JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 5 : 1137~1143 May. 2015

내부 중요정보 유출 방지를 위한 차단 시스템 개발

주태경[1] · 신 원[2*]

A New Filtering System against the Disclosure of Sensitive Internal Information

Tae-kyung Ju[1] · Weon Shin[2*]

[1]Dept. of Computers and Media Engineering, Tongmyong University, Busan, 608-711, Korea
[2*]Dept. of Information Security, Tongmyong University, Busan, 608-711, Korea

요 약

다양한 서비스를 제공하는 인터넷 환경에서 수많은 중요정보가 전송되고 있으나, 대부분의 내부 사용자는 어떠한 중요 정보가 전송되는지 모르고 있다. 본 논문에서는 네트워크 패킷 내에 포함된 중요정보를 지속적으로 모니터링하고, 유출 여부를 사용자에게 알려주는 차단 시스템 개발을 목표로 한다. 이를 위하여 중요정보 필터링 시스템을 설계하고 구현하여 그 결과를 분석한다. 사용자는 제안 시스템을 사용하여 중요정보의 유출 여부를 시각적으로 직접 확인할 수 있으며, 해당 패킷을 폐기할 수도 있다. 본 연구 결과는 중요정보 유출 방지에 기여함으로써 기업 내부정보를 대상으로 하는 다양한 사이버 침해를 줄이는데 기여할 수 있을 것으로 판단한다.

ABSTRACT

Sensitive internal information has been transmitted in a variety of services of Internet environment, but almost users do not know what internal information is sent. In this paper, we intend to develop a new filtering system that continuously monitors the sensitive information in outbound network packets and notifies the internal user whether or not to expose. So we design a filtering system for sensitive information and analyze the implementation results. Thus users visually can check whether disclosure of the important information and drop the corresponding packets by the proposed system. The results of this study can help decrease cyber threats various targeting internal information of company by contributing to prevent exposure of sensitive internal information.

키워드 : 중요정보, 네트워크 패킷, 데이터 유출 방지, 모니터링 도구

Key word : Sensitive information, Network packet, Data loss prevention, Monitering tool

Received 05 March 2015, **Revised** 30 March 2015, **Accepted** 14 April 2015

*** Corresponding Author** Weon Shin(E-mail:shinweon@tu.ac.kr, Tel:+82-51-629-1284)
Dept. of Information Security, Tongmyong University, Busan, 608-711, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.5.1137 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

수많은 정보가 컴퓨터시스템에 저장되어 인터넷을 통하여 공유되고 재가공하여 배포할 수 있는 환경이 구축됨에 따라 매년 관련 산업이 폭발적인 성장을 거듭하고 있다. 그러나 관련 서비스의 성장과 새로운 사용자 요구사항, 다양한 기능이 컴퓨터 시스템에 경쟁적으로 도입됨에 따라 이를 악용한 역기능 또한 함께 증가하고 있는 추세이다. 해킹 공격 및 악성코드 유포, 기업 중요정보 변조 및 유출, 개인정보 유출 등의 피해 사례가 지속적으로 보고되고 있다[1].

그러나 인터넷을 통한 다양한 서비스는 각종 서버와 데이터베이스로 구성되어 네트워크로 연결되어 있고, 각종 중요 정보가 시스템에 축적되므로 다양한 취약점이 존재할 뿐만 아니라 이에 따른 위협도 함께 발생하고 있다. 또한 개인 PC 내 백그라운드로 동작하는 키로거, 루트 킷, 트로이목마, 웜 과 같은 악성코드에 의해 자신도 모르는 사이에 중요정보가 유출 될 수 있다. 이로 인해 기업 내 중요 정보 유출로 인한 피해도 갈수록 증가 하고 있는데, 특히 중소기업의 경우 대기업에 비해 기술유출 비중이 높고, 유출 피해금액 또한 갈수록 증가하고 있는 것으로 나타나고 있다. 중소기업 내 중요정보 유출에 관한 피해는 주로 내부자의 정보유출로 인해 발생하는 경우가 많은데, 내부자는 E-mail, FTP, P2P, 메신저 등을 이용해 네트워크로 중요정보 및 고객정보를 유출할 수 있다.

따라서 본 논문에서는 네트워크 패킷 내에서 내부 중요정보 유출 여부를 모니터링하고, 이를 차단할 수 있는 도구 개발을 목표로 한다. 이를 위하여 2장에서는 관련 연구를 살펴보고, 3장에서 내부 중요정보 차단 시스템의 설계와 구현을 제안한다. 4장에서 시스템 동작 및 실험 결과를 제시하고, 마지막 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 패킷 캡처 라이브러리

패킷 캡처를 수행하는 대표적인 라이브러리로는 pcap(packet capture), libpcap(Portable Packet Capturing Library), WinPcap, WinDivert(Windows Packet Divert) 등이 있으며, tcpdump, snort, WireShark와 같은 범용 소프트웨어에 널리 이용되고 있다[2-4]. 그림 1은 WinPcap의 NPF(Net Group Packet Filter)의 구조를 나타내는데, NIC(Network Interface Card)를 통해 지나가는 패킷을 복사하여 User Level에 전송함으로써 필터, 모니터링, 로깅이 가능하도록 지원하는 것을 알 수 있다. 다른 라이브러리도 WinPcap과 구조는 상이하지만, 유사한 기능을 가지고 있다.

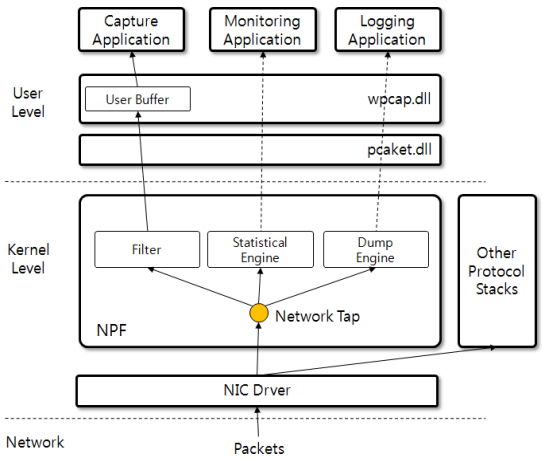

그림 1. WinPcap의 NPF 구조
Fig. 1 NPF structure of WinPcap

반면 WinDivert는 Windows Vista / 7 / 8, Windows Server 2008에서 동작하는 사용자 모드 라이브러리로 패킷에 대한 캡처/도청/수정/차단/수정 등이 가능하다[5]. WinDivert는 다른 라이브러리와는 다르게 사용자 모드 애플리케이션이 윈도우 네트워크 스택(Windows Network Stack)에서 전송된 네트워크 패킷을 캡처/수정/폐기할 수 있는 기능을 지원한다. 그림 2는 WinDivert의 기본 구조를 나타내는데, 새로운 패킷이 생성이 되면 먼저 사용자가 미리 정의한 필터 규칙(Filter Rule)에 해당하는 패킷인지 아닌지를 구분한다. 만약 필터 규칙에 해당하지 않는 패킷이라면 네트워크를 통해 패킷이 전송되고, 필터 규칙에 해당하는 패킷이라면 패킷이 애플리케이션으로 우회된다. WinDivert는 WinPcap 및 libpcap에서 제공하는 스니핑(Sniffing) 기능을 제공할 뿐 만 아니라, 폐기(Dropping), 필터링(Filtering), 수정(Modification), 재주입(Re-injection)과 같은 다양한 기능을 추가로 제공한다[5].

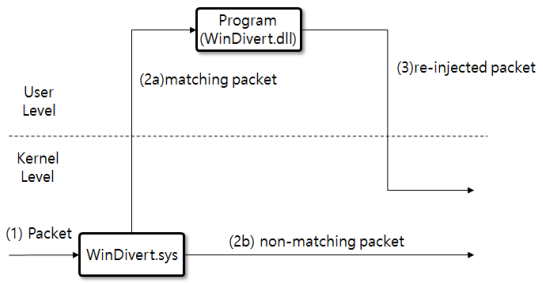

그림 2. WinDivert의 구조
Fig. 2 WinDivert architecture

2.2. 기존 연구

중요정보 유출을 탐지하기 위한 기존 연구들을 살펴보면 다음과 같다.

김유진 등[6]은 쿠키, 인터넷 임시 파일, 로그 파일, 각종 문서파일 등 사용자가 인지하기 어려운 파일 내 개인정보를 찾고 발견된 개인정보에 대해 민감도에 따른 위험도를 산출 하여 사용자에게 삭제를 권고 하는 시스템을 개발하였다.

김원규 등[7]은 DoS, SYN Flooding, ACK Strom, Port Scan, TCP connect Sacn, SYN steath scan 탐지 룰을 정의하고, pcap과 iptables를 이용한 Linux기반 호스트 IPS를 제안하였다. 이 방안은 개인정보 유출 및 해킹 사고에 대응하기 위해 iptables의 차단기능을 활용하였지만, 구현에서 활용한 libpcap은 기본적으로 NIC로부터 전송되는 패킷을 붙잡아 두지 못하며 단순히 패킷을 복사하여 애플리케이션 계층으로 전송하기 때문에 iptables의 차단 기능만으로는 모든 패킷의 유출을 완전히 막을 수 없다는 단점이 있다.

홍정환[8]은 snort를 개량하여 Linux 호스트에서 활용 가능한 침입 탐지 시스템 구현하고, FTP Keylog, IRC Botnet에 의한 정보유출 탐지 예를 보였는데, 유출되는 패킷 내 개인정보를 정규표현식을 이용해 탐지하고, 포렌식 수행을 돕는 기능을 구현하였다. 하지만 중요정보가 단순히 정규표현식을 적용하였을 경우 오탐이 발생 할 가능성이 매우 높다. 또한 탐지된 패킷을 직접 차단하지 못하여 개인정보를 그대로 노출 할 수밖에 없는 한계가 있다. 표 1은 기존 연구와 제안 시스템과의 차이점을 간략히 나타내고 있다.

표 1. 기존 연구와 제안 시스템 비교
Table. 1 Comparison between the previous studies and the proposed system

	Detect information disclosure	Drop packets	OS
Yu-jin Kim et al[6]	Recommend to delete Sensitive information	×	Windows
Won Kyu Kim et al[7]	N/A	△	Linux
Jeong Hwan Hong[8]	△	×	Linux
The proposed system	○	○	Windows

Ⅲ. 차단 시스템의 설계 및 구현

본 논문에서는 기존 연구의 단점을 개선하여 네트워크 패킷 내 내부 중요정보를 탐지할 뿐 아니라 유출이 발견된 경우 해당 패킷을 사용자가 폐기할 수 있는 시스템을 제안한다.

3.1. 시스템 구성

그림 3은 제안 시스템의 구성도이다.

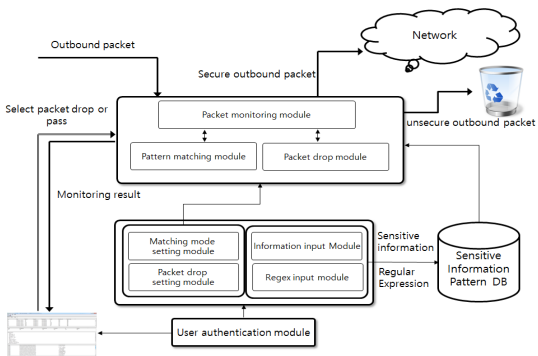

그림 3. 시스템 구조
Fig. 3 System architecture overview

구성요소로 '사용자 인증 모듈(User Authentication Module)', '정보 입력 모듈(Information Input Module)', '정규표현식 입력 모듈(Regex Input Module)', '매칭 모드 설정 모듈(Matching Mode Setting Module)', '패턴

매칭 모듈(Pattern Matching Module)', '패킷 폐기 모듈(Packet Drop Module)', '패킷 모니터링 모듈(Packet Monitoring Module)', 'UI(User Interface)' 이 존재한다. 제안 시스템은 중요정보와 정규표현식 패턴매칭과 수동 패킷 폐기, 자동 패킷 폐기, 모니터링 모드를 구현하였다. Windows 7 환경의 Visual Studio 2012에서 패킷 모니터링 및 패킷 폐기를 구현하기 위해 Win32 API 기반에서 WinDivert-1.1.6 라이브러리를 이용하였다. 또한 각각의 중요정보 특징에 맞게 패킷 내 다량의 중요정보를 탐지 할 수 있도록 하기 위해 정규표현식 라이브러리 PCRE-8.35를 이용하였다.

3.2. 시스템 구현 방안

제안 시스템 구성 요소의 구현 방안은 다음과 같다.

첫째, 사용자 인증 모듈은 허가받지 않은 사용자가 모니터링 도구를 실행하고 각종 설정을 변경할 수 없도록 사용자 인증 정보를 등록하고 인증된 사용자만 사용할 수 있도록 한다.

둘째, 정보 입력 모듈은 고유 식별정보, 민감 정보 등 중요정보를 입력 받아 중요정보 패턴 데이터베이스에 암호화하여 저장한다.

셋째, 정규표현식 입력 모듈은 중요정보 각각의 특성에 맞춘 정규표현식을 입력받는 모듈이다. 입력받은 정규표현식은 중요정보를 탐지하기 위해 패턴과 같이 이용되어 지는데 예를 들면 주민등록번호 정규표현식을 등록하면, 주민등록번호 특성을 가지는 패킷 내 문자열들을 모두 탐지하는데 이용된다. 입력된 정규표현식은 '중요정보 + 정규표현식' 탐지 방식에 이용되어 진다.

넷째, 매칭 모드 설정 모듈은 패킷 내 중요정보 탐지 방식을 결정하는 모듈이다. 탐지 방식에는 '중요정보' 탐지방식과 '중요정보 + 정규표현식' 탐지 방식 중 하나를 설정 할 수 있다. '중요정보' 탐지 방식은 미리 입력된 중요정보를 패킷에 일대일 매칭 한다. '중요정보 + 정규표현식'은 정규표현식을 이용해 패킷 내 중요정보 문자열들을 추출하고, 추출된 문자열 중 입력받은 중요정보가 존재 하는지 패턴 매칭 하게 된다. 만약에 중요정보는 입력되지 않고, 정규표현식만 등록 되어진 경우에는 무 특정 다수 중요정보 탐지가 가능하다. 주로 중소기업 내 다수의 중요정보를 보호하고자 하거나, 개인이 파일 내 다수의 중요정보 유출을 보호하고자 할 때 이용 할 수 있도록 구현 되어있다.

다섯째, 패킷폐기 설정 모듈은 중요정보가 탐지된 패킷을 폐기하는 방식을 결정하는 모듈이다. 폐기 방식에는 수동 패킷 폐기, 자동 패킷 폐기, 모니터링 방식 중 하나를 결정 할 수 있다. 수동폐기는 사용자가 직접 패킷의 폐기 여부를 YES 혹은 NO와 같은 방법으로 실시간 결정 할 수 있는 방식이다. 자동폐기는 탐지된 패킷을 사용자에게 묻지 않고 경고 또는 의심 패킷 여부에 따라 프로그램이 자동 폐기 하는 방식이고 모니터링 모드는 폐기기능을 수행하지 않고 모니터링만 수행 한다.

마지막으로 패킷 모니터링 모듈은 아웃바운드(Outbound) 패킷을 대상으로 패킷 분석을 실시하는데, 패킷 매칭 모듈과 패킷 폐기 모듈을 이용 하여 패킷들을 지속적으로 모니터링, 패턴매칭, 패킷폐기 역할을 수행한다.

3.3. 패킷 필터링 방안

그림 4는 제안 시스템 동작을 간략히 나타내는 순서도이다.

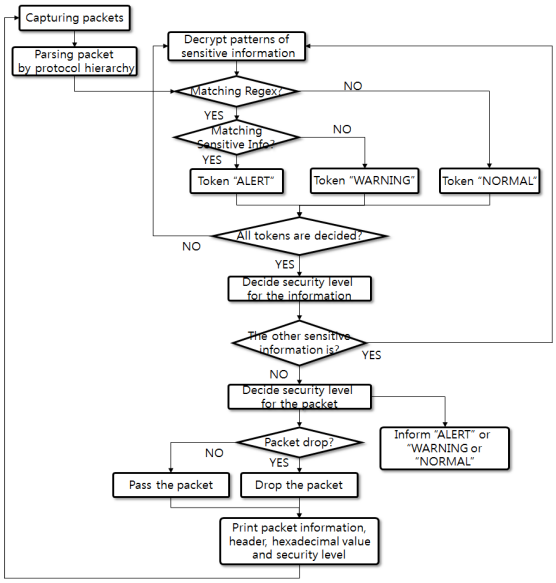

그림 4. 제안 시스템의 동작
Fig. 4 Algorithm of the proposed system

제안 시스템은 최초 패킷 발생 시 패킷을 붙잡아 두고 TCP/IP 계층에 따라 파싱(Parsing)을 수행한다. 그 다음 중요정보의 토큰별로 정규표현식 패턴 매칭을 수

행하여 페이로드 내 중요정보의 토큰을 일차적으로 모두 걸러낸다. 정규식과 일치하는 중요정보가 존재하면 추가적으로 일대일 매칭을 수행 하여 토큰의 보안 레벨(Security Level)을 결정한다. 표 2는 토큰의 보안 레벨 분류를 나타내고 있다.

표 2. 보안 레벨 분류
Table. 2 Security level classification

Category	Details	Conditions
Regular expression pattern	Alert	All matches
	Warning	Regular expression matches
	Pass	Regular expression mismatches
Sensitive information pattern	Alert	Sensitive information matches
	Warning	Sensitive information partially matches
	Pass	Sensitive information

토큰의 보안 레벨은 표 2의 상세 내용에 따라 결정된다. 중요정보 하나와 관련한 토큰 각각에 보안 레벨이 모두 결정되면, 최종적으로 패킷에 대한 보안 레벨을 결정한다. 패킷의 보안 레벨에 따라 사용자에게 'Alert', 'Warning', 'Normal' 등의 결과를 통지하고, 동시에 패킷의 폐기(Drop) 또는 통과(Pass) 여부를 결정한다.

Ⅳ. 시스템 동작 및 실험

4.1. 메인 화면

그림 5는 제안 시스템의 메인화면이다.

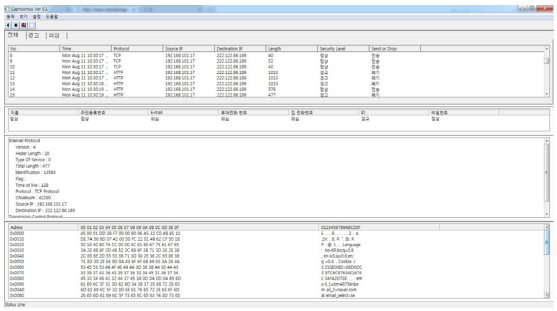

그림 5. 메인 화면
Fig. 5 Main screen

메인화면은 모니터링한 패킷을 프로토콜 계층에 따라 보여주고 사용자가 그 내용을 확인할 수 있도록 해준다. 중요정보와 전체가 일치하는 경우에 경고를, 일부가 일치하는 경우 의심을 출력하여 사용자에게 중요정보 유출 여부를 알려준다. 특히, 경고인 경우 패킷의 전송 혹은 폐기 여부를 사용자가 직접 선택할 수 있도록 구현하였다.

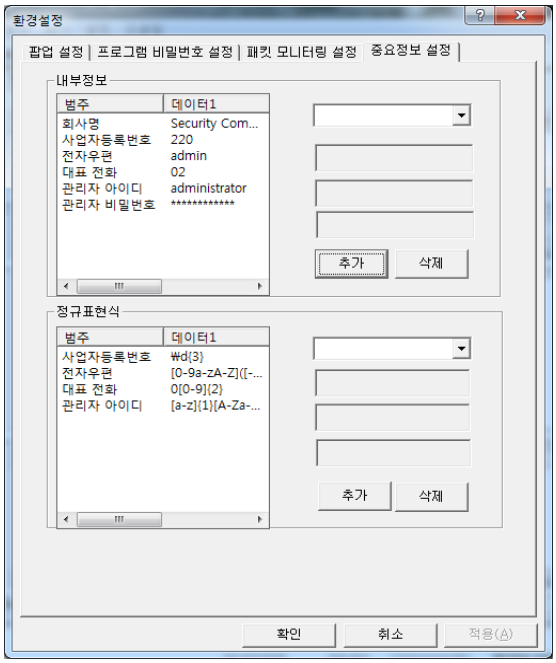

그림 6. 환경 설정
Fig. 6 Configuration UI

그림 6은 환경설정 화면으로, 중요정보 설정은 중요정보와 정규표현식을 입력받는다. 그림 5와 같이 중요정보와 정규표현식은 토큰 별로 나누어서 입력 받고 있다. 그 이유는 중요정보가 네트워크로 전송 되어질 때, 다양한 토큰 별로 나누어져서 전송 되어질 수 있기 때문이다. 이러한 사실은 단순 패턴 매칭을 수행 하였을 경우 정확도가 떨어질 수 있다. 예를 들어 계좌번호를 네트워크를 통해 패킷으로 전송 한다고 하였을 경우 111111-22-333333, phonNum1=111111 phonNum2=22 phonNum3=333333, 11111122333333 등 같은 중요정보라도 다양한 형태로 전송 되어 질 수 있기 때문에 사용자가 입력한 개인정보에 따라 단순히 정규식을 적용

하거나 일대일 매칭을 수행 하면 패킷 내 중요정보가 존재 하더라도 탐지 하지 못하는 경우가 발생할 수 있다. 따라서 토큰별로 일대일 매칭 혹은 정규식을 적용하여 중요정보 탐지 정확도를 올릴 수 있다.

4.2. 실험 및 분석

실험환경은 PC에 키로거(Keylogger), 원격 접속 소프트웨어, 제안 도구를 설치하고, 노트북에 Windows 7과 원격 접속 소프트웨어를 설치하여 동작하였다. 본 실험은 다음과 같은 시나리오로 진행되었다.

1. 키로거가 설치된 PC에 에 중요정보를 입력한다.
2. PC에 설치된 원격 접속 소프트웨어를 이용하여 외부 PC로 원격접속 후 중요정보파일을 유출한다.

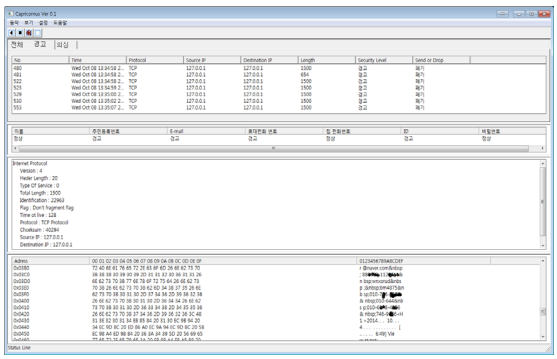

그림 7. 키로거 전송 중요정보 포함 패킷을 필터링
Fig. 7 Filtering packets including sensitive information by a keylogger

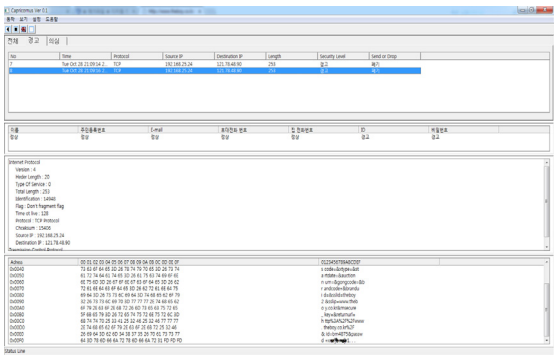

그림 8. 웹사이트 접속 시 중요정보를 포함하는 패킷을 필터링
Fig. 8 Filtering packets including sensitive information for accessing a website

그림 7은 키로거를 통해 수집된 ID, 패스워드, 이메일, 주민등록번호, 핸드폰 번호, 집 전화번호 등을 포함하는 중요정보 파일을 원격 접속 소프트웨어를 통해 외부 PC로 전송을 시도 했을 때 관련 패킷들이 차단 됨을 타나내고 있다. 파일 전송이 차단되자 원격 접속 소프트웨어가 폐기된 패킷의 재전송을 여러 차례 시도 하려 했음을 알 수 있다. 그림 8은 노트북으로 무선네트워크 환경에서 제안도구를 이용해 온라인 쇼핑몰 T 사이트에서 로그인 할 때 패킷 모니터링 결과를 나타내고 있다. 모니터링 결과 ID, 패스워드가 암호화 되지 않은 상태로 전송 되려 했고 패킷 폐기가 이루어지고 접속이 차단됨을 확인할 수 있다.

Ⅴ. 결 론

정보화 사회에서 정보는 곧 재화와 같은 의미를 가진다. 최근 기업 내 기업정보 및 중요정보 유출과 관련한 사건이 지속적으로 증가하고 있는데, 이러한 정보 유출은 재화 유출과 같다 할 수 있다. 특히, 중소기업은 대기업에 비해 기술유출 비중이 높고, 피해금액도 갈수록 증가하고 있다. 또한 2013년 기준으로 중소기업의 10.2%가 최근 3년간 기술유출로 인해 피해를 경험하였으며, 피해 중소기업들은 기술유출 1건당 평균 16.9억원의 매출액이 감소한 것으로 나타났다[9]. 하지만 중소기업 1개사 당 기업 전체 매출액의 0.24%만을 보안관리 비용으로 지출하고 있는 것으로 나타나 내부자 및 악성코드에 의한 기업 중요정보와 개인정보 변조 및 유출과 같은 피해가 갈수록 증가할 것으로 보인다[9].

본 논문에서는 정규표현식 기반의 패턴매칭을 수행하여 중소기업 및 개인이 무특정 다수의 중요정보 유출을 탐지 및 차단을 수행하는 시스템을 구현하고 실험을 수행하였다. 이를 통하여 제안 시스템은 외부로 유출시키려는 중요정보 파일 및 패킷을 차단함을 확인할 수 있었다. 따라서 전문 지식이 없는 사용자도 사내 PC에 제안 도구를 설치하여 내부자 및 악성코드에 의한 중요정보 유출 차단을 수행함으로서, 영세한 기업 내 중요 정보 유출 방지에 도움이 될 수 있을 것이라 예상한다.

REFERENCES

[1] KrCERT/CC, “Korea Internet Incident Trend Report”, Korea & Security Agency, December 2014.

[2] pcap[Internet]. available: http://en.wikipedia.org/wiki/Pcap

[3] Luis MartinGarcia, PROJECT LIST [Internet]. available: http://www.tcpdump.org/related.html

[4] The WinPcap Team, WinPcap Documentation [Internet]. availavle: http://www.winpcap.org/docs/docs_412/html/main.html

[5] basil, WinDivert 1.1: Windows Packet Divert[Internet]. available: https://reqrypt.org/windivert-readme.txt

[6] Yu-jin Kim, Seng-phil Hong, “Risk Detection and Control Mechanism Design for the protection of Personal Information”, *Proceeding of the Korean Society for Internet Information*, pp.59-60, 2010.

[7] Won Kyu Kim, Seung Hwi Kim, Jae Hyuk Lee, Tae Chul Hwang, Young Yeol Choo, “Implementation of Host Intrusion Prevention System Based on Linux”, *Proceeding of the Fall Conference of the Korea Multimedia Society*, pp. 95-98, 2006.

[8] Jeong Hwan Hong, "Protection of Private Information Via Packet Filtering and Pattern Matching with Regular Expressions", MA Thesis, Hanyang university, 2007.

[9] Min-sun No, “Current Status and Challenges for the Support Policies of Technologies Protection for Small and Medium Business”, *KOSBI Issue Paper*, Korea Small Business Institute, no. 14-17, December 2014.

주태경(Tae-kyung Ju)

2014년 2월 : 동명대학교 정보보호학과 졸업
2014년 3월 ~ 현재 : 동명대학교 컴퓨터미디어공학과 석사 과정
※관심분야 : 네트워크 보안, 소프트웨어 보안

신원(Shin, Weon)

2001년 8월 : 부경대학교 전자계산학과 이학박사 졸업
2002년 3월 ~ 2005년 1월 (주)안철수연구소 선임연구원
2005년 3월 ~ 현재 동명대학교 정보보호학과 전임강사, 조교수, 부교수
※관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식