시나리오 기반의 통합 보안 로그 분석을 통한 개인정보 유출 탐지 방안 연구

류승태
고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
e-mail : debugman@korea.ac.kr

A Study of Detection Measures about the Personal Information Leakage through Scenario-Based Integrated Security Log Analysis

Seung-Tae Ryu
Dept. of Software Engineering, Graduate School of Computer and Information Communication, Korea University

요 약

최근 정보기술의 발달로 기업의 비즈니스 모델이 아날로그에서 디지털로 전환되고 있다. 기업에서는 다양한 서비스 제공을 위해 고객의 개인정보를 수집하고 있으며, 이러한 정보는 보안 위협의 대상이 되고 있다. 대다수 기업에서는 다양한 분야의 보안 솔루션이 구축 운용되고 있으나, 솔루션 개발사들의 서로 다른 보안 로그들로 인해 통합 분석에 어려움을 겪고 있으며 이로 인해 보안 모니터링 업무 효율이 낮아지는 문제점을 안고 있다. 본 연구에서는 시간적 연관성을 기반으로 통합 보안 로그를 분석 하고 시나리오화 하여 좀 더 빠르고 정확한 개인정보 유출의 이상징후를 탐지할 수 있는 방안을 제안한다.

1. 서론

최근 수년간 컴퓨터의 성능 향상과 빠른 인터넷의 보급으로 인해 대부분의 비즈니스 모델이 아날로그에서 디지털로 전환되어 왔다. 은행, 카드사, 보험 등 금융산업과 일반 기업에 대한 정보기술의 영향은 상당하다 하겠다. 그러나 이러한 정보기술은 동전의 양면과 같이 그 자체가 지닌 위험성 때문에 필수적으로 역기능을 수반하게 된다. 기업에서는 다양한 정보기술 서비스를 제공하기 위해 고객의 개인정보를 수집하고 있으며, 이러한 정보는 보안 위협의 대상이 되고 있다.

우리나라의 대규모 개인정보 침해 사례를 보면 <표 1>과 같이 1 억건 까지도 발생하는 등 규모가 커짐을 볼 수 있으며[1], 2014 년 상반기에만 개인정보 유출 사고가 20 건 이상에 이르고 있다[2]., 2014 년 초에 발생한 카드 3 사 개인정보 유출 사고처럼 전/현직 내부 직원의 정보유출이 상당부분을 차지하고 있다. 이처럼 다수의 개인정보 유출 사고의 원인이 기술적 문제뿐만 아니라 관리적 문제로도 발생 할 수 있다는 인식이 높아지고 있으며, 대부분의 기업에서는 발생 가능한 보안 위협에 대비하기 위해 E-Mail, 메신저 등의 네트워크 보안 솔루션과 USB 저장매체, 프린트 등에 대한 EndPoint 보안 솔루션, DB 접근 제어 솔루션을 도입 운영하고 있다.

본 논문에서는 기업에 도입된 보안 솔루션에서 발생하는 보안로그의 통합 분석을 통하여 내부 관리 문제로 인한 개인정보 유출의 보안 사고 예방을 위한 방안을 제시하고자 한다.

<표 1> 대규모 개인정보 침해 사례

발생일	발생기업	피해규모
2008. 2	옥션	1800 만명
2008. 4	하나로텔레콤	600 만명
2008. 9	GS 칼텍스	1,150 만명
2010. 3	신세계몰 등 25 개 업체	2,000 만명
2011. 4	현대캐피탈	175 만명
2011. 5	리딩투자증권	12,000 건
2011. 5	세티즌	140 만명
2011. 6	대부업체, 저축은행, 채팅사이트	1,900 만건
2011. 7	SK 컴즈(네이트, 싸이월드)	3,560 만명
2011 8	삼성카드	47 만건
2011.11	넥슨	1,320 만건
2012. 5	EBS	400 만건
2012. 7	KT	870 만건
2012.12	BC 카드, 국민카드 ISP 시스템	18,000 만건
2014. 1	KCB, NH 카드, 롯데카드, 국민카드	10,400 만건

2. 보안 솔루션을 이용한 모니터링

2.1 개인정보 유출 사례 및 유출 경로

개인정보의 유출 유형은 크게 기술적 문제로 인한 보안 사고와 내부 관리 문제로 인한 보안 사고로 나뉠 수 있다. 전자는 해커가 악성코드 등을 이용하여 사내 정보 시스템에 침입해 개인정보 등을 유출하는 것이며, 후자는 고객 정보 데이터베이스에 접근 가능한 내부 권한자가 악의적으로 개인정보를 유출하는 등의 관리적 문제에 따른 것이라 하겠다.

<표 2>과 같이 수년째 대형 개인정보 유출 사고가 이어지고 보안 투자와 조직 내 정보보호 인식의 중요성이 높아지는 상황임에도 불구하고 악의적인 내부자 소행에 의한 정보유출이 끊임없이 발생하고 있다.

<표 2> 개인정보 유출 사례 및 유출 경로

유출 사건	유출 경로
GS 칼텍스	담당 직원이 고객정보를 빼내 DVD 에 구워 판매하려 함
카드 3 사	DB 접근권한이 있는 외주사 직원이 1 년 이상 시간에 걸쳐 USB 에 개인정보를 복사하여 유출
IBK 캐피탈	직원이 고객정보와 신용정보를 조회, 유출
삼성카드	영업직원이 당사 서버를 해킹하여 고객정보 유출
신세계몰	중국 해커에 의해 고객정보 유출
메리츠화재	내부직원이 분석목적으로 고객 데이터 유출

2.2 보안 솔루션의 모니터링 기능 및 문제점

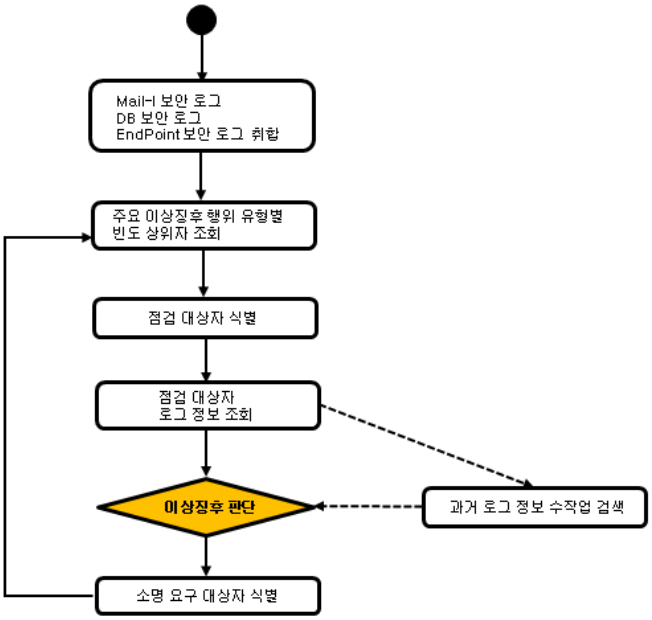
최근의 유출 사례에서도 알 수 있듯이 개인정보 유출의 위협이 내부 위협으로도 발생할 수 있다는 인식이 높아짐에 따라 조직에서는 주요 정보 자산이 외부로 유출되는 것을 막기 위하여 다양한 보안 솔루션을 도입, 운용하고 있다.

대부분의 기업들은 인터넷을 이용한 업무가 증가함으로 인해 사내에서 사외로 정보가 유출될 가능성이 있는 E-Mail, P2P, WEBHARD, 메신저 등에 대한 네트워크 보안 솔루션, 다양한 정보를 저장하고 있는 DB 에 대한 접근 제어 및 모니터링 솔루션, EndPoint 에서의 유출 통제를 위한 USB 저장매체, 프린트 등에 대한 보안 솔루션을 활용하고 있다.

이러한 보안 솔루션의 활용은 개인정보 유출에 대한 위협에 대비한다는 측면도 있지만, 도입함으로써 여러 비용이 발생하게 된다. 다양한 방식의 보안 솔루션 도입에 따른 비용 투자, 보안 솔루션 운용방법을 익히기 위한 시간 투자, 운용을 위한 물리적 공간과 관리 조직 및 인력 확보가 필수 조건으로 요구된다.

보안 관리자는 다수의 보안 솔루션에서 쏟아져 나오는 수많은 정보들 중 의미 있는 정보가 무엇인지 판단하고, 선택된 정보를 이용하여 최종 의사 결정을 내려야 한다. 대다수 보안 관리자는 주요 이상징후 행위 유형의 빈도 상위자 중에서 상세 검색 대상자를 직관으로 식별 하고 상세 검색 대상자의 로그 정보를 조회하고 필요 시 과거 로그 데이터에 접근하여 검색을 수행 하게 된다. 이러한 방식은 보안 관리자의 업무 과중으로 이어지고 있으며, 개인정보 유출의 이상징후 모니터링에 대한 업무 효율도 낮아지게 된다.

(그림 1)은 이러한 로그 분석 과정을 도식화한 것이다.



(그림 1) 일반적인 보안로그 분석 Flow

3. 시나리오 기반의 통합 보안 로그 분석을 통한 개인정보 유출 이상징후 모니터링

본 연구에서는 해킹 등 외부위협에 대한 보안 솔루션이 아닌, 내부자에 의한 개인정보 유출 보안 솔루션을 대상으로 하고 있으며, 기업 내에서 일반적으로 사용하고 있는 네트워크 보안 솔루션, DB 접근 제어 솔루션, EndPoint 보안 솔루션 등을 주 대상으로 한다. 또한 관리자의 경험과 직관에 기반한 판단의 일부를 자동화 하고 유출 행위에 대한 시나리오를 기반으로 개인정보 유출 이상징후를 탐지하는 방안을 제시한다. 각각의 보안 솔루션에서 수집되는 보안 로그를 통합한다고 해서 정보보호 활동에 유의미한 데이터를 바로 추출 할 수 있는 것은 아니다. 보안 대상이 되는 개인정보에 대하여 수집, 가공, 유출행위에 대한 정보의 흐름을 시나리오화하는 것이 필요하다.

본 연구에서 제시하는 시나리오 기법은 미래에 일어날 수 있는 여러 가지 상황을 연극의 대본처럼 '스토리(story)' 형식으로 전달하여 미래의 다양한 모습을 쉽게 이해할 수 있도록 도와주는 예측기법[3]이라 할 수 있다.

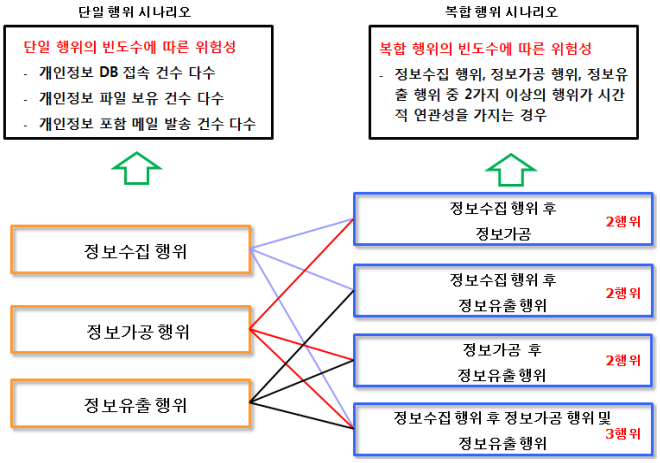
이를 위해서는 보안 로그들의 행위들을 단일 행위 시나리오로 정의, 분류하고 개별 시나리오를 개인정보 유출의 가능성이 있는 복합 시나리오로 재정의 하

는 것이 중요하다. 행위는 정보수집, 가공, 유출행위로 구분할 수 있으며 정의는 <표 3>과 같다. 분류된 시나리오는 시간적 연관성을 기반으로 유출을 의심할 수 있는 복합 시나리오로 재정의 할 필요가 있다.

<표 3> 시나리오 행위 정의

행위	정의
정보수집 행위	파일 서버, 데이터베이스 등에 접속하여 개인정보 조회, 개인 PC 또는 다양한 저장매체에 저장 하는 행위
정보가공 행위	저장된 정보에 대한 편집 행위
정보유출 행위	E-Mail, 메신저, USB, 프린트 등을 이용한 유출 행위

개별 단위 행위들의 다양한 조합을 통해 복합 시나리오를 정의하는 방식은 (그림 2)와 같다. 복합 시나리오의 개별 행위는 사내에 구축 운용중인 보안 솔루션에서 수집되는 다양한 로그를 대상으로 다시 한번 재정의가 필요하다.



(그림 2) 복합 시나리오 정의

<표 4>는 발생 가능한 행위들을 시간적 연관성을 기반으로 복합 시나리오로 정의한 것이다. 이때 업무상 필요에 의한 행위들로 인해 복합 시나리오에 적용되는 사용자가 많을 수 있다. 정당한 행위자는 복합 시나리오에 의한 이상징후에서 제외 시켜야 하며, 이는 개별 행위에 대한 임계치 또는 관리 대상을 두어 제외 시킬 수 있다.

<표 4> 복합 시나리오 예시

행위	예시
복합	개인정보 DB 접속 후 개인정보가 포함된 파일을 첨부하여 외부로 발송 하는 경우
	휴일, 퇴근 이후 시간에 network(mail, ftp, p2p)을 통해 파일을 외부로 전송하는 경우
	개인정보 패턴 보유수가 갑자기 많아지고, 프린트를 이용하는 횟수가 증가하는 경우

사내의 모든 사용자를 대상으로 보안 로그를 분석하는 것이 가장 바람직하지만, 이러한 방식은 많은 시스템 비용과 시간을 필요로 한다.
따라서 <표 5>와 같이 사내에 구축되어 있는 인사정보 DB 나 업무 시스템과 연동하여 개인정보 취급자, 퇴직 신청자, 퇴직 우려자, 인사 징계자 등의 관리대상을 별도 그룹핑하고 관리하여 일별 우선 검토 대상으로 선별하는 것이 효율적이다.

<표 5> 관리대상 그룹 정의

관리대상	퇴직 신청자/ 우려자	부서장에게 퇴직 의사 전달자
		퇴직 신청자
		채용 사이트 접속자
	인사 징계자	인사부서 정보 연동
	개인정보 취급자	인사부서 정보 연동
	핵심인력	사내 주요 업무 수행자
	관리자	보안정책 예외자, 시스템 권한자

<표 6>은 시나리오 행위에 대한 프로파일링 분류를 정의한 내용이다.한국씨티은행의 개인정보 유출 사건은 내부 직원이 회사 전산망에 저장된 대출 채무자의 정보를 수집하여 A4 용지 1 천 100 여장에 출력해 유출한 사건이며, 카드 3 사의 개인정보 유출 사건은 권한이 있는 관리자가 고객정보 DB 에 접속하여 대량의 고객 정보를 저장하고, 이 후 USB 등에 복사하여 유출한 사건이다. 해당 사건들은 <표 6> 프로파일링에 의하면 [1 - 3 - 6], [1 - 3 - 7] 의 시나리오에 해당 한다.

<표 6> 시나리오 행위 프로파일링 분류 예시

구분	선정된 행위	NO
정보 수집	고객정보 Database 접속하여 정보 조회	1
	파일서버에 접속하여 고객정보 다운로드	2
정보 가공	고객정보를 로컬 PC 에 파일로 저장	3
	고객정보를 하나의 파일로 또는 다수의 파일로 편집	4
정보 유출	E-Mail 로 유출	5
	USB 저장	6
	프린트 출력	7

위 두 사건처럼 다수의 개인정보 유출 사건은 내부 권한자에 의한 유출이 대부분을 차지 하고 있다. 복합 시나리오 기법을 적용한다면 내부 권한자가 개인정보를 조회 후 파일로 저장하면 유출 전 단계로 1 차 경고하며, 이 후 E-Mail 이나 USB 등으로 저장하는 경우 유출로 의심하여 2 차 경고를 발생시켜 개인정보 유출 사고 예방에 활용 할 수 있을 것이다.

4. 결론 및 향후 연구

내부자에 의한 개인정보 유출 사건 발생시, 기업은 피해보상, 브랜드 이미지 실추 등 손실과 비용이 발생하게 된다. 유출사건의 피해는 기업 뿐만 아니라 사용자에게도 발생하며, 유출된 개인정보의 일부가 보이스 피싱이나 스팸 등에 사용됨으로써 2 차 피해를 야기한다. 이러한 피해를 예방하기 위해 기업에서는 다양한 보안 솔루션을 도입 운용하고 있다. 그러나 여러 업체에서 개발된 보안 솔루션들은 서로 다른 특징들로 인해 보안업무 활동의 복잡성과 관리포인트를 증가시키고 있으며, 보안 담당자의 효율적인 보안 업무를 저해하는 부작용을 낳고 있다. 이러한 문제점들을 개선하기 위해 시간적 연관성을 기반으로 복합 시나리오 기법을 활용한 개인정보 유출 이상징후 탐지 방안을 연구하였으며, 해당 연구를 기반으로 개인정보 보안 모니터링에 대하여 체계적인 정책을 수립하고 적용함으로써 효과적이고 효율성 있는 정보보호 활동의 목표를 이룩할 수 있을 것이다.

향후 연구로는 실시간 빅데이터 분석 기술을 활용하여 개별 행위 발생 시점에서 과거 행위와의 연관성을 분석하여 이상징후를 실시간 탐지 할 수 있는 분석 시스템 설계가 요구된다.

참고문헌

[1] 이용수, “우리나라의 개인정보 침해 실태와 한국우정의 대책”, 우정경영연구소 우정정보 98 2014 가을

[2] NIA 개인정보보호 주간동향 제 54 호 2014.6.5

[3] 임현, 한종민, 정민진, “미래예측을 위한 시나리오 분석 및 시스템 구축방안”, 한국과학기술기획평가원 ISSUE PAPER 2009-09