Journal of The Korea Society of Computer and Information
Vol. 19, No. 10, October 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.10.107

기업 모바일 사용자를 위한 확장된 BYOD 솔루션의 설계

박 재 경*, 김 성 진**

The design of the expanded BYOD solutions for business mobile users

Jae-Kyung Park*, Sung-Jin Kim**

요 약

최근 스마트폰의 사용은 대기업과 같은 회사 조직이나 공공기관 등의 조직에서도 업무 목적으로 많이 사용되고 있다. 개인이 사용하는 스마트폰은 개인정보에 대한 보안만을 신경 쓰면 되지만 기업이나 업무 목적일 경우에는 보다 신중한 접근이 필요하다. 업무용 스마트폰을 통한 해킹은 조직의 네트워크를 파괴할 수 있으며 이는 매우 심각한 피해로 이어질 수 있다. 이러한 상황을 대비하기 위해 기존의 솔루션인 MDM이나 MAM으로 보안 문제를 해결하려고 하였으나 스마트폰 사용자의 불편함과 조직적인 통제의 한계가 있다. 본 논문에서는 이러한 문제를 보다 폭넓게 해결할 수 있는 방안을 제안하고자 한다. 안전한 모바일 트래픽 관리 장치를 통해 기업이나 기관의 스마트폰을 사용하는 사용자에게는 편의성을 제공하고 스마트폰을 제공하는 조직에게는 보다 강력한 통제 수단을 제공할 수 있다. 또한 이를 확장하여 유무선이 통합되고 보안에 대한 새로운 서비스를 제공할 수 있는 방안을 제안하고자 한다.

▸ Keywords : MDM, MAM, 트래픽 관리, 모바일, BYOD

Abstract

In recent years, large companies and public institutions in the Smartphone business purposes has been used a lot. Personal Smartphone are worried about security of personal information only. But if you are a corporate or business purposes requires a more cautious approach. It can destroy an organization's network to hack Smartphones have very serious damage. For this purpose, the existing solution, and try to solve security issues with MDM or MAM. However, Smartphone users discomfort and there is a limit of organizational control. In this paper, we can propose with these issues more broadly would like to suggest. Secure mobile traffic management system enables companies or agencies the ease for users to use a

• 제1저자 : 박재경, • 교신저자 : 김성진
* 투고일 : 2014. 9. 17, 심사일 : 2014. 10. 7, 게재확정일 : 2014. 10. 24.
* 한국과학기술원 사이버보안연구센터(Cyber Security Research Center in KAIST)
** 숭실대학교 정보과학대학원 정보보안학과(Graduate School of Information Sciences)

Smartphone. And, for organizations that provide smart phones are more powerful and can provide a means of control. In addition, wired/wireless integration and security measures that can provide new services to offer.

▸ Keywords : MDM, MAM, Traffic Management, Mobile, BYOD

I. 서 론

최근 들어 기업이나 기관의 스마트폰을 통한 모바일 오피스는 점차 늘어나고 있는 추세에 있다. 이러한 증가 추세에 따라 보안에 대한 문제나 위협도 늘어나고 있는 추세이다. 모바일 오피스는 언제 어디서든 스마트폰을 이용하여 업무를 처리할 수 있는 환경으로 편리성이 매우 높다. 그러나 모바일 오피스는 긍정적인 측면도 있으나 부정적인 측면도 강해 단말에 대한 물리적인 위협, 단말에 대한 네트워크 적 위협, 단말을 경유한 인트라넷 위협 등 치명적인 보안 위협 요소에 노출되어 있다[2][10]. 이와 같은 모바일 오피스의 보안을 해결하기 위해 BYOD(Bring Your Own Device) 솔루션이 등장했으며 최근 MDM(Mobile Device Management)을 거쳐 MAM(Mobile App Management)으로 진화되고 있는 실정이다. 하지만, MDM은 기기 자체에 대한 보안을 제공하나 매우 불편한 솔루션이며 MAM은 응용 프로그램에 따른 보안을 제공하나 기기 자체에 대한 보안성은 떨어지는 각기의 단점을 가지고 있다. 최근 3G를 넘어서 4G인 LTE 및 LTE-A로 모바일 네트워크가 진화하면서 모바일 트래픽의 대역폭은 급격히 확장되고 있으며 이를 바탕으로 모바일 오피스도 급속히 확산되고 있다[7]. 따라서 기기 자체에 대한 솔루션에 한정된 BYOD로는 현재의 보안 상황을 모두 해결할 수 없으므로 보다 확장된 개념의 e-BYOD가 필요하다고 볼 수 있다.

본 논문에서는 기존 솔루션이 가지고 있는 한계성을 넘어설 수 있는 방안을 제시하고 또한 모바일 기기만에 국한하지 않고 모바일 네트워크를 포함하는 솔루션을 제한하고자 한다. 특히 기업에서는 업무용 모바일 기기를 별도로 지급하여 사용자는 여러 대의 모바일 기기를 지녀야하는 불편함이 있고 개인용 모바일 기기에는 기업의 MAM이나 MDM을 통해 강력히 제어할 수 없는 한계가 있다. 그러나 이와 같은 근원적인 문제점을 해결하려고 하기 보다는 각각의 위협요소에 대한 개략적인 처방에 급급하여 여전히 위협 요소가 잔존하는 실정이다.

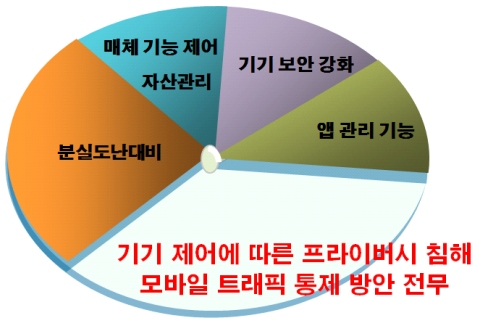

그림 1. 모바일 오피스의 보안 위협
Fig. 1. Security Threat of Mobile office

본 논문에서는 그림 1과 같이 모바일 오피스의 구조 및 특징, 구조적 취약점 및 이로 인해 필연적으로 유발될 수밖에 없는 위협 요소들을 파악하고 근본적인 대응책은 무엇이며 솔루션은 무엇인지를 제안하고자 한다. 본 논문에서는 이러한 모바일 오피스의 보안적인 문제를 MSM(Mobile Switching Management)을 통해 제안하되 현재 싱글 유심을 멀티 유심 구조를 통해 제안하여 모바일 환경에서의 개인과 기업의 정보보호 및 자료유출을 방지할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 살펴본다. 3장에서는 본 논문에서 제안하고자 하는 MSM 기법과 듀얼 유심에 대해서 기술하고, 4장에서는 본 논문이 제안하는 솔루션을 전체적으로 설계한다. 그리고 마지막으로 5장에서는 결론 및 향후 연구방향에 대해서 기술한다.

II. 관련연구

2.1 MDM(Mobile Device Management) 서비스

우리나라는 세계적 IT 분야에 강자로 그 중에서 모바일 산업은 매우 영향력이 크다고 할 수 있다. 삼성전자나 LG전자 등을 통해서 하루에도 수백 가지 휴대폰 제품이 출시되고 있으며 최근에는 PC 운영체제와 유사한 스마트폰 출시가 가장 많이 되고 있다. 스마트폰은 매년 10 ~ 20%의 매우 높은 성장률을 유지하며 휴대폰의 주류가 될 것으로 예측하고 있고 이런 스마트폰이 주목을 받으면서 대두가 되고 있는 것 역시 바로 보안문제라고 할 수 있다. 안드로이드 OS나 IOS 등이 탑재되면서 발생하는 보안 문제가 최근 중요한 이슈가 되고 있으며 실제로 다양한 보안 위협이 나타나고 있다. 이런 휴대폰 기기의 보안 위협을 대응하기 위해 다양한 보호대책의 필요성에 따라 모바일 기기의 관리 기술인 MDM이 출현하게 되었다[6].

MDM 개념은 언제 어디서나 모바일기기가 전원이 켜진 상태로 있으면 원격에서 모바일 기기를 관리할 수 있는 시스템이다. MDM의 초기 사용 목적은 원격에서 휴대폰 등 모바일 기기의 어플리케이션 배포, 데이터 및 환경설정 변경, 모바일 분실 및 장치 관리들을 통합적으로 관리해 주는 시스템이였다. 이후 짧은 서비스 다운타임과 최소의 비용으로 모바일 보안과 기능을 최적화시켜주는 시스템이었으나 최근 보안 위협에 대한 강화대책으로 관리의 필요성이 대두되면서 모바일 보안의 핵심요소가 되었다. 모바일 VPN을 통해 안전하게 보안된 통신을 제공하여 메일, 웹, 그룹웨어, USB 저장매체 등 다양한 통신 채널에 대해 포괄적 보호기능을 제공함과 동시에 중앙 관리 콘솔을 통해 전사적 모니터링 및 사용자 환경에 대한 통제를 수행할 수 있다. 그러나 이러한 MDM은 사용자에게 매우 많은 제약을 가져오게 하였으며 특히, 개인이 사용하는 모바일 단말에 이러한 MDM을 설치하여야 하는 기업 환경에서는 부작용이 속출하고 있는 실정이다. 이러한 부작용을 보완하는 솔루션이 필요하며 본 논문에서 제안하고자 한다.

2.2 MAM(Mobile App Management) 서비스

MDM의 진화는 빠르게 이어졌고 많은 활용도 가져온 것이 사실이다. 이는 스마트 기기의 확산이 급격히 전개되고, 시장에서의 오구가 계속 높아지고 있기 때문이다. 특히 개인 스마트 기기가 업무에 활용됨에 따라 우려되는 보안 위협을 해소하기 위해서는 단순 기기관리가 아닌 애플리케이션 관리까지 수렴해야 한다는 요구가 높아짐에 따라 MDM은 MAM으로 진화하고 있으며 지속적인 앱 관리가 가능해진 실정이다. 이러한 변화는 유선 네트워크에서의 요구와 일치한다. 최근 정보보안의 흐름을 살피면 지능형지속가능위협과 같은 중요한 공격의 대두 그리고 애플리케이션에 대한 통제 요구가 높아지고 있는 실정이다.

고도로 지능화된 사이버 위협이 스마트폰, 스마트 패드와 같은 모바일 기기에서도 전개될 것이기에 보다 강력한 보안성을 유지하기 위해서는 기기뿐만 아니라 기기의 애플리케이션까지 연계한 보안이 요청되며, 이에 발맞춰 MDM은 단순 기기관리에서 보안을 위한 애플리케이션까지 확장된 형태의 MAM으로 진화하고 있는 것이다[8].

MAM 솔루션이 가지는 가장 큰 장점은 튼튼한 BYOD 보안을 구현할 수 있다는 점으로 기존 MDM 솔루션은 기업에서 지정하는 앱만 설치, 구동할 수 있었다. 즉, 직원들이 자신의 모바일 기기를 자기 마음대로 사용하지 못하게 되는 상황을 만들었고, 이는 업무효율성 제고에 오히려 악영향을 가져왔다. 또한 MDM 솔루션은 특성상 스마트폰에 있는 대부분의 데이터를 열람할 수 있어서 결코 개인정보보호 이슈에서 자유로울 수 없으므로 강제적으로 개인에게 이러한 솔루션을 강요하는 것은 매우 위법적인 방법이다[9].

반면 MAM 솔루션은 엔터프라이즈 앱과 그 앱에서 생성, 열람, 변경되는 데이터만 관리하기 때문에 개인정보침해에 대한 요소가 크게 줄어든다. MAM 솔루션은 개인의 영역과 기업의 영역을 나눠서 관리한다는 개념이다. 하지만 MDM과 같은 강력한 제어가 불가능하므로 개인이 소유한 스마트폰의 경우 보안상 허점이 발생할 수 있다는 단점을 가지고 있다.

III. 본론

이번 장에서는 다중 유심을 이용한 MSM & MTM 즉, e-BYOD 솔루션을 제안하고자 한다.

3.1 e-BYOD 시스템 구성

본 논문에서 제안한 e-BYOD 시스템의 구성도는 그림 2와 같다. 멀티 유심을 사용하는 사용자는 모바일 스위칭 관리(MSM - Mobile Switching Management)를 통해 제어를 받으며 각기 스위치될 때마다 해당 환경에 적합한 형태로 운용할 수 있다. 즉, 개인이 사용하는 유심으로 변환이 될 경우는 어떠한 제한도 가해지지 않으며 자유롭게 모바일 폰을 사

용할 수 있다. 하지만, 이때는 모바일 오피스를 전혀 사용할 수 없으므로 업무와는 무관하다. 또한 업무 시 발생한 어떠한 데이터도 공유되지 않는다는 장점을 가진다. 데이터는 이동통신망을 통해 서비스될 때 모바일 트래픽 관리장치(MTM-Mobile Traffic Management)에 의해 그림 2와 같이 보안 서비스를 받게 된다.

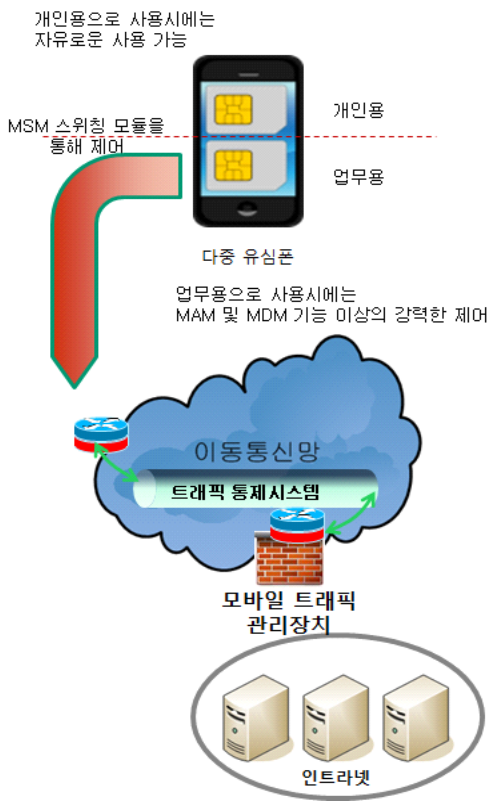

그림 2. e-BYOD 시스템 구성도
Fig. 2. e-BYOD System Architecture

네트워크 기반 모바일 오피스 관리 솔루션은 그간 모바일 오피스 환경에서 기피 대상이 되었던 네트워크 보안 솔루션의 한계를 효과적이고 합리적으로 극복할 수 있다. 모바일 오피스 단말의 모든 트래픽에 대해 유선 이상의 정교한 고성능의 네트워크 보안을 적용할 수 있는 방안이라 할 수 있다. 다만, 이동통신망의 경우 특정한 이동통신 사업자에 의해 제공되는 망을 사용하므로 일반 사용자나 기업이 이동통신망에 직접적인 보안을 적용하는 것은 거의 불가능하며 본 논문에서는 이동통신망 사업자가 이를 적극적으로 지원한다는 가정 하에 설계를 진행해 나가고자 한다.

3.2 MSM - Mobile Switching Management

본 논문에서 제안하는 MSM은 현재 국내에서는 사용되지 않는 듀얼 유심폰을 대상으로 한다. 동남아나 외국에는 사업가나 직장인들이 사업상의 목적으로 듀얼유심이 장착된 스마트폰을 사용하는 경우가 많다. 국내에는 이동통신 사업자들의 이해관계나 스마트폰 제조업체의 이해관계로 인해 출시되지 못하고 있는 상황이나 향후에는 도입을 검토 중에 있다. 본 논문에서는 삼성전자의 갤럭시 S 듀오스를 대상으로 설계하였다. 따라서, 본 논문에서 제안하는 전체 구성은 그림 3과 같으며 다음과 같은 전제를 갖는다.

- 이동통신 가입자는 듀얼 유심폰을 사용
- 이동통신 망은 별도의 보안 솔루션이 적용되지 않음
- 제안된 보안 솔루션은 이동통신망 내부 코어망에 설치

본 논문에서 제안하는 MSM은 스마트폰에 앱 형태로 설치되어 운영된다. 이동통신 가입자가 해당 스마트폰을 개인용으로 사용할 때와 업무용으로 사용할 때 사용하는 유심이 다르며 스마트폰의 앱을 통해 유심을 동적으로 교체할 수 있다. 이때 MSM은 각각의 유심이 동작할 때의 환경이 서로 물리적으로 분리되게 유지하는 기능을 갖는다. 즉, 동일한 스마트폰을 사용하더라도 물리적인 저장장치가 달라 개인용으로 생성된 문서나 사진 등을 업무용 유심이 동작하는 환경에서는 사용할 수 없다. 또한 업무용으로 사용할 때의 자료를 개인용 유심에서는 사용할 수 없는 특징을 가진다. 이처럼 하나의 스마트폰을 통해 두 개 이상의 환경을 자동적으로 변환해주는 기능을 MSM이라고 한다.

3.3 MTM - Mobile Traffic Management

본 논문에서 제안하는 MTM은 현재 유선에서 사용되는 보안 서비스를 모바일 환경에서도 적용하기 위한 방안을 제안한 것으로 기존의 보안 장비들을 통해 유선상의 보안을 적용해 왔지만 이동통신망의 경우 망 사업자가 망을 관리하므로 개인이나 기업이 이동통신망에 대한 보안을 직접 할 수가 없는 상황이다. 이를 보완하기 위해 이동통신망 사업자가 적용할 수 있는 이동통신 관리 방안을 MTM이라고 한다.

기존에 연구되었던 모바일 트래픽 집중 시스템[1][2]의 경우에는 이론적인 연구에 불과하였지만 본 논문에서는 이를 보다 구체적으로 설계하여 실제 이동통신망에 적용할 수 있는 방안을 제시하고자 한다. 네트워크 기반 모바일 오피스 관리 솔루션은 모바일 트래픽 집중 시스템과 모바일 트래픽 관리

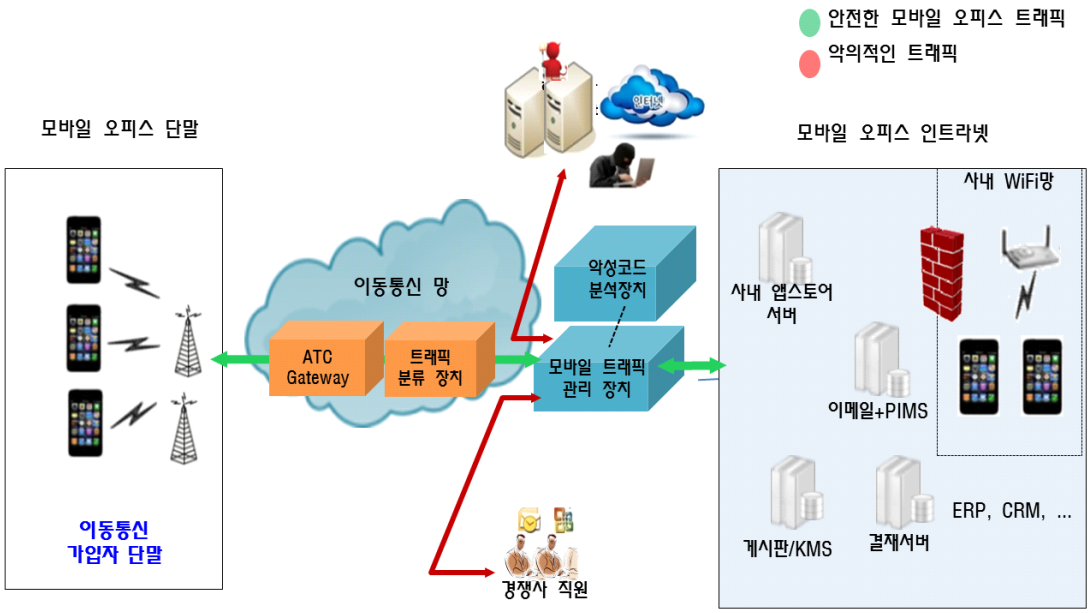

그림 3. e-BYOD 세부 시스템 구성도
Fig. 3. System Detail Architecture of e-BYOD

시스템으로 구성되며 모바일 트래픽 집중 시스템은 이동통신 망내의 코어 장비와 기관/기업 트래픽 집중 시스템으로 구성된다. 모바일 트래픽 관리 시스템은 기관/기업용 모바일 트래픽 관리 장치, 악성코드 분석장치로 구성된다.

3.4 트래픽 분류 장치

트래픽 분류장치는 ATC 게이트웨이로부터 집결된 트래픽을 수신하여 고속의 트래픽 DPI 분류 엔진 모듈을 통하여 종류를 파악하고 트래픽의 목적에 따라 트래픽을 분류하여 분류

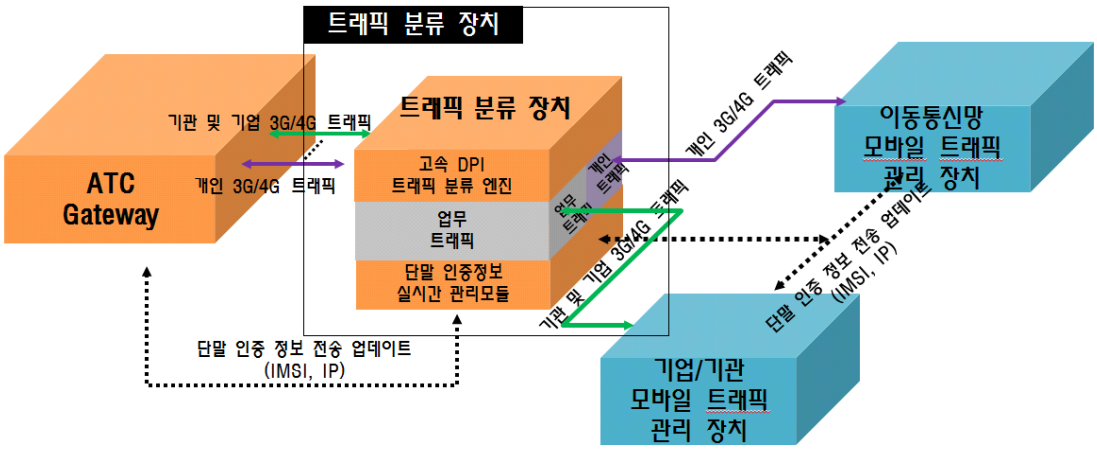

그림 4. 트래픽 분류 장치 구성도
Fig. 4. Traffic Classification Device Architecture

된 트래픽을 각 목적의 장치에 전송하는 기능을 수행한다. 수신된 트래픽이 기관 및 기업의 트래픽인 경우 본 논문에서 제안하는 구성에 따라 기관 및 기업의 모바일 트래픽 관리 장치에 전송하거나, 공용 트래픽 관리 장치에 전송한다. 수신된 트래픽이 개인용 트래픽인 경우 이동통신망에 설치된 트래픽 관리 장치에 전송한다. 트래픽 분류 장치의 또 하나의 주요 기능으로 ATC 게이트웨이에서 실시간으로 수신한 단말의 인증정보를 트래픽 관리 장치에 전송한다. 다음 그림 4는 트래픽 분류 장치의 구성도를 나타내고 있다.

트래픽 분류 장치의 고속 DPI 트래픽 분류 엔진은 모바일 트래픽을 기관 및 기업 또는 개인으로 구분하며, 특히 개인 트래픽의 경우 개인의 사생활 침해를 최소화하기 위하여 일상적인 트래픽은 이동통신망 내에 위치하는 트래픽 관리 장치를 통해 분석되며, 트래픽에 내에 데이터 페이로드 부분의 의심스러운 트래픽에 대해서는 기관 및 기업 트래픽으로 분류하여 좀 더 정밀한 DPI 기능을 수행하게 한다. 분류된 트래픽은 각각의 트래픽 관리 장치로 전달되어 각 장치 내에서 2단계의 수준의 DPI 기능을 수행하게 된다. 단말 인증정보 실시간 관리 모듈은 ATC 게이트웨이로 부터 단말 인증 정보를 실시간으로 수신하고 수신된 데이터를 기업 및 기관 모바일 트래픽 관리 장치와 이동통신망 내의 트래픽 관리 장치에 전송하여, 본 논문의 제안 내의 모든 장치들은 실시간적으로 단말의 IP를 동기화하게 된다.

3.5 모바일 트래픽 관리 장치

모바일 트래픽 관리 장치는 트래픽 분류 장치를 통해 집중된 모바일 트래픽을 안전하게 관리하는 장치로 기존 유선상의 보안 장비와 유사한 기능을 가지나 모바일이란 특수한 환경에 맞도록 설계하는 것이 가장 중요하다. 또한 모바일 트래픽은 음성, SMS, MMS, 데이터 등이 다양하게 복합적으로 서비스되는 환경이므로 이러한 특성을 잘 파악하여 설계하도록 한다. 그리고, 최근 가장 큰 사회적 이슈가 되고 있는 스미싱을 해결하기 위해 문자메시지 내부에 표시된 링크를 추적할 수 있는 기능도 포함하여야 한다.

그밖에도 유선상에서 필요한 보안 기능 및 모바일 환경에서 필요한 보안 기능을 표 1과 같이 정의하였다.

표 1. 악성코드 분석 장치 기능
Table 1. Malware Analysis Device function

항목	주요 기능
코드 추출 기능	• 복사된 모바일 오피스 단말의 인터넷 하향 트래픽 패킷을 분석하고 각 패킷에 포함된 코드를 추출하는 엔진
	• 고성능 병렬 트래픽 처리 구조와 대용량 세션 처리를 위한 동시 세션 처리 방식 사용
코드 리버싱 기능	• 코드에 대한 행위 속성 프로파일링 DB 생성
능동형 필터 DB 분석 기능	• 코드 행위 속성 프로파일링 DB와 능동형 필터 DB를 비교 분석하여 코드가 기존 능동형 필터 DB에 포함된 코드임을 판별하는 엔진 • 정확하고 신속한 데이터베이스 비교를 위하여 최적화된 데이터베이스 구조 사용
악성코드 실시간 분석 기능	• 코드를 악성코드 분석 가상 머신상에서 코드의 행위 속성 프로파일링 DB 요소별로 참조하면서 자동 동적 수행하고, 가상 머신 내의 실행 결과를 분석하면서 코드의 악성 유무를 분석하는 엔진 • 코드의 악성 유무가 판단되면, 능동형 필터 DB 저장 모듈을 통해 능동형 필터 데이터를 데이터베이스에 저장

3.6 악성코드 분석 장치

능동형 악성코드 분석장치는 악성코드의 행위기반 분석 엔진의 실시간 검증 기술을 통해 능동형 악성코드 오토마타 DB를 실시간적으로 생성하며, 악성코드 행위 유형 속성에 대한 프로파일의 오토마타 DB를 자가 증식하여 같은 유형의 변종 악성코드를 능동적으로 분석 할 수 있는 장치이다[4]. 이는 패턴 기반의 악성코드 탐지 방식의 한계를 극복하고 유사 악성코드 및 예측 변형 가능한 변종 악성코드 조차 실시간적으로 탐지할 수 있는 자가 증식형 능동형 악성코드 분석장치이다.

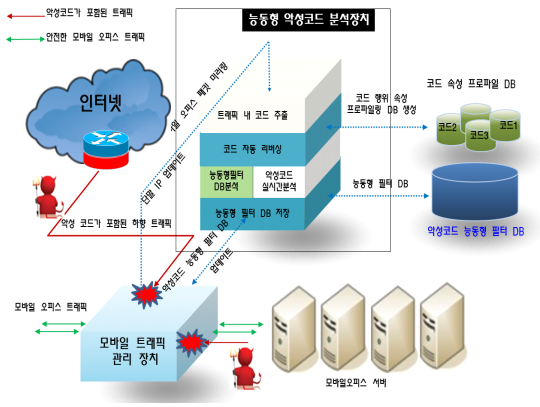

그림 5. 능동형 악성코드 분석장치 구성도
Fig. 5. Active Malware Analysis Device Architecture

능동형 악성코드 분석장치는 모바일 트래픽 관리 장치로부

터 모바일 오피스 단말의 인터넷에서 하향으로 유입되는 모바일 트래픽(3G/4G/WiFi)과 모바일 오피스에서 단말로 향하는 하향 트래픽을 실시간으로 OUT OF PATH 방식으로 트래픽 관리 장치로부터 미러링 받아 미러링 된 트래픽 내의 패킷에서 코드를 추출한다[5]. 추출된 코드는 자동 리버싱 엔진을 통하여 코드 행위 속성 프로파일 DB 형태로 저장하여 능동형 필터 DB와 비교 분석 가능한 대상이 되게 한다. 능동형 필터 DB분석 엔진에서는 추출된 코드가 이미 능동형 필터 DB에 존재하는 경우 기존 악성코드인 경우이므로 추출된 코드에 대한 분석을 종료한다. 추출된 코드가 능동형 필터에 존재하지 않는 경우 추출된 코드는 다시 악성코드 실시간 분석 엔진을 통해 실시간 적으로 자동 분석되며, 동적 분석 결과 코드가 악성임이 판별되면, 추출된 코드에 대한 프로파일링 데이터를 기초로 하여 능동형 필터 DB를 데이터베이스에 저장한다. 능동형 악성코드 분석장치는 신규 악성코드 능동형 필터 DB가 생성되는 경우 변경 사항을 모바일 트래픽 관리 장치에 실시간으로 업데이트 한다. 그림 5는 능동형 악성코드 분석 장치를 이루는 핵심 모듈에 대한 구성 및 모바일 트래픽 관리 장치간의 연동 관계를 표시한 그림이다.

표 2. 모바일 트래픽 관리 장치 기능
Table 2. Function of Mobile Traffic Management Device

항목	주요 기능
악성 유해 사이트 차단 (스미싱 방지)	• 블랙 리스트 URL, IP 기준 접속 차단 • 사용자정의 사이트 차단 - URL, IP • 국가별 접속 제한
모바일 DDoS 차단	• SYN Flooding 공격 차단 • TCP/UDP Flooding 공격 차단
모바일 오피스 단말 트래픽 관리	• 모바일 오피스 단말에서 발생하는 양방향 트래픽에 대한 로그 기록
유선 보안 기능	• 단말 트래픽 필터링 • IP 패킷 필터링 • 상태기반감시 • 양방향 정책 수립 가능 • 사용자 정의 설정 • 세션 타임 아웃 • 네트워크 그룹지정 관리 • 오브젝트 그룹지정 관리 • 트래픽 제한
단말 관리 기능	• 단말 등록 및 관리 • 부서별 단말 그룹 관리 • 직책별 단말 그룹 관리 • 단말 인증 정보 관리 • - 단말 IMSI, • - 단말 IP 실시간 연동 • 단말 인증 정보 실시간 업데이트 • - 트래픽 집중장치 연동
정보 유출 방지 기능 (DLP)	• 이메일 첨부 파일 유출 차단 • 모바일 웹, 웹 메일 첨부 파일 유출 차단 • FTP 파일 유출 차단 • 메신저 파일 전송 유출 차단

이러한 능동형 악성코드 분석장치의 주요 핵심 모듈은 다음의 표 2와 같으며 모바일 악성코드를 분석하여 스마트폰이 좀비화 되는 것을 방지하는 기능을 갖는다.

본 논문에서 제안한 이러한 세부 시스템을 통하여 이동통신에 대한 보안 서비스를 보다 강화랄 수 있으며 유선상에서 제공되는 보안 서비스 이상의 서비스를 제공할 수 있다고 판단한다.

Ⅳ. 실험 및 고찰

본 논문에서 제안한 내용을 검증하기 위해서는 통신사의 망을 사용하거나 비슷한 형태로 망을 구성해야 한다. 따라서 본 실험에 사용한 갤럭시 S Duos에 USIM 칩을 두 개 장착하였고 표 3과 같이 USIM에 따라 각기 다른 IP가 설정되어 실험하였다.

표 3. 실험 환경 설정 정보
Table 3. Test setup information

종류	IP Address	용도
모바일 폰	Samsung 갤럭시 S Duos	듀얼폰
USIM 1	28.199.229.145 (MAC-78:F7BE:CD:71:B2)	개인용
USIM 2	100.123.156.164 (MAC-78:F7BE:CD:71:B2)	기업용
통신	PPTP 터널링 사용	VPN

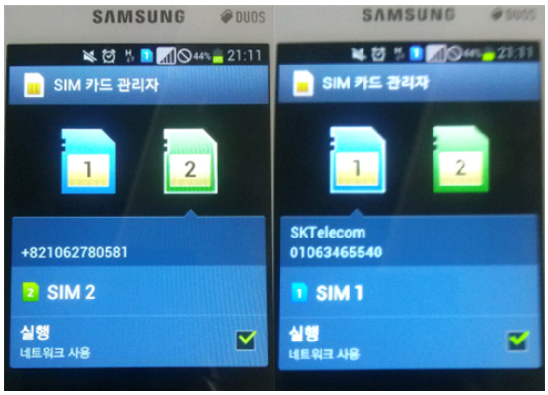

그림 6. 스마트폰 Dual USIM 화면
Fig. 6. Dual USIM Display of phone

그림 6과 같이 스마트폰에서 SIM 카드 관리자를 통해 사용자가 사용할 때 활성화된 USIM을 선택할 수 있다. 이를 각각 개인용도와 업무용도로 나누어 실험하였다. 본 논문에서 사용한 실험의 구성은 다음 그림 7과 같다. 해당 USIM을 통해 LTE로 통신하였으며 다만 통신사 망 내부에 MTM을 설치할 수 없으므로 실험망에 트래픽 분류장비를 설치하여 실험하였고 이 장비에서 IP를 통해 정보를 구분하여 USIM1의 보안정책은 인터넷망으로 통과로 USIM2의 정보는 악성코드 URL 검사로 보안 설정 후 실험 하였다.

LTE 통신이 실험망으로 연결되기 위해서는 VPN 터널링을 사용하여야만 한다. 스마트폰 설정에서 PPTP를 설정한 후 VPN 접속 주소를 실험망에서 사용하는 주소를 입력한 후 실험망의 VPN 서버와 터널링을 통해 봉 실험을 진행하였다.

그림 7. 실험 환경 구성도
Fig. 7. Test environment Architecture

위의 실험환경을 바탕으로 개인용 USIM을 사용할 경우에는 업무서버에 접근할 수 없으므로 보안 정책에서 인터넷으로 통과되며 업무용일 경우는 악성코드 URL 검사를 진행하며 이때 필터링 장비로는 WebCure[3] 장비를 사용하여 실험하였다. 다음 표 4는 업무용일 경우 필터링한 링크와 필터링 결과를 나타내고 있다.

표 4. 실험 데이터 및 결과
Table 4. Test data and result

항목	내용	처리 결과
정상 링크	http://www.naver.com	통과
악성유포지	http://www.korarthro.com/mm/index222.html	차단
악성유포지	http://222.239.252.41/_img/index.html	차단
악성유포지	http://198.2.221.201/luku.html	차단
악성유포지	http://www.korarthro.com/mm/index222.html	차단
악성경유지	http://www.dkilbo.com	통과

위 실험의 결과와 같이 모바일 환경에서 브라우저를 통해 인터넷에 접속할 때 악성코드가 유포되는 유포지를 포함할 경우는 차단되는 것을 알 수 있다. 다만, 악성코드 경유지의 경우에는 크롤링 등의 추가적인 검사를 하지 않으므로 통과되는 것을 알 수 있다. 본 실험을 통해 모바일 환경에서도 충분히 악성코드에 대한 트래픽을 차단할 수 있다는 것을 확인하였다. 향후에는 모바일 폰을 제어하는 것이 아니라 트래픽을 중심으로 보안을 처리할 경우 훨씬 더 효율적이라고 볼 수 있다.

V. 결론

최근 기업들은 기업용 폰 도입이 매우 활발해지고 있고 또한 기업용 폰을 이용한 모바일 오피스가 매우 활발해지는 상황이다. 이러한 기업이나 기관의 모바일 보안을 위해 보안 기능을 적용하지 않을 수 없는 것이 현실이기는 하지만 개인이 사용하는 만큼 개인의 의사나 프라이버스로부터 자유롭지 못해 많은 직원들이 불만을 가지고 있다. 또한 이러한 불만이 조직과 개인의 갈등으로 발전되는 부작용을 해소해야만 한다.

본 논문에서는 이러한 기업용 폰의 보안 장치를 통해 조직과 개인의 갈등을 해소하고 향상된 보안 기능을 제공하는 것을 목표로 연구하였다. 안전한 모바일 오피스를 구축하여 기업이 보다 폭넓은 오피스 문화를 형성할 수 있으며 기존의 폰 자체에 앱 등을 설치하는 것보다 매우 현실적이고 효과적인 방안을 제시하였다. 본 논문에서 제안한 MSM이나 MTM을

통해 보다 안전한 기업 모바일 보안을 이룰 수 있을 것으로 확신한다.

또한 이동통신사는 해외에서와 같이 스마트폰에 멀티유심을 지원할 수 있는 정책을 세워 개인용과 기업용을 동시에 지원 가능한 서비스를 시행해야 할 것이다. 그리고 이동통신 코어망에서 보안 서비스를 시행하여 보다 안전한 이동통신 서비스를 제공해야 할 것이다. 이에 대한 추가적인 연구와 관심이 더욱 필요하다고 판단한다.

참고문헌

〔1〕 L. Byeong-Choon and S. Seung-Jung, "The Study of Privacy Security in Mobile Traffic Control Environment", International Journal of Security and its Applications, Vol. 8, No.2, pp. 178-182, 2014.

〔2〕 Hyo-Nam Kim, "Realtime hybrid analysis based on multiple profile for prevention of malware", Hongik Univ. Feb. 2014.

〔3〕 Jae-Kyung Park, "A Realtime Malware Detection Technique Using Multiple Filter", Journal of The Korea Society of Computer and Information, Vol. 19, No. 7, July 2014.

〔4〕 Jin-Kyung Kim, "A design of anomaly detection with automata dynamic profile", Hansei Univ., Feb. 2014

〔5〕 Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution", Proc 33rd IEEE Symp Security and Privacy, 2012.

〔6〕 Mobile security technology research society, "Demand and outlook for mobile security technology", Data collection for Mobile security technology research society seminar, Sept. 2011.

〔7〕 Mislan RP, Cellphone crime solvers. Spectrum, IEEE, 34-39. doi: 10.1109/MSPEC.2010.5491013, 2010.

〔8〕 Androulidakis, Digital evidence in mobile phones. IT security professional magazine, Issue 13, pp 36-39, 2010.

〔9〕 Jansen WA, Delaitre A, Moenner L, Overcoming impediments to cell phone forensics. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS '08). IEEE Computer Society, Washington, DC, USA, 483-0.1109/HICSS, 2008.

〔10〕 K. Hyo-Nam and P. Jae-Kyoung, "A Study on the Malware Realtime Analysis Systems Using the Finite Automata", Journal of the Korea society of computer and information, VOL.18, NO.5, pp.69-76, 2013.

저 자 소 개

박 재 경

1994: 동국대학교 컴퓨터공학과 공학사.
1996: 홍익대학교 전자계산학과 이학석사.
2002: 홍익대학교 전자계산학과 이학박사
현 재: 학국과학기술원 사이버보안연구센타 책임연구원
관심분야: 네트워크 보안, 사이버 보안
Email : wildcur@kaist.ac.kr

김 성 진

1995: 한국방송통신대학교 전자계산학과
2014: 숭실대학교 정보과학 정보과학대학원 정보보안학과 석사
현 재: ㈜아이티노매즈 대표이사
관심분야: 사이버보안, 네트워크 보안, 데이터베이스 보안
Email : sujnkim@gmail.com