情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

문서 읽기 행위를 이용한 연속적 사용자 인증 기반의 내부자 문서유출 탐지기술 연구*

조 성 영,[1†] 김 민 수,[1] 원 종 일,[1] 권 상 은,[1] 임 채 호,[1] 강 병 훈,[1,3‡] 김 세 헌[1,2]
[1]KAIST 정보보호대학원
[2]KAIST 산업 및 시스템 공학과
[3]조지메이슨대학교 응용IT학과 및 정보보호시스템학과

A system for detecting document leakage by insiders through continuous user authentication by using document reading behavior*

Sungyoung Cho,[1†] Minsu Kim,[1] Jongil Won,[1] SangEun Kwon,[1] Chaeho Lim,[1]
Brent ByungHoon Kang,[1,3‡] Sehun Kim[1,2]
[1]Graduate School of Information Security, KAIST
[2]Department of Industrial and Systems Engineering, KAIST
[3]Department of Applied Information Technology and Center for Secure Information System, George Mason University

요 약

기업 내의 문서 유출을 탐지・제어하기 위한 다양한 기술들이 연구되고 있다. 하지만 이러한 기술들은 대부분 외부에 의한 문서 유출을 대상으로 하고 있으며, 문서에 대한 정당한 권한을 가지고 있는 내부자에 의한 문서 유출을 탐지하고 제어하는 연구는 미비한 수준이다. 본 연구에서는 내부자에 의한 문서 유출을 탐지하고 제어하기 위하여 사용자의 문서 읽기 행위를 관찰한다. Microsoft Word 로거에서 추출할 수 있는 속성으로부터 각 사용자의 관찰된 문서 읽기 행위에 대한 패턴을 만들고 시스템에 적용함으로써 문서를 읽고 있는 사용자가 실제 사용자인지 여부를 판단한다. 이를 통하여 사용자가 문서를 읽는 행위를 바탕으로 효과적으로 문서 유출을 방지할 수 있을 것으로 기대한다.

ABSTRACT

There have been various techniques to detect and control document leakage; however, most techniques concentrate on document leakage by outsiders. There are rare techniques to detect and monitor document leakage by insiders. In this study, we observe user's document reading behavior to detect and control document leakage by insiders. We make each user's document reading patterns from attributes gathered by a logger program running on Microsoft Word, and then we apply the proposed system to help determine whether a current user who is reading a document matches the true user. We expect that our system based on document reading behavior can effectively prevent document leakage.

Keywords: Document Reading, Continuous Authentication Insider Threat Detection

접수일(2012년 10월 22일), 수정일(2013년 1월 28일), 게재확정일(2013년 2월 15일)
* 본 연구는 국방과학연구소와 KAIST 정보보호대학원의 연구지원으로 수행되었습니다.

† 주저자, sungyoung.cho@kaist.ac.kr
‡ 교신저자, bkang5@gmu.edu

I. 서 론

핵심 기술이 포함된 문서에 대한 유출은 여러 방면으로 일어나고 있다. 해킹, 조직의 외부자 또는 거래업체에 의해서도 일어나지만 가장 위협적이고 높은 비율을 차지하는 요소는 내부 직원에 의한 문서 유출이다[1]. 내부 직원에 의한 문서 유출이란 문서에 대해 정당한 권한을 가지고 있는 내부자가 다양한 방법을 통해 문서를 외부로 유출시키는 것이다. 오늘날 대부분의 문서가 컴퓨터로 작성되고 보관됨에 따라 문서의 유출을 막기 위하여 새로운 방법의 문서 보안이 필요한 실정이다.

내부자에 의한 보안 위협은 오래전부터 인지해오고 있다. 그러나 조직의 외부자와 달리, 정당한 권한을 가지고 있는 사용자라는 점에서 내부자에 의한 위협을 탐지 및 통제하기는 쉽지 않다. 정당한 권한을 가지고 있는 사용자는 내부 기밀문서를 열람할 수 있으며 손쉽게 유출할 수 있다. 이러한 내부자에 의한 위협을 방어하기 위해 노트북, 카메라, 핸드폰 등의 이동 저장기기의 반·출입을 금지, 통제하는 물리적인 방법에서부터 복사기, 프린터 등의 사무용 기기 보안, 전자문서보안, 데이터베이스 보안 등의 논리적인 방법에 이르기까지 다양한 관리체계 및 솔루션이 실제 도입되고 있다. 그러나 현재까지 문서에 대한 권한이 있는 자가 악의적인 목적으로 해당 정보를 외부 유출하는 것을 막을 수 있는 솔루션이 드문 것이 현실이다[2].

본 연구는 사용자의 문서를 읽는 행위를 관찰하고 분석함으로써 내부자의 불법 행위 중 문서에 대한 권한이 있는 자가 문서를 유출하는 경우 이를 탐지하고 통제하는 하나의 새로운 방법을 제시한다. 문서를 읽는 사용자는 평소의 문서 읽는 습관에 따라 문서를 읽는 패턴을 보일 것이다. 문서 읽는 패턴에는 문서를 읽는 속도, 특정 부분에 머무르는 시간, 앞의 내용을 찾기 위하여 앞으로 넘기는 횟수 등을 포함한다. 이를 위하여 가장 많이 쓰이는 문서 도구인 Microsoft Word에서 동작하는 로거(logger) 프로그램을 매크로 형식으로 개발하고, 문서를 읽을 때 발생되는 이벤트를 로거 프로그램을 통하여 수집하였다. 수집된 데이터를 바탕으로 사용자의 문서 읽는 행위를 나타낼 수 있는 특징들을 추출하였고, 추출된 특징들을 이용하여 기계학습(machine learning)을 통하여 사용자의 고유한 문서 읽기 패턴을 학습을 하도록 한다. 실제 일상 업무 중 특정 사용자가 문서를 읽을 때 그 행위를 관찰하고 패턴을 생성하여 이 패턴이 기계학습된 사용자의 패턴과 일치하는지 여부를 통하여 연속적 사용자 인증(continuous user authentication)을 수행한다. 사용자 인증에 실패하면 시스템에 경고하고 사용자의 시스템 사용을 차단할 수 있도록 한다. 이러한 시스템을 통하여 내부자의 불법 행위를 탐지하고 제어할 수 있을 것으로 기대한다.

이 논문은 다음과 같이 구성된다. 2장에서 내부자에 의한 문서 유출을 방지하기 위한 기존의 솔루션을 소개하고, 3장에서 생체인식을 이용한 사용자 인증 시스템에 대한 간략한 설명을 한다. 4장에서는 이 연구에서 제안하고자 하는 문서 읽기 행위를 통한 불법행위 탐지 프레임워크를 제안하고, 5장에서 실험 방법 및 결과를 소개한다. 6장에서는 이 연구에 대한 결론 및 향후 연구 방향을 제시한다.

II. 관련 기술

2.1 DLP (Data Loss Prevention)

DLP[3]는 기업 내부자의 고의나 실수로 인한 외부로의 정보 유출을 방지하는 내부정보 유출 방지 솔루션이다. 사내에서 주고받는 데이터를 내용이나 형식 등을 기준으로 탐지해 중요 정보 유출을 차단할 뿐만 아니라 데이터 보호 규제에도 대응할 수 있다. 즉, 암호화와 필터링, 모니터링 등을 통해 외부로 데이터가 유출되는 것을 방지하는 기술이다.

DLP는 일반적으로 데이터를 분류하고 그 흐름을 감시하는 방식으로 데이터를 보호하게 된다. 초기 DLP는 메일 감시 등을 통하여 정보 유출을 차단하는 데 그쳤으나 이후에는 FTP, 보안 웹 메일, 인스턴트 메시지까지 확장되었고 매체 제어 기술(USB 디스크, CD-ROM, 네트워크 드라이브 등의 쓰기 금지)등이 접목되었다. 예를 들어 네트워크를 통해 내보내거나, USB 등의 저장 매체에 옮기는 작업, 프린터로 출력하는 작업 등을 감시하고 분류된 데이터의 경우 그 활동을 제한하게 된다.

DLP의 기능 또는 기술은 크게 네 가지 부분으로 나누어 설명할 수 있다. 첫째, 접근제어가 가능하다. 즉, 정보의 중요도에 따라 그룹화하고 각 정보에 대한 접근권한 관리 시스템 접근제어와 물리적 접근제어로 나눌 수 있다. 둘째, 암호화를 할 수 있다. 이 기능은 접근 제어 기술과 병행하여 사용가능하다. 셋째, 필터링 기능이다. 트래픽 제어(FTP, 메신저 P2P 등 유출가능 서비스 제한), 컨텐츠 제어(외부 송신 정보 검

사 후 발송여부 결정)가 가능하다. 마지막으로 활동을 감시할 수 있다. 유출가능 프로세스를 감시하여 정보 유출을 탐지할 수 있다.

DLP의 장점으로는 애플리케이션에 많은 부담을 주지 않는다는 것이다. DLP는 벤더 및 애플리케이션에 중립적이다. 따라서 보다 다양한 컨텐츠에 대하여 감시/차단할 수 있다. 또한 데이터 흐름을 모니터링하여 유출 및 유출 시도 시 실시간으로 증거 수집이 가능하다. 이것은 다양한 정보 유출 경로를 모두 지원해주며 실시간 차단을 가능하게 해 준다. 그리고 자료의 변경 또는 포맷의 변환에 있어서도 지속적인 시스템을 제공해 준다. 또한 내부 사용자가 데이터 전체의 흐름을 관찰 할 수 있기 때문에 업무에도 도움이 된다. 그러나 유출된 이후 보안을 보장하지 못한다는 단점이 있다. 즉, 유출된 자료의 2차적인 전파는 통제할 수 없다.

2.2 DRM (Digital Rights Management)

DRM[4]은 문서를 암호화하여 사용권한을 제한시켜 정보를 안전하게 유통하는 보안시스템이다. DRM 솔루션을 통해 불법 복제와 변조를 방지할 수 있으며 적법한 사용자만이 합법적인 방식으로 콘텐츠 사용을 가능하게 한다. 또한 디지털 콘텐츠의 무단 사용을 방지함으로써 디지털 콘텐츠 제공자의 지적재산권과 저작권에 관한 권리와 이익을 보호할 수 있다.

DRM은 단순 보안 기술이라기보다는 조금 더 포괄적인 개념으로 보는 것이 적절하다. 즉, 디지털 콘텐츠의 생성, 보관, 유통, 사용, 폐기에 이르는 전체 라이프 사이클에 걸쳐 디지털 콘텐츠 자체의 보호 및 저작권을 보호하는 상위 레벨의 보안 기술이기 때문이다.

DRM은 문서가 유출되더라도 열람을 방지할 수 있으며 유출된 문서의 추적이 가능하다. 또한 개별 문서에 대한 유통기한 및 열람횟수 제한이 가능하기 때문에 효율적으로 문서를 유통, 저장할 수 있다. 그러나 DRM 솔루션의 단점은 암호화 해체 권한을 가진 자가 문서를 유출할 경우, 유출 차단 방법이 없다는 것이다. 그리고 DLP 솔루션과 다르게 애플리케이션에 종속적이기 때문에 새로운 애플리케이션 적용 기간 동안에는 해커들의 공격을 받을 수 있다는 보안의 허점이 있다.

2.3 SBC (Server Based Computing)

최근 컴퓨터 아키텍처가 엔터프라이즈 시장을 중심으로 혁신적인 변화를 거쳐 온 가운데, 기존의 메인프레임, 인터넷과 웹 애플리케이션의 도입 등으로 인한 단점을 보완하는 가운데 제안된 것이 SBC[5]이다. 이는 모든 사용자의 OS, 애플리케이션 및 정보를 100% 서버에 두고 필요할 때마다 서버에 접속해서 사용하는 솔루션이다. 이 솔루션에서 사용자 PC는 단지 실행결과만 보여주는 환경이다. 부연하자면 원격 데스크톱 연결을 통해 시트릭스의 ICA (Independent Computing Architecture), 마이크로소프트의 RDP (Remote Desktop Protocol) 등의 방식으로 서버에 접속을 하여 해당 컴퓨터에 설치된 애플리케이션 및 정보, 도구를 안전하고 간편하게 사용할 수 있게 해주는 방식이다. 이 방식은 모든 처리가 100% 서버에서 이루어지고 팻 클라이언트 (fat client)와 반대된다는 의미에서 씬 클라이언트 (thin client) 컴퓨팅이라고 표현하기도 한다. SBC는 많은 면에서 메인프레임과 비슷하다.

클라이언트/서버 아키텍처에서 서버와 클라이언트가 애플리케이션의 처리를 나누어 분담하고, 인터넷 아키텍처에서는 웹 브라우저가 HTML 렌더링의 역할을 수행하는 데 반하여, SBC에서는 애플리케이션, 데이터, CPU 등의 모든 파워를 SBC 환경의 서버에 의존한다. 씬 클라이언트는 단지 ICA, RDP 등과 같은 특정 프로토콜을 통해 커넥션을 관리하고 키보드, 마우스 입력과 화면 출력만을 처리할 뿐이다. 이러한 SBC 솔루션의 장점은 모든 자료가 로컬에 존재하지 않으므로 유출 원천 차단이 가능하다는 것이다.

그러나 서버에서 모든 애플리케이션을 통제해야 하므로 모든 종류의 풍부한 멀티미디어 사용자 경험을 누릴 수 있는 팻 클라이언트와 달리 동영상, 게임 등과 같은 부분에서 상당한 제한이 존재하는 등 실행 속도가 저하될 수 있다. 또한 설치형 소프트웨어에 기반을 둔 클라이언트/서버 아키텍처, 즉 팻 클라이언트에 비해 모든 요청이 서버에 요청되기 때문에 많은 서버를 구입해야 하는 등 초기 투자비용이 높으며 내부에서 협업이나 자료 전달에 대한 대안이 취약하다.

III. 생체인식 기반의 재인증 시스템

3.1 생채인식 (Biometrics)

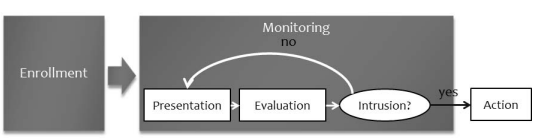
생체인식이란 사람의 신체적, 또는 행위적 정보를 이용하여 시스템 상에서 사용자를 인식하는 방식을 말한다. 바이오 인증, 생체 인증 등과 같은 다양한 용어

로도 사용이 가능하다. 생체인식은 사람의 고유한 정보를 이용한다는 점에서 다른 사용자가 이 정보를 훔치기 어려우며(difficult to stolen), 사용자들이 자신이 가지고 있는 정보를 이용할 수 있기 때문에 잊어먹을 염려가 없으며(difficult to forgotten), 다른 사용자들이 훔치려고 하는 사용자의 정보를 복제 또는 흉내 내기가 어렵기 때문에(difficult to forge) 기존의 비밀번호 기반의 사용자 인증에 비하여 매우 강력한 인증 수단으로 떠오르고 있다.

생체인식은 두 가지 종류로 구분할 수 있다. 그 중 하나인 생리학적 생체인식(physiological biometrics)은 홍채, 지문, 동맥 등과 같은 사람의 신체적인 정보를 이용하여 사용자를 인식하는 방법이다. 사용자의 신체적인 정보를 얻기 위해서는 별도의 하드웨어가 필요하다는 단점이 있지만[6], 일단 하드웨어가 구비되어 적절한 시스템이 구축되면 인식률은 매우 높다[7].

생리학적 생체인식은 정확도가 높다는 점에서 사용자를 인증함에 있어 실제 도입된 사례들이 있지만[8], 실제 기업 등 조직에서 생리학적 생체인증을 사용하기 위하여 도입되어야 하는 하드웨어 비용이 크다는 점에서 실용적 측면에서 한계가 존재한다. 이러한 추가적인 하드웨어 비용이 없이 사용자를 인식할 수 있는 행동기반 생체인식(behavioral biometrics)에 대한 연구가 활발히 진행되고 있다[6][9]. 키보드, 마우스와 같이 일상적으로 사용되는 하드웨어를 사용한다는 점에서 비용적인 측면의 이점이 있다. 행동기반 생체인식은 사용자가 컴퓨터를 사용하면서 키보드나 마우스를 통하여 입력을 할 때 발생되는 행동을 모니터링하고 이를 바탕으로 각 사용자마다의 고유한 행동 패턴을 생성한다. 이렇게 생성된 패턴이 시스템에 저장되어 특정 사용자가 키보드나 마우스를 통하여 일련의 행동을 할 때 이 패턴과 시스템에 저장된 패턴과 비교하여 사용자를 인증하게 된다.

행동기반 생체인식은 생리학적 생체인식에 비해 상대적으로 저렴하지만 아직 인식률은 낮다[10]. 또한 키보드를 통한 생체인식의 경우, 사용자가 입력하는 정보를 바탕으로 행동 패턴을 만들게 되는데 이 과정에서 사용자가 개인정보와 같은 민감한 정보를 입력하는 경우 심각한 개인정보보호 문제가 발생하게 된다. 이에 비하여 마우스를 통한 생체인식의 경우 사용자가 입력하는 정보의 범위는 키보드보다 극히 제한적이어서 개인정보보호와 관련한 문제가 적다.



[그림 1] 연속적 사용자 인증 시스템의 개요. 등록 모드와 인증 모드로 구분할 수 있다.

3.2 연속적 인증 시스템

연속적 인증 시스템이란 사용자가 시스템에 대하여 이미 인증을 한 상태에서 사용자가 시스템에서 일련의 작업 도중에 다시 인증을 받는 것을 말한다. 재인증(Re-authentication)이라고도 한다. 이는 기존의 전통적인 인증 시스템이 가지고 있는 취약점을 보완하기 위한 것이다. 전통적인 인증 시스템이 받을 수 있는 공격에는 로그인 시간에 사용자가 비밀번호 등을 이용하여 인증을 할 때 발생할 수 있는 비밀번호에 대한 사전 공격(dictionary attack), 인증 후 사용자의 세션 도중 로그아웃하지 않고 자리를 비웠을 때 권한이 없는 다른 사용자가 권한이 있는 사용자인 것처럼 가장(masquerading)하여 정보를 훔치는 등의 행위를 하는 세션 하이재킹 공격(session hijacking attack) 등이 있다. 재인증 시스템은 주로 인증된 사용자가 작업 중인 컴퓨터 환경을 보호하기 위하여 제안되었다.

연속적 인증 시스템은 세션 중에 사용자를 인증하기 때문에 사용자가 시스템에서 중요한 작업을 하고 있을 경우 이를 방해하여 능률을 저하시키지 않아야 한다. 따라서 연속적 인증 시스템은 명시적으로 사용자에게 능동적인 반응을 요구하지 않는다는 점에서 소극적(passive)이어야 하고, 가장된 사용자가 연속적 인증 시스템의 존재를 인지하고 이에 대해 의도적인 반응을 보이지 않아야 한다는 점에서 투명(transparent)해야 한다.

연속적 인증 시스템을 위해서는 [그림 1]과 같이 사용자를 인증하기 위한 정보를 등록하는 등록(enrollment) 단계와, 사용자의 정보를 얻기 위하여 모니터링하고 획득한 정보를 평가하여 사용자를 인증하는 인증(authentication) 단계로 나누어 볼 수 있다. 연속적 인증 시스템에서 사용자를 인증하기 위한 정보로써 사용자의 행동을 모니터링하고 데이터를 수집하는 방법이 소극적이면서도 투명하다는 점에서 효과적이다.

행동기반 신체 인식을 이용한 연속적 인증 시스템

에 대한 많은 연구가 이루어지고 있다. 과거 유닉스나 리눅스와 같은 명령어 인터페이스(command line interface)에서 명령어를 입력하는 순서(command sequence)를 이용하여 호스트 기반 침입탐지시스템(host-based intrusion detection system)들[11, 12]이 제안되었다. 이 시스템에서 특정 사용자가 평소에 입력하는 명령어의 순서를 지속적으로 모니터링하고 이를 바탕으로 그 사용자에 대한 프로파일이 생성되며, 사용자의 프로파일과 비교하여 평소의 패턴과 다른 패턴의 행위가 관측되면 그 이러한 행위를 비정상적인 행위(abnormal behavior)로 간주한다. 이러한 시스템은 최근 컴퓨터 시스템에서 많이 사용되는 그래픽 사용자 인터페이스(Graphic User Interface)에는 적합하지 않다는 문제점이 있다.

키보드에서의 키 입력 패턴(keystroke dynamics)을 이용한 연속적 사용자 인증에 대한 연구[13, 14, 15]도 활발히 진행되고 있다. 시스템의 각 사용자들은 키보드를 이용하여 입력하는 과정에 있어 고유한 패턴을 가지고 있고 이를 바탕으로 사용자를 인증할 수 있다는 것이다. 키 입력 패턴은 키를 누르는 시간 또는 키를 누르고 손가락에서 떼는 시간, 또는 연속적으로 두 키를 입력할 때의 시간 간격 등을 이용하여 측정될 수 있다. 이러한 특정 두 키를 입력할 때의 시간 간격을 측정하기 위해서 이러한 특정 두 키가 포함된 단어나 문장이 입력되어야 하고 이러한 단어나 문장이 입력되기 전까지는 측정되기 어려우므로 인증에 오랜 시간이 걸릴 수 있다는 문제점이 있다. 또한 사용자가 키보드를 통하여 입력하는 정보에는 사용자가 민감하게 반응할 수 있는 개인정보가 포함되어 있어 프라이버시 문제가 발생할 수 있다.

키보드에서의 키 입력 패턴을 이용한 사용자 인증보다는 덜 오래되었지만 마우스의 움직임 패턴을 이용한 연속적 사용자 인증에 대한 연구[6, 9, 16]도 진행되고 있다. 시스템의 각 사용자들은 마우스를 이용하여 입력하는 과정에 있어 고유한 패턴을 가지고 있어 이를 바탕으로 사용자를 인증할 수 있다는 것이다. 마우스 커서가 움직이는 거리, 방향, 클릭(single click, double click)이나 휠링(wheeling)을 포함한 이벤트 등으로부터 마우스 움직임 패턴을 측정할 수 있다. 키보드에 비하여 제한된 입력값을 받기 때문에 키보드에서의 키 입력으로부터 발생할 수 있는 프라이버시 문제는 덜 심각한 수준이다. 하지만 마우스 움직임은 화면의 해상도와 같은 환경, 마우스의 종류, 작업 환경 등의 외부적인 요소에 따라 다르게 보일 수 있다는 점에서 한계가 있다.

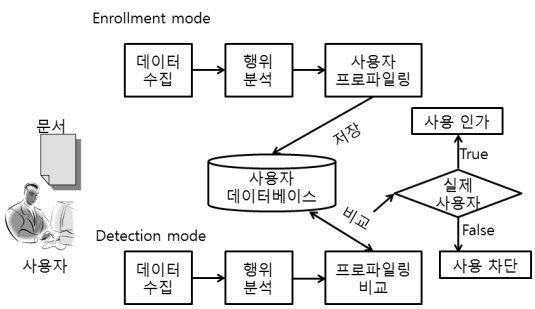
이 연구에서는 사용자가 업무 중, 특히 문서를 읽으면서 발생하는 행위를 모니터링하고 이를 바탕으로 사용자를 재인증하는 프레임워크를 제안한다. 4장에서는 이 프레임워크를 보다 자세히 살펴본다.

IV. 문서 읽기 행위를 통한 불법행위 탐지 프레임워크

4.1 프레임워크 제안

이 연구에서는 [그림 2]로 표현된 내부자의 문서 읽기 행위를 모니터링함으로써 문서유출 등의 불법 행위를 탐지하는 프레임워크를 제시한다. 이 시스템을 회사와 같은 조직에서의 활용 예시를 통하여 설명하면 다음과 같다.

등록 모드(Enrollment mode)에서는 조직 내의 신입 직원이 사내 교육 매뉴얼을 읽도록 한다. 이러한 교육 매뉴얼은 워드 문서(.doc, .docx)나 한글 문서(.hwp), PDF 문서(.pdf)와 같은 전자 문서의 형태로 되어 있으며, 효과적인 동기 부여를 위하여 교육 매뉴얼을 읽고 난 후 적절한 시험을 치르게 하여 교육 인증을 하도록 한다. 사용자가 이러한 전자 문서를 읽는 동안, 워드 프로세서에 내재된, 또는 시스템에 내재된 로거(logger) 프로그램이 사용자가 문서를 읽는 행위를 기록하게 된다. 로거 프로그램의 형태는 워드 프로세서 내에 매크로 형식으로 포함되거나, 별도의 프로그램 형태로 존재하며, 사용자가 문서를 읽는 동안 로거 프로그램의 동작 여부를 의식적으로 인지하지 못한다. 이는 연속적 인증 시스템의 두 가지 특성인 소극적 특성과 투명 특성을 만족한다. 이렇게 로거 프로그램을 통하여 수집된 사용자의 문서 읽기 행위는 적절한 특징으로 변환되어 각 사용자마다의 고유한 읽



[그림 2] 문서 읽기 행위를 통한 불법행위 탐지 프레임워크

기 패턴으로 프로파일링되어 사용자 데이터베이스에 저장한다.

탐지 모드(Detection mode)에서는 사용자가 평소 업무 활동을 통하여 문서를 읽을 때 앞에서 언급한 로거 프로그램이 사용자의 문서 읽는 행위를 모니터링하고 기록한 후, 적절한 특징으로 데이터를 변환하고, 사용자 데이터베이스에 저장된 패턴과 비교한다. 만약 사용자가 평소에 보이는 패턴과 다른 패턴을 보인다면 수상한 행동을 하는 것으로 간주하고 시스템에 경보를 내린 후 해당 사용자의 시스템의 사용을 차단한다. 다음 절에서는 프레임워크에서 사용된 로거 프로그램과 로거 프로그램에서 추출할 수 있는 속성을 바탕으로 추출된 특징에 대하여 언급한다.

4.2 로거 프로그램을 통한 특징 추출

4.2.1 로거 프로그램

이 연구에서 제안한 프레임워크에는 Microsoft Word 워드프로세서를 사용하였다. 이는 전 세계적으로 가장 많이 사용하는 문서 편집 프로그램이며, Microsoft Office의 확장성이 좋기 때문이다. 사용자가 Microsoft Word로 작성된 워드 문서를 읽는 동안의 이벤트들을 수집하기 위하여 로거 프로그램을 개발하고 이를 사용하였다. 로거 프로그램은 매크로 형식으로 제작되어 사용자가 워드 문서를 열 때 자동으로 실행되며, 사용자가 문서를 읽는 동안의 이벤트들을 별도의 파일에 기록한다. Microsoft Word 기반 로거 프로그램에서 기록하는 26개의 속성들 중 일부를 〔표 1〕에 정리하였다.

〔표 1〕은 Microsoft Word 로거 프로그램에서 추출하는 26개의 속성들 중 사용자가 문서를 읽는 행동과 직접적인 연관이 있는 것만을 선택한 것이다. 〔표 1〕로부터 도출할 수 있는 값들은 다음의 다섯 가지로 정리할 수 있다.

Δ time
Δ document vertical scroll percentage
Δ page vertical scroll percentage
Δ zoom percentage
Δ cursor position

'Δ time'은 〔표 1〕에서 제시된 속성들 중 하나인 timestamp의 차이로써 계산되며, 어떠한 속성 값이 변화하였을 때의 지속 시간을 나타낸다. 특히 나머지 네 값들과 함께 작용하여 시간에 따른 변화율을 계산하는데 유용하다.

〔표 1〕 Microsoft Word 로거 프로그램에서 수집하는 주요 정보

속성	설명
timestamp	로그가 기록된 시간(초)
totalNumberOfPages	문서의 전체 페이지 수
currentVisiblePageNumbr	현재 보고 있는 페이지 번호
docZoomPercentage	문서 확대 축소 비율
docVerticalPercentScrolled	문서 세로 스크롤 비율
pageVerticalPercentScrolled	현재 페이지에서 위치하는 스크롤 위치
selectedText	선택된 글자
elapsedTime	머문 시간

'Δ document vertical scroll percentage'와 'Δ page vertical scroll percentage'는 각각 표 1에서 제시된 속성들 중 문서를 읽고 있는 위치에 관한 값을 나타내는 docVerticalPercentScrolled와 pageVerticalPercentScrolled의 차이로써 계산된다. 이는 문서의 종적(vertical) 스크롤 위치의 변화 정도를 나타내며, 현재 읽고 있는 페이지에 대한 스크롤 변화 정도와 문서 전체에 대한 스크롤 변화 정도는 연관되어 있다.

'Δ zoom percentage'는 〔표 1〕에서 제시된 속성들 중 하나인 docZoomPercentage의 차이로써 계산되며, 문서를 확대 및 축소하는 비율의 변화를 나타낸다. 사용자마다 편한 배율로 문서를 보기 때문에 개인별로 다를 수 있다. 하지만 사용자가 문서를 읽고 있는 위치를 변화하는 것에 비하여 자주 확대 및 축소해서 보는 것은 아니기 때문에 상대적으로 중요한 요소는 아니라고 판단하였다. 하지만 고연령층의 경우 근시가 심하여 문서를 확대하여 보는 경향이 있는 등 다양한 연령대를 고려한다면 충분히 고려될 수 있다.

'Δ cursor position'은 〔표 1〕에서 제시된 속성들 중 하나인 selectedText의 변화 여부로써 계산된다. 즉, 선택된 글자가 변경되었다는 것은 커서 위치에 변화가 발생했다는 것을 나타내며, 이러한 커서 위치의 변화는 키보드 또는 마우스를 통하여 커서를 움직이면서 읽을 때 나타나므로 'Δ cursor position'은 사용자의 문서 읽기 습관을 잘 표현해 주는 값이라고 볼

〔표 2〕 사용자의 문서 읽는 행위를 나타날 수 있는 특징들

특징	비고
Mean Forward Velocity(FV)	페이지당 읽는 속도의 평균 $FV=\frac{\sum_i V_i}{n},\ V_i=\frac{\Delta Page\ Vertical\ Scroll\ Percentage}{\Delta Elapsed Time},\ i=1,...,n$
Backward Frequency(BF)	페이지당 문서를 뒤로 이동시킨 누적 횟수
Click Ratio (CR)	페이지당 SelectedText가 변경된 빈도(frequency) $CR=\frac{Count(\Delta Selected Text)}{Elapsed\ Time}$

수 있다. 만약 어떤 사용자가 키보드의 방향키(→, ←, ↑, ↓)를 이용하여 문서를 읽는다면 커서가 움직이는 속도가 빠를 것이며, 마우스를 이용하여 문서를 읽는다면 휠(wheel)을 이용하여 문서를 넘길 것이며 중요한 포인트를 짚을 때만 마우스를 클릭하여 커서를 이동할 것이므로 키보드를 통한 커서의 움직임에 비해 둔할 것이다.

4.2.2 문서 읽는 행위에 관한 특징 추출

4.2.1에서 다룬 다섯 가지 값들을 이용하여 〔표 2〕에 정리되어 있는 세 가지의 특징들로 사용자의 문서 읽는 패턴을 표현할 수 있다. 여기서 한 사람이 특정 문서를 읽었을 때 한 페이지에서 발생하는 이벤트들을 한 세션(session)으로 정의하였을 때 각 세션에 대해서 세 가지의 특징을 바탕으로 사용자들을 구분할 수 있다.

우선 문서 읽는 속도와 관련하여, 스크롤을 아래로 읽으면서 문서를 읽는 방향인 정방향에 대한 스크롤 위치의 변화를 시간의 변화율로 나눈 평균 정방향 스크롤 속도(Mean Forward Velocity)를 하나의 특징으로 선택하였다.

한편, 역방향으로 문서를 읽는다는 것은(예를 들어 2페이지에서 1페이지로 문서를 보는 것) 문서를 거꾸로 읽는 것이 아니라 앞에서 언급되었던 내용이 기억나지 않을 때라든지 다시 한 번 참조하고자 할 때 마우스 휠 또는 키보드의 방향키를 이용하여 순식간에 이동하는 것을 의미한다. 이와 같이 문서의 특정 부분을 다시 보기 위하여 역방향으로 문서를 읽는 것 또한 고유한 사용자의 패턴을 판단할 수 있는 중요한 근거가 될 수 있다. 이러한 역방향으로 문서를 보는 것과 관련하여 속도가 아닌 횟수 또는 빈도로 대신하여 역방향 움직임 빈도(Backward Frequency)를 제안한다.

마지막으로 클릭 비율(Click Ratio)은 문서 내에서 'Selected Text'가 얼마나 자주 변화하는지에 대한 빈도를 의미한다. 여기서 'Selected Text'의 변화는 커서 위치의 변화를 나타내는 'Δ cursor

timestamp			totalNumber OfPages	currentVisible PageNumbr	docZoom Percentage	docVertical PercentScrolled	docHorizontal PercentScrolled	Current PageNumber	pageVertical PercentScrolled	cursor PageNumbr	selectedText	elapsedTime
1320442851	21:40:51	0:00:00	8	1	140	0	7	1	0	1	T	0
1320442877	21:41:17	0:00:26	8	1	140	2	0	1	16	1	T	26
1320442967	21:42:47	0:01:56	8	1	140	3	0	1	24	1	p	90
1320443005	21:43:25	0:02:34	8	1	140	4	0	1	32	1		38
1320443018	21:43:38	0:02:47	8	1	140	7	0	1	56	2	f	13
1320443073	21:44:33	0:03:42	8	1	140	6	0	1	48	1	h	55
1320443074	21:44:34	0:03:43	8	1	140	4	0	1	32	1	o	1
1320443076	21:44:36	0:03:45	8	1	140	2	0	1	16	1	a	2
1320443178	21:46:18	0:05:27	8	1	140	4	0	1	32	1	.	102
1320443231	21:47:11	0:06:20	8	1	140	8	0	1	64	2	o	53
1320443251	21:47:31	0:06:40	8	1	140	9	0	1	72	2	B	20
1320443252	21:47:32	0:06:41	8	1	140	10	0	1	80	2	c	1
1320443253	21:47:33	0:06:42	8	1	140	11	0	1	88	2	e	1
1320443291	21:48:11	0:07:20	8	1	140	12	0	1	96	2	S	38
1320443292	21:48:12	0:07:21	8	2	140	13	0	2	4	2	a	1
1320443299	21:48:19	0:07:28	8	2	140	15	0	2	20	2	s	7
1320443312	21:48:32	0:07:41	8	2	140	17	0	2	36	2	u	13

〔그림 3〕 로거 프로그램을 통하여 수집된 데이터의 일부

position'와 밀접한 연관이 있으며, 키보드의 방향키 또는 마우스 클릭을 이용한 커서 위치의 변화 정도를 통하여 사용자의 문서 읽기 행위를 나타내는 하나의 특징으로 볼 수 있다.

V. 실험 및 분석 결과

5.1 데이터 수집 방법

피험자는 〔표 3〕의 환경과 같이 VMWare vSphere〔17〕 서버에 구축한 가상 머신에 접근하여 실험을 수행한다. 피험자가 가상머신에 접속하면 실험을 위하여 작성된 예제문서와 문제를 접하게 된다.

〔표 3〕 실험 환경

서버	CPU	Intel(R) Zeon(R) E5620 2.4GHz
	OS	VMWare ESXi 5.0
가상 머신	RAM	512MB
	HDD	20GB
	OS	Windows XP
	워드 프로세서	Microsoft Word 2010

문제의 수는 10개이며, 문제를 푸는 동안 문서를 읽는 일련의 과정이 로거 프로그램을 통하여 기록된다. 여기서 문제를 제시하여 문서를 읽는 동안 문제를 풀게 하는 것은 모든 피험자에게 문서를 읽게 하는 동기를 똑같이 부여하고자 한 것이며, 문서를 읽는 행위가 사용자들마다 다르다는 결과를 제시하기 위하여 사용자들의 행위라는 독립변수 이외의 다른 조건에 대하여 통제함으로써 각각의 피험자가 같은 목적으로 문서를 읽더라도 문서를 읽는 패턴이 다르게 나타나고자 하는 것을 보이고자 하는 것이다.

문제를 텍스트파일로 주어진 것은 문서를 읽으면서 문제를 풀 때 발생하는 이벤트를 Mirosoft Word 기반의 로거 프로그램이 기록하지 않음으로써 순수한 문서 읽는 행위만을 관찰하기 위한 것이며, 문제를 푼 답의 정답 여부에 대해서는 문서 읽는 행위 자체와는 큰 연관이 있지 않기 때문에 따로 점검하지 않는다. 실험에 실험을 통하여 수집된 데이터는 〔그림 3〕와 같이 기록되었다.

5.2 실험 순서

피험자는 가상 머신에 설치된 Microsoft Word 2010을 사용하여 주어진 1단 구성의 23페이지짜리 두 종류의 문서를 읽게 되며 동시에 텍스트 파일(.txt)형식으로 제시된 문제를 푸는 과정을 거치게 된다. 여기서 사용된 문서는 주간잡지 『매일이코노미』에 연재된 '장례문화'와 관련된 기사〔18〕, '소셜커머스'와 관련된 기사〔19〕를 사용하였다. 이 지문을 사용한 이유는, 일반 대중이 쉽게 접하여 읽을 수 있고 적절한 표와 그래프가 삽입되어 사람들의 문서 읽는 습관을 보다 분명하게 관찰할 수 있을 것으로 보았기 때문이다.

5.3 분석 방법

우선 실험을 통하여 수집된 데이터를 통하여 관찰된 각 행위에 대하여 A 또는 B로 라벨링(labeling)하였다. 여기서 B를 인증 받고자 하는 사용자, A를 B 이외의 사용자로 정의하였다. 여기서 이루어지는 분석은 B라는 사용자의 문서를 읽는 행위에 대하여 기계학습을 수행한 후, 이렇게 학습된 기계에 B와 B 이외의 사용자들(A)의 문서 읽는 행위를 테스트 셋(test set)으로 입력하였을 때 B와 B가 아닌 사용자를 잘 구분할 수 있는지를 보기 위한 것이다. 즉, 기계 학습을 통하여 B라는 사용자가 평소에 문서를 읽는 행위가 학습되었을 때, 실제 시스템에 B라고 로그인하여 사용하고 있는 사용자의 문서 읽는 행위를 모니터링하고 학습된 B의 문서 읽는 행위와 비교하여 B의 행위와 다르다고 한다면 비정상적인 행위로 간주한다.

분석에서는, 한 사람당 한 문서만을 읽었기 때문에 주어진 데이터의 양이 적기 때문에 각 사람당 문서를 읽은 각 페이지에 대하여 인스턴스를 생성하였다. 라벨링된 데이터는 Weka〔20〕를 이용하여 Supervisor 기계학습을 수행하였고, Naive Bayes, Support Vector Machine(SVM), Classification and Regression Tree (CART), 그리고 Random Forest 분류기 알고리즘을 사용하였다. 평가는 10-folds cross validation에 의하여 수행하였다.

〔표 4〕 기계학습을 수행한 분류기 알고리즘별 성능 측정 결과

알고리즘	Accuracy	False positive	False negative	AUC
Naive Bayes	85.59%	0.74%	13.67%	.769
SVM	86.20%	0%	13.80%	.500
CART	91.50%	3.57%	4.93%	.946
Random Forest	96.55%	1.11%	2.34%	.988

5.4 분석 결과

10명의 피험자로부터 수집한 데이터를 분석한 결과는 〔표 4〕와 같이 나타낼 수 있다. 여기서 false negative rate는 인증 받고자 하는 사용자가 권한이 없는 것으로 간주되는 확률이며, 정상적인 사용자가 중요한 작업 도중 인증이 잘못되어 시스템을 제대로 사용하지 못할 확률이다. 따라서 false negative rate가 높을수록 정당한 사용자에게 불편을 야기할 확률이 높다는 것을 의미한다. 한편 false positive rate는 권한 없는 사용자가 인증 받고자 하는 사용자로 잘못 분류될 확률이며, false positive rate가 높다는 것은 보안상 중대한 문제가 발생하여 권한 없는 사용자라도 쉽게 권한 있는 사용자인 것처럼 인증되어 문서 유출이 가능하다는 것을 나타낸다.

기계학습을 수행한 결과, 앙상블 알고리즘(ensemble learning algorithm)인 Random Forest가 정확도, false positive rate, 그리고 true positive rate와 false positive rate의 관계를 나타내는 ROC(receiver operating characteristic) 곡선의 면적(AUC; Area Under Curve)에서 다른 분류기 알고리즘에 비해 매우 좋은 성능을 보여 주는 것으로 확인되었다. 특히 정확도와 AUC는 다른 어떤 분류기 알고리즘에 비해서 보다 높은 수치를 나타내는 것으로 확인되었다.

다만 가장 좋은 성능을 나타내는 Random Forest도 접근 제어 시스템에서의 유럽 기준(the European Standard For Access Control Systems)에서 요구하는 수준인 0.001% 미만의 false positive rate(또는 false acceptance rate) 0.001%, 1% 미만의 false negative rate (또는 false rejection rate)을 충족시키지 못하고 있다. 이는 이 시스템을 단독으로 사용할 수 없다는 것이다. 기존의 마우스 움직임을 통한 사용자 인증 시스템에 관한 연구〔9〕에서도 접근 제어 시스템에서의 유럽 기준을 충족시키지 못하는 것으로 나타났다. 하지만 이 시스템을 제안하고자 한 목적은 기존의 인증 시스템과 결합하여 기존의 인증 시스템이 가지고 있는 문제점을 보완하고자 하고자 한 것이었으며, 다른 탐지 시스템과 결합하였을 때 전반적인 오탐율은 낮아질 것으로 기대한다.

VI. 결론 및 향후 연구

내부자에 의한 핵심 문서의 유출은 이미 시스템에서 인가된 정당한 권한을 가진 사용자에 의한 불법 행위라는 점에서 기존의 시스템으로는 유출을 막기 어려운 점이 있다. 이 연구에서는 이러한 문제를 해결하고자 내부자가 문서에 접근하는 과정을 확인하여 사용자의 신원을 확인하고 재인증하는 프레임워크를 제안하고 성능을 평가하였다.

Microsoft Word 로거 프로그램으로부터 추출할 수 있는 속성을 바탕으로 사용자의 문서 읽기 패턴을 나타낼 수 있는 특징들을 추출하였다. 10명의 사용자를 대상으로 두 가지 문서에 대하여 실험하였으며, 비교적 낮은 false positive rate를 가져왔다.

향후 연구에서 보완해야 할 점은 몇 가지로 정리될 수 있다. 먼저, 현재 연구에서는 10명의 피험자를 대상으로 분석을 수행하였다. 어떠한 기업이나 조직에서 10명의 수치는 매우 적은 수준이지만, 연구를 수행하면서 실제 사람들이 문서를 읽는 행위를 모니터링하기 위해서는 피험자들의 동의와 함께 실험 과정에서 피험자가 지루해하거나 흥미를 느끼지 못하는 등 다양한 변수로 인하여 많은 사람들로부터 의미 있는 데이터를 수집하는 것은 매우 어려운 과정이다. 추후 연구에서 보다 많은 사용자들이 여러 개의 문서를 읽는 과정을 통하여 지속적으로 데이터를 수집하고 분석한다면 보다 더 좋은 결과를 가져올 것으로 예상된다.

두 번째는, 본 연구에서는 문서에 대한 권한이 없는 자가 문서를 유출하는 경우에 대하여 탐지하는 것을 제안하고 있다. 또한 문서에 대한 권한이 있는 자가 문서를 유출하는 경우에는 현재 문서를 유출하고자 하는 자와 현재 시스템에 로그인되어 있는 사용자가 일치하지 않을 때만 탐지할 수 있다, 그러나 문서에 대한 권한이 있는 자가 정상적으로 로그인하여 문서를 유출하는 상황에서는 문서를 읽는 행위만으로는 문서 유출 여부를 확인하기 어려우며, 문서를 읽으면서 나타나는 부수적 행위(마우스나 키보드를 통한 명령 입력) 등을 추가적으로 고려하여야만 한다.

또한 추출할 수 있는 특징들이 실험 문서에 독립적인 요소인지를 판단하는 것도 과제이다. 향후 연구를 통하여 보다 높은 성능을 가져올 수 있으며 사용자의 문서 읽기 패턴을 보다 잘 표현할 수 있는 특징들이 무엇인지 밝혀내는 것도 추후 연구 주제로 남겨 두었다.

마지막으로 연속적 인증이 이루어지는 횟수나 연속적 인증에 소요되는 시간 또한 추후 연구해야 할 과제

중 하나로 뽑힌다. 연속적 인증이 이루어지는 횟수는 사용자의 일상적인 업무에 방해가 되지 않아야 한다는 점과 인증을 통한 효과적인 위장자 공격의 탐지 가능성을 모두 고려하여 결정되어야 한다. 연속적 인증에 소요되는 시간은 신속한 재인증을 통하여 위장자 공격을 빨리 탐지할 수 있는 가능성과 충분한 데이터의 수집으로 인한 낮은 오탐율을 모두 고려하여 결정하여야 한다.

이 연구에서 제안한 프레임워크의 실제 적용까지는 지속적인 연구가 요구되지만 이 프레임워크가 활성화되면 비교적 적은 비용으로 내부자에 의한 정보유출을 막을 수 있을 것으로 기대한다.

참고문헌

〔1〕 Richardson, R., "CSI Computer Crime & Security Survey," Computer Security Institute, 2008.

〔2〕 장항배, 여상수, 박길철, 이창훈, "내부정보 유출방지를 위한 문서보안 컴포넌트 개발 연구," 보안공학연구논문지, 5(2), pp.123-132, 2008년 4월.

〔3〕 Liu, S. and Kuhn, R., "Data loss prevention," IEEE IT Professional, vol. 12, no. 2, pp 10-13, Mar./Apr. 2010.

〔4〕 Liu, Q. and Safavi-Naini, R. and Sheppard, N.P., "Digital rights management for content distribution," Australian Computer Society Inc., Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, vol. 21, pp 49-58, 2003.

〔5〕 Volchkov, A., "Server-based computing opportunities," IEEE IT professional, vol. 4, no. 2, pp 18-23, March-April 2002.

〔6〕 N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," ACM in Proceedings of the 18th ACM conference on Computer and Communications Security, pp. 139-150, Oct. 2011.

〔7〕 T. Ruggles, "Comparison of biometric techniques," tech. rep., California Welfare Fraud Prevention System, http://www.bio-tech-inc.com/bio.htm, 2002.

〔8〕 정연덕, "생체인식기술(Biometrics)의 효과적 활용과 문제점," 특허청 지식재산21, 통권 제86호, pp. 1-16, 2004년 7월.

〔9〕 A. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 3, pp. 165~179, Jul./Sep. 2007.

〔10〕 H. Gamboa and A. Fred, "A behavioral biometric system based on human computer interaction," Proceedings of SPIE, vol. 54, pp. 4-36, 2004.

〔11〕 T. Lane and C.E.Brodly, "Temporal sequence learning and data reduction for anomaly detection," In DARPA Information Survivability Conference & Exposition Ⅱ, vol. 2, no. 3, pp. 295-331, 1999.

〔12〕 I. Traore, I. Woungang, Y. Nakkabi, M.S. Obaidat, A.A.E. Ahmed, and B. Khalilian, "Dynamic sample size detection in learning command line sequence for continuous authentication," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 42, no. 5, pp. 1343-1356, Oct. 2012.

〔13〕 S. Cho, C. Han, D.H. Han, and H.I. Kim, "Web-based keystroke dynamics identity verification using neural network," Journal of organizational computing and electronic commerce, vol. 10, no. 4, pp. 295-307, 2000.

〔14〕 F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," ACM Transactions on Information and System Security, vol. 5, no, 4, pp. 367-397, Nov. 2002.

〔15〕 E. Yu and S. Cho, "Keystroke dynamics identity verification - its problems and practical solutions," Computers & Security, vol. 23, no. 5, pp. 428-440, July 2004.

〔16〕 Z. Jorgensen and T. Yu, "On mouse

dynamics as a behavioral biometric for authentication," In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 476-482, Mar. 2011.
〔17〕 VMWare vSphere. http://www.vmware.com/kr/products/datacenter-virtualization/vsphe re/
〔18〕 매경이코노미, "5조원대 장례 비즈니스… 상주는 봉," http://news.mk.co.kr/v2/econo my/view.php?sc=50000010&cm=%C4%BF%B9%F6%BD%BA%C5%E4%B8%AE&year=2012&no=141884&relatedcode=000090143, 2012년 3월.
〔19〕 매경이코노미, "소셜 커머스, 유통지도 바꿀까", http://news.mk.co.kr/v2/economy/view.php?sc=50000010&cm=%C4%BF%B9%F6%BD%BA%C5%E4%B8%AE&year=2012&no=202943&relatedcode=000130165, 2012년 4월.
〔20〕 Weka 3, http://www.cs.waikato.ac.nz/ml/weka/

〈著者紹介〉

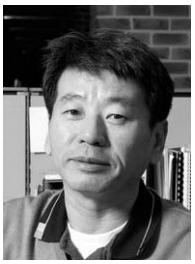
조 성 영 (Sungyoung Cho) 학생회원
2009년 8월: KAIST 정보통신공학과 학사
2013년 2월: KAIST 정보보호대학원 석사
2013년 3월~현재: KAIST 정보보호대학원 박사과정
〈관심분야〉 데이터마이닝, 통계분석, 사용자 인증, 정보보호 평가 및 인증, 정보보호 정책

김 민 수 (Minsu Kim) 학생회원
2011년 2월: KAIST 전산학과 학사
2013년 2월: KAIST 정보보호대학원 석사
2013년 3월~현재: KAIST 정보보호대학원 박사과정
〈관심분야〉 취약점, 악성코드, 시스템 보안, 기계 학습

원 종 일 (Jongil Won) 정회원
2012년 2월: KAIST 전기 및 전자공학과 학사
2012년 2월~현재: KAIST 정보보호대학원 석사과정
〈관심분야〉 시스템 보안, 모바일 네트워크 보안

〈著者紹介〉

권 상 은 (SangEun Kwon) 학생회원
2011년 8월: KAIST 전산학과 학사
2013년 2월: KAIST 정보보호대학원 석사
〈관심분야〉 데이터마이닝, 정보보호 평가 및 인증, 정보보호 정책



임 채 호 (Chae-ho Lim) 종신회원
1986년: 홍익대학교 전산학과 학사
2001년: 홍익대학교 전자계산학과 박사
2006년~2009년: NHN(주) 보안실 실장, 연구센터 수석
2009년: 한국정보보호학회 부회장
2011년 2월~현재: KAIST 정보보호대학원 연구교수
〈관심분야〉 인터넷 보안, 정보보호 위험 관리, 정보보호 관리 및 정책

강 병 훈 (Brent ByungHoon Kang) 정회원
1993년: 서울대학교 컴퓨터공학과 학사
1995년: 美 메릴랜드 주립 대학교 컴퓨터 공학 석사
2004년: 美 UC 버클리대학교 컴퓨터 공학 박사
2009년~현재: 美 George Mason University, Dept. of Applied Information Technology and Center for Secure Information Systems, 부교수
2010년 8월~현재: KAIST 정보보호대학원 겸임교수
〈관심분야〉 시스템 보안, 봇넷, 스팸 대응, 웹/DNS 분석

김 세 헌 (Sehun Kim) 종신회원
1972년: 서울대학교 물리학과 학사
1981년: 美 스탠포드대학교 경영과학 박사
1982년~현재: KAIST 산업 및 시스템공학과 및 정보보호대학원 교수
1996년~1999년: 한국정보보호진흥원 이사
2003년: 한국정보보호학회 회장
2004년~2007년: 국가정보원 자문교수
2008년~2009년: 한국경영과학회 회장
2009년~현재: 방송통신위원회 인터넷 정보보호 협의회 회장
2012년~현재: 한국과학기술한림원 정회원
〈관심분야〉 침입탐지 및 조기경보, 보안경영 및 정책