Computer Security

Hw#2

- 공인인증서 조사 -

학　　과　컴퓨터공학과
학　　번　201211704
이　　름　김기홍
제 출 일　2016.10.02

부경대학교

<목 차>

1 서론

우리는 Hw#2에서 공인인증서에 대한 것을 자세하게 조사해봄으로써 우리가 실제로 흔히 사용하고 있는 기술이 어떤 구조를 가지고 있고, 어떻게 동작이 되어 지며 더 나아가 관련 법령, 활용 분야, 유출 사례 및 문제 개선에 대해 알아보면서 전체적인 개념을 학습한다. 관련 내용을 참조한 출처는 보고서의 끝 부분에 첨가하도록 한다. '공인인증서'라는 기술에 대한 보고서이므로 대체로 참조 글이 많은 사실을 서론에서 미리 밝힌다.

2 공인인증서란?

'공인인증서'는 전자 서명의 검증에 필요한 공개키에 소유자 정보를 추가하여 만든 일종의 전자 신분증이다. 이는 MIT의 펠더(Loren Kohnfelder)가 1978년에 처음 제안했다. 공인인증서는 신뢰할 수 있는 인증기관이 전자서명 하여 생성하며 인증기관이 공개키를 공증해준다고 생각하면 된다. 비유를 하자면, 일상생활에서 사용하는 인감증명서에 비유할 수 있다.

공인인증서로 전자서명을 하면 상대방이 서명한 사람이 누구인지 확인할 수 있고, 전자 문서의 위조나 변조를 예방할 수 있으며, 거래사실을 증명할 수 있다. 즉, 인증, 무결성, 부인 방지를 보장한다.

3 공인인증서의 구조

공인인증서의 구조를 어느 인증서나 같은 내용을 가지고 있는 '기본 영역' 그리고 인증서에 따라 그 구성 내용이 다르지만 일반적으로 포함하고 있는 '확장 영역'으로 나누어 소개한다.

(1) 인증서의 기본 영역

항목	설명
버전	인증서의 형식 구분
일련번호	인증서를 발급한 인증기관 내의 인증서 일련번호
서명 알고리즘	인증서를 발급할 때 사용한 알고리즘
발급자	인증서를 발급한 인증기관의 Distinguish Name
유효 기간(시작, 끝)	인증서를 사용할 수 있는 기간(초 단위)
주체	인증서 소유자의 Distinguish Name
공개키	인증서의 모든 영역을 해시해서 인증기관의 개인키로 서명한 값

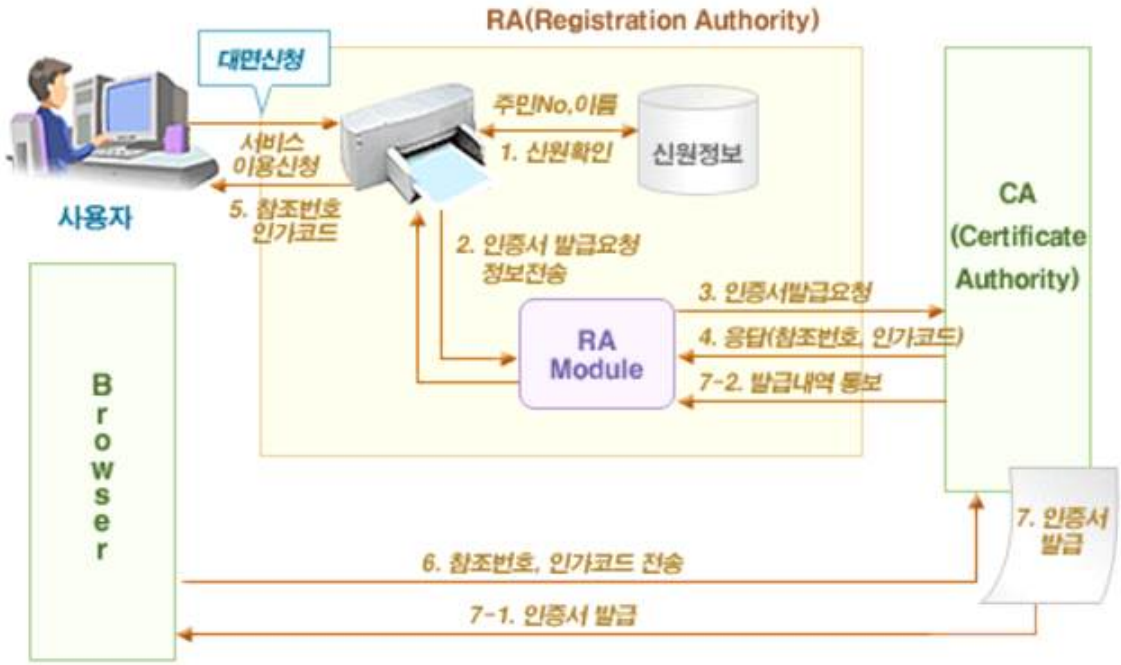
(2) 인증서의 확장 영역

항목	설명
기관 키 식별자	인증서를 확인할 때 사용할 인증기관 공개키의 유일 식별자
주체 키 식별자	인증서 소유자의 공개키에 대한 유일 식별자
주체 대체 이름	인증서 사용자의 이름 혹은 또 다른 별개의 이름에 대한 부가 정보
CRL 배포 지점	인증서의 폐기 여부를 확인하기 위한 인증서 폐기 목록(CRL)이 있는 위치
키 사용 용도	인증서에 포함된 공개키의 용도
손도장 알고리즘	인증서를 hash하는 데 쓰이는 알고리즘
손도장	증명서가 개봉되지 않았음을 증명하는 hash 자체

4 공인인증서의 동작

4.1 공인 인증 과정

공인인증서를 통한 공인 인증 과정은 다음과 같다.



공인인증서를 발급 받기 위해서는 반드시 RA(은행)에서 대면확인을 통해 본인임을 증명해야 한다. 그러면 RA는 고객의 신청 정보로 CA(인증기관)로 인증서 발급 요청을 하게 된다. 그러면 CA는 RA를 통해 고객에게 임시 번호의 역할을 하는 참조번호와 인가코드를 전달한다. 고객은 전달받은 참조번호와 인가코드를 이용하여 CA로부터 일정한 유효기간을 갖는 인증서를 발급 받는다. 그 후에 CA는 신규 발급한 인증서의 발급 정보를 각 금융기관 등에 배포함으로써, 인증서의 유효성을 검증한다.

4.2 전자서명 알고리즘

우리나라에서 사용되는 전자서명 알고리즘에는 크게 RSA, ECDSA, KCDSA가 있다. 먼저 RSA는 Rivest , Shamir, Adleman 암호학의 거장 세 사람의 이름을 따서 만든 정수론 기반 공개키 암호화 알고리즘이다. 다음으로 ECDSA는 Ellptic Curve Digital Signature Algorithm의 약자로서 타원 곡선 전자 서명 알고리즘을

뜻한다. 이 방법은 적은 메모리 공간으로도 RSA와 대등한 안전성을 보유하고 있고 처리 속도 또한 빨라 이동 단말기에 활용된다. 마지막으로 KCDSA는 Korean Certifice-based Digital Signature Algorithm의 약자로서 ELGamal 전자서명 방식을 개선하여 1998년 대한민국 표준으로 채택되었다.

5 공인인증서의 폐기

어떤 이유에서든지 인증서가 한 번 폐기되면 더 이상 사용할 수 없다. 예를 들면 공격자가 인증서에 포함된 공개키에 대응되는 개인키를 확보하면 그 인증서는 더 이상 제 역할을 할 수 없다. 즉, 인증서 폐기의 목적은 시기적절하게 폐기하여 인증서 사용에 따른 피해를 줄이는 것이다.

인증기관은 폐기된 인증서 목록을 주기적으로 발급한다. 이를 CRL(Certification Revocation List)이라고 한다. 물론 이 목록도 공격자가 접근이 불가능해야하기 때문에 인증기관이 전자서명을 한다.

인증서 폐기 목록에는 bad-list와 good-list 방법이 있다. bad-list는 목록에 폐기된 인증서에 관한 정보만 유지되는 것이고, good-list는 사용할 수 있는 인증서만이 목록에 존재한다.

6 관련법령 및 제도

공인인증서의 암호체계에 대해 간단히 소개하고 전자금융거래법 개정안이 국회 본회의를 통과한 후 있었던 변화에 관해 정리하고 향후 전망을 해본다.

6.1 공인인증서의 암호체계

공인인증서의 암호체계는 분산처리 등 컴퓨팅 환경의 급속한 발달로 인하여 기존 암호 알고리즘의 안전성이 저하되어 수준이 높은 암호 알고리즘이 필요하기 때문에 한국인터넷진흥원은 2009년 9월 공인인증서 암호체계 고도화 기본계획을 세우게 된다. NIST 등 암호전문기관은 국내 공인전자서명인증 체계에서 이용 중인 RSA 1024, SHA-1 알고리즘은 2011년이후 안전성 담보가 어려울 것으로 전망했다. 따라서 전자서명의 RSA 알고리즘의 키 길이를 1024비트에서 2048비트로 상향 조정하고, 전자서명의 해시 알고리즘을 SHA1에서 SHA256으로 상향조정하였다. RSA는 공개키 암호화 알고리즘으로서 우리가 배웠기 때문에 생략하고 SHA는

보고서 마지막에 간단하게 살펴보도록 한다. 그리고 전자거래업체에서는 공인인증서를 이용하는 응용 SW에서 고도화된 인증서를 처리할 수 있도록 SW 업그레이드를 시키게끔 하였다.

6.2 전자금융거래법 개정안

2014년 9월 30일 전자금융거래법 개정안이 국회 본회의를 통과했고, 2015년 10월 15일 시행되었다. 이는 금융감독원이 2002년 9월부터 공인인증서 사용을 전자금융거래에 강제하던 것을 마침내 포기한 것이다. 그리고 근본적인 규제 전략 변화도 시도하고 있다. 첫째로, 2015년 2월 3일 개정에서는 "보안 3종 세트"라고 불리는 보안프로그램들의 설치 의무가 폐기되었다. 그리고 2015년 3월 18일 개정에서는 공인인증서 사용 강제 조항을 삭제하였다. 대신 금융회사가 거래의 종류, 성격, 위험수준 등을 고려하여 안전한 인증방법을 사용하도록 조항을 개정하였다. 마지막으로 2015년 6월 24일 그동안 금융감독원이 수행해 왔던 "보안성 심의" 제도가 말끔히 폐지되고, 그 대신 전문성과 독립성이 있는 보안감사업체에 의한 보안점검 제도가 도입되었다.

이러한 규제 체제의 변화는 전자금융거래 시장에 커다란 변동을 불러일으키리라 예상된다.

7 공인인증서의 종류와 활용분야

공인인증서는 모든 이용분야에서 이용할 수 있는 '범용 공인인증서'와 인터넷 뱅킹 등 특정분야에서만 이용할 수 있도록 해당 기관이 고객에게만 발급하는 '용도제한 공인인증서'가 있다.

'범용 공인인증서'가 있으면 인터넷뱅킹, 온라인 증권, 전자상거래, 전자정부 민원서비스, 4대 사회보험, 국세청 홈텍스, 전자세금계산서, 전자입찰/조달, 온라인 교육, 예비군 등 다양한 분야의 업무를 하나의 공인인증서만으로 편하게 이용할 수 있다.

'용도제한 공인인증서'는 인증서의 용도가 은행/카드/보험용, 증권/카드/보험용, 특정목적용과 같이 국한되어있는 인증서를 말한다.

8 공인인증기관

우리나라 공인인증기관에는 한국정보인증(KICA), 코스콤(KOSCOM), 금융결제원(KFTC), 한국정보사회진흥원, 한국전자인증(KECA), 한국무역정보통신(KTNET) 이상 6군데가 있다. 전자서명법에 따라 거래 사실을 공정하게 관리, 보증할 수 있는 공신력과 인증 시스템을 안전하게 구축, 관리할 수 있는 인력, 기술력, 자금력을 갖춘 기관으로, 정보통신부가 지정하였다.

9 공인인증서 유출 사례와 문제 개선

공인인증서가 유출된 수많은 사례 중 2012년에 발생한 스팸 메일을 위장한 트로이 목마 프로그램 해킹 사건이다. 이 사건은 전문해커 2명이 스팸메일에 트로이 목마 프로그램을 심어두어 손쉽게 공인인증서 및 암호를 얻어내면서 부당한 이익을 챙긴 사건이다.

KSIA 전자서명인증관리센터에서는 해킹, 전자금융사기에 의해 공인인증서가 유출되는 문제를 개선하기 위해서 보안토큰, USIM, 금융IC카드, Secure Element 등 유출이 불가능한 안전한 저장매체에 저장하여 이용하는 것을 권장한다.

저장매체	사진	특징
보안토큰		C칩 내 안전하게 공인인증서 저장 이용 가능
USIM		스마트폰의 USIM 내 공인인증서 저장 이용 가능
금융IC카드		IC칩 내 안전하게 공인인증서 저장 이용 가능
Secure Element		스마트폰 등 디바이스 내 독립적인 H/W저장 공간으로 보안 영역에서 안전하게 공인인증서 저장 이용 가능

10 참조

정보 보안 개론(저자 양대일)
공인인증서 - 위키피디아
KISA 전자서명인증관리센터
공인인증서 폐지 1년, 전자금융 환경 변화의 시작 – slow news(필자 김기창)
공인인증서 암호체계 고도화 기본계획 – 한국인터넷진흥원(KISA)
어제보다 오늘 덜 어리석은 개발자 – weicome

※ 부록 – SHA

SHA는 Secure Hash Algorithm의 약자로서 이 함수들은 서로 관련된 암호학적 해시 함수들의 모음이다. 이들 함수는 미국 국가안보국(NSA)이 1993년에 처음으로 설계했으며 미국 국가 표준으로 지정되었다.

여기서 언급된 SHA-1과 SHA-256의 특성을 비교하고 마치도록 한다.

알고리즘	해시값 크기	내부 상태 크기	블록 크기	길이 한계
	워드 크기	과정 수	사용되는 연산	충돌
SHA-1	160	160	512	64
	32	80	+, and, or, xor, rotl	공격법만 존재
SHA-256	256	256	512	64
	32	64	+, and, or, xor, shr, rotr	-