보안을 위한 프로세서 기술 동향

김지훈
서울과학기술대학교
전기정보공학과

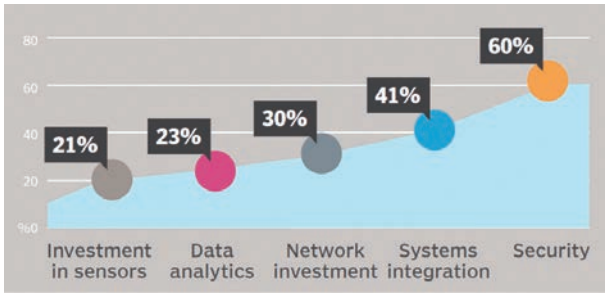
김동규
한양대학교
융합전자공학부

Ⅰ. 서 론

지난 수십여년간의 눈부신 컴퓨터 시스템의 발전에 힘입어 전 세계는 이제 디지털, 인공지능, 산업용 로봇등이 많은 주목을 받고 있는 제4차 산업혁명의 시기를 맞이하고 있다. 고성능 프로세서 및 메모리, 그리고 소프트웨어에 이르기까지 다양한 분야에서 컴퓨터 시스템은 끝없는 발전을 거듭해왔고 인터넷과 함께 전세계가 하나로 연결되며 현재에 이르렀다. 이와 같은 컴퓨터 시스템들은 PC (Personal Computer)의 형태에서 스마트폰의 형태로 최근 진화함에 따라 개인의 주요 정보를 다루는 일들이 보다 늘어나게 되었다. 모든 사물이 서로 연결되어 보다 나은 서비스를 제공해줄 것으로 기대되는 IoT (Internet of Things)는 이미 다양한 형태의 국내 이동통신사들의 서비스로 우리의 삶속에 자리 잡고 있으며, 향후 IoT 시대와 함께 사람 주변의 더욱 많은 사물들이 내부의 프로세서와 함께 인터넷에 연결될 것으로 예상됨에 따라 〈그림 1〉에서 나타난 것과 같이 그 어느때보다 보안의 중요성이 더욱 높아지고 있다[1]. 특히, 자동차 및 헬스케어 시스템과 같은 경우는 사람의 생명과 직접적으로 연결될 수 있는 분야이기에 향후 점차 다양한 기능이 추가될 해당 분야에서의 보안은 전세계적으로 많은 주목을 받고 있다[2-3].

TEE (Trusted Execution Environment)를 하드웨어에 기반하여 격리실행을 수행하는 시스템은 학계와 산업계로부터 많은 주목을 받아왔으며, 현재 널리 사용되고 있다.

이와 같은 보안은 소프트웨어 수준에서부터 하드웨어 수준에 이르기까지 다양한 방식으로 진행되어왔으며, 대부분의 방식들은 중요 프로그램의 실행을 격리된 (isolated) 환경에서 진행하는 것으로 이루어져



〈그림 1〉 IoT에서 가장 큰 당면과제에 대한 조사 결과 (복수 응답 포함)[1]

〈그림 2〉 여러 공격에 대한 기본적인 대응방식

왔다. 소프트웨어 기반의 방식은 대부분 하이퍼바이저에 기반을 둔 가상머신의 형태로 구현된다. 하지만 이와 같은 방식들은 일반적으로 고성능 시스템에서 주로 사용되고, 성능 저하에 대한 부담을 갖고 있다는 단점을 지니고 있다[4]. 반면, TEE (Trusted Execution Environment)를 하드웨어에 기반하여 격리실행을 수행하는 경우에는 이와 같은 단점을 극복할 수 있다는 점에서 학계와 많은 프로세서 회사들의 주목을 받아왔으며, 그 결과물들이 현재 널리 사용되고 있다.

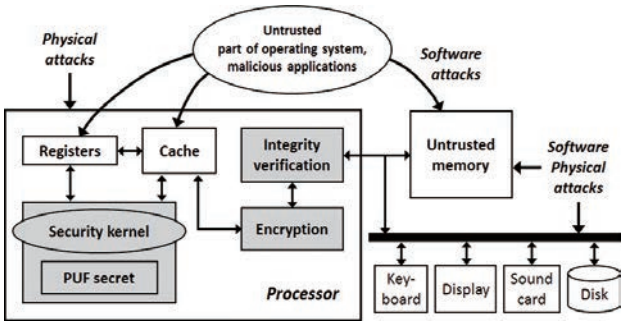
본 기고문에서는 이와 같은 TEE를 구성하기 위한 보안 프로세서들의 기술 동향에 대해서 소개하고자 한다. 이를 위해 2장에서는 기본적인 배경지식을 소개하고, 3장에서는 학계에서 연구된 대표 결과물들에 대해서 설명한다. 4장에서는 대표적인 프로세서 회사인 Intel과 ARM의 보안을 위한 프로세서 기술에 대해서 살펴보고, 5장에서 결론 및 연구방향으로 끝을 맺고자 한다.

Ⅱ. 배경 지식

본 기고문에서 다루는 보안은 하드웨어적으로 구성된 보안시스템의 반도체 칩에 대한 Micro-probing과 같은 Invasive Attack은 다루지 않고 있으며, 이와 같은 방법은 다양한 센서들을 통해서 방어한다고 가정한다. 세상에는 다양한 형태의 공격이 존재하기 때문에, 이를 고려하면 보다 유연하게 대처할 수 있는 소프트웨어 기반의 보안기법이 중요하지만 이와 같은 보안 소프트웨어 자체가 공격대상이 되는 경우가 많기에, 하드웨어 기반의 보안이 많은 주목을 받아오고 있다. 이와 같은 하드웨어 기반의 보안을 통해서 시스템은 정보의 기밀성 (Confidentiality), 무결성 (Integrity), 그리고 가용성 (Availability)을 유지하는 것이 주목적이다. 위의 〈그림 2〉에서 나타난 것과 같이 감시 및 도청과 같은 Passive Attack에는 정보를 암호화 (Encryption)하는 것을 통해서 보안을 유지하고, 위변조등을 행하는 Active Attack에 대해서는 인증 (Authentication)을 수행하여 보안을 유지하는 것이 가장 일반적인 방식이다. 이를 위하여 주로 대칭키 기반 암호 알고리즘들은 기밀성을 위해 많이 사용되고, Hash 함수들은 무결성를 위해서 많이 사용되며 공개키 기반의 암호 알고리즘들은 인증 및 전자서명 등에 주로 활용이 된다. 〈표 1〉은 이와 같은 부분을 고려하여 기존의 다양한 암호 관련 알고리즘들이 여러 목적에 따라서 사용되고 있음을 보여준다. 그리고 이와 같은 알고리즘에 적극적으로 활용이 되는 키 생성에는 RNG (Random Number Generator)와 PUF (Physical Unclonable Function)이 많이 사용이 되고 있고, 관련한

〈표 1〉 정보보안을 위한 다양한 알고리즘

Security Concept	Algorithm
Confidentiality	AES 3DES
Authenticity	SHA-1 SHA-2 AES CMAC GMAC
Confidentiality &	AES CCM
Authenticity	GCM
Digital Signatures	RSA DSA EC-DSA
Key Transport	AES-WRAP RSA
Key Agreement	DH EC-DH
Key Derivation	NIST IKEv2 TLS1.2 TLS1.0-1.1
Data At Rest Confidentiality	XTS-AES



〈그림 3〉 AEGIS의 전체 개념도

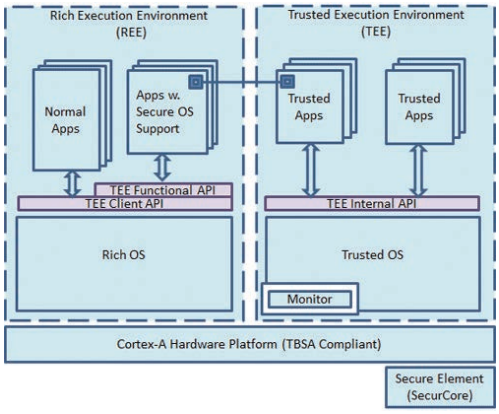
회로 구현에 대한 연구들이 활발히 진행 중이다[5].

본 기고문에서는 이와 같은 다양한 알고리즘과 RNG, PUF등의 구성요소들을 기반으로 하는 다양한 보안 프로세서의 동향에 대해서 다루고 있다.

Ⅲ. 보안프로세서 관련 연구 동향

이와 같은 하드웨어 기반의 보안시스템을 위하여 학계에서는 많은 연구가 진행되어왔다. XOM (eXecute Only Memory)방식은 off-chip 메모리로 나가는 데이터에 대해 항상 암호화 하고, MAC (Message Authentication Code)를 기반으로 무결성을 검증하는 기법을 제안하였으며, MIT에서 발표한 AEGIS는 이와 같은 개념을 포함한 전체 보안 프로세서의 구현까지 진행을 하였다[7]. 특히 〈그림 3〉에 나타난 것과 같이, AEGIS는 PUF에 대한 연구부터 시작을 하여 코드 및 데이터가 저장될 수 있는 모든 공간이 소프트웨어 공격에 노출되어있다는 가정 하에 보안을 위한 특수 명령어를 OpenRISC에 추가하여 전체 시스템을 구현하였다. 최근 해당 연구 그룹은 뒤에서 설명할 Intel의 SGX (Software Guard Extensions)의 문제점을 분석하고, 이를 고려하여 최소한의 기존 프로세서에 대한 수정만을 요구하면서 신뢰할 수 있는 security monitor software를 기반으로 하는 Sanctum이라는 프로세서를 발표하였고, Rocket RISC-V 코어를 기반으로 구현하였다[8]. 해당 연구들은 모두 Code Injection Attack 혹은 Code Reuse Attack등과 같은 문제를 일으키는 소프트웨어가 아니라는 가정을 담고 있으며, 이와 같은 공격들은 Stack 영역을 실행하지 못하게끔 MPU (Memory Protection Unit)에서 NX (Non eXecutable)비트를 기반으로 설정한다거나 프로그램의 실행 흐름이 정상적인지를 판단하는 방식으로 방어하고자 많은 연구들이 이루어지고 있다.

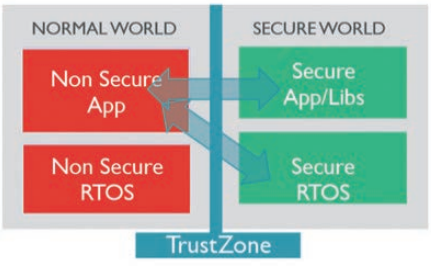
> ARM은 2015년 ARMv8-M 아키텍쳐를 통해 Cortex-M을 위한 TrustZone까지 확장된 기술을 발표하였다.



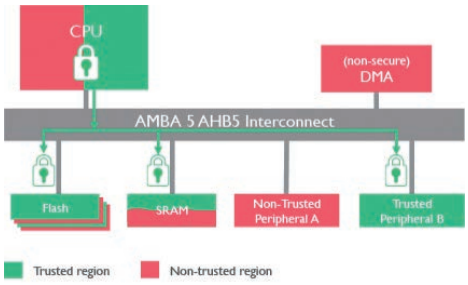
〈그림 4〉 ARM TrustZone 기반의 TEE 구현

Ⅳ. 산업계의 보안 프로세서 기술 동향

ARM 프로세서는 현재 대부분의 스마트폰에 채용되면서 전 세계 모바일 시장을 석권하고 있으며, 이에 걸맞게 TrustZone이라고 불리는 보안 기술을 함께 가지고 있다. TrustZone은 〈그림 4〉에서 보이는 것과 같이 일반 OS환경인 REE (Rich Execution Environment)와 TEE를 격리시킬 수 있는 하드웨어적인 기반과 소프트웨어 구성을 제공하며, 시스템상의 메모리뿐만 아니라 SoC



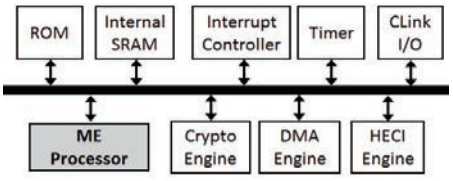
〈그림 5〉 ARMv8-M에서의 TrustZone



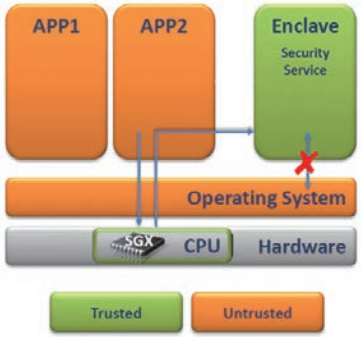
〈그림 6〉 AMBA AHB5를 통한 TrustZone 지원

(System-on-a-Chip)에 연결되는 여러 Peripheral들도 AMBA AXI Interconnect에 존재하는 NS (Non-Secure) 비트를 통해 REE에서 구동되는 Normal World와 TEE에서 구동되는 Secure World로 구분하여 각각 격리된 실행환경을 제공한다. 이와 같은 기존의 Cortex-A급 프로세서에만 제공되던 TrustZone은 2015년 공개된 ARMv8-M 아키텍처에서 〈그림 5〉 및 〈그림 6〉과 같이 마이크로컨트롤러에 주로 사용되는 AHB기반 Cortex-M을 위한 TrustZone으로 확장되었다. 특히, 여기서는 기존의 Cortex-A를 위한 TrustZone에서 Secure World에 존재했던 Monitor Mode가 없으며 Secure World와 Normal World사이의 전환이 적은 지연시간을 갖는 것이 특징이다. 이와 같은 전환은 Guard 명령어인 SG (Secure Gateway)를 통해서 이루어지며, 진입지점을 관리함으로써 보안성을 높인 것을 알 수 있다. ARM은 이와 같은 기술을 기반으로 기존의 스마트폰 시장에서의 확고했던 지위를 보안이 중요시되는 IoT시장에서도 Cortex-M을 토대로 다져나갈 것으로 판단된다. 하지만 이와 같은 TrustZone기반의 시스템은 Secure World에서 악의적인 프로그램이 수행가능하다는 단점을 지니고 있고, 최근 화웨이 HiSilicon 기기에서 이와 같은 취약성이 발견되었다[4].

Intel SGX을 통해 사용자 권한에서 동작하는 응용프로그램들은 Enclave를 기반으로 보다 안전한 실행 환경을 갖출 수 있다.



〈그림 7〉 Intel Management Engine 구조[4]



〈그림 8〉 Intel SGX 개념도[12]

Intel은 2000년대 초반 TPM (Trusted Platform Modules)라고 불리는 작은 보안 칩을 root of trust로 활용하였으며, 2007년에는 〈그림 7〉에 나타난 것과 같은 ME (Management Engine)이라는 프로세서를 통하여 보안을 강화하였다. ME는 컴퓨터의 모든 메모리와 네트워크, 그리고 모든 연결기기에 접근할 수 있으며 Intel AMT (Active Management Technology)를 구동하고, 최근 발표된 모든 Intel 프로세서에 내재되어 있다. 공식적으로 발표되지는 않았지만 Intel ME는 ARC, ARCompact, 그리고 SPARC v8 명령어 집합을 활용하는 것으로 파악되고 있으며 해당 코드들은 LZMA (Lempel-Ziv-Markov chain Algorithm) 혹은 Huffman encoding으로 압축되어있는 것으로 분석되고 있다[10]. AMD 역시 Intel의 ME와 유사한 기술을 ARM TrustZone에 기반을 둔 PSP (Platform Security Processor)라는 이름으로 보유하고 있다[11].

또한, Intel은 2013년 〈그림 8〉과 같이 SGX 기술을 통하여 사용자 권한에서 동작하는 응용프로그램들이 Enclave라 불리는 안전한 영역을 직접 관리함으로써, 새로운 명령어와 데이터구조를 기반으로 보다 높은 상위 권한을 가진 운영체제 혹은 악의적 의도를 지닌 공격자들로부터 자신을 안전하게 보호할 수 있는 실행 환경을 제공한다. Enclave는 코드와 데이터를 포함하는 프로세스 내의 TEE이며, 기밀성과 무결성을 제공한다. 그리고 2016년에는 기존의 SGX를 보완하여 Dynamic Memory

Management가 가능한 SGX2 관련 명령어와 함께 발표하였다[13]. Intel SGX는 cache timing attack 및 소프트웨어 부채널공격(Side-Channel Attack)에 취약성을 보이고 있다는 연구결과가 발표되었다[8].

Ⅴ. 향후 연구 및 결론

이상 살펴본 것과 같이, 향후 보안의 중요성이 더욱 증가할 것으로 예상됨에 따라 컴퓨터 시스템의 핵심적인 기능을 수행하는 프로세서와 관련하여 많은 보안 기술들이 연구되고 있고 이미 상용화 되고 있는 것을 알 수 있다. 기존의 PC 및 스마트폰 시장과는 달리, IoT는 굉장히 다양한 시스템이 존재할 것으로 예상되며 이에 따라 x86 및 ARM외에도 다른 프로세서기반 플랫폼도 시장에 진입할 수 있을 것으로 판단된다. 이와 같은 상황을 고려하여 국내에서도 보안 프로세서 설계 기술 확보를 위한 꾸준한 연구가 진행되어야 할 것으로 판단된다.

참고문헌

[1] "SearchNetworking 2015 Purchasing Intentions Survey," TechTarget, May 2015.

[2] 김호원, 김동규, "IoT 기술과 보안," 정보보호학회지, 22(1), 2012년 2월, 7-13.

[3] Rob Coombs, "Designing Security & Trust into Connected Devices," ARM Techcon 2015.

[4] Fengwei Zhang and Hongwei Zhang, "SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security," HASP 2016.

[5] Ruby B. Lee, "Security Basics," HotChips 2014.

[6] David Lie, et al., "Architectural Support for Copy and Tamper Resistant Software," ASPLOS 2000.

[7] G. Edward Suh, et al., "Design and Implementation of the AEGIS Single-Chip Secure Processor Using Physical Random Functions," ISCA 2005.

[8] Victor Costan, et al., "Sanctum: Minimal Hardware Extensions for Strong Software Isolation," Usenix Security Symposium, 2015.

[9] www.arm.com

[10] Igor Skochinsky, "Intel ME Secrets," RECON 2014.

[11] AMD TATS BIOS Development Group, "AMD Security and Server Innovation," UEFI Spring PlugFest, 2013.

[12] Victor Costan and Srinivas Devadas, "Intel SGX Explained," http://eprint.iacr.org/2016/086.pdf, 2016.

[13] Frank McKeen, et al., "Intel Software Guard Extensions (Intel SGX) SGX2," HASP 2016.

김지훈

- 2004년 2월 KAIST 전자전산학과 학사
- 2009년 8월 KAIST 전기 및 전자공학과 박사
- 2009년 7월~2010년 2월 삼성전자 DMC연구소 책임연구원
- 2010년 3월~2016년 2월 충남대학교 전자공학과 부교수
- 2016년 2월~현재 서울과학기술대학교 전기정보공학과 부교수

〈관심분야〉
SoC (System-on-Chip), 프로세서 설계, Security / Biomedical System

김동규

- 1992년 2월 서울대학교 컴퓨터공학과 학사
- 1994년 2월 서울대학교 컴퓨터공학과 석사
- 1999년 2월 서울대학교 컴퓨터공학과 박사
- 1999년 9월~2006년 2월 부산대학교 정보컴퓨터공학과 조교수
- 2006년 3월~현재 한양대학교 융합전자공학부 정교수

〈관심분야〉
보안 SoC 설계, Crypto-coprocessor 설계, 하드웨어 암호 IP 설계, 암호 및 보안 프로토콜 분석, 보안 알고리즘 설계 및 분석