제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

클라우드 컴퓨팅을 활용한 모바일 악성코드 탐지 방식 연구

김호연*, 최영현*, 정성민*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail :*{hykim, yhchoi, smjung}@imtl.skku.ac.kr, **tmchung@ece.skku.ac.kr

A Study on a Mobile Malware Detection Method Using a Cloud Computing

Ho-Yeon Kim*, Young-Hyun Choi*, Sung Min Jung*
Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information Communication Engineering, Sungkyunkwan University

요 약

모바일 보안이 이슈화 됨에 따라 안티 바이러스 소프트웨어를 제공하는 벤더들은 시그니쳐 기반의 모바일 안티 바이러스 제품들을 제공하고 있다. 시그니쳐 기반의 악성코드 탐지 방식은 새로운 방식의 악성코드를 탐지 하지 못하는 단점 때문에, 악성코드 행위 자체를 분석하는 악성코드 동적 및 혼합분석이 연구되고 있다. 본 논문에서는 자원의 제약이 있는 모바일 플랫폼에서 동적 행위 분석 및 정적 분석을 혼합한 혼합 분석을 클라우드 환경에서 처리하는 프레임워크를 제안하고자 한다.

1. 서론

시장 조사기관 가트너의 보고서에 따르면 2010년 전세계 스마트폰 OS의 보급 대수는 약 3억대로 전년대비 72.1%의 판매 상승률을 보였다[1]. 또 다른 시장 조사기관은 IDC(International Data Corporation)는 스마트폰의 보급 대수가 2011년 약 4억 5천만대로 증가할 것이며, 2015년에는 약 9억 2천대로 스마트폰 보급이 증가할 것으로 전망하고 있다[2]. 모바일 디바이스의 증가 추세에 따라 모바일 플랫폼에서 동작되는 모바일 악성코드 또한 증가하고 있다.

악성코드로부터 모바일 디바이스를 보호하기 위하여 대부분의 안티 바이러스 업체들은 모바일 디바이스 전용 안티 바이러스 프로그램을 제공하고 있다. 하지만 기존의 안티 바이러스 제품은 시그니쳐를 기반으로 한 정적 분석으로, 악성코드 미탐지의 소지가 있다. 악성코드 미탐지는 통화내역, 위치정보, 사진들과 같은 민감한 개인정보를 저장하고 있는 모바일 플랫폼에서는 매우 높은 위협 요인이 된다. 이에 따라서 미탐율이 낮은 동적 분석을 모바일 플랫폼에서 수행하는 연구가 진행되고 있다[3]. 하지만 낮은 데이터 처리율을 갖는 모바일 플랫폼에서의 동적 분석은 높은 다양한 입력을 요구하기 때문에 높은 오버헤드가 발생된다.

모바일 플랫폼의 낮은 처리 능력 문제를 해결하기 위하여 클라우드 내에서 모바일 플랫폼의 악성코드 분석을 수행하는 연구 또한 진행되고 있다[4][5]. 하지만 클라우드 내에서 분석이 완료되기 전까지 모바일 플랫폼에서는 SMS수신, 어플리케이션 실행 등이 제한되기 때문에 사용자의 불편함을 초래한다.

본 논문에서는 모바일 악성코드를 분석하기 위하여 악성코드 혼합 분석을 수행하고, 낮은 처리 효율을 보완하기 위하여 클라우드 환경에서 혼합 분석을 수행한다. 악성코드 분석 수행 시 실행할 수 없는 어플리케이션, SMS 수신, 다른 디바이스와의 연결 등을 해결하기 위하여 클라우드 내에서 분석이 수행되는 동안 모바일 플랫폼에서는 제한된 어플리케이션 수행을 제공한다. 제한된 어플리케이션 수행은 해당 어플리케이션의 환경에서 악용 가능한 기능을 원천적으로 차단한다.

본 논문의 구성은 다음과 같다. 2장 관련연구에서는 클라우드 컴퓨팅의 이점과 클라우드를 활용한 악성코드 분석 연구에 대하여 살펴보며 3장에서는 제안하는 프레임워크를 기술하고, 4장에서 결론 및 향후 연구에 대하여 소개한다.

2. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅 기술은 그리드 컴퓨팅, 유틸리티 컴퓨팅, 씬 클라이언트, 제로 클라이언트 등 다양한 모습으로 진화되어 왔다.

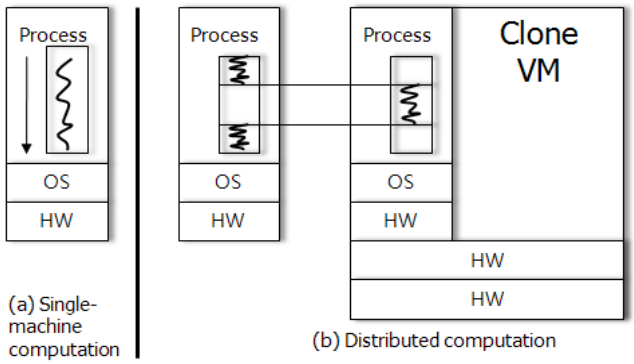
본 논문에서 제안하는 클라우드 컴퓨팅을 사용한 모바일 혼합 분석방식의 경우 다음과 같은 이점이 있다.

- 분산 컴퓨팅을 활용한 처리효율 증대 : 클라우드 컴퓨팅은 수 천, 수 만개의 노드 컴퓨터들 간의 분산, 병렬 처리가 가능하다. 악성코드들의 탐지를 위해 동적, 정적 또는 혼합 분석 방식이 사용될 때 보다 빠른 처리할 수 있다.
- 제한된 자원에 구애받지 않는 분석 가능 : 모바일 디바이스는 PC에 비하여 적은 메모리 및 베터리 사용으로, 낮은 처리효율을 보여준다. 악성 행위 분석 시 클라우드 컴퓨팅을 사용하여 정보 분석을 하는 방법을 분석하는 동안 이동성 및 다른 어플리케이션 사용에 제약을 받지 않아 낮은 자원을 사용함으로 써 제한되는 처리능력 및 자원을 보상받을 수 있다.
- 다양한 분석방식의 제공으로 오탐율 및 미탐율 감소 : 적은 자원을 활용하는 모바일 디바이스에서의 악성코드 탐지 방식은 정적 또는 동적 분석의 한 방식만을 사용할 수밖에 없었다. 하지만 클라우드 내에서는 다양한 환경을 구축할 수 있어 수행시간 대비 높은 효율을 보일 수 있다.

2.2 클라우드 기반의 악성코드 분석

정적 분석의 미탐율을 보완하기 위하여 동적 분석 및 혼합 분석이 연구되고 있으나, 높은 오버헤드와 다양한 입력 값을 요구하는 동적 분석은 작업을 수행하는데 많은 컴퓨팅 자원을 요구한다. 따라서 이를 해결하기 위하여 클라우드 컴퓨팅의 높은 처리율을 이용한 악성코드 탐지 방식이 연구되고 있다.

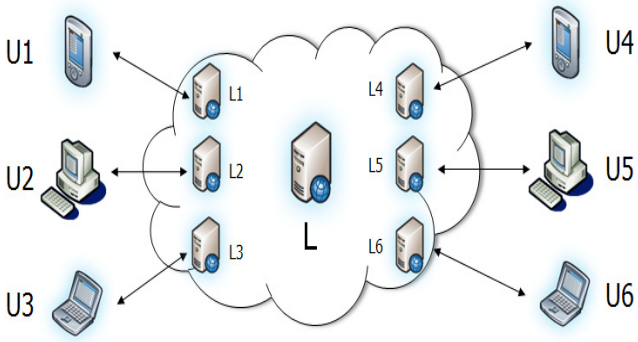
클라우드 컴퓨팅의 다양한 이점을 기반으로 한 클라우드 컴퓨팅 기반의 한 악성코드 분석 방식에 대한 많은 연구가 진행되고 있다. 버클리 대학 인텔 연구실의 B. G. Chun 등은 클론클라우드를 기반으로 한 모바일 디바이스의 처리효율을 높이는 연구를 진행하고 있다[4]. 이들이 연구하는 클론클라우드 기술은 모바일 디바이스 환경과 동일한 복제본을 클라우드 환경에 올려놓는 방식이다. 클론클라우드의 기본 아키텍쳐는 다음 (그림 1)과 같다. 클론클라우드는 모바일 디바이스에 구동되는 어플리케이션 중 많은 자원을 소모하는 어플리케이션을 클라우드 시스템 내의 클론에서 구동한다. 이를 통하여 모바일 디바이스는 적은 자원을 사용하면서도 높은 처리효율을 나타낸다. 하지만 클론 클라우드는 클라우드 내에서 클론이 모든 작업을 처리하기 전까지는 모바일 디바이스 상에서 실질적인 구동을 할 수 없다. 이러한 환경에서는 단순 URL을 첨부한 SMS와 MMS, 첨부파일 다운로드 등과 같은 즉각적인 결과가 요구되는 작업에서는 적합하지 않다. 또한 클론클라우드 내에서 어플리케이션에 대한 악성코드 분석 시 클라우드 시스템 내에서 분석이 끝나지 않는 한 어플리케이션을 구동할 수 없다는 문제가 존재한다.



(그림 1) 클론 클라우드 시스템 모델

Loreno Martignoni등은 클라우드 컴퓨팅을 활용한 행위 분석의 프레임워크를 제안하였다[5]. 제안된 프레임워크는 악성코드 분석 시 많은 시간을 요하고 많은 자원을 소모하는 행위 분석을 클라우드 시스템에서 분석하는 방식이다. 기본적인 아키텍쳐는 다음 (그림 2)와 같다.

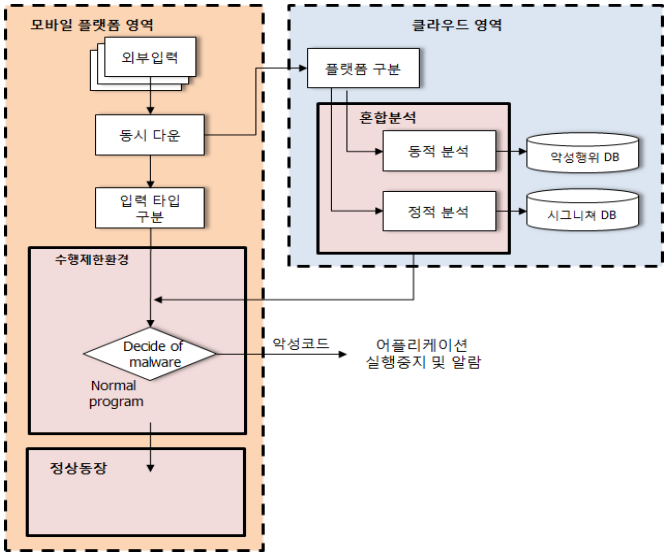
Loreno 등이 제안하는 모델은 다수의 사용자들이 클라우드 서버와 1:1로 연결되어 독립적인 환경을 갖는 다수의 유저들에 맞도록 설계되었다. 하지만 본 모델에서도 외부 클라우드 시스템에서의 처리에 의존도가 높기 때문에 동시에 많은 트래픽이 몰리는 환경에서는 각 독립된 사용자들은 해당 분석을 수행하는 동안 각 디바이스에서는 많은 오버헤드가 발생하게 된다.



(그림 2) 행위기반 동적 분석 모델

3. 제안모델

동적 및 정적 분석을 클라우드 컴퓨팅 환경에서 구현 시 클라우드 시스템에서의 분석에 높은 의존도를 보이며 악성코드의 분석 결과가 나올 때 까지 해당 어플리케이션 및 첨부 파일등을 수행할 수 없는 단점이 있다. 본 장에서는 이러한 문제를 해결하기 위해 제한된 수행을 제공하는 악성코드 탐지 방식을 제안한다. 제안하는 모델의 기본 아키텍쳐는 (그림 3)과 같다.



(그림 3) 제한된 수행을 제공하는 모바일 악성코드 탐지 모델

본 모델에서는 모바일 디바이스에서 외부로부터의 입력되는 다양한 입력들(예를 들어, 블루투스를 통한 파일 전송, 어플리케이션을 통한 다른 어플리케이션 다운로드, e-mail 첨부파일 다운로드, MMS 수신, 수신된 URL에 대한 접속 등)을 모바일 디바이스 내에서는 제한된 환경에서 수행을 시작하며, 이와 동시에 클라우드 시스템 내에 동일 파일 및 URL을 전송시킨다. 이와 같은 방식의 악성코드 분석으로의 이점은 분석 시 많은 자원을 사용함으로써 성능 저하를 보이지 않으며, 이와 더불어 분석이 끝나지 않더라도 사용자는 제한된 환경 내에서 일정 작업을 수행할 수 있다.

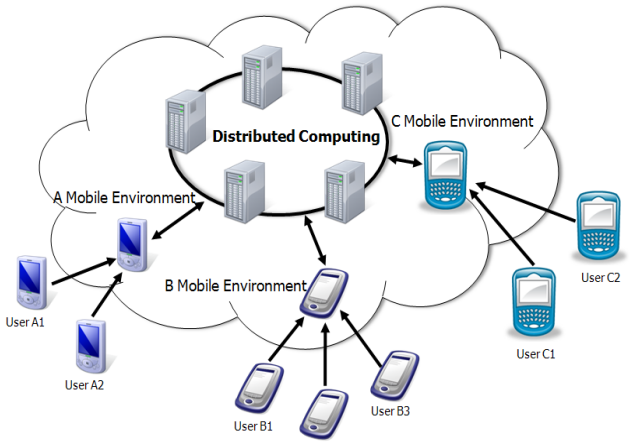
3.1 클라우드 환경

모바일 디바이스로부터 수신한 정보들을 분석하는 클라우드 컴퓨팅환경은 다음 (그림 4)와 같다.

- User : 외부로부터 수신된 데이터를 전송하는 end user로써, 클라우드 환경에 자신과 유사한 환경을 갖는 서버에 정보를 전송한다.
- Mobile Environment : 혼합 분석을 수행하기 위하여 end user와 유사한 환경으로 구축된 서버를 일컫는다.
- 분산 컴퓨팅 환경 : 혼합 분석을 보다 빠르게 수행하기 위하여 클라우드 시스템 내에 분석정보를 공유하고 처리하는 서버를 일컫는다.

3.2 혼합 분석

혼합 분석은 이미 분석된 정보로 DB화 된 시그니쳐 기반의 정적분석과 행위에 대한 모니터링 정보를 기반으로 한 동적 분석이 수행된다. 정적 분석의 경우 분석가가 분석한 시그니쳐와 웹크롤러, 클라이언트 허니팟과 같은 자동 웹 사이트 분석 도구로부터 얻은 악성 웹 사이트 정보들을 기반으로 정적 분석이 수행된다.



(그림 4) 악성코드 분석 환경

동적 분석의 경우 end user와 유사한 환경(Device Model, OS version)을 구축한 서버에서 수행된다. 동적 분석은 현재 시스템 메모리 상태와 수행중인 어플리케이션 목록, 시스템 매니저 환경등과 같은 다양한 변수들이 사용된다. 따라서 불필요한 오버헤드가 발생하기 때문에 end user와 동일한 환경이 아닌 유사한 환경에서 동적 분석이 수행된다. 실시간으로 변화하는 메모리 정보, 분석되는 동안의 또 다른 외부로 부터의 입력들은 무시된다. 본 방식의 경우 동적 분석이 갖는 이점인 실시간 환경에 따른 변수의 활용을 제공할 수는 없지만 대신 유사 환경에서 다양한 입력을 넣어보며 수행할 수 있어 정적 분석이 검출해 내지 못한 다양한 악성행위를 검출해 낼 수 있다.

4. 결론 및 향후 연구

본 프레임워크는 모바일 디바이스에서의 효율적인 혼합 분석을 위해 클라우드 시스템을 사용하였다. 기존의 모바일 악성코드 분석과는 달리 동적 분석의 모든 이점을 사용할 순 없지만 모바일 디바이스의 특성인 높은 이동성과 민감한 정보를 제한된 환경에서나마 제공할 수 있다. 따라서 사용자의 반응에 대한 즉각적인 피드백이 있어야 하는 모바일 디바이스의 요구사항을 만족시키면서 악성코드의 혼합 분석을 수행할 수 있을 것으로 기대된다.

향후 연구 계획으로는 제한된 프레임워크를 기반으로 실제 프로토타입의 개발과 각 모바일 플랫폼에서의 수행 제한사항에 관한 연구, 다양한 샘플을 활용하여 간소화된 제한사항으로 낮은 오탐 및 미탐율을 보이도록 프레임워크를 개선해나갈 것이다.

Acknowledgement

본 논문은 중소기업청에서 지원하는 2011년도 산학연 공동기술개발사업(No.00044301)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] 가트너, http://www.gartner.com, 2011.
[2] IDC, http://www.idc.com, 2011.
[3] S. Dai, Y. Liu, T. Wang, T. Wei, and W. Zou, "Behavior-based malware detection on mobile phone", pp.1-4, 2010.
[4] B. G. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti, "Clonecloud: Elastic execution between mobile device and cloud," , pp.301-314, 2011.
[5] L. Martignoni, R. Paleari, and D. Bruschi, "A framework for behavior-based malware analysis in the cloud," Information Systems Security, pp.178-192, 2009.