정된다. 이와같이 스풀 데이터의 경로가 대부분 디폴트값으로 정해져있기 때문에 악의적인 공격자가 쉽게 접근이 가능하다.

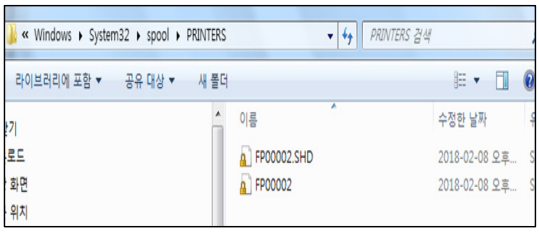


Fig. 3. The spool file stored in the spool path C:\Windows\System32\spool\PRINTERS

2.4 메타 데이터(Meta Data)

본 논문과의 목적과 의미에 맞게 설명하자면 메타데이터란 어떤 목적을 가지고 만들어진 데이터라고 정의할 수 있다. 여기서 목적이라는 의미는 공공PC나 각각의 사용자의 어떤 행위에 대해 발생하는 데이터를 말할 수 있다. 또 어떤 행위라 함은 사용자는 프린터를 이용하기 위해 인쇄버튼을 누르게 되는 행위를 하게 되는데 이러한 행위로 인해 메타 데이터라고 표현할 수 있는 스풀 데이터가 생성된다. 또 프린트를 이용한 행위에 대해서 사용자가 어떤 행위를 했는지 예를 들어 사용자의 프린트 내역 정보나, 금전적인 내용 등을 서버에게 보내 사용자의 정보를 업데이트를 시켜야 한다. 이때 공공PC, 사용자 PC 또는 관리자 PC에서는 해당 행위에 대한 데이터를 패킷에 담아 서버에게 보내게 된다. 이러한 패킷에 들어있는 내용 또한 메타 데이터라고 할 수 있다.

III. 공격 시나리오

2장에서 설명한 내용을 토대로 공격자는 크게 두 가지 방법으로 공격이 가능하다. 첫 번째는, 악의적인 공격자가 사용자 PC, 관리자 PC의 네트워크에 접근이 가능할 때 사용 가능한 네트워크에 대한 공격 시나리오이고, 또 다른 하나는 악의적인 공격자가 사용자 PC, 관리자 PC의 네트워크에 접근을 하지 못하였을 때의 메타 데이터에 대한 공격 시나리오이다.

3.1 네트워크에 대한 공격 시나리오

네트워크 공격에 대해서는 악의적인 공격자가 프린터 관리 솔루션 PC에 직접 접근이 할 수 있는지의 여부에 따라 대해 네트워크 공격 시나리오가 달라지지만 큰 차이는 없다. 악의적인 공격자가 어디에 접근 하느냐에 따라 다른데 먼저 악의적인 공격자가 프린터 관리 솔루션의 관리자 PC에 직접 접근이 가능할 경우와 다른 하나는 프린터 관리 솔루션의 관리자 PC에 접근이 불가능 할 때의 공격이다. 관리자 PC에 접근이 불가능 할 경우에는 악의적인 공격자는 사용자의 PC에 직접 접근해야 한다. 이에 각각의 공격 시나리오에 대해 설명한다.

3.1.1 관리자 PC와 같은 네트워크 대역일 경우

공격자가 관리자 PC와 같은 네트워크 대역에 연결되어 있는 경우는 쉽게 접근이 가능하다.

먼저 관리자 PC에 악의적인 공격자가 접근이 가능 할 경우의 전체적인 공격 시나리오를 Fig. 4에 도식화하였다. Fig. 4에서 정상적인 흐름을 보면 일반 사용자가 공공PC에서 프린트 서비스를 요청하게 되면(①) 사용자의 PC는 관리자 PC에게 해당 작업을 요청하게 된다. 그러면 관리자 PC에서는 사용자의 요청을 각 제조사의 프린터 관리 서버에게 보내(②) 프린터 관리 서버는 해당 작업을 처리한다.

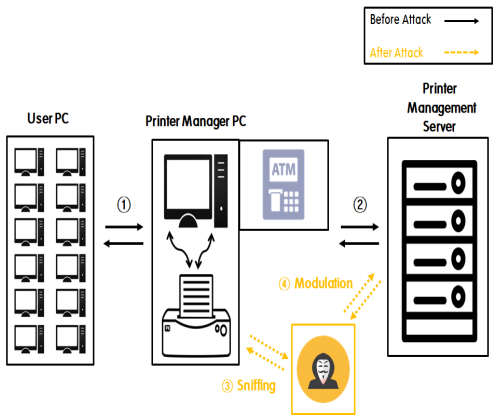


Fig. 4. Overall scenarios where a malicious attacker can access the administrator's PC

이때 악의적인 공격자는 해당 관리자 PC에 ARP 스푸핑 공격 기법을 이용해 프린터 관리 서버에 보내야할 정상적인 통신 흐름을 공격자를 거쳐 가도록 설정한다. 이때 악의적인 공격자로 오는 통신 내용(③) 중 사용자의 회원정보, 로그인 정보, 과금 정보 등에 대해 민감한 데이터를 변조하여 프린터 관리 서버에게 보내게 되면(④) 프린터 관리 서버는 이러한 사실을 전혀 알지 못한 채 악의적인 공격자의 공격이 성공적으로 이루어진다.

3.1.2 관리자 PC와 다른 네트워크 대역일 경우

다음은 악의적인 공격자가 관리자 PC의 네트워크에 직접 접근하지 못하고 일반 사용자가 사용하고 있는 공공PC와 같은 네트워크에서 접속하는 경우에 이루어지는 공격 시나리오이다. 크게 다른 점은 없지만 가장 큰 차이점은 악의적인 공격자의 위치이다.

공격자가 관리자 PC와 같은 네트워크 대역에서 접속하는 경우에는 공격자가 관리자 PC와 프린터 관리 서버 사이에 위치하는 반면, Fig. 5에 보인 바와 같이 다른 네트워크 대역에서 접속하는 경우에는 공격자가 일반 사용자와 관리자 PC사이에 존재한다. 전자의 경우에는 공격자가 프린터 관리자 PC에게만 도청 및 변조 공격을 위해 ARP 스푸핑 공격을 하면 되지만 후자의 경우에는 일반 사용자를 대상으로 ARP 스푸핑 공격을 해야 하므로 공격할 대상이 많아질수록 해당 패킷들을 처리해주어야 하기 때문에 악의적인 공격자의 PC에서 얼마나 빠르고 정확하게 처리하느냐에 따라 결과가 달라진다.

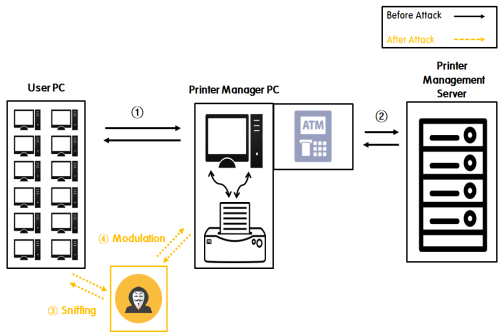


Fig. 5. Overall scenarios where a malicious attacker can not access the administrator's PC

3.2 메타 데이터에 대한 공격 시나리오

메타 데이터에 대한 공격시나리오는 3.1에 나오는 네트워크 공격으로 공격이 불가능할 때, 즉 공격자가 사용자 PC나 관리자 PC와 같은 네트워크 대역으로 접근이 불가능한 경우의 공격 시나리오이다. 네트워크로 접근이 불가능한 경우 악의적인 공격자는 직접 사용자의 PC나 관리자 PC에 물리적인 접근을 시도할 것이다.

공공기관에서는 대부분 관리자 PC에 대한 물리적인 접근이 어렵다고 볼 수 있지만 이는 공공기관에 따라 다르다. J사의 제품의 경우 관리자 PC가 사용자의 PC와 함께 외부에 노출되어 물리적으로 쉽게 접근이 가능하게 운영되는 사례가 있었다.

하지만 일반 사용자가 이용하는 사용자 PC는 J

사, P사 모두 외부에 노출되어 있어 관리자 PC에 비해 공격자가 물리적으로 쉽게 접근 가능하다. 이 점을 이용해 공격자는 공동으로 사용하는 공공 사용자 PC에 직접 접근하여 프린터 메타 데이터를 탈취하는 프로그램을 설치하고 실행시킬 수 있다.

먼저 공격자는 일반 사용자로 위장하여 공공 사용자 PC에 접근한다. 그런 다음 공격자는 공격자가 미리 만들어둔 악성 프로그램을 설치하고 시스템 백그라운드에서 실행시켜 악성 행위를 시작한다. 여기서 말하는 악성 행위는 대부분의 프린터는 스풀 데이터의 경로가 디폴트값으로 정해져있기 때문에 이 스풀 데이터가 저장되는 경로를 계속해서 시스템 백그라운드에서 탐색하다가 스풀 메타 데이터가 해당 경로에 생성되면 공격자가 설정해둔 경로에 복사 저장을 하거나 공격자의 이메일로 보내는 행위를 말한다. J사 제품의 경우는 공공 사용자 PC에서 사용자의 이용이 끝난 후 PC의 재부팅이 이루어지지 않아 공격자가 실행시킨 악성 프로그램이 시스템 백그라운드에서 계속 실행이 되어 사용자의 민감한 프린트 스풀 데이터가 공격자에게 탈취당하게 된다.

IV. 공공기관 프린터 서비스 공격 사례

본 논문에서는 앞서 설명한 다양한 공격기법을 활용하여 2개의 제조사의 프린터 관리 솔루션에 대해 분석해보았다.

4.1 ID/Password의 노출 사례

일반적으로 ID/Password의 로그인 정보는 정보 노출을 방지하기 위해 HTTPS 보안통신 프로토콜로 암호화하여 관리 서버로 보내는 것이 일반적이다. 하지만 테스트 중인 J사와 P사 제품의 경우 프린터 관리 서비스에서는 보안통신을 적용하지 않아 로그인 정보가 Fig. 6, Fig. 7처럼 평문으로 노출됨을 확인하였다. 그렇게 되면 프록시를 이용한 중간자 공격으로 통신 내용을 쉽게 도청할 수 있다.

사용자의 로그인 정보가 유출된 Fig. 6, Fig. 7를 보면 회원 ID와 패스워드를 볼 수가 있는데 이는 패스워드 재사용 공격[8]에 취약할 수 있다. 일반적으로 사용자는 여러 서비스에서 동일한 암호를 사용하곤 하는데 악의적인 공격자가 위와 같은 방식으로 암호를 획득하게 된다면 사용자의 여러 계정에 접근할 수 있는 가능성이 있다. 조사에 따르면 사용자가

Fig. 6. Exposure of login information

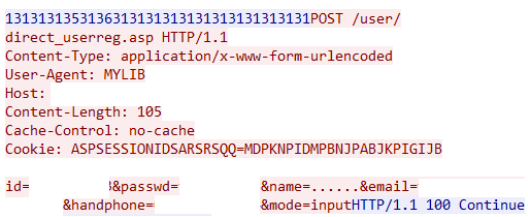


Fig. 7. Exposure of Membership Information

보유한 암호의 수와 암호의 재사용 빈도를 측정해 보았을 때 사용자는 세 개 이하의 암호를 가지고 있으며 그 중 높은 확률로 같은 암호를 재사용하고 있다. 사용자들은 새로운 서비스에 계정을 생성하고 패스워드를 설정할 때 새로운 패스워드를 기억하는 것이 어렵기 때문에 평소에 사용하는 패스워드를 입력하게 되는 것이다. 이러한 특징 때문에 사용자의 ID와 password를 한번 해킹당하면 악의적인 공격자가 사용자의 다른 계정이나 서비스에도 접근이 가능하다는 것을 알 수가 있다.

4.2 과금 금액 노출 및 변조사례

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 또한 서버에서는 검증을 하지 않고 그대로 받아들이도록 되어 있어서 악의적인 공격자가 마음대로 해당 금액의 데이터를 변조할 수 있다. Fig. 8-1은 사용자가 금액 충전시 발생한 패킷이고 Fig. 8-2는 공격자 PC에서 데이터를 원하는 금액으로 변조하여 프린터 서버로 전송하는 사례를 보여준다. 서버는 데이터의 인

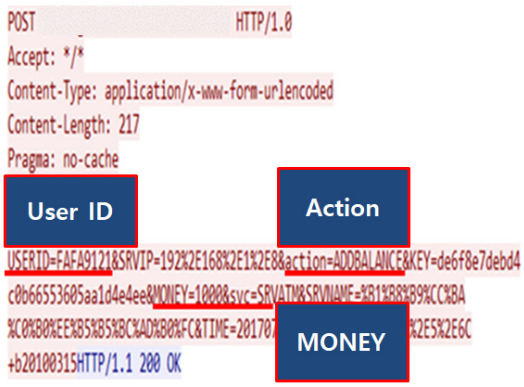


Fig. 8-1. Charging money in user's account

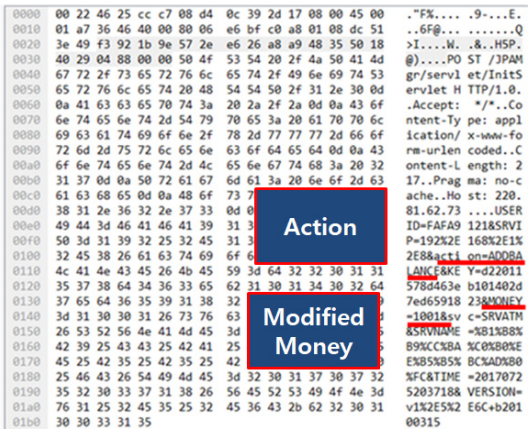


Fig. 8-2. Modification of user's charging message

증성의 여부를 검증하지 않고 그대로 받아들이기 때문에 사용자 계정에는 변조된 금액이 충전되는 것을 확인할 수 있다.

4.3 스풀 메타 데이터 추출 사례

공공 PC에서 사용자가 프린터를 이용하는 경우 프린트할 데이터를 프린터에게 전달하기 위해 스풀 데이터가 생성되는데 이것을 가로채어 탈취하는 프로그램을 제작하였다. 이 프로그램을 사용자 PC에 미리 설치하고 백그라운드로 실행시킨다. 다른 사용자가 동일 PC를 이용하여 프린트 작업을 하는 경우 Fig. 9-1과 같이 스풀 데이터가 지정 폴더에 저장된다. SPLViewer 프로그램을 이용하여 Fig. 9-2와 같이 원본 문서를 복구할 수 있었다.

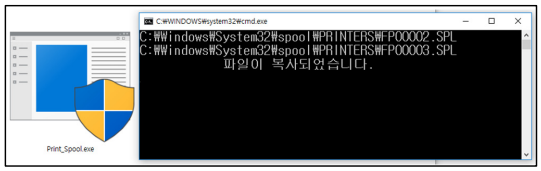


Fig. 9-1. A program that intercepts spooled data

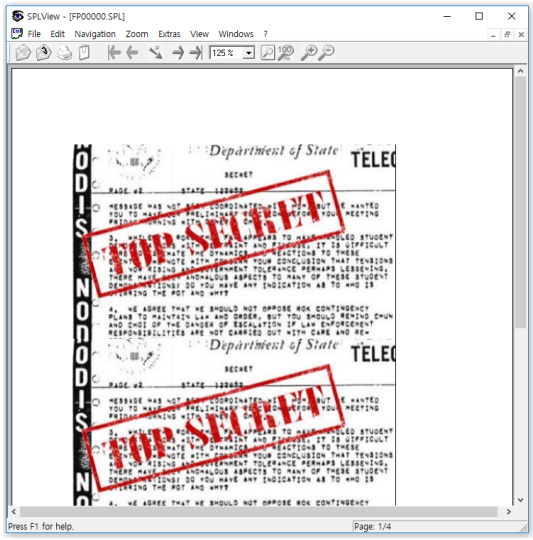


Fig. 9-2. Convert to original document with tool(SPLView)

V. 취약점 개선 방안

본 논문에서 확인된 취약점은 네트워크 기반의 클라이언트/서버 환경의 서비스에서 가장 기본적인 보안 대책인 HTTPS 통신을 사용하지 않는 것과 서버가 인가된 클라이언트에서 보내온 데이터인지 메시지 인증을 확인하지 않는 문제점, 공동으로 사용하는 공공 PC에 대한 허술한 관리, 메타 데이터에 대한 접근제어 부재 등의 원인을 생각해볼 수 있다.

먼저 네트워크 기반의 취약점을 해결하기 위해서는 서버에 인증서를 설치하고 HTTPS 보안통신을 사용하도록 구성해야 할 것이다. 예를 들어 프린터 관리 PC를 서버에 초기 등록 시 인증서를 발급하여 장착하도록 하고 인증서로 프린터 관리 PC의 신분을 인증하고 서명된 통신만을 받아들이도록 운영할 수 있다. 또한 프린터 관리 PC의 시스템보안, 해킹 대응을 위해 인증서의 저장 및 서명 작업은 하드웨어 보안모듈을 이용하도록 구성할 수 있을 것이다.

다음은 공공 PC의 특성상 많은 사용자들이 이용하기 때문에 특히 보안관리에 신경을 써야 하지만 대부분 관리가 잘 되고 있지 않고 있다. 현실적으로 일반사용자와 악의적인 공격자를 구분할 수 없으므로 공공기관에서는 사용자들이 공공 PC를 사용할 시 최소한의 로그 파일을 생성하여 주기적으로 로그파일에 대해 분석하는 방법과 주기적으로 공공PC에 대한 보안 점검을 하여야 할 것이다. 또한 일반 사용자가 공격 프로그램을 설치하거나 하는 등의 공격이 발생하지 않도록 공공PC의 권한관리가 필요하다.

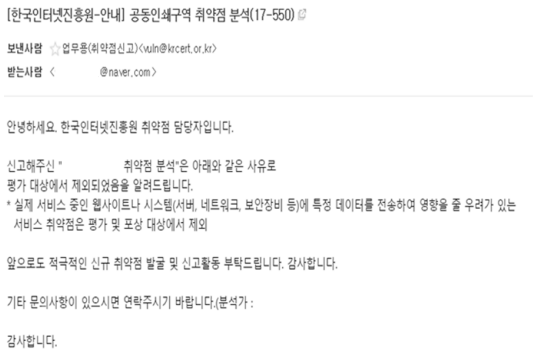
VI. 취약점 신고 결과

이러한 취약점을 확인한 후 해당 업체에 제보를 하였지만 개선이 되지 않고 있다. 우리나라에서는 많은 기업들이 보안인력의 부족과 해당 취약점을 개선할 때 발생되는 비용 때문에 취약점이 있다는 사실을 알고서도 이에 대한 조치를 하지 않는 경우가 많다. 그래서 해당 취약점이 업체에 피드백되고 빠르게 개선되도록 하기 위해 KISA[9]에 취약점 제보를 하였다.

KISA에서는 신규 취약점을 빠르게 발굴하고 개선해나갈 수 있도록 하기 위해 취약점 신고 포상제[10]를 실시하고 있는 것으로 알고 있다. 그러나 취약점 담당자로부터 받은 응답은 Fig. 10에 보인 바와 같이 "실제 서비스 중인 웹사이트나 시스템(서버, 네트워크, 보안장비 등)에 특정 데이터를 전송하여 영향을 줄 우려가 있는 서비스 취약점은 평가 및 포상 대상에서 제외된다"는 것이었다. 이는 실제 서비스 중인 웹사이트나 시스템에 특정 데이터를 전송하여 영향을 줄 수 있다는 것 자체가 취약점이 있다는 것인데 이를 취약점으로 신고 받지 않고 평가대상에서 제외된다는 것은 애초의 취약점 신고포상제의 취지와 맞는지 고려해 보아야 한다.

애초에 버그 바운티(Bug Bounty) 제도란 소프트웨어 또는 웹 서비스의 취약점을 찾아낸 사람에게 포상금을 지급하는 제도로서 신고포상제 운영이 자체 취약점 분석보다 보안 연구비를 절감하고 대량의 취약점을 발견하는데 효율적이기 때문에 많은 기업들이 운영하는 것이다. 외국의 경우에는 기업의 서비스나 제품 등을 해킹해 취약점을 발견한 화이트 해커에게 포상금을 지급하는 버그 바운티 제도를 통해 빠르게 보안 패치를 적용하고 있는 상황이다.

하지만 국내에서는 2012년 이 제도를 도입했지만


[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.

Fig. 10. Reply from KISA for our vulnerability reporting

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.

VII. 결 론

현재 공공기관에서 도입하여 사용되고 있는 프린터 관리 시스템에 대한 취약점 분석 결과 보안통신 프로토콜인 SSL/TLS, HTTPS를 적용하지 않고 운영되고 있어서 공격자가 네트워크 공격을 통해 메시지를 도청하거나 변조할 수 있는 위험성이 있고 공격자가 일반 사용자 PC에 직접 접근하여 공격프로그램을 설치할 경우 다른 사용자의 프린트 내용을 탈취할 수 있다는 것을 확인하였다. 이를 개선하기 위해서는 보안통신을 적용하여 서버가 클라이언트의 신원을 확인할 수 있어야 하고 통신이 도청되거나 변조되지 못하도록 해야 한다. 공격자가 PC에 직접 접근하여 공격 프로그램을 설치하거나 하는 등의 공격이 발생하지 않도록 엄격한 권한관리가 필요하다.

프린터 관리 시스템 뿐만 아니라 우리가 일상적으로 사용하는 많은 서비스, 어플리케이션, 솔루션 등이 아직까지 보안통신 프로토콜인 SSL/TLS, HTTPS를 적용하지 않고 운영되는 경우가 많으며, 클라이언트/서버 환경에서 인가된 클라이언트가 보내는 데이터인지를 서버에서 확인하지 않는 경우가 많

은 것이 사실이다. 서비스, 어플리케이션, 솔루션 개발자들뿐만 아니라 이러한 제품을 취급하는 회사들은 이러한 취약성에 대해 인식하고 보안기술을 적절히 활용하여 신뢰성 있는 제품을 구현하려는 노력이 필요하다고 생각된다.

또 많은 회사들에서 보안인력의 부족과 해당 취약점을 개선할 때 발생되는 비용적인 부분 때문에 취약점이 있다는 사실을 알고서도 이에 대한 조치를 하지 않는 경우가 많다. 이를 해결하기 위해서 공공기관인 KISA가 취약점 신고포상 제도를 운영하고 있는데 KISA에서는 이 제도에 부정적인 기업입장을 우선시하기보다는 해당 기업에서도 빠르게 보안패치를 해나갈 수 있도록 압박하는 애초의 목적에 맞게 운영했으면 하는 바람이다.

References

[1] Kyoung Hee Joung. (2015). An Analysis on the Results of the Operation for Library Remuneration System. JOURNAL OF THE KOREAN SOCIETY FOR LIBRARY AND INFORMATION SCIENCE, 49(4), 265-288.

[2] Jong-Chul Kim, Young-Seok Kim. (2012). A Study on the Provision of the Copyright Limitations for Libraries of the Korean Copyright Act. Journal of Korean Library and Information Science Society, 43(1), 349-369.

[3] Jae-Hyun Hong, Kyoung-Hee Joung, Ho-Sin Lee. (2005). A Study on Development of the Copyright Guideline on Reproduction and Transmission in Libraries. Journal of Korean Library and Information Science Society, 36(1), 505-525.

[4] Donghwi Shin, Younsung Choi, Sangjoon Park, Seungjoo Kim, Dongho Won. (2007). Cryptanalysis on the Authentication Mechanism of the NateOn Messenger. Journal of the Korea Institute of Information Security & Cryptology, 17(1), 67-80.

[5] A. Ornaghi and M. Valleri. Man in the middle attacks: demos. In Black Hat USA, 2003.

[6] Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. IEEE Security & Privacy, 7(1), 78-81.

[7] SPLViewer, http://www.lvbprint.de/bin/current/SplViewSetup.exe,2018.06.15

[8] Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (pp. 44-55).

[9] KISA, https://www.kisa.or.kr/business/violation/violation1_sub4.jsp,2018.06.15

[10] https://www.krcert.or.kr/consult/software/vulnerability.do?orgSiteUrl=https://www.krcert.or.kr, 2018.06.15

〈저자소개〉

지 우 중 (Woojoong Ji) 학생회원
2018년 2월: 중부대학교 정보보호학과 학사
2018년 3월: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 Network security, IoT security, Security Engineering

이 경 문 (Kyungmoon Lee) 정회원
2000년 2월: 인하대학교 컴퓨터공학과 학사
2015년 3월~현재: 한국정보기술연구원 멘토
2015년 3월~현재: 이스타미디어 수석연구원
2016년 3월~현재: 중부대학교 정보보호학과 산학협력중점교수
〈관심분야〉 네트워크 보안, 무선 네트워크 프로토콜

이 병 천 (Byoungcheon Lee) 종신회원
1986년 2월: 서울대학교 물리학과 학사
1988년 2월: 서울대학교 물리학과 석사
2002년 2월: KAIST 정보보호 박사
2002년 3월~현재: 중부대학교 정보보호학과 교수
〈관심분야〉 정보보호, 암호, 인증, 네트워크보안, 웹보안, IoT보안