헬스케어시스템을 위한 역할 기반의 신뢰협상 모델

조현숙, 이형
chojo@dju.ac.kr, hlee@dju.ac.kr

대전대학교
042-280-2556

키워드 : 보안(security), 신뢰관리, 신뢰 협상, 헬스케어, 역할기반 접근제어

-Abstract-

Security is crucial for the successful deployment of large distributed systems. Many of these systems provide services to people across different administrative domains. The traditional identity-based access control mechanisms are unscalable and difficult to manage. Unlike the closed systems, open systems provide services to people from different security domains.

Healthcare systems need to be highly available in order for the patients to get a timely treatment. The healthcare information should be available to authorized users both inside the administrative domain and outside the domain, such as pharmacies and insurance companies.

In this paper, we first analyzed the necessities and advantages of importing attribute-based trust-management models into open distributed systems. Then we reviewed traditional access-control models and presented the basic elements of the new trust-management model.

목차

신뢰관리 시스템

- Trust management system
  - 인터넷 상에 구현되는 개방형 시스템들이 늘어남에 따라 자원의 공유는 필수
  - 사용자들은 데이터 및 서비스를 제공받기 위하여 서로 다른 도메인에서 접근
  - 서비스와 자원은 불법적인 접근으로부터 안전성을 제공받아야 할 필요
  - 비개방형 시스템들은 일반적으로 서비스 요청자의 신원정보(identity information)에 기반하여 접근 여부를 결정
  - 개방형 시스템에서는 신원정보를 알아내는 것은 불가능한 경우도 있고 불필요한 경우도 있음
  - 분산시스템에서는 속성(attribute) 및 역할(role)에 기반한 새로운 신뢰모델이 요구
  - 속성에 기반하여 신뢰 문제를 해결하기 위한 시스템을 신뢰관리 시스템이라 함

기존의 신뢰관리 접근모델

- **강제적접근제어**(mandatory access control: MAC)
  - 접근제어 정책들이 사용자의 액션이나 결정에 독립적인 모델
  - Bell과 LaPadula가 처음 제안
  - 이 모델에서 접근제어는 객체(object)의 종류 또는 민감도 및 주체(subject)의 종류에 기반
  - 그러나 MAC 모델은 대형시스템인 경우 융통성과 확장성이 부족
- **임의접근제어**(discretionary access control: DAC)
  - 사용자들이 객체의 주인이고 자신들이 소유하고 있는 객체들을 액세스하는 권한을 가지고 있다는 사실에 기초
  - DAC 모델은 대형시스템에서 사용될 수 있는 주체-객체 액세스 메트릭스에 기초
  - 일반적으로 이 모델은 융통성이 결여되어 있고 관리하기가 어려움

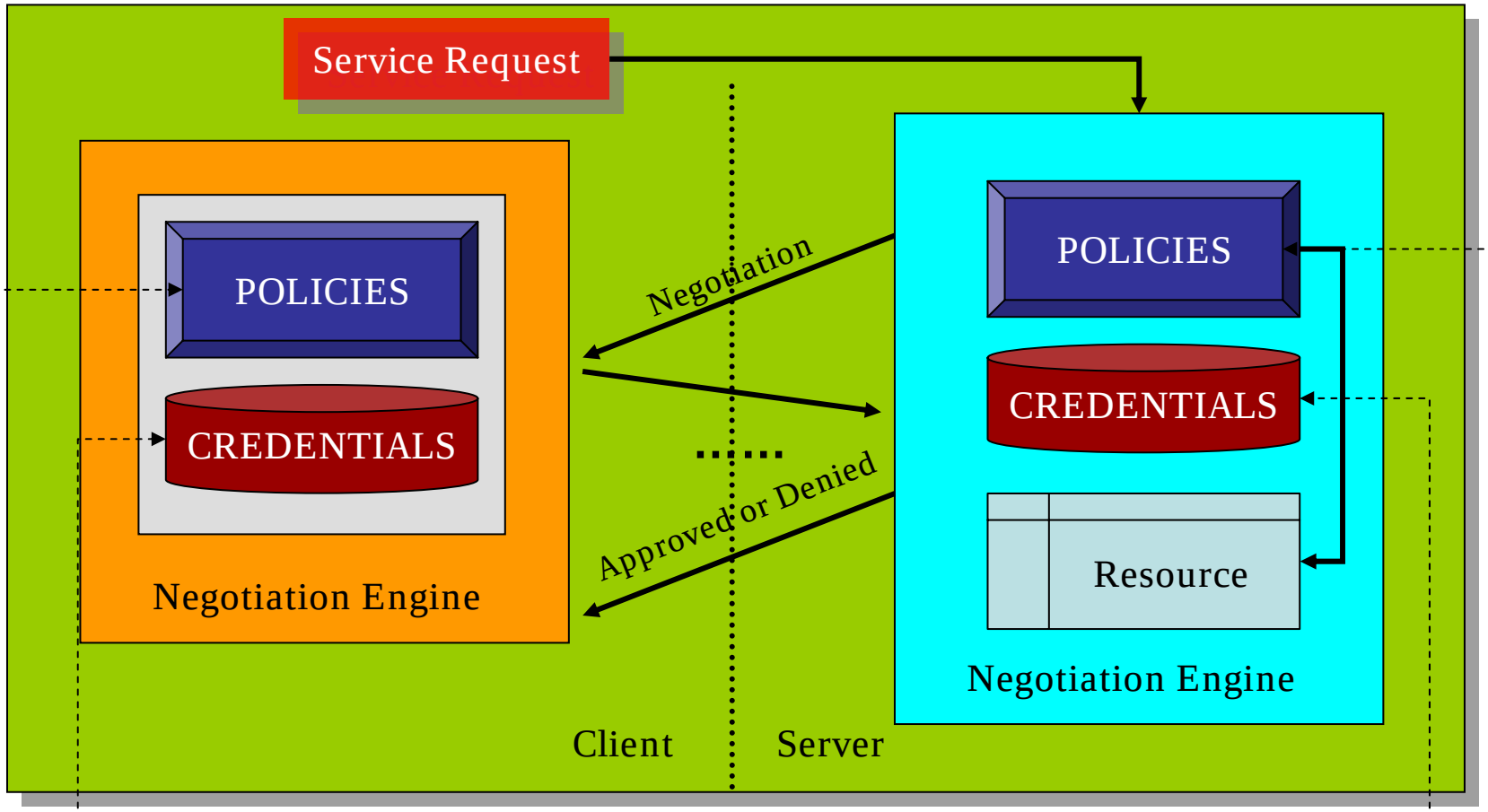
역할 기반 접근모델

- 역할기반 액세스 (role-based access control: RBAC)
  - 역할이라는 새로운 개념을 사용
  - 역할 : 조직에서의 특정 작업 기능을 의미
  - 자원에 대한 액세스 권한은 역할과 관련이 되어 있으며, 역할은 사용자들에게 할당됨
  - 이러한 역할은 속성(attribute)으로 명시되어 인증서에 포함되게 되고 이렇게 하면 속성을 아주 간편하게 관리할 수 있으며, 신뢰 관리에서 분산 인증서 관리가 가능

신뢰 관리의 요소

인증서에 대한 접근 관리 위하여 정의된 것

인증서와 자원에 대한 접근 관리 위하여 정의된 것



신뢰 관리 시스템의 일반적인 구조

엔티티의 속성 정보를 포함, 엔티티의 속성과 역할을 기술하고 있는 CA에 의해 발행

신뢰 협상 (Trust Negotiation)

- 인증서와 로컬 정책을 상대방에게 반복적이고 선택적으로 오픈하여 제공하는 과정
- 이 과정은 모르는 사람들 사이에 속성 정보를 이용하여 신뢰를 구축하기 위한 것
- 신뢰 협상은 요청을 받았을 때 정책의 어느 부분이 부합하는지를 검사하고 다음에 어느 정책과 인증서를 제공해야 하는지를 결정

기존의 대표적인 신뢰 관리시스템

- PolicyMaker
- Keynote
- RT (Role-based Trust management)
- TrustBuilder
- Cassandra

PolicyMaker

- 신뢰 관리시스템을 구현한 최초의 프로토타입
- 보안정책, 인증서 및 관계를 규정하고 기술하는 통합적인 방법을 채택
- 인증서와 정책은 정책 언어의 선택이 정해져 있지 않고 열려있는 상태란 점에서 완전히 프로그래밍 가능
- 인증서는 특정 작업을 수행하기 위하여 키를 직접 권한검증(authorization)과 바인드
  - 키를 단지 이름과 바인드하는 시스템(X.509/PGP)과는 차별성이 있음
  - 위와같은 시스템은 실제 역할과 속성을 잃어버려 결국 시스템의 융통성이 저하됨
- 간편하면서 최소한의 기능을 갖도록 설계되어 있기 때문에 정책 기능, 암호 검증, 인증서 취합 등 대부분의 부하는 호출하는 응용에 위치

Keynote

- policyMaker와 동일한 원칙에 의해 디자인되었으나 인증과 엑세스 컨트롤을 위한 권한 검증을 분류하는 대신 직접적으로 액션에 권한을 부여하는 인증서를 사용
- Keynote 디자인에 있어서 두가지 추가적인 목적은 “표준화”와 “응용들의 용이한 통합”
- 이러한 목적을 위하여 PolicyMaker보다 신뢰 관리 엔진으로서 신뢰성은 향상시키고 호출되는 응용과는 덜 관련되어져 더욱 신뢰할 수 있게 구성
- Keynote는 또한 특정 선언 언어로 인증서와 정책을 표현하였고
- 특정 선언 언어로 고정시킴으로서 효율성, 호환성,인증서와 정책들을 주의깊게 씀으로서 얻는 광범위한 활용성 측면에서 PolicyMaker보다 실용화에 더 다가감

RT(Role-based Trust-mgmt language)

- 분산 환경의 권한 검증에 있어서 정책과 인증서를 나타내기 위한 역할 기반의 신뢰 관리 언어의 집합
- 기본 아이디어 : 권한검증이 공개키 보다는 엔티티의 속성에 기반
  - 기존의 SPKI/SDSI, PolicyMaker, Keynote, Delegation logic 등의 시스템은 권한검증에 있어서 위임(delegation)의 개념을 사용
- RT 시스템 : RBAC 모델과 SDSI 기법과 위임 로직을 결합한 것이며, RBAC 모델에서 역할의 개념을 채택
  - RBAC에서 역할의 개념은 집중화된 기관에서만 사용가능하기 때문에 이러한 제약 조건을 극복하기 위하여 SDSI의 로컬네임스페이스 개념을 차용
  - 이들은 인증서가 집중화된 형태로 저장될 필요가 없으며, 주체나 발행자의 저장소에 따라 분산될 수 있다는 사실을 제시
- RT 시스템은 역할과 신뢰 관리 개념을 장점을 잘 활용, 이러한 장점으로 인하여 RT는 PolicyMaker/Keynote 시스템과 달리 풍족한 표현력을 가짐
- 인증 체인 검색 문제 (credential chain discovery problem)를 해결하였으며 이를 위하여 전방검색 및 후방검색 알고리즘을 제안하였음.

TrustBuilder

- 정책을 기술하기 위해 XML 기반의 정책 언어인 TPL을 사용하고 시스템 내에 다른 인증서를 나타내기 위하여 내부 인증서 포맷을 가지고 있음
- 다른 인증서를 사용하기 위하여 이 시스템은 특정 포맷을 내부 포맷으로 변환하기 위한 변환부호기 (transcoder)를 가짐
- 현재는 X.509 V3 변환 부호기만 제공되며, 이 시스템은 Web 서버들, SOAP RPC, Corba interceptors, SSL/TLS 및 IPSec 등 다양한 환경에 구현
- TrustBuilder는 내용기반 신뢰 협상, 자동 신뢰 협상 등 수많은 기능을 포함
- 특징은 다른 솔루션과 비교하여 상대적으로 실제 시스템에 적용 가능한 완전한 프레임워크

Cassandra

- 신뢰 정책을 표현하기 위한 언어이자 시스템
- Cassandra의 정책은 일부 제한조건을 가지고 있는 Datalog에서 파생한 언어로 표현
- Cassandra는 영국 헬스케어시스템을 위해 개발되었기 때문에 헬스케어 시스템의 보안을 위한 많은 기능을 가지고 있음
- 이 시스템은 파라미터화한 역할과 액션을 기반으로 하고 있으며, 강력한 역할 취소 정책을 포함
- 관리 도메인 사이에 인증서 기반의 액세스 제어를 제공
- Cassandra는 언어의 다른 셋의 표현을 제공하는 제한 도메인 (constraint domain) 개념을 채택
  - 응용들은 자신들의 요구 사항에 맞게 시스템에 접근하기 위해 적절한 제한 도메인을 선택할 수 있고 따라서 Cassandra는 언어를 작으면서도 효율적으로 유지

연구 목적

- 신뢰협상을 위한 인증서 검색 알고리즘을 연구하여 헬스 케어 시스템에 적합한 신뢰 협상 방안을 제시
- 웹서비스 기반의 분산시스템에서 최대 이슈인 보안상의 문제를 해결하면서 서비스 할 수 있는 신뢰관리시스템 모델 제안

연구 범위

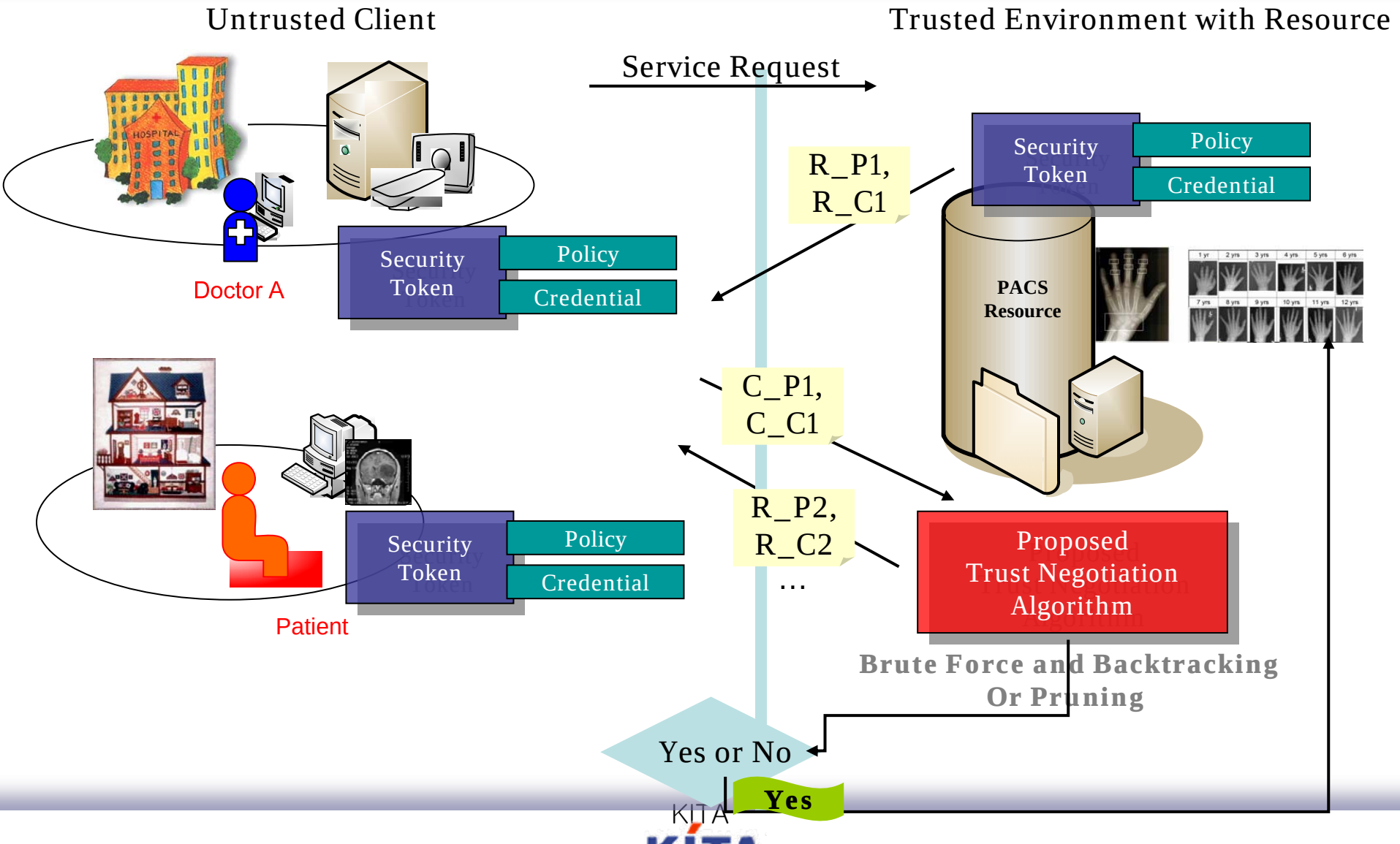
- Scope
  - 기존의 신뢰 관리 기술에 대한 연구
  - 헬스케어 시스템에 적당한 신뢰 협상 알고리즘 제안
  - 제안하는 신뢰협상 모델 평가

- Contents
  - 신뢰 협상 구조 정의
  - 정의한 신뢰협상 구조에 대한 상세 컴포넌트 정의
  - 제안한 모델의 헬스케어 시스템에 적용 예제 제시

연구방법

- 기반 기술 연구
  - 기존의 인증서 검색 알고리즘 분석
  - 헬스케어시스템에 적용가능한 인증서 검색 알고리즘 분석 및 설계
- 웹서비스를 위한 기반 연구
  - 웹서비스에서의 엑세스 제어 모델 설계
  - 특정 헬스케어 시스템(예. PACS)에 적용하기 위한 시나리오 연구
- 신뢰관리시스템 모델 연구
  - 인증서 검색 알고리즘 구현
  - 신뢰협상 모델 적용 시나리오 구현
  - 특정 헬스케어 시스템에 적합한 신뢰관리시스템 테스트베드 구축

모델 구조


Untrusted Client
Trusted Environment with Resource
Service Request
HOSPITAL
Doctor A
Security Token
Policy
Credential
R_P1, R_C1
Security Token
Policy
Credential
PACS Resource
C_P1, C_C1
R_P2, R_C2
...
Patient
Security Token
Policy
Credential
Proposed Trust Negotiation Algorithm
Brute Force and Backtracking Or Pruning
Yes or No
Yes

참고 문헌

[1] Matt Blaze, Joan Feigenbaum, Jack Lacy, Decentralized Trust Management, IEEE conference on Security and Privacy, Oakland, CA, May 1998.

[2] Matt Blaze, Joan Feigenbaum, Jack Lacy et al, RFC 2704, The KeyNote Trust-Management System Version 2, Spet, 1999.

[3] Moritz Y. Becker, Cassandra: flexible trust management and its application to electronic health records, Technical Report UCAM-CL-TR 648, University of Cambridge, Computer Laboratory, 214pp. October 2005.

[4] Ninghui Li, William Winsborough, John Mitchell, Distributed Credential Chain Discovery in Trust Management, Journal of Computer Security, Vol. 11, No. 1, PP 35-86, Feb, 2003.

[5] Ninghui Li, John C. Mitchell, William H. Winsborough, Design of a Role-based Trust-management Framework, Proceedings of the 2002 IEEE Symposium on Security and Privacy.

[6] Marianne Winslett, et.al, Negotiating Trust on the web, IEEE Internet Computing, 2002.

[7] Amir Herzberg, Yosi Mass, Joris Michaeli, Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers.

[8] Adam Hess, Kent E. Seamons, An Access Control Model for Dynamic Client-Side Content, SACMAT'03, 2003, Como, Italy.

[9] Ting Yu, Marianne Winslett, KentE. Seamons, Interoperable Strategies in Automated Trust Negotiation, 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, November 2001.

[10] Elisa Bertino, Elena Ferrari, Anna Squicciarini, Trust Negotiations: Concepts, Systems, and Languages, IEEE Web Engineering, July/Aug 2004.

[11] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-Based Access Control Models, IEEE computer, vol. 29, page 38-47, 1996.

[12] W. Winsborough, K. Seamons, V. Jones, Automated Trust Negotiation, 2000.

[13]Role-Based Access Control Models, Ravi S. Sandhu, Edward, J. Coyne, Hal L. Feinstein and Charles E. Youman, IEEE Computers, Volume 29, Number 2, Feb 1996, pages 38-47.