# 공급망 보안기술 동향

## Trends in Supply-Chain Security Technologies

**김대원** (Daewon Kim, dwkim77@etri.re.kr) 보안취약점분석연구실 책임연구원
**강동욱** (Dongwook Kang, dkang@etri.re.kr) 보안취약점분석연구실 선임연구원
**최용제** (Yongje Choi, choiyj@etri.re.kr) 보안취약점분석연구실 책임연구원
**이상수** (Sangsu Lee, sangsu@etri.re.kr) 보안취약점분석연구실 책임연구원
**최병철** (Byeongcheol Choi, corea@etri.re.kr) 보안취약점분석연구실 책임연구원/실장

### ABSTRACT

Security threats in supply-chains can be targeted at all the users who use products related to these supply-chains as well as at single equipment or individuals. This implies that these security threats can cause nationwide economic and social damages. In particular, it is true that hardware security threat analysis technology in supply-chains has significant technical barriers due to the lack of software knowledge as well as the need to study and understand undisclosed hardware designs. In this paper, we discuss the future direction of studies by introducing basic concepts and attack cases, along with domestic and foreign technology trends related to supply-chain security technology.

**KEYWORDS** 공급망 보안, 하드웨어 보안분석, 백도어

## Ⅰ. 서론

정보화시대에 따른 IT 기술의 발달은 우리의 일상생활뿐만 아니라 산업 생태계에도 변화를 초래하여, 대부분의 제조업체는 제품의 설계로부터 생산 및 판매, 유지에 이르는 전 과정에서 다양한 하드웨어 또는 소프트웨어를 구성하여 사용하고 있다. 공급망(Supply-Chain)이란 판매 제품의 생산, 유통, 유지에 요구되는 모든 부품과 서비스를 공급하는 개별 기업들의 집합을 의미한다.

이때 사용되는 하드웨어 및 소프트웨어는 제조·유통의 과정을 거쳐 기업에 공급되는데, 이러한 공급 과정에서 해킹 및 각종 보안 위협에 노출될 수 있어 최근 공급망 보안의 필요성이 강하게 제기되고 있다. 특히 하드웨어를 통한 백도어 형태의 공격은 분석과 탐지가 매우 어려울 뿐만 아니

* DOI: https://doi.org/10.22648/ETRI.2020.J.350413
* 본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No. 2020-0-00215, 시스템/디바이스의 하드웨어 공급망 위협 대응 핵심기술 개발].

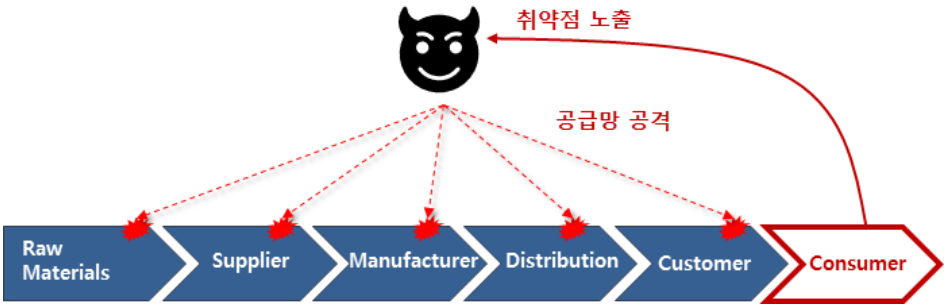



그림 1 공급망 위협 개념도

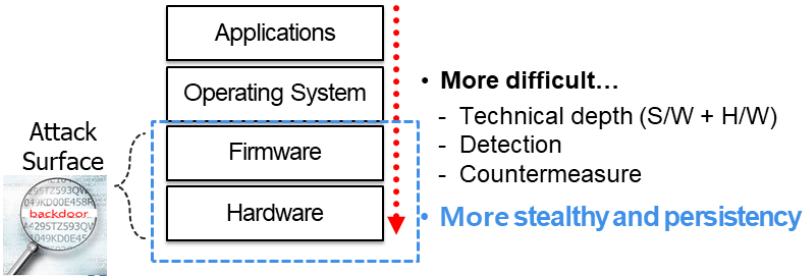



그림 2 하드웨어 공급망 공격 분석 및 탐지의 어려움

라, 점차 확대되는 추세로 실제 이와 관련된 다양한 보안 사고들이 보고되고 있다(그림 1)[1].

특히 하드웨어 기반 공격의 대응 기술들은 일반적인 소프트웨어 대상 분석기술에 비해 보다 높은 난이도와 종합적 분석을 요구하고 있으며, 주로 IC(Integrated Circuit)칩/PCB(Printed Circuit Board)/펌웨어를 대상으로 보안분석 및 취약점 탐지를 수행한다(그림 2).

본 고에서는 이러한 공급망 보안 관련 기술들의 동향 파악을 목적으로, Ⅱ장에서 주요 공급망 공격 사례들을 소개하고, Ⅲ장에서는 국내외의 다양한 대응 기술 연구 및 개발 동향에 대해 소개한다. 마지막으로, Ⅳ장에서는 본 고의 결론으로 이러한 상황에 대응하기 위한 조속한 연구 개발의 필요성에 관해 기술하고 있다.

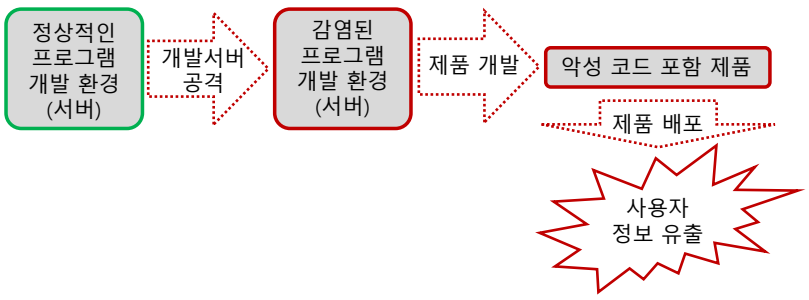
## Ⅱ. 공급망 공격 사례들

공급망 공격의 대표적인 사례로는 ASUS 업데이트 서버 공격, 보안업체 Avast 서버 공격, MeDoc의 업데이트 서버 공격 등이 있다.

2019년도 ASUS 공격 사례는 해외 보안업체인 카스퍼스키(Kaspersky)사에 의해 발견되어 셰도우해머 작전(Operation ShadowHammer)이라 명명된 공격사건이다. 공격자는 ASUS의 업데이트 서버를 공격하고 업데이트 파일을 변조하여, 전 세계적으로 100만 대 이상의 PC를 감염시킨 것으로 추정되고 있다[2]. 공격에 사용된 변조 업데이트 파일은 ASUS의 정상적인 인증서로 서명되어 있어 변조 여부의 파악이 어려우며, 변조 파일에 하드 코딩된 MAC(Media Access Control) 주소 리스트에 의해 추


해당 공격절차 참조 : "공급망 공격 사례 분석 및 대응 방안," KISA, 2019-KA-T02, 2019.

그림 3 ASUS 업데이트 서버 공격 절차




해당 공격절차 참조 : "공급망 공격 사례 분석 및 대응 방안," KISA, 2019-KA-T02, 2019.

그림 4 넷사랑 서버 공격 절차

가 악성코드가 다운로드되도록 구현되었다(그림 3)[1].

Avast 서버 공격은 2017년 발생한 사건으로, 공격자는 Avast가 만든 씨클리너(CCleaner) 소프트웨어의 공식 서버에 침투하여 해당 소프트웨어에 악성코드를 은닉하여 이를 다운로드한 대략 220만 사용자의 PC를 감염시킬 수 있었다. 해당 공격으로 일반 사용자 PC가 주로 감염되었지만, 공격자가 실제로 노린 건 시스코, 마이크로소프트, 구글, 소니, HTC와 같은 대형 IT 기업들이었던 것으로 분석되었다[3].

MeDoc은 회계 관리 소프트웨어로서 우크라이나 정부 기관과 자국 내 90%의 기업이 사용하던 것으로 알려져 있다. 공격자는 MeDoc의 업데이트 서버를 해킹하여 업데이트 요청 시 랜섬웨어가 포함된 제품이 배포되도록 변조하였으며, 이로 인한 경제적 피해 규모가 대략 10조 원대로 추정되는 대규모 사태를 야기하였다[4,5].

이와 유사한 국내 사례로는 넷사랑 서버 공격과 싸이월드/네이트 정보 유출 사건 등이 있다.

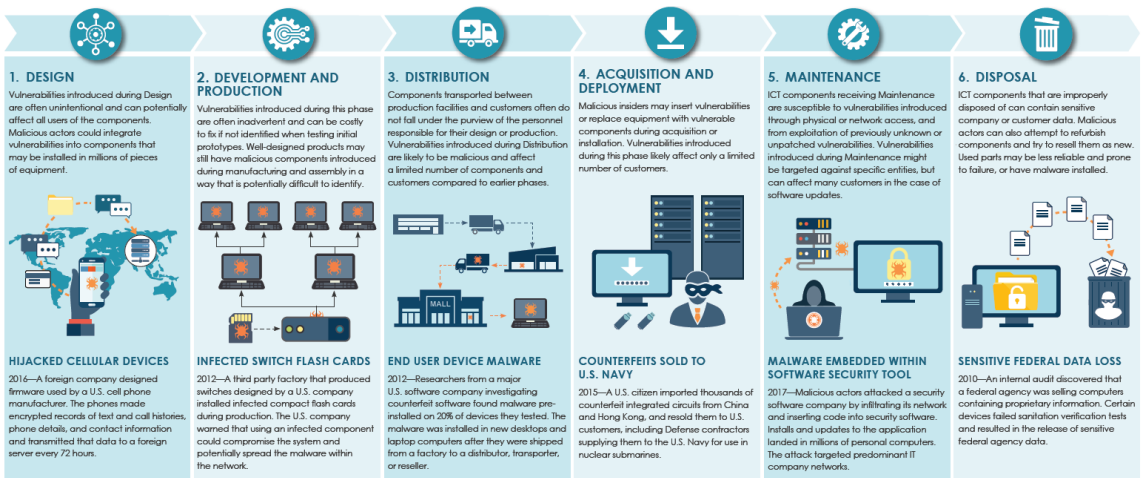
넷사랑 프로그램은 서버 및 애플리케이션 원격 관리 소프트웨어이다. 넷사랑 서버 공격은 2017년 발생하였으며, 그림 4와 같이 공격자는 빌드 서버의 팀뷰어 계정을 탈취하여 서버에 침입한 후, 배포 패키지 빌드에 사용되는 파일에 Shadowpad 악성코드를 삽입하였다. 이후 감염된 해당 제품 패키지는 파일 서버를 거쳐 업데이트 서버에 업로드되어 넷사랑 제품 사용자들에게 배포되었다. 이로 인해 감염된 사용자 PC는 사용자 정보를 C&C(Command and Control) 서버로 전송하였을 뿐

만 아니라 해당 제품에 은닉된 백도어를 통하여 공격자는 정상 인증 과정 없이 사용자의 시스템에 접근할 수 있었다. 해당 공격은 비정상 도메인 접속을 확인하는 방식으로 해외 보안업체인 카스퍼스키사에 의해 발견되었다[1,6].

싸이월드/네이트 정보 유출 사건은 2011년 네이트 사내 특정 업데이트 서버가 해킹되어 사내망에 접속한 PC들을 악성코드에 감염시킨 사건으로, 이를 통해 공격자는 감염된 PC를 통하여 싸이월드/네이트 사용자 DB(DataBase)로 접근하여 저장되었던 3,500만 고객의 개인정보들(이름, ID, 비밀번호, 주민등록번호 등)을 중국 해킹 그룹으로 유출할 수 있었다.

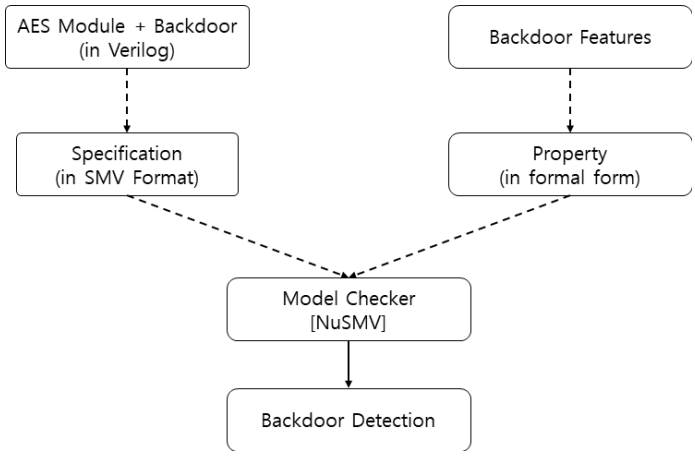
위 사례들에는 주요 공급망 서버들이 공격의 대상이었지만, 미국 국토안보부 산하 사이버 보안 및 기반 시설 보안국(CISA: Cybersecurity and Infrastructure Security Agency)에서 발표한 자료에 따르면 미국에서 발생하였던 공격 사례들을 통하여 실제로는 공급망의 모든 과정이 공격의 대상이 될 수 있음을 알 수 있다. 휴대전화의 플래시 메모리에 저장된 악성 펌웨어로 인하여 72시간 간격으로 중국 서버로 사용자 정보를 전송하도록 하였던 공격 사례, 미국 유명 업체의 네트워크 스위치 생산과정에 삽입된 플래시 카드로 인하여 시스템 손상과 해당 장비에 의한 악성코드 확산을 초래한 공격 사례, 제품 배송 단계에서 악의적인 소프트웨어가 재설치된 공격 사례 등을 통하여 공급망의 모든 단계에서 공격 취약성에 대한 주의가 필요함을 확인할 수 있다(그림 5)[7].

뿐만 아니라 해당 제품을 구성하는 하드웨어 부품으로까지 공격의 범위가 확대될 수 있음을 보여준 대표적 사건이, 2018년 블룸버그를 통해 알려진 서버 제조업체 Supermicro사 메인보드의 스파이칩 발견 사건이다[8]. 이는 해당 보드를 생산하는 중국 내 업체에 몰래 침투한 중국 정보기관에 의해 스파이칩이 장착된 것으로 보안 전문가들은 예상하고 있다. 이러한 방식으로 해당 장비가 공격당하면 기존 소프트웨어 기반의 탐지 기술로는 이를 발견하는 것이 거의 불가능하다고 알려져 있다. 특히, 최근 PC 및 네트워크 장비의 대형 제조사들이




출처 Supply Chain Risks for Information and Communication Technology, CISA, Dec. 2018.

그림 5 CISA의 공급망 공격 사례




출처 박재현, 김승주, "정형 기법을 이용한 하드웨어 AES 모듈 백도어 탐색 연구," 한국정보보호학회 논문지, 제29권 제4호, 2019. 8.

그림 6 AES 모듈 백도어 탐지 절차

제품에 필요한 부품 조달을 위해 글로벌 공급망을 운용하면서 단일 제품에 대해서도 다양한 취약성 발생 루트가 존재할 수 있게 된다는 점에서 매우 심각한 문제로 간주된다.

사실 해당 사건의 진실성 여부에 대해서는 아직까지 논쟁이 계속되고 있으며 명확한 결론이 맺어지지 않았지만, 많은 보안 전문가들은 이러한 공격의 유효성과 위험성에 대해서는 대체로 동의하고 있는 상황이다. 실제로 Monta Elkins라는 보안 전문가는, 인터넷을 통해 쉽게 구할 수 있는 소형 프로세서에 악성코드를 탑재하여 타겟이 되었던 CISCO 방화벽 장비의 비밀번호 인증체계를 무력화하고 손쉽게 새로운 관리자 계정 생성이 가능하도록 하여 방화벽을 원하는 대로 제어할 수 있음을 증명하였으며, 이는 2019년 10월 Wired지에 게재되기도 하였다[9].

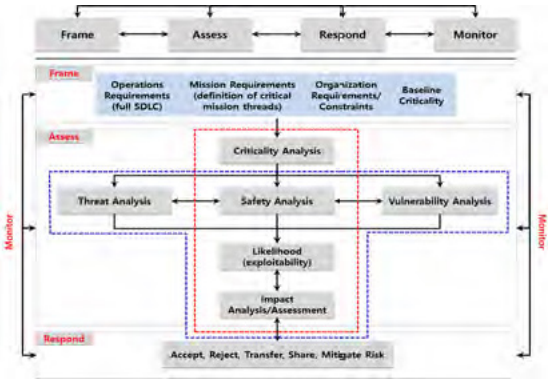
## Ⅲ. 국내·외 기술 동향

본 장에서는 공급망 관련 보안 위협으로 최근 주목받는 하드웨어(IC칩/PCB/펌웨어 등) 기반 공격들에 관한 대응연구들을 주로 소개한다.

### 1. 국내 기술 동향

국내 연구기관 혹은 민간 기업 등에서 공급망을 통해 생산된 제품에 대해 하드웨어 수준의 보안 취약점을 분석하는 기술이 구체화 된 사례는 찾기 어려우며, 일부 개념 검증 수준의 취약점 탐지 기술과 공급망 공격에 대한 대응 체계를 다루는 연구가 진행되어 왔다.

고려대학교 김승주 교수 연구팀은 AES(Advanced Encryption Standard) 암호 모듈의 비밀 키 복원 정보를 탈취할 수 있는 하드웨어 백도어를 탐지하는 기술을 제안하였다(그림 6)[10]. 이 기술은 정형 검증 도구인 NuSMV 모델 체커를 사용하여 AES 모듈의 Verilog HDL(Hardware Description Language) 코드를 분석하고 백도어 포함 여부를 확인하였다. 또한, 더욱 광범위한 백도어 기법을 커버하기 위해 부채널 공격 등 다양한 공격 기법에서 비밀 키 복구를 위해 활용될 수 있는 정보들을 유출 대상 정보로 정의하고 이를 기반으로 검증 모델을 구축하였다.




출처 김동원, 한근희, 전인석, 최진영, "자동차 공급망 위험관리(A-SCRM) 방안 연구," 한국정보보호학회 논문지, 제25권 제4호, 2015. 8.

**그림 7 자동차 공급망 위험관리 프로세스**

고려대학교 최진영 교수 연구팀은 자동차 공급망 공격에 대한 대응으로 자동차 시스템에서 보호해야 할 자산과 보안 위협을 정의하고 이들에 대한 위협을 제거하기 위한 자동차 공급망 위험관리 프로세스 모델을 제안하였다(그림 7)[11].

그림 7과 같이 해당 모델은 기준 정의 단계와 평가 단계, 실행 단계, 모니터링 단계로 구성되며, 기준 정의 단계에서 타 단계의 요구사항들을 정의하고 있다. 평가 단계는 수집된 데이터에 기반하여 위험성 평가를 수행하며, 실행 단계에서는 안전 경로와 보안 경로에서 도출된 위험을 통제하는 방안을 결정한다. 마지막 모니터링 단계를 통해 실행 중인 위험관리 방안을 보완하고 위험 수준이 허용 가능한 범위에서 유지되도록 돕는다.

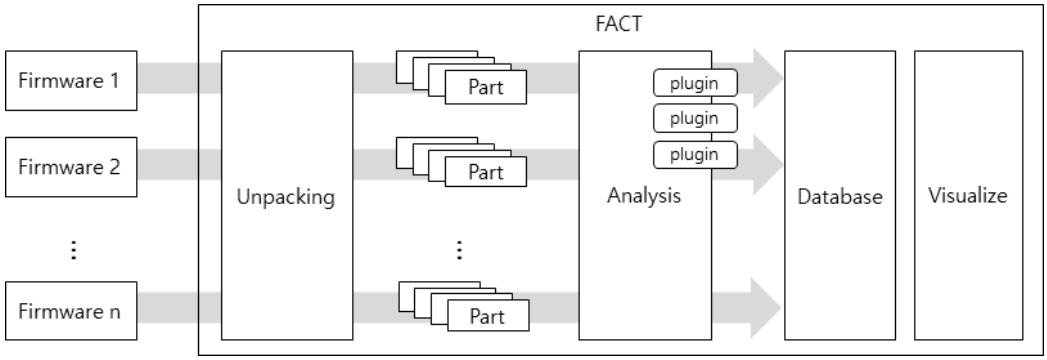
## 2. 국외 기술 동향

미국, 일본 등에서도 하드웨어 공급망 공격에 대한 심각성을 인지하고 관련 사례와 구체적인 기술적 자료들을 공개하거나 공급망 공격 탐지를 자동화할 수 있는 기술에 관한 선행 연구가 진행되고 있다.

미국의 Trust-Hub[12]는 하드웨어 보안 관련 정보를 공유하는 웹 기반 플랫폼으로 하드웨어 백도어 및 부채널 공격 사례에 대한 튜토리얼과 함께 하드웨어 취약점 분석 및 공격 관련 논문들의 데이터 자료들을 제공한다. 또한, 하드웨어 취약점 데이터베이스와 하드웨어 로직의 분석 난이도를 높여 하드웨어 백도어 탐지를 어렵게 하는 난독화 기법들에 대해서도 자세한 설명을 제공하고 있다. 일본은 2017년부터 하드웨어 악성 행위 탐지 기술 개발에 착수하여 Trust-Hub에 공개된 다양한 악성 회로의 탐지가 가능한 도구 개발을 자체적으로 추진 중인 것으로 알려져 있다.

퍼듀대학의 Prashast Srivastava 등은 리눅스 기반 펌웨어의 취약점 분석을 위한 장치 독립적인 에뮬레이션 기반 동적 분석 기술인 FirmFuzz를 제안하였다[13]. 이 기술은 정보수집, 분석준비, 퍼징의 세 단계로 구성된다. 정보수집 단계는 정적 분석을 통해 퍼징 과정의 커버리지를 증가시키기 위한 정보를 수집하고 분석준비 단계는 에뮬레이션 및 동적 분석을 위한 위장 드라이버 및 취약점 탐지 기능을 펌웨어 이미지에 추가한다. 연구팀은 Firm-Fuzz를 활용하여 당시 시중에 출시되었던 IP 카메라와 라우터를 포함한 27개 장치의 32개 펌웨어 이미지를 분석하여 기존에 알려지지 않았던 새로운 7개의 취약점을 탐지하였다고 보고하였다.

OWASP(Open Web Application Security Project)는 임베디드 시스템의 펌웨어 보안성 분석을 위한 방법론인 FSTM(Firmware Security Testing Methodology)을 공개하였다[14]. 이는 타겟 장치 및 펌웨어 관련 정보 수집, 펌웨어 획득, 펌웨어 분석, 파일 시스템 추출, 파일 시스템 분석, 펌웨어 에뮬레이션, 동적 분석, 취약점 검증 등의 단계로 구성되며 각 단계를 수행하기 위한 구체적인 방법과 활용




출처 The Firmware Analysis and Comparison Tool (FACT). https://github.com/fkie-cad/FACT_core

그림 8 FACT의 펌웨어 언패킹 및 분석 과정

가능한 도구 등도 소개하고 있다. FSTM에서 펌웨어 분석과 파일 시스템 추출 및 분석 도구로 소개된 FACT(Firmware Analysis and Comparison Tool)는 펌웨어 및 파일 시스템 분석을 자동화해 주는 웹 기반 도구로 다양한 펌웨어 언패킹 도구를 통합하고 펌웨어 분석을 자동화 및 병렬화하여 효율성을 높였을 뿐만 아니라 분석 결과의 요약 및 세부 사항을 웹 페이지에서 확인 가능하며 플러그인 기반의 분석 기능 확장도 지원하고 있다. 또한, 다수의 펌웨어 분석 결과들을 데이터베이스에 저장하고 이들을 쉽게 비교할 수 있는 기능을 제공한다(그림 8).

## Ⅳ. 결론

공급망을 대상으로 보안 위협은 지속적으로 증가하고 있을 뿐만 아니라 최근에는 소프트웨어 기반의 기존 공격방식을 탈피하여 하드웨어 장치로까지 공격이 확대되고 있는 추세이다. 특히 하드웨어 공급망 취약점은 물리적 부품 수준의 보안 이슈이므로, 해당 부품을 제거하고 관련된 회로로직을 수정하기 전까지는 근본적으로 해결되지 않는다. 하지만 CPU나 DMA(Direct Memory Access) 컨트롤러, PCI(Peripheral Component Interconnect) 컨트롤러와 같이 비교적 기능이 명확한 부품이 아닌 여러 IC칩들은 외견만으로 기능과 사용 목적을 정확하게 파악하는 것이 극히 어려워, 일반인은 쉽게 위협 여부를 파악할 수 없거나 파악하여도 쉽게 대응하기 어려운 고난이도 기술이 사용되고 있다.

그럼에도 불구하고 국내의 경우 이러한 공격에 대한 종합적이고 체계적인 분석력을 가진 전문 연구기관 또는 연구사례가 절대적으로 부족한 실정이다. 이에 반해 미국, 유럽, 일본 등 IT 선진국들은 이미 하드웨어 공급망 위협의 파급효과를 인지하여 다양한 대응 수단을 마련하고 있으며 Trust-HUB 같은 구체적 연구사례도 보고되고 있다. 심지어 소수의 중국 기업들은 타겟 하드웨어의 분석으로부터 다양한 정보를 취득하여 제공하는 서비스를 영리활동으로 추진하고 있다. 만약 이러한 기술 격차를 해당 국가 또는 개인이 악용하여 국내를 향한 사이버 공격으로 활용할 경우 현재 상황에서의 대응은 거의 불가능하다고 예상된다.

따라서, 향후 예상되는 주요 인프라 장비에 대한 하드웨어 공급망 위협에 대응하고, 동 분야 국제적 기술 격차를 해소할 수 있도록 하드웨어적 보안 취약성 존재 여부를 판별할 수 있는 분석체계 구축과


그림 9 하드웨어 공급망 공격 대응을 위한 종합적 분석체계

이에 필요한 원천기술의 조속한 연구 개발이 요구되고 있다(그림 9).

## 약어 정리

| | |
|---|---|
| AES | Advanced Encryption Standard |
| C&C | Command and Control |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DB | DataBase |
| DMA | Direct Memory Access |
| FACT | Firmware Analysis and Comparison Tool |
| FSTM | Firmware Security Testing Methodology |
| HDL | Hardware Description Language |
| IC | Integrated Circuit |
| MAC | Media Access Control |
| OWASP | Open Web Application Security Project |
| PCB | Printed Circuit Board |
| PCI | Peripheral Component Interconnect |

## 참고문헌

[1] "공급망 공격 사례 분석 및 대응 방안," KISA, 2019-KA-T02, 2019.

[2] "Operation ShadowHammer," Kaspersky, Mar. 2019. https://securelist.com/operation-shadowhammer/89992

[3] OndrejVlckk, "CCleaner APT Attack: A Technical Look Inside," RSAConference2018.

[4] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, Oct. 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[5] "2017 cyberattacks on Ukraine," Wikipedia, Oct. 2019. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

[6] "ShadowPad in corporate networks," Kaspersky, Aug. 2017. https://securelist.com/shadowpad-in-corporate-networks/81432/

[7] "Supply Chain Risks for Information and Communication Technology," Cybersecurity and Infrastructure Security Agency, Dec. 2018. https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_nrmc_supply-chain-risks-for-information-and-communication-technology.pdf

[8] "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S.

Companies," Bloomberg Businessweek, Oct. 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[9] "Planting Tiny Spy Chips in Hardware Can Cost as Little as $200," Wired, Oct. 2019. https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

[10] 박재현, 김승주, "정형 기법을 이용한 하드웨어 AES 모듈 백도어 탐색 연구," 한국정보보호학회 논문지, 제29권 제4호, 2019. 8.

[11] 김동원, 한근희, 전인석, 최진영, "자동차 공급망 위험관리(A-SCRM) 방안 연구," 한국정보보호학회 논문지, 제25권 제4호, 2015. 8.

[12] Trust-Hub. https://trust-hub.org

[13] Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, Mathias Payer, "FirmFuzz: Automated IoT Firmware Introspection and Analysis," Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, 2019. 11.

[14] The Firmware Analysis and Comparison Tool (FACT). https://github.com/fkie-cad/FACT_core