모바일 클라우드 환경에서의 비정상 행동 모니터링 및 탐지

[1] 김태현 O, [2] 정재윤, [2] 현종환, [2] 리건, [1] 홍원기

[1] 포항공과대학교 정보전자융합공학부, [2] 포항공과대학교 컴퓨터공학과

{[1]ggobugi3, [2]dejavu94, [2]noraki, [2]gunine, [1]jwkhong}@postech.ac.kr

요 약

클라우드 컴퓨팅과 모바일 환경은 사용자에게 확장성, 신축성 및 이동성 등 다양한 기능들을 제공하는 현대 사회에서 매우 중요한 기술이다. 이 두 가지 기술을 결합하여 모바일 클라우드 서비스를 제공한다면, 사용자들에게 강력한 컴퓨팅 파워와 편리함을 동시에 제공하여 보다 많은 이점을 제공할 것이다. 모바일 클라우드는 클라우드에서 사용자에게 가상 모바일 인스턴스를 제공하고, 사용자는 모바일 클라우드에 접속하여 다양한 작업을 빠르고 편리하게 수행할 수 있다. 이와 같은 새로운 서비스를 제공하기 위해서는 보안 문제가 먼저 해결되어야 한다. 본 논문에서는 모바일 클라우드 서비스를 소개하고, 보안 위협에 대처하기 위한 한 가지 방법으로 모바일 클라우드 환경에서 호스트와 네트워크 정보를 통해 비정상 행동을 모니터링하고 탐지하는 방법을 제시한다. 또한 제시한 방법을 검증하기 위해 실제 모바일 클라우드 환경을 구성한 후, 가상 모바일 인스턴스에 악성 프로그램을 설치하여 비정상 행동을 제대로 탐지하는지 살펴본다.

1. 개요

클라우드 컴퓨팅은 컴퓨팅 자원을 유연하게 제공하여 사용자에게 확장성, 신축성 등의 많은 이점을 제공한다. 일부 사람들은 이미 클라우드 컴퓨팅을 통해 다양한 서비스를 이용하고 있으며, 앞으로 점점 더 많은 사용자들이 클라우드 컴퓨팅 환경을 접하게 될 것이다. 또한 개인 뿐 아니라 중소기업 등의 회사들도 업무 환경을 구축하기 위해 클라우드를 도입하여 많은 비용과 시간, 노력, 에너지를 절감할 수 있다. 클라우드 컴퓨팅 못지 않게 모바일 환경도 현대 사회에서 매우 중요하고 편리한 기술이다. 스마트폰과 스마트 태블릿 등 수많은 모바일 기기들이 보급되면서, 다양한 모바일 서비스들이 제공되고 있다. [1]에 따르면, 이미 2011 년 3 월에 안드로이드 마켓에는 20 만개, 아이폰 앱스토어에는 30 만개의 어플리케이션이 등록되었으며, 이 숫자는 매우 빠르게 증가하고 있다. 최근에는 이러한 모바일 서비스들도 클라우드 컴퓨팅의 장점을 살리고자, 클라우드 기반의 서비스로 제공되는 경우가 많아지고 있다. 클라우드 기반의 서비스는 모바일 기기의 컴퓨팅 파워가 부족하더라도 복잡한 작업을 클라우드 환경에서 수행할 수 있도록 해준다. 또한 모바일 기기를 통해 언제 어디서든지 클라우드에 저장된 데이터로 접근할 수 있기 때문에, 기존의 일반 서비스들 보다 유연성이 높다.

모바일 기기와 클라우드 서비스의 융합을 통해 앞으로는 클라우드 환경에서 가상 모바일 장치를 지원하는 새로운 모바일 클라우드 서비스가 제공될 것으로 기대된다. Virtual smartphone over IP [2]는 가상 모바일 인스턴스를 제공하는 좋은 예이다. 클라우드 내부의 가상 인스턴스는 하나의 모바일 기기에 대응되고, 사용자는 자신의 인스턴스에 접속하여 모바일 클라우드 서비스를 사용한다. 본 논문에서는 모바일 클라우드를 막강한 컴퓨팅 파워와 저장공간을 지닌 클라우드가 여러 가상 모바일 인스턴스를 제공하고 관리하는 환경으로 정의한다.

그러나 모바일 클라우드 서비스를 제공하기에 앞서, 서비스 공급자는 그와 관련된 보안 이슈들을 알아야 한다. IDC 보고서 [3]에 따르면, 74.6%의 서비스 공급자들이 클라우드 서비스에서 가장 중요한 이슈가 보안이라고 응답했다. 게다가 최근 클라우드를 대상으로 한 공격들로 인해 클라우드 서비스에 대한 안전과 믿음을 보장하기 더 힘들어졌다.

본 논문에서는 모바일 클라우드의 보안 문제들을 해결하기 위한 한 가지 방법으로 비정상 행동을 탐지하는 방법을 제안한다. 현재 모바일 단말을 위한 백신 어플리케이션들은 시그니쳐 기반으로 악성 프로그램을 탐지하고 있으나, 모바일 클라우드 환경에서는 해당 어플리케이션을 모든 단말에 설치하도록 강제하기 힘들다. 대신 클라우드 환경에서 어플리케이션의 행동을 탐지하는 방법으로 이 문제를 해결할 수 있다. 이를 위해서 본 논문에서는 가상 호스트와 네트워크의 정보를 가지고 어플리케이션의 행동을 모니터링하고, 기계학습을 통해 비정상행동을 탐지하는 방법을 제안한다. 본 논문에서 제안하는 방법을 테스트하기 위해 모바일 클라우드 환경을 구축하여, 가상 모바일 인스턴스에 악성 프로그램을 설치하고 성공적으로 비정상 행동을 탐지하는지 관찰하였다.

*"본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)으로부터의 지원 (R31-2010-000-10100-0) 및 2011 년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원 (No. 2011-0020518)을 받아 수행되었습니다."

본 논문은 다음과 같은 순서로 구성되었다. 2 장에서는 모바일 장치와 클라우드 환경에서 비정상 행동을 탐지하는 것과 관련된 앞선 연구들을 소개한다. 3 장에서는 모바일 클라우드 서비스를 정의하고, 4 장에서는 모바일 클라우드 환경에서 비정상 행동 모니터링 방법과 구조를 제안한다. 5 장에서는 실제 구현한 모바일 클라우드 환경에서 테스트한 결과를 가지고 제안한 방법을 평가하며, 6 장에서는 연구 내용을 요약하고 향후 연구방향에 대해 다룬다.

2. 관련 연구

가. 모바일 기기에서의 비정상 행동 모니터링

모바일 기기에서 행동을 모니터링 함으로써 악성 프로그램을 탐지하는 것에 중점을 둔 선행 연구들은 다음과 같다. *Shabtai* 등은 [4]에서 안드로이드를 사용하는 모바일 기기에서 행동기반 악성 프로그램 탐지 프레임워크를 구현하였다. 그들은 CPU, 메모리, 네트워크 사용량을 모니터링하는 자신들의 어플리케이션을 모바일 기기에 설치하여 각 어플리케이션에 대한 정보를 얻고, 이를 다양한 기계학습 알고리즘을 통해 악성 프로그램을 탐지하였다. *Damopoulos* 등은 [5]에서 스팸과 관련된 악성 프로그램을 다뤘지만, 그 외의 일반적인 악성 프로그램들은 탐지하지 못했다. 그들은 스마트 기기의 행동을 웹브라우징, SMS, 전화 등으로 정의했고, 기계학습 알고리즘을 통해 높은 정확도로 비정상 행동을 탐지하였다.

나. 클라우드 환경에서 비정상 행동 모니터링

다양한 연구 팀들이 클라우드 컴퓨팅 환경에서의 침입 탐지를 연구해왔다. *Roschke* 등은 [6]에서 클라우드 환경에서 악의적인 행동을 탐지하는 방법을 제안하였다. 그들은 Host IDS 와 Network IDS 를 고려한 IDS 관리 시스템을 제안하였지만, 악의적인 행동을 어떻게 정의하고 탐지할 것인지는 다루지 않았다. *Vieira* 등은 [7]에서 그리드와 클라우드 컴퓨팅 침입 탐지 방법을 제안하였다. 그들은 각 노드들의 행동 분석과 지식기반 분석을 혼합해 탐지했지만, 가상화 된 노드를 고려하지 않았고 클라우드 컴퓨팅의 성능에 영향을 끼칠 수 있는 서비스 노드에서 분석을 수행하였다.

3. 모바일 클라우드 서비스 정의

모바일 클라우드 서비스를 정의하기 전에 모바일 클라우드를 정의할 필요가 있다. 모바일 클라우드에 대한 여러 가지 정의가 있는데, 크게 두 가지로 나눌 수 있다. 첫 번째는 모바일 클라우드를 구성하는데 모바일 기기에 보다 많은 역할을 부여하는 것이다. *Warner* 등은 [8]에서 모바일 클라우드를 모바일 기기를 통해 클라우드에 접속하는 동시에 모바일 기기 자체가 클라우드의 한 부분이 되는 것으로 정의하였다. *Marinelli* 는 [9]에서 모바일 클라우드를 많은 모바일 기기들이 클라우드 그룹을 구성하여 작업의 실행속도를 높이기 위해 작업을 여러 모바일 기기들에 할당하는 것으로 정의하였다.

본 논문에서는 모바일 클라우드를 클라우드 내에서 작업을 수행하고 그 결과를 모바일 기기에 전달하는 것으로 정의한다. 이 정의를 기반으로 우리는 모바일 클라우드를 통해 가상 모바일 인스턴스를 제공하는 새로운 모바일 클라우드 서비스를 제안한다. 가상 모바일 인스턴스는 실제 모바일 기기에서 모바일 클라우드에 접속함으로써 사용할 수 있다. 즉, 사용자는 자신의 모바일 기기를 통해 모바일 클라우드에 접속하여 가상 모바일 인스턴스를 사용함으로써, 모바일 클라우드의 CPU, 메모리, 네트워크 자원들을 사용할 수 있다. 이 경우, 모바일 기기는 지금보다 적은 역할을 담당하게 된다. 모바일 클라우드 서비스 제공자는 모바일 클라우드에 접속하고 화면을 전송하는 뷰어 어플리케이션을 만들어 배포하고, 사용자는 이 어플리케이션을 통해 모바일 클라우드에 있는 자신의 가상 모바일 인스턴스에 접근하여 서비스를 이용하게 된다. 그림 1은 본 논문에서 사용하는 모바일 클라우드 서비스를 보여준다. 모바일 클라우드 서비스를 통해 어떤 모바일 기기든지 슈퍼 컴퓨터가 될 수 있고, 높은 성능을 요구하는 서비스들을 사용할 수 있게 된다.

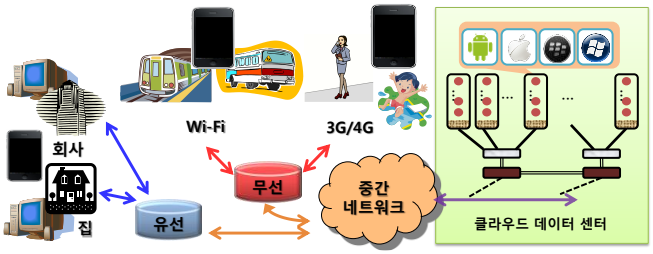

그림 1. 모바일 클라우드 서비스 개념도

4. 비정상 행동 탐지 방법과 구조

가. 비정상 행동 탐지 방법

행동이란 모바일 클라우드 내부의 가상 인스턴스 뿐만 아니라 가상 인스턴스에서 실행되는 어플리케이션들의 행동을 모두 포함한다. 예를 들어 모바일 어플리케이션이 모바일 클라우드 환경에서 어떤 행동을 수행할 때, CPU 나 메모리 등의 가상 자원을 사용하게 된다. 또한 어플리케이션이 클라우드 내부나 외부의 네트워크 자원을 사용하는 경우에는 네트워크 트래픽을 발생시키게 된다. 이러한 행동들이 가상 자원의 사용량을 변화시키게 되고, 각각의 어플리케이션마다 특정한 행동 패턴을 보인다고 가정했다. 만약 비정상 행동이 감지된다면, 해당 내용을 모바일 클라우드 관리자와 해당 인스턴스를 사용하는 사용자에게 알린다.

가상 모바일 인스턴스는 스마트폰이나 태블릿과 같이 일반적인 모바일 기기와 같은 역할을 한다. 일

반 모바일 기기에서 대부분의 현재 백신 어플리케이션들은 시그니쳐 기반의 방식으로 악성 프로그램들을 탐지한다. 시그니쳐 기반의 탐지방법은 검사 시간이 빠르고 정확도가 높지만, 시그니쳐가 변형되었거나 등록되지 않은 새로운 악성 프로그램은 탐지하지 못하는 단점이 있다. 만약 모바일 클라우드가 서비스된다면, 지금보다 더 많고 다양한 새로운 악성 프로그램들이 등장할 것이다. 따라서 지금의 백신 어플리케이션들로는 그들을 탐지하거나 막을 수 없다. 게다가 모바일 클라우드 환경은 수 많은 가상 인스턴스들을 제공한다. 만약 하나의 가상 모바일 인스턴스가 악성 프로그램에 감염된다면, 같은 모바일 클라우드 내부의 다른 가상 인스턴스로 쉽게 감염될 수 있고, 이는 전체 클라우드 시스템에 큰 피해를 입힐 수 있다. 따라서 클라우드 내부의 네트워크에 대한 모니터링도 필요하다. 이러한 보안 문제를 해결하기 위해 본 논문에서는 가상 모바일 인스턴스의 호스트 데이터와 네트워크 데이터를 함께 모니터링하는 행동 기반의 비정상 탐지 방법을 제안한다. 이 방법을 통해 알려지지 않은 악성 프로그램도 대처할 수 있을 것으로 기대한다.

나. 모바일 클라우드 모니터링 구조

그림 2는 모바일 클라우드와 비정상 행동 탐지를 위한 구조를 나타낸다. 모바일 클라우드 노드는 크게 서비스노드와 비서비스노드로 나눠진다. 서비스노드는 사용자에게 직접 모바일 클라우드 서비스를 제공하는 노드로 이루어진 그룹이며, 비서비스노드는 백그라운드 작업을 수행하거나 서비스 노드를 관리하는 등 모바일 클라우드 서비스를 간접적으로 지원하는 노드들로 이루어진 그룹이다.

서비스노드는 여러 개의 가상 모바일 인스턴스(VMI)들로 구성되어있으며, 하이퍼바이저는 각 가상 인스턴스를 생성하고 수정하고 삭제하며 관리한다. 각각의 가상 인스턴스를 모니터링 하기 위해, 가상 모바일 인스턴스에 에이전트 어플리케이션을 설치한다. 에이전트 어플리케이션은 각 가상 모바일 인스턴스에 대한 호스트 데이터를 모니터링한다. 네트워크 데이터는 네트워크 모니터링을 위한 별도의 가상 인스턴스에 의해 포트 미러링 방식을 통해 모니터링된다.

호스트 데이터는 가상 모바일 인스턴스에 에이전트 어플리케이션을 설치하여 모니터링한다. 이렇게 함으로써 가상 모바일 인스턴스의 CPU 와 메모리 사용량 등을 포함한 자세한 정보를 모니터링 할 수 있다. 모바일 클라우드 내부의 네트워크는 실제 데이터가 전송되는 데이터 네트워크 (peth0)와 관리를 위한 컨트롤 네트워크 (peth1)로 구분되는데, 호스트 정보는 컨트롤 네트워크인 peth1 을 통해 Analyzer 로 전송된다. 데이터 네트워크는 가상 모바일 인스턴스와 외부 서버 사이의 통신에 주로 쓰이며, 컨트롤 네트워크는 데이터 네트워크의 성능에 영향을 미치지 않는다.

네트워크 정보를 모니터링하기 위해서 가상 라우터를 통한 포트 미러링 방법을 사용한다.

하이퍼바이저에서 모니터링: 하이퍼바이저는 각 가상 모바일 인스턴스들을 관리하기 때문에, 이들이 사용하는 자원을 직접 모니터링하는 것이 가능하다. 그러나 많은 양의 데이터가 계속해서 생성되는 네트워크 데이터를 모두 하이퍼바이저에서 모니터링하기란 매우 부담이 된다. 실시간 네트워크 모니터링으로 인해 하이퍼바이저에 부담이 가중되면 정작 중요한 임무인 각 가상 모바일 인스턴스들의 작업 스케줄링, 자원분배 등의 작업에 영향을 끼쳐 클라우드의 전체적인 성능이 저하되는 결과를 초래할 수 있다.

포트 미러링: 따라서 하이퍼바이저의 부담을 최소화하기 위해서 하이퍼바이저에 설치된 가상 라우터는 가상 네트워크 인터페이스만을 관리하고, 네트워크 정보는 포트 미러링을 통해 다른 노드로 옮겨 모니터링한다. 각 가상 모바일 인스턴스에서 생성되는 데이터들은 Dom0 와 하이퍼바이저를 거쳐 전송되는데, Dom0 에 있는 가상 라우터에서 네트워크 데이터를 포트 미러링을 통해 VMI0 로 전송한다.

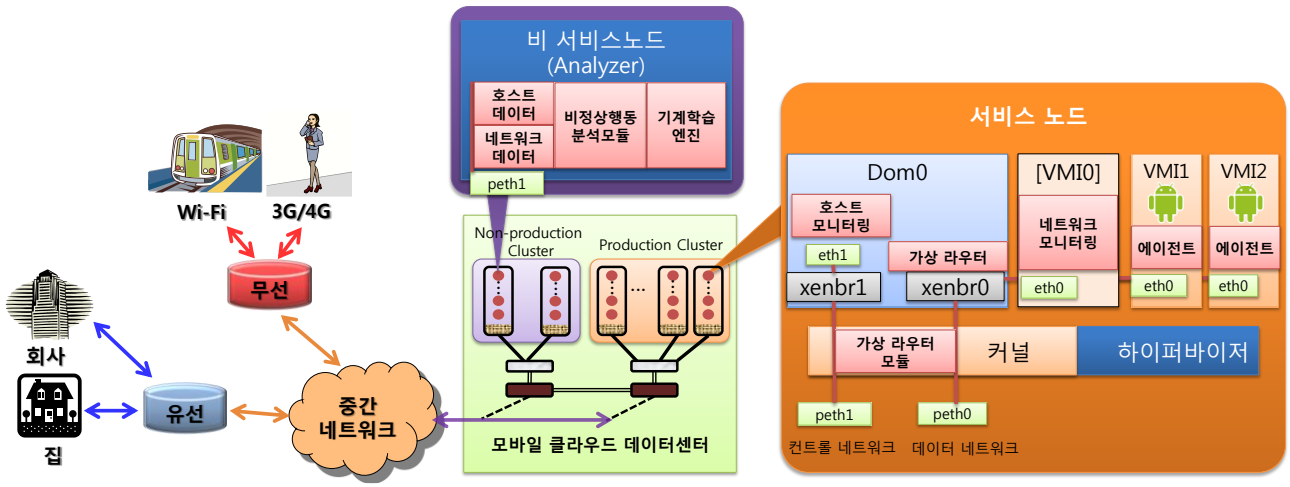

그림 2. 비정상 행동 모니터링 및 탐지를 위한 모바일 클라우드 구조

별도의 가상 인스턴스에서 모니터링: 서비스 노드에 네트워크 모니터링을 담당하는 별도의 가상 인스턴스 (VMI0)를 추가한다. VMI0 는 플로우 생성기와 특성 추출기를 포함한다. 플로우 생성기는 데이터 패킷을 플로우로 변환하며, 플로우는 IP 헤더, TCP/UDP 헤더, payload 등 일반적인 네트워크 정보들을 포함한다. 그러나 이렇게 생성된 모든 플로우를 분석하기에는 데이터 크기가 너무 크기 때문에, Tshark 를 이용해 의미 있는 특징들을 추출하는데 이를 담당하는 것이 특성 추출기이다. 네트워크 데이터는 VMI0 를 거치면서 중요한 정보들로 압축되어, 호스트 데이터와 마찬가지로 컨트롤 네트워크를 통해 Analyzer 로 전송된다. 이렇게 함으로써 서비스할 수 있는 가상 인스턴스의 개수가 하나 줄어들지만, 하이퍼바이저의 부담을 가중시키지 않기 때문에 네트워크 모니터링으로 인한 클라우드 전체의 성능 저하를 최소화할 수 있다.

다. 정보 수집

ㄱ) 호스트 정보 수집

스마트 기기의 경우 루트 권한을 얻으면 시스템의 모든 정보들을 자세히 살펴볼 수 있다. 마찬가지로 각 가상 모바일 인스턴스의 루트 권한을 얻는다면 커널단계까지 포함한 인스턴스에서 발생하는 모든 이벤트를 모니터링 할 수 있고, 보다 자세하고 정확하게 비정상 행동을 탐지할 수 있다. 그러나 루트 권한으로 실행할 경우 악성 프로그램의 위협에 쉽게 노출되고, 공격 당했을 경우 피해가 더 커진다. 따라서 본 논문에서 가상 모바일 인스턴스에 설치하는 모바일 에이전트는 루트 권한이 없이 일반 사용자 권한에서 실행되도록 구현하였다. *Shabtai* 등은

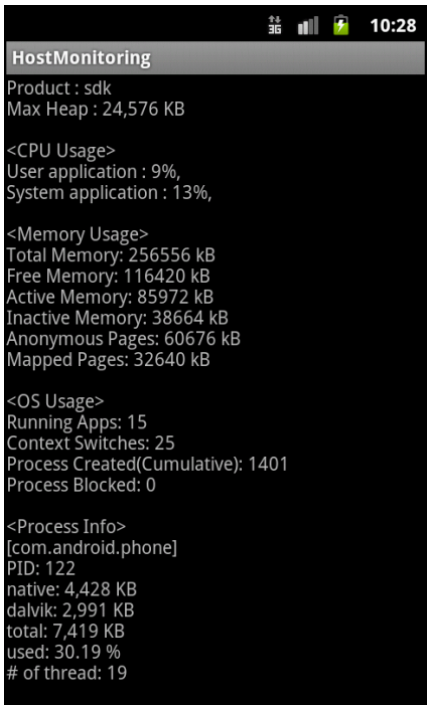

그림 3 . 에이전트 어플리케이션 실행 예시화면

[4]에서 모니터링 가능한 항목들과 악성 프로그램과의 관계를 분석하였다. 그러나 모니터링 항목의 수가 80 개가 넘고, 대부분은 상관관계가 적었다. 따라서 본 논문에서는 그 중 정상 또는 비정상 행동과 높은 관계가 있는 약 20 개의 항목들을 선정하여 각 항목들을 종류에 따라 CPU, 메모리, 운영체제, 프로세스, 네트워크 그룹으로 나누어 모니터링하였다. 그림 3은 호스트 정보를 모니터링하기 위해 가상 모바일 인스턴스에서 에이전트 어플리케이션을 실행했을 때 결과를 보여주는 예시화면이다. 네트워크와 프로세스 별 정보는 모바일 플랫폼의 API 를 사용해 정보를 얻고, OS 와 네트워크, 메모리 정보는 모바일 플랫폼의 사용자 명령어와 시스템 파일을 통해 정보를 얻어온다.

ㄴ) 네트워크 정보 수집

네트워크 자원을 사용하는 악성 프로그램은 3 가지 종류가 있다. 가상 모바일 인스턴스의 정보를 사용자 몰래 빼돌려 외부의 특정 서버로 전송하거나, 가상 모바일 인스턴스를 좀비로 감염시키고 봇넷을 형성하여 DDoS 공격에 사용, 또는 네트워크 사용량을 대폭 늘려 과다요금을 청구하는 등 네트워크와 관련된 악성 프로그램들을 탐지하기 위해서는 가상 모바일 인스턴스에서 수집하는 네트워크 정보뿐만 아니라 네트워크 단계에서 보다 자세하고 정확한 정보가 필요하다. 본 논문에서는 가상 라우터의 포트 미러링 기능을 통해 자세한 네트워크 정보를 모니터링한다. 그림 4에서와 같이 각 가상 모바일 인스턴스에서 생성된 네트워크 데이터들은 가상 라우터를 거쳐 데이터 네트워크로 전송된다. 이때 네트워크 모니터링을 위해 가상 라우터에서 포트 미러링을 통해 동일한 네트워크 데이터를 VMI0 로 전송한다. VMI0 에서는 1 분마다 플로우 생성기가 네트워크 데이터를 5-tuple 형식의 플로우로 변환하고, 특성 추출기는 플로우로부터 플로우와 패킷 종류별 개수와 크기 등의 정보를 추출한다. 이렇게 생성된 정보를 컨트롤 네트워크를 통해 비 서비스

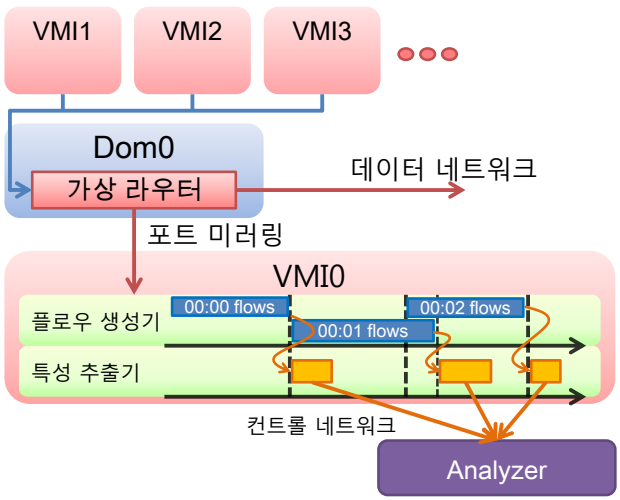

그림 4. 네트워크 정보수집

노드에 있는 Anayzer 로 전송하여 분석한다. 만약 악성 프로그램에 감염되어 특정 항목이 갑작스럽게 변동하는 등 네트워크의 사용 유형이 변경되면, 네트워크와 관련된 해당 악성 어플리케이션을 감지할 수 있다.

라. 비정상 행동 탐지

Analyzer 는 호스트와 네트워크에서 모니터링한 정보를 받아 기계학습을 통해 비정상 행동이 탐지되었는지 모니터링한다. 기계학습 툴은 Weka 를 사용하였고, 비정상 행동을 학습시키기 위한 알고리즘은 Random Forest (RF) 를 사용하였다. RF 알고리즘은 독립적으로 샘플링 된 랜덤 벡터들에 의해 형성된 decision tree 들의 조합으로, 다른 학습 알고리즘들에 비해 높은 정확성을 보인다. 수집한 정보들은 학습 알고리즘을 적용하기 위해 벡터 형식으로 변환된다.

본 논문에서는 각 호스트의 행동을 다음 3 가지 단계로 정의한다: 비활성화, 활성화, 비정상. 비활성화 상태는 가상 모바일 인스턴스가 사용 중이 아니고, 백그라운드에서 몇 가지 기본 어플리케이션들만이 돌아가는 상태를 의미한다. 활성화 단계는 사용자가 가상 모바일 인스턴스에 접속하여 게임이나 웹브라우징 등 어떤 기능을 사용하고 있는 상태를 의미한다. 만약 실행중인 어플리케이션 중 하나 이상이 지속적으로 루트 권한을 요청한다던가 내부의 자료를 외부의 특정 서버로 전송하려고 시도하는 등 악의적인 행동이 탐지되어 악성 프로그램으로 판단되면, 해당 호스트는 비정상 상태로 설정된다.

5. 실험 결과

그림 5는 악성 프로그램인 GoldMiner2 를 설치한 가상 모바일 인스턴스의 상태 변화를 나타낸다. 일반 어플리케이션을 실행하다가 20:30 부터 21:00 까지 GoldMiner2 를 실행시켰다. Analyzer 는 이 가상 머신에서 비정상 행동이 감지된 것을 확인하고, 비정상 상태로 설정하는 것을 볼 수 있다. 노란색으로 표시된 제일 낮은 층이 비활성화 상태이고, 녹색으로 표시된 중간 층이 활성화 상태이며, 붉은색으로 표시된 제일 높은 층이 비정상 상태를 나타낸다. 악성 프로그램의 실행을 종료한 21:00 이후에도 비정상 상태로 변경되는 이유는 악성 프로그램을 종료한 후에도 백그라운드에서 잠깐 실행되기 때문이다.

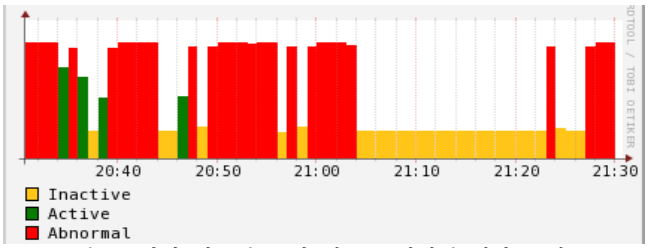

그림 5. 가상 인스턴스 별 행동 모니터링 결과 그래프

6. 결론

본 논문은 모바일 기기의 가상화를 지원하는 모바일 클라우드 서비스를 제시했고, 모바일 클라우드 서비스에서 중요한 보안 문제를 해결하기 위한 한 가지 방법으로 비정상 행동을 모니터링하고 탐지하는 방법을 제안하였다. 또한 제안한 방법을 검증하기 위해 실제로 모바일 클라우드 환경을 구축하여 10 개의 가상 모바일 인스턴스를 설치하고, 실제 악성 어플리케이션을 실행한 후 비정상 행동을 제대로 탐지하는 것을 살펴보았다.

모바일 클라우드 서비스는 아직 상용화되지 않은 연구 분야이기 때문에 앞으로 연구할 내용들이 다양하다. 제안한 방법을 보다 객관적으로 입증하기 위해 다양한 악성 프로그램들을 실행해서 더 많은 실험 데이터로 검증을 하고, 정확성을 높이기 위해 추가적으로 모니터링 할 항목들을 조사하며, 제안된 방법의 성능을 향상시키기 위해 구조나 알고리즘을 개선하는 방향으로 연구할 것이다. 그러나 모니터링 항목이 늘어나면 그만큼 오버헤드가 발생하여 처리 시간이 늘어나므로, 이들을 함께 고려해야 한다.

7. 참고 문헌

[1] Distimo, "The battle for the most content and the emerging tablet market", April, 2011, http://www.distimo.com/blog/2011_04_the-battle-for-the-most-content-and-the-emerging-tablet-market/.

[2] E. Y. Chen and M. Itoh, "Virtual Smartphone over IP", The next IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2010), Montrreal, Canada, June 2010, pp.1-6.

[3] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges", IDC eXchange, August 14, 2008.

[4] A.Shabtai, U. Kanonov, and Y.Elovici, "Andromaly: a behavioral malware detection framework for android devices", Journal of Intelligent Information Systems, January 2011, pp 1-30.

[5] D.Damopoulos, S.A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke, and S. Grizali, "Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifier", Security and Communication Networks, Vol.5, No.1, January 2011, pp.3-14.

[6] S. Roschke, F. Cheng, C. Meinel, "Intrusion Detection in the Cloud", Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, Chengdu, China, December 12-14, 2009, pp.729-734.

[7] Vieira. K, Schulter. A, Westphall. C.B, and Westphall. C.M, "Intrusion Detection for Grid and Cloud Computing", IT Professional, vol.12, no.4, July-Aug. 2010, pp.38-43.

[8] S. A. Warner and A. F. Karman, "Defining the Mobile Cloud", NASA IT Summit 2010, August 16-18, 2010.

[9] E. E. Marinelli, "Hyrax: cloud computing on mobile devices using MapRecuce", a Mater Thesis, CMU-CS-09-164, Carnegie Mellon University, September, 2009