http://dx.doi.org/10.14400/JDC.2016.14.2.191

서비스 기반 RBAC의 효율적인 개인별 정책 설계에 관한 연구

문형진, 한군희
백석대학교 정보통신학부

A Study on Design for Efficient Personal Policy of Service based RBAC

Hyung-Jin Mun, Kun-Hee Han
Division of Information and Communication Engineering, Baekseok University

요 약 기업이나 기관에는 법률과 지침에 근거하여 개인정보 보호를 위한 정책이 수립한다. 하지만 개인별로 정보 유출시 침해정도가 다름에도 기관은 개인정보의 특수성을 고려되지 않은 상태로 접근제어가 이루지고 있다. 개인정보의 특수성을 고려하여 개인이 자신의 정보를 보호하기 위한 정책을 수립할 필요하다. 하지만 기관에 있는 시스템의 이해가 부족한 개인이 자신의 정책을 수립하기는 쉽지 않다. 효율적으로 개인이 자신의 정책을 수립하기 위해 기관에서 제공하는 서비스별로 접근권한을 부여할 수 있는 시스템이 요구된다.
본 논문에서는 기관에서 제공된 서비스항목을 기준으로 개인별 정보보호 정책을 수립이 가능한 모델과 그 방법을 제안하다. 제안 방법을 통해 세밀한 권한부여와 자신의 수립한 정책변경이 용이하고, 궁극적으로 자신의 정보에 대한 맞춤형 접근제어가 가능하다.

주제어 : 역할기반접근제어, 서비스기반접근제어, 프라이버시 보호, 개인별정책

Abstract The organizations and companies establish personal information protection policy under the law and guidelines. They carry out access control without consideration for distinctiveness of the information although the damage degree varies when the information is leaked. Considering the distinctiveness, a policy needs to be made for individuals to protect his personal information. However, he is not able to write the policy because of lack of understanding the system. To write his own policy efficiently, the system that authorizes ones according to service list provided by organizations is necessary.
This paper suggests the model and method that write personal policy for his information protection based on the service list provided by organizations. Through this model, fine-grained authorization and policy change are easily made and ultimately the access control customized according to one's own information is possible.

Key Words : RBAC, Service based Access Control, Privacy Protection, Personal Policy

Received 7 November 2015, Revised 10 January 2016
Accepted 20 February 2016, Published 28 February 2016
Corresponding Author: HyungJin Mun(Division of Information and Communication Engineering, Baekseok University)
Email: jinmun@gmail.com

ISSN: 1738-1916

1. 서론

다양한 서비스를 받기 위해 기관이나 기업에 개인정보를 제공하고 있지만 정보주체인 개인은 정보사용에 대한 사항을 확인하기 쉽지 않다. 뿐만 아니라 개인정보 특수성으로 인해 개인별로 세심한 정보 접근제한 등이 쉽지 않다.

대부분의 개인정보들이 기관에서 개인별 서비스를 목적으로 수집되었지만 수집된 정보와 목적에 반하여 사용하는 사례가 많아 개인들은 불안해하고 있다. 특히, 정보를 수집한 기관들은 수집된 정보를 사용하는 사용자의 역할에 맞게 정보를 접근할 수 있도록 접근권한을 부여하므로 시공간에 상관없이 접근할 수 있는 권한이 있는 역할을 가진 사용자라면 언제 어디서든지 정보 접근이 가능하다.

은행 등에서 대출이나 적금 관련하여 개인의 신용정보를 확인하기 위해 동의서를 요구하지만 동의서를 철회하는 기간이 지정되지 않으면 언제까지 정보를 접근할 수 있는 지에 대한 제한사항이 없다.

정보주체인 개인이 해당 서비스를 받는 시간에만 자신의 정보를 제공할 수 있는 접근제어모델이 필요하다. 이처럼 서비스 기반으로 보호하는 모델의 요구사항은 다음과 같다.

- 시스템에서 개인이 요구한 서비스를 제공하기 위한 서비스 시간의 시작과 끝을 알아야 한다.
- 효율적으로 서비스를 제공하기 위해 온라인을 통해 실시간으로 처리가 가능해야 한다.
- 정보를 제공하는 서비스 시간을 손쉽게 수정이 가능해야 한다.

개인별 정책수립이 필요한 이유는 다음과 같다.

1. 개인정보보호 모델은 정보주체의 동의를 얼마나 적절하게 구할 수 없다.

2. 사용약관을 통해 일괄적으로 사용자의 동의를 구하는 것은 적절하지 못하다.

3. 개인의 모든 정보에 대한 세밀한 접근 권한 부여 및 사용동의를 제공하는 것이 어렵다.

4. 사용자의 기술적 이해가 부족으로 인해 정보 오남용을 차단할 필요가 있다.

서비스를 제공하는 기관이나 기업이 프라이버시 측면에서 개인사용자에게 서비스단위로 정보사용 동의를 구할 수 있도록 배려해야 한다.

하지만, 기존 접근제어 기술인 역할기반의 RBAC는 다음과 같은 요구사항을 만족하기 어렵다.

- 일반 사용자인 개인이 자신의 정보를 어디까지 제공해야 하는지, 누구에게 제공해야 하는지를 결정하기가 어렵다.
- 정보시스템의 이해 없이 개인의 모든 정보 에 대한 접근 권한을 결정하는 정책을 세우기 어렵다.

2. 관련연구

2.1 프라이버시보호기술

개인정보의 빈번한 유출사례로 인해 인터넷 및 전자기기 사용자들이 두려움을 가지게 되면서 개인정보 보호에 대한 정책 및 기술 등 활발한 연구들이 진행되고 있다[1,2,3,4,5,6]. 개인정보 보호를 위한 가이드라인이나 법률이 UN, OECD 등의 국제기구에서 제정되고 있다. 지침 등에서 정보주체인 개인의 사용동의, 개인의 통제권 등을 강조하고 있다[7].

개인정보를 보호하는 기술로 암호화기술을 활용하는 연구가 활발하게 진행되고 있다[8,9,10]. HP연구소에서는 시스템적으로 대량의 개인정보를 보호하기 위한 기술을 제안하였다[8]. 중요하고, 민감한 정보 필드 전체에 대해 암호화하여 저장하고, 접근권한이 있는 사용자에게 키를 제공하여 정보를 접근할 수 있는 시스템을 제안하므로 개인정보를 보호하고 있다. P2MS 모델은 개인별로 정책을 기준으로 보호가 필요한 모든 정보를 각기 다른 키를 이용하여 암호하는 기법을 제안하였지만 정책수립 및 키 관리 등의 문제점을 가지고 있다[9].

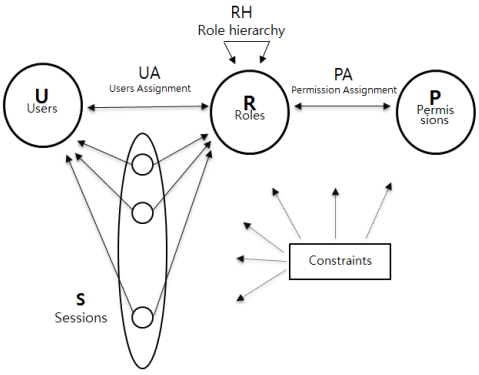
Sesay, S 는 저장된 개인정보를 3개의 등급(민감한 정보, 분류된 정보, 분류되지 않은 정보)으로 나누고, 민감한 정보와 분류된 정보에 대해서 암호화하여 데이터베이스에 저장하였다. 하지만 민감한 정보는 개인마다 다르지만 이를 반영하지 못하였다[10].

2.2 접근제어기술

2.2.1 RBAC 96

RH. Sandu가 제안한 역할기반접근제어(RBAC)는

기관이나 기업과 같이 복잡한 조직의 구조에서 적용이 가능한 기술이다[11,12,13]. 기관 내의 사용자들의 역할에 권한을 부여하므로 역할에 부합하지 않은 접근을 통제할 수 있는 기술이다[Fig. 1]. 하지만 개인정보와 같이 개인마다 민감한 정도가 다르고, 개인정보의 특수성으로 인해 RBAC 접근제어기술이 적합하지 않다. RBAC 접근제어 기술을 응용하여 개인정보 보호에 적용가능한 모델이 제안되었다[9,14].



[Fig. 1] RBAC96 Model

2.2.2 SpRBAC

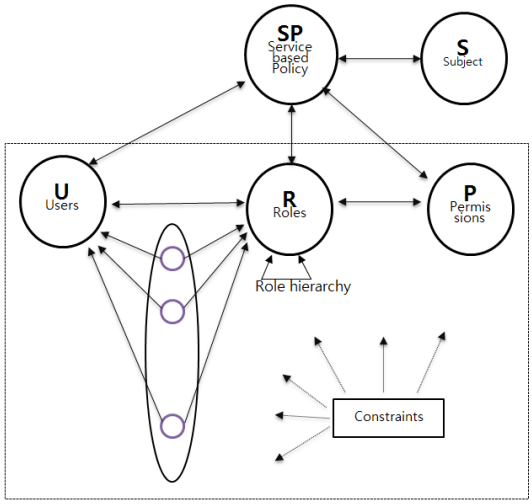
인터넷 사용자인 개인마다 각기 다른 민감한 정도의 차이가 있고 개인정보에 대한 특수성이 있기 때문에 개인이 자신의 정책을 수립하는 것이 필요하지만 개인별 정책을 수립하기 위해서는 개인이 시스템의 이해와 접근제어에 대한 이해가 필요하다[15,16].

SpRBAC 모델을 기반으로 민감한 개인정보관리시스템역시 개인별 정책 수립이 쉽지 않다.

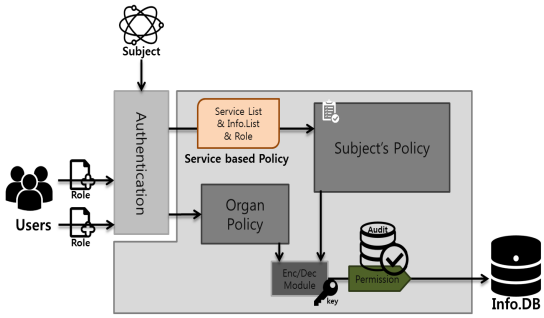
3. 제안모델

3.1 Service Based RBAC Model

RBAC 접근제어 모델에서 개인별 정책을 수립을 위한 서비스 기반으로 접근제어모델을 제안한다[Fig. 2]. 제안한 접근제어 모델을 기반으로 정보주체인 개인의 정보를 개인별 정책에 기반하여 관리할 수 있는 정보시스템의 프레임워크은 [Fig. 2]와 같다.



[Fig. 2] Proposed Model



[Fig. 3] Framework for proposed model

[Fig. 2, 3]에 보듯이 현실적으로 정보주체인 개인이 개인별 정책을 수립하기 쉽지 않기 때문에 기관이나 기업에서 제공하는 다양한 서비스 항목을 개인에게 제공한다. 개인에게 제공된 서비스 항목에서 서비스 받고 싶은 항목을 체크하면 체크된 항목을 기반으로 개인별 정책이 자동으로 수립되고, 개인이 서비스를 받고 난 후에는 체크를 해제하므로 써 정보사용에 대한 동의를 철회할 수도 있다.

3.2 Component

3.2.1 정보주체(Subject)

정보주체는 자신의 정보를 제공하는 고객으로, 기관이나 기업은 고객에게 다양한 서비스를 제공하기 위해 반

드시 개인의 정보가 필수적으로 요구한다.

3.2.2 사용자(User) 및 역할(Role)

- 사용자는 기관이나 기업의 구성원으로 서비스를 제공하기 위해 정보사용 주체를 의미한다. 사용자에게 개인이 요구하는 서비스를 제공하기 위해 해당 정보를 접근권한이 부여가 되어야 한다. 사용자의 역할이 존재하여 접근할 수 있는 범위가 역할에 맞게 기관의 정책에 의해 정해져 있다. 세밀한 접근제어를 위해 기관의 정책이외에도 정보주체가 수립된 정책에 의해 접근을 통제받을 수 있다.

-역할은 정보사용자마다 개인정보 보호를 위한 정책에 명시되어 있다. 이 정책에는 정보사용자의 역할이나 접근 범위, 서비스별로 필요한 정보목록 등 개인정보 사용 및 관리에 대한 정책이 수립되어 있다.

3.2.3 개인별 정책

개인정보는 다른 정보와 다르게 피해주체가 개인에게 있고, 침해 정도 역시 개인마다 다르다. 이로 인해 개인별로 정보보호를 위한 정책이 필요하다. 개인별 정책을 정보주체인 개인이 수립하는 것이 맞지만 기관 시스템의 이해와 접근제어에 대한 이해가 부족한 개인의 정책을 수립하기 쉽지 않다. 제안모델에서는 서비스별로 규격화하여 자신의 받고자 하는 서비스를 선택함으로써 개인별 정책이 자동으로 생성된다. 서비스별 정책수립은 최소한의 개인정보만을 접근하도록 규격화되어 있다.

3.2.4 권한(Permission)

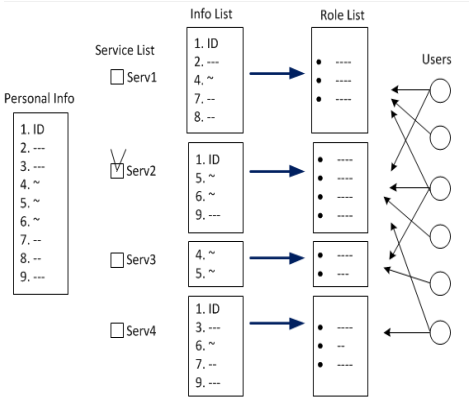
개인의 정보에 대한 접근권한은 기업의 정책과 정보주체인 개인의 정책의 교집합으로 구성된다. 즉, 기업의 정책에서 허용되었다할지라도 해당정보의 주체의 정책에서 허용하지 않는다면 접근이 불가능하다.

3.2.5 세션(Session)

세션은 사용자가 접근 가능한 역할에 의해 생성된다. 개인별 정책에서 허용된다면 세션 생성과 철회는 RBAC 모델과 동일하다.

3.3 Service Policy

기관에서 제공하는 서비스에 대한 정책을 제공하고, 서비스 기반으로 개인별 정책을 [Fig. 4]과 같이 수립한다.



[Fig. 4] Structure of Service Policy

서비스별 정책에 대한 구성은 다음과 같다.

- Personal Info : 기관이나 기업이 다양한 서비스를 제공하기 위해 개인으로부터 수집할 수 있는 최소한의 정보목록이다.
- Service List : 기관에서 고객인 개인에게 제공되는 서비스 목록이다.
- Info List : 서비스마다 제공하는데 반드시 필요한 정보의 최소목록이다.
- Role List : 서비스마다 개인의 정보에 접근 가능한 사용자의 역할목록이다.
- User : 기관내에 정보를 접근하는 사용자의 직함이나 이름을 제공할 수도 있다.

기관에서 [Fig. 4]와 같이 서비스목록을 제시한다. 서비스별로 사용되어지는 개인의 정보목록, 이 정보를 사용하는 사용자의 역할을 보여준다. 제공된 정보를 보고 개인은 체크함으로써 자신의 정책을 손쉽게 작성이 가능하다. 뿐만 아니라 언제든지 서비스가 종료된 경우 체크된 서비스를 해제함으로 개인별 정책의 변경이 가능하다.

4. 평가 및 결론

기관의 서비스가 다양해지고, 필요한 정보를 요구하는 서비스에 따라 세밀한 접근제어가 필요함에도 불구하고,

일괄적인 사용과 관리로 지정되어 있는 정책으로는 개인정보 특수성을 반영하고 있지 못하다. 개인정보의 특수성, 민감정도로 인해 개인정보보호기준이 일관적인 보호에서 개인별 요구에 맞는 보호로 변하고 있다. 하지만 인터넷 사용자인 개인이 자신의 요구에 맞게 정책을 수립하는 것이 쉽지 않다.

제안모델을 통해 정보보호에 대한 기술적인 이해 없이도 손쉽게 정책을 수립하고 세밀한 접근근제어가 가능하다.

<Table 1>은 프라이버시 보호를 위한 정책수립, 접근제어의 측면, 수립된 정책의 변경 편이성 측면에서 기존 모델과 비교한 표이다.

〈Table 1〉 Analysis of Models

	policy building	fine-grained access control	policy change
RBAC[11]	×	△	×
P2MS[9]	△	○	×
SpRBAC[15]	○	○	△
proposed Model	○	○	○

제안모델은 서비스기반의 접근제어와 개인별 정책을 통한 세밀한 정보접근이 가능하다.

하지만, 기관은 제공하는 서비스에 따라 사용되는 개인정보목록, 정보사용자의 역할에 따른 적절한 정보접근권한 부여 등 서비스 목록에 따른 접근권한의 세밀한 분석이 필요하다. 다양한 상황 발생이 발생할 경우 개인정보정책이 정적으로 수립되어 능동적으로 상황에 맞게 수정되지 않는다. 향후 연구로 정보주체인 개인의 사용패턴, 개인정보의 민감도 등을 분석하여 그에 맞는 적절한 보호와 능동적인 개인정보보호 정책을 수립하는 기술에 대한 연구가 필요하다.

REFERENCES

[1] J.Y Go, K.H Lee, “SNS disclosure of personal information in M2M environment threats and countermeasures”, Journal of the Korea Convergence Society, Vol. 5, No. 1, pp.29-34, 2014.

[2] BBC News. S. Korea credit card firms punished over data theft. BBC News Business. http://www.bbc.co.uk/news/business-26222283, Feb 17, 2014

[3]J.L. Yoo, “Personal Information Protection in Digital Era-Reviewing Personal information protection Act-”, Journal of Digital Convergence, Vol. 9, No. 6, pp81-90, 2011.

[4]J.H. Kim, J.Y. Go, K.H. Lee, “A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing”, Journal of the Korea Convergence Society, Vol. 6, No. 1, pp85-91, 2015.

[5] H. Zoo, H Lee, J. Kwak, Y Kim, “Data Protection and Privacy over the Internet: Towards Development of an International Standard”, Journal of Digital Convergence, Vol. 11, No. 4, pp57-69, 2013.

[6] K.J. Lee,“Analysis of Threats Factor in IT Convergence Security”, Journal of the Korea Convergence Society, Vol. 1, No. 1, pp49-55, 2010

[7] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 2013

[8] M.C. Mont, S. Pearson, P. Bramhall., “An Adaptive Privacy Management System For Data Repositories,” TrustBus2005 (LNCS Vol. 3592), pp.236-245, 2005.

[9] H.J. Mun, K.M. Lee, S.H. Lee, “Person-Wise Privacy Level Access Control for Personal Information Directory Services,” EUC2006 (LNCS Vol. 4096), pp.89-98, 2006.

[10] S. Sessay, Z. Yang, J. Chen, D. Xu, “A Secure Database encryption scheme”, Proceedings of second IEEE Consumer Communications and Networking Conference, pp.49-53, 2005.

[11] R.S. Sandhu, E.J.Coyne, H.L. Feinstein, C.E. Youman, “Role Based Access Control Models.” IEEE Computer, Vol. 29, No. 2. pp38-47

[12] D. F. Ferraiolo, D. R Kuhn, "Role-Based Access

Control," Poceedings of the 15th National Computer Security Conference, pp.554-563, 1992.

[13] D.F. Ferraiolo, J.F. Barkley, D.R. Kuhn,"A Role Based Access Control Model and Reference Implementation within a Corporate Intranet", ACM Transactions on Information and System Security(TISSEC), Vol. 2, No. 1, pp.34-64, 1999.

[14] H. Mun, N. Um, N. Sun, Y. Li, S. Lee,“ Subject-wise policy based access control mechanism for protection of personal information”. In International conference on convergence information tech (ICCIT2007), pp.2242-2247, 2007.

[15] H.J. Mun, “A Role based personal sensitive information protection with subject policy”, Ph.D. dissertation. Chungbuk University, 2008.

[16] H.J. Mun, J.S. Suh, “Sensitive personal information model for RBAC system”. Journal of computer information, Vol. 13, No. 5, pp.103 - 110, 2008.

[17] Keun-Ho Lee, “A Method of Defense and Security Threats in U-Healthcare Service”, Journal of the Korea Convergence Society, Vol. 3, No. 4, pp. 1-5, 2012.

[18] Kwang-Jae Lee, Keun-Ho Lee, “A Study of Security Threats in Bluetooth v4.1 Beacon based Coupon Convergence Service”, Journal of the Korea Convergence Society, Vol. 6, No. 2, pp. 65-70, 2015.

[19] Bo-Kyung Lee, “A Study on Security of Virtualization in Cloud Computing Environment for Convergence Services”, Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 93-99, 2014.

문 형 진(Mun, Hyung Jin)

- 1996년 2월 : 충남대학교 수학과(이학사)
- 2002년 2월 : 충남대학교 수학과(이학석사)
- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2008년 3월 ~ 현재 : 백석대학교 강사
- 관심분야 : 프라이버시보호, 네트워크보안, 접근제어
- E-Mail : jinmun@gmail.com

한 군 희(Han, Kun Hee)

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
- E-Mail : hankh@bu.ac.kr