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

(Markov Chain Model-Based Trainee Behavior Pattern Analysis for Assessment of Information Security Exercise Courses)

이 택 † 김 도 훈 †
(Taek Lee) (Dohoon Kim)
이 명 락 †† 인 호 †††
(Myongrak Lee) (Hoh Peter In)

요 약 본 논문에서는 정보보안 실습 훈련 과정 동안에 참여자들이 보이는 행동 패턴들을 관찰·분석하고 주어진 실습 미션의 성패를 결정짓는 행위 패턴을 추정하는 마코브 체인 행위 모델링 기법과 알고리즘을 제안한다. 제안 알고리즘은 미션의 성공에 가장 큰 공헌을 하는 행위 패턴은 어떤 것이고 반대로 실패를 유도하는 행위 패턴은 어떤 것인가를 분석 평가하는데 활용된다. 제안 방법의 적용 및 실효성 검증을 위해 사례연구로서 "불필요한 네트워크 서비스 차단"에 관한 미션 수행 데이터를 분석하였다.

키워드 : 행위 패턴 분석, 정보보안 실습, 평가 자동화

Abstract In this paper, we propose a behavior pattern analysis method for users tasking on hands-on security exercise missions. By analysing and evaluating the observed user behavior data, the proposed method discovers some significant patterns able to contribute mission successes or fails. A Markov chain modeling approach and algorithm is used to automate the whole analysis process. How to apply and understand our proposed method is briefly shown through a case study, "network service configurations for secure web service operation".

Key words : Behavior Pattern Analysis, Information Security Exercise, Evaluation Automation

1. 서 론

교육 및 실습 훈련은 사회공학적 취약점들을 이용하는 각종 정보보안 위협들에 대해 현실적으로 가장 능동적으로 대처할 수 있는 유일한 방법이다. 정보보안 훈련 프로그램은 학습자들에게 민감한 정보 자산들을 다루는 상황에서 자신들이 어떤 오류를 범할 수 있는지 인지시킬 수 있는 좋은 기회를 제공하며, 정보 보안 위험 관리를 위해서 과연 어떤 지식 기술이 부족한가에 대해 깨닫게 만들어주는 기회를 제공해준다. 훈련 프로그램에는 여러 형태가 있겠지만, 특히 실무 위주의 실습 수행을 통해 터득하는 훈련 내용이 가장 효과적인 것으로 보고된다[1].

일단 실습 훈련 세션을 완료하면 감독자는 실습 훈련 참여자들이 과연 할당된 미션을 성공적으로 수행하였는가 아니면 실패하였는가에 관해 평가해야 한다. 이 단계에서 감독자는 매우 중요한 정보를 얻게 된다. '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 패턴은 무엇인가?' 즉, 훈련 미션의 참여자들로부터 수집된 양질의 행위 분석 데이터로부터 분석가(감독자)는 이 같은 질문들에 대한 해답을 찾아낼 수 있다.

본 연구에서는 훈련 참여자들의 행위 패턴 관찰을 위해 가상 보안훈련장(Virtual Security Training Lab) 시스템을 이용하였다[2]. 해당 시스템은 훈련 참여자들에게 실제 리눅스 서버 시스템이 설치되어 있는 가상 실습 공간(가상 머신)을 제공한다. 동시에 미션 수행 도중 참여자들로부터 쉘을 통해 입력되는 모든 명령(행동)들이 관찰되고 기록된다. 미션 성패 여부에 대한 평가와 훈련 과정에 대한 행위 패턴 분석을 위해서 본 논문에

· 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0000142). 또한 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업' 지원비를 받았음
· 이 논문은 2010 한국컴퓨터종합학술대회에서 '정보보안 훈련 시스템에서 미션 성취도 평가를 위한 마코브체인 모델 기반의 학습자 행위 패턴 분석'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 고려대학교 컴퓨터전파통신공학과
comtaek@korea.ac.kr
karmy01@korea.ac.kr
†† 비 회 원 : 고려대학교 컴퓨터전파통신공학과
lmr2010@korea.ac.kr
††† 종신회원 : 고려대학교 컴퓨터전파통신공학과 교수
hoh_in@korea.ac.kr
(Corresponding author임)

논문접수 : 2010년 8월 10일
심사완료 : 2010년 10월 15일

서는 마코브 체인 모델(Markov Chain Model) 기반의 모델링 기법과 관련 분석 알고리즘을 제안한다. 해당 알고리즘은 시간의 흐름에 따라 관찰되는 행위 시퀀스를 하나의 체인 모형으로 보고 미션의 성공 및 실패 가능성을 확률적으로 추정 분류한다. 아울러 미션 성패에 가장 결정적 공헌(확률 결정에 대한 기여도 측면에서)을 한 행동 패턴도 찾아준다.

2. 관련 연구

정보보호 실습 교육을 위해 가상머신 관련 기술들[3-5]이 이용되고 있다. 가상머신 기술은 실습 교육의 현실성 증대와 실습 환경 재현과 유지관리의 편의성을 제공한다. 그러나 현재 이들 연구는 가상 실습 공간 제공에만 초점을 맞추고 있을 뿐 사용자들의 오류 발견과 실습 환경 개선을 위한 사용자-시스템 상호작용 분석은 제공하지 않는다.

그밖에 컴퓨터 기반 교육 지원 시스템 분야는 아니지만 사용자들의 행동 패턴들을 포착하고 이를 분석하는 기술은 시스템 사용자 세션 및 행위 모델링 분야[6,7]나 침입탐지 시스템 설계 분야[8,9]에서 활발히 연구되고 있다. 이들 연구는 일부 관찰 데이터를 이용해 시스템 사용자들을 개개인별로 식별[6,7]하거나 정상 사용자와 비정상 사용자를 분별[8,9]하는 것을 목표로 삼는다. 예를 들어 침입탐지 시스템 기술은 정상범주의 사용자 행동 샘플들을 모아 정상 행위 모델로 정의하고 주어진 테스트 케이스가 해당 모델에서 얼마나 벗어났는가(확률적으로 이질적인가)를 정량적으로 계산한다.

현재 저자들이 파악하기에 가상머신 실습 공간에서 사용자들의 행동패턴 분석과 실습 과정 평가를 위한 자동화 기술은 기존에 연구된 바가 거의 없다. 본 연구에서는 가상머신 기술은 실습 공간 제공의 역할을 함과 동시에 실습자들을 관찰 분석하여 교육 피드백을 제공할 수 있는 훌륭한 인프라가 될 수 있다는 점에 착안하여 실습자들의 행동 패턴을 분석하기 위한 기법을 제안하고자 한다. 관련 연구 분야와는 달리 사용자 분별을 위한 기법이 아니라 미션 성패에 영향을 미치는 행위 패턴들을 발견하기 위한 기법이다.

3. 행위 분석 모델의 설계

3.1 행위 체인의 다양성과 제한성

미션 수행 과정은 연속적인 의사결정들의 나열이라 할 수 있다. 훈련자들은 매 순간 적절한 행동을 선택하고 선택된 일련의 행동들이 모여 미션 수행 전 과정이 완성된다. 사례연구에서 보여줄 리눅스 보안 실습 미션도 마찬가지이다. 실습자들은 적절한 리눅스 명령어들을 입력하여 미션을 달성해나간다.

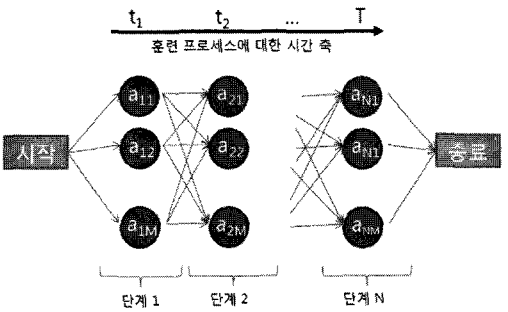

그림 1 훈련자의 동적 행위 모델

이러한 상황을 모델링한다면 그림 1과 같이 N 단계로 구성되는 동적 프로세스로 표현할 수 있다. 이때 N은 관찰 가능한 최대 길이의 행위 체인이라 가정 하자. 프로세스는 시간 축에 기반한 t_1에서 t_N까지의 의사결정 과정이라 할 수 있다. 매 단계에서 훈련자로부터 관찰 가능한 행동 상태 a의 종류는 모두 M개라 가정한다. 관찰 가능한 모든 경우의 수들로부터 다양한 패스가 발생할 수 있다. 결국 미션 성패 여부는 바로 훈련자에 의해 결정되는 특정 행위체인에 의해 결정된다.

3.2 마코브 체인 모델을 이용한 행위 체인 모델링

미션 수행 과정 중 훈련자는 다음 행동을 준비하기 위해 현재 행동을 취하는 것이고 다음 행동은 또 다시 다음 다음 행동을 준비하기 위해 취해지는 하나의 의사결정이라 할 수 있다. 이러한 반복 과정은 결국 궁극적인 최종 목표를 지향하며 이루어진다. 이를 정형화하기 위해 확률변수 X_t을 시간 t에서 훈련자가 취할 수 있는 어떤 행동이라 하자. 이때 시간 t = 0, 1, 2, …와 모든 행동 a에 대한 $P(X_{t+1}=a_{t+1}|X_t=a_t, X_{t-1}=a_{t-1}, \cdots, X_1=a_1) = P(X_{t+1}=a_{t+1}|X_t=a_t)$ 관계를 가정할 수 있다면 해당 이산 확률과정은 마코브 체인이라 정의된다. 즉, 시간 t+1에서 관찰되는 행동의 분포 확률은 현 행위 체인 상의 과거 행동들 간의 어떤 의존성과도 무관하게 단지 시간 t에서 관찰된 행동 확률에 의해서만 결정된다는 것을 의미한다. 마코브 체인 모델링에서는 시간 t에서 모든 행동 i와 j에 대해 $P(X_{t+1}=j|X_t=i)=p_{ij}$와 같은 확률을 정의하고 이를 전이확률(transition probability)라 칭한다. 행위 i가 관찰되고 바로 j가 관찰되었을 때 행동 i에서 j로 전이가 발생 하였다 말하고 확률 p_{ij}로 표시한다. 앞으로 p_{ij}확률 값을 요소로 갖는 i행 j열의 행렬을 ATM (Action Transition Matrix)라 명명한다. 당연히 ATM은 확률모델이기 때문에 관찰되는 행동 상태 a에 대해 다음과 같은 성질들을 갖는다.

$$p_{ij} = P(X_t = a_j \mid X_{t-1} = a_i)$$
$$p_{ij} \geq 0, \ \sum_{j=1}^{M} p_{ij} = 1 \qquad (1)$$

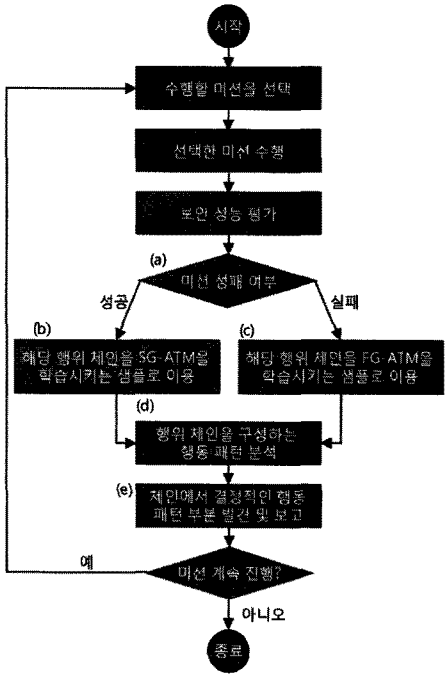

그림 2 ATM을 이용한 행위분석 과정

ATM은 행위 체인 전체나 체인을 구성하는 일부 행동 패턴들의 출현(관찰) 가능성을 추정하기 위해 이용된다. 미션을 마친 훈련 참여자들은 평가 결과에 따라 최종적으로 성공 그룹이나 실패 그룹 둘 중 하나로 분류된다(그림 2). 앞으로 SG-ATM은 성공 그룹(Success Group)에 속하는 훈련자 샘플들로부터 만들어진 ATM을 뜻하고(그림 2(b)), FG-ATM은 실패 그룹(Failure Group)에 속하는 훈련자 샘플들로 만들어진 ATM을 뜻하는 것으로 간주한다(그림 2(c)).

3.3 훈련 진행 도중 ATM을 생성하는 과정

ATM은 행렬 자체 내에 훈련 참여자의 행동 다양성 정보를 모두 내포한다. 그림 2는 이러한 ATM을 도출하는 방법과 ATM을 이용한 오류적인 행동 패턴을 발견하는 전체 과정의 흐름을 계략적으로 설명한다.

분석자(감독자) 입장에서는 당연히 SG-ATM이 미션 성공에 기여하는 행동 패턴 정보를 담고 있기 때문 FG-ATM보다 더 관심의 대상이 될 수 있다. 어떤 행위 패턴이 SG-ATM에서는 자주 발견되나 FG-ATM에서는 좀 처럼 발견되지 않는다면 바로 해당 패턴이 아마도 미션 성공에 공헌도가 큰 행동 패턴일 것이다. 반대로 FG-ATM에서는 발견되는데 SG-ATM에서는 발견되지 않는 패턴들이 있을 것이다. 이들은 바로 실패를 유발하는 오류적 행동 패턴들일 것이다.

그림 2에서 처리 단계(a)는 훈련자의 미션 성패를 결과 위주의 평가 방식으로 검사한 다음 현재 관찰된 행위 체인을 성공 샘플로 이용할 것인가 아니면 실패 샘플로 이용할 것인가를 분별한다. 마코브 체인 모델은 지도 학습 알고리즘(supervised learning algorithm)에 속하기 때문에 분류 결과(성공 또는 실패) 정보를 미리 알고 있는 샘플들을 통해 모델이 기계 학습된다. 그런데 ATM을 학습시키는 과정 중에 해결해야 할 중요한 문제들이 다음과 같이 발생한다.

- 행동 범위를 한정하는 문제: 매 단계에서 관찰될 수 있는 행동(action state)의 범위에 따라 2차원 행렬 형태인 ATM의 사이즈가 결정된다(그림 1에서 M값). 사이즈는 곧 구해야 하는 확률 값의 수를 M^2 만큼 증가시킨다. 행동 범위 모델링 단계에서 관찰 가능한 상태를 어느 정도로 한정하고 축약 할 것인가는 중요한 문제다.
- 유사 행동의 인코딩 동일화 문제: 간혹 관찰되는 행동들이 유사한 경우 이를 서로 다른 종류로 판단하는 것이 아니라 의미론적으로 동일하다면 하나의 행동으로 축약화하여 인코딩할 필요가 있다(예: 리눅스 에디터 명령 vi, vim, pico 등).
- ATM 구성 확률값 도출 문제 : 일단 ATM의 차원이 결정되면 다음으로 시간의 흐름에 따라 관찰되는 일련의 행동들로부터 행동과 행동 사이의 전이확률 값을 구하여 ATM을 구성해야 한다(그림 2(b),(c)). 예를 들어 시간 T까지 관찰된 훈련자의 행위 체인이 $O = o_1o_2o_3\cdots o_t\cdots o_T$ 라 하자. 여기서 $o \in A = \{a_1, a_2, \cdots, a_M\}$를 의미한다. 먼저 임의의 행렬 U를 정하고 구성 요소 u_{ij} 값은 행위 체인 O상에서 행동 $o_{t-1}=a_i$가 관찰되고 바로 이어서 $o_t=a_j$가 관찰되는 모든 경우를 셈하여 정한다. 결국 2.2절에서 소개한 특성 조건들 식 (1)이 만족하도록 행렬 U를 이용해 ATM을 유도해낸다.

즉, 구성 요소 p_{ij}는 $p_{ij} = u_{ij} / \sum_{j=1}^{M} u_{ij}$ 로 정의된다. 여러 훈련자들로부터 계속 관찰되는 학습 샘플 용도의 행위 체인을 수용하여 새롭게 확률 값을 재계산하기 위해 행렬 U를 갱신해야 한다. 새로운 샘플로부터 얻어진 임의의 행렬 U_{new}를 가정하자. 지금까지 계산해온 행렬은 U_{pre}로 칭한다. 결국, 행렬 ATM을 새롭게 계산하기 위한 행렬 U는 $U=U_{pre}=U_{pre}+U_{new}$로 누적해서 다시 정의된다. 그림 2의 반복 과정을 통해 U가 계속 갱신되고 더불어 이를 바탕으로 ATM 모델이 계속 학습된다.

4. 미션 성공에 결정적인 행동 패턴 발견

만약 어떤 임의의 행위 체인 O가 주어지고 해당 체인이 성공 그룹에서 관찰될 가능성을 추정하고자 한다면 다음과 같은 식 (2)를 이용하면 된다. 실패 그룹(FG-

ATM)에 대해서도 마찬가지이다.

$$P(O|SG-ATM) = P(o_1, o_2, ..., o_T)$$
$$= P(o_1)P(o_2|o_1)P(o_3|o_2,o_1)...P(o_T|o_{T-1},...,o_1)$$
$$= P(o_1)P(o_2|o_1)P(o_3|o_2)...P(o_T|o_{T-1})$$
$$= P(o_1)\prod_{i=1}^{T-1}P(o_{i+1}|o_i) \quad (2)$$

예를 들어 어떤 테스트 케이스 행위 체인 O가 주어졌을 때 각각 P(O|SG-ATM)과 P(O|FG-ATM) 값들을 구하고 이 둘을 비교하여 어느 쪽이 더 큰 확률 값을 갖는가를 기준으로 미션 성공과 실패의 가능성을 추정할 수 있다. 만약 주어진 행위 체인 O가 성공의 가능성이 높은 것으로 진단되었다면 과연 O를 구성하는 어떤 행동 패턴 부분이 성공을 결정하는데 가장 큰 공헌을 하였는가를 세부적으로 파악할 수도 있다. 반대로 실패 그룹으로 분류될 가능성이 높다면 도대체 어떤 오류적 행동 패턴 때문에 실패로 분류되었는가를 세부적으로 추적할 수 있다.

표 1 행위 패턴 분석 알고리즘

```
1   C[T]: 분류결과 저장을 위한 행렬
2   W[T]: 전환점 기록을 위한 행렬
3   G[T]: pSG 와 pFG 사이 확률 차를 기록하는 행렬
4
5     C[T], W[T], G[T] 초기화
6     for each t from 2 to T {
7        O=o1o2 … ot 행위체인 획득
8        pSG ← P_SG-ATM(o1)∏ P_SG-ATM(oi+1|oi)
9        pFG ← P_FG-ATM(o1)∏ P_FG-ATM(oi+1|oi)
10       if  pFG > pSG  then {
11            C[t]←' FG' , G[t] ← pFG / pSG
12            if C[t-1] is not equal to C[t] then {
13              W[t] ←' fromSGtoFG'  }
14            } elseif  pFG < pSG {
15               C[t]←' SG' , G[t] ← pSG / pFG
16               if C[t-1] is not equal to C[t] then {
17                  W[t] ←' fromFGtoSG'  }
18    }}}
19    C[T], W[T], G[T]에 기록된 부분들을 세부 분석
```

어떤 행위 체인이 주어졌을 때 체인을 구성하는 행동 시퀀스 정보를 이용하여 미션의 성패 여부를 추정하고 결과의 결정적 전환점을 찾아내는 과정이 알고리즘 표 1에 설명되어 있다. 알고리즘 표 1의 행1에서 3까지는 알고리즘의 중간 결과들을 저장하기 위해 준비된 1차원 행렬들이다. 행렬 $C[T]$는 현재까지 입력으로 들어온 행위 체인 정보에 의존해 분류된 결과 SG 또는 FG를 기록한다. 예를 들어 $C[t]$가 FG로 기록되었다는 것은 시간 t 지점까지 관찰된 행동 패턴만으로 볼 때 해당 행위 체인은 실패 그룹으로 분류될 가능성이 높다는 것을 의미한다. $W[T]$는 확률적 진단 결과가 결정되는 전환점 부분을 기록하는 행렬이다. 즉, $C[T]$ 상에서 갑자기 기록 결과가 …FG→FG→SG…로 돌아서거나 …SG→SG→FG…로 돌아서는 전환점들을 파악한다. $G[T]$는 미션 성패를 진단할 때 기준이 되는 확률 값의 차이를 의미한다. 다시 말해, p_{SG}과 p_{FG} 사이의 확률 비율 차를 기록한다. $G[T]$를 참고하여 결과 분류를 결정하는 확률 차가 얼마나 큰 차이인가 미묘한 차이인가를 확인 할 수 있다. 행8과 9에서 p_{SG}와 p_{FG}는 지금까지 관찰된 행위 체인이 각각 SG-ATM과 FG-ATM에서 발생할 확률 값을 저장한다.

5. 사례연구

실험 데이터는 가상보안훈련장 테스트베드 시스템[2]을 이용하여 추출하였다. 실습 실험을 위해 참여자들은 "리눅스 시스템을 웹 서버 전용으로 꾸미기 위해 현재 실행중인 네트워크 서비스들 중 불필요한 서비스를 찾아 차단하라"는 미션을 할당 받았다. 훈련 참여자들은 원격 접속이 가능한 가상 머신(우분투 7.10 리눅스 설치) 실습공간에서 주어진 미션을 수행하였다.

주어진 미션을 수행하는 과정에서 참여자들은 그림 3과 같은 행동(명령어) 분포를 보였다. 그림 3의 왼쪽 표(a)는 관찰된 명령어들을 분류하고 행동 상태(action state)로 인코딩하기 위한 매핑 룰을 의미한다. 즉, 그림 1의 M값은 여기서 14로 정해지고 결국 ATM의 크기도 14×14 행렬로 정해진다. 그리고 그림 3의 오른쪽 그래프(b)는 관찰된 명령어들의 빈도 분포를 의미한다. 명령어 a3, a13, a14는 실습 작업 도중 가장 흔하게 이용되는 명령어들이기 때문에 빈도수가 상대적으로 높았으며 분석 이후 SG-ATM과 FG-ATM 모두에서 똑 같이 고르게 관찰되었다. 따라서 빈도수는 높았지만 미션의 성패 여부를 결정하는 영향력 있는 행동(명령어)들은 아니라는 것을 파악할 수 있었다.

예를 들어 어떤 행위 체인 $O=o_1o_2\cdots o_7$가 o_1=a1, o_2=a7, o_3=a3, o_4=a2, o_5=a4, o_6=a5, o_7=a1와 같이 주어졌다고

(a) 관찰 명령어들에 대한 인코딩 룰

명령어	상태 코드	관찰수
lsof, netstat	a1	3
cd /etc/init.d	a2	2
ls	a3	23
sshd stop	a4	3
vsftpd stop	a5	2
man	a6	2
ps	a7	10
kill sshd	a8	1
kill vsftpd	a9	1
cat xinetd	a10	1
clear	a11	5
kill ?	a12	1
cd ?	a13	27
etc.	a14	23

(b) 관찰 명령어들의 히스토그램

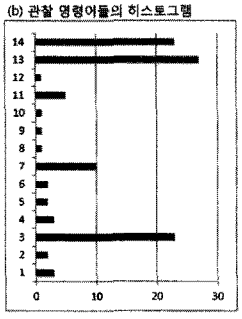

그림 3 미션 수행 도중 관찰된 명령어 집합

표 2 실습 행위 체인 분석 결과

관찰 행위 체인		a1 →	a7 →	a3 →	a2 →	a4 →	a5 →	a1
SG-ATM에서 p_{ij}		0.2	0.06	0.06	0.03	0.06	0.12	0.13
FG-ATM에서 p_{ij}		0.2	0.07	0.05	0.05	0.07	0.07	0.07
누적 체인 확률	p_{FG}		0.01176	0.00069	2.4E-05	1.5E-06	1.8E-07	2.2E-08
	p_{SG}		0.01429	0.00071	3.2E-05	2.3E-06	1.7E-07	1.2E-08
분류 결과 C[T]			FG	FG	FG	FG	SG	SG
확률차 G[T]			1.21	1.03	1.36	1.55	1.06	1.85

가정하자. 이때 표 2는 표 1의 알고리즘을 통해 도출된 해당 행위 체인의 분석결과를 보여준다.

$C[T]$에 대한 분류 결과 행에서 보여지듯이 궁극적으로 성공 그룹으로 분류되는 결정적인 행동 패턴 전환점은 o_5=a4→o_6=a5 지점인 것을 확인할 수 있다. 최종 의사결정 확률 차 $G[T]$ 또한 1.85배로 가장 높았다. 결론적으로 해당 행위 체인 O는 성공 사례로 분류될 가능성이 실패 사례로 분류될 가능성에 비해 1.85배로 더 높게 추정되었다. 행위체인 상에서 o_5→o_6는 전환점으로 기록되었으며 o_5→o_6와 o_5→o_6는 미션을 성공으로 이끈 가장 영향력 있는 행동 패턴이었다. 이러한 패턴들에 등장하는 행동들 'sshd stop', 'vsftpd stop', 'ps'는 실제 실험에서도 결정적인 열쇠 역할을 하는 명령어들인 것으로 밝혀졌다.

6. 결론 및 향후 연구

본 논문에서는 정보보안 실습 훈련 프로그램에서 훈련 참여자들의 훈련 과정을 관찰하고 행동 패턴들을 분석 하기 위한 ATM 행렬과 관련 분석·평가 알고리즘을 제안하였다. 이는 꼭 보안 분야뿐만 아니라 미션에 의해 주도적으로 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.

만약 본 논문에서 제안되는 분석 방법을 실제 가상보안훈련장 시스템의 분석·평가 기능으로 구현하여 제공한다면 시스템 이용자 다수의 훈련 수행 내용 평가 과정을 보다 효율적으로 자동화 할 수 있을 것이다. 아울러 훈련장 시스템으로부터 실시간 모니터링 되는 훈련자들의 행위 데이터를 소스로 하여 행위 평가를 실시간으로 수행하여 오류적 행위에 대해 즉각적인 온라인 피드백(예: HCI형태의 알림/경고)을 제공한다면 매 순간 자신들이 내려야 하는 의사결정을 좀 더 신중하게 할 것이고 행동 교정 효과가 나타날 것이다.

향후 연구에서는 이러한 추가 분석과정과 함께 3.3절에서 거론한 주요 세가지 문제를 개선하기 위한 심도 있는 연구가 계속 진행되어야 한다. 본 논문에서는 실습 훈련자의 행위 분석을 위한 기본적인 아이디어를 제안하였고 하나의 적용 사례 연구를 보였다. 제안 모델의 고도화와 모델 정확도 및 신뢰성 확보를 위해 사례연구의 확대와 다수의 샘플 확보가 더욱 필요하다.

참 고 문 헌

[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, pp.1462-1464, Nov. 2008.

[3] Ji Hu, Christoph Meinel, and Michael Schmitt, "Tele-lab IT security: an architecture for interactive lessons for security education," *Proceedings of the 35th SIGCSE technical symposium on Computer science education*, 2004.

[4] Jeremiah K. Jones and Gordon W. Romney, "Honeynets: an educational resource for IT security, *Proceedings of the 5th conference on Information technology education*, 2004.

[5] Online information security e-learning center (http://www.sis.or.kr)

[6] Alfredo Milani, Judit Jasso, and Silvia Suriani, "Modeling Online User Behavior," *IEEE International Conference on e-Business Engineering*, pp.22-24, Oct. 2008.

[7] Jose A. Iglesias, Plamen Angelov, Agapito Ledezma, and Araceli Sanchis, "Modeling Evolving User Behaviours," Evolving and Self-Developing Intelligent Systems, 2009.

[8] Ashish Garg, Ragini Rahalkar, Shambhu Upadhyaya, and Kevin Kwiat, "Profiling Users in GUI based Systems for Masquerade Detection," *IEEE Information Assurance Workshop*, pp.48-54, 2006.

[9] Debin Gao, Michael K. Reiter, and Dawn Song, "Behavioral Distance for Intrusion Detection," *RAID 2005*, LNCS 3858.