RBAC(Role Based Access Control)을 이용한 BYOD(Bring Your Own Device) 접근제어 관한 연구

배요한*, 이희조
*고려대학교 컴퓨터 정보통신대학원 디지털정보.미디어공학과
Email : byh1058@korea.ac.kr , heejo@korea.ac.kr

Access Control Model using RBAC in BYOD(Bring Your Own Device)

Yo-Han Bae*, Hee-Jo Lee
Dept. of Computer Information and Communication Engineering, Korea University

요 약

BYOD 는 다양한 기기에서 상호 운용되고, 상황에 따라 다른 접근권한을 가질 수 있다. BYOD 는 기업의 입장에서는 생산성 향상과 기기에 대한 비용 감소 등의 장점을 가지고 있다. 하지만 보안의 중대한 취약점을 가지고 있고 기업은 개인이 사용하는 각기 다른 기기들에 대해서 통제하기 힘들다는 점과 관리비용은 오히려 상승할 수도 있다는 점 등의 단점들이 부각이 되고 있다. BYOD 에 접근 가능한 권한들을 효율적으로 관리하여 접근권한 관련 설정 오류를 최소화하고, 권한이 없는 사용자의 접근을 차단하기 위한 'BYOD 환경에 적합한 접근 제어 기술'이 요구된다. 따라서 본 논문에서는 BYOD 시장의 급속한 발달과, 스마트 폰 하드웨어,소프트웨어의 발전에 맞춰 RBAC(Role Based Access Control)을 이용한 접근제어 방법을 제안한다. 이는 사용자 특성, 역할 특성, 시스템 특성에 따라 권한 활성화 제약이 가능하며, 권한 위임과 권한 상속 시에 시간, 위치정보, 위기 상황 발생여부에 따라 제약을 할 수 있다.

1. 서론

스마트폰, 태블릿 PC 등 개인 소유의 IT 단말기의 높은 보급률로 BYOD(Bring Your Own Device)에 대한 관심이 날로 증가하고 있다. 이는 개인 IT 장비를 업무에 활용하는 새로운 업무 트렌드로 기업이 제공하는 일반적인 PC 를 주요 업무용 단말기로 이용하면서 개인 IT 장비를 업무 보조적 수단으로 활용하는 것을 의미한다. 이는 'BYOD (Bring Your Own Device)' 가 급부상하고 있지만 기업들의 보안과 관리능력이 부족하고 직원들이 개인용 IT 기기를 통해 접속할 수 있는 정보를 보호할 수 있는 능력이, 개인용 IT 기기 사용 증가율에 미치지 못하고 있기 때문이다. 예를 들어, 보안을 위해 기기에 백신을 설치하게 하거나, 특정 프로그램을 제한하기 위해 제어 프로그램을 설치, 네트워크 접근 제어 방식(NAC: Network Access Control)을 통해 기기들 접근 제어, 보안 취약점 업데이트 등과 같은 통제가 개인용 기기에서는 제대로 반영되기 어렵기 때문이다. 이러한 문제로 인하여 BYOD 환경의 시스템 내부에 접근 가능한 권한들을 효율적으로 관리하여 접근권한 관련 설정 오류를 최소화 하고, 권한이 없는 사용자의 접근을 차단하기 위한 'BYOD 환경에 적합한 접근제어 기술'이 요구된다. [8]

접근제어를 위해 개발된 보안 정책으로는 임의적 접근 통제(DAC : Discretionary Access Control), 강제적 접근 통제(MAC : Mandatory Access Control), 역할 기반 접근 통제(RBAC : Role Based Access Control)모델들이 있다.[6,7] 그러나 이들 모델들은 모두 BYOD 환경에 대한 시간 제약에 따른 자원의 사용제한을 하지 못한다는 제약이 있고, 역할 계층상에서 상위 역할에 배정된 사용자가 하위 역할의 모든 접근 권한을 상속받게 되어 불필요한 권한의 실행을 허가하게 되어 최소 권한 원칙을 위배하게 되는 제약이 있다. 이러한 문제점들을 해결하기 위하여 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC (Generalized Temporal Role Based Access Control)[1,2,3]와 조건(condition), 목적(purpose), 의무(obligation)개념을 포함하여 프라이버시를 강화한 PRBAC(Privacy-aware Role Based Access Control)[4,5]의 모델의 특성을 이용하여 확장된 역할접근제어(RBAC) 방법을 제안하며, 본 논문에서 BYOD 환경을 분석하여 접근제어 요구사항들을 정리하여 사용자 특성, 역할 특성, 시스템 특성에 따른 권한 제약방식과 시간, 위기 상황 발생여부에 따라 제약이 가능한 권한 위임 및 상속 방식을 제시한다.[12]

본 논문의 구성은 다음과 같다. 2 장에서는 BYOD

환경 에서 접근제어 요구사항을 정리하며, 3 장에서는 이에 만족하는 적합한 접근제어 모델을 제안하며, 4 장에서 제안모델과 기존 모델을 비교 분석하여, 5 장에서 결론을 유도한다.

2. BYOD 환경에서의 접근제어 요구사항

최근에는 기존 접근제어 방법에 다양한 특성이 추가된 접근제어 방법들이 제안되고 있으나, BYOD 환경에서는 여러 가지 특성을 동시에 가지고 있어야 하므로, 기존의 접근 제어 방법을 그대로 적용할 수 없다. 본 논문에서는 BYOD 환경을 분석하여 접근제어 요구사항들을 [표 1] 정리하였다.[1,9,10]

<표 1> BYOD 환경에서 접근제어 요구사항

요구사항		
1	사용자 권한 활성화 제약	권한 사용 시간
		사용자의 위치정보
		권한 유효기간
		위기 시 권한 (비) 활성화
2	권한 위임	사용자간 위임
		역할간 위임
		다중 위임
3	권한 위임 제약	위임된 권한 사용 시간
		사용자의 위치정보
		타 역할 계층 사용자간 권한 위임
		위임된 권한 유효기간
		위기 시 임의 위임 가능
4	권한 상속 제한	역할계층 레벨
		유효기간

예를 들어 데이터 운영시스템과 BYOD 기기 와의 접근제어가 발생한 경우를 설명할 수 있다. BYOD 의 특정 기기가 데이터 운영시스템의 데이터에 접근하고자 할 때, 접근하려는 주체(BYOD)의 위치에 따라 접근을 허가하고, 정해진 시간 외에는 권한을 가진 주체라도 해당 권한을 사용할 수 없도록 조치해야 한다. 또한 데이터 운영시스템은 BYOD 기기에 권한을 부여할 때, 유효 기간을 설정하여 일정시간 이후에는 재 인증이 이뤄지도록 해야 한다. 데이터 운영시스템에는 Data Administrator, Data Operator, 실시간 모니터링 업무 수행자와 같은 관리자 들이 각각 업무에 필요한 다양한 역할들을 부여 받아야 한다고 가정할 수 있다. Data Administrator 가 자리를 비울 경우, 상황에 맞게 권한의 일부를 동료에게 위임할 수 있어야 한다. 또한 데이터 운영시스템이 공격을 받아 일부 프로세스가 동작하지 않을 경우, 위기상황을 감지하여 다른 프로세스에 권한을 위임함으로써 시스템운영이 중단되는 상황을 피할 수 있어야 한다. 하지만 무분별한 권한위임은 보안상 심각한 위협으로 작용될 수 있으므로 사용자가 위임된 역할을 사용하는 시간이나 사용자의 위치정보에 따라 권한위임에 제한을 두어야 한다. 또한 위임된 권한이 남용되지 않도록 권한 위임 시 유효기간을 설정해야 한다. 역할기반 접근제어에서 역할계층을 사용하면 상위계층 역할이 하위 계층 역할의 퍼미션을 상속받게 된다. 이때 모든 역할의 퍼미션이 역할계층의 레벨에 따라 상속될 경우 상위 계층 역할을 부여 받은 사용자에게 필요 이상의 객체접근이 허용될 수 있으므로 역할계층의 레벨과 상속 유효기간에 따라 상속된 역할에 제한을 가할 수 있어야 한다.

3. RBAC (Roll Base Access Control)

본 논문에서는 역할접근제어 방식 중 GTRBAC (Generalized Temporal Role Based Access Control)의 시간과 주기에 따른 권한 활성화 제약 특성과 PRBAC 의 조건(condition), 목적(purpose), 의무(obligation), 프라이버시를 강화한 특성을 병합하여 제안한다.[9,11]

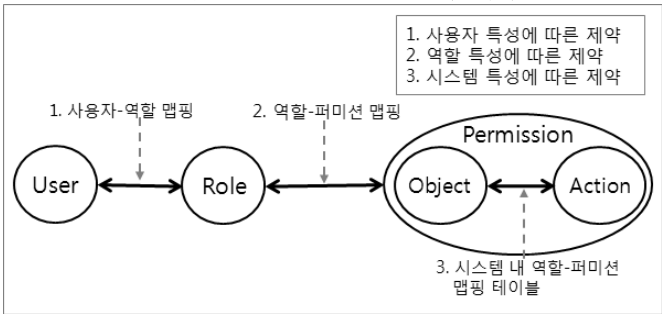
3.1 RBAC 기본 구성

RBAC 의기본모델은 사용자(U), 역할(R), 인가권한(P), 세션(S)으로 구성되어 있다. 사용자(User)와 역할(Role)은 역할은 접근제어 정책을 구현하는 중요한 의미적 구조이다. 역할 계층은 관련성이 있는 역할들간의 부분순서 관계로서 정의되며 기업의 권한과 책임의 체계와 매우 유사하여 적합하다. 인가권한(Permision)은 접근대상이 되는 객체(object)와 접근방법(action)으로 구성된다. 세션(Session) : 사용자는 시스템의 로그인을 통해 그들이 가진 역할의 집합을 활성화 할 때 세션을 형성한다. 사용자 배정과 인가권한 배정은 사용자 배정과 인가권한 배정은 다대다 관계이며, RBAC 모델에서 가장 중요한 요소이다.[13]

3.2 권한 활성화 제약

RBAC 모델은 사용자 특성과 역할 특성에 따라 사용자의 위치 정보, 시간, 주기 등을 고려하여 접근 권한 활성화의 제약을 할 수 있으며, 크게 3 가지 제약으로 구분할 수 있다. 사용자-역할 맵핑, 역할.퍼미션 맵핑, 시스템 관리자에 의해 관리되는 시스템 특성에 따른 제약방식을 제안한다. [그림 1]참조.[1,2,9]

<그림 1> RBAC 권한 활성화 제약



3.2.1 사용자 특성에 따른 권한 제약

관리자는 사용자를 식별 및 인증하고, 정당한 사용자에게 적절한 역할을 부여한다. 특정 시스템의 객체에 접근하려는 주체는 유효한 인증 크래덴셜을 시스템 관리자에게 제시하여 주체가 객체 접근에 대한 퍼미션이 부여된 역할을 수행하고 있는지 증명해야 한다.
[9,10,14]

3.2.2 역할 특성에 따른 권한 제약

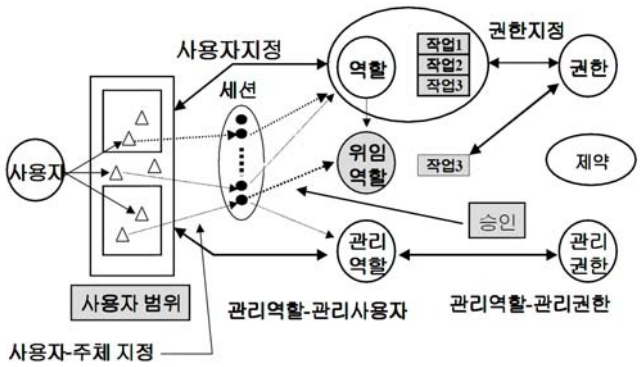
역할의 특성에 따라 특정 객체에 접근 시 정해진 시간 안에 또는 특정 위치 안에서만 접근권한이 필요할 수 있다. 이러한 경우에는 역할유효조건에 해당 시간 또는 위치를 적용하여 역할이 특정시간과 위치에서만 퍼미션이 활성화 되어 접근권한을 사용할 수 있도록 한다.[4,5]

3.2.3 시스템 특성에 따른 권한 제약

BYOD 환경에 적용되는 다양한 시스템들은 서로 다른 시스템 환경과 특성을 가지므로 각 시스템 관리자들이 시스템 특성에 따라 사용자의 객체접근에 추가적인 제한을 두어야 한다. 따라서 각 시스템마다 객체접근조건과 의무사항을 이용하여 시스템 관리자들로 하여금 객체접근에 대한 추가적인 제한을 가할 수 있도록 해야 한다.[4,5,9]

3.3 권한위임 방법

<그림 2> RBAC 권한 위임 모델



[그림 2]에서 실제 사용자가 시스템을 통해 업무을 수행하면서 다른 사용자에게 권한의 일부를 위임해야 하는 상황이 발생할 수 있다. 하지만 무분별한 권한 위임은 보안상 심각한 위협으로 작용이 될 수 있으므로, 권한위임에 제한을 두어야만 한다.[9,11]

3.3.1 권한 위임 제한

무분별한 권한위임은 보안상 심각한 위협이 될 수 있으므로 권한위임에 제한을 두어야만 한다. 권한 위임이 발생하는 과정에서 위임속성값에 포함된 조건을 이용하여 위임속성값의 유효기간, 사용자의 시간, 위치정보에 따른 다양한 제한을 가할 수 있게 되며, 이벤트 조건을 추가하여 위기 상황이 발생할 경우 각 상황을 예외적으로 처리하여 해당 담당자가 없더라도 위임된 권한이 활성화되어 필요한 기능을 수행할 수 있도록 한다. 또한 역할 계층이 서로 다른 사용자에게 각각 다른 역할을 위임할 수 있게 된다.[7,14]

3.3.2 권한 상속 제한

역할계층을 사용하는 RBAC 에서는 상위 계층 역할이 하위 계층 역할의 퍼미션을 상속받게 된다. 이때 모든 역할의 퍼미션이 역할계층의 레벨에 따라 상속될 경우 상위 계층 역할을 부여받은 사용자에게 필요 이상의 객체접근이 허용될 수 있으므로 상속제한조건을 사용하여 상속이 부분적으로 일어나도록 제한할 수 있다.[5,10]

4. 제안 모델과 기존 모델의 비교

시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있고, 역할 활성화와 이벤트, 트리거를 이용하여 사용자 수를 제한하고 워크 플로우에 해당하는 작업을 다룰 수 있는 장점을 가지는 GTRBAC (Generalized Temporal Role Based Access Control)[1,2,3] 모델과 사용자, 의무, 역할, 데이터, 목적, 행동 그리고 조건의 7 개체로 구성되어 있는 PRBAC(Privacy-aware Role based Access Control)[4,5]의 기존 접근제어 모델의 특징을 비교하면 다음 [표 2]와 같다. [표 2]에서 기존 모델과 제안 모델과의 비교 항목은 접근제어 모델을 실제 BYOD 환경에 적용하기 위하여 반드시 고려되어야 하는 항목이다.

<표 2> 제안 모델과 기존 모델의 비교

			GTRBAC	PRBAC	제안모델
1	일반 역할 및 권한		○	○	○
2	역할 활성화 유효시간과 기간 제약		○	×	○
3	권한 위임	사용자간 위임	×	○	○
		역할간 위임	×	○	○
		다중 위임	×	○	○
4	권한 위임 제약	위임된 권한 사용 시간	○	×	○
		타 역할 계층 사용자간 권한 위임	×	○	○
		권한 유효기간	○	×	○
		위기 시 임의 위임 기능	×	×	○
5	권한 상속 제한	역할의 활성화 제약과 유효 시간 제약	○	×	○
		역할계층 레벨	×	○	○

구성원간의 연속적인 업무환경을 고려하기 위하여 워크플로우가 고려되어야 하고, 시간과 기간에 따른 권한을 제어할 수 있어야 하며, 역할의 상속을 제한하여 최소 권한 만으로 업무 수행이 가능하여야 하며, 사용자에게 할당된 권한을 위임 할 수가 있어야 한다.

기존의 역할제어모델은 모델은 권한의 상속 제한 기능, 권한의 위임 기능 두 가지 모두를 고려하지 않고 있으며, 워크플로우를 고려하지 않는 경우도 있어 BYOD 환경에 적용하기에는 무리가 따르며, 제안 모델 또한, 사용자의 위치 정보에 따른 역할의 활성화 제한과 역할의 제한적 상속 기능을 제공하지 않아 BYOD 환경의 접근제어에 적용할 수 없는 단점이 있다.[12]

5. 결론 및 향후 연구

본 논문은 BYOD 환경을 분석하여 접근제어 요구사항들을 정리하고, 제안한 요구사항들을 만족하는 방법을 제안하였다. 기존 모델들은 요구사항의 일부만을 만족하고 있다. 제안된 RBAC 모델은 GTRBAC[1,2,3]의 시간에 따른 권한활성화 제약 특성과 PRBAC[4,5]의 조건 · 의무 개념을 동시에 가지며, 다양한 권한 활성화 제약 방식과 권한 위임 방식을 가진다. 사용자 특성, 역할 특성, 시스템 특성에 따라 권한 활성화 제약이 가능하며, 또한 다양한 권한 권한위임방법을 가지며 권한위임과 권한상속 시 제약이 가능하다. 이러한 다양한 제약방법은 문서로 정의된 접근제어 정책을 실제 시스템에 유연하게 반영하고 불필요한 권한 활성화, 권한 위임, 권한상속이 발생하지 않도록 하여 요구사항을 만족 시킬 것으로 예상된다.

향후 연구로는 권한부여 정책과 제약조건 정책간의 충돌 그리고 제약조건 정책간의 충돌에 대한 연구가 필요하며, 이 방안을 기초로 한 보안 관리체계의 구체적 모델화와 실체 BYOD 환경 시스템에 적용을 통한 성능분석이 향후 과제로 남는다.

참고문헌

[1] Elisa Bertino, Piero A. Bonatti, Elena Ferrari, “TRBAC:A temporal role-based access control model. ACM Trans,” Inf. Syst. Secur. (TISSEC), vol. 4, no. 3, pp.191-233, Aug. 2001.

[2] James Joshi, Elisa Bertino, Arif Ghafoor,“Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model,” COMPSAC, pp. 951-956, Aug.2002.

[3] James Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, “A Generalized Temporal Role-Based Access Control Model.” IEEE Trans. Knowl. Data Eng. (TKDE), vol. 17, no. 1, pp. 4-23, Jan. 2005.

[4] Anour F. A. Dafa-Alla, Eun Hee Kim, Keun Ho Ryu, Yong Jun Heo, “PRBAC: An Extended Role Based Access Control for Privacy Preserving Data Mining,” ACIS-ICIS, pp. 68-73, Jul. 2005.

[5] Qun Ni, Elisa Bertino, Jorge Lobo, Seraphin B. Calo, “Privacy-Aware Role-Based Access Control,” IEEE Security & Privacy (IEEESP), vol. 7, no.4, pp. 35-43, Jul.2009.

[6] David F.Ferraiolo, D.Richard Kuhn, Ramaswamy Chandramouli, Role-Based Access Control, 2nd edition, Artech House, Inc., 2007.

[7] Edward J. Coyne, John M. Davis, Role Engineering for Enterprise Security Management, Artech House, Inc., 2008.

[8] Bill Morrow, BYOD security challenges_control and protect your most sensitive data ,2012, Quarri Technologies,

[9] 황유동, 박동규, “기업환경의 접근제어를 위한 확장된 GTRBAC 모델 ” , 한국멀티미디어학회, 2005.02, 8 권 2 호

[10] 이우묘, SG-RBAC : 스마트그리드 환경에 적합한 역할 기반 접근제어 모델,情報保護學會論文誌第 23 卷 第 2 號, 2013. 4

[11] 조혁현, RBAC 에 기초한 통합형 프라이버시 보호 모델, 情報保護學會論文誌第 20 卷 第 4 號, 2010. 8

[12] 이봉근, 유헬스케어 서비스 환경을 위한 RBAC 기반의 프라이버시 모델, 韓國情報技術學會論文誌 제 9 권 제 9 호 2011 년 09 월

[13] 김도우, 홈네트워크서비스를위한 RBAC 기반의접근제어시스템의 설계, 한국해양정보통신학회,2005 9 권,제 2 호

[14] 나현혜, 프라이버시-인지 역할기반 접근 제어의 산술연산 구현 전략, 2011 한국컴퓨터종합학술대회 논문집 Vol.38,