RAW 데이터 통신을 하는 네트워크 프린터의 보안 요구사항 도출

조한익 · 정영현 · 조영복*

대전대학교 정보보안학과

Prevent Information Leakage of Network Printers using the RAW Protocol

Han-ik Cho · Young-hyeon Jeong · Young-bok Cho*

Daejeon University

E-mail : gksdlrdl36@naver.com

요 약

우리는 일반적으로 출력을 위해 인쇄 환경을 컴퓨터와 프린터를 1:1로 로컬연결을 사용하고 있다. 그러나 이런 로컬연결 환경은 공간적, 시간적, 금전적 물리적 한계를 가지고 있어 이를 보완하기 위해 네트워크 기반의 인쇄환경으로 발전되었다. 네트워크 프린터는 문서를 출력하기 위해 패킷으로 데이터를 수신하게 되는데 보안 프로토콜을 지원하지 않는 것이 일반적이다. 따라서 네트워크 프린터를 이용시 인쇄물에 대한 중간자 공격이나 스푸핑 등 네트워크 공격에 노출되어 인쇄중인 문서의 내용이 탈취될 가능성이 있다. 따라서 본 논문에서는 보안 프로토콜이 지원되지 않는 네트워크 프린터 환경에서 인쇄물에 대한 중간자 공격에 대응하기 위한 요구사항을 도출하고 정의한다.

ABSTRACT

The printing environment for output is commonly referred to as computers and printers using local connections in 1: 1 format. However, the local connection environment has spatial, temporal, and financial physical limitations. Therefore, a network-based output environment has been proposed and utilized as a way to supplement this.A network printer receives data in packets for document output, and generally does not support a security protocol. Therefore, when a network printer is used, there is a possibility that the content of a document being printed is stolen by being exposed to a network attack such as a meson attack or spoofing against a printed matter. In this paper, we define and define the requirements to cope with the meson attack on printed materials in a network printer environment where security protocol is not supported.

키워드

네트워크 프린터, RAW socket, man Man in the Middle Attack

Ⅰ. 서 론

과거 프린터는 LPT 포트, COM 포트, USB 포트 등을 이용하여 컴퓨터와 프린터를 물리적인 연결을 통하여 통신을 해왔다. 이러한 통신 방식은 프린터와 PC의 일 대 일로 연결되기 때문에 문서 작업이 많은 기업이나, 관공서, 학교와 같은 기관에서 공간적, 시간적, 금전적 낭비가 존재했다. 이러한 부분을 보완한 네트워크 프린터는 NFC, Bluetooth, 무선 LAN, 유선 LAN과 같은 네트워크 통신 기능을 접목하여 한 대의 프린터에 PC 뿐만 아니라 스마트 폰과 같은 디바이스를 네트워크 통신을 이용하여 일대 다로 인쇄 작업을 할 수 있게 발전하였다. 네트워크 프린터는 통신을 위해 TCP/IP 프로토콜을 사용하고 있다. 인쇄를 요청하는 장치에서 인쇄 대상 파 일에 관한 정보를 프린터가 해석할 수 있는 언어인 PCL, PJL로 기록한 뒤 스풀링을 거쳐 SPL 파일을 생성하여 네트워크를 통해 프린터에게 패킷 단위로 전송을 하는데, 패킷 전송을 위한 통신 프로토콜 종류는 IPP 프로

* corresponding author

토콜 RAW 프로토콜, LPD 프로토콜 등이 존재한다. 2018년 12월 4일 한 해커가 유튜버 홍보를 위하여 약 5만대의 프린터를 해킹하여 홍보한 사건이 있다. 이때 해킹을 당한 프린터는 9100번 포트를 사용하는 RAW 통신을 사용한 네트워크 프린터이다. 또한, 통신 상 보안이 존재하지 않고 패킷이 그대로 노출되는 특징이 있기 때문에 중간자 공격에 의해 네트워크 패킷이 스니핑과 같은 도청을 당할 위험이 있어서 인쇄되는 모든 정보의 노출의 위협이 있다. 개인의 경우 관공서를 거치지 않아도 인터넷을 통해 출력이 가능한 각종 공문서, 교육기관의 시험 출제 문제, 기업의 기밀 내용을 담은 파일 등 다양한 민감한 정보들이 유출 될 가능성도 존재한다.

사물인터넷 검색 엔진 Shodan에서 2019년 4월 1일 9100번 포트와 PJL을 사용하는 네트워크 프린터는 약 3만 6천여 개가 검색되었다. 해커들은 이러한 검색 엔진을 통해 손쉽게 불특정 다수의 공격 대상을 확보 할 수 있다. 여러 국가에서 피해사례가 속출하고 있는 만큼 네트워크 프린터를 사용하는 개인 및 각종 집단과 기관에서는 네트워크 프린터의 보안 설정에 대한 경각심이 요구된다.

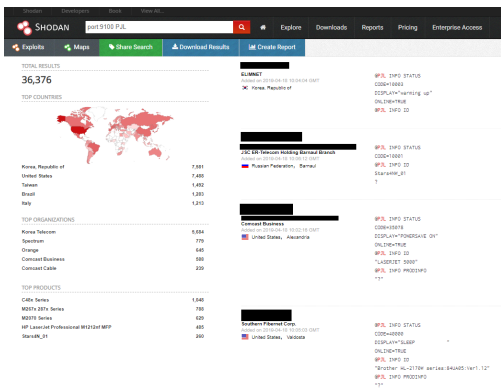


그림 1. 9100 port Shodan 검색 결과

Shodan[1]에서 검색되는 개방되어 있는 9100 port는 공격 가능한 프린터이다. 본 논문에서는 Raw통신을 이용하는 네트워크 프린터가 왜 보안이 취약한지 증명하고 보안 요구사항을 도출한다.

II. 배경지식

2.1 네트워크 프린터 통신

네트워크 프린터는 디바이스와 표준 TCP/IP 통신을 한다. PC는 인쇄 문서를 스풀링한 후에 송신을 하는데 송신에 사용되는 통신 방식은 일반적으로 LPR/LPD(Line Print Deamon)와 RAW 통신이다. LPR/LPD 서비스는 TCP/IP 인쇄 서버 서비스로 515 port를 사용하여 인쇄 작업을 하는 인쇄 서비스다. RFC 1179에 규정되어 있으며 TCP/IP가 일반적으로 사용하는 프로토콜이다. RAW 방식은 문서가 네트워크로 연결된 프린터로 전송되기 전에 번역되는 방식 중 하나로 텍스트나 복잡한 문서를 인쇄하고자 할 때 사용된다. Windows OS 및 표준 TCP/IP를 사용하지 않는 시스템의 기본 프로토콜로 9100번 포트를 사용한다. IPP(Internet Printing Protocol) 프로토콜[2]은 wel-known prot 631번을 사용해 TCP/IP를 사용하는 인터넷 및 인트라넷상의 인쇄 작업의 전송, 감시 그리고 관리를 위한 표준이다. 통신을 위해서는 HTTP 서버 java, SSL이 필요하고 보안을 위해 IPPS를 지원하는데, TLS 암호화 통신 기능이 있고 사용자 인증 기능이 있어, 패킷 스니핑의 위험과 외부 공격으로부터 차단을 할 수 있다는 특징이 있다. 그러나 모든 프린터가 IPP를 지원하지 않는다는 단점을 가지고 있다.

2.2 인쇄 데이터

프린터는 인쇄 데이터를 표현하기 위한 여러 개의 포맷이 존재한다. PJL(Printer Job Language), PCL(Printer Command Language), PS(Post Script)등이 있지만 하나로 통일된 표준이 존재하지 않고, 각 프린터 제조사마다 보유한 독자적인 언어들이 존재하지만. 본 논문에서는 가장 널리 사용되고 있는 HP사의 PJL, PCL[6]에 대해 작성하겠다. PJL은 프린터 언어 전환, 작업 분리, 환경 명령, 상태 되읽기, 장치 관리 및 파일 체계 명령과 같은 작업 수준 제어를 한다. PCL은 출력 할 문서의 폰트, 그래픽, 색상, 등 정보를 통해 이미징 작업을 한다.

III. Raw 데이터 통신의 취약성

3.1 패킷 덤프

네트워크 프린터는 PC나 스마트 폰과 통신을 위해 TCP/IP를 사용하고 있다. 인쇄를 요청하는 장치에서 인쇄 문서에 관한 정보를 프린터가 해석 할 수 있는 언어(PCL, PJL, Post Script 등)로 기록한 뒤 운영체제에서 제공하는 스풀링을 거친 뒤에 SPL 파일을 생성하여 네트워크를 통해 프린터에 패킷 단위로 전송을 한다. Raw 통신을 사용하는 네트워크 프린터는 패킷이 원시 형태로 전송된다.

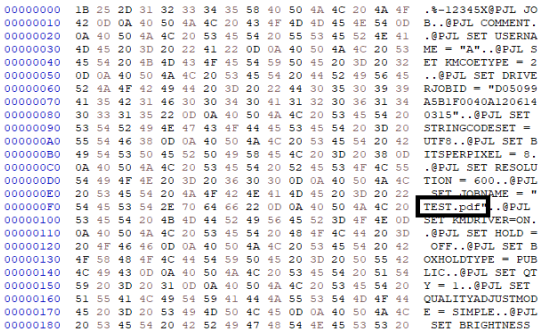


그림 2. PJL 내용

그림2는 Raw 형태로 송신되는 패킷을 와이어샤크로 덤프한 뒤 문서편집기로 실행한 사진이다. 덤프 된 패킷에서 식별 가능한 내용은 사용자가 설정한 출력 옵션이다. 출력하는 문서 파일명과 출력명령을 내린 사용자 ID등이 있다.

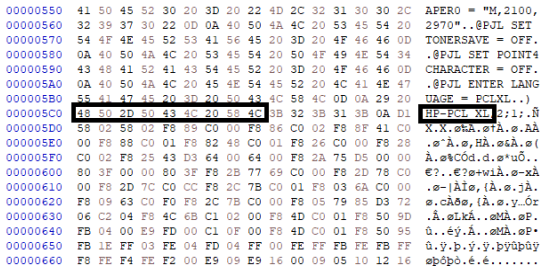
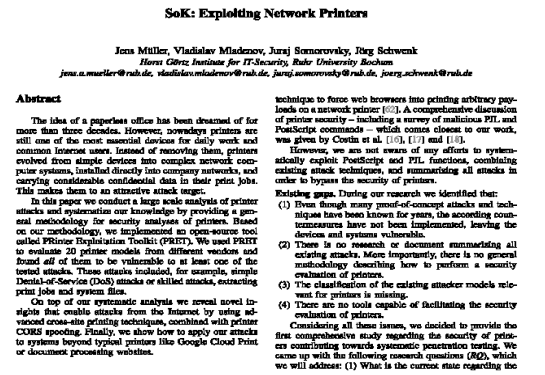


그림 3. PCL 내용

그림3은 PCL이 시작하는 영역을 표시한 그림이다. 0x000005C0부터 파일의 끝까지 PCL로 문서의 페이지 정보, 문자, 글꼴, 이미지, 색상 등 출력에 사용되는 모든 정보들이 기록되어 있다. 사진에서 확인 할 수 있는 정보는 PCL로 기록되어 있는 바이너리 형태의 내용들이지만 PCL Converter 프로그램을 이용하면 바이너리로 존재하는 패킷을 원본 문서로 복원 할 수 있다.



SoK: Exploiting Network Printers

Jens Müller, Vladislav Mladenov, Juraj Somorovsky, Jörg Schwenk
Horst Görtz Institute for IT-Security, Ruhr University Bochum
jens.a.mueller@rub.de, vladislav.mladenov@rub.de, juraj.somorovsky@rub.de, joerg.schwenk@rub.de

Abstract

The idea of a paperless office has been dreamed of for more than three decades. However, nowadays printers are still one of the most essential devices for daily work and common Internet users. Instead of removing them, printers evolved from simple devices into complex network computer systems, installed directly into company networks, and carrying considerable confidential data in their print jobs. This makes them to an attractive attack target.

In this paper we conduct a large scale analysis of printer attacks and systematize our knowledge by providing a general methodology for security analyses of printers. Based on our methodology, we implemented an open-source tool called PRinter Exploitation Toolkit (PRET). We used PRET to evaluate 20 printer models from different vendors and found *all* of them to be vulnerable to at least one of the tested attacks. These attacks included, for example, simple Denial-of-Service (DoS) attacks or skilled attacks, extracting print jobs and system files.

On top of our systematic analysis we reveal novel insights that enable attacks from the Internet by using advanced cross-site printing techniques, combined with printer CORS spoofing. Finally, we show how to apply our attacks to systems beyond typical printers like Google Cloud Print or document processing websites.

그림 4. 복원된 원본 문서

만약 중간자 공격과 같은 네트워크 공격에 의해 패킷 스니핑을 통해 피해자의 네트워크 프린터 전송 패킷을 확보하면 공격자는 원본 형태의 문서로 변환시킬 수도 있으며, 패킷을 덤프 후 동일한 모델의 프린터에 전송시켜 피해자의 출력 문서를 공격자가 출력 할 수도 있다는 위협이 있다.

3.2 서비스 거부

네트워크 프린터에 외부 공격자가 인쇄 작업 패킷을 전송하여 강제로 출력 명령을 내려 프린터의 자원을 고갈 시키는 방법을 통해 프린터를 마비시킬 수도 있고 인쇄 작업 패킷에 악성코드를 삽입하여 프린터의 RIP(Raster Image Processor)에서 처리 할 수 없을 만큼 연산에 많은 시간이 요구되는 문서 출력명령을 내리는 방법과, PostScript 명령어에 %! {} loop 명령을 추가하여 패킷을 전송하면 프린터는 무한루프 상태에 빠지게 된다. 이러한 서비스 거부 공격은 프린터의 악성코드에 대한 취약성도 있지만, 네트워크를 통해서 프린터에게 악성코드를 쉽게 전송 할 수 있으며, 검색 엔진을 통해 그 대상을 쉽게 확보 할 수 있다는 위험성이 있다.

3.3 ARP Spoofing

ARP Protocol은 주소 결정 프로토콜이다. 동작 과정은 ARP Request와 ARP Reply 순서로 이루어지는데, 특정 호스트B의 MAC 주소를 얻기 위해 ARP Request 패킷을 Broadcast를 하면 해당하는 호스트B가 ARP Reply 패킷을 A에게 Unicast한다. Reply 패킷을 받은 호스트A는 ARP Cache Table에 B의 MAC 주소를 저장한다. ARP Cache Table은 가장 마지막에 오는 ARP Reply패킷을 기준으로 갱신되는 ARP Protocol의 구조적인 특징이 ARP Spoofing공격[7]에 이용된다.

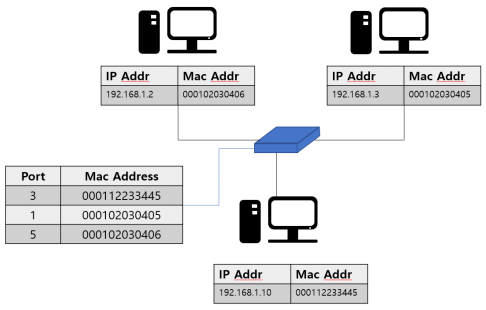


그림 5. ARP 스푸핑 동작 과정

Ⅳ. 실험 및 결과

본 논문에서는 네트워크 프린터의 취약점을 실험을 하기 위해 ARP Spoofing 공격을 진행하였다. 네트워크 구성과 공격자, 피해자의 PC성능은 [표1]과 같다.

표 1. 공격자와 피해자 PC 환경

	공격자	피해자
운영체제	Kali linux	Windows10
CPU	i7-4790k 4.00Ghz	i5-8600k 3.6Ghz
RAM	16GB	16GB

[표 2]는 네트워크 구성도를 정리한 것으로 실험에 사용된 기기들의 IP주소와 MAC 주소를 나타내고 있따. 공격자의 IP 주소는 192.168.0.3이고 MAC 주소는 00-72-63-69-82-c3이다.

표 2. 네트워크 구성도

	IP	MAC
게이트웨이	192.168.0.1	64-e5-99-da-e0-d8
피해자	192.168.0.2	D0-C6-37-55-AF-7D
공격자	192.168.0.3	00-72-63-69-82-c3
프린터	192.168.0.4	30-cd-a7-f2-62-ff

스푸핑을 진행하였을 때 IP주소와 매칭된 MAC 주소의 변경을 확인할 수 있다.

```
인터페이스: 192.168.0.2 --- 0x8
  인터넷 주소           물리적 주소           유형
  192.168.0.1           00-72-63-69-82-c3     동적
  192.168.0.3           00-72-63-69-82-c3     동적
  192.168.0.4           00-72-63-69-82-c3     동적
```

그림 6. 감염된 ARP 테이블

그림 6은 ARP Spoofing을 공격을 받은 피해자의 ARP Cache Table이다. 게이트웨이와 프린터의 MAC address가 공격자의 MAC address로 변조되어 있다. 이렇게 되면 프린터로 가야할 패킷이 공격자에게 전송되고 공격자는 자신에게 오는 패킷을 프린터에게 보내서 출력을 시키고 있다.

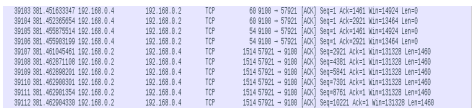


그림 7. 피해자의 데이터 스트림

그림 7은 공격자에게 오고 있는 피해자가 프린터에게 전송중인 패킷 스트림이다. 이 패킷 스트림의 내용은 공격자가 얻을 수 있는 내용은 그림 8과 같다.

```
←%-12345X@PJL JOB
@PJL COMMENT
@PJL SET USERNAME = "Cho"
@PJL SET KMCOETYPE = 2
@PJL SET DRIVERJOBID = "ACDE48001D91041211272D00C6"
@PJL SET STRINGCODESET = UTF8
@PJL SET BITSPERPIXEL = 8
@PJL SET RESOLUTION = 600
@PJL SET JOBNAME = "HWP Document"
@PJL SET KMDRIVER=ON
@PJL SET HOLD = OFF
@PJL SET BOXHOLDTYPE = PUBLIC
@PJL SET QTY = 1
@PJL SET QUALITYADJUSTMODE = SIMPLE
@PJL SET BRIGHTNESS = 0
@PJL SET CONTRAST = 0
@PJL SET SCREEN = AUTO
```

그림 8. 공격자가 탈취한 패킷

그림 8은 공격자가 획득한 패킷이다. 공격자는 탈취한 패킷을 다시 프린터에 보내 출력을 할 수도 있고, 패킷을 이용하여 원본 문서로 복원 시킬 수도 있다.

그림 9. 복원된 원본 문서

그림 9는 공격자가 획득한 패킷을 원본 문서로 복원시킨 사진이다. 공격자는 패킷 스니핑을 통해 간단하게 피해자의 인쇄 데이터를 확보할 수 있었다. 인쇄 데이터는 원본으로 복원될 수도 있고, 프린터에 보내 출력할 수도 있다. 이러한 점을 고려하였을 때 기업, 학교, 관공서 등 다양한 기관에서 네트워크 프린터를 사용할 시 간단한 패킷 스니핑 공격을 통해 문서의 내용이 유출당할 수 있다. 이를 방지하기 위해선 내부 망에서 이루어지는 중간자 공격에 대한 보안이 요구된다.

Ⅴ. 결 론

현재 대중적으로 사용되고 있는 네트워크 프린터는 다수의 사용자가 사용하기 편리하다는 장점을 가지고 있지만, 보안에는 취약하다는 문제점을 가지고 있다. 그 이유는 네트워크와 프린터가 표준 TCP/IP Raw 통신을 하는데 이 과정에서 데이터 암호화가 이루어지지 않는다는 문제점을 ARP Spoofing을 통해 보안 요구사항을 도출했다. 인터넷 프린터 프로토콜을 이용하여 통신을 하면 해결을 할 수 있지만. 모든 프린터가 인터넷 프린터 프로토콜을 지원하진 않는다. 따라서 Raw 통신을 안

전하게 사용하기 위해선 IP주소와 MAC 주소의 정적 관리가 요구된다.

References

[1] https://www.shodan.io
[2] Soo-Hong kim, "A Study of Implementation for Internet Printing Protocol (IPP) System," SpringerPlus, , Dec. 2003
[3] Vorgelegt von, Muller Jens, "Exploiting Network Printers:A Survey of Security Flaws in Laser Printers and Muliti-Function Devices", Sep. 2016
[4] Woojoong Ji, Hyoungshick Kim "A Security Vulnerability Analysis for Printer Kiosks", Feb. 2019
[5] Kwangwoo Lee, Seungjoo Kim, Dongho Won "Smart printing service Security Technology Research Trend", May. 2011
[6] "PCL XL Feature Reference Protocol Class 3.0 Supplement", July. 2002
[7] KISA, "ARP spoofing Attack analysis and countermeasures", jun. 2007
[8] KISA-WP-2008-0017 "A Study on Printer Test Method based on Security Functionality", Nov. 2008