ISSN 2234-4438
중소기업융합학회 논문지 제6권 제3호 pp. 29-35, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.3.029

디바이스 불변 정보를 이용한 사용자 인증 시스템 설계

김성열*
청주대학교 컴퓨터정보공학과

Design of a User Authentication System using the Device Constant Information

Seong-Ryeol Kim*
Department of Computer & Information Engineering, Cheongju University

요 약 본 논문은 디바이스 불변 정보를 이용한 사용자 인증 시스템(DCIAS)을 설계 제안한다. 네트워크상의 시스템 접근 시 사용자 인증에 사용될 접근 디바이스 불변정보를 이용한 새로운 패스워드를 설계 정의하고, 다른 응용들에서 획득한 패스워드를 재사용하는 수동적 재전송 공격으로부터 요구되는 보안 위협에 대처할 수 있도록 신 개념 사용자 인증 시스템을 설계 제안한다. 또한 서버 내에 임의의 암호화된 장소에 설계 정의한 패스워드를 저장하여 네트워크를 통한 불법적인 시스템 접근을 무력화시키도록 설계한다. 따라서 제안한 본 시스템을 이용하면 어떠한 네트워크를 통하여 시스템에 접근하더라도 어느 곳에 패스워드가 저장되어 있는지를 알 수 없고, 설상 알았다고 하더라고 저장된 정보가 암호화되어 있어 해독이 쉽지 않아 네트워크상의 어떠한 재전송 공격이라도 무력화할 수 있다는 강력한 보안 특성을 갖는다.

키워드 : 디바이스 불변정보, 보안위협, 사용자 인증, 패스워드

Abstract This paper presents the design of a user authentication system (DCIAS) using the device constant information. Defined design a new password using the access device constant information to be used for user authentication during system access on the network, and design a new concept the user authentication system so that it can cope with the threat required from passive replay attacks to re-use the password obtained in other applications offer. In addition, by storing a password defined by the design of the encrypted random locations in the server and designed to neutralize the illegal access to the system through the network. Therefore proposed using the present system, even if access to the system through any of the network can not know whether any where the password is stored, and if all right even stored information is not easy to crack's encrypted to neutralize any replay attacks on the network to that has strong security features.

Key Words : Device Constant information, Password, Security threat, User authentication

1. 서론

오늘날 급변하는 IT 기술과 네트워크 환경의 급속한 발전에 따라 인터넷 사용이 보편화되고, 관련 시스템과 정보 유통량이 급증함에 따라 정보 유출에 대한 피해가 급격히 증가되고 있어 정보보안에 관한 사회적 이슈가 커지고 있는 실정이다. 또한 사용자들이 네트워크를 이용하여 업무운영과 수행, 각종 업무들의 접근하기 위하여 서버에 접속을 시도하나, 적법한 사용자인가를 확인하는 사용자 인증 문제가 최근에 커다란 초점으로 대두되고 있다.

Received 2016-07-19 Revised 2016-08-12 Accepted 2016-09-02 Published 2016-09-30
*Corresponding author : Seong-Ryeol Kim (srkim@cju.ac.kr)

이러한 문제는 적법한 사용자라도 네트워크 접속과정에서 침입자가 통신 상태를 감청하여 ID와 패스워드를 도용하거나 스니퍼(sniffer), IP 스푸핑(spoofing)등을 이용하여 ID와 패스워드를 쉽게 해킹하여 침입 수단으로 다시 사용될 수 있다는 것이다[1,2,4,8].

따라서 본 연구는 기본적인 사용자 인증 방법인 패스워드 시스템과 패스워드 누출 방지 기술을 연구하여 각종 서버의 사용자 인증 시스템으로 활용할 수 있도록 디바이스 불변 정보를 이용한 사용자 인증 시스템(DCIAS: Device Constant Information user Authentication System)을 설계 제안한다[1,2,4,8].

본 시스템 설계개념으로는 각종 접근 디바이스의 불변정보, 예를 들어 NIC (Network Interface Card)의 MAC(Media Access Control) address나 고유 IP (Internet Protocol) address, NAND flash memory의 최초 Bad Block 정보 등과 같은 불변정보 중에 하나를 이용하여 새로운 패스워드 설계에 이용한다[5,6]. 또한 다른 응용들에서 획득한 패스워드를 재사용하는 수동적 재전송 공격으로부터 요구되는 보안 위협에 대처할 수 있도록 서버 내에 임의의 암호화된 장소에 패스워드를 저장할 수 있도록 설계 정의하여 네트워크를 통한 불법적인 시스템 접근을 원천적으로 무력화시키도록 새로운 사용자 인증 시스템을 설계 제안한다[2].

2. 관련연구

본 연구를 위한 관련 연구로는 사용자 인증 요구사항, 사용자 인증기법과 패스워드 노출방지기법, 그리고 디바이스 불변정보에 관하여 고찰한다[1,3,7,8].

2.1 사용자 인증 요구사항

사용자가 네트워크를 통해 서버에 접근을 요청할 때에 서버는 사용자 확인, 필요한 권한 부여 등과 같은 일련의 과정이 사용자 인증이다. 사용자 인증 시 요구되는 요구사항은 사용자의 식별(Identification) 및 인증(Authentication), 사용 권한의 허가(Authorization), 책임추적성(Accountability) 등이 요구되는데, 먼저 식별은 서버에게 사용자 식별자(ID)를 확인을 요청하는 과정으로 각 서버의 사용자들은 유일한 식별자를 갖는다[3,4,7,8]. 이러한 사용자의 식별자는 개인 신원을 나타내기 때문에 사용자의 책임추적성 분석에도 중요한 자료로 활용된다. 따라서 사용자 식별자는 반드시 유일한 것을 사용해야 하고, 공유할 수 없다. 그리고 인증은 임의의 서버 정보에 접근할 수 있는 사용자의 자격을 검증하는 것으로 서버의 부당한 접속이나 사용, 정보의 부당한 절취 또는 변조, 전송 등을 방지할 수 있어야 한다. 또한 인가는 사용자 또는 프로그램, 프로세스에게 이용 권한 부여를 의미하며. 이는 권한 요구자가 어떠한 일을 하거나 어떠한 역할에 대한 권한을 부여하는 것으로 철저한 검증과정을 거쳐 부여하여야 하며, 책임추적성은 네트워크 환경에서 누가, 언제, 어디서, 어떠한 행동을 한 과정을 기록하여 필요시 그 행위자를 추적하여 발생 가능한 책임소재를 명확하게 할 수 있어야 한다.

2.2 사용자 인증기법

각종 서버의 사용자 인증 기법으로는 사용자 ID와 패스워드를 이용하는 인증 방법을 기본적으로 사용되고 있다. 그러나 각종 서버에 대부분의 사용자들은 신원을 밝히지 않은 상태로 접근하면 서버에서 접근 사용자의 신원을 확인할 방법은 없다. 이러한 익명성으로 인하여 서버에서는 적절한 접근제어 구현이 쉽지 않고, 메시지가 평문으로 전송되기 때문에 기밀성도 기대할 수 없다[1,8]. 따라서 이러한 문제점을 해결하기 위하여 다음과 같은 사용자 인증 기법들을 사용한다[1,3,8].

2.2.1 기본 인증 기법

사용자 ID와 대응되는 패스워드 정보를 암호화된 상태로 서버에 저장하고 있다가 접속을 시도하는 사용자의 패스워드를 암호화하여 저장된 값과 일치여부를 확인하여 접속을 허용하는 기법으로 구현과 사용이 단순하다는 장점은 있으나 사용자 패스워드가 단순히 인코딩 되어 서버로 전송되므로 재전송 공격(replay attack)에 취약하고, 서버는 사용자 ID와 패스워드 정보를 관리해야 하는 부담이 있다[1-3,8].

2.2.2 네트워크 주소를 이용한 접근제어

클라이언트 시스템마다 부여되어 있는 IP 주소 정보를 이용하여 서버에 대한 접속을 제어하는 기법으로 IP 필터링이라고도 한다. 네트워크 주소의 구조적 특성을 이용하여 특정 도메인에 속하는 클라이언트들도 손쉽게 접근제어가 가능하다. 기본 인증 기법과 같이 사용자 ID

와 패스워드가 노출되지 않으므로 안전하지만, 공격자는 자신의 IP 주소를 변조할 수 있어 신분위장 공격에는 취약[1-3]하다. 또한 시스템별로 접근제어를 제공하기 때문에 사용자별 접근제어는 기대할 수가 없어 기본 인증 기법과 네트워크 주소를 이용한 기법의 혼합한 형태가 많이 이용되고 있다[1,8].

2.2.3 메시지 다이제스트 인증

사용자 정보에 단일방향 특성을 갖는 메시지 다이제스트(Message Digest : MD) 함수를 적용하여 서버에 접속에 필요한 정보를 전송하는 방법으로, 사용자 ID와 패스워드가 네트워크상에 그대로 노출되는 기본 인증 기법의 단점을 보완하고 있다[1-3,8]. 즉, 클라이언트 사용자 ID와 패스워드 정보를 MD5와 같은 단일방향 함수로 다이제스트하여 전송하면, 서버는 저장되어 있는 사용자 정보와 비교하여 인증을 수행한다. 이때 재전송 공격을 막기 위해 시간 정보와 함께 전송하며, 평문 형태의 패스워드 정보를 메시지 다이제스트한 값만 보관하고, 평문 정보는 클라이언트나 서버 시스템에서 완전히 삭제함으로 요구되는 보안 특성을 충족할 수 있다.

2.3 패스워드 노출 방지 기법

2.3.1 S/Key 일회용 패스워드 시스템

네트워크상의 도청과 재전송 공격, 수동적 공격에 대하여 사용자의 패스워드를 보호하기 위하여 제공하는 시스템이다[1-3]. 여기서 사용되는 일회용 패스워드 생성방법은 먼저 첫 번째 일회용 패스워드 생성은 사용자의 비밀 패스워드(s)를 정해진 특정 수(n)만큼의 단방향 함수를 수행하여 생성]한다. 예를 들어 n을 5이라고 가정하면, 첫 번째 일회용 패스워드는 p(1)= f(f(f(f(f(s))))이며, 다음 패스워드는 사용자의 패스워드를 단방향 함수에 n-1번 즉, p(2)=f(f(f(f(s))))를 수행하여 생성한다. 따라서 일회용 패스워드 p(i)의 사용을 도청하고 있는 도청자는 다음 패스워드 p(i+1)를 생성해낼 수 없다. 최초의 사용자 비밀키를 알지 못하면 도청이 불가능하게 된다.

2.3.2 Challenge-Response 방법

Challenge-Response 방법은 사용자가 인증 요구와 함께 사용자 식별 번호((Personal Identification Number : PIN)를 인증 서버에게 전달하면, 인증 서버는 난수를 생성하여 challenge로 사용자에게 전달한다[1,4]. 이와 동시에 인증 서버는 이용자의 사용자 식별 번호에 해당하는 패스워드를 키 데이터베이스에서 꺼내 이것을 이용하여 난수의 암호화를 시작한다. Challenge를 받은 사용자는 그것을 자신의 패스워드로 암호화하여 response로 인증 서버에게 반환한다. 사용자로부터 response를 받은 인증 서버는 서버 자신이 계산한 값과 수신된 response 값을 비교하여 일치하는 경우에 사용자를 적법한 사용자로 인증한다[4,8].

2.3.3 Time-Synchronous 방법

Time-Synchronous 방법에서 서버는 난수 발생 알고리즘과 64비트의 비밀키, 사용자는 특정키를 가지고 있다[1-4]. 사용자가 응용 서비스를 제공받기 위해 응용 서버에 로그인을 시도하면 서버는 4자리 숫자의 PIN과 6자리 숫자의 난수가 필요하며, 필요한 난수는 토큰 안에 저장되어 있는 “비밀키”와 “시간”을 초기 값으로 하여 토큰 안의 알고리즘을 통해 생성된다. 이렇게 생성된 10자리 숫자가 서버로 전송되면, 서버는 4자리 숫자(PIN)를 인덱스로 하여 서버에서 해당 “비밀키”를 찾아 알고리즘에 “시간”과 “비밀키”를 이용하여 생성된 6자리 난수를 수신된 6자리 난수와 일치여부를 검사하여 일치되면 요구하는 서비스를 이용할 수 있는 권한을 부여하는 사용자 인증 절차를 종료한다.

2.4 디바이스 불변정보

2.4.1 NIC MAC address

모든 네트워크 서버에 접속하기 위해서는 통신접속장치(NIC)가 필요하며, 이 NIC는 불변 고유한 물리 MAC address를 가지고 있으며, 이더넷과 같은 브로드캐스트 네트워크에서 해당 세그먼트의 고유한 노드들을 식별하며, 프레임들은 특정 호스트 식별에 이용된다. 이러한 MAC address는 영구적이고, 전역적인 고유 식별을 위해 설계되었지만, 필요에 따라 소프트웨어적으로 변경하여 사용할 수 있다[5]. 이러한 MAC address 변경은 네트워크 가상화나 보안 취약점에 대처하는 MAC spoofing에서 이용되기도 한다. 그러나 최초 부여한 물리 MAC address는 변하지 않으므로 본 연구에 적용할 수 있다.

이러한 물리 MAC address는 48bits인 MAC-48과 64bits인 EUI-64가 있으나, 현재 대부분의 NIC는 MAC-48이 사용되고 있으며, EUI-64는 IEEE 1394 (Fire wire)나 IPv6, ZigBee, IEEE802.15.4(저속 WPAN),

6LoWPAN 등에서 사용되고 있다[5].

2.4.2 IP address

일반적으로 고유의 IP를 사용하는 시스템에서는 한번 적용한 IP는 변하지 않으며, 이러한 IP 종류는 IPv4와 IPv6가 있으며, IPv4는 32bits로 구성되며 IPv6는 128bits로 구성된다. 그러나 임의 IP를 선택적으로 사용하다 반환하는 동적 호스트 구성 프로토콜(DHCP: Dynamic Host Configuration Protocol)를 사용하면 한정된 IP를 효과적으로 이용할 수는 있으나, IP가 유동적으로 사용할 때마다 변하기 때문에 본 개념을 적용할 수는 없고 변하지 않는 고정 IP를 사용한다면 본 개념을 적용할 수 있다.

2.4.3 NAND Bad Block Information

NAND 플래시 메모리는 일반적인 플래시 메모리 특성과 NAND만의 고유특성을 가지는 메모리로 Write하기 전에 Block 단위로 Erase 한다는 일반적인 플래시 메모리 특성과 NAND만의 고유 특성인 Serial 전송, Page 단위로 Read/Write하며, Bad Block을 가지고 있다는 특성을 가지고 있다[6]. 이러한 Bad Block은 NAND 플래시 메모리에만 존재하는 불량 블록으로 생산 중에 또는 사용 도중에 발생한다. 생산 중에 발생한 초기 Bad Block 정보는 변하지 않으며, NAND spare 영역의 여섯 번째 바이트를 “0x00”으로 표시하고 사용도중 발생하는 Bad Block일 때는 “0x59”로 표시되어 주기적으로 변할 수 있다는 특성을 가지고 있다[1]. 따라서 변하지 않는 최초 Bad Block 정보를 본 연구에 적용할 수 있다[6].

3. 디바이스 불변정보를 이용한 사용자 인증 시스템(DCIAS) 설계

3.1 설계 배경과 개념

현재 네트워크 서버 시스템들은 대부분 UNIX 계열(LINUX 계열 포함)이며, 사용자 인증에 사용되는 패스워드는 기본적으로 데이터 암호화 표준(Data Encryption Standard : DES)라고 하는 단방향 암호화 알고리즘을 사용해서 암호화하며, 암호화된 패스워드는 /etc/passwd에 쉐도우 패스워드인 경우에는 /etc/shadow에 저장한다[3,4]. 사용자의 인증 과정은 로그인할 때 입력한 패스워드는 먼저 암호화한 후에, 패스워드 저장 파일의 암호화된 패스워드와 비교하여 일치하면 사용자 접근을 허용한다.

이러한 패스워드 사용자 인증 시스템은 간단한 방법으로 구현 가능하지만, 패스워드가 네트워크상에 평문으로 전송된다는 단점이 있다. 평문으로 전송되는 패스워드는 스니핑(sniffing)과 같은 방법에 의해 쉽게 가로챌 수 있다. 네트워크에 연동되어 있는 호스트뿐만 아니라 외부에서 내부 네트워크로 접속하는 모든 서버들에게도 위협이 된다[3,4]. 또한 등록되어 있는 사용자의 수가 매우 많거나, 이들의 패스워드를 자주 변경해 주어야 할 때, 서버 인증 관리자에게 너무 큰 부담이 될 수 있다. 이러한 문제점을 해결하기 위한 다른 패스워드 인증 시스템도 구현 과정과 관리가 복잡하여 일반 사용자들에게 문제는 상존한다.

따라서 본 논문에서는 패스워드 평문을 암호화하고 암호화된 패스워드 암호문에 디바이스 불변정보를 첨가하여 새로운 암호 패스워드를 설계한다. 기존 패스워드 저장위치가 /etc/passwd나 /etc/shadow로 획일화되어 있는 방식을 개선하여 패스워드 저장 위치와 파일명을 암호화하여 임의의 장소에 저장할 수 있도록 생성하여 원천적으로 패스워드 저장위치에 접근할 수 없도록 차단함으로 기존 사용자 인증 시스템들의 문제점을 해결하고자 한다[4].

3.2 DCIAS 암호화 기법 설계

DCIAS 설계개념을 충분히 반영하여 사용자 인증 정보인 패스워드의 암호화와/복호화하고 디바이스 불변정보를 결합하고 암호화된 패스워드가 저장될 위치와 파일명 생성과 암호화 기능을 수행할 수 있도록 패스워드 암호화/복호화, 결합 알고리즘과 저장 파일명/위치명 생성 암호화 알고리즘을 설계한다.

제안하는 DCIAS의 암호화 알고리즘은 1차로 기존의 평문형태의 패스워드를 DES 또는 RSA 암호화 기법을 이용하여 암호화하여 암호 패스워드를 생성하고, 2차로 디바이스 불변정보(MAC 또는 IP address, 초기 Bad Block Information 등)를 첨가하여 DCIAS 암호 패스워드(DCIAS cipher Password: DcP)를 생성한다.

그리고 3차로 저장 위치명/파일명(secured Path and File name: sPF)의 생성 암호화 알고리즘을 설계하여 저장장소를 엄폐할 수 있도록 한다. 이러한 기법은 1,2차 암호화 기법을 복합적으로 적용하고 3차로 저장장소를 엄

폐할 수 있어 사용자 인증시스템의 보안강도와 보안 특성을 높일 수 있다.

3.2.1 DcP와 sPF 구조

DcP 구조는 다음과 같이 정의하며 암호화에 사용하며, DcP는 1차 암호화한 패스워드(cipher Password : cP)와 디바이스 불변정보인 DCI의 순서쌍으로 구성한다. 암호키는 기존의 DES나 RSA 암호화에 사용되는 암호키를 1차 암호키로 사용하며, 이를 이용하여 암호화된 암호문에 2차 디바이스 불변정보인 DCI를 결합하여 DcP 암호문을 생성하도록 설계한다.

Table 1. Design of DcP Encryption Structure

```
Cipherkey = < DES, RSA key etc>
cP Ciphertext() = <Cipherkey, password>
DCI() = Device Constant Information
                        /* MAC or IP address etc
DcP Ciphertext() = cP Ciphertext() ‖ DCI()
```

sPF 구조는 디렉토리 path와 파일명을 포함하고 있으며 그 구조는 Table 2와 같다.

Table 2. Design of sPF Encryption Structure

```
Cipherkey = < DES, RSA key etc>
character = alphabet ‖ number ‖ character      sPF
= < directory path, file name>
sPF path() = </character/character/ ... >
sPF file() = <character.spf>
sPF Cipherpathname() = <Cipherkey, sPF path()>
sPF Cipherfilename() = <Cipherkey, sPF file()>
```

여기서 사용한 첨자()는 송수신 식별을 위한 첨자로 송신 암호화 측에서는 (S), 복호화 측에서는 (R)을 사용하기 위한 식별자이다.

3.2.2 DcP 암호화/복호화 알고리즘

DcP 암호화 알고리즘은 Table 3과 Table 4와 같은 암호화 알고리즘과 복호화 알고리즘으로 구성하며, 암호화 알고리즘은 기존방식인 암호화(DES 또는 RSA 등) 기법으로 암호화한 패스워드 암호문 cP(S)에 디바이스 불변정보인 DCI(S)를 첨가하여 암호문 DcP(S)을 생성하도록 Table 3과 같이 설계한다.

Table 3. DcP Encryption Algorithm

```
<DcP Encryption Algorithm>

  cP ciphertext(S )= DES or RSA encryption
                        result of the passwd text
  get source any device DCI(S)
  DcP ciphertext(S) = cP ciphertext(S) ‖ DCI(S)
                              /*concatenation*/
  put DcP ciphertext(S)
  Sending or stored DcP ciphertext(S) for user
            or server user authentication system
```

DcP 암호문을 복호화하는 알고리즘은 Table 4와 같으며, 수신된 암호문 DcP(R)을 암호문 cP(R)과 첨가된 DCI(R)를 분리하고, 현재 저장되어 있는 DCI와 분리된 DCI(R)와 비교하여 동일할 경우 분리된 암호문을 복호화하여 평서문으로 변환하도록 설계한다.

Table 4. DcP Decryption Algorithm

```
<DcP Decryption Algorithm>

  Received or get DcP ciphertext(R)
  cP ciphertext(R) = cP ciphertext(R) in DcP
  DCI(R) = destination DCI(R) in DcP
          /*splitting cP cipher text and DCI */
  get source any device DCI
  if DCI = DCI(R)
    then
        plain text = DES or RSA decryption
                     result of the cP cipher text
        put plain text
    else
        Decryption   Error
```

3.2.3 암호화된 저장 위치명/파일명 생성 알고리즘

암호화될 저장 위치명/파일명(secured Path and File name: sPF)의 생성과 암호화 알고리즘은 Table 5와 같다. 사용자 ID(userID)를 암호키, 저장 위치(sPFpath)를 /etc/userID/로, 저장 파일명(sPFfile)을 userID로 기본(default) 값으로 지정가능하나, 필요에 따라 변경할 수 있도록 설계한다.

Table 5. sPf Encryption Algorithm

```
<sPf Encryption Algorithm>

  sPF = < directory path, file name>
  sPF path(S) = </etc//useID/DCIASpwd/>
  sPF file(S) = <userID.spf>
                          /* Initial value */
  sPF Cipherpathname(S) = DES or RSA
          encryption result of the sPF path(S)
  sPF Cipherfilename(S) = DES or RSA
          encryption result of the sPF file(S)

<sPf Decryption Algorithm>

  Received or get sPF Cipherpathname(R) and
                    sPF Cipherfilename(R)
  sPF path(R) = DES or RSA decryption result
                of the sPF Cipherpathname(R)
  sPF file(R) = DES or RSA decryption result
                of the sPF Cipherfilename(R)
  if pathname = sPF path(R)
          and filename = sPF file(R)
    then
        Perform user authentication process
                /* DcP decryption process */
    else
        User authentication is fails!
```

3.3 DCIAS 동작 과정

DCIAS 패스워드와 패스워드 저장 위치명/파일명의 암호화/복호화 동작과정은 다음과 같다.

3.3.1 DCIAS 암호화 동작과정

DCIAS 암호화 동작과정은 설계된 알고리즘에 따라 다음 Fig. 1과 같이 동작한다.

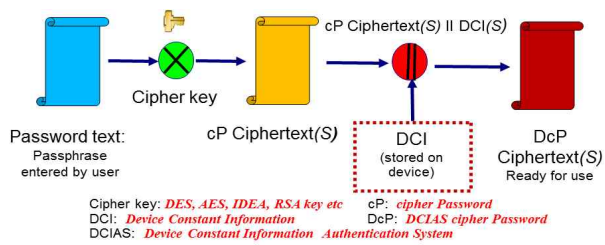

Fig. 1. Encryption process using DCIAS

먼저 패스워드 평서문을 암호화(DES 또는 RSA) 기법을 이용하여 암호화하여 암호화된 패스워드 cP(S)을 생성하고, 여기에 디바이스가 가지고 있는 불변정보 DCI(S)를 결합 첨가하여 DCIAS 암호문(S)을 생성한다. 이러한 암호화 과정을 통해 생성된 DCIAS 암호문 즉, DcP(S) 형태로 저장하거나 필요에 따라 전송하여 사용자가 활용하도록 한다.

3.3.2 DCIAS 복호화 동작과정

DCIAS 복호화 동작과정은 설계된 알고리즘에 따라 다음 Fig. 2와 같이 동작한다.

먼저 저장되어 있거나 수신된 DCIAS 암호문 DcP(R)에서 암호화된 암호문(R)과 cP(R)과 DCI(R)를 분리한다. 분리된 DCI(R)는 현재 디바이스가 가지고 있는 DCI와 비교하여 암호문 cP(R)의 복호화 여부를 결정한다.

내장된 DCI와 수신된 DCI(R)가 동일하면 수신된 암호문 cP(R)을 암호화 기법을 이용하여 복호화하여 평서문으로 복원하며, 동일하지 않으면 복호화를 시행하지 않고 복호 오류처리를 한다. 복원된 패스워드 평서문은 사용자 인증에 사용된다.

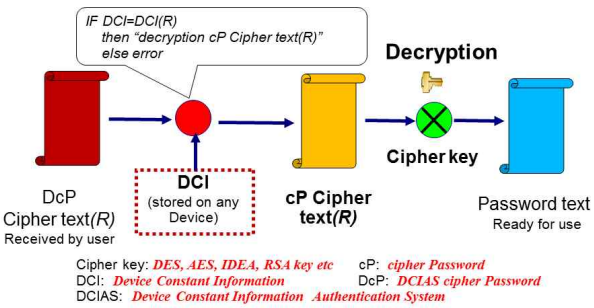

Fig. 2. Decryption process of the DCIAS

3.4 제안 시스템의 보안 특성

설계 제안한 DCIAS 암호 패스워드(DcP)는 1차와 2차의 결합키의 형태로 암호화 기법을 복합적으로 이용할 수 있도록 설계하였다. 따라서 기존의 DES 또는 RSA 암호기법을 사용하여 1차로 암호화하여 암호 패스워드(cP)를 생성함으로써 1차 암호화 기법은 이미 수많은 검증 연구를 통해 보안특성을 만족함이 보장되고 있으며, 2차로 사용되는 디바이스 불변정보 DCI를 이용하여 새로운 암호 패스워드(DcP)을 생성함으로 이 또한 DCI 정보가 자체적으로 디바이스에 내장되어 불변한다는 특성을 가지고 있어 DCIAS에 의해 생성된 패스워드는 사용자 인증 보안 특성을 충족하는데 전혀 문제가 없으며, 3차로 암호

패스워드(DcP)를 저장하는 저장소 즉, 저장위치와 저장 파일을 임의로 생성하여 암호화하여 부여함으로 명확하게 사용자 인증성과 기밀성을 보장할 수 있어 보안강도를 더욱 높일 수 있다.

4. 결론

본 연구는 디바이스 불변 정보를 이용한 사용자 인증 시스템(DCIAS)을 설계 제안하였다. 네트워크상의 시스템 접근 시 사용자 인증에 사용될 접근 디바이스 불변정보를 이용한 새로운 패스워드를 설계 정의하고, 다른 응용들에서 획득한 패스워드를 재사용하는 수동적 재전송 공격으로부터 요구되는 보안 위협에 대처할 수 있도록 신 개념 사용자 인증 시스템을 설계 제안하였다.

설계 제안한 DCIAS는 1차로 기존의 암호화 기법인 DES나 RSA 기법을 이용하고, 2차로 디바이스 불변정보를 이용하여 DCIAS 패스워드를 설계하고 또한 3차로 서버 내에 임의의 암호화된 장소를 설계하여 생성된 암호 패스워드를 저장함으로서 네트워크를 통한 불법적인 시스템 접근 자체를 무력화시킬 수 있도록 설계하였다.

따라서 본 연구 결과로 설계 제안한 DCIAS를 적용하면 어떠한 네트워크를 통하여 시스템에 접근하더라도 어느 곳에 패스워드가 저장되어 있는지를 알 수 없고, 설상 알았다고 하더라고 저장된 패스워드가 암호화되어 있어 해독이 쉽지 않고 네트워크상에 전송 패스워드도 암호화된 패스워드가 전송됨으로 네트워크상의 패스워드 가로채기나 어떠한 재전송 공격이라도 무력화할 수 있다는 강력한 보안 특성을 만족시킬 수 있어 보다 향상된 사용자 인증 보안강도를 증강시킬 수 있을 것으로 기대한다.

ACKNOWLEDGEMENTS

본 논문은 2014학년도에 청주대학교 산업과학연구소가 지원한 학술연구조성비 (특별연구과제)에 의해 연구되었음.

REFERENCES

[1] Hong Gi Kim and Im Yeong Lee, “A Study on One-Time Password Authentication Scheme in Mobile Environment,” *Journal of Korea Multi-media Society*, Vol .14. No. 6, pp. 785-793, Jun. 2011.

[2] H. R. Ryu, N. S. Hong and T. K. Kwon, “Behavioural Analysis of Password Authentication and Countermeasure to Phishing Attacks-from User Experience and HCI Perspectives,” *Journal of Internet Computing and Services(JICS)*, Vol. 15, No. 3, pp. 79-90, Jun. 2014.

[3] Paul Cobbaut, “Linux Security,” http://linux-training.be/linuxsec.pdf, 2015. 5.

[4] Y. R. Pak, “Password Security Technology,” http://www.codeok.net/, 2016. 8

[5] Wikipedia, “MAC address,” https://en.wikipedia.org/wiki/MAC_address, 2016.8.

[6] YUYUJAJEOK, “NAND,” http://pastime0.tistory.com/entry/NAND, 2016. 8.

[7] I. G. Jeun, *Domestic password usage and encryption Implementation Guide*, KISA, 2011. 11.

[8] NCC, “Information Security,” http://www.nacr.cz/dlm/presentations/dresdner.pdf, 2016. 8.

저 자 소 개

김 성 열(Seong-Ryeol Kim) [정회원]

- 1982년 2월 : 숭실대학교 전자계산학과 공학사
- 1987년 2월 : 숭실대학교 대학원 전자계산학과 공학석사
- 1992년 2월 : 숭실대학교 대학원 전자계산학과 공학박사
- 1982년~1984년 : 한국전력공사 전자계산소 근무
- 1984년~1990년 : 오산대학 전자계산과 교수
- 1997년~1998년 : 호주QUT ISRC 객원 교수
- 1990년~현재 : 청주대학교 컴퓨터정보공학과 교수

<관심분야> : 컴퓨터네트워크, 컴퓨터보안, IT융합기술, 사물인터넷