情 報 保 護 學 會 誌
第21卷 第3號, 2011. 5

# 스마트 프린팅 서비스 보안 기술 연구 동향

이 광 우*, 김 승 주**, 원 동 호***

요 약

최근 스마트폰, 스마트 TV 등의 스마트 기기의 도입에 따른 스마트 서비스의 등장은 기존의 방송, 통신, 교통, 업무 환경을 계속 변화시키고 있다. 즉, 기존과 달리 스마트 서비스 환경에서는 스마트 기기들이 곳곳에 배치되어 유·무선 네트워크를 통해 정보를 주고받으며, 각종 서비스를 제공한다. 따라서 스마트 기기들 간의 통신은 기존 ICT(Information and Communication Technology) 시스템과 동일하게 전송 데이터를 보호하기 위한 보안 기술이 요구된다. 특히 스마트워크에서는 시간과 장소에 국한되지 않고 언제 어디서든 효율적인 업무 수행이 가능하도록 스마트폰 및 태블릿 PC와 같은 모바일 기기를 이용하게 된다. 이러한 상황에서는 여러 공간에서 업무가 이루어질 수 있으며, 프린팅 역시 다양한 네트워크 환경에서 이루어질 수 있다. 이에 본 논문에서는 업무 공간의 다양성과 모바일 기기의 도입에 따른 프린팅 서비스 기술의 발전 및 개발 현황을 살펴보고, 안전한 프린팅과 관련하여 진행되고 있는 표준화 동향을 살펴보고자 한다.

## Ⅰ. 서 론

저탄소 녹색성장 정책에 따라, 효율적으로 온실가스 배출을 감소시키고, 청정에너지와 녹색기술의 연구개발이라는 목표 하에 다양한 분야의 기술을 접목한 융합 기술에 대한 관심이 높아지고 있다[1]. 최근에는 이러한 시대적 요구를 반영하여 '스마트 기술'이 사회적 트렌드로 자리잡아가고 있다. 즉 기존의 가전 기기 및 통신 장치에 ICT 기술이 접목되어, 스마트폰, 스마트TV 등의 스마트 관련 제품과 스마트 그리드, 스마트 오피스, 스마트워크 등의 관련 개념이 등장하고 있다.

스마트 기기의 다양화 및 대중화에 따른 고도화된 스마트 서비스의 등장은 기존의 방송, 통신, 교통, 업무 환경을 계속 진화시키고 있다. 즉, 스마트 서비스 환경에서는 스마트 기기들이 곳곳에 배치되어 유선(Serial, Parallel, Ethernet) 네트워크 및 무선(WiFi, ZigBee, RFID, Bluetooth, NFC, 3G Network 등) 네트워크를 통해 원하는 서비스에 대한 정보 및 데이터를 주고받으며, 다양한 서비스를 제공한다. 따라서 스마트 기기들 간의 송수신 정보는 제3자의 간섭이나 침입으로부터 보호되어야 하며, 기존 ICT 시스템과 같이 전송 데이터에 대한 암호화 및 무결성, 기기 간의 상호 인증, 그리고 기기 자체에 대한 템퍼링 공격을 막기 위한 보안 기술 등이 요구된다.

스마트워크에서는 시간과 장소에 얽매이지 않고 언제 어디서든 효율적인 업무 수행이 가능하도록 스마트폰 및 태블릿 PC와 같은 모바일 기기를 이용하게 되며, 회사, 자택, 스마트워크센터, 공공장소 등의 다양한 공간에서 업무가 이루어질 수 있다[2]. 이와 함께 프린팅 역시 다양한 네트워크 환경에서 이루어질 수 있다. 하지만, 공공장소와 같이 신뢰할 수 없는 공간에서 업무를 수행하다가 기업의 영업비밀정보가 포함된 문서, 고객의 개인정보가 포함된 문서, 대외비 문서 등을 안전하지 않은 방법으로 프린팅 또는 전송하게 될 경우, 제3자에게 해당 문서가 유출될 수 있으며, 사회적·국가적·경제적으로 큰 문제를 초래할 수 있다. 이에 본 논문에서는 업무 공간의 다양성과 모바일 기기의 도입에 따라 변화하는 프린팅 기술의 발전 및 개발 현황을 살펴보고, 안전한 프린팅 기술 개발을 위해 진행되고 있는 표준화 동향을 살펴보고자 한다.

* 성균관대학교 정보보호연구소 (kwlee@security.re.kr)
** 고려대학교 정보보호대학원 부교수 (skim71@korea.ac.kr)
*** 성균관대학교 정보통신공학부 교수 (dhwon@security.re.kr)

본 논문의 구성은 다음과 같다. 2장에서는 스마트워크의 개념과 스마트워크 환경에서의 프린팅 보안 기술의 중요성을 살펴보고, 3장에서 스마트 프린팅 서비스 및 보안기술 개발 동향을 소개한다. 4장에서는 스마트 프린팅 보안과 관련된 표준화 동향을 살펴보고, 마지막으로 5장에서 결론을 맺는다.

## Ⅱ. 스마트워크의 개념 및 프린팅 보안 기술의 중요성

스마트워크는 ICT 기술이 주도하여 스마트 코리아를 실현하는 핵심 원동력으로, 생산성 저하, 고령화, 저출산, 일자리 창출과 같은 국가 사회 현안 문제를 해결하기 위해 추진되었다. 스마트워크센터는 공무원이나 일반 기업의 근무자들이 직장이 아닌 주거지와 가까운 지역에서 근무할 수 있도록 조성한 환경이다. 스마트워크센터에는 업무에 필요한 ICT 인프라(PC, 프린터 또는 복합기, 전화기, 영상회의설비 등)를 갖추어져 있으며, ICT 시스템의 보안 취약점인 정보유출을 막기 위해 서버 보안, 네트워크 보안, 보안 USB 도입, 개인 저장기록 자동소거 SW 등을 도입하고 있다. 또한 정보보호 대응체계를 고도화하여 발생할 수 있는 보안 문제를 미연에 방지하고자 노력하고 있다[2].

하지만, 하나의 프린터를 다수의 사용자가 공유하고 있거나 불특정 다수의 사람들이 접근할 수 있는 공개된 공간에 프린터가 설치되어 있다면, 다양한 보안 문제가 발생할 수 있다. 예를 들어, 중요 문서를 프린팅한 후 프린팅한 사실을 잊어버린 경우나 동일한 문서를 여러 차례에 걸쳐 프린팅한 후 불필요하게 프린팅된 자료를 세절하지 않고 휴지통에 버릴 경우, 중요 문서가 제3자에게 노출될 수 있으며, 이를 통해 해당 관공서나 기업은 큰 대가를 치룰 수 있다. 또한 HDD가 탑재되어 있는 프린터의 경우에는 HDD를 분리하지 않고 폐기하였거나 HDD 완전삭제를 수행하지 않은 경우에 HDD에 완전히 삭제되지 않고 남아있는 데이터를 복구하여 실제 프린팅한 문서를 추출할 수 있다. 스마트워크 환경에서는 여러 장소에서 업무가 이루어질 수 있으므로, ICT 인프라에 대한 보안과 함께 프린팅에 대한 보안 역시 강조되어야 한다.

## Ⅲ. 스마트 프린팅 서비스 및 보안 기술 개발 동향

최근 스마트워크의 등장과 함께 프린팅 관련 업체에서는 모바일 기기(스마트폰, 태블릿 PC)를 이용하여 원하는 문서나 사진을 간편하게 출력할 수 있는 기술들이 개발되고 있다.

### 3.1 HP의 ePrint 서비스

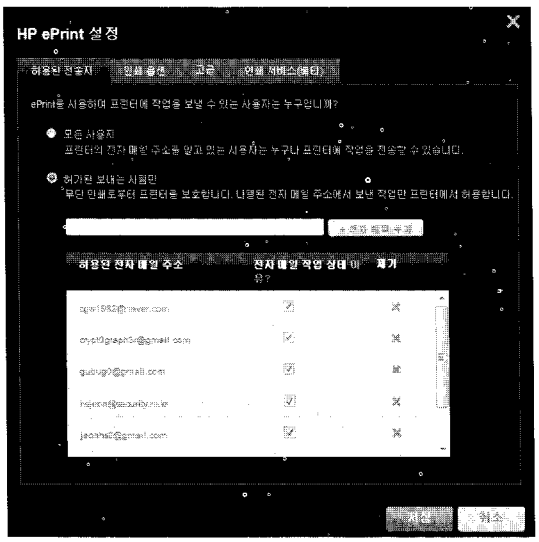
HP에서는 최근 ePrint 서비스를 발표하였다[3]. ePrint는 이메일을 전송할 수 있는 노트북, 태블릿 PC, 스마트폰 등의 무선 기기를 이용하여 특정 주소로 이메일을 전송하면, 언제 어디서나 ePrint 서비스가 적용되어 있는 해당 프린터로 문서를 출력해주는 기술이다. 이는 HP에서 ePrint 서비스가 적용되는 모든 프린터에 프린터 고유 이메일 주소를 지정하였기 때문이다. 이 서비스는 출력하고자 하는 문서를 이메일(*******@hpeprint.com)에 첨부하여 전송하면, HP 자체 네트워크 서버에 기록되며, 프린터가 해당 이메일을 수신하여 문서를 출력하게 된다.


〔그림 1〕 HP의 ePrint 서비스

이 방식은 지정된 이메일 주소로 첨부파일을 전송하여 출력하는 방식이므로, 임의의 사용자가 해당 프린터의 이메일 주소로 스팸 메일을 전송하면 해당 프린터의 자원을 고갈시킬 수 있다는 문제점을 가지고 있다. 따라서 HP에서는 이러한 문제점을 방지하기 위해 웹페이지를 통하여 ePrint 서비스 수신이 가능한 이메일 목록을 설정할 수 있도록 권한 설정 기능을 제공하고 있다. 또한 프린터에 ePrint 문서 출력 요청 이메일이 들어온 경우, 지정된 사용자에게 이메일로 통보해주는 기능을 가지고 있다.

이 방식은 이메일 전송이 가능한 모든 시스템에서 별

도의 드라이버나 소프트웨어를 설치하지 않아도 편리하게 프린팅이 가능하다는 장점을 가지고 있다. 반면에 HP의 웹사이트가 유지 보수 중에는 아래 [그림 3]과 같이 기능 제한 모드로 운영되어 프린팅 권한 설정이 불가능하다는 단점을 가지고 있다.




〔그림 2〕 ePrint 프린팅 권한 설정


〔그림 3〕 ePrint 서비스 유지보수에 의한 기능제한 모드

또한 ePrint 서비스는 기업이나 공공기관의 관점에서 프린팅하고자 하는 문서의 원본 파일이 HP가 관리하는 서버에 그대로 저장되므로, 중요 문서가 제3자에게 노출될 수 있다는 문제점을 가지고 있다. 따라서, 이러한 문제점을 개선하기 위해 HP에서는 기업 사용자를 위한 엔터프라이즈 솔루션을 공급하고 있다. 이 솔루션은 해당 기업에서 관리되는 내부 서버에 출력 문서 파일을 전송함으로써, 외부 서버에 문서가 전송되어 유출되는 문제를 개선하였다.

### 3.2 신도리코의 U-Print 서비스

신도리코는 U-Print 기술을 이용한 프린팅 서비스를 제공한다[4]. U-Print 기술은 모바일 기기를 이용하여 문서를 출력하면, 해당 데이터는 중앙서버에 먼저 저장되고 그 서버와 네트워크로 연결되어 있는 모든 복합기에서 언제 어디에서든지 프린팅이 가능하도록 해주는 기술이다. 사용자는 서버에 연결되어 있는 프린터에 가서 생체인식 또는 스마트카드 등을 이용하여 인증을 받은 후 해당 문서를 프린팅할 수 있다.

### 3.3 Apple의 AirPrint 서비스

AirPrint는 Apple사에서 개발한 아이폰(iPhone), 아이패드(iPad)에 iOS 4.2 이상의 운영체제를 탑재한 경우 또는 및 맥북(Macbook)에 Mac OS X를 탑재한 경우, 주변에 있는 프린터로 무선 프린팅을 해주는 서비스이다[5]. AirPrint를 이용하기 위해서는 무선 프린팅을 하기 위한 무선 장치(아이폰, 아이패드, 맥북) 이외에 AirPrint 서비스를 지원하는 무선 프린터가 요구된다. 현재 AirPrint 서비스를 제공하는 무선 프린터는 HP에서 17종이 개발되어 있으며, 향후 계속 증가할 것으로 예상된다.


〔그림 4〕 Apple의 AirPrint 서비스

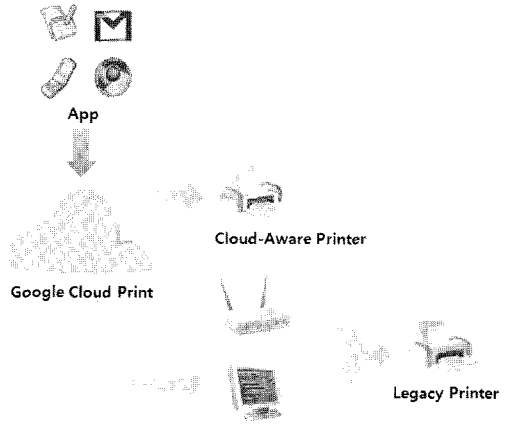
만약 AirPrint 서비스를 제공하는 무선 프린터가 없을 경우에는, 일반 프린터를 무선 노트북에 연결한 후 무선 노트북에 Elpamsoft에서 배포하는 AirPrint Installer for Windows(x86 & x64) v1.1를 설치하여 AirPrint 서비스를 이용할 수 있다. 이 방식은 Windows의 사용자 계정에 기반하여 HTTP 프로토콜에서 지원하는 Digest Authentication이라는 인증 기능을 제공하며, SSL Handshake 프로토콜에 기반하여 무선 장치와 프린터 구간의 데이터를 암호화하여 안전하게 전송한다.

AirPrint는 프린팅을 하고자 하는 무선 장치(아이폰, 아이패드, 맥북)에 별도의 드라이버를 설치하지 않아도

출력이 가능하다는 장점을 가지고 있다.

### 3.4 구글(Google)의 클라우드 프린팅

구글 클라우드 프린트(Google Cloud Print) 프로젝트는 크롬 운영체제 사용자가 시간과 장소뿐만 아니라, 출력을 수행하는 어플리케이션에 구애받지 않고, 어떤 프린터로도 문서를 출력할 수 있도록 하는 것을 목표로 하는 프로젝트이다[6]. 구글 클라우드 프린트는 크롬 운영체제의 웹 호스팅 기반 프록시를 통해 출력 작업을 라우팅해 줌으로써 웹이나 데스크톱, 모바일 애플리케이션 에 프린터 드라이버를 설치하지 않아도 된다는 장점을 가지고 있다.




〔그림 5〕 구글 클라우드 프린팅의 개념

구글 클라우드 프린팅은 애플리케이션이 요청한 출력 작업을 사용자가 선택한 특정 옵션에 맞춰 적절한 프린터로 전송하는 일을 맡으며, 작업 진행 상태를 사용자에게 알려준다.

### 3.5 삼성전자의 유비쿼터스 프린팅과 DLNA 기술

삼성전자는 2009년부터 한국마이크로소프트와 협력하여 퍼블릭 클라우드 프린팅 서비스를 개발하였다. 마이크로소프트의 퍼블릭 클라우드 컴퓨팅 서비스는 윈도우 애저를 활용한 클라우드 프린팅 서비스로써, 작성한 문서를 인터넷의 가상 서버에 저장해놓고, 공항이나 커피숍과 같이 공공장소에 설치된 프린터를 통해 해당 문서를 다운로드 받아 출력하는 서비스이다. 이 클라우드 프린팅 서비스는 자택, 사무실, 공공기간 어디에서든 원하는 문서를 프린팅하는 기술이다. 또한 삼성전자의 무선 네트워크 제품에는 DLNA (Digital Living Network Allicance)가 탑재되어 있다. DLNA란 가전이나 PC, 스마트폰 등이 홈네트워크를 통해 음악이나 사진, 동영상 등 미디어 콘텐츠를 자유롭게 공유할 수 있도록 지원하는 규격이다. 따라서 DLNA 인증을 받은 제품(스마트폰, 스마트TV, 디지털 카메라, 디지털 복합기, 프린터 등) 간에는 해당 규격의 프로토콜을 통해 프린팅을 요청할 수 있다. 현재 삼성전자 디지털 복합기 15종, EPSON 프린터 10종, HP 프린터 9종이 프린팅 기능을 제공하는 규격으로 DLNA 인증을 획득하였다[7]. 이 밖에도 원터치 프린팅, 원터치 무선 네트워크 설정 등 사용자가 쉽고 편리하게 원하는 문서를 프린팅할 수 있도록 다양한 솔루션을 제공하고 있다.

## Ⅳ. 스마트 프린터 보안 기술 관련 표준화 동향

스마트 프린팅 서비스에 대한 표준화 활동은 주로 IEEE P2600 Working Group, Printer Working Group에서 이루어지고 있으며, Wi-Fi Alliance, Bluetooth, Trusted Computing Group 등이 해당 기술에 보안과 관련된 요소 기술들을 포함하여 표준화하고 있다.

### 4.1 IEEE P2600 Working Group

IEEE P2600 Working Group은 2004년 40여개 이상의 기관 및 업체에서 100여명의 관계자들이 모여 조직한 IEEE Computer Society의 IEEE 정보 보증 표준 위원회(Information Assurance Standards Committee)의 지원을 받는 표준화 작업반으로, 현재 대다수의 주요 프린터 제조업체가 참여하고 있다[8]. 또한 프린터, 팩스, 스캐너가 결합된 형태의 제품인 복합기가 정보보호 관점에서 중요해지자 NIAP(National Information Assurance Partnership)과 미국방조달청(DLA, Defense Logistics Agency)의 관계자도 표준화 작업반에 참여하게 되었다. 이 표준화 활동에서는 프린터, 팩스, 스캐너, 복사기와 같이 종이 문서를 출력하는 복합기에서 발생할 수 있는 위협을 분석하고, 해당 위협을 해결하기 위한 보안 대책을 제시하고 있으며, 구현된 제품의 보안기능을 평가하기 위해 공통평가기준(CC, Common Criteria)에 기반한 평가기준인 보호프로파일(Protection

Profile)을 개발하는 등 많은 노력을 기울이고 있다.

IEEE P2600은 복합기 내부에 저장된 사용자 데이터와 시스템 관리 데이터, 물리적인 복합기 자원, 복합기 운영 펌웨어 등을 복합기가 보호해야 할 자산으로 정의하고, 복합기가 안전하게 보호해야 할 자산의 중요도에 따라 A, B, C, D의 네 가지 운영환경을 제시하였다[9].

〔표 1〕 운영환경별 보안 요구사항 수준

| 운영환경 / 보안 항목 | A | B | C | D |
|---|---|---|---|---|
| 자산의 가치 | 고 | 중 | 중저 | 저 |
| 물리적 보안 | 고 | 중 | 저 | 저 |
| 네트워크 보호 | 고 | 중 | 중 | 저 |
| 법 및 구제 | 고 | 중저 | 저 | 저 |
| 인적 자원 신뢰 | 고 | 중 | 저 | 저 |

IEEE P2600 작업반에서는 이러한 운영환경별 자산, 위협, 보안 요구사항의 수준 등의 특성을 반영하여 전체 표준화 작업의 지침이 되는 표준 지침 문서 1종과 각 운영환경별 보호프로파일 4종을 개발하였으며, 추가로

〔표 2〕 IEEE P2600 작업반 표준 목록

| 표준명 | 내용 |
|---|---|
| IEEE Std. 2600™ -2008 | 전체 표준화 작업의 지침이 되는 문서로, 복합기 및 관련 시스템에 대한 정의, 운영환경, 자산, 위협, 보안 기능에 대해 서술하고 있다. |
| IEEE Std. 2600.1™ -2009 | 운영환경 A를 위한 보호프로파일로, NIAP에서 2009년에 평가인증을 받았다. 운영환경 A는 대기업이나 정부기관 등 중요정보를 취급하여 보안 강도가 높게 적용되어야 하는 환경을 위해 작성되었다. |
| IEEE Std. 2600.2™ -2009 | 운영환경 B를 위한 보호프로파일로, BSI (British Standards Institution)에서 2010년에 평가인증을 받았다. 운영환경 B는 중소기업부터 대기업, 일부 정부기관 등의 환경에 필요한 요구사항을 명시하였다. IEEE 2600.1보다는 상대적으로 보안 요구사항의 강도가 낮다. |
| IEEE Std. 2600.3™ -2009 | 운영환경 C를 위한 보호프로파일이며, 2010년 출판되었으며, 운영환경 C는 인쇄소나 공공 도서관 또는 인터넷 카페와 같이 높은 수준의 보안이 요구되지 않은 환경을 위해 작성되었다. |
| IEEE Std. 2600.4™ -2010 | 운영환경 D를 위한 보호프로파일로 2010년 출판되었으며, 소규모 사무실이나 가정 등과 같이 거의 보안이 요구되지 않는 환경을 위해 작성되었다. |

제품 개발자를 위한 안내서 1종을 2011년에 개발 및 배포하고 있다. 이상에서 살펴본 각 표준 문서별 세부 내용은 다음과 같다.

2011년 4월 현재, IEEE P2600 작업반에 따르면, Ricoh(2010년 2월), 삼성전자(2010년 11월), Lexmark (2011년 2월) 3개 프린터 회사만이 IEEE Std. 2600.1 보호프로파일을 준수하여 CC 인증을 획득하였다.

### 4.2 PWG (Printer Working Group)

Printer Working Group(이하 PWG)은 IEEE -ISTO (Industry Standards and Technology Organization)의

〔표 3〕 PWG에서 현재 진행 중인 세부 작업반

| 작업반 | 활동 |
|---|---|
| Workgroup for Imaging Management Solutions (WIMS) | WIMS에서는 기존에 정의된 출력 장치나 서비스 관리 요소들을 표준 관리 프로토콜 (SNMP, CIM 등)에 맵핑하는 작업을 수행하고 있다. |
| Multifunction Device Working Group (MFD) | MFD에서는 다양한 장치 및 서비스에서의 상호 호환성을 제공하기 위하여 복합기에 기본적으로 요구되는 사항을 도출하여, 단일화된 표준 모델을 설계하고, 관련 문법을 정의하는 것을 목적으로 하고 있다. |
| PWG Semantic Model (SM) | SM은 다른 PWG의 작업반에서 작성한 문서 및 IETF에 제출된 문서의 의미 요소를 설명하고, HLD (High Level Design)와 XML 스키마의 작성을 담당하고 있다. |
| PWG MIB WG (PMP) | PMP는 프린터 관리를 위해 요구되는 다양한 MIB(Management Information Base) 표준을 개발해왔다. 현재는 IANA 등록 관리와 MIB 개발 지원을 위해 WIMS 산하에서 작업중이다. |
| The Internet Printing Protocol (IPP) | IPP에서는 인터넷 프린팅 프로토콜 산업 표준을 개발하였다. IPP는 현재 IANA 등록 및 PWG/ISTO 표준 관리, 그리고 향후 네트워크 프린팅에 요구되는 서비스 개발을 위해 활동중이다. |
| Imaging Device Security (IDS) | IDS에서는 네트워크에서 클라이언트 및 다른 장치의 보안 상태를 검증하고 측정하기 위한 요구사항 정의 및 프로토콜의 개발을 목표로 하고 있다. |
| Cloud Imaging | Cloud Imaging에서는 클라우드 기반 프린팅의 요구사항 및 모델을 정의하고, 프린터 및 복합기가 IPP 및 SOAP와 결합되기 위한 방법을 정의하기 위해 논의 중이다. |

프로그램으로 프린터/복합기 제조사, 프린터 서버 개발자, 운영체제 공급자, 프린팅 관리 응용프로그램 개발자 등이 참여하고 있으며, 프린터, 복합기, 응용프로그램, 운영체제 간의 상호호환을 지원하기 위한 작업들을 수행하는 대표적인 프로그램이다[10]. PWG의 세부 작업반에서는 활동은 다음 [표 3]과 같다.

PWG의 세부 작업반 중 스마트 워크에서의 프린팅과 관련된 세부 작업반으로는 Cloud Imaging 작업반과 IPP 작업반이 있다. 이 중 Cloud Imaging 작업반은 2011년 3월부터 초기 드래프트 문서 작업을 시작하여 아직까지 분석할 자료가 공개되어 있지 않다.

반면에 IPP 작업반은 Novell의 제안에 의해 1996년부터 활동을 시작하였다. 현재 IETF RFC에 표준 문서 17개가 등록되어 있으며, IANA 표준 후보로 12건이 올라가 있다. IPP 프로토콜은 인터넷을 통해 원격 프린팅을 지원하기 위한 개발된 네트워크 표준 프로토콜로 1999년 초기 버전인 IPP/1.0이 표준화 되었으며, 2000년에 IPP/1.1이 표준화 되었다. IPP 프로토콜은 원격 프린팅 외에도 프린트 잡(print job)과 출력 문서 속성을 관리할 수 있으며, 보안 기능으로 접근제어, 인증, 암호화를 지원하고 있다.

또한 IPP 작업반에서는 프린터 드라이버를 설치하지 않아도 모바일 기기에서 출력이 가능하도록 2010년 2월부터 IPP Everywhere 표준화 작업을 진행하고 있다.

### 4.3 Wi-Fi Alliance와 Bluetooth

스마트폰과 같은 모바일 기기가 많아지면서 프린터를 포함한 주변기기들이 무선 네트워크 인터페이스를 채택하는 경우가 증가하고 있다. 무선 네트워크는 유선 네트워크와 달리 제3자에 의한 도청이 쉽기 때문에, 보안 설정이 중요하다. 하지만, 긴 길이의 비밀키나 패스워드를 입력해야 하기 때문에 사용자는 불편함을 느끼게 된다. 이러한 불편함을 개선하기 위해서 2007년 Wi-Fi Alliance는 무선 네트워크 보안 설정을 쉽고 안전하게 제공하는 WPS(Wi-Fi Protected Setup) 기술을 발표하였다[11]. WPS 기술의 목표는 무선 네트워크 보안 설정 과정을 간소화하는 것으로 크게 4가지 방식이 있다. PIN(Personal Identification Number) 방식은 화면에 표시되거나 제품에 붙어있는 일련번호를 다른 제품에 입력하여 두 기기간 보안 설정을 WPA2로 만드는 것이며, PBC(Push-Button Configuration) 방식은 사용자가 양쪽 기기에 있는 버튼을 눌러 WPA2로 무선 보안을 설정하는 방식이다. 이 외에도 근거리에 디바이스를 가져가면 보안 설정이 되는 NFC(Near Field Communication) 방식과 USB를 사용하여 양쪽 기기의 보안을 설정하는 USB 방식이 있다[11].

또한 Wi-Fi Alliance에서는 두 무선 기기가 AP를 거치지 않고도 서로 데이터를 송수신할 수 있도록 하는 Wi-Fi Direct 인증 프로그램을 개발하였으며, 이와 유사한 기술로 블루투스 3.0이 있다[12]. 블루투스 3.0은 2009년에 발표되었다. 이 기술은 802.11 PAL(Protocol Adaptation Layer)을 이용하여 최대 24Mbps의 속도를 갖는다. 따라서 블루투스 기기 간에 대용량 그림, 동영상, 파일 전송이 가능하며, PC를 모바일 기기와 동기화를 할 수 있고, 프린터를 대용량 문서의 출력이 가능하다. Wi-Fi Direct나 블루투스3.0을 이용할 경우, 모바일 기기에서 프린터로 직접 출력이 가능하며 보안 설정이 가능하다. 이 점은 기존 클라우드 기반 프린팅 방식이나 네트워크 프린팅 방식과 달리 인터넷을 거치지 않아도 출력이 가능하므로 보안 관점에서는 장점이 될 수 있다.

### 4.4 TCG(Trusted Computing Group)

이 밖에도 프린터의 보안 기능을 향상시키기 위한 기술로 TPM(Trusted Platform Module) 기술이 적용될 수 있다. TPM은 프린터 내부 상태 정보에 대한 임의적인 변경 및 삭제를 방지할 수 있으며, 프린터 플랫폼 자체에 대한 무결성을 제공할 수 있다. 현재 TPM에 대한 표준화 활동은 신뢰 컴퓨팅 및 보안 기술에 대한 산업 표준을 정의하고 있는 TCG(Trusted Computing Group)에 의해 주도되고 있다[13]. 신뢰 컴퓨팅에서 가장 기본이 되는 TPM은 부채널 공격에 대해서도 정보 유출 차단 및 훼손 방지(tamper-proof)가 보장되어야 하므로, 하드웨어 형태의 칩으로 구현된다. 하드웨어 형태의 TPM 칩에는 암호 프로세서가 탑재되어 안전한 암호학적 연산 기능이 가능하며, 물리적 공격으로부터 TPM 고유키를 안전하게 저장할 수 있는 비휘발성 메모리를 가지고 있다. 현재 TPM은 Infineon, Atmel, Broadcom, Intel, Sinosun, ST마이크로일렉트로닉스, Nuvoton, ITE, TOSHIBA 등에 의해 제조되고 있다[14].

## V. 결 론

최근 국내에서 발생한 두 차례(2010.7.7, 2011.3.4)의

대형 DDoS 공격은 정보보호 및 관련 보안 기술 연구의 중요성을 보여주기에 충분했다. 또한 향후 DDoS 공격은 일반 PC 뿐만 아니라 스마트폰 및 기타 임베디드 시스템을 통해서도 가능할 것이라고 전문가들은 예상하고 있다. 이에 따라 스마트 코리아를 실현하기 위한 스마트 워크 기술이 현실화되어 가는 현 시점에서 다른 ICT 시스템 보안에 대한 관심은 증대되고 있는 반면, 일상적으로 널리 사용되고 있는 프린터나 디지털 복합기의 보안에 대해서는 아직까지 관심이나 투자가 부족한 실정이다. 물론 지난 2007년 IT 보안인증사무국에서는 디지털 복합기를 정보보호가 필요한 정보보호 시스템으로 분류하고, 보안적합성 검증 대상 제품에 포함시켰으며, HDD에 대한 완전삭제 기술을 의무화하고 있다. 또한 정보보호제품에 대한 CC 평가·인증을 통해 제품에 대한 신뢰성을 확보하고 있다[15].

하지만, 디지털 복합기나 프린터는 운영 환경에 따라 요구되는 보안 요구사항 역시 달라진다. 프린터는 일반적으로 다수의 사용자가 함께 공유하거나 비교적 접근하기 쉬운 공간에 설치되어 있는 경우가 대부분이다. 물론 공공기관 및 기업 내의 프린터나 디지털 복합기는 정보 시스템 관리자의 통제 하에 안전하게 관리되고 있을 수 있지만, 일반적으로 사용하는 디지털 복합기나 프린터는 보안 기능이 적용되어 있지 않으므로 프린팅한 정보가 쉽게 유출될 수 있다. 따라서 가까운 시기에 스마트워크가 활성화되면, 원격 근무지나 공공장소에서의 프린팅에 의한 기밀 정보 및 개인정보 유출 사건가 빈번히 발생할 수 있다. 이에 본 논문에서는 프린팅 서비스 현황과 관련 보안 기술 현황 및 표준화 동향을 살펴보았다. 마지막으로 본 논문을 통해 향후 국내에서도 디지털 복합기와 프린터에 대한 보안 기술 연구가 보다 활성화되는 계기가 되기를 기대해 본다.

## 참고문헌


[1] 문승일, "저탄소 녹색성장과 스마트 그리드", ), (정보통신표준화소식) TTA Journal, 통권 제129호 (2010년 5/6월), pp.51-55

[2] 행정안전부 스마트워크센터, http://www.smartwork.go.kr

[3] HP ePrintCenter, http//www.hp.com/go/ePrintCenter

[4] 신도리코, http://www.sindoh.com

[5] Apple, "Apple's AirPrint Wireless Printing for iPad, iPhone & iPod touch Coming to Users in November", http://www.apple.com/pr/library/2010/09/15airprint.html

[6] Google Cloud Print (Labs), http://code.google.com /intl/ko-KR/apis/cloudprint/docs/overview.html

[7] Digital Living Network Alliance, http://www.dlna.org

[8] IEEE P2600 Working Group, http://grouper.ieee.org /groups/2600/

[9] IEEE Std. 2600TM-2008, "IEEE Standard for Information Technology: Hardcopy Device and System Security", June, 2008.

[10] Printer Working Group, http://www.pwg.org

[11] Wi-Fi Alliance, http://www.wi-fi.org

[12] Bluetooth Special Interest Group (SIG), Bluetooth Core Specification Version 3.0 + HS, http://www.bluetooth.com

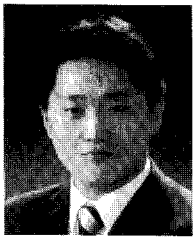
[13] Trusted Computing Group™, http://www.trustedcomputinggroup.org

[14] 이광우, 김승주, 원동호, "스마트미터의 신뢰성 및 안전성 향상을 위한 TPM 관련 평가인증 제도 분석", 한국정보보호학회 학회지 제20권 5호, pp.48-55, 2010.10.

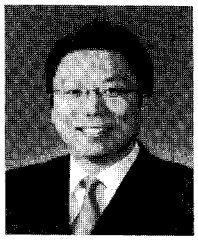
[15] 국가사이버안전센터, IT보안인증사무국, http://service1.nis.go.kr

[16] 이광우, 김승주, "기업 비밀정보 유출 방지 및 보호 관점에서의 디지털 복합기 보안 기술 동향 분석", 한국정보보호학회 학회지 제20권 1호, pp.47-55, 2010.02

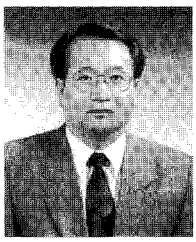
## 〈著者紹介〉

**이 광 우 (Kwangwoo Lee)**
종신회원
2005년 성균관대학교 정보통신공학부 졸업(학사)
2007년 성균관대학교 대학원 컴퓨터공학과 졸업(공학석사)
2009년 성균관대학교 대학원 전자전기컴퓨터공학과 박사수료
관심분야 : 암호이론, 정보보호제품 보안성 평가, 전자투표, 디지털 복합기 보안



**김 승 주 (Seungjoo Kim)**
종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: KISA(舊 한국정보보호진흥원) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 정보보호대학원 부교수
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재: 한국정보보호학회 이사
2005년~현재: 교육인적자원부 유해정보차단 자문위원
2007년~현재: 대검찰청 디지털수사 자문위원
2007년~2009년: 전자정부 서비스 보안위원회 사이버 침해사고대응 실무위원회 위원
2008년: 한국은행 금융정보화추진 분과위원회 자문위원
2010년~현재: 방송통신위원회 정보통신망침해사고민관합동조사단 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET



**원 동 호 (Dongho Won)**
종신회원
1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1992년~1994년 성균관대학교 전자계산소 소장
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 대검찰청 컴퓨터범죄 수사 자문위원
2002년~2004년 성균관대학교 연구처장
2002년~2003년 감사원 IT 감사 자문위원
2002년~2004년 산학연 정보보안협의회 회장
2005년~현재 : 정보보호인증기술연구소 소장
2005년~2008년 한국정보보호진흥원 이사
2009년~현재 : 성균관대학교 BK21 사업단장
관심분야 : 암호이론, 정보이론, 정보보호