2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

보안 시스템 평가를 위한 정형화 도구 리스트와 가이드 라인[1]

이지연[1], 유희준[1], 최진영[1], 남윤순[2]
고려대학교 컴퓨터학과 정형기법 연구실[1], 한국정보보호센터[2]
e-mail : {jylee,hyoo, choi}@formal.korea.ac.kr
namy@kisa.or.kr

Endorsed Tools List and Guideline for high-level security system evaluation

Ji-Yeon Lee[1], Hee-Jun Yoo[1], Jin-Young Choi[1], Yun-Sun Nam[2]
Dept. of Computer Science and Engineering, Korea University[1]
Korea Information Security Agency [2]

요 약

현대 사회는 정보통신 기술의 발달로 정보 시스템의 사용이 급격히 증가 되고 있다. 정보화의 가속화에 따라 다양한 역기능들 또한 도출되고 있다. 여러 가지 역 기능들로부터 정보를 보호하고 안정한 정보 유통을 위한 양질의 정보보호 시스템을 위해 정보보호 제품에 대한 평가를 수행하고 있다. 각국의 평가 등급을 살펴 보면, 정형기법을 사용한 시스템이 높은 등급을 받고 있다. 특히, 미국의 평가 등급인 TCSEC 을 관리하는 NIST 에서는 최상위 등급을 받기 위해서는 정형화 시스템을 사용해야 한다. 이를 위해 미국에서 시행하고 있는 승인된 TOOL 리스트와 이 리스트에 포함되기 위한 평가와 가이드 라인을 분석하여 현재 사용하고 있는 tool 들을 평가해보고 국내 실정에 맞는 최고 등급 평가에 사용될 수 있는 검증 받은 도구 리스트와 가이드라인의 초안을 제시하고자 한다.

1. 서론

현대 사회는 정보통신 기술의 발달로 정보 시스템의 사용이 급격히 증가 되고 있다. 정보화의 가속화에 따라 다양한 역기능들 또한 도출되고 있다. 인터넷 등 정보 통신망에 대한 취약성 및 위험이 가중되고 있고 정보 유출, 파괴, 정보 위,변조 등의 컴퓨터 범죄와 해킹 급증, 바이러스 감염, 서비스 방해 , 불건전 정보 유통 등 정보화 역기능이 확산 되고 있는 추세로 체계적이고 총체적 정보보호 대책이 필수로 요구되고 있다[2]. 컴퓨터 범죄로부터 정보를 보호하고 안전한 정보 유통에 의한 정보화를 촉진하고, 보안성, 신뢰성이 검증된 양질의 정보보호 시스템을 보급함으로써 효율적인 정보보호 체계를 구축하고, 다양한 정보보호 시스템 수요 및 시장을 창출해서 정보보호 산업을 육성하기 위해 정보보호 제품에 대한 평가가 요구되고 있다. 현재 우리나라에서 사용하는 평가제도는 제품의 기능과 품질에 따라 이들을 7 개의 등급으로 나누어 인증하는 방법을 사용하고 있다. 이 중 최상위 등급인 K7 에서는 보안정책의 정형화 모델과 일치되도록 정형화된 보안 기능을 기술하고 원시 프로그램과 정형화된 기능명세서 사이의 일치성 검증을 요구하고 있다. K7 등급은 최고의 보안 기능이 보장되어야 함으로 그에 따르는 요구사항과 거기에 사용되는 정형화 tool 들데 대한 기준이 따로 정의될 필요가 있다. 지금 현재 미국에서는 최상위 등급인 A1 을 받기 위해 사용하는 정형화 시스템을 위한 승인된 tool 리스트와 가이드 라인이 정해져 있다. 최상위 등급을 받는 보안 시스템을 위해서는 그 기능을 검증할 수 있는 정형화 시스템의 기능 또한 검증 되어야 한다. 우리나라에서도 K7 등급을 받기 위해 요구되는 정형화 시스템에 대해서 정확한 기준과 가이드 라인을 정하고 이를 평가의 기준으로 사용해야 한다[6]. 이를 위해 인정할 수 있는 정형화 시스템에 대한 기준이 정해져서 개발자들이 이를 알고 사용할 수 있게 해야 한다. 하지만 우리나라는 이런 기준들이 아직 미비한 실정

[1] 본 연구는 2000년도 한국정보보호센터의 지원을 받은것이다.

이다. 본문에서는 미국에서 시행하고 있는 승인된 TOOL 리스트[3]와 이 리스트에 포함되기 위한 평가와 가이드 라인[1]을 분석하여 국내 실정에 맞는 최고 등급 평가에 사용될 수 있는 가이드라인을 제시한다. 현재 NIST 에서 제공하는 ETL 은 최근에 나와있는 도구에 대해서 언급을 하고 있지 않다. 따라서 여기서는 최근 많이 사용되고 있는 정형 도구를 ETL 의 조건에 만족하는 지를 검사해서 ETL 을 확장해 보려고 한다. 본 논문의 구성은 2 장 A1 등급을 받기 위해 필요한 정형화 시스템 평가 리스트와 평가 받기 위한 가이드 라인을 소개하고 3 장에서는 몇몇 정형도구들이 NIST 에서 제시한 ETL 에 추가될 수 있는 조건을 만족하는 지에 대해서 살펴보고 4 장에서 결론을 맺겠다.

2. ETL 평가 방법

TCSEC(Trusted Computer System Evaluation Criteria)와 TNI(Trusted Network Interpretation) 는 보안 요구사항의 세가지 타입을 지원하기 위해서 시스템을 특징과 보증에 기반을 두고 7 개의 계층으로 분류한다. 정책, 책임, 보증.. 보증 요구 사항 중 하나인 디자인 명세와 검증은 TCSEC 와 TNI 의 상위 계층에서 나타난다. 가장 높은 신뢰 등급, A1 은 모순이 없도록 시스템을 위한 정형화 보안 정책 모델로의 명세를 요구한다.
이런 평가 단계에서 사용되는 ETL (Endorsed Tools List) 은 NCSC (National Computer Security Center)가 일정한 절차와 기준에 따라 승인한 정형화 시스템의 명단을 작성해 놓은 것으로, 시스템 개발자들에게 A1 후보시스템의 디자인에 사용되기 위해서 NCSC 에 의해 승인한 정형화 명세와 검증 tool 을 알리기 위해 작성된다.
ETL 에 부가나 삭제는 NCSC 의 결정과 같은 필요에 따라 일어난다. 강요된 이유는 ETL 에 있는 검증 tool 의 부가사항을 정당화 하기 위해 존재해야한다. 제안된 tool 은 tool 의 현재 set 에서 제공하지 않는 충분한 기능을 제공해야만 한다.

이런 평가의 과정을 거치기 위해서 NCSC 의 ETL(Endorsed Tools List) 의 후보인 정형 검증 시스템에 필요한 조건들을 설명하는 가이드 라인이 존재한다. 이 가이드 라인은 NCSC 의 ETL(Endorsed Tools List) 의 후보인 정형 검증 시스템에 필요한 조건들을 설명한다. 검증 시스템의 NCSC 승인을 위해 필요한 조건은 TCSEC 와 TNI 에서 정해진다. TCSEC 와 TNI 는 각각 자동화되었던 정보와 네트워크 시스템에 추가되는 보안 통제들을 평가하기위해 사용된 표준들이다. ETL 을 위한 평가는 다음 세가지 종류이다 . (1) ETL 에 포함되기를 원하는 새로운 검증 시스템에 대한 평가. (2) 이미 ETL 에 포함된 시스템의 새로운 버전에 대한 재평가. (3) ETL 에서 삭제 시키기 위한 재평가. 와 같은 세 종류의 평가가 이루어 진다.
(1)의 평가의 경우, ETL 에 처음 포함되기 위해서 고려해야 될 사항은 승인을 원하는 후보 tool 은 현재 승인 된 tool 이 갖지 못하는 개선점과 충분한 특징을 제공해야만 한다. 개발자는 완성시키기 위해 노력 했지만, 요구사항이 완벽하게 만족되지 않는다면, 요구사항의 중요성의 평가 팀에 의해 평가 되어야 한다. 평가 팀은 문제점이 본질적이거나 해로운 것인지를 판단해야 한다. 예를 들어 열악한 사용자 인터페이스는 방법론의 정당성 결핍처럼 중요하지는 않다. 완전하게 만족되지 않는 요구사항은 확인이 되어야 하고 최종 평가 보고서에 문서화 되어야 한다.
개발자는 NCSC 에게 검증 시스템의 복사본을 뒷받침하는 문서와 tools, test suites, (구성 관리....) configuration management evidence 와 source code 제출해야 한다. 게다가 시스템 개발자들은 NCSC 평가자들을 지원해야 한다. 예를 들어, 개발자들을 필요하다면 질문에 대답하고 training 을 제공하고, 평가 팀과 만나야 한다.

이 평가의 주요 과정은

1) 개발자는 NCSC 검증 의원회 의장에게 승인 요구를 제출해야 한다.
2) 의원회는 검증 시스템이 ETL 에 이미 존재하는 시스템보다 개선 되었거나. 이미 존재하는 시스템에 부족한 기능이나 유용한 방법을 제공하는지를 결정해야 한다.
3) 2)의 결과가 만족스럽다면, 평가 팀이 구성되고 검증 시스템 평가가 시작된다.
4) 평가 완료 후에.. TAR (Technical Assessment Report) 가 평가 팀에 의해 쓰여진다.
5) 의원회는 TAR 를 다시 조사하고 승인 추천장을 만든다
6) 의회 의장은 동의하거나 동의하지 않는다.
7) 동의 된다면, 검증 시스템을 위한 ETL 엔트리가 발행된다.
8) TAR 가 검증 시스템을 위해 발행.

(2) 평가의 경우, 인증을 위한 재 평가는 ETL 에 포함된 승인된 시스템의 새로운 버전을 평가하는 것을 말한다. 변화와 강화의 수가 승인을 위한 재평가의 중요한 근거가 된다. 이런 재 평가의 의도는 승인된 시스템의 개선을 허락하고 원래 승인된 버전의 보증이 유지되는 동안 ETL 에 **state-of-the-art** 기술을 지원하기 위한 것이다. 매각인은 VR(Vendor Report) 의 내에 개선된 근거의 요약을 준비해야 한다. VR 에는 보증이 유지된다는 것과 승인된 버전 이후의 검증 시스템에 나타나는 모든 변화를 이해할 수 있는 충분한 설명이 포함 되어야 한다. 이를 평가하는 의원회는 매각자들이 검증시스템의 변화, 보증의 연속성과 보유력의 논증하는 기술적인 개요를 설명하기를 기대한다. 재평가 주기는 의회 의장에 의한 승인 판단으로 마무리 되고, 결정이 찬성이라면, ETL 에 첨가 되고, 전에 승인된 버전은 삭제 된다.

이 평가의 주요 과정은

1) 매각자는 VR 과 다른 중요 사항들을 NCSC 검증 의원회 의장에게 제출한다.
2) VR 의 재조사를 위해 평가 팀이 결성된다.

3) 평가팀은 몇 가지 비평을 추가하고 검증 의원회에 그것을 제출한다.
4) 매각자는 의회에서 VR 을 설명할 수 있다.
5) 의원회는 승인 추천안을 만든다.
6) 의회 의장은 승인에 동의 하거나 동의하지 않는다.
7) 동의 된다면, 개정된 검증 시스템을 위한 ETL 엔트리가 발행된다.
8) VR 이 개정된 검증 시스템을 위해서 발행.

(3) 평가의 경우, 검증 시스템이 승인 되면, 그것은 지원 되고 다른 시스템에 의해 대체 되지 않는 한 ETL 에 포함된다. 의원회는 ETL 에서 검증 시스템의 삭제를 최종 결정하기도 한다. 예를 들어 너무 많은 bugs 가 있다거나, 사용자의 결핍, 지원, 유지와 지원의 부족, 비견고함 등은 ETL 로부터 검증 시스템을 삭제할 근거들이다. 삭세 시킬 경우, 의원회는 정형화된 공고를 하고, 그들의 결정의 정당성을 서술해서 제공한다. 검증 시스템의 방법론과 시스템 명세를 통해서 검증 시스템의 질과 완성도를 평가하는 기술적인 요소들은 다음과 같은 네 가지로 분류된다: 1) 방법론 2) 특징 3) 보증 4) 문서 . 방법론은 기본적인 원리이고 검증 시스템의 구조내의 규칙이다. 검증 시스템의 방법론은 그 시스템에서 정형 검증을 실행하는 동안 사용되는 규칙들로서 사용되는 제안들의 집합으로 이루어져 있다. 이 부분은 시스템 승인을 위해 필요하지만 충분한 조건은 아니다. 특징은 검증시스템의 기능적인 면을 포함한다. 특징에서는 명세 언어, 명세 처리 장치, 추론 메커니즘으로 나누어서 언어 표현, 내부 문법의 균일성, 입출력, 컴포넌트의 적합성, 구성의 적합성등을 체크한다. 보증은 검증시스템이 갖는 신뢰의 정도와 자신감이다. 보증에서는 에러 회복, 예측가능성, 견고성을 체크한다. 문서는 검증 시스템의 구성요소들, 적용, 가동과 유지를 모두 나타낸 기술적 문서와 매뉴얼로 구성된다. 이 분류들은 검증시스템의 각 컴포넌트들로 확장된다. 이 컴포넌트들은 최소한 다음 사항들을 포함한다; 사용자가 올바른 조건을 표현하게 하는 수학적 명세 언어, 명세를 설명하고 추론 메커니즘의 의해 설명될 수 있는 추측을 생성하는 명세 처리장치, 처리장치에 의해 생성된 추측을 설명하고 올바른 조건이 만족되는 지를 증명하거나 입증을 확인하는 추론 메커니즘들이다. NCSC 는 검증시스템의 유용성을 평가하기 위해서 지원 요소들을 고려하는데, 이는 다음과 같은 3 가지 로 분류된다.: 1) 특징 2)보증 3) 문서 사용자를 지원하기 위해 제공되는 두 가지 특징은 인터페이스와 검증 시스템의 베이스 하드웨어이다. 특징에서는 사용자 인터페이스, 보증을 제공하기 위해서는 구성 관리, 테스트, 유지와 같은 세가지 방법을 쓴다. 마지막으로 문서는 앞에서와 마찬가지로 검증 시스템의 구성 요소들, 적용, 가동과 유지를 모두 나타낸 기술적 문서와 메뉴얼로 구성된다.

3. ETL 의 확장

2 장에서 언급된 내용에 따라, 최근에 많이 사용되고 있는 몇 가지 tool 을 대상으로 평가 기준에 맞게 ETL 에 포함될 수 있는지 여부를 조사해 보기로 한다.
논리 기반의 정형 명세 언어인 Z 를 지원하는 ORA 사에서 개발한 Z/EVES[4]와 그래픽한 명세인 Statechart 를 지원하는 I-Logic 사가 개발한 STATEMATE MAGNUM[5]을 요구 조건과 비교해서 ETL 에 포함될 수 있는지를 조사하였다.

이 조사에서는 크게 방법론과 시스템 명세에 기반한 질적인 완성도 측면과, 구현과 여러가지 다른 지원 요인에 기반한 유용성측면으로 나누어져 세부사항들을 조사하였다.

	Z/EVES	STATEMATE MAGNUM
방법론	개발자가 사용한 정확한 방법론에 대한 문건이 도구와 함께 제공되지 않는다. 하지만, 기존의 증명 시스템인 EVES 에 Z 표현을 확장하여 사용하였다.	개발자가 사용한 정확한 방법론에 대한 문건이 도구와 함께 제공되지 않는다. 상태전이가 기반으로 제작되었다.
특징 (명세 언어, 명세 처리 과정, 추론 메커니즘)	Z 는 일차 논리와 집합론에 기반한 명세 언어로 표현이 수학적 기호를 사용해서 명확하고, 수학적 정리를 만들어서 증명하는 방법을 사용하여 명확한 추론 기법을 제공해준다.	그래픽한 명세를 도와주기 위해서 개발된 도구로, 상태 전이를 기반으로 하고 있다. 여기에 계층성을 첨가해서 이벤트의 발생에 따라 상태를 전이해 가면서 명세를 검사해 나가는 기법을 사용하고 있다.
문서	시스템 구현에 관한 문서는 없지만, 사용되는 수학적 응용에 대한 문서를 제공해 주며, 사용자가 시스템을 사용하면서 참고할 문서를 제공해 준다.	시스템 구현에 관한 문서가 없다. 방법론에 대해 언급한 문서도 없다.

[표 1] 도구 완성도에 대한 평가 결과

	Z/EVES	STATEMATE MAGNUM
특징	사용자가 자신이 작성한 명세에 대해서 만족성 여부를 검사하기 위해서 새로운 정리를 만들어서 검사를 수행할 수 있다. 이 점이 도메인 검사만 수행하는 다른 Z 관련 도구와 비교해서 우수하다.	이 도구의 최대 특징은 Z/EVES 와 비교하면 명세의 정확성을 검증하는 부분이 부족하지만, 도구를 처음 접하는 사람도 손쉽게 명세를 작성할 수 있다는 것이다. 앞의 Z/EVES 는 언어 자체가 처음 접하는 사람에게는 매우 어려운 도구이다.
보증	명세가 작성되어 검사하는 항목이 도메인 검사, 타입 검사, 타입의 일치성 검사 등 명세 전반에 걸쳐서 검사를 하며, 검사를 통과한 것에 대해서는 수학적 이론에 따라 올바르다는 것을 보장한다.	명세가 작성되면 이벤트를 발생시켜서 시스템의 제어가 어떻게 변해가는 상황을 시뮬레이션하여 관찰할 수 있다. 올바른 동작을 하는지를 시뮬레이션을 통해서 보증한다.
문서	사용자 매뉴얼에서 도구의 동작과 명세를 검사하는 부분에 대한 설명을 하고 있다. 그 외에 라이브러리에 대한 문서도 제공을 한다.	사용자 매뉴얼에서 도구의 동작과 명세를 검사하는 부분에 대한 설명을 하고 있다.

[표 2] 유용성 측면에서의 평가 결과

이러한 도구에 대한 검사 조건은 크게 두 종류로 나누어 본다. 하나는 도구 완성도에서 나올 수 있는 결과에 대한 평가이고, 다른 하나는 도구의 유용성에 대한 평가이다.

각 항목에 대해서 평가 항목과 우리가 수행한 두 도구에 대한 평가 결과는 각각 [표 1]과 [표 2]로 작성하였다.

위에서 작성된 표를 기준으로 두 도구를 판단해 보면, Z/EVES 의 경우에는 다른 Z 관련 도구들이 제공하지 못하고 있는 사용자가 정리를 생성해서 증명함으로써, 원하는 정리가 만족하는지를 검사할 수 있다는 장점을 가지고 있다. 또한, STATEMATE Magnum 의 경우에는 표에서 언급하지는 않았지만, 코드 생성을 통해서 자동 구현을 할 수 있다는 장점을 가지고 있다. 또한, 여러 검증 도구에 적용할 수 있는 코드를 생성해서 개발될 시스템에 대한 특성을 검사할 수 있다는 것도 큰 장점이라고 할 수 있다.

NIST 에 제시하는 ETL 에 추가될 수 있는 조건 중에 다른 도구가 가지지 못한 장점을 하나이상 가지고 있다면, 도구 리스트에 추가될 수 있다는 조건을 가지고 있다.

우리가 참고한 1993 년의 NIST 의 ETL 자료가 최종 버전이라면, 그 문서에는 Z/EVES 와 STATEMATE Magnum 이 포함되어 있지 않음으로 ETL 에 추가될 수 있을 것이다.

4.결론

정보보호를 위해 제정된 정보보호 시스템의 평가 등급 중 최상위 등급은 우리가 기대하는 보안의 수준을 제공해야 하고 그 기능들을 우리가 확인할 수 있어야 한다. 그러기 위해서 K7 등급의 요구사항 중 하나인 정형화된 모델에서 사용되는 정형화 시스템은 우리가 그 tool 이 하는 기능을 믿을 수 있어야 한다. 그러기 위해서 본문에서 제안한 과정들이 필요하다. 하지만 아직 우리나라는 정형화 시스템에 대해 개발자들이 참고할 만한 기준이 없는 실정이다. 이 경우 검증 받지 않은 tool 을 사용해서 K7 의 요구사항을 만족 시킬 경우에는 그 보안 시스템의 정확성을 장담 할 수 없고, 이에 따르는 위험 부담이 더욱 커질 수 있다.

이런 위험 부담을 방지하기 위해서 우리나라의 평가 기준에도 정형화 시스템의 승인이 필요하다. 이런 승인 tool 리스트에 명시된 tool 을 사용해서 정형화 모델링을 할 경우 사용된 정형 언어의 검증뿐만 아니라, 정형 언어를 검증하는 시스템에 대한 검증이 되어 보다 명확하고 정확한 시스템을 명세하고, 검증된 결과에 대한 신뢰도가 증가하게 된다. 이렇게 검증된 방법과 도구를 사용하여 문서화하는 경우 세계 각국의 평가 등급에서 고등급을 획득하여 보안 시스템 수출에 많은 도움이 된다.

참고문헌

[1] National Computer Security Center, Guidelines for Formal Verification Systems, NCSC ,1989
[2] William Stallings , Network Security Essentials: Application and Standards, Prentice Hall, 1999
[3] National Computer Security Center, Endorsed Tools List, NCSC, 1993
[4] Mark Saaltink, The Z/EVES 2.0 User's Guide, ORA, 1999
[5] I-Logix Inc. , STATEMATE MAGNUM User Guide, I-Logix Inc, 1996
[6] 한국 정보 보호 센터, 국내.외 정보보호 시스템 평가 가이드, 한국 정보 보호 센터, 1998