프라이버시 보호 기능이 추가된 인증서 프로화일에 관한 연구

정회원 양 형 규*

Enhanced Certificate with User's Privacy Protection Methods

Hyung kyu Yang* *Regular Members*

요 약

CA가 공개키를 포함하는 X.509 인증서를 사용자에게 발급할 때, 사용자는 하나 이상의 subject name을 "subject" 필드와 "subjectAltName" 확장 필드에 명시해야 한다. "subject" 필드 또는 "subjectAltName" 확장 필드는 DN, 전자메일 주소, IP 어드레스 등의 계층적인 구조를 포함할 수 있다.

본 논문에서 우리는 인증서 소유자의 프라이버시 보호를 위한 요구 조건들을 제시하였고, 그리고 공개키 인증서 내의 "subject" 필드와 "subjectAltName" 확장 필드에 포함돼 있는 사용자의 프라이버시를 보호하는 즉, 제시한 요구조건들을 만족하는 방법을 제안하였다.

Key Words : PKI, Public-key certificate, Privacy, zero-knowledge

ABSTRACT

When a Certification Authority (CA) issues X.509 public-key certificate to bind a public key to a user, the user is specified through one or more subject name in the "subject" field and the "subjectAltName" extension field of a certificate. The "subject" field or the "subjectAltName" extension field may contain a hierarchically structured distinguished name, an electronic mail address, IP address, or other name forms that correspond to the subject. In this paper, we present the requirements for certificate holder's privacy protection and propose the methods to protect the user's privacy information contained in the "subject" field or the "subjectAltName" extension field of a public-key certificat

Ⅰ. 서 론

"digital IDs"라고도 불리우는 공개키 인증서는 X.509 파일 양식을 사용하며, 또한 인증서 양식, 유일한 일련 번호, 인증서를 서명하기위해서 사용되는 알고리즘, 인증서를 발급하는 CA(Certification Authority)의 이름, 인증서 유효 기간, 인증서 소유자 정보, 인증서 소유자의 공개키, 그리고 발급 기관인 CA의 서명으로 구성된다.

위의 구성 요소들 중에 인증서 소유자 정보는 인증서 소유자의 이름과 국적, email 주소, 소유자의 조직, 그리고 소유자가 일하는 조직 내의 부서와 같은 다른 신상 정보를 포함한다. 또한, 이것은 소유자의 그림, 소유자 지문의 법전화, 그리고 소유자의 패스포트 번호 등을 포함한다.

여기에서 우리는 현재 사용하고 있는 공개키 인증서는 신뢰된 기관 이외의 제 삼자에게 노출돼서는 안돼는 인증서 소유자의 프라이버시와 관련된

* 강남대학교 컴퓨터미디어공학부 (hkyang@kangnam.ac.kr)
논문번호 : KICS2005-01-027, 접수일자 : 2000년 10월 24일
※본 논문은 2004년도 강남대학교 교내 연구비 지원에 의한 것임

너무나 많은 민감한 정보를 포함한다는 사실에 주목해야 한다. 이것은 개인 정보 보호(개인 정보 보호란 개인과 밀접한 관련이 있는 정보가 습득되고, 노출되고, 불법적으로 사용되는 경우를 제어하기 위한 개인의 권리로써 정의할 수 있다)라는 관점에서 바람직하지 않다[1].

본 논문에서 우리는 이러한 문제점을 해결하기 위해서 프라이버시 보호 기능을 제공하는 인증서(PEC: Privacy Enhanced Certificate)를 제안한다. 제안한 방식은 인증서 소유자와 관련된 민감한 정보는 쉽게 검증할 수 없게 했으며 인증서 소유자의 동의를 얻어야만 검증이 가능하도록 하였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 프라이버시 요구 조건들을 제시하였다. 그리고 3장에서는 공개키 인증서와 관련된 표준 문서를 분석하고, 4장에서는 프라이버시 보호 기능이 추가된 인증서 양식과 프로토콜을 제안하였고, 5장에서는 제안한 프로토콜을 본 논문에서 제시한 요구조건을 만족하는지 분석하였으며, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 프라이버시 요구조건

최소권한(Need-to-know) 원칙은 가장 기본적인 보안 원칙들 중의 하나이다[2-4]. 이 원칙은 정보란 그 정보에 대한 합법적인 요구를 가진 사람에게만 제공돼야 한다는 것을 의미한다. 이것은 최소 원칙 개념과 비슷하며 또한 지켜져야 한다. 최소권한 원칙의 실행은 신뢰성 있는 내부자의 배반으로 인한 악의적인 공격에 대한 손상 범위를 줄일 수 있다.

최소권한 원칙을 기반으로 인증서 검증자는 오직 자신의 업무 수행 시 요구되는 정보만을 알 수 있도록 한다. 따라서 본 논문에서는 다음과 같은 요구조건 R1과 R2가 인증서의 프라이버시 기능을 제공하도록 하였으며, 더욱이 인증서 소유자가 자신과 관련된 프라이버시 정보의 오용을 제어하기 위해서 요구조건 R3도 고려하였다. 다음은 본 논문에서 제시한 요구조건들이다.

- R1. 노출불가능성(Invisibility) : 인증서 소유자의 프라이버시 정보는 인증서 소유자의 동의 없이 다름 사람에게 노출될 수 없다.
- R2. 변경불가능성(Soundness) : 인증서 소유자는 불법적으로 인증서내에 포함된 자신의 프라이버시 정보를 변경 시킬 수 없다.
- R3. 비전이성(Non-transferability) : 필요하다면, 인증서 소유자는 자신의 프라이버시 정보를 인증서로부터 복원할 수 있으며, 그것을 확인 연산(confirming operation)을 통해서 검증자에게 보여 줄 수 있다. 그리고 악의적인 의도를 가진 검증자는 인증서 소유자가 제 삼자에게 자신이 소유한 정보가 맞는지 틀리는지를 확인 시키는 과정인 확인 연산으로부터 어떠한 정보도 얻을 수 없다.

Ⅲ. 관련 연구 및 분석

본 장에서 de facto 표준으로 사용하고 있는 4개의 관련된 표준안을 설명하고 분석하고자 한다.

3.1 X.509 public-key certificate

X.509 프로토콜은 공개키 인증서에 대한 다음과 같이 구조를 정의한다[5].

- X.509Cert = <Version, SerialNumber, Algorithm, Issuer, Validity, Subject, SubjectPublic KeyInfo, Extensions, Signature>. 단,

(1) Version: 인증서 양식을 구별하기 위해서 version 필드를 사용한다.
(2) SerialNumber: CA 내에서 유일한 넘버이다.
(3) Algorithm: 인증서를 서명할 때 사용되는 알고리즘의 종류를 정의한다.
(4) Issuer: CA의 이름을 정의한다.
(5) Validity: 인증서 만료일을 정의한다.
(6) Subject: 발급된 인증서를 소유한 사용자에 대한 정보를 정의하고, 인증서 소유자의 국적, e-mail, 조직, 여권넘버 등과 같은 정보를 포함한다.
(7) SubjectPublicKeyInfo: 사용할 알고리즘 이름과 공개키를 포함한다.
(8) Extensions: 부가적인 subject identification 정보, key attribute 정보, 정책 정보 그리고 인증경로제약과 같은 자료를 전한다.
(9) Signature: 인증서에 대한 CA의 서명

위에서 서술한 것처럼, X.509 공개키 인증서 내에는 "subject field" 혹은 "subjectAltName" 확장 필드에 포함된 인증서 소유자의 프라이버시를 보호해줄 메카니즘이 없다. 그래서 X.509 공개키 인증서는 요구조건 R1과 R3를 위반한다.

3.2 Hongkong post office e-Cert format

Hongkong post office e-Cert personal certificate 양식은 X.509 공개키 인증서를 기본으로 한다[6]. 그

런데 Hongkong post office e-Cert personal certificate 양식에서는 인증서 소유자의 HKID(Hongkong Identity Card No.) number는 HKID number의 해쉬 값의 형태로 인증서에 저장된다. 단, HKID number는 인증서 소유자의 개인키로 다음과 같이 서명 된다: cert_hkid_hash=H(RSAprivatekey,H(hkid_number)) 단, H(•)는 안전한 해쉬 함수를 의미하고 RSA(•)는 서명함수이다. 해쉬 값 cert_hkid_hash는 인증서의 "subjectAltName" 확장 필드에서 사용된다.

Hongkong post office e-Cert persnal certificate 양식은 요구조건 R1과 R2를 만족시킨다. 그러나 논문 [6]에서는 인증서 소유자가 HKID를 cert_hkid_hash 값으로부터 복원해서 이 값을 제 삼자에게 증명할 수 있는 어떠한 방안도 제시하지 못했다. 이것은 인증서에 저장된 HKID number를 소용없게 만드는 일이다.

3.3 KISA's Subject Identification Method

2002년에 KISA에서는 IETF 표준안으로서 Subject Identification Method(SIM)을 제안하였다[7]. SIM은 사회보장넘버, 운전면허번호와 같은 저장 가능한 민감한 개인 정보를 이중으로 해쉬한 값의 형태로 인증서의 "subjectAltName" 확장 필드에 안전하게 저장하는 방안이다. SIM은 다음과 같은 방법으로 계산한다. SIM = <r, H(H(pwd,r,sensitive_id_info))>. 단, H(•)는 안전한 해쉬함수이고, pwd는 인증서 소유자가 선택한 패스워드이고, 그리고 r은 Registration Authority(RA)에 의해서 생성된 랜덤 salt이다.

제 삼자에게 인증서에 보관된 인증서 소유자의 중요한 개인 정보를 보여주기 위해서 위 방식은 다음과 같은 확인 절차 과정을 사용한다.

1) 인증서 소유자 A는 B에게 안전한 방법으로 pwd, sensitive_id_info, 그리고 자신의 인증서를 송신한다.
2) 검증자 B는 A의 인증서의 "subjectAltName" 확장필드로부터 r을 추출한다.
3) B는 pwd, r, 그리고 sensitive_id_info을 이중으로 해쉬한 값을 계산하고 계산한 값을 이중 해쉬한 값과 A의 인증서에 보관된 H(H(pwd, r, sensitive_id_info))와 비교한다.

만약 A가 중요한 개인 정보, sensitive_id_info에 대한 소유를 어떠한 정보의 노출 없이(예를 들면, 저장된 운전자면허번호의 경우에 A는 자신이 운전면허번호 노출 없이 운전면허번호를 소유하고 있다는 사실만을 증명 할 수 있다) 증명하기를 원한다면, A는 B에게 단계 1)에서 pwd와 sensitive_id_info 대신에 해쉬 값 H(pwd, r, sensitive_id_info)를 보내면 된다.

KISA의 SIM은 요구조건 R1과 R2를 만족시킨다. 그러나 검증자 B가 A의 sensitive_id_info과 pwd를 얻는다면, B는 제 삼자에게 주어진 sensitive_id_info와 pwd가 A의 중요한 신분 정보이고 이것은 타당하다는 것을 증명 할 수 있다. 따라서 KISA의 SIM은 요건조건 R3를 위반한다.

3.4 VeriSign's CZAG extension

1997년에 사용자가 opt-out을 실행하지 않을 때[8], VeriSign은 Class 1 인증서내에 사용자의 국적, zip code, 생년월일과 CZAG라 불리는 성별 정보를 포함하는 조건부 One-Step Registration을 발표했다. CZAG 정보는 인증서내에서 암호화된 형태로서 저장되고, 참여한 웹 싸이트에 의해서 license fee를 지불하고 VeriSign으로부터 이용할 수 있는 소프트웨어를 이용해서 읽혀 질 수 있다.

그러나 논문 [9]에서 Renfro는 VeriSign CZAG 방식은 다음과 같은 약점을 갖고 있다고 지적했다. 첫 번째, 시스템은 본의 아니게 약한 암호화 방식을 사용했으며 그리고 참여한 싸이트와의 접속이 시간 경과 되거나 혹은 잘못사용해서 종료될 때 참여 웹 싸이트를 폐지시킬 수 있는 폐기 메카니즘을 갖지 못했다. 둘째로, 보호 방식에 대한 사용자의 기대치와 약속한 실제 보호 방식 간에 명확한 모순이 존재한다.

3.5 Hwang's revised SET certificate

원래의 SET에서, 카드 넘버와 만료일자등을 포함하는 중요한 신용카드정보는 카드소유자의 인증서 내부에서는 평문이 아니라 해쉬된 값으로 저장된다[10-12]. "acquirer"(신용카드 지불방식에 대한 전송 모델에서 사용되는 4 가지의 역할이 있다. "issuer"는 "cardholder"에게 신용카드를 발급하는 금융 기관이다. "acquirer"는 "merchant"에게 지불 인가와 지불을 수행하는 금융 기관이다.)는 PI(Payment Instruction)에 대한 카드소유자의 서명을 검증할 것을 요구하고, 신용카드정보를 입력으로 해쉬 값을 계산하고 그리고 결과 값을 카드소유자의 인증서 내에 저장된 "subject name"과 비교한다.

위의 과정에서 카드소유자의 중요 정보는 "acquirer"에게 노출되고, 이것은 카드소유자의 관점에서 볼 때 예기치 않았던 정보 노출일 수 있다. 그러므로 논문[13]에서 Hwang등은 카드소유자의 위와 같은 우려를 없애기 위해서 SET 인증서에 대한 개정판을 제안하였다.

Hwang등은 카드소유자의 신용 카드 정보가 한번의 해쉬 연산 대신에 두 번의 해쉬 연산 후 인증서 내에 저장 되도록 제안하였다. 만약 H(H(credit_card_info))가 인증서 내에 저장됐다면, 오직 H(credit_card_info)만이 PI내에서 볼 수 있어야한다. 인증서와 PI와의 일관성을 확인함으로써 "acquirer"는 카드 넘버를 알지 못한 상태에서 카드의 유효성을 아직도 검증할 수 있다. 이때 "acquirer"는 PI으로부터 받은 H(credit_card_info)을 인가를 위해서 발급자에게 보낸다.

그러나, 대부분의 신용 카드 넘버는 단지 16비트만을 사용하기 때문에 credit_card_info는 소모적인 공격에 의해서 쉽게 H(H(credit_card_info))로부터 얻을 수 있다. 따라서 Hwang의 개정된 SET 인증서는 요구조건 R1과 R3를 위반한다.

본 논문에서 KISA의 SIM처럼 Hwang의 방식을 수정할 수도 있지만 이런 수정 방식은 아직도 요구조건 R3를 위반하게 된다.

Ⅳ. 제안한 프라이버시 보호 기능이 추가된 인증서 프로화일

본 논문에서 우리는 인증서의 "subject" 필드가 인증서 소유자에 대한 기본적인(중요하지않은) 정보만을 포함하고 그리고 "subjectAltName" 확장 필드는 소유자의 사진, 소유자의 지문 그리고 소유자의 여권번호 등과 같은 인증서 소유자의 프라이버시와 관련한 n 개의 중요한 정보를 표시한다고 가정한다. 즉, subjectAltName = <$Privacy_1$, $Privacy_2$, ..., $Privacy_n$> 이다. 단, $Privacy_i$($1 \le i \le n$)은 인증서 소유자의 개인 정보를 포함한다.

4.1 제안 방식 1

우선 CA는 Diffie-Hellman 소수 p(단, 모든 $1 \le i \le n$ 에 대해 $|p| > |Privacy_i|$이고 $|p|$와 $|Privacy_i|$는 p와 $Privacy_i$의 비트-길이 이다)와 위수 p-1상에서의 생성자 $g \in Z_p$ 그리고 암호학적으로 안전한 해쉬 함수 H(•) 그리고 공개 시스템 파라미터로서 안전한 용장도(혹은 패딩) 함수 R(•)를 선택한다[14].

제안한 형식에서 "subjectAltName" 확장 필드는 다음처럼 재 정의한다. NewSunjectAltName=<$BlindPrivacy_1$,...,$BlindPrivacy_n$>. 여기서 $BlindedPrivacy_i$ ($1 \le i \le n$)는 subjectPublicKeyInfo 필드에 저장된 공개 키 PKsubject에 대응하는 비밀 키 SKsubject를 이용해서 다음과 같이 정의한다.

$$BlindedPrivacy_i = R(Pivacy_i) \oplus ((g^{H(i, SK_{subject})} \bmod p) \bmod 2^{|Privacy_i|})$$

지금부터 사용자는 선택적으로 자신의 개인 정보를 다음처럼 웹 싸이트에 오픈할 수 있으며 보여줄 수도 있다.

1) 인증서 소유자 A는 자신의 인증서를 서버 B에게 송신한다.
2) B는 A에게 인증서 소유자의 추가적인 어떤 정보가 필요하다고 얘기한다.
3) B의 요구에 따라 A는 B에게 다음 값을 비밀리에 송신한다.

$$y_i = g^{H(i, SK_A)} \bmod p$$

단, $BlindedPrivacy_i$는 B가 요구한 정보를 포함한다.

4) A와 B는 다음처럼 기저 g의 yi에 대한 이산대수 값을 알고 있다는 사실을 영지식 프로토콜을 이용해서 증명한다[15].
   a) A는 $t = g^v \bmod p\ (v \in_R Z_{p-1})$을 계산해서 B에게 보낸다.
   b) B는 "a small set of possible challenges"와 {1, 2, ..., k}로부터 challenge c를 선택한 후 이것을 다시 A에게 보낸다.
   c) A는 $r = v - c \cdot H(i, SK_A) \bmod p$을 계산해서 이것을 B에게 보낸다.
   d) B는 방정식 $t = g^{r \cdot y_i^c} \bmod p$을 검사한다.
5) 만약 A가 타당한 증명을 완성하는데 성공한다면, B는 $Privacy_i$를 복원해서 용장도(혹은 패딩)을 다음과 같이 계산해서 검사한다.

$$Privacy_i = R^{-1}(BlindedPrivacy_i \oplus (y_i \bmod 2^{|BlindedPrivacy_i|})$$

단, R^{-1}(•)는 R(•)의 역함수이다.

4.2 제안방식 2

만약 $Privacy_i$($1 \le i \le n$)가 인간이 기억할 수 있는

값이라면, 본 논문에서는 BlindedPrivacy$_i$($1 \le i \le n$)을 다음처럼 정의한다.

$$BlindedPrivacy_i = R(HashedPrivacy_i) \oplus ((g^{H(i, SK_{subject})} \bmod p) \bmod 2^{|Privacy_i|})$$

단, HashedPrivacy$_i$ = H(Privacy$_i$) 이다.

KISA의 SIM에서처럼 만약 A가 Privacy$_i$을 노출하지 않고 Privacy$_i$을 알고 있다는 사실만을 증명하기를 원한다면, A는 B에게 $y_i = g^{H(i, SK_A)} \bmod p$을 송신한다. A와 B가 기저 g의 y_i에 대한 이산대수 값을 알고 있다는 사실을 영지식 증명 프로토콜을 실행한 후, B는 HashedPrivacy$_i$를 복원해서 이것의 용장도(혹은 패딩)를 검사한다.

만약 B가 추가로 개인 정보를 보여 달라고 요구한다면, A는 역시 B에게 자신이 기억하고 있는 Privacy$_i$을 송신한다. 이때 B는 다음 식이 맞는지 틀리는지 검사한다.

$$H(Privacy_i) = HashedPrivacy_i = R^{-1}(BlibdedPrivacy_i \oplus (y_i \bmod 2^{|BlindedPrivacy_i|})$$

V. 분 석

5.1 R1 : Invisibility

만약 위수 p-1상에서 생성자 g가 Z_p상의 모든 원소가 g의 멱승으로 사용될 수 있는 특성을 갖는다면, 랜덤 오라클 모델에서 우리는 해쉬 함수 H(•)는 랜덤 함수처럼 작동한다고 가정한다[16]. 따라서 $g^{H(i, SK_{subject})} \bmod p$는 Z_p상에서 랜덤하게 선택한 정수와 구별불가능하며, $R(privacy_i) \oplus (g^{H(i, SK_{subject})} \bmod p$ 역시 랜덤하다.

그러므로 $SK_{subject}$를 모르는 사람은 인증서로부터 Privacy$_i$에 대한 정보를 얻을 수 없다.

5.2 R2 : Soundness

악의의 인증서 소유자 A가 불법으로 자신의 정보 Privacy$_i$를 Privacy$_i$로 변경시킬려고 한다고 가정하자. 이것을 실행하기 위해서 악의의 A는 단계 3)에서 y_i = BlindedPrivacy$_i$ ⊕ R(Privacy$_i$)를 계산한 후 이것을 B에게 보내고 그리고 기저 g상에서의 y_i에 대한 이산대수 값을 안다는 사실을 영지식 증명을 이용해서 증명한다.

그러나 이산대수문제의 어려움 때문에 악의의 A는 기저 g상에서의 y_i에 대한 이산대수 값을 안다는 사실에 대한 타당한 영지식 증명을 구성하는데 최대한 k^{-1}의 확률을 가지고 성공할 수 있다.

다음과 같은 다른 시나리오를 생각해보자. 악의의 A는 $BlindedPrivacy_i \oplus ((g^{SK} \bmod p) \bmod 2^{|BlindedPrivacy_i|})$가 정당한 형식을 가질 때까지 반복해서 $sk \in_R Z_{p-1}$을 발견할려고 한다고 가정하자. 그러나 안전한 용장도 함수 R(•) 때문에 위의 시도가 성공할 확률은 무시해도 좋다.

5.3 R3 : Non-transferability

제안한 방식을 사용하면 서버 B는 A의 프라이버시 정보를 다른 사람에게 노출 시킬 수 없다. 물론 B는 A와 B사이의 통신 데이터 사본을 만들 수 있다. 그러나 B는 임의의 프라이버시 정보 Privacy$_i$에 대해서 자신이 항상 A의 지식을 생성할 수 있는 시뮬레이터를 만들 수 있다고 확신시키기 위해서 이러한 사본을 이용할 수 없다. 이러한 통신 데이터 사본을 시뮬레이션하기 위해서 B는 challenge를 선택해서 다음과 같이 영지식임을 증명하기 위해서 일반적인 트릭을 사용한다.

1) 프라이버시 정보 Privacyi을 선택한다.
2) y_i = (padi || (BlindedPrivacy$_i$ ⊕ R(Privacy$_i$))) $\in_R Z_p$를 계산한다.
   단, pad$_i$는 (|p|-|BlindedPrivacy$_i$|) 비트 랜덤 패딩이다.
3) $r \in_R Z_{p-1}$과 $c \in_R \{1,2,...,k\}$을 선택한다.
4) $t = g^r \cdot y_i^{-c} \bmod p$를 계산한다.
5) (y_i, t, c, r, Privacy$_i$)를 출력한다.

중요한 사실은 시뮬레이터가 생성한 사본은 프로토콜이 올바르게 실행했을 때의 사본과 구별할 수 없음이다. 사실상 시뮬레이터가 생성한 사본의 분포는 프로토콜을 정직하게 실행을 때의 사본의 분포와 동일하다. 위와 같은 이유로 우리가 인증서 소유자의 프라이버시 정보의 노출을 3DES나 AES와 같은 블록 암호 방식을 이용해도(예를 들면, $BlindedPrivacy_i = E_{H(i, SK_A)}(Privacy_i)$ 막을 수 없는 이유이다. 따라서 카드 소유자의 프라이버시 정보 노출을 막기 위해서는 제안한 방식을 사용해야만 한다.

VI. 결 론

본 논문에서는 인증서 소유자의 프라이버시 정보에 대한 요구 조건들을 제시하였고, 4개의 관련 표준 문서들(X.509 public-key certificate, Hongkong's

e-Cert, KISA's SIM, 그리고 VeriSign's CZAG)과 최근에 제안된 프로토콜을 분석하였다. 또한 최소권한(need-to-know) 원칙을 기본으로 우리는 인증서 소유자의 프라이버시를 보호하기 위해서 즉, 요구조건 R1, R2 그리고 R3를 만족하는 수정된 공개키 인증서 형태와 이와 관련한 프로토콜을 제안하였다.

참 고 문 헌

[1] E.IITF principles, supra note 19, at 5.

[2] J.J. Hwang and S.C. Hsueh, "Greater protection for credit card holders : a revised SET protocol", Computer Standards and Interfaces 19, pp.1-8, 1988.

[3] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen, and M. Waidner, "Design, implementation, and deployment of the iKP secure electronic payment system", *IEEE Journal on Selected Areas in Communications* 18(4), pp. 611-627, April 1991

[4] Australian Transaction Report and Analysis Center, "RGEC report -- research and technical advice volume 3", http://www.austrac.gov.au/text/publications/rgec/3/pdf/ch1.pdf, Dec, 1999

[5] R. Housley, W. Ford, W. Polk, and D. Solo, "*Intenet X.509 public key infrastructure certificate and Certificate Revocation list (CRL) profile*", *IETF RFC 3280*, April 2002

[6] Hongkong Post, "*e-Cert certification practice statement*", 2001

[7] J. Park, J. Yoon, S. Kim, S. Park, J.Lee, H. Lee, and T. Polk, "*Internet X.509 public key infrastructure subject identification method*" draft-ietf-pkix-sim-03.txt, Feb. 2004

[8] Verisign, "*VeriSign enhances digital IDs to enable universial website login and one-step registration*", http://www.verisign.com/press/product/isv.html, , April 1997

[9] S.G. Renfro, "VeriSign CZAG: privacy leak in X.509 certificates", Proceedings of the 11th USENIX Security Symposium, August 2002

[10] MasterCard and VISA, "Secure Electronic Transaction (SET) specification", Book 1 : Business Description, version 1.0(1997)

[11] MasterCard and VISA, "Secure Electronic Transaction (SET) specification", Book 2 : Programmer's Guide, version 1.0(1997)

[12] MasterCard and VISA, "Secure Electronic Transaction (SET) specification", Book 3 : Formal Protocol Definition, version 1.0 (1997)

[13] J.J. Hwang, T.C. Yeh, and J.B. Li, "Securing on-line credit card payments without disclosing privacy information", Computer Standards and Interfaces 25, pp.119-129, 2003.

[14] W. Diffie and M.E. Hellman, "New Directions in cryptography", *IEEE* Trans. Inform. Theory, IT-22, pp.644-654, 1976

[15] J. Camenisch and M. Stadler, "Proof systems for general statements about discrete logarithms", Technical Report TR 260, 13pages, *Department of Computer Science, ETH Zurich*, March 1997

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", Proc. First Annual Conference on Computer and Communications Security, ACM, 1993

양 형 규(Hyung kyu Yang) 정회원

한국 통신학회 논문지 2005년 1월호 참조

현재 강남대학교 컴퓨터미디어공학부 부교수