# 모바일에이전트를 활용한 기업정보 보안에 관한 연구

조상현*, 이희조**, 박현도***
고려대학교 컴퓨터정보통신대학원
e-mail : king2415@ korea.ac.kr*
heejo@korea.ac.kr**
hyundo95@korea.ac.kr***

# A Study on Business Information Security using Mobile Agents

Sang-Hyun Jo*, Hee-Jo Lee **, Hyun-Do Park***
Graduate School of Computer and Information Technology, Korea University.

**요 약**

최근 모바일 시스템은 고성능 단말기의 보급과 발달한 인터넷 환경으로 인하여 점점 방대해지고 복잡해지고 있으며, 특히 많은 회사들이 기업경쟁력 향상의 극대화,고객 서비스 만족 극대화 등의 이슈로 무선인터넷망을 활용한 다양한 데이타를 필요로 하는 모바일시스템을 빠르게 도입하고 있다. 본 논문에서는 다양한 데이타를 활용함에 있어 불가피하게 기업시스템에 접근해야 함에 있어 기업 IP 정보등 사용자 정보가 노출되는 문제점을 분석하여 모바일 에이전트를 활용하여 이것을 해결할 하나의 모델을 제시함으로써 편리하고 안정적인 응용을 보이고자 한다.

## 1. 서론

최근 이동 기술의 발달과 스마트폰등의 다양한 기능을 갖춘 단말기의 급속한 발달로 국내 스마트폰 시장이 크게 발달을 하고 있다[그림1][1]. 특히 기업현장에서는 더 빠르고 더 다양한 정보(고객정보,영업정보,주문정보)를 필요로 하는 데이터가 많아짐으로써 기업용 모바일 시스템의 도입이 많아지고 있다. 또한 이러한 정보를 보여 주기 위해서는 모바일장치에 최초 수동적으로 기업정보 등을 입력해야 하는 불편함 또한 발생하고 있다.이런 불편한 점을 해소시키고자 서비스배치프로토콜 [SLP (service location Protocol)]을 활용 하여 모바일 네트워크상에서 데이터베이스 연결, CDMA 연결등과 같은 자원을 배분하거나 사용률을 네트워크 자원에 맞게 배분하여 사용한다[2]. 특히 이 프로토콜의 특징 중 하나는 서버에이전트(server agent)와 모바일에이전트(mobile agent) 사이에서 발생하는 연결작업을 정의하고 감시 하고 네트워크 아이피를 관리한다. 그래서 현재 대부분 모바일 에이전트에서는 기업시스템에 접근하기 위한 아이피 정보를 직접 관리하고 있다. 이에 있어 악의적인 사용자에 의해 아이피 정보 및 사용자 정보의 노출에 따른 문제점이 존재한다. 이로 인해 이런 기업정보에 대한 접근 및 피해를 최소화하기 위한 관리가 필요하다.

본 논문에서는 기업정보시스템에 모바일 정보기기가 안전하게 접근할 수 있는 모바일 인증 관리시스템을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 민감정보유출기법, 그리고 모바일 에이전트에 대한 관련연구를 살펴본다. 3장에서는 제안하는 모바일인증서버시스템의 구조에 관해 설명한다. 4장에서는 제안하는 모바일인증서버시스템의 성능 및 실제 스마트폰과 연동하여 평가한 후 논문의 결론을 맺는다.


[그림 1] 국내 스마트폰 판매량

## 2. 관련연구

국내에서는 아직까지 모바일 악성코드가 발생하지 않았다. 그렇지만 해외에는 이미 600여종의 모바일 악성코드가 발생하여 피해를 유발하고 있다[3]. 현재 스마트폰의 증가로 국내의 모바일 환경 또한 더 이상 안전하지 않으며 많은 위협을 받고 있다. 또한 이러한 상황에서 기업에서 도입하는 모바일 시스템 역시 더 이상 안전을 보장 할수 없다. 그리고 2008년에 유포된 악성코드들 중 대표적인 악성코드로 Infojack의 경우 정상적인 애플리케이션이 스마트

폰으로 다운로드 될 때, 설치파일에 포함 되어 설치되고 설치완료 후 스마트폰의 보안 설정을 변경하여 단말기의 시리얼 번호,설치된 애플리케이션 등 단말기의 정보를 외부로 전송하여 2차 공격을 용이하게 한다[4] .

이처럼 사용자의 정보를 유출시키는 대표적인 악성코드는 Flexispy, PBStealer등이 있다. 이 중 Flexispy는 스파이웨어 형태로 스마트폰의 개인정보(SMS)등을 특정 웹서버로 전송하는 바이러스의 일종이다[5] .

| 발생연도 | 모바일 바이러스 종류 |
|---|---|
| 2004 | Mosquitos, Cabir's turn (Cabir.A,B), Duts Pocket PCs, Brador's turn, Skulls A,B, CabirC,D,E, Skulls.C, MGDropper, |
| 2005 | Lasco.A,, Locknut.A/ Gavino.A & B, CommWarrior.A, Locknut.B, Fontal.A, Skulls.K |
| 2006 | 29A., and Romride (NokiaLive.sis), Redbrowser, FlexiSpy |
| 2007 | TIOS/Tigraa, Spy-Wokiscan, SymbOS/Mobispy, Exploit-MP4 |
| 2008 | WinCE/InfoJack, SymbOS/Kiazha.A, SymbOS/Beselo, SymbOS/SmsSend.F, Exploit-CVE2007-0071 |
| 2009 | PWS-Banker.gen.de, PWS-BoldDie, Exploit-MSDirectShow.b |

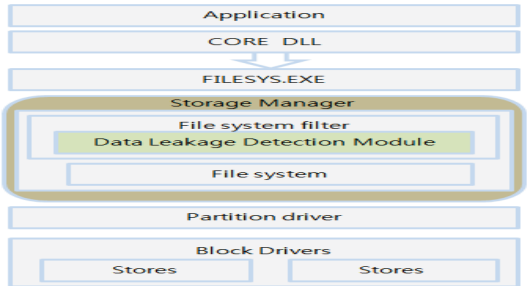
[표 1] 모바일 바이러스 종류

표 1에서 보듯이 2004년부터 매해 끊임없이 신종 모바일 바이러스들과 그 변종들이 지속적으로 출현하고 있다[6]. 이러한 사례들을 통해 모바일 사용자의 기업정보 등이 외부로 노출될 위험성을 내포하고 있다.

## 2.1관련연구

### 2.1.1 민감정보유출기술

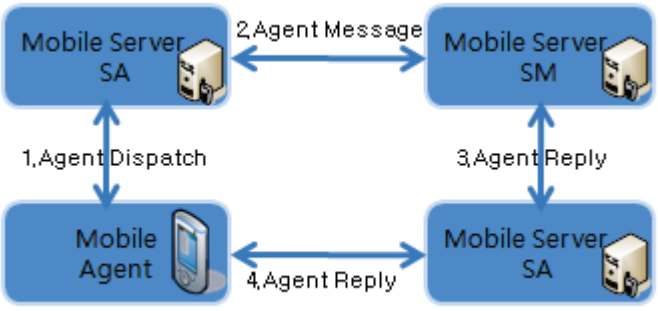
그림 2에서 알 수 있듯이,이 기술은 단말기 내부 파일로부터 민감정보가 포함된 파일을 분류 및 선정하여 외부 유출 시도 시 탐지 및 차단을 위한 시그니쳐(패턴) 생성을 한다. 그리고 그 패턴을 참조하여 파일 시스템 필터를 이용하여 파일에 I/O를 체크하여 민감정보 유출을 사전에 방지하는 기능을 한다. 민감정보로 지정된 파일에 대하여 I/O의 변경되었을 경우 이를 확인 및 지정하여 파일에 대한 정책을 생성 하여 파일에 대하여 제2차 확산을 막을 수 있다[7]. 그러나 시그니처에 대한 정책을 생성 전에는 막을 수 없는 문제점이 있으며 이를 분석하고 반영해야 하는 부담이 생긴다.




[그림.2 ] 민감정보유출기술

### 2.1.2 모바일에이전트(agent)

모바일 에이전트(agent)는 모바일에서 네트워크 및 호스트 와의 연결 및 특정작업을 대신 담당하는 역할을 한다. 그리고 특징 중에는 모바일 에이전트 사용자가 요청한 작업을 수행하는 한개의 호스트로 한정되어 수행하지 않고 또 다른 모바일 에이전트 객체가 그 작업을 수행할 수 또 다른 호스트로 이동하여 작업을 요청한다[8]. 이러한 에이전트는 특정 작업을 동작하기 위해 자신을 복제하여 작업부하를 분산하며 자신의 현재 상태를 저장하여 네트워크를 통해 이동하여 상태를 복원하여 작업에 대한 실행을 끊김없이 동작할 수 있다. 이러한 동작으로 인하여 호스트에 부하를 줄여주는 장점이 있다[2][9]. 다음 그림3은 에이전트 기본 동작원리이다.




* SA: Service Agent , * SM : Service Manager

[그림3] 모바일 에이전트(agent)

그러나 모바일 에이전트는 고정된 IP 와 사용자 정보를 보유한 상태로 서버접속을 한다. 현재 대부분의 모바일 에이전트는 IP와 개인정보를 재사용의 편리함을 위해 따로 저장하여 보관을 하고 있다. 이에 악의적인 사용자가 저장된 IP와 사용자 정보를 활용하여 서버로 공격을 시도할 수 있다. 이에 적절한 대응이 필요하다.

## 3. 제안 모델의 프레임 워크

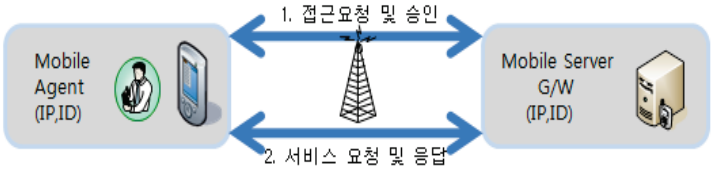
본 논문에서는 시그니처와 무관하게 별도의 인증방법을 통하여 기업정보 유출을 최소화 하고 관리에 용이성을 두고자 하는데 그 목적이 있다.

### 3.1 모바일 시스템의 문제점

그림 4,5는 일반적인 기업용 스마트폰에 적용된 일반적인 모바일시스템 과 모바일 에이전트 개인정보이다. 그림 4에서 보듯이 서버의 IP정보 와 사용자ID가 노출이 되어있다. 또한 이 파일 정보는 스마트폰 내부에 저장되어 있기 때문에 공격자에게 쉽게 노출된다. 그리고 그림 5와 같이 정보가 외부로 노출 시 기업의 IP정보 및 사용자 노출로 인하여 피해가 발생한다. 그림 5와 같은 시스템 구조는 오픈 된 네트워크 상의 호스트를 이동하면서 작업을 수행한다. 클라이언트 와 호스트 사이에 방어나 제어를 해주는 장치가 없는 구조이므로 공격자로부터 안전하게 보호하는 것이 관심사이다.

```
IP ADDRESS:192.168.0.100
PORT:5109
IDNAME:TEST
VERSION=1.0.0.1
```

[그림.4] 모바일에이전트(agent) 사용자정보




[그림.5 ] 일반적인 모바일 제안시스템

현재 대부분의 공개 네트워크는 보안에 취약한 구조를 가지고 있으며 앞에서 설명한 일반적인 기업용 스마트폰에 적용된 시스템의 구조 역시 안전을 보장받을 수 없으므로 정보를 유출하기 위한 악성코드의 공격에 대한 적절한 대응이 필요하다[10].

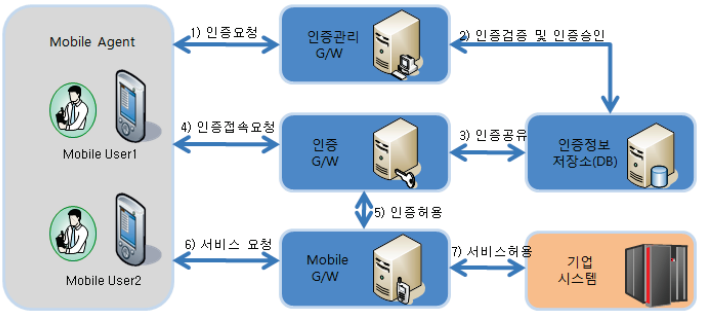
본 논문에서는 이러한 문제점을 최소화 하고자 인증서버를 두어 검증된 클라이언트만 접속이 용이하도록 시스템을 구성하였다. 또한 동일IP의 중복접속을 차단하여 검증되지 않은 사용자의 접속을 사전에 차단할 수 있다.

모바일 인증 관리시스템은 모바일 에이전트를 활용하여 어떠한 상황을(저장소에 사용자 ID,비밀번호,사용자폰번호, 사용자단말기Mac) 기반으로 하여 모바일서버의 정보를 기존처럼 저장하지 않고 인증서버에서 인증된 사용자에게만 사내 정보시스템 정보를 부여한다.

### 3.2 모바일 인증 관리시스템 제안

모바일 에이전트와 모바일인증시스템은 다음과 같이 동작을 한다. 모바일 인증 시스템은 크게 3가지로 분류된다.모바일에이전트(agent),모바일서버(인증관리G/W,인증G/W,Mobile G/W,인증정보보관소(DB)),기업시스템 등으로 구성된다. 이 시스템은 모바일 인증서버 모듈 과 모바일에이전트 모듈 사이에 각자의 연결을 스레드로 구현한다.

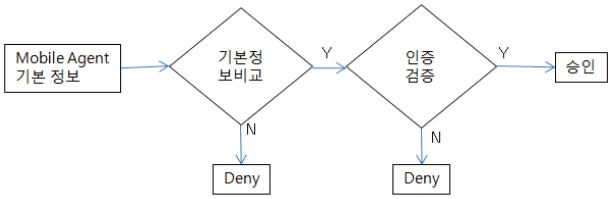
1) 인증관리G/W로 인증을 요청한다. 인증 요청 시 사용자 아이디 , 비밀번호 , 전화번호 ,단말기 MAC을 보낸다.
2) 인증 검증 전에 인증정보 저장소에 중복사용자가 존재하는지 확인 후 인증 IP 및 인증코드를 부여한다.
3) 인증성공 후 인증 정보는 인증G/W와 공유하여 모바일 에전트의 접속을 위해 대기한다.
4) 인증성공 후 인증 G/W로 모바일 에이전트에 대해서 접속을 허용한다. 이때 인증 관리 G/W 연결을 차단한다.
5) 인증이 허용된 사용자는 인증G/W를 통하여 요청자가 현재 사용 중인지 여부를 체크 후 발급 또는 갱신 후 인증 G/W에 정보를 등록한다.
6) 모든 인증단계가 마무리 되면 모바일 에이전트는 인증IP등을 통한 인증정보를 기반으로 모바일 G/W에게 서비스를 요청하여 작업을 수행할 수 있다. 만약 IP정보 및 아이디 정보가 노출이 되어도 실제 IP가 아닌 인증 전 IP이므로 시스템에는 장애가 발생하지 않는다. 인증IP의 주기는 1일이며 매일 최초 접근 시 인증IP를 부여받는다.또한 인증번호 역시 주기는 1일이며 인증IP부여 시 동일하게 발급을 한다. 인증IP,인증번호, 단말기MAC, 사용자ID/PW,의 정보가 전부 일치 않을 시는 인증 G/W에서 원천적으로 접근을 막는다.




[그림6] 모바일 인증 시스템

### 3.3 Certification (인증) 시스템 구조

인증서버G/W 와 인증에이전트로 구성되며 인증서버G/W에서는 별도로 모바일에이전트의 인증 정보를 보안이 강화된 데이터 베이스에 보관하다가 모바일에이전트에서 인증에이전트가 인증을 요청하면 인증서버G/W에서는 인증정보 데이타베이스를 조회한 후 이전에 인증을 통하여 사용한 이력이 있는지, 혹은 현재 새롭게 허가 받은 사용자인지 확인 후 인증키 와 인증IP를 부여하는 방식이다. 그리고 원할한 인증을 위하여 인증서버G/W는 이중화서버방식으로 구현한다. 또한 사용자의 인증정보를 서버에서 받아 사용함으로써 인증파일을 시스템 내에 보관해 둘 필요가 없는 구조이므로 안전한 대처방안이 된다.

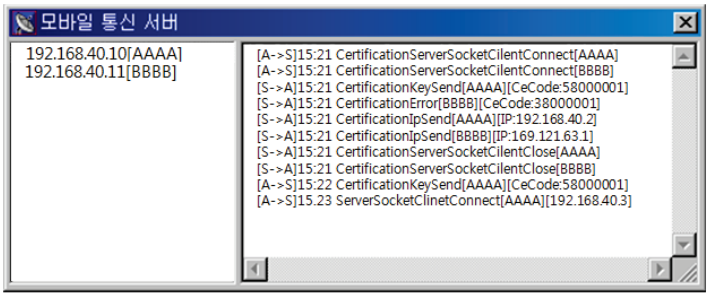



[그림7] 모바일에이전트(agent) 인증정보검증 구조도

## 4. 구현 및 실험

모바일 인증관리 시스템을 구현하기 위한 모바일 장치는 HP iPAQ 3800 시리즈이며, 운영체제는 Microsoft사의 Windows Mobile 2003 Se을 탑재하였다. 한편 모바일 서버는 Windows XP Professional을 탑재한 랩탑이고 모바일 서버 관련소프트웨어는 Microsoft Visual C++ 6.0로 구현하였다. 모바일서버의 첫번째 역할은 무선 디바이스로부터 사용자의 접속을 수용하는 것이다. 그리고 사용자의 원활한 접속을 위해 사용자 별로 스레드를 생성한다. 새로운 접속이 발생시 인증데이타베이스에서 이전 사용자 인지 새로운 사

용자인지를 체크하여 모바일서버 접근을 허용한다. 그림 8은 스마트폰과 인증서버 사이에 인증을 위한 일련의 과정을 순차적으로 나타낸 것이다. 먼저 서로 다른 사용자는 인증 서버로 접속을 시도한다. 인증서버는 사전에 등록된 인증데이타베이스를 검색하여 사용자의 정보를 확인하고 정상적인 사용자인경우 인증IP 와 인증키를 전송한다. 허가된 사용자는 인증 IP 와 인증키를 이용하여 내부시스템으로 접근하여 서비스를 요청할 수 있다. 그러나 정상적인 사용자가 아닌 경우는 불필요한 인증IP 와 인증키를 전송한다. 이에 비인증 사용자는 사내시스템의 IP정보를 알 수 없으므로 접근을 최소화 할 수 있다.




[그림8] 모바일 인증 시스템 동작과정

그림 9는 인증을 요청 후 성공하면 인증키와 인증IP를 부여한다. 그리고 인증번호와 인증IP를 통하여 기업시스템으로 서비스를 요청한다. 인증IP 및 인증일이 있어서 모바일 에이전트(agent)가 로그인 시 활용된다.

```
<MOBILE>
  <CERT_IP>192.168.20.10</CERT_IP>
  <IDNAME>9192</IDNAME>
  <CERT_DATE>20100310</CERT_DATE>
  <VERSION>100001</VERSION>
</MOBILE>
```

[그림9] 모바일 인증 후 모바일 에이전트(agent) 정보

인증IP와 소스상에 공용변수로 존재하며 모바일 에이전트가 로그 아웃 시 소멸한다.인증키는 64비트 암호화되어 레지스트리에 저장되며 발급 후 1일이 지나면 인증저장소 에서 소멸한다. 인증키 노출 시 제2차 공격을 막기 위해 인증키의 주기는 1일로 하였다.

## 5. 결론

본 논문에서는 인증G/W를 활용하여 인증되지 않은 모바일 에이전트는 기업정보시스템의 접근을 최소화 할 수 있는 시스템을 제안하였다.이를 위해 스마트폰과 모바일서버 사이에 인증역할을 하는 인증G/W를 설계하고 구현하여 인증여부를 체크하여 기업정보IP의 노출을 최소화 할 수 있있다는 것 확인하였다. 그러나 인증G/W라는 Corpus를 이용하여 인증되지 않은 모바일 에이전트는 차단되거나 접근하는데 있어 최소화 할 수 있었으나 기존보다 접속에 약간의 시간이 더 소요된다. 향후 시그니쳐 분석에 따른 사전 차단 기능에 대한 개선이 요구된다. 그래서 접근 전후 차단에 대한 범용성을 향상 시킬 계획이다.

## 6. 참고문헌

[1]. http://korea.researchonasia.com(디지털타임스,로아그룹)
[2]. E. Guttman, C. Perkins, J. Veizades, and M. Day, "Service Location Protocol, Version 2" IETF, RFC 2608, June 1999.
[3]. 심재홍*, 이석래** :" 모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석" December 2009
[4].Eray Erkut, Ingo Zehenthofer : "A Guide To Embedded Systems Security ", December , 2008
[5].FlexiSpy is a product of a company called Vervata (http://www.vervata.com/) . The FlexiSpy homepage is at http://www.flexispy.com/.
[6]. Zahraa F. Muhsen, Shadi Aljawarneh, Ayman Al Nsour, Nedia Fadhil Muhsain : "Ensuring the Survivability of Mobile Content ", August 2009
[7]. 김 기 영*, 강 동 호* : "개방형 모바일 환경에서 스마트폰 보안기술" , October 2009
[8]. 박선희 ," 에이전트(agent)의 발전 및 응용에 관한 연구", 목원대 석사학위 논문 , 2000
[9]. D.Chess, C.Harrison, A.Kershenbaum. "Mobile agents:Are they a good idea, In Mobile Object Systems: Towards the Programmable Internet", Vol. 1222 of Lecture Notes in Computer Science, Spring-Verlag, 1997.
[10]. Michael S. Greenverg, Jennifer C. Byington, "Mobile Agents and Security," IEEE Communications