설계단계에서 보안 속성 설계

신성윤* · 신광성*· 이현창**· 진찬용**

*군산대학교 컴퓨터정보통신공학부

**원광대학교 정보·전자상거래학부

Security Attribute Design in Security

Seong-Yoon Shin* · Kwang-Seong Shin**· Hyun-Chang Lee**· Chan-Yong Jin**

*Kunsan National University

**Wonkwang University

E-mail : {s3397220,waver}@kunsan.ac.kr, {hclglory,jcy85336}@wku.ac.kr

요 약

본 논문에서는 단위업무시스템별 구성요소의 식별 방법을 나타냈다. 단위업무시스템별 보호대상을 정의하였고 구성 요소별로 설명하였다. 보안 속성 설계 작성 기준을 설명하고 예시를 들도록 하였다.

ABSTRACT

In this paper, we showed how to identify specific components of unit production systems. Business units were defined by the system protected, was explained by component. The security attributes based on description and was designed to create lift the examples.

키워드

구성 요소(component), 보안 속성(security attribute)

Ⅰ. 서 론

설계전체에 대한 보안 활동에 대한 점검이 이루어지고 반영계획 등이 수립된 후에 구현단계로 이행되어야 구현단계의 안전성을 확보할 수 있다 [1].

Ⅱ. 보호대상 정의 식별

2.1 단위업무시스템별 구성요소 식별

모든 독립된 업무시스템에 대해서 보호대상을 개별적으로 식별한다. 단위업무시스템은 업무시스템이 설치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈간의 통신을 위한 인터페이스로 구분하여 식별한다.

2.2 단위업무시스템별 보호대상 정의

모든 단위업무시스템은 노드(node), 모듈(module), 그리고 인터페이스(interface)를 설계하면서 보호대상을 정의한다. 시스템과 노드, 노드와 모듈, 모듈과 인터페이스는 각각 1:N의 구조를 가질 수 있다.

Ⅲ. 보안속성설계

3.1 보안의 속성 설계

개별 업무시스템별로 보호대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석단계에서 정의된 보안 기준에 따라 보안속성을 설계한다. 보호대상 정의 테이블에 보안속성 설계를 추가하여 보안속성 설계로 상세화를 수행한다. 표 1은 보안의 속성 설계의 예이다.

3.2 보안 속성 설계 작성 기준 및 예시

보안 속성 설계 작성 기준은 크게 보호대상과 액세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 그리고 암호화로 분류한다. 보호대상은 인증 및

접근 제어를 실행하는 모듈의 교유한 속성 및 보안 설정을 기술하는 것이다. 표 3과 같이 노드, 모듈, 파일/디렉토리, 소유권, 그리고 퍼미션에 관한 설명과 예시를 들었다.

표 1. 보안속성 설계의 예
Table 1. Example of Security Attribute Design

① Object to Protect				
Node	Module	File/ Directory	Ownership	Permission
SSO /EAM Server	SSO /EAM Policy Server Module	sso/safeagent/keybd	SSO	755
② Object of Access Permission				
Node	Module		User	
EP	SSO Agent		SSO	
③ Access Control				
Network I/F	IP		Port	
SSO I/F(Socket)	191.191.111.200		7030 2040	
④ Identification and Authentication				
ID	PW		Etc.	
KEY	X		C	
⑤ Encryption				
Data		Grade	Method	
Authenticated Key		1	SSL	

표 2. 보호대상의 예시
Table 3. Object to Protect

속성	설명	예시
Mode	보호대상으로 식별한 시스템의 노드의 시스템 명	Web Server, SSO Server #1
Module	보호대상 시스템에서 구동되는 어플리케이션 또는 패키지 명	Merchandise Handling Module, EAI Engine
File /Directory	노드에서 모듈이 설치되어 있는 파일 또 는 디렉토리 경로	etc/bin, webroot/
Ownership	보호대상으로 식별한 파일/디렉터리를 소유할 계정명. 대부분의 경우 전용계정명과 일치하게 됨	root, kis_001
Permission	보호대상으로 식별한 파일/디렉터리에 대해 설정할 퍼미션 기록. 기본적으로 는 700을 권장하나, 특별한 사유에 의해 추가권한 부여시 이를 기록	800, 740, 666

Ⅳ. 결 론

본 논문에서는 단위업무시스템별 구성요소의 식별 방법과 노드, 모듈, 그리고 인터페이스의 설계에 대한 단위업무시스템별 보호대상을 정의하였다. 그리고 개별 업무시스템별로 보호 대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석단계에서 정의된 보안 기준에 따라 보안속성을 설계한다.

참고문헌

[1] Korea Information Sedurity Agency, “Security Guide V 1.0 for secure software development and introduction”, 2008