네트워크 바이오 인증 기반 산업기술 유출방지 시스템에 관한 연구★

이대성*

요 약

첨단기술을 보유하고 있는 기업이나 핵심정보를 처리하는 정보기관은 조직의 기밀이 유출되는 시점에서 막대한 경제적 손실은 물론, 치명적인 피해에 따른 조직의 존립 자체가 흔들리게 된다. 기존의 오프라인으로 유출되던 기밀정보는 최근 유비쿼터스 통신 환경을 기반으로, 다양한 장비를 통해 언제든지 네트워크를 통해 유출이 가능해졌다. 본 논문에서는 네트워크로 전송되는 기밀유출을 차단하기 위해 전송되는 모든 패킷에 대해 실시간으로 패킷을 인증하고 차단하는 통신 프로토콜을 제안한다. 특히, 기밀유출을 시도하는 사용자를 구분하기 위하여 전송되는 패킷마다 사용자 바이오 정보를 투명하게 삽입하는 기법을 제시한다. 또한, 실험을 통해 사용자 바이오 정보를 삽입하고 패킷마다 인증하더라도 효과대비 그 성능이 크게 저하되지 않음을 확인한다.

A Study on Industrial Security Outflow Prevention System Based on Network Biometric Authentication

Daesung Lee*

Abstract

Enterprise which has a core technology or organization which manages a core information will be walking into a critical situation like a ruins when organization's confidential information is outflowed. In the past confidential information that was leaked to the off-line, recently the outflow made possible through a variety of equipment at any time via the network based on the ubiquitous communication environment. In this paper, we propose to authenticate and block all packets transmitted via the network at real-time in order to prevent confidentials outflow. Especially in order to differentiate between users who attempt to disclose confidentials, we propose to insert user's biometric information transparently at per-packet basis, and also verify a performance by simulation

keywords : Industrial Security , Per-Packet Authenticaiton, Biometric Authentication

접수일(2011년 09월 09일), 수정일(1차: 2011년 09월 15일)
게재확정일(2011년 09월 16일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

* 경기대학교 산업기술보호특화센터

1. 서 론

최근의 IT(Information Technology) 보안기술은 사이버 공간의 영역을 벗어나 물리 공간으로 확대되고 있으며, 이러한 추세를 반영하여 융합보안 기술에 대한 연구가 활발히 진행되고 있다[1]. 또한, 산업간 융합, 기술간 융합화 추세에 따라 IT 보안기술과 물리보안 기술간의 융합을 통해 산업기밀 유출방지를 위한 새로운 연구개발에 대한 요구가 일어나고 있다.

그 동안 산업기술 유출로 인한 피해액은 꾸준히 증가하여 연간 80조 이상의 경제적 손실이 일어난 것으로 보고되고 있다[2, 3]. 첨단기술을 보유한 기업들은 산업기밀 유출로 인해 새로운 첨단기술의 연구개발 의욕을 상실하고 있으며, 기밀 유출에 따른 경쟁력 약화로 폐업을 하게되는 상황이 발생하기도 한다.

본 연구에서는 산업기밀이 첨단기술을 보유하거나 접근가능한 내부자에 의해 대부분 발생한다는 사실에 착안하여 산업기술 유출방지를 위한 사용자 인증 방법을 제시한다. 현재 사용자 인증 방법은 공인인증서를 이용한 PKI(Public Key Infrastructure) 방식이 주류를 이룬다. 그러나 공인인증서는 대리사용이 가능하기 때문에 산업기밀 유출자의 신분 확인에 있어 그 한계를 드러낸다.

본 논문에서 제안하는 기법은 본인 인증의 요소로써 사용자 바이오정보를 이용한다. 바이오정보를 이용하는 인증 방법은 출입구 등과 같이 현장에서 주로 사용되는 인증 방법이었으나, 최근 바이오 인식기술의 발달과 함께 네트워크를 이용하여 원격으로 인증하는 연구들이 활발히 진행되고 있다[4, 5, 6].

본 연구의 강점은 사용자 바이오정보를 패킷마다 투명하게 삽입하고 인증하여 기술유출이 발생하는 시점에서 사용자 권한등급과 정보등급을 구분하여 패킷의 차단유무를 결정할 수 있다는 것이다. 설령 산업기밀이 유출되었다 하더라도 바이오정보를 이용한 신분확인을 통해 유출자 신원을 정확히 규명할 수 있다.

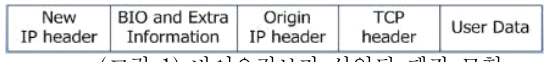
본 논문의 구성은 다음과 같다. 본론에서 산업기술 유출방지를 위해 바이오정보를 패킷마다 투명하게 삽입하는 방법, 바이오정보 암복호화를 위한 키생성 및 분배 방법, 그리고 인증 경량화 방법에 대해 언급하고, 결론에서 제안된 시스템의 비용대비 효과와 향구 연구방향에 대해 언급한다.

2. 본 론

본 논문에서는 산업기술이 네트워크를 통해 유출되지 않도록 하기 위하여 네트워크로 전송되는 패킷마다 사용자 바이오정보를 투명하게 삽입하고 인증 및 차단여부를 결정하는 프로토콜을 제안한다. 첫째로, 패킷 내에 투명성을 보장하는 바이오정보 삽입기술에 대해 알아보고, 둘째로 바이오정보 암복호화를 위한 키생성 및 분배 기법, 마지막으로 바이오정보가 삽입된 패킷 인증 경량화 기법에 대해 살펴본다.

2.1 투명성(transparency)을 보장하는 바이오정보 삽입기술

산업기술 유출방지를 위하여 네트워크로 전송되는 모든 패킷에 대해 실시간으로 사용자 바이오정보를 삽입해야 하며, 사용자 의지와는 무관하게 네트워크 사용 시에 자동으로 바이오정보가 삽입되는 투명성(transprency)이 보장되어야 한다. 이러한 바이오정보의 투명성 보장을 위하여 사용자 바이오정보는 응용프로그램의 데이터로 삽입되는 것이 아니라, (그림 1)과 같이 TCP/IP 프로토콜 스택(stack) 내에 삽입된다.



(그림 1) 바이오정보가 삽입된 패킷 모형

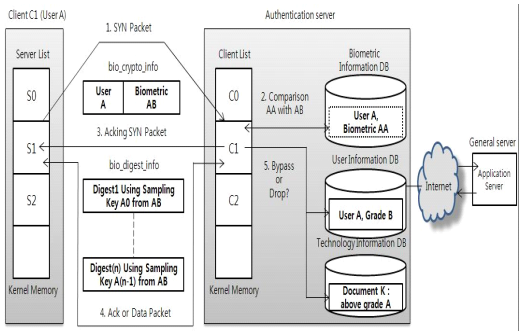
(그림 1)은 IPSec(IP Security)와 유사하게 터널링 기법을 적용하여 패킷을 변조하고 바이오정보를 TCP/IP 프로토콜 스택 내에 삽입한 그림이다. 바이오정보를 TCP/IP 프로토콜 스택 내에 삽입하기 위해 본 연구에서는 커널 모듈 프로그램을 통해 3계층(네트워

(그림 1)의 바이오패킷 흐름에 의한 산업기술 유출방지 처리과정은 (그림 2)와 같다.

(그림 2)의 1단계는 클라이언트가 일반서버로 전송하는 SYN 패킷을 중간 인증서버에서 들여다보는 과정을 보여준다. 이때 전송되는 SYN 패킷은 일반적인 TCP SYN 패킷과 다르다. 전송되는 SYN 패킷은 사

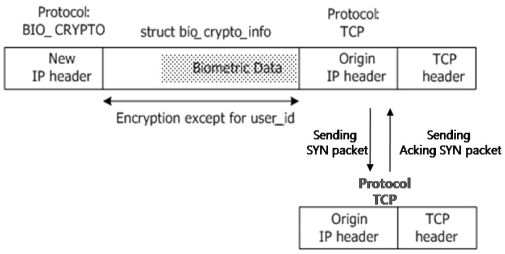
용자 A의 암호화된 바이오정보(AB)를 포함하고 있다.

(그림 2)의 2단계는 실시간으로 수집되어 전송된 바이오 정보(AB)를 데이터베이스에 등록되어 있는 바이오 정보(AA, 사용자가 현장 방문하여 등록한 바이오 정보)와 비교하여 인증한다. 이때, 비교되는 두 바이오 정보(AA, AB)가 100% 일치하거나 일정 경계(threshold) 값을 만족시키지 못하면 인증에 실패한다. 실시간으로 수집되어 전송된 바이오정보는 바이오정보의 특성상 데이터베이스에 저장되어 있는 바이오 정보와 100% 일치하는 것이 거의 불가능하기 때문에, 이 경우는 복사본으로 간주하고 실패 처리한다.



(그림 2) 산업기술 유출방지 바이오패킷 흐름도

인증이 성공하면 클라이언트(C1)에 관한 정보(바이오정보, IP주소, 포트번호 등)는 인증서버의 Client List 자료 구조 형태로 커널 메모리에 현재 세션 기간 동안 유지되고, 바이오정보를 포함했던 패킷은(그림 3)과 같이 중간 인증서버에서 변형되어 외부로 전송된다.



(그림 3) 인증서버에서 변조되는 패킷 변화
(SYN 또는 Acking SYN 패킷 경우)

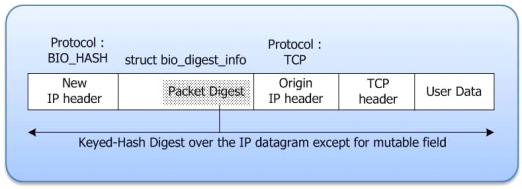
(그림 3)의 3단계는 TCP/IP 3-방향 핸드쉐이크 프로토콜 과정에서 일반서버가 보내는 Acking SYN 패킷을 중간 인증서버에서 (그림 3)과 같이 바이오정보가 포함된 패킷 형태로 변조하여 보내게 된다. 중간 인증 서버가 보내는 Acking SYN 패킷도 일반적인 TCP Acking SYN 패킷과 다르다. 이때 보내는 Acking SYN 패킷은 향후 통신에 있어 HMAC[7] 해쉬 계산을 위한 암호키를 바이오정보로부터 어떻게 추출할 것인지에 대한 지시 사항을 포함하고 있다. 이러한 지시 사항은 클라이언트가 (그림 2)의 1단계에서 보냈던 SYN 패킷처럼 bio_crypto_info 구조체 내에 포함된 형태로 일회성 세션키를 통해 암호화되어 전송된다.

클라이언트는 SYN 패킷 전송 시에 실시간으로 수집된 바이오 정보((그림 3)의 회색 영역)와 추가적인 정보(바이오정보의 크기, 시퀀스 번호 등)를 bio_crypto_info 구조체에 포함시킨 후 사용자 ID를 제외하고 bio_crypto_info 구조체를 일회성 세션키로 암호화하여 전송한다.

중간 인증서버가 Acking SYN 패킷을 전송 시에도 bio_crypto_info 구조체 형태로 암호화되어 전송되며, 이 때는 향후 통신에 있어 클라이언트가 바이오정보로부터 HMAC 해쉬 암호키를 어떻게 추출할 것인지 알려주는 지시를 담고 있다.

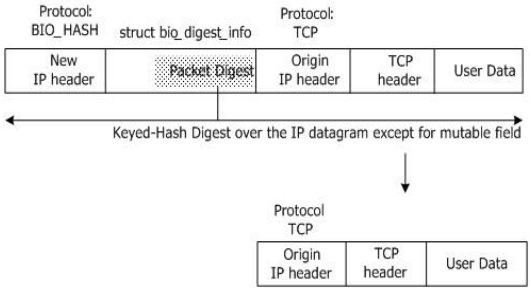
(그림 2)의 4단계에서는 클라이언트가 마지막 ACK 패킷을 전송함으로써 TCP 3-방향 핸드쉐이크를 완성한다. 이때부터 (그림 2)의 3단계에서 서버가 알려준 지시에 따라 난수를 생성하고 바이오정보 중에서 생성된 난수로부터 56 비트(bit) 영역을 추출하고 이 영역을 바이오패킷의 HMAC 해쉬 계산용 암호키로 사용한다.

(그림 4)는 클라이언트가 전송하는 마지막 ACK 패킷과 TCP 3-방향 핸드쉐이크 완성 후 데이터 통신에 사용되는 패킷의 모양을 나타낸다. 바이오패킷 다이제스트 인증 값((그림 4) 회색 영역)은 원래의 IP 헤더와 새로운 IP 헤더 사이에 위치하며, 패킷 전체에 대한 HMAC 해쉬 값으로 bio_digest_info 구조체 내에 삽입되어 전송된다. 이때 HMAC 해쉬 계산을 위해 사용되는 암호키는 (그림 2) 3단계에서 서버가 알려준 지시로부터 획득한다.



(그림 4) 사용자 데이터 전송 시 패킷 모양

(그림 5)는 데이터 통신 시에 인증서버에서 변조되는 패킷 모형을 나타낸 것으로 인증이 성공하면 일반 패킷 형태로 모양이 변조된 후 외부로 전송된다.



(그림 5) 인증서버에서 변조되는 데이터 패킷의 변화

(그림 2)의 5단계는 TCP 3-방향 핸드쉐이크 완성 후, 데이터 통신 시에 데이터의 정보 등급과 사용자별 권한등급을 비교하여 패킷 차단여부를 결정하는 과정이다. 사용자 권한등급보다 데이터 정보등급이 높은 경우는 패킷을 차단하여 외부로 유출되지 않도록 한다.

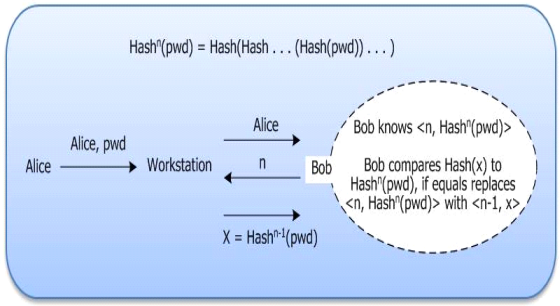
2.2 바이오정보 암복호화를 위한 키생성 및 분배 기법

네트워크로 전송되는 사용자 바이오정보는 개인의 중요 기밀정보이기 때문에 반드시 암호화하여 전송하는 것이 필요하다. 본 논문에서는 다양한 암호키 교환 기법들 중에서 Lamport 일회성 패스워드 기법[8]을 적용하여 바이오정보 암호화를 위한 암호키를 공유한다.

■ Lamport 일회성 패스워드 인증

산업기밀 유출은 주로 조직의 내부에서 발생한다. 따라서, 공유된 비밀환경의 구성이 용이하므로 양자간에 암호키 교환이 언제나 가능하다. 본 논문에서는 Lamport 일회성 패스워드 인증 기법을 적용하여 로그인 시마다 암호키가 변화되도록 하였다.

Lamport는 안전하지 않은 통신 채널을 통해 일회성 패스워드들을 생성하고 이를 인증하는 기법을 제시하였다. (그림 6)은 Lamport의 일회성 패스워드 인증 기법을 나타낸다. Alice는 초기 패스워드(pwd)를 반복적으로 일방향 해쉬 함수에 적용하여 일련의 패스워드를 미리 계산한다. Alice가 최초 로그인 전에 Bob은 이미 마지막 해쉬 함수 값 $H^n(pwd)$ 과 일방향 해쉬 함수 H 가 적용될 횟수 n을 알고 있다.



(그림 6) Lamport 일회성 패스워드 인증

x 번째 로그인 시에 Alice는 $H^{n-x}(pwd)$ 을 전송하고 Bob은 해쉬 함수를 한번 더 적용한 $H(H^{n-x}(pwd))$ 를 계산하고 인증한다. 인증이 성공하면 Alice가 보냈던 일회성 패스워드 $H^{n-x}(pwd)$ 와 해쉬 함수의 적용 횟수 $n-x$ 만을 기억한다. 다음 $x+1$ 번째 로그인 시에도 같은 방법을 적용하여 인증에 성공할 경우, Bob은 기억하고 있던 $< H^{n-x}(pwd)$, $n-x >$를 $< H^{n-x-1}(pwd)$, $n-x-1 >$로 변경한다.

2.3 바이오패킷 인증 경량화 기술

전송되는 패킷마다 바이오정보를 암호화/복호화하는 과정은 고비용을 초래한다. 본 논문에서는 최초 통

신연결 요청 패킷인 SYN, Acking SYN 패킷인 경우만 바이오정보 암복호화를 수행하고, TCP 3-방향 핸드쉐이크 완성 이후 데이터 통신 시에는 HMAC 해쉬 기법에 기반하여 패킷 인증을 경량화 한다.

```
sturct bio_crypto_info {
    char user_id[20];    /* Not Encrypted. The user_id for search of already exchanged session key */
    ---------- Encrypted Area ----------
    struct bio_crypto_header {
        unsigned long c_sequence;     // sequence number for anti-replay attack
        int seed_RNG;                 // the seed value for random number generator
        int mod_divisor;              // the divisor of modulous operation
    } c_header;
    struct bio_crypto_data {
        unsigned int real_crypto_len;          // the size of biometrics-data
        unsigned char bio_data[BIO_FULL_SIZE]; // lively collected biometrics-data
    } c_data;
};

struct bio_digest_info {
    struct bio_hash_header {
        unsigned long h_sequence;     // sequence number for anti-replay attack
        unsigned int key_start_bit;   // the start-bit number in the biometrics-data used as
                                      per-packet symmetric-key for message authentication code
    } h_header;
    struct bio_hash_data {
        unsigned int real_hash_len;   // the size of a digested message
        unsigned char HMAC_SHA1_result[SHA1_DIGEST_SIZE];  // the digest over the IP datagram
    } h_data;
};
struct list_head {struct list_head * next; struct list_head * prev; };

struct host_list {
    struct list_head list;          // list chain
    int int isServer;               // 1 : server,  0 : client
    unsigned int list_key[2];       // the searching key for host_list (source address, port and destination port bitwise-OR)
    unsigned int origin_pmtu;       // original path MTU(Maximum Transmit Unit)
    unsigned char DES_eKey[16][8];  // encryption key
    unsigned char DES_dKey[16][8];  // decryption key
    struct bio_crypto_info host_bio;// the saving area for biometrics-data
} server_list, client_list;
```

(그림 7) 시스템 구현에 사용되는
주요 자료구조 예시

(그림 7)은 본 연구의 구현에 있어 사용되는 주요 자료구조들을 보여준다. bio_crypto_info구조체는 TCP 3-방향 핸드쉐이크 프로토콜에서 사용되는 구조체로 암호화되어 전송되고, bio_digest_info 구조체는 실제 데이터 통신에 사용되는 구조체이다.

bio_crypto_info 구조체에서는 bio_data 와 seed_RNG, mod_divisor가 중요하다. bio_data에는 클라이언트에서 수집된 바이오 정보가 들어있다. seed_RNG와 mod_divisor는 (그림 2)의 3단계에서 바이오정보 인증에 성공했을 경우에 인증서버가 클라이언트에게 보내는 지시로써 seed_RNG는 난수생성 함수에 대한 근원(seed) 값을, mod_divisor는 생성된 난수로부터 나머지 연산 적용 시에 제수(divisor)를 나타낸다.

$$key\_start\_bit = RNG(seed\_RNG)\ \%\ \mathrm{mod}\_divisor \quad [식\ 1]$$

[식 1]은 클라이언트가 초기 SYN 패킷 인증과정에서 공유된 바이오정보로부터 일정영역을 추출하여 HMAC 키를 계산하는 식이다. RNG는 난수 생성 함수(Random Number Generator)이며, 계산된 key_start_bit는 실시간으로 수집된 바이오정보 중에서 HMAC 키의 시작 위치에 대한 비트 색인(index) 값이다.

(그림 7)의 bio_digest_info 구조체에서 key_start_bit과 HMAC_SHA1_result는 클라이언트가 생성하여 전송하는 것으로 key_start_bit는 [식 1]에 의해 계산된 해쉬 계산을 위한 암호키의 시작위치이고, HMAC_SHA1_result는 암호키를 이용하여 계산되는 패킷 전체에 대한 HMAC 다이제스트 값이다.

이와 같이 기 전송되어 공유된 바이오정보로부터 해쉬용 암호키를 생성하고 패킷마다 암호키를 이용한 인증 다이제스트 값을 첨부하여 전송한다(그림 4). 패킷마다 암호화를 하지않고 속도가 빠른 해쉬 인증 기법을 통하여 인증 비용을 최소화한다.

3. 결 론

산업기밀과 같은 중요정보를 처리하는 조직이나 단체는 본인 인증 시스템이 완벽히 이루어져야 한다. 산업기밀이 유출되었을 경우, 언제 누구로부터 어떻게 유출되었는지 확인할 수 있어야 하기 때문이다. 이러한 완전범죄가 불가능한 인증 시스템의 도입은 상대적으로 산업기밀이 유출되는 것을 최소화할 수 있다.

현재 사용자 본인을 인증하는 대표적인 방법으로는 공인인증서를 이용한다. 그러나, 공인인증서는 대리 사용이 가능하기 때문에 사용자 본인에 대한 인증이라기보다는 공인인증서를 이용하는 시스템이나 해당 프로세스에 대한 인증으로 해석할 수 있다.

본 논문에서는 산업기밀 유출방지를 위한 사용자 인증의 방법으로 사용자 바이오정보를 삽입하고 인증하는 방법을 제시하였다. 특히, 사용자 바이오정보를 SYN 패킷과 같은 통신 연결요청 시점에서부터 삽입하여 전송함으로써 Dos 공격의 한 형태인 SYN flooding 공격을 방어할 수 있으며, 패킷마다 인증함으로써 악의적인 사용자에 의한 중간자 공격을 방어할 수 있다.

또한, 패킷마다 인증하는데 소요되는 고비용을 줄이기 위해 최초 통신 연결요청 시에만 암호화/복호화를 수행하고 실제 데이터 통신 시에는 수집된 바이오정보의 일부를 암호키로 사용하여 패킷에 대한 다이제스트를 계산함으로써 패킷마다 인증하는 데 소요되는 비용을 최소화 하였다.

제안된 기법들은 리눅스 운영체제에서 Netfilter를 이용하여 커널 모듈로 구현되었다. 커널 모듈로 구현되었기 때문에 모듈의 추가 및 삭제가 용이하며 IP 계층에서 구현되었기 때문에 바이오정보 삽입의 투명성을 제공할 수 있었다.

실험을 통해 확인한 결과, 바이오정보를 이용한 패킷 인증 기법은 패킷마다 인증하는 유사기법들과 비교 실험한 결과 평균 1.16배의 시간이 소요됨을 확인하였다. 네트워크 바이오인증 시스템의 효율성을 고려했을 때 1.16배의 시간 소요는 가치있는 시간으로 판단될 수 있으며, 최적화 기법을 이용하여 성능을 개선한다면 기존의 기법들과 성능면에서 동일할 것으로 생각된다.

향후 연구로는 멀티캐스트와 같은 다자간 통신에 있어서도 산업기밀 유출방지를 위해 바이오정보를 이용하여 사용자 신원을 확인하는 연구가 진행되어야 할 것이다.

참고문헌

[1] 국가사이버안전센터, “유비쿼터스 네트워크 구현에 필수적인 정보보호(유비쿼터스 보안) 기술 동향분석”, 국가정보원, 2004

[2] 임영모, “핵심기술 해외유출의 실태와 대책” 삼성경제연구소,2004

[3] 임영모, “기술유출의 실태와 대책”, 삼성경제연구소, 2005

[4] H. S. Kim, S. W. Lee, and K. Y. Yoo, “ID-based Password Authentication Scheme using Smart Cards and Fingerprints”, ACM Operatin Systems Revie, pp.32-44, 2003

[5] M. Scott, "Cryptoanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints", Cryptology ePrint Archive Report, 2004

[6] D. S. Lee, K. C. Kim, and Y. B. Yoo, "IPBio: Embedding Biometric Data in IP Header for Per-Packet Authentication", Lecture Notes in Computer Science, pp. 927-938, vol 4331, 2006

[7] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, 1997

[8] L. Lamport, "Password Authentication with Insecure Communication", Communications of the 43th Annual IEEE Symposium on Foundations of Computer Science(FOCS), pp. 271-282, 2002

[저 자 소 개]

이 대 성 (Daesung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사

email : xdilemma@naver.com