한국컴퓨터정보학회 동계학술대회 논문집 제19권 제1호 (2011. 1)

Hypervisor를 이용한 스마트폰 사용자 프라이버시 보호

유재성*, 이광우*, 김승주*, 원동호°
°*성균관대학교 정보보호연구소
e-mail:{jsyou, kwlee, skim, dhwon}@security.re.kr

User Privacy Protection for Smart Phone using Hypervisor

Jaesung Yoo*, Kwangwoo Lee*, Seungjoo Kim*, Dongho Won°
°*Information Security Group, Sungkyunkwan University

● 요 약 ●

현재 사용되고 있는 스마트폰에서는 어떤 개인정보들이 외부로 제공되고 있는지 사용자에게 알려주지 않는다. 스마트폰 개인정보 유출로 인한 피해 사례가 증가하면서, 스마트폰 사용자 프라이버시 보호의 중요성이 부각되고 있다. 본 논문에서는 스마트폰 사용자가 설정한 개인정보보호 정책을 기반으로 개인정보 접근권한을 각 어플리케이션에 부여하고, 어플리케이션이 허가되지 않은 정보에 대한 접근을 요청한 경우, 이를 차단하고 사용자에게 경고 메시지를 보여주는 방법을 제안한다. 제안하는 기법은 물리적인 하드웨어에 대한 접근을 모니터링하고 제어할 수 있는 Hypervisor 기술을 이용한다. 본 논문에서 제안하는 기법은 사용자가 허가하지 않은 개인정보의 유출을 차단할 수 있고, 프라이버시를 안전하게 보호할 수 있다.

키워드: 스마트폰(Smartphone), 하이퍼바이저(Hypervisor), 프라이버시(Privacy)

I. 서 론

스마트폰 사용자가 증가하면서, 스마트폰에 저장된 개인정보가 유출되는 사례가 발생하고 있다. 스마트폰에는 사용자 프로필 정보, 장치 고유 식별자 정보, 위치정보 등 개인 프라이버시를 위해 보호되어야 할 정보들이 존재한다. 하지만, 현재 사용되고 있는 스마트폰에서는 설치된 어플리케이션이나 악성코드를 통해 개인정보가 유출되어도 사용자가 인지하지 못한다는 문제점을 가지고 있다. 이처럼 스마트폰 사용자의 개인정보가 악용되는 피해를 줄이기 위해, 사용자는 자신의 어떤 정보가 제공되고, 어떻게 사용되는지, 혹은 제공하고 싶지 않은 개인정보가 유출되지는 않는지에 대한 정보를 제공받을 필요가 있다. 이에 본 논문에서는 Hypervisor를 통해서 어플리케이션의 사용자 개인정보 접근을 모니터링하고, 비정상적인 접근이 발생할 경우, 접근을 차단하고 사용자에게 알려주는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트폰 사용자 프라이버시 보호를 위해 사용되는 기술인 P3P(The Platform for Privacy Preferences)와 Xen Hypervisor를 설명하고, 3장에서는 사용자 프라이버시 보호 정책 생성하는 방법에 대해 살펴본다. 4장에서는 Xen Hypervisor를 이용한 개인 프라이버시 정보의 접근제어 방법을 제안하고, 5장에서 결론을 맺는다.

* 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다.(계약번호 UD100002KD)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (NIPA-2010-(C1090-1031-0005))
○ 교신저자, dhwon@security.re.kr

II. 관련 연구

1. P3P(The Platform for Privacy Preference)

W3C(World Wide Web Consortium)의 P3P는 정보통신서비스 제공자와 서비스 이용자 사이에서 개인정보보호정책을 자동으로 분석할 수 있도록 XML 형식으로 표현하는 플랫폼이다.[1] 서비스 이용자는 자신의 개인정보정책 허용수준을 설정하고, 서비스 제공자인 웹 서버는 서비스 이용자의 개인정보 사용정책을 설정한 후, <그림 1>과 같이 동작한다.

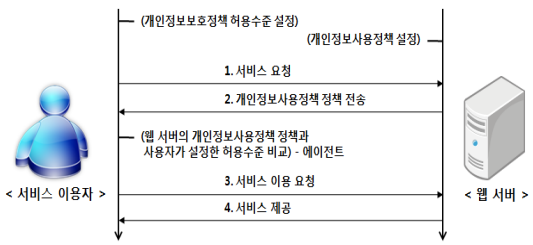

그림 1. P3P 동작과정
Fig. 1. Operation of P3P

서비스 이용자가 웹 서버에 서비스를 요청하면, 웹 서버는 XML 파일로 저장된 개인정보 사용정책을 서비스 이용자에게 전송한다. 서비스 이용자는 자신이 직접 웹 서버의 정책을 확인하는 것이 아니라, 인터넷 익스플로러와 같은 에이전트를 통해서 서비스 이용자가 설정한 개인정보정책과 웹 서버의 정책을 비교한다. 비교한 결과, 두 정책이 부합하면 서비스 이용을 요청한다.

P3P를 이용하면, 서버는 정당하게 서비스 이용자의 개인정보를 수집할 수 있다. 하지만, 서비스 이용자는 웹 서버가 정책에 언급된 개인정보만을 수집하는지, 정책을 위배하고 다른 중요 개인정보를 수집하는지 판단할 수 없다.

2. Xen Hypervisor

Xen Hypervisor[2]는 오픈 소스로 제공되는 가상머신 모니터다. <그림 2>는 기본적인 Xen Hypervisor 시스템의 구성을 나타낸 것이다.

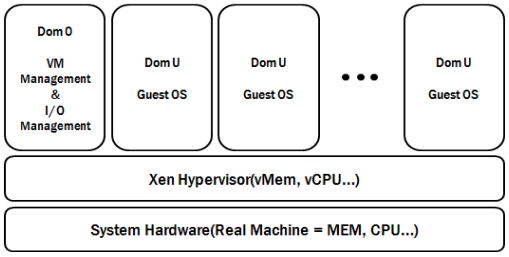

그림 2. Xen Hypervisor 시스템 구성도
Fig. 2. System Architecture of Xen Hypervisor

Xen Hypervisor는 시스템 하드웨어의 상위 소프트웨어 레이어 형태로 존재하며, 여러 운영체제가 하나의 시스템에서 독립적으로 실행될 수 있도록 가상 리소스 역할을 담당한다. 또한, 입출력 장치에 대한 접근을 제어한다.

Xen에서 도메인이라 불리는 가상머신은 Xen Hypervisor의 최상위 계층에 존재한다. Dom 0는 가장 먼저 생성되는 가상머신으로, 다른 가상머신들과 입출력장치를 관리한다. Dom 0는 다른 가상머신들(Dom U)을 반가상화 기법을 이용하여 실행한다. 반가상화는 가상머신에서 특권 명령어가 발생하면, 이를 Hypervisor가 처리할 수 있는 형태로 변형시켜서 가상머신이 Hypervisor 영역으로 침범하지 못하게 하는 기법이다.

위와 같은 Xen Hypervisor를 사용하면, 가상 머신들의 동작을 모니터링할 수 있으며, 가상머신이 시스템 하드웨어에 접근하는 것을 제어할 수 있다. 본 논문에서 언급하는 Hypervisor는 모두 Xen Hypervisor를 의미한다.

III. 사용자 프라이버시 보호 정책 생성방법

스마트폰 사용자 프라이버시 보호를 위해서는 설치된 어플리케이션이 허가되지 않은 개인정보에 접근하는 것을 모니터링하고 차단해야 한다. 하지만, 현재 많이 사용되고 있는 아이폰과 안드로이드 폰에서는 위와 같은 기능을 제공하지 않는다. 아이폰에서는 어플리케이션 설치 전에 사용자 개인정보 수집에 대한 약관 동의 여부를 확인하고, 안드로이드 폰에서는 어플리케이션에서 수집되는 개인정보 항목들을 사용자에게 명시한 후, 설치여부를 확인한다. 사용자 측면에서는 모든 어플리케이션에서 명시하는 개인정보 수집 정책을 일일이 확인하기 번거롭다. 또한 어플리케이션 설치 후, 정책에서 명시하지 않은 개인정보들을 수집하는지에 대한 여부를 판단할 수 없다. 어플리케이션들의 사용자 개인정보 접근을 모니터링하기 위해서는, 각 어플리케이션들의 접근 권한을 명시한 정책이 마련되어야 한다. 본 논문에서는 이러한 접근권한 정책을 설정하기 위해서 P3P를 이용한다.

먼저 스마트폰 사용자가 자신의 개인정보보호정책 허용수준을 설정하고, 어플리케이션의 설치파일에는 사용자 개인정보 사용정책이 포함되어 있음을 가정한다. 어플리케이션 설치 시, 사용자 에이전트는 사용자가 설정한 개인 정보보호정책과 어플리케이션의 사용자 개인정보 사용정책을 비교하고, 두 정책이 부합하면 설치를 진행한다. 이 때, 어플리케이션에서 명시한 사용자 개인정보 사용정책에 따라 개인정보에 접근할 수 있는 권한이 어플리케이션에 부여되며, 이 정보는 Hypervisor가 참고하는 보안 정책 파일에 기록된다.

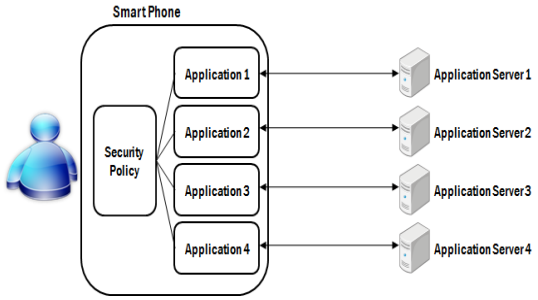

그림 3. 사용자 프라이버시 보호를 위한 보안 정책 생성
Fig. 3. Making Privacy Policy for Privacy Protection

<그림 3>은 스마트폰에 설치되는 모든 어플리케이션들의 사용자 개인정보 접근권한이 보안 정책파일에 포함되어 있음을 나타낸 것이다. 이렇게 생성되는 보안 정책파일은 Hypervisor에서 어플리케이션의 사용자 개인정보 접근을 제어하는데 사용된다.

IV. Hypervisor를 이용한 사용자 프라이버시 정보 접근제어

본 장에서는 Hypervisor를 이용해서 스마트폰에 설치된 어플리케이션이 허가된 개인정보 이외의 다른 정보에 접근하는 것을 모니터링하고, 비정상적인 접근은 차단하는 기법을 제안한다.

<그림 4>는 본 논문에서 제안하는 스마트폰 환경에 적합한 Hypervisor Architecture를 나타낸다. 일반적으로 스마트폰은 안드로이드, iOS, 윈도우모바일과 같은 단일 운영체제를 기반으로 동작하기 때문에, 단일 운영체제 기반의 Hypervisor Architecture

를 제안한다.

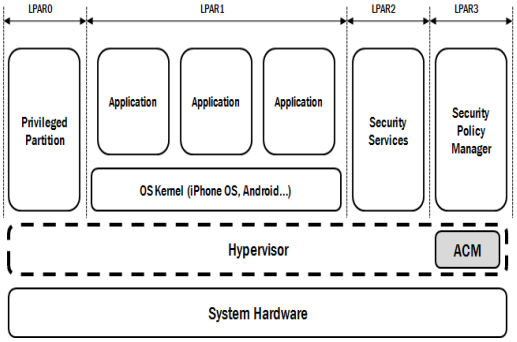

그림 4. 스마트폰 환경의 Hypervisor Architecture
Fig. 4. Hypervisor Architecture for Smart Phone

본 논문에서 제안하는 Hypervisor Architecture는 네 개의 논리 파티션으로 구성되고, 역할은 아래와 같다.

- Privileged Partition : 입출력 파티션이라고도 불리며, 입출력장치를 제어한다.
- OS Kernel 및 Application : 스마트폰에 설치되는 운영체제 및 어플리케이션이다.
- Security Services : 논리 파티션들의 공유 리소스에 대한 접근권한 규칙을 관리한다.
- Security Policy Manager : Xen Hypervisor를 위해 보안정책을 수립하고 관리한다.

스마트폰에 설치된 어플리케이션의 사용자 개인정보 접근제어는 Hypervisor 레이어 내에 존재하는 ACM(Access Control Module)이 담당한다. ACM은 Security Policy Manager에서 관리하는 보안정책을 기준으로 접근제어를 수행한다. <그림 5>는 ACM에서 어플리케이션의 개인정보 접근을 모니터링하고 통제하는 방법을 나타낸 것이다.[4]

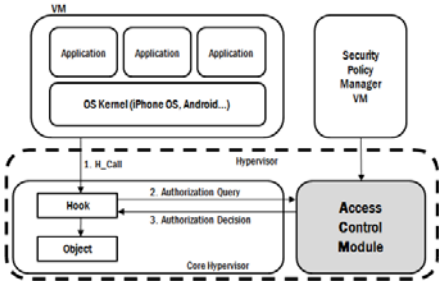

그림 5. Hypervisor 기반의 보안 모니터링
Fig. 5. Monitoring based on Hypervisor

스마트폰에 설치된 어플리케이션이 Hypervisor를 통해 사용자 개인정보에 접근하기 위한 과정은 아래와 같다.

1. 사용자 개인정보에 접근하기 위해 운영체제를 통해 Hypervisor Call 메시지를 Hypervisor에게 전달한다.
2. Hypervisor Call 메시지가 전달된 후, Hypervisor는 ACM에게 해당 어플리케이션이 요청한 사용자 개인정보에 접근할 수 있는 권한을 가지고 있는지 질의한다.
3. ACM은 사용자의 개인 정보보호정책을 기준으로 만들어진 보안정책을 참고하여, 사용자 개인정보에 대한 어플리케이션의 접근권한을 알려준다.
4. Hypervisor는 사용자 개인정보의 접근권한을 가진 어플리케이션일 경우 접근을 허용하고, 그렇지 않으면 어플리케이션의 접근을 차단함과 동시에 사용자에게 경고 메시지를 전달한다.

위와 같은 과정을 통해서 Hypervisor는 어플리케이션의 사용자 개인정보 접근을 모니터링 하고, 비정상적인 접근일 경우 차단한다. 사용자 측면에서는 자신의 개인정보보호 정책을 설정한 후, Hypervisor를 통해서 정책에 위배되는 어플리케이션의 개인정보 접근을 확인하고 차단할 수 있다. 이를 통해 스마트폰 사용자는 원하지 않는 개인정보 유출을 막을 수 있고, 자신의 개인 프라이버시를 보호할 수 있다.

V. 결 론

본 논문에서는 스마트폰 사용자 프라이버시 보호를 위하여, 사용자 개인정보 제공 정책을 기반으로 Hypervisor가 어플리케이션의 개인정보 접근을 모니터링하고, 통제하는 방법을 제안하였다. 사용자 프라이버시 보호를 위해서는 어플리케이션의 개인정보 접근을 모니터링하고 차단할 수 있는 기능이 사용자에게 제공되어야 한다.

하지만, 현재 사용되고 있는 스마트폰에서는 사용자가 원하지 않는 개인정보 노출여부를 확인할 수 없었다. 본 논문에서 제안한 방법을 스마트폰에 적용할 경우, 사용자는 허용하지 않은 개인정보의 유출을 차단할 수 있고, 프라이버시를 안전하게 보호할 수 있을 것으로 기대된다.

참고문헌

[1] W3C, “The Platform for Privacy Preferences 1.1(P3P 1.1) Specification” 2006.

[2] P.Barham, B.Dragovic, K.Fraser, S.Hand, T.Harris, A.Ho, R.Neugebauer, I.Pratt, and A.Warfield. “Xen and the art of virtualization” In Proceedings of the 19th ACM Symposium on Operating Systems Principles, October 2003.

[3] R.Sailer, T.Jaeger, E.Valdez, R,Caceres, R.Perez, S.Berger, J.L.Griffin, L.Doorn. "Building a MAC-Based Security Architecture for the Xen Open-Source Hypervisor" In

Proceedings of the 21st Annual Computer Security Applications Conference, December 2005.

[4] R.Sailer, E.Valdez, T.Jaeger, R.Perez, L.Doorn, J.L.Griffin, S.Berger. “sHype: Secure Hypervisor Approach to Trusted Virtualized Systems” RC23511(W0502-006) February 2005.