제 3자 사용자 정책을 적용한 ACL 설계

이경효°, 오병균 , 이상국
{mediakh, obk}mokpo.ac.kr, sglee@icu.ac.kr

*Kyeong hyo Lee, *Byeong-Kyun Oh, Sang Gug Lee
*Department of information Security, Mokpo National University

요 약

본 논문은 Web환경에서의 사용자의 권한을 검증하고 권한에 대한 이중적인 접근제어 서비스를 제공하는 역할기반의 WAC시스템의 블럭 설계서를 제안한다. WAC시스템은 User Interface Block, Access Control Block, Cipher module Block, DataBase로 구성 되며, WAC 시스템의 기능분류모델을 이용한 Block의 세부사항과 WAC시스템 기본 Bock(Access Control Bock)의 기본 기능 설계 및 사용자 접근제어 기능 설계, DES기반의 암호 Bock 기능 설계, 인터페이스 설계 대한 WAC 시스템의 전체적인 Block 설계에 대하여 기술한다.

1. 서 론

최근 IT제품의 광범위한 보급과 인터넷의 활성화로 인하여 많은 개인정보 유출의 위협이 증대되고 개인정보 도용 피해 또한 증대되었다. 하지만 IC카드나 플래쉬 메모리등을 이용한 key 부여 방식 등의 방법이 보급되어 있으나 휴대에 대한 불편성과 사용하기 어렵다는 단점이 있어 여러 가지 보안 연구가 되고 있다. 하지만 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.

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.

따라서 본 논문에서는 WACL시스템에 정의되어 있는 블록들 간의 연동을 통한 접근제어 서비스를 위한 WACL의 기능을 시험한 절차를 기술하였다. 또한 WACL 블록 설계서에 기술된 기능을 기반으로 작성하였고, 주변 블록은 시험을 위해 실제 시스템간의 연동을, 각 절차는 시험의 목적 및 절차 순서로 기술하였다.

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력 핵심기술개발사업의 일환으로 수행하였음. [2005-S-106-02, RFID/USN용 센서태그 및 센서노드 기술]

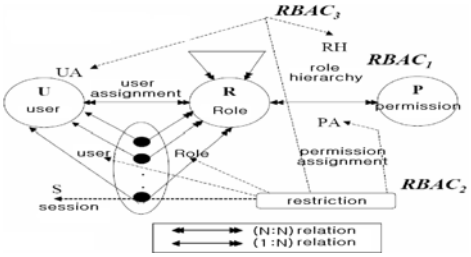
2. 관련연구

2.1 역할기반의 접근통제

주체에 대한 행위나 역할에 의해 접근 권한이 결정되는 접근 제어 방식으로 역할은 접근 제어 정책을 구현하는 중요한 의미적 구조로서 조직의 업무 기능에 따라 역할과 권한이 생성되고, 역할에 부여된 접근 권한에 따라 역할 수행에 필요한 최소한도의 자원 접근이 가능하며, 업무 권한과 책임에 따라 접근 구조의 변경 없이도 역할을 변경할 수 있게 한 것이다. 또한 권한을 세분화한 다중 등급 보안(MLS) 기능과, 파일 시스템, 프로세스, 네트워크 포트, 레지스트리에 대한 강제적 접근 제어, 개개의 파일 또는 네트워크 포트에 대한 접근 권한 제어, 프로세스를 주체로 한 동일 파일에 대한 다양한 보안 기능 등 제어 기능이 있다.

- Ravi S. Sandhu의 RBAC 모델
  - -RBAC0 : RBAC의 최소 특성을 가지는 기본 모델
  - -RBAC1 : RBAC0에 다른 역할로부터 허가를 상속받을 수 있는 역할 계층(Role Hierarchy)의 특성을 추가
  - -RBAC2 : RBAC0에 RBAC요소들에 제한 조건을 가할 수 있는 제약(Constraints)을 추가, RBAC1과 RBAC2는 포함관계가 아님

-RBAC3 : RBAC1 과 RBAC2 의 수용



[그림 3] Ravi S. Sandhu의 RBAC 모델

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.

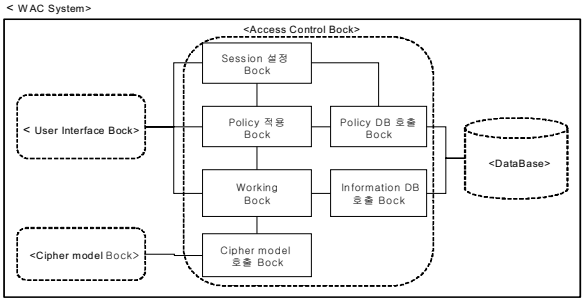
-데이터는 내/외부적으로 일관성을 유지

- 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.

2.4 기능 시험 절차

본 논문은 Web환경에서의 사용자의 권한을 검증하고 권한에 대한 이중적인 접근제어 서비스를 제공하는 역할 기반의 WAC시스템의 블럭 설계서를 제안한다. WAC시스템은 User Interface Block, Access Control Block, Cipher modul Block, DataBase로 구성 되며, WAC 시스템의 기능분류모델을 이용한 Block의 세부사항과 WAC시스템 기본 Bock(Access Control Bock)의 기본 기능 설계 및 사용자 접근제어 기능 설계, DES기반의 암호 Bock 기능 설계, 인터페이스 설계 대한 WAC 시스템의 전체적인 Block 설계에 대하여 기술한다.



[그림 2] WAC System Access Control Block 구조

3. WAC 시스템 기본 기능 시험

3.1 사용자 인증 및 세션 유지 시험

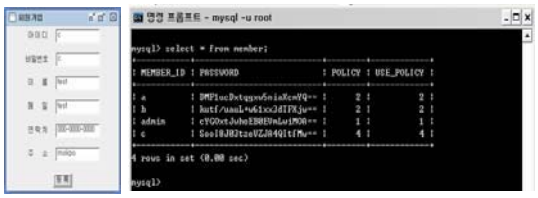
ID및 PW 방식을 이용한 시스템 정당한 사용자임을 판별하고 세션을 생성 유지를 시험한다. MD5 해쉬를 이용하여 저장된 password 해쉬 값과 interface를 통하여 입력받은 password값을 해쉬 하여 비교하여 사용자인증이 됨을 시험한다.

3.1.1 시험 항목

- 아이디 등록을 통하여 등록된 password 해쉬 값 확인
- 등록된 아이디를 통하여 login확인
- 비등록 및 password 틀린 경우 오류메시지 확인

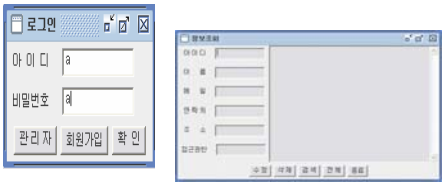
3.1.2 시험 결과

- 아이디 등록을 통하여 등록된 password 해쉬 값 확인



[그림 5] 로그인 화면

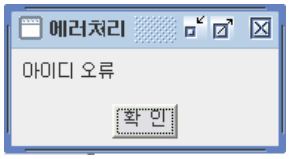
- 등록된 아이디를 통하여 login확인('a'라는 사용자 로그인)



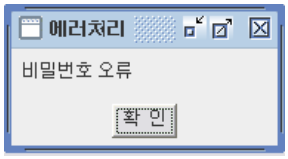
<사용자 로그인> <로그인 성공 화면>

[그림4] 사용자 로그인과 로그인 성공 화면

- 비 등록 및 password 틀린 경우 오류메시지 확인



<아이디 에러처리>



<비밀번호 에러처리>

3.2 정보제공 시험

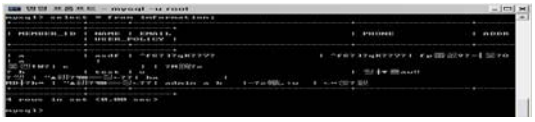
작업공간에서 정당한 사용자로부터 정당한 정보 요청 시 요청정보에 대하여 응답함을 시험한다. 정보는Database에 암호화 되어있으며 요청이 있을 경우 그 요청에 의하여 정보를 복호화 후 제공됨은 시험한다.

3.2.1 시험 항목

- database의 암호화된 자료 확인
  - 등록된 보안등급 2급인 'a'라는 사용자를 이용하여작업 실행 확인아이디 등록을 통하여 등록된 password 해쉬 값 확인

3.2.2 시험 결과

- Database의 암호화된 자료 확인



- 서비스 지원 작업 실행 확인

<전체 버튼 확인>

<검색 버튼 확인>

<수정 버튼 확인>

<삭제 버튼 확인>

<종료 버튼 확인>

[그림 5] 서비스 지원 작업 실행

3.3 관리자 접근제어 기능 시험

관리자 접근제어 시험은 정당한 사용자가 업무를 수행하려할 때 사용자의 권한과 업무 권한을 비교하여 허용 및 거부를 판별하는지 시험한다. 시험을 위하여 미리 지정한 각 등급별 사용자를 이용하여 등급에 따른 업무 수행을 시험한다.

3.3.1 시험 항목

- 등록된 보안등급 2급인 'a'라는 사용자를 이용하여 (전체-모든 사용자 사용가능, 검색-보안등급 3이상 사용자만 사용가능)작업 실행 확인
- 등록된 보안등급 4급인 'c'라는 사용자를 이용하여 (전체-모든 사용자 사용 가능, 검색-보안등급 3이상 사용자만 사용가능)작업 실행 확인

3.3.2 시험 결과

- 등록된 보안등급 2급인 'a'라는 사용자를 이용하여 작업 실행 확인

<전체 버튼 확인>

<검색 버튼 확인>

- 등록된 보안등급 4급인 'c'라는 사용자를 이용하여 작업 실행 확인

<전체 버튼 확인>

<검색 버튼 확인>

[그림 5] 관리자 접근제어 시험

3.4 정보제공자 접근제어 기능 시험

정보제공자 접근제어 시험은 정당한 사용자가 제공된 정보에 대해 접근하고자 제공자가 지정한 사용자별 정책에 의하여 정보의 접근의 허용 여부를 시험한다. 정보제공자가 정보제공을 하면서 제공정책을 설정하여 정보를 제공하고 이후 정보제공자가 허용한 사용자와 정보를 허용하지 않은 사용자를 이용하여 정보제공정책을 시험한다.

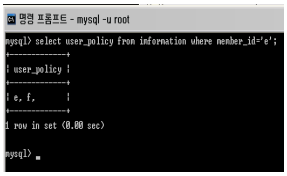
3.4.1 시험 항목

- 보안등급 3급인 'e', 'f'의 사용자의 정보 접근 정책 리스트를 확인

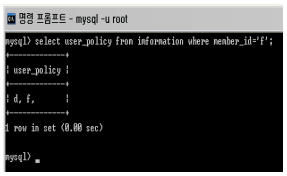
• ‘d’라는 사용자가 ‘f’, ‘e’ 사용자의 정보를 검색 확인

3.3.2 시험 결과

• 보안등급 3급인 ‘e’, ‘f’의 사용자의 정보 접근 정책 리스트를 확인

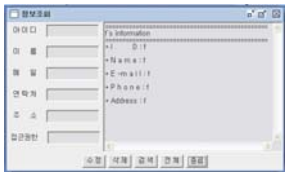


<e 사용자의 접근 정책 리스트>



<f 사용자의 접근 정책 리스트>

• ‘d’라는 사용자가 ‘f’, ‘e’ 사용자의 정보를 검색 확인



<f 사용자 검색 결과>

<e 사용자 검색 결과>

[그림 7] 정보제공자 접근제어 시험

3.5 Cipher model Block의 암호화 및 복호화 기능

자료에 대하여 암호화 및 복호화가 이루어지는지 시험한다. 절자는 User interface Block부터 정보 입력 시 입력 받은 값이 저장 시 암호화 되어 Database에 저장되고 사용자 요청 시 Database로부터 암호화된 정보를 요청하여 복호화 후 User interface Block으로 전송하는지 확인 한다. 시험결과는 Database 저장된 자료와 인터페이스 화면에 출력된 화면으로 확인한다.

3.5.1 시험 항목

• 회원 가입시 정보 및 회원 수정 정보가 암호화 되어 Database에 저장됨을 확인

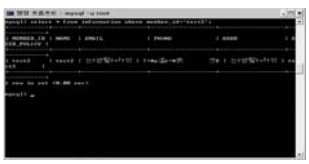
• 해당권한을 가진 사용자를 이용하여 암호화된 정보를 요청시 복호화가 이루어지를 확인한다(보안등급 2인‘a’라는 사용자 이용)

3.5.2 시험 결과

• 회원 가입시 정보 및 회원 수정 정보가 암호화 되어 Database에 저장됨을 확인

• 회원 가입시 암호화 단계 확인

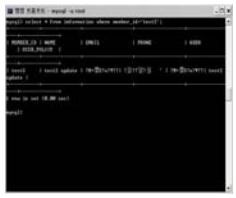
<회원가입 입력 폼>



<Imformation Database 확인>

• 개인 정보 수정시 암호화 단계

<정보 수정 폼>



<Imformation Database 확인>

- 해당권한을 가진 사용자를 이용하여 암호화된 정보를 요청 시 복호화가 이루어지를 확인한다(보안등급 3인 ‘test2’라는 사용자 이용)

4. 결론

본 논문은 Web환경에서의 사용자의 권한을 검증하고 권한에 대한 이중적인 접근제어 서비스를 제공하는 역할 기반의 WAC시스템의 블럭 설계서를 제안한다. WAC시스템은 User Interface Block, Access Control Block, Cipher module Block, DataBase로 구성 되며, WAC 시스템의 기능분류모델을 이용한 Block의 세부사항과 WAC시스템 기본 Bock(Access Control Bock)의 기본 기능 설계 및 사용자 접근제어 기능 설계, DES기반의 암호 Bock 기능 설계, 인터페이스 설계 대한 WAC 시스템의 전체적인 Block 설계에 대하여 기술한다.

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.