ARM TrustZone을 이용한 보안 IPC의 설계

유성배○ 김세원 유시환 유혁
고려대학교 컴퓨터·전파통신공학과
{sbyoo, swkim, shyoo, hxy}@os.korea.ac.kr

Design of Secure IPC using ARM TrustZone

Sung-bae Yoo○ Se-won Kim See-hwan Yoo Chuck Yoo
Department of Computer and Radio Communications Engineering, Korea University

요 약

스마트폰과 같은 모바일 기기들의 사용이 점차 증가하고 있다. 이와 동시에 모바일 기기에 관련한 악성 코드 역시 가파르게 증가하고 있다. 모바일 기기의 기능이 복잡해지면서, 코드에 대한 검증이나, 악성코드에 대한 대처가 점점 힘들어지고 있다. 모바일 기기에 저장되는 개인정보는 점점 증가하고 있고, 특히 모바일 결제와 모바일 뱅킹과 같이 높은 신뢰성이 요구되는 애플리케이션의 수 또한 점차 증가하고 있다. 따라서 모바일 기기의 신뢰성은 점차 중요해지고 있다. 이를 위해 본 논문에서는 ARM사의 TrustZone extension을 이용하여 IPC(Inter Process Communication)에 대한 신뢰성을 어떻게 높일 수 있을지에 대해 논의하고, 신뢰성 있는 IPC를 제안하고자 한다.

1. 서 론

스마트폰과 같은 모바일 기기들의 사용이 점차 증가하고 있다. 그와 동시에 모바일 기기의 쓰임은 점차 다양해지고 모바일 기기의 기능은 점차 복잡해지고 있다. 이에 따라, 모바일 운영체제는 이미 데스크탑 운영체제 만큼이나 복잡해졌다[2]. 따라서 코드에 대한 검증이나 악성코드에 대한 대처는 점점 어려워지고 있다.

전자상거래, 전자지갑(예를 들어, Google Wallet) 등의 높은 신뢰성이 요구되는 애플리케이션은 점차 증가하고 있으며, 신뢰성 있는 모바일 애플리케이션의 중요성은 전보다 점차 커지고 있다[3]. 모바일 애플리케이션의 신뢰성을 지키기 위해서 보안이 필요한 요소들을 고립시키는 기법이 필요하다. 이를 위해서, 기존 운영체제에서는 샌드박싱 기법이 주로 사용이 된다. 하지만, Apple iOS jail-breaking[4]이나, Android Rooting[5]과 같은 경우를 봐도, 이러한 기법들은 쉽게 뚫릴 수 있으며, 안전하지 않다. 그러므로 운영체제를 신뢰하기 어렵다.

또한, 보안이 필요한 요소들을 단순히 하나의 공간에 고립시키는 것뿐만 아니라, 해당 요소들과 안전하게 통신할 수 있는 방법이 필요하다[2]. 보안이 필요한 애플리케이션끼리의 신뢰성 있는 통신은 다른 보안적인 요소들을 구성해나갈 수 있는 중요한 빌딩 블록(building block)이라고 할 수 있다[7]. 따라서, 신뢰할 수 있는 IPC(Inter Process Communication)는 보안상으로 안전한 시스템의 가장 기본적인 요소이다.

본 논문에서는 ARM TrustZone을 IPC에 적용하여, 신뢰성을 높이고자 한다. ARM TrustZone을 이용하여 IPC 코드와 데이터를 운영체제로부터 분리시키고, 어플리케이션이 사용할 때, 신뢰성을 보장할 수 있는 IPC를 제안하고자 한다.

2. 관련 연구

2.1. IPC의 신뢰성 향상

Dan R. K. Ports 등이 제안한 방법에서는 VMWare에서 Overshadow 기법을 사용하여, VMM(Virtual Monitor Manager)이 IPC로 사용되는 공유메모리의 내용을 운영체제가 읽거나 쓸 수 없게 함으로써, IPC의 신뢰성을 높였다[7]. L4droid에서는 안전한 스마트폰을 만들기 위해 안드로이드에 L4를 적용하였다. 안드로이드 IPC인 바인더를 검증된 L4 IPC로 대체함으로써, IPC의 신뢰성을 높였다[1].

2.2. IPC 공격 모델

Dan R. K. Ports의 논문에서는 악의적인 운영체제가 보안이 필요한 애플리케이션간의 IPC 메시지를 가로채거나 변조할 수 있다고 주장하였다[7].

일반적인 운영체제의 경우도 이러한 문제점을 가지고 있다. 악의적인 프로세스가 충분히 Rooting이나 Jail-breaking과 같은 기법을 통해 관리자 권한을 얻을 수 있다. 그리고 관리자 권한을 지니고 있으면, 부트 시퀀스를 수정하거나, 커널 모듈(또는 드라이버) 등을 로드하는 것이 가능하다[8]. 이러한 경우, 악성 코드를 커널과 동등한 권한으로 실행시킬 수 있다.

IPC 공격의 응용 예는 다음 두 가지로 나눌 수 있다.

IPC 메시지를 가로채는 공격에 대해서는 모바일 결제와 모바일 뱅킹과 같은 애플리케이션의 경우가 가장 대표적이다. 결제 암호화 모듈과 결제 창을 띄우는 애플리케이션이 서로 다른 프로세스로 이루어져 있을 경우, IPC 메시지를 중간에서 가로채서 결제정보를 획득할 수 있다.

IPC 메시지 변조에 대해서는 소프트웨어 라이선스 관

리가 대표적이며, 구글 플레이(Google Play)의 LVL (License Verification Library)을 예로 들 수 있다. LVL은 배포자의 애플리케이션에 포함되어 현재 사용자가 해당 애플리케이션의 라이선스를 가지고 있는지 여부를 판단한다. 라이선스 여부를 판단 할 때, LVL과 마켓 애플리케이션은 안드로이드의 IPC인 Binder로 통신하게 된다[9]. 이 때, IPC 메시지를 변조하여, 라이선스가 없음에도 라이선스가 있는 것처럼 하여 라이선스 테스트를 통과할 수 있다.

2.3. ARM TrustZone

ARM TrustZone은 하나의 물리 프로세서 코어를 secure과 normal의 두 가지 world로 나누어 준다. 각 world마다 CPU의 상태 및 페이지테이블 관련 레지스터는 banked 되어있으며, 주소 공간 역시 분리되어 있다. secure world에는 보안이 필요한 애플리케이션을, normal world에는 일반적인 애플리케이션을 고립시켜 실행할 수 있다.

메모리 접근을 제어하여, 메모리 영역을 고립시킬 수도 있다. TZASC(TrustZone Address Space Controller) 또는 TZMA(TrustZone Memory Adater)를 이용하여 secure world에서만 접근 가능한 메모리 영역을 지정할 수 있다. secure world에서만 접근 가능한 메모리 영역을 normal world에서 접근하였을 경우 monitor모드에서 TrustZone 페이지폴트가 발생하게 된다.

world간의 스위칭을 위해, CPU 모드[1]에 monitor모드가 추가되었다. monitor모드로의 진입은 SMC(Secure Monitor Call) 명령어가 실행된 경우나, IRQ 및 FIQ 발생시 이루어지게 된다. SMC 명령어는 kernel 모드에서만 실행이 가능하다[6].

3. TrustZone을 이용한 보안 IPC의 설계

3.1. 전체 구조

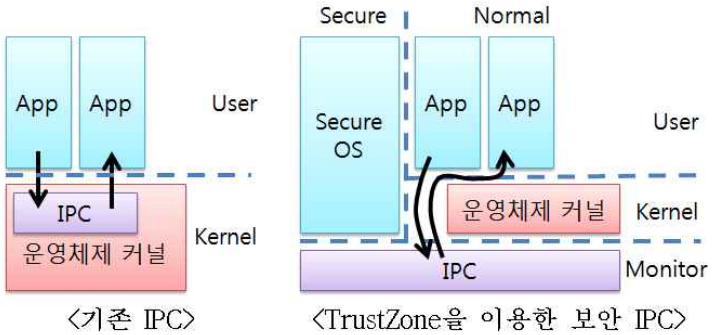

그림 1 본 논문에서 제안하는 IPC와 기존 IPC의 차이

기존의 IPC는 운영체제에서 제공해주는 형태이므로, IPC 메시지에 대한 공격에 대해 취약한 구조를 가지고 있다[7].

1) ARM의 CPU 모드에는 FIQ, IRQ, Abort, Kernel, User, Undefined가 있다.

본 논문에서 제안하는 TrustZone을 이용한 보안 IPC에서는 커널을 거치지 않고 바로 monitor모드에 있는 IPC를 이용하게 되므로 이러한 취약점을 개선할 수 있다.

3.2. IPC 메시지 송/수신

user모드에서는 SMC 명령어를 실행할 수 없으므로, kernel모드를 거치지 않고 monitor으 가기 위해서 TrustZone의 페이지폴트를 이용한다.

보안 애플리케이션이 초기화될 때, mmap을 이용하여 secure world에서만 접근 가능한 메모리 영역을 두 영역을 매핑(mapping)한다. (a) IPC 메시지를 전송받기 위한 영역, (b) monitor에 진입하기 위한 영역이다.

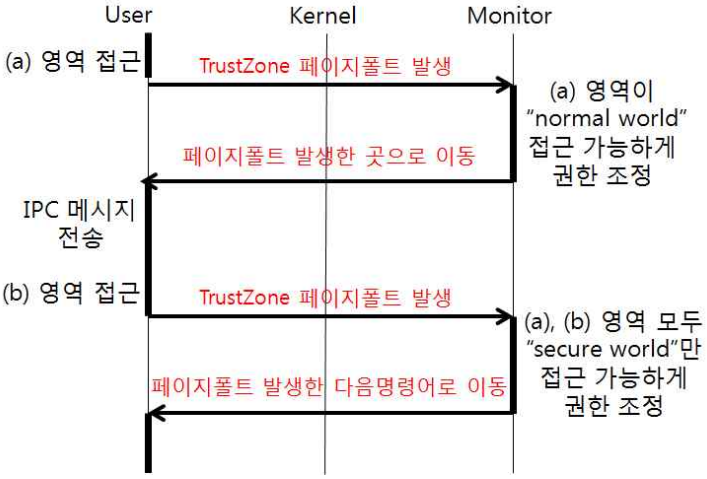

그림 2 IPC 송/수신시 흐름도

애플리케이션에서 내용을 송/수신하고자 할 때는 (a) 영역에 바로 접근하여 복사 작업을 한다.

하지만, (a) 영역이 secure world에서만 접근이 가능한 영역이므로 TrustZone 페이지폴트가 일어난다. 그리고 monitor모드의 페이지폴트 핸들러가 실행된다.

악의적인 프로세스를 막기 위해, 현재 프로세스가 (a) 영역을 초기화했었던 프로세스인지 확인한다. 프로세스마다 주소공간이 틀리므로, 페이지테이블 레지스터를 통해 식별이 가능하다.

사용이 가능하면 monitor모드의 페이지폴트 핸들러에서는 (a) 영역을 잠시 normal world에서도 접근 가능하게 변경한다.

그런 후에 normal world쪽으로 돌아간다. 돌아갈 때, 페이지폴트를 낸 명령어의 주소로 돌아간다. 아까와는 달리 메모리를 접근할 수 있으므로 페이지폴트 없이 실행된다.

마지막으로 모든 작업이 끝난 후에, (b) 영역에 접근한다. 마찬가지로 페이지폴트가 일어나고, monitor에 진입한다. 이때, (a), (b) 영역 모두를 secure world만 접근하게 바꾸어 놓는다.

4.3. IPC 중에 IRQ 또는 FIQ 발생시

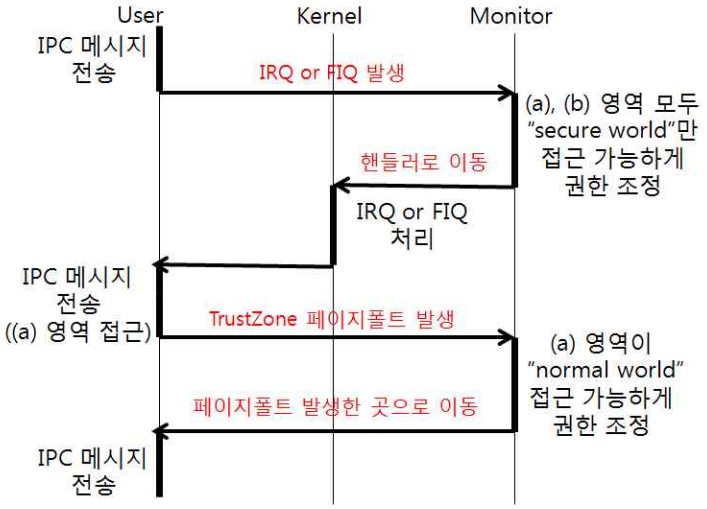

그림 3 IPC 중에 IRQ 또는 FIQ 발생시 흐름도

IPC 메시지 송/수신 중에 IRQ나 FIQ가 발생하여, 도중에 커널 쪽 코드가 선점할 수 있다.

따라서, monitor모드의 IRQ/FIQ 핸들러에서 (a) 영역, (b) 영역 모두를 secure world만 접근 가능하도록 변경한다.

4. 구현 및 테스트

ARM cortexA8인 Samsung S5PC100 CPU의 보드에서, 메모리 영역중 iRAM으로 구현하였다. 하드웨어 디버거를 이용해 설계대로 동작함을 확인하였다. monitor 모드의 핸들러가 의도한 대로 실행되었으며 메모리 영역의 접근 권한 역시 의도한 대로 바뀜을 확인하였다.

5. 결 론

IPC의 실행코드를 monitor로 고립시킬 수 있었다. 또한, IPC의 데이터를 secure world만 접근 가능한 영역에 복사함으로써, normal world에서는 접근이 불가능하게 고립시켰다. 또한, TrustZone의 페이지폴트 과정을 이용함으로써, 초기화된 이후에는 IPC의 실행과정 중간에 커널이 개입되지 않도록 하였다.

따라서, ARM TrustZone을 이용하여 신뢰성 있는 IPC를 제공할 수 있었다.

6. 참고 문헌

[1] Matthias Lange, Steffen Liebergeld, Adam Lackorzynski, Alexander Warg, and Michael Peter. 2011. L4Android: a generic operating system framework for secure smartphones. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11). ACM, New York, NY, USA

[2] Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, Jonathan M. McCune. Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me? In Proceedings of the 5th international conference on Trust and trustworthy computing (TRUST'12)

[3] He Liu, Stefan Saroiu, Alec Wolman, and Himanshu Raj. 2012. Software abstractions for trusted sensors. In Proceedings of the 10th international conference on Mobile systems, applications, and services (MobiSys '12). ACM, New York, NY, USA

[4] Theinfow. http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=mark_benson

[5] Thesnkchrmr. RageAgainstTheCage. http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=mark_benson. March 24, 2011

[6] ARM Limited. ARM security technology: Building a secure system using TrustZone technology. WhitePaper PRD29GENC-009429C, 2009

[7] Dan R. K. Ports and Tal Garfinkel. 2008. Towards application security on untrusted operating systems. In Proceedings of the 3rd conference on Hot topics in security (HOTSEC'08). USENIX Association, Berkeley, CA, USA

[8] Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, and Jacob R. Lorch. 2006. SubVirt: Implementing malware with virtual machines. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP '06). IEEE Computer Society, Washington, DC, USA

[9] Application Licensing - Google Developers site. http://developer.android.com/guide/google/play/licensing/index.html