정보통신망 침입탐지시스템 평가기준 K4 등급 보안기능요구사항과 공통평가기준 보안기능요구사항간의 비교 연구

이태승, 김태훈, 조규민, 이경구

한국정보보호진흥원

A studty on the comparison between IDS K4 SFR and Common Criteria SFR

Tae-Seung Lee, Tai-Hoon Kim, Kyu-Min Cho, Koung-Goo Lee

Korea Information Security Agency

요 약

본 논문에서는 기존의 평가기준에 기반하여 평가□인증 받은 침입탐지시스템 제품의 대다수를 차지하는 K4 등급의 보안기능요구사항과 공통평가기준 보안기능요구사항을 본 논문에서 설정한 보안목적과 자산에 기반하여 비교 분석함으로써 이들 보안기능요구사항간의 호환 가능성을 검토하고 상호 호환되지 않는 K4 보안기능요구사항에 대해서는 새로운 공통평가기준 기반 기능 컴포넌트의 필요성을 제시한다.

I. 서론

정보통신부고시 제2002-40호에 의거 침입탐지시스템은 정보보호시스템 공통평가기준에 의해서도 평가 및 인증을 받을 수 있게 되어 기존의 정보통신망 침입탐지시스템 평가기준과의 보안기능요구사항과의 비교 연구가 필요하게 되었다[1][2].

본 논문은 보안기능요구사항 선택 시 근거가 되는 보안기능요구사항의 보안목적과 보안목적이 보호하는 자산을 기반으로[1][3] 두 평가기준 보안기능요구사항의 보안목적과 자산을 식별 한 후, 이를 기반으로 기존의 평가기준으로 평가□인증 받은 침입탐지시스템 제품의 대다수를 차지하는 K4 등급의 보안기능요구사항을 공통평가기준의 보안기능요구사항과 비교 분석함으로써 이들 보안기능요구사항간의 호환 가능성을 검토하고 상호 호환되지 K4 등급의 보안기능요구사항에 대해서는 새로운 공통평가기준 기반 기능 컴포넌트의 필요성을 제시한다.

II. 본문

1. 비교 항목에 기반한 K4 보안기능요구사항의 분석

공통평가기준 기능 컴포넌트와의 비교를 위해 K4 보안기능요구사항을 보안목적과 자산을 중심으로 분석할 경우, 표 1과 같이 보안기능요구사항별 자산을 식별할 수 있으며, 식별된 자산 중 침입탐지시스템 자체 자산을 보안기능의 보안목적과 연관시켜 보다 세부적으로 분류할 경우 표 1의 세부자산을 식별할 수 있다.

표 1에서 식별된 세부자산 중 수집□분석 데이터는 'K4.1의 축약 감사데이터 생성' 및 'K4.2 보안위반 분석' 보안기능요구사항과 연관되는 자산으로써 K4.1의 축약 감사데이터 용어가 침입탐지시스템 자체의 사후 책임추적성(accountability)을 목적으로 하는 K4.6의 감사데이터와 혼동될 수 있으므로 본 논문에서는 수집□분석 데이터라는 새로운 용어를 사용하여 식별한다. 또한 인증 데이터는 'K4.4 신분확인'과, 감사 데이터는 'K4.6 보안감사' 보안기능요구사항과 연관시켜 사용하기 위해 식별한다. 마지막으로 환경구성 데이터는 보안위반 목록과 같이 침입탐지시스템 보안기능 수행 시 필요한 일반적인 데이터를 위해 식별한다.

표 1: K4 보안기능요구사항의 보안목적과 자산

보안기능	내용	세부자산	자산
K4.1	수집, 축약	수집□분석 데이터	침입탐지시스템을 포함하여 침입탐지시스템이 운영되는 호스트 또는 네트워크 시스템(보호대상 시스템)
K4.2	분석		
K4.3	대응		
K4.4	신분확인	인증데이터	침입탐지시스템 자체
K4.6	보안감사	감사데이터	
K4.5	데이터보호	환경구성, 감사 데이터 등	
K4.7	보안관리		
K4.8	보안기능 보호		

2. K4 보안기능요구사항과 공통평가기준 기능 컴포넌트와의 대응 정도

본 절에서는 비교 항목인 보안목적과 자산에 따라 K4 보안기능요구사항을 분석한 결과인 표 1에 따라 K4 보안기능요구사항을 침입탐지시스템 자체 보호를 위한 보안기능과 보호대상시스템 보호를 위한 보안기능으로 구분하여 공통평가기준 기능 컴포넌트와의 호환 가능성을 검토, 분석한다.

1) 침입탐지시스템 자체 보호를 위한 K4 보안기능요구사항

■ K4.4 신분확인

K4.4.1의 식별, K4.4.2의 인증, K4.4.3의 인증실패 관리를 통해 침입탐지시스템에 접근하는 사용자의 신분확인을 요구하는 K4.4는 표 2의 공통평가기준 기능 컴포넌트 'FIA_UID.2 모든 행동 이전에 사용자 식별', 'FIA_UAU.2 모든 행동 이전에 사용자 인증', 'FIA_UAU.4 재사용 방지 인증 메커니즘', 'FIA_UAU.7 인증 피드백 보호', 'FIA_AFL.1 인증 실패 처리' 기능 컴포넌트와 호환 가능하다.

표 2: K4.4와 호환 가능한 기능 컴포넌트

FIA_UID.2 모든 행동 이전에 사용자 식별
FIA_UID.2.1 TSF는 사용자를 대신하여 TSF가 중재하는 모든 행동을 허용하기 전에 각 사용자를 성공적으로 식별해야 한다.
FIA_UAU.2 모든 행동 이전에 사용자 인증
FIA_UAU.2.1 TSF는 사용자를 대신하여 TSF가 중재하는 모든 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.
FIA_UAU.4 재사용 방지 인증 메커니즘
FIA_UAU.4.1 TSF는 [할당 : 식별된 인증 메커니즘]에 관련된 인증 데이터의 재사용을 방지해야 한다.
FIA_UAU.7 인증 피드백 보호
FIA_UAU.7.1 TSF는 인증이 진행되는 동안 사용자에게 [할당 : 피드백 목록]만을 제공해야 한다.
FIA_AFL.1 인증 실패 처리
FIA_AFL.1.1 TSF는 [할당 : 인증 사건의 목록]에 관련된 [할당 : 회수] 번의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다. FIA_AFL.1.2 실패한 인증 시도가 정의된 회수에 도달하거나 초과하면, TSF는 [할당 : 대응 행동의 목록]을 수행해야 한다.

■ K4.5.1 저장된 데이터 무결성

침입탐지시스템 내에 저장된 식별 및 인증 데이터, 침입탐지시스템 실행파일 및 환경 설정 파일 그리고 보안위반 사건 목록의 무결성 확인을 요구하는 K4.5.1 레이블 198은 표 3의 'FPT_TST.1 TSF 자체 시험' 기능 컴포넌트와 호환될 수 있지만, 'FPT_TST.1.1' 기능 엘리먼트를 추가적으로 요구하게 된다.

이와 같은 경우 [1]의 기능 엘리먼트 본문 내용에 따라 'FPT_TST.1.1' 기능 엘리먼트를 'FPT_TST.1' 기능 컴포넌트로부터 배제시킬 수는 없고 응용 시 주의사항 등을 통해 'FPT_TST.1' 기능 컴포넌트의 보안범위를 K4.5.1에 맞게 설명해줄 필요가 있다.

또한 무결성 확인시 오류가 발견될 경우, 이에 대한 대응행동을 요구하는 K4.5.1 레이블 199과 호환될 수 있는 기능 컴포넌트가 공통평가기준에 없으므로 [1]의 보안기능요구사항 확장 방법에 따라 새로운 기능 컴포넌트 정의가 필요하다.

표 3: K4.5.1과 호환 가능한 FPT_TST.1

FPT_TST.1 TSF 자체 시험
FPT_TST.1.1 TSF는 TSF의 정확한 운영을 입증하기 위하여 [선택 : 시동시, 정규 운영 동안 주기적으로, 인가된 사용자 요구시], [할당 : 자체시험이 발생해야 하는 조건] 조건시 자체 시험을 실행해야 한다.
FPT_TST.1.2 TSF는 인가된 사용자에게 TSF 데이터의 무결성을 검증하는 기능을 제공해야 한다.
FPT_TST.1.3 TSF는 인가된 사용자에게 저장된 TSF 실행 코드의 무결성을 검증하는 기능을 제공해야 한다.

■ K4.5.2 내부전송 데이터 무결성

보안기능이 물리적으로 분리되어 있는 경우 보안기능간의 데이터 전송 시 무결성 확인 기능과 무결성 오류 발견 시 이에 대한 대응 행동을 요구하는 K4.5.2는 표 4의 공통평가기준 'FPT_ITT.3 내부전송 TSF 데이터 무결성 검사' 기능 컴포넌트와 호환 가능하다.

표 4: K4.5.2와 호환 가능한 FPT_ITT.3

FPT_ITT.3 내부전송 TSF 데이터 무결성 검사
FPT_ITT.3.1 TSF는 TOE의 분리된 부분간에 전송되는 TSF 데이터의 [선택 : 변경, 치환, 순서변경, 삭제, [할당 : 기타 무결성 오류]]를 탐지할 수 있어야 한다.
FPT_ITT.3.2 데이터 무결성 오류가 탐지된 경우 TSF는 다음의 대응행동을 취해야 한다 : [할당 : 취해질 대응행동의 명세].

■ K4.5.3 내부전송 데이터 보호

보안기능이 물리적으로 분리되어 있는 경우 보안기능간에 데이터가 전송 시 데이터 노출 방지를 요구하는 K4.5.3은 표 5의 공통평가기준 'FPT_ITT.1 내부전송 TSF 데이터의 기본적인 보호' 기능 컴포넌트와 호환 가능하다.

표 5: K4.5.3과 호환 가능한 FPT_ITT.1

FPT_ITT.1 내부전송 TSF 데이터의 기본적인 보호
FPT_ITT.1.1 TSF는 TOE의 분리된 부분간에 TSF 데이터가 전송될 때 노출로부터 TSF 데이터를 보호하여야 한다.

■ K4.6.1 감사데이터 생성

표 1의 감사 데이터 정의에 따라 항목 5, 6을 제외한 K4.6.1은 표 6의 공통평가기준 'FAU_GEN.1 감사 데이터 생성' 기능 컴포넌트와 호환될 수 있지만, 항목 5와 6은 표 1에서 정의한 'FAU_GEN.1'의 감사 데이터 범위와 다르므로 이를 만족시키기 위해서는 [1]의 보안기능요구사항 확장 방법에 따라 새로운 기능 컴포넌트를 정의할 필요가 있다.

표 6: K4.6.1과 호환 가능한 FAU_GEN.1

FAU_GEN.1 감사 데이터 생성
FAU_GEN.1.1 TSF는 다음과 같은 감사대상 사건들의 감사 레코드를 생성할 수 있어야 한다. a) 감사 기능의 시동과 종료 b) [선택 : 최소, 기본, 상세, 지정되지 않음] 감사 수준에 따른 모든 감사대상 사건 c) [할당 : 기타 특별히 정의된 감사대상 사건]
FAU_GEN.1.2 TSF는 최소한 다음 정보를 각 감사 레코드 내에 기록해야 한다. a) 사건 일시, 사건 유형, 주체의 신원, 사건 결과(성공 또는 실패) b) 각 감사 사건 유형에 대하여, 보호프로파일/보안목표명세서에 포함된 기능 컴포넌트의 감사대상 사건 정의에 기반한, [할당 : 기타 감사관련 정보]

■ K4.6.2 감사데이터 보호

K4.6.2는 공통평가기준 'FAU_STG.3 감사 데이터 손실 예측시 대응 행동'과 'FAU_STG.4 감사 데이터의 손실 방지' 기능 컴포넌트와 호환 가능하다.

■ K4.6.3 보안감사 검토

K4.6.3은 K4.6.1의 항목 5, 6을 제외하고는 공통평가기준 'FAU_SAR.1 감사검토', 'FAU_SAR.2 감사검토 권한 제한', 'FAU_SAR.3 선택가능한 감사검토' 기능 컴포넌트와 호환 가능하다.

■ K4.7 보안관리

K4.7을 공통평가기준 기능 컴포넌트와 비교하기 위해서는 K4.7 항목 1 ~ 항목 12를 공통평가기준 보안 관리 클래스 구성에 따라 TSF 기능 관리와 TSF 데이터 관리로 구분해야 한다. 그 결과 K4.7 항목 1, 2, 3, 8, 9, 12는 공통평가기준 'FMT_MOF.1.1 보안기능 관리' 기능 컴포넌트와, 항목 4, 5, 9, 10은 'FMT_MTD.1 TSF 데이터 관리' 기능 컴포넌트와, 항목 7, 11은 'FMT_MTD.2 TSF 데이터 한계치 관리' 기능 컴포넌트와 호환

가능하다.

■ K4.8.2 안전한 경로

보안 기능과 관리자간에 안전한 경로를 보장하는 수단을 요구하는 K4.8.2는 공통평가기준 'FTP_TRP.1 안전한 경로' 기능 컴포넌트와 호환 가능하다.

2) 보호대상시스템 보호를 위한 K4 보안기능요구사항

■ K4.1 축약 감사 데이터 생성

K4.1은 보호대상시스템 보호를 위해 침입탐지에 필요한 데이터를 수집, 축약할 것을 요구하고 있지만 공통평가기준에는 K4.1의 보안목적과 자산을 충분히 만족시킬 수 있는 기능 컴포넌트가 존재하지 않으므로 [1]의 보안기능요구사항 확장 방법에 따라 새로운 컴포넌트를 정의할 필요가 있다.

■ K4.2 보안위반 분석

K4.2는 K4.1에서 생성한 수집□분석 데이터를 보안위반 사건 목록과 비교함으로써 보안위반 여부를 분석해야 함을 요구하고 있다. 공통평가기준에는 K4.2의 보안목적과 유사한 'FAU_SAA.1 잠재적인 위반 분석' 기능 컴포넌트가 존재하지만 관련된 자산이 서로 다르므로 [1]의 보안기능요구사항 확장 방법에 따라 새로운 컴포넌트를 정의할 필요가 있다.

■ K4.3 보안감사 대응

K4.3은 침입탐지시스템이 보안위반 가능성 및 사실 탐지 시 대응기능 수행을 요구하고 있지만 K4.2의 경우와 같이 관련된 자산이 서로 다르므로 [1]의 보안기능요구사항 확장 방법에 따라 새로운 컴포넌트를 정의할 필요가 있다.

III. 결론 및 향후 연구계획

본 논문에서는 기존의 평가기준에 기반으로 평가□인증 받은 침입탐지시스템 제품의 대다수를 차지하는 K4 등급의 보안기능요구사항을 표 1의 비교 항목에 기반하여 공통평가기준 보안기능요구사항과 비교 분석하였다.

비교 분석 결과, 침입탐지시스템 자체 보호를 위한 보안기능요구사항인 'K4.4 신분확인', 'K4.5 데이터 보호', 'K4.6 보안감사', 'K4.7 보안관리', 'K4.8 보안기능의 보호'는 공통평가기준 보안기능요구사항과 상당부분 호환 가능하지만, 보호대상시스템 보호를 위한 침입탐지시스템 핵심 기능인 'K4.1 축약 감사데이터 생성', 'K4.2 보안위반 분석', 'K4.3 보안감사 대응 보안기능요구사항'은 표 1을 따라 비교할 경우 공통평가기준 보안기능요구사항과 호환되기가 어렵다는 것을 알 수 있었다.

따라서 이에 대한 보완을 위해 향후에는 K4 등급과 공통평가기준의 보안기능요구사항간의 호환에 필요한 새로운 공통평가기준 기반 기능 컴포넌트 정의 및 이에 필요한 요소를 분석 연구할 필요가 있다고 사려된다.

참고문헌

[1] 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5

[2] 정보통신부고시 제2000-62호, 정보통신망 침입탐지시스템 평가기준, 2000. 7.29

[3] ISO/IEC JTC 1/SC 27N 3065, Guide for the Production of PPs and STs Version 0.92, 2002. 4.10