기업 정보 유출 방지를 위한 MFP 보안 취약점 분석 및 보안대책

이동범, 최명균, 곽진
순천향대학교 정보보호학과
e-mail : dblee@sch.ac.kr, mgchoi@sch.ac.kr, jkwak@sch.ac.kr

MFP Security Vulnerability Analysis and Security Policy for Enterprise Information Loss Prevention

Dongbum Lee, Myeonggyun Choi, Jin Kwak
Dept of Information Security Engineering, Soonchunhyang University

요 약

MFP는 프린터, 복사기, 스캐너, 팩스 등의 장치가 결합되어 있는 임베디드 장치로써 출력, 복사, 스캔, 팩스 외에도 대용량의 문서 데이터를 저장하고 네트워크 통신을 이용한 원격 유지보수, 다중 전송 등의 기능을 갖고 있다. 이러한 MFP는 최근 기업 및 공공기관에서 업무의 효율성 증대와 경비절감을 위해 중요한 문서를 처리하는 장비로 널리 보급되고 있다. 하지만 내부 직원이나 공격자들에 의해 중요한 문서들이 외부로 유출되면서 기업의 피해가 증가하고 있다. 따라서 본 논문에서는 기업 내부 정보 유출을 방지하기 위해 MFP에서 발생할 수 있는 다양한 보안 취약점과 그에 따른 대책을 분석하였다.

1. 서론

최근 컴퓨터가 널리 보급되고 인터넷 등 네트워크 기술이 발전하면서 MFP(Multi Function Printer : 디지털 복합기)는 복사 및 프린트와 같은 기본적인 기능 외에도 Web 브라우저를 통한 관리기능, 네트워크 운영, 무선 LAN 지원 등 기본 기능을 편리하게 사용하기 위해 다기능화·고급화가 진행되고 있다. 기능이 다양해지고 복잡해지면서 다양한 경로를 통해 기업 또는 기관의 중요한 내부정보가 유출되어 심각한 피해를 발생시키는 사고가 증가하고 있다[1].

일본 네트워크보안협회의 통계자료에 따르면, 정보유출의 주요 유출 경로로는 이메일, FTP, USB, CD, 노트북, 매체, 출력물 및 문서 등이 있는데, 그 중 출력물에 의한 내부정보 유출 건수가 73% 이상을 차지하며 매체별 유출 비율 중 가장 많은 것으로 분석되었다. 따라서 출력물에 의한 내부정보 유출을 방지하기 위해서 MFP 시스템의 안전한 사용을 위해 플랫폼 자체의 보안 취약점, 네트워크 연결로 인한 보안 취약점 등 MFP에서 발생할 수 있는 다양한 보안 취약점에 대한 대응책을 고려해야 한다[2].

따라서 본 논문에서는 MFP의 보안 취약점 및 대책을 분석하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서 MFP 시스템의 개념을 분석하고, 3장에서는 MFP 시스템의 보안 취약점과 보안 대책을 분석한다. 마지막으로 4장에서는 결론을 맺는다.

2. MFP 시스템

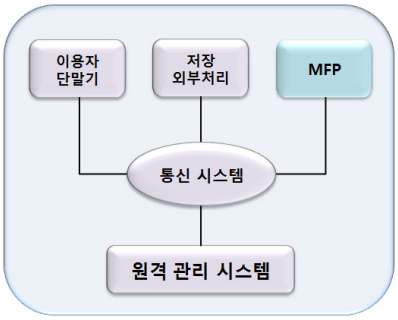
2.1 개념

MFP는 원래 이미징 작업을 중심으로 수행하는 장치였지만 팩스기능이 결합되어 전자화된 이미지 데이터를 전송하는 기능과 네트워크 기능이 추가되어 비약적으로 발전하였다. 네트워크 기능이 추가됨에 따라 하나의 MFP를 여러 사용자가 공유하며, MFP를 기존의 업무 시스템 등과 연계시키고 있다.

(그림 1) MFP 개념

2.2 구성요소

MFP의 구성요소를 살펴보면 (그림 2)와 같이 MFP는 중앙의 통신 시스템을 통하여 이용자 단말기나 기타 외부 장치, 처리장치 등 다른 서비스와 연계하여 작동한다.



(그림 2) MFP 구성요소

□ 이용자 단말기

이용자 단말기는 네트워크 및 통신 시스템을 통하여 MFP를 사용하는 단말기를 말한다. MFP 사용자는 인쇄 및 팩스 전송 등을 수행하는 일반 사용자뿐만 아니라 MFP 본체의 구성을 변경하거나 설정하는 관리자와 일부 소프트웨어를 추가하거나 삭제를 수행하는 보수자를 포함한다.

□ 저장·외부 처리

저장·외부 처리는 주로 MFP 외부 시스템 중 사람이 직접 조작하지 않고 자동적으로 기계가 처리하는 시스템으로 구성된다. MFP의 사용 환경에서 특히 문서의 장기 저장 및 작업 데이터의 임시 저장 및 스풀 처리를 저장하거나 문자 추출, 업무 시스템과의 통합, 문서의 검색 처리 등 다양한 작업을 포함한다.

□ 통신 시스템

통신 시스템은 MFP가 외부 시스템과 통신하기 위한 MFP 외의 통신 시스템을 말한다. 통신 시스템에는 Ethernet 스위치, IP 라우터, 배선, 무선 LAN 접근 지점 등이 있다. MFP에 USB 허브를 통하여 연결하는 경우는 USB 허브와 USB 케이블도 포함된다. 통신 시스템에서 일반적인 사무실에 적합한 MFP 사용 형태는 MFP를 사용하는 기업의 LAN과 VPN과 같은 기업 내에서 폐쇄적인 네트워크에 한정하는 것이 일반적이다. MFP와 사용자 단말기, 저장·외부 처리는 모두 기업의 폐쇄된 네트워크에 연결되어 있다. 하지만 예외적으로 기업의 외부 서비스 업체가 제공하는 원격 관리 서비스와 같이 인터넷과 기업 외부의 네트워크를 경유하는 경우가 있다.

□ 원격 관리 시스템

원격 관리 시스템은 통신 시스템을 통하여 MFP의 관리 작업을 원격으로 수행하기 위한 MFP의 외부 시스템이다. MFP의 구성 변경이나 설정작업 및 보수작업 등을 하기 위해 MFP 업체에서 배포하는 전용 소프트웨어, MFP의 설정을 변경하기 위해 사용되는 브라우저가 원격 관리 시스템에 포함된다.

3. MFP 시스템 취약점 분석 및 보안대책

3.1 데이터 도청

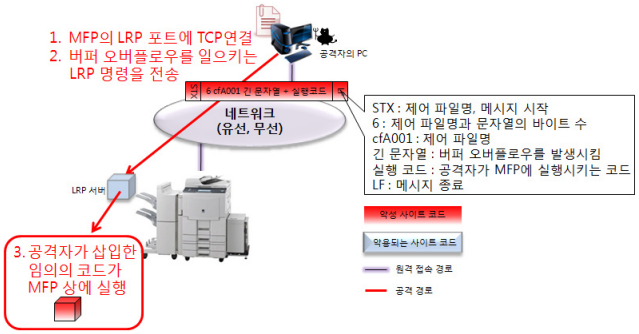
MFP는 프린터, 스캐너, 팩스 등의 여러 장치가 결합되어 있다. 이러한 여러 장치간의 통신을 암호화 등 보안 대책이 구성되어 있지 않은 상태에서 공격자가 MFP에 물리적인 접근이 가능하게 되면 문서 및 주소 등 데이터가 도청될 가능성이 존재한다[3].

□ 보안 대책

- o MFP가 설치되어 있는 장소에는 입·퇴실 관리를 철저히 하고 허가된 사람만이 출입
- o MFP 본체에 불필요한 기기나 장치가 부착 및 설치되어 있지 않은지 확인
- o 고속 대용량의 표준 통신 버스에 통신 데이터 보호 기능의 탑재를 검토

3.2 드라이버 프로토콜을 통한 침입

클라이언트에서 MFP를 조작하는 드라이버 프로토콜의 취약점으로 인해 MFP의 제어 시스템에 침입할 수 있다. (그림 3)에서는 LPR(Line PRinter Daemon protocol)의 취약점을 이용하여 MFP 제어시스템에 침입하는 과정을 나타낸다.



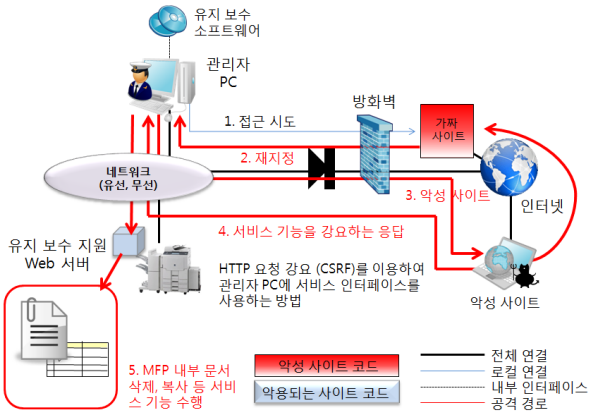
(그림 3) 프로토콜을 통한 침입

□ 보안 대책

o LPR, RAW9100, IPP, SMB, WS/Print SOAP 등 MFP에서 사용할 서버를 식별하고 MFP에 해당하지 않는 서버 기능과 서비스를 기다리는 포트를 정지해 둔다.
o MFP에서 작업 데이터를 투입할 수 있는 호스트로 특정 인쇄 스풀서버와 스캔 및 팩스 게이트웨이 서버 등을 제한한다.
o 상호 인증 방식을 가진 드라이버 프로토콜과 드라이버를 사용하여 운영한다.

3.3 원격 관리 인터페이스를 악용한 정보 유출

공격자가 MFP의 원격 관리 인터페이스를 사용하여 내부 정보 및 MFP와 관련된 다른 시스템의 정보를 불법으로 취득한다. (그림 4)에서는 HTTP 요청을 사용하여 MFP의 정보를 취득하는 과정을 나타낸다[4].



(그림 4) 원격관리 인터페이스 악용

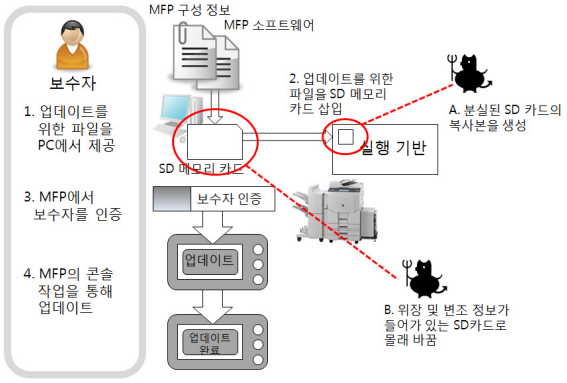
□ 보안 대책

o 불필요한 장소·업체로부터 원격관리를 받지 않음
o 보수 업자가 제공하는 원격 유지 보수 서비스에 접속할 때 상호 인증 및 보호 방식을 확인
o 이용자가 원격 유지 보수 서비스에 접속할 때 통신로를 보호하기 위해 다른 네트워크와 격리하여 사용
o 네트워크 구성 및 주소 구성이 변경되기 때문에 보수 기능의 실행 추적과 침해 감시 기록을 정기적으로 검사

3.4 분리형 매체에 따른 데이터 유출

MFP에 탑재된 SD카드 슬롯은 특정 파일을 포함하는 SD카드를 삽입하여 특정 작업을 하면 MFP의 설정 및 구성을 일괄적으로 업데이트 한다.

이러한 작업을 악용하면 MFP를 구성하는 인증서, 비밀번호 및 주소가 공격자에게 노출되어 공격자가 MFP의 내부 구성이나 설정을 변경할 수도 있으며, 임의의 MFP 소프트웨어가 추가될 가능성이 있다. (그림 5)에서는 SD카드를 이용하여 MFP 일괄 업데이트 하는 작업 중에 데이터가 유출되는 과정을 나타낸다.



(그림 5) SD카드를 통한 데이터 유출

□ 보안 대책

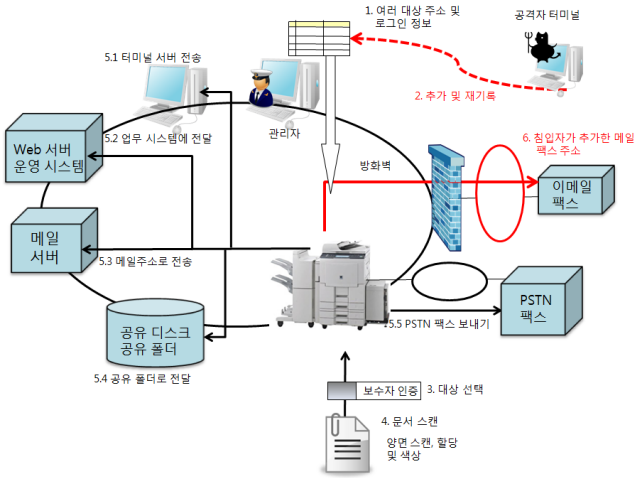
o 보수자 인증을 위한 비밀번호를 적절하게 등록하여 운영
o 자동 일괄 업데이트 기능에 대한 보수 작업을 완료한 후에는 해제
o 정상 작동 중에는 자동 일괄 업데이트 기능이 해제되어 있는지 확인
o MFP의 SD카드 슬롯에 의도하지 않았던 임의의 매체가 삽입되어 있는지 확인

3.5 다중 전송에 따른 데이터 유출

MFP에서는 스캔 된 이미지 또는 팩스로 받은 이미지를 여러 사람에게 일괄 전송하는 기능이 있다. 이때. 일괄적으로 보내는 여러 대상 중에 의도하지 않은 대상이 포함되어 있는 경우 중요한 정보가 유출될 가능성이 있다.

(그림 6)은 어떠한 문서를 일정한 절차를 거쳐 스캔한 이미지를 여러 대상에 일괄 전송 처리하는 도중에 공격자에 의해 데이터가 유출되는 것을 보여준다. 먼저 관리자 단말로부터 복수의 대상 주소와 로그인 정보 등을 MFP에 전송한다. 이 절차를 전후로 공격자 단말기는 관리자 단말기로 위장하거나 관리자 터미널에 요청하여 강제적으로 공격을 실행하여 공격자의 메일 팩스 주소를 추가한다.

다음 MFP의 사용자가 MFP의 콘솔에서 이 대상을 선택하고 해당 문서를 스캔 위치에 놓고 시작버튼을 누르면 해당 검색 방법으로 문서를 검색하고 자동으로 여러 대상 문서 이미지가 전송된다. 이 주소 목록에 공격자의 주소가 섞여있는 경우 사용자는 공격자에게 기밀 정보를 전송하게 된다.



(그림 6) 다중 전송시 데이터 유출 경로

□ 보안 대책

- o 이미지를 다수의 대상에게 일괄 전송하는 경우, 팩스 전용망 및 VPN과 같이 폐쇄된 네트워크에서 메일 팩스와 IP팩스를 운영
- o MFP 내부의 대상 설정 변경 내용을 모니터링하여 대상의 구성 상태를 정기적으로 검사
- o 허용되지 않은 목적지의 전자인증서가 MFP 내부의 주소록과 공유 주소록에 추가 또는 혼입되어 있지 않은지 정기적으로 검사
- o 대상 및 전송의 성공 여부를 기록하여 정기적으로 검사

4. 결론

MFP는 하드웨어 및 소프트웨어의 기능이 다양하기 때문에 구성이 복잡하고 사용하는 프로토콜도 다양한 임베디드 기기이다.

하지만 MFP 인터페이스에 대한 공격으로 네트워크를 통한 공격에 의한 각종 위협에 노출되어 있으므로, MFP에서 발생할 수 있는 다양한 보안 취약점에 대한 대응책을 고려해야 한다.

따라서 MFP의 보안 수준 및 안정성을 유지하기 위해 향후 예상되는 차세대 인터넷 및 클라우드 서비스와의 제휴 기능을 바탕으로 한 향후 연구가 필요하다고 사료된다.

참고문헌

[1] 정보보호학회지, “기업 비밀정보 유출 방지 및 보호 관점에서의 디지털 복합기 보안 기술 동향 분석”, 제 20권 제 1호, 2010년 2월, pp47-55

[2] 일본네크워크보안협회, “http://www.jnsa.org”

[3] MITRE Corporation, “The Common Weaknesses Enumeration (CWE) Initiative”

[4] Ju An Wang , Hao Wang , Minzhe Guo , Linfeng Zhou , Jairo Camargo, Ranking Attacks Based on Vulnerability Analysis, Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, p.1-10, January 05-08, 2010