디지털 복합기에 대한 보안 취약점 분석

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

A Study on Security Vulnerability Analysis for Multi Function Printer

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

요 약

디지털 복합기는 프린터, 복사기, 스캐너, 팩스 등의 장치가 결합되어 있는 임베디드 장치로써 출력, 복사, 스캔, 팩스 외에 네트워크 통신을 이용한 원격 유지보수, 다중 사용자가 맞물려 있는 장치이다. 이러한 디지털 복합기는 최근 기업 및 공공기관에서 업무의 효율성 증대와 경비절감을 위해 중요한 문서를 처리하는 장비로 널리 보급되고 있다. 하지만 산업 스파이나 공격자들에 의해 중요한 문서들이 외부로 유출되면서 기업의 피해가 증가하고 있다. 따라서 본 논문에서는 디지털 복합기에서 발생할 수 있는 다양한 보안 취약점 및 보안 위협을 기밀성, 무결성, 가용성, 부인방지 측면에서 분석하였다.

1. 서론

네트워크 기술의 발전과 IT의 보급에 의해 디지털 복합기(MFP : Multi Function Printer)는 복사 및 프린트와 동일한 기본적인 기능 외에도 Web 브라우저를 통한 관리 기능, 네트워크 운영, 무선 LAN 지원 등 기본 기능을 편리하게 사용하기 위해 다기능화·고급화가 진행되고 있다. 따라서 제품의 안전한 사용을 위해서 정보보안 측면에서 알려진 취약점의 영향을 받는 플랫폼의 사용으로 인한 위험, 네트워크 연결로 인한 위협 등 설계 단계부터 다양한 위협에 대한 대응책을 고려해야 한다.

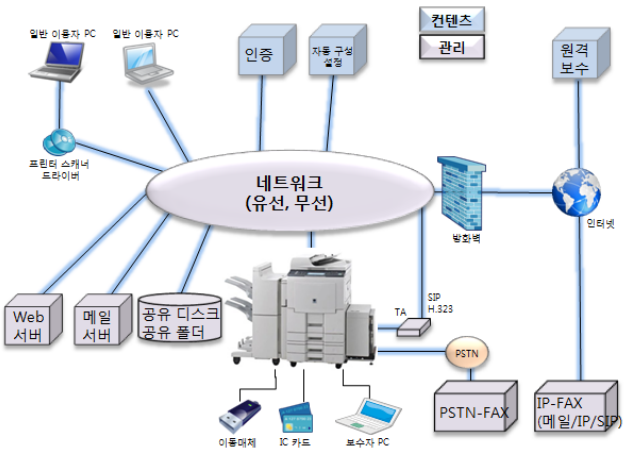
또한 개발자가 예상하지 못한 사용형태 및 설계단계의 간과 또는 잠재적인 문제점이 취약점이 되거나 추후 인지 및 설치조건이나 기밀정보의 관리 체제가 갖추어지지 않는 등 운영상의 문제점도 충분히 취약점이 될 수 있다.

따라서 본 논문에서는 MFP의 정보보안 요구사항에 대한 취약점 및 공격 방법을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서 MFP에 대한 개념을 정리하고 3장에서는 MFP에 대한 보안 취약점을 분석한다. 마지막으로 4장에서는 결론을 맺는다.

2. MFP 개념

다음의 (그림 1)은 MFP의 시스템 구성을 보여주고 있다. MFP에는 USB 메모리와 같은 이동식 매체와 인증을 위한 IC카드 리더가 연결되는 경우가 있다. 기종에 따라서는 미리 MFP 본체 내에 내장되어 있는 경우가 있다.



(그림 1) MFP 시스템 구성

MFP의 오른쪽 하단에 있는 보수자 PC(단말기)는 보수자가 MFP의 고장 진단을 수행하고 백업하기 위한 장치이다. 그림의 왼쪽에는 일반 사용자 PC(단말기)와 관리자 PC(단말기)가 있다. 일반 사용자 단말기는 내부에 MFP 드라이버(프린터 스캐너 드라이버)를 설치, MFP와 통신하여 MFP의 서비스를 사용한다. 관리자 단말기는 MFP를 원격으로 설정하는데 사용한다.

그림의 오른쪽 아래에 있는 것은 팩스 기능이다. PSTN-FAX(PSTN 팩스)는 기존의 전화망을 사용한 아날로그 팩스 모뎀에 의한 이미지 전송할 수 있다. IP-FAX(IP 팩스)는 메일 서버를 사용한 메일 팩스와 IP 주소로 직접 상대방의 MFP에 SMTP을 접속하는 IP 팩스 또한 SIP를 사용하여 팩스 이미지를 전송하는 SIP 팩

스가 있다.

또한 기존 PSTN 팩스의 경우 SIP 또는 H.323로 가변 TA장치를 사용하여 IP화 할 수 있다. TA를 사용하면 원격지의 PSTN 팩스 간의 통신을 IP 네트워크 또는 인터넷을 통하여 중계하고 기존 PSTN을 통해 팩스 통신비용을 줄일 수 있는 장점이 있다.

MFP 왼쪽의 공유 디스크/공유 폴더는 MFP가 스캔한 이미지나 팩스로 수신한 이미지를 저장하는데 자주 이용된다. 그 왼쪽의 메일 서버는 스캔한 이미지나 수신한 팩스의 이미지를 이메일로 수신하고자 할 때 MFP에서 이미지를 전송하는 대상이다. 또한 MFP 내부 이상이나 실패한 작업을 메일 서버를 통하여 관리자나 사용자에게 통지하는 경우도 있다. Web 서버는 MFP가 내장되어 있는 Web 브라우저를 사용하여 MFP 외부의 이미지를 사용하거나 MFP 외부의 업무 시스템과 연계하는데 이용될 수 있다. 인증은 네트워크에서 MFP의 외부에서 인증 서비스를 제공하는 서버 등으로 SSO(Single Sign On) 기능을 제공할 수도 있다[1].

인증의 오른쪽에 있는 자동 구성 설정은 MFP를 포함하는 네트워크 내에서 자동적으로 IP주소 할당, 정확한 시간 동기화, MFP의 가동 감시 기능이 있다. 그림의 오른쪽 상단의 원격 보수는 MFP 제조업체와 서비스 업체가 원격지에서의 MFP 유지 보수 서비스이다. 원격 보수는 토너와 드럼의 수명 모니터링, 인쇄 등의 사용 매수를 모니터링 한다.

3. 보안 취약점 분석

본 장에서는 보안 위협을 포괄적으로 확인할 수 있도록 일반적인 정보 보안에 대한 요구사항으로서 정보보안 관리 표준인 ISO/IEC 27001의 기밀성, 무결성, 가용성, 부인방지에 대한 요구사항을 적용시켜 위협에 대한 공격방법 및 취약점을 분석한다[2].

또한 위협의 원인이 될 수 있는 취약점을 열거할 때는 CWE 일반적인 취약점 유형을 토대로 현 단계의 공격 기법의 예제 및 사용 실수 등을 가정하여 포괄적으로 취약점을 분석하였다[3][4].

3.1 기밀성 측면

기밀성 측면에서 본 보안 위협으로는 MFP 본체 전자인증서의 비밀키와 사용자 또는 다른 시스템의 ID와 비밀번호가 노출되고 문서나 서버의 스푸핑에 악용될 위협이 존재한다. 이로 인해 MFP에서 보호되고 있는 기밀문서 및 주소록 등의 중요 정보들이 지속적으로 유출 되거나 변조될 보안 위협이 존재한다.

<표 1> 기밀성 측면에서 본 보안 취약점

공격방법	보안 취약점
- 관리자의 ID와 비밀번호를 아래의 경로 중 하나가 도청되고 공개될 가능성 : 장치 사이의 버스 네트워크/원격 통신, USB·SD 메모리, Bluetooth와 같은 기계 입출력	- MFP 본체 장치 간의 인터페이스에서 통신되는 데이터가 보호되지 않는 취약점
- 공격자가 관리자로 가장한 후 MFP의 관리자 모드를 사용하여 MFP의 공유 문서가 공격자에게 노출	- 기본 관리자 비밀번호를 누구나 사용할 수 있는 취약점 - 관리자 비밀번호가 지정되어 있지 않은 취약점
- 공격자는 MFP와 업무 시스템 사이에서 보호되지 않은 통신을 도청하여 얻은 ID 또는 비밀번호 세션 정보를 사용하여 MFP를 연결하는 업무 시스템에 공격자가 MFP로 가장하여 연결하고 업무 시스템의 정보가 공격자에 의해 제거 되거나 갱신	- ID, 비밀번호 및 세션정보를 포함하는 구성 정보가 보호되지 않은 채 MFP 내부에 저장되는 취약점 (다른 시스템과 통신로 변경, 비밀번호를 보호하는 인증 절차가 없거나 선택되지 않음)

3.2 무결성 측면

무결성 측면에서 본 보안 위협으로는 사용자의 ID 및 비밀번호가 변경되어 MFP가 제공하는 서비스를 사용자가 사용을 못하게 되거나 MFP 전자인증서의 비밀키가 변조되어 전자인증서를 사용하는 보안 기능이 정지 또는 무효가 될 수 있다. 이로 인해 MFP에 저장되어 있는 기밀문서들이 변조 되거나 인증을 할 수 없게 되는 보안위협이 존재한다.

<표 2> 무결성 측면에서 본 보안 취약점

공격방법	취약점
- 공격자가 관리자로 위장 로그인하여 MFP 본체 전자인증서의 비밀키를 공격자가 생성한 비밀키로 교체하여 MFP의 서버에 대한 SSL/TSL 통신을 지속적으로 전송	- 전자인증서의 비밀키를 안전한 IC/ TMP에 저장하지 않는 취약점

- 공격자는 SQL 인젝션을 악용하여 MFP 내부의 관리 구성 정보를 변경하고, 회사의 이메일, 팩스를 받는 상대방이 해독 불가능이 되거나 회사에서 받은 메일, 팩스 내용을 확인할 수 없게 된다. 경우에 따라 공격자에 의해 발송된 메일, 팩스를 특정 회사로부터 전송된 문서라고 인식	- 관리 구성 정보에 접근할 경우 인증을 우회하는 취약점 - 특정 클라이언트의 인증서와 대상을 연결하여 관리하지 않는 취약점 (믿을 수 있는 루트 CA에서 발급한 클라이언트 인증서를 신뢰하는 취약점)
- MFP에 “POP before SMTP 인증”이 설정되어 있을 경우, POP3 또는 IMAP4 인증 후 몇 분 안에 MFP의 IP주소를 출발IP로 가장한다면 인증 없이 SMTP 메일 송신 서비스를 사용할 수 있기 때문에 공격자가 MFP를 사칭하여 메일, 팩스 및 정크메일을 발송	- IP 주소를 세션 정보에 사용하고 있기 때문에 추측이 쉬운 취약점

3.3 가용성 측면

가용성 측면에서 본 보안 위협으로는 MFP 내부에서 생성하고 등록한 전자인증서 또는 비밀키가 삭제되어 전자서명이나 파일 암호화, 서버 인증서의 검증을 사용할 수 없게 되는 것이다. 그리고 CA 인증서가 삭제 및 수정되어 서버 인증서, 문서의 서명, 코드 서명을 계층적으로 검증할 수 없으며, 사용자 및 다른 시스템을 위한 ID, 패스워드가 변경되어 MFP를 사용할 수 없게 된다.

<표 3> 가용성 측면에서 본 보안 취약점

공격방법	취약점
- 관리자로 위장한 공격자가 MFP의 시간 설정을 1년 앞으로 변경하고 MFP에 저장되는 본체와 대상의 주소, 다른 시스템의 전자인증서를 비활성화 시켜 사용할 수 없게 한다. 그대로 MFP는 통신 경로와 콘텐츠를 보호하지 않고 계속 실행하여 공격자는 네트워크상에서 쉽게 도청하고 문서가 누설됨	- 전자인증서는 1년 정도의 유효기간이 있는 취약점 - MFP 내부의 전자인증서의 유효기간이 만료되는 시점을 알기 어려운 취약점
- 공격자가 EMC 공격 등으로 MFP 내부 IC/TPM 보안 부품의 데이터만 파괴하고 그에 대한 서버 인증서와 클라이언트 인증서를 사용한 보안 기능을 정지시킴	- 보안 IC/TPM을 상실할 경우 MFP 본체의 전자인증서를 사용할 수 없는 취약점
- 어떤 MFP 내부에 본체용 전자인증서가 과실 또는 통신 네트워크 모듈의 취약점으로 침입하여 MFP 본체 전자인증서가 변조되거나 손상되었기 때문에 본체의 SSL/TLS 서버 기능과 S/MIME의 보호 기능을 사용자가 사용 불가능하게 됨	- MFP 본체의 전자인증서가 손상되면 MFP의 보안 서비스를 사용할 수 없는 취약점

3.4 부인방지 측면

부인방지는 특정한 절차를 거쳐 어떠한 작업을 수행한 사실을 사후에 증명함으로써 사실 부인을 방지하는 보안 기술이다. 이러한 부인방지에서 발생할 수 있는 보안 위협으로는 MFP의 전자인증서를 등록한 특정 관리자명에 대해서 확실하게 그 관리자가 실행한 것을 증명하지 못하거나, 사용자 또는 다른 시스템의 ID 및 패스워드에 대해서 신규 등록·변경·삭제를 한 사용자들을 식별하는 기록이 없고 입증할 수 없는 보안위협이 존재한다.

<표 4> 부인방지 측면에서 본 보안 취약점

공격방법	취약점
- 공격자가 관리자로 가장하여 MFP의 전자인증서를 일시적으로 제거했지만 작업 기록에 잘못된 정보를 추가하여 다른 관리자가 작업하는 것처럼 가장하거나 작업 기록을 지운 다음 다른 관리자가 조작한 것 같이 수정	- 작업 기록에 사용자명이 기록되고 있었지만, 그 사용자명은 사용자로부터 임의의 문자열을 투입할 수 있는 취약점
	- 작업 기록에 사용자명이 기록되어 있었지만 그 기록은 다른 사용자가 변경 가능한 취약점

4. 결론

MFP는 문서의 복사, 인쇄, 스캔 및 팩스 등의 업무상 필수적인 처리를 수행하고 있는 임베디드 장치이다. 최근 기업 및 공공기관에서 업무의 효율성 증대를 위해 널리 보급되고 있다. 하지만 최근 출시되고 있는 MFP는 장치의 특성상 항상 네트워크에 연결되어 있으므로 네트워크에서 발생할 수 있는 보안 취약점 및 보안 위협이 MFP

에서도 존재한다. 뿐만 아니라 기업의 내부 비밀정보를 유출하기 위한 산업 스파이가 증가함에 따라 물리적인 측면에서의 보안 취약점도 존재하고 있어 MFP의 보안을 유지하기가 어렵다. 따라서 MFP를 도입하고 있는 기업의 보안 관리자는 MFP에서 제공하고 있는 보안 기능을 명확히 파악하여 해당 기업에 맞는 보안 솔루션을 도입해야 한다. 또한, MFP에서는 민감한 정보인 다수의 개인정보를 다루는 경우가 많기 때문에 이에 대한 보안대책을 강구해야 할 것이다.

참고문헌

[1] GAO Research, Leader in Embedded Technology, "MFP - Multi Function Periperals/Prints"

[2] Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on, 17-19 Dec. 2007, pp 381-388

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

[4] Orvis William J, Van Lehm Allan L. "Data Security Vulnerabilities of Facsimile Machines and Digital Copiers", DoE, CIAC-2304 January 1995.