Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1257

다기능 주변기기에 대한 보호프로파일에 관한 연구

이 동 범†‡
서원대학교

A Study on Protection Profile for Multi-function Devices

Dongubm Lee†‡
Seowon University

요 약

다기능 주변기기는 원래 이미지 처리 작업을 중심으로 수행하는 장치였지만 팩스 기능이 결합하여 전자화된 이미지 데이터를 전송하는 기능과 네트워크 기능이 추가되어 비약적으로 발전하였다. 또한, 다기능 주변기기는 인터넷 응용, 애플리케이션 확장, 원격 공유, 이미지 처리의 기능이 추가되었다. 하지만 다기능 주변기기는 네트워크 연결로 인한 위협으로 발생하는 데이터 노출 및 도청 등의 보안 취약점이 발생할 수 있다. 따라서 다기능 주변기기에 대한 평가 기준이 필요하지만, 현재는 다기능 주변기기에 대한 공통된 보호프로파일이 존재하지 않아서 제품에 대한 안전성을 평가하는데 구체적인 평가 기준을 적용하지 않아 평가 품질의 균일성을 유지하는 것이 어려웠다. 따라서 본 논문에서는 다기능 주변기기에 대한 위협을 분석하여 안전한 다기능 주변기기를 사용하기 위해서 공통평가기준을 기반으로 다기능 주변기기에 대한 보호프로파일을 개발하였다.

ABSTRACT

Multi-functional devices was originally an equipment performing image processing, but function transmitting image data digitized by combining fax function and function of network are added and it was rapidly developed. Also, functions of internet application, application expansion, remote sharing and image treatment were added to multi-functional devices. But, multi-functional devices can cause security vulnerability such as data exposure, eavesdropping, etc. because of the threatening by network connection. Therefore, common criteria of multi-functional devices are necessary, but there is no protection profile for multi-functional devices now. Therefore, concrete standards of evaluation are not applied to evaluate secure for products, so it was difficult to maintain uniformity of evaluation quality. Therefore, this paper developed protection profile for multi-functional devices based on common criteria of evaluation so as to analyze threats of multi-functional devices and use secure multi-functional devices.

Keywords: Multi-functional devices, Common Criteria, Protection Profile

I. 서 론

IT 기술의 빠른 변화에 따라 업무 효율성을 제공하기 위하여 다기능 주변기기(MFP : Multi-function devices)를 널리 사용하고 있다. MFP는 복사, 프린터, 팩스 등 기본적인 기능 외에도 웹 브라우저를 통한 관리 기능, 무선 LAN 지원 등 다양한 기능을 제공하고 있다.

MFP는 원래 이미지 처리 작업을 중심으로 수행하는 장치였지만 팩스 기능이 결합하여 전자화된 이미지 데이터를 전송하는 기능과 네트워크 기능이 추가되어 비약적으로 발전하였다. 네트워크 기능이 추

접수일(2015년 6월 29일), 수정일(2015년 8월 27일), 게재확정일(2015년 10월 2일)
† 주저자, dblee@seowon.ac.kr
‡ 교신저자, dblee@seowon.kr(Corresponding author)

가됨에 따라 하나의 MFP를 여러 사용자가 공유하여, MFP를 기존의 업무 시스템과 연계시켜 업무 효율성을 제공하고 있다.

하지만 MFP의 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. 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.

국제상호인정협정(CCRA : Common Criteria Recognition Arrangement)은 정보보호제품의 안전성을 회원국 간 상호 인정하여 활용을 증진하는 국제협약으로써 1998년 미국, 영국, 캐나다 등 5개국이 평가하고 인증한 정보보호제품을 회원국 상호간 인정하기로 한 협정이 모태이다. 2000년 5월 미국, 영국, 프랑스 등 13개국 정부기관이 참여하여 CCRA에 서명함으로써 공식 출범하였다[1].

CCRA에서는 공통평가기준 및 공통평가방법론(CEM : Common Evaluation Methodology)의 세부 평가 가이드라인, 기술적 변동사항 및 주요 평가 정책 등을 새롭게 제도에 반영하기 위한 세부 위원회들로 구성되어 있다. 이 세부 위원회들은 크게 CCRA 관리 위원회(MC : Management Committee), CCRA 집행 위원회(ES : Executive Subcommittee), CC 개발 위원회(DB : Development Board)로 구성된다[2, 3].

지금까지의 CCRA 활동은 CC/CEM 개발과 각국의 인증 제도간 CC/CEM 적용의 협력에 초점을 맞추어 왔다. 최근 CCRA 회원국의 정부 기관과 제품 개발업체, 평가기관이 협력하여 공통 보호프로파일(cPP : collaborative Protection Profile) 개발을 촉진하는 것에 대해 CCRA 회원국 간에 관심이 높아지고 있다. 이러한 보호프로파일은 여러 국가에서 정부 조달을 위해 활용되는 것을 의도하고 있다[4].

따라서 본 논문에서는 안전한 MFP를 사용하기 위해서 ISO/IEC 15408 공통평가기준(CC : Common Criteria)을 기반으로 MFP에 대한 cPP를 개발하였다.

본 논문의 구성은 다음과 같다. 2장에서는 CCRA 변화 및 CC의 개념에 대해서 살펴보고, 3장에서는 MFP를 분석한다. 4장에서는 MFP를 위한 cPP를 제안하고, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 CCRA의 변화

본 논문에서는 CCRA의 변화의 핵심에 초점을 맞추어 관리 위원회가 이러한 보호프로파일의 적절한 취급에 대해 합의에 이른 기본적인 프레임워크에 대해 분석한다.

다음은 보호프로파일을 관리하는데 필요한 프레임워크에 초점을 둔 관리 위원회의 비전을 나타낸다.

- □ 일반적으로 시판되고 있는 정보통신 기술을 이용한 인증 제품의 일반적인 보안 수준은 이들 제품의 가격과 시기적절한 이용 가능성에 큰 영향을 주지 않고 향상할 필요가 있다.
- □ 그 목표를 지원하고 합리적이고 비교 가능하며 재현할 수 있으면서도 비용 대비 효과적인 평가 결과를 달성하기 위해 cPP 및 지원 문서를 개발하는 기술 커뮤니티(TC : Technical Communities)를 구축함으로써 표준 등급을 높일 필요가 있다.
- □ 상호 인정은 cPP의 달성 가능한 공통 수준에 근거한 것이어야 한다.
- □ cPP는 유사한 제품에 대해 여러 공급자가 각각 독자적인 보안목표명세서(ST : Security Target)를 제공하고 있는 모든 제품 종류에 대해 개발되어야 한다.
- □ cPP나 지원 문서는 인증 제품이 예상된 보안 등급을 달성하는 것을 보증하기 위해 취약성에 대한 분석 요구사항이 필요하다.

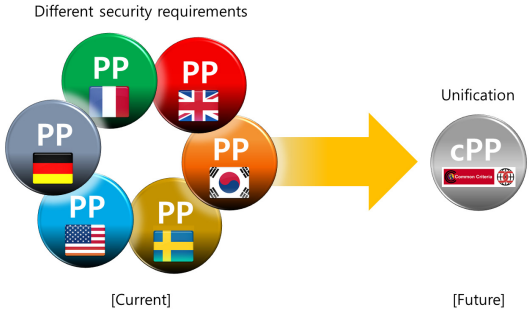

Fig. 1. Common security requirements

2.2 공통평가기준

CC 인증은 정보 기술 보안의 관점에서 정보 기술에 관련된 제품과 시스템이 적절히 설계되어 그 설계가 제대로 구현되어 있는지를 평가하기 위한 국제 표준이다. CC 평가에서는 평가보증수준(EAL : Evaluation Assurance Level)을 정하고 있으며, 7단계(EAL1 ~ EAL7)가 정의되어 있다. EAL은 평가 대상의 검증이 어느 정도까지 진행되었는지를 나타내는 척도이며, 평가 대상의 보호 자산의 가치와 보안 기능에 요구되는 신뢰도에 의해서 EAL을 선택한다[5-7].

서방 국가들이 자국에서 보유하고 있는 인증 평가 제도(미국 : TCSEC, 유럽 : ITSEC)를 기반으로 상용 제품에 대한 활용 및 국제적인 조달의 목적에서 공통평가기준을 책정하는 프로젝트로 CC 개발이 시작되었으며, 1999년 CC는 ISO 표준(ISO/IEC 15408)로 제정되었다.

IT제품 등의 안전성을 객관적으로 평가한 결과를 국제적으로 상호 인정하는 프레임워크로 CCRA가 2000년 5월에 설립되었다. 2014년 7월 현재 25개국이 CCRA에 가입하고 있다. IT 보안 평가 및 인증 제도에서 승인된 평가기관은 IT 제품을 CC에 근거한 보안 평가를 시행하여 인증기관은 평가 보고서 및 평가 과정의 타당성에 대해서 CC에 따라 검증을 한다. 인증기관이 적절하다고 판단한 경우 인증이 수여되고 인증된 제품은 CCRA 회원국 간에 서로 통용된다.

또한 2013년 9월에 개최된 ICCC (International Common Criteria Conference)에서 CCRA 새로운 배열에 관한 기본 합의가 발표되면서 2014년 9월에 CCRA 새로운 배열을 발표 했다. 향후 조달되는 IT 제품에 대한 보안 요구사항(cPP)을 제품의 공급업체와 평가기관이 중심이 된 국제 기술자 집단(iTC)이 공동으로 개발한다. CCRA는 정부 조달에서 고려되는 보안 요구사항을 공통의 cPP로 개발하고 각국이 cPP에 따라 제품 평가를 실시함으로써 효율적으로 보안 제품 평가 및 제품 조달이 가능해진다.

Table. 1. CCRA Members

Certificate Authorizing Members	Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Republic of Korea, Spain, Sweden, Turkey, United Kingdom, United States
Certificate Consuming Members	Austria, the Czech Republic, Denmark, Finland, Greece, Hungary, Israel, Pakistan

2.3 보호프로파일

보호프로파일은 공통평가기준을 사용하여 TOE를 평가할 때 그 평가대상 제품의 종류에 따라 구현에 의존하지 않는 요구가 정리된 문서로서 보안 문제를 해결하기 위한 보안 요구사항을 공통평가기준에서 선택하여 작성한 시스템과 제품별 보안기능 요구사항, 보증 요구사항을 기술한 문서이다.

제품의 평가를 위해 인정된 보호프로파일에 따라 제품을 개발하고 평가를 받거나, 혹은 개발된 제품의 제원을 보호프로파일로 등록하고 평가를 받게 된다. IT 제품과 시스템별 특성에 맞는 보안 목적을 효과적으로 표현하기 위해 평가 기준의 보안기능 요구 사항을 선택하여 보호프로파일을 작성한다.

2.4 MFP의 CC 인증 제품 분석

2015년 현재 MFP의 CC 인증 제품수를 보면 128건으로 분석된다[8].

일본이 가장 많은 85건이며, 한국이 20건, 캐나다는 8건으로 나타나며, 나머지 국가는 6건 미만이다.

일본의 경우 [9]의 표준을 이용하여 68건을 인증받았고, [10]의 표준을 이용하여 6건을 인증 받았다. 또한 [11]의 표준을 이용하여 5건을 인증 받았으며, 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 6건을 인증을 받았다.

한국의 경우 [9]의 표준을 이용하여 6건을 인증

Table. 2. The number of certified products

Scheme	Certified Products
Japan	85
Korea	20
Canada	8
Sweden	5
United States	5
Germany	3
Australia	2
Total	128

받았고, [10]의 표준을 이용하여 5건을 인증 받았다. 또한 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 9건을 인증을 받았다.

캐나다의 경우 [10]의 표준을 이용하여 1건을 인증 받았고, 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 7건을 인증을 받았다.

스웨덴의 경우 [10]의 표준을 이용하여 3건을 인증 받았고, 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 2건을 인증을 받았다.

미국의 경우 [10]의 표준을 이용하여 1건을 인증 받았고, [11]의 표준을 이용하여 4건을 인증 받았다.

독일의 경우 [10]의 표준을 이용하여 1건을 인증 받았고, 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 2건을 인증을 받았다.

오스트레일리아의 경우 기존 표준을 이용하지 않고, 자체적인 ST를 이용하여 2건을 인증을 받았다.

III. 다기능 주변기기

3.1 기능

MFP는 기능적으로 복사, 프린터, 스캐너, 팩스 기능이 일체된 장비를 지칭하며, MFP에는 USB 메모리와 같은 착탈식 매체와 인증을 위한 IC 카드 리더가 연결되어 있다[12-14]. 다음의 Fig. 2.는 MFP 시스템의 구성을 나타낸다.

- □ 단말기 : 보수자 단말기는 보수자가 MFP의 고장 진단을 수행하고 백업하기 위한 장치이며, 일반 사용자 단말기와 관리자 단말기가 있다. 일반 사용자 단말기는 내부에 MFP 드라이버(프린터/스캐너 드라이버)를 설치하여 MFP와 통신을 수행하여 MFP의 서비스를 사용한다. 관리자 단말기는 MFP를 원격에서 설정하는데 사용한다.
- □ PSTN 팩스 : PSTN(Public Switched Telephone Network) 팩스는 기존의 전화망을 사용한 아날로그 팩스 모뎀을 통해 이미지를 전송할 수 있다. IP 팩스는 메일 서버를 사용하는 메일 팩스와 IP 주소로 직접 상대방의 MFP에 SMTP(Simple Mail Transfer Protocol)에 접속하는 IP 팩스 또한 SIP(Session Initiation Protocol)를 사용하여 팩스 이미지를 전송하는 SIP 팩스가 있다.
- □ 공유 폴더/디스크 : 공유 폴더/디스크는 MFP가 스캔한 이미지나 팩스로 수신한 이미지를 저장하는데 이용된다.
- □ 메일 서버 : 메일 서버는 스캔한 이미지나 수신한 팩스의 이미지를 이메일로 수신하고자 할 때 MFP에서 이미지를 전송하는 대상이다. 또한, MFP 내부에서 발생한 오류나 실패한 작업을 메일 서버를 통하여 관리자나 사용자에게 통지하는 서비스를 제공한다.
- □ 웹 서버 : 웹 서버는 MFP에 내장된 웹 브라우저를 사용하여 MFP 외부의 이미지를 사용하거나 MFP 외부의 업무 시스템과 연계하는데 이용한다.
- □ 인증 : 인증은 네트워크에서 MFP의 외부에서 인증 서비스를 제공하는 서버 등으로 SSO(Single Sign On) 기능을 제공한다.
- □ 자동 구성 설정 : 자동 구성 설정은 MFP를 포함하는 네트워크에서 자동으로 IP 주소를 할당하고, 시간을 동기화한다.
- □ 원격 보수 : 원격 보수는 MFP 제조업체와 서비스 업체가 원격지에서의 MFP를 유지 보수하기 위한 서비스로 토너와 드럼의 수명 모니터링, 인쇄 등의 사용 매수에 대한 모니터링을 수행한다.

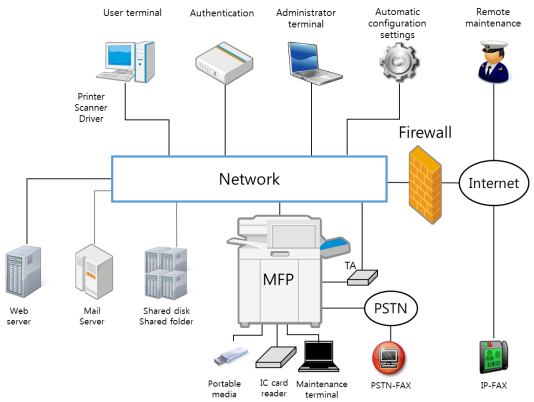

Fig. 2. MFP system

3.2 특성

- □ 이미징 : MFP의 기본 기능인 복사, 인쇄, 스캔, 팩스를 위한 화상 처리와 인쇄 및 읽기의

고해상도화, 고속화가 있으며, 화소수의 증가, 색 농도의 증대, 종이 공급과 인자 속도의 고속화가 진행되고 있다.

□ 어플리케이션 확장 : MFP 개발업체 이외의 타 업체가 개발한 애플리케이션은 특정한 전용 형식의 파일 처리 및 외부 인증 기능과의 연계 기능 등이 있다. 인증에 대해서는 기존의 단일 기능을 대상으로 한 인증 절차뿐만 아니라 여러 기능에서 사용할 수 있는 개방형 인증 절차도 있다.

□ 원격 공유 : 네트워크의 고속화에 의해 원격지와 고속 파일 공유 및 기능의 공유가 더욱 사용하기 쉬워지고 있으며, 파일 공유뿐만 아니라 프린트 기능을 USB 장치로 원격지에서 공유하는 기능도 있다.

□ 인터넷 응용 : MFP에 내장된 기능뿐만 아니라 네트워크에 있는 다양한 기능을 응용하여 활용할 수 있다. 예를 들면 MFP 내부에 공유할 수 있도록 축적된 문서를 고속으로 검색하기 위해 인덱스를 부여하는 서비스와 스캔한 이미지에서 문자를 추출하여 검색하기 쉽게 하는 기능 및 사진 이미지로부터 얼굴을 감지하고 자동으로 분류하는 기능 등이 있다.

IV. 다기능 주변기기를 위한 보호프로파일

본 보호프로파일에서 고려되는 MFP는 하드 카피 문서를 디지털 형식으로 변환하거나(스캔), 디지털 문서를 하드 카피 형태로 변환하는 방법(인쇄), 전화선을 통해 하드카피 문서를 전송하거나(팩스), 하드 카피 문서를 복제하기 위해 사용한다[9, 10].

MFP의 주된 목적 또는 여러 목적에 따라 여러 다른 구성으로 구현된다. 프린터, 스캐너, 복사기, 팩스기 등의 단순한 장치는 단일 기능으로 구현된 단일 목적을 가진다. 복사기로도 사용할 수 있는 팩스기 또는 프린터로 사용할 수 있는 복사기 등의 장치는 주된 단일 목적에 보조적인 기능이 추가되어 있다.

본 보호프로파일에서 고려되는 모든 MFP는 MFP의 보안기능을 관리하는 권한이 적절하게 부여된 사용자에 대한 기능을 제공하는 것을 전제로 하고 있다.

다음은 TOE의 기능을 나타낸다.

□ 인쇄 : 전자 양식에서 종이 문서를 생성

□ 스캔 : 하드 복사 양식에서 전자 문서를 생성

□ 복사 : 하드 복사 문서를 복제

□ 팩스 : 하드 복사 형태의 문서를 스캔하고 전화선을 통해 전자 형식으로 전송

□ 문서 저장 및 추출 : 1건의 문서 처리 작업 사이에 전자 문서를 저장하고, 1개 또는 복수의 후속하는 문서 처리 작업에 접근. 마지막 문서 처리 작업에 저장된 전자 문서를 꺼냄

4.1 TOE 범위

본 보호프로파일의 객체는 생성, 읽기, 수정, 삭제 가능한 데이터 및 실행 가능한 기능이다. 이러한 객체와 객체간의 통신은 추상적으로 정의되어 있다.

TOE 외부에서 생성된 사용자 데이터와 TSF 데이터가 TOE에 전송되는 경우 및 TOE가 사용자 데이터와 TSF 데이터를 생성하여 TOE에서 전송되는 경우가 예상된다. 이러면 무단 공개 및 변경으로부터 각 데이터를 보호하는 충분한 보안 대책이 TOE 환경에 존재하는 것으로 기대된다. TOE는 옵션으로 이 보호를 지원하는 기능을 제공할 수 있다[15-24].

다음은 TOE의 범위를 Fig. 3.에서 나타낸다.

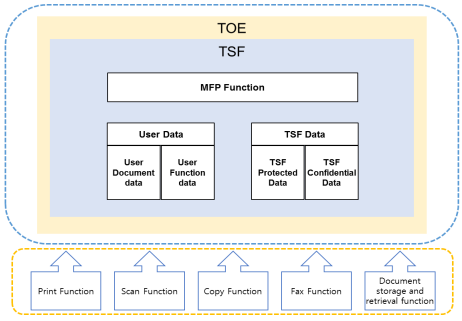

Fig. 3. Scope of TOE

4.1.1 사용자 데이터

사용자 데이터는 사용자가 작성하거나 사용자들을 위해 작성된 TOE 보안기능의 오퍼레이션에 영향을 주지 않는 데이터이다. 사용자 데이터는 사용자 문서 데이터와 사용자 기능 데이터의 객체로 이루어진다.

다음은 사용자 데이터의 구분을 나타낸다.

□ 사용자 문서 데이터 : 하드 카피 또는 전자 양식, 이미지 데이터 또는 하드 카피 장치가 원

고를 처리하고 하드 카피 출력을 생성하는 동안 임시로 저장된 데이터

□ 사용자 기능 데이터 : TOE가 처리하는 사용자 문서 또는 작업에 대한 정보

4.1.2 TSF 데이터

TSF 데이터는 TOE가 작성하거나 TOE용으로 작성된 데이터이며, TOE의 오퍼레이션에 영향을 미치는 데이터를 가리킨다. TSF 데이터는 TSF 보호 데이터와 TSF 기밀 데이터의 객체로 이루어진다.

다음은 TSF 데이터의 구분을 나타낸다.

□ TSF 보호 데이터 : 관리자와 데이터 소유자 이외의 사용자에 의한 변경이 TOE 오퍼레이션 보안에 영향을 미칠 수 있지만, 그 공개가 허용되는 자산

□ TSF 기밀 데이터 : 관리자와 데이터 소유자 이외의 사용자에 의한 수정 또는 공개가 TOE 오퍼레이션 보안에 영향을 미칠 수 있는 자산

4.2 보안문제 정의

본 절에서는 TOE 및 TOE 운영환경에서 다루어야 하는 보안 문제를 정의한다. 보안 문제 정의는 TOE 및 TOE 운영환경이 다루도록 의도된 위협, 조직의 보안정책 및 가정사항을 정의한다[25-29].

Table. 3. 은 본 논문에서 사용하는 보호프로파일의 표시 기호를 나타낸다.

Table. 3. Acronyms

T	Threats
P	Organizational security policies
A	Assumptions
O	Security objectives for the TOE
OE	Security objectives for the operational environment

4.2.1 위협

위협원은 일반적으로 TOE 및 보호대상 시스템에 불법적인 접근을 시도하거나 비정상적인 방법으로 TOE에 위해를 가하는 IT 실체 및 사용인이다. 위협원은 중간 수준의 전문지식, 자원, 동기를 가진다.

□ T. 고장

: TOE를 사용하는 도중에 전원 공급이 중단되거나, 충격 등으로 TSF 서비스가 불완전하게 종료되어 사용자 데이터 및 TSF 데이터가 노출 및 손상되어 위협원이 이를 악용할 수 있다.

ex) MFP 본체 내부의 일부 기기에 전원 계통이나 신호 변경 계통 등에 직접 연결하여 전기적인 부하를 주거나 전자파에 의해 전기적인 부하를 주어 MFP의 작동을 정지시킬 수 있다.

□ T. 논리적인 공격

: 위협원이 논리적인 인터페이스를 악용하여 사용자 데이터나 TSF 데이터를 변경, 노출할 수 있다.

ex) MFP 내부에서 실행되는 소프트웨어 중 하나의 취약점을 사용하여 임의의 코드를 주입하여 관리자 모드를 취득하고 MFP 내부의 파일 시스템에 지시하여 소프트웨어를 삭제 및 갱신할 수 있다.

□ T. 전송 데이터 노출

: 위협원이 TOE와 외부 실체 사이에 통신을 도청하여 사용자 데이터 및 TSF 데이터를 노출할 수 있다.

ex) MFP 본체 내부 구조의 버스, 디버그 단자, 모듈 버스 단자, 기기의 연결 단자 등에 전기적으로 연결하여 버스 또는 단자에서 통신 데이터를 도청할 수 있다.

□ T. 연속 인증 시도

: 위협원이 연속적으로 인증을 시도하여 TOE에 접근할 수 있다.

ex) 공격자가 MFP 입력 취약점을 사용하여 MFP가 받아들이는 특정 서비스 포트의 인증 기능만이 통과되도록 실행 중인 소프트웨어에 후크를 삽입하고 이후 공격자가 인증 없이 MFP를 공격하고 다른 시스템에 위장 접근이 이루어지고 다른 시스템의 업무 데이터 유출할 수 있다.

□ T. 위장

: 위협원이 인가된 사용자로 위장하여 TOE에 접근할 수 있다.

ex) MFP가 작업 데이터를 받아 연결을 설정할 때 다른 시스템 간에 주고받는 인증 절차의 통신 내용이 보호되지 않아 공격자에게 ID와 비밀번호를 유출되고 명의가 도용될 수 있다.

□ T. 잔여 정보
: TOE가 자원을 재사용할 경우, 객체의 정보를 적절하게 제거하지 못해 위협원이 정보에 불법적으로 접근할 수 있다.
ex) 스풀 서버 또는 스캔 결과를 저장하는 파일 서버에서는 작업 데이터 또는 스캔 결과 파일을 인증 과정을 거치지 않는 재기록이 가능한 공개 폴더에 저장하여 공격자가 쉽게 문서에 접근 및 삭제를 할 수 있다.

4.2.2 조직의 보안정책

본 절에서 기술하는 조직의 보안정책은 본 보호프로파일을 수용하는 TOE에 의해서 다루어진다.

□ P. 감사
: 보안과 관련된 모든 행동에 대한 책임을 추적하기 위해 보안 관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다.
ex) MFP 정보와 운영 중 사고 등의 기록으로부터 적절한 운영이 이루어지는지 여부와 그 결과 대책으로서 무엇을 수행해야 할지 검토되어야 한다.

□ P. 안전한 관리
: 인가된 관리자가 안전한 방식으로 TOE를 관리할 수 있도록 관리 수단을 제공해야 한다.
ex) 관리자는 MFP의 운영을 지원하는 역할을 하고 설정의 추가 및 삭제, 실행 정보를 검색, 모니터링 등을 실시해야 한다.

4.2.3 가정사항

다음의 조건들이 본 보호프로파일을 수용하는 TOE 운영환경에 존재한다고 가정한다.

□ A. 신뢰된 사용자
: TOE의 인가된 사용자로 악의가 없으며, TOE 사용 기능에 대하여 적절히 교육받았고, 사용자 지침에 따라 정확하게 의무를 수행한다.
ex) MFP 사용자는 MFP에서의 문서 취급 방법

Table. 4. Rationale for Security Objectives

Security Objectives / Security Problem Definition	Security Objectives for the TOE							Security Objectives for Operational Environment				
	O. Audit	O. Management	O. User authentication	O. Residual information protection	O. Store data protection	O. Access control	O. Transmitted data protection	OE. Timestamp	OE. Trust Manager	OE. Life-cycle protection	OE. Internal hardware	OE. Secure use
T. Failure		X									X	
T. Logical attacks	X				X	X						
T. Transmitted data exposure	X						X					
T. Continuous authentication attempt	X		X									
T. Camouflage	X		X									
T. Residual information				X							X	
P. Audit	X		X					X		X		
P. Secure management		X										
A. Trust user												X
A. Trust developer										X		
A. Trust Manager									X			
A. Internal hardware											X	

및 인증 방법, 조작을 모를 때의 연락처 등의 교육을 이수해야 한다.

□ A. 신뢰된 개발자
: MFP의 개발 및 생산 단계 동안에 TOE 및 관련된 개발 도구는 개발자에 의해 불법적으로 변경되거나 노출되지 않는다.
ex) 개발자는 관리 도구를 사용하여 MFP 내부 정보 및 MFP와 관련된 다른 시스템의 정보를 변경 및 노출되지 않게 해야 한다.

□ A. 신뢰된 관리자
: TOE의 인가된 관리자로 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 의무를 수행한다.
ex) MFP의 운영을 지원하는 역할을 하고 설정의 추가 및 삭제, 실행 정보의 검색, 모니터링 등을 실시해야 한다.

□ A. 하부 하드웨어
: TOE가 운영되는 하부 하드웨어로 TOE의 보안기능을 지원하기 위해 암호 연산을 제공하며, 물리적으로 안전하다.
ex) MFP는 공격자의 물리적인 접근으로부터 안전해야 하며, 여러 장치간의 통신을 암호화 등으로 보호해야 한다.

4.3 보안목적

제안하는 보호프로파일은 보안목적을 TOE에 대한 보안목적 및 운영환경에 대한 보안목적으로 분류하여 정의한다. TOE에 대한 보안목적은 TOE에 의해서 직접 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안 기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야 하는 보안목적이다[30-32].

4.3.1 TOE 보안목적

다음은 TOE에 의해 직접 다루어져야 하는 보안목적이다.

□ O. 감사
: TOE의 보안과 관련된 행동의 책임추적이 가능하도록 보안 관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야 한다.
ex) 감사 기록은 정기적으로 관리자가 감사 내용을 요약하거나 추출하여 검토해야 한다.

□ O. 관리
: TOE의 인가된 사용자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.
ex) MFP의 관리자 콘솔에서 구성 관리 정보를 변경할 수 있기 때문에 관리자의 인증 절차가 필요하다. 필요에 따라 IC 카드와 생체 인식 정보의 요구를 검토해야 한다.

□ O. 사용자 인증
: TOE가 사용자를 유일하게 식별해야 하며, TOE의 관리 및 객체에 대한 접근을 허용하기 전에 사용자의 신원을 인증해야 한다. 또한, 악의적인 연속 인증 시도에 대응수단을 갖추어야 한다.
ex) MFP에서 관리자를 식별하기 위해 비접촉 IC 카드와 지문 등 생체 정보의 사용을 검토해야 한다.

□ O. 잔여정보 보호
: TOE가 TSF를 사용하는 작업영역에 사용 종료 시, 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.
ex) 사용자 단말기를 인증하여 MFP에서 그 사용자 단말기의 세션 정보를 생성한 경우 작업이 완료되면 사용자 단말기의 세션 정보를 제거해야 한다.

□ O. 저장 데이터 보호
: TOE에 저장된 사용자 데이터 및 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
ex) MFP의 스토리지에 저장된 데이터 및 기밀정보를 암호화 등으로 보호해야 한다.

□ O. 접근통제
: TOE의 접근통제 정책에 따라 TOE에 대한 접근을 통제하여야 한다.
ex) MFP를 사용하는 환경에서 적용되는 보안정책을 MFP에도 적용하기 쉽도록 보안 도구를 검토해야 한다.

□ O. 전송 데이터 보호
: 단말기와 MFP 사이에 전송되는 TSF 데이터를 인가되지 않은 노출, 변경으로부터 보호해야 한다.
ex) MFP 내부 장치 사이의 인터페이스에서

송·수신되는 작업 데이터의 통신로를 안전하게 보호해야 한다.

4.3.2 운영환경에 대한 보안목적

다음은 TOE가 보안 기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야 하는 보안목적이다.

□ OE. 타임스탬프
: TOE 운영환경에서 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안 관련 사건을 정확하게 기록해야 한다.
ex) MFP의 운용 기록을 기록하는 로그, 인증 서버, 암호화 기능, 전자인증서 등을 위해서 시간을 시스템에 동기화해야 한다.

□ OE. 신뢰된 관리자
: TOE에 인가된 관리자로 악의가 없으며, TOE 관리 기능에 대하여 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행해야 한다.
ex) 관리자는 MFP의 사용 설명서대로 MFP의 불필요한 서비스를 중지시키고 사용할 서비스만 작동시켜야 한다.

□ OE. 생명주기 내 보호
: MFP의 제조, 발급 각 과정에 대해 물리적, 인적, 절차적 보안 대책이 수립되어 운영되어야 한다.
ex) 제품의 기획 및 개발 과정을 통해 제품의 취약점을 분석하고, 취약점 검사 도구, 소스 코드의 정적 분석 도구, 방화벽, 침입 테스트 도구 등의 사용을 고려해야 한다.

□ OE. 하부 하드웨어
: TOE가 물리적으로 안전한 IC 칩 상에서 동작하는 것을 보장해야 하며, TOE의 하부 하드웨어는 다양한 물리적인 공격에 대한 대응책을 가지고 있어야 한다.
ex) IC 칩은 MFP의 보안 기능성을 지원하기 위해 난수 생성 및 암호 연산을 제공하며, 역공학 분석 등을 이용한 물리적 공격으로부터 MFP를 보호하기 위한 물리적 보호 기능을 제공한다.

□ OE. 안전한 사용
: TOE가 인가된 사용자에 의해 안전한 방식으로 설치, 관리, 사용되어야 한다.
ex) 관리자는 MFP의 사용 설명서대로 MFP의 불필요한 서비스를 중지시키고 사용할 서비스만 작동시켜야 한다.

4.4 보안목적의 이론적 근거

보안목적의 이론적 근거는 보안목적을 보안 문제 정의에서 기술한 위협, 조직의 보안정책, 가정사항을 상호 참조하고, 위협, 조직의 보안정책, 가정사항을 다양한 각도에서 확인한 결과 보안목적에서 해결되어 향후 검토 사항에서 제외되는 것을 나타내는 근거를 마련하는 것이다.

보안목적이 모든 위협에 대응함을 입증해야 하며, 모든 조직의 보안정책을 수행함을 입증해야 한다. 또한, 운영환경에 대한 보안목적이 모든 가정사항을 지원함을 입증해야 한다.

보안목적의 이론적 근거는 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해 다루어지고, 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다루는 것을 입증한다.

4.5 보안기능 요구사항

보안기능 요구사항은 TOE의 전반적인 기능성 모델을 기반으로 선택된다. 이 기능성 모델은 자원, 사용자, 주체, 객체, 오퍼레이션에 관해 규정하고 있다. 보안기능 요구사항에서는 보안 목적이 TOE의 기능 요구사항 모델의 범위 내에서 준수하는 것으로 보안 기능을 정의한다.

다음의 Table. 5.는 본 보호프로파일에서 식별한 TOE 보안목적을 만족하게 하도록 보호프로파일에서 사용하는 보안기능 요구사항에 대한 컴포넌트들을 나타낸다.

4.6 보안기능 요구사항의 이론적 근거

보안 요구사항의 이론적 근거는 서술된 보안 요구사항이 보안목적을 만족하게 하기에 그 결과 보안 문제를 다루기에 적절함을 입증한다.

보안기능 요구사항의 이론적 근거는 각 TOE 보안 목적은 적어도 하나의 TOE 보안기능 요구사항에 의해서 다루어지고, 각 보안기능 요구사항은 적어도 하나의 TOE 보안목적을 입증한다.

Table. 5. Security Functional Requirements

Class	Component	
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_ITC.1	Import of user data without security attributes
	FDP_ITC.2	Import of user data with security attributes
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.3	TSF-initiated termination

I. 결 론

MFP는 기존에 복사를 중심으로 한 이미지 처리 작업을 수행하는 장치였지만 여기에 팩스가 통합되어 전자화된 이미지 데이터를 전송하는 기능과 네트워크 기능이 추가되어 비약적으로 기능이 향상하였다.

네트워크를 통하여 MFP를 여러 사용자가 공유하는 원격 공유와 MFP를 기존의 업무 시스템 등과 연계시키는 애플리케이션 확장 등의 기능이 추가되어 MFP의 신뢰성에 대한 보안 요구사항이 증가하게 되었다.

또한, 현재는 MFP에 대한 보호프로파일이 국가별로 동일하지 않아 제품에 대한 안전성을 평가하는데 구체적인 평가 기준을 적용하지 않아 평가 품질의 균일성을 유지하는 것이 어려웠다.

따라서 본 논문에서는 MFP에 대한 일반적인 보안기능 요구사항과 달성 가능한 보증 수준의 최소 집합을 정하는 MFP에 대한 cPP를 개발하였다.

MFP에 필요한 보안 기능이 포함되어 있으며, 잘 구현되고 취약점이 없는지 평가하기 위한 구체적인 평가 작업이 기술되므로 안전한 MFP를 단기간에 효과적으로 평가할 수 있고 어떤 평가기관이 평가를 시행하여도 재현성 있는 일관된 평가 결과를 얻을 수 있을 것으로 예상한다.

또한, 평가에 걸리는 시간을 단축할 수 있어 시기적절하게 평가된 MFP를 조달할 수 있어 평가 비용을 절약할 수 있다.

References

〔1〕 https://www.niap-ccevs.org/ccra/
〔2〕 http://www.commoncriteriaportal.org/i

ccc/
〔3〕 Xu, L., Wang, B., Zhang, N., Goto, Y., Cheng, J., "Providing Users with Suitable Services of Information Security Engineering Cloud based on ISO/IEC 15408," IEEE 4th International Conference on Software Engineering and Service Science, Beijing, China, pp. 321-325, 2013.
〔4〕 CCRA, "Vision statement for the future direction of the application of the CC and the CCRA," Common Criteria Recognition Arrangement Common Criteria Management Committee Vision Statement, pp. 1-4, Sep. 2012.
〔5〕 CCRA, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model," v3.1r4, pp. 29-47, Sep. 2012.
〔6〕 CCRA, "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components," v3.1r4, pp. 13-184, Sep. 2012.
〔7〕 CCRA, "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components," v3.1r4, pp. 9-17, Sep. 2012.
〔8〕 http://www.commoncriteriaportal.org
〔9〕 IEEE, "IEEE Standard for a Protection Profile in Operational Environment A," pp. 33-49, Sep. 2009.
〔10〕 IEEE, "IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. Operational Environment B," pp. 35-52, Feb. 2010.
〔11〕 IEEE, "US Government Protection Profile for Hardcopy Devices," v1.0, pp. 5-14, Feb. 2010.
〔12〕 Taguchi, K., Yoshioka, N., Tobita, T., Kaneko, H., "Aligning security requirements and security assurance using the common criteria," Fourth International Conference on Secure Software Integration and Reliability Improvement, pp. 69 - 77, Jun. 2010.
〔13〕 Canon, "Canon image RUNNER ADVANCE C5200 Series 2600.1 model Security Target," v1.05, pp. 13-24, Oct. 2012.
〔14〕 IPA, "Research Report on the Security of MFPs," v1.0, pp 20-32, Aug. 2013.
〔15〕 FUJI XEROX, "Xerox Multi-Function Device Security Target," v1.4, pp. 18-26, Dec. 2014.
〔16〕 Hewlett-Packard, "LaserJet Enterprise MFP M525, M725, and M830 Series and Color LaserJet Enterprise MFP M575, M775, and M880 Series Firmware with Jetdirect Inside Security Target," v2.0, pp. 12-30, Jun. 2014.
〔17〕 TOSHIBA, "Loops/e-STUDIO306LP Multifunctional Digital Systems Security Target." v1.0, pp. 4-16, Nov. 2014.
〔18〕 FUJI XEROX, "Xerox D136 Copier/Printer Security Target," v1.0.3, pp. 21-27, Aug. 2013.
〔19〕 FUJI XEROX, "Xerox Work Centre 7232/7242 Security Target," v1.0.4, pp. 8-17, Feb. 2008.
〔20〕 RICOH, "RICOH MP 1601/1301 Security Target," v1.1, pp. 11-23, May. 2013.
〔21〕 KONICA MINOLTA, "bizhub C253/bizhub C203/ineo+253/ineo+203 Control Software Security Target," v1.03, pp. 18-25, Sep. 2007.
〔22〕 National Cyber Security Center, "Smart Card Open Platform Protection Profile," v2.2, pp. 13-20, Dec. 2010.
〔23〕 National Cyber Security Center, "Network Intrusion Prevention System Protection Profile," v2.1, pp. 11-20, June. 2010.
〔24〕 National Cyber Security Center, "Software-based Secure USB System Protection Profile," v1.0, pp. 11-17, Apr. 2010.
〔25〕 TOSHIBA, "e-STUDIO 2555c/3055c.3555

c/4555c/5055c/2555cse/3055cse/3555cse/4555cse/5055cse Multifunctional Digital Systems Security Target," v1.0, pp. 14-41, Apr. 2013.
〔26〕 RICOH, "MP 1601/1301 Security Target," v1.1, pp. 35-39, May. 2013.
〔27〕 RICOH, "MP 2001/2501 series Security Target," v1.0, pp. 34-31, Apr. 2013.
〔28〕 Cannon, "Canon image RUNNER ADVANCE 8200 Series 2600.1 model Security Target," v1.04, pp. 19-23, Mar. 2013.
〔29〕 Cannon, "Canon image RUNNER ADVANCE 6200 Series 2600.1 model Security Target," v1.04, pp. 29-44, Mar. 2013.
〔30〕 Cannon, "Canon image RUNNER ADVANCE C2200 Series 2600.1 model Security Target," v1.1, pp. 48-51, Jun. 2013.
〔31〕 KONICA MINOLTA, "bizhub C554e/bizhub C454e/bizhub C364e/bizhub C284e/bizhub C224e PKI Card System Control Software Security Target," v1.06, pp. 27-45, Jun. 2013.
〔32〕 RICOH, "Canon image RUNNER ADVANCE C9200 PRO Series/C7200 Series 2600.1 model Security Target," v1.08, pp. 29-44, Mar. 2013.
〔33〕 RICOH, "MP C4503/C4503G/C5503/C5503G/C6003G , MP C4503A/C5503A, MP C6003 (Ricoh/Savin/Lanier/nashuatec/Rex-Rotary/Gestetner/infotec) Security Target," v1.0, pp. 34-41, Oct. 2013.

〈저자소개〉

이 동 범 (Dongbum Lee) 정회원
2008년 2월: 순천향대학교 학사
2010년 2월: 순천향대학교 석사
2015년 2월: 순천향대학교 박사
2015년 3월~현재: 서원대학교 정보보안학과 조교수
〈관심분야〉 보안성 평가, 정보보호관리