H/W 정보의 인증을 통한 내부정보유출 방지 기법*

양 선 옥** · 최 낙 귀*** · 박 재 표**** · 최 형 일*****

A Authentication technique of Internal Information Hacking Protection based on H/W Information

Yang, Sun Ok · Choi, Nak Gui · Park, Jae Pyo · Choi, Hyung Il.

〈Abstract〉

To the cause of the development of IT technology and the Internet, information leakage of industry is also facing a serious situation. However, most of the existing techniques to prevent leakage of information disclosure after finding the cause of defense. Therefore, in this paper by adding information about the Hardware to offer a way to protect the information.

User authentication information to access the data according to different security policies to reflect a little more to strengthen security. And the security agent for the data by using a log of all actions by the record was so easy to analyze. It also analyzes and apply the different scenarios possible. And the analysis of how to implement and how to block.

The future without the use of security agents to be able to control access to data and H/W information will be updated for the study will be done.

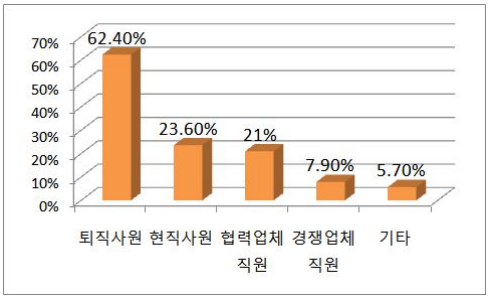
Key Words : Security, Authentication, Data-Protection

Ⅰ. 서론

인터넷과 IT 기술의 발달로 인하여 정보의 가치가 매우 높아지고 있다. 그에 따라 각 기업이 가지고 있는 정보나 기술 유출에 대한 사고가 매우 빈번하게 발생하고 있다. 유출된 정보를 통해 개인의 명의 도용 문제나 기업의 기밀문서나 핵심기술이 경쟁 업체로 넘어가면서 개인과 기업, 국가에 큰 손실을 발생하고 있다.

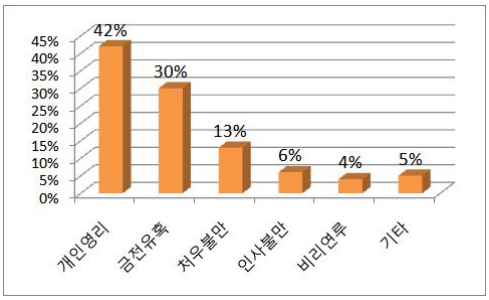
이러한 사고의 대부분은 <그림1>의 산업 기밀 유출 관련자 현황에서 보는 바와 같이 해당 기업체에 근무했던 퇴직사원이나 현직사원에 의해서 일어나는 것을 알 수 있다[1].

* 이 논문은 2006년 정부(교육인적자원부)의 재원으로 한국 학술진흥 재단의 지원을 받아 수행된 연구(KRF-2006-005-J03801)임.
** 숭실대학교 전자계산원 디지털디자인학과 교수
*** 숭실대학교 정보과학대학원 정보보호학과
**** 숭실대학교 정보미디어기술연구소 연구원(교신저자)
***** 숭실대학교 미디어학부 교수



<그림1> 산업기밀 유출 관련자 현황(복수응답)

또한 정보나 기밀을 유출하는 원인을 살펴보면 다음 <그림 2>와 같이 개인적인 영리나 금전적인 문제로 기밀을 유출하는 것을 알 수 있다[2].



<그림2> 동기별 기밀 유출 현황

현재 기업의 핵심 정보 유출에 대한 심각성을 인식한 기관이나 대기업은 정보 유출의 방지를 위하여 많은 예산을 들여서 관리체계를 만들기 위해 노력하고 있다. 정보유출 방지를 위해서 암호화나 DRM과 같은 보안 기술을 개발하고, 제도화 된 정책을 만들려고 노력하고 있다.

그러나 이러한 기술이나 정책을 운영할 전문적인 지식을 보유한 보안 담당자가 매우 부족한 현실이다. 그러므로 정보 보호를 위해서 정보에 대한 접근 자체를 통제할 수 있는 새로운 기법이 필요하다.

본 논문에서는 H/W 정보를 이용한 강력한 인증정보를 통하여 정보에 대한 접근을 통제를 함으로써 정보의 공개를 방지하는 방법을 제안하고자 한다.

II. 관련연구

2.1 정보유출 방법 및 방지 기술

기업의 정보는 다양한 형태의 서버에 저장되거나, 종이문서나 백업미디어에 저장하여 보관된다. 저장된 데이터는 사용자의 요청에 의해 접근, 열람이나 수정, 출력이 가능하며 필요시에는 개인 PC에 저장하여 활용하게 된다. 그러나 이렇게 PC에 저장된 자료는 인터넷을 통해 외부로 전송될 수 있고, USB와 같은 이동 저장매체나 노트북 등에 저장되어 외부로 반출될 수 있다.

정보의 유출은 메일이나 웹하드 등의 네트워크를 이용하는 온라인을 통한 유출 방법과 USB, CD/DVD, 출력물 등을 이용하는 오프라인을 통한 방법이 있다.

2.2 온라인을 통한 정보 유출 및 방지 기술

인터넷과 초고속 정보통신의 발전으로 메일 전송, VPN, P2P, FTP, 웹하드, 메신저 서비스, 블루투스나 적외선 통신 등 다양한 방법을 통하여 장소에 구애받지 않고 외부에서도 쉽게 사내 정보에 접근할 수 있고 외부로 유출할 수 있다.

그러므로 이러한 정보의 유출을 막을 수 있는 기술로는 불법적인 접근을 차단할 수 있는 침입차단시스템(Firewall)이나 공격을 탐지하고 차단할 수 있는 침입방지 시스템(Intrusion Prevention System)이 있으며[3], 모든 어플리케이션 및 정보를 서버에 두어 100% 서버에서 실행되고, 클라이언트는 단지 서버의 실행 결과만을 보여 주는 서버 기반 컴퓨팅을 이용하여 인증 과정을 거친 인가자만 정보에 접속할 수 있도록 함으로써 내부 직원에 의한 보안사고 및 정보 유출을 차단할 수 있다[4].

또한 정보에 접근하는 사용자 인증이나 디지털 콘텐츠의 안전한 분배와 불법 복제 방지를 위한 DRM기술을 이용하여 정보의 온라인 유출을 방지할 수 있다[5].

2.3 오프라인을 통한 정보유출 및 방지기술

하드웨어와 소프트웨어의 발전으로, 그에 따른 다양한 데이터의 수집과 보관으로 인하여 점차 데이터의 용량이 커지고 있다. 데이터의 용량이 커지면서 그에 맞게 저장매체 또한 발전하여 데이터를 저장할 수 있는 용량은 대형화되고, 휴대하기 편하도록 크기는 소형화되고 있다. 노트북의 무단 반출, 출력물의 외부 무단반출에 의한 방법이 있으며, CD/DVD를 이용한 저장매체를 통한 반출, USB 메모리스틱을 이용한 반출, Parallel, Serial 포트에 의한 전송 및 저장에 의한 반출, 데이터의 저장이 가능한 휴대폰이나 MP3 Player, 디지털 카메라, 디지털 캠코더 등 복합적인 기기들을 이용하여 파일을 저장하여 반출할 수 있다. 그러므로 이러한 오프라인을 통한 정보의 유출을 막기 위해서는 다음과 같은 기법이 필요하다.

저장장치나 매체를 제어하기 위해서는 CD/DVD를 이용할 수 있는 장치를 읽기만 가능하도록 제어하고, USB 메모리를 이용할 수 없도록 PC의 USB 포트의 사용을 제한하여 정보의 유출을 방지할 수 있다[6].

또한 데이터에 대해서는 암호화를 통해서 정보를 보호하고 업무 상 발생하는 출력물에 대해 사용자와 출력문서, 사용출처를 로그 및 이미지로 저장하고, 출력물에 워터 마크를 삽입함으로써 중요 문서가 외부에 유출될 경우 최단 시간 이내에 출력물 유출과 관련해 사용 출처 및 책임 추적을 하여 정보를 보호할 수 있다[7].

그리고 출입자에 대해서는 CCTV를 설치함으로써 자산을 유출하려는 자를 심리적으로 압박할 수 있으며, 유출이 발생하였을 경우 녹화된 자료를 확인하여 추적할 수 있으며 인가된 사용자만이 출입이 가능하도록 통제하여 외부로의 정보유출을 통제할 수 있으며, 출입 시 개인마다 사용하는 식별자를 이용하면 출입시간을 확인하여 정보유출 시에는 추적할 수 있다. 대부분의 기업들이 쉽게 할 수 있는 방법으로 비밀번호를 이용하며, IC Card를 이용하는 방법, 생체 정보를 이용하는 방법 등이 있다.

2.4 온, 오프라인을 통한 정보유출 방지기술의 문제점

온라인을 통한 정보의 유출은 방화벽을 통하여 불법 패킷을 차단하고, 침입탐지 시스템이나 침입방지 시스템을 통하여 네트워크의 패킷을 모니터링하고, 인가된 사용자만이 접속하여 정보에 접근하며, 제 3자가 도청을 할 수 없도록 회선을 암호화 하는 VPN을 이용하며, 외부의 불법적인 침입에 대응하기 위한 방화벽, 사용자의 권한을 설정하여 DB에 대한 접근을 통제 할 수 있다.

오프라인을 통한 정보의 유출은 인가된 저장장치 및 저장매체만 사용하도록 통제하며, 데이터의 암호화가 있으며, 무단반출을 방지하기 위한 출입통제 및 CCTV를 통하여 방지할 수 있다.

이처럼 내부 정보를 보호하기 위한 다양한 방지 기술이 있지만 한 가지의 방법을 이용하여 내부 정보를 보호한다면, 다시 말해서 제 3자의 도청을 막기 위해서 암호화를 한다고 해도 내부 사용자는 그 비밀에 접근이 가능하므로 유출이 될 수 있고, CCTV만을 설치했다고 해서 내부자가 정보를 가지고 나가는 것을 확인할 수 없으므로 한 가지 방법으로는 부족하다. 또한 여러 가지 방법을 혼합하여 보호한다고 하더라도 이를 관리하기 위해서는 많은 인원이 필요하며, 대부분의 기업들이 보안에 대한 전문적인 지식을 보유하고 있는 직원의 부재가 문제이다.

내부 사용자의 정보를 이용한 기존의 내부 정보에 대한 접근 방법에 따른 방지 기술은 내부 사용자의 정보를 도난·분실·권한 위임에 의하여 노출 되어, 그 정보를 이용하는 정보유출 시도자의 불법적인 차단에 대해서는 차단이 어려우며, 한 번의 사용자 인증을 통하여 여러 시스템에 접근이 가능하기 때문에 더욱 문제가 크다.

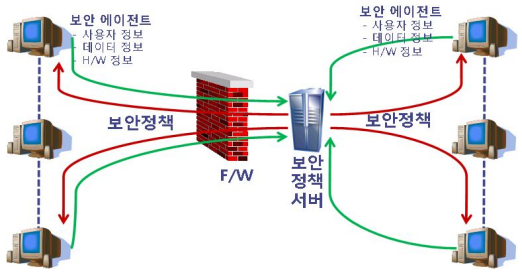
Ⅲ. H/W 정보의 인증을 통한 내부 정보유출 방지 기법

3.1 H/W 정보의 인증을 통한 내부 정보유출 방지 개요

내부의 사용자가 정보의 접근을 위해서는 기본적으로 개인PC 또는 PDA와 같은 단말 장치를 이용하게 되는데, 정보에 접근하려는 H/W의 정보를 얻기 위하여 단말기에 보안 에이전트를 설치한다.

보안 에이전트는 보안정책서버에서 정보를 확인하여 그에 적합한 정책을 전송하며, 보안 에이전트는 전송받은 보안정책에 따라 정보의 접근을 제어한다. 이와 같은 처리 과정과 처리 과정에서 주고받는 정보들을 서버에 기록함으로서 정보의 접근에 대한 행위를 분석하고 감사한다.

H/W 정보의 인증을 통한 내부 정보유출 방지를 위한 구성은 <그림3>과 같다.

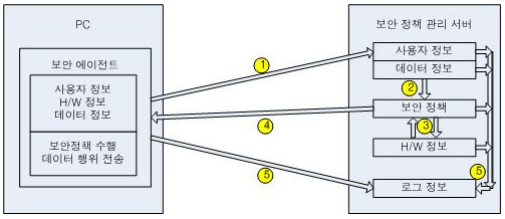


<그림3> H/W인증을 통한 정보유출 방지 구성도

정보에 접근을 시도하려하는 시점부터 정보에 대한 통제를 함으로써 기존의 방법에 비하여 좀 더 적극적으로 탐지 차단할 수 있다.

3.2 H/W 정보의 인증을 통한 접근제어 기법

H/W 정보의 인증을 통한 접근제어는 <그림4>와 같은 과정을 거친다.



<그림4> H/W인증을 통한 접근제어 흐름도

① 에이전트는 사용자 정보, H/W 정보, 데이터 정보를 서버로 전송한다.

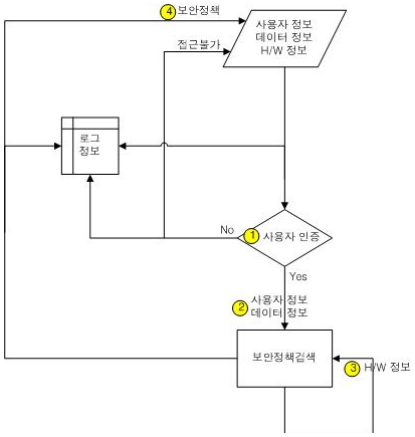
② 서버는 보안정책 리스트에서 사용자 정보, 데이터 정보에 맞는 보안 정책을 검색한다.

③ 서버는 검색된 보안정책 중 에이전트로부터 전송받은 H/W 정보에 가장 적합한 보안정책 데이터베이스에서 선택한다.

④ 결정된 보안정책은 에이전트로 전송되고, 에이전트는 보안정책에 따라 데이터의 접근을 통제한다.

⑤ 보안정책을 적용하기까지의 모든 과정과 보안정책 적용 후의 데이터에 대한 모든 행위를 서버로 전송한다.

보안 정책 관리 서버 내에서의 정책결정 프로세스는 <그림5>와 같다.



<그림5> 보안정책 결정 프로세스

① 사용자 정보를 확인한다.
② 인가된 사용자인 경우, 사용자 정보와 데이터 정보에 적합한 보안정책을 검색한다.
③ 검색된 여러 보안정책 중, H/W 정보에 적합한 보안정책을 검색한다.
④ 사용자 정보, 데이터 정보, H/W 정보에 맞는 최종 보안정책을 결정한다.

<표 1> 사용자 정보

USER_ID	사용자ID
USER_NAME	사용자명
PASSWORD	비밀번호
EMP_NO	사원번호
GROUP_ID	그룹ID
INS_USER	입력자
INS_DATE	입력일자
UPD_USER	수정자
UPD_DATE	수정일자

PC에는 보안에이전트가 설치되어 있으며, 보안 정책 관리 서버와의 통신을 위하여 네트워크에 연결되어 있어야 하며, 그렇지 않을 경우 데이터에 접근 할 수 없다.

사용자가 PC를 이용하여 데이터에 접근을 시도하면, 에이전트는 사용자 정보, H/W 정보, 데이터 정보를 서버로 전송한다. 보안 정책 관리 서버는 보안 에이전트로부터 전송받은 데이터를 분석한다. 첫 번째로 사용자의 정보를 확인하여 내부 사용자인지 확인한다. 내부 사용자가 아닐 경우 데이터에는 접근 불가능하다. 내부 사용자가 확인이 되면 두 번째로 데이터 정보를 확인한다. 사용자와 데이터의 정보를 가지고 해당하는 보안 정책을 검색한다. 세 번째로 검색된 보안정책과 H/W의 정보를 비교하여 해당하는 최종 보안정책을 결정하여 보안 에이전트에 전송한다.

보안 에이전트는 서버로부터 전송받은 보안정책에 따라 데이터의 접근을 제어한다. 데이터의 접근부터 시작하여 인증 과정 및 데이터에 대한 모든 행위를 기록으로 남겨 보안 사고에 대한 감사 자료로 사용한다.

보안 정책 관리 서버에는 사용자 정보, 인가된 H/W 정보, 데이터의 보안 정책을 보관하고 있다. 사용자 정보는 <표 1>과 같이 구성할 수 있다.

사용자 정보에는 일반적으로 널리 사용하는 인증방법인 ID와 Password를 이용하고, 기업에 맞는 사용자 고유의 식별자와 그룹별로 공유할 수 있는 부분이 있을 수 있으므로 그에 맞는 그룹의 정보를 가지고 있어야 한다. 그 외에 사용자를 등록한 정보와 사용자 정보를 수정한 정보를 기록으로 남긴 다면, 사용자 정보에 대한 기록도 남김으로써 권한 부여한 관리자나 정보를 수정한 관리자 또한 추적할 수 있다.

H/W의 정보는 <표 2>와 같이 사용자 정보에 등록되어 있는 사용자가 사용할 H/W의 정보로 구성된다.

기업에서는 대게 일괄적으로 구매를 하게 되므로 정보가 비슷하나, 각각의 H/W의 정보가 모두 똑같을 수는 없다. 예를 들어, NIC의 Mac Address처럼 고유의 식별자를 이용하여 구분이 가능하다.

<표 2> H/W 정보

제조회사	D	모델	D
운영체제	Windows XP Home Edition	언어	한국어
운영체제 버전	5.1	운영체제 서비스팩	Service Pack 2
IE 버전	6.0.2900.2180	IE 서비스팩	2
프로세서	3400Mhz	메모리	1016 Mb
IP 주소	2	Mac Address	0C 31
NIC #1 랜카드	Broadcom NetXtreme 57xx Gigabit Controller - 패킷 스케줄러 미니 포트		
NIC #1 IP 주소	2 (00 31)		
CD-ROM	TSSTcorp CDRWDVD TS-H492C		
비디오 카드	Intel(R) 82945G Express Chipset Family		
	Intel(R) 82945G Express Chipset Family		
사운드 카드	SoundMAX Integrated Digital Audio		
모니터	플러그 앤 플레이 모니터 [1280 X 1024 X 60 Hz]		
프린터	hp deskjet 5600 series []		
	HP LaserJet 4V [프린터]		
	HP LaserJet 5000 Series PCL [프린터4]		
	HP LaserJet 5000 Series PCL [프린터5]		
	HP LaserJet 5000 Series PCL [프린터6]		
	FX Document Centre 285 PCL 6 K [IP_2 3]		
바이오스	D 7 Phoenix ROM BIOS PLUS Version 1.10 A07		
바이오스 날짜	03/31/06		

데이터의 정보는 <표 3>과 같이 구성된다. 파일명, 파일형식, 생성자와 일자 등을 포함하고 있으며, 새로 생성된 파일의 경우, 이를 생성한 사용자에게만 모든 권한이 주어지게 된다.

<표 3> 데이터 정보

파일명	Readme.hwp	파일 형식	한글과컴퓨터 한글 문서
크기	248K	만든 이	최낙귀
만든 일자	2006년 7월 17일(월) 오전 7:00	수정 일자	2006년 7월 17일(월) 오전 7:00
접근 일자	2008년 10월 10일(월) 오전 3:26		

위와 같은 기본 정보를 바탕으로 <표 4>와 같이 보안정책을 생성한다.

<표 4> 보안정책

데이터	사용자 정보	H/W 정보	권한
파일명	All User(0)/ AU(1)/ AG(2)	All H/W(0) AH(1) A'H(2)	All Read Save Delete Print None

생성된 파일에 대해서 생성자는 그룹에 따라 권한을 부여할 수 있다. 기본정책은 방화벽과 마찬가지로 모든 데이터에 대하여 모든 사용자의 모든 H/W는 접근 불가이다. 보안정책은 기본정책에 따르며, 데이터와 사용자의 정보, H/W 정보에 따라 기본정책이 자동적으로 부여되거나 관리자에 의하여 수동으로 생성한다.

보안정책의 설정을 간단하게 표시하기 위하여, 사용자의 정보는 인가된 모든 사용자(All User(0)), 인가된 사용자(AG(1)), 인가된 사용자 그룹(AG(2))으로 표시한다. 내부 데이터에 접근하는 것이므로 비인가 된 사용자의 경우는 접근이 불가능하다. H/W의 정보는 모든 H/W(All H/W(0)), 인가된 H/W(AH(1)), 비인가 된 H/W(A'H(2))로 구분한다. 데이터, 사용자, H/W 정보에 따른 권한은 열람, 저장, 삭제, 출력, 모든 행위 허가 또는 불가로 구분한다. 권한은 여러 가지를 선택할 수 있다. 또한, 사용자가 데이터에 접근하려는 그 시점부터 에이전트는 데이터에 대한 모든 행위를 모니터링 하여 서버로 전송하고 서버에 로그를 남긴다.

보안정책관리 서버의 기능 구성은 다음과 같다.
- 사용자의 인증 정보 보관
- 인가된 H/W의 정보 보관
- 데이터의 정보 보관
- 보안정책 보관
- 사용자, H/W, 접근 데이터에 따른 보안정책 결정 및 배포
- 데이터의 대한 모든 행위에 대한 로그 저장

데이터 보안 에이전트는 인가된 사용자가 사용할 H/W에 설치한다. 에이전트는 사용자의 정보, 데이터 정보, H/W 정보를 서버로 보낸다. 서버는 보안 에이전트로부터 전송받은 정보에 맞는 데이터의 보안정책 결정하여 보안 에이전트로 배포한다.

보안 에이전트는 서버로부터 받은 보안정책에 따라 데이터의 접근을 제어하게 되고, 데이터의 접근 시점부터 발생하는 데이터에 대한 모든 행위는 서버로 보내어 로그를 남긴다.

데이터 보안 에이전트의 기능 구성은 다음과 같다.
- 사용자의 정보 수집(ID, Password)
- H/W의 정보 수집(CPU, RAM, IP, Mac Address, etc)
- 사용자 정보, H/W 정보, 데이터 정보를 서버로 전송
- 보안 정책에 따른 데이터의 접근 제어
- 데이터에 대한 모든 행동을 서버에 전송

Ⅳ. 정보 유출 방지 기술의 평가

4.1 정보접근에 대한 가상 시나리오

4.1.1 가상 시나리오 1

직원 A는 부모님과 따로 거주하는데 주말을 이용하여 부모님 댁에 들러서 부모님의 회갑이 화요일이므로 휴가

를 얻기 위해서 부모님 집에 있는 PC를 이용하여 원격으로 회사에 접근하여 내부규정을 확인하고 휴가계를 작성하려고 한다. 가상 시나리오는 <표 5>와 같다.

<표 5> 가상 시나리오 1

	전개과정	내용
데이터보안 에이전트	데이터 보안 에이전트	PC의 정보 수집 및 서버로 전송 - 사용자정보: 직원 A - 데이터정보: 내부규정.doc - H/W정보: 부모님 PC
보안 정책 관리 서버	사용자 인증	직원 A 인증
	보안정책 검색 (사용자정보, 데이터정보)	- 내부규정.doc / 1 / 1 / All - 내부규정.doc / 0 / 1 / Real/Print - 내부규정.doc / 0 / 2 / Read
	보안정책 검색 (H/W 정보)	- 내부규정.doc / 0 / 2 / Read
데이터보안 에이전트	데이터 보안 에이전트	'내부규정.doc' 파일에 대한 보안정책 적용 (열람 가능/출력 불가능)

직원A의 사용자 정보, "내부규정.doc"의 데이터 정보, 부모님 PC의 H/W 정보를 보안정책 관리서버로 전송한다. 사용자 정보를 통해 정상적인 사용자인지 확인 후 데이터 정보와 함께 보안정책을 검색한다. 검색된 3건의 보안정책 중, H/W 정보를 적용하여 가장 적합한 보안정책을 검색하여 보안 에이전트로 전송한다.

직원 A는 인가된 사용자(0)이기는 하나 비인가 된 PC(2)를 이용하기 때문에 '내부규정.doc' 문서는 열람은 가능하나 출력은 불가능하다.

4.1.2 가상 시나리오 2

내부규정을 확인한 직원 A는 5일인 것으로 확인하고 월요일부터 금요일까지 휴가를 내기 위하여 '휴가계.doc' 파일에 접근하려 한다. 가상 시나리오는 <표 6>과 같다.

직원A의 사용자 정보, "휴가계.doc"의 데이터 정보, 부모님 PC의 H/W 정보를 보안정책 관리서버로 전송한다. 사용자 정보를 통해 정상적인 사용자인지 확인 후 데이터 정보와 함께 보안정책을 검색한다. 검색된 1건의 보안정책이 H/W 정보와 상관없으므로, 검색된 보안정책을 보안 에이전트로 전송한다.

<표 6> 가상 시나리오 2

	전개과정	내용
데이터보안 에이전트	데이터 보안 에이전트	PC의 정보 수집 및 서버로 전송 - 사용자정보:직원 A - 데이터정보:휴가계.doc - H/W 정보:부모님 PC
보안 정책 관리 서버	사용자 인증	직원 A 인증
	보안정책 검색 (사용자정보, 데이터정보)	- 내부규정.doc / 0 / 0 / All
	보안정책 검색 (H/W 정보)	검색 불필요
데이터보안 에이전트	데이터 보안 에이전트	'휴가계.doc' 파일에 대한 보안정책 적용 (모든 권한 부여)

'휴가계.doc'파일은 인가된 모든 사용자(0)에게 H/W에 상관없이(0) 모든 권한을 가지고 있으므로 휴가계를 작성하여 출력한다.

4.1.3 가상 시나리오 3

직원 A는 휴가계를 제출하기 위하여 오전에 잠시 출근하여 팀장에게 휴가계와 내부규정을 보여드리고 5일의 휴가를 가게 되었다. 그러나 갑자기 휴가를 가게 되어 금요일까지 작성해 놓아야 할 부서매출실적을 마치지 못했다. 팀장은 직원 A에게 전화하여 금요일 회의에 제출해야하므로 꼭 마무리를 지어놓으라고 한다. 낮에는 부모님 관광을 시켜드리면서 짬짬이 시간을 내어 일을 한다. 가상 시나리오는 <표 7>과 같다.

직원A의 사용자 정보, "부서매출실적.doc"의 데이터 정보, 직원A의 노트북의 H/W 정보를 보안정책 관리서버로 전송한다. 사용자 정보를 통해 정상적인 사용자인지 확인 후 데이터 정보와 함께 보안정책을 검색한다. 검색된 2건의 보안정책 중, H/W 정보에 해당하는 1건의

<표 7> 가상 시나리오 3

	전개과정	내용
데이터보안 에이전트	데이터보안 에이전트	PC의 정보 수집 및 서버로 전송 - 사용자정보: 직원 A - 데이터정보: 부서매출실적.doc - H/W정보: 00:18:8B:11:16:E9
보안 정책 관리 서버	사용자 인증	직원 A 인증
	보안정책검색 (사용자 정보, 데이터 정보)	- 부서매출실적.doc / 2 / 1 / All - 부서매출실적.doc / 2 / 2 / Read
	보안정책검색 (H/W 정보)	- 부서매출실적.doc / 2 / 1 / All
데이터보안 에이전트	데이터보안 에이전트	'부서매출실적.doc' 파일에 대한 보안정책 적용 (모든 권한 부여)

보안정책이 검색되고, 보안 에이전트로 전송한다.

'부서매출실적.doc' 파일은 인가된 사용자 그룹(2)과 인가된 H/W(1)에 모든 권한을 부여하므로 파일을 수정하였다.

4.1.4 가상 시나리오 4

직원 A는 숙소로 돌아와 부모님께 사정을 말씀드리고 회사로 돌아와 일을 마무리 하였다. 일을 급하게 하여 잘못된 데이터로 인해 징계를 받게 된 직원 A는 휴가를 망치면서까지 열심히 일한 자신에게 돌아온 결과에 앙심을 품고, 회사의 기밀을 빼내 경쟁업체에 넘겨 이익을 챙기기로 결심한다. 가상 시나리오는 <표 8>과 같다.

직원A의 사용자 정보, "기밀문서.doc"의 데이터 정보, 회사에서 사용하는 PC의 H/W 정보를 보안정책 관리서버로 전송한다. 사용자 정보를 통해 정상적인 사용자인지 확인 후 데이터 정보와 함께 보안정책을 검색한다. 1건의 보안정책이 검색되며, H/W 정보를 확인하고, 보안 에이전트로 전송한다.

'기밀문서.doc'파일은 인가된 사용자(1)와 인가된 H/W(1)에 모든 권한을 부여하게 된다.

<표 8> 가상 시나리오 4

	전개과정	내용
데이터보안 에이전트	데이터보안 에이전트	PC의 정보 수집 및 서버로 전송 - 사용자정보: 직원 A - 데이터정보: 기밀문서.doc - H/W정보: 02:E3:FF:05:46:19
보안정책 관리 서버	사용자 인증	직원 A 인증
	보안정책검색 (사용자 정보, 데이터 정보)	- 기밀문서.doc / 1 / 1 / All
	보안정책검색 (H/W 정보)	- 기밀문서.doc / 1 / 1 / All
데이터보안 에이전트	데이터보안 에이전트	'기밀문서.doc' 파일에 대한 보안정책 적용 (모든 권한 부여)
	데이터보안 에이전트	'기밀문서.doc'를 'secret.doc'로 저장 '기밀문서.doc'에 대한 행위 서버로 전송
보안정책 관리 서버	보안정책 복사	- secret.doc / 1 / 1 / All

직원 A가 '기밀문서.doc'를 'secret.doc'라는 이름으로 저장하였으나 '가상 시나리오 6'에서와 같이 보안 에이전트는 보안 정책 관리 서버에 모든 행위를 전달하고, '기밀문서.doc'의 보안정책을 그대로 반영하여, <표 9>와 같이 'screct.doc' 파일에 대한 새로운 보안정책을 추가한다.

<표 9> 변경된 보안정책

데이터	사용자 정보	H/W 정보	권한
All	0	0	None
휴가계.doc	0	0	All
내부규정.doc	1	1	All
내부규정.doc	0	1	Read/Print
내부규정.doc	0	2	Read
부서매출설적.doc	2	1	All
부서매출설적.doc	2	2	Read
기밀문서.doc	1	1	All
secret.doc	1	1	All

<표 11> 정보유출 방지시스템과 비교

항 목	기존의 시스템	제안하는 시스템
인증방법	ID/Pass 이용 인증서 이용	ID/Pass 이용 H/W정보 이용
접근범위	한 번의 인증을 통하여 여러 시스템 접근 가능	접근하려는 데이터에만 가능
보안정책	한 번의 인증을 통하여 접근 가능한 시스템에 따라 보안정책 결정	인증 정보와 데이터에 따라 보안정책 결정
감사기능	각각의 시스템의 로그 확인	종합적인 보안 로그 확인 가능
보안 에이전트	상황에 따라 필요	필요
인증정보 민감도	인증방법의 변경 쉬움	H/W정보 변경 시 재인가 필요

4.1.5 가상 시나리오 5

직원A는 'secret.doc'라는 이름으로 저장한 파일을 CD에 담아 직원 A의 인증정보와 보안 에이전트를 함께 경쟁업체인 △△에 건네주었다. △△회사의 C 부장은 ○○회사의 직원 A로부터 받은 'secret.doc'에 접근하여 데이터를 확인하려 한다. 가상 시나리오는 <표 10>과 같다.

<표 10> 가상 시나리오 5

	전개과정	내용
데이터보안 에이전트	데이터보안 에이전트	PC의 정보 수집 및 서버로 전송 - 사용자정보: 직원 A - 데이터정보: secret.doc - H/W정보: C부장 PC
보안정책 관리 서버	사용자인증	직원 A 인증
	보안정책검색 (사용자 정보, 데이터 정보)	- secret.doc / 1 / 1 / All
	보안정책검색 (H/W 정보)	- 해당 보안정책 없음
	로그 기록	- 보안담당자에게 경고
데이터보안 에이전트	데이터보안 에이전트	- 모든 권한 없음

직원A의 사용자 정보, "secret.doc"의 데이터 정보, △△회사의 C 부장PC의 H/W 정보를 보안정책 관리서버로 전송한다. 사용자 정보를 통해 정상적인 사용자인지 확인 후 데이터 정보와 함께 보안정책을 검색한다. 1건의 보안정책이 검색되며, H/W 정보를 확인지만 해당 보안정책이 검색되지 않는다. 보안정책 관리서버는 보안 담당자에게 경고 메시지를 통하여 알린다.

보안 담당자는 'secret.doc'파일에 대한 로그를 역추적하고, 직원A를 진술을 통하여 모든 상황을 파악한다. 경찰의 협조에 의하여 유출된 정보를 회수하여 내부정보의 유출을 방지할 수 있다.

4.2 정보 유출 방지 기술의 비교분석

기존의 정보유출 방지 시스템과 제안하는 H/W 정보를 이용한 보안을 비교하면 <표 11>과 같다.

인증방법의 경우 기존의 시스템의 주로 ID/Password를 이용하거나 인증서를 이용하여 도난·분실·권한 위임 및 위·변조 등에 쉽게 노출될 수 있고, 그 결과 정당한 사용자의 정보만 있다면 쉽게 시스템에 접근 가능하였다. 그러나 H/W의 다양한 정보를 이용하여 인증할 경우에는 H/W를 분실하지 않는 이상 가장 기본적인 인증을 통과하지 못하게 되므로 시스템에 접근 할 수 없다.

접근 범위의 경우 기존의 시스템은 한 번의 인증을 통하여 여러 시스템에 접근하여 다양한 데이터를 획득할 수 있지만, 제안방법은 접근하려는 데이터에만 접근하도록 하여 다른 데이터에는 접근할 수 없도록 함으로써 접근범위를 최소화하여 보안을 강화하였다. 그러나 제안하는 시스템의 경우 데이터가 많은 경우 보안정책 관리의 어려움이 발생할 수 있다.

보안 정책의 경우 기존의 시스템은 한 번의 인증을 통하여 다양한 시스템에 접근이 가능하지만, 제안 방법은 사용자 정보, H/W 정보, 데이터 정보에 따라 각각의 상황에 맞는 보안정책을 할당하게 되므로 보안정책에 등록되어 있지 않은 상황일 경우 데이터에 접근을 불가능하

게 함으로써 보안을 강화하였다.

감사 기능의 경우 기존의 시스템은 다양한 시스템의 조합으로 각각의 보안로그를 확인하여 종합적인 분석을 해야 하지만, 제안방법은 사용자, H/W, 데이터의 접근에 대한 정보를 모두 기록으로 남기도록 되어 있으므로 종합적으로 로그의 확인이 가능하다.

기존의 시스템은 내부에서의 접근은 보안에이전트 없이 ID/Password의 인증만으로도 접근이 가능하지만 외부에서 VPN이나 telnet 등을 이용하려 접근할 때에는 에이전트가 필요하다. 제안하는 방법은 H/W 정보를 수집하는 기능과 서버로부터 받는 보안정책의 적용을 위한 에이전트가 필수이다.

기존의 시스템에서는 사용자의 몇 가지 정보만을 확인하여 password의 변경이 가능하지만, 제안방법에서는 H/W의 추가 또는 교체가 발생하였을 때 보안담당자에게 확인하여 재인가 받아야하는 불편함이 있다.

Ⅴ. 결론

기존의 온라인을 통한 방지기술은 위·변조나 노출되기 쉬운 정상적인 사용자의 정보를 이용하여 접근하려는 정보유출 의도자에게는 소용이 없으며, 오프라인을 통한 방지기술은 휴대성이 쉬운 저장매체를 이용하여 유출된 정보에 대해서는 통제가 불가능하다.

본 연구에서는 기존의 정보유출 방지 기술의 단점을 보완하여 H/W 정보를 이용한 인증방법을 제안하였다. 인증정보로써 사용자 정보와 H/W의 정보를 이용함으로써 도난·분실·권한 위임 및 위·변조에 대한 인증정보의 노출에 대한 보안을 강화하였으며, 접근하려는 데이터에 따라 인증을 확인함으로써 접근 범위를 최소화하여 보안을 강화하였다. 또한 인증정보에 따라 각각의 데이터에 맞는 보안정책을 적용함으로써 각각의 상황에 따른 다양한 보안정책의 구현을 통해 유연하게 대처 할 수 있게 하였다. 데이터에 접근하기 위해서는 사용자 정보와 H/W 정보를 이용하여 인증을 하게 되며, 인증정보 뿐만 아니라 데이터에 대한 모든 행위를 기록함으로써 쉽게 확인할 수 있도록 하였다. 또한 정보 유출 시나리오를 통하여 제안하는 기법이 잘 동작함을 보였다.

본 연구에서 H/W 정보의 수집과 보안정책을 적용하기 위해 설치해야했던 보안에이전트와 H/W 정보의 변경에 따른 서버의 H/W 정보의 갱신에 대한 문제점이 있었다. 향후 에이전트 없이 접근을 통제할 수 있는 방법과 H/W 정보 변경 시에 서버의 H/W 정보도 간단하게 갱신할 수 있는 방법이 연구 되어야한다.

참고문헌

[1] 중소기업청, 중소기업 산업기밀관리 실태보고 조사, 2008.07.

[2] 산업기밀보호센터, 첨단기술보호동향8호, 2007.

[3] Douligeris, Christos/Serpanos, Dimitrios Nikolaou, “Network Security”, 2007.

[4] 류한선, Server Based Computing, 소프트뱅크미디어랩.

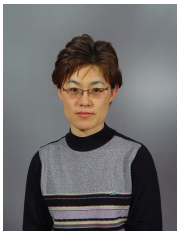
[5] 최형규, 정보시스템 보호 및 해킹방지를 위한 보안시스템 구축에 관한 연구, 숭실대, 2002.12.

[6] 박희섭, 안전한 개인 휴대형 저장장치 보안관리 설계 및 구현, 공주대, 2008.02.

[7] 박태훈, 기업의 정보유출 방지를 위한 동향부석 및 문서보안 시스템 적용방안에 대한 연구, 동국대, 2006.02.

논문접수일 : 2009년 1월 22일
수 정 일 : 2009년 2월 10일(1차)
2009년 2월 25일(2차)
게재확정일 : 2000년 3월 1일

■ 저자소개 ■



양 선 옥
Yang, Sun Ok

1997년 ~현재 숭실대학교 전자계산원 교수
2000년 2월 숭실대학교컴퓨터과학과(공학박사)
1993년 2월 숭실대학교 컴퓨터학과(공학석사)
1991년 2월 숭실대학교 컴퓨터학부(공학사)

관심분야 : HCI, 컴퓨터비전, 멀티미디어에이전트
E-mail : soyang@ssuci.ac.kr

권 순 홍
Kwon, Soon hong

2006년 8월~현재 숭실대학교 정보과학대학원 정보보안학과 석사과정
2006년 2월 한국디지털대학교 디지털정보학과(공학사) 디지털경영학과(경영학사)

관심분야 : 정보보안
E-mail : pjerry@dreamwiz.com

박 재 표
Park, Jae Pyo

2008년 3월~현재 숭실대학교 정보미디어기술연구소 연구원
2004년 8월 숭실대학교컴퓨터과학과(공학박사)
1998년 8월 숭실대학교 컴퓨터학과(공학석사)
1996년 2월 숭실대학교 컴퓨터학부(공학사)

관심분야 : 유비쿼터스, 컴퓨터통신, 보안
E-mai : pjerry@dreamwiz.com

최 형 일
Choi, Hyung Il

1987년 ~현재 숭실대학교 미디어학부 교수
1987년 미시간대학교 전산공학과(공학박사)
1982년 미시간대학교 전산공학과(공학석사)
1979년 연세대학교 전자공학과(공학사)

관심분야 : 컴퓨터비전, 퍼지 및 신경망 이론. 비디오검색, 패턴인식, 인터페이스 에이전트, 지식기반 시스템
E-mail : hic@ssu.ac.kr