# ARM기반 리눅스 커널에서 시스템콜 인터셉트 공격

이형찬○, 김충희, 이정현
숭실대학교 컴퓨터학과
lee.hyeongchan@ssu.ac.kr, kchclub3@gmail.com, jhyi@ssu.ac.kr

# System Call Interception Attack on ARM-based Linux Kernel

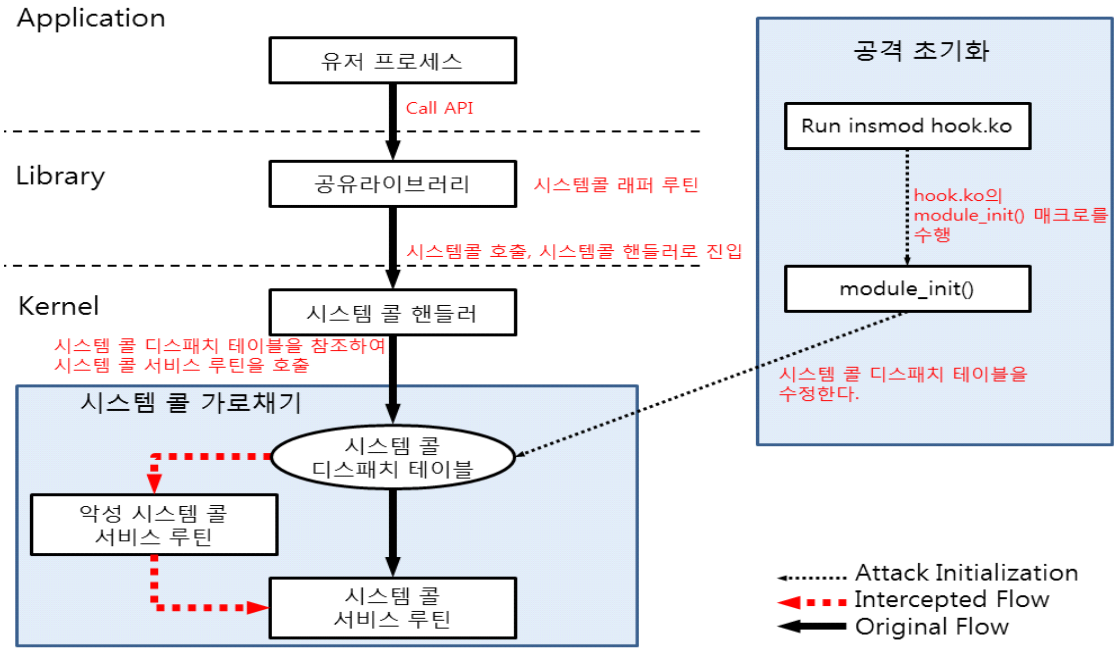
Hyeongchan Lee○, Chung Hui Kim, Jeong Hyun Yi
School of Computer Science and Engineering, Soongsil University

## 1. 서론

리눅스는 다양한 하드웨어를 지원하는 운영체제로서 임베디드 시스템, 서버, 데스크탑 PC 등 여러 목적으로 사용되고 있으며, 최근 ARM기반 스마트폰 운영체제로도 많이 사용되고 있다. 본 논문에서는 안드로이드 프레임웍의 커널로 사용되기도 하는 모바일 리눅스에서 LKM(Loadable Kernel Module)을 통한 시스템 콜 인터셉트 공격 가능성에 대한 연구 결과를 보고한다. 시스템콜 인터셉트 공격이 루트 권한을 획득한 상태에서 백도어, 루트킷 등의 공격을 시도하기 위해 사용되면, 루트킷은 커널 모드에서 사용자의 모든 입력을 가로챌 수 있어, 손쉽게 ID, 패스워드를 절취 할 수 있다. 공격 기법에 대한 검증 실험은 리눅스 커널 기반의 Maemo 플랫폼을 적용한 노키아 N900 스마트폰에서 실시하였으며, 실험 결과를 토대로 시스템콜 인터셉트 공격에 대응하기 위한 기술적 방안도 함께 토의하고자 한다.

## 2. 시스템 콜 인터셉트 공격

시스템 콜은 사용자 프로세스가 커널에 접근하여 커널이 제공하는 서비스를 받기 위해서 사용되는 인터페이스이며, 이를 조작하여 인터페이스의 흐름을 가로채는 것을 시스템 콜 인터셉트 공격이라 한다. [그림 1]는 일반적인 시스템 콜 호출과 시스템 콜 인터셉트 공격을 나타낸다.




[그림 1] 시스템 콜 인터셉트 공격 흐름도

† 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 20100011057)

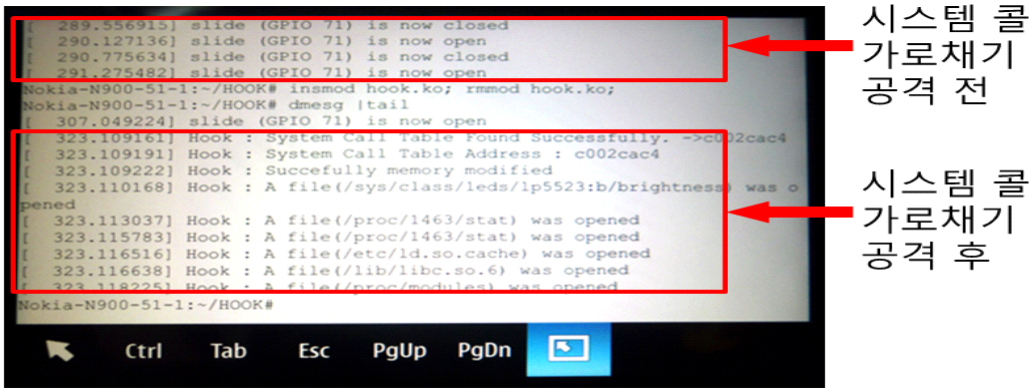
일반적인 시스템 콜의 경우, 사용자 프로세스가 공유라이브러리를 통하거나 혹은 공유라이브러리를 통하지 않고 시스템 콜을 호출하게 된다. 시스템 콜의 핸들러는 시스템 콜 디스패치 테이블을 참조하여 시스템 콜의 서비스 루틴을 수행하고 결과 값을 반환하게 된다.

이에 반해 시스템 콜 인터셉트 공격이 수행된 경우, 사용자 프로세스는 앞서 말한 정상적인 과정을 통해 변조된 시스템 콜 디스패치 테이블을 참조하여, 공격자가 정의한 시스템 콜 서비스 루틴을 호출하게 된다. 호출된 악성 시스템 콜 서비스 루틴은 악성행위를 한 후, 원래의 시스템 콜 서비스 루틴을 호출하게 되며, 그 반환 값을 다시 사용자 프로세스에게로 반환한다.

이러한 시스템 콜 인터셉트 공격을 취하기 위해서, 악성 LKM, 아래 hook.ko로 표기된 LKM은 module_init() 매크로가 수행될 때, 시스템 콜 디스패치 테이블을 찾아내어, 목표 시스템 콜 서비스 루틴을 악성 시스템 콜 서비스 루틴으로 교체한다.

## 3. 실험 결과

테스트에 사용된 스마트폰은 노키아 N900으로 Linux 기반 Maemo 5를 플랫폼으로 채택하고 있으며, 커널 버전은 2.6.28 이다. 개발환경은 Ubuntu 9.04 커널 버전 Linux 2.6.28-18-generic이며, Maemo 5 Fremantle SDK를 설치하였다.




[그림 3] 노키아 N900에서 시스템 콜 인터셉트 공격

[그림 2]는 루트 쉘이 설치된 노키아 N900 장치에서, 실제로 시스템 콜 인터셉트 공격을 수행한 화면이다. 시스템 콜 sys_open을 가로채는 코드가 삽입된 LKM hook.ko를 insmod로 설치 한 후, dmesg로 디버그 메시지를 추출하였다. '시스템 콜 인터셉트 공격 후' 부분을 보면, 시스템 콜 sys_open이 수행될 때 매개변수 값으로 설정된 파일이름을 고스란히 가로채어 디버그 메시지로 출력함을 확인할 수 있으며, 이는 ARM 프로세서 기반 리눅스 Maemo 5에서 LKM으로 시스템 콜을 가로챌 수 있음을 의미한다. 즉 LKM으로 시스템 콜을 가로채서 악성행위를 하는 ARM 기반 리눅스 루트킷이 제작 가능함을 확인할 수 있었다.

## 4. 대응방안에 대한 논의

본 논문에서 논의된 시스템콜 인터셉트 공격은 악의적인 LKM이 어떠한 검증도 없이 설치되기 때문에 이루어진다. 이에 대한 대응방안으로 LKM을 신뢰할 수 있는 인증기관에서 서명을 하는 것을 고려해 볼 수 있다. 일반적으로 x86 PC에서 적용은 너무 많은 모듈의 수 때문에 어려울 것이라고 생각되나, ARM 기반의 스마트폰의 경우 제조사가 선택적으로 제공하며, 제한된 모듈을 제공한다면 가능할 것으로 판단된다. LKM이 커널에 설치될 경우 sys_init_module()이 호출되게 되는데, 이때 모듈이 신뢰할 수 있는 인증기관에 의해 서명되었는지 확인할 수 있을 것이다. 하지만, 이러한 기법은 LKM의 이점을 반감시킬 수 있다. 좀 더 구체적으로 LKM의 이점은 필요에 따라 동적으로 링크 / 언링크를 하여, 자원을 효율적으로 관리함으로써, 커널의 성능을 올리는 것에 있는 반면, LKM을 링크할 때 서명을 확인해야 하는 추가적인 부하가 발생한다. 따라서, 이러한 단점을 해결하면서 LKM을 검증할 수 있는 메카니즘 개발이 필요할 것으로 사료된다.

## 5. 결 론

본 논문에서는 ARM 프로세서 기반 리눅스 커널을 탑재한 Maemo 5에서 LKM으로 시스템 콜을 가로채서 악성행위를 하는 루트킷이 제작 가능함을 보였다. x86에서 사용할 수 있는 커널의 기능들 중 일부 기능들은 ARM 기반 리눅스에서는 동일하게 사용할 수 없고, 실제 디바이스에서 동작하는 커널과 개발용으로 공개된 커널이 상이한 관계로 공격기법 구현상의 별도의 노하우가 필요하였다.

시스템콜 인터셉트 공격이 스마트폰에 적용되면, 사용자의 각종 패스워드와 개인정보의 유출의 우려가 현실화 될 수 있다. 따라서, 이러한 취약점을 사전에 대비하기 위한 방어 기술 확보에 대한 지속적인 연구가 필요하고, 이를 통해 궁극적으로 안드로이드를 비롯한 리눅스 진영의 개방형 스마트폰 플랫폼의 보안 기술에 대한 연구가 보다 활성화되기를 기대해 본다.