산업 기술의 유출방지와 보호를 위한 네트워크 3D 프린터 보안체크리스트 연구

우제혁*, 박민제*, 이진근*, 장종민*, 유성환*, 윤지인**, 박의성**, 이원**
한국정보기술연구원 KITRI 차세대 보안 리더 양성 프로그램 BoB*
wpgur0510@gmail.com* alswp951@gmail.com* ExploitSori@gmail.com*,
wkdwhdals0@gmail.com* sung32114@gamil.com*, lazy_jean@naver.com**
park.uiseong@gmail.com**, abraham.won@gmail.com**

A Study On Security Check List of Networked 3D Printers For Prevention of Divulgence And Protection of Industrial Technology

Jae-Hyuk Woo*, Min-Jea Park*, Jin-Geun Lee*, Jong-Min Jang*, Sung-Whan Yoo*,
Jee-In Yoon**, Ui-Seong Park**, Won Lee**,
Korea Information Technology Research Institute Best of the Best*

요 약

3D 프린터는 생산의 효율성을 높이며 비용을 절감할 수 있고 맞춤형 생산이 가능하여 3D 프린터 시장은 더욱 확대될 것으로 예상된다. 이러한 3D 프린터에서 보안 사고가 발생할 경우 도면과 같은 산업 기술이 유출되거나 생산에 차질이 생기는 등 산업 전반에 피해를 끼칠 수 있다. 따라서 3D 프린터 보안 수준을 체계적으로 점검하고 향상시킬 수 있도록 기준에 대한 연구가 필요하다. 이에 본 논문에서는 3D 프린터의 Attack Vector를 분석하여 체크리스트 "레벨 1" 항목 6종을 설정하고, 이를 세분화한 "레벨 2" 항목을 3D 프린터의 Attack Tree 분석을 통해 도출한 항목과 KISA의 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드에서 추출한 항목을 융합함으로써 총 50종 도출했다. 또한, 도출한 체크리스트를 검증하기 위해 국내 3D 프린터 1대의 보안 수준을 점검한 결과 62%의 '취약' 항목을 확인할 수 있었다.

1. 서 론

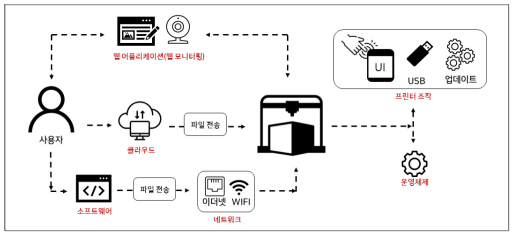
3D 프린터 시장은 2020 기준 약 20억의 규모이며 2022년에 약 32억 규모로 확대될 것으로 예상된다.[1] 3D 프린터는 원하는 3D 모델을 출력하는 기기로, 맞춤형 생산이 가능하고 생산의 효율성을 높여 비용을 절감할 수 있는 점에서 주목받는 기술이다. 특히 세포조직, 임플란트, 인공 뼈 등 맞춤형 의료기기 등이 필요한 바이오 분야와 다품종 생산과 관련된 제조 분야, 건설 산업 분야 등에서 기술개발이 증가하고 있다.[1]

하지만, 만약 3D 프린터 보안사고가 발생할 경우, 도면과 같은 산업 기술이 유출되거나 생산에 차질이 생기는 등 산업 전반에 큰 피해를 초래할 수 있다. 실제로 군사 무기를 3D 프린터로 제작하고 있으며 해외에서도 일반 사람이 3D 프린터로 불법 총기를 제작하여 유죄 판결이 나는 사건이 발생하고 있다.[2][3] 올해 카네기멜론 대학교의 3D 프린터 네트워크 보안 연구에 따르면, 3D 프린터와 연결된 IoT 기기의 해킹 가능성을 제시했다.[4] 또한, 해킹을 통한 도면 탈취 및 변조로부터 산업 피해가 발생할 수 있으며 이는 산업보안의 새로운 공격 벡터이다. 3D 프린터 보안성을 높이기 위해 체계적으로 보안 수준을 점검하고 향상할 수 있는 기준이 필요하지만, 관련 연구는 부족한 실정이다.

따라서 본 논문에서는 산업 기술의 유출방지와 보호를 위한 3D 프린터의 보안 점검 체크리스트 도출 연구를 수행한다. 이를 위해 3D 프린터의 Attack Vector를 분석하여 항목 6종을 설정하고, 이를 세분화한 항목을 도출하기 위해 3D 프린터의 Attack Tree 분석을 통해 도출한 항목과 KISA를 통해 추출한 항목을 융합하는 방법론을 사용한다.[5][6][7] 또한, 도출한 체크리스트의 실효성을 검증하기 위해 국내 제조사의 3D 프린터 보안 수준을 점검하였으며 이를 통해 산업 보안에 기여하고자 한다.

2. 3D 프린터 보안 점검 체크리스트 연구

2.1 3D 프린터의 Attack Vector 분석을 통한 레벨 1 항목 설정



(그림 1) 3D 프린터 Attack Vector

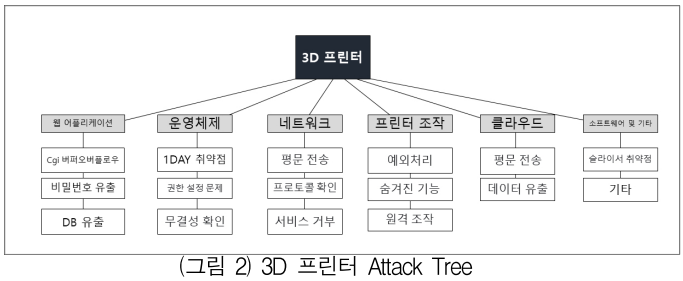
그림 1과 같이 네트워크를 사용하는 3D 프린터에서는 일반적으로 소프트웨어에서 도면 파일을 가공하여 네트워크를 통해 전송하며, 이외에도 웹 모니터링 기능과 클라우드 기능을

활용할 수 있다. 또한 UI(User Interface)와 USB를 통한 펌웨어 업데이트 기능을 이용해 프린터 조작이 가능하고, 운영체제는 3D 프린터 내부 환경 설정을 다루고 있다. 이러한 3D 프린터 기능 분석을 바탕으로 크게 6개의 Attack Vector를 식별했으며, 이를 표 1과 같이 체크리스트의 레벨 1 항목으로 설정하였다.

레벨 1 항목	설명
웹 어플리케이션	3D 프린터의 웹 모니터링 페이지에서의 취약점
운영체제	3D 프린터의 계정 관리 및 내부 프로그램 취약점
네트웍크	3D 프린터의 네트워크 통신 과정에서의 취약점
프린터 조작	3D 프린터의 동작을 제어하는 부분에서의 취약점
클라우드	외부 서버에서 출력파일을 클라우드 형태로 가져올 때 취약점
소프트웨어&기타	내부 3D 슬라이서 및 어플리케이션과 그 외를 다룬 취약점

(표 1) 레벨 1 항목 설명

2.2 3D 프린터의 Attack Tree 분석을 통한 레벨 2 항목 설정



(그림 2) 3D 프린터 Attack Tree

설정한 3D 프린터의 레벨 1 점검항목에서 일반적으로 발생 가능한 취약점을 CVE 등을 분석하여 그림 2와 같이 Attack Tree로 표현했다. 무결성 확인, 평문 전송, 원격 조작 등의 발생 가능 취약점을 식별했으며, 이를 통해 레벨 1 항목을 세분화한 총 34종의 레벨 2 항목을 설정할 수 있었다.

2.3 체크리스트 융합을 통한 레벨 2 항목 보완

레벨 1 항목	레벨 2 항목		
	Attack Tree 분석	KISA 가이드 추출	총 합
웹 어플리케이션	6	15	21
운영체제	11	1	12
네트워크	4	0	4
프린터 조작	7	0	7
클라우드	0	3	3
소프트웨어&기타	3	0	3
총합	34	16	50

(표 2) 체크리스트 융합을 통한 레벨 2 항목 도출 결과

설정한 34종의 레벨 2 항목을 보완하기 위해 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드 항목을 각 분야 항목과 비교, 대조함으로써 16개의 추가적인 레벨 2 점검항목을 식별하였으며, 위의 표 2와 같이 총 50종의 체크리스트를 도출했다.

2.4 체크리스트 검증

레벨 1 항목	레벨 2 항목	취약한 항목
웹 어플리케이션	21	8
운영체제	12	9
네트워크	4	4
프린터 조작	7	6
클라우드	3	2
소프트웨어&기타	3	2
총합	50	31

(표 3) 체크리스트 검증 결과

도출한 체크리스트의 실효성을 검증하고자 국내 3D 프린터 제조사 A사의 기기를 점검하였으며, 그 결과 표 3과 같이 총 50개의 체크리스트 항목에서 31개의 항목이 취약(보안 수준 38%, 취약 항목 62%)인 결과를 얻을 수 있었다.

3. 결론

3D 프린터는 제조, 건설 등의 다양한 산업 분야에서 활용되고 있으며 앞으로도 다양한 산업에 활용이 될 것이다. 이에 따라 보안사고 발생 시 도면 유출, 생산 중단 등 산업 전반에 피해를 끼칠 수 있다. 따라서 본 논문에서는 3D 프린터에 대해 산업에 적용하기 전 적절한 산업 보안성을 검토하고자 총 6종의 레벨 1 항목을 바탕으로 총 50종의 레벨 2 항목을 3D 프린터의 Attack Tree 및 KISA 가이드의 분석, 융합을 통해 도출했다. 또한, 체크리스트의 실효성을 검증하고자 국내 3D 프린터 제조사인 A사의 기기 1대를 점검하여 50개 항목 중 31개의 '취약' 항목 결과를 확인했다.

그러나 해당 연구는 제조사 A의 3D 프린터기기에 대해 체크리스트 검증이 이루어졌다는 한계가 존재한다. 따라서, 체크리스트를 기반으로 다수의 타 제조사의 3D 프린터 보안 점검으로 실효성을 검증하고 보완하는 후속 연구가 필요하다.

본 논문에서 제안한 체크리스트를 통해 3D 프린터의 보안 수준을 점검하고 포괄적 기준으로 활용되기를 바라며 취약점을 사전에 확인함으로써 산업기술 유출 및 보안 사고를 방지할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 김용기, 기술시장동향 70호 3D프린팅 기술 및 시장동향 보고서. 서울:과학기술일자리진흥원, 2019.

[2] 김성현, 「영국 20대 대학생, 3D 프린트로 권총 만들었다 유죄 판결」, 『YTN』, 2019년 06월 21일, "https://www.ytn.co.kr/_ln/0104_201906211435075122"(2020년 12월 05일 접속)

[3] 남정범, 김철, 유기용, "3D 프린팅 기술의 국방 군수분야 적용방안". 국방과 기술 421호 (2014):94-103.

[4] Matt McCormack et al, Security Analysis of Networked 3D Printers and their Deployments, 2020.

[5] 한국인터넷진흥원, 웹 서버 구축 보안점검 안내서. 한국인터넷진흥원, 2010.

[6] 이성영, 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드. 한국인터넷진흥원, 2017.

[7] 장향배, 산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구, 2015