정 보 보 호 학 회 지
제25권 제3호, 2015. 6

정보보호를 위한 3D프린터 위험관리 및 평가기법 제안

신 수 민*, 이 창 준**, 박 준 용***

요 약

제조 분야의 미래유망기술로써 각광받고 있는 3D프린터 기술은 다양한 방식으로 활용되고 있다. 시제품의 제작비용과 시간을 절감시키고 1인 맞춤형 제품 생산이 가능하게 하였으며, 의료 및 산업분야 전반에 걸쳐 그 시장과 규모는 나날이 증대되고 있다. 하지만 이에 반하여 환경오염, 무기제작, 지적재산권, 의료 윤리 및 규제, 국가 보안 위험 등과 같은 문제점 또한 적지 않게 제기되고 있다. 본 고에서는 정보보호 관점에서 네트워크와 연결된 3D프린터가 가진 잠재적인 취약점에 대해 알아보고, 조직에서 이를 예방하기 위한 관리적 방법에 대해 NIST IR 8023의 생명주기에 기반 한 단계별 위험관리 및 위험평가에 대한 가이드를 제공하고자 한다.

Ⅰ. 서 론

산업용 스캐너, 의료용 스캐너, 비디오 게임 등의 3차원 설계 데이터를 기반으로 실물 모형, 프로토타입, 툴 및 부품 등 3차원 물건을 제작하고 반복적 생산이 가능한 3D프린터는 1980년대 초반 미국 3D Systems사에 의해 플라스틱 액체를 굳혀 물건을 만드는 프린터를 개발하기 시작하여 2009년 영국의 아드리안 보어에 의해 시작된 RepRap(replicating rapid prototype)이라는 오픈 소스 프로젝트에서 3D프린터 기술에 대한 설계 및 사용방법을 공개하였고 3D프린터와 관련된 특허가 만료됨에 따라 다양한 프린터가 상용화되고 활성화되는 계기가 되었다[1].

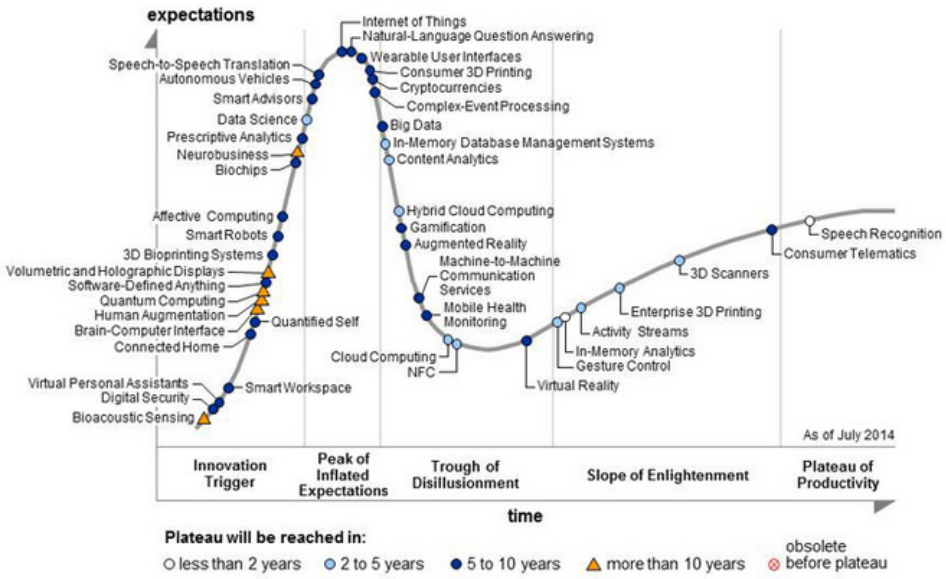
가트너(Gartner)는 심포지엄/ITxpo 2014에서 Computer Everywhere, The Internet of Things, 3D Printing을 2015년 가장 중요한 세 가지 전략적 기술 동향이 될 것으로 예상하였으며, [그림 1]의 'Hyper Cycle 2014 for Emerging Technologies'에서는 3D프린터를 미래유망기술로 명시하고, 이를 산업용(Enterprise 3D printing)과 의료용(3D Bio-printing) 그리고 가정용(Consumer 3D Printing) 기술로 나누어 기술성숙도 및 시장에서의 기대감을 예측하고 있다[2].

이와 같이 산업, 의료, 개인 활동과 관련된 분야에서 3D프린터는 전반적으로 엄청난 영향을 불러일으켰고 다양한 사례를 통해 이를 활용하고 있다. 포드(Ford)와 GE(General Electronic)에서는 3D프린터를 활용해 부품들을 기존과 대비하여 30% 절감된 비용으로 생산했고[3], 미시간(Michigan) 대학에서는 3D 프린트 된 부목을 이식해서 18개월 된 개럿 피터슨(Gerrett Peterson)이라는 아이의 기도를 확보하여 생명을 구했으며[4], B.T. Wittbrodt는 렙렙(RepRep)과 같은 저가 3D프린터의 사용은 일반 가정에서 경제적인 이득과 생

〔표 1〕 3D 프린팅 응용 및 활용 분야별 분류

구 분		응용사례
산업용	자동차	대시보드, 바디패널 등의 시제품
	패션	신발, 의류 등의 시제품
	건축	축소 모형 제작
	로봇산업	본체 및 부품 제작
	우주항공	부품 및 모형제작
	문화/예술	유물 복원
	식품	식자재, 건강 기능성 제품 등
의료용		인공 치아 / 뼈 / 관절 등 보형물 등
가정용(개인용)		장난감, 개인 맞춤형 액세서리 등

* 동국대학교 국제정보대학원 정보보호학과 (2014125538@dongguk.edu)
** 동국대학교 국제정보대학원 정보보호학과 (cjun3@daum.net)
*** 동국대학교 일반대학원 정보통신공학과 (park1jun@naver.com)



〔그림 1〕 Hype Cycle for Emerging Technologies, 2014

산성 향상을 달성할 수 있다고 주장했다[5].

하지만 이러한 3D프린터 기술이 급속하게 발전하고 확장됨에 따라 환경오염, 무기제작, 지적재산권, 의료 윤리 및 규제, 국가 보안 위험 등의 그에 대한 문제점 역시 제기되고 있다. 2013년 디펜드 디스트리뷰티드는 3D프린터로 제작한 총기인 '리버레이터'를 공개하고 발사에 성공하면서 우려를 일으켰으며[6], Stephanie M Santoso와 Erica L. Neely는 3D프린터 기술에 따른 지적재산권 이슈에 대한 문제를 제기하였다[7,8]. 또한 NIST에서는 프린터 및 스캐너 등과 같은 복제 장치의 기술적 취약점에 대해 명시하고 이에 대한 위험을 관리하기 위한 방안에 대해 제시하였다[9].

본 고에서는 위와 같은 3D프린터의 문제점 중 복제 장치가 가지고 있는 보안 취약점에 따른 위험을 관리하기 위한 관리적 부분에 대해 NIST IR 8023[9]에 기준하여 서술한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 3D 프린터 위험에 대한 개요를 설명하고 3장에서 시스템 개발 라이프 사이클(SDLC : System Development Life-Cycle)에 준한 위험관리 단계별 가이드를 소개하며, 4장에서는 실제 3D프린터를 사용하고 있는 기업을 대상으로 위험관리 및 평가기법에 따른 평가를 실시한다. 마지막으로 5장에서는 3D프린터를 통한 조직의 정보보호 방향을 제시한다.

Ⅱ. 3D프린터 위험 개요

2.1. 3D프린터 주요 기술 및 특징

제조업의 혁신이자 신 성장 산업엔진인 3D 프린팅은 플라스틱 액체와 같은 원료를 사출해 3차원 모양의 고체 물질을 자유롭게 찍어내는 기술이다. 전통적인 생산 방식은 입체의 재료를 기계가공 및 레이저를 이용하여 자르거나 깎는 절삭가공(Subtractive Manufacturing)의 형태로 제품을 제작하였으나, 3D프린터는 이와 반대되는 개념으로 물체 정보를 3D 그래픽 설계 프로그램을 통해 만들어낸 후 3D프린터를 통해 가루, 액체나 실(絲) 형태의 원료를 사용 하여 사출하고자 하는 형상대로 얇은 층을 무수히 반복해서 쌓아 만드는 적층 가공(Additive Manufacturing)기술을 사용한다[4].

3D프린터는 적층 방식과 제작 재료에 따라 다양한 기술로 분류할 수 있는데 적층 방식은 압출, 분사, 광경화, 파우더 소결, 인발, 시트 접합 등으로 구분되며 제작 재료는 폴리머, 금속, 종이, 목재, 식재료 등 다양한 소재를 사용할 수 있다[4].

적층방식과 재료에 따른 3D 프린팅 주요 기술 방식은 아래[표 2]와 같다.

〔표 2〕 3D 프린팅 주요 기술 방식

분류	기술명	특 징
Extrusion	FDM[1]	필름형태로 출력하는 방식
Jetting	MJM[2]	광경화성 수지와 WAX를 동시 분사 후, UV Light로 공형화하는 방식으로 적층
	Polyjet	광경화와 잉크젯 방식의 혼합
	3DP[3]	분말원료에 분사하는 방식
Light Polymerised	SLA[4]	레이저를 투사하여 경화시키는 방식으로 적층
	DLP[5]	빛을 DLP에 투사하여 적층
Granular Sintering	SLS[6]	파우더에 선택적으로 레이저를 조사·소결, 파우더를 도포하는 공정을 반복하여 적층
	SLM[7]	파우더에 금속 레이저를 조사하여 용융시키는 방식으로 적층
	EBM[8]	금속 파우더를 용해하는 방식
Directed Energy Deposition	DMD[9]	레이저 빔을 조사하여 일시적으로 용융풀을 생성, 여기에 금속 분말을 공급하여 클래딩 층을 형성(DMT로도 알려짐)
Wire	EBF³[10]	금속원료에 전자빔을 조사시켜 경화시키는 방식으로 적층
Sheet Lamination	LOM[11]	모델의 단면 형상대로 절단된 층을 접착제로 접합하여 조형

2.2. 3D프린터 위협 및 취약점

2.2.1 일반적인 위협 및 취약점

NIST IR 8023의 Replication Devices 위험관리를 참고하여 3D프린터의 위협 및 취약점에 대해 정리한 내용은 아래와 같다[9].

- Denial of service(DoS) : 인터넷과 연결된 3D프린터는 침해 위험에 노출되어 있어 사용 시 문제가 발생할 수 있음.
- Spam : 인증을 거치지 않은 불필요한 작동으로 인해 소모품이 낭비됨.
- Default admin / configure : 초기 패스워드나 설정 등을 변경하지 않고 사용하여 원격지의 불특정 인원에 의해 권한이 탈취되어 3D프린터가 오작동 될 수 있음.
- Data capture : 3D프린터에서 암호화 하지 않고 전송하거나 저장된 데이터가 탈취 될 수 있음.
- Alteration / Corruption of data : 데이터가 침해 발생으로 변조되거나 손상, 이 같은 문제는 발견하기 힘들고 3D프린터 성능을 저하시킴.
- Outdated or Unpatched : 3D프린터에 내장된 운영체제가 공개된 취약점에 대한 업데이트의 최신 패치가 이루어지지 않았을 경우 연결된 네트워크를 통해 다양한 침해 위험이 나타날 수 있음.

2.2.2 네트워크 연결 위협 및 취약점

네트워크를 통해 연결된 3D프린터는 개별적으로 연결된 경우에 비해 편의성(Convenience)과 비용절감 효과(Cost-Effect)를 가져오지만 개별적으로 연결된 프린터보다 더 많은 위험과 취약성에 노출되는 문제점을 가지고 있다.

- Unencrypted Information : 암호화 되어 있지 않은 정보는 유출되거나 비인가 접근, 데이터 무결성 확보에 문제가 발생함.
- Open ports / protocols : 개방된 포트와 프로토콜은 공격자로부터 3D프린터로의 접근을 허용하며, 비인가 접근에 대한 탐지(데이터 이동, 삭제, 사용기록, 사용기록 삭제)를 어렵게 함.
- Denial of service (DoS) : 인터넷에 연결된 3D프린터는 장치를 일시적으로 사용할 수 없게 되는 결과의 위협으로부터 더욱 취약해질 수 있음.
- Wireless connectivity : 블루투스나 IEEE 802.11을 사용하여 다른 장치들과 인터넷 통신을 할 때 송·수신 데이터가 암호화되지 않은 경우, 데이터 유출로 인한 위험발생 가능성이 높음.
- Access permissions : 비인가자가 접근 권한을 획득할 경우, 인터넷에 연결된 3D프린터 접속을 통한 악성코드를 임의로 설치하고 통제 권한을 악용

1) Fused Deposition Modeling
2) Multi Jetting Modeling
3) 3 Dimensional Printing
4) Stereo Lithography Apparatus
5) Digital Light Processing
6) Selective Laser Sintering
7) Selective Laser Melting
8) Electron Beam Melting
9) Direct Metal Deposition
10) Election Beam FreeForm Fabrication
11) Laminated Object Manufacturing

하여 잠재적인 위험 상황을 야기할 수 있음.

- Botnets : 3D프린터의 메모리 및 처리 전력은 같은 네트워크상의 조직 자산 또는 외부 조직의 자산을 공격하기 위한 DoS 봇넷의 일부로 사용될 수 있음.
- Hop/Relay Points : 손상된 3D프린터는 같은 네트워크상의 다른 조직 자산에 접근하기 위해 사용되거나 외부 네트워크상의 공격의 실제 기점을 은폐하기 위해 사용될 수 있음.

2.2.3 비휘발성 저장매체 위협 및 취약점

3D프린터는 장치 제어 및 작업 관리를 위해 비휘발성 저장매체를 활용한다. 즉, 저장, 처리 및 전송되는 모든 정보는 비휘발성 저장매체에 기록된다. 따라서 메모리에 저장된 개발 단계의 정보(기업, 정부, 군사)가 방치될 경우 잠재적으로 자료의 조작/변조 등이 발생하여 제품 개발에 영향을 주거나 다양한 침해 사고가 발생할 수 있다.

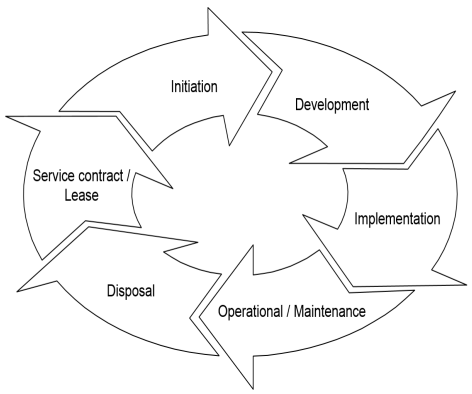
- Unencrypted information : 암호화 되지 않은 상태로 내장 메모리에 저장되어 있는 정보는 누구에게나 노출되어 유출 되거나 변조될 위험함.
- Sanitization : 방치되거나 버려진 내장 메모리에 저장된 정보는 비인가 사용자를 통한 유출됨.
- Access : 외부 유지보수 인력 또는 복제 장치에 원격 또는 물리적 접근 권한이 있는 다른 사람은 저장된 정보를 복사 또는 다운로드 할 수 있음.
- Unauthorized Access : 3D프린터 유지보수를 위해 사용자가 아닌 3자가 직접 또는 원격 접속을 통해 내장 메모리에 저장된 정보를 탈취됨.

Ⅲ. 3D프린터 위험 관리 및 평가기법

3D프린터의 취약점을 통해 조직정보에 위험이 발생하였을 때 조직에 주는 피해 수준과 감내 수준 등에 대한 고려는 정보보호에 있어서 매우 중요하다. 따라서 3D프린터 도입 시부터 개발, 구현, 운영/유지보수, 처분, 서비스 계약 및 임대까지의 시스템개발 라이프 사이클[12] 각각의 단계에서 정보보호에 대한 사항이 고려되어야 하며, 이를 전반적으로 통제하기 위한 위험 관리가 요구된다[10].

3.1 SDLC를 통한 3D프린터 위험 관리

3D프린터에 RISK 관리에 대해 SDLC를 적용하기 위하여 아래 [그림 1]은 (1)도입(Initiation), (2)개발(Development), (3)구현(Implementation), (4) 운영/유지보수(Operation/Maintenance), (5)처분(Disposal), (6) 서비스계약 및 임대(Service Contract / Lease Agreements) 생명주기를 도식하였다.



〔그림 2〕 SDLC를 통한 3D프린터 RISK관리

3.1.1 도입(Initiation)

도입 단계에서는 어떻게 사용할 것인가를 결정해야 한다. 도입 결정 시 고려할 사항은 아래와 같다.

- 누가, 어디에서 사용 하는가?
- 네트워크에 연결할 것인가?
- 3D프린터를 통해 정보를 처리, 저장, 전송 할 때 정보 등급 수준(낮음, 중간, 높음)은?
- 필요한 기능은 무엇인가?
- 구매할 것인가, 임대할 것인가?
- 3D프린터의 기밀성, 무결성, 가용성 및 정보의 저장, 처리, 전송 보호를 위해 무엇을 할 것인가?
- 장치가 작동하는데 있어 적절한 영향 수준에서 보안 요구에 대해 지원하고 제공하는가?
- 3D프린터를 위해 조직이 원하거나 필요한 계약은?
- 장비 설치, 설정, 관리 및 유지 보수하는데 필요한 기술은 무엇이며, 직무 교육은 필요한가?

12) SDLC(Systems Development Life Cycle) : 시스템개발 라이프 사이클

3.1.2 개발(Development)

개발 단계에서는 3D프린터 도입 단계에서 언급된 사항들에 대해 가용한 보안 옵션을 고려하는 단계이다. 보안옵션에 포함되어야 하는 고려사항은 다음과 같다.

- 편집 가능한 설정
- 제조업체가 제공한 보안 설정
- 완전 삭제 기능
- 비휘발성 저장매체의 물리적 보호
- 내구연한을 고려한 유지보수 지원
- 저장, 전송 간 암호화 기능
- 경고/시작 모니터링 활동
- 감사 기록(로깅) 기능
- 인증 기능(패스워드/pin, 스마트카드 등)
- 접근 통제 수준/역할
- 네트워크/포트 설정 기능
- 위조 증거 솔루션
- 안전한 자동 종료

3.1.3 구현(Implementation)

구현 단계는 3D프린터를 운영하기 전 단계로 장비를 보호할 수 있는 안전한 장소에 설치하고 보안옵션을 보안계획에 따라 적절하게 설정하는 단계이다.[1]

- 제조업자가 요구한 보안의 적절한 구성 적용과 검토
  - 장치를 보정하고 구성하는 필요에 따라 장비 제조업체 (OEM)와 적극적으로 의사소통
  - 장치가 측정되고 안전하게 구성될 때까지 다른 시스템으로부터 장치를 격리
  - 장치에서 원하지 않는 응용 프로그램을 제거
  - 복제 장치를 이용가능토록 표준화된 보안 구성을 적용
- 사용 및 암호화 구성
  - 네트워크 암호화 프로토콜의 사용(예를 들어, TLS/SSL, IPSec, WPA2)
  - 패스워드 암호화 및 다른 구성 설정
  - 비휘발성 저장매체에 대한 암호화를 구성
- 비휘발성 저장매체에 대해 사용자에게 알리기 위해 device에 경고 스티커를 붙인다. 경우에 따라 즉각 이미지 복구 방법에 대한 지시는 포함될 수 있음.
- 접속 제한
  - 사용자 계정 및 권한 검토
  - 관리자/권한 접근을 primary와 secondary 권한으로 제한한다
  - 환경 설정 변경이 가능한 사용자 및 서비스 벤더 기술자 제한
  - 원격 접속 제한
  - call-home 기능을 사용하지 않도록 설정, 제조업자에 의한 모니터링을 허용하지 않음
  - 무선 네트워크 식별자 전송 및 네트워크 자동 연결 설정해제
  - 제한이나 파일공유 불가
  - 사용하지 않는 네트워크 포트 사용하지 않기
  - 물리적 보안 실행
  - MAC 주소와 IP주소 범위, 이메일 주소를 화이트리스트 / 블랙리스트로 구분
- 식별과 인증 사용
  - 권한 있는 접속에 대한 식별과 인증 요구
  - 벤더사의 최초 설정 패스워드 변경
  - 사용자에 대한 인증된 검색 구현 push/pull printing
- 이미지 대체기능 구성
  - 즉각적인 이미지 덮어쓰기 사용
  - 최소 3단계로 overwrite 시간을 계획
- 감사 사용
- 모니터링/실패 에러 처리 기술
  - 재부팅 덤프 메모리
  - 관리자 에러 알림
  - 블럭 반복 요청
  - 큐나 저장작업에 대해 time-out 사용

3.1.4 운영/유지보수(Operation/Maintenance)

운영/유지보수 단계에서 발견된 취약점에 대한 업데이트와 패치가 이루어지지 않아 취약점에 노출되면 아래와 같은 침해 위험이 발생한다. 따라서 판매자의 안내에 따라 보안에 대한 설명과 정기적인 업데이트 및 패치가 필요하다.

- 디스플레이 오작동시 잘못된 정보가 표시됨
- 일반적인 경우보다 소모품의 소모가 빠름
- 작업이 실패하거나 시간을 초과하는 경우가 생김

- 의도 하지 않게 기기의 설정이 변경됨
- 작업 완료 시간이 예상보다 많이 소요됨
- 평소보다 많은 네트워크 대기시간 발생함
- 알 수 없는 IP로 통신되거나 이메일 통신이 증가함
- 장치의 핵심 영역 주위에 물리적 표시(예를 들면, 비휘발성 저장장치 영역, 표시 영역)

3.1.5 처분(Disposal)

제조사로부터 평가받은 장비의 내구연한이 자체 평가한 내구연한(Expected Life of 3D Printer)보다 정확하다. 재 구매 시 내구연한이 경과한 장비는 NIST SP 800-53의 가이드에 따라 처분한다.[10]

- 내부 저장매체의 저장 자료에 대한 완전한 삭제 후 파기 여부 확인
- 패스워드나 인증 정보에 대한 삭제나 변경 여부 확인
- 공장 초기 설정으로 초기화 여부 확인

3.1.6 서비스 계약 및 임대(Service Contract / Lease Agreements)

3D프린터 서비스 계약이나 임대 시 정보보호와 관해 합의한 내용의 준수 여부를 아래와 같이 고려해야 한다.

- 기기를 외부에서 수리해야 될 때에는 비휘발성 저장매체를 제거함
- 기술자들이 유지보수를 위해 3D프린터에 접속하기 전 비휘발성 저장매체를 정리
- 유지보수 기술자들이 비휘발성 저장매체에 저장된 조직의 정보(패스워드, 설정정보)를 삭제하도록 못하도록 해야 함.
- 유지보수 기술자에 의한 정보 삭제를 통제함

3.2 역할과 책임(Role & Responsibility)

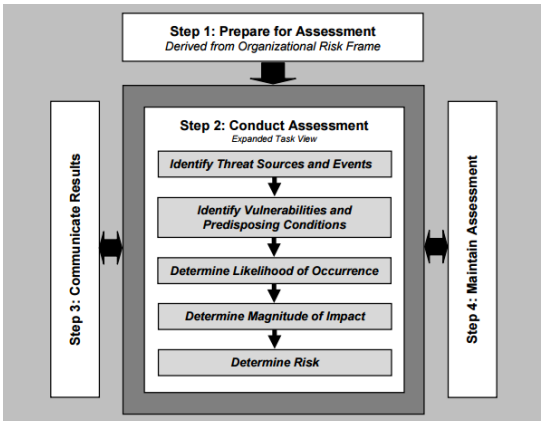
3D프린터에 대한 위험을 관리할 때 사용자에 대한 부분 또한 중요하게 인식된다. 이에 연관된 사용자들의 역할과 책임에 대해 정의하면 다음과 같다.

〔표 3〕 역할과 책임

역할	책임
권한 담당자	시스템을 운영할 책임을 공식적으로 맡은 권한을 가진 고위 관리 또는 경영진.
일반 통제 제공자	조직의 위험 관리 전략에 따라 일반 통제에 대한 사항을 보증하는 책임을 가진 자.
계약 담당자	계약을 관리, 체결하기 위한 권한을 가진 자.
정보 소유자	시스템 내 계획에 따른 이익과 사업을 대표하는 자.
정보시스템 소유자	시스템의 보안 통제가 채택되고 구현되며, 문서화 및 조직의 위험 관리 전략에 따라 운영되는지를 보증하는 책임을 가진 자.
정보시스템 보안 담당자	정보 시스템을 위한 적절한 운영 보안 정책을 유지하는 것을 보증하는 책임을 가진 자.
보안 통제 평가자	정보 시스템에 의해 상속되거나 채택된 보안 통제에 대한 평가를 실행할 책임을 가진 자.
정보시스템 관리자	IT 제품에 대한 보안 구성 설정을 통합하고 합의된 통제를 구현할 책임을 가진 자.

3.3 위험도 산정

3D프린터에 대한 위험도 측정은 위험에 대한 허용가능 수준 여부를 판단할 수 있는 기반을 마련함과 동시에 비용대비 효과적인 대응책을 강구하여 위험의 수준을 감소시키는데 그 목적이 있다. 3D프린터에 대한 위험도 산정은 NIST SP 800-30 Rev.1 “Guide for Conducting Risk Assessments”의 Step.2, Conduct Assessment 이론과 국내 보안 컨설팅업체의 위험평가를 접목한 개념을 적용한다[11][12].



〔그림 3〕 RISK ASSESSMENT PROCESS

3.3.1 자산 가치 분석에 따른 보안등급 산정

3D프린터는 그 용도와 활용에 따라 다양한 가치를 지니는 자산이나 본 고에서는 보안의 속성에 초점을 두어 정성적인 방법에 따라 기밀성, 무결성, 가용성 측면에서 자산 보안 등급(Asset Security Level)을 산정한다. 자산 보안 등급은 기밀성 값 + 무결성 값 + 가용성 값을 합하여 산정한다.

- 1등급(3점) : 자산 가치 평가 합계 7~9점
- 2등급(2점) : 자산 가치 평가 합계 5~6점
- 3등급(1점) : 자산 가치 평가 합계 3~4점

〔표 4〕 자산 보안 등급

구분		기밀성	무결성	가용성
자산 가치	상	3	3	3
	중	2	2	2
	하	1	1	1

3.3.2 위협 및 취약점 분석

3D프린터의 위협 및 취약점은 2.2절에서 명시한 위협 및 취약점을 참조하며, 이를 기반으로 한 3D프린터에 대한 전반적인 위협 및 취약점 목록을 도출해 보면 다음과 같다.

〔표 5〕 위협 및 취약점 기준

위협 및 취약점	영향		
	기밀성	무결성	가용성
Spam			○
Default admin / configure	○	○	○
Data capture	○		
Alteration / Corruption		○	○
Outdated or Unpatched	○		
Unencrypted Information	○		
Open ports / protocols	○		○
Denial of service (DoS)			○
Wireless connectivity	○		
Access permissions	○		
Botnets			○
Hop/Relay Points			○
Unencrypted information	○	○	
Sanitization	○	○	
Access	○		
Unauthorized Access	○		

3.3.3 위험요인 작성 및 평가

위험요인은 3D프린터를 대상으로 관리적·물리적·기술적 취약점 분석을 통해 “현황의 문제로부터 실제 발생할 수 있는 위협에 대한 실현 가능한 시나리오”를 항목별로 명시한 것으로 2.2절의 위협 및 취약점과 3장의 위험 관리 부분을 기반으로 작성한다.

위험 요인 점수(Risk Factor Value, RFV)는 위험요인 평가 중 실제로 3D프린터의 취약점을 이용하여 일어날 수 있는 위험의 정도를 나타낸 것으로 다음과 같이 0에서 5까지 총 6가지 점수로 분류한다.

〔표 6〕 위험 수준을 고려한 위험 요인 점수

점수	위험 정도	설명
0	Negligible Risk	무시해도 좋은 수준
1	Very Low Risk	매우 낮은 수준
2	Low Risk	낮은 수준
3	Moderate Risk	중간 수준
4	High Risk	높은 수준
5	Very High Risk	매우 높은 수준

3.3.4 기존 보호대책 평가

기존 보호대책은 위에서 제시한 3D프린터 위험요인에 대해 조직에서 적용하고 있거나 운영하고 있는 보호대책으로서 이를 통해 위험을 감소시킬 수 있다. 위험요인에 대한 기존 보호대책 평가는 적용, 일부적용, 미적용으로 분류하며 보호대책 적용 여부에 따라 기존 보호대책 값(Existing Protection Countermeasures, EPC)을 산정하여 추후 노출위험도에 적용한다.

〔표 7〕 보호대책에 따른 평가 기준

보호대책	설명	기존 보호대책 값 (EPC)
적용	위험 시나리오를 잘 막을 수 있는 수준, 보호대책 적용 양호	1
일부 적용	위험 시나리오를 일부 방지할 수 있는 수준, 보호대책 부분적 적용	0.5
미적용	보호대책이 적용되어 있지 않음	0

〔표 8〕 3D프린터에 대한 보안 위험요인 평가 테이블

분야		위험요인과 연관된 질문	위험요인 점수(RFV) Y / N	기존보호대책(EPC) Y / P / N	위험수용 여부 및 조치방안
기획/ 안전한 구성	1	적용가능한 통제가 구현된 시스템 보안 계획 내에 3D프린터가 존재하는가?	· Y = 0 · N = 4		
	2	3D프린터 또는 이를 제어하는 소프트웨어가 관련된 보안 인증을 획득하였는가?(예를 들어, CC 인증)	· Y = 0 · N = 1		
	3	공급 / 제조업체는 장치에 대한 보안 구성에 대한 정보를 제공하는가?	· Y = 0 · N = 1		
	3.1	안전한 구성을 사용할 경우, 이 구성이 3D프린터에서 구현이 되는가?	· Y = 0 · N = 2		
제 3자	4	임대된 3D프린터인가? (구매하여 소유할 경우 N/A)	· Y = 3 · N = 0		
	4.1	임대했을 경우, 임대계약 상에 3D프린터 내부의 저장장치에 대한 소유권에 대해 규정하고 있는가?	· Y = 0 · N = 4		
	5	3D프린터 서비스 계약은 되어 있는가?	· Y = 0 · N = 2		
	5.1	서비스 계약이 되어 있을 경우, 계약상 3D프린터가 조직의 통제를 벗어나기 전 HDD 및 SSD, 비휘발성 저장장치 제거에 대한 사항이 규정되어 있는가? (서비스 계약이 아닐 경우 N/A)	· Y = 0 · N = 5		
	5.2	서비스 계약이 되어 있을 경우, 계약상 서비스 기술자가 임의의 형태로 3D프린터 내에 저장된 정보를 삭제하지 못하도록 하는 사항이 규정되어 있는가? (서비스 계약이 아닐 경우 N/A)	· Y = 0 · N = 2		
	5.3	서비스 계약이 되어 있을 경우, 계약상 오직 OEM 또는 승인된 OEM 부품만 사용되어야 하는 사항이 규정되어 있는가? (서비스 계약이 아닐 경우 N/A)	· Y = 0 · N = 3		
	6	서비스 계약이 아닐 경우, 3D프린터의 저장 미디어가 조직의 통제를 떠나기 전에 위생처리/제거 등에 관한 정책과 절차를 준수하는가?	· Y = 0 · N = 5		
저장 장치	7	3D프린터는 HDD 또는 SSD/비휘발성 저장매체를 가지고 있는가?	· Y = 4 · N = 0		
	7.1	3D프린터 저장 미디어는 손쉽게 물리적으로 접근이 가능한가?(분해하지 않거나 도구가 요구되는지)	· Y = 2 · N = 0		
	7.2	저장된 정보는 논리적으로 접근하거나 볼 수 있는가? (장치 콘솔 또는 웹 접속이 가능한가)	· Y = 2 · N = 0		
	7.3	3D프린터의 암호화된 저장 미디어가 승인된 암호 표준을 준수하는가? (FIPS 140 또는 CC)	· Y = 0 · N = 4		
	8	3D프린터의 암호화된 장치 구성 설정이 승인된 암호 표준을 준수하는가? (FIPS 140 또는 CC)	· Y = 0 · N = 2		
	9	3D프린터가 완전 삭제 기능을 제공하는가?	· Y = 0 · N = 5		
	9.1	가능한 경우, 완전 삭제 기능을 사용할 수 있는가? (가능하지 않을 경우 N/A)	· Y = 0 · N = 4		
	9.2	가능한 경우, 즉시 데이터 덮어 쓰기 기능을 사용할 수 있는가? (가능하지 않을 경우 N/A)	· Y = 0 · N = 3		
	10	3D프린터 재부팅 시 복제된 문서 / 이미지 / 객체의 메모리를 덤프하는가?	· Y = 0 · N = 2		

분야		위험요인과 연관된 질문	위험요인 점수(RFV) Y / N	기존보호대책(EPC) Y / P / N	위험수용 여부 및 조치방안
네트워크	11	3D프린터가 네트워크와 연결되어 있는가?	· Yes = 4 · No = 0		
	11.1	조직이 승인한 네트워크 프로토콜을 사용하여 암호화된 네트워크 통신을 하는가? (IPSec, SSL/TLS, WPA2 등)?	· Yes = 0 · No = 5		
	11.2	조직으로부터 승인된 표준(FIPS 140이나 CC기준)을 사용한 암호화된 네트워크 상의 권한있는 접속이 이뤄지는가?	· Yes = 0 · No = 2		
	11.3	3D프린터가 알 수 없거나 원하지 않는 주소로 통신되는 것을 예방하는가?(whitelist/blacklist)	· Yes = 0 · No = 2		
	11.4	3D프린터가 알 수 없거나 원하지 않는 주소로부터 통신되는 것을 예방하는가?	· Yes = 0 · No = 4		
	11.5	3D프린터가 방화벽에 의해 보호되는가?	· Yes = 0 · No = 2		
	11.6	3D프린터가 원격 설정을 허용하는가?	· Yes = 4 · No = 0		
	11.7	3D프린터가 재택에서 접속하는 것을 허용하는가?	· Yes = 2 · No = 0		
	11.8	3D프린터가 원격 모니터링을 허용하는가?	· Yes = 3 · No = 0		
	12	3D프린터가 무선(Bluetooth, IEEE 802.11 등)을 통해 접속되는가?	· Yes = 4 · No = 0		
	12.1	무선 식별자 브로드캐스팅 설정이 Disabled 되어 있는가?	· Yes = 0 · No = 4		
	13	3D프린터가 유지보수(업데이트, 장애처리 등)을 위한 기술자의 외부 접속을 허용하는가?	· Yes = 2 · No = 0		
	13.1	3D프린터 또는 벤더사가 외부접속을 요청하는가?	· Yes = 4 · No = 0		
	14	3D프린터의 사용하지 않거나 열려있는 포트가 있는가?	· Yes = 5 · No = 0		
소프트웨어/펌웨어	15	3D프린터 소프트웨어/펌웨어가 패치 또는 업데이트가 되었는가?	· Yes = 0 · No = 4		
	15.1	제조사의 기술자에 의해서만 패치가 진행되는가?	· Yes = 2 · No = 0		
	16	3D프린터 서버에 대한 구성설정이 안전하게 진행 되는가?(3D프린터 서버가 없을 경우 N/A)	· Yes = 0 · No = 3		
	16.1	3D프린터 서버가 패치 및 업데이트 되었는가? (3D프린터 서버가 없을 경우 N/A)	· Yes = 0 · No = 4		
	16.2	제조사의 기술자에 의해서만 3D프린터 서버가 패치되는가?(3D프린터 서버가 없을 경우 N/A)	· Yes = 2 · No = 0		
	17	소프트웨어와 펌웨어를 최신상태로 유지하기 위한 조직의 패치 관리 프로그램을 3D프린터가 포함하고 있는가?	· Yes = 0 · No = 5		
	18	주기적으로 3D프린터에 대한 취약점 진단을 실시하고 있는가?	· Yes = 0 · No = 4		

분야		위협요인과 연관된 질문	위협요인 점수(RFV) Y / N	기존보호대책(EPC) Y / P / N	위험수용 여부 및 조치방안
물리 보안	19	3D프린터에 대한 물리적 접근을 통제할 수 있는가?	· Yes = 0 · No = 2		
	20	3D프린터 내부 저장매체에 대한 물리적 접근을 통제 할 수 있는가?(자물쇠 등을 사용)	· Yes = 0 · No = 2		
	21	3D프린터 내의 소모품(가공 재료 등)은 안전한가?	· Yes = 0 · No = 1		
	22	3D프린터가 민감하거나 잠재적으로 위험한 물질 또는 부품 등을 사용하고 있는가?	· Yes = 1 · No = 0		
	22.1	3D프린터 내에 민감하거나 잠재적으로 위험한 물질 또는 부품들은 안전하게 보호되고 있는가?	· Yes = 0 · No = 3		
접근 통제	23	3D프린터의 저장장치에 논리적 접근이 통제되는가?	· Yes = 0 · No = 2		
	24	3D프린터 설정(구성)에 대한 접근이 통제되는가?	· Yes = 0 · No = 2		
	25	모든 벤더사가 제공하는 Default Password가 변경되어 있는가?	· Yes = 0 · No = 4		
	26	가능할 경우, 지정되고 훈련된 직원에 한해 3D프린터에 대한 권한 있는 접근(물리적/논리적)이 이뤄지는가?	· Yes = 0 · No = 3		
	27	작업 완료를 위해 개인 사용자 검증을 요구하는가?	· Yes = 0 · No = 1		
	28	조직의 정책에 따라 3D프린터가 계정 관리 및 인증에 대한 통제를 기능적으로 제공하는가? (패스워드 길이, 패스워드 변경, 로그아웃 절차 등)	· Yes = 0 · No = 2		
	29	3D프린터가 도메인 자격증명을 통해 인증과 식별을 허용하는가?	· Yes = 0 · No = 1		
	30	일정 시간이 경과되면 사용자 로그아웃이 자동적으로 이루어지는가?	· Yes = 0 · No = 2		
모니터링	31	3D프린터 사용에 대해 모니터링이 되는가?	· Yes = 0 · No = 3		
	32	3D프린터는 관리자의 실수 또는 잠재적인 사고에 대해 알려주는가?	· Yes = 0 · No = 2		
	33	3D프린터에서 감사/로깅이 가능하고 활성화되어 있는가?	· Yes = 0 · No = 3		
	34	3D프린터에서 자동적으로 감지하고 DoS 공격을 예방할 수 있는가?	· Yes = 0 · No = 1		
	35	3D프린터가 대기 작업에 대한 시간 제한을 적용하는가?	· Yes = 0 · No = 2		
	36	3D프린터에 대한 온도를 모니터링 하고 과열 시 자동적으로 종료하는 통제가 이뤄지는가?	· Yes = 0 · No = 2		
총 위협요인 점수 :					

3.3.5 노출위험 평가 및 위험등급 산정

노출위험은 위험요인 평가 중 실제로 3D프린터의 취약점을 이용하여 일어날 수 있는 위험의 정도를 나타낸 것으로 3.3.3항 및 3.3.4항에서 언급한 위험요인 점수와 기존 보호대책을 기반으로 산출하며 아래와 같은 공식을 적용할 수 있다. 노출위험도 산정 시 위협 및 취약점에 대한 부분을 별도 구분하지 않고 하나로 간주하였으며, 이에 따라 공식에서 ×2를 적용하였다.

노출위험도(ERV) = (RFV-(RFV×EPC))×2

〔표 9〕 위험요인별 노출위험도(ERV)

구분		위험 요인 점수(RFV)					
		0	1	2	3	4	5
기존보호대책값(EPC)	적용(1)	0	0	0	0	0	0
	일부 적용(0.5)	0	1	2	3	4	5
	미적용(0)	0	2	4	6	8	10

위 공식을 통해 [표 8]과 같은 개별적인 노출위험도(ERV)가 산출되며, 이를 합산하여 총 노출위험도(Total Exposed Risk Value)를 계산한다.

$$\text{총 노출위험도(TERV)} = \sum_{n=1}^{k} ERV$$

위험등급(Risk Level, RL) 산정은 총 노출위험도(TERV) 점수에 따라 6단계로 분류한다.

〔표 10〕 총 노출위험도에 따른 위험등급 산정

위험등급(RL)	총 노출위험도(TERV)	비고
1	0 ~ 50	무시해도 좋은 수준
2	50 ~ 100	매우 낮은 수준
3	100 ~ 150	낮은 수준
4	150 ~ 200	중간 수준
5	200 ~ 250	높은 수준
6	250 이상	매우 높은 수준

3.3.6 위험 산정

3D프린터에 대한 위험은 자산 보안등급에 위험등급을 더하여 다음과 같이 계산할 수 있다.

위험(RISK) = ASL + RL

〔표 11〕 위험 산정 기준표

구분			위험등급					
			1	2	3	4	5	6
자산 보안 등급 (ASL)	상	3	4	5	6	7	8	9
	중	2	3	4	5	6	7	8
	하	1	2	3	4	5	6	7

- 높은 위험 : 위험 산정 점수 7~9점
- 보통 위험 : 위험 산정 점수 4~6점
- 낮은 위험 : 위험 산정 점수 2~3점

Ⅳ. 3D프린터 Risk 평가 결과

4.1 평가방법

위에서 언급된 위험도 산정 방법을 기초로 모 기업에서 실제 운용 중인 서로 다른 모델의 3가지의 3D프린터에 대한 위험평가를 진행하였다. 평가 방법은 3D프린터 엔지니어와 1:1 인터뷰 및 실제 구동환경 실사를 통해 자산 보안 등급 및 3D프린터 위험 요인 평가, 기존 보호대책 평가를 실시하고 이를 기반으로 노출위험도를 산출하였다. 평가에 사용된 제품의 사양은 [표13]과 같다.

〔표 12〕 3D프린터에 대한 위험평가 결과

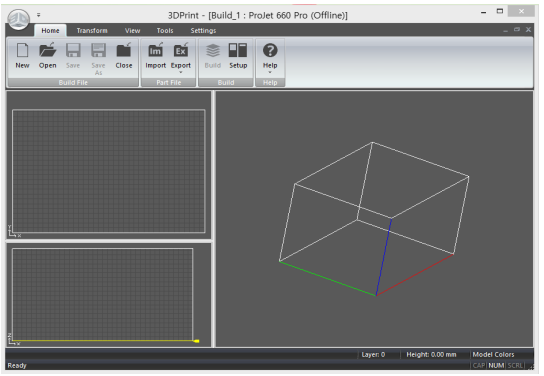
구분		A제품	B제품	C제품
위험		4 (보통 위험)	7 (높은 위험)	7 (높은 위험)
자산 보안 등급(ASL)		2	3	3
위험등급(RL)		2	4	4
노출 위험도 (ERV)	총 노출위험도	94	188	182
	구성	4	6	2
	저장장치	38	42	38
	네트워크	0	78	90
	S/W 펌웨어	22	22	22
	물리보안	4	10	2
	접근통제	16	20	16
	모니터링	10	10	12

4.2 평가결과 분석

시험 평가 결과 각 제품의 점검항목에 따른 위험평가 결과는 [표12]와 같다.

기업 자체적으로 3D프린터를 구매하여 사용 중이므로 제 3자 임대에 의한 위협 및 취약점은 배제하였다. A제품의 경우 3D프린터가 네트워크 포트를 지원하나 실제 운영하는 조직에서 이를 활용하고 있지 않고 로컬에서 사용하였으며, B의 경우는 네트워크에 연결되어 있고 이를 통해 3D 프린팅 출력 작업을 함에 따른 잠재적인 취약점들이 식별되었다(개방된 포트 및 방화벽 미설정, 원격 접속 허용 등). C의 경우 B와 유사하나 별도의 공간에 격리되어 사용되고 있었음을 확인하였다.

전반적으로 3D프린터 장비 자체에 보안성을 위한 기능을 제공하고 있지는 않았으며, 주로 네트워크 및 소프트웨어 취약점이 존재하였다. 제공되는 소프트웨어는



〔그림 4〕 3D프린터 소프트웨어

3D 프린팅을 위한 기능들 위주로 메뉴가 설정되어 있었으며, 구동 환경 또한 Window 기반으로 제작되어 있어 운영체제 취약점에 따른 위험 역시 내재하고 있었음을 확인하였다. 벤더사가 제공하는 Default Password

〔표 13〕 위험평가 대상 3D프린터 사양

구분	A제품	B제품	C제품
조형 크기 (순 제작 용적)	43 x 27 x 150mm (1.69 x 1.06 x 5.90인치)	HD : 298 x 185 x 203mm HS : 298 x 185 x 203mm UHD : 298 x 185 x 203mm XHD : 298 x 185 x 203mm	254 x 381 x 203mm
기본 해상도	56μ(유효 해상도: 585dpi*)	HD : 375 x 375 x 790 DPI (xyz): 32μ HS : 375 x 375 x 790 DPI (xyz): 32μ UHD : 750 x 750 x 890 DPI (xyz): 29μ XHD : 750 x 750 x 1600 DPI(xyz), 16μ	600 x 540 dpi
적층 두께	0.03 mm (0.0012 in)	부품 치수 25.4mm당 0.025 ~ 0.05mm	0.004인치(0.1mm)
사용 재료	VisiJet® FTX Green 및 FTX Cast	VisiJet M3-X, VisiJet M3 Black, VisiJet M3 Crystal, VisiJet M3 Proplast,, VisiJet M3 Navy, VisiJet M3 Techplast, VisiJet M3 Procast Support Material : VisiJet S300	VisiJet PXL
태블릿/스마트폰 연결	-	예	예
Print3D 앱	-	태블릿, 컴퓨터 및 스마트폰으로 원격 모니터링 및 제어	태블릿, 컴퓨터 및 스마트폰으로 원격 모니터링 및 제어
네트워크 호환성	TCP/IP 100/10 base T		
입력 파일	STL	STL 및 SLC	STL, VRML, PLY, 3DS, FBX, ZPR
전력요건	100-240VAC, 50/60Hz, 2.0A	100 - 127VAC, 50/60Hz, 단상, 15A; 200 - 240*VAC, 50Hz, 단상, 10A	100~240V, 15~7.5A
지원 OS	Windows-Based OS	Windows XP Professional, Windows Vista, Windows 7	Windows® 7 및 Vista®
작동 온도	-	18-28ºC(64-82ºF)	13 ~ 24°C

또한 별도 수정이 불가하게 되어있으며, 저장장치에 대한 물리보안 및 통신 간 암호화에 대한 보완이 요구되는 실정이다.

Ⅳ. 결 론

본 고에서는 지금까지 3D프린터가 가진 잠재적인 취약점에 대해 알아보고, 조직에서 이를 예방하기 위한 관리적 방법에 대해 NIST IR 8023의 생명주기에 기반 한 단계별 위험관리 및 평가에 대해 연구하였으며, 모 기업에서 실제 사용 중인 3D프린터에 대한 위험 평가를 실시함으로써 위험관리에 대한 실태를 확인하였다. 3D프린터 기술은 제조 분야에서 혁신을 유발하였음은 물론 3차 산업혁명의 주역으로 향후 의료, 산업, 서비스 등 다양한 목적으로 기업에서 활용되어질 것이다. 하지만 3D프린터가 가진 취약점은 조직 정보의 무결성, 신뢰성, 유용성에 위험을 가져다 줄 수 있는 요소가 잔존하고 있으며, 이를 예방하기 위한 물리적·관리적·기술적 조치는 다소 미흡한 실정이다. 앞으로 3D프린터뿐만 아니라 IoT로 서로 연결되는 대다수의 장비들에 대한 보안 위험분석 및 평가가 요구되며, 본 논문에서 소개한 3D프린터 위험관리 및 위험평가를 통해 전산 및 네트워크 기능을 가지고 있는 장치들에 대한 조직의 정보보호 활동이 촉진되기를 기대해본다.

참 고 문 헌

[1] 3D Printing Industry, “History of 3D Printing : The Free Beginner’s Guide“, http://3dprintingindustry.com/3d-printing-basics-free-beginners-guide/history/, May 2014

[2] Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business, STAMFORD, Conn., August 11, 2014

[3] 3D Printing Technology, “3D printing helps Ford, GE & Mattel find efficiencies” http://www.3ders.org/articles/20130613-3d-printing-helps-ford-ge-mattel-find-efficiencies.html, Jun.13, 2013

[4] 곽기호, 박성우, “글로벌 3D 프린터산업 기술 동향 분석”, 기계기술정책, 기계저널 2013. 10., Vol. 53

[5] ROB STEIN, “Doctors Use 3-D Printing To Help A Baby Breathe“, http://michiganradio.org/post/doctors-use-3-d-printing-help-baby-breathe, MAR 18, 2014

[5] B.T. Wittbrodt, A.G. Glover, J. Laureto, G.C. Anzalone, D. Oppliger, J. L. Irwin, J.M. Pearce, “Life-Cycle Economic Analysis of Distributed Manufacturing with Open-Source 3-D Printers”, Mechatronics 23 (2013), pp. 713-726.

[6] Kelsey D. Atherton, “HOW THE WORLD'S FIRST 3-D PRINTED GUN WORKS”, http://www.popsci.com/technology/article/2013-05/worlds-first-fully-3-d-printed-gun-here, May 7, 2013

[7] Stephanie M Santoso, Stephen B Wicker, Cornell University, USA, The future of three-dimensional printing : Intellectual property or intellectual confinement?, New Media & Society June 12, 2014

[8] Erica L. Neely, “The Risks of Revolution: Ethical Dilemmas in 3D Printing”, Ohio Northern University, Jun, 2014

[9] NIST IR 8023, “Risk Management for Replication Devices”, NIST, February 2015

[10] NIST SP 800-64 Rev. 2, “Security Considerations in the System Development Life Cycle.”, Oct 2008

[11] NIST SP 800-30, “Guide for Conducting Risk Assessments”, NIST, Sep 2012

[12] ㈜씨에이에스, “정보보안컨설팅 위험평가 매뉴얼”, 2014

[13] NIST SP 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations“,

[14] NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View.”

[15] NIST SP 800-88, “Guidelines for Media Sanitization”

[16] 정승현, 신수민, “기업 정보보호를 위한 3D 프린터 위험관리”, 정보보호학회 동계학술대회, 2014. 12

[17] KISA, “정보보호 관리체계 위험관리 가이드”, 2004. 11.

〈저 자 소 개〉

신 수 민 (Su-Min Shin)
학생회원

2014년 3월～현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 모바일 보안, 침투테스트, ISMS, 개인정보보호

이 창 준 (Chang-Jun Lee)
학생회원

2014년 3월～현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 개발 보안, 금융 보안, 개인정보보호

박 준 용 (Jun Yong Park)
학생회원

2012년 2월 : 동국대학교 정보보호학과 석사
2012년 7월～2014년 2월 : (주)한국IT컨설팅 보안사업부 선임연구원
2014년 2월～현재 : 동국대학교 엔터테인먼트 컴퓨팅 연구센터 연구원
2012년 3월～현재 : 동국대학교 정보통신공학과 박사과정
<관심분야> 융합보안, 스마트그리드보안, 개인정보보호, 위험평가