JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 5 : 1125~1130 May. 2015

설계단계의 보안 방안에서 보안 속성 설계에 대한 연구

신성윤*

A Study on Security Attribute Design in Security Plan of The Design Phase

Seong-Yoon Shin*

School of Computer & Information Communication Engineering, Kunsan National University, Kunsan 573-701, Korea

요 약

본 논문에서는 단위업무시스템별 구성요소의 식별 방법을 노드, 모듈, 그리고 인터페이스로 나타냈다. 단위업무시스템별 보호대상을 정의하였고, 구성 요소별로 노드, 모듈, 그리고 인터페이스에 대하여 설명하였다. 보호대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석단계에서 정의된 보안 기준에 따라 보안속성 설계 및 상세화를 수행한다. 그리고 보안 속성 설계 작성 기준은 보호대상과 액세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 그리고 암호화로 분류하여 각각을 설명하고 예시를 들도록 하였다.

ABSTRACT

In this paper, a method to identify components per unit task system is expressed with node, module, and interface. We define security subject per unit task system and explain node, module, and interface per component. According to the defined security standard in design phase, we also perform to design and elaborate security attributes for node and module as identified security subjects in their defined tables. And then we describe the composition standard for security attribute design with some examples, after classifying it into security subject, access subject, access control area, identification or verification area, and encryption.

키워드 : 노드, 모듈, 인터페이스, 보안 속성

Key word : node, module, interface, security attribute

Received 11 March 2015, **Revised** 23 March 2015, **Accepted** 06 April 2015

* **Corresponding Author** Seong-Yoon Shin(E-mail:s3397220@kunsan.ac.kr, Tel:+82-63-469-4860)
School of Computer & Information Communication Engineering, Kunsan National University, Kunsan 573-701, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.5.1125 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

설계단계의 보안 활동은 분석단계에서 산출된 보안 요구사항 분석서를 기반으로 애플리케이션을 안전하게 개발하기 위한 네트워크, 서버 등의 개발 환경 보안과 보안 요구사항을 반영한 애플리케이션 보안 설계를 수행하는 것이다. 설계전체에 대한 보안 활동에 대한 점검이 이루어지고 반영계획 등이 수립된 후에 구현단계로 이행되어야 구현단계의 안전성을 확보할 수 있다[1].

DB 보안에서 설계 단계는 DB 접근제어 규칙, DB 작업결재 규칙 등과 같이 각 기술요소별로 구현을 위 한 상세 규칙을 정의하고 시험 계획을 수립하는 단계이다. DB 접근제어에 대한 설계 단계의 주요 수행 내용은 접근제어 규칙 정의로, 여기에는 사용 자 인증, 로그인, SQL 통제, 로깅, 경보, SQL 마스킹 등에 대한 상세 규칙이 정의되어야 하며, 모니터링 지표를 정의하고 상세 운영 방안을 수립하는 내용이 포함된다. DB 암호화에 대한 설계 단계의 주요 수행 내용은 복호화 권한을 부여할 대상과 그 권한의 통제 방법 정의, 암호화키 및 알고리즘의 정의 등이다[2].

소규모 프로젝트에서는 보안담당자가 없는 경우가 있을 수 있으므로 시스템 분석 및 설계자가 이를 보완하여야 한다. 이는 시스템 설계자가 보안 전문가가 아니기 때문에 이 부분을 소홀히 할 수 있으며, 소프트웨어가 개발되고 설치되어 운영될 고객 기업에 기본적인 보안 취약점을 분석하여야 한다[3].

본 논문은 2장에서 관련연구를 살펴보고, 3장에서 단위업무시스템별 구성요소 식별과 단위업무시스템별 보호대상 정의에 대하여 알아보며, 4장에서는 매우 중요한 보안의 속성 설계와 보호대상과 액세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 그리고 암호화로 분류한 보안 속성 설계 작성 기준에 대하여 살펴보고, 5장에서 결론을 맺도록 한다.

Ⅱ. 관련연구

분석단계의 보안을 위하 관련 연구를 보면, 먼저, 안전한 S/W 개발을 위하여 보안취약점을 제거하고 보안을 고려하여 기능을 설계 구현하도록 하며 보안관련 법제도 및 규정과 그 세부내역들을 제시하였다[4]. [4]에서는 또한 국내외 해킹 사례를 살펴보았고, S/W 개발 보안의 주요 이슈도 들었다. 그리고 보안 관련 법 제도 및 규정의 실례 또한 세부적으로 살펴보았다.

분석 단계에서는 식별 및 인증의 보안요건을 제시하는데 개별 ID의 유일한 식별 패스워드 길이 제한 및 표준 조합을 적용과 주기적인 변경, ID/PW 이외의 보다 강화된 인증 방식 제공 및 인증 프로세스의 보안 요건 만족 등을 들 수 있다[5].

그리고 암호화에서는 중요 정보의 전송 또는 저장 시 정보의 기밀성과 무결성 보장과, 감사 로그에서는 부인방지를 위해 모든 전자 금융 거래 관련 내역은 로깅 및 보관되어야 한다는 것을 제시하였다[6].

업무수행자인 사용자의 역할과 데이터 사용행위를 기반으로 한 접근 및 권한 통제가 이루어져야 한다는 점과 조직의 운명을 좌우하는 매우 중요한 정보의 대량 조회 및 변경 작업은 반드시 사전 결재를 취득해야 가능하다는 점도 강조하였으며, 일정한 시간 동안 아무런 행위도 하지 않는 세션에 대하여 통제를 하는 것은 당연하다는 것도 제시하였다[7].

그리고 분석단계의 마지막인 취약점 관리에서, 시스템의 어플리케이션 및 IT 인프라에 대한 취약점 관리는 식별되어야 하고 개발 단계에서 실행 가능한 취약점 관리 방안이 도출되어야 한다는 것이다.

이렇게 분석단계의 과정을 거친 후 다음으로 설계단계로 들어가게 되는 것이다.

Ⅲ. 보호대상 식별 정의

3.1. 단위업무시스템별 구성요소 식별

모든 독립된 업무시스템에 대해서 보호대상을 개별적으로 식별한다. 단위업무시스템은 그림 1과 같이 업무시스템이 설치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈간의 통신을 위한 인터페이스로 구분하여 식별한다.

3.2. 단위업무시스템별 보호대상 정의

모든 단위업무시스템은 노드(node), 모듈(module), 그리고 인터페이스(interface)를 설계하면서 보호대상을 정의한다. 시스템과 노드, 노드와 모듈, 모듈과 인터

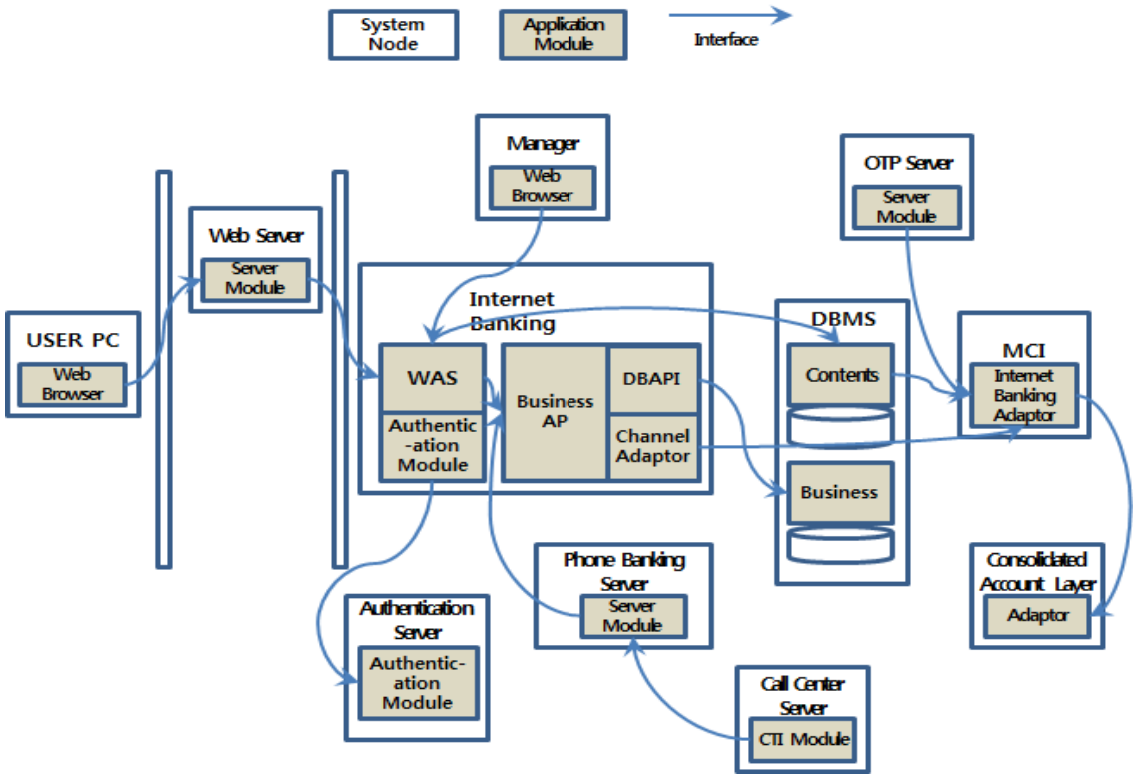

그림 1. 단위업무시스템별 구성요소
Fig. 1 Components per Unit-specific Business Systems

페이스는 각각 1:N의 구조를 가질 수 있다. 표 1은 단위업무시스템별 보호 대상의 예시로서 각각 업무 시스템과 노드는 1:N의 구조, 노드와 모듈은 1:N의 구조, 모듈과 인터페이스는 1:N의 구조를 갖는 것을 보여 준다. 표 2는 단위업무시스템을 구성하고 있는 노드, 모듈, 그리고 인터페이스에 대하여 설명하고 있다.

표 1. 보호대상의 정의 예
Table. 1 Defining Example of Protection Object

Business System	Node	Module	Interface
Homepage	Web Server	Apache	HTTP
			Socket
	WAS Server	Jeus	Socket
		EAI	XML MQ
	DB Server	Contents DBMS	DB Listener
		Bis. DBMS	DB Listener

표 2. 업무시스템 구성요소 설명
Table. 2 Component Description of Business Systems

Component	Explanation
System Node	It means a physical system with an IP address that the application module is installed. To identify a particular business system, system is included in the business and other systems to communicate with each other.
Application Module	From the application of modules to be installed inside the system, it means the application module includes a component for the business system.
Interface	It means to cover all the communication system for exchange of information between the application module. (ex: FTP, DB-Link, EAI, SOCKET, HTTP, rhost)

Ⅳ. 보안속성설계

4.1. 보안의 속성 설계

개별 업무시스템별로 보호대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석단계에서 정의된 보안 기준에 따라 보안속성을 설계한다. 보호 대상 정의 테이블에 보안속성 설계를 추가하여 보안속성 설계로 상세화를 수행한다.

그림 2는 개별업무시스템의 예를 나타내고, 표 3에서는 이 개별업무시스템에 3.2에서 정의한 보호대상 정의 테이블에 보안속성 설계를 추가하여 보안속성 설계로 상세화한 예이다.

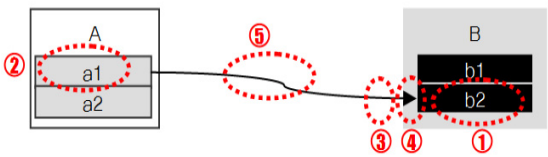

그림 2. 개별업무시스템의 예
Fig. 2 Examples of Individual Business Systems

표 3. 보안속성 설계의 예
Table. 3 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

4.2. 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 고유한 속성 및 보안설정을 기술하는 것으로 표 4와 같이 노드, 모듈, 파일/디렉토리, 소유권, 그리고 퍼미션에 관한 설명과 예시를 들었다.

표 4. 보호대상의 예시
Table. 4 Object to Protect

Attribute	Explanation	Ex.
Mode	The system name of a node in the system identified by the protected.	Web Server, SSO Server #1
Module	Application or package name running on the protected system.	Merchandise Handling Module, EAI Engine
File /Directory	File or directory path where the module is installed in the node.	etc/bin, webroot/
Ownership	Account name that will own the file/directory identified as protected. In most cases it matches the account name.	root, kis_001
Permission	Written permissions set for files/directories you identified with protection. Basically, it recommends 700, but it records when additional authorization by special reasons.	800, 740, 666

액세스 허용대상은 보호대상으로 접근을 허용 할 모듈의 고유한 속성을 기술하는 것으로 표 5와 같이 노드(node), 모듈(module), 그리고 사용자(user)에 관한 설명과 예시를 들었다.

표 5. 액세스 허용 대상의 예시
Table. 5 Object of Access Permission

Attribute	Explanation	Ex.
Node	System name of the node in the system identified by object to access	Web Server, SSO Server #1
Module	Application or package name running on the system identified by object to access	Merchandise Handling Module, EAI Engine

User	Record dedicated account name identified as object to protect. Due to the nature of modules, if you need to run it recorded a non-dedicated account (root etc.)	root, kis_001

접근통제 영역은 액세스 허용대상이 보호대상으로의 접근 시 사용되는 통신방식과 접근을 제한 할 보안 속성을 기술하는 것으로 표 6과 같이 네트워크 I/F, IP, port에 대한 설명과 그 예시를 들었다.

표 6. 접근통제 영역의 예시
Table. 6 Access Control Area

Attribute	Explanation	Ex.
Network I/F	Network interface scheme of the system node/module identified by the object to protect.	ftp, http, xml, EAI
IP	IP address to be used by the nodes identified by the object to access.	10.10.10.4, unlimited
port	The port number defined to allow access from the identification module by the object to protect.	tcp80, tcp/udp443, tcp3389

식별 및 인증 영역은 액세스 허용 대상이 보호대상으로의 접근 시 사용되는 인증방식을 기술하는 것으로 표 7과 같이 ID, PW, 그리고 기타 추가적인 인증 방법(etc.)에 대한 설명과 그 예시를 들었다.

표 7. 식별 및 인증 영역의 예시
Table. 7 Area of Identification and Authentication

Attribute	Explanation	Ex.
ID	All forms of ID acceptable access module by approaching object to protect or text of ID in the case of a fixed ID.	Key File, ID
PW	Whether to perform password authentication when accessing.	O, X
etc.	In addition to ID, PW certificates, when applying an additional authentication method, it will be described the method in detail.	Certification, Token

다음으로는 암호화인데 암호화는 의미를 알 수 없는 형식(암호문)으로 정보를 변환하는 것이다. 암호문의 형태로 정보를 기억 장치에 저장하거나 통신 회선을 통해 전송함으로써 정보를 보호할 수 있다. 따라서 표 8에서는 데이터(data), 등급(grade), 그리고 방식(method)에 대한 설명과 그 예시를 들었다.

표 8. 암호화의 예시
Table. 8 Encryption

Attribute	Explanation	Ex.
Data	It displays the data name if there is more data than a certain rating data is defined in the design phase of the data stored or processed in the module.	ID, Password, Account Information
Grade	Rating of data identified.	1, 2 ,3
Method	Encryption method to be used when the data encryption compliance.	SSL, hash, Field Encryption, Expert Encryption

Ⅴ. 결 론

분석단계에서는 보안관련 법 제도 및 규정, 식별 및 인증의 보안 요건 정의, 암호화에서 보안 요건의 정의, 그리고 접근통제와 취약점 관리를 위한 보안요건의 정의 등 다양한 연구를 수행하였다.

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. 그리고 보안 속성 설계 작성 기준은 크게 보호대상과 액세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 그리고 암호화로 분류하였다. 또한 보호대상과 액세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 그리고 암호화에 대한 설명과 예시도 나타냈다.

본 논문은 타 연구처럼 특정 부분이나 한 부분을 묘사한 것이 아니라 설계단계의 보안에서 보안 속성설계

에 관한 전반적인 부분을 기술하여 그 특징을 나타내어 다른 분야의 논문 작성의 기준이 될 것이다.

REFERENCES

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

[2] Data Expert Knowledge Potal(DBGuide.net), “DB Security Procedures and Technical Elements”, 2015.

[3] Myoung-Gyu Jung and Man-Gon Park, “Consideration Factors in the Design Phase for Small Software Development Projects that are Difficult to Build Information Security Systems,” *Proceeding of KMMS*, Vol. 13, No. 2, pp. 716-719, 2010.

[4] Seong-Yoon Shin, Kil-Hyun Jeong, “Case Analysis of Legal System and Regulations according to the Needs of S/W Development Security,” *J. of KSCI*, Vol. 19, No. 10, pp. 117-124, 2014.

[5] Seong-Yoon Shin, “ A Study on Definitions of Security Requirements for Identification and Authentication on the Step of Analysis,” *J. of KSCI*, Vol. 19, No. 7, pp. 87-93, 2014.

[6] Seong-Yoon Shin, Kang-Ho Lee, “A Study of Definition of Security Requirements on Encryption and Audit Logging,” *J. of KSCI*, Vol. 19, No. 9, pp. 85-91, 2014.

[7] Seong-Yoon Shin, “ The Definitions of Security Requirements for Control Access on the Step of Analysis,” *J. of KSCI*, Vol. 19, No. 11, pp. 97-103, 2014.

신성윤(Seong-Yoon Shin)

군산대학교 컴퓨터정보공학과 박사
한국정보통신학회 국문지부회장
군산대학교 컴퓨터정보통신공학부 교수
※관심분야 : 멀티미디어 시스템 및 응용, 가상현실, 텔레메틱스