http://dx.doi.org/10.3745/KTCCS.2013.2.11.489

A Monitoring Tool for Personal Information Leakage Prevention in Network Packets

Tea Kyung Ju† · Chong Min Hong†† · Weon Shin†††

ABSTRACT

Personal information has been transmitted in a variety of services of Internet environment, but individual users do not know what information is sent. In this paper, we aim to develop a monitoring tool that continuously monitors personal sensitive information in network packets and informs the user whether or not to leak. So we implement a monitoring tool of personal information and analyze the experiment results. In addition, we introduce a prevention of confidential information in company and a leakage prevention of medical information, for applications that take direct advantage. The results of this study, by contributing to prevent leakage of personal information, can help reduce cyber threats variously targeting personal information of users.

Keywords : Personal Information, Monitoring Tool, Leakage Prevention, Network Packet

네트워크 패킷 내 개인정보 유출 방지를 위한 모니터링 도구 개발

주 태 경† · 홍 정 민†† · 신 원†††

요 약

다양한 서비스를 제공하는 인터넷 환경에서 수많은 개인정보가 활용되고 있으나, 개인 사용자는 자신의 어떠한 개인 정보가 전송되는지 모르고 있다. 본 논문에서는 네트워크 패킷 내에 개인정보를 지속적으로 모니터링하고, 유출 여부를 사용자에게 알려주는 모니터링 도구 개발을 목표로 한다. 이를 위하여 개인정보 모니터링 도구를 구현하고, 그 결과를 분석한다. 또한 기업 기밀정보 유출 방지, 의료정보 유출 방지 등 직접 활용할 수 있는 응용 분야에 대해 제시한다. 본 연구 결과는 개인정보 유출 방지에 기여함으로써 개인정보를 대상으로 하는 다양한 사이버 침해를 줄이는데 기여할 수 있을 것으로 판단한다.

키워드 : 개인정보, 모니터링 도구, 유출 방지, 네트워크 패킷

1. 서 론

개인용 컴퓨터(PC)가 보편화되어 누구나 인터넷에 접속하여 원하는 정보를 얻고 재가공하여 배포할 수 있는 환경이 구축됨에 따라 매년 관련 산업이 폭발적인 성장을 거듭하고 있다. 최근에는 개인용 컴퓨터보다는 노트북 컴퓨터를 기반으로 한 Tablet PC, MID(Mobile Internet Device)가 보편화 되었으며, 간단한 업무 처리는 물론 엔터테인먼트, DMB(Digital Multimedia Broadcasting)와 무선 인터넷 접속 등과 같은 작업들을 이동 중에 수행할 수 있다. 이를 통해 언제 어디서나 손쉽게 장소에 구애받지 않고 누구나 개인용 컴퓨터를 사용할 수 있게 되었다. 그러나 사용자의 폭발적 증가와 새로운 기능의 경쟁적 도입에 따라 이를 이용한 역기능 또한 함께 증가하고 있는 추세이다. 해킹을 통한 정보 변조 및 유출, 악성코드를 통한 중요정보 유출, 분산서비스거부공격(DDoS)을 위한 좀비 역할 등의 사례가 지속적으로 증가하는 것으로 보고되고 있다[1].

그러나 인터넷을 통한 다양한 서비스는 각종 서버와 데이터베이스로 구성되어 있으면서 네트워크로 연결되어 많은 정보가 시스템에 축적되고 있기 때문에 이로 인한 여러 가지 취약점이 발생한다. 특히, 각종 포털 사이트 및 상거래 서비스에서는 홍보 및 마케팅, 전자거래 등을 이유로 다양한 개인정보를 다루고 있으므로 공격자에게는 매우 매력적인 공격 대상이 될 수 있다. 또한, 사용자가 사용하는 개인용 컴퓨터가 취약하여 악성코드에 감염되거나 백도어 설치, 서비스 업체 내부자에 의한 유출 등으로 언제든지 개인정보가 유출될 가능성을 내재하고 있는 상황이다. 최근 발생한

† 준 회 원 : 동명대학교 정보보호학과 학부생
†† 정 회 원 : 동명대학교 간호학과 조교수
††† 종신회원 : 동명대학교 정보보호학과 부교수
논문접수 : 2013년 10월 4일
심사완료 : 2013년 11월 2일
* Corresponding Author : Weon Shin(shinweon@tu.ac.kr)

일련의 개인정보 유출의 내막을 면밀히 조사해 보면 이와 같은 원인으로 사건들이 발생했음을 확인할 수 있다.

본 논문에서는 네트워크 패킷 내에서 개인정보를 관찰하고 유출 여부를 모니터링할 수 있는 도구 개발을 목표로 한다. 이를 위하여 2장에서는 관련 기술과 연구를 살펴보고, 3장에서 개인정보 모니터링 도구의 설계와 구현, 실험결과를 분석한다. 4장에서 응용 분야를 제시하고, 마지막 5장에서 결론을 맺는다.

2. 관련 법 및 기술

2.1 개인정보 개요

개인정보보호법[2]에서 말하는 개인정보는 “고유식별정보”와 “민감정보”로 구분된다. 그 중에서 “민감정보”는 개인정보보호법 제23조에서 규정하고 있다.

> 제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. (이하 생략)

또 하나의 개인정보인 “고유식별정보”에는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등이 속한다. 이는 개인정보보호법 제24조에서 다음과 같이 규정하고 있다.

> 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다. (이하 생략)

특히, 안전행정부는 법률에서 개인정보 침해를 방지하기 위하여 다량으로 주민등록번호를 수집, 보유, 활용하는 공공기관 및 일정 기준 이상의 개인정보처리에 대해 공인인증서, 아이핀(i-Pin), 휴대전화 인증 등의 주민등록번호를 대체할 수 있는 수단의 제공을 의무화하고 있다. 그리고 고유식별정보 또한 분실, 도난, 유출, 변조, 훼손되는 것을 방지하기 위하여 암호화 등의 방법을 사용하도록 하고 있다[2].

2.2 패킷 모니터링 개요

패킷 모니터링(Packet Monitoring)은 네트워크상에서 발생하는 여러 일들을 이해하기 위하여 네트워크에 흘러 다니는 실제 데이터인 패킷을 수집하고 해석하는 과정이다. 패킷 모니터링을 통하여 패킷 분석을 수행할 수 있고, 이를 통해 프로토콜의 동작 방식을 파악할 수 있을 뿐 아니라 네트워크 문제 발생시 즉각 대응할 수 있도록 도와준다. 패킷 모니터링을 수행하기 위해서는 완성된 소프트웨어 형태의 패킷 분석기와 라이브러리 형태인 패킷 캡처 라이브러리가 주로 사용되고 있다.

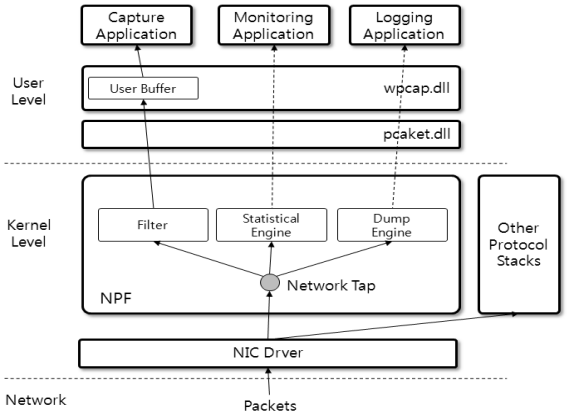

Fig. 1. NPF structure of WinPcap

그 중 패킷 분석기(Packet Analyzer)는 네트워크를 지나다니는 패킷들을 실시간으로 수집, 각 프로토콜 포맷에 맞게 분석할 수 있도록 해주어서 실제 네트워크상에서 일어나는 대부분의 일을 확인할 수 있는 아주 유용한 도구이다. 다양한 운영체제를 지원하는 오픈 소스 패킷 분석기로는 Wireshark[3]가 가장 많이 사용되고 있으며, Windows 운영체제에서는 Microsoft사의 Microsoft Network Monitor[4]도 많이 사용된다. 또한 패킷 캡처 라이브러리(Packet Capture Library)는 운영체제 상에서 패킷 캡처를 수행하여 분석할 수 있게 해주는 도구인데, 다양한 운영체제를 지원하는 libpcap[5], Windows 운영체제에 특화된 WinPcap[6] 등이 있다. 운영체제 자체가 제공하는 패킷 라이브러리에는 많은 한계가 있으므로, 일반적으로 공개된 패킷 캡처 라이브러리를 활용하여 패킷 분석기를 제작하고 이를 이용하여 패킷 모니터링을 수행한다. Fig. 1은 WinPcap에서 동작하는 NPF(Netgroup Packet Filter)의 구조를 나타내는데, 이를 통하여 프로토콜 계층별 데이터를 필터링하거나 모니터링할 수 있도록 구현되어 있다.

3. 개인정보 모니터링 도구 설계 및 구현

3.1 전체 시스템 구성과 구현 방법

제안 개인정보 모니터링 도구는 Windows 7의 Visual Studio 2010 환경에서 Win32 API를 이용하여 개발되었으며, 패킷 캡처를 구현하기 위하여 오픈 소스 라이브러리인 WinPcap 4.1.3을 사용하였다. 사용자 로그인을 처리하기 위하여 패스워드를 SHA-512로 해쉬하여 저장하도록 구현하였으며, 개인정보 패턴을 안전하게 저장하기 위하여 128bit AES를 통하여 암호화를 구현하였다.

개인정보 모니터링 도구는 중요 개인정보를 미리 저장해 둔 후 컴퓨터 시스템에서 나가는 아웃바운드 패킷을 모니터링하다가 지정된 개인정보 패턴과 일치하면 경고 또는 주의하는 방식으로 이루어진다. 개인정보 모니터링 도구는 “사용자 인증 모듈”, “개인정보 입력 모듈”, “패킷 모니터링 모듈”, “화면 출력 UI” 네 개의 모듈로 나누어 동작하는데, Fig. 2는 전체 시스템은 구성을 보여준다.

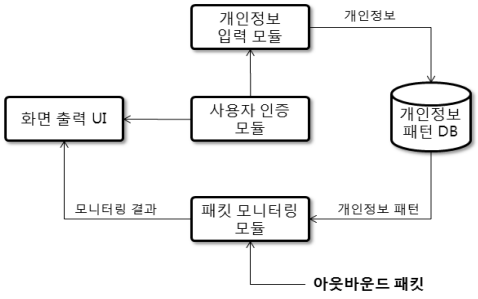

Fig. 2. Diagram of system

사용자 인증 모듈은 허가받지 않은 사용자가 모니터링 도구를 실행하고 각종 설정을 변경할 수 없도록 사용자 인증 정보를 등록하고 인증된 사용자만 사용할 수 있도록 한다. 프로그램 실행 시와 설정을 변경할 경우 로그인 패스워드를 입력하여 사용하도록 해준다.

개인정보 입력 모듈은 개인정보 중 고유식별정보와 민감정보를 입력한 후 암호화하여 저장한다. 고유식별정보에는 이름, 주민등록번호, 패스워드 등을 포함하고, 민감정보에는 이메일 주소, 전화번호, 아이디 등을 포함하여 개인정보 패턴 DB(Database)에 암호화하여 저장한다. Fig. 3은 환경설정에서 개인정보를 설정하여 저장하는 화면이다.

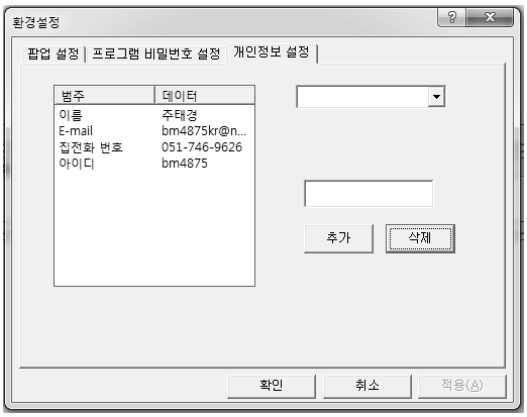

Fig. 3. Example of setting personal information

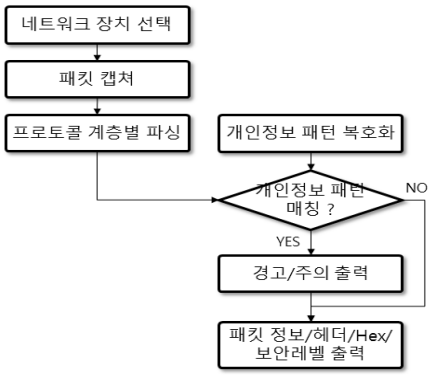

Fig. 4. Algorithm of the monitoring tool

```
DWORD WINAPI Capture(LPVOID Param)
{
   패킷 필터 규칙 설정;
   네트워크 디바이스 목록 가져오기;
   사용자가 선택한 네트워크 디바이스 열기;
   do{
      네트워크상에서 캡처한 데이터를 저장;
      저장된 데이터를 대상으로 2계층 프로토콜 파싱;
      3계층 프로토콜을 결정;
      if(3계층 프로토콜 파싱 가능){
         3계층 프로토콜을 파싱;
         4계층 프로토콜을 결정;
         if(4계층 프로토콜 파싱 가능){
            4계층 프로토콜을 파싱;
            5계층 프로토콜을 결정;
            if(5계층 프로토콜 파싱 가능)
               디코딩 수행;
         }
      }
      사용자 패킷 필터 규칙 적용;
   }while(사용자 정지가 아닌 동안);
}
```

Fig. 5. Packet capture algorithm

패킷 모니터링 모듈은 아웃바운드(Outbound) 패킷을 대상으로 패킷 분석을 실시하는데, 개인정보 패턴과 일치하는 패킷들을 지속적으로 모니터링한다.

Fig. 4는 패킷 분석 과정을 다이어그램으로 보여주는데,

```
/* 5계층 프로토콜 패킷 파서 함수 */
void Layer5_HTTP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
void Layer5_POP3(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
void Layer5_TELNET(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
/* 4계층 프로토콜 패킷 파서 함수 */
void Layer4_TCP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
void Layer4_UDP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
/* 3계층 프로토콜 패킷 파서 함수 */
void Layer3_IP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
void Layer3_ARP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
void Layer3_RARP(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
/* 2계층 프로토콜 패킷 파서 함수 */
void Layer2_Ether(INPUT void *vP, struct _PACKETINTFO * pInfo, struct _HEADERINFO * hInfo, SECINFO * sInfo)
```

Fig. 6. Packet parser functions per protocol layers

네트워크 장치를 선택하고 해당 장치에서 네트워크 패킷을 장치 드라이버로부터 읽어와서 2계층 데이터링크(Data Link Layer), 3계층 네트워크(Network Layer), 4계층 전송(Transport Layer), 5계층 어플리케이션(Application Layer)까지 각 계층에서 패킷을 조립하고 파싱(Parsing)하여 저장된 개인정보 패턴과 비교하여 일치하는 경우 그 결과를 알려준다. Fig. 5는 패킷 캡처 알고리즘을 간략하게 보여준다. 지속적으로 패킷을 캡처하고, 사용자가 설정한 패킷 필터 규칙을 적용하여 일치 여부를 반환한다. Fig. 6은 각 계층별 패킷 파서 함수를 나열하였는데, 각 계층의 프로토콜에 따라 각각 파싱을 수행하도록 구성되어 있다.

화면 출력 UI(User Interface)는 모니터링한 패킷을 프로토콜 계층에 따라 각각 보여주고 사용자가 그 내용을 확인할 수 있도록 해준다. 또한, 개인정보와 전체가 일치하는 경우에는 “경고”를, 일부가 일치하는 경우에는 “의심”을 출력하여 사용자에게 메시지 창을 통하여 개인정보 유출 여부를 알려준다. Fig. 7은 사용자 인터페이스를 통하여 보여주는 모니터링 도구의 결과 화면이다.

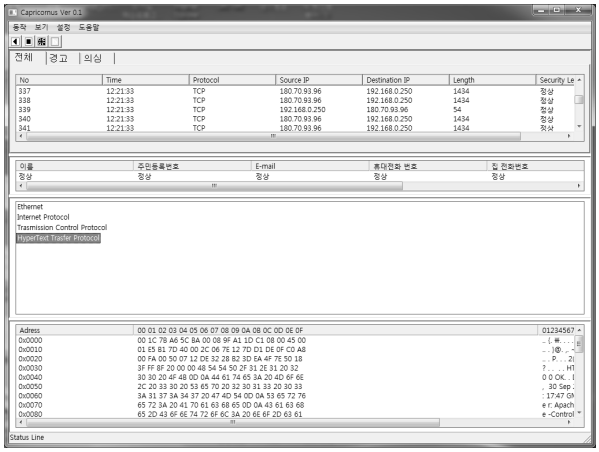

Fig. 7. User interface of the monitoring tool

Fig. 8은 모니터링 중 발생한 경고 및 주의 메시지 창을 보여주는데, 아웃바운드 패킷이 개인정보 패턴과 일치하는 경우 별도의 메시지 창을 띄우고 사용자에게 메시지, 패킷 번호, 보안레벨, 시간을 알려준다.

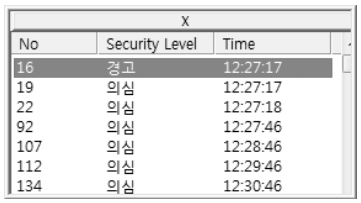

Fig. 8. Warning examples

3.2 구현 결과

모니터링 도구 구현 후 실험을 수행하기 위하여 개인정보 패턴의 일치여부에 따라 Table 1과 같이 경고와 주의를 설정하였다. 아웃바운드 패킷에 일치하는 개인정보가 탐지된 경우 “경고”로, 부분 일치하는 개인정보가 탐지된 경우 “주의”로 별도의 메시지 창을 통해 사용자에게 통지한다. 경고와 주의로 분류되지 않는 패킷에 대해서는 정상 패킷으로 간주하고 어떠한 경고도 발생하지 않는다.

Table 1. Classification examples of warning

종류	구분	상세 내용
주민등록번호	경고	모두 일치, 뒤 7자리 일치
	의심	연속된 앞 6자리 일치
	정상	경고와 의심을 제외한 경우
이름	경고	모두 일치
	의심	연속된 한글 2개 이상 3개 미만
	정상	한글 1개 이하
이메일	경고	모두 일치
	의심	도메인 앞 연속된 문자열 50%이상 일치
	정상	도메인 일치 시 무시
집 전화번호	경고	모두 일치
	의심	연속된 가운데 3~4자리, 끝 4자리
	정상	지역번호
휴대폰 전화번호	경고	모두 일치
	의심	연속된 가운데 3~4자리. 끝 4자리
	정상	경고와 의심을 제외한 경우
아이디	경고	모두 일치
	의심	연속된 문자열 50%이상 일치
	정상	50% 미만 일치
비밀번호	경고	모두 일치
	의심	연속된 문자열 50%이상 일치
	정상	50% 미만 일치

또한, 해당 개인정보는 개인정보 설정 기능을 통하여 별도로 저장한 후 모니터링 도구를 실행하였다. 가장 많이 사용하는 부라우저인 Internet Explorer를 사용하여 P2P 사이트 등 3개의 사이트에 접속하여 로그인한 경우의 결과는 Table 2와 같다.

Table 2. Experiment results

사이트	패킷 개수	패킷 평균 크기(B)	경고	의심
F NAS 로그인	50	234	1	0
T사이트 로그인	37	781	0	1
M사이트 로그인	733	518	112	2
T사이트 회원정보 수정	978	583	3	8
M사이트 회원정보 수정	437	484	107	2

제안 모니터링 도구는 개인정보 유출 경고와 유출 의심에 해당하는 패킷을 모두 찾아내어 100% 적중률을 보였으나, 다음과 같은 특징이 발견되었다. 첫째, 메일 주소 등 각종 개인정보의 인코딩 방식을 달리하거나 정보를 잘게 쪼개어서 탐지가 어렵도록 만든 사이트도 있다. 둘째, 회원정보 변경시 이메일 주소, 성명, 아이디 등이 반복적으로 패킷에 들어 있어 탐지가 높은 사이트도 있다. 셋째, 유명 사이트 및 포털 사이트 등은 암호화를 수행하므로 탐지 여부를 확인할

수 없으나, P2P 사이트, 소규모 사이트, 오래된 사이트에서 유출 경고와 유출 주의가 많이 발생하고, 일반적으로 가입 이후 회원정보 수정 페이지에서도 유출 경고와 유출 주의가 많이 발생한다.

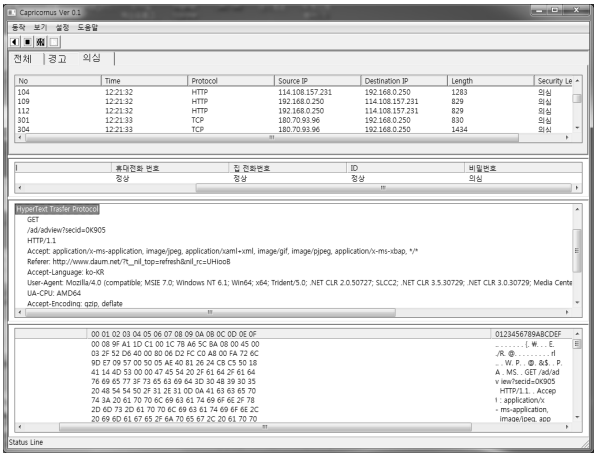

Fig. 9. Screenshot of the monitoring tool

Fig. 9는 제안 모니터링 도구의 실행 결과인데, 모니터링 한 모든 패킷을 관찰할 수 있고 각 패킷에 대한 세부 내용도 확인할 수 있도록 구현되었다.

4. 응용 분야

제안 모니터링 도구는 그 자체만으로도 일반 PC에 설치된 상태에서 평소에 개인정보를 모니터링하다가 유출이 탐지되는 경우 사용자에게 그 내용을 통지할 수 있으나, 시스템 구성 또는 프로그램 변경을 통하여 사용 분야를 확장할 수도 있다. 이에 대한 응용분야로 스마트폰 개인정보 유출 방지, 의료정보 유출 방지에 제안 모니터링 도구를 직접 활용할 수 있다.

첫째, 제안 개인정보 모니터링 도구가 설치된 PC에 무선 네트워크 접속을 위한 환경 구성을 통하여 스마트폰 개인정보 유출 방지에 활용할 수 있다. 최근에 출시되는 무선 NIC (Network Interface Card)는 무선 AP(Access Point) 기능도 함께 포함하고 있으므로, 모니터링 도구가 설치된 PC에 무선 NIC를 연결한 후 무선 AP로 설정한 후 스마트폰으로 Wi-Fi 기능을 이용하여 PC에 무선으로 접속하면 스마트폰의 모든 패킷을 PC에서 모니터링 할 수 있게 된다. 제안 모니터링 도구에서는 스마트폰의 무선 패킷도 함께 모니터링 함으로써 개인정보 유출 여부를 확인할 수 있다. 즉, 별도의 프로그램 소스 변경 없이 간단한 무선 네트워크 환경 구성만으로 일반 PC의 개인정보 유출은 물론 이 PC에 무선으로 접속하는 스마트폰 내의 개인정보 유출 방지에도 함께 적용할 수 있다.

둘째, 제안 개인정보 모니터링 도구는 개인정보 입력과 패턴 부분의 프로그램 수정을 통하여 기업 내의 중요정보

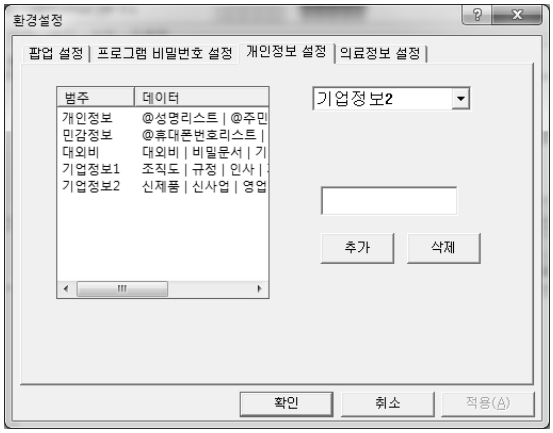

Fig. 10. Example of setting company information

유출 방지에 활용할 수 있다. 최근 기업에서는 이메일, 메신저, USB 메모리, SD카드, CD-RW, 프린터 등 모든 정보 유출 경로에 따라 흐름을 제어하는 DLP(Data Loss Prevention)[7]를 도입하기도 한다. 대규모 조직에 적합하고, 전사적인 정책 수립과 함께 전문인력이 투입되어야 하는 보안 솔루션으로 많은 기업이 도입을 검토하고 있지만, 소규모 기업에는 도입이 적합하지 않고 영세한 기업도 적용하기 어려운 단점이 있다. 반면 제안 모니터링 도구는 손쉽게 업무용으로 사용하는 기업 PC에 제안 개인정보 모니터링 도구를 설치하고 기업정보에 대한 부분을 입력해 두면 아웃바운드 패킷을 모니터링하다가 관련 중요 정보가 유출되는 경우 이를 탐지할 수 있게 된다. 단순히 해당 단어만을 입력하는 것이 아니라 이들 단어를 기반으로 하는 별도의 리스트를 만들어 활용하면 더 정교한 패턴 모니터링도 가능하게 된다. Fig. 10은 기업정보 설정을 입력할 수 있도록 수정한 예인데, 다양한 범주에 중요 기업정보를 입력하면 기업정보 유출 방지에 적용할 수 있다.

셋째, 제안 개인정보 모니터링 도구는 개인정보 입력 부분과 패턴 부분의 프로그램 수정을 통하여 의료정보시스템의 의료정보 유출 방지에도 활용할 수 있다. 개인정보보호법[2]은 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정하고 있는 일반법이므로 의료분야를 규율하고 있는 다른 법령 등에 환자나 의료기관 등의 개인정보 처리와 관련된 특별한 규정이 있으면 해당 법령이 우선 적용되며 그렇지 않은 경우 개인정보 보호법이 적용된다. 즉, 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보가 대상이 되며, 의료법[8]에 규정이 있는 경우 의료법을 우선 적용하고 규정이 없는 경우 개인정보보호법을 적용한다. 이를 위하여 보건복지부에서는 의료기관 개인정보보호 가이드라인[9]을 공표하여 구체적인 사례들을 설명하였다. 즉, 가이드라인에서는 환자 관리를 위한 등록번호, 병명, 수술명, 수술날짜, 입퇴원날짜, 의료보험(자동차보험), 산부인과 정보, 사망 정보, 진료과(담당의), 마약사용 정보, 향정신성약물 정보, 감염여부 정보, 간호 일정, 간호수행 정

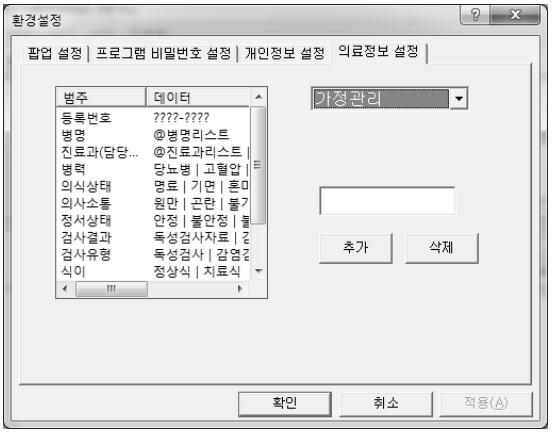

Fig. 11. Example of setting medical information

보, 분만 정보, 검사날짜, 검사결과 등의 의료정보는 민감정보로 분류할 수 있고, 제안 개인정보 모니터링 도구의 보호 대상이 된다. 따라서 병원 내의 의료정보 시스템에서 사용하는 PC에 제안 개인정보 모니터링 도구를 설치하면 아웃바운드 패킷을 대상으로 의료정보 유출 여부를 모니터링 할 수 있다. Fig. 11은 의료정보 설정을 입력할 수 있도록 수정한 예인데, 다양한 범주에 중요 의료정보를 입력하여 의료정보 유출 방지에 적용할 수 있다.

5. 결 론

해마다 개인정보 유출로 인한 굵직한 사건들이 언론에 보도되고 있으며, 이로 인한 피해액도 막대한 것은 물론 2차 범죄에 악용될 수 있는 우려도 큰 것으로 파악되고 있다. 특히, 최근 사이버 침해의 60~70%가 보안에 대한 개념도 희박하고 대응 방법에 대해서도 한계를 가질 수밖에 없는 일반 개인이 표적의 대상으로 한다는 것은 매우 큰 시사점을 제시하고 있다.

본 논문에서는 네트워크를 통하여 개인정보 유출 방지를 목적으로 하는 모니터링 도구를 설계하고 패킷 캡처 라이브러리를 이용하여 실제 구현한 후 실험하였다. 제안 개인정보 모니터링 도구는 PC 기반 환경에서 개인정보 유출 방지에 직접 적용할 수 있고, 약간의 수정을 거쳐서 기업 또는 의료 환경에서 기업정보 보호와 의료정보 보호에도 직접 응용할 수 있다. 특히, 최근 개인정보를 이용하여 개인을 대상으로 하는 피싱(Phishing), 스미싱(Smishing, SMS Phising) 등 심각한 위협들이 급증하고 있는데, 제안 개인정보 모니터링 도구는 개인 단위의 개인정보 유출을 미연에 방지함으로써 이로 인한 2차 범죄 방지에 도움을 줄 수 있을 것으로 판단한다.

참 고 문 헌

[1] KrCERT/CC, “Korea Internet Incident Trend Report,” Korea & Security Agency, November, 2012.

[2] Korea Ministry of Security and Public Administration, *Personal Information Protection Act,* Korea Ministry of Government Legislation, September, 2011.

[3] Wireshark [Internet], http://www.wireshark.org/

[4] Microsoft Network Monitor [Internet], http://www.microsoft.com/en-us/download/details.aspx?id=4865

[5] TCPDUMP/LIBPCAP [Internet], http://www.tcpdump.org/

[6] WinPcap [Internet], http://www.winpcap.org/

[7] K. H. Nam, H. S. Kang, J, H, Kil and S. I. Kim, “Data Loss Prevention Technology Trends,” *Weekly Technology Trends Report*, Vol.1413, pp.1-9, 2009.

[8] Korea Ministry of Health and Welfare, Medical Service Act, Korea Ministry of Government Legislation, August, 2013.

[9] Korea Ministry of Health and Welfare, *Privacy Guidelines for Medical Institutions*, Korea Ministry Of Security And Public Administration, September, 2012.

주 태 경

e-mail : jtk4556@naver.com

2007년~현 재 동명대학교 정보보호학과 학부생

관심분야 : 소프트웨어보안, 리버스엔지니어링, 침입탐지

홍 정 민

e-mail : cmhong@tu.ac.kr

2005년 이화여자대학교 간호과학과 (간호학석사)

2011년 이화여자대학교 간호과학과 (간호학박사)

2011년~현 재 동명대학교 간호학과 조교수

관심분야 : 의료정보, 간호정보, 성인간호, 노인간호, 간호교육

신 원

e-mail : shinweon@tu.ac.kr

1998년 부경대학교 전자계산학과 (이학석사)

2001년 부경대학교 전자계산학과 (이학박사)

2002년~2005년 (주)안철수연구소 선임연구원

2005년~현 재 동명대학교 정보보호학과 부교수

관심분야 : 소프트웨어보안, 악성코드대응, 디지털포렌식