논문 14-39B-04-05
The Journal of Korea Information and Communications Society '14-04 Vol.39B No.04
http://dx.doi.org/10.7840/kics.2014.39B.4.228

안전한 보안 감시 시스템을 위한 효율적인 접근 제어 기법

양 수 미[◆°], 박 재 성[*]

An Efficient Access Control Mechanism for Secure Surveillance Systems

Soomi Yang[◆°], Jaesung Park[*]

요 약

사회 안전 서비스 제공을 위한 보안 감시 시스템이 보편화되어, 보안 감시 시스템에 대한 접근성이 확대되고, 향상되는 만큼 안정성 확보를 위한 접근제어 기법이 요구된다. ONVIF(Open Network Video Interface Forum)에서 제정하는 표준은 보안 감시용 스마트 카메라의 호환성을 목적으로 만든 표준으로, 클라이언트에게 제공될 웹 서비스의 프레임워크를 정의하고 있다. 본 논문에서는 ONVIF 표준을 따르는 보안 감시 카메라 네트워크에서 안전한 시스템 접근을 위하여 웹 서비스의 정보 보호 기법을 수용하고, 웹서비스의 안전한 제공을 위한 효율적인 접근 제어 모델을 제안 한다.

Key Words : Access Control, Surveillance System, Attribute Certificates, Communication Sciences, Network

ABSTRACT

In recent general social surveillance systems, secure access control mechanism is needed. ONVIF establishes standards for interoperability between cameras and defines web service framework for it. In this paper we present an efficient attribute based access control mechanism for surveillance system networks which follow the ONVIF standards. It accommodates web service information security techniques and provides efficient secure access control.

Ⅰ. 서 론

사회 안전 서비스 제공을 위한 보안 감시 시스템이 보편화되어, 공공 카메라이외에, 사설 카메라도 많이 설치되어 운영되고 있다. 카메라로부터 수집되는 영상 정보는 다양한 계층의 관련자 - 경찰서, 행정관서, 관리기관의 담당인력-을 포함하여, 교통 정보 등의 공공 자료를 원하는 일반인에게까지 제공되고 있다. 이에 따라 보안 감시 시스템에 대한 접근성이 확대되고, 향상되는 만큼 안전성 확보를 위한 접근 제어 기법이 요구된다.

최근에 설치되는 카메라는 전용선을 쓰는 CCTV (Closed Circuit Television)이 아닌 인터넷 기반의 IP 카메라이며, 독립적으로 처리기와 저장소를 가지고, 촬영된 영상으로부터 정보를 추출하고, 이벤트를 발생시키며, 원격 관리시스템을 조정할 수 있는 스마트 카

※ 본 연구는 경기도 지역협력연구센터 (GRRC SUWON 2013-B1) 지원에 의하여 수행되었습니다.
◆° First Author and Corresponding Author : The University of Suwon, Department of Information Security, smyang@suwon.ac.kr, 정회원
* The University of Suwon, Department of Information Security, jaesungpark@suwon.ac.kr, 종신회원
논문번호 : KICS2014-04-115, Received December 10, 2013; Revised January 14, 2014; Accepted March 25, 2014

메라 형태이다.

ONVIF(Open Network Video Interface Forum)[1]에서 제정되는 표준은 보안감시용 스마트 카메라의 호환성을 목적으로 만든 표준으로, 클라이언트에게 웹 서비스를 제공하도록 웹 서비스 프레임워크를 정의하고 있다[2]. OASIS(Organization for the Advancement of Structured Information Standards)[3]의 웹 서비스 표준을 따르고 있으며, 호환성을 위한 WS-I(Web Services Interoperability)의 basic profile 2.0을 준수한다[4].

본 논문에서는 안전한 보안감시 시스템을 위하여, ONVIF를 따르는 보안감시 카메라 웹 서비스의 안전한 제공을 위한 효율적인 접근제어 모델을 제안한다.

논문은 다음의 순서로 구성되어있다. 2장에서 접근제어와 관련된 기존 연구를 살펴본다. 3장에서 효율적인 접근제어 모델을 제시한다. 4장에서 성능분석을 한다. 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

대규모 네트워크 시스템을 위한 접근제어 시스템으로 역할기반 접근제어(RBAC, Role Based Access Control)[5,6]가 있다. 이는 공개키 기반구조(PKI, Public Key Infrastructure)와 더불어 동작하는 권한관리 기반구조 (PMI, Privilege Management Infrastructure)를 구축하여 보다 접근제어 정책 관리가 수월한, 융통성 있는 접근제어 기능을 제공한다[7].

속성기반 접근제어(ABAC, Attribute Based Access Control)[8] 는 규칙 기반 접근 제어로 OASIS의 SAML(Security Assertion Markup Language)[9,10]과 XACML(eXtensible Access Control Markup Language)[11,12]을 이용한다.

SAML은 인증 및 인가와 관련된 정보를 XML 형식으로 주고 받을 수 있는 프레임워크를 정의한다. XML로 표현된 보안 정보를 “assertions”라고 부르며 서명되고 암호화되어 무결성을 유지한다. assertions의 교환을 위한 프로파일, 프로토콜 등이 정의되어 있다.

XACML은 복잡한 정책과 규칙을 다룰 수 있는 기능을 제공함으로써 SAML을 보완한다. 일반적인 인가(authorization) 구조와 접근제어 정책을 표현하고 교환 및 공유할 수 있는 정책언어를 정의한다. 접근제어의 인가 결정을 위한 요청 및 응답 구문을 제공한다.

SAML과 XACML은 접근 제어를 위한 보안 정보의 교환에 필요한 데이터 형식을 정의하는데 중점을 두고 있다. 본 논문에서는 동적 변화를 수용하는 유연한 권한 속성 구조의 구축에 중점을 둔다. 웹 서비스의 접근제어에 있어서 인증보다는 인가에 초점을 맞추며, 속성 기반 접근제어 모델을 개선하여 규모 확장성을 제공하면서, 호환성을 유지하는 유연한 기법을 제공한다. 이는 다양한 센서를 이용하는 보안 감시 시스템[13,14]에서도 적용가능하다.

Ⅲ. 확장된 속성 기반 접근 제어 모델

대규모 보안감시 시스템의 보안정책은 매우 복잡하게 구성되며, 여러 부서에 의해 관리된다. 이는 관련 부서가 경찰서, 행정관서, 사법부 등의 공공기관이외에 아파트 관리사무소, 동네 자율방범대를 비롯하여 일반인에 이르기까지 다양하기 때문이다. 이들의 보안정책은 각기 독립적으로 관리되고 있으며, 보안 정책의 수정에 많은 비용이 소요되고, 일관성 유지도 어렵다. 이러한 문제에 대한 해결방법으로 보안 정책을 표현하는 공통적인 언어를 확립하고, 각기 독립된 보안정책이 공통언어로 표현되고, 공통의 프로토콜로 통신할 수 있다면, 모든 보안정책의 집행을 총체적으로 관리할 수 있다. 즉, 기관 별로 자율적인 정책결정을 보장하면서, 서로 호환성과 일관성을 유지하는 게 가능하다.

추론을 위한 환경 정보 및 비디오 또는 바이오매트릭 정보는 XML로 된 웹서비스의 형태로 클라이언트에게 제공된다. 웹 서비스 기술의 발전은 정보 시스템들이 플랫폼 독립적으로 정보를 공유하고, 협업할 수 있도록 하고 있다. 이는 논리적으로는 정책이 다른 조직의 네트워크에 접근하는 것이 가능하게 하는 것이고, 심각한 보안 문제를 야기한다. 즉, 한쪽에서는 정보를 제공해서 협업을 증진해야 하지만, 다른 쪽에서는 민감한 고급 데이터가 접근 되지 않도록 해야 하는 것이다. 동적으로 변화하는 환경에서 위의 두 가지 목적을 다 달성하기 위해서는 접근제어 관리가 쉬우면서도 정교하고 융통성있는 체계로 만들어져야하는데, 기존의 접근제어 모델은 정적이고, 세분화되지 않아, 다양한 사용자 계층의 동적인 변화를 수용하지 못한다.

속성 기반 접근 제어는 기존의 역할 기반 접근 제어를 일반화한 것으로, 역할의 정의가 확대되고, 웹 서비스에 적용하기 쉽다. 보안 정책들은 XML로 표현되고, 이는 X.509 속성 인증서 (Attribute Certificate)에 포함가능하고, 로컬 저장소나 LDAP 디렉토리 등에 저장된다. 시스템 관리자에 의해 운영되는 속성 인증서 관리 모듈은 사용자에게 X.509 속성인증서를 할당한다. 이는 사용자와 발행자를 조작할 수 없게 서명

하여 속성인증서와 연결한다. 속성 인증서 관리 모듈은 속성인증서의 생성, 수정, 취소 등을 수행한다.

SAML은 신원 정보와 보안 정보가 보안 도메인을 넘어서 공유될 수 있도록하는 XML 기반 프레임워크이다. SAML 도메인 모델은 그림 1과 같다. 속성 assertion은 서명되고 암호화되어있는 보안 토큰이다. 보안 토큰으로 SAML assertion 이외에 PMI 속성인증서의 사용이 가능하며, 권한 정의 속성인증서의 구조화로 확장된, 효율적인 접근 제어가 가능하다.

그림 1에서 속성 인증기관 (Attribute Authority)은 주체와 관련된 모든 속성을 관리한다. 보안 감시 카메라는 모든 접근 요청에 대해 주체의 속성을 관리하는 속성 인증기관을 접근해서 정책 시스템에서 요구하는 속성 값을 요청 및 확인해야 한다.

그림 1에서 속성 인증기관이 가지는 정책 데이터베이스(Policy)에 속성과 관련된 권한 정보가 구조화 되어 저장되어야 하며, 이것이 여러 기관 간에 일관성 있게 구조가 유지되어야 한다. 본 논문에서는 행정기관 간의 상하 관계 및 포함관계를 유지하는 트리구조 형태를 가진다.

PDP(Policy Decision Point)는 인가 인증기관(Authorization Authority)으로서 XACML 요청을 받아 정책에 따라 해당하는 응답을 보낸다. XACML에서 SAML 적용 dataflow는 그림 2와 같다.

인증 단계에서 목적지 사이트는 주체의 속성이 가진 권한을 확인해야 한다. 속성이 가진 권한을 특정 위치에 유지하는 것은 정책을 공유하는데 장애가 된다. 속성의 권한은 서로 관련이 되어 있고, 포함관계가 되기도 한다. 즉, 상위 역할이 하위 역할의 권한을 상속받을 수 있다. 이러한 권한 관계를 전체 보안 감시 시스템 내에서 트리형태로

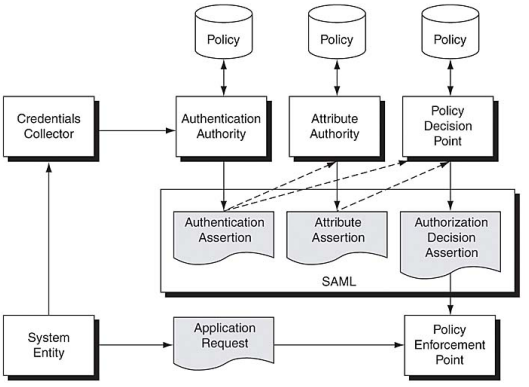

그림 1. SAML 도메인 모델
Fig. 1. SAML domain model

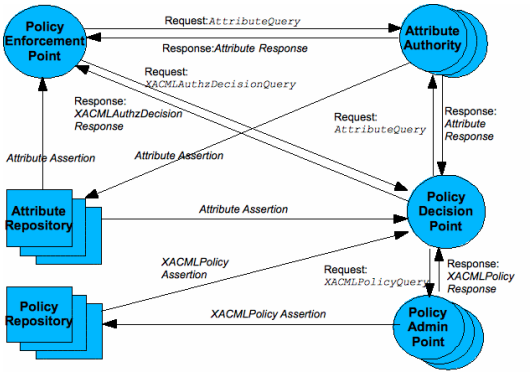

그림 2. XACML에서의 SAML 데이터 플로우
Fig. 2. SAML data flow in XACML

구조화하고, 적절히 분산 배치하는 것은 접근 제어 시스템의 확장성과 유연성 및 접근성을 높이게 된다.

Ⅳ. 성능 분석

권한 속성 데이터 복제의 주된 목적은 작업 실행에 소요되는 데이터 접근 시간을 줄여 결과적으로 작업의 응답시간을 감소시키고자 하는 것이다. 복제 기법의 비용은 수집된 자료를 바탕으로 다음의 수학적 추론에 따라 계산한다.

노드 v 가 노드 w 에 존재하는 데이터 d 를 읽기 비율, $\lambda_r(v,w)$와 쓰기 비율, $\lambda_w(v,w)$로 접근하고자 한다고 하자. 만약 데이터 d 의 복제가 전체 속성 인증 기관 시스템 안에 없다면 시스템의 각 노드 v 는 노드 w 에 존재하는 데이터 d 를 직접 접근해야 하며 데이터 전송 비용 C(v,w) 는 식 (1)과 같이 된다.

$$C(v,w) = (\lambda_r(v,w) + K \cdot \lambda_w(v,w)) \cdot p(d)/b(v,w) \quad (1)$$

K는 읽기 비용에 대한 쓰기 비용의 비율이고, 기준 비용은 패킷 크기 p(d) 가 된다. b(v,w) 은 노드 v 와 w 간의 대역폭이다. 전송비용 C 는 응답시간을 나타낸다.

Ri를 속성 데이터 d 의 복제 집합이라고 하면, 노드 v 가 데이터 d 를 사용하는데 소요되는 총 비용은 가장 가까운 노드로부터 읽어 들이고 가장 먼 노드까지 데이터 갱신이 이루어지는 점을 고려하면 접근 및 갱신에 드는 관리비용 C(v,N)은 식 (2)와 같이 된다.

$$C(v,N) = C(v,w) + \sum_i C_i(v,R_i)$$
$$= (\lambda_r(v,d(v,w,R_i))/b(v,c(v,w,R_i)) + K\lambda_w(v,f(v,w,R_i))/b(v,f(v,w,R_i))) \cdot p(d) \quad (2)$$

N은 전체 노드이고, Ci 는 각 속성 데이터 복제 Ri 에 대해서 소요되는 추가 비용이다. C(v,Ri) 은 노드 v와 w 간의 가장 가까운 노드를 가리키고, f(v,Ri) 은 노드 v 와 r 간의 가장 먼 노드를 가리킨다. 쓰기 비용의 경우, 일관성 유지를 위한 전체 복제에 대한 갱신 패킷은 브로드캐스팅 패킷을 쓰는 것으로 가정한다. 브로드캐스팅 패킷을 쓰는 것이 규모 확장성을 고려했을 경우에 좋은 방안이 된다. 속성 데이터 복제를 둠으로써 읽기 및 쓰기를 위한 데이터 전송 시간이 감소하고 그에 따라 응답시간이 감소한다. 반면에 쓰기 비용은 복제 데이터에 대한 일관성 유지를 위한 메시지 전송으로 인해 관리 비용이 증가된다. 그러므로 읽기와 쓰기 비율에 따라 복제의 규모를 정해야 한다. 일관성 유지 등을 비롯한 관리 비용, C(v, N)이 최소가 되도록 하는 것이 필요하다.

컴퓨팅 노드의 존재는 시간에 따라 변화할 수 있는데, 권한 속성 인증기관(Authorization Authority)이 사용자 의도에 따라 생성되기도 하고 사라지기도 하지만, 사용자의 의도와 상관없이 장애가 발생하기도 하기 때문이다. 이는 노드의 존폐가 자유롭게 변화 가능함을 의미한다. 그러므로 속성 데이터 복제는 기존의 복제 기법에 더하여 신뢰할 수 없는 네트워크 환경에 대한 보정이 추가되어야 한다. 게다가 노드의 동작 여부에 대한 정보는 전파되는데 시간이 걸리므로 전체 노드가 이루는 네트워크 환경에 대한 정확한 시각을 실시간으로 가지기는 어렵다. 네트워크 환경에 대한 모델을 세우고, 변화에 대한 예측 및 적응이 시도되어야 한다.

각 노드가 아무런 규제 없이 자유롭게 생성되고 제거되는 환경에서 각 노드는 무작위로 단조(uniform) 분포한다. 무작위적인 단조분포는 이항 분포(Binomial Distribution)로 표현된다. 노드의 생성은 비율 λ의 포아송 프로세스(Poisson Process)를 따르는 것으로 가정한다. 포아송 분포는 이항 분포 B(k; p, n)에 $p = \lambda t/n, q = 1 - \lambda t/n$를 대입한 후 n을 무한대로 취하여 얻는다. 노드의 삭제는 비율 μ을 가지는 지수분포(Exponential Distribution)를 따르는 것으로 가정한다. 지수분포는 포아송 분포로부터 유추된다. 매개변수 μ의 지수분포에서 장애율(노드 삭제비율)이 μ이고, 평균 수명이 $1/\mu$이다. 시스템 내의 노드 수를 대략 일정하게 유지하기 위해 노드의 생성과 삭제가 같은 비율로 일어나는, λ = μ인 포아송 프로세스임을 가정한다. 권한 속성 구조에서 메시지가 전송될 때, 메시지가 장애 노드로 전달될 확률은 지수분포의 성질에 따라 식 (3) 과 같다.

$$P = 1 - (1 - e^{-T\mu}) \cdot \frac{1}{\mu} \cdot \frac{1}{T} \quad (3)$$

T는 장애를 감지하는데 드는 최대시간이다. 그러므로 메시지 손실률, L,은 각 에지에서 장애노드가 아닌 노드로 전달된 경우를 빼면 식 (5)와 같다.

$$L = 1 - (1 - P)^h = 1 - \left(\frac{1 - e^{-\mu T}}{\mu T}\right)^h \quad (4)$$

h는 필요한 데이터를 접근하는데 소요되는 홉 수이다. 이로부터 노드 가용성이 1/(1-L) 임을 고려하여 식 (2)에 주어진 비용을 구할 수 있다. 필요한 전체 관리 비용, E, 는 식 (6)과 같다.

$$E = \frac{C(v,N)}{1-L} + N \cdot \frac{M}{T_M} \cdot \frac{p(M)}{b(r,N)} = \frac{C(v,N) \cdot (\mu T)^h}{(1 - e^{-\mu T})^h} + \frac{N \cdot M \cdot p(M)}{T_M \cdot b(r,N)} \quad (5)$$

첫 번째 항목은 기존의 데이터 복제 알고리즘에 노드 장애에 대한 고려를 추가한 비용이다. 두 번째 항목은 테이블 유지 비용이다. 각 노드의 상태 파악을 위하여 M 개의 관리 메시지가 매 T_M 초 마다 전송된다.

인가 시스템 구축에 있어서, 각 보안 감시 카메라가 속한 조직과 개별 카메라의 환경에 따라 달라질 수 있으므로, 단일의 정책을 세우더라도, 융통성의 여지를 두어야 한다. 어떤 형태의 메시지와 전송 수준의 보안을 수립할 것이냐는 서비스 수준에 종속되어야하고, 개별 서비스마다 달라질 수 있다.

속성인증서의 권한 속성 구조화에 따른 성능 향상은 그림 3과 같다. grouped는 구조화가 된 경우이고, ungrouped는 그렇지 않은 경우이다. 구조화된경우에 관리 비용 E가 작아짐을 볼 수 있다. TLS와 SAML의 적용 수준이 정책적용에 있어서 가변적이어야 하며, 사용자에 따라 달리 제공되어야한다.

권한 속성의 구조화에 있어서 복제 없이, 중복성을 제거하여 그림 1의 Policy 데이터베이스에 대한 정규화를 도입할 경우 성능 변화는 표 1과 같다. 정규화된

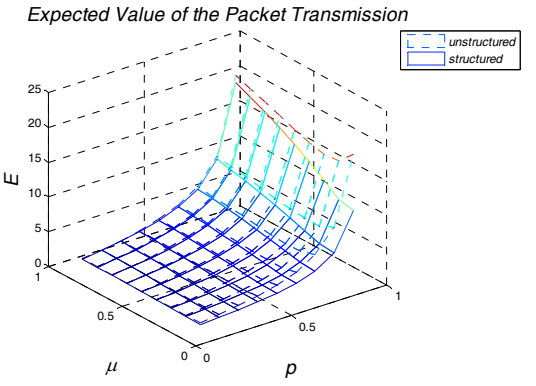

그림 3. 관리 비용 비교
Fig. 3. Comparison of management cost

경우, 복제가 없어 성능의 향상을 보이지만, 노드의 안정성이 확보되어야한다. 또한 전체 권한 속성의 개수가 A이고, 확장되는 하위 권한의 수가 최소 m, 최대 M일 경우, h는 식 (7)과 같이 계산되는데, 정규화로 인해 속성 권한 탐색 체인이 지나치게 길어져 속도 저하를 가져올 수 있다.

$$\log_M A < h_A < \log_m A \qquad (6)$$

표 1. 정규화 비교
Table 1. Comparison of normalization strategy

	un-normalized		normalized	
	ungrouped	grouped	ungrouped	grouped
p=0.1	2.54	1.39	1.66	1.21
p=0.9	45.53	20.27	26.30	14.74

V. 결 론

본 연구는 다양한 카메라 소스로 부터 얻어지는 영상 정보 및 이벤트 정보를 기반 데이터로 하여 과거와 현재 상황을 인지하고 대처하며, 또한 예측되는 사건에 대비할 수 있는 보안 감시 시스템 구조에 있어서, 접근 제어 정보의 저장 및 전달의 안전성을 높이기 위한 방안을 제안한다.

다양성과 확장성을 가지는 보다 향상된 사회 안전 공공서비스를 제공하는 보안 감시 시스템을 위하여 규칙 기반의 접근제어를 도입하고 웹 서비스의 정보 보호 기법의 적용 방안을 고찰하였다. 보안 감시 카메라의 정보 접근을 위한 속성 권한을 구조화하고, 분산된 형태와 병행하여 통합된 형태로 관리하고 분석하는 데 요구되는 정보 보호 기법 적용 방안을 살펴보았다. 이는 서비스 제공 과정을 지역 처리와 분산 처리로 병행하는 웹서비스 기반의 보안 감시 시스템 프레임워크에서 필수적이며 효과적인 접근 제어 기반 구조를 제공한다.

References

[1] ONVIF(Open Network Video Interface Forum) http://www.onvif.org

[2] T. Senst, M. Patzold, R. H. Evangelio, V. Eiselein, I. Keller, and T. Sikora, "On building decentralized wide-area surveillance networks based on ONVIF," *IEEE Int. Conf. AVSS*, pp. 420-423, Klagenfurt, Aug.-Sept. 2011.

[3] OASIS (Organization for the Advancement of Structured Information Standards), http://www.oasis-open.org

[4] Web Services Interoperability Organization, Basic Profile Version 2.0, http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html, Nov. 2010.

[5] B. Shafiq, B.D.J. Joshi, E. Bertino, and A. Ghafoor, "Secure interoperation in a multidomain environment employing RBAC policies," *IEEE Trans. Knowledge and Data Eng.*, vol. 17, no. 11, Nov. 2005.

[6] Y. Lee, D. Park, Y. Hwang, and S. You, "The role-based access control model considering context and privacy," *J. KICS*, vol. 34, no. 6, pp. 179-186, 2009.

[7] ISO 9594-8:2008 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2008.

[8] NIST, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," 2013.

[9] SAML 2.0 Profile of XACML, Version 2.0, http://docs.oasis-open.org/xacml/3.0/xacml-profile-saml2.0-v2-spec-cd-1-en.html, Apr. 2009.

[10] G. Kim, D. Won, and U. Kim, "An Extended SAML Delegation Model Based on Multi-Agent for Secure Web Services," *J. KIISC*, pp. 111-122, Aug. 2008.

[11] OASIS XACML Version 3.0, http://docs.oasis-

open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf, Jan. 2013.

[12] J. Kim and S. U. Lee, “Conflict Detection Algorithm for XACML Policies,” in *Proc. KISS*, pp. 550-552, Jun. 2013.

[13] D. Choi, D. Kim and S. Yang, “Design and Implementation of Intelligent Surveillance Systems for Secure and Efficient Public Service Provision,” in Proc. KICS, pp. 20-21, 2014

[14] S. Oh, S. Moon and S. Choi, ″Intelligence Security and Surveillance System in Sensor Network Environment Using Integrated Heterogeneous Sensors,″ in Proc. KICS, pp. 551-562, 2014

양 수 미 (Soomi Yang)

1985년 2월 : 서울대학교 컴퓨터공학과 졸업
1987년 2월 : 서울대학교 컴퓨터공학과 석사
1997년 2월 : 서울대학교 컴퓨터공학과 박사
1988년 3월~2000년 9월 : 한국통신 연구소 연구원
2004년 9월~현재 : 수원대학교 정보보호학과 교수
<관심분야> 정보보호, 시스템 보안, 네트워크 보안

박 재 성 (Jaesung Park)

1995년 2월 : 연세대학교 전자공학과 졸업
1997년 2월 : 연세대학교 전자공학과 석사
2001년 2월 : 연세대학교 전기, 전자공학과 박사
2001년~2002년: Univ. of Minnesota (PostDoc.)
2002년~2005년 LG전자 (선임연구원)
2005년~현재 : 수원대학교 정보보호학과 부교수
<관심분야> 네트워크 성능 분석 및 프로토콜 개발