韓國 컴퓨터情報學會 論文誌
第9卷 第3號, 2004. 9.

2004-9-3-1-8

웹 기반 응용을 위한 직무 기반 접근 제어 시스템 모델 설계

이 호*

Design of a System Model for the Role-Based Access Control for Web-Based Applications

Lee, Ho*

요 약

본 논문의 목적은 안전한 직무 기반 접근 제어 모델을 웹 기반 응용 시스템에 통합하기 위해 필요한 시스템 모델을 설계하는 것이다. 이를 위해 우선 시스템 아키텍처 설계에 본보기로 활용할 수 있는 유저-풀 방식의 시스템 아키텍처 모델을 제안하고, 이 시스템 아키텍처가 웹 기반 응용 시스템에서 실제로 어떻게 직무 기반 접근 제어를 수행하는지를 보여주는 시스템 동작 모델을 제안하고자 한다. 그리고 본 논문에서 제안한 시스템 모델을 기존의 시스템과 비교 분석 함으로써 기존 방식에 대한 개선 효과를 제시한다.

Abstract

The purpose of this paper is to design a system model which is needed for integrating the secure role-based access control model into web-based application systems. For this purpose, firstly, the specific system architecture model using a user-pull method is presented. This model can be used as a design paradigm. Secondly, the practical system working model is proposed, which specifies the mechanism that performs role-based access control in the environment of web-based application systems. Finally, the comparison and analysis is shown in which the merits with the proposed system model is presented.

▸ Keyword : 직무 기반 접근 제어, Role-Based Access Control, RBAC

• 제1저자 : 이호
• 접수일 : 2004.08.27, 심사완료일 : 2004.09.08
* 국립 한국재활복지대학 정보보안과 부교수

Ⅰ. 서 론

웹은 인터넷상에서 전자 상거래 등이 가능하도록 하는 중요한 기반 기술이라고 할 수 있는데, 웹 환경에서 다양한 기술 및 구성 요소를 통합하기 위해 HTTP 프로토콜이 널리 이용되고 있다. 웹, 운영체제, 데이터베이스 시스템의 통합이 지속적으로 증가하고 있는 것으로 보아 기업 차원의 컴퓨터 활용을 위해 앞으로도 지속적으로 웹 기술을 사용할 것이라는 예측을 가능하게 한다. 그러나 현재 널리 사용되고 있는 웹 서버 기반의 보안 시스템에서는 아직도 사용자 인증 수준이거나 또는 사용자 기반의 접근 제어를 많이 이용하고 있다. 웹과 직무 기반 접근 제어의 통합은 기업 차원의 대규모 인터넷 기반 시스템의 보안을 강화할 수 있는 효과적인 수단을 제공할 수 있다. 본 논문에서는 참고 문헌 [1][9]에서 제안한 안전한 직무 기반 접근 제어 모델을 기업 차원의 대규모 웹 기반 응용 시스템에[2] 통합하기 위한 시스템 모델을 제안한다.

Ⅱ. 시스템 아키텍처 모델

웹을 이용하는 환경에서 접근제어를 위해 사용자의 속성 정보를 획득하는 방식으로 두 가지를 고려해 볼 수 있는데 유저-풀 방식(UPM)과 서버-풀 방식(SPM)이 그것이다[3]. UPM에서는 사용자가 속성 서버((그림 1)에서는 직무 서버가 그 역할을 수행함)로부터 속성 정보를 받아서, 접근 허가를 얻기 위하여 웹 서버에 보낸다. 반면에, SPM에서는 클라이언트가 사용자 인증을 위한 정보를 웹 서버에 제시하면, 웹 서버가 사용자 속성 정보를 속성 서버로부터 획득한 후에 사용자를 위한 접근 허가를 결정한다. 여기서는 UPM을 채택함으로써 (그림 1)에서처럼 클라이언트가 직무 서버로부터 사용자 속성 정보가 포함된 번들 인증서를(본 논문 3.1 참조) 받아서 웹 서버((그림 1)의 웹 기반 응용 시스템)로 보내는 방식을 사용한다.

본 논문에서 제안하는 웹 기반 응용을 위한 직무 기반 접근 제어 시스템의 모델은 (그림 1)에서와 같이 직무 기반 접근 제어(이하 RBAC) 관리 툴, 직무 서버, 웹 기반 응용 시스템의 세 가지 구성 요소로서 구성된다. 각 구성 요소 간의 인터랙션 및 각 구성 요소를 구성하고 있는 단위 기능이 (그림 1)에 표현되어 있다.

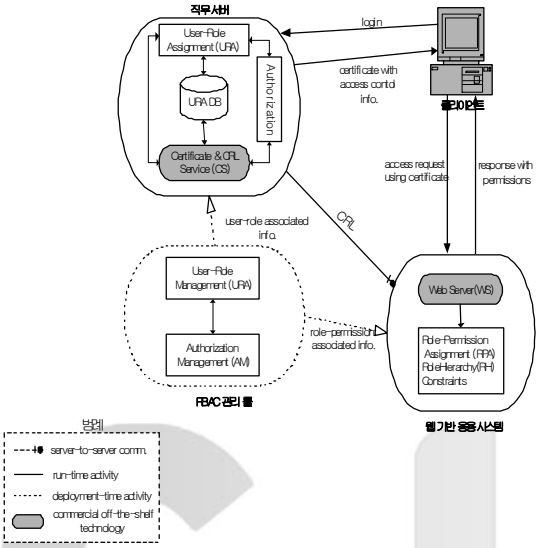

그림 1. 유저-풀 방식의 시스템 아키텍처
Figure 1. System Architecture using UPM

2.1 RBAC 관리 툴(RMT)

RMT는 다음의 역할을 수행하는 소프트웨어 툴로서 RBAC 시스템의 관리자가 시스템 배치 시에 RBAC의 운영에 필요한 각종 데이터를 생성하고 관리하는데 사용한다. RMT에 의해 만들어진 데이터 중에서 사용자-직무 관련 정보는 직무 서버로 직무-접근허가 관련 정보는 웹 기반 응용 시스템으로 보내진다.

① 사용자-직무 관리(URM) : 직무의 생성, 변경, 삭제 및 사용자의 단일 또는 복수의 직무에 할당이나 해지 등으로 인하여 발생하는 사용자-직무 관련 정보를 처리한다.

② 접근 허가 관리(AM) : 직무 서버에 저장되는 직무나 웹 서버에 저장되는 객체에 부여되는 보안 속성 정보의 생성, 변경 및 삭제를 처리한다. 즉 주체와 객체의 접근 제어 정보의 구성 요소 중에서 보안 속성 정보를 그 처리 대상으로 한다.

2.2 직무 서버

직무 서버는 RBAC이 적용되는 도메인 내에서 클라이언트를 위하여 다음 역할을 수행하는 전용 서버이다.

① 사용자 인증 : 클라이언트의 로그인 요청 시에 그 클라이언트가 RBAC이 적용되는 도메인의 웹 서버를 접근할 수 있는 자격이 있는지를 인증한다.
② 사용자-직무 할당(URA) : 인증된 사용자의 직무를 URA DB에서 검색하여 해당되는 직무를 사용자에게 할당한다.
③ 인증서 서비스(CS) : 클라이언트가 웹 서버에 접근을 요구할 때 필요한 사용자의 직무 및 보안 속성 정보를 포함하는 인증서를 발행한다. 아울러 주기적으로 인증서 해지 목록(CRL)을 게시하여 웹 서버들이 인증서 해지 목록을 입수토록 함으로써 클라이언트 인증 절차 수행 시에 해지된 인증서를 사용하지 못하도록 하는 기능을 담당한다.
④ URA DB : 각 사용자에 부여된 직무에 관한 DB를 유지 관리한다.

2.3 웹 기반 응용 시스템

웹 기반 응용 시스템은 웹을 기반으로 하는 응용 시스템이 동작하는 서버로서 응용 프로그램이 실행되기 위해 웹 서버(WS)가 설치되어 있다. 클라이언트가 웹 서버의 자원(객체)에 대해 접근을 요구하면 웹 기반 응용 시스템의 구성요소인 RPA와 RH & Constraints 기능이 함께 접근 허가 결정에 참여한다.

① 직무-접근허가 할당(RPA) : 사용자의 직무에 따른 보안 속성과 웹 서버 자원(객체)의 보안 속성을 비교하여 사용자의 객체에 대한 접근 요구에 대한 접근 허가를 결정한다.
② RH & Constraints(직무계층 및 제약조건) : 웹 서버마다 독립적으로 정한 원칙에 따라서 접근 허가 결정에 적용되는 직무 계층 및 RBAC 구성 요소에 대한 제약 조건이 달라지는데 접근 허가 결정 시에 직무 계층 및 제약 조건을 적용하는 역할을 담당한다 [4].

III. 시스템 동작 모델

3.1 안전한 직무 정보 전달 메커니즘

(그림 2)는 시스템 모델에서 직무 정보가 어떻게 안전하게 전달될 수 있는지를 보여주는 개념도이다. 직무 서버는 사용자가 어떤 직무를 부여받고 있는지에 대한 사용자-직무 할당 정보 데이터베이스를 가지고 있는데

① 클라이언트가 인증에 의하여 합법적인 사용자임이 확인되면,
② 사용자는 직무 서버로부터 도메인 내에서 자신에게 할당된 직무 정보를 획득한다.
③ 사용자가 자신의 직무를 사용하여 웹 서버에 접근을 요구하면 웹 서버는 사용자의 ID가 아니고 직무 정보를 이용하여 웹 서버와의 트랜잭션 허가 여부를 결정한다.

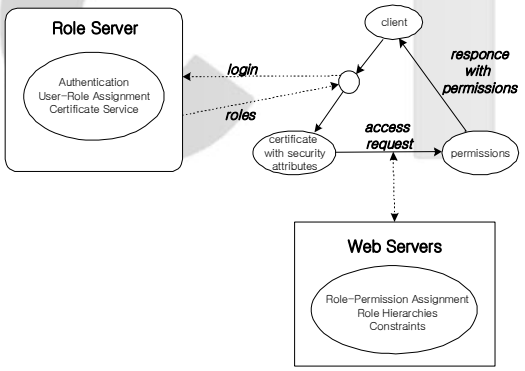

그림 2. 안전한 직무 정보 전달 메커니즘
Figure 2. Secure Mechanism for Role Information Transfer

이러한 과정에서 문제가 되는 것은 클라이언트가 제시하는 직무 정보를 웹 서버가 어떻게 신뢰할 수 있느냐는 것이다. 즉, 악의적인 사용자가 위조된 직무 정보를 이용해 웹 서버에 접근을 시도했을 때 이를 어떻게 방지할 수 있는가 하는 것이다. 이러한 문제점을 해결할 수 있는 방법으로서 여기서는 (그림 3)과 같은 절차를 거쳐 발행되는 번들 인증

서란 수단을 이용하는 방법을 제안한다. 번들 인증서란 X.509 v3의 확장 필드를 이용하여, SSL 등과 같은 기존의 표준안과 호환성을 유지하면서 웹상에서 안전한 속성 서비스를 하기위한 주체 식별자(ID)와 접근 제어 정보를 같이 포함하고 있는 인증서이다[5]. 이처럼 사용자의 ID, 직무 및 접근 제어 정보가 포함되어 있는 번들 인증서를 유저-풀 방식을 이용하여 전달토록 함으로써 직무 서버와 웹 서버 간에 속성 정보 전달을 위한 별도의 채널이 없이도 보안이 유지되는 직무 정보의 전달이 가능할 수 있다.

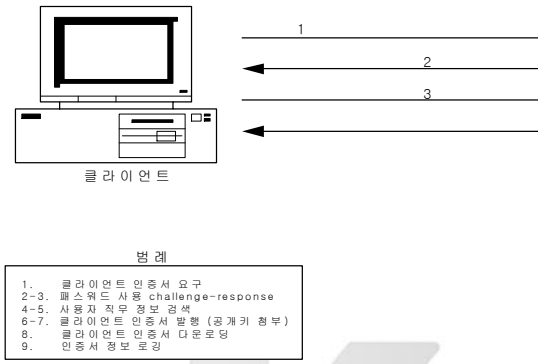

그림 3. 번들 인증서 발행 절차
Figure 3. Procedure of Issuing Bundled Certificates

3.2 안전한 직무 기반 접근 제어(SRBAC)의 웹상에서의 동작 메커니즘

(그림 4)는 번들 인증서(BC)의 발행, 웹 서버에서의 번들 인증서 처리 과정 및 RBAC 엔진의 임무 수행 과정을 보여준다. 클라이언트가 RBAC이 적용되는 도메인 내의 웹 서버와 트랜잭션을 하고자 하는 경우에는

① 세션의 시작 단계에서 클라이언트는 직무 서버와 연결을 설정하고,
② 직무 서버가 사용자를 인증하고 나면,
③ 직무 서버는 URA DB에서 사용자의 직무를 검색하여,
④ 사용자의 ID와 보안 속성들(직무 포함)을 포함시켜 인증서 서비스를 이용하여 번들 인증서를 생성하고,
⑤ 번들 인증서를 클라이언트로 전달하여 클라이언트 시스템에 저장한다.

따라서 사용자는 인증서의 유효 기간이 만료되기 전까지는 직무 서버로부터 번들 인증서를 재발급 받지 않아도 된다. 이것은 사용자가 번들 인증서에 포함된 직무를 인증서가 유효한 기간 동안에는 RBAC이 적용되는 도메인 내에서는 언제나 사용할 수 있다는 것을 의미한다. 여기서는 사용자 ID, 직무 및 접근 제어 정보는 동일한 인증기관에 의해 전자 서명 되는 방법을 사용하는 것으로 전제한다.

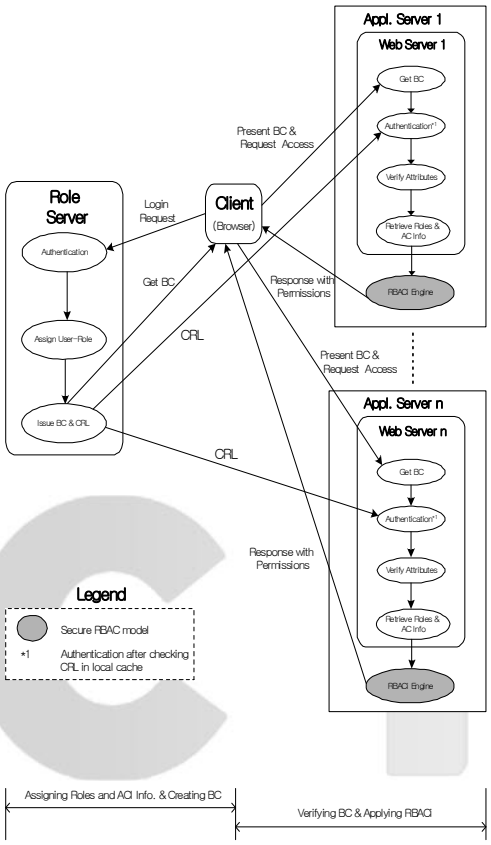

그림 4. SRBAC의 웹상에서의 동작 메커니즘
Figure 4. Operating Mechanism of SRBAC on WWW

사용자는 자신의 클라이언트 시스템에 복수개의 번들 인증서를 보관할 수 있다. 클라이언트가 특정한 웹 서버를 그 서버의 URL을 사용하여 접근하는 순간에, 클라이언트 측의 웹 브라우저와 상대측인 웹 서버는 SSL 프로토콜을 이용하여 서로를 인증하게 된다. 즉, 클라이언트의 브라우저가 웹 서버로부터 X.509 인증서를 받아 내용을 확인하여 자신의 시스템에 저장되어 있는 번들 인증서 중에서 부합하는 번들 인증서를 찾아 이를 웹 서버로 보내게 된다. 웹 서버는 클라이언트로부터 수신한 번들 인증서를 검사하여 사용자 인증을 하게 되는데, 이때 웹 서버의 로컬 캐시에 저장되어

있는 인증서 해지 목록을 먼저 확인하여 수신한 인증서가 이미 해지된 것인지를 확인하여 이상이 없는 경우에만 인증서 유효 기간과 전자 서명된 정보의 이상 여부를 확인한다. 이러한 일련의 과정을 정상적으로 통과하면 웹 서버는 번들 인증서가 포함하고 있는 직무 및 접근 제어 정보를 신뢰하여 이 정보를 응용 시스템의 RBAC 엔진이 사용하도록 전달한다. 그러면 RBAC 엔진은 안전한 직무 기반 접근 제어 메커니즘을 적용하여 주체(사용자)의 객체(자원)에 대한 접근 허가를 결정하는 과정을 수행한다.

3.3 인증서 해지 목록 처리 메커니즘

인증 기능((그림 4)에서 Issue BC & CRL이 담당)이 인증서를 해지하면 인증서는 유효 기간이 만료되기 전에 무효화되는데 인증서를 해지하는 사유로는 다음과 같은 것들이 있다[6].

① 인증서 주체의 개인키가 노출되었거나 그럴 가능성이 있는 경우
② 인증서의 불법 취득이 드러난 경우
③ 인증서의 주체가 더 이상 신뢰 받는 엔터티가 아닌 경우

이러한 사유로 해지된 인증서는 인증 기능이 인증서 해지 목록을 이용하여 배포한다. 웹 서버가 사용자가 제시한 번들 인증서를 받았을 때 그 인증서가 해지된 것인지를 확인하기 위하여 인증서 해지 목록의 배포 때마다 인증 기능으로부터 복사한 최신의 인증서 해지 목록을 항상 자신의 로컬 캐시에 보관하고 있다. (그림 4)의 직무 서버의 구성 요소인 Issue BC & CRL 기능이 인증서 해지 목록을 게시하는 기능을 수행하고 웹 서버는 인증서 해지 목록을 입수하기 위해서 Issue BC & CRL 기능과 주기적으로 정보를 교환한다.

3.4 웹 서버에서의 직무 기반 접근 제어 방법

일반적인 파일 시스템에서의 접근 허가는 어떤 사용자(주체)가 어떤 접근 권한을 사용하여 서버의 어떤 정보(객체)를 액세스할 수 있는지를 정의하도록 되어있다. 반면에 웹 서버에서의 접근 허가는 웹 사이트를 방문하는 불특정한 사용자들을 대상으로 하여 그들이 특정한 페이지를 볼 수 있는지, 스크립트를 실행할 수 있는지, 웹 서버에 정보를 업로딩할 수 있는지 등에 대한 접근 권한을 통제할 필요가 있다[7].

본 논문에서는 사용자가 웹 서버에 접근을 시도하면 웹 서버는 사용자에게 허용할 접근 허가를 결정하기 전에 우선 번들 인증서에 포함된 보안 속성 정보를 근거로 하여 RBAC 엔진 실행 시에 필요한 정보를 획득한 후 RBAC 엔진을 실행하여 접근 허가를 결정한다. 이 RBAC 엔진은 안전한 직무 기반 접근 제어 모델을 적용하여 (그림 5)와 같이 접근 제어 결정을 하도록 구성되어 있다[8].

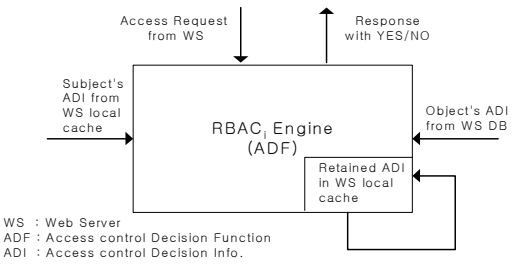

그림 5. RBAC1 엔진의 접근 제어 결정
Figure 5. Decision of Access Control by RBAC Engine

IV. 비교 분석

본 논문에서 제안한 시스템 모델은 기존의 접근 제어를 위한 시스템과 비교하여 다음과 같은 특성을 갖는다.

① 기존의 사용자 기반의 접근 제어를 위한 모델이 아니고 웹 환경에서 보안이 보장되는 직무 기반 접근 제어를 위한 모델이다.
② 유저-풀 방식을 사용하여 사용자 보안 속성 정보를 획득하기 위한 별도의 채널 없이도 직무 서버만을 사용하여 사용자 보안 속성 정보를 획득 할 수 있도록 구성되어 있다.
③ 전담 서비스를 하는 직무 서버를 모델에 도입하여 사용자 인증, 보안 정보 검색, 인증서 발급 기능 등을 웹 서버로부터 분리시켰다. 따라서 웹 서버는 접근 제어를 이용한 웹 서비스에만 전념할 수 있으므로 웹 서버의 부하가 경감된다.
④ 직무 서버가 발행하는 번들 인증서를 사용해 웹 서버를 접근함으로써 위장 사용자가 위조된 직무를 사용

하여 서버에 불법 접근하는 것을 차단한다.

⑤ RBAC 엔진을 시스템에 포함시킬 수 도 있고 직무에 객체 접근 허가를 직접 부여하는 방법을 사용하면 RBAC 엔진을 시스템에 포함시키지 않고서도 구현이 가능한 모듈러한 구조이다.

⑥ 사용자 정보를 단일 직무 서버에서 집중 통제함으로써 사용자 속성 정보 관리를 단순화 하고 정보의 분산으로 인한 불일치 문제를 원천적으로 방지한다.

⑦ 시스템 배치 시에 사용하도록 RMT를 시스템 구성에 도입함으로써 시스템 관리를 효과적으로 할 수 있다.

⑧ 번들 인증서 메커니즘, CRL 메커니즘, 웹을 기반으로 하는 안전한 직무 기반 접근 제어 메커니즘, SSL 등을 통합하여 보안이 취약한 웹 환경에서도 보안이 보장될 수 있는 시스템 구성이 가능하다.

<표 1>은 위에서 비교 분석한 내용을 요약한 것이다.

표 1. 시스템 모델 비교 분석
Table 1. Comparison between System Models

대상 항목	기존 시스템	제안 시스템
접근 제어 모델	일반적인 컴퓨팅 환경을 위한 사용자 기반 접근 제어 모델	웹 기반 응용을 위한 안전한 직무 기반 접근 제어 모델
속성 정보 처리 방식[3]	SPM	UPM
직무 정보 처리	웹 서버에 통합	전용 직무 서버 도입
인증서 방식	일반 인증서(X.509)	번들 인증서(X.509 확장 필드)
RBAC 엔진 배치	웹 서버에 통합	웹 서버와 분리 가능
직무 서버 구성	분산 서버	단일 서버
시스템 관리	제한적 기능	RMT 적용
보안 시스템 구성	개별적	통합적

V. 결론 및 향후 연구과제

본 논문의 목적은 참고 문헌[1][9]에서 제안한 안전한 직무 기반 접근 제어 모델을 웹을 기반으로 하는 응용 시스템에 통합하기 위한 시스템 모델을 설계하는 것이다.

이를 위하여 유저-풀 방식의 시스템 아키텍처 모델을 제안함으로써 유사한 목적을 갖는 시스템 아키텍처 설계를 하는데 본보기가 될 수 있도록 하였다. 시스템 아키텍처에는 X.509를 근간으로 하는 번들 인증서가 도입되었으며, 직무 서버, 웹 기반 응용 시스템, RBAC 관리 툴 등이 시스템을 구성하도록 설계되었다.

본 논문에서 제안한 시스템 아키텍처 모델을 보다 구체화하기 위하여 시스템의 동작 모델을 제안하였다. 이 동작 모델은 시스템이 실제로 어떻게 동작하여 웹 기술을 기반으로 하는 응용 시스템에서 직무 기반 접근 제어 실행이 가능한 지를 설명한다. 이 시스템 동작 모델을 참고로 하여 실제로 시스템을 구현할 때에 대두되는 기술적인 문제들을 해결할 수 있을 것으로 판단된다.

웹 서버에서의 접근 허가는 웹 사이트를 방문하는 불특정한 사용자들을 대상으로 하여 서버 자원에 대한 접근 권한을 통제하는 것을 필요로 한다. 이러한 특성을 갖는 웹 기반 응용 시스템에서는 기존의 사용자 및 파일 시스템을 기반으로 하는 복잡한 접근 제어보다는 웹 기반 환경에 최적화된 안전하면서도 단순한 방식의 직무 기반 접근 제어가 보다 효과적일 것으로 판단된다. 따라서 본 논문에서 제안한 웹 기반 응용을 위한 직무 기반 접근 제어 시스템 모델은 웹을 기반으로 하는 기업의 업무 처리를 위한 다양한 용도의 응용 시스템 구축에 널리 활용할 수 있을 것으로 사료된다. 본 논문의 연구 결과를 기존의 COTS(Commercial Off-The-Shelf Technology) 기술과 접목한다면 대규모의 상용 시스템 구현도 가능할 것으로 기대된다.

참고문헌

[1] 이호, "웹 기반 응용을 위한 직무기반접근 제어 모델의 설계", 한국 사이버테러 정보전 학회 정보보증논문지 제2권 제2호, pp. 59-66, 2002. 12

[2] Gail-Joon Ahn, Ravi Sandhu, Myong Kang, Joon Park, "Injecting RBAC to Secure a Web-based Workflow System", In Proc. of ACM RBAC 2000, pp. 1-10, 2000.

[3] Joon S. Park, "Secure Attribute Services on the Web", PhD Thesis, George Mason University, Aug., 1999.

[4] Ravi S. Sandhu, Edward J. Coyne, "Role-Based Access Control Models", IEEE Computer, pp. 8-47, Feb., 1996.
[5] Joon S. Park, Ravi Sandhu, "RBAC on the Web by Smart Certificates", In Proc. of ACM RBAC 1999, pp. 1-9, 1999.
[6] Network Working Group of Internet Society, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC:2459, Jan., 1999.
[7] Elisa Bertino, Silvana Castano, Elena Ferrari, "On Specifying Policies for Web Documents with an XML-based Language", In Proc. of ACM RBAC 2001, pp. 57-65, 2001.
[8] 이호 "웹 기반 응용 시스템을 위한 안전한 직무 기반 접근 제어 모델에 관한 연구", 박사 학위 논문, 성균관 대학교 대학원, pp. 75-76, 2002.
[9] 이호, 정진욱, "안전한 인터넷 사용을 위한 접근 제어 메커니즘 설계", 한국 컴퓨터정보학회 논문지, Vol. 5 No. 3, pp. 84-90, 2000.

저 자 소 개

이 호
1989년 벨기에 VUB 대학원 정보공학과(공학 석사)
2002년 성균관 대학교 대학원 정보공학과(공학 박사)
1982년 ~ 1991년 한국전자통신연구원 선임 연구원
현재 국립 한국재활복지대학 정보보안과 부교수
<관심분야> 시스템 보안, 네트워크 보안, 컴퓨터 네트워크