Web 기반의 접근제어 시스템 설계

이경효*, 조아앵*, 박익수*, 오병균*
목포대학교 정보공학부 정보보호전공
e-mail: {mediakh, agcho, upark, obk}@mokpo.ac.kr*

Design of Web based Acess Control System

Kyeong hyo Lee*, A Aeng Jo, Ik-Su Park, Byeong-Kyun Oh*
Department of information Security, Mokpo National University

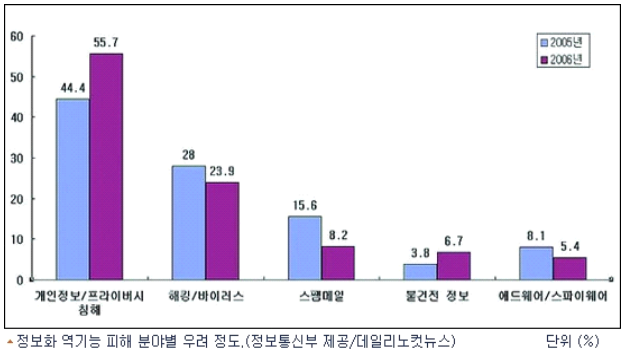
요 약

개인정보는 정보서비스의 효율적인 운용과 새로운 비즈니스 모델에서 수익창출을 위한 자원으로 활용되고 있다. 이로 인하여 중요 정보에 대한 불법적인 사용 또는 개인정보 소유자의 허가 없는 사용으로 개인 프라이버시 침해가 발생되고 있다. 따라서 본 논문에서는 각 정보 시스템에서 사생활보호와 중요정보보호를 위한 정보 보안정책 모델을 제안한다. 제안된 모델은 정보 제공정책 모델과 정보 사용정책 모델로 구성하여 정보자기결정권을 부여하여 이중적인 접근제어 방식을 적용하고자 한다.

1. 서론

최근 IT제품의 광범위한 보급과 인터넷의 활성화로 인하여 많은 개인정보 유출의 위협이 증대되고 개인정보 도용 피해 또한 증대되었다. 하지만 IC카드나 플래쉬 메모리 등을 이용한 key 부여 방식 등의 방법이 보급되어 있으나 휴대에 대한 불편성과 사용하기 어렵다는 단점이 있어 여러 가지 보안 연구가 되고 있다. 기존 운영체제들은 네트워크가 없는 컴퓨팅 환경에서 개발 되어 보안사항을 고려하여 설계되지 않았다. 네트워크 시스템이 발달됨에 따라 독립적인 시스템에 악의적인 공격자들에 의해 보안상의 허점을 이용한 공격이 나타나게 되었고 어플리케이션 수중의 정보보호 솔루션이 등장하면서 솔루션 자체의 취약점 노출을 이용한 공격들로 인한 피해도 증가하게 되었다. 전자상거래 및 인트라넷에서 개인정보 유출에 대한 프라이버시 보호가 필요하게 되었고 가상공간의 개인정보를 불법으로 수집, 남용하거나 악의적인 목적으로 이를 수집 사용하여 개인정보와 사생활이 침해당하는 사례도 증가하게 되었다. 또한 통합된 e-비즈니스 환경의 관리를 위하여 싱글 사인-온과 사용자 역할 기반의 세분화된 접근 관리의 필요성이 대두되면서 안전한 프라이버시 보호 모델링 기술이 중요하게 인식되었다. 향후 상황인식 환경에서 개인정보의 수집에 대해 프라이버시를 최대한 보장 하면서, 다양한 서비스마다 각기 다른 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용 범위를 제공하는 지능형 개인정보보호 에이전트 및 접근제어 기술이 필요하게 되었다. 국가적인 차원에서 인터넷 기반의 전자문서 관리 및 데이터베이스 인터넷 뱅킹과 같은 인터넷 비즈니스에 관한 취약점을 보완하기 위한 기술적인 보안이 요구되고 있다.

접근제어의 목표는 비인가자 또는 통신 시스템의 위협으로부터 응용프로그램 및 시스템을 보호하는 것이다. 최근 연구되는 역할기반 접근 방법의 기본적 개념은 개별적인 사용자보다 권한 또는 역할이 주어지는 접근적 권한이다. 사용자들은 서로 다른 권한에 따라 정보 시스템내의 행위가 주어지고 접근제어시스템은 사용자와 그룹이 사용하는 전통적인 접근법을 통하여 보안 관리에 대하여보이지 않는 유연성을 제공한다.



[그림 1] 정보보호의 유출사례를 통한 개인정보 현황

[그림 1]은 정보화 역기능 피해 분야별 우려 정도를 나타낸 것으로 정보보호의 유출사례를 통해서 개인정보의 현황을 살펴볼 수 있다. 따라서 본 논문에서는 최근 많이 발생하고 있는 Web 상의 정보 유출에 대한 악의 적인 주체로부터 접근에 대한 권한을 분리하여 중요 정보에 대하여 보호하며 정당한 주체로 하여금 정보를 편리하게 접근하

고 이용할 수 있도록 Web기반의 접근제어 시스템을 제안한다. 제안된 모델은 정보 제공정책 모델과 정보 사용정책 모델로 구성하여 정보자기결정권을 부여하여 이중적인 접근제어 방식을 적용하고자 한다.

2. 관련연구

2.1 임의적 접근통제

(DAC : Discretionary Access Control)

- 권한 있는 사용자가 임의의 다른 사용자에게 객체에 대한 접근을 허용할 수 있는 기법
- 어떠한 사용자든 임의적으로 그 비밀 정보에 접근이 가능토록 되어 있어 보안상의 문제가 야기, 유닉스 또는 리눅스 시스템에서 사용 주체나 주체가 속해 있는 그룹의 식별자에 근거 하여 객체에 대한 접근을 제한하는 방법
- 접근을 요청하는 사용자의 식별에 기초하여 어떤 객체에 대해 사용자가 접근 권한을 추가 혹은 삭제 가능
- 모든 개개의 주체와 객체 단위로 접근제한이 설정되며, 객체의 소유주에 의하여 접근 제한이 변경 가능한 각 주체와 각 객체간의 접근 통제 관계를 정의

2.2 강제 접근통제

(MAC : Mandatory Access Control)

- 객체에 포함된 정보의 비밀성(레이블로 표현된 허용 등급)과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한 (접근허가(clearance))에 근거하여 객체에 대한 접근을 제한하는 방법
- 분류된 시스템 데이터와 각 등급의 사용자 간에 강력한 보호를 위하여 요구되는 많은 정보들이 적용
- 하위 비밀 등급의 객체로 정보의 흐름을 방어하므로 흐름-제어(flow-control) 정책으로 정의
- 데이터에 대한 접근은 주체와 객체가 갖는 보안 등급의 정의를 통한 강제적인 정책에 의해 결정
- 객체 보안 등급 = 보안등급(security level : 정보를 반영한) + 응용분야의 범주(category : 객체 정보가 언급)

2.3 보안 모델 정의

보안 모델이란 어떤 조직에서 보안 정책을 실제 로 구현하기 위한 이론적인 모델로서 70년대부터 80년대까지 미 국방성의 지원을 받아 개발되었다.

- 기밀성 모델

최초 보안 모델은 군사적인 용도로 개발되었기 때문에 기밀성에 많은 중점을 두고 있다. 기밀성이란 한 조직의 중요 정보가 보관 및 전달되는 과정에서 의도하지 않은 노출로부터 보호되는 것을 의미한다. 보관 중인 정보의 기밀성은 접근 통제를 통해 구현될 수 있으며, 전달 중인 정보의 기밀성은 암호화 등을 통해 구현될 수 있다.

- 무결성 모델

인터넷의 발달과 더불어 전자 상거래나 온라인 뱅킹이 출현하면서 인가되지 않은 사용자에 의해 데이터가 수정되는 것을 통제하는 무결성에 대한 중요성이 더욱 강조되고 있다.

-인가된 사용자라 할지라도 권한이 없는 데이터를 수정하는 것을 통제하여야 한다.

-데이터는 내/외부적으로 일관성을 유지

- 접근 통제 모델

접근 통제 모델은 모델이 가지고 있는 접근 통제 메커니즘을 보안 모델로 발전시켰는데, 이러한 모델에는 접근 행렬 모델(Access Matrix Model)과 테이크-그랜트 모델(Take-Grant Model)이 있다.

3. Web기반 접근제어 시스템 설계

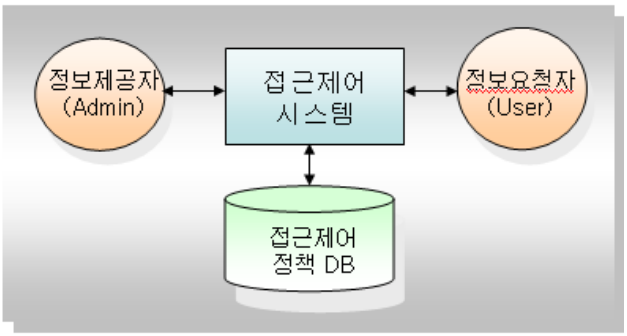
Web기반의 접근제어 시스템은 Web환경에서 정보를 제공함으로써 사용하는 주체에 대하여 편리성을 제공함과 동시에 주체가 다양하며 수많은 개인정보를 보호를 요구하는데 역할과 관리를 통하여 이를 효율적으로 통제하며 보호할 수 있다.

역할에 의한 접근은 각각의 주체를 역할들로 종속시킴으로써 각 주체에 대한 역할에 따른 업무만을 함으로써 각 객체에 대한 정보에 대한 보호의 효율성을 높일 수 있다. 중요정보에 접근 허가하는 측면에서는 관리역할을 제공하고 개인정보를 사용하는 측면에서는 사용역할을 부여하게 하여 중요정보에 대한 효율적인 보호와 관리를 강화시킨다.

암호화단계를 이용하여 중요정보에 대하여 암호화된 자료 형태로 보관함으로서 중요정보가 노출되더라도 암호화된 정보만 노출되어 중요정보의 노출에 대한 위험에 대해 대비한다.

3.1 접근제어 시스템 환경 구성요소

접근제어 시스템 환경 구성요소는 정보를 제공하는 정보제공자와 정보서비스를 위하여 정보를 요청하는 시스템 내부와 외부사용자 등이 있다. [그림 2]는 개인정보시스템 환경에서 구성요소를 나타내고 있다



[그림 2] 정보시스템 환경 구성요소

개인정보제공자(Admin)가 정보서비스를 이용하기 위하여

개인정보를 제공할 때 사용범위와 목적을 부여한 보안정책을 설정한다. 개인정보 요청자(SP)는 개인정보 이용에서 사용범위에서만 정보를 사용할 수 있다.

3.1.1 기본 설계 시스템 구성요소

■ 사용자별
- Informer 정보제공자
- User 사용자
- Administrator 관리자

■ 정책 DB
- 정보제공자 정책
- 관리자 정책(그룹별 권한, 인증)

■ 암호모듈
- 관리자, 정보제공자 정책에 따라 자료 차별적으로 암호화
- 비밀키 기반 구조

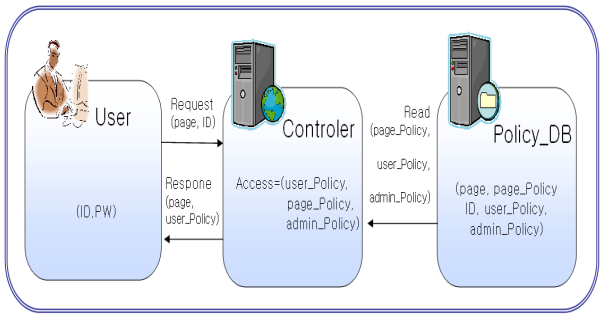
■ Acess Control
- 정책 DB와 서버에 접근해오는 사용자 권한 부여
- 암호모듈 연동 및 제어

■ Web Server
-Web 환경으로 손쉽게 자료를 접근하고 관리함

3.2 WEB 기반 접근 제어 시스템 설계

3.2.1 구동 프로토콜

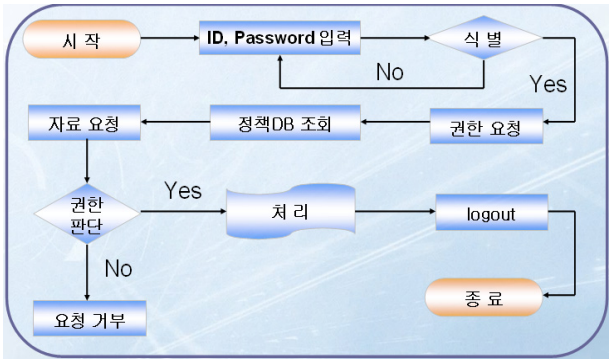
User로부터 정보 페이지에 관한 요청(Request(page)이 있을 경우 Controler는 Policy DB로부터 해당 페이지 권한(page_Policy)과 사용자 권한(user_Policy)을 받아와 사용가능한 사용자임을 구별하여 User에게 해당 서비스를 제공한다. [그림 3]에서는 User과 Controler와 Policy사이의 구동 프로토콜을 나타낸다.



[그림 3] 구동 프로토콜

3.2.2 시스템 처리 흐름

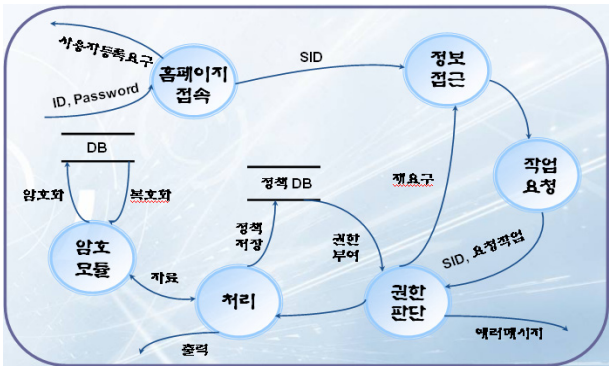
[그림 4]에서 처럼 User의 ID, Password를 사용하여 인증 절차를 거쳐 식별확인을 한다. 인증을 거친 사용자에 한하여 권한을 요청을 받고 요청을 받을 경우 정책 DB 조회 후 자료 요청 유형에 따라 권한 판단을 하여 처리 여부를 결정한다.



[그림 4] 시스템 처리 흐름

3.2.3 자료 흐름

1) 식별 요청 : 정당한 사용자 여부를 식별한다.
2) 정보접근 : 접근 하고자하는 자료의 위치를 판별한다.
3) 작업요청 : 수행하고자 하는 작업을 조회, 입력, 수정, 삭제로 구분한 다음 요청을 선택한다.
4) 권한판단 : 요청에 따른 처리는 판별 요청에 해당하는 처리 작업을 수행한다.



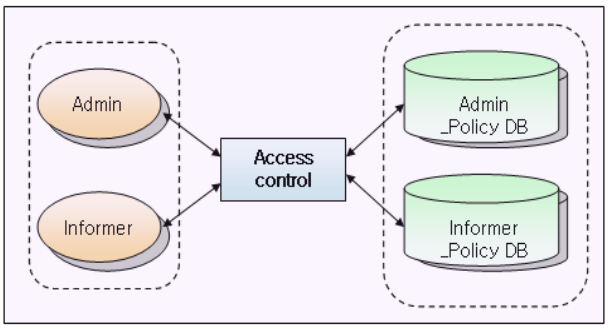
[그림 5] 자료 흐름도

3.2.4 정보제공 정책과 정보제공자 정책

Informer등급은 사용목적(Purpose)과 접근모드(Access)를 이용하여 중요정보에 대한 접근 가능 여부를 등급으로 나타낸다.

Admin등급은 정보제공자가 제공하는 정보에 대하여 사용목적에 때라 타인의 접근 여부를 결정하는 등급을 나타낸다.

정보접근등급은 중요 정보 중에서 더 세분화하여 정보에 대한 악용 가능 여부를 판단하여 중요성 정도에 따라 분리하여 등급을 나타낸다. [그림6]에 나타낸 다음 등급들은 서로 유기적으로 연동 가능하도록 하여 각 등급을 중복으로 이용 가능하게 한다.

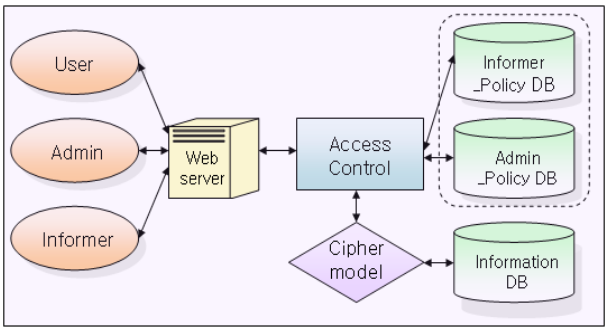


[그림 6] 정보 제공 정책

3.2.5 정보사용 정책

Informer(관리자)는 사용목적(Purpose)과 접근모드(Access)를 이용하여 중요정보 제공정책(Informer_Policy)을 생성하고 중요정보를 관리 한다. Informer_Policy DB(관리자 접근제어정책)를 이용하여 중요정보 사용자(User)와 중요정보 제공자(Admin)가 정보서비스를 위해 정보를 요청하면 Informer_Policy 모델에서 설정한 정책을 적용하여 중요 정보 사용 허가를 하기 위해 사용한다.

Admin(정보 제공자)는 정보를 제공하면서 공개하는 정보에 대하여 접근 제어정책을 설정하여 악의적인 사용자로 부터 노출을 막기 위하여 Admin_Policy DB(제공자 접근제어정책)을 수립한다.



[그림 7] 정보 사용 정책

User (사용자)와 Admin(정보제공자)가 Web server를 통하여 정보에 접근하고자 할 때 web server는 Access Control(접근제어 제어모듈)로 요청하게 된다. Access Control은 Informer_Policy DB(관리자 접근 제어 정책)과 Admin_policy DB(제공자 접근제어 정책)에 따라 접근여부의 권한을 부여하고 권한에 합당한 요청에 대하여는 Cipher_Model(암호/복호 모듈)에게 정보를 요청하게 된다. Cipher_Model은 요청에 따라 지정 정보를 복호화하여 Web server로 요청 정보를 제공하게 된다.

4. 결론

전통적인 접근 제어 모델에는 MAC(Mandatory Access control), DAC(Discretionary Access control) 등과 같은 모델들이 있으나, 프라이버시 정책을 적용하기 위해 설계되어 있지 않았다. 또한 RABC 모델을 적용하여 DAFMAT가 제안되었으나 프라이버시 보호를 적용하는데 있어 목적결합과 필요의 원칙 등을 모델링하지 못하였다. 즉 기존의 역할 기반 접근제어에서는 위치와 시간 등에 따른 접근 제어 등과 같이 다양한 상황 정보에 근거한 접근 제어를 수행 할 수 는 문제점이 있었다. 따라서 본 논문에서는 최근 발생하고 있는 Web 상의 정보 유출에 대한 악의 적인 주체로부터 접근에 대한 권한을 분리하여 중요 정보에 대하여 보호하며 정당한 주체로 하여금 정보를 편리하게 접근하고 이용할 수 있도록 Web기반의 접근제어 시스템을 제안하였다.

제안한 모델을 통해 User (사용자)와 Admin(정보제공자)가 Web server를 통하여 정보에 접근하고자 할 때 web server는 Access Control(접근제어 제어모듈)로 요청하게 된다. Access Control은 Informer_Policy DB(관리자 접근제어 정책)과 Admin_policy DB(제공자 접근제어 정책)에 따라 접근여부의 권한을 부여하고 권한에 합당한 요청에 대하여는 Cipher_Model(암호/복호 모듈)에게 정보를 요청하게 된다. Cipher_Model은 요청에 따라 지정 정보를 복호화하여 Web server로 요청 정보를 제공할 수있게 하였다. 향후 분산 네트워크 환경과 유비쿼터스 환경에서 활용하기 위하여 시스템 구현이 추가적으로 필요하다. 그리고 개인정보보호 기술의 모델의 평가를 위하여 추가적인 평가 도구 연구가 필요하다.

5.참고 문헌

[1] Christine Varney, Hogan & Hartson, "Privacy and Security Best Practices", Liberty Alliance Project, November 12, 2003.

[2] C.A. Ardagna, E. Damiani, S. De Capitanidi Vimercati & P. Samarati, "XML-based Access Control Languages", Information Security Technical Report. Vol. 9, No. 3, 1363-4127/04/© 2004, Elsevier Ltd.

[3] G. Karjoth and M. Schunter. "A privacy policy model for enterprises", In 15th IEEE Computer Security Foundations Workshop, pages 271 - 281. IEEE Computer Society Press, 2002.

[4] G. Karjoth, M. Schunter, and M. Waidner, "The Platform For Enterprise Privacy Practices - Privacy-enabled Management Of Customer Data", In Proceedings of the Privacy Enhancing Technologies Conference, page to appear, San Francisco, CA, April 14-15 2002.

[5] Arun Kumar, Neeran Karnik, Grirish Chafile, "Context Sensitivity in Role-Based Access Control", ACM SIGOPS Operating Systems Review, 53-66, 2002.

[6] 오세종, 박석, "역할기반 접근제어에서 기업환경에 적합한 역할계층의 구성에 관한 연구", 한국통신정보보호학회 학술발표회

[7] 심재훈, "역할기반 접근제어 모델에 기초한 사용자 수준의 위임 기법", 석사학위 논문, 1999.1