정보보안 훈련 시스템에서 미션 성취도 평가를 위한 마코브 체인 모델 기반의 학습자 행위 패턴 분석

이택○ 김도훈 이명락 인호
고려대학교 정보통신대학
comtaek@korea.ac.kr○, karmy01@korea.ac.kr, lmr2010@korea.ac.kr, hoh_in@korea.ac.kr

Markov Chain Model-Based Trainee Behavior Pattern Analysis to Evaluate Mission Completion in Security Training System

Taek Lee○ Dohoon Kim Myongrak Lee Hoh Peter In
College of Information and Communications, Korea University

1. 연구 개요

정보보안 교육·훈련 프로그램은 사회 공학적 방법 및 인간 취약성을 이용하는 각종 보안 위협들에 대해 현실적으로 가장 능동적이며 포괄적으로 대처할 수 있는 유일한 방법이다. 훈련 프로그램들은 훈련 참여자들에게는 민감한 정보 자산들을 다루는 상황에서 자신들이 어떤 오류들을 범할 수 있는지 인지시킬 수 있는 좋은 기회를 제공하며, 업무 수행 상황에서 정보보안 위험 관리 측면에서 과연 나는 어떤 지식 기술이 부족한가에 대해 깨닫게 만들어주는 기회를 제공해준다. 훈련 프로그램에는 여러 형태가 있겠지만, 특히 실무 위주의 실습 미션 수행을 통해 터득하는 교육훈련이 가장 효과적인 것으로 보고된다[1].

일단 훈련 세션을 완료하면 훈련 감독자는 훈련 참여자들이 과연 할당된 미션을 성공적으로 수행하였는가 아니면 실패하였는가에 관해 평가해야 한다. 이 단계에서 감독자는 매우 중요한 정보를 얻게 된다. 즉, 미션을 성공한 그룹과 실패한 그룹에는 어떤 행동 패턴 차이가 있는가? 실패한 그룹에서는 도대체 어떤 공통적 오류 패턴으로 인해 미션에 실패하였는가? 실패 그룹에서는 공통적으로 발견되나 성공 그룹에서는 찾아보기 힘든 행위 패턴이 있는가? 훈련 미션 참여자들로부터 수집된 양질의 행위 분석 데이터로부터 분석가(감독자)는 이 같은 질문들에 대한 해답을 찾아낼 수 있다. 궁극적으로 이러한 분석 데이터는 필요시 오류의 수정 보완을 위한 재교육 및 교정 훈련의 중요한 피드백 정보가 된다.

본 연구에서는 훈련 참여자들의 행위 패턴 관찰을 위해 현재 저자들에 의해 연구되고 있는 가상 보안 훈련장 (Virtual Security Training Lab) 시스템을 이용하였다[2]. 일단 훈련 참여자들의 역할은 시스템 보안 관리자라 가정하였다. 해당 시스템은 훈련 참여자들에게 실제 리눅스 서버 시스템이 설치되어 있는 가상 실습 공간(가상 머신)을 제공한다. 그리고 미션 수행 도중 쉘을 통해 입력되는 모든 명령(행동)들이 관찰되고 DB로 기록되도록 하였다. 하나의 사례 연구 실험으로서 훈련 참여자들은 "리눅스 시스템을 웹 서버 전용으로 꾸미기 위해 현재 실행중인 네트워크 서비스들 중 불필요한 서비스를 찾아 차단하라"는 미션을 할당 받았다. 다수의 훈련 참여자들은 원격 접속이 가능한 리눅스 가상 머신 실습공간에서 주어진 미션을 수행하였다.

미션 성패 여부에 대한 평가와 훈련 과정에 대한 행위 패턴 분석을 위해 확률 과정 분석이 가능한 마코브 체인 모델 (Markov Chain Model) 기반의 모델링 기법과 관련 분석 알고리즘을 제안한다. 해당 알고리즘은 시간의 흐름에 따라 관찰되는 훈련 참여자들의 행위 시퀀스를 하나의 체인 모형으로 보고 미션의 성공 및 실패 가능성을 확률적으로 추정 분류한다. 제안 알고리즘을 이용하면 분류 결과에 가장 큰 결정적 공헌(확률 결정에 대한 기여도 측면에서)을 한 행동 패턴 분석 또한 가능해진다.

2. 제안 연구의 교육적 활용 가치

마코브 체인 모델로 표현되는 ATM(Action Transition Matrix: 관찰되는 확률 과정의 가능성을 추정하

는데 이용되는 행렬)은 자체적으로 풍부한 행위 패턴 정보를 담고 있어 여러 테스트 케이스에 대한 포괄적인 시각의 패턴 분석이 가능하다. 성공 그룹에서 발견되는 패턴들은 실패 그룹에서는 좀처럼 나타나지 않는다. 이들은 성공에 결정적으로 영향을 미치는 패턴들일 것이다. 이렇듯 훈련 참여자들의 세세한 행동 관찰과 패턴 분석 과정 없이는 훈련 참여자들로부터 겉으로는 잘 드러나지 않는 공통적이거나 고질적인 실수(오류적 행동 패턴)들을 발견하는 것이 힘들다. 당연히 이로 인해 실패 그룹에게 실수를 교정하기 위한 어떤 학습피드백을 주는 것 또한 어려워진다. 일반적으로 정보보안 실습 훈련 프로그램뿐만 아니라 컴퓨터 기반의 전통적인 학습 시스템(예:e러닝 시스템, 실습 시스템)이 결과 위주의 점수제 평가에만 의존하여 학습 결과를 진단하였다. 학습 중간 과정 평가 및 학습 행위 과정의 심도 있는 패턴 분석 없이는 구체적이고 잠재적인 실수들을 찾아내기 힘들며 나아가 향후 효과적인 학습 커리큘럼의 제작이나 진정한 맞춤형 교육 컨텐츠의 제작도 힘들어진다.

3. 결론 및 향후 연구

본 연구에서는 정보보안 실습 훈련 프로그램에서 훈련 참여자들의 훈련 과정을 관찰하고 행동 패턴들을 분석 하기 위한 ATM 행렬과 관련 분석평가 알고리즘을 제안하였다. 이는 꼭 보안 분야뿐만 아니라 어떤 미션 달성을 위해 진행되는 컴퓨터 기반의 학습 시스템 영역이라면 두루 적용될 수 있다. 특히, 제안 방법은 훈련내용 평가 책임자에게 훈련 참여자들의 미션 수행 과정의 적합성을 분석적으로 평가할 수 있는 기회를 제공함과 동시에 미션 성패 여부에 결정적인 행동 패턴을 발견할 수 있는 좋은 기회를 제공한다.

제안 분석 이론을 실제 가상보안훈련장 시스템의 분석평가 기능으로 구현하여 제공한다면 시스템 이용자 다수의 훈련 수행 내용 평가 과정을 보다 효율적으로 자동화 할 수 있을 것이다. 아울러 훈련장 시스템으로부터 모니터링 되는 훈련자들의 행위 데이터를 소스로 하여 훈련 과정 평가를 실시간으로 수행하여 오류적 행위에 대해 즉각적인 온라인 피드백(예: HCI 형태의 알림/경고)을 제공한다면 급박한 매 순간 의사 결정을 좀 더 신중하게 하도록 도울 수 있고 행동 교정 효과가 나타날 것이다.

제안 방법은 확률기반 모델링 특성의 한계 상 오류의 종류와 오류의 이유에 대한 정보는 제공하지 않는다. 그러나 실제 학습 피드백 제공 측면에서는 이러한 오류의 종류나 발생 이유 파악도 중요한 의미를 갖기 때문에 별도의 추가적인 분석이 필요하다. 본 논문에서는 기본적으로 컴퓨터 기반 훈련 시스템 사용자들의 행위 분석을 위한 아이디어를 제안하였고 간단한 적용 사례연구를 보였다. 그러나 통계적으로 보다 신뢰할 수 있는 분석 결과를 도출하기 위해서는 다수의 사례연구가 진행되어야 하고 이에 기반한 풍부한 행위 데이터 확보가 필요하다.

사사(Acknowledgement)

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0000142)

참고문헌

[1] Lance J. Hoffman, Tim Rosenberg, Ronald Dodge, and Daniel Ragsdale, “Exploring a National Cybersecurity Exercise for Universities”, IEEE SECURITY & PRIVACY, Sep./Oct. 2005.

[2] Taek Lee, Dohoon Kim, Yeonkyun Shin, Seungyong Shin, and Hoh Peter In, “An Architecture of Virtual Security Training Laboratory for Cybersecurity Exercise”, Proceedings of The 30th Korea Information Processing Society Fall Conference, Vol.15, No.2, Pages:1462-1464, Nov. 2008.