RFID 스마트카드내 DNA STR Information과 일회용 의사난수를 사용한 다중 사용자 인증시스템

성 순 화† · 공 은 배††

요 약

본 논문에서는 DNA 생체정보와 소유자 기반의 hardware 분야인 RFID(Radio Frequency Identification) 스마트카드, 그리고 Software 인증 분야인 PKI 전자서명을 도입한 다중 사용자 인증시스템을 제시한다. 이는 현 시스템의 인가된 자의 접근 방법인 ID or password가 안전한 방법이 아니므로 논문[1]에서 제안한 사항을 다음과 같이 개선하였다. 즉, 사용자 인증 카드인 two card(the biometric registered seal card and the DNA personal ID card) 대신 하나의 RFID 스마트카드로 사용자 인증을 할 수 있고, 카드 분실시 사용자 정보 노출의 위험을 저가의 RFID로 해결한다. 또한 DNA personal ID만으로 일난성 쌍둥이, 수혈한 환자, 암세포에서 돌연변이가 발생한 경우의 사용자 인증이 어려운 경우까지 사용자 ID에 대응하는 일회용 의사난수와 DNA 정보로 사용자 인증을 해결하였다. 그러므로 현 생체 정보 사용자 인증시스템의 단점인 패턴 매칭과 패턴 비교의 에러를 정확한 digital DNA 생체정보로 안전하게 스마트카드에 저장하여 터미널에 로그온하는 local applications에 적용할 수 있다. 스마트카드내 RFID는 사용자를 관독, 추적, 관리할 수 있으므로 카드 분실시 카드 위치를 추적하고 개인 정보를 관리할 수 있으며, 어떠한 개인 DNA 정보도 노출되지 않는다. 현 PKI 전자서명의 비밀키 안전성 문제는 사용자가 시스템에 접근할 때마다 사용자 ID에 대응하는 무한에 가까운 일회용 의사난수와 DNA정보로 PKI 전자서명의 비밀키 안전성을 해결한다. 뿐만 아니라 이러한 시스템은 생체정보의 RFID 스마트카드 사용 확대 계기로, 신용카드, 신분증, 그리고 여권 등에서도 이용할 수 있다. 제시한 시스템의 안전성은 통계학적 분석으로 보여진다.

Multi User-Authentication System using One Time-Pseudo Random Number and Personal DNA STR Information in RFID Smart Card

Soon Hwa Sung† · Eun Bae Kong††

ABSTRACT

This paper suggests a multi user-authentication system comprises that DNA biometric information, owner's RFID (Radio Frequency Identification) smartcard of hardware token, and PKI digital signature of software. This system improved items proposed in [1] as follows : this mechanism provides one RFID smartcard instead of two user-authentication smartcard (the biometric registered seal card and the DNA personal ID card), and solves user information exposure as RFID of low price when the card is lost. In addition, this can be perfect multi user-authentication system to enable identification even in cases such as identical twins, the DNA collected from the blood of patient who has undergone a medical procedure involving blood replacement and the DNA of the blood donor, mutation in the DNA base of cancer cells and other cells. Therefore, the proposed system is applied to terminal log-on with RFID smart card that stores accurate digital DNA biometric information instead of present biometric user-authentication system with the errors of pattern matching and pattern comparision. RFID in smart card can manage personal information and trace the card situation when the card is lost, which doesn't expose any personal DNA information. The security of PKI digital signature private key can be improved because secure pseudo random number generator can generate infinite one-time pseudo random number corresponding to a user ID to keep private key of PKI digital signature securely whenever authenticated users access a system. In addition, this user-authentication system can be used in credit card, resident card, passport, etc. accelerating the use of biometric RFID smart card . The security of proposed system is shown by statistical analysis.

키워드 : RFID 스마트카드(RFID Smart Card), DNA STR Information, DNA Personal ID, 일회용 의사난수(One-time Pseudo Random Number), PKI 전자서명 개인키(PKI Digital Signature Private Key)

1. 서 론

인터넷 확산과 더불어 해킹 및 불법 침입 급증으로 외부에서 방화벽 시스템 및 침입 탐지 시스템을 통과한 침입 및 내부망에서 발생하는 불법 침입에 대비한 보안 대책이 필요하게 되었다. 정보보호센터는 2000년 4월부터 8개월간 접수된 국내 컴퓨터 해킹 피해 상담 1640건 중 69.8%가 개인용 PC의 해킹 피해인 것으로 집계하였으며[2], 유형별 보안사고 현황을 2000년 CSI/FBI Computer Crime & Security Survey(미국)에 의하면 내부자에 의한 정보 사고가 보안 사고의 97%에 이른다고 보고하였다[3]. 보안 사고 유형별 피

† 준 회 원 : 충남대학교 대학원 컴퓨터공학과
†† 정 회 원 : 충남대학교 컴퓨터공학과 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 9월 1일

해액은 CSI/FBI'98 Report에 의하면 비인가 내부자 접근이 가장 많았다[4].

현재, 인가된 자가 시스템에 접근하는 방법으로는 ID or Password가 대부분이다. 각자의 중요한 정보를 보호하기 위해 1인당 평균 4~5개의 ID를 소유하거나 약 10개 정도의 Password를 기억하는 등 많은 노력을 기울이고 있다. 그러나 이러한 방법은 안전한 방법이 아니다는 것을 피해 사례에서 쉽게 찾아 볼 수 있다. 이는 모든 암호 및 암호 장치는 해제 또는 도난될 수 있고 모든 잠금 장치는 해제될 수 있기 때문이다. 따라서 컴퓨터가 사용되기 수백년 전부터 절대 유일의 보안 장치를 개발하려는 노력이 진행되어 왔고 그 결과 살아있는 개별 인간의 신체 일부를 이용한 생체 인식 기술이 발달하여 오늘에 이르게 되었다. 지문인식 시스템은 땀이나 물기가 스캐너에 배어있는 경우 에러 발생률이 크게 높아진다는 점, 지문이 닳아 없어진 사람도 간혹 있다는 점 등이 지문인식 시스템의 한계로 인식하고 있다. 얼굴 인식은 입력된 화상으로부터 처리 대상인 얼굴 영역을 추출하는 방법으로 DB 상의 인상 사진과 인상 사진이 아닌 다른 사진 영상과 유효한 비교를 하기는 여전히 어렵다. 또한 눈을 이용한 생체인증에서는 홍채와 망막의 혈관이 인증을 목적으로 사용되고 있다. 그 중 망막인식은 성공적인 망막 패턴 검색을 위해서 사용자가 안경을 낀 경우 안경을 벗고 검색기에 접안해야 하며, 빛에 대한 두려움을 유발하는 등 일반인을 대상으로 사용하기는 비효율적인 면이 있다. 또한 홍채인식은 외상 또는 아주 드문 병을 제외하고는 사람의 일생 동안 변화되지 않으며 콘택트렌즈나 안경을 착용해도 인식이 가능하므로 활용범위가 넓으나 안경에 타인의 홍채 사진을 붙여 접근을 시도할 경우 망막이나 홍채 모두 인증 보안에 염두를 두어야 한다. 뿐만 아니라 이러한 생체 인증시스템은 비슷한 패턴 매칭과 형태 비교를 요구하므로 일반적 모든 시스템에 표준화된 절대적 identification을 제공하지 못한다. 이러한 점은 터미널에 로그온하는 사용자 확인과 같은 local applications에 제한을 받고 있다.

따라서 이러한 생체 인증시스템의 단점을 감안하여 본 논문은 본질적으로 digital인 각 개인의 DNA 정보를 RFID 스마트 카드에 저장하여, 사용자 인증 뿐만 아니라 카드 분실 시 위치 추적과 DNA를 포함한 개인정보의 누출을 막을 수 있는 편리성과 효율성을 제시한다. 또한 일회용 의사난수를 사용하여 PKI 전자서명의 단점인 비밀키의 안전성을 높일 수 있으며, DNA personal ID만으로 사용자를 인증할 수 없는 일난성 쌍둥이, 수혈한 환자, 암세포에서 돌연변이가 발생한 경우까지 사용자 인증시 사용자ID에 대응하는 일회용 의사난수로 사용자 인증이 가능하다. 본 논문은 다단계 사용자 인증시스템인 DNA 생체정보와 RFID 스마트카드, 그리고 PKI 전자서명을 사용한 다중 사용자 인증방식을 제시한다. 논문 구성은 2장에서는 DNA 정보수집에서 DNA personal ID 생성과정과 RFID 스마트카드에 대하여 기술하고, 3장에서는 PKI 전자서명 개인키의 안전성을 높이기 위한 안전한 의사난수 발생기, 4장에서는 제시한 다중 사용자 인증시스템, 그리고 5장 결론으로 이루어진다.

2. 관련 연구

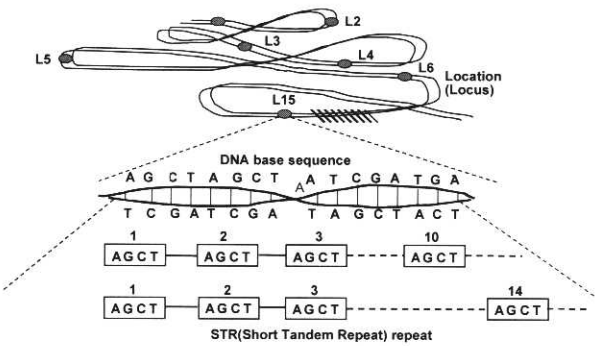
2.1 DNA 정보수집

망막 스캔, 얼굴 인식, 지문, 그리고 handwriting 등 비슷한 패턴 매칭과 형태 비교를 요구하는 이러한 방법은 일반적으로 모든 시스템에 표준화된 절대적 identification을 제공하지 못한다. 이러한 것은 터미널에 로그온하는 사용자 확인과 같은 local applications에 제한을 받고 있다. 반면, biometric information의 여러 가지 형태중 DNA information은 수집하고 분석하기가 더 어려운 것 중 하나이다. 또한 privacy issue 때문에 biometric verification의 요소로 DNA 정보 사용은 인증과 같은 application에 아주 제한되어 왔다. 그럼에도 불구하고 DNA information은 본질적으로 digital이고 STR(Short Tandem Repeat)이 모인 locations 수를 증가시킴으로써 identification 정확성이 증가될 수 있기 때문에 지문과 망막 스캔에서 가능하지 않은 potential applications을 가진다.

인간의 몸은 약 50조 cells로 이루어져 있다. 전체 DNA sequence가 손상되지 않는다면 2개의 나선구조를 가진 약 1.5m의 band를 형성한다. 이 나선구조 위에는 4종류의 bases A, G, C and T(the first letters of the chemical names Adenine, Guanine, Cytosine, and Thymine)가 배열되어 있다[5].

DNA는 약 30억 characters의 정보를 가지고 있으며 이 정보는 인간 프로테인을 위한 template 디자인 역할을 한다. (그림 1)은 DNA의 STR information을 나타낸다.

DNA 나선 구조의 base sequences중 STR(Short Tandem Repeat)이라고 불리우는 locations(loci)는 짧은 base sequences의 반복이고, 이 반복 수 혹은 반복 카운트는 각각 확실히 다르다[1].



(그림 1) The STR information of DNA

2.2 DNA personal ID 생성 과정

DNA personal ID α_A는 STR 카운트를 가르키는 pairs 값을 sequence함으로써 생성된다. 이는 multiple loci로부터 모아진다[6].

Step 1 : 각 locus에서 STR 카운트가 측정된다.

Step 2 : 각 locus에서 얻어진 STR 카운트 값은 ascending order에서 sequence된다.

$$L : j \,||\, k, \qquad j \le k$$

측정에 의해 같은 사람의 같은 STR 카운트는 (j, k) 혹은 (k, j)로 나타난다. 그러므로 j와 k는 두 경우에서 ascending order에서 sequence된다. 이는 (j, k | j ≤ k)을 사용하여 그 사람과 일대일로 일치함을 계산하기 위함이다. 이 과정은 sequencing operation으로 인용된다.

Step 3 : DNA personal ID α_A는 다음과 같은 $L_i(j, k)$ sequence에 관해 생성된다.

$$\alpha_A = L_1 || L_2 || L_3 || \cdots || L_n$$

L_i는 i 번째 STR 카운트(j, k)를 가르킨다.

생성된 α_A는 어떤 확률에서 유일한 personal identification information이 된다.

또한 DNA personal ID 매칭 확률은 STR counts의 빈도 분산의 major points의 수가 증가할 수록 감소한다는 것을 실험 결과로 얻었고, locus multiplicity가 증가할수록 동일한 DNA personal IDs number가 감소된다는 실험 결과를 얻었다[1].

따라서 되도록이면 locus multiplicity를 증가시킴으로써 각 개인의 유일한 DNA personal ID를 얻을 수 있다. 그러므로 본 논문은 스마트카드에 허용된 용량의 최대 locus multiplicity를 수용하기 위해 해쉬함수를 사용하여 DNA personal ID α_A의 해쉬값 δ_A를 생성한다.

DNA personal ID는 동일한 쌍둥이, 수혈 받은 환자로부터 모아진 DNA, 암세포와 다른 세포의 DNA 돌연변이가 발생될 경우에는 추가적인 측정이 필요하다. 이러한 예외적인 경우까지 포함한 정확한 사용자 인증의 가능한 접근은 수학적 처리과정를 적용함으로써 DNA information를 사용하여야 한다[7].

그래서 본 논문은 예외적인 경우를 포함한 안전한 DNA personal ID의 가능한 접근을 수학적 처리 과정으로 DNA information을 적용시키려고 한다. 이러한 접근은 아주 극소수의 DNA personal IDs 매칭을 구별하기 위해 전체 시스템에 더해져야 한다.

2.3 DNA personal ID mapping

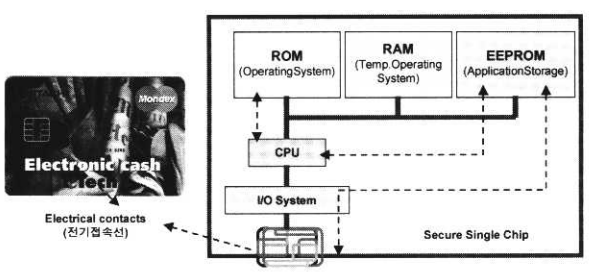
생성된 DNA personal ID는 α_A로 표시한다. 이 α_A에 적용된 hash function 처리 결과는 δ_A로 표시한다.

$$\delta_A = h(\alpha_A)$$

Secure Hash Algorithm(SHA-1)[8]은 일방향 hash function의 일반 목적이고 h에 대해 사용되어진다. α_A는 n(STR multiplicity) = 15일 때 약 10^{50} -bit size의 정보가 되고, n = 30일때 약 10^{100} - bit 정보가 된다. SHA-1는 입력이 2^{64} bits 보다 작은 bit string일 때 160 - bit message digest를 출력하는 one-directional functional computation을 구성하기 때문에 이 hash function 알고리즘을 사용할 수 있다. 이때 h는 public으로 δ_A의 일반성을 보장함으로 같은 사람의 δ_A은 그 사람의 DNA가 어디에서 모아지든 상관없이 같은 값을 가진다는 것을 말한다[1].

2.4 Smart Card

Smart card는 저장된 비밀정보를 통한 사용자 인증 정보를 생성하여 수신측에서는 수신한 정보를 기반으로 사용자 인증을 한다. PSE(Personal Security Environment)의 최종 목표로 다양한 비밀 정보 보관 등을 통한 다용도로 사용 가능하며, 매체에 대한 다양한 국제적인 기술 표준화가 진행되고 있다. 이러한 스마트카드의 외양 및 내부 구조는 (그림 2)에서 볼 수 있다. 일반적인 스마트카드는 외부로부터의 파손을 통한 내부 데이터의 복제 방지를 위한 장치(파손시 내부 데이터의 소멸 등)가 되어 있다. 또한 스마트카드 내부의 EEPROM(Electrically erasable & programmable ROM)에 공개키나 개인키 등의 데이터를 저장할 수 있다. 최근 삼성전자의 스마트카드 IC는 64k바이트의 대용량 EEPROM, ARM사의 32비트 보안용 프로세서 SC100, 첨단 암호화 프로세서를 내장, 전자상거래, 신용카드, 전자화폐 등에서 요구되는 RSA, DSS(Digital Signature Standard) 전자서명 기능 등을 최단 시간에 실행할 수 있다[9]. 본 논문에서는 접촉식 스마트카드와 비접촉식 RFID 카드의 성능을 조합한 combi 카드를 사용한다.



(그림 2) 스마트카드 내부 Microprocessor

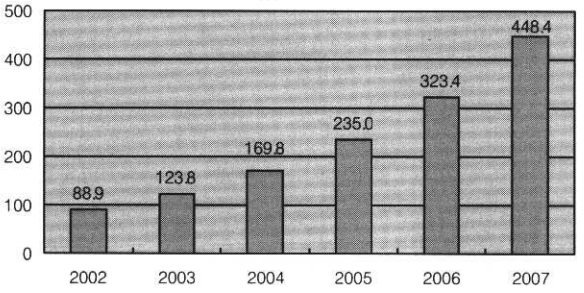
2.5 RFID(Radio Frequency Identification)

송수신 주파수를 이용한 RFID는 DSRC(Dedicated Short Range Communication)라고도 하는 무선 식별을 말한다. 초소형 반도체에 식별 경보를 입력, 주파수를 이용해 이 칩을 지닌 물체나 동물, 사람등을 판독, 추적, 관리할 수 있는 기술로 유비쿼터스 컴퓨팅 기반기술의 하나로 꼽히며, 유통분야에서 현재의 바코드를 대체하는 것을 비롯해 물류, 교통, 보안, 가전분야로 적용이 확대될 것이다. 전국적으로 구축돼 있는 CDMA(Code Division Multiple Access)망과 RFID 시스템을 연계하는 네트워크 구축 움직임이 있을 전망이다.

RFID는 물체나 동물 또는 사람 등을 식별하기 위해 전

자기 스팩트럼 부분의 무선 주파수내에 전자기 또는 정전기 커플링 사용을 통합시킨 기술이다. 이는 바코드를 대체할 기술로서 산업계에서의 사용이 점차 늘고 있다. 장점은 직접 접촉을 하거나 가시대역 상에 스캐닝 할 필요가 없으며, line-of-sight 판독에 대한 제한이 없고, 바코드 라벨이 찌져지거나 쉽게 손상될 수 있는 것에 비해 튼튼하다. 그리고 바코드는 정보를 일단 입력하면 다시 입력할 수 없으며, 입력할 수 있는 정보량도 한정된 것(1D 바코드경우 : 10~20자, 2D 바코드경우 : 100~3000자)에 비해 RFID는 정보를 다시 입력할 수 있어 정보 저장 능력이 확장되어 있다. 또한 RFID 시스템은 다양한 기능 제공으로 읽고, 쓰기가 가능한 RFID 태그가 휴대 가능한 DB 역할을 하며, 판독기 접근이 가능한 모든 지점에서 입력된 정보에 대한 수신 및 수정이 가능하다. 즉 RFID 태그를 가지고 있는 우편물은 수집 및 운송지점에서의 처리된 시간을 확인할 수 있으며 이렇게 획득한 정보는 기본적인 서비스 측정 작업에 사용되어 질 수 있다. RFID 시스템은 안테나, 트랜시버, 그리고 트랜스폰더라고 불리는 3가지 요소로 구성된다[10]. 따라서 RFID는 제시한 스마트카드에 장착되어 휴대 가능한 DB 역할로 사용자 DNA 정보의 판독, 추적, 관리를 할 수 있다.

Exhibit 1
Global Shipments of RFID Hardware to Support Supply Chain Management Applications (Millions of Dollars)



Source : Venture Development

(그림 3) Global Shipments of RFID Hardware(Millions of Dollars)

3. 의사난수 발생기

3.1 의사난수 발생기 개요

정보보호 시스템에서 기밀성과 인증성 기능이 실현되기 위하여 암호 알고리즘 입력기 생성과 시스템 변수 생성, random challenge 등에 활용할 수 있는 난수 발생기가 적용되어야 한다. 난수 발생기는 정보보호 시스템이 갖추어야 할 기본적인 요소이며, 수학적인 논리에 의하여 안전성이 증명 가능하도록 설계되어야 한다.

난수는 그것이 생성되기 전에 예측할 수 없는 수이다. 어떤 수가 $0, \cdots, 2^n-1$ 사이의 난수라고 가정하면 2^{-n}의 확률보다 높은 확률로 난수를 예측할 수 없다. 뿐만 아니라 m개의 난수가 생성되어 있고, m-1개의 난수에 대하여 알고 있다고 하더라도, m번째 수도 역시 2^{-n}의 확률보다 높은 확률로 m번째 수를 예측할 수 없어야 한다. 그러나 이러한 참난수(True random number)를 발생하는 것은 현실적으로 불가능해서 난수와 구별하기 어려운 의사난수(Pseudo random number)를 생성하여 난수로 사용한다. 의사난수란 난수와 구별할 수 있는 효율적인 알고리즘이 존재하지 않는 수를 의미한다[11].

3.2 의사난수 발생기의 문제점

컴퓨터 난수의 경우 각 원소들의 최대/최소 값을 임의로 한정시킬 수 있다. 각 수가 0~255로 구성되고 곧 k = 256이라 할 경우 그 수들 n개 중에서 또한 n이 무한히 커질 때 수 0의 개수는 n/k에 수렴한다. 즉 정 256각형의 주사위형 연필을 n번 굴릴 때 순서대로 나오는 수들과 같이 빈도수에 있어 거의 균일한 수열을 난수(random number)라 한다. 보기엔 어떤 규칙도 없이 엄격한 순서에 따라 나열되지만 그것은 어느 한값에 의해 초기화되어 발생된다. 곧 10개의 난수를 출력하라고 컴퓨터에 지시하면 8, 3, 1, 6, 0, 4, 2, 9, 5, 7 등으로 출력하는데 난수 생성 전에 고의로 특정하게 초기화시키면 그에 따라 언제라도 똑같은 차례의 난수가 발생되는 성질을 가지고 있다. 바로 난수 초기화값(seed)이 고정되면 발생되는 난수는 언제나 동일한 내용과 발생 순서를 가진다. 이것이 컴퓨터 난수의 특징 곧 재현성이다. 난수의 성질을 지녔으면서도 재현성에 있어 비난수적인 즉 규칙적인 난수라 해서 의사(pseudo)난수라 한다. 프로그래밍 언어 C나 C++에서는 난수를 초기화시키는데 srand(seed)(seed 값은 unsigned int 곧, 0~65535)명령을 쓰고, 난수를 실제 발생시키는 데는 rand( ) (정수 0~32767가 발생)를 쓴다. 난수 '100'으로 초기화해 10개의 난수를 출력하라는 컴파일 가능한 프로그램 코드는 아래와 같다.

```
# include < stdio.h >
# include < stdlib.h >
main( )
{
char again ;
srand(100) ;
for (again = 0 ;  again  <  10 ; again++)
        printf("%d", rand( )) ;
}
```

결과 값은 1862, 11548, 3973, 4846, 9095, 16503, 6335, 13684, 21357, 21505이다.

이것은 항상 동일한 난수를 출력한다. 프로그램 중 srand(100)가 난수를 '100'으로 고정 초기화시키기 때문이다. 즉 초기화됐으면 그것으로 종속된 난수들이 발생되어 난수들과 그 초기 값은 한 짝이 된다.

그러므로 y(n)는 각각 5개의 난수를 원소로 하는 집합의 집합이고 x(n)은 난수군 y(n)의 초기화 값(seed)들의 집합이면,

y(0) = {1, 12, 41, 65, 83}
y(1) = {123, 101, 82, 32, 5}
…
y(n-1) = {4, 24, 46, 51, 7}
y(n) = {난수 1, 난수 2, 난수 3, 난수 4, 난수 5}

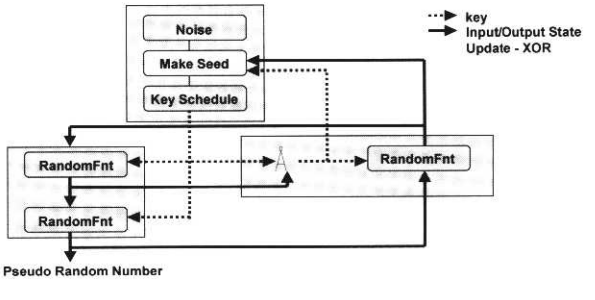
x(0) = y(0)의 초기화 값(seed)
x(1) = y(1)의 seed
…
x(n-1) = y(n-1)의 seed
x(n) = y(n)의 seed

처럼 일대일(1 : 1)로 대응하며, x(a) = y(b)의 seed일 경우 a = b이고 이것을 만족하는 b는 하나만 존재한다. 따라서 모든 y(y(0), y(1), …, y(n-1), y(n))는 각각 서로 다르다. 또한 x(n)는 y(n)을 위해 키로서 다루어진다. 이 경우 y(n) 각각은 발생된 난수를 한데 모아 놓은 배열로서 일종의 난수표이다. y(n)의 개수 곧, n + 1의 값은 256의 1536제곱이다. 이중에서 한 개를 취해 문서를 암호화하고 복호화하는 것이다. 일종의 일대일 함수 관계로 함수 y = f(x)에서 f(x)는 키 x에 의한 특수식이 된다.

f("키") = 특수함수("키")에서 특수함수에 키 하나를 입력하면 일대일 대응 법칙에 따라 꼭 하나의 특수함수 값이 생성된다. a = 키 1, b = 키 2일 경우 두 함수 값이 f(a) = f(b)라면 a, b는 서로 같고, a≠b이면서 f(a) = f(b)인 a, b는 없다. 또한 단방향(one-way) 함수이므로 f(a) 값으로부터 a를 구하지는 못한다. 여기서의 특수함수 값은 키에 의해 만들어진 한 개의 정수값이 아니고 수만, 수십만개의 난수(0~255)로 이루어진 한 개의 집합이다. 이때 특수함수는 난수를 초기화하는 값을 거의 무한대로 확장하기 위해서이다. 즉 srand(100)에서 "100"이 키의 역할을 한다. 난수를 초기화하는 값의 범위가 크면 클수록 안전성이 비례하여 커진다. 난수 초기값 srand(x)의 x는 unsigned int형으로 100,000을 넘지 못한다. 따라서 암호화의 안전성을 확장하는데 장애가 되고 있다.

3.3 일회용 의사난수 생성을 위한 안전한 의사난수 발생기

인증 알고리즘에서 요구되는 의사난수 생성기는 하드웨어로 의사난수를 생성하기보다는 소프트웨어로 구현되는 것이



(그림 4) 안전한 의사난수 발생기 구조

더 적합하다[12-14]. 따라서 키의 안전성 확장을 위한 블록 암호 알고리즘을 기반으로한 램덤함수를 사용한 안전한 의사난수 발생기를 도입한다[16].

도입된 의사난수 발생기는 3개의 알고리즘으로 이루어진다. 잡음정보로부터 생성한 seed를 새롭게 갱신시키는 re-seeding 알고리즘과 seed로부터 의사 난수를 생성하는 램덤화 알고리즘이며, 램덤화 알고리즘의 입력 값을 새롭게 갱신시키는 업데이트 알고리즘이다.

① Reseeding 알고리즘은 잡음 정보로부터 seed를 생성하는 알고리즘과 seed를 이용해서 키를 생성하는 알고리즘으로 구성된다. 즉 seed 생성 알고리즘과 키 생성 알고리즘으로 구성된다.

$$(noise \| state) = (I1 \| I2 \| I3 \| I4)$$
$$(O1 \| O2) = RandomFnt(I1 \| I2, key)$$
$$(O3 \| O4) = RandomFnt(I2 \oplus O2 \| I3, key)$$
$$(O5 \| O6) = RandomFnt(I3 \oplus O4 \| I4, key)$$

② 램덤화 알고리즘은 의사난수 발생기에 대한 여러 공격에 안전하게 하기 위하여, RandomFnt함수를 두 번 반복하여서 의사난수를 생성하도록 한다.

$$Rand1 = RandomFnt(state, key)$$
$$Rand2 = RandomFnt(Rand1, key)$$

Rand2가 출력되는 의사난수이고, Rand1은 업데이트 알고리즘의 입력으로 사용된다.

③ 업데이트 알고리즘에서는 램덤화 알고리즘의 출력값을 이용하므로 Rand2는 생성된 의사난수로 사용될 값이나 공격자에게 쉽게 노출될 수 있다. 만일 키도 새롭게 업데이트 되지 않고 공격자에게 노출된다면, RandomFnt 함수가 역으로 계산될 수 있게 된다. 그러므로 난수를 생성한 후 키와 state를 제외한 모든 내부 변수들은 모두 0으로 초기화 시켜야 하며, 키는 새롭게 업데이트 하여야 한다. 기호로 표시된 Update-XOR 연산은 키를 각 라운드에 사용되는 128비트씩 128비트 Rand1과 XOR 하는 것이다. 이러한 과정으로 키는 업데이트되며, 업데이트된 키와 Rand2를 RandomFunt함수의 입력으로 한 결과로 입력(state)을 업데이트시킨다.

$$Key = keyoutput1$$
$$State = RandomFnt(Rand2, key)$$

이러한 의사난수 발생기는 내부함수 RandomFnt이 차분공격, 선형 근사 공격과 같은 암호 분석에 안전하며, 전체적인 구조는 선택 평문 공격, 기지 출력 공격 등과 같이 기존에 알려진 공격들에 안전하도록 설계되었다. 또한 생성된 의사난수 수열의 난수성을 알아보기 위해 189개의 통계적 난수 검정을 시행하여 미국 AES(Advanced Encryption Standard)[15] 선정 기준 중 하나인 난수성 평가 기준으로 제시한 모든 기준을 통과한 안전한 의사난수 발생기이다[16].

4. Proposed user-authentication system

현 인증 메커니즘은 단일 인증 메커니즘에서 다중 인증 메커니즘 조합 사용을 통한 강한 인증을 요구한다. 그 종류로는 PIN + PKI 인증서, 스마트 카드 + PKI 인증서, 생체 인식 + PKI 인증서 등이 있다. 본 논문은 다중 사용자 인증메커니즘을 통한 강한 사용자 인증시스템으로 생체 인증 분야의 DNA와 소유기반의 Hardware token 분야의 RFID 스마트 카드(IC Card), 그리고 Software 인증 분야인 PKI 전자서명의 다단계 사용자 인증시스템을 제안한다.

4.1 DNA biometric signing

현재 많이 사용되고 있는 애매한 측정으로 아날로그 표현을 나타내는 지문과는 달리 DNA personal ID는 본질적으로 확실성을 가지는 디지털 정보이다. 따라서 2.3절에서 언급한 DNA personal ID인 α_A를 해쉉한 δ_A를 key pair로 전자서명하여 information security system에서 identifier로 사용할 수 있다. 전자서명용 key pair는 전자서명 즉 송신할 원문의 다이제스트를 암호화하는데 사용할 사용자의 개인키와 공개키를 뜻한다.

Hash function을 사용하여 private information DNA personal ID인 α_A를 private하게 유지한다는 것은 그 역함수 값을 나타낼 수 없다는 점에서는 안전하나, DNA는 사람의 신체에서 쉽게 체취하거나 훔칠 수 있어 α_A를 분석할 수 있다. 따라서 DNA personal ID인 α_A를 private하게 유지하기 위해서 해쉉한 δ_A를 key pair로 전자서명하여 private를 유지시킨다. 즉 private key로 δ_A를 암호화하고 public key를 생성하여 Certification Agency(CA)에 등록한다. 이렇게 biometric personal authentication과 biometric signing은 다음과 같은 구체적이 방법으로 구성된다.

- Secret key : X_A 2^{160}(bit string of about 160 bits)
- Secret key generation method : $X_A = \delta_A + r_A$
- Person's secret random number : r_A(개인 ID에 대응하는 안전한 의사난수 발생기에서 발생한 값)

r_A는 등록 터미널에서 개인 ID를 입력하면 이에 대응하는 안전한 의사난수 발생기에서 발생한 값이다. Biometric information α_A는 훔친 다른 사람의 DNA일 수도 있으므로 해쉉한 δ_A를 key pair로 전자서명하여 CA에 등록할 때, 전자서명의 개인키가 안전성이 있어야 한다.

따라서 안전성이 높은 개인키를 얻기 위해서 사용자는 사용자 인증시마다 ID를 입력하면 이에 대응하는 안전한 의사난수 발생기에서 생성한 값 r_A를 선택하여 해쉉한 δ_A과 함께 안전성을 부여한 개인키를 생성한다. 이때 ID는 유효기간을 두어 변경할 수 있으며 기억할 수 없을시 CA에 일정 절차를 거쳐 확인할 수 있다. 따라서 지금 사용하고 있는 단순 ID만으로 사용자를 인증하는 메커니즘보다 복합적인 메커니즘으로 안전성 절차를 다단계로 확인할 수 있는 계기를 마련한다.

- Public key : Y_A
- Public key generation method : $Y_A = g^{XA} (\mathrm{mod}\ p)$
- p : a large prime number
  g : a source element of order p
- Registration with a CA : registers Y_A, g^{rA}, p, g, personal information(사용자 ID 등)

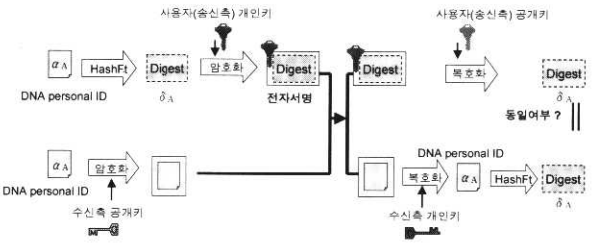
Public key Y_A , g^{rA}, p, g, personal information는 CA에 등록이 되어 CA가 관리한다.

DNA personal ID만으로 일난성 쌍둥이, 수혈한 환자, 암세포에서 돌연변이가 발생한 경우의 사용자 인증이 어렵다. 제시한 시스템은 이와 같은 특별한 사용자 인증까지 포함한다.

따라서 본 논문은 DNA personal ID의 해쉉한 α_A 값을 안전한 의사난수 발생기에서 생성한 secrete random number (r_A)로 구성된 비밀키 $X_A = \delta_A + r_A$로 sign하여 스마트카드에 저장한다. 이때 r_A는 사용자 인증시 마다 r_A가 unlock되어 사용자 인증시 다른 난수(1회용 난수)를 사용하여 sign함으로 안전성을 더해 준다. 즉 사용자 인증시 마다 변하는 r_A에 따라 DNA 정보가 안전하게 사용자 인증에 사용된다. 그러므로 r_A가 사용자 인증 안전성에 많은 영향을 미친다.

4.2 δ_A를 key pair로 전자서명

Biometric signing은 스마트카드를 사용한 PKI 전자서명으로 실행된다. DNA personal ID는 해쉉되어 δ_A를 생성하여 생성된 δ_A를 다시 비밀키인 $X_A = \delta_A + r_A$로 암호화하여 사용자 ID와 함께 저장된다. 이때 digital signing program이 함께 저장되며, 사용자 인증시 마다 비밀키가 unlock되고 digital signing 후 lock되어 비밀키가 안전하게 유지된다. 스마트카드에 사용자 ID, 사용자 ID를 포함한 DNA personal ID α_A, 비밀키 $X_A = \delta_A + r_A$, 비밀키 $X_A = \delta_A + r_A$로 암호화된 δ_A, digital signing program이 저장된다.



(그림 5) 해쉬함수와 key pair를 사용한 전자서명

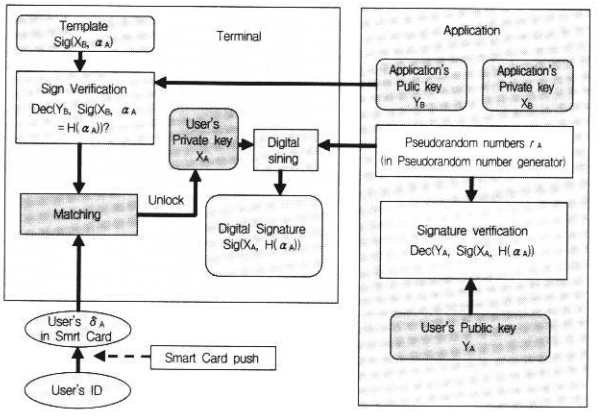
(그림 5)의 전자서명은 각 개인 DNA 정보인 DNA personal ID α_A를 해쉬함수로 처리한 결과 δ_A를 사용자 비밀키 $X_A = \delta_A + r_A$로 암호화하여 digital signature를 생성한다. 그리고 DNA personal ID α_A를 수신측(사용자 인증 요구기관)의 공개키(Y_B)로 암호화하여 digital signature에 첨

부한다. 이러한 두 정보를 수신측이 수신하면 사용자 개인키로 암호한 digital signature는 사용자(송신측)의 공개키로 복호화되어 δ_A가 되고 첨부된 암호문은 수신측의 개인키(X_B)로 복호화하여 δ_A가 된다. 이들 둘을 비교하여 동일하면 사용자 인증이 된다. 이때 수신측의 공개키 Y_B는 CA에 등록되어 관리된다.

특히 사용자(송신측) 인증시 비밀키 $X_A = \delta_A + r_A$, 공개키 $Y_A = g^{XA} \pmod p$에서 r_A의 안전한 생성이 반드시 필요하다. 왜냐하면 r_A는 전자서명의 비밀키 구성 요소이기 때문에 전자서명 비밀키 안전성에 영향을 주기 때문이다. 따라서 r_A는 본 논문에서 제시한 안전한 의사난수 발생기에서 생성된 일회용 값이므로 DNA 개인정보 노출 방지에 도움을 줄 수 있다.

4.3 Multiuser-authentication system

논문[1]에서 제안한 사항을 개선한 다단계 인증시스템으로 강한 사용자 인증시스템을 제안한다. 생체인증 정보와 RFID 스마트카드, 그리고 PKI 전자서명의 다중 사용자 인증시스템으로 논문[1]의 제안 사항을 다음과 같이 개선한다. 사용자 인증 카드인 two card(the biometric registered seal card and the DNA personal ID card) 대신 하나의 RFID 스마트카드로 사용자 인증을 할 수 있고, 카드 분실시 사용자 정보 노출의 위험을 RFID로 해결한다. 또한 DNA personal ID만으로 일난성 쌍둥이, 수혈한 환자, 암세포에서 돌연변이가 발생한 경우의 사용자 인증이 어려운 경우까지 사용자 ID에 대응하는 일회용 의사난수와 DNA 정보로 사용자 인증을 해결하였다. 제안된 시스템은 (그림 6)에서 사용자 ID를 터미널에 입력하면 카드 인식기에서 RFID 스마트카드를 입력하라는 메시지에 따라 카드를 넣는다. 카드 안의 사용자 ID를 읽어 카드에 등록된 δ_A를 터미널로 불러온다. 한편 application administrator의 비밀키로 α_A를 signing한 것이 template로 터미널에 keeping된다. Template의 signing α_A를 application administrator의 공개키(Y_B)로 복호한 후 해쉬한 것을 카드에서 읽어 온 δ_A와 비교한다. 비교 후 template와 사용자 RFID 스마트 카드에서 읽어온 δ_A와 매칭한다면, 카드에 기록된 비밀키 X_A가 unlock되어 card 내부의 digital signing program이 사용자 비밀키 X_A(의사난수 발생기에서 새로 생성된 일회용 의사난수 r_A와 δ_A)로 digital signing된다. Signature(X_A)를 document information(δ_A)에 전자서명 완료하면 비밀키 X_A는 lock된다. 스마트카드가 digital signing function을 가지고 있으므로 signature는 비밀키 X_A정보를 누설하지 않고 첨부할 수 있다. 뿐만 아니라 비밀키 $X_A = \delta_A + r_A$는 r_A가 안전한 의사난수 발생기에서 생성된 값이므로 개인키의 안전성을 높혀 전자서명의 비밀키 안전성 문제를 해결할 수 있다. Challenge-Response 사용자 인증 Scheme은 여러 번의 절차로 인해 다소 느리지만, PKI 전자서명은 컴퓨터 처리시간 단축과 처리량 최소화로 개인 DNA 정보에 대한 인증과 무결성을 확인할 수 있다. 또한 현 생체 인증시스템은 표준화된 절대적 identification을 제공하지 못하지만 제시한 사용자 인증시스템은 터미널 로그온으로 표준화된 절대적 사용자 확인이 가능하다.



(그림 6) 네트워크에서의 터미널 로그온 다중 사용자 인증시스템

4.4 Statistical analysis of multiuser-authentication system

제안된 다단계 사용자 인증시스템은 다음과 같은 이항분포 확률로써 안전성 테스트를 실행했다.

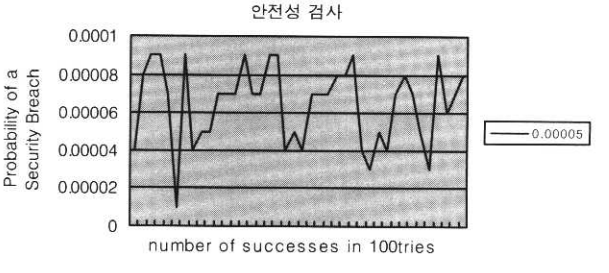
$$P_r(1 \le x \le t) = \sum t!^{t} \frac{p^x(1-P)^{t-x}}{x!(t-x)!}$$

t : number of tries

x : number of successes in "t" tries

P_r : Probability of success

100번 시도하여 성공한 횟수 x와 P(probability of a security breach)의 결과를 그래프로 나타내었다.



(그림 7) 다중 사용자 인증시스템 안전성 검사

따라서 시도 성공 횟수에 따라 Probability of a Security Breach이 0.0001를 넘지 않으므로 제시한 시스템은 안전하다고 할 수 있다.

5. 결 론

제안한 다중 사용자 인증시스템은 터미널에 로그온하는 local application에 제한을 받아온 생체 인증시스템의 단점

을 DNA 생체정보+RFID 스마트카드+PKI 전자서명의 local application으로 보다 강한 사용자 인증을 제공해 준다. 많은 양의 DNA 정보를 효율적인 해쉬함수로 스마트카드에 안전하게 저장하여 각 개인의 privacy를 보장할 수 있다. Access control과 security의 전망이 밝은 저가의 RFID로 카드의 개인 정보를 원거리에서 판독, 추적, 관리할 수 있어 개인을 보호할 뿐만 아니라, 카드 분실시 어떠한 개인 정보도 노출시키지 않는다. 현 전자서명 개인키의 안전성 해결을 위해 사용자 인증시마다 사용자 ID에 대응한 무한에 가까운 일회용 난수를 사용하여 개인키의 안전성을 향상시켰다. 또한 DNA personal ID만으로 일난성 쌍둥이, 수혈한 환자, 암세포에서 돌연변이가 발생한 경우의 사용자 인증이 어려운 경우, 인증시마다 사용자 ID에 대응하는 무한에 가까운 일회용 의사난수 값으로 사용자를 인증할 수 있다. 이러한 생체 인증분야의 DNA와 소유기반의 Hardware token 분야의 RFID 스마트카드(IC Card)와 Software 인증 분야로 PKI 전자서명의 다단계 사용자 인증시스템으로 더 강한 사용자 인증시스템이 될 수 있다. 따라서 사용자 DNA 정보를 안전하게 하나의 RFID 스마트카드에 보호 저장할 수 있고, RFID로 카드정보를 판독, 추적, 관리할 수 있으므로 카드 분실시 어떠한 개인 DNA 정보도 노출되지 않아 논문 [1]에서 제시한 사항들을 향상시켰다. 또한 RFID 스마트카드 사용으로 전자지불 시스템의 변화를 가져올 수 있다. 이러한 다중 사용자 인증시스템은 안전성이 통계적 분석으로 확인되었을 뿐만 아니라, 생체정보의 RFID 스마트카드 사용확대 계기로 신용카드, 신분증, 그리고 여권 등에서도 이용할 수 있다.

그러나 각 개인의 DNA 정보를 얻어 RFID 스마트카드에 저장하는 비용과 저장된 DNA 정보가 본인의 DNA 정보인지 확인하는 비용이 많이 든다는 것을 염두에 두어야 한다. 뿐만 아니라 제시한 시스템은 개인 DNA를 RFID 스마트카드에 저장하여 사용자 인증시마다 카드인식기에 입력하여 인증해야 함으로 개인의 DNA를 실시간으로 인증할 수 없다. 그러므로 앞으로 실시간 사용자 DNA 정보를 인증할 수 있는 편리하고 효율적인 복합 인증시스템 연구가 필요하다.

참 고 문 헌

[1] Yukio Itakura, Masaki Hashiyada, Toshio nagashima, Shigeo Tsujii, "Proposal on personal identifiers generated from the STR information of DNA," Int. Journal Information Security, pp.149-160, April, 2002.

[2] http://www.kisa.or.kr.

[3] CSI/FBI Computer Crime & Security Survey Report, 2000.

[4] CSI/FBI Computer Crime & Security Survey Report, 1998.

[5] Brown TA(2000) Genome, trans. Muramatsu M. Medical Science International, p.154.

[6] Itakura, Y., Nagashima, T., Tsujii, S., Statistical verification of DNA information for personal identification, Information Processing Society of Japan, CSS 2000, pp. 121-126, 2000.

[7] Tsujii, S., Itakura, Y., Yamaguchi, H., Kituzawa, A., Saito, S., Kasa-hara, M., A public key encryption method having a structure in which biological information is embedded in a secret key, Technical Report of IEICE, SCIS 2000, D07, 2000.

[8] http://www.itl.nist.gov/fipspubs/fip180-1.htm.

[9] http://www.e-smartcom.net/product/product-smartcard-eCOS%20CARD.htm.

[10] http://members.tripod.lycos.co.kr/temafu/postal/RFID-1_2.htm.

[11] P. Gutmann, "Software Generation of Practically Strong Random Numbers, extended version," available at http://www.cryptoengines.com/~peter/06random.pdf, June, 2000.

[12] 3GPP TSG SA WG3 Security-S3#15, "Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms," Sep., 2000.

[13] 3GPP TS 35.201 ; F8 and F9 Algorithms Specification ; this is available at http://www.etsi.org/dvbandca/3gpp/3gppspecs.htm.

[14] B. E. Jung, H. Ryu, K. Kim, K. Y. Chang and O. Y Yi, "Analysis and Implementation for 3GPP Authentication Mechanism," Proceeding of WISA, pp.87-102, 2001.

[15] http://csrc.nist.gov/CryptoToolkit/aes.

[16] 송정환, 현진수, 구본욱, 장구영, "블록 암호 알고리즘 기반 의사난수 발생기 제안과 안전성 분석", 정보처리학회논문지 C, 제9-C권 제6호, 2002.

성 순 화

e-mail : shsung@ce.cnu.ac.kr

1983년 경북대학교 전자공학과(전산학)(공학사)

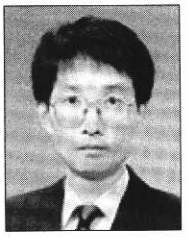
2000년 한남대학교 컴퓨터공학과(공학석사)

2001년~현재 충남대학교 컴퓨터공학과 (박사과정)

2000년~현재 대덕대학 겸임교수

2002년~현재 충남대학교 시간강사

관심분야 : 정보보호, 네트워크 보안, 암호학, 사용자 인증시스템



공 은 배

e-mail : keb@ce.cnu.ac.kr

1978년 서울대학교 계산통계학과(학사)

1981년 서울대학교 계산통계학과(석사)

1991년~1995년 Oregon State Univ. 전산학과(박사)

1996년~현재 충남대학교 소프트웨어 연구센터 기술협력부장

현재 충남대학교 컴퓨터공학과 교수

관심분야 : 인공지능, 기계학습, 전자상거래, 암호학