이메일을 통한 기밀정보 유출 유형의 내부자 위협 탐지 기술

이영재[O], 강성원[*], 김경미[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {kronosyuki[O], S193802[*], kkkkmm2001[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Insider Threat Detection Technology against Confidential Information Loss using Email

Youngjae Lee[O], Seongwon Kang[*], Kyungmi Kim[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

내부자 위협이란, 조직의 보안 및 데이터, 시스템에 대한 내부 정보에 접근하는 현 임직원 및 전 임직원, 계약자와 같이, 동일한 조직 내부의 사람들로부터 발생하는 위협을 의미한다. 일반적으로 내부자들은 업무를 위하여, 시스템에 대한 합법적인 접근 권한을 가지며, 만약 이러한 권한이 오남용되는 경우에는 조직에 매우 심각한 피해를 입힐 수 있다. 이러한 내부자 위협은 외부로부터의 위협보다 방어 및 탐지가 훨씬 어려운 한 계점이 있으며, 그 피해 규모가 매우 방대하다는 문제점도 존재한다. 이에 따라, 본 논문에서는 내부자 위협을 탐지하기 위하여, 이메일을 통한 기밀정보를 유출하는 유형의 위협에 대응하는 방안을 제안한다. 제안하는 방안은 조직 내에서 이메일을 발신하는 경우를 대상으로, 파일이 포함된 이메일에 발신자를 식별하기 위하여, 파일에 키 값 및 서명을 삽입하며, 발신되는 이메일을 모니터링하여 첨부된 파일의 유형을 파악함으로써, 동적 그래프를 통하여 시각화한다. 내부 시스템 및 네트워크에서의 보안관제 담당자 및 관리자는 시각화된 그래프를 확인함으로써, 직관적으로 정보 유출을 파악하고 대응할 수 있을 것으로 판단된다. 본 논문에서 제안하는 방안을 통하여, 조직 내의 내부자 위협을 탐지할 수 있으며, 데이터 유출 사고가 발생하는 경우, 유출자를 빠르게 식별하고 초기에 대응할 수 있을 것으로 판단된다.

키워드: 내부자 위협(insider threat), 탐지 기술(detection technology), 기밀정보 유출(confidential information loss), 이메일(email)

I. 서론

내부자 위협이란, 조직의 보안 및 데이터, 시스템에 대한 내부 정보에 접근하는 현 임직원 및 전 임직원, 계약자와 같이, 동일한 조직 내부의 사람들로부터 발생하는 조직에 대한 악의적인 위협을 의미하며[1], 이러한 위협으로 인하여, 기밀정보 및 지적재산의 유출, 시스템 가용성 침해 등이 발생한다[2]. 일반적으로 내부자들은 업무를 위하여, 시스템에 대한 합법적인 접근 권한을 가지며, 만약 이러한 권한이 오남용되는 경우에는 조직에 매우 심각한 피해를 입힐 수 있다.

이러한 위협이 가능한 이유는 내부자는 데이터에 물리적인 접근이 가능하고, 외부로부터의 공격과정인 방화벽이나 침입탐지시스템과 같은 경계 보안을 위한 대책들을 우회할 필요가 없으며, 이러한 특징으로 인하여, 조직 내부의 네트워크 및 시스템, 데이터에 정당하게 접근이 가능하기 때문이다.

이에 따라, 내부자 위협은 외부로부터의 위협보다 방어 및 탐지가 훨씬 어려운 한계점이 있으며, 그 피해 규모가 매우 방대하다는 문제점도 존재한다. 따라서 본 논문에서는 내부자 위협을 탐지하기 위하여, 이메일을 통한 기밀정보를 유출하는 유형의 위협에 대응하는 방안을 제안한다.

II. 제안하는 내부자 위협 탐지 기술

제안하는 방안은 조직 내에서 이메일을 발신하는 경우를 대상으로, 키 값 및 서명 삽입, 실시간 모니터링 시스템을 통하여, 내부자 위협을

탐지하며, 내부자로 인한 정보 유출을 신속히 파악하고 대응할 수 있을 것으로 판단된다.

파일이 포함된 이메일에 발신자를 식별하기 위하여, 파일에 키 값 및 서명을 삽입하며, 발신되는 이메일을 모니터링하여, 첨부된 파일의 유형을 파악함으로써, 동적 그래프를 통하여 시각화한다. 식별 가능한 파일 유형은 hwp, docx, xlsx, pdf와 같은 문서 및 소스코드와 같은 기밀정보가 저장될 수 있는 파일 유형을 포함하며, 시각화를 통하여 파일 유형에 따른 추세를 파악할 수 있다. 내부 시스템 및 네트워크에서의 보안관제 담당자 및 관리자는 시각화된 그래프를 확인함으로써, 내부자로부터 발생하는 이상 징후를 탐지하여 내부자 위협 및 유출자를 빠르게 식별하고 초기에 대응할 수 있을 것으로 판단된다. 제안하는 방안의 전반적인 과정을 그림 1에 나타내었다.

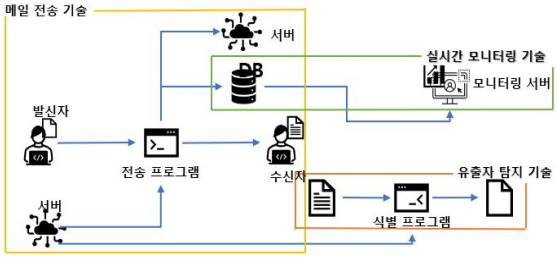

Fig. 1. 내부자 위협 탐지를 위한 모니터링 및 유출자 식별 과정

그림을 살펴보면, 내부자 위협을 탐지하기 위하여, 모니터링 기술과 유출자 탐지 기술, 이메일 전송 기술을 제공한다.

1. 모니터링 기술

모니터링 기술은 이메일에 첨부된 파일과 관련된 정보를 실시간으로 수집하여 동적 그래프로 출력하며, 출력되는 그래프에는 파일 유형 및 파일 개수, 시간과 같이 관리자가 이상 징후를 식별할 수 있는 정보를 포함한다. 또한, 필요에 따라, 필터링 기능을 통하여 특정 파일 확장자만 출력하는 기능도 제공한다.

2. 유출자 탐지 기술

유출자 탐지 기술은 유출된 파일을 통하여 유출자를 탐지하는 방안을 제공하며, 유출된 파일을 확보하는 경우, 해당 파일에 삽입된 키 값을 토대로 유출자의 서명을 검증하며, 검증된 서명을 통하여 유출자의 신상을 확인할 수 있다. 서명 및 검증을 위하여, RSA 알고리즘과 같이 안전한 공개키 알고리즘을 사용한다.

3. 이메일 전송 기술

이메일 전송 기술은 내부자가 이메일을 작성하고 보내는 기능을 제공하고, 본 논문에서는 구현의 용이함을 위하여 구글 메일을 활용하였다. 제안하는 방안의 대부분 기술이 이메일을 발신할 때 제공되므로, 내부자는 조직에서 제공하는 이메일 서비스를 사용하여야 하며, 파일을 첨부하여 이메일을 발신하는 경우에는 첨부된 파일에 내부자를 식별하기 위한 키 값과 서명을 삽입한다. 향후, 삽입된 키 값과 서명을 검증하기 위하여, 키 값과 개인키 및 공개키는 데이터베이스에 저장하며, 이메일을 성공적으로 발신한 경우에는 첨부된 파일의 확장자 및 시간과 같이 모니터링을 위한 정보를 데이터베이스에 저장한다.

상기와 같은 기술들을 활용하여 유출자를 식별하는 과정을 살펴보면, 만약 내부자가 파일을 첨부하여 이메일을 발신하면, 그 파일의 확장자를 확인하고 파일에 내부자를 식별할 수 있는 키 값 및 서명을 삽입하여 서버에 저장한다. 해당 키 값은 값이 중복되지 않도록 UUID (Universally Unique IDentifier) v4로 생성하며, 만약 첨부된 파일이 유출된 기밀파일로 알려질 경우, 유출자를 식별하기 위한 정보로 활용된다. 이메일 수신자는 키 값 및 서명이 삽입된 파일을 수신하지만, 삽입된 키 값 서명은 특별히 파일을 분석하지 않는 한, 직관적으로 확인하기 어렵다. 모니터링 과정을 살펴보면, 이메일에 포함된 파일의 유형 및 파일 개수, 시간과 같이 관리자가 이상 징후를 식별할 수 있는 정보를 데이터베이스에 저장하며, 이러한 정보는 실시간으로 동적 그래프로 시각화한다.

만약 기밀정보가 유출되는 상황이 발생하여 그 파일을 확보한 경우, 해당 파일에 삽입된 키 값을 추출하고, 키 관리 서버로부터 키 값을 조회하여 삽입된 서명을 검증한다. 서명 검증결과, 내부자로 확인된 경우에는 유출자로 판단하여 조치를 취할 수 있다.

III. 결론

본 논문은 이메일을 대상으로, 내부자 위협으로 인한 기밀정보 유출을 탐지하기 위하여, 키 값 및 서명 삽입, 실시간 모니터링 시스템을 통하여, 유출자를 식별함으로써 내부자 위협을 탐지하는 방안을 제안하였다. 제안하는 방안을 통하여 내부자 위협을 완벽하게 탐지할 수는 없지만, 효과적으로 내부자 위협을 예방할 수 있을 것으로 사료된다.

향후 연구로는, 자체 메일 서비스를 확보하기 위한 방안을 연구하고, 키 값 및 서명을 효과적으로 은닉하기 위한 스테가노그래피 기술을 적용할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542, NRF-2021R1A4A2001810).

REFERENCES

[1] 이재용, 김인석, "내부자 보안위협 분석을 통한 전자금융 이상거래 탐지 및 대응방안 연구," 한국전자거래학회지, 제23권, 제4호, pp. 153-169, 2018년 11월.

[2] Ponemon Institute, "2022 Cost of Insider Threats Global Report," 2022.