Journal of the KNST

2020; Vol.3, No.2; pp. 113-117

ISSN: 2635-4926

https://doi.org/10.31818/JKNST.2020.09.3.2.113

Received: 2020/06/24
Revised: 2020/07/09
Accepted: 2020/08/17
Published: 2020/08/31

*Corresponding Author:
Taekyoung Kwon
Tel: +82-2-2123-4523
E-mail: taekyoung@yonsei.ac.kr

FPGA 기반 임베디드 시스템의 사이버 보안 위협 동향 분석

A Study of Cyber Security Threat Analysis on FPGA-based Embedded Systems

정세연[1], 조민기[2], 황은비[1], 권태경[3*]

[1]연세대학교 정보대학원 석사과정
[2]연세대학교 정보대학원 통합과정
[3]연세대학교 정보대학원 정교수

Seyeon Jeong[1], Mingi Cho[2], Eunbi Hwang[3], Taekyoung Kwon[*]

[1]Master course student, Information Security Lab, GSI, Yonsei University
[2]Integrated M.S/Ph.D course student, Information Security Lab, GSI, Yonsei University
[3]Professor, Information Security Lab, GSI, Yonsei University

Abstract

FPGA(Field Programmable Gate Array)는 하드웨어 및 소프트웨어의 장점을 가진 필드 프로그래밍과 재구성이 가능한 집적회로이다. 따라서 FPGA는 개발시간이 짧으며, 오류의 재수정이 가능하고, 초기 개발비가 저렴하다는 장점이 존재한다. 이러한 장점을 가진 FPGA는 임베디드 시스템 설계에서 중요하게 여겨지고 있으며, 오늘날 FPGA는 군사 시스템, 무기체계, 항공 우주 등에서 사용되고 있다. FPGA의 설계는 하드웨어 제조사, 서드파티 IP (intellectual property) 제공자, 위탁(outsourcing) 업체 등과 함께 이루어진다. 여러 경로를 통하여 설계가 진행되기 때문에 FPGA 기반 임베디드 시스템 생태계에서는 각 절차마다 악의적인 목적을 가진 공격자가 HT를 삽입할 가능성이 존재한다. 본 논문에서는 FPGA 기반 임베디드 시스템을 대상으로 이루어지는 보안 위협을 식별하고 동향을 분석해보고자 한다.

Field programmable gate array (FPGA) is field-programmable and reconfigurable integrated circuits, aiming at both hardware and software advantages. Therefore, the FPGA has the advantages that the development time is short, errors can be corrected, and the initial development cost is low. FPGAs with these advantages are considered important in embedded system design, and are used in various fields such as military systems, weapon systems, and aerospace. FPGA based embedded systems are designed with hardware manufacturers, third-party IP (intellectual property) providers, and outsourcing companies. Since multiple parties cooperate in the development, there is a possibility that a malicious attacker in an arbitrary party could inject the hardware trojan. In this paper, we identified and analyzed security threats targeting FPGA-based embedded systems.

Keywords

프로그래머블 반도체(Field Programmable Gate Array, FPGA),
하드웨어 보안(Hardware Security)
하드웨어 트로이목마(Hardware Trojan)

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD190016ED).

본 논문은 해군과학기술학회 2020년 춘계학술대회 발표논문을 기반으로 작성되었습니다.

1. 서론

FPGA(field programmable gate array)는 빠른 개발과 함께 초기 기술 비용이 적으며, 추가 비용이 반복적으로 발생하지 않는다는 소프트웨어의 일부 장점과 성능, 전력 효율이 높다는 하드웨어의 장점을 결합한 장치이다. 이러한 장점으로 인해 임베디드 시스템(embedded system) 설계에 있어 FPGA는 특히 라우팅, 신호 처리 또는 암호화 같은 대량 처리가 필요한 응용프로그램에서 중요하게 여겨진다. FPGA는 은행 업무, 군사 시스템, 항공 우주, 또는 비디오 신호처리 (예를 들어, HDTV 또는 네트워크 라우팅)와 같은 다양한 분야에서 사용된다.

FPGA는 하드웨어 제조사, 서드파티 IP 제공자, 위탁업체 등에 의해 하드웨어 설계가 이루어진다. 이러한 경로를 통하여 설계가 진행되기 때문에 FPGA의 개발 및 배포 단계에서 악의적인 목적을 가진 공격자가 HT (hardware trojan)를 삽입할 가능성이 존재한다. 만약 FPGA를 대상으로 공격이 이루어진다면 실제 사용 중인 시스템에 서비스 중지와 같은 피해를 입을 수 있다. 따라서 본 논문에서는 FPGA를 대상으로 이루어질 수 있는 위협을 분석하고 대비하기 위해 FPGA 기반 임베디드 시스템의 사이버 보안 위협 동향에 대하여 분석하였다.

2. 배경 기술

2.1 HT (hardware trojan)

HT는 하드웨어에 삽입되는 트로이 목마를 지칭한다. 하드웨어 회로에 은밀하게 삽입되는 HT는 현대 시스템의 안전과 보안에 심각한 위협이 된다. HT는 설계된 하드웨어 내에 숨겨져 있는 구성요소로서 겉보기에는 특정 작업을 수행하는 것처럼 보이지만, 실제로는 악의적인 목적을 갖고 숨겨진 작업을 수행하게 된다. 하드웨어 설계의 복잡성이 증가함에 따라 우리나라에서 제작된 IP뿐만 아니라, 해외에서 수입된 IP를 사용하는 등 설계 및 제조 프로세스의 세계화가 이루어졌다. 하지만, 이에 따라 HT가 신뢰할 수 없는 공급자, IP (intellectual property) 및 해외 파운드리(off-shored foundries)에 의해 삽입될 수 있으므로 이 위협의 심각성이 증가하였다.

2.2 FPGA 기반 임베디드 시스템 생태계

(1) 개발/생산 단계: 임베디드 시스템에 탑재될 펌웨어를 만들기 위하여 개발자가 개발 도구를 사용하여 코딩을 통해 펌웨어를 개발하고 생성하는 단계를 나타낸다. 펌웨어 제작을 위한 소스의 코딩 및 빌드 과정을 통해 펌웨어 생성이 이루어지게 된다. 또한 개발 과정 중에 외부 라이브러리가 필요할 경우, 3PIP (third party intellectual property)를 제공받아 사용할 수 있다. 여기서 3PIP란 필요할 때 사용할 수 있게 제3자가 사전에 구현해놓은 라이브러리, IP core 등을 말한다. 이후 3PIP 제공자로부터 제공받은 라이브러리와 개발한 소스가 함께 합쳐져 합성 또는 컴파일 과정을 통해 펌웨어 파일의 생성이 이루어진다. 생성된 펌웨어를 임베디드 시스템에 탑재할 경우, 펌웨어를 동작시킬 수 있게 된다. FPGA에서 이러한 펌웨어 파일을 비트스트림(bitstream)이라고 지칭한다.

(2) 설치 단계: 개발 단계에서 생산된 펌웨어는 임베디드 시스템이 필요한 곳에 전파되고, 임베디드 시스템에 펌웨어 탑재, 즉 설치가 이루어지게 된다.

(3) 운용/관리 단계: 설치된 임베디드 시스템을 안전하고 원활하게 관리하기 위해 지속적인 유지 보수가 이루어지게 되는데, 이를 운용/관리 단계라고 한다.

2.3 FPGA 기반 임베디드 시스템 개발 절차

FPGA 기반의 임베디드 시스템 개발 절차는 Fig. 1과 같다. FPGA 개발자는 먼저 HDL(hardware description language)로 회로를 설계한 다음, Xilinx Vivado, 또는 Intel Quartus와 같은 FPGA 설계 소프트웨어(design software)를 사용하여 구성 정보를 포함하는 비트스트림 파일을 생성한다[1]. 예를 들어, Xilinx Vivado를 사용하기 위해 HDL은 합성(synthesis) 과정을 수행하여 Xilinx 고유의 넷리스트 파일인 NGC 파일로 변환된다. 그 후, 이것은 전체 설계를 가지는 NGD(native generic database) 파일로 변환된다. 이 NGD 파일은 물리적 설계를 가지는 NCD(native circuit description) 파일로 매핑(mapping) 된다. 이 NCD 파일은 실제 대상 디바이스를 대상으로 배치 및 배선(place & route) 과정을 거쳐 최종적으로 비트스트림 파일로 변환된다.

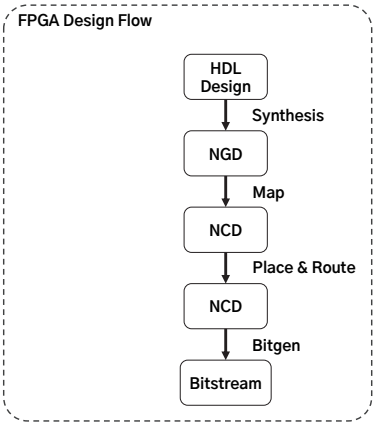

Fig. 1. FPGA development step

2.4 DPR(dynamic partial reconfiguration)

FPGA는 펌웨어의 일부만 수정 가능하다는 장점이 존재한다. 이러한 기능을 제공하기 위해서 Fig. 2와 같은 구조를

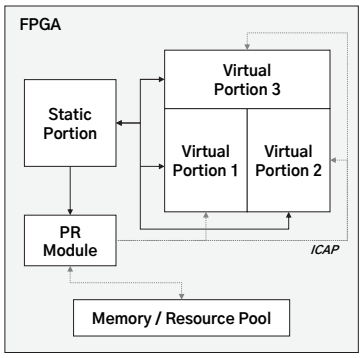

Fig. 2. FPGA system model

가진다. 여러 작업을 병렬로 실행하기 위해 FPGA는 여러 VP(virtual portion)로 나뉜다. 각각의 VP는 다른 VP의 운영에 영향을 주지 않고 독립적으로 작동할 수 있다. 각각의 VP조차도 다른 VP의 지속적인 운영에 영향을 미치지 않으면서 런타임에 다른 기능으로 재구성(reconfiguration)할 수 있다[2]. 이를 DPR(dynamic partial reconfiguration)이라고 한다.

3. FPGA 기반 임베디드 시스템의 위협

3.1 FPGA의 위협 모델

Fig. 3은 FPGA 라이프 사이클의 일반적인 예를 고려하여 나타낸 FPGA 위협모델이다. 이는 FPGA의 전체 개발 과정 동안 HT가 삽입될 수 있는 것을 보여주며, 개발 단계뿐만 아니라 배포 단계 이후에도 악의적인 재구성 기능을 통하여 HT가 삽입될 수 있다. HT는 회로를 설계할 때 악의적인 설계 디자이너, 신뢰되지 않은 CAD tool 사용[3], 악의적인 3PIP 설계자에 의해 삽입 가능하며 개발된 비트스트림이 배포될 때 공격자에 의해 FPGA에 삽입될 수 있다. 또한 개발 단계에서 HT가 삽입되지 않더라도, PR(partial reconfiguration) 기능을 악용하거나, 배포된 비트스트림을 직접 수정하여 HT 삽입이 가능하다.

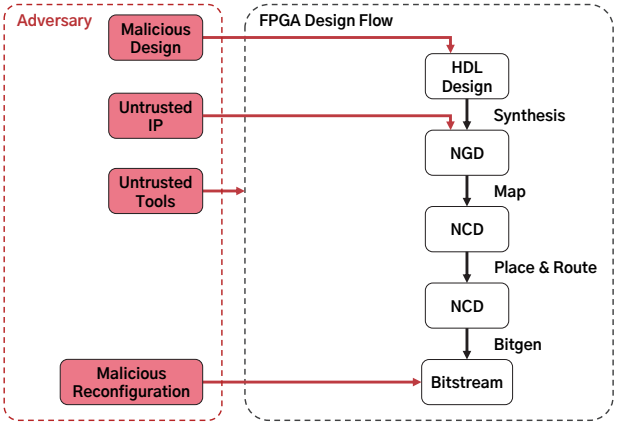

Fig. 3. FPGA threat model

3.2 FPGA 개발/생산 단계에서의 사이버 보안 위협

개발/생산 단계에서는 Fig. 4와 같이 개발과 생산에 관련된 신뢰되지 않은 설계 도구, 신뢰되지 않은 개발자, 신뢰되지 않은 3PIP 제공자, 신뢰되지 않은 SoC 통합자 모두가 공격자가 될 가능성을 지니고 있다.

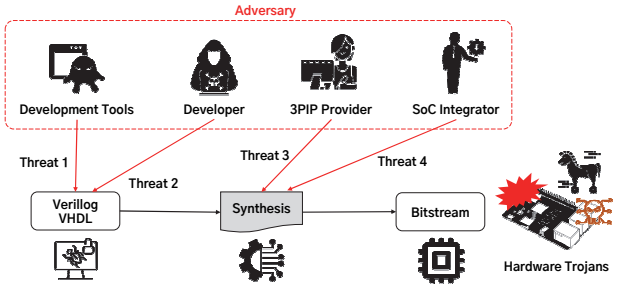

Fig. 4. Threats in development and production phase

(1) 신뢰되지 않은 설계 도구: FPGA 장비에 탑재될 비트스트림을 생성하기 위해서는 개발 도구를 사용하게 된다. 그러나 만약 정상적인 소프트웨어가 아닌 악의적인 소스를 삽입하는 개발 도구일 경우, 개발자도 모르게 정상적인 소스 코드에 HT가 삽입되어 배포될 가능성이 존재한다.

(2) 신뢰되지 않은 개발자: FPGA 개발자들은 FPGA 장비에 탑재될 비트스트림을 생성하기 위하여 비트스트림의 기능을 구성하는 소스 코드를 작성한다. 만약 개발자들 중에서 일부 개발자가 부정 거래 등을 통해 금전적 이익을 취하려고 하거나 기타 악의적인 목적을 가졌을 경우, 다른 개발자들 모르게 정상적인 소스 코드에 HT를 삽입하여 배포할 가능성이 존재한다.

(3) 신뢰되지 않은 3PIP 제공자: FPGA 비트스트림을 생성할 때 개발상의 편의를 위해 3PIP를 제공받아 사용하는 경우가 존재한다. 이때 만약 3PIP 제공자가 부정 거래 등을 통해 금전적 이익을 취하려고 하거나 기타 악의적인 목적을 가지고 있을 경우, HT가 포함된 3PIP를 사용하여 생성된 비트스트림에 HT가 탑재될 가능성이 존재한다.

(4) 신뢰되지 않은 SoC 통합자: FPGA 장비에 탑재될 비트스트림을 생성하기 위해서는 개발 툴을 사용한 소스 코드 작성 이후에 합성 과정이 이루어지게 된다. 그러나 만약 SoC 통합자가 부정 거래 등을 통해 금전적 이익을 취하려고 하거나 기타 악의적인 목적을 가졌을 경우, 합성 과정에서 HT가 포함된 새로운 IP를 만들거나 기존의 IP를 수정하여 HT를 삽입할 가능성이 존재한다.

이와 같이 개발/생산 단계에서 설계 도구, 개발자, 3PIP 제공자, SoC 통합자 등의 위협 요소에 의하여 HT가 비트스트림에 삽입될 경우, HT가 삽입되었는지 모른 채 FPGA에 설치가 이루어질 것이다. 만약 비트스트림이 설치된 장비

가 테스트 장비가 아닌 실제 운행 중인 비행기, 군함이나 상용 임베디드 시스템, 무기체계라면 HT가 트리거되어 동작할 경우 많은 피해가 발생할 것이며, 자칫 큰 인명 피해로 이어질 수도 있다.

3.3 FPGA 설치 단계에서의 사이버 보안 위협

설치 단계에서는 Fig. 5와 같이 부채널 공격으로 인한 사이버 보안 위협이 발생할 수 있다. 부채널 공격은 암호 구현에서의 물리적인 상태 정보를 활용하여 암호화 기술을 무력화시키는 방법을 말한다.

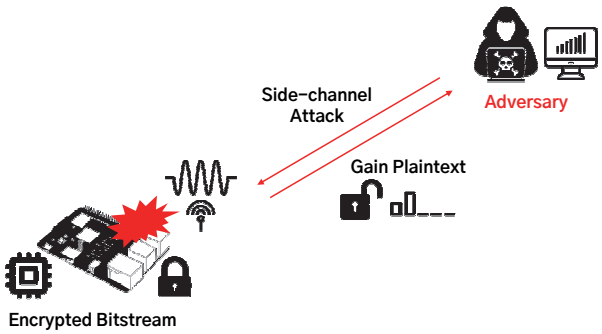

Fig. 5. Threats in installation phase

FPGA는 전원이 들어올 때 비트스트림에 저장되어 있는 프로그래밍된 회로 설정을 불러와서 회로를 구성한다. 그러나 내부 비휘발성 메모리가 존재하지 않는 경우, 외부에서 비트스트림을 불러와서 회로를 구성하게 된다. 이때 비트스트림은 정보가 유출되는 것을 방지하기 위해 암호화된 상태로 전송된다. 이때 공격자는 비트스트림의 회로 정보를 분석하고 HT를 삽입하기 위하여 부채널 공격을 통해 비트스트림의 복호화를 시도할 수 있다.

2011년 Moradi 등의 연구에서는 부채널 공격 방법 중 하나인 전력 분석 방법을 통해 하드웨어 장비가 사용하는 전력량을 측정하여 비밀키 추출에 활용 가능한 것을 보여주었다[4]. 전력 소비를 측정하여 전력 소비에 대한 모델을 생성하고 암호화 로직 수행 시 수집된 데이터들에 대한 통계적 분석을 수행하여 암호화 키를 추출하는 방법인 차분 전력 분석을 이용하여 Xilinx FPGA와 Intel Altera FPGA 상의 DES, AES 복호화 로직을 대상으로 암호화 키를 추출하는 것이 가능하다는 것을 증명하였다.

이렇듯 전력 분석과 같은 전력 소모량의 변화를 통하여 FPGA의 복호화 로직을 대상으로 암호화키 추출이 가능하다. 공격자는 이와 같은 방법으로 암호화키를 추출한 후 비트스트림을 복호화하여 HT를 삽입 가능할 것이다.

3.4 FPGA 운용/관리 단계에서의 사이버 보안 위협

운용/관리 단계에서는 Fig. 6과 같이 원격 DPR 기능으로 인한 사이버 보안 위협이 발생할 수 있다. FPGA는 선 배포 후에 비침습 방식으로 수정이 가능한 DPR 기능을 갖고 있다. DPR 기능이 최근에 이르러 IoT 기반 및 임베디드 시스템 보안 어플리케이션의 맥락에서 봤을 때 네트워크를 통해 수행하는 것이 거의 필수적이게 되었다. 즉, 기존에는 내부적으로 DPR 기능을 통해 비트스트림을 수정하였으나 이제는 Fig. 7과 같이 외부에서 원격으로 DPR 기능을 통해 비트스트림 수정이 가능하다[5].

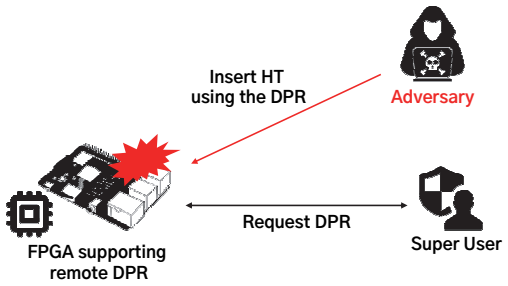

Fig. 6. Threats in operation and management phase

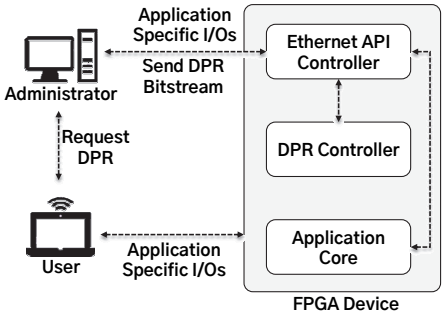

Fig. 7. FPGA supporting remote DPR

원격 DPR의 기본적인 장점은 물리적 접근 없이 여러 장치가 서로 원격으로 통신하여 여러 FPGA 기반 기능 모듈의 기능을 조절할 수 있다는 것이다. 이를 통해 임베디드 시스템 환경에서 동시에 작동하는 방대한 장치 네트워크를 보다 효율적으로 연결하고 관리할 수 있다. FPGA가 네트워크에 연결된 사용자 그룹의 모든 사용자에게 제공하는 서비스 중 하나는 네트워크 연결을 통해 전송된 일반 텍스트의 실시간 개인 키 암호화이다. 암호화 키는 암호 하드웨어 코어에 하드 코딩되거나 FPGA가 접근할 수 있는 안전한 온보드 메모리 모듈에 저장된다. FPGA는 DPR을 지원하며, 이는 FPGA에서 기존 회로의 기능을 추가하거나 수정하는데 활용될 수 있다.

보안적인 요소를 고려하여 원격 DPR 기능은 일반 사용자가 아닌 기능이 허가된 특정 사용자만이 사용할 수 있으며, DPR 시도가 로그로 기록되고 있을 것이다. 따라서 악의적인 사용자는 자신의 존재를 밝히지 않고 FPGA를 임의로 수정하는 것이 불가능하다. 그러나 만약 악의적인 공격자가 금전적 이익을 취하려고 하거나 기타 악의적인 목적을 가지고 장기간으로 접근하여 DPR 작업이 승인될 때까지 기다릴 경우, HT를 삽입할 가능성이 존재한다.

2017년 Johnson 등의 연구에서는 비트스트림 수정 및 재구성(reconfiguration) 기능을 활용하여 HT 삽입이 가능하다는 것을 제안하였다[5]. 이외에도 사전에 DPR 기능을 사용하여 트리거 가능하도록 HT를 탑재하였을 경우, 허가된 악의적인 사용자가 원격으로 HT를 동작시켜 피해를 유발할 가능성이 존재한다. 이 경우에는 트리거 시 오버헤드를 줄일 뿐만 아니라 실용적이며 HT를 사전에 탐지하기가 더욱 어려울 것이다.

4. 결론

본 논문에서는 FPGA 기반의 임베디드 시스템에 대한 사이버 보안 위협 동향에 대하여 분석하였다. FPGA는 현재 금융, 방위, 항공 우주 등 많은 곳에서 사용되고 있으며, 점점 보편화되어 가는 만큼 보안에 대해서도 관심을 가져야 할 필요가 있다. 앞서 설명한 위협 외에도 FPGA 대상의 사이버 보안 위협이 다양하게 존재할 것이다. 이러한 보안 위협을 막기 위해서는 사용 중인 기능에 대한 분석을 통해 반드시 필요한 기능만 사용하고, HT 탐지를 위한 활발한 연구가 진행되어야 할 것이다.

참고문헌

[1] Note, J. B., Rannaud, É., "From the Bitstream to the Netlist," the International Symposium on Field-Programmable Gate Arrays (FPGA), Vol. 8., 2008. pp. 264-264.
[2] Guha, K., Majumder, A., Saha, D., Chakrabarti, A. "Reliability Driven Mixed Critical Tasks Processing on FPGAs Against Hardware Trojan Attacks," In 2018 21st Euromicro Conference on Digital System Design (DSD). IEEE, 2018. pp. 537-544.
[3] Rajendran, J. J., Sinanoglu, O., Karri. R., "Building trustworthy systems using untrusted components: A high-level synthesis approach," IEEE Transactions on Very Large Scale Integration (VLSI) Systems 24.9, 2016. pp. 2946-2959.
[4] Moradi, A., Barenghi, A., Kasper, T., Paar, C. "On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs," Proceedings of the 18th ACM conference on Computer and communications security. 2011.
[5] Johnson, A. P., Patranabis, S., Chakraborty, R. S., Mukhopadhyay, D., "Remote dynamic partial reconfiguration: A threat to Internet-of-Things and embedded security applications," Microprocessors and Microsystems, 52, 2017. pp. 131-144.