Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Method for Detecting Unauthorized Internet Access Node in Private Financial Network

Hyung-Jin Cho[1], Eunjin Kim[2], Huy Kang Kim[*3]

[1]*Department of Financial Security, School of Information Security, Korea University*
[2]*Department of International Industrial Information, Kyonggi University*
[3]*School of Information Security, Korea University*

ABSTRACT

Recently, many companies make efforts to enhance security to detect and prevent an APT(Advanced Persistent Treat) attack that mainly target on the companies' PC devices. Most global companies run several branch offices that have numerous PC devices, but they are not easily controlled by a central security policy. Although security policies enforce to prevent unauthorized internet access, there are various detour techniques such as using tethering, open VPN or RogueAP. If a company fails to control all end user's PC devices, this can threaten the company's overall security. Especially, this can be the most critical problem in finance business domain. In this paper, we introduce a method to detect unauthorized internet access node in the closed private network. We conduct this method to find out the unauthorized nodes against the security policy. We deploy this detection method in the real network of a finance company in South Korea. As a result, we can classify several types of unauthorized nodes, and improve the detection techniques.

KEYWORDS: Rogue AP, NAC, White list, Unauthorized internet access node, WIPS

ARTICLE INFO: Received 20 October 2015, Revised 11 December 2015, Accepted 11 December 2015.

1. 서 론

최근 국내 기업들은 악성코드 감염의 원인이 되는 사용자 PC단말 보안강화를 위해 내부 통제를 강화하고 있으며, 외부로부터의 APT (Advanced

[*]Corresponding author is with the School of Information Security, Korea University, Anam Campus, Anam-dong 5-ga, Seoul, 136-713, KOREA.
E-mail address: cenda@korea.ac.kr

Persistent Treat) 공격 방어를 위한 다양한 보안 체계 확립을 위해 노력하고 있다. 또한, 금융권의 경우에는 정부의 주도 아래 관련 법령이 개정 되었으며, 이에 맞춰 인터넷과 업무망을 분리하여 운영할 수 있도록 망분리 사업이 추진되고 있다.

표 1. 금융회사 망분리 의무화 관련 법령
Table 1. Laws related to the network separation in finance domain

일 시	기 관	법 령
2013. 7.	금융위원회	금융전산 보안 강화 종합대책 - 망분리 의무화
2013.12	금융감독원	전자금융감독규정 제15조 제1항 제3호, 제5호 - 망분리 의무화

하지만, 일부 금융회사에서는 업무의 특성 상 다수의 계열사 및 지점을 운영하고 있는데, 일부 지점에서 업무의 편의성 및 내부통제 부재로 인해 ADSL과 같은 임의의 인터넷 회선을 설치하여 운영하는 경우가 발생하고 있는 것이 현실이다. 금융회사에서 보안정책을 강화하여 이런 문제를 통제, 감독을 하려 노력하고 있지만, 모든 지점의 모든 PC 단말기까지 감시를 실시간으로 하기에는 현실적인 문제가 있다.

표 2. 금융회사 보안 사고 유형
Table 2. Incident Types Happened in Finance Companies

사건 일시	대상 기관	공격유형
2011. 4.12	금융회사 1개	관리통제 범위에 있지 않던 외부 협력업체의 노트북 PC 단말에 APT공격으로 인한 선 침입 후 전사 네트워크에 공격 확산
2013. 3.20	금융회사 3개, 언론기관 3개	지점 PC 단말을 APT공격으로 침입한 뒤 전사 네트워크에 공격 확산

2013년에 발생한 3.20 사태 역시, 내부 사용자의 PC 단말이 악성코드에 감염되어 발생한 대규모 사이버 테러사건 유형이었다. 이러한 유형으로 과거 국내 금융회사에서 발생한 사고들은 <표 2>와 같다.

금융회사에 대한 공격 형태는 아래 <그림 1>과 같이 PC단말을 통하여 이루어 졌다.

그림 1. 금융회사에 대한 일반적인 공격 형태
Figure 1. Typical Attack Path that Aims at Finance Companies

통제 및 관리가 되지 않는 비인가 인터넷 회선을 통해 '망분리 시스템 무력화, 내부 업무 직접 공격, 폐쇄망 환경에서의 센터 집중화 보안관제 우회, 인터넷 차단 정책 우회, 내부 사용자 인터넷 구간 보안정책 우회, 내부망 접속 업무 PC 단말에서 사설 인터넷 사용' 과 같은 보안정책 위반사례가 발생할 수 있다. 이러한 보안정책 위반으로 인한 제2의 3.20 사태와 같은 심각한 보안 위협이 발생할 수 있으므로, 비인가 PC 단말 및 네트워크들은 반드시 통제 되어야 한다.

일반적인 네트워크 환경에서 비인가 AP 탐지 등과 같은 연구는 최근까지 활발히 진행되고 있으나, 금융망에 적합한 비인가 PC단말 탐지에 대한 연구는 그간 소개되지 않았다. 따라서, 본 논문에서는 금융망 환경에서 운영 중인 보안 시스템을 우회하여 구축된 비인가 PC단말 탐지 방법론에 대한 연구를 수행하고자 한다.

본 논문에서는 금융망에 적합한 비인가 PC단말 및 네트워크 탐지기술 개발을 위한 설계 및 분석을 수행한다. 이를 위한 각 장의 구성은 다음과 같다.

2장에서는 관련연구로서 전통적인 금융권에서의 비인가 탐지 방법, 유선 및 무선 환경에서의 비인가 단말 탐지 기술인 NAC (Network Access Control) 기반 비인가 사용자 단말 차단 시스템[1]과 Rogue AP 탐지 기법[6]을 소개한다. 또한, 업무용 PC 단말에 대한 USB 모뎀 차단 등 매체제어솔루션을 이용한 PC 단말 관리에 대해 소개한다.

3장에서는 금융망에 적합한 비인가 PC단말 탐지 유형을 정의하고, '금융망에 적합한 비인가 PC단말 및 네트워크 탐지 기술'을 설계한다.

4장에서는 제안한 탐지 기술을 기존 솔루션 탐지기술과 비교하여 제안 기술을 특성을 분석한다.

마지막으로, 5장에서는 본 논문의 결론을 맺는다.

2. 관련 연구

전통적으로 금융권에서는 비인가 인터넷을 탐지하기 위해 다음 <표 3>와 같은 방법을 사용하고 있다.

표 3. 비인가 인터넷을 탐지하는 전통적 기법
Table 3. Traditional Detection Methods of Unauthorized Access Network toward Internet

구분	탐지 방법
1	자체 외부 인터넷 사용 여부 확인
2	전산담당자를 통해 해당 IP Address를 어떤 용도로 사용하는지 확인 요청
3	ipconfig.kr, ipip.kr 등으로 공인 IP Address 확인
4	ARP Table을 통하여 확인
5	실사점검 진행

❍ 자체 외부 인터넷 사용 여부 확인
- 보안담당 부서에서 모르는 임의의 사설망 회선 계약 내용이 있는지 정기적으로 확인하여 비인가된 네트워크 이용이 발생하였는지 여부 확인

❍ 전산담당자를 통해 해당 IP Address를 어떤 용도로 사용하는지 확인 요청
- 대부분 공유기 또는 사설망으로 추정되며, 간혹 네트워크 프린터 IP Address 설정을 잘못하여 사용하는 경우도 발생

❍ ipconfig.kr, ipip.kr 등으로 인가된 공인 IP Address 여부 확인
- 폐쇄망 내 단말기에서 유선 또는 원격 등으로 확인하고, 해당 금융회사에서 관리하는 센터 집중화 IP Address가 아닌 IP Address가 발견될 경우 비인가 인터넷 이용으로 판단
- 실제로, 실험대상 기업은 부서별/권역별 특성에 맞게 보안정책 및 네트워크의 효율적 관리를 위해 인터넷 집중센터를 통한 공인 IP Address를 특정그룹으로 구분관리하고 있으며, 설정 예는 <표 4> 와 같다.

표 4. 인터넷 집중센터 공인 IP Address (예시)
Table 4. Example of Public IP Address segmentation for Centralized Internet Center

구분	IP Address
A-본부	1.XX.X.X.
B-본부	14.XX.X.X
D-영업본부	1.2XX.X.X
E-영업본부	1.23X.X.X

❍ ARP Table을 통하여 확인
- 폐쇄망 내 단말기에서 arp -a 명령어를 사용하여 해당 IP Address가 존재하는지 확인

❍ 실사점검 진행
- 비인가 인터넷 회선 점검을 위해 현장에 대한 육안점검을 수행함.
(단, 이 방법은 지리적, 시간적, 인력적 제한이 있는 단점이 있음)

2.1 일반적인 금융권 비인가 단말 구성

폐쇄된 환경에서 비인가 PC단말 탐지 및 차단 시스템의 구성의 예시는 아래 <그림 2>과 같다. 이러한 비인가 단말을 식별 및 차단하기 위해, WIPS(Wireless Intrusion Prevention System)와 같은 보안 장비가 운영되고 있으나 다양한 우회 방법들이 존재하여 완벽하게 비인가 단말을 차단한다고 볼 수는 없다.

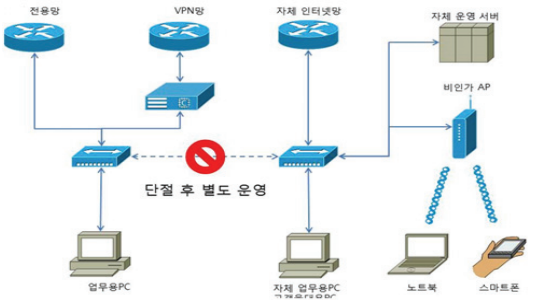

그림 2. 비인가 PC 단말 탐지 시스템 구성도
Figure 2. Network Diagram of Unauthorized PC Detection System

2.2 NAC 기반 비인가 사용자 단말 차단 시스템

다수의 금융망에는 외부망으로부터의 공격을 차단하기 위해 PC 단말, 서버 등에 네트워크 접근을 허용하는 NAC (Network Access Control) 기술 기반의 장비들이 도입되어 있다. NAC은 사용자 PC 단말이 내부망에 접근하기 전에 보안정책을 준수했는지 여부를 점검하는 기술이다. 그러나, 인터넷 등 외부망으로부터 게이트웨이를 통해 접속하는 장치에 대해서는 NAC을 적용하기가 어렵다.

이러한 문제점을 해결하기 위해 최근에 L3기반 NAC환경에서 비인가 사용자 격리 조치를 위한 보안 시스템이 소개되었다[1]. 특히, [1]에서 제안한 기술은 별도의 장비를 구매 할 필요가 없어 비용적인 측면과 운영적인 측면에서 큰 효과를 나타냈다.

외부 네트워크에서 내부 네트워크 접근에 중점을 둔 보안 플랫폼을 기반으로 내부 네트워크의 보안 정책인 NAC을 적용시켜 구현한 연구도 같이 진행되었다 [2].

또한, 기업 내부의 네트워크 보호 및 정보자산 침해 방지를 위해 NAC시스템 구축 사례를 바탕으로 기업 네트워크 보안 효과를 높일 수 있는 방안을 제시하였다 [3].

기업에서 요구하는 사용자PC 단말에 대한 보안 요구 사항을 수집하여 적합한 NAC모델을 설계하고, 이 모델을 어떻게 적용해야 효과적인지 분석하고, 실제 적용한 사례에 대한 연구도 진행되었다 [4].

2.3 Rogue AP 탐지 기법

Rouge AP는 사용자의 편의성을 위해 보안 정책을 적용되지 않은 비인가 AP이며, Rouge AP 설치는 건물 내부에 한정되지 않기 때문에 외부망으로부터의 위협에 노출되어 있다. 이러한 Rouge AP를 탐지하기 위해 모바일 단말 및 원격서버를 이용한 무선랜 보안 시스템이 제안되었다. WIPS, DLP (Data Leakage Prevention) 와 같은 무선망 보안 시스템은 가격이 비싸고 관리가 힘들지만, 제안 기법[5]은 이러한 문제점을 해결하였다. 또한, 제안 기법은 관리자에 의해 AP 및 단말 정보가 서버에 저장되고, 개인 장치에는 어플리케이션에만 설치하면 다양한 무선망에 적용할 수 있는 장점을 가지고 있다.

2014년에 k-SVM (Kernel Support Vector Machine)을 이용한 Rogue AP 탐지하는 기법이 소개되었다[6]. 제안 기법은 홉 (Hop) 간 RTT (Round Trip Time) 값을 특징 점으로 하고 분류기로 k-SVM을 사용하였다.

인증 네트워크 내에서 스마트 폰을 이용한 비인

가 AP의 탐지 및 차단하는 기법이 소개되었다[7]. 제안 기법은 탐지 프로그램을 사용하여 무선 센서를 통해 비 인가된 모바일 AP의 무선 패킷을 분석 후 차단하였다.

무선 환경에서 발생되는 보안 위협을 탐지하고 방지하는 시스템을 오픈 소스 기반인 Kismet과 Wireshark을 사용하여 IPtable을 사용하여 침입을 방지하는 방법도 소개되었다 [8].

Radius 인증 서버 네트워크 내에서 테더링 기반 Rogue AP 탐지 및 대응기법도 제안되었으며, 탐지 기반은 센서를 이용하여 비컨 프레임 (Beacon Frame)을 스니핑 (Sniffing)하고, 인가된 AP와의 차이점을 분석해서 Rogue AP를 탐지 하였다. 또한 탐지된 Rogue AP에 직접적인 DoS공격들을 시도하여 Rogue AP의 운용을 차단하는 방법도 함께 연구되었다 [9].

별도의 하드웨어 없이 무선랜 침해 방지를 위해 Probe Request / Respose Frame을 활용하여 맥 주소를 위장한 Rogue AP를 탐지하고, 무선랜 침해방지 센서에 적용하기 위한 기법들도 연구 되었다 [10].

2.4 매체제어솔루션을 이용한 PC 단말 보안

매체제어솔루션을 이용하여 사용자PC 단말의 미디어장치 (PDA, 스마트폰, 무선랜, 휴대용 저장 장치)에 의한 외부 네트워크의 임의접속을 시도하려고 하는 경우에도 제한하고 있다. 상세한 매체제어 정책은 다음 <표 5>와 같다.

요컨대, 2장에서 소개한 전통적 방식, 구축 운영중인 솔루션 (NAC, 단말 매체제어솔루션, WIPS)들은 다음과 같은 문제점을 가지고 있다.

전통적인 방식은 실시간 탐지 대응이 불가능하며, 직접 조사를 위한 시간적, 지리적, 인력적 제약이 있다.

표 5. 사용자 매체제어 정책

Table 5. Security Policies of Media Control for User PC

매체제어정책	내용
PDA 쓰기 통제	PDA의 쓰기에 대한 권한을 제어
스마트폰 쓰기 통제	스마트폰 사용권한을 제어
무선랜 쓰기 통제	무선랜 사용권한을 제어
테더링 쓰기 통제	테더링 사용권한 제어
휴대용 저장 장치 쓰기 통제	휴대용 저장 장치 (USB, 외장형 HDD 등) 쓰기에 대한 권한 제어

NAC과 매체제어솔루션을 사용한 방식은 임의의 외부 임대 회선을 PC 단말기나 스위치(L2)에 직접 연결할 경우 탐지를 하지 못한다. 또한, 자체 전용망을 구축하여 외부 인터넷과 직접 연결한 경우 등 비인가 PC 탐지 기능이 떨어진다. 고정 ARP를 통한 우회, IP Address 변조 및 ARP 캐시 포이즈닝을 통한 네트워크 마비 등에 취약한 문제를 가진다 [5].

WIPS는 PC 단말이 인가되지 않은 외부 무선AP에 접근하는 것을 차단하기에는 유용하나, 적용범위를 넓히려면 다수의 WIPS를 도입해야 하므로 비용문제 및 설치 관리의 문제가 발생한다.

본 논문에서는 전통적인 방식이나 기존 운영 중인 솔루션에서 탐지하지 못한 비인가 접속 PC 단말을 탐지하기 위한 기법을 제안한다.

3. 제안 기법

3.1 비인가 탐지 범위

본 논문에는 금융망에서 빈번히 발생하는 비인가 단말 및 네트워크 현황을 아래 <표 6>과 같이 식별하였다. 또한, 식별된 비인가 유형을 기준으로 분석을 수행하였다.

표 6. 금융회사 비인가 노드 유형
Table 6. The Type of Unauthorized Node(PC) in Finance

현 황	비고
업무용 PC 단말에서 무선랜 혼용 사용	업무용PC 단말의 무선랜과 내부망이 연결된 유선랜 혼용 사용
무선공유기 사용	무선공유기와 내부망 연결 사용
업무용 PC 단말과 사설망 직접 연결 사용	업무용pc가 연결된 통신장비(L2)에 사설망 직접 연결
유선 공유기 사용	내부망 ↔ 유선 공유기 ↔ 업무용 PC 단말
자체 구축된 전용망을 통해 인터넷 사용	자제 서버를 구축하여, 외부 인터넷 직접 연결

3.2. 제안 방법론

본 논문에서는 다음 <표 7>와 같이, 기업 네트워크 내 단말들에 각 단말의 네트워크 정보를 수집하기 위한 Agent를 제작 및 배포하고, 수집서버를 이용하여 정보를 수집 분석하여 비인가 PC 단말을 탐지할 수 있도록 하였다.

표 7. 제안 기법
Table 7. The Proposed Method

순번	내용	비고
1	단말 네트워크 정보수집 Agent 제작	공인 IP Address 정보, ipconfig 정보, ARP 상태정보, 라우팅 테이블 정보, 최근 조회한 DNS 쿼리 정보를 수집
2	Agent 배포	전 단말에 파일 배포가 가능한 단말 관리 솔루션을 이용하여 제작한 Agent를 배포
3	단말 네트워크 정보 수집	Agent로부터 수신되는 정보를 DB에 저장
4	비인가 단말 탐지	수집된 정보로부터 비인가 단말 탐지

비인가 탐지를 위해 'PC단말 공인 IP Address 정보, ipconfig 정보, 스위치 ARP 상태정보, 라우팅 테이블 정보, 최근 조회한 DNS 쿼리 정보'를 수집하는 Agent를 제작하며, 수집 정보의 목적은 다음 <표 8>와 같다.

표 8. 수집 정보 및 목적
Table 8. Objective of selecting information

수집 정보	수집목적
PC단말 공인 IP Address 정보	접속IP Address가 허용된 IP Address인지 여부 확인
PC단말 ipconfig 정보	현재 IP Address가 허용된 IP Address인지 여부 확인
스위치 ARP 상태정보	단말기가 접속한 인접 단말기 IP Address를 확인하여, 허용되지 않은 IP Address인지 여부 확인
라우팅 테이블 정보	default gateway를 확인하여, 허용 gateway 여부 확인
최근 조회한 DNS 쿼리 정보	인터넷 접속 DNS 캐쉬 정보를 추적하여, 허용되지 않은 도메인 접속 여부 확인

또한, 수집된 정보들을 이용하여 아래 <표 9>와 같은 탐지 규칙을 이용하여 비인가 단말을 식별한다.

표 9. 비인가 노드(단말) 탐지 기준
Table 9. Detection Rules of Unauthorized Node

수집 정보	탐지 기준
PC단말 공인 IP Address 정보	PC단말 공인 IP Address와 기업 내 인가 IP Address 비교
PC단말 ipconfig 정보	단말 IP정보와 단말보안관리 시스템의 사용자 리스트 비교
스위치 ARP 상태정보	스위치 장비의 ARP 정보와 기업 내 인가 IP Address 비교
라우팅 테이블 정보	인가된 gateway와 비인가 gateway 비교
최근 조회한 DNS 쿼리 정보	접근 차단된 도메인 확인

또한, 오탐률을 줄이기 위해 아래와 같이 구성하여 비인가 단말을 식별하였다.

❍ TCP/IP를 이용하는 통신은 네트워크 및 보안 장비에 설정되어 있는 라우팅 정보를 수집한 후 수집서버로 데이터를 전송한다.

❍ 내부망에 연결된 업무용 PC 단말을 대상으로 탐지 Agent를 설치하며, 설치된 Agent는 주기적으로 해당 사용자 PC 단말의 IP Address 정보와 라우팅 정보를 수집하여 수집서버로 전송한다.

❍ 수집서버는 Agent로 부터 수집된 정보 중 현재 설정된 IP Address정보가 내부망에서 허용된 IP Address인지 확인하며, 허용되지 않은 IP Address로부터의 접속일 경우 비인가 인터넷 망을 사용하고 있는 사용자로 판단한다.

실제로 본 논문에서 제안한 방법을 A사에 구축 및 적용을 하였으며, 개략적인 시스템 구성은 <그림 3>과 같다.

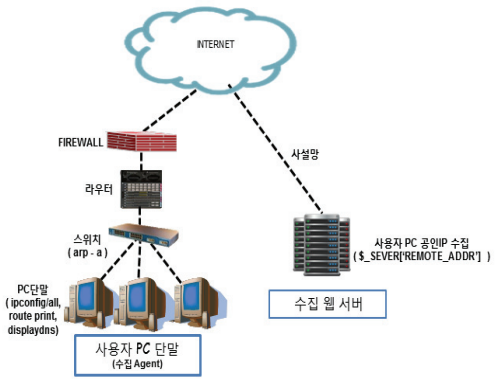

그림 3. 제안한 시스템 구성도

Figure 3. Overview of the Proposed System

3.3. 제안 방법 설계

수집 웹 서버 및 사용자 PC 단말의 개발 환경은 아래 <표 10>과 같다.

표 10. 개발 환경

Table 10. Development Environment

구분	사용자 PC	수집 서버
OS	Windows 7	Linux Ubuntu 14.03
S/W	Visual Studio 2010 MFC	Apache, php, MySql
N/W	-	사설망

3.3.1. 수집 Agent 설계

Agent 클라이언트에서는 'IP Address 정보, ARP 상태정보, 라우팅 테이블 정보, 최근 조회한 DNS 쿼리 정보'를 <그림 4>와 같이 Desktop.bmp 파일로 저장한다.

```
char *tempfile = "Desktop.bmp";

    char optest[200] = { 0 };
    sprintf(optest, "ipconfig /all >> %s&arp -a >> %s&route print >> %s&ipconfig/
displaydns >> %s", tempfile, tempfile, tempfile, tempfile);
    system(optest);
```

그림 4. 단말 정보 수집

Figure 4. gathering Information of User PC

각 정보를 수집하기 위한 명령어는 아래 <표 11>과 같다.

표 11. 수집 명령어

Table 11. Command lists for gathering Information

수집 정보	명령어
공인 IP Address 정보 (PHP 명령)	$_SEVER['REMOTE_ADDR']
단말 ipconfig 정보	ipconfig / all
스위치 ARP 상태정보	arp -a
라우팅 테이블 정보	route print
최근 조회한 DNS 쿼리 정보	ipconfig / displaydns

<그림 5>은 수집된 IP Address 정보와 ARP 정보 등을 서버로 전송하는 부분이며, 전송 효율성을 증가시키기 위해 Base64로 인코딩하여 수집서버로 전송한다.

```
hSocket = socket(PF_INET, SOCK_STREAM, 0);
if (hSocket == INVALID_SOCKET)
    ErrorHandling("hSocket() error!");

memset(&servAddr, 0, sizeof(servAddr));
servAddr.sin_family = AF_INET;
servAddr.sin_addr.s_addr = inet_addr(host);
servAddr.sin_port = htons(atoi(port));

if (connect(hSocket, (SOCKADDR *)&servAddr, sizeof(servAddr)) == SOCKET_ERROR)
    ErrorHandling("connect() error!");

SEND_RQ("POST ");
SEND_RQ(uri);
SEND_RQ(" HTTP/1.1\r\n");
SEND_RQ("Accept: text/html, application/xhtml+X-X-X-XML, */*\r\n");
SEND_RQ("Accept-Language: ko-KR\r\n");
SEND_RQ("User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n");

char *encode_data = NULL;
size_t encode_size = 0;
encode_data = base64_encode(xor_data, idx, &encode_size);

char content_header[100];
sprintf(content_header, "Content-Length: %d\r\n", encode_size + 7);
SEND_RQ(content_header);
```

그림 5. 수집된 단말 정보 전송

Figure 5. Sending the gathered node information

수집된 정보를 통신장비의 로그에서 숨기를 위해, <그림 6>와 같이 POST 형태로 수집 서버에 전송한다.

```
SEND_RQ("DATA=");
int i;
for(i = 0; i < encode_size; i++) {
    char *chr = &encode_data[i];
    send(hSocket, chr, 1, 0);
}

SEND_RQ("\r\n");

recv(hSocket, encode_data, 1024, 0);

closesocket(hSocket);
WSACleanup();
```

그림 6. POST 방식 전송

Figure 6. Transmission via POST method

3.3.2. 수집 서버 설계

수집 서버는 A사에서 허용하고 있는 공인 IP Address을 <그림 7>과 같이 valid_ip로 설정하고, 공인 IP Address이외의 IP Address로 설정된 모든 단말은 비인가로 식별한다.

```
$valid_ip = array("14.[redacted]","1.23[redacted]","14.[redacted]","1.2[redacted]");
$eip = $_SERVER["REMOTE_ADDR"];
for ($i = 0; $i < sizeof($valid_ip); $i++) {
    if (strpos($valid_ip[$i], $eip) != false) {
        exit(0);
    }
}
```

그림 7. 공인 IP Address 설정의 유효성 검증

Figure 7. Validation of the Public IP address setting

<그림 8>는 클라이언트로부터 수집된 정보를 BASE64 디코딩을 수행하여, 서버로 데이터를 전송한 공인 IP Address와 실제 클라이언트에 설정되어 있는 IP Address를 파싱하여 EXT_IP_Addr과 Internal_IP_Addr로 비교할 수 있도록 출력하는 부분이다.

```
$decText = base64_decode($getData);
$cvtDecText = iconv("cp949", "utf-8", $decText);
//echo strlen($decText);
$encText = base64_encode($decText);


$cvtDecText = str_replace(array("\r\n","\r","\n"), "\n", $cvtDecText);
//echo $cvtDecText;
$lines = explode("\n", $cvtDecText);
$lineNum = sizeof($lines);
$iip = "0.0.0.0";

for ($i = 0; $i <= $lineNum; $i++) {
        //echo $lines[$i] . "<br>";
        $pos = strpos($lines[$i], "(기본 설정)");
        if ($pos != false) {
                //echo $lines[$i] . "<br>";
                $pos2 = strpos($lines[$i], "IPv4 주소");
                if ($pos2 != false) {
                        //echo $lines[$i] . "<br>";
                        // filter 추가 예정
                        $arrayEIP = explode(":", $lines[$i]);
                        $arrayEIP = explode("(", $arrayEIP[1]);
                        $iip = trim($arrayEIP[0]);
                        //echo $eip;
                }
        }
}
```

그림 8. 수집된 각 단말 정보의 IP address 비교

Figure 8. Match for the Collected IP address Information for Each Node

DB에 저장된 수집정보는 <그림 9>과 같이 모든 사용자에 대한 수집일시, EXT_IP, INT_IP 정보를 출력하도록 구성한다.

```
$conn = mysql_connect($[redacted], $[redacted], $[redacted]);
mysql_select_db($ninzagw, $conn);

$query = "select idx, eip, iip, data, version from nzclient order by desc";
$result = mysql_query($sql, $conn);
echo "<table width=100% border=1 cellpadding=1 cellspacing=0>";
while($row=mysql_fetch_array($result))
{
echo "<tr>";
    echo "<td boder=1>";
    echo $row(idx);
    echo "</td>";
    echo "<td boder=1>";
    echo $row(date);
    echo "</td>";
    echo "<td boder=1>";
    echo $row(eip);
    echo "</td>";
    echo "<td boder=1>";
    echo $row(iip);
    echo "</td>";
    echo "<td boder=1>";
    echo $row(version);
    echo "</td>";
```

그림 9. 수집된 단말 정보 출력

Figure 9. Printing the Collected Node's Information

수집된 정보의 상세보기 기능을 제공하기 위해 수집 정보 중 'IP Address 정보, ARP 정보, DNS 쿼리 정보'를 저장하는 부분을 <그림 10>과 같이 구성한다.

```
$query = "select data from nzclient where idx = $idx";
$result = mysql_query($sql, $conn);

while($row=mysql_fetch_array($result))
{

$decText = base64_decode($row[data]);

echo "<pre>";
echo $decText;
echo "</pre>";
```

그림 10. 수집된 단말 정보 DB저장

Figure 10. Saving the Collected Information in the Database

4. 실험 결과

4.1. 실험 절차

제안 기법을 활용하여 비인가 단말 식별을 위해 단말 관리 시스템을 이용하여 개발한 Agent를 설치하였다. 특히, 다양한 환경에서 클라이언트가 실행될 수 있도록 약 4개월간 개발 및 테스트 과정을 거쳤다.

수집된 정보 (IP Address 정보, 스위치 ARP 정보, 라우팅 테이블 정보, 최근 조회한 DNS 쿼리 정보)를 이용하여 3.2절에서 소개한 수집정보 목적에 따라, <그림 11>과 같이 5단계로 비인가 인터넷 접속 노드를 식별하였다.

- ❍ 1단계 : PC단말 공인 IP Address 정보와 실험 대상 A사의 인가된 공인 IP Address를 비교하여 비인가 노드를 식별함. 비인가 IP Address로 식별되면 비인가 노드로 저장하고, 비인가 IP Address가 아닌 경우 2단계를 수행
- ❍ 2단계 : ipconfig 정보에서 단말의 IP Address를 추출하여 비인가 IP Address여부를 체크하여 비인가 노드를 식별함. 비인가 IP Address로 식별되면 비인가 노드로 저장하고, 비인가 IP Address가 아닌 경우 3단계를 수행
- ❍ 3단계 : 스위치 ARP 정보에서 단말기가 접속한 인접 단말기 IP Address가 허용되지 않은 IP Address인지 여부 확인하여 비인가 노드를 식별함. 해당 IP Address가 비인가 IP Address로 식별되면 비인가 노드로 저장하고, 비인가 IP Address가 아닌 경우 4단계를 수행
- ❍ 4단계 : 라우팅 테이블 정보에서 default route를 확인하여 비인가 gateway 여부를 확인하여 비인가 노드를 식별하거나 비인가 gateway로 확인되면 비인가 노드로 저장하고, 정상 gateway인 경우 마지막 5단계를 수행

○ 5단계 : 인터넷 접속 DNS 캐쉬 정보에서 허용되지 않은 도메인 접속 여부 확인하여 비인가 노드를 식별함. 허용되지 않는 도메인 접속 기록이 확인되면 비인가 노드로 저장하고, 정상 도메인만 확인된 경우에는 정상 노드로 저장

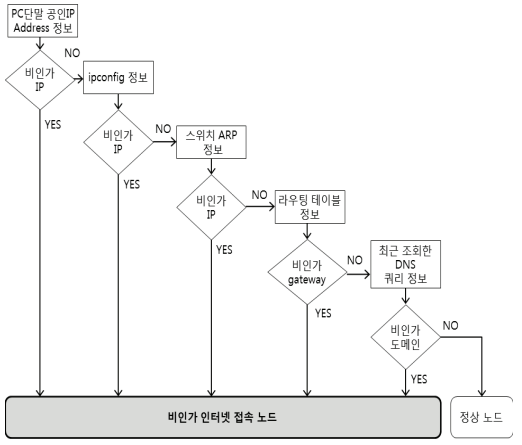

그림 11. 비인가 인터넷 접속 노드 식별 절차

Figure 11. The Procedure for Identifying Unauthorized Internet Access Noed

4.2. 실험 결과 및 분석

제안기법의 실험 절차에 따라 실험한 결과는 다음과 같다. <그림 12>는 실제 비인가 게이트웨이 탐지 Agent를 설치한 A사로부터 수집된 외부 IP Address와 내부 IP Address 정보를 나타낸다. 실험 결과 약 1.2%의 단말이 비인가 단말로 식별되었다. 이 식별된 비인가 단말들은 WIPS, NAC솔루션을 이용하여 통제를 하는 기존 환경에서는 식별하지 못하는 단말 노드들이다.

전체 클라이언트로부터 수집된 정보 중 1단계 ipconfig 정보를 이용한 비인가 IP Address를 식별한 결과, 약 1.2%의 단말이 비인가 게이트웨이를 사용 중인 것으로 파악되었다.

<표 12>는 제안기법을 통해 발견한 비인가 단말의 유형 및 식별 방법을 나타낸다.

법인	대그룹	사번	이름	iip	eip	비고
계	계	K200	배	10.101	121.1	
계	계	K200	김	10.101	121.1	
계	계	K321	김	10.101	121.1	
계	계	K200	조	10.101	121.1	
계	계	K200	조	10.101	121.1	
계	계	K420	한	10.101	121.1	
계	계	K200	정	10.101	121.1	
계	계	K200	남	10.101	121.1	
계	계	K200	박	10.101	121.1	
계	계	K200	김	10.101	121.1	
계	계	K201	최	10.101	121.1	
계	계	K200	이	10.101	121.1	
계	계	K200	김	10.101	121.1	
계	계	K200	유	10.101	121.1	
계	계	K420	정	10.101	121.1	
계	계	K198	박	10.101	121.1	
계	계	K200	권	10.101	121.1	
계	계	K139	김	10.101	121.1	

그림 12. 수집된 단말 정보 출력 화면 (1단계 결과)

Figure 12. Result of Experiment (1st Stage)

실험결과를 분석해보면 모두 A사에서 인터넷을 허용하지 않은 단말에 접속한 결과였다. 해당 기업의 폐쇄망에서 가동 중인 이러한 비인가 단말은 악성코드 감염 위험에 노출되어 있을 뿐만 아니라, 악성코드 감염 시 내부망으로 접속이 가능한 위험도 높은 단말들이었다.

표 12. 비인가 단말 유형 식별 방법

Table 12. Means of Identifying Unauthorized Node

비인가 단말 유형	식별 방법
업무용 PC 단말의 무선랜 혼용 사용	인가되지 않은 무선랜 IP Address
무선공유기 사용	인가되지 않은 무선공유기 IP Address
업무용 PC 단말과 사설망 물리적 연결 사용	인가되지 않은 공인 IP Address
유선 공유기 사용	인가되지 않은 유선 공유기 IP Address
자체 구축된 전용망을 통해 인터넷 사용	인가되지 않은 공인 IP Address 탐지

5. 결 론

본 논문에서는 통제 및 관리가 되지 않는 비인가 인터넷 회선을 식별하기 위해, 금융망 환경에서 운영 중인 보안 시스템을 우회하여 구축된 비인가 노드 탐지 방법론을 제안하였다.

이를 통해, 망분리 시스템의 안정화 및 폐쇄망 환경에서의 센터 집중화 보안관제 우회 차단의 효과가 나타날 것으로 기대된다. 특히, 제안하는 방법론을 기반으로 금융망에서 발생 가능한 비인가 노드 유형을 정의하였고, 그에 적합한 비인가 노드 탐지 기법을 설계하였다. 그 결과, NAC과 같은 기존 보안장비에서 식별하지 못한 비인가 노드를 발견하였다.

그러나, 제안 기법은 가상머신(VM, Virtual Machine)을 이용한 비인가 단말 식별에 제한됨에 따라, 향후연구로서 MBR등의 영역 확인을 통한 비인가 단말 식별 기법 연구가 필요하다.

References

[1] D.-H. Park, *The security system to isolate unauthorized user from internal network in the NAC deployment environment*, Graduate School of computer science, Soongsil University, 2012.

[2] C.-W. Ro, K-T. Kang, I-W. Lee, and J.-H. J, *Computer network security platform configuration with NAC*, The Korea Contents Society, Vol. 7, No. 1, pp. 8-11, 2009.

[3] Y.-M. Song, G.-H. Soon, and J.-K. Hyun, *A case study on NAC system implementation for infringement prevention of information assets*, Journal of the Korea Industrial Information Systems Research. Vol. 19 No. 6, pp. 107-117, 2014.

[4] H.-S. Jun, *Effective network security model for dynamic network access control*, Graduate School of Information Management and Security, Korea University, 2008.

[5] J.-S. Park, M.-H. Park, and S.-H. Jung, *A whitelist-based scheme for detecting and preventing unauthorized AP access using mobile device*, The Journal of The Korean Institute of Communication Sciences. Vol. 38, No. 8, pp.632-640, 2013.

[6] J.-W. Lee, S-Y. and Lee, J.-S. Moon, *Detecting rogue AP using k-SVM method*, Journal of the Korea Institute of Information Security and Cryptology. Vol. 24, No. 1, pp. 87-95, 2014.

[7] J.-W. Lim, J.-D. Jang, C.-P. Yoon, and H.-B. Ryu, *Mobile malicious AP detection and cut-off mechanism based in authentication network*, Convergence security journal. Vol. 12, No. 1, pp. 55-61, 2012.

[8] C. Xun, *A study on security threat detection factorin a wireless environment*, Graduate School of computer science Paichai University, 2015.

[9] J.-D. Jang, *Tethering-based rogue AP detection and prevention mechanismin radius authentication server network*, Graduate School of Embedded Sw, 2011.

[10] D.-Y. Chung, S.-H. Kim, and B.-H. Chung, *A method for detecting Rogue AP based on the Probe Request/Response Frame*, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Vol. 1, pp. 1181-1182, 2015.

금융 폐쇄망 환경에서의 비인가 인터넷 접속 노드 탐지 기법

조형진[1], 김은진[2], 김휘강[3]
[1]*고려대학교 정보보호대학원 금융보안학과*
[2]*경기대학교 국제산업정보학과*
[3]*고려대학교 정보보호대학원*

요 약

최근 기업들은 APT(Advanced Persistent Treat)공격 방어를 위해 사용자 PC단말에 대한 보안강화를 위해 노력하고 있다. 하지만 많은 계열사 및 지점을 보유한 기업의 경우에는 업무의 편의성 및 내부통제 부재로 인해 임의의 사설망을 설치하여 운영하는 사례가 발생한다. 이러한 문제들로 인해, 보안사고가 발생하였으며 심각한 보안 위협이 초래 할 수 있다. 일반적인 무선 네트워크 환경에서 비인가 AP 탐지 등과 같은 연구는 활발히 진행되고 있으나, 금융망에 적합한 비인가 단말 탐지에 대한 연구는 소개되지 않았다. 따라서, 본 논문에서는 금융망 환경에서 비인가 단말 탐지 방법론에 대한 연구를 제안한다. 금융망에 운영중인 보안 시스템을 우회하여 구축된 비인가 단말 및 네트워크에 대한 탐지기술을 개발, 설계 및 분석을 수행한다. 제안하는 방법론을 기반으로 금융망에서 발생 가능한 비인가 노드 유형을 정의하였고 적합한 탐지 기법을 설계하였다. 실험 결과, 보안장비에서 식별하지 못한 비인가 노드를 발견하였으며 보안 우회 차단효과가 나타낼 것으로 기대한다.

Hyung Jin Cho received his B.S degree in Computer Engineering from Dong-A University, Busan, Korea, in 1998. Currently, he is a M.S. student in Korea University, Seoul, Korea. In Jan. 1998, he joined the Division of Information Security at financial company, Korea, and he is currently serving as a Senior manager. His current research interests include policies of information security, finance security, network security and vulnerabilities.
E-mail address: nacfchj@korea.ac.kr

Eunjin Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1999. She received the MS degree and the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2001 and 2007, respectively. She is now an associate professor in Department of International Industrial Information at Kyonggi University. Her current research interests include Management information systems, security economics.
E-mail address: ejkim777@kgu.ac.kr

Huy Kang Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1998. He received the M.S. degree in Industrial & Systems Engineering from KAIST in 2000. He worked as Technical Director at NC soft from 2004 to 2010. He received the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2009. He is now an associate professor in School of Information Security at Korea University. His current research interests include Online game security, network security, network forensic, IDS, botnet detection.
E-mail address: cenda@korea.ac.kr