보안카드와 비밀번호를 이용한 사용자 인증 시스템의 보안 강화 기법

박인국*, 이필중**

포항공과대학교, 정보통신과

Technique To Strengthen The Security Of The User Authentication System Using Security Card And Password

In Kook Park*, Pil Joong Lee**

Graduate School of Information Technology, POSTECH*

Department of Electronic and Electrical Engineering, POSTECH**

요 약

본 논문에서는 사용자만이 알고 있는 비밀번호와 그 사용자만이 소유하는 보안카드를 이용하여 계산된 변동비밀번호의 1회 입력만으로 비밀번호와 보안카드를 통합하여 동시에 확인함으로써 안전하게 사용자 인증을 할 수 있는 방법을 제시한다. 본 논문에서 제안하는 사용자 인증 시스템은 변동비밀번호의 1회 입력만으로 지식기반 인증의 비밀번호와 소유기반 인증의 보안카드를 동시에 확인하여 사용자 인증이 이루어지기 때문에 서버의 효율성을 증가 시키며, 보안카드의 분실, 도난, 복제 등에 따른 위험성과 비밀번호의 추측, 노출에 따른 위험성을 줄여 보다 안전한 사용자 인증 시스템을 구축할 수 있다. 또한 본 논문에서 제안하는 시스템은 현재 사용되고 있는 텔레뱅킹(폰뱅킹), 인터넷(PC)뱅킹, 증권 매매, 전자 결재 등과 같은 기존의 비밀번호를 이용한 사용자 인증 시스템에 큰 교체 없이 적은 추가 비용으로 쉽게 적용하여 보다 안전한 인터넷과 금융 거래의 활성화에 기여할 수 있을 것이다.

I. 서론

사용자 인증은 사람과 사람이 만나서 대화를 하거나 사무를 처리하는 과정에서 언제나 발생하는 일이다. 일상적인 거래(물건의 구입, 은행 예금의 인출 등)를 하거나 행정적인 공무(주민등록의 발급, 조세 부과 등)를 수행할 경우 그 사무의 전제로서 자신이 상대하고 있는 상대방이 과연 내가 상대하고자 하는 진정한 그 사람인지를 확인할 수 있어야 한다.

이러한 사용자 인증은 일반적으로 사용자의 주민등록증을 확인하거나, 비밀번호, 기타 신체적 특징 등을 확인함으로써 이루어지고 있다. 그러나 익명성을 기반으로 한 인터넷의 발전은 이러한 사용자 인증에 있어서 어려운 문제를 제기하고 있다. 특히 인터넷을 통한 전자상거래의 발달로 인하여 인터넷에서 신원을 신속하고도 신뢰성 있게 확인하는 것은 인터넷 산업의 발전에 가장 중요한 전제 조건이자 또한 가장 큰 걸림돌로 작용하고 있다.

이렇듯 인터넷의 발달로 인하여 사용자 인증이 우리 생활의 일부분으로 자리 잡은 지금, 비밀번호를 이용한 사용자 인증 시스템은 사용자들의 편리성과 사용상의 간편성으로 인하여 사용자 인증을 위한 대표적인 수단으로 사용되고 있다.

그러나 정보 보안 공격 기술이 고도화되고 보안 침해 사례가 일반화되면서 기존의 비밀번호를 사용한 인증 방식은 비밀번호의 망각, 노출, 추측 등의 문제로 인하여 많은 문제점이 제기되었다. 그래서 오늘날 대부분의 금융 거래에서는 금융거래 시 비밀번호에 더하여 보안카드 사용을 의무화하여 2중으로 사용자 인증을 수행하게 하여 보다 안전한 방법으로 사용자를 인증할 수 있도록 하고 있다. 그러나 이러한 2중의 사용자 인증 방법 역

* 본 연구는 대학 IT연구센터 육성·지원사업과 교육부 두뇌한국 21 사업, Com2Mac-KOSEF의 연구결과로 수행되었음.

시 여전히 비밀번호의 노출 및 보안카드의 분실 등에 따라 문제점을 내포하고 있으며, 비밀번호와 보안카드를 이중으로 사용하여 2회 인증을 해야 한다는 사용자의 불편성을 증가시키고 있다.

본 논문에서는 이러한 기존의 문제점을 보안하여 비밀번호 및 보안카드의 노출을 방지하며, 1회 인증만으로 안전하게 사용자 인증을 수행하도록 하는 방법을 제시한다.

본 논문의 2장에서는 기존의 사용자 인증 방법의 예를 통하여 기존 방식의 문제점을 살펴보며, 3장에서는 본 논문에서 제안하는 시스템을 상세히 설명하며, 4장에서는 결론을 맺는다.

II. 사용자 인증

일반적으로 사용자 인증은 사용자의 지식, 소유, 생물학적 특징에 따라 아래의 3가지 방식으로 분류된다.

① 지식기반 인증은 그 사용자만이 알고 있는 정보를 확인함으로써 신원을 인증하는 방식으로, 패스워드와 비밀번호가 대표적인 예라고 할 수 있다. 하지만 이 방식은 정보가 쉽게 망각, 노출, 추측될 수 있다는 단점을 지니고 있다.

② 소유기반 인증은 그 사용자만이 소유하고 있는 소유물을 확인함으로써 신원을 인증하는 방식으로, 신분증, 신용카드, 보안카드 등이 대표적인 예라고 할 수 있다. 하지만 이 방식은 소유물이 분실, 도난, 복제될 수 있다는 위험성을 지니고 있다.

③ 생물학적 특징기반 인증은 그 사용자만의 생물학적 특징을 확인함으로써 신원을 인증하는 방식으로, 지문, 얼굴모양, DNA, 목소리 등이 대표적인 예라고 할 수 있다. 하지만 이 방식은 그 특징을 분석하는 과정에서 피할 수 없는 오류가 발생하는 문제점이 있다.[1]

위에서 제시한 바와 같이 일반적으로 단일의 사용자 인증 방식의 사용은 많은 문제점을 내제하고 있음을 알 수 있다. 따라서 오늘날 많은 사용자들은 비용적인 측면과 불편성을 감수 하더라도, 보다 안전한 보안 시스템을 구성하기 위하여 같은 인증 방식을 중복 사용하거나(예: 지식기반인증 방식 + 지식기반인증 방식) 서로 다른 인증 방식을 중복 사용하고 있다. (예: 지식기반 인증 방식 + 소유기반 인증 방식) 같은 방식의 중복 사용은 같은 종류의 단점이 반복된다는 문제점을 극복하지 못하므로 그 효과는 크지 않다고 할 수 있다. 따라서 그보다는 서로의 단점을 보완하는 2가지 이상의 다른 방식들을 혼합하여 다중으로 사용함으로써 서로의 단점을 보안하여 향상된 보안성을 제공하는 것이 더 좋다고 하겠다.

한 예로 기존의 텔레뱅킹(폰뱅킹)에서는 사용자(은행고객)만이 알고 있는 2가지 비밀번호(6자리의 텔레뱅킹 비밀번호 및 4자리의 계좌 비밀번호)와 그 사용자만이 소유하는 보안카드가 사용자 인을 위하여 순차적으로 이용된다. 비록 이렇게 3가지의 지식/소유기반 인증 방식을 적용하는 것은 그들 중 한두 가지를 사용하는 것보다는 안전하나 아래에 제시한 바와 같은 지식기반 인증 방식에서의 문제점과 소유기반 인증 방식에서의 문제점을 따로따로 공격할 경우 안정성이 위협 받게 된다.

[지식기반 인증 방식의 문제점]

① 사용자 개인만이 알고 있어야 하는 텔레뱅킹 비밀번호와 계좌 비밀번호는 번호입력장치의 노출로 인한 훔쳐보기가 가능하다.

② 악의 있는 제 3자는 번호입력장치에 key stroke 감지 장치를 심어놓고 필요한 정보를 알아낼 수 있다.

③ 비밀번호를 은행창구직원 혹은 심부름 해주는 대리인에게 알려주는 경우 그들이 도용해서 추후 사용할 가능성이 있다.

④ 비밀번호의 자리 수가 많지 않으므로 인한 추측이 용이하다.

[소유기반 인증 방식의 문제점]

① 사용자 개인만이 가지고 있어야 하는 보안카드는 분실한 카드를 타인이 습득하거나, 고의로 훔쳐갈 수 있는 위험성이 있다.

② 타인이 보안카드를 훔쳐서 복사해 놓고 몰래 돌려주는 위험이 있다.

오늘날 이러한 문제점들을 보안하기 위한 많은 연구가 진행되고 있는 가운데 본 논문에서는 적은 비용과 간단한 사용 방식으로 기존의 사용자 인증 시스템이 가지는 문제점을 보완하여 향상된 보안 체계를 구축 할 수 있는 시스템을 제안하고자 한다.

III. 제안하는 사용자 인증 시스템

1. 제안 시스템의 구성

본 논문에서 제안하는 사용자 인증 시스템은 크게 사용자 및 서버로 구성 된다.

사용자는 그 사용자만이 알고 있는 비밀번호를 생성하여 서버에 등록하는 주체로서, 서버가 사용자 사전 등록 단계에서 발급한 보안카드를 소유하며, 변동비밀번호 생성을 위한 산술 연산을 수행한다.

서버는 보안카드의 생성 및 발급을 담당하며, 전송된 변동비밀번호의 유효성 검사를 통한 사용자 인증을 수행한다. 또한 서버는 개인인증 DB를 안전하게 관리하며, 거래 승인을 위한 보안 등급을 결정한다. (사용자 인증을 위해 서버가 발급한 모든 보안카드는 같을 확률이 매우 작은 것으로 생각한다.)

2. 사용자 인증을 위한 절차

사용자 인증을 위한 절차는 사용자 사전 등록 단계와 (거래 승인을 위한)실시간 사용자 인증 단계로 나누어진다.

[사용자 사전 등록 단계]

① 사용자 U는 비밀번호 P_U를 임의로 생성하여 기억한다.

② U는 서버 S에게 자신의 ID인 ID_U와 P_U를 전달한다. 여기서 P_U의 전달은 안전하게 이루어져야 한다.

③ S는 ID_U를 갖는 U의 신원을 확인한다.

④ S는 U의 ID_U와 함께 보안카드 F_U의 식별번호 IF_U와 $h(P_U, ID_U, IF_U, 부가정보)$를 안전한 개인인증 DB에 보관하고, P_U는 안전하게 파기한다. 여기서 h는 공개되어도 상관없는 일방향 함수이고 부가정보는 사용자 별로 고정된 값이다. S는 IF_U로부터 유일한 F_U를 만들 수 있고 그 방법은 공개되지 않는다. F_U는 일정 범위내의 코드번호 N이 주어지면 N에 해당되는 코드숫자 C_{UN}을 찾을 수 있는 코드표이다.

⑤ S는 F_U를 U에게 안전하게 전달한다.

[실시간 사용자 인증 단계]

① U가 S에게 ID_U을 보낸다.

② S는 일정 범위내의 N을 임의로 생성하여 U에게 보낸다.

③ U는 F_U에서 N에 해당하는 C_{UN}을 찾는다.

④ U는 P_U와 C_{UN} 이용하여 산술 연산 방법 O로 통해 변동비밀번호 T_{UN}을 구한다.

⑤ U는 S에게 T_{UN}을 보낸다.

⑥ S는 개인인증 DB에서 U의 ID_U를 이용하여 IF_U와 $h(P_U, ID_U, IF_U, 부가정보)$를 찾아낸다.

⑦ S는 N과 IF_U로부터 C_{UN}을 계산한다.

⑧ S는 O와 C_{UN}을 이용하여 T_{UN}으로부터 P_U를 계산한다.

⑨ S는 계산한 P_U와 U로부터 받은 ID_U, 개인인증 DB에서 찾아낸 IF_U, 부가정보를 h에 넣은 결과와, 개인인증 DB에서 찾아낸 $h(P_U, ID_U, IF_U, 부가정보)$를 비교하여 같으면 그 사용자가 U임을 인증하고, P_U는 안전하게 파기한다.

⑩ 비교 결과가 틀리면, 틀린 횟수를 확인하고 그 횟수가 제한 범위를 넘으면 인증이 되지 않은 것으로 결론을 내리고, 그 횟수가 제한범위를 넘지 않으면 단계 ②로 돌아간다.

실시간 사용자 인증 단계에서 서버와 사용자는 미리 정해진 고정된 산술 연산 방법을 사용하는 대신 서버는 단계 ②에서 보안 등급에 따라 매번 다른 산술 연산 방법을 임의로 선택하여 사용자에게 보내어 사용하게 함으로써 보안성을 강화시킬 수 있다.

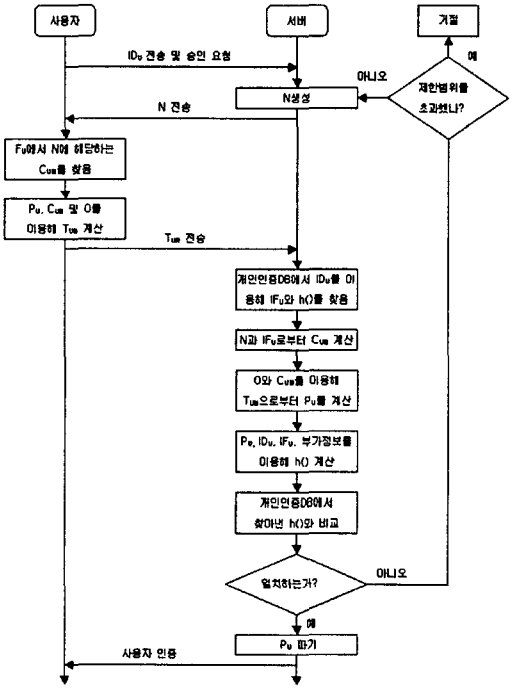

그림 1 : 제안 시스템의 흐름도

서버는 다양한 사용자의 요구와 인증 방식의 다양성을 위해 보안카드의 소유 대신 사용자가 휴대폰을 소유하고 있다는 것을 이용하여 사용자 인증을 수행할 수 있다.

아래에서는 휴대폰을 이용하는 경우의 사용자 인증 시스템의 동작 과정을 설명한다.

[사용자 사전 등록 단계]

① 사용자 U는 비밀번호 P_U를 임의로 생성하여 기억한다.

② U는 서버 S에게 자신의 ID인 ID_U와 P_U 및 휴대폰 번호 M_N을 전달한다. 여기서 P_U의 전달은 안전하게 이루어져야 한다.

③ S는 ID_U를 갖는 U의 신원을 확인한다.

④ S는 U의 ID_U와 함께 사용자의 휴대폰 번호 M_N와 $h(P_U, ID_U, M_N,$ 부가정보)를 안전한 개인인증 DB에 보관하고, P_U는 안전하게 파기한다.

[실시간 사용자 인증 단계]

① U가 S에게 ID_U을 보낸다.

② S는 인증코드 C_U를 임의로 생성하여 U의 휴대폰으로 전달한다.

③ U는 P_U와 C_U를 이용하여 산술 연산 방법 O를 통해 변동비밀번호 T_{UN}을 구한다.

④ U는 S에게 T_{UN}을 보낸다.

⑤ S는 O와 C_U를 이용하여 T_{UN}으로부터 P_U를 계산한다.

⑥ S는 계산한 P_U와 U로부터 받은 ID_U, 사용자의 휴대폰 번호 M_N, 부가정보를 h에 넣은 결과와, 개인인증 DB에서 찾아낸 $h(P_U, ID_U, M_N,$ 부가정보)를 비교하여 같으면 그 사용자가 U임을 인증하고, P_U는 안전하게 파기한다.

⑦ 비교 결과가 틀리면, 틀린 횟수를 확인하고 그 횟수가 제한 범위를 넘으면 인증이 되지 않은 것으로 결론을 내리고, 그 횟수가 제한범위를 넘지 않으면 단계 ②로 돌아간다.

보안카드를 이용하는 경우와 마찬가지로 실시간 사용자 인증 단계에서 서버와 사용자는 미리 정해진 고정된 산술 연산 방법을 사용하는 대신 서버는 단계 ②에서 보안 등급에 따라 매번 다른 산술 연산 방법을 임의로 선택하여 사용자의 휴대폰으로 보내어 사용하게 함으로써 보안성을 강화시킬 수 있다.

3. 산술 연산 방법

실시간 사용자 인증 단계에서 사용되는 산술 연산 방법은 사용자가 계산을 위한 보조 기구의 도움 없이도 쉽게 계산을 수행하여 그 결과를 산출할 수 있는 연산이어야 한다.

변동비밀번호의 계산을 위해 사용되는 산술 연산은 연산의 계산 복잡도에 따라 인증을 위한 보안 등급을 결정짓는다. 아래는 산술 연산의 복잡도를 결정짓는 요소이다.

① 사용자가 연산을 위해 기억해야 하는 비밀번호의 숫자 수.

② 사용자가 연산을 위해 필요로 하는 보안카드(휴대폰) 코드숫자의 숫자 수.

③ 산술 연산식의 어려움.

(서버는 사용자의 편리성과 보안성의 균형을 맞추기 위하여 보안카드의 사용 없이 비밀번호 하나만을 입력하는 방법을 가장 낮은 보안 등급으로 사용할 수 있다.)

보다 높은 보안 등급은 보다 어려운 산술 연산의 복잡도를 가지기 때문에 사용자의 불편을 초래할 수 있다. 따라서 사용자와 서버는 보안 등급을 신중하게 결정하여 사용하여야 한다.

다음은 변동비밀번호의 생성을 위해 사용 가능한 산술 연산의 예들이다.

가. 비밀번호와 보안카드의 코드숫자를 사용하는 산술 연산의 예

(A) 비밀번호(9371)와 보안카드 코드숫자(3864)에 대하여 같은 자리별 덧셈을 수행한 후, 각 덧셈 결과에 *mod*10을 하는 연산.

(9+3)=12 *mod*10=2, (3+8)=11 *mod*10=1,

(7+6)=13 *mod*10=3, (1+4)=5 *mod*10=5

→ 변동비밀번호 : 2135

(B) 비밀번호(9371)의 각 자리 수에 대해 보안카드 코드숫자의 특정 자리 수(3) 하나만을 사용하여 각각 덧셈을 수행한 후, 각 덧셈 결과에 *mod*10을 하는 연산.

(9+3)=12 *mod*10=2, (3+3)=6 *mod*10=6,

(7+3)=10 *mod*10=0, (1+3)=4 *mod*10=4

→ 변동비밀번호 : 2604

나. 비밀번호와 인증코드를 사용하는 산술 연산의 예

· 휴대폰의 인증코드는 알파벳을 포함하여 구성될 수 있다. 알파벳과 숫자의 연산은 알파벳을 숫자만큼 순환 이동하는 연산을 적용한다. 예를 들어 알파벳 a에 3을 더하는 연산은 a를 오른쪽으로 3번 이동한(a -> b -> c -> d) d가 연산의 결과가 되는 것이다. 따라서 숫자와 알파벳이 혼합된 인증코드를 사용한 산술 연산의 경우, 인증코드의 숫자에 대해서는 비밀번호와 보안카드를 사용하는 경우와 동일한 방식으로, 인증코드의 알파벳에 대해서는 인증코드의 숫자만큼 순환 이동하는 연산을 수행하도록 한다.

(A) 휴대폰의 인증코드(9A7Z)와 비밀번호(3864)에 대하여 같은 자리별 덧셈을 수행한 후, 숫자간의 덧셈 결과엔 *mod*10을, 숫자와 알파벳의 덧셈은 순환 이동 방식을 사용하는 연산.

(9+3)=12 *mod*10=2, (A+8)=A>>>8=I,

(7+6)=13 *mod*10=3, (Z+4)=Z>>>4=D

→ 변동비밀번호 : 2I3D

위의 예들은 변동비밀번호를 생성하기 위해 사용 가능한 단지 몇 가지의 산술 연산 방법을 제시한 것이다. 서버는 산술연산 방법의 난이도와 사용자의 편리성, 보안 등급에 따라 다양한 산술 연산 방법을 적용하여 시스템을 구성할 수 있다.

4. 제안 방식의 효율성

본 논문에서 제안하는 사용자 인증 방식은 다음과 같은 효율성을 가진다.

① 공격자는 사용자의 비밀번호, 보안카드의 코드숫자, 사용된 산술 연산 방식 모두를 알아야만 공격 가능하므로 기존의 시스템보다 강화된 보안성을 제공한다.

② 서버는 지식기반 인증 방식의 비밀번호와 소유기반 인증 방식의 보안카드를 순차적으로 두 번 확인하는 대신 한번에 확인함으로써 효율성이 증대된다.

③ 사용자의 비밀번호와 보안카드의 노출 가능성이 감소하기 때문에 보다 안전한 비밀번호 사용 체계를 구축 할 수 있다.

④ 텔레뱅킹(폰뱅킹), 인터넷(PC)뱅킹, 증권 매매, 전자 결재 등과 같은 현재 사용되고 있는 비밀번호를 이용한 사용자 인증 시스템을 아주 조금만 수정함으로써 보안성을 강화 시킬 수 있다.

⑤ 적은 추가 비용만으로 사용자 인증 시스템을 보완할 수 있으며, 간단한 사용 방식으로 인해 다양한 응용이 가능하다.

이렇듯 본 논문에서 제안하는 사용자 인증 시스템은 사용자 인증을 위해 지식기반 인증과 소유기반 인증을 순차적으로 2회 사용함으로써 제기되는 비밀번호의 노출, 추측과 보안카드의 분실, 습득, 복제 등과 같은 기존 방법의 단점을 보완하여, 지식과 소유를 통합하여 동시에 확인함으로써 기존의 비밀번호를 이용한 사용자 인증 시스템을 보완하여 보다 안전한 시스템을 구현할 수 있다.

5. 제안 시스템의 고려사항

가. 보안카드의 습득, 복제에 의한 변동비밀번호 공격

보안카드를 습득 또는 복제하고 있는 악의 있는 제 3자가 제안된 방식의 변동비밀번호 두 개를 획득하였을 경우 사용자의 비밀번호를 알아낼 수 있다. 다음은 두개의 변동비밀번호로 사용자의 비밀번호를 알아내는 과정을 설명하고 있다.

사용자가 인증 위해 사용한 코드숫자, 비밀번호, 변동비밀번호는 다음과 같다.

· 코드숫자 : C_{UN1} = 1234, C_{UN2} = 2345,
C_{UN3} = 4019, C_{UN4} = 5881, …

· 비밀번호 P_U = 3456,

· 변동비밀번호 : $T_{UN1} = C_{UN1} + P_U$ = 4680,
$T_{UN2} = C_{UN2} + P_U$ = 5791

악의 있는 제 3자가 변동비밀번호 T_{UN1}과 T_{UN2}를 획득하였을 경우, T_{UN1}에서 각각의 C_{UN}을 뺀 값과 T_{UN2}에서 각각의 C_{UN}을 뺀 값을 비교해 봄으로써 비밀번호를 알아낼 수 있다.

· $T_{UN1} - C_{UN1}$ = **3456**, $T_{UN1} - C_{UN2}$ = 2345,
$T_{UN1} - C_{UN3}$ = 0671, $T_{UN1} - C_{UN4}$ = 9209, …

· $T_{UN2} - C_{UN1}$ = 4567, $T_{UN2} - C_{UN2}$ = **3456**,
$T_{UN2} - C_{UN3}$ = 1782, $T_{UN2} - C_{UN4}$ = 2345,…

· 일치하는 값 3456이 비밀번호

이 경우는 보안카드의 안전한 관리가 무엇보다도 중요한 요소로 작용하며, 사용자는 이를 방지하기 위해 변동비밀번호 생성을 위해 매번 다른 산술 연산 방법을 적용하여 공격이 어렵게 만들 수 있다.

나. 무차별 대입 공격

악의 있는 제 3자가 무차별 대입 공격(Brute-force attack)을 사용하여 공격할 경우, 기존의 방식은 두 인증 방식 모두에 대해 이 공격을 적용해야 하는 반면, 제안하는 방식은 변동비밀번호 하나에 대해서만 이 공격을 적용하면 된다. 하지만 현재 대부분의 인증 시스템에서는 비밀번호의 입력 횟수를 제안하고 있기 때문에 이 문제의 가능성은 배제할 수 있다.

IV. 결론

인터넷과 금융 거래의 활성화로 인해 비밀번호 및 보안카드의 사용이 날로 증가하고 있는 가운데, 기존 보안 체계의 취약성과 사용자들의 부주의로 인하여 보안사고 또한 날로 증가하고 있는 추세이다. 이러한 시점에서 본 논문에서 제안한

사용자 인증 시스템은 비밀번호 및 보안카드를 안전하게 사용할 수 있는 효율적인 방법을 제시함으로써, 기존 보안 체계의 취약성과 사용자들의 부주의로 인하여 발생하는 보안 사고를 줄여 안전한 사용자 인증 체계를 구축하여 인터넷과 금융 거래의 활성화를 촉진할 수 있을 것이다.

참고문헌

[1] Lynn M. LoPucki, "Human Identification Theory and Identity Theft Problem", *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=263213*

[2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", *CRC Press*, 1997

[3] 강경근, "인터넷에서의 개인정보보호", *대검찰청인터넷범죄수사대*, 컴퓨터 범죄 사례, 2001

[4] 박창섭, "암호 이론과 보안", *대영사*, 1999