1회용 암호와 네트워크 IP Tracking을 이용한 인증시스템의 설계

채병수*, 차홍준**

Design of Model of Evidence System using the Single Cryptology and Network IP Tracking

Byeung-Soo Chae*, Hong-Jun Tcha**

요 약

이 연구는 정보유통시스템으로 컴퓨터통신망에서 파일저장 장치의 보안과 인증시스템으로 설계하고 연구하려는 것으로 컴퓨터 정보처리에 이용되고 활용되어야 할 암호화된 정보와 데이터 파일 저장장치에 대한 보안을 유지되도록 사용자 이용권한(access)을 시스템적 접근 문제로 해결하려는 인증네트워크 시스템으로서, 1회용 암호와 네트워크 IP Tracking을 이용한 인증시스템의 설계를 연구하였다.

ABSTRACT

This research attempted to build up a system of security and identification for storage devices in a communication network. This identification Network System will configure security of information encoded and any computer data-medium by control of the access right of the user.

Key Word

IP Tracking, One-time Cipher, Authentication System, Genetic Algorithm, Information processing

Ⅰ. 서 론

21세기 정보화사회(情報化社會)는 사회적 기반시설(SOC:Social Organization Construction)로서 구축된 인터넷 네트워크가 유비쿼터스(ubiquitous) 환경에 있게 되었다. 그러나, 통신 통로(通路)에서 뿐만 아니라, 파일(file)에 의한 임시저장 매체로 유통시켜야 할 과정에서도, 정보와 데이터의 신뢰와 확신성이 보장 받아 저야 할 요구가 필요하게 되었다[1].

이 연구는 정보유통시스템으로 컴퓨터통신 망에서 파일저장 장치의 보안과 인증시스템으로 설계하고 연구하려는 것으로, 컴퓨터 정보처리에 이용되고 활용되어야 할 암호화된 정보와 데이터 파일 저장장치에 대한 보안을 유지되도록 사용자 이용권한(access)을 시스템적 접근 문제로 해결하려는 인증네트워크 시스템이다. 실제로 on-off 이동성 정보와 데이터 파일 저장 매체로서 Memory stick의 무결성 보안을 목표하므로, 이를 사용하려는 사용자에 대한 인증문제의 확인을 IP 추적(IP tracking)으로 하고, 그 추적된 기록역사(history DB)에 따라 사용자 인증을 확신 받으려는 것이다.

* 강원대학교 컴퓨터과학과(bschae@kangwon.ac.kr)
** 강원대학교 컴퓨터과학과 교수
#논문번호 : KIIECT2009-02-13 #접수일자 : 2009.05.25 #최종논문접수일자 : 2009.06.18

Ⅱ. 연구배경

1. 암호

암호(暗號 password)는 통신의 내용을 비밀로 은닉(隱匿)하기 위하여 사용하는 말로서, 오늘날 암호는 문자를 비트로 바꾸어, 이를 n비트씩 나눈 평문과 k 비트 키를 입력하여 n 비트씩으로 된 암호문을 출력하는 블록 암호, 1비트 단위로 암호연산을 수행하는 스트림 암호, 그리고 공개 키 암호로 구분된다.

1) DES

DES(Data Encryption Standard)는 1975년 IBM의 투취만(W. Tuchman)과 메이어 (C. Meyer)의 중심으로 연구한 알고리즘을 제시하였다. 공개적인 검증을 거쳐 재 인증함으로서 안전하다는 신뢰를 얻게 된 대칭키 암호이면서 블록암호이다.

2) 공개 키

공개 키(公開: public key)는 인증기관에 의해 제공되는 키 값으로서, 이는 개인키와 함께 결합하여 비대칭 암호 작성법이라 하여, 메시지 및 전자서명의 암호화와 복호에 사용된다.

3) 일회용 암호

일회용 암호는 이론적으로 암호문으로부터 키의 특성을 전혀 파악할 수 없도록 한 시스템이나, 실제로 사용하기에는 다소 불편하므로 연구와 개선을 하고 있으나 평문의 길이가 n인 임의의 문자열로 이루어져 있으면, 키 역시 n길이의 임의의 문자열이 출현 빈도가 모두 같도록 선택하여야 한다[2][3].

(1) 키 제작의 문제

일회용 키 스트림(stream)은 완전 무작위 수열이어야 하지만 이러한 수열은 보내는 사람과 받는 사람이 서로 같이 공유한다는 것이 매우 불편하므로 가짜 무작위(pseudo-random) 수열을 이용하기 위하여 간단한 규칙에 의해 만들어지는 규칙만을 주고받게 한다. 이 시스템은 키 교환 문제에 유리하지만, 완벽한 안전성을 보장하지는 못한다.

(2) 전달의 문제

어떠한 전달자이던 방법에서는 보안성이 없다. 이는 전달자의 고의든 아니든 사고를 막을 대안이 없고, 또 예측도 할 수 없기 때문이다.

2. 유전자 알고리즘

1) 유전자 알고리즘

다윈(Charles Darwin)은 1859년 발행된 "The origin of species"에서 종(種)이 어떻게 변할 수 있는지를 설명하는 구조로 자연도태(natural selection)를 제시하였고, 다윈은 자연에 잘 적응하는 개체는 생존하고 그렇지 못하면 도태하는 적자생존의 원리, 개체군(population) 중에서 환경에 대한 적합도가 높은 개체가 살아남을 확률이 높아서 재생할 수 있게 되며, 이때 교배와 돌연변이로 다음 세대의 개체군을 형성하게 된다고 했다. 멘델은 다윈과 같은 시대에 살았으나 전혀 교류가 없이, 1866년 현대 유전학의 토대를 마련한 식물의 잡종성에 대한 연구를 발표하였다[4].

2) 유전자 알고리즘의 요소

유전자 알고리즘(GA)은 대부분의 방법들은 염색체의 개체집단, 적합도에 따른 선택과정, 새로운 자손을 생성하기 위한 교배, 그리고 새로운 자손을 위한 변이와 돌연변이이다.

GA는 현재의 개체집단에서 각 염색체에 대해 점수(적합도)를 부여하는 적합도 함수를 가장 많이 필요로 하므로 염색체의 적합도가 주어진 문제를 얼마나 직접 잘 해결하는가에 좌우된다.

(1) 적합도 함수

가장 흔한 GA의 응용분야는 함수 최적화이다. 즉, 이는 복잡한 다변수 함수를 최대화하는 매개변수 값들의 집합을 찾아내려는 것이다.

(2) GA 연산자

가장 단순한 형태의 유전자 알고리즘은 선택, 교배, 그리고 돌연변이의 세 연산자들을 포함한다.

① 선택(selection)

이 연산자는 재생산을 위하여 개체집단에서 염색체들을 선택하는 것이므로 더 적합한 염색체일수록 더 많이 선택되어 재생산되게 된다.

② 교배(crossover)

임의(random)로 어떤 위치를 선택하고, 두 염색체들 사이에 그 이전과 이후의 배열의 일부분을 교환하여 두 개의 자손을 생성한다.

③ 돌연변이(mutation)

염색체내의 어떤 bit들은 임의로 역전시키는 것이

다. 실 예로, 문자열 '00000100'은 두 번째 위치에서 돌연변이 되면 '01000100'이 되는 돌연변이는 보통 0.001%의 매우 작은 확률을 가지고 각 bit 위치에서 발생하는 것이다.

3) 단순 유전자 알고리즘

정의된 문제와 후보 해들에 대한 기호 문자열 표현이 주어졌을 때는 알고리즘 1 에서 선택은 교체로 끝나는 것으로, 염색체가 한번이상 선택되어 부모가 되었다는 뜻이다.

확률은 교배율이라 하며 두 부모가 한 점에서 교배되는 확률로 정의되며 한 쌍의 부모에 대한 교배율에 의해서 교배가 일어나게 된다[5].

알고리즘 1. 단순 유전자 알고리즘

1. 임의로 생성된 n개의 ℓbit 염색체들의 개체집단을 문제가 되는 후보 해로 시작한다.
2. 개체집단에서 각 염색체 x의 적합도 f(x)를 계산한다.
3. n개의 자손이 생성될 때까지 다음 단계를 반복한다.
   a. 현재 개체집단으로부터 한 쌍의 부모 염색체를 선택한다.
   b. 선택확률 'Pc'의 적합도 함수를 증가시킨다.
   c. 확률 'Pm'을 각 위치에서 두 자손을 돌연변이 시키고, 얻어진 염색체를 새로운 개체집단에 포함시킨다. 만일, n이 홀수이면 한 개의 새로운 개체는 버릴 수 있다.
   d. 현재 개체집단을 새로운 개체집단으로 교체한다.
   e. 단계 2.로 간다.

3. 인증과 서명

1) 인증에 사용되는 원칙

디지털통신 문화 속에서의 정보화 사회에서는 컴퓨터통신과 정보통신에서 유통되는 정보의 보호와 보안을 목적하여 인증시스템과 이에 개입되는 암호말(暗號語: password)시스템이 인증기술이다[3][6][7][8].

2) 암호말 인증 기법

컴퓨터와 통신시스템에서는 그림1.의 인증 검증자가 암호말을 사용하여 인증 요구자를 식별하여, 사용자를 인증하려는 인증방식의 기법을 가진다[9].

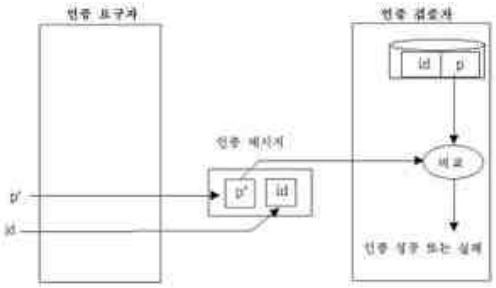


그림 1. 암호말 인증의 기본 기법

Fig 1. basis techniques of password authentication

즉, 인증 요구자는 식별자 'id'와 암호말 'p'를 이용하여 인증 메시지를 생성하고, 네트워크를 통해 인증 메시지를 검증자에게 보내고, 검증자는 인증 요구자가 보내온 인증 메시지에 포함된 암호말 'p'를 이미 저장된 암호말 'p'로 검증하게 한다. 이 같은 암호말의 인증 기법에서는 다음의 문제를 갖게 된다[10].

- 암호말의 노출 : 네트워크를 통해 암호가 보호되지 않은 상태로 전달
- 암호말의 재연 : 일정한 값을 갖는 암호말이 반복적으로 사용
- 검증자 침해 : 인증 검증자가 저장 관리를 하고 있는 암호말 정보가 노출되는 현상이 발생

따라서, 그림 1 의 기본 인증처리 기법에서의 문제점들을 해결하기 위하여, 그림 2 및 그림 3 과 같이 개선되거나, 변형된 암호말 인증 기법이 제시되었다.

그림 2 은 인증 요구자로부터 인증 검증자로 전달되는 암호말은 일 방향 함수 'f'를 수행한 값으로 사용하도록 하여 암호말이 노출되는 것을 막았다.

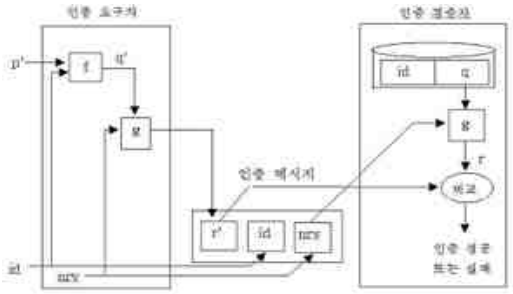


그림 2. 암호말 노출/재연 방지 인증 기법
Fig 2. authentication techniques of prevention of password exposure/reconstruct

그림 3 은 암호말과 같은 역할을 하는 변형된 개념의 키(key)와 암호(暗號: Cryptography) 알고리즘을 사용해 구성한 기법으로서, 인증을 요구하는 자로부터 인증해 줄 검증자로 전달되는 정보를 암호말 또는 서명으로 인증하는 경우이다.

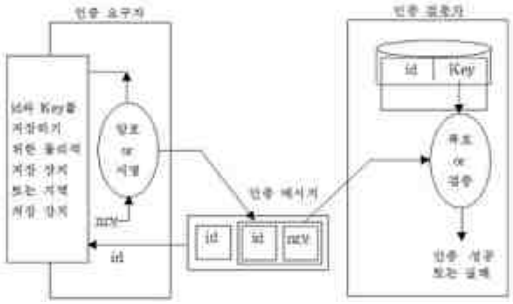


그림 3. 암호화 기반의 인증 기법
Fig 3. authentication techniques of encode on a base

Ⅲ. 정보의 저장매체와 통신

1. 정보 저장의 매체

정보(情報)는 우리 주위 사정이나 정황의 보고(報告)를 의미한다. 오늘에 이르러서는 통신, 컴퓨터, 자동제어가 발달되자 새로운 개념으로 사람을 떠나 객관적으로 전달하거나, 처리될 수도 있게 정보를 수집, 가공으로부터 재생산하는 재화가치를 가지게 되었다[11].

2. USB 저장장치

1) USB 메모리의 특성

USB 메모리의 특성은 플래시 메모리(Flash Memory)로서 비휘발성 메모리로 소비전력이 작고 저장된 데이터를 보존하는 ROM(Read Only Memory)의 장점과 정보의 입출력이 자유로운 RAM(Random Access Memory)의 장점을 가졌다.

2) USB 파일시스템

파일시스템(File System)은 저장장치 내에서 데이터를 쓰고 지우기 위해 반드시 필요한 것으로, 이는 FAT(File Allocation Table) 파일시스템, HPFS(High Performance File System), NTFS(New Technology File System), UFS(Unix File System) 시스템 중. USB메모리는 FAT 파일시스템으로 한다[12].

3) USB 데이터의 전송

USB Mass Storage를 위한 전송 프로토콜에는 데이터 전송에 사용되는 transaction format에 따라 구분할 수 있는데, Control-Bulk-Interrupt Transfer를 사용하는 CBI Transport와 Bulk Transfer만을 사용하는 Bulk-Only Transport가 있다[13].

4) USB 저장구조 구조

USB 저장장치가 컴퓨터 포트와 연결되면 호스트 컨트롤러는 디바이스에 대한 정보를 요청하며, 이 디스크립트 정보는 장치의 제조사, 저장용량 및 저장 파일에 대한 메타 데이터를 통하여 응답하고 호스트 컨트롤러는 디스크립트 정보획득 후, 각 USB 저장장치의 구분을 위해 인식된 순서대로 고유 주소를 지정한다[14].

Ⅳ. 인증시스템의 요소와 기술

1. 인증기술

인증기술은 일반적으로 사용자에 대해, 다음과 같은 하나 이상의 범주에 속한 증명의 원칙에 근거한다.

2. 패스워드 인증 메커니즘

패스워드 인증 메커니즘은 네트워크를 통해 패스워드가 보호되지 않은 상태로 전달되므로 패스워드가 노출되며, 일정한 값을 갖는 패스워드가 반복적으로

사용되는 패스워드의 재연이 되고, 인증 검증자가 저장 관리를 하고 있는 인증 정보가 노출되었을 때, 이를 분석함으로 패스워드를 추측할 수 있는 검증자 침해를 받을 수 있는 문제가 있다.

(1) 일방향함수의 사용 메커니즘

일 방향 함수를 사용하여 구성한 패스워드 메커니즘은 인증 요구자로부터 검증자로 전달되는 패스워드는 일방향 함수 f를 수행한 값으로 패스워드 노출, 재연을 방지 한다.

(2) 암호기반의 메커니즘

암호기반 인증 메커니즘은 패스워드 인증 메커니즘은 아니지만 패스워드와 같은 역할을 하는 변형된 개념의 키와 암호 알고리즘을 사용하여 구성한 것으로, 인증 요구자로부터 검증자로 전달되는 인증 메시지를 암호, 또는 서명하여 인증을 수행한다.

3. 일회용 패스워드

패스워드 시스템의 단점과 사용자의 신분확인에 신뢰성을 더하기 위하여 정보통신망에 사용자 비밀정보의 유통 보안에 확신성이 요구된다. 사용자 정보를 단 한 번의 유효성을 갖도록 패스워드를 사용하려는 것을 일회용 패스워드 방식(one-time passwords scheme)이라 한다[15].

① 시간동기(time synchronous) 방식
② 대칭키 방식
③ 공개키(public key) 방식[16.
④ 서명고리(signature chain) 방식
⑤ 일방향 함수(one way function) 방식

4. 추적(Tracking) 기술

추적(track)은 지나간 자취를 찾아가는 것이다. 정보의 추적은 원래의 정보로부터 변화되었거나, 진화된 새로운 정보를 추론 할 수 있도록, 모든 정보의 계보를 기반으로 탐지하고 검색하는 것이다.

1) 정보의 탐색

인터넷에 발달은 다양한 정보와 데이터들의 유통으로부터 축척되어지는 지식 모음의 창고를 이룬, 데이터웨어하우스를 생성하고 축적된 지식을 바탕으로 새로운 지식을 유추하거나, 추론한다.

2) 정보인식

(1) 정보인식기술

정보인식기술(IAT: Information Awareness Technology)은 광범위한 우리 주변의 환경으로부터 발생되는 다양한 정보와 폭넓은 지식들을 연속적으로 수집하고, 탐색하여 누적하는 운영관리로부터 경험된 지식을 바탕으로 정의되는 정보 추론과정을 실행한다.

(2) 정보인식의 절차

정보인식(情報認識: information recognize)은 인간의 행동이나 존속되는 사회에 있어서, 정보라는 의미있는 사물에 관한 사정이나 정황을 알게 하는 것이다[17].

Ⅴ. 인증시스템 설계와 구현의 실제

1. 시스템 구현 환경

시스템 실행의 가시적인 Window display를 위한 환경으로 Pentium 3.0Ghz CPU를 가지고, Microsoft Window XP 운영체제에서 MS Visual Studio 2005/C++ 언어로 구현된 독립된 시스템(Singularity system)으로 구현하였다.

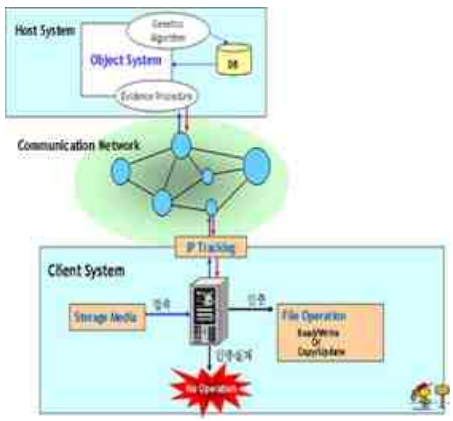


그림 4. 네트워크 IP Tracking 인증시스템 모형의 구조

Fig 4. Structure of Network IP Tracking Evidence System Design

인증시스템 모형의 구조는 Client System, Network, 그리고 Host System으로 구성된다. 즉, Memory stick과 같은 Storage Media를 이용할

Client System 영역에서 사용할 수 있는 권한 인증을 목적하므로 Networking된 On-line 상태로 인증 검색을 할 수 있는 목적시스템(Source System)이 인식될 주(host)시스템이 연결되어야 한다. Client System은 어떠한 제약조건 없이 USB에 의한 접속에서 실행될 수 있으므로 초기 인증 프로시저의 IP Tracking 할 수 있는 On-line Network환경에서 알고리즘 2 의 프로세서가 구현될 수 있도록 한다.

알고리즘 2. 인증 프로세서 알고리즘

Initial System Booting Processor
① System IPL
② User ID 와 Password 입력
③ BIOS 참조와 Trans Processing에서 인증키 생성
Host Driver Active Processor
④ 인증키의 IP Tracking으로 주(object)시스템 확인
⑤ 시스템 확인으로부터 인증 키 생성
⑥ 인증 키 DB 및 전송처리
Storage Media Driver Active Processor
⑦ User ID 와 인증 암호 값 전송
⑧ IP Tracking에 의한 인증 키(자식: new Key) 값 접수
⑨ 인증 키(부모: old Key) 값에 의한
유전자 복호화 키(자식: new Key) 생성
⑩ 인증의 판독과 권한 부여

2. 인증시스템의 설계

인증시스템은 네트워크 IP Tracking 인증시스템 모형의 구조에 의한 Storage Media 초기설정 모형, 인증 모형, 운영구조로 구현할 수 있도록 설계한다,

1) Storage Media 초기설정 모형

Storage Media인 Memory stick을 초기설정하면서 주 시스템에 등록시키려는 모형으로, 이는 알고리즘 2 의 Initial System Booting Processor의 기능이므로 그림 5. 에서와 같이 설계 했다.

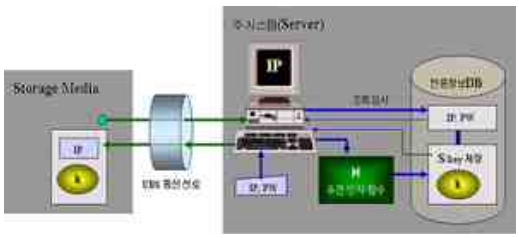


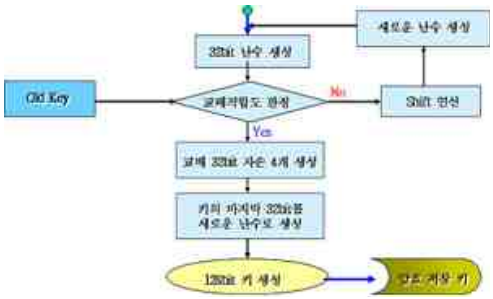
그림 5. Storage Media 초기 설정 모형

Fig 5. Design of the first setting stage of Storage Media

여기서, Storage Media인 Memory stick은 일반적인 USB로 접속할 수 있는 저장매체로서, 이는 보안성이 없이 누구나가 이용할 수 있는 Device이다.

Device 저장매체로서 파일 보안성 유지를 위한 초기설정은 이용검증을 확인받을 수 있는 Host System에 종속되어있는 목적시스템(Source System)에 등록되어야 한다. 즉, USB 접촉 Device 기능의 저장매체를 항상 최초의 목적시스템에 접속한 후, 검증 서버시스템의 사용자(IP)와 암호 키(PW)에 의한 시스템 접속을 할 수 있도록 조회정보를 인증정보DB에 등록되고, 알고리즘 3에서와 같은 유전인자함수(H) 처리에 의한 S/Key 인증 값을 통보 받으면서부터 사용권한을 인증 확인 받을 수 있게 등록된다.

알고리즘 3. 유전인자함수(H) 키 생성 알고리즘



2) Storage Media의 인증 모형

Storage Media인 Memory stick을 초기설정을 한 후, 이를 어떠한 장소이든 사용할 때, IP Tracking에 의한 주 시스템 Server에서부터 사용권한을 인증 받는 과정모형으로 그림 6에서와 같이 설계 하였다.

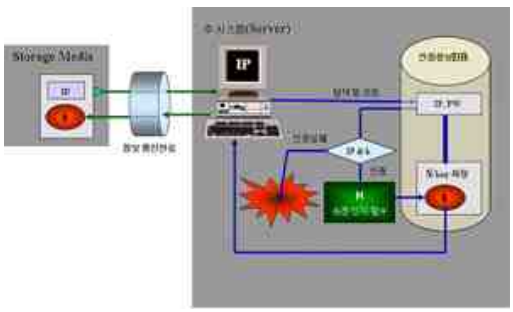


그림 6. Storage Media의 인증 모형

Fig 6. Design authentication of Storage Media

이는 USB 기능을 가진 Memory stick과 같은 Storage Media가 초기설정으로부터 인증 암호 키 값을 이미 가지고 있으므로 On-line 네트워크로 접속할 수 있는 어떠한 Client System에서도 사용할 수 있다는 것이다. 초기설정으로 서버(source computer)에 등록(인증정보DB) 된 저장매체이므로, 이는 On-line 네트워크 된 어떠한 Client System에서라도 접속되면, Memory stick과 같은 Storage Media에 Device Driver 모듈 프로세서는 알고리즘 2의 Host Driver Active Processor로서, 인증키의 IP Tracking으로 주(object)시스템을 추적해 서버시스템을 확인하고, 시스템 확인으로부터 검증된 인증키를 새로 생성하여, 인증 키 DB에 저장한 후, 이를 다음 인증 키 값으로 전송처리 한다. 이 과정에서 서버의 확인으로부터 인증이 실패되면, 즉시 인증정보DB의 관련정보가 소멸되어지게 하였다.

3) Storage Media의 운영 구조

주 시스템 Server에서부터 인증 받고, 새로운 다음 암호 키를 받은 후, 사용되는 실행 모형 설계 와 USB기능을 갖춘 Memory stick과 같은 Storage Media는 메모리스틱의 구조에서 Flash Memory를 활용할 수 있도록 한 Drive Flag Register의 Setting이 되어야 하며 알고리즘 2의 Storage Media Driver Active Processor가 서버로부터 사용자 ID와 인증암호 키 값을 IP Tracking을 거쳐 인증 키(자식: new Key) 값을 수신 후, 수신 전 인증 키(부모: old Key) 값으로 알고리즘 3에 의한 유전자 복호화 키(자식: new Key)를 생성하여 인증의 판독과 권한 부여로부터 Flash Memory를 활용할 수 있도록 한 Drive Flag Register의 Setting하므로 사용권한을 주며 어떠한 Storage Media이든 이용권한의 인증에 실패한다면, 그 이용권한 뿐만 아니라 Data 파일의 보안성을 상실하게 된다.

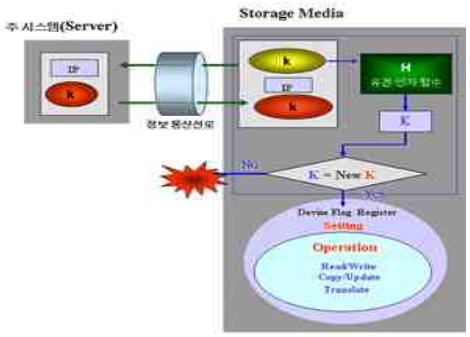


그림 7. Storage Media의 운영구조

Fig 7. operation Structure of Storage Media

3. 시스템의 구현과 실제

Window NT의 시스템 환경에서 IPL 초기 커널과 간편화로서 실행되어지는 것으로, 그림 4 에서와 같은 구조로 알고리즘 2를 구현하고, 이 실제를 했다.

1) 시스템의 구현

USB 기능의 Storage Media인 Memory stick을 주 시스템의 목적시스템에서 초기화 booting을 할 때, 'ID: '와 'PW: '를 받아 Windows로 전환하기 전에 BIOS 참조와 Trans Processing을 제어하면서, 인증정보DB를 실행할 수 있도록 하고, 알고리즘 3 의 유전인자함수(H) 키 생성 알고리즘이 동작되는 'genetic_number()' 프로시저가 실행되도록 구현하는 것이다.

2) 키 생성 프로세서

사용자 목적시스템의 IPL처리와 정보통신을 위한 네트워크 설정을 완료 한 후, USB 기능이 있는 Storage Media인 Memory stick을 접속하면, 이로부터 발생되는 키 생성 프로시저 'in_key_procedure()'에 의해서 사용자 IP 정보와 패스워드(PW)를 입력하도록 나타낸다. 이 때, 목적시스템인 서버는 인증정보DB에 조회 심사 과정을 거칠 수 있도록 시스템 준비를 하고, 초기 암호 키 값을 생성한다.

3) 목적시스템 Sever의 인증처리

알고리즘 2 의 Host Driver Active Processor는 'driver_active_procedure()'에 의해, 목적시스템 확인을 IP Tracking으로 실현한 후, IP와 인증 키 값으로 인증정보DB를 검색하므로, 이로부터 권한 인증

의 환경을 나타내 주며 확인된 목적시스템으로부터 Storage Media인 Memory stick의 IP와 인증암호 키 값에 의한 Sever의 인증정보DB에 조회하고, 이로부터 새로운 인증 암호 키 값을 유전자 함수(H) 처리로 생성하게 된다.

4) 처리 암호 키의 저장처리와 갱신

암호인증 키 처리를 위해 Server 시스템에서 알고리즘 2 의 인증정보DB에 기록과 동시에 Storage Media인 Memory stick의 USB 기능으로 정보전송과 갱신처리 과정을 한다. Storage Media Driver Active Processor는 'media_driver_active_procedure()'에 의한 실행을 하는 데, 이는 알고리즘 2 에 의해 User ID 와 인증암호 값을 전송하고, IP Tracking에 의한 인증 키(자식: new Key) 값을 접수하면 , 인증 키(부모: old Key) 값에 의한 유전자 복호화 키(자식: new Key)를 생성하여서, 인증의 판독과 권한 부여를 하게 되지만, 그렇지 않을 경우는 사용할 수 없게 한다.

Ⅵ. 결론 및 제안

오늘의 컴퓨터통신이 기반(基盤) 한 정보유통과정에서 보안 문제는 컴퓨터의 이용 형태에 따른 암호처리들이 그 해독과 수리적 확신성으로 검증되어서 무결성을 보장받게 되었다.

이 논문은 정보유통시스템으로서 이동성 저장매체인 Memory stick과 같은 파일장치의 데이터 보안성을 무결성과 확신성으로 유지될 수 있는 사용권한을 받도록 인증시스템설계로부터 이를 구현하고, 알고리즘 2 에 의한 프로시저로 그 실제를 보였다.

실제로 on-off 이동성 정보와 데이터 파일 저장매체를 사용할 권한을 획득하려는 보안시스템을 목표했으므로, 이 사용자에 대한 확신성 인증문제의 확인을 IP 추적(IP tracking)으로 인증정보DB(history DB)에서 확인 받고, 또 사용자 인증을 확신 받을 수 있도록 주 시스템 Sever와 Client와 on-line 네트워크 구조를 갖추도록 설계하여, 이를 구현한 것에서 그 실용성을 시뮬레이션 결과로 확인 받았다.

2. 제안

정보유통 암호 처리의 실제로부터 모형 과정을 기술한 신뢰성과 확신성의 측정을 위한 도구적 대안으로 제안 설계된 암호 인증처리 시스템의 구현 시스템은 실증적 실행 평가로 시뮬레이션에서 확인 받았으나, 이 논문으로 제안된 설계 모형에서 동작되어야 할 USB 기능의 자동화 프로시저 모듈의 하드웨어적 ROM 처리의 문제가 남기어 졌다.

참고문헌

[1] 천재홍, "유비쿼터스 홈 네트워크에서의 정보보호 기술 연구", 한국컴퓨터정보학회지, pp. 65-75, 2007.

[2] 이용권; "유전자 알고리즘을 이용한 일회용 인증 암호 키 설계와 구현", 강원대학교 일반대학원, 박사학위논문, 2007.

[3] Hughes, L. Jr.; "Actually Useful Internet Security Techniques", Chapter 3 and 4, pp. 67-125, New Riders, 1995.

[4] Mende A Bl; "Versuche uber Pflanzen-Hybriden" Verhandlungen des naturforschenden Vereins Brunn v.4, 1866.

[5] 공송곤, 김인택, 박대희, 박주영, 신요안, 유전자 알고리즘 입문, 진영사, 1997

[6] ITU-T; "Information Technology-OSI-Security Frameworks for Open Systems; Authentication Framework", ITU-T X.811, 1995.

[7] ISO/IEC, "Information Technology-OSI-Security Frameworks for Open Systems; Authentication Framework", ISO/IEC 10181-2, 1996.

[8] 원동호, 김세헌; "정보보호 관리 및 정책", 한국정보호진흥원, 2002.

[9] 장청룡, 양형규, 채홍철, 이용권, 이보영; "일회용 패스워드 표준(안) 개발", 한국정보보호센터, 1998.

[10] M. S. Merkow, J. Breihaupt; "The Complete Guide to Internet Security", Amacom, 2000.

[11] 전석호, 정보화와 뉴미디어, eBook, 2006.
[12] 정준석, 정원용, 임베디드 개발자를 위한 파일 시스템의 원리와 실습, 한빛미디어, 2006.
[13] 안희중, 한성용, 박희상, 이철훈; “Embedded System을 위한 iROSTM 기반의 USB Mass Storage 설계 및 구현, 한국정보과학회, 학술발표 논문집, Vol. 29. NO.1, 2002.
[14] 최오훈, 임정은, 나홍석, 백두권; “USB 저장장치의 효율적인 통합을 위한 시그마 허브”, 정보과학회논문지, 데이터베이스 제35권 제6호 , 2008.
[15] Markus Kuhn; “A one-time password login package”, Computer Laboratory, University of Cambridge, 2003.
[16] Gustavus J. Simmons; "Contemporary Cryptology - The Science of Information Integrity", IEEE PRESS, pp. 27-31, 1992.
[17] 차홍준; 컴퓨터과학(Computer Science), 강호출판사, 2008.

저자약력

채병수(ByeungSoo, Chae)

2003년 강원대학교 전자계산학과 학사
2006년 강원대학교 컴퓨터과학과 석사
2009년 강원대학교 컴퓨터과학과 박사

<관심분야> 시스템프로그래밍, 정보보안

차홍준(Hong-Jun Tcha)

1991년 성균관대학교 통계학과 박사
2004년 노동부 기술사검정위원
현 재 강원대학교 컴퓨터과학과 교수

<관심분야> 시스템프로그래밍, GIS, 전산통계