논문 14-39C-01-01

한국통신학회논문지(J-KICS) '14-01 Vol.39C No.01
http://dx.doi.org/10.7840/kics.2014.39C.1.1

상황 인지 기술과 모바일 단말 관리 기술을 이용한 비인가 단말 탐지 및 차단 기법

문 지 만◆, 정 수 환°

A Scheme for Detecting and Preventing an Unauthorized Device Using Context Awareness and Mobile Device Management

Jiman Mun◆, Souhwan Jung°

요 약

본 논문에서는 AP와 모바일 단말을 이용하여 내부 네트워크의 정보 유출 및 변조를 방지하고 비인가 단말의 탐지 및 접속 차단을 하는 방법을 제안한다. 기존의 비인가 단말 탐지 및 차단 기법은 Evil Twin과 같은 형태의 탐지 기법이 주를 이루고 있다. 그러나 기존의 연구들은 다양한 형태로 발생하는 보안 사고를 모두 해결할 수 없으며 다양한 환경의 네트워크에서 효과적으로 대응하는데 문제가 있다. 이러한 문제를 해결하기 위해 기업에서는 다양한 정책과 가이드라인을 통해 대비를 하지만 꾸준히 늘어나는 보안 문제로 인해 모든 것을 대비하기는 어려운 상황이다. 본 논문에서는 위의 문제를 해결하기 위해 상황 인지 기술과 모바일 단말 관리 기술 기반의 비인가 단말 탐지 및 차단 기법을 제안한다. 먼저, 모바일 단말이 내부 네트워크의 진입을 시도할 때 모바일 단말의 상황 정보를 인지하여 모바일 단말의 접속 허가 여부 및 권한을 판별하고 이 결과 값을 이용하여 모바일 단말에게 알맞은 관리 기술을 적용하여 내부 데이터 유출 및 침해를 방지한다.

Key Words : Context Aware, Mobile Device Management, Mobile Security, Bring Your Own Device, Authentication

ABSTRACT

This paper proposed a method that prevents data leakage and modulation and detects an unauthorized device by using AP and mobile device. Most of existing method for detecting and preventing an unauthorized device are similar to type of Evil Twin. However, in previous studies can not resolve many security accident and have the problem to cope with effectively security accident on various network. In order to solve these problem, companies prepare security accident through the varies policy and guideline. but It is hard to prevent all security accident because it is consistently increasing everyday. This paper suggests technique of detecting and preventing an unauthorized device using Context Awareness and Mobile Device Management. Firstly, when mobile device go into internal network, server distinguish access permission and authorization of mobile device using acquiring the conetxt information of mobile device. By using this result, server applies the appropriate management technique to the mobile device for leakage and accident of internal network.

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (NIPA-2013-H0301-13-1003)

◆ First Author : 숭실대학교 전자공학과 통신망보안 연구실, jmmun@ssu.ac.kr, 학생회원

° Corresponding Author : 숭실대학교 정보통신전자공학부 통신망보안 연구실, souhwanj@ssu.ac.kr, 종신회원

논문번호 : KICS2013-10-466, 접수일자 : 2013년 10월 28일, 심사일자 : 2013년 12월 11일, 최종논문접수일자 : 2013년 12월 20일

Ⅰ. 서 론

BYOD(Bring Your Own Device)는 개인이 소유하고 있는 단말기를 업무에 바로 활용하는 것을 말한다. 2011년 5월에 발표한 IDC 보고서에 따르면 이미 업무에 사용되고 있는 단말기의 40.7%가 개인 소유의 장비이다. 또한, Cisco의 시장 조사에 따르면 "BYOD는 지금 가장 성장하고 있는 트렌드로서, 근로자의 78%는 일을 하는데 자신의 기기를 소유하고, 44%는 적어도 일주일에 한 번 재택근무를 하여 매년 2500달러를 절약한다."고 발표하였다.[1] BYOD가 점차 많은 곳에서 적용됨에 따라 자연스럽게 스마트폰 시장 및 관심이 커지고 있다.

스마트워크는 ICT(Information & Communication Technology) 기술을 이용하여 기존의 사무실을 벗어나 시간과 장소에 구애받지 않고 언제 어디서나 효율적으로 일할 수 있는 업무 개념을 말한다.[15] 이 기술은 스마트폰의 높은 이동성과 편리성으로 기존의 컴퓨터가 가지고 있던 기능들을 언제, 어디서나 이용할 수 있게 함으로서 사용자로 하여금 사회적, 경제적 효과를 얻을 수 있도록 한다. 그러나 많은 장점을 가지고 있는 스마트폰은 회사의 기밀 정보 유출 및 스마트폰 해킹 등의 피해로 인해 심각한 문제가 대두되고 있다.[2] 또한, 악의적인 사용자에 의한 공격이 아닌 사용자의 부주의로 인한 스마트폰의 분실 및 도난으로 인해 기업의 중요 정보 노출 사고의 비율도 증가하여 기업에서는 MDM(Mobile Device Management) 기술을 이용하는 기업의 수가 증가하고 있다. 또한, 불법 단말의 침입을 막기 위해 WIPS(Wireless Intrusion Prevention System), WIDS(Wireless Intrusion Detection System)과 같은 장비들을 이용하여 사전에 인가된 단말들만 접속을 허용하는 등의 방식을 사용하였지만 장비 가격이 비싸고 관리가 어렵다는 점으로 인해 규모가 작은 기업들은 사용하는 데에 어려움을 갖고 있다.

본 논문에서는 위의 문제를 해결하기 위해 두 가지 기술을 기반으로 하여 하나의 서버에서 모바일 단말들을 관리하고 데이터 유출 및 침해를 방지할 수 있는 기법을 제시한다. 먼저 서버는 내부 네트워크를 구성하고 있는 AP(Access Point)들의 정보를 데이터베이스에 저장하여 Whitelist를 생성하고 사용자 및 모바일 단말들의 정보를 관리하여 내부 네트워크에 진입을 할 경우 관리를 할 수 있도록 한다. 또한, 모바일 단말에게 전달받은 정보를 기반으로 Context Aware 기술을 사용하여 각기 다른 권한을 부여하도록 한다. 모바일 단말에서는 Agent를 실행시키면 모바일 단말의 정보와 사용자의 정보를 종합하여 서버에게 전송을 하고 자체적으로 운영되는 MDM 기능이 동작을 하게 된다. 이를 통해 외부에서 내부 네트워크로 접속을 시도하는 불법 단말을 차단하고, 내부 네트워크에 접속한 유저가 외부로 내부 데이터를 유출하는 것을 방지함으로서 보다 안전한 내부 네트워크 관리를 할 수 있는 기법을 제안한다.

이후 본 논문은 다음과 같이 구성된다. 2장에서는 무선 환경에서 발생할 수 있는 보안 위협에 유형과 현재 사용이 되는 기술들에 대해 알아보고, 3장에서는 제안하는 기법에서 사용되는 서버 및 모바일 단말에서의 동작 메카니즘의 설명을 통해 비안가 단말 탐지 및 차단 기법과 도메인 기반으로 서비스를 하는 방법에 대해 알아본다. 4장에서는 제안하는 기법의 실제 구현 결과를 보고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1 비인가 단말 탐지 기법

최근 무선 네트워크 인프라가 다소 잘 갖추어져 많은 사람들이 사용함으로서 위협 및 사고 또한 잦아지고 있다. 이는 위조 AP, 위조 단말과 같이 비인가 단말들이 설치가 되고 일반 사용자들이 접근을 함으로서 사고로 발생을 하게 되는데, 어디에 설치되고, 비인가 단말에 대한 접속 허용 문제로 생각해 볼 수 있다.[3] 기존에 제안된 비인가 단말 탐지하는 방법은 중앙에서 관리 서버가 탐지하는 서버 중심의 탐지 방법과 단말에서 탐지를 하는 단말 중심의 탐지 방법으로 분류가 된다.

먼저 서버 중심의 탐지 기법은 허가된 AP 및 단말을 Whitelist 방식으로 관리하고, 단말이 접속 요청을 시도하면 Whitelist의 정보들의 비교를 통해 비인가 단말을 검출하는 기법을 사용한다. 이 기법은 다시 무선구간과 유선구간을 기준으로 탐지하는 기법으로 나뉜다.

첫째로 무선 구간에서의 탐지 기법은 AirDefence[4], AirTight[5] 등에서 제공하는 WIPS(Wireless Intrusion Prevention System)은 무선 상의 패킷을 분석하여 정상적인 단말을 분류 및 탐지하는 장비로서 무선 구간에서 존재하는 위협에 대한 침입탐지 및 방지를 위한 솔루션이다. WIPS는 내부에 설치된 센서를 통해서 802.11 상에서 사용되는 주파수 대역의 채널을 지속적으로 감시하며, 단말들에서 보내는 비콘 프레임의 정보를 수집한다. 센서에서 수집된 정보를 기반으로

WIPS 서버는 침입탐지 및 차단을 수행한다. 하지만 도입 비용이 크고 추가적인 구축 및 확장성에 한계로 인해 제약 사항이 있어 규모가 크지 않은 회사들에게는 시스템을 도입하는 데에 어려움이 있다. Suman Jana[6]은 무선 AP가 주기적으로 전송하는 비콘 프레임 및 프로브 메시지를 수집하고 사전에 수집하여 DB에 저장된 Clock Skew와의 비교를 통해 비인가 AP를 탐지하는 기법이다. Payal Bhatia[7]은 안테나를 통해 수신된 무선 공유기의 RSS(Received Signal Strength)를 수집 후 분석하여 비인가 공유기를 탐지하는 기법이다. 위의 기법들은 추가적인 장비가 필요하고 사전에 모든 단말의 정보를 수집하여 저장하는 일련의 작업이 요구되어 스마트폰과 같은 모바일에 적용하는 데에는 어려움이 존재한다.

두 번째로 유선 구간에서의 탐지 기법은 OS Fingerprint 정보 비교, 유선에서의 패킷 전송 지연 차이 등과 같은 정보를 측정 및 비교하여 내부의 비인가 단말을 탐지한다. Sachin Shetty[8]은 유선과 무선을 구별하기 위해 단말의 bottleneck bandwidth를 이용한다. bottleneck bandwidths는 packet-pair 기법을 사용하고, 무선 탐지 시 단말의 IP 주소가 화이트 리스트에 등록이 되어 있는지를 판단하여 비인가 AP를 탐지한다. Wei Wei[9]는 IAT(Inter-packet Arrival Time)을 이용하여 트래픽의 패턴을 구분해내고, 네트워크 Edge에서 트래픽을 분석하여 비인가 단말 검출 방법을 제시한다. 추가적으로 TCP ACK 패킷의 RTT(Round-Trip Time)를 이용한 방법들이 있으며 이러한 기법은 대규모의 네트워크 환경에서 제한적인 기법이어서 적용하는 데에 어려움이 존재한다.

다음은 모바일 단말 중심의 탐지 기법으로 특정 무선 네트워크에 접속 시, 비인가 단말 및 위조 단말 보안 위협을 탐지하고, 접속을 차단하여 안전한 접속을 지원한다. 기존의 제안된 비인가 및 위조 단말 탐지 기법들은 Evil Twin과 유사한 형태의 위조 AP에 대한 탐지 방법이 많은 연구가 되고 있다. Fanglu Guo[10]는 AP에서 주기적으로 전송하는 비콘 프레임에서 MAC 정보를 이용하여 정상적으로 동작하는 AP와 불법 단말로 의심이 되는 AP와 비교를 통해 탐지를 수행한다. Diogo Monica[11]는 단말에서 워터마크 기술을 이용한 기법으로 워터마크를 삽입한 패킷을 에코 서버로 송수신하여 패킷을 확인한다. 단말에서 무선 상의 채널을 바꿔가면서 감시한 후 워터마크가 포함된 수신 패킷이 다른 채널에서 감지되면 Evil Twin 공격으로 판단하는 기법이다. Yimin Son[12]은 Evil Twin의 공격 기법과 같은 구조의 통신 구조 특징을 이용하는 기법으로, 단말이 Evil Twin AP와 정상적인 AP를 거쳐 연결이 된다. 가운데 설치된 Evil Twin AP로부터 걸리는 패킷 전송 지연 시간으로 인해 IAT가 증가하는 특징을 사용하여 위조 AP를 탐지하는 기법이다. 앞서 설명한 기법들은 이동성이 좋은 무선 단말에서 IAT 값의 변경이 빈번하고 단말들 간의 거리와 네트워크의 상태에 따라 변동이 크다는 점을 이용한 기법들이다. 또한 모바일 단말과 서버 간의 잦은 통신으로 인해 모바일 단말의 배터리 소모율이 높아져 적용하는 데에 어려움을 갖고 있다. 이와 같이 기존의 기법들이 Evil Twin 공격과 유사한 형태의 위조 및 불법 단말을 해결하는 탐지 기법을 사용하고 있다.

2.2 상황 인지 시스템

상황은 다양한 연구 분야에서 다양한 의미로 제시되어 쓰이고 있으며 상황에 대해 구체적으로 정확하게 정의하는 것이 어렵다. 최초로 상황에 대한 의미와 정의를 소개한 Schilit와 Theimer는 상황은 '위치'를 의미하였다. 이를 시작으로 상황에 대한 많은 연구가 진행 되었고, 현재는 사용자의 정보, 물리적 환경의 상황, 사물의 정보 등 다양한 것들이 상황이 되었다. 이를 이용한 상황 인지 시스템들은 앞서 정의한 상황을 수집 및 가공하여 원하는 작업들이 각각의 상황에 맞추어 적절하게 동작하는 시스템을 말한다. 그림 1은 상황 인지 기술이 개발 및 응용되고 있는 분야에 대한 그림이다. 상황 인지 기술은 우리가 살고 있는 일상생활 분야뿐만 아니라 통신, 기계, 군사, 의료 시설, 보안 등과 같이 다양한 분야에서 활용이 된다. 국내에서 연구되고 있는 상황 인지 시스템은 한국전자통신연구원(ETRI)가 개발한 Context-Aware Middleware for URC System(CAMUS)가 있다.[13] CAMUS는 네트워

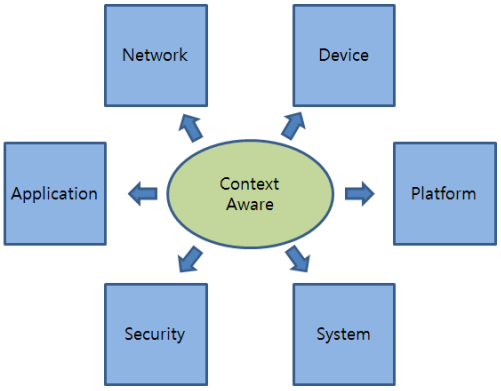


그림 1. 상황 인지 기술 개발 및 응용 분야
Fig 1. The Field of development/Applications of Context Aware Technology

크 기반의 u-로봇이 상황 인지를 할 수 있도록 제작한 CAMUS 플랫폼을 사용하고 센서를 통하여 받는 정보를 분석 및 저장하여 상황을 판단한다. Jinsung Byun[14]은 위치 기반의 상황 인지 서비스를 하는 기법을 제안하였다. 이 기법은 위치와 사용자를 기반으로 하여 최적의 서비스를 제공하기 위해 각 방에 시스템을 설치를 한다. 이 시스템이 수집하는 상황 정보를 사용하여 상황을 추론하고 이를 통해 공간과 사용자의 특성에 따라 적합한 서비스를 제공하는 기법이다.

Ⅲ. 상황 인지 및 MDM 기술을 이용한 제안 기법

본 논문에서 제안하는 서버/모바일 단말간의 상황 인지 기술과 MDM 기술을 기반으로 동작하는 솔루션으로 모바일 단말에는 앱이 서버에는 모바일 단말 및 사용자에 대한 정보가 미리 데이터베이스에 저장이 되어져 있어야 한다. 또한, 사내의 네트워크를 구성할 때에 무선 AP가 존재를 해야 한다. 이는 일반적으로 물리적 망분리를 가능하게 하며 제안하는 기법에서는 서버가 모바일 단말이 도메인을 판단하는 기준으로서 내부인지 외부인지를 알게 해준다. 앞서 말한 AP는 흔히 구할 수 있는 어떠한 AP도 가능하며 모바일 단말의 사용 지원을 위해 무선 AP로 설치를 해야 한다. 따라서 제안하는 기법은 모바일 단말에 제안하는 기법의 솔루션이 설치되어야 하며, 내부 네트워크를 구성해주는 AP가 존재를 해야 한다. 이는 적은 비용으로 구성이 가능하며 쉽게 구성할 수 있는 환경으로 규모가 작은 회사나 연구실과 같은 환경에서 쉽게 구성 및 구현이 가능하다.

3.1. 제안 기법의 구성

그림 2는 제안하는 기법의 전체 구성도를 보여준다. 모바일 단말을 사용하는 사용자(악의적 사용자), 내부 네트워크에서 동작하고 있는 내부 AP, 내부 네트워크를 관리하는 서버로 구성이 된다. 앱이 설치된 모바일 단말은 앱을 실행 시키면 처음으로 모바일 단말의 정보를 획득해오는 과정이 있다. 이 과정을 통해서 모바일 단말은 IMEI(International Mobile Equipment Identity), 모바일 단말기 전화번호, BSSID를 획득을 한다. 본 논문에서 사용하는 BSSID는 모바일 단말이 가지고 있는 MAC Address로 48bit를 사용한다. IMEI와 모바일 단말기 전화 번호, BSSID는 사용자나 일반 앱에서 바꿀 수 없는 정보로 사전에 서버의 데이터베이스에 등록을 시킨 후에 사용자 인증 및 모바일 단말의 인증을 할 수 있는 정보가 된다. 또한, 사내 내부에 설치된 합법적인 AP에 접속을 시도하게 되면 서버와 자동으로 SSL채널을 형성하고 서버와의 안전한 통신 채널을 확보한다. 채널을 확보하면서 앱에서는 MDM 기능들을 동작시켜 블루투스, 테더링, 스크린샷 등과 같은 기능들을 할 수 없도록 MDM 기능을 동작시킨다. 후에 서버에서는 Login 페이지를 호출하여 사용자에게 로그인을 하도록 하고 이 때, 사용자가 ID와 PW를 입력하는 순간 서버에서는 모바일 단말기의 정보와 사용자의 정보를 동시에 받아 사용자의 상황 정보를 얻어 이를 사용자 권한 부여에 활용하도록 한다. 서버에 성공적으로 접속을 한 모바일 단말기는 서버를 통해 내부의 데이터를 처리 및 제어할 수 있고 모니터링을 할 수 있게 된다. 그림 3은 제안하는 모바일 단말과 서버가 가지고 있는 기능들을 모듈별로 나타낸 그림이다. 우선 모바일 단말기는 스크

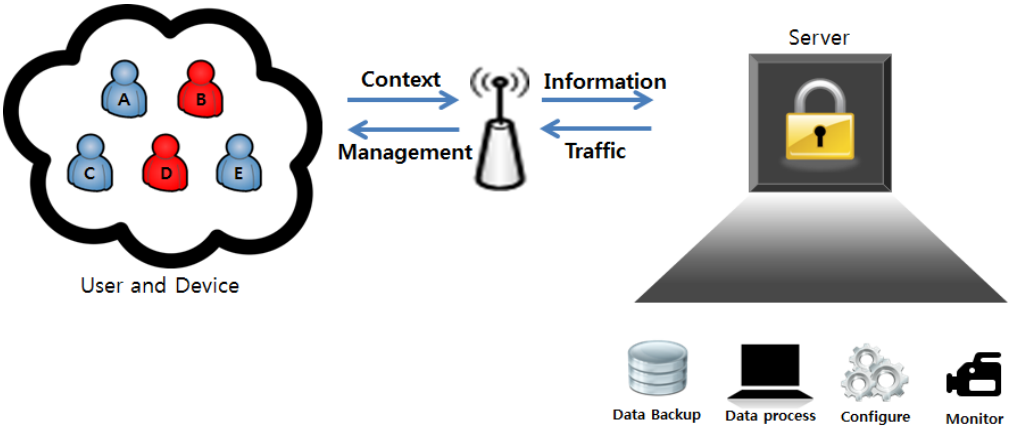


그림 2. 제안하는 기법의 구성도
Fig 2. Configuration of Proposed Scheme

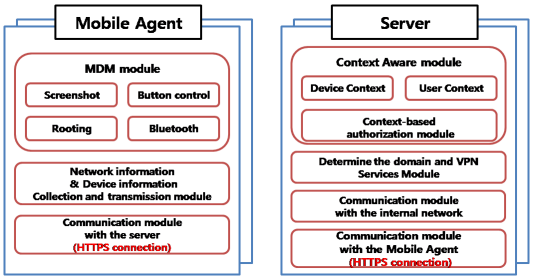


그림 3. 모바일과 서버의 구성도
Fig 3. Architecture of Mobile and Server

린샷, 버튼 제어 및 루팅, 통신 인터페이스를 관리해 주는 MDM 모듈, 서버에게 전달을 해줘야 하는 상황 정보를 수집하는 모듈, 서버와의 안전한 통신을 하기 위한 통신 모듈이 개발되었고, 서버는 단말로부터 전송받은 상황 정보를 수집 및 처리하는 상황 인지 모듈, 도메인 판단을 통해 VPN 연결을 요청하는 VPN 서비스 모듈, 모바일 단말과의 통신 모듈이 존재하며, 이들의 통신으로 인해 제안하는 기법의 동작을 한다.

본 논문에서 사용되는 모바일 단말의 IMEI, 전화번호, BSSID는 루팅이 되지 않는 일반 단말에서 사용자단의 앱을 이용하여 임의로 바꿀 수 없는 정보이다. 제안하는 시스템에서 사용하는 앱은 모바일 단말의 루팅을 감지하여 앱을 종료시키는 기능이 존재하기 때문에 앞서 말한 정보를 바꿀 수 없으며, HTTPS 통신을 사용하여 정보를 안전하게 전송하여 정보의 기밀성을 보장할 수 있다.

3.2. 제안 기법의 동작 과정

모바일 환경에서 안전하게 내부 네트워크를 접근하고 스마트워크를 수행하기 위한 이 시스템은 스마트워크를 수행하기 위해서 먼저 모바일 단말에서 앱을 실행시킨다. 앱이 실행이 되면 사용자 및 모바일 단말기의 위치에 관한 상황 정보를 구별하기 위해 사내의 AP에 접속을 할 것인지, 외부의 일반 AP 혹은 데이터망을 이용하는지를 판단한다. 내부 AP를 이용한다면 IEEE 802.1x AP 인증을 마치고 서버의 로그인 페이지를 보여주고, 데이터망이거나 외부 AP를 이용할 시 서버와 VPN 연결을 시도한다. VPN 연결이 끝난 단말기는 서버의 로그인 페이지를 통해 서버에 접속을 할 수 있다. 서버에서 로그인 페이지를 제공할 때 모바일 단말과 서버는 HTTPS 채널을 생성하여 단말기가 종료버튼을 누를 때까지 유지한다. 로그인 수행 시 서버는 모바일 단말의 정보, 모바일 단말의 위치, 사용자의 정보를 획득할 수 있고 서버는 이 상황 정보를

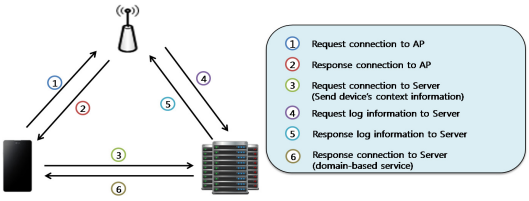


그림 4. 도메인 기반 서비스를 위한 Context 전달 과정
Fig 4. Context transfer process for Domain-based Service

종합하여 인증 및 권한 부여를 수행한다. 우선 서버는 모바일 단말의 위치를 알기 위하여 사내의 AP를 이용을 하게 된다. 단말기가 서버에 접속을 하기 위해 AP에 접속을 시도할 때, AP는 Log를 남기게 되고 모바일 단말이 서버에 접속할 때 보내는 모바일 단말의 정보를 AP의 Log와 비교를 하는 작업을 통해 같은 모바일 단말 정보 및 Log가 있을 경우 서버는 모바일 단말이 내부에서 접속을 시도한다고 판단할 수 있으며, 모바일 단말기의 정보 및 사용자의 정보를 활용하여 사용자에게 적절하게 권한을 부여할 수 있도록 한다.

그림 4는 서버가 AP를 이용하여 단말의 내부 및 외부를 판단하는 방법을 나타낸 순서도이다. 단말이 처음 앱을 시작하고 서버에 접속을 할 때, 단말은 서버에게 자신이 가지고 있는 상황 정보를 보낸다. 서버는 단말에게서 받은 상황 정보에서 AP의 SSID를 확인을 하는데, 데이터망을 사용하거나 내부에서 관리하는 AP의 SSID가 아닐 경우 외부라 판단을 하게 되며, SSID가 내부의 AP일 경우에는 해당 AP에게 Log 정보를 요청하여 모바일 단말의 상황 정보와 AP의 실제 Log 정보를 비교하여 단말이 실제 내부 AP에 접속을 했는지 판단을 하여 도메인 기반 서비스를 수행한다. 또한 서버는 단말에게 받은 상황 정보를 이용해 권한을 부여할 때, 위치 상황 정보, 사용자의 직책이나 등급, 사용자 ID, 사용자 단말의 IMEI를 And 조건으로 연결하여 판단을 하고, 단말의 위치 정보와 단말의 ID, 사용자의 신원을 통하여 더욱 적절하게 권한을 부여할 수 있도록 한다.

Ⅳ. 제안 기법의 구현 실험 및 논의

제안하는 기법은 본 저자의 연구실을 배경으로, 연구실 내에 2개의 AP와 하나의 서버 및 모바일 단말을 가지고 테스트 환경을 구성하였다. 그림 5는 제안하는 기법에서 앱이 동작하는 순서를 나타낸 순서도이다. 먼저 두 개의 AP는 서로 다른 SSID를 소유하도록 하였고 그 중 하나는 내부의 관리되어지는 AP이다. 모

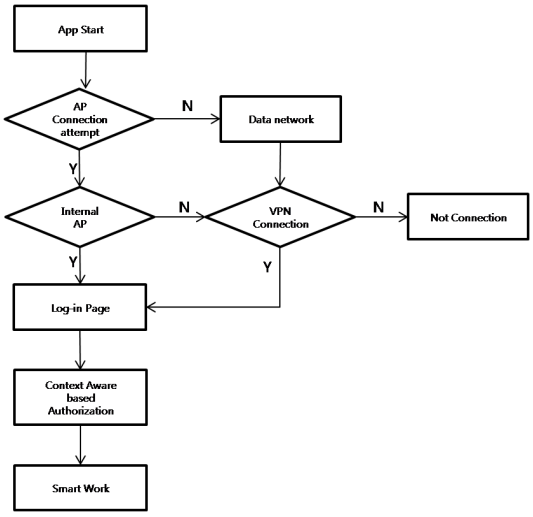


그림 5. 제안 시스템의 순서도
Fig 5. Flowchart of Proposed System

바일 단말은 관리되는 AP로 접속을 시도하게 되고 AP와의 인증을 끝마치면 내부 네트워크에 접속이 완료가 된다. 후에 앱을 동작시키면 모바일 단말에서 접속해 있는 AP의 정보를 서버에게 전송하고 서버는 전송받은 SSID와 AP에게서 얻어온 Log 정보를 이용하여 모바일 단말이 실제로 내부 네트워크에 접속을 해 있는지 검사를 한다. 검사를 통해 모바일 단말이 실제로 내부에 접속을 해있다면 외부 네트워크에 접속해 있는 경우보다 많은 권한을 획득할 수 있도록 하였다. 만약 모바일 단말이 AP와의 인증을 실패하였거나 데이터망을 사용을 하였다면 관리되어지는 AP에 Log 정보가 기록되지 않아 외부 네트워크라고 판단을 한다. 외부에서 관리되는 AP의 SSID와 비슷한 SSID로 설정한 위조 AP를 사용한다 할지라도 서버는 내부에서 관리되는 AP에서 Log 정보를 해당 모바일 단말의 Log 정보를 얻어올 수 없어 외부 네트워크라고 판단을 한다.

제안하는 기법에서 사용되는 앱은 사내에서 내부 네트워크를 통해 업무용으로 배포함으로서 사용자의 모바일 단말에 미리 설치가 되어 있다. 단말기에 설치된 앱을 통해 서버와 통신을 시작하게 되는데, 처음 앱을 실행 시 모바일 단말의 정보를 읽어와 서버에 전달을 하면서 서버의 Login 페이지로 연결이 된다. 내부에 있지 않은 모바일 단말에게는 서버가 먼저 VPN을 연결할 수 있도록 안드로이드 VPN 연결 페이지를 호출한다. 서버와의 로그인이 끝난 모바일 단말 및 사용자는 자신의 상황 조건에 합당한 권한을 부여 받아 서버의 일들을 처리할 수 있도록 한다.

그림 6은 실제 앱이 동작을 하면서 데이터 망을 사용할 때(좌측)와 WLAN 망을 사용할 때(우측)의 모습을 나타내었다. 데이터망을 사용하여 접속을 시도할 때는 로그인 페이지와 동시에 VPN 연결 페이지를 호출하여 VPN을 연결한 후 정상적인 로그인을 할 수 있게 된다. 3번째 그림에서 각 접속 화면을 보여주는데 데이터망을 사용한 좌측의 결과는 A의 작업만 가능하도록 서버에서 응답을 하고 WLAN을 사용하는

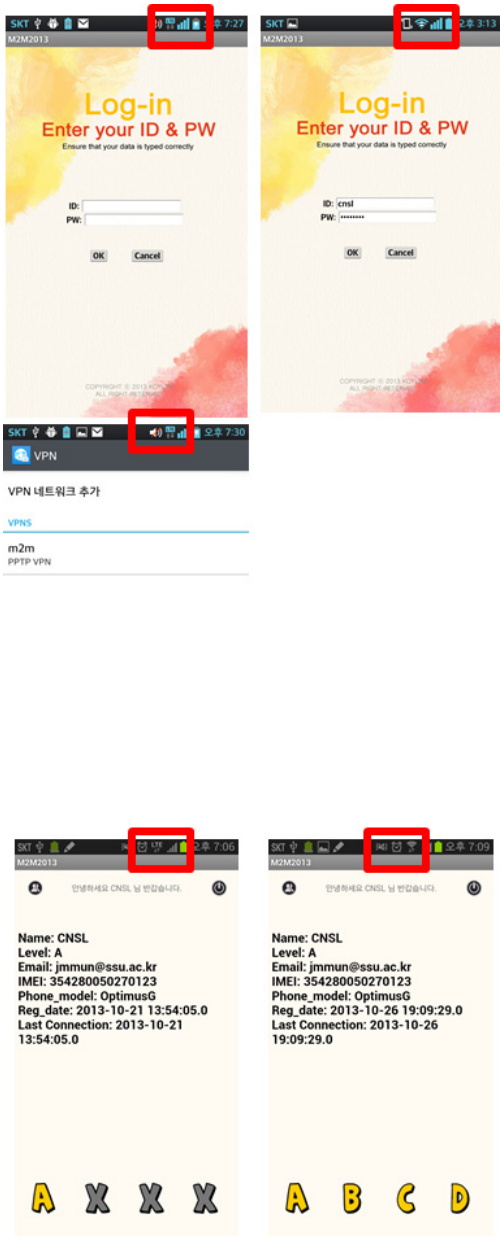


그림 6. 앱의 동작 모습
Fig 6. Operation Figure of App

경우에는 정상적으로 모든 기능들을 다 이용할 수 있도록 하였다.

본 논문에서 제안하는 기법은 위의 구현 결과로 보았을 때, 비인가 단말이 내부 네트워크에 접속을 하기 위해서는 가장 먼저 AP의 인증을 거쳐야 하며, 그렇지 않다면 VPN 연결이 필요하다. AP의 인증이 뚫렸다 할지라도 서버에서는 단말기와 사용자의 상황 정보를 활용하여 권한을 부여하여 최소의 권한만 부여하기 때문에 내부 정보의 유출 및 변조를 효과적으로 막을 수 있다.

Ⅴ. 결 론

본 논문에서는 BYOD와 같이 스마트폰의 활용도가 높고 스마트워크가 가능한 환경에서 발생할 수 있는 내부 데이터 유출 및 침해, 불법 모바일 단말 침입을 방어하기 위하여 서버와 모바일 단말 간에 상황 인지 기술과 MDM기술을 접목한 솔루션을 제안하였고, 제안 기법은 모바일 단말에 설치된 앱과 AP, 서버와의 통신을 기반으로 이루어지며 앱은 스크린샷 방지, 블루투스 방지, 테더링 방지 기능 등을 통하여 사용자가 내부 데이터를 유출하기 어렵도록 되어 있으며, 실행 시 모바일 단말의 정보와 로그인 시 사용자의 정보를 서버로 보냄으로서 서버에게 상황 정보를 전달하게 된다. 서버는 모바일 단말과 사용자의 상황 정보를 받아 이를 기반으로 사용자에게 권한을 차등부여하게 된다.

제안하는 기법을 사용함으로서 내부 네트워크의 데이터 유출 및 침해와 내부 사용자의 악의적인 소행을 최소화하고 내부 네트워크에 비인가 사용자가 쉽게 접근하지 못 하도록 하였으며, 서버에서는 모바일 단말의 상황 정보를 이용하여 해당 보안 등급에 맞는 권한만을 부여함으로서 사고를 방지할 수 있다. 또한, WIPS와 같은 보안 장비를 이용하지 않아 비교적 적은 비용으로 내부 네트워크의 침입을 방지할 수 있으며 이를 통해 규모가 작은 기업에서도 효과적으로 내부 데이터 보호 및 침해를 방지할 수 있다. 또한 기존의 기법들은 모바일 단말의 위치를 서버에서 파악할 수 없어 각 환경에 맞는 적절한 권한과 접근 제어 기법을 적용할 수 없었지만 본 논문에서는 서버가 모바일 단말의 위치가 내부인지 외부인지 판단을 할 수 있어 안전한 원격 접속 제어 및 사용자들에게 적절한 권한 부여와 내부 데이터를 보호할 수 있다.

References

[1] A. Scarfo, “New security perspectives around BYOD,” in *Proc. 2012 Seventh Int‘l Conf. Broadband, Wireless Computing, Commun. and Applications(BWCCA)*, pp. 446-451, Nov. 2012.

[2] K. Rhee, H. Kim, and H. Y. Na, “Security test methodology for an agent of a mobile device management system,” *Int’l J. Security and Its Applications*, Vol. 6, No. 2, Apr. 2012.

[3] J. Burke, B. Hartselle, B. Kneuven, and B. Morgan, Wireless security attacks and defense, Retrieved May 2006, from http://www.windowsecurity.com/whitepapers/Wireless_Security/Wireless-Security-Attacks-Defenses.html.

[4] AirDefense, “Tired of rogues: Solutions for detecting and eliminating rogue wireless networks,” *AirDefense white paper*, 2011.

[5] AirTight Networks, “Conquering the minefield of Soft rogue APs in the enterprise,” *AirTight white paper*, 2012.

[6] S. Jana and S. K. Kasera, “On fast and accurate detection of unauthorized wireless access points using clock skews,” *IEEE Trans. Mobile Computing*, Vol. 9, No. 3, pp. 449-462, Mar. 2010.

[7] P. Bhatia, C. Laurendeau, and M. Barbeau, “Solution to the wireless evil-twin transmitter attack,” in *Proc. IEEE CRiSIS 2010*, pp. 1-7, Oct. 2010.

[8] S. Shetty, M. Song, and L. Ma, “Rogue access point detection by analyzing network traffic characteristics,” in *Proc. IEEE MILCOM* 2007, pp. 1-7, Oct. 2007.

[9] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley, “Identifying 802.11 traffic from passive measurements using iterative bayesian inference,” in *Proc. In: 25th IEEE int’l conf. on computer commun.(INFOCOM)*, pp. 1-12, Apr. 2006.

[10] F. Guo and T. Chiueh, “Sequence number-based MAC address spoof detection,” in *Proc. RAID 2005*, pp. 309-329, Sept. 2005.

[11] D. Monica, and C. Ribeiro, “WiFiHop -

mitigating the evil twin attack through multi-hop detection," in *Proc. ESORICS 2011*, pp. 21-39, Sept. 2011.

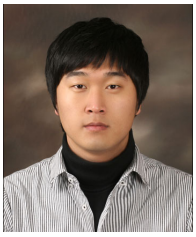
[12] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks? - To catch an evil twin access point," in *Proc. IEEE/IFIP DSN 2010*, pp. 323-332, Chicago, IL, USA, Jun. 2010.

[13] H. Kim, Y. J. Cbo, and S.-R. Oh, "CAMUS - a middleware supporting context-aware services for network-based robots," *IEEE Workshop on Advanced Robotics and Its Social Impacts*, pp. 237-242, Jun. 2005.

[14] J. Byun, I. Hong, B. Kang, and S. Park, "A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting," *IEEE Trans. Consumer Electronics*, vol. 57, no. 2, May 2011.

[15] S. K. Park and J. h. Lee, "Propulsion systems and practices for smart work(스마트워크 추진 체계 및 사례)," *J. KICS,* vol. 29, no 12, pp. 3-9, Nov. 2012

문 지 만 (Jiman Mun)



2012년 2월 : 숭실대학교 정보통신전자공학부 졸업
2012년 3월~현재 : 숭실대학교 전자공학과 석사과정
<관심분야> 무선 네트워크 보안, 클라우드 보안

정 수 환 (Souhwan Jung)

1985년 2월 : 서울대학교 전자공학과 졸업
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임연구원
1996년 6월 : University of Washington 박사
1997년 Stellar One Corp. Senior Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 및 무선 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안