한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

S/W 설계 단계에서 보안 속성 설계

신성윤*, 신광성°, 이현창**
*°군산대학교 컴퓨터정보공학과
**원광대학교 정보 · 전자상거래학부(융복합창의연구소)
e-mail:{waver, syshin}@kunsan.ac.kr°*, hclglory@wku.ac.kr**

Design of Security Attributes in Step of S/W Design

Seong-Yoon Shin*, Kwang-Seong Shin°, Hyun-Chang Lee**,
*°Dept. of Computer Information Engineering, Kunsan National University
**Division Computer and Electronic Commerce(Institure of Convergence and Creativity),
Wonkwang University

● 요 약 ●

본 논문에서는 모든 독립된 업무 시스템에 대해서 보호 대상을 개별적으로 식별해야 한다는 것을 제시한다. 모든 단위 업무 시스템은 노드, 모듈, 인터페이스를 설계하면서 보호대상을 정의해야 한다. 이에 따라서 개별 업무 시스템별로 보호 대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석 단계에서 정의된 보안 기준에 따라 보안 속성을 설계해야 한다는 것이다.

키워드: 보안 속성(security attribute), 보호 대상(object to protect)

I. 서 론

설계단계의 전반의 보안 활동에 대한 검토와 점검이 수행되고 반영계획 등이 수립된 후에 구현단계로 가서 수행하여야 구현단계의 안정성을 보장할 수 있다.

보통 시스템 내부에 산적되어 있는 오류와 결함은 시스템 사용 시에는 드러나거나 발견되지 않는다. 그리고 시스템 사용 시에는 문제가 되지 않는 결함도 흔히 발견된다. 그렇지만 보안 측면에서 이를 보면 시스템 공격자가 특정 조건을 만들어서 오류와 결함을 증대시키도록 유도할 수 있다.

II. 관련연구

[1]에서는 개인정보를 구성하는 각 속성정보의 관리 정책을 결정할 기준으로 속성정보의 동적 보안수준 측정법을 제시하였으며 동적 보안수준 측정법은 개인정보의 가변적 특성을 측정 요소로 채택한다고 하였다.

[2]에서는 사용자에게 할당해야 하는 보안 속성을 이야기 하는데, 사용자 계정이 만들어진 후 보안 관리자는 사용자에게 보안 속성을 지정한다. 올바른 기본값을 설정한 경우 다음 단계는 기본값에 대한 예외가 필요한 사용자에 대해서만 보안 속성을 할당하는 것이다.

III. 단위 업무 시스템 별 구성 요소 식별

모든 독립된 업무 시스템에 대해서 보호 대상을 개별적으로 식별해야 한다. 단위 업무 시스템은 업무 시스템이 설치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈 간의 통신을 위한 인터페이스로 구분하여 식별하도록 한다.

IV. 단위 업무 시스템 별 보호 대상 정의

모든 단위 업무 시스템은 노드, 모듈, 인터페이스를 설계 하면서 보호 대상을 정의한다. 시스템과 노드, 노드와 모듈, 모듈과 인터페이스는 각각 1:N의 구조를 가질 수 있다.

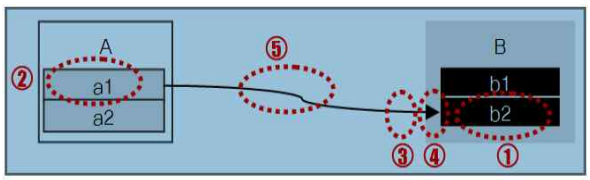
[보호대상 정의 (예시)]

업무시스템	노드	모듈	인터페이스
홈페이지	웹서버	Apache	HTTP
			Socket
	WAS서버	Jeus	Socket
		EAI	XML MQ
	DB서버	컨텐츠 DBMS	DB Listenser
		비즈 DBMS	DB Listenser

구성요소	설명
시스템 노드	어플리케이션 모듈이 설치될, IP 주소를 가진 물리적 시스템을 의미함. 특정 업무시스템 식별 할 때, 해당 업무에 포함되는 시스템 및 상호 통신을 하는 타 시스템을 포함.
어플리케이션 모듈	시스템 내부에 설치되는 어플리케이션 모듈 중 해당 업무시스템의 구성요소에 포함되는 어플리케이션 모듈을 의미함.
인터페이스	어플리케이션 모듈 상호간의 정보교환을 위한 모든 통신방식을 포괄하여 의미함. (예: FTP, DB-link, EAI, SOCKET, HTTP, rhost)

그림 1. 보호 대상 정의

V. 보안 속성 설계



[보안속성 설계 (예시)]

① 보호대상					② 액세스 허용대상		
노드	모듈	파일/디렉터리	소유권	퍼미션	노드	모듈	사용자
SSO/EAM서버	SSO/EAM정책서버 모듈	sso/safeagent/keydb	SSO	755	EP	SSO Agent	SSO

③ 접근통제			④ 식별 및 인증			⑤ 암호화		
네트웍I/F	IP	Port	ID	PW	기타	데이터	등급	방식
SSO I/F (socket)	192.190.100.206	7010 7020	KEY	X	X	인증키	1	SSL

그림 2. 보안 속성 설계 예시

개별 업무 시스템 별로 보호 대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석단계에서 정의된 보안 기준에 따라 보안 속성을 설계한다. 보호 대상 정의 테이블에 보안 속성 설계를 추가하여 보안 속성 설계로 상세화 한다.

VI. 결론

본 논문에서는 보안의 속성 설계 시 우선 보호 대상 식별과 정의를 수행해야 한다는 것이다. 또한 독립된 업무 시스템들은 보호 대상을 개별적으로 식별하고 단위 업무 시스템들은 노드, 모듈, 인터페이스를 설계하면서 보호대상을 정의해야 한다. 따라서 개별 업무 시스템별로 보호 대상 정의 테이블에서 식별된 보호 대상 노드, 모듈은 분석 단계에서 정의된 보안 기준에 따라 보안 속성을 설계한다.

참고문헌

[1] In Joo Jang, Hyeong Seon Yoo, “Dynamic Sensitivity Level Measurement for Privacy Protection,” The Journal of Society for e-Business Studies, Vol. 17, No. 1, pp. 137-150, 2012.2.

[2] http://docs.oracle.com/cd/E26925_01/html/E25903/manageusers-27.html