情報保護學會論文誌
第 20卷 第 6號, 2010. 12

침입차단서비스 보안기능 분석을 통한 보안SLA 등급화 지표 개발

이 완 석[1†], 고 웅[2], 원 동 호[3], 곽 진[2‡]
[1]한국인터넷진흥원, [2]순천향대학교, [3]성균관대학교

Development of S-SLA's Grading Indicator based on the Analyses of IPS's Security Functions

Wansuk Yi[1†], Woong Go[2], Dongho Won[3], Jin Kwak[2‡]
[1]KISA, [2]Soonchunhyang University, [3]Sungkyunkwan University

요 약

특정 서비스를 보다 안전하게 제공받기 위한 사용자가 증가함에 따라 서비스수준협약(SLA)에 대한 관심이 증가하고 있다. 그러나 침입차단서비스와 같은 보안서비스에 대해 기존의 SLA는 관련 보안 분야가 미비하여 제대로된 수준 협약이 어려운 실정이다. 기존의 SLA에서 보안 분야는 권고사항의 수준으로 제공되고 있다. 이에 본 논문에서는 기존 침입차단서비스 제품의 보안 기능을 분석하여 공통보안기능과 개별보안기능을 분류하고, 이를 통해 보안서비스의 품질을 보장하기 위한 보안SLA(S-SLA : Security Service Level Agreement) 등급화 지표를 제안한다. 이를 통해 보안서비스에 대한 세분화된 서비스 협약이 가능할 것이다.

ABSTRACT

Internet service providers provide various security services, such as firewall, intrusion detection, intrusion prevention, anti-virus, along with their main Internet services. Those security service users have no idea what kind of quality services they are guaranteed. And therefore, Internet users interest in Security Service Level Agreement(SLA) increases as their interest in secure Internet service increases. However, there wasn't any researches in the S-SLA area domestically and there are only limited SLA indexes related to system or service maintenances at the moment. Therefore, this paper analyses security functions in IPS services and categorize them into common and independent security functions. Finally to improve quality of security services, this paper proposes S-SLA indexes depending on the different security levels. This will be subdivide into agreement on security service.

Keywords: S-SLA, IPS, Grading Indicator, Security Function

I. 서 론

현재 다양한 서비스에 대한 개발 및 투자로 인해 사용자가 언제 어디서든지 자신이 원하는 서비스를 제공받는 사회가 구축되어 가면서, 이를 보다 안전하고 효율적으로 제공받기 위한 사용자의 요구사항 또한 증가하고 있다.

이러한 사용자의 요구사항은 서비스 품질 개선 및 서비스의 안전성 등에 대한 요구가 반영된 것으로, 이를 위하여 서비스 제공자의 다양한 노력이 이루어지고 있다.

그 중 서비스 제공자와 이용자간의 보다 효율적인

접수일(2010년 9월 25일), 수정일(2010년 12월 8일), 게재확정일(2010년 12월 16일)
† 주저자, wsyi@kisa.or.kr
‡ 교신저자, jkwak@sch.ac.kr

서비스 제공을 위해 서비스수준협약(SLA : Service Level Agreement)을 제공하는 서비스 제공자가 증가하고 있다. SLA는 사용자가 원하는 서비스의 품질 보장을 위한 문서화된 협약이라 할 수 있으며, 서비스의 유지보수 측면에 초점을 맞추어 가용성, 처리량, 장애 처리 등의 지표를 정의하고 있다. 그러나 보안서비스와 관련된 사항은 서비스 제공자에 따라 자체적으로 선정하도록 권고하고 있다.

이러한 SLA는 특히 침입차단시스템 등의 서비스를 제공하는 관제 업체들에게 필수적으로 필요한 부분이라 할 수 있다. 그러나 기존 SLA의 보안서비스 관련 사항은 권고의 수준에 머물러 있어, 실제 제품의 보안기능 분석 및 지표 도출을 통해 사용자가 요구하는 수준의 보안서비스 제공에 한계를 가지고 있다. 따라서 본 논문에서는 침입차단서비스의 보안기능을 분석하고, 이를 기반으로 침입차단서비스에 대한 보안 SLA(S-SLA : Security Service Level Agreement) 지표를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 S-SLA 및 보안서비스에 대하여 설명하며, 3장에서는 침입차단서비스의 보안기능을 분석한다. 4장에서는 분석된 보안기능을 기반으로 침입차단서비스에 대한 S-SLA 지표를 제안하고, 5장에서 결론을 맺는다.

II. 관련연구

2.1 S-SLA

서비스수준협약(SLA : Service Level Agreement)은 보장된 품질 수준과 관련되는 측정지표를 기술하는 서비스 제공자와 사용자들 사이의 공식적인 계약이다. 일반적인 SLA는 대역폭, 지연, 손실 등과 같은 유지보수와 관련된 측정지표와 보장 수준을 나타낸다. 서비스 제공자에 의하여 구현되는 SLA는 측정될 수 있으며, 추적될 수 있는 지표에 기초한다. 이와 같은 측정지표로 서비스 제공자뿐만 아니라 사용자들도 잘 이해하고 있는 서비스 가용성(availability)을 예로 들 수 있다. 예를 들어, 특정 보안서비스의 가용도가 99.999%일 때 1년에 접속 불량 시간 10분 이내의 품질 서비스 제공이 가능하다는 의미를 가지고 있다.

ITU-T X.805 권고안에서는 보안서비스 항목으로 통신망을 위한 종단간 보안 프레임워크를 기술하고 있으며, 종단간 네트워크 보안을 위한 보안 구조를 보여주고 있는 등 8가지 항목의 보안요구사항을 정의하고 있다.

〔표 1〕 ITU-T X.805 S-SLA 속성

SLA 속성	보안 목적
접근 제어	권한이 부여된 사람이나 장비만 접근 허용
인증	신원 검증
부인 방지	행위에 대한 기록 제공
데이터 기밀성	데이터 공개 보호
통신 보안	정당한 정보 흐름 보증
데이터 무결성	데이터 정확성, 변경 보호
가용성	자원의 정당한 사용 보증
비밀성	정보 노출 방지

S-SLA는 네트워크상의 미리 정해진 특정 경계(boundary)와 조건 안에서 유효하다. SLA 경계는 유효한 사용자 시나리오 하에서 다른 서비스 특징들에 대한 트래픽 흐름을 기술하는 참조 연결을 문서화함으로써 이를 통해 식별된다. 또한, 참조 연결은 트래픽과 어플리케이션 클래스의 보안 요구사항을 기술한다. S-SLA를 기술하기 위하여 사용되는 참조 연결은 어떻게 이런 보안 요구사항들이 구현되는지와 제한 사항에 대한 상세한 내용을 제공해야 한다〔1〕〔2〕.

2.2 침입차단서비스

침입차단서비스(IPS)는 기관의 보안 정책에 따라 인가된 인터넷 서비스에 대한 액세스는 허용하고, 인가되지 않은 서비스에 따르는 트래픽을 철저하게 막음으로써 효율적인 보안 서비스를 제공하도록 한다. 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 차단하고, 허가되거나 인증된 트래픽만 허용하는 적극적인 보안 대책이라고 할 수 있다.

침입차단서비스의 기본은 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공하는 것이다. 일반적으로 외부와의 투명한 접근을 허용함으로써 내부 망 전체가 위험에 노출되어 있을 경우, 외부와 내부 네트워크간의 유일한 경로에 침입차단서비스를 설치함으로써 불법적인 트래픽을 차단할 수 있는 것이다.

침입차단서비스를 구축하고 이를 운용함에 있어서 다음과 같은 효과를 얻을 수 있다.

- 위협에 취약한 서비스에 대한 보호
- 호스트 시스템에 대한 액세스 제어

- 보안성 향상
- 프라이버이스 보호 기능 확장
- 네트워크 사용에 대한 로그 기록 및 통계자료
- 네트워크 엑세스 제어 정책에 대한 구현

일반적인 침입차단서비스의 구성요소는 〔표 2〕와 같다[3].

2.3 기존 S-SLA 연구 한계점

SLA에서 보안 분야는 이를 구체적이고 독립적으로 구성하는 형태가 아닌, 기존의 SLA에 보안 관련 조항이 추가되는 형태를 가지고 있다. 이와 같은 보안 관련 조항들은 서비스수준협약에서 고려되어야 할 다양한 보안 영역을 포함하지 못하고, 세부 조항이 구체적이지 못한 실정이다. 또한 보안 관련 조항을 필수적으로 SLA에 포함시켜야 하는 것이 아니라 이를 포함하도록 권고하는 수준에 머물러 있으며, 보안 환경 분석, 관련 시설 및 환경 구축 등이 선행되어야 하므로 적용하기가 쉽지 않다. 이러한 이유로 대부분의 서비스수준협약에서 보안 관련 사항이 포함되는 경우가 미비하다.

따라서 본 논문에서는 SLA의 보안 분야를 특화한 S-SLA를 제안하기 위하여 국내 보안 제품 중 침입차단서비스를 제공하는 제품의 보안 기능을 분석하고 이를 통해 국내에 통용되는 제품 실정에 맞는 S-SLA 등급을 분류한다.

III. 침입차단서비스 보안기능 분석

3.1 침입차단서비스의 기능 분석

본 논문에서 분석한 침입차단시스템 제품은 대표성 및 공정성을 위하여 IT인증사무국에 등록된 공통평가기준 인증 제품을 기준으로 분석하였다. 침입차단시스

〔표 2〕 침입차단서비스의 기능

구성요소	내용
네트워크 정책	설계, 설치, 사용에 직접적으로 영향을 줄 수 있는 두 가지 레벨의 네트워크 정책 - 상위레벨 : 네트워크 엑세스 정책, 예외 조건 등 - 하위레벨 : 실질적인 엑세스 제어, 서비스 필터링
사용자 인증 시스템	스마트카드, 인증 토큰, 생체인식, 스포트웨어 매커니즘 등을 사용하며, 현재 많이 사용하고 있는 인증 시스템으로는 일회용 패스워드가 있음
패킷 필터링	라우팅 인터페이스를 지나는 패킷을 필터링 하는 기능 - 출발지 IP 주소 - 목적지 IP 주소 - TCP/IP 출발지 포트 - TCP/IP 목적지 포트
응용 계층 게이트웨이	송신자 응용 서비스가 보내는 정보를 그대로 전달하며, 내부와 외부간의 모든 응용 레벨의 트래픽에 대한 로깅이나, Telnet, FTP 등에서 사용자 인증 등을 수행
스크린 라우터	라우터가 패킷의 헤더 내용을 분석하여 필터링(스크린)하는 장비 - 출발지 및 목적지 주소에 의한 스크린 - 포트 번호에 의한 스크린 - 프로토콜별 스크린
베스천 호스트(Bastion Hosts)	침입차단서비스의 가장 중요한 기능으로서 액세스 제어 및 응용 시스템 게이트웨이로서 프럭시 서버의 설치, 인증 로그 등을 담당
이중 네트워크 호스트	2개 이상의 네트워크(내·외부)에 동시에 접속된 호스트를 말하며, 보통 게이트웨어 호스트라는 시스템을 가리킴. - 두 네트워크간의 유일한 경로를 제공 - 모든 내·외부 트래픽이 통과
스크린 호스트 게이트웨이	이 시스템을 내부 네트워크에 두어 스크린 라우터가 내부로 들어가는 모든 트래픽을 전부 스크린 호스트에게만 전달되도록 하는 기능. 외부로 나가는 트래픽에 대해서도 스크린 호스트에서 출발한 트래픽만 허용.
스크린 서브넷	일명 DMZ의 역할을 외부 네트워크와 내부 네트워크 사이에 두어 완충 지역 개념의 서브넷 운영.
암호장치	특정 기관의 네트워크가 공공의 인터넷을 통해 여러 지역으로 분산되어 있을 경우에 적합. 지역적으로 떨어진 지점 네트워크간의 안전한 데이터 송수신 가능

〔표 3〕 침입차단서비스 보안기능

	제품 A (EAL3)	제품 B (EAL3)	제품 C (EAL4)	제품 D (EAL4)	제품 E (EAL4)	제품 F (EAL4)	제품 G (EAL4)	제품 H (EAL4)	제품 I (EAL4)	제품 J (EAL4)	제품 K (EAL4)
보안 경보	O	O	O	O	X	O	O	O	O	O	O
감사 데이터 생성	O	O	O	O	O	O	O	O	O	O	O
사용자 신원 연관	O	O	O	O	X	O	O	O	O	O	O
잠재적인 위반 분석	O	O	O	O	X	O	O	O	O	O	O
감사 검토	O	O	O	O	O	O	O	O	O	O	O
감사 검토 권한 제한	X	X	O	X	X	X	X	X	X	X	X
선택 가능한 감사 검토	O	O	O	O	O	O	O	O	O	O	O
선택적인 감사	O	O	O	O	O	O	O	O	O	O	O
감사 증적 저장소 보호	O	O	O	O	O	O	O	O	O	O	O
감사 데이터 손실 예측시 대응행동	O	O	O	O	O	O	O	O	O	O	O
감사 데이터의 손실 방지	O	O	O	O	O	O	O	O	O	O	O
암호키 생성	X	X	X	O	X	X	O	O	X	X	X
암호키 분배	X	X	X	O	X	X	O	O	X	X	X
암호키 파기	X	X	X	O	X	X	O	O	X	X	X
암호 연산	X	X	X	O	X	X	O	O	X	X	X
완전한 접근통제	X	X	X	O	X	O	X	O	X	X	X
보안속성에 기반한 접근통제	X	X	X	O	X	O	X	O	X	X	X
부분적인 정보흐름통제	O	O	O	O	O	O	O	O	O	O	O
단일 계층 보안속성	O	O	O	O	O	O	O	O	O	O	O
인증 실패 처리	O	O	O	O	O	O	O	O	O	O	O
사용자 속성 정의	O	O	O	O	O	O	O	O	O	O	O
인증	O	O	O	X	X	X	X	X	O	O	O
비밀정보의 검증	X	X	X	O	O	O	O	O	X	X	X
모든 행동 이전에 사용자 인증	X	X	X	O	O	O	O	O	X	X	X
재사용 방지 인증 메커니즘	X	X	X	O	X	O	O	X	X	X	X
인증 피드백 보호	O	O	O	O	X	O	O	O	O	O	O
모든 행동 이전에 사용자 식별	O	O	O	O	O	O	O	O	O	O	O
보안기능 관리	O	O	O	O	O	O	O	O	O	O	O
보안속성 관리	O	O	O	O	O	O	O	O	O	O	O
안전한 보안속성	X	X	X	O	X	X	O	X	X	X	X
정적 속성 초기화	O	O	O	O	O	O	O	O	O	O	O
보안기능 데이터 관리	O	O	O	O	O	O	O	O	O	O	O
데이터 한계치의 관리	O	O	O	O	X	O	O	O	O	O	O
안전한 보안기능 데이터	X	X	X	O	X	X	X	X	X	X	X
관리기능 명세	O	O	O	O	O	O	O	O	O	O	O
보안 역할	O	O	O	O	O	O	O	O	O	O	O
가명성	X	X	X	O	X	X	O	O	X	X	X
인가된 사용자 관찰가능성	X	X	X	X	X	X	O	X	X	X	X
추상기계 시험	O	O	O	O	O	O	O	O	O	O	O
장애시 안전한 상태 유지	O	O	O	O	X	O	O	O	O	O	O
외부 전송 데이터의 변경 탐지	X	X	X	X	O	X	X	X	X	X	X
내부 전송 데이터의 기본적인 보호	X	X	X	X	O	O	X	X	O	X	O
기능 복구	X	X	X	O	X	O	X	X	X	X	X
재사용 공격 탐지 및 대응행동	X	X	X	O	X	X	O	O	X	X	X
보안정책 우회불가성	X	X	O	O	X	O	O	O	O	O	O
보안기능 영역분리	X	X	O	O	X	O	O	O	O	O	O
신뢰할 수 있는 타임스탬프	X	X	O	O	X	O	O	O	O	O	O
자체 시험	O	O	O	O	O	O	O	O	O	O	O
오류에 대한 내성(부분적용)	X	O	O	O	X	O	O	O	O	O	O
최대 할당치	O	O	O	O	O	O	X	O	O	O	O
최대와 최소 할당치	X	X	X	X	X	X	O	X	X	X	X
세션 잠금	O	O	O	O	X	O	O	O	O	O	O
세션 종료	O	O	O	O	O	O	O	O	O	O	O
안전한 채널	X	X	O	O	X	O	O	O	O	O	O

템 인증 제품은 EAL3+ 제품과 EAL4 제품으로 총 11개 제품이며, 각 제품의 보안목표명세서(ST : Security Target)의 보안기능요구사항을 기반으로 분석하였다[4][5].

다음은 각 보안 기능에 대하여 설명한 것이다.

- □ 감사 데이터 생성 : 침입차단시스템에서 보안관리에 관련된 사건들이 발생하면 주체 및 객체에 대한 식별자, 사건 유형 및 결과, 사건의 날짜 및 시간 별로 감사데이터를 생성
- □ 감사 검토 : 인가된 관리자가 침입차단에 대한 감사기록을 요구하면 객체신원, 사용자 신원, 사건 유형 등과 외부 네트워크 호스트를 구분하여 관리자가 있는 클라이언트로 감사 기록을 전송하고, 클라이언트 화면에 사건유형별, 시간별, 결과별로 정렬 및 검색하여 볼 수 있도록 보고서 형태로 출력
- □ 선택 가능한 감사 검토 : 인가된 관리자가 침입차단시스템 웹 보안관리 화면을 통해 각 감사기록 종류 별로 키워드, 동작 등을 기준으로 감사기록을 검색
- □ 선택적인 감사 : 인가된 관리자가 침입차단시스템에서 IP 프로토콜, 객체 신원, 사용자 신원, 사건 유형 등의 감사 환경 설정 값에 기반하여 감사 대상 사건을 포함시키거나 배제
- □ 감사 데이터 손실 예측시 대응행동 : 침입차단시스템이 저장매체의 잔여량 한계치를 초과하거나 원격 로그서버와 통신이 원활하지 않을 경우 관리자에게 메일로 알리거나 경고창 발생
- □ 사용자 신원 연관 : 침입차단시스템에서 발생하는 모든 사건들에 대해서 연관된 관리자 신원과 감사 대상 사건을 연관시켜서 감사 데이터에서 관리자나 일반 사용자와 연관시켜 감사 데이터를 생성하고 저장
- □ 감사 증적 보호 : 생성된 감사 증적에 대해 인가된 관리자만이 접근할 수 있도록 시스템 파일로 저장
- □ 감사 데이터의 손실 방지 : 침입차단시스템에서 감사 저장소의 잔여량을 주기적으로 점검하여 감사 저장소의 포화를 미리 예측하고, 감사 저장소의 포화시 감사 데이터의 손실을 방지
- □ 보안 경보 : 침입차단에 대한 잠재적인 보안 위반을 탐지한 경우 인가된 관리자에게 선택적으로 메일 발송, 경고창 발생, 세션 종료 등의 행동을 함
- □ 잠재적인 위반 분석 : 침입차단시스템에서 인증 시도시 인증실패 감사 사건, 통제규칙 위반 감사 사건, 무결성 위반 감사 사건 등의 발생시 잠재적 위반으로 분석하여 관리자에게 메일로 알리거나 경고창 발생
- □ 감사 검토 권한 제한 : 침입차단시스템에서 감사 레코드의 읽기가 허용된 사용자를 제외하고는 모든 사용자들의 감사 레코드 읽기를 금지
- □ 암호키 생성 : 명세된 암호키 생성 알고리즘과 명세된 암호키 길이에 따라 침입차단시스템에서 사용될 암호키를 생성
- □ 암호키 분배 : 명세된 암호키 분배 방법에 따라 침입차단시스템에서 사용될 암호키를 분배
- □ 암호키 파기 : 명세된 암호키 파기 방법에 따라 침입차단시스템에서 사용한 암호키를 파기
- □ 암호 연산 : 침입차단시스템에서 명세된 암호 알고리즘과 명세된 암호키 길이에 따라 암호 연산을 수행
- □ 부분적인 정보흐름통제 : 침입차단시스템에서 허용하고 있는 규칙을 제외한 모든 접속을 거부하거나 명시적으로 차단하는 규칙을 제외하고는 모든 접속을 허용
- □ 단일 계층 보안속성 : 침입차단시스템에서 정보를 송·수신하는 외부 IT 실체와 정보의 허용 또는 거부함에 있어 사용자 식별이 가능한 통제 규칙, 탐지 규칙, 사용자 정의 탐지규칙 등을 적용
- □ 완전한 접근통제 : 침입차단시스템의 모든 주체와 객체간의 모든 오퍼레이션이 관리자 접근통제 정책에 의해서 수행
- □ 보안속성에 기반한 접근통제 : 주체 및 객체의 목록과 각각의 보안속성에 기초하여 객체에 대한 관리자 접근통제 정책을 강제
- □ 인증 실패 처리 : 사용자 또는 관리자 인증시 연속 인증 실패 횟수를 초과한 경우 연속 인증 실패 처리에 따라 인증 지연 시간 동안 인증을 지연하거나 사용자 아이디의 사용을 정지
- □ 사용자 속성 정의 : 침입차단시스템에 접근하는 외부 IT 실체나 인가된 관리자를 식별하고 식별 후 인증을 요청하는 절차를 거침
- □ 모든 행동 이전에 사용자 식별 : 침입차단시스템에서 모든 행동을 허용하기 전에 각 IT 실체나 인가된 관리자를 성공적으로 식별할 때 인증 방법(기본인증, 일회용 인증)을 제시
- □ 인증 피드백 보호 : 침입차단시스템에서 식별

및 인증이 진행되는 동안 패스워드를 입력시 입력값이 보이지 않도록 특수문자로 표시

□ 인증 : 침입차단시스템에 네트워크로 접근하는 주체에 대하여 관리자 인증포트 제한적 허용을 우선 적용하여 접근을 결정하고 관리자를 식별한 후 인증방법을 로그인창에 표시하고 저장된 인증방법에 따라 인증

□ 모든 행동 이전에 사용자 인증 : 침입차단시스템에서 관리자 또는 일반 사용자 인증을 필요로 하는 관리자 또는 일반 사용자에 대해서 인증을 수행하고 보안정책을 적용

□ 비밀정보의 검증 : 침입차단시스템에 인증하기 위해 사용되는 패스워드의 최소길이, 조합규칙 등의 기준을 적용하여 패스워드를 검증하는 메커니즘을 제공

□ 재사용 방지 인증 메커니즘 : 관리자 또는 일반 사용자가 침입차단시스템에 접근시 일회용 패스워드 메커니즘을 이용하여 인증 수행

□ 보안기능 관리 : 침입차단시스템에서 인가된 관리자만이 감사 기록 검토 및 검색, 보안위반사건 목록 조회, 무결성 점검, 시스템 정보 조회 및 변경 등의 보안기능을 결정, 중지, 개시, 변경하는 능력을 제공

□ 보안속성 관리 : 침입차단시스템에서 인가된 관리자만이 사용자 객체 관리, 사용자 그룹 객체 관리, 보안등급 객체 관리 등의 보안속성을 설정

□ 보안 역할 : 침입차단시스템에서 식별 및 인증을 통해 사용자를 관리자 역할에 연관시켜 인가된 관리자가 보안기능을 수행

□ 보안기능 데이터 관리 : 침입차단시스템에서 인가된 관리자만이 취약성 목록을 최신 데이터로 갱신할 수 있고 제품을 구성하는 중요 파일, 감사 데이터, 보안위반사건 목록 등을 제외한 환경구성 데이터 등의 보안기능 데이터의 관리를 할 수 있음

□ 안전한 보안속성 : 침입차단시스템에서 보안속성값에 대해 유효성을 검사하여 안전한 보안속성을 제공

□ 관리기능 명세 : 침입차단시스템에서 SSL 기반의 인터페이스를 통해 기능 관리, 보안 속성 관리, 보안기능 데이터 관리 등을 수행

□ 정적 속성 초기화 : 침입차단시스템에서 인가된 관리자만이 접근통제 규칙, 탐지규칙의 속성을 초기화

□ 데이터 한계치의 관리 : 침입차단시스템에서 인가된 관리자만이 감사 데이터 저장소 용량, 실패한 인증 시도 횟수에 대한 한계치를 관리

□ 안전한 보안기능 데이터 : 침입차단시스템에서 입력받은 값의 유효성을 확인하여 안전한 값만 설정되도록 제공

□ 가명성 : 침입차단시스템에서 별칭을 사용하여 외부 네트워크에서 내부 네트워크의 IP 주소를 파악할 수 없도록 함

□ 인가된 사용자 관찰가능성 : 침입차단시스템에서 관리자가 보안관리 인터페이스를 통해 패킷 필터링, 주소변환 등을 실시간으로 조회

□ 자체시험 : 침입차단시스템에서 제품이 시동시, 정규 운영 동안 주기적, 인가된 사용자의 요구시에 자체 시험을 실행하고 무결성을 검증

□ 장애시 안전한 상태 유지 : 침입차단시스템에서 통신 오류가 발생하여 검사가 실패하는 경우 자동 리부팅을 하여 안전한 상태를 유지

□ 추상기계 시험 : 일반적인 응용 중에 하부 추상기계인 하드웨어와 운영체제가 정상적으로 운영되는지 시그널을 보내 시험을 수행

□ 보안정책 우회불가성 : 침입차단시스템으로 들어오는 모든 패킷이 보안 정책에 적용되도록 제공

□ 보안기능 영역분리 : 침입차단시스템에서 보안기능을 수행하기 위해 보안정책을 수립할 때 인터페이스별로 신뢰할 수 있는 영역과 신뢰할 수 없는 영역을 분리

□ 신뢰할 수 있는 타임스탬프 : 침입차단시스템에서 외부타임스탬프 서버로부터 신뢰할 수 있는

〔표 4〕 공통평가기준 평가 등급

평가등급	내용
EAL1	보안에 대한 위협이 심각하지 않은 경우 적용 가능
EAL2	낮은 수준에서 중간 수준의 독립적으로 보증된 보안이 요구되는 경우 적용 가능
EAL3	중간 수준의 독립적으로 보증된 보안이 요구되는 경우 적용 가능
EAL4	중간 수준에서 높은 수준의 독립적으로 보증된 보안이 요구되는 경우 적용 가능
EAL5	높은 수준의 독립적으로 보증된 보안이 요구되는 경우 적용 가능
EAL6	자산이 귀중하고 위험이 높은 경우 적용 가능
EAL7	자산이 매우 귀중하고 위험이 극도로 높은 경우 적용 가능

시간 정보를 가져오거나 신뢰된 관리자가 시간을 변경하여 타임소스를 안전하게 관리

□ 내부 전송 데이터의 기본적인 보호 : 침입차단시스템에서 물리적으로 분리되어 있는 시스템 간의 데이터를 암호화된 자체 프로토콜, https, 인코딩 등의 안전한 방법으로 전송

□ 재사용 공격 탐지 및 대응행동 : 침입차단시스템에서 인증을 위한 데이터에 대한 재사용을 탐지하고 재전송 시도 방지와 같은 대응 기능을 수행

□ 기능 복구 : 침입차단시스템에서 프로세스 재기동 기능이 제품을 구성하는 어플리케이션 프로세스의 비정상적인 종료가 발생하였을 경우 프로세스를 재기동시켜주는 역할을 함

□ 외부 전송 데이터의 변경 탐지 : 침입차단시스템에서 외부로부터 전송받은 업데이트 파일의 해시값을 생성하여 업데이트 서버가 전송해준 해시값과 비교하여 데이터 변경을 탐지

□ 최대 할당치 : 침입차단시스템에서 지정된 시간에 IT 실체에서 보낼 수 있는 SYN 패킷의 최대 할당치를 두어 서비스거부공격을 차단

□ 최대와 최소 할당치 : 침입차단시스템에서 패킷 필터링 보안정책 규칙과 인터페이스별로 대역폭의 최대 할당치와 최소 할당치를 두어 전체 트래픽중 관리자가 정의한 대역폭을 보장

□ 오류에 대한 내성(부분적용) : 침입차단시스템에서 자신의 네트워크 인터페이스의 링크 상태를 검사하여 응답이 없을 경우 장애가 발생한 것으로 간주하여 감사기록하고 인가된 관리자에게 알림

□ 세션 종료 : 침입차단시스템에서 관리자 또는 사용자가 로그인 후 일정 시간 동안 아무 활동이 없을 경우 해당 세션을 잠그고 이후 활동을 요청하면 로그인 화면을 출력

□ 세션 잠금 : 침입차단시스템에서 관리자 또는 사용자가 로그인 후 비 활동 중이면 인증을 취소하여 세션은 무력화되고 재인증을 요구

□ 안전한 채널 : SSL 기능을 호출하여 SSL 프로토콜을 형성하거나 신뢰된 제품과 ASEN을 구현하여 암호화 통신을 함으로써 안전한 채널 형성

각 제품은 공통평가기준(CC)의 평가 등급을 가지며 EAL1~7까지로 나뉜다[15][16][17].

〔표 5〕 침입차단서비스 공통보안기능

		제품 A (EAL3)	제품 B (EAL3)	제품 C (EAL4)	제품 D (EAL4)	제품 E (EAL4)	제품 F (EAL4)	제품 G (EAL4)	제품 H (EAL4)	제품 I (EAL4)	제품 J (EAL4)	제품 K (EAL4)
보안 감사 영역	감사 데이터 생성	O	O	O	O	O	O	O	O	O	O	O
	감사 검토	O	O	O	O	O	O	O	O	O	O	O
	선택 가능한 감사 검토	O	O	O	O	O	O	O	O	O	O	O
	선택적인 감사	O	O	O	O	O	O	O	O	O	O	O
	감사 증적 저장소 보호	O	O	O	O	O	O	O	O	O	O	O
	감사 데이터 손실 예측시 대응행동	O	O	O	O	O	O	O	O	O	O	O
	감사 데이터의 손실 방지	O	O	O	O	O	O	O	O	O	O	O
사용자 데이터 보호 영역	부분적인 정보흐름통제	O	O	O	O	O	O	O	O	O	O	O
	단일 계층 보안속성	O	O	O	O	O	O	O	O	O	O	O
식별 및 인증 영역	인증 실패 처리	O	O	O	O	O	O	O	O	O	O	O
	사용자 속성 정의	O	O	O	O	O	O	O	O	O	O	O
	모든 행동 이전에 사용자 식별	O	O	O	O	O	O	O	O	O	O	O
보안 관리 영역	보안기능 관리	O	O	O	O	O	O	O	O	O	O	O
	보안속성 관리	O	O	O	O	O	O	O	O	O	O	O
	정적 속성 초기화	O	O	O	O	O	O	O	O	O	O	O
	보안기능 데이터 관리	O	O	O	O	O	O	O	O	O	O	O
	관리기능 명세	O	O	O	O	O	O	O	O	O	O	O
	보안 역할	O	O	O	O	O	O	O	O	O	O	O
보안 기능 보호 영역	자체 시험	O	O	O	O	O	O	O	O	O	O	O
제품 기능 접근 영역	세션 종료	O	O	O	O	O	O	O	O	O	O	O

IV. S-SLA 등급화 지표 개발

4.1 S-SLA 지표 개발

3장에서 분석한 침입차단시스템 제품 〔표 3〕를 보게 되면, 모든 제품에서 동일하게 제공되는 보안기능과 각 제품에 따라 달리 제공되는 보안기능으로 나눌

〔표 6〕 침입차단서비스 개별보안기능

		제품 A (EAL3)	제품 B (EAL3)	제품 C (EAL4)	제품 D (EAL4)	제품 E (EAL4)	제품 F (EAL4)	제품 G (EAL4)	제품 H (EAL4)	제품 I (EAL4)	제품 J (EAL4)	제품 K (EAL4)
보안 감사 영역	보안 경보	O	O	O	O	X	O	O	O	O	O	O
	사용자 신원 연관	O	O	O	O	X	O	O	O	O	O	O
	잠재적인 위반 분석	O	O	O	O	X	O	O	O	O	O	O
	감사 검토 권한 제한	X	X	O	X	X	X	X	X	X	X	X
암호 지원 영역	암호키 생성	X	X	X	O	X	X	O	O	X	X	X
	암호키 분배	X	X	X	O	X	X	O	O	X	X	X
	암호키 파기	X	X	X	O	X	X	O	O	X	X	X
	암호 연산	X	X	X	O	X	X	O	O	X	X	X
사용자 데이터 보호 영역	완전한 접근통제	X	X	X	O	X	O	X	O	X	X	X
	보안속성에 기반한 접근통제	X	X	X	O	X	O	X	O	X	X	X
식별 및 인증 영역	인증	O	O	O	X	X	X	X	X	O	O	O
	비밀정보의 검증	X	X	X	O	O	O	O	O	X	X	X
	모든 행동 이전에 사용자 인증	X	X	X	O	O	O	O	O	X	X	X
	재사용 방지 인증 메커니즘	X	X	X	O	X	O	O	X	X	X	X
	인증 피드백 보호	O	O	O	O	X	O	O	O	O	O	O
보안 관리 영역	안전한 보안속성	X	X	X	O	X	X	O	X	X	X	X
	데이터 한계치의 관리	O	O	O	O	X	O	O	O	O	O	O
	안전한 보안기능 데이터	X	X	X	O	X	X	X	X	X	X	X
프라이버시 영역	가명성	X	X	X	O	X	X	O	O	X	X	X
	인가된 사용자 관찰가능성	X	X	X	X	X	X	O	X	X	X	X
보안 기능 보호 영역	추상기계 시험	X	X	O	O	O	O	O	O	O	O	O
	장애시 안전한 상태 유지	O	O	O	O	X	O	O	O	O	O	O
	외부 전송 데이터의 변경 탐지	X	X	X	X	O	X	X	X	X	X	X
	내부 전송 데이터의 기본적인 보호	X	X	X	X	O	O	X	X	O	X	O
	기능 복구	X	X	X	O	X	O	X	X	X	X	X
	재사용 공격 탐지 및 대응행동	X	X	X	O	X	X	O	O	X	X	X
	보안정책 우회불가성	X	X	O	O	X	O	O	O	O	O	O
	보안기능 영역분리	X	X	O	O	X	O	O	O	O	O	O
	신뢰할 수 있는 타임스탬프	X	X	O	O	X	O	O	O	O	O	O
자원 활용 영역	오류에 대한 내성(부분적용)	X	O	O	O	X	O	O	O	O	O	O
	최대 할당치	O	O	O	O	O	O	X	O	O	O	O
	최대와 최소 할당치	X	X	X	X	X	X	O	X	X	X	X
제품 기능 접근 영역	세션 잠금	O	O	O	O	X	O	O	O	O	O	O
안전한 경로/채널 영역	안전한 채널	X	X	O	O	X	O	O	O	O	O	O

〔표 7〕 침입차단서비스 S-SLA 지표

대분류	세부 지표	기능명
보안 감사 및 대응	위반 탐지 대응 기능	감사 데이터 생성
		감사 검토
		선택 가능한 감사 검토
		선택적인 감사
		감사 데이터 손실 예측시 대응행동
		사용자 신원 연관
	감사 데이터 보호 기능	감사 증적 보호
		감사 데이터의 손실 방지
	보안 위반 탐지 기능	보안 경보
		잠재적인 위반 분석
	감사 검토 제한 기능	감사 검토 권한 제한
키 관리 및 암호화	키 관리 기능	암호키 생성
		암호키 분배
		암호키 파기
	암호화 기능	암호 연산
데이터 보안 및 접근 통제	정보 흐름 통제 기능	부분적인 정보흐름통제
		단일 계층 보안속성
	접근 통제 기능	완전한 접근통제
		보안속성에 기반한 접근통제
인증 및 인증 정보보호	인증 기능	인증 실패 처리
		사용자 속성 정의
		모든 행동 이전에 사용자 식별
		인증 피드백 보호
		인증
		모든 행동 이전에 사용자 인증
		비밀정보의 검증
	일회용 패스워드 기능	재사용 방지 인증 메커니즘
보안 관리 및 권한 설정	권한 설정 기능	보안기능 관리
		보안속성 관리
		보안 역할
		보안기능 데이터 관리
		안전한 보안속성
	보안 관리 기능	관리기능 명세
		정적 속성 초기화
		데이터 한계치의 관리
		안전한 보안기능 데이터
가명성 보장 및 시스템 관찰	가명성 제공 기능	가명성
	시스템 관찰 기능	인가된 사용자 관찰가능성
시스템 및 데이터 보호	무결성 검증 기능	자체시험
	장애 대응 기능	장애시 안전한 상태 유지
	운영 점검 기능	추상기계 시험
	시스템 점검 기능	보안정책 우회불가성
		보안기능 영역분리
		신뢰할 수 있는 타임스탬프
	데이터 위·변조 탐지 및 복구 기능	내부 전송 데이터의 기본적인 보호
		재사용 공격 탐지 및 대응행동
		기능 복구
		외부 전송 데이터의 변경 탐지
대역폭 관리 및 가용성 보장	대역폭 관리 기능	최대 할당치
		최대와 최소 할당치
	가용성 보장 기능	오류에 대한 내성 (부분적용)
세션 보호	세션 보호 기능	세션 종료
		세션 잠금
보안 채널	보안 채널 생성 기능	안전한 채널

수 있다. 이 중에서 동일하게 제공되는 보안기능은 침입차단서비스 제품을 구성하기 위한 기본적인 보안기능으로 분류 할 수 있으며, 본 논문에서는 이를 '공통보안기능'으로 분류한다. 또한, 각 제품에 따라 달리 제공되는 보안기능은 제품에 따라 추가적인 보안기능으로 사용될 수 있으므로, '개별보안기능'으로 분류할 수 있다.

〔표 6〕에서 분석한 바와 같이 각 구분에 해당하는 보안 기능 영역은 동일한 보안목적을 가지므로, 해당 제품에 유사한 기능들이 함께 분류되어 있다. 따라서 본 기능들의 유사성에 따라 S-SLA 지표를 설정할 수 있다. 다음 표는 침입차단서비스의 보안기능에 따른 S-SLA 지표를 도출한 것이다.

4.2 S-SLA 지표 등급화

본 논문에서 적용되는 보안등급은 보안 제품에서의 보안 기능 출현 빈도와 보안 기능의 적용 수에 따라 상관관계를 가진다. 이러한 이유는 침입차단서비스를 의미하는 기본적인 보안 기능들의 집합과 추가적인 보안 기능의 증가가 가져오는 복잡성에 기인한다.

실제 제품의 보안 기능 출현 빈도는 그 빈도가 높을수록 침입차단서비스라는 서비스를 제공하기 위한 기본적인 보안 기능에 가깝다. 서로 다른 침입차단서비스 제품이라 하더라도 기본적으로 제공해야 하는 기능이 존재하고 이러한 기능은 침입차단서비스 본연의 기능을 수행하기 위한 것이기 때문이다. 상대적으로 출현 빈도가 낮은 보안 기능은 부가적인 선택 기능이 되며, 이러한 선택 기능이 결합되는 경우 각각의 보안기능이 가지는 보안성으로 인하여 전체 보안성의 향상을 가져올 수 있다. 따라서 출현 빈도가 낮은 보안 기능의 선택은 보안등급의 향상을 가져올 수 있다.

이와 같은 보안 기능이 S-SLA에 다수 포함되는 경우 고려해야 하는 보안 분야가 많아지고 이로 인해 서비스 제공 업체에서 제공해야 하는 보안서비스 수준이 증가된다. 따라서 보안등급은 보안 기능의 출현 빈도와 S-SLA에 포함되는 보안 기능의 수에 따라 분류를 나눌 수 있다.

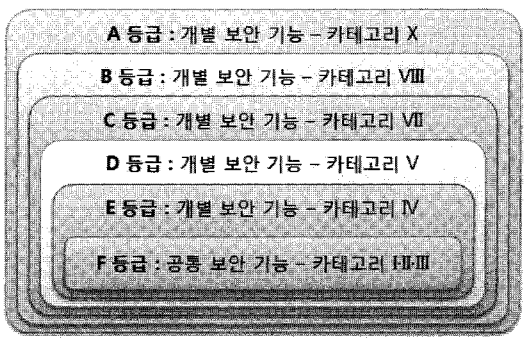
침입차단서비스의 등급화는 각 제품에 모두 포함된 공통보안기능과 선택적으로 포함된 개별보안기능을 통하여 이루어진다. 공통보안기능은 침입차단서비스를 제공하기 위하여 기본적으로 포함되어야 하는 기능으로써 모든 제품이 가지고 있는 기능을 포함하고 있다. 그리고 침입차단서비스에서 EAL3 제품이 가장 낮은 보안등급으로 그 이하의 제품이 없다는 것은 최소한 EAL3 제품의 기능만큼은 제공이 되어야 침입차단서비스를 제공할 수 있다는 의미로 해석할 수 있다. 따라서 EAL3 제품에 포함된 기능을 최소한의 적용 수준으로 규정하여 구분하고 모든 제품에 포함된 기능이 아니더라도 EAL3 제품에 포함된 기능일 경우, 이를 공통보안기능으로 설정하였다. 이와 같은 공통보안기능은 S-SLA 등급화에서 가장 낮은 수준의 등급을 가진다. 본 논문에서 공통보안기능은 카테고리 Ⅰ·Ⅱ·Ⅲ으로 분류하여 정의하고 있다.

공통보안기능 외의 개별보안기능들은 11개 제품 중 포함된 제품의 개수와 보안 기능의 연계성에 따라 분류된다. 11개 제품 중 8개 제품에 포함된 기능은 서로 다른 등급의 보안 수준을 구분하는데 사용된다. 소수의 제품에 포함되는 기능의 경우, 꼭 필요한 경우는 아니더라도 보안성 향상과 사용자의 요구에 따라 추가적으로 제공할 수 있는 기능으로 분류할 수 있으므로, 보다 높은 등급의 S-SLA 등급을 구분하는데 사용된다. 각 개별보안기능을 구성하는 카테고리는 공통보안기능에 추가되는 형식으로 구성되며, 보안등급의 정의에 따라 추가적인 보안 기능이 가지는 보안성과 공통보안기능의 보안성이 적용되어 종합적인 보안성의 증가를 가져오게 된다. 본 논문에서 개별보안기능은 카테고리 Ⅳ부터 Ⅹ까지 분류하여 정의하고 있다.

다음은 침입차단서비스 등급화 단계를 도식화한 것이다. 각 상위 등급은 하위 등급의 보안 기능을 포함한다.

4.2.1 공통보안기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ (예외 항목 Ⅵ, Ⅸ, Ⅹ 포함)

침입차단서비스의 공통보안기능은 EAL3 등급 제품과 EAL4 등급 제품에 모두 포함된 공통적인 보안



〔그림 1〕 침입차단서비스 등급화

기능이다. 공통보안기능은 EAL3, EAL4 등급 제품에 모두 적용되어 있거나, 몇 개의 EAL3 등급 제품과 EAL4 등급 제품에만 적용되어 있는 보안 기능을 포함한다.

그 중 카테고리 I은 EAL3 등급 제품과 EAL4 등급 제품에 모두 포함되어 공통적으로 제공하는 보안 기능이며, 카테고리 II는 EAL3 등급 제품에 모두 포함되어 있고 EAL4 등급 제품에서 몇 개의 제품에만 포함되어 제공하는 공통보안기능이다. 그리고 카테고리 III은 EAL3 등급 제품과 EAL 4 등급 제품에서 몇 개의 제품만 포함되어 제공하는 공통보안기능이다.

공통보안기능-카테고리 I·II·III의 인증 기능 중 모든 행동 이전에 사용자 인증(VI)과 비밀정보의 검증(VI) 기능은 EAL4 등급 제품에 포함되는 기능이지만, 적용 범위가 공통보안기능의 세부 지표인 '인증 기능'에 포함될 수 있으므로 해당 기능을 공통보안기능에 포함한다.

공통보안기능-카테고리 I의 권한 설정 기능 중 하나인 안전한 보안속성(IX) 기능은 적용 범위가 세부 지표인 '권한 설정 기능'에 포함될 수 있으므로 해당 기능을 공통보안기능에 포함한다.

공통보안기능-카테고리 I·II의 보안 관리 기능 중 하나인 안전한 보안기능 데이터(X) 기능은 적용 범위가 세부 지표인 '보안 관리 기능'에 포함될 수 있으므로 해당 기능을 공통보안기능에 포함한다.

공통보안기능-카테고리 II의 대역폭 관리 기능 중

〔표 8〕 공통보안기능 - 카테고리 I·II·III

대분류	세부 지표	기능명	카테고리
보안감사 및 대응	위반 탐지 기능	감사 데이터 생성	I
		감사 검토	I
		선택 가능한 감사 검토	I
		선택적인 감사	I
		감사 데이터 손실 예측시 대응행동	I
		사용자 신원 연관	II
	감사 데이터 보호 기능	감사 증적 보호	I
		감사 데이터의 손실 방지	I
	보안 대응 기능	보안 경보	II
		잠재적인 위반 분석	II
데이터 보안 및 접근통제	정보흐름통제 기능	부분적인 정보흐름통제	I
		단일 계층 보안속성	I
인증 및 인증 정보보호	인증 기능	인증 실패 처리	I
		사용자 속성 정의	I
		모든 행동 이전에 사용자 식별	I
		인증 피드백 보호	II
		인증	III
		모든 행동 이전에 사용자 인증	VI
		비밀정보의 검증	VI
보안 관리 및 권한 설정	권한 설정 기능	보안기능 관리	I
		보안속성 관리	I
		보안 역할	I
		보안기능 데이터 관리	I
		안전한 보안속성	IX
	보안 관리 기능	관리기능 명세	I
		정적 속성 초기화	I
		데이터 한계치의 관리	II
		안전한 보안기능 데이터	X
시스템 및 데이터 보호	무결성 검증 기능	자체시험	I
	장애 대응 기능	장애시 안전한 상태 유지	II
대역폭 관리 및 가용성 보장	대역폭 관리 기능	최대 할당치	II
		최대와 최소 할당치	X
	가용성 보장 기능	오류에 대한 내성(부분적용)	III
세션 보호	세션 보호 기능	세션 종료	I
		세션 잠금	II

〔표 9〕 개별보안기능 - 카테고리 Ⅳ

대분류	세부 지표	기능명	카테고리
시스템 및 데이터 보호	운영 점검 기능	추상기계 시험	Ⅳ

하나인 최대와 최소 할당치(X) 기능은 적용 범위가 '최대 할당치'에 포함될 수 있으므로 해당 기능을 공통 보안기능에 포함한다.

4.2.2 개별보안기능 - 카테고리 Ⅳ

카테고리 Ⅳ는 EAL4 등급 제품에서만 제공하는 보안 기능이며, 사용자는 S-SLA 협약 시 침입차단서비스 제품에서 운영 점검 기능의 추가적인 서비스를 원할 때, 선택할 수 있다.

4.2.3 개별보안기능 - 카테고리 Ⅴ

카테고리 Ⅴ는 EAL4 등급 제품에서만 제공하는 보안 기능이며, 사용자는 S-SLA 협약 시 침입차단서비스 제품에서 시스템 점검 및 보안 채널 생성 기능의 추가적인 서비스를 원할 때, 선택할 수 있다.

4.2.4 개별보안기능 - 카테고리 Ⅶ (예외 항목 Ⅷ, Ⅸ, Ⅹ 포함)

카테고리 Ⅶ는 EAL4 등급 제품에서만 제공하는 보안 기능이며, 사용자는 S-SLA 협약 시 침입차단서비스 제품에서 데이터 위·변조 탐지 및 복구 기능의 추가적인 서비스를 원할 때, 선택할 수 있다.

개별보안기능-카테고리 Ⅶ의 데이터 위·변조 탐지 및 복구 기능 중 재사용 공격 탐지 및 대응행동(Ⅷ), 기능 복구(Ⅸ), 외부 전송 데이터의 변경 탐지(Ⅹ) 기능은 적용 범위가 세부 지표인 '데이터 위·변조 탐지 및 복구 기능'에 포함될 수 있으므로 해당 기능을 개별

〔표 10〕 개별보안기능 - 카테고리 Ⅴ

대분류	세부 지표	기능명	카테고리
시스템 및 데이터 보호	시스템 점검 기능	보안정책 우회불가성	Ⅴ
		보안기능 영역분리	Ⅴ
		신뢰할 수 있는 타임스탬프	Ⅴ
보안 채널	보안 채널 생성 기능	안전한 채널	Ⅴ

〔표 11〕 개별보안기능 - 카테고리 Ⅶ

대분류	세부 지표	기능명	카테고리
시스템 및 데이터 보호	데이터 위·변조 탐지 및 복구 기능	내부 전송 데이터의 기본적인 보호	Ⅶ
		재사용 공격 탐지 및 대응행동	Ⅷ
		기능 복구	Ⅸ
		외부 전송 데이터의 변경 탐지	Ⅹ

보안기능-카테고리 Ⅶ에 포함한다.

4.2.5 개별보안기능 - 카테고리 Ⅷ

카테고리 Ⅷ는 EAL4 등급 제품에서만 제공하는 보안 기능이며, 사용자는 S-SLA 협약 시 침입차단서비스 제품에서 키 관리, 암호화, 접근통제, 일회용 패스워드, 가명성 제공 기능의 추가적인 서비스를 원할 때, 선택할 수 있다.

4.2.6 개별보안기능 - 카테고리 Ⅹ

카테고리 Ⅹ는 EAL4 등급 제품에서만 제공하는 보안 기능이며, 사용자는 S-SLA 협약 시 침입차단서비스 제품에서 감사 검토 제한, 시스템 관찰 기능의 추가적인 서비스를 원할 때, 선택할 수 있다.

4.2.7 등급 분류

본 논문에서는 침입차단서비스 S-SLA 등급화를

〔표 12〕 개별보안기능 - 카테고리 Ⅷ

대분류	세부 지표	기능명	카테고리
키 관리 및 암호화	키 관리 기능	암호키 생성	Ⅷ
		암호키 분배	Ⅷ
		암호키 파기	Ⅷ
	암호화 기능	암호 연산	Ⅷ
데이터 보안 및 접근통제	접근통제 기능	완전한 접근통제	Ⅷ
		보안속성에 기반한 접근통제	Ⅷ
인증 및 인증 정보보호	일회용 패스워드 기능	재사용 방지 메커니즘	Ⅷ
가명성 보장 및 시스템 관찰	가명성 제공 기능	가명성	Ⅷ

〔표 13〕 개별보안기능 - 카테고리 X

대분류	세부 지표	기능명	카테고리
보안 감사 및 대응	감사 검토 제한 기능	감사 검토 권한 제한	X
가명성 보장 및 시스템 관찰	시스템 관찰 기능	인가된 사용자 관찰가능성	X

총 6등급(A, B, C, D, E, F)으로 분류하였으며, 제공되는 보안기능의 제품 적용 정도와 제품의 EAL 등급에 따라 차등적으로 등급을 분류하였다. F 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ을 포함하는 등급이며, E 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ에 개별 보안 기능 - 카테고리 Ⅳ를 추가한 등급이다. D 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ에 개별 보안 기능 - 카테고리 Ⅳ·Ⅴ를 추가한 등급이며, C 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ에 개별 보안 기능 - 카테고리 Ⅳ·Ⅴ·Ⅶ을 추가한 등급이다. 또한 B 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ에 개별 보안 기능 - 카테고리 Ⅳ·Ⅴ·Ⅶ·Ⅷ을 추가한 등급이며, A 등급은 공통 보안 기능 - 카테고리 Ⅰ·Ⅱ·Ⅲ과 개별 보안 기능 - 카테고리 Ⅳ·Ⅴ·Ⅶ·Ⅷ·X 모두를 포함한 등급이다.

〔표 14〕와 같은 침입차단서비스를 위한 S-SLA 등급화를 통하여 사용자는 자신이 원하는 보안기능을 선택적으로 제공받을 수 있으며, 이를 통해 불필요한 서비스를 최소한으로 줄일 수 있는 장점이 존재한다. 이러한 보안기능의 부분 선택 방식을 통해 사용자가 부담해야할 금전적인 이익과 불필요한 기능으로 인해 발생할 수 있는 문제점 등을 미연에 방지할 수 있다.

〔표 14〕 침입차단서비스 S-SLA 등급 분류

S-SLA 등급	세부 지표 목록							기능명
A 등급	감사 검토 제한 기능							감사 검토 권한 제한
	시스템 관찰 기능							인가된 사용자 관찰가능성
	B 등급	키 관리 기능						암호키 생성, 암호키 분배, 암호키 파기
		암호화 기능						암호 연산
		접근통제 기능						완전한 접근통제, 보안속성에 기반한 접근통제
		일회용 패스워드 기능						재사용 방지 메커니즘
		가명성 제공 기능						가명성
		C 등급	데이터 위·변조 탐지 및 복구 기능					내부 전송 데이터의 기본적인 보호, 재사용 공격 탐지 및 대응행동, 기능 복구, 외부 전송 데이터의 변경 탐지
			D 등급	시스템 점검 기능				보안정책 우회불가성, 보안기능 영역분리, 신뢰할 수 있는 타임스탬프
				보안 채널 생성 기능				안전한 채널
				E 등급	운영 점검 기능			추상기계 시험
					F 등급	위반 탐지 기능		감사 데이터 생성, 감사 검토, 선택 가능한 감사 검토, 선택적인 감사, 감사 데이터 손실 예측시 대응행동, 사용자 신원 연관
						감사 데이터 보호 기능		감사 증적 보호, 감사 데이터의 손실 방지
						보안 대응 기능		보안 경보, 잠재적인 위반 분석
						정보흐름통제 기능		부분적인 정보흐름통제, 단일 계층 보안속성
						인증 기능		인증 실패 처리, 사용자 속성 정의, 모든 행동 이전에 사용자 식별, 인증 피드백 보호, 인증, 모든 행동 이전에 사용자 인증, 비밀정보의 검증
						권한 설정 기능		보안기능 관리, 보안속성 관리, 보안 역할, 보안기능 데이터 관리, 안전한 보안속성
						보안 관리 기능		관리기능 명세, 정적 속성 초기화, 데이터 한계치의 관리, 안전한 보안기능 데이터
						무결성 검증 기능		자체시험
						장애 대응 기능		장애시 안전한 상태 유지
						대역폭 관리 기능		최대 할당치, 최대와 최소 할당치
						가용성 보장 기능		오류에 대한 내성(부분적용)
						세션 보호 기능		세션 종료, 세션 잠금

V. 결 론

서비스수준협약(SLA)은 서비스를 보다 효율적이고 명확하게 이용하기 위해 꼭 필요한 기준이라고 할 수 있다. 각 서비스에서 제공될 수 있는 기능의 성능 및 기준치를 규정하고 서비스 이용 시 이에 대한 확인을 통해 자신이 서비스를 제대로 제공받고 있는지 확인할 수 있다. 사용자 뿐만 아니라 사업자 측면에서도 자신이 제공하는 서비스가 정상적으로 동작하고 있는지 확인할 수 있는 근거로 활용할 수 있다. 특히 보안서비스는 타 서비스에 비해 상대적으로 보다 안전하고 확실한 서비스를 제공할 필요가 있어, 이와 같은 서비스수준협약이 절실하다.

그러나 보안서비스에 대한 서비스수준협약인 S-SLA에 대한 국내의 연구 및 사용자의 인식 수준은 전무한 실정이다. 따라서 보다 효율적이고 명확한 보안서비스를 제공받기 위하여 S-SLA에 대한 연구가 필요하다.

이에 본 논문에서는 S-SLA에 대한 인식 제고와 보다 효율적이고 명확한 보안서비스수준협약을 위한 침입차단서비스의 S-SLA 지표 개발 및 등급화 방안을 제안하였다. 이를 위하여 침입차단서비스의 보안기능을 분석하고, 각 보안기능을 6개의 등급으로 나누어 도출하였다. S-SLA 등급은 서비스를 이용하고자 하는 사용자가 선택적으로 이용할 수 있다.

본 논문에서 제안한 S-SLA 지표 및 등급화 방안은 추후 다양한 서비스의 S-SLA 지표 및 기준 개발을 위한 초석 자료로 활용할 수 있을 것으로 기대되며, 국내 S-SLA 환경 조성 및 사용자 인식의 제고를 가져올 수 있을 것으로 판단된다.

VI. 참고문헌

[1] 김대웅, 이길행, 김영선, "서비스수준협약(SLA) 기술동향," 전자통신동향분석, 19(6), pp. 55-65. 2004년 12월.

[2] 한국정보화진흥원, "SLA를 강화한 정보시스템 운영계약 참조모델," 2005년 12월.

[3] 조현정, "차세대 네트워크 보안기술 기반의 침입방지시스템(IPS)," 정보과학회지, 23(1), pp. 21-26, 2005년.

[4] LG CNS, "SafezoneIPS V4.0 보안목표명세서 V4.00.01," IT보안인증사무국, 2010년 5월.

[5] 모보, "SecureGate-II V1.0 보안목표명세서," IT보안인증사무국, 2009년 11월.

[6] 나우콤, "SNIPER IPS V7.0e 보안목표명세서 v1.02," IT보안인증사무국, 2009년 9월.

[7] 시큐아이닷컴, "SECUI NXG V2.2.0 보안목표명세서 v1.2," IT보안인증사무국, 2008년 월.

[8] 안철수연구소, "TrusGuard SCM 1.0 and TrusGuard SCM Manager 1.5 보안목표명세서," IT보안인증사무국, 2008년 12월.

[9] 삼성네트웍스, "eXshield V1.0.1.R 보안목표명세서 V1.10," IT보안인증사무국, 2008년 6월.

[10] 어울림정보기술, "SECUREWORKS SEPION V4.0 보안목표명세서 Version 1.3," IT보안인증사무국, 2008년 1월.

[11] 퓨처시스템, "FutureUTM 6000 V1.0 보안목표명세서," IT보안인증사무국, 2009년 11월.

[12] 정보보호기술, "TESS TMS V4.5 보안목표명세서 V19," IT보안인증사무국, 2006년 12월.

[13] 어울림정보기술, "SECURE WORKS IPSWall 1000 V4.0 보안목표명세서 Version 1.23," IT보안인증사무국, 2006년 8월.

[14] 안철수연구소, "Absolute IPS-NP v1.0 보안목표명세서," IT보안인증사무국, 2010년 3월.

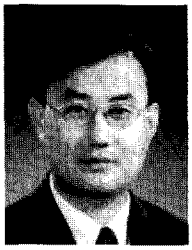
[15] ISO/IEC, "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 1: Introduction and general model," 2007.

[16] ISO/IEC, "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 2: Security functional components," 2007.

[17] ISO/IEC, "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 3: Security assurance components," 2007.

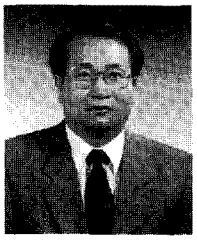
[18] Ganna Frankova, "Service Level Agreements: Web Services and Security," Lecture Notes in Computer Science, Vol. 4607, pp. 556-562, August. 2007.

〈著者紹介〉

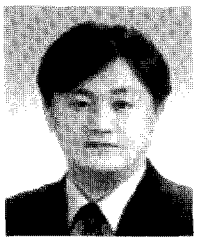


이 완 석 (Wan S. Yi) 특별회원
1991년 5월: Va. Tech. 전산과학과 학사 졸업
2001년 2월: 동국대학교 정보보호학과 석사 졸업
2004년 9월~현재: 성균관대학교 전자공학과 박사과정
1994년 7월~96년 6월: 현대정보기술 사원
1996년 7월~현재: 한국정보보호진흥원 인터넷서비스보호팀장
〈관심분야〉 정보보증, 정보보호 제품 평가, 정보통신기반보호, 신규 IT서비스 보호 등

고 웅 (Woong Go) 학생회원
2008년 2월: 순천향대학교 정보보호학과 졸업
2008년 3월~2010년 2월: 순천향대학교 정보보호학과 석사
2010년 3월~현재: 순천향대학교 정보보호학과 박사과정
〈관심분야〉 정보보호, 보안성 평가, 개인정보보호, 융합보안 등



원 동 호 (Dongho Won) 평생회원
1976년~1988년: 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
〈관심분야〉 암호이론, 정보이론, 정보보호 등



곽 진 (Jin Kwak) 종신회원
1994~2006년: 성균관대학교 전자공학과(공학사 공학석사, 공학박사)
2006~2006: 일본 큐슈대학교 방문연구원
2006~2006: 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007: 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009: 정보통신연구진흥원 집필위원
2009~2009: 순천향대학교 공과대학 교학부장
현재 : 정보통신산업진흥원 기술평가위원, 디지털아이디관리포럼 기술평가위원, 한국정보통신기술협회 JTC/SC27 분과 기술위원, 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원, 순천향대학교 정보보호학과 학과장, 순천향BIT 창업보육센터 소장, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원, 교육과학기술부 국가기술 수준 평가 전문위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원
〈관심분야〉 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등