속성기반 위협문장 생성 모델

최 승, 최상수, 이강수
한남대학교 컴퓨터공학과

Attribute-Based Threats Statement Generation Model

Seung-Choi, Sang-Soo Choi, Gang-Soo Lee
Dept. of Computer Engineering, Han-Nam University

요 약

PP/ST의 보안환경 개발은 정보보호제품에 대하여 이력서라고 할 수 있다. 이에 기존의 위협문장 생성모델을 개선하여 속성기반 위협문장 생성모델을 제시한다. 본 모델은 PKB의 속성들을 이용하여 위협문장 생성시 각 항목(주어, 목적어, 동기, 동사, 결과)에 속성을 추가·확장하여, 문장이 컨텐츠 뿐만 아니라 특수성을 갖게 된다. 본 논문에서 제시된 모델은 PP/ST 개발시 위협문장을 생성할 때 활용될 수 있다.

1. 서론

현대사회는 정보통신 기술의 발달로 인하여 인간의 삶의 질(quality)이 어느 때보다 높아 졌다. 하지만, 정보화의 역기능으로 인해 IT제품 특히, 정보보호제품에 대한 성능 및 신뢰성 평가가 중요시되고 있다.

이에 IT제품의 선진국인 미국, 영국, 독일, 프랑스, 캐나다, 네덜란드 등 6개국이 각 나라마다 별도로 존재했던 평가기준을 통합 수용할 수 있는 IT 보안성 평가기준인 "공통평가기준(CC,common critiera)"을 개발하여, 1999년 6월에 국제표준(ISO/IEC 15408)으로 채택되었고, 현재 버전 2.2가 개발되어 공개된 상황이다.

CC는 기능요구사항과 보증요구사항으로 구성되어있고, 기능요구사항의 일부를 선택하여 7수준의 보안수준 중 하나를 택하여 제품 유형별 공통보안기능요구사항인 PP(protection profile)와 특정한 정보보호제품에 대한 보안기능요구사항명세서인 ST(security target) 및 평가대상물(TOE ,target of evaluation)을 개발을 한다.

PP/ST에는 TOE를 사용하려는 환경상의 보안성과 적용하고자 하는 방법상의 보안성을 설명해야 하는 TOE 보안환경 구성요소가 포함되어 있다[1,2]. 보안환경에는 가정사항, 위협, 조직의 보안정책의 세부분으로 구성된다. 특히, 위협은 시스템 또는 조직에 피해를 초래할 수 있는 원하지 않는 사건의 잠재적 원인으로 보안에 해를 끼치는 행동이나 사건 또는 자산에 손실을 발생시키는 행동이나 사건을 말한다[3].

PP/ST 중 IT 보안요구사항을 이끌 수 있는 보안목적과 매핑이 되는 '보안환경' 부분의 개발은 정보보호제품에 대한 이력서라고 할 수 있다. 즉, 보안환경이 정밀하게 개발되었다면, 정보보호제품의 기능이 최적으로 발휘될 수 있다.

이에 본 논문에서는 보안환경 중에서 위협문장을 생성할 때, 특수성, 용이성, 구체성, 측정성, 명확성 및 일관성을 갖기 위해 속성기반 위협 문장 생성 모델을 제시한다.

먼저 2장에서는 이전 연구의 위협문장 생성 모델에 대해 알아보고, 3장에는 속성기반 위협문장 생성모델을 제시하고, 4장에서는 사례를 보이며, 5장에서는 결론을 맺는다.

2. 이전 연구 : 위협문장 생성 모델

본 연구팀은 일관성과 정형성이 있는 위협문장을 생성(구성)하기 위하여 위협 문장 생성모델을 제시한바 있으며[4], 그림 1과 같이 '*주어(위협원)*', '*목적어(자산)*', '*동사*

본 연구는 과학기술부 지역협력연구사업(과제번호 : R12-2003-004-01001-0) 연구비지원에 의하여 수행되었음

<위협문장> ::= <주어> "가" + <목적어> "를" + <동사> "한다" + <영향> "결과로서 …을 손상시킨다."
<주어> = <위협원(treat agent)> ::= 시스템관리자 | 인가사용자 | 악의적개인 | 물리적 환경 | 개발자 | 시스템 | 자연재해 | …
<목적어> = <자산(Asset)> ::= 시스템 | 정보 | SW | HW | 인간 | …
<동사> = <공격방법(threat method, scenario)> = 삽입 | 삭제 | 변경(쓰기) | 방해 | 엿보기 | …
<기타> = <피해결과> ::= 기밀성 손상 | 무결성 손상 | 가용성 손상 | 책임성손상

그림 1. 위협문장 생성규칙

(공격방법)', '기타(피해결과)'로 규칙에 따라 위협문장이 생성되고, 위협문장 생성모델에 '위협원수×자산수×동기수×공격방법수×결과수' 만큼의 문장이 생성된다. 즉, 2240 가지의 위협문장이 생성된다.

이 생성알고리즘은 문맥, 즉 문장의 각 항목(주체, 객체, 동기, 방법, 결과)에 따라 의미가 달라진다. *'악의적 개인'* 이 어느 정도의 강도가 있는지, *'인가 사용자'*가 어느 정도의 권한이 있는지는 표현하기가 어렵다. 또한, 생성된 문장만으로 그 위협을 파악하기에도 무리가 있다. 따라서 본 논문에서는 기존 위협문장 생성 모델의 각 항목에 속성을 추가·확장하여, 속성기반 위협문장 생성 모델을 제시한다.

3. 속성기반 위협문장 생성 모델

본 장에서는 PKB의 속성을 분석하여 기존 위협문장 생성 모델에 적용, 확장한다. 이에 본 논문에서는 속성을 '값을 갖고 구성요소의 특성이나 다른 구성요소와 구별할 수 있는 특징을 갖는 것'으로 정의를 한다.

3.1 PKB 속성 분석

위협 문장의 속성들을 분석하기 위해 다음과 같이 PKB 속성들을 분석하였다.

PKB에서는 에이전트(에이전트 타입, 인증, 태도, 동기, 정교성, 지역성, 환경), 방법(생명주기단계, 인간역할, 행동, 취약성), 결과(손실타입, IT기능, 위치, 보안기능)를 속성(Attribute)으로 정의하고 있다[5].

그림 2와 같이, 속성들을 다시 일반속성(General attribute)과 세부속성(Detailed attribute)으로 정의·분류하고, 각 속성들을 특징 질 수 있는, 예컨대, *'에이전트 타입'* 세부속성에는 *'인간', '인간 이외'*라는 특징을 갖고 있다. 이 특징을 속성 값(Attribute Value)으로 정의한다. 즉, 각 일반속성에는 한 개 이상의 세부 속성이 있고, 각 세부 속성에는 한 개 이상의 속성 값이 존재한다. 예를 들면, 일반속성 *'결과'*는 세부속성 *'손실타입', 'IT기능'* 및 *'위치'*가 있고, 세부 속성 *'위치'*에는 *'모든 위치', '환경', 'TOE', '해당없음'*의 속성값이 있다.

일반속성= {'에이전트', '방법', '결과'}
세부속성= {'에이전트_타입', '인증', '태도', '동기', '정교성', '지역성', '환경', '생명주기단계', '인간역할', '행동', '손실타입', 'IT기능', '위치'}
속성 값 = {'인간', '인간 이외', '인증된', '특권이 있는', '식별된', 'None', '우연한', '신중한', '심사숙고한', '건설적', '악의적', '부주의', '상', '중', '하', '제로', '모든 위치', '로컬', '원격', '통신', '재해', '누설방사', '전력', '색다른 주위 상황', '모든 단계', '개발 단계', '운영 단계', '배치 단계', '임무 없음', '서비스 사용자', '시스템 임무', '모든', '가용성', '기밀성', '무결성', '보안 보호', '독단적 기능', '시스템', '사용자 데이터', '사용자 처리', '모든 위치', '환경', 'TOE'}

그림 2. 일반속성, 세부속성, 속성 값

3.2 속성기반 위협문장 생성 모델

본 절에서는 3.1절에서 분석된 PKB 속성을 이전 연구에서 제시한 위협문장 생성 모델에 적용한다.

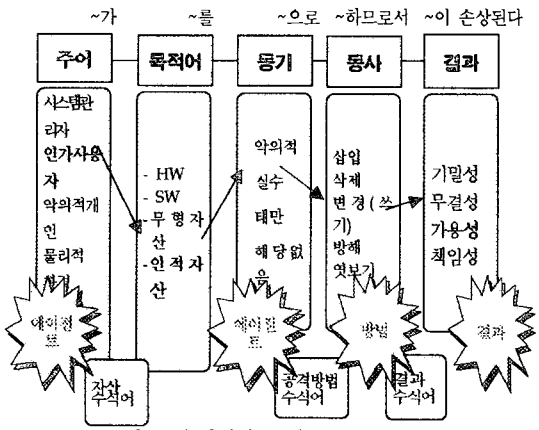

그림 3. 속성기반 위협문장 생성 모델

그림 3과 같이 기존 위협문장 생성 모델을 PKB에서 정의된 속성들을 추가·확장한다. 즉, *'주어(주체, 위협원)+PKB(에이전트)', '동기+PKB(에이전트)', '동사(공격방법)+PKB(방법)', '결과(영향)+PKB(결과)'*로 한다.

구체적으로 주어 항목은 그림 4와 같이 기존 모델에 일

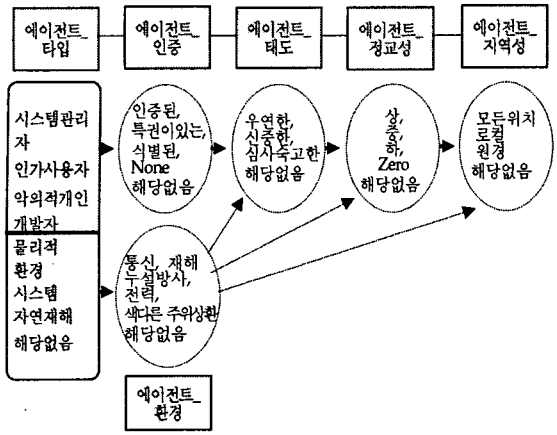

그림 4. 주어 확장, 추가 및 생성 프로세스

반_세부_속성 값을 추가한다. 여기에서 실선 화살표는 직접적인 생성 프로세스를 보이며, 점선 화살표는 간접적인 프로세스를 보인다.

예를 들면, 악의적 개인을 주어로 선택하면, 에이전트 타입은 '*인간*', 인증은 '*없고*', 태도는 '*신중한*', 정교성은 '*중*', 지역성은 '*원격*'의 속성을 가질 수 있다. 즉, 악의적 개인은 '*인증이 없는 인간이면서 공격의 강도가 신중하고, 중 정도의 능력이 있으며, 원격에서 공격을 가한다*'는 *속성*을 갖게된다.

생성 모델의 동기, 동사, 결과는 그림 5~7과 같다.

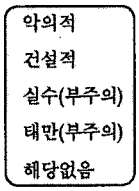

그림 5. 동기 확장

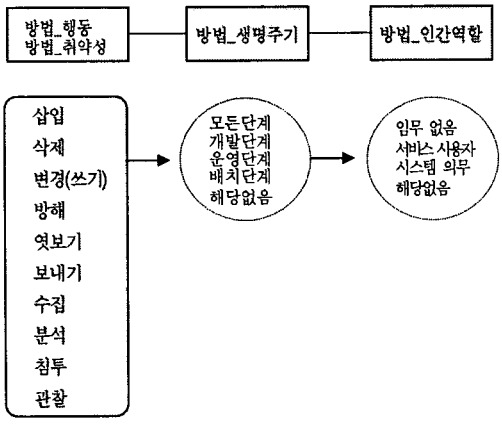

그림 6. 동사(공격방법)확장, 추가 및 생성프로세스

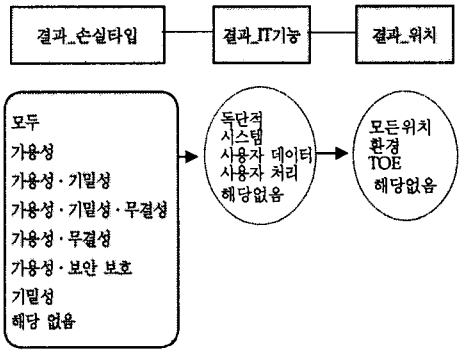

그림 7. 결과(영향) 확장, 추가 및 생성 프로세스

속성기반 위협문장 생성 모델은 다음과 같은 특징을 갖는다.

- 특수성 : 문장의 컨텐츠 기반이 아닌, 켄텐츠에다 속성을 추가함으로써 문장이 특성을 갖게 된다.
- 용이성 : 속성기반 위협문장으로 생성된 문장은 PP/S T 개발시에 쉽게 적용할 수 있다.
- 구체성 : 8×4×4×10×7 = 8,960가지의 위협문장이 생성된다.
- 측정성 : 속성 중 '태도', '동기', '정교성'으로 위협원(해커)의 공격 강도를 측정할 수 있다.
- 명확성 : 위협문장이 명확해진다.

4. 사례 연구

속성기반 위협문장 생성모델로 표 1과 같이 문장을 생성하고, 속성값을 선택하였다. 이 문장은 그림 8과 같이 기존 PP중 T.ATTACK_DATA와 관련이 있고, PKB 위협문장 중 T.Hack_Prcsr_OverLoad와 대응이 된다.

<생성 문장>
악의적 개인이 인적자산을 악의적으로 삭제하여 가용성이 손상된다.

표 1. 사례 문장과 속성

항 목	문 장	속 성(세부속성 : 속성값)
주어	악의적 개인	에이전트 타입 : 인간 인증 : None 태도 : 신중함 정교성 : 중 지역성 : 해당 없음
목적어	인적자원	·
동기	악의적	악의적
동사	삭제	생명주기단계 : 운영단계 인간역할 : 해당없음
결과	가용성	손실타입 : 가용성 IT 기능 : 해당 없음 위치 : 해당 없음

- PP 명 : A Goal VPN PP For Protecting Sensitive information
  위협문장 : T.ATTACK_DATA(TOE 인가자 또는 비인가자가 악의 있는 코드를 사용하여 TOE 혹은 사이트 보안운영을 중단시킬 수 있다[6].)
- PKB 위협 문장
  T.Hack_Prcsr_OverLoad(해커가 시스템 작업 과부하를 야기하여 서비스거부를 초래할 수 있다[5].)

그림 8. 사례문장과 관련된 위협 문장

5. 결론

본 논문에서는 기존 위협문장 생성 모델을 확장하여 속성기반 위협문장 생성 모델을 제시하였다. 본 모델은 PKB의 속성들을 이용하여 위협문장 생성시 각 항목(주어, 목적어, 동기, 동사, 결과)에 속성을 추가·확장하였다. 또한, 사례를 통해, 생성된 문장과 기존 PP와 PKB의 관련된 위협문장을 보임으로써, 본 모델로 생성된 위협문장은 기존 위협문장과 상관 대응됨을 보였다.

제시된 모델은 특수성, 용이성, 구체성, 측정성 및 명확성의 특성과 일관성을 갖고 있기 때문에, PP/ST개발시 위협문장을 생성할 때 활용될 수 있다.

그러나, 본 모델을 이용하여 개발된 PP/ST 유효성 검증이 필요하고, 위협문장 뿐만 아니라 정책 및 가장사항에 대한 추가적인 연구가 진행되어야 할 것으로 사료된다.

[참고 문헌]

[1] CC, Common Criteria for Information Technolog y Security Evaluation, Version 2.1, CCIMB-99-0 31, August 1999, http://www.commoncriteria.org/site_In dex.html.

[2] 정보통신부, 한국정보보호진흥원, 정보보호시스템 공통평가기준(정통부고시 제 2003-52), 2003.11.4

[3] ISO/IEC PDTR 15446, "Information technology - Security techniques - Guide for the production of protection profiles and security targets", Draft, November 12, 2003.

[4] 고정호, 이강수, PP의 보안환경을 위한 위협문장 생성 방법, 한국전자거래학회지, 제 8권 3호, 2003년 8월.

[5] NIAP, List of Threat, Attack, Policy, Assumpti on, and Environment Statement Attribute, CC Pr ofiling Knowledge base Report, 2002, http://niap.nist.gov/tools/CCTB60f-Documentation/CC_ PKB/ Reports /Index.htm.

[6] Networking, PP-026, A Goal VPN Protectoin Profile For Protecting Sensitive Information-v2.0, D raft, 10 July, 2000.