(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0042413
(43) 공개일자 2009년04월30일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/20* (2006.01)
(21) 출원번호 10-2007-0108157
(22) 출원일자 2007년10월26일
심사청구일자 2007년10월26일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초동 삼풍APT 3동 405호
(74) 대리인
이원희

전체 청구항 수 : 총 6 항

(54) 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의추측공격에 대한 보안을 강화하는 방법

(57) 요 약

본 발명은 종래의 암호 설정 방법이 가지는, 공격자에 의한 추측공격을 방지하여 보다 안전한 전자상거래가 가능하도록 하는 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의 추측공격에 대한 보안을 강화하는 방법을 제공하는 데 그 목적이 있는 것으로서,

본 발명에 따른 공인인증서의 추측공격에 대한 보안을 강화하는 방법은,

하나 이상의 영문자 또는 하나 이상의 숫자를 조합하여 제1 암호화부를 입력하는 단계; 적어도 하나 이상의 인덱스를 가지며, 상기 인덱스 각각에 하나 이상의 난수가 기재되어 있는 보안카드로부터 적어도 하나 이상의 난수를 추출하여 상기 난수를 상기 제1 암호화부 다음에 순차적으로 입력하여 제2 암호화부를 입력하는 단계로 이루어지는 것을 특징으로 한다.

대 표 도 - 도4



특허청구의 범위

청구항 1

하나 이상의 문자 또는 하나 이상의 숫자를 조합한 제1 암호화부를 입력하는 단계;

적어도 하나 이상의 인덱스를 가지며, 상기 인덱스 각각에 하나 이상의 난수가 기재되어 있는 보안카드로부터 적어도 하나 이상의 난수를 추출하여 상기 난수를 상기 제1 암호화부 다음에 순차적으로 입력하여 제2 암호화부를 입력하는 단계

로 이루어지는 것을 특징으로 하는 공인인증서의 추측공격에 대한 보안 강화 방법.

청구항 2

청구항 1에 있어서,

상기 보안카드는 공인인증서를 사용하기 위한 은행의 보안카드인 것을 특징으로 하는 공인인증서의 추측공격에 대한 보안 강화 방법.

청구항 3

청구항 1에 있어서,

상기 난수는 공인인증서를 사용하기 위한 은행의 보안카드의 코드표 비밀번호인 것을 특징으로 하는 공인인증서의 추측공격에 대한 보안 강화 방법.

청구항 4

청구항 1에 있어서,

상기 제2 암호화부는 입력되어야 할 난수가 속해 있는 인덱스가 표시되어 있는 것을 특징으로 하는 공인인증서의 추측공격에 대한 보안 강화 방법.

청구항 5

비밀키 암호화 알고리즘(encryption Algorithm)과 상기 알고리즘에 의해 암호화된 비밀키(encrypted Data), 및 보안카드의 인덱스 번호를 포함하여 구성되는 것을 특징으로 하는 암호화된 비밀키의 구조.

청구항 6

청구항 5에 있어서,

상기 비밀키 암호화 알고리즘은 PBKDF2(Password based key derivation function)인 것을 특징으로 하는 암호화된 비밀키의 구조.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 난수가 기재되어 있는 카드, 즉 예를 들면 은행의 보안카드의 코드표 비밀번호, 인덱스를 이용한 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의 추측공격에 대한 보안을 강화하는 방법에 관한 것이다.

배 경 기 술

<2> 공인인증서는 전자상거래를 할 때 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인 방지 등을 목적으로 공인인증기관(CA)이 발행하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서이다.

<3> 최근 들어 공인인증서 누출에 따른 보안사고가 급증하고 있다. 보통 전자메일을 이용하여 공인인증서를 저장하다가 보안사고가 많이 일어난다.

<4> 일반적인 암호의 사용에 있어서 통상의 사용자들은 각기 다른 암호를 외우기가 불편하다는 이유로 보안이 덜 필요한 전자메일 계정의 비밀번호와 같은 비밀번호나 집이나 핸드폰 전화번호 등 자신의 특징을 표시하는 비밀번호를 암호로 많이 사용하게 된다.

<5> 이러한 점은 의도적으로 또는 우연히 타인의 전자메일 계정을 획득한 공격자가 전자메일의 비밀번호를 알게 되었을 경우, 이 비밀번호로부터 전자메일에 저장되어 있는 공인인증서의 비밀번호를 추측할 수 있게 된다.

<6> 이와 같은 비밀번호의 추측성을 예방하기 위해 단순히 비밀번호의 자릿수를 증가하는 것은 사용자들이 긴 자릿수의 암호를 기억하기가 어렵고, 또한 공격자들의 추측공격을 완벽하게 방지하는 것이 어렵다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<7> 본 발명은 상기와 같은 종래의 암호 설정 방법이 가지는, 공격자에 의한 추측공격을 방지하여 보다 안전한 전자상거래가 가능하도록 하는 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의 추측공격에 대한 보안을 강화하는 방법을 제공하는 데 그 목적이 있다.

과제 해결수단

<8> 상기와 같은 본 발명의 목적은 달성하기 위해 본 발명에 따른 공인인증서의 추측 공격에 대한 보안 강화 방법은,

<9> 하나 이상의 문자 또는 하나 이상의 숫자를 조합한 제1 암호화부를 입력하는 단계; 적어도 하나 이상의 인덱스를 가지며, 상기 인덱스 각각에 하나 이상의 난수가 기재되어 있는 보안카드로부터 적어도 하나 이상의 난수를 추출하여 상기 난수를 상기 제1 암호화부 다음에 순차적으로 입력하여 제2 암호화부를 입력하는 단계로 이루어지는 것을 특징으로 한다.

<10> 또한, 상기 보안카드는 공인인증서를 사용하기 위한 은행의 보안카드인 것을 특징으로 한다.

<11> 또한, 상기 난수는 공인인증서를 사용하기 위한 은행의 보안카드의 코드표 비밀번호인 것을 특징으로 한다.

<12> 또한, 상기 제2 암호화부는 입력되어야 할 난수가 속해 있는 인덱스가 표시되어 있는 것을 특징으로 한다.

<13> 본 발명에 따른 암호화된 비밀키의 구조는,

<14> 비밀키 암호화 알고리즘(encryption Algorithm)과 상기 알고리즘에 의해 암호화된 비밀키(encrypted Data), 및 보안카드의 인덱스 번호를 포함하여 구성되는 것을 특징으로 한다.

<15> 또한, 상기 비밀키 암호화 알고리즘은 PBKDF2(Password based key derivation function)인 것을 특징으로 한다.

효 과

<16> 상기한 바와 같은 본 발명에 따른 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의 추측공격에 대한 보안을 강화하는 방법에 의하면,

<17> 의도적으로 또는 우연히 타인의 전자메일 계정을 획득한 공격자가 전자메일의 비밀번호를 알게 되었을 경우라도, 공격자에 의한 추측공격을 방지하여 보다 안전한 전자상거래가 가능하도록 하는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<18> 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 본 발명을 설명함에 있어서 관련된 공지기능 혹은 구성에 대한 구체적인 설명은 본 발명의 요지를 모호하게 하지 않기 위해 생략한다.

<19> 도 1은 종래의 암호화된 비밀키의 구조를 개념적으로 도시한 도이다. 도 2는 종래의 개인키 정보(Private-key information)의 구조를 개념적으로 도시한 도이다. 도 3은 PBKDF2(Password based key derivation function)으로부터 비밀키를 암호화할 추출키(Derivation key)를 생성하는 방법과 그에 쓰이는 용어를 설명하고 있는 도이다. 도 4는 본 발명에 따른 암호화된 비밀키의 구조를 도시한 것으로, 보안카드의 인덱스 번호가 추가된 것이 도시되어 있다.

<20> 도 1을 참조하면, 현재 공인인증서는 공인인증서의 개인키를 도 1과 같이 암호화하여 저장한다. 상기 개인키는 비밀키를 암호화하는 비밀키 암호화 알고리즘(encryption Algorithm)과 이 알고리즘에 의해 암호화된 비밀키(encrypted Data)를 포함하여 구성된다.

<21> 도 1에 도시된 개인키 정보(Private-key information)는 도 2와 같이 정의되는 데, 도 2를 참조하면, 상기 개인키 정보(Private-key information)는 비밀키의 버전(Version), 비밀키 생성 알고리즘(Private Key Algorithm), 비밀키(Private Key), 그리고 비밀키의 속성(Attribute)을 포함하여 구성된다.

<22> 도 1에서 도시된 비밀키 암호화 알고리즘(encryption Algorithm)은 개인키 정보(Private-key information)의 암호화된 알고리즘을 정의하고 있다. 상기 비밀키 암호화 알고리즘(encryption Algorithm)은 사용자가 공인인증서에 입력한 비밀번호를 이용하여 비밀키를 암호화할 키를 추출하게 된다. 패스워드로부터 비밀키를 유도하는 방법으로 잘 알려진 것은 PKCS#5의 PBKDF1과 PBKDF2, 그리고 PKCS#12의 PBKDF가 있으며, 도 3에는 이 중 PBKDF2에 대한 설명이 개념적으로 도시되어 있다.

<23> 도 3을 참조하면, PBKDF2(Password based key derivation function)으로부터 비밀키를 암호화할 추출키(Derivation key)를 생성하는 방법과 그에 쓰이는 용어를 설명하고 있다.

<24> 본 발명에 따른 공인인증서의 추측공격에 대한 보안 강화 방법은, 여기서 사용되고 있는 P(Password; 공인인증서에 입력하는 암호)에 하나 이상의 난수(예를 들면, 보안카드의 코드표 비밀번호)를 추가하는 것이다.

<25> 즉, 먼저, 하나 이상의 문자 또는 하나 이상의 숫자를 조합한 제1 암호화부를 입력한다.

<26> 예를 들면, "1234"와 같은 숫자로 조합된 제1 암호화부를 입력한다.

<27> 그 다음, 적어도 하나 이상의 인덱스를 가지며, 상기 인덱스 각각에 하나 이상의 난수가 기재되어 있는 보안카드로부터 적어도 하나 이상의 난수를 추출하여 상기 난수를 상기 제1 암호화부 다음에 순차적으로 입력하여 제2 암호화부를 입력하여, 공인인증서의 추측공격에 대한 보안을 강화할 수 있게 된다.

<28> 예를 들면, 상기 제2 암호화부에 입력되어야 할 인덱스가 3번째 인덱스이며, 상기 보안카드의 3번째 인덱스에 난수 "5678" 이 기재되어 있는 경우, 입력되어야 하는 암호는 "12345678"이 된다. 여기서 "5678"이 제2 암호화부에 해당한다.

<29> 상기 제2 암호화부에 기재되는 난수는 사용자가 통상 사용하며 외우고 있는 암호인 제1 암호화부와는 전혀 다르고, 또한, 전화번호나 주민번호와 같은 자신의 특징을 표시하는 번호와는 전혀 관계없는 랜덤성이 큰 번호이므로, 공인인증서의 추측공격에 대한 보안을 강화할 수 있게 된다.

<30> 이 때, 상기 보안카드는 사용자가 휴대할 수 있는 카드인 것이 바람직하며, 구체적으로 상기 보안카드는 공인인증서를 사용하기 위한 은행의 보안카드인 것이 더욱 바람직하다. 또한, 상기 난수는 공인인증서를 사용하기 위한 은행의 보안카드의 코드표 비밀번호인 것이 바람직하다.

<31> 보안카드의 코드표 비밀번호를 제2 암호화부로 사용하기 위해 보안카드의 코드표 비밀번호뿐만 아니라, 그 비밀번호의 고유 인덱스(INDEX)가 필요하다. 인덱스(INDEX)가 있어야 사용자에게 암호와 함께 보안카드의 코드표 비밀번호를 물어볼 때 코드표의 몇 번째 숫자를 입력해야 하는지 알 수 있기 때문이다.

<32> 상기 인덱스(INDEX)는 평문으로 저장하더라도 보안상 문제가 되지 않기 때문에, 도 4에 도시된 바와 같이, 도 1의 비밀키 정보의 구조에 보안카드의 인덱스 번호(Secret Key Index Number)를 추가한다.

<33> 이상과 같이 본 발명에 따른 암호화된 비밀키의 구조 및 이를 이용하여 공인인증서의 추측공격에 대한 보안을 강화하는 방법을 예시한 도면을 참조로 하여 설명하였으나, 본 명세서에 개시된 실시예와 도면에 의해 본 발명이 한정되는 것은 아니며, 본 발명의 기술사상 범위내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

도면의 간단한 설명

<34> 도 1은 종래의 암호화된 비밀키의 구조를 개념적으로 도시한 도이다.

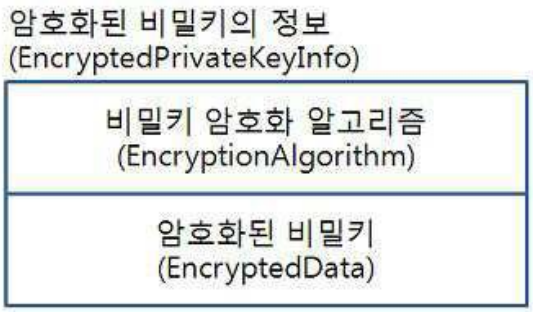
<35> 도 2는 종래의 개인키 정보(Private-key information)의 구조를 개념적으로 도시한 도이다.

<36> 도 3은 PBKDF2(Password based key derivation function)으로부터 비밀키를 암호화할 추출키(Derivation key)를 생성하는 방법과 그에 쓰이는 용어를 설명하고 있는 도이다.

<37> 도 4는 본 발명에 따른 암호화된 비밀키의 구조를 도시한 것으로, 보안카드의 인덱스 번호가 추가된 것이 도시되어 있다.

도면

도면1



도면2



도면3



도면4


암호화된 비밀키의 정보
(EncryptedPrivateKeyInfo)
비밀키 암호화 알고리즘
(EncryptionAlgorithm)
암호화된 비밀키
(EncryptedData)
보안카드의 인덱스 번호
(SecretKeyIndexNumber)