Journal of Digital Contents Society Vol. 16 No. 2 Apr. 2015(pp. 345-353)
http://dx.doi.org/10.9728/dcs.2015.16.2.345

보안관제시스템 보호프로파일 개발

손승완*, 김광석*, 최정원* 이강수*

요 약

보안관제시스템은 보안관제를 위해 보안관제센터에서 운영하고 있는 시스템이다. 최근 인터넷 가입자의 급격한 증가와 더불어 생활 전반의 모든 일들이 웹 서비스를 통하여 이루어짐에 따라 네트워크 보안에 대한 필요성이 급격히 증가하였고, 이에 따라 사이버 보안관제가 큰 이슈가 되어 각 기관에서는 보안관제시스템을 구축하여 보안관제 업무를 수행하고 있다. 하지만 보안관제시스템에 대한 보안 기능 요구사항이 정확히 명시되지 않아, 보안관제시스템을 구축 및 설계 개발 하는데 있어 많은 어려움이 있어 보호프로파일이 필요성이 요구된 실정이다. 본 논문에서는 보안관제시스템의 보안 기능 요구사항 명세를 위한 보안관제시스템 보호프로파일을 개발 하였다.

키워드 : 보안관제, 보안관제시스템, 보호프로파일

Development of Managing Security Services System Protection Profile

Seung-Wan Son*, Kwang-Seok Kim*, Jung-Won Choi*, Gang-Soo Lee*

Abstract

Security Management System is a system which operates in the security control center for security control. All living things across the Internet in recent years, with the rapid increase in the subscriber base has increased the need for network security dramatically depending on yirueojim through web services, thus cyber security sheriff, I have a big issue to build a security management system, each agency and perform control tasks. But the security functional requirements for security management system would not specified exactly, in developing a security management system to build and design a situation that PP's needs require a lot of trouble. In this paper, we develop a Managed Security System Protection Profile for the security functional requirements specification of the security management system.

Keywords : Managing Security, Managing Security Services, Protection Profile

1. 서론

보안관제란 용어는 영어로는 Managing Security Services 또는 Security Monitoring & Control 등으로 사용되고 있는데 Monitoring의 사전적 의미는 '컴퓨터의 프로그램 수행 중 일어날 수 있는 여러 가지 오류에 대비하기 위한 감시활동'이라고 설명되어 있다.

우리나라에서는 보안관제의 개념에 관한 명확한 정의가 없는 상태에서 민·관·군에서도 '보안관제'란 용어를 도입하여 사용해 오고 있다.[1]

최근에는 생활 전반의 모든 일들이 웹 서비스를 통하여 이루어짐에 따라 네트워크 보안에 대한 필요성이 급격히 증가하였고, 사이버 보안 관제가 큰 이슈로 떠오르고 있다. 이러한 보안 관제를 위해서 각 기관에서는 보안 관제 센터를

※ Corresponding Author : Gang-Soo Lee
Received : March 13, 2015
Revised : April 27, 2015
Accepted : April 30, 2015
* Hannam University Computer Engineering
Tel: +82-42-629-7549 , Fax: +82-42-629-8120
email: gslee@hnu.ac.kr
▣ 본 연구는 한남대학교의 2014학년도 교비학술연구비 지원에 의해 수행되었음

구축해 MSSS(MSSS, Managing Security Services System)를 운영하고 있다.

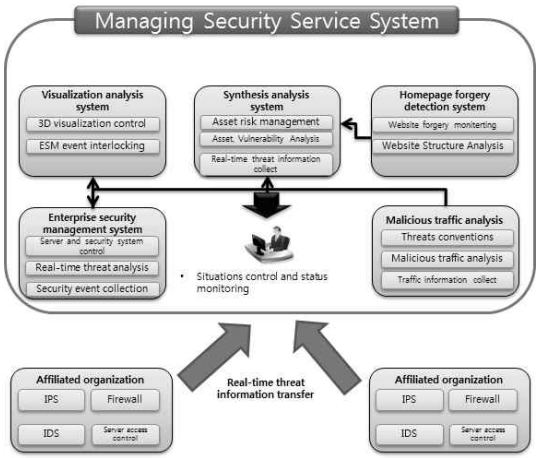
본 논문에서는 사이버 보안 관제센터 운영을 위한 MSSS 보호프로파일 개발 한다. 2장에서는 MSSS의 운영환경과 MSSS의 범위를 설정하고, 3장에서는 보안문제를 정의하며 보안목적을 도출한다. 4장에서는 3장에서 도출한 내용을 바탕으로 보안기능요구사항을 도출하고, 5장에서는 저자가 속해 있는 연구팀에서 개발한 SRS-Gen 개발 지원도구를 이용하여 보호프로파일을 개발하며, 6장에서 제어시스템 보호프로파일과 비교분석 후 7장에서 결론을 맺는다.

2. 보안관제시스템 개요

2.1 보안관제시스템의 운영환경

MSSS는 그래프나 그림으로 시각화 하여 표현하는 시각화 분석시스템, 자산별 위험도 관리 및 취약점을 분석하고 실시간 위협정보를 수집하는 종합 분석 시스템, 홈페이지의 위변조를 탐지하고 웹사이트의 구조를 분석하는 홈페이지 위변조 시스템, 유해 트래픽 분석 및 트래픽 정보를 수집하는 유해트래픽 분석 시스템, 서버 및 보안 시스템을 관리하고 실시간 보안 위협을 분석하며 보안 이벤트를 수집하는 통합 보안 관리 시스템으로 구성되어 운영된다.

(그림 1) MSSS의 운영 환경[2]



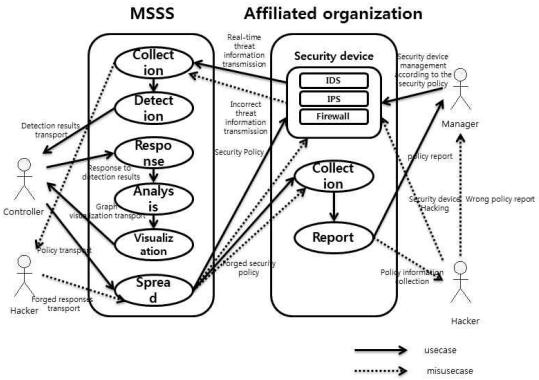
(Figure 1) MSSS operating environments[2]

(그림 1)은 MSSS의 운영환경을 나타낸 그림이다. MSSS를 운영하는 보안관제센터에서는 각각의 피관제기관의 IPS, 방화벽 등으로부터 실시간으로 보안 위협 정보를 전송 받는다. 전송받은 보안 위협 정보를 이용하여 각각의 시스템에서 업무를 처리하고 그 결과를 가지고 보안관제사는 상황 관제 및 현황을 모니터링하고 사고처리 및 경보를 발령한다.

2.2 보안관제시스템 취약점 분석

MSSS의 취약점을 분석하기 위해 usecase 및 misusecase다이어그램을 이용하였다.

(그림 2) MSSS의 usecase 및 misusecase 다이어그램



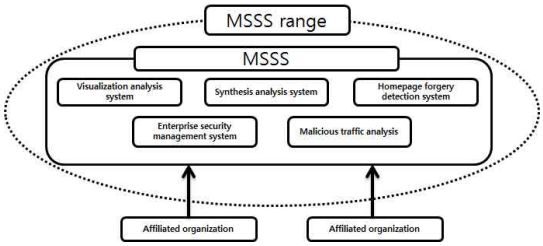
(Figure 2) MSSS usecase and misusecase diagram

(그림 2)는 MSSS의 usecase 및 misusecase 다이어그램을 나타낸 그림이다. 실선으로 표시된 정상적인 경우 MSSS는 피관제기관으로부터 실시간 위협정보를 전송받아 위협을 탐지하여 관제사에게 전송한다. 관제사는 전송받은 위협정보를 통해 대응책을 마련하고 피관제기관으로 보안정책 및 경보를 발령한다. 점선으로 표시된 비정상적인 경우 위협원은 피관제기관을 대신하여 MSSS에 위·변조된 위협을 전송하거나 MSSS에 직접 침투하여 위·변조된 보안정책 및 경보를 발령시킨다. 또한 피관제기관에 침투하여 피관제기관의 관리자에게 위·변조된 정보를 전송할 수도 있다.

2.3 MSSS 범위 설정

보호프로파일에서 MSSS의 범위는 시각화 분석 시스템, 종합분석시스템, 통합 보안관리시스템, 유해트래픽 분석 시스템, 홈페이지 위변조 탐지 시스템을 하나로 묶어 MSSS로 정의하고, 피관제기관의 각 보안장비로부터 정보를 전송받는 통신망 까지를 그 범위로 한다.[3]

(그림 3) MSSS의 범위[2]



(figure 3) MSSS range

MSSS는 산하기관과의 통신을 통해 산하기관으로부터 로그정보 및 이벤트를 수집한다. 따라서 산하기관과의 통신에서 전송되는 로그 정보 및 이벤트는 노출 및 변경으로 부터 보호되어야 한다. 또한 관리자 및 사용자의 신원을 식별 및 인증해야 하며, 보안과 관련된 행동에 대한 책임을 추적하기 위해 감사로그를 생성하고 감사로그로부터 감사데이터를 검토해야 한다.

3. 보안문제 및 보안목적 정의

3.1 보안문제 정의

보안문제 정의는 MSSS 및 MSSS 운영환경이 다루도록 의도된 위협, 조직의 보안정책 및 가정사항을 다룬다.

3.1.1 위협

위협은 일반적으로 MSSS가 보호하고자하는 자산에 불법적인 접근을 시도하거나 비정상적인 방법으로 자산에 위해를 가하는 행위 및 행위자를 말한다. 다음은 위협에 대한 항목이다.[3],[4],[5]

T.1 고장

MSSS가 외부의 공격 등에 의해 고장이 발생하여 사용자에게 정상적인 서비스를 제공하지 못해 위협원이 이를 악용할 수 있다.

T.2 기록실패

위협원은 저장용량을 소진시켜서 MSSS의 보안관련 사건이 기록되지 않도록 할 수 있다.

T.3 연속인증시도

위협원은 MSSS에 접근하기 위해 연속적으로 인증을 시도하여 인가된 사용자 권한을 획득 할 수 있다.

T.4 가장

위협원은 인가된 주체로 가장하여 MSSS에 접근할 수 있다.

T.5 저장데이터훼손

위협원은 데이터를 인가되지 않은 방식으로 노출, 변경, 삭제할 수 있다.

T.6 장애

TSF데이터 혹은 사용자 데이터는 MSSS 장애를 통해 위협원에게 변경되거나 노출될 수 있다.

T.7 전송데이터 훼손

위협원은 통신상의 데이터를 인가되지 않은 방식으로 노출, 변경할 수 있다.

T.8 불법서비스 접근

위협원은 허가되지 않은 자산에 접근하여, 정상적인 자산의 서비스 제공을 방해할 수 있다.

T.9 남용

MSSS의 인가된 사용자는 고의로 또는 기타 이유로 MSSS 보안기능을 손상시킬 수 있다.

T.10 정보누출

위협원은 MSSS를 정상적으로 사용하는 동안 MSSS로부터 누출된 정보를 악용할 수 있다.

T.11 과도한 역할 획득

사용자에게 역할이 할당되는 과정에서, 사용자는 과도하게 설정되거나 상충되는 역할을 통해 객체에 대한 의도되지 않은 접근 허가를 획득할 수 있다.

T.12 불법침해

위협원은 불법적인 접근이나 악성프로그램 설치 등을 통해 객체를 손상시키거나 MSSS 동작 오류를 일으킬 수 있다.

T.13 유사성

위협원은 MSSS가 보호하는 자산에 접근하기 위해 등록자와 유사하거나 동일할 가능성이 높은 참조 템플릿을 공격할 수 있다.

T.14 불법정보유출

내부의 사용자가 네트워크를 통하여 불법적으

로 정보를 외부로 유출할 수 있다.

3.1.2 조직의 보안정책

조직의 보안 정책은 본 보호프로파일을 수용하는 MSSS에서 준수되어야 한다. 다음은 조직의 보안정책에 대한 항목이다.[3],[4],[6],[7],[8],[9],[10]

P.1 감사

보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 적절하게 검토되어야 한다.

P.2 안전한 관리

MSSS는 인가된 관리자가 안전한 방식으로 MSSS를 관리할 수 있도록 관리 수단을 제공해야 한다.

P.3 식별 및 인증

정보에 대한 접근이 인가되기 전에 식별 및 인증 과정을 거쳐야 한다.

P.4 비밀성

MSSS와 통신하는 통신상대로부터 전송되는 네트워크 트래픽은 MSSS 보안정책에서 명세된 경우 MSSS에 의해서 암·복호화 된다.

1.1.1 3.1.3 가정사항

가정사항은 운영환경에서 시행되거나 유지되어야 하는 가정사항을 보여준다. MSSS가 가정사항을 만족시키지 못하는 운영환경에 설치될 경우, MSSS는 모든 보안 기능성을 제공할 수 없게 될 것이다. 다음은 가정사항에 대한 항목이다.[3],[4],[6],[7],[8],[9],[10]

A.1 물리적 보안

MSSS는 물리적으로 안전한 환경에 위치하며 인가되지 않은 물리적 접근으로부터 보호된다.

A.2 신뢰된 관리자

MSSS의 인가된 관리자는 악의가 없으며, MSSS 관리 기능에 대하여 적절히 교육받았고, 모든 관리자 지침에 따라 정확하게 의무를 수행한다.

A.3 운영체제 보강

MSSS에 의해 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장한다.

A.4 안전한 채널

원격의 MSSS 관리자와 MSSS 사이에 전송되는 TSF 데이터를 인가되지 않은 방식으로부터 보호된다.

3.2 보안목적 정의

보안목적은 MSSS에 대한 보안목적 및 운영환경에 대한 보안목적으로 분류하여 정의한다. MSSS에 대한 보안목적은 MSSS에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 MSSS가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 보안목적이다.

다음은 MSSS에 대한 보안목적과 운영환경에 대한 보안목적을 정의한 항목이다.[3],[4],[5],[11],[12]

1.1.2 3.2.1 MSSS에 대한 보안목적

O.1 감사

MSSS는 보안과 관련된 모든 행동의 책임 추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야 한다.

O.2 관리

MSSS는 MSSS의 인가된 관리자가 MSSS를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.

O.3 식별 및 인증

MSSS는 사용자를 유일하게 식별해야 하며, MSSS의 관리 및 객체에 대한 접근을 허용하기 전에 사용자의 신원을 인증해야 한다.

O.4 저장데이터보호

MSSS는 MSSS에 저장된 TSF데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.

O.5 전송데이터보호

MSSS는 통신과 전송되는 데이터를 인가되지 않은 노출, 변경으로부터 보호해야 한다.

O.6 정보흐름통제

MSSS는 보안정책에 따라 외부망에서 내부망으로 인가되지 않은 정보흐름을 통제해야 한다.

O.7 안전한 상태유지

MSSS는 TSF의 장애가 발생한 경우 안전한 상태를 유지해야 하며, 장애에 의한 TSF 및 TSF 데이터 손실을 탐지하기 위한 자체 시험을 수행해야 한다.

1.1.3 3.2.2 운영환경에 대한 보안목적

OE.1 안전한 채널

원격의 MSSS 관리자와 MSSS 사이에 전송되는 TSF 데이터를 인가되지 않은 방식으로부터 보호되어야한다.

OE.2 운영체제보강

MSSS에 의해 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장해야 한다.

OE.3 신뢰된 관리자

MSSS의 인가된 관리자는 악의가 없으며, MSSS 관리 기능에 대해 적절히 교육을 받았고, 모든 관리자 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다.

OE.4 물리적 보안

MSSS는 물리적으로 안전한 환경에 위치해야 하며, 인가되지 않은 물리적 접근으로부터 보호되어야 한다.

3.3 보안목적의 이론적 근거

보안목적의 이론적 근거는 명세한 보안목적이 적합하고, 보안문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다. 보안목적의 이론적 근거는 각 위협, 조직의 보안정책, 가정사항이 최소한 하나의 보안목적에 의해서 다루어지고, 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다룬다는 것을 입증한다.

다음의 <표 1>은 보안목적의 이론적 근거를 나타낸 표이다.

<표 1> 보안목적의 이론적 근거

Security object / Threat	MSSS Security object							Operating environments security object			
	O.1	O.2	O.3	O.4	O.5	O.6	O.7	OE.1	OE.2	OE.3	OE.4
T.1		X		X			X				
T.2	X										
T.3			X								
T.4	X		X								
T.5			X	X							
T.6							X				
T.7				X	X			X			
T.8		X				X					
T.9	X		X								
T.10						X					
T.11		X	X							X	
T.12			X				X				
T.13			X								
T.14						X					
P.1	X		X								
P.2		X								X	
P.3			X								
P.4					X						
A.1											X
A.2										X	
A.3									X		
A.4					X			X			

<Table 1> Security objectives rationale

4. 보안기능 요구사항 정의

4.1 보안기능요구사항 정의

본 장에서는 앞에서 도출한 보안문제 및 보안목적을 바탕으로 보안기능요구사항을 도출한다. 보안기능 요구사항은 CC V3.1 R4를 근간으로 한다. CC에 명시되어 있지 않은 보안기능 요구사항을 도출하기 위해 확장 컴포넌트를 정의해야 한다. 본 보호프로파일에서는 3개의 확장 컴포넌트를 정의하였다. 다음의 <표 2>는 확장 컴포넌트를 포함한 본 보호프로파일의 보안기능 요구사항을 나타낸다. [7],[9],[13],[14]

<표 2> 보안기능 요구사항

Security functional requirements	Explanation
FAU_ARP.1	Security alarms
FAU_ARP.2	Security Response [Expansion]

Security functional requirements	Explanation
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_COL.1	Collect audit data [Expansion]
FAU_SAA.1	Potential Violation Analysis
FAU_SAA.4	Complex attack heuristics
RAU_SAR.1	Audit Review
RAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1	Subset access control
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MTD.2	Management of limits on TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_STA.1	Audit occurred when performing statistical data
	[Expansion]
FPT_FLS.1	Failure with preservation of secure state
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.2	Notification of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_RCV.3	Automated recovery without undue loss
FPT_RCV.4	Function recovery
FPT_TST.1	TSF testing
FTA_SSL.1	TSF-initiated session locking
FTP_ITC.1	Inter-TSF trusted channel

<Table 2> Security functional requirements

4.2 보안기능요구사항의 이론적 근거

보안기능요구사항의 이론적 근거는 MSSS 보안목적이 적어도 하나의 MSSS 보안기능 요구사항에 의해서 다루어지고, MSSS 보안기능 요구사항은 적어도 하나의 MSSS 보안 목적을 다룬다는 것을 입증한다. <표 3>은 보안목적과 보안기능요구사항 사이의 대응관계를 보여준다.

<표 3> 보안목적과 보안기능 요구사항 대응

Security object / Security issues	MSSS Security object							Operating environments security object			
	O.1	O.2	O.3	O.4	O.5	O.6	O.7	OE.1	OE.2	OE.3	OE.4
FAU_ARP.1	X		X								
FAU_ARP.2	X										
FAU_GEN.1	X										
FAU_GEN.2	X									X	
FAU_COL.1	X										
FAU_SAA.1	X		X								
FAU_SAA.4	X										
RAU_SAR.1	X										
RAU_SAR.2	X										

Security object / Security issues	MSSS Security object							Operating environments security object			
	O.1	O.2	O.3	O.4	O.5	O.6	O.7	OE.1	OE.2	OE.3	OE.4
FAU_SAR.3	X										
FAU_SEL.1	X										
FAU_STG.1	X										
FAU_STG.3	X										
FAU_STG.4	X										
FDP_ACC.1				X							X
FDP_ETC.1											X
FDP_IFC.1				X		X					
FDP_ITT.1					X						
FDP_UCT.1					X		X				
FDP_UIT.1					X		X				
FIA_AFL.1				X							
FIA_ATD.1	X			X		X				X	
FIA_UAU.2		X	X	X							
FIA_UID.1		X	X	X						X	
FIA_UID.2	X	X	X	X		X				X	
FMT_MOF.1		X		X							
FMT_MSA.1		X						X	X		
FMT_MTD.2		X									
FMT_SMF.1		X							X		
FMT_SMR.1		X	X						X		
FMT_STA.1		X									
FPT_FLS.1		X				X	X				
FPT_ITC.1				X	X						
FPT_ITT.1		X		X	X			X			
FPT_PHP.1				X							X
FPT_PHP.2	X										X
FPT_PHP.3		X									X
FPT_RCV.3		X					X				
FPT_RCV.4							X				
FPT_TST.1		X		X			X				
FTA_SSL.1		X		X							
FTP_ITC.1					X			X			

<Table 3> Security objectives and security functional requirements

5. SRS-Gen을 이용한 보호프로파일 개발

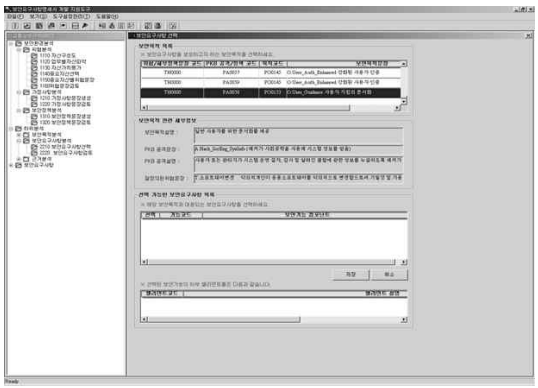
본 논문에서 개발한 MSSS 보호프로파일은 저자가 속해있는 연구팀에서 개발한 SRS-Gen이라는 개발 지원 도구를 이용하여 보호프로파일을 완성하였다.

SRS-Gen은 보호프로파일 개발 시에 꼭 필요한 위협, 가정사항, 보안정책, 보안목적 문장을 생성기능을 포함하고 있으며, 보안요구사항 생성기능까지 갖추고 있다.[16],[17]

SRS 개발 지원도구는 자산 파악, 위협문장생성, 가정사항문장생성, 보안정책문장생성, 보안목적문장생성, 보안요구사항 선택 등의 모듈로 구성되어 있고, DB 와의 연동을 통해 보호프로파일을 생성한다.

(그림 4)는 SRS 개발 지원도구의 실행 화면의 한 예로 보안 요구사항 선택 화면을 나타낸 것이다.

(그림 4) 개발 지원 도구 보안기능요구사항 선택화면



(Figure 4) Development Support Tools security functional requirement selection screen

6. 제어시스템 보호프로파일과의 비교분석

MSSS는 제어시스템과 유사한 운영환경을 가지고 있다. 이에따라 MSSS 보호프로파일과 제어시스템 보호프로파일을 비교분석 하였다. [14]

<표 4> 제어시스템 보호프로파일과의 비교분석

MSSS PP	Control system PP
· CC V3.1 R4-based writing. ·Set the range of M	· Written in older versions of CC, CC does not have the lat

MSSS PP	Control system PP
MMS to the system and avoid network to communicate with ATC to operate in the center, except for blood ATC. · Minimize the extended components definition.	est version of the latest artist. · Setting a range of the control system for all operating system environment to a range including the sensor of the control system. ·Plenty is extended component.

<Table 4> Comparative analysis of the control System Protect Profile

7. 결 론

본 논문은 MSSS을 정의 하고, CC V.31 R4에서 보안기능 요구사항을 도출하여 SRS 지원도구를 통해 MSSS 보호프로파일을 개발 하였다. 본 논문에서 개발한 MSSS 보호프로파일은 MSSS의 운영 및 설계에 있어서 기초가 될 수 있다.

사이버 보안이 큰 이슈가 되고 있는 만큼 MSSS의 중요성은 더욱더 커지고 있다. MSSS는 사이버 보안 뿐만 아니라 다양한 분야에서 사용이 가능하므로 MSSS를 솔루션 형태로 만들어 제품화 시켜 보급할 필요성이 있다. 최근에 개인정보 유출이 문제가 되고 있는 만큼 본 보호프로파일을 응용한 개인정보보호 보안관제 보호프로파일 개발을 향후 과제로 남긴다.

References

[1] Y. J. Kim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services”, Journal of the Korea Institute of Information Security and Cryptology, Vol.19, No.1, February 2009.

[2] S. J. Ann, “Security Monitering & Control”, Leehan media, April 2014.

[3] Korea Information Security Agency, "Guide for the production of Protection profiles and Security targets", July 2007.

[4] CC, "Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 4", September 2012.

[5] H. J. Lee, "Reuse way of Protection Profile to draw Security Functional Requirements Based on Common Criteria", Sogang University Graduate School of Information and Communication, December 2012.

[6] K. S. Han, "Design of instrumentation and control system nuclear protection profile(NPP-ICS) based on nuclear cyber security guideline", Hannam University, February 2013.

[7] Korea Information Security Agency, "Enterprise Security Management System Protection Profile V 2.0", September 2008.

[8] Korea Information Security Agency, "Intrusion Detection System Protection Profile V2.0", April 2008.

[9] Korea Information Security Agency, "Network Intrusion Prevention System Protection Profile V2.1", June 2010.

[10] Korea Information Security Agency, "Role Based Access Control System Protection Profile V2.0", July 2008.

[11] H. S. Jo, "A Study on Development to Be Protection Profile for Interoperability of Heterogeneous DRM Systems", information processing society journal C, Vol.16, No., February 2009.

[12] Y. J. Jo, "Analysis of Security Requirements on DCU and Development Protection Profile based on Common Criteria Version 3.1", Journal of the Korea Institute of Information Security and Cryptology, Vol.24, No.5, October 10.

[13] CC, "Common Criteria for Information Technology Security Evaluation Part 2: Security functional com

ponents Version 3.1 Revision 4", September 2012.

[14] NIST, "System Protection Profile-Industrial Control Systems Version 1.0", October 2004.

[15] H. Jung, "A Study on the Security Requirements for Developing Protection Profiles", Journal of the Korea Institute of Information Security and Cryptology, Vol.17, No.1, February 2007.

[16] G. S. Ko, "Support tool for cloud system security functional requirement specification", Hannam University, February 2011.

[17] Y. S. Kim, "Development of Security Functional Requirement Specification Tool of Information Security Operational System Level", Journal of Security Engineering, Vol.07, No.1, February 2007.

손 승 완

2013년 : 한남대학교 컴퓨터공학과 공학사
2015년 : 한남대학교 대학원 컴퓨터공학과 공학석사

관심분야 : 정보보호, 보안관제, 소프트웨어공학

김 광 석

2013년 : 한남대학교 컴퓨터공학과 공학사
2015년 : 한남대학교 대학원 컴퓨터공학과 공학석사

관심분야 : 정보보호, 보안관제, 소프트웨어공학

최 정 원

2014년 : 한남대학교 컴퓨터공학과 공학사
2015년 : 한남대학교 대학원 컴퓨터공학과 석사과정 재학

관심분야 : 정보보호, 보안관제, 소프트웨어공학

이 강 수

1981년 : 홍익대학교 학서
1983년 : 서울대학교 대학원 전산학 이학석사
1985년 : 서울대학교 대학원 전산학 이학박사

1987년~현 재: 한남대하교 컴퓨터통신무인기술학과 교수

관심분야 : 보안공학, 소프트웨어공학, 웹공학