하드웨어 트로이목마 탐지기술 동향

Trends of Hardware-based Trojan Detection Technologies

최양서 (Y.S. Choi, yschoi92@etri.re.kr) 보안취약점분석연구실 책임연구원
이상수 (S.S. Lee, sangsu@etri.re.kr) 보안취약점분석연구실 책임연구원
최용제 (Y.J. Choi, choiyj@etri.re.kr) 보안취약점분석연구실 책임연구원
김대원 (D.W. Kim, dwkim77@etri.re.kr) 보안취약점분석연구실 책임연구원
최병철 (B.C. Choi, corea@etri.re.kr) 보안취약점분석연구실 책임연구원/실장

ABSTRACT

Information technology (IT) has been applied to various fields, and currently, IT devices and systems are used in very important areas, such as aviation, industry, and national defense. Such devices and systems are subject to various types of malicious attacks, which can be software or hardware based. Compared to software-based attacks, hardware-based attacks are known to be much more difficult to detect. A hardware Trojan horse is a representative example of hardware-based attacks. A hardware Trojan horse attack inserts a circuit into an IC chip. The inserted circuit performs malicious actions, such as causing a system malfunction or leaking important information. This has increased the potential for attack in the current supply chain environment, which is jointly developed by various companies. In this paper, we discuss the future direction of research by introducing attack cases, the characteristics of hardware Trojan horses, and countermeasure trends.

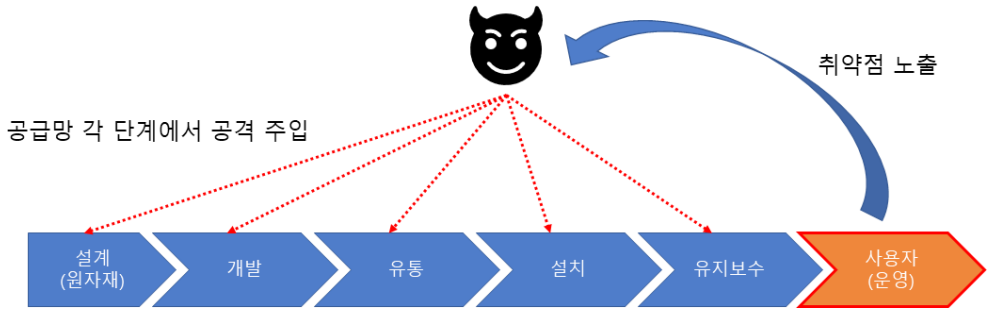
KEYWORDS H/W 트로이목마 탐지 대응기술, 공급망 보안, 하드웨어 보안, 하드웨어 트로이목마

Ⅰ. 서론

최근 크게 이슈가 되고 있는 보안 분야로 공급망 보안 분야가 있다. 여기서 공급망이라는 것은 특정 제품을 생산하여 소비자에게 전달하는 일련의 과정을 의미한다. 이를 단계적으로 나눠보면 설계(원자재), 개발, 유통, 설치, 유지보수 및 사용자로 구분해 볼 수 있고, 이들 간의 물류의 흐름 전체를 공급망이라고 할 수 있다. 세부적으로는 이러한 공급망에서 요구되는 조직, 사람, 활동, 정보 및 자원 전체를 공급망에 포함한다.

정보화 시대의 도래로 IT 기술은 크게 발달하였고, IT 기술은 우리의 일상과 산업에 매우 큰 영향을 미치고 있다. IT 기술이 접목된 다양한 기기 및

* DOI: https://doi.org/10.22648/ETRI.2021.J.360608
* 본 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No. 2020-0-00215, 시스템/디바이스의 하드웨어 공급망 위협 대응 핵심기술 개발].



출처 Reproduced with permission from [1].

그림 1 공급망 각 단계별 공격 주입

제품들은 단일 기업에서 원자재 확보, 부품 제조, 제품 생산 및 유통이라는 제품 개발 및 배송 전 과정을 모두 독자적으로 진행할 수 없는 구조를 가지고 있다. 특정 제품을 제조하는 데 있어서 설계, 부품의 조달, 조립 및 완제품 생산 그리고 배송의 공정에서 다양한 업체와의 협력 등을 통해 일련의 공급망이 구성되어 제품 생산이 진행된다.

그림 1과 같이 IT 제품 역시 공급망의 다양한 공정에서 각종 해킹 및 보안 위협에 노출될 수 있어 공급망 보안 이슈가 크게 대두되고 있는 것이다[1]. 이러한 공급망 보안은 크게 하드웨어 공급망 보안과 소프트웨어 공급망 보안으로 나눌 수 있다. 소프트웨어 공급망 보안의 가장 일반적인 공격 방법은 임베디드 장치 또는 특정 기기의 펌웨어 조작을 통한 악의적인 행위 시도를 들 수 있고, 하드웨어 측면에서 본다면 특정 부품의 교체, 설계와 다른 부품 사용 및 삽입 그리고 악성 행위를 수행하는 회로 추가 등에 대한 위협이 존재할 수 있다.

특히, 하드웨어 공급망 보안과 관련하여 이슈가 되고 있는 것 중에 하나는 집적회로(IC) 내에 존재할 수 있는 하드웨어 트로이목마[2] 공격과 이에 대한 존재 여부를 확인하는 것이다.

반도체 업계는 집적회로 생산 비용을 낮추기 위해 아웃소싱을 통한 물품 제조를 추진하고 있고, 이를 통한 비용 절감 덕분에 많은 시스템들은 다수의 IP(Intellectual Property)로 구성되게 되었다. 이러한 IP는 다른 공급업체에서 제공되며, 타사에서 구현한 CAD 도구를 사용하여 설계 및 조립된다. 또한 제조, 조립 및 포장은 해외 서비스 제공업체를 통한 아웃소싱으로 진행하는 경우가 많아 위조 및 전자 회로의 수정과 같은 여러 보안 위협에 노출되게 된다. 악의적으로 또는 의도적으로 회로에 적용된 이런 수정을 하드웨어 트로이목마라고 하며 오래전부터 학계 및 산업계의 주목을 받고 있다. 본고에서는 하드웨어 공급망 보안과 관련한 하드웨어 트로이목마 탐지기술 동향에 대해서 기술한다.

Ⅱ. 하드웨어 공급망 공격 사례

2018년 블룸버그를 통해 알려진 서버 제조업체 'Supermicro'에 장착된 메인보드의 스파이 칩 발견 사건[3]은 공급망 위협이 하드웨어 단으로 확장되고 있다는 것을 암시하기도 해 세계적으로 주목받은 사건이었다. 스파이 칩이 설치된 서버는 애플, 아마존 등을 포함한 미국의 수십 개 기업과 정부기관들이 사용하고 있었는데, 이는 해당 보드를 생산하는 중국 하청 업체에 몰래 침투한 중국 정보기

관에 의해 스파이 칩이 장착된 것으로 보안 전문가들은 예상하고 있다[4].

매사추세츠주 메튜에 있는 Tytronix Inc. 및 Epic International Electronics는 2007년 2월부터 2012년 12월까지 250만 달러 상당의 위조 반도체를 판매했는데, 이는 모토로라(Motorola Inc.)나 내셔널 세미컨덕터(National Semiconductor) 등의 회사에 납품되었다. 연방 당국은 위보 반도체 칩에 악성 코드나 백도어가 포함될 수 있다고 밝혔다. 동일한 업체는 100개의 위조 반도체를 2012년 2월 잠수함 기지에 납품하였는데, 이에 대한 사용 전 테스트 과정에서 칩이 조작되었다는 것이 밝혀졌다[5].

2013년 Edward Snowden이 공개한 문서에 따르면 TAO(Tailored Access Operations) 부서와 기타 NSA 직원이 감시 대상 조직에 배송되는 서버, 라우터 및 기타 네트워크 장비를 가로채 변조된 펌웨어를 설치하였다. 이 펌웨어에는 운영체제가 재설치 되더라도 동작하는 맞춤형 BIOS 익스플로잇 코드가 포함된 것으로 알려졌다[6].

상기 사건 외에도 2012년, 미국 업체가 설계한 네트워크 스위치가 생산과정에서 시스템 손상과 네트워크로 악성 코드 확산을 가능하게 하는 감염된 소형 플래시 카드가 삽입된 사건[7]이 있었으며, 2016년 미국보안회사가 중국산 휴대 전화(ZTE)의 플래시 메모리에 저장된 펌웨어로부터 중국 서버로 사용자 정보를 72시간마다 송신하는 악성 코드를 발견한 사건[8]도 있었다. 또한 IC칩 변조와 관련해서는 2012년 미군사용 장비에서 사용되는 중국산 칩에서 백도어를 발견[9]하였고, 2013년 러시아에 수출된 중국산 전기다리미에 내장된 악성회로가 주위 무선 LAN을 이용하여 PC에 악성코드를 보내고 다량의 스팸 메일을 보내는 사건이 발생[10]하였다. 2018년 대만 VIA Technologies가 개발한 C3 프로세서에서 백도어 발견 등의 사건이 있었다[11].

이와 같이 해당 장비가 하드웨어 적으로 공격당할 경우 기존 소프트웨어 기반의 탐지기술로는 이를 발견하는 것이 매우 어렵다고 알려져 있는 상황에서, PC 및 네트워크 장비의 대형 제조사들이 제품에 필요한 부품 조달을 위해 글로벌 공급망을 운용하면서 단일 제품에 대해서도 다양한 취약성 발생 경로가 존재할 수 있게 된다는 점은 매우 심각한 문제로 대두되고 있다.

이미 2018년 말 시만텍은 '사이버 보안 전망: 2019년과 그 이후' 보고서[12]에서 향후 하드웨어 공급망 공격의 확산과 칩(Chip) 변조 및 BIOS 등에 사용되는 펌웨어 변조 등을 언급하며 이러한 공격들은 기존 기술로는 제거가 매우 어려운 영역에 속한다고 언급했고, 트렌드마이크로는 '2020 보안 예측 보고서'[13]에서 기업들은 클라우드와 공급망에 대한 지속적 보안 위협에 직면할 것이라 예측했다.

Ⅲ. 하드웨어 트로이목마

Ⅱ장에서 언급된 사례와 더불어 하드웨어 공급망 공격의 가장 대표적인 방법 중에 하나가 하드웨어 트로이목마를 이용한 방식이다. 하드웨어 트로이목마란 집적회로의 회로를 변조하여 악성행위를 수행하는 것으로 특정 정보 유출, 시스템 지연 및 오작동 또는 시스템의 보안 기능을 우회하기 위해 활용된다. 이러한 하드웨어 트로이목마는 서버, PC 등 컴퓨터 시스템의 보드 상에 적용되는 것뿐만 아니라, KVM 스위치, 키보드, 마우스 네트워크 카드, 기타 네트워크 장비 등에도 적용될 수 있으며, 이를 기반으로 특정 사이트의 접근 암호 등을 탈취하는 것도 가능하다[14].

하드웨어 트로이목마는 칩 로직 함수의 매우 작은 부분을 변조하여 특정한 입력에 의해 칩의 출력

이 변경되도록 만드는데, 이를 통해 다양한 공격을 시도한다. 공격자 입장에서 봤을 때, 트로이목마는 해당 칩 또는 장치를 구현하고 설계 및 운영 시험을 수행하는 과정에서는 활성화되지 않아야 한다. 그래야만 최종적으로 제품화될 때까지 트로이목마의 존재가 알려지지 않기 때문이다. 이를 위해 트로이목마는 트로이목마 자체 기능과 칩 기능 및 생산 테스트를 고려해서 설계되게 된다.

이러한 하드웨어 트로이목마는 다양한 방식으로 분류되고 있다. 대표적으로는 Karri에 의해 제안된 5가지 특성에 기반한 분류 기법[15]과 Jain 등에 의해 제안된 활성화 방식에 따른 분류 방식[16]이 있다.

1. 5가지 특성 기반 분류

Karri는 하드웨어 트로이목마의 칩 내 삽입 단계, 추상화 레벨, 활성화 방식, 효과 및 설치 위치에 따라 그림 2와 같이 분류한다[15].

여기서 칩 내 삽입이라는 것은 해당 칩 내에 하드웨어 트로이목마가 삽입되는 단계를 의미하는 것으로 최초 규격 정의 단계, 설계 단계, 제조 단계, 시험 단계, 조립 단계로 구분될 수 있다.

추상화 레벨은 실제 칩 상에서 어떤 수준으로 하드웨어 트로이목마가 구현되는가를 의미하는 것으로, 시스템레벨, 레지스터 전송레벨, 게이트 레벨, 트랜지스터 레벨, 물리레벨로 구분된다.

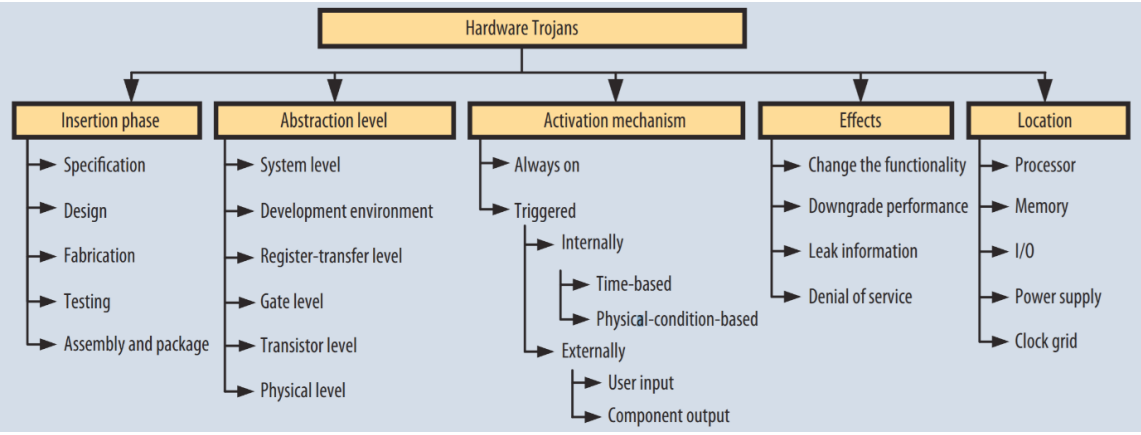
활성화 방식은 하드웨어 트로이목마의 동작이 시작되는 방식에 관한 것으로 항상 동작하고 있는 것과 특정 조건에 맞는 경우 시작되는 방식이 있다. 이때 특정 조건에 따라 시작되는 방식은 내부 트리거와 외부 트리거로 나눌 수 있다.

또한 트로이목마는 활성화될 때 수행하는 악성 행위가 미치는 영향(목적)에 따라 구분되기도 한다. 이는 기능의 변경, 성능 저하, 정보 유출 및 서비스 거부 등으로 구분될 수 있다.

마지막으로 하드웨어 트로이목마가 설치되는 위치에 따라 구분할 수 있는데, 프로세서, 메모리, 입출력, 전원공급장치, 클럭 그리드 등으로 구분된다.

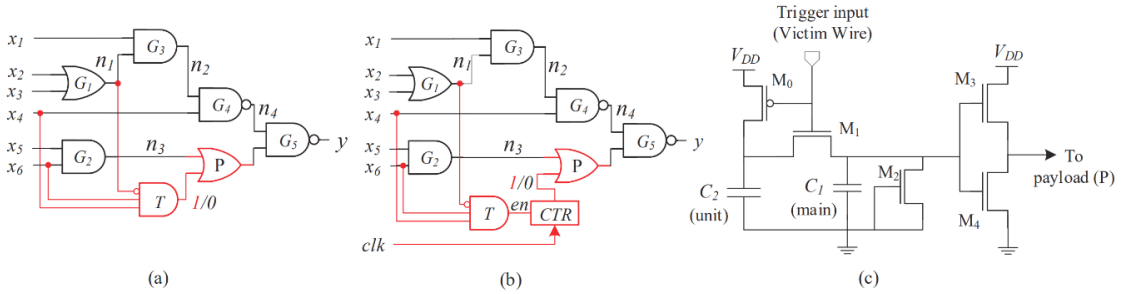
2. 트로이목마 활성화 방식 기반 분류

하드웨어 트로이목마는 악성행위를 유발하는



출처 Reprinted with permission from [15].

그림 2 하드웨어 트로이목마 분류 기법



출처 Reprinted with permission from [16].

그림 3 하드웨어 트로이목마 분류: (a) 조합 트로이목마, (b) 순차 트로이목마, (c) 아날로그 트로이목마

회로를 실행시키는 트리거(Trigger)와 트리거로 활성화되는 실제 기능 부분인 페이로드(Payload)로 구성되어 있다. 하드웨어 트로이목마를 활성화시키는 트리거는 외부로부터 발생하는 직접적인 입력(PI: Primary Input)이나 내부 회로가 특정한 값이나 일련의 값들이 발생하는 경우 동작된다.

이러한 하드웨어 트로이목마를 트리거의 종류, 즉 활성화 방식으로 구분하면 그림 3과 같이 조합 트로이목마(Combinational Trojan), 순차 트로이목마(Sequential Trojan), 아날로그 트로이목마(Analog Trojan)의 세 종류로 분류 가능하다[16].

조합 트로이목마는 특정 상태에서 트리거를 활성화시키는 입력이 발생하면 즉각적으로 해당 트로이목마가 활성화되는 단순한 형태의 트리거를 사용하는 트로이목마를 의미한다. 이러한 조합 트로이목마는 정해진 입력이 만족되는 순간 트리거가 활성화됨과 동시에 바로 페이로드 부분이 활성화되어 악성행위가 시작된다.

순차 트로이목마는 조합 트로이목마와 달리 트리거가 활성화되기 위해서는 다양한 입력이 만족되어야 하는데, 특히 트리거 활성화를 위한 입력 패턴이 순차적으로 정확히 발생하거나, 정확한 입력이 N번 이상 반복적으로 발생해야 페이로드 활성화가 시작되는 형태이다.

이를 위해 순차 트로이목마의 트리거는 조합 로직(Combinational Logic)과 함께 상태 요소(State Elements)가 포함되게 된다. 그림 3(b)는 트리거가 AND 게이트와 카운터로 구성된 순차 트로이목마를 보여주고 있다. 이런 형태의 트로이목마는 특정 트리거 조건이 충족되더라도 카운터를 증가시키고, 카운터가 특정 개수에 도달되어야 실행되기 때문에 특정 테스트 패턴이나 입력을 통해 발견될 확률이 매우 낮게 된다.

아날로그 트로이목마는 트리거 활성화를 위하여 아날로그 입력을 활용하는 트로이목마를 의미한다. 트리거 활성화를 위한 아날로그 입력은 다양한 형태가 활용될 수 있다. Yang 등은 참고문헌[17]에서 그림 3(c)와 같이 주변 전선을 활용하여 콘덴서가 전하를 축적하도록 함으로써 트리거 회로를 활성화하는 방법을 제안하였다. 또한 이러한 전압을 사용하는 방식을 기존 순차 트로이목마에 접목한 형태의 트리거를 활용하는 방식도 제안되었다[18].

IV. 하드웨어 트로이목마 탐지기술 동향

1. 하드웨어 트로이목마 대응 방안

하드웨어 트로이목마에 대한 대응 방안으로는

IC칩 상에 존재하는 트로이목마에 대한 탐지 기법과 IC칩에 트로이목마가 설치되지 않도록 하는 예방 기법으로 구분될 수 있다.

여기서 트로이목마 설치 예방 기법으로는 설계에 Built-in Locking 메커니즘을 적용하여 설계의 실제 기능과 구현 내용을 숨기는 회로 난독화 기법 등을 적용함으로써 트로이목마 삽입을 어렵게 하거나[19], 칩 제조업체를 분리하여 특정 위치에 트로이목마를 삽입하더라도 그 결과가 정확히 어떤 방식으로 나타나는지를 예측하지 못하도록 하는 방안[20]이 제안되었다.

하드웨어 트로이목마의 탐지는 포스트-실리콘(Post-silicone) 방식과 프리-실리콘(Pre-silicone) 방식으로 나눌 수 있다. 포스트-실리콘 방식은 칩 제조가 완료된 상태에서 해당 칩 내에 하드웨어 트로이목마가 포함되어 있는지를 확인하는 방식이고, 프리-실리콘 방식은 칩 제조 이전에 설계 단계에서 트로이목마의 포함 여부를 확인하는 방식이다.

포스트-실리콘 방식은 파괴적 방식과 비파괴적 방식으로 구분 가능하다. 파괴적 방식은 점검 결과가 비파괴적 방식보다 신뢰성이 높다는 특징이 있으나, 점검 수행 후 점검 대상 IC칩을 재사용할 수 없는 방식으로 IC칩 리버스 엔지니어링[21] 기법 등이 존재한다. 비파괴적 방식은 점검을 수행하더라도 점검 대상 칩을 재사용할 수 있는 방식으로 기능 테스트와 사이드 채널 분석이 포함될 수 있다. 본고에서는 포스트-실리콘 방식의 비파괴적 탐지 기법을 중심으로 살펴본다.

프리-실리콘 방식에는 코드 커버리지 분석, 구조분석, 논리테스트, 기능분석 등이 존재하는데, 여기서 코드 커버리지 분석이란 설계된 IP의 검증 과정에서 실행된 코드라인의 백분율을 이용하여 전체 논리회로 중 어느 정도가 실행되는지를 확인하는 것으로 실행되지 않는 코드가 많은 경우 트로이목마가 존재할 수 있다고 판단한다. 구조분석은 특정 지표를 이용하여 활성화 확률이 낮은 회로를 의심스러운 것으로 판단하는 방식이고, 논리테스트는 설계된 회로를 시뮬레이션을 통해 수행하여 포스트-실리콘 방식과 유사하게 확인하는 것을 말하며, 기능분석은 특정 IP가 어떤 기능을 수행하는지를 확인하여 트로이목마와 유사한 기능이 존재하는 경우 의심하는 방식을 의미한다[22].

2. 트로이목마 탐지기술 동향

생산이 완료된 IC칩에 하드웨어 트로이목마가 포함되어 있는지 여부를 살펴보기 위해 비파괴적인 포스트-실리콘 하드웨어 트로이목마 탐지기술에 대한 연구가 지속되어 왔다. 이러한 연구에 대하여 본고에서는 조합 트로이목마 탐지기술과 순차 트로이목마 탐지기술로 구분하여 동향을 살펴보고자 한다.

가. 조합 트로이목마 탐지기술

일반적으로 조합 트로이목마에 대한 탐지를 위해서는 해당 트로이목마를 실행시켜 악성 행위가 발생하는지 여부를 확인하는 방법을 취하게 된다. 이때 가장 중요한 것은 악성 행위 발생을 위해 필요한 입력을 만들어 내는 일인데, 이는 마치 SW 취약점 점검을 위하여 퍼징을 수행하는 것과 유사한 개념이다.

이렇듯 다양한 입력을 만들어 내는 방법에 대한 연구가 다수 존재하는데, Zhou 등은 조합 트로이목마에 대한 일반화된 모델을 제안하고 Single Net Trigger(Type-1 Trojan) 탐지를 위해 어떻게 시험 패턴을 생성할 것인가를 보여줬다[23]. 이 논문에서는 점검 대상 전체 회로에 대하여 Conditional Stuck-At Fault(SAF)를 기반으로 모든 가능한 Type-1

조합 트로이목마를 실행시킬 수 있는 입력 패턴(CSP: Conditional SAF Pattern)을 생성할 수 있음을 보였으며, 이러한 CSP는 높은 차수의 트로이목마를 탐지하는데도 활용될 수 있음을 보였다.

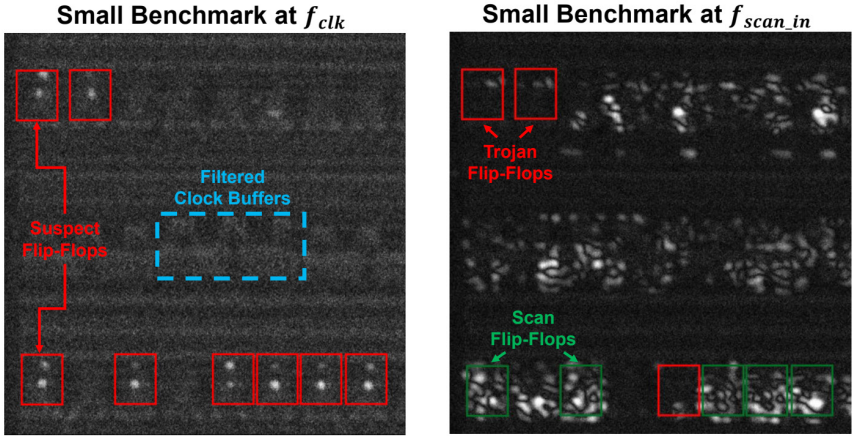
Cruz 등은 부분 스캔을 위한 테스트 셋의 효율을 향상시키기 위해 모델 검사 도구에서 활용할 수 있는 자동 입력 패턴 생성 방안을 제안하였다[24]. Salmani 등은 게이트 레벨 넷리스트들의 개별 넷들에 대해 관찰가능성(Observability)과 제어가능성(Controllability) 값을 추출하고, 이를 기계학습과 신경망을 이용하여 구분함으로써 트로이목마를 탐지하는 방법을 제시하였다[25]. 이 외에도 다수의 기계 학습을 통한 트로이목마 탐지기술이 제안되었다[26,27].

그러나 이와 같은 조합 트로이목마 탐지기술은 대부분 칩 내에 트로이목마가 존재하는지 여부를 판단하기 위한 것으로 큰 규모의 칩의 경우 모든 회로를 실행시킬 수 있는 시험 셋을 만들어 내는 것이 매우 어려워 실질적인 활용이 어려운 면이 있다. 또한, 조합 트로이목마가 아닌 순차 트로이목마의 경우에는 탐지가 거의 불가능한 단점이 있다.

나. 순차 트로이목마 탐지기술

하드웨어 트로이목마를 설치하는 공격자들은 가능하면 트로이목마가 발견되지 않기를 바란다. 이를 위해서는 트로이목마를 실행시키는 트리거가 매우 낮은 확률로 발생되어야 하는데, 이러한 측면에서 봤을 때 조합 트로이목마보다는 순차 트로이목마가 발견될 확률이 낮다.

그러나 이와 같은 순차 트로이목마 역시 발견 가능한데, 대표적인 방법 중 하나가 DFT(Design-For-Test) 구조를 활용하는 것이다. 일반적으로 대부분의 칩에는 테스트를 위한 DFT 구조(또는 Scan 구조)가 포함된다[28]. DFT를 구성하기 위해 기능이 확인된 회로(Flip-flops)를 스캔 회로(Scan flip-flop)로 변경하게 된다. 스캔 회로는 설계된 회로의 기능 시험을 위해 다양한 입력을 시험자가 만들 수 있도록 회로에 원하는 입력을 삽입하는 회로를 추가한 회로이다. 이를 통해 다양한 입력을 삽입하여 회로의 정상 작동 여부를 확인하게 된다.



출처 Reprinted with permission from [29].

그림 4 소형 s1423 T607 트로이목마 EOFM 이미지: (a) 필터링된 클록 버퍼를 사용하여 클록 주파수 EOFM 측정에서 의심되는 flip-flop 식별, (b) 스캔 입력 주파수 EOFM 측정에 대한 트로이목마 탐지 결과.

만약 점검 대상 칩에 하드웨어 트로이목마가 포함되어 있다면, 이와 같이 다양한 입력을 만들어 낼 수 있는 스캔 회로로 변경되고 시험하는 과정에서 탐지될 가능성이 높아진다. 왜냐하면, 스캔 회로로 변경되면 순차 트로이목마가 조합 트로이목마 형태로 변경되게 되고, 이에 따라 시험자는 다양한 입력을 통해 트로이목마 트리거가 활성화되는 입력을 만들어 낼 가능성이 높아지기 때문이다. Stern은 비파괴 후면 레이저 검증 접근 방식을 사용하여 트로이목마를 탐지하기 위해 이 개념을 이용했다[29]. 본고에서는 일반적인 EOFM(Electro-Optical Frequency Mapping) 이미지를 비교하는 방법을 사용했는데, 일반적인 상황에서 전원을 인가하고 점검 대상 IC칩의 후면에 적외선을 쐬어 확보한 내부 회로 이미지와 스캔 모드 상태에서 변경된 입력 값을 인가하여 보이는 이미지를 비교하여 트로이목마를 찾는 방식을 이용했다(그림 4 참고).

또 다른 순차 트로이목마 탐지 방법의 하나인 사이드 채널 활용 방법으로는 전력[30], 온도[31], 지연[32]과 방사선[33] 등을 이용한 방법에 제안되고 있다. 다만, 이러한 방식은 골든 서킷(Golden Circuits)[34]이나 관련 시뮬레이션 데이터가 확보되어 비교가 가능한 경우에 활용할 수 있는 방법이다. 여기서 골든 서킷이란 트로이목마가 포함되지 않은 회로를 의미하는 것으로 비교를 통해 트로이목마의 설치 여부를 확인해 볼 수 있는 회로를 말한다.

Hossain[30]은 전력 분석에 기반하여 트로이목마를 탐지하는 세 가지 기법을 제안하였는데, 이들 기법의 가장 핵심적인 사항은 IC칩의 악성행위 탐지를 위해 서킷 분할 기반 전력 사이드 채널 분석이다. 여기서 세 가지 방법은 골든 칩을 이용한 스캔 분할 방법론(Scan Segment Methodology)과 골든 칩 없이 분할된 세그먼트 상의 동일 전력 사용 세그먼트를 비교하는 EP(Equal-Power Self-referencing) 및 2개의 동일 세그먼트 페어를 만들고 이를 비교하는 EPN(Equal-Power Neighboring Self-referencing)으로 트로이목마의 탐지 효율을 증대시켰다.

온도를 이용한 트로이목마 탐지 방법으로는 참고문헌 [31,35] 등이 있는데, 특히 참고문헌 [35]는 골든 칩 없이 분석 대상 칩에 대하여 정지 상태의 온도 지도와 GDSII[36] 파일에서 얻을 수 있는 실행상태의 온도 지도를 활용한 하드웨어 트로이목마 탐지 방법을 제안하였다.

최근에는 기계학습을 이용한 하드웨어 트로이목마 탐지기술이 제안되고 있다. Vashistha는 골든 칩의 GDSII 레이아웃과 점검 대상의 원자현미경 이미지를 비교하여 악의적으로 변조한 회로를 찾아내는 방안을 제안하였다[37]. 이는 기존에 제안된 다양한 하드웨어 트로이목마 탐지 방법에 적용될 수 있을 것으로 예상된다.

V. 결론

정보화 시대의 도래로 다양한 영역에 IT 기술이 접목되면서 항공, 산업, 국방, 사회 간접 시설 등 매우 중요한 부분에 정보 시스템과 IT 기술이 활용되기 시작하였다. 정보 시스템에서 사용하는 각종 소프트웨어와 하드웨어는 다양한 공급의 단계를 통해 전달되는데, 이를 통칭하여 공급망이라 한다.

정보통신 환경에서는 다양한 보안 위협이 존재하는데, 이에 대응하기 위한 기술개발 역시 지속적으로 이루어져 왔다. 그러나 공급망 차원에서의 위협과 이에 대한 공격에 대해서는 확실한 대응이 매우 어려운 것이 현실이다.

특히 하드웨어 공급망 위협의 경우, IC칩에 공격 회로를 심거나, 칩 자체를 교체하는 등 직접적인 하드웨어에 대한 공격으로 납품 이후에는 공격 탐

지도 차단도 매우 어렵게 된다. 본고에서는 이러한 하드웨어 공급망 공격의 대표적인 경우인 하드웨어 트로이목마의 공격 사례와 대응 기술 동향에 대해 정리해 보았다.

하드웨어 트로이목마는 IC칩 내에 악성 행위를 수행하는 회로를 추가하여, 특정 조건에서 발동되도록 구현된 악성 회로로 단순하게는 조합 트로이목마와 순차 트로이목마 그리고 아날로그 트로이목마로 구분되기도 하며, 좀 더 세부적으로는 트로이목마가 칩에 삽입되는 단계, 트로이목마의 실질적인 구현 레벨, 활성화 방법, 공격 목적, 트로이목마의 운영 위치 등으로 구분하기도 한다.

하드웨어 트로이목마를 탐지하기 위한 기술로 칩으로 구현된 후의 탐지와 구현되기 전의 탐지 방법에 대해 언급하였으며, 구현된 후 탐지 방법은 파괴적 탐지 방법과 비파괴적 탐지 방법으로 구분하였다. 파괴적 탐지 방법은 리버스 엔지니어링이 있으며, 비파괴적 탐지 방법에는 기능 테스트와 사이드 채널을 이용하는 방법이 있는데, 사이드 채널은, 특히 온도, 지연시간, 전력사용량 및 방사선 촬영을 이용한 이미지 비교 등의 방법이 있었다.

하드웨어 트로이목마는 앞으로 더욱 정교한 방법으로 공격이 발전할 것으로 예상되나 이에 대한 효과적인 탐지와 대응 기술 개발은 부족한 현실이다. 이를 극복하기 위한 기술 개발 방안에 대하여 심도 있는 연구가 추진되어야 할 것이다.

용어해설

IP(Intellectual Property) IC칩 설계에서 말하는 IP는 재이용이 가능한 기능 블록을 지칭하는 것으로 하드웨어 또는 소프트웨어 기능 블록을 의미함

익스플로잇 코드 시스템의 취약점을 활용하여 공격자가 원하는 악성 행위를 수행하게 하는 실행 코드

GDSII 형식 집적회로(integrate circuit) 또는 IC-layout artwork의 데이터 교환을 위한 산업 표준 데이터베이스 파일 형식

약어 정리

CSP	Conditional SAF Pattern
DFT	Design-For-Test
EOFM	Electro-Optical Frequency Mapping
EP	Equal-Power Self-referencing
EPN	Equal-Power Neighboring Self-referencing
GDS	Graphic Design System
IC	Integrated Circuit
IP	Intellectual Property
SAF	Stuck-At-Fault

참고문헌

[1] 김대원 외, "공급망 보안기술동향," 전자통신동향분석, 제35권 제4호, 2020, pp. 149-157.

[2] W. Hu et al., "Detecting hardware Trojans with gate-level information-flow tracking," Computer, vol. 49, no. 8, 2016, pp. 44-52.

[3] Bloomberg Businessweek, "The big hack: How china used a tiny chip to infiltrate us companies," 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

[4] 이응규, 김정덕, "ICT 공급망 공격 사례 연구," 정보화연구, 제16권 제4호, 2019, pp. 383-396.

[5] Mail Online, "Man pleads guilty in counterfeit sub parts case," June 3, 2014, http://www.dailymail.co.uk/wires/ap/article-2647551/Man-pleads-guilty-counterfeit-sub-parts-case.html

[6] Ars Technica, "Your USB cable, the spy: Inside the NSA's catalog of surveillance magic," Dec, 31, 2013, Available from: https://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/ [Retrieved Jan. 22, 2017].

[7] CISA, "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-forinformation-and-communication-technology.pdf

[8] ZDNet, "Researchers find backdoor on ZTE android phones," May 15, 2012, Available from: https://www.zdnet.com/article/researchers-find-backdoor-on-zte-android-phones/ [Retrieved Jan. 22, 2017].

[9] CNBC, "Hackers could access US weapons systems through

chip," June 8, 2012, https://www.cnbc.com/id/47700647

[10] BBC, "Russia: Hidden chips 'launch spam attacks from irons'," Oct. 28, 2013, https://www.bbc.com/news/blogs-news-from-elsewhere-24707337

[11] Tom's Hardware, "Hacker finds hidden 'god mode' on Old x86 CPUs," Aug. 10, 2018, https://www.tomshardware.com/news/x86-hidden-god-mode,37582.html

[12] ITWorld, "사이버 보안 전망: 2019년과 그 이후," 2018. 12. 17, https://www.ciokorea.com/news/113286

[13] Trend Micro, "Trend micro security predictions for 2020," 2019. 11. 19, https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020

[14] J.P. Dunning, "Building Trojan hardware at home," BlackHat Asia, 2014, https://www.blackhat.com/docs/asia-14/materials/Dunning/Asia-14-Dunning-Building-Trojan-Hardware-At-Home.pdf

[15] R. Karri et al., "Trustworthy hardware: Identifying and classifying hardware Trojans," Computer, vol. 43, no. 10, 2010, pp. 39-46.

[16] A. Jain, Z. Zhou, and U. Guin, "Survey of recent developments for hardware Trojan detection," in Proc. IEEE Int. Symp. Circuits Sys. (ISCAS), (Daegu, Korea), May 2021, pp. 1-5.

[17] K. Yang et al., "A2: Analog malicious hardware," in Proc. Symp. Secur. Priv. (SP), (San Jose, CA, USA), May 2016, pp. 18-37.

[18] C. Kison et al., "Security implications of intentional capacitive crosstalk," IEEE Trans. Inf. Forensics Secur. vol. 14, no. 12, 2019, pp. 3246-3258.

[19] J.A. Roy, F. Koushanfar, and I.L. Markv, "Ending piracy of integrated circuits," Computer, vol. 43, 2010, pp. 30-38.

[20] K. Vaidyanathan, B.P. Das, and L. Pileggi, "Detecting reliability attacks during split fabrication using test-only BEOL stack," in Proc. Annu. Design Autom. Conf. June 2014, (San Francisco, CA, USA), pp. 1-6.

[21] R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," in Cryptographic Hardware and Embedded Systems-CHES, Springer, Berlin, Heidelberg, Germany, 2009, pp. 363-381.

[22] S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Morgan Kaufmann Publishers, Burlington, MA, USA, 2021.

[23] Z. Zhou, U. Guin, and V.D. Agrawal, "Modeling and test generation for combinational hardware Trojans," in Proc. IEEE VLSI Test Symp. (San Francisco, CA, USA), Apr. 2018.

[24] J. Cruz et al., "An automated configurable Trojan insertion framework for dynamic trust benchmarks," in Proc. Des., Autom. Test Eur. Conf. Exhibition, (Dresden, Germany), Mar. 2018, pp. 1598-1603.

[25] H. Salmani, "COTD: Reference-free hardware Trojan detection and recovery based on controllability and observability in gate-level netlist," IEEE Trans. Inf. Forensics Secur. vol. 12, no. 2, 2016, pp. 338-350.

[26] M. Nourian, M. Fazeli, and D. Hely, "Hardware Trojan detection using an advised genetic algorithm based logic testing," J. Electron. Testing, vol. 34, 2018, pp. 461-470.

[27] X. Xie et al., "Hardware Trojans classification based on controllability and observability in gate-level netlist," IEICE Electron. Expr. vol. 14, no. 18, 2017, pp. 1-12.

[28] M. Bushnell and V. Agrawal, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits, vol. 17, Springer, Boston, MA, USA, 2004.

[29] A. Stern et al., "SPARTA-COTS: A laser probing approach for sequential Trojan detection in COTS integrated circuits," in Proc. IEEE Int. Conf. on Phys. Assur. Inspection Electron. (PAINE), (Washington, DC, USA), Dec. 2020.

[30] F.S. Hossain et al., "Variation-aware hardware Trojan detection through power side-channel," in Proc. Int. Test Conf. (ITC), (Phoenix, AZ, USA), Nov. 2018, pp. 1-10.

[31] J. Zhong and J. Wang, "Thermal images based Hardware Trojan detection through differential temperature matrix," Optik, vol. 158, 2018, pp. 855-860.

[32] X. Cui et al., "Hardware Trojan detection using the order of path delay," J. Emerg. Technol. Comput. Syst. (JETC), vol. 14, no. 3, 2018, pp. 1-23.

[33] J. He et al., "Hardware Trojan detection through chip-free electromagnetic side-channel statistical analysis," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. vol. 25, no. 19, 2017, pp. 2939-2948.

[34] F.S. Hossain et al., "Detecting hardware Trojans without a Golden IC through clock-tree defined circuit partitions," in Proc. IEEE Eur. Test Symp. (ETS), (Limassol, Cyprus), May 2017, pp. 1-6.

[35] Y. Tang et al., "Golden-chip-free hardware Trojan detection through quiescent thermal maps," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. vol. 27, no. 12, 2019, pp. 2872-2883.

[36] Calma, GDS II Graphic Design System User's Operating Manual, 1st ed., 1978, Available from: http://www.bitsavers.org/pdf/calma/GDS_II_Users_Operating_Manual_Nov78.pdf [Retrieved Apr. 21, 2020].

[37] N. Vashistha et al., "Trojan scanner: Detecting hardware Trojans with rapid SEM imaging combined with image processing and machine learning," in Proc. Int. Symp. Testing Failure Anal. (ISTFA), 2018, p. 256.