한국산학기술학회논문지
Vol. 11, No. 10 pp. 3958-3963, 2010

안전한 통신을 위한 메신저 프로토콜 설계

신승수[1*], 한군희[2]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부

A Design of Messenger Protocol for Secure Communication

Seung-Soo Shin[1*] and Kun-Hee Han[2]
[1]**Dept. of Information Security, College of Information & Communication, Tongmyong University**
[2]**Division of Information & Communication Engineering, Baekseok University**

요 약 인터넷 메신저는 개인뿐만 아니라 기업에서도 많이 사용하고 있다. 메신저는 메일, 쪽지, SMS 서비스 등의 많은 기능을 제공하고 있다. 이러한 서비스를 제공하고 있는 메신저는 보안상의 많은 문제점이 제기되고 있다. 기존 Nate-on은 사용자의 개인 정보를 서버 DB에 저장을 하여 내부자 공격에 노출되고, 클라이언트간의 데이터 또한 네트워크상에 단순히 전달되었다. 이러한 정보 노출 문제점을 해결하기 위한 프로토콜을 제안한다.

Abstract Internet messenger applications are utilized not only by individuals but also in corporate environments since it provides many convenient functions such as email, chatting and SMS services. However convenient they may be, current messenger applications have revealed a great deal of security problems. For instance, the existing Nate-on messenger is exposed to internal threats since it stores sensitive information in the database of its server and transmits communication data through the network without any safety measures intact. In order to solve such problematic issues of existing messenger applications, we propose the following protocol.

Key Words : Nate-on, Sniffing, MD5, SHA-1, SMS, Session-key

1. 서론

초고속 인터넷이 널리 보급되면서 오프라인에서만 가능했던 많은 서비스들은 온라인에서도 사용할 수 있게 되었다. 현재 보편화된 온라인 메신저 중에서 특히 네이트온 메신저는 국내에서 가장 많은 사용자에게 서비스를 하고 있다. 네이트온 메신저는 쪽지, 채팅, E-Mail, 화상대화, 원격접속 서비스, SMS(Simple Message Service) 또는 MMS(Multimedia Messaging Service)를 통하여 휴대폰으로 메시지를 전송하는 서비스들을 이용하거나 SSO(Single Sign On) 기능 등의 수많은 서비스들을 제공하고 있다[1].

네이트온의 인증 메커니즘은 사용자의 정보들이 암호화되어 전송되도록 하고 있다 그러나 네이트온은 인증정보를 만들 때 동일 사용자에 대해서는 항상 동일한 인증정보를 생성한다. 그 결과 공격자가 임의의 사용자에 대한 인증정보가 네트워크로 전송되는 것을 확인할 수 있다면 공격자는 그 인증정보를 가지고 재전송공격(Replay Attack)을 할 수 있다. 이를 통해 공격자는 다른 사용자로 가장할 수 있다. 또한 공격자는 사전공격(Dictionary Attack)을 통해 획득한 인증정보에서 직접 사용자의 패스워드를 추출할 수도 있다. 그러나 네이트온의 재전송공격 및 패스워드 취약점은 2007년에 발표되었다. 이후 네이트온 메신저의 보안 업그레이드를 통해 해당 취약성이 보완되었으며, 현재는 앞에서 설명하고 있는 공격이 불가능하다. 그러나 이외에도 네이트온의 취약점은 통신내용에서 사용자간의 메시지가 그대로 노출된다[2].

이러한 문제점을 해결하기 위해 윤영준 등[3]이 프로토콜을 제안하였다. 윤영준 등[3]은 Alice가 Bob에게 난수를 전달하여 세션키를 생성하였지만, 본 논문에서 제안한 프로토콜은 두 클라이언트가 동일한 난수를 이미지

*교신저자: : 신승수(shinss@tu.ac.kr)
접수일 10년 08월 20일 수정일 10년 09월 29일 게재확정일 10년 10월 15일

배열을 통해 얻은 128비트의 입력값을 확장된 P-Box를 통해 256비트의 확산된 출력값을 생성하여 사용함으로써 스니핑 공격과 그 밖의 다양한 공격에 대한 안전성과 효율성이 향상된 프로토콜을 제안한다. 제안한 프로토콜은 서버 관리자 또는 제3자는 악의적인 의도로 사용자의 중요 정보를 알 수 없고 네트워크상에 노출되었던 클라이언트간의 통신내용도 알 수 없다.

본 논문의 구성은 다음과 같다. 2장에서는 국내·외 연구동향에 대해서 분석하고, 3장에서는 새로운 프로토콜을 설계를 한다. 그리고 4장에서 제안한 프로토콜을 스니핑과 다양한 공격에 대한 안정성을 분석한 후, 마지막으로 5장에서 결론을 맺는다.

2. 연구 동향

2.1 그래픽 패스워드

본 논문에서는 Client간의 사용되는 N(nonce)은 그래픽 패스워드를 응용하여 세션 키로 활용하게 된다. 이 그래픽 기반의 패스워드에 관한 연구에 대해 살펴본다.

알파벳-숫자 패스워드는 사람의 기억력에 단순하게 의존하게 된다. 그러나 이미지를 패스워드로 사용하는 그래픽 패스워드(Graphical Password) 기법에서의 인간의 두뇌 작용은 더욱 복잡하다. 그림에 대한 기억력은 연상이나 회상을 동반하게 되는데, 그 결과 사람은 과거에 선택하였던 이미지 등을 더 오래 더 정확하게 기억할 수 있을 것으로 보인다[4].

이러한 그래픽을 이용한 인증 방법 중에 하나인 PassfacesTM의 기본 바탕이 되는 Calentine의 연구에 의하면, 사람의 얼굴은 알파벳-숫자 패스워드에 비하여 연상이 용의하고 오래도록 기억하기 수월하다고 한다[5].

대표적인 그래픽 패스워드 기법들은 RealUser.com에서 개발하고 판매하고 있는 인식 기반의 이미지 인증 시스템인 PassfacesTM, 해시 가시화(Hash Visualization) 기법을 사용하여 패스워드 대신 사용하는 PassIcons, PassStrings, PassPoints등이 있다. 또한 이렇게 그래픽 이미지를 선택함으로써 인증을 수행하는 기법들 이외에도 PDA 등에 그림을 그림으로써 인증을 수행하는 DAS(Draw-A-Secret)와 알고 있는 이미지에 의하여 전혀 다른 결과를 도출하도록 하는 인지 인증(Cognitive Authentication) 기법이 있다[6].

2.2 메신저에 대한 공격기법

스니핑(sniffing)은 해킹기법으로서 네트워크를 통해 전송되는 패킷들을 훔쳐보는 것을 말한다. 다시 말해 공격자가 악의적인 목적을 갖고 네트워크 트래픽을 도청하는 것을 스니핑이라고 한다.

스니핑이라는 기술이 공격에 활용될 수 있는 것은 TCP/IP 프로토콜 설계상의 문제라고 할 수 있다. TCP /IP가 이와 같이 설계된 이유는 인터넷이 활성화되기 이전에 설계된 TCP/IP 프로토콜은 주로 학술적인 목적으로 사용되었기 때문이다. 그러므로 TCP/IP 프로토콜은 특별히 보안이 고려되지 않은 상태로 사용되고 있다. 그 결과 누구나 네트워크에서 TCP/IP 패킷들을 잡아서 내용들을 열람할 수 있었다. 하지만 인터넷이 TCP/IP 프로토콜 기반으로 활성화되었기 때문에, 인터넷의 각 호스트들이 패킷들을 송수신하면서 기밀성과 무결성 등의 보안 요소들을 전혀 제공받지 못한다. 그렇기 때문에 공격자가 스니핑이라는 기술을 이용하여 네트워크를 통해 전송되는 패킷들을 잡을 수 있으며, 이 패킷이 담고 있는 데이터의 내용을 모두 열람할 수 있게 된다[7].

네이트온 메신저 프로그램은 인증정보 생성 방법에 따라 사용자별로 다른 MD5 해시 값을 전송하겠지만 해시 함수의 인자로 고정된 문자열인 사용자 패스워드와 사용자 ID 또는 E-Mail 주소만 사용하기 때문에 동일한 사용자에 대해서는 항상 동일한 해시 값을 인증서버로 보내게 된다. 그러므로 공격자가 임의의 사용자에 대한 해시 값을 얻을 수만 있다면, 공격자가 인증 서버의 IP 주소를 얻고 획득한 사용자의 해시 값을 가지고 재전송 공격이 가능하다. 뿐만 아니라, 공격자는 스니핑을 통하여 얻은 사용자의 E-Mail 주소와 인증정보인 해시 값(패스워드||E-Mail주소)을 이용하여 사용자의 패스워드를 검출할 수 있다. 즉 유추된 패스워드와 사용자의 E-Mail을 해시 함수에 입력한 후, 그 해시 값을 스니핑을 통해서 얻은 해시 값과 비교하여 일치하면 해당하는 패스워드가 사용자가 사용하는 패스워드인 것이다. 이때 사용하는 해시함수는 속도가 빠르다고 검증된 알고리즘이다. 따라서 해시 값을 유추된 패스워드와 사용자의 E-Mail에 대한 해시함수에 대한 해시 값을 스니핑을 통해서 얻은 해시 값과 비교하는 모든 과정도 빠르게 구현될 수 있다[1].

3. 제안 프로토콜

본 논문에서 제안한 프로토콜에서는 중요한 개인정보는 사용자만이 알 수 있는 개인키로 암호화되어 있기 때문에 서버 관리자 또는 제3자는 악의적인 의도로 사용자의 중요한 정보를 알 수 없다. 또한 네트워크상에 노출되었던 통신 내용도 송·수신과정에서 암·복호화되기 때문에 안전한 통신을 할 수 있다. 안전한 메신저 통신을 위

해 본 논문에서 사용될 표기법은 표 1과 같이 정의한다.

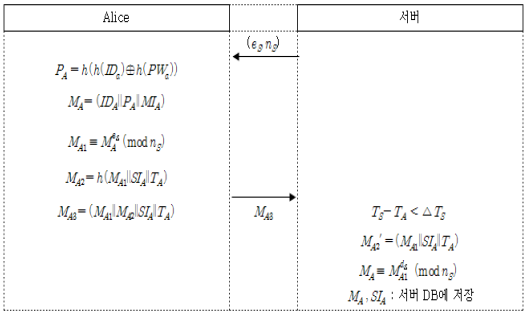
[표 1] 표기법

기호	설명
ID_A	엘리스의 아이디
PW_A	엘리스의 패스워드
M_A	엘리스의 메시지
P_A	엘리스의 로그인 패스워드
MI_A	엘리스의 공개 정보
SI_A	엘리스의 비밀 정보
T_A	엘리스의 타임스탬프
(e_A,n_A)	엘리스의 공개키
d_A	엘리스의 개인키
$\oplus$	배타적 논리합
N_A	앨리스의 난수
$h()$	해시함수

기존 네이트온에서 쪽지 패킷 정보에는 사용자의 ID와 E-Mail 주소, 사용자간의 데이터 송·수신시 중요한 정보 등이 그대로 노출되는 문제점이 있다. 이러한 중요 정보들을 보호하고자 새로운 프로토콜을 제안한다. 제안한 프로토콜은 회원가입 단계, 로그인 단계, 쪽지·채팅에 필요한 난수 생성 및 전송 단계, 세션키 생성 단계로 구성 된다.

3.1 회원가입 단계

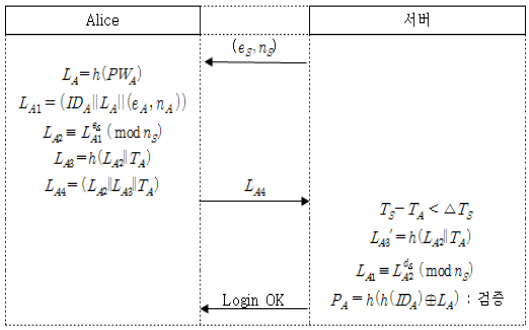
Alice는 회원가입 시 서버로 연결요청을 하고 서버는 Alice에게 1024비트의 공개키(e_S,n_S)를 생성하여 송신한다. Alice는 수신한 서버의 공개키를 저장하고, 자신의 중요한 정보(비밀번호, 주민번호, 전화번호, 우편번호, 상세주소)를 암호알고리즘을 적용한 다음 서버로부터 받은 공개키로 암호화하여 서버에게 전송한다. 이러한 과정은 다음 그림 1과 같다.



[그림 1] 회원가입 단계

3.2 로그인 단계

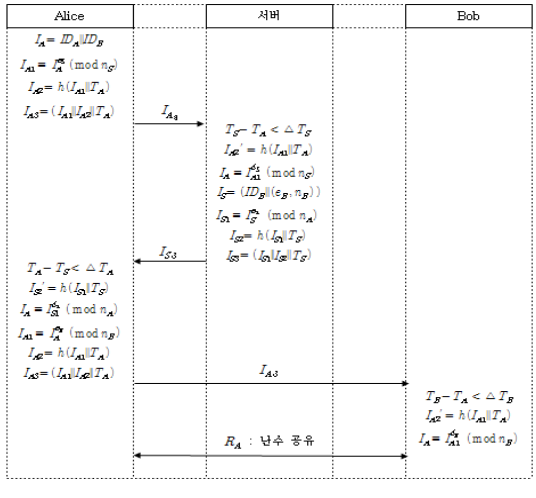
Alice는 회원가입을 마치고 메신저 서버로 접속하기 위해 ID_A, PW_A을 입력하고 접속을 한다. 로그인 과정은 다음 그림 2와 같다.



[그림 2] 로그인 단계

3.3 쪽지·채팅에 필요한 난수 생성 및 전송 단계

윤영준 등[3]이 제안한 프로토콜에서는 난수를 세션키로 사용하여 통신 내용을 송·수신 시 암·복호화하여 사용하였다. 그러나 본 논문의 프로토콜에서는 클라이언트가 쪽지·채팅을 하기 위하여 난수를 생성하여 다른 클라이언트에게 전송하고, 클라이언트들은 난수로부터 이미지 배열과 확장된 P-Box를 통하여 세션키를 생성한다. 송·수신 시 암·복호화에 필요한 키를 따로 전송할 필요가 없다. 쪽지·채팅에 필요한 난수 생성 및 전송단계 과정은 다음 그림 3과 같다.



[그림 3] 쪽지·채팅에 필요한 난수 생성 및 전송 단계

3.4 세션키 생성 단계

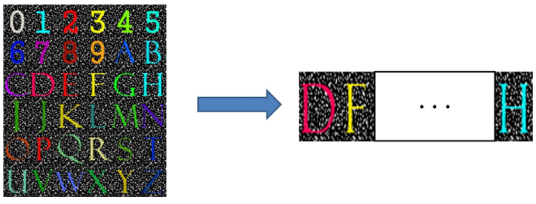
Alice가 Bob과 쪽지·채팅을 원할 경우, 먼저 쪽지· 채팅에 필요한 세션키를 공유하기 위해서 Alice는 Bob에게 난수를 전달한다. Bob은 수신된 난수를 확장된 P-Box에 입력하여 세션키를 생성한다. 세션키를 생성하는 과정은 다음과 같다.

① Alice는 Bob에게 난수를 전달하고, Alice와 Bob은 서로 공유된 난수를 가지고 $h(R_A)$을 계산한다.

② $h(R_A)$의해서 생성된 128비트(8비트 * 16개)의 해시 값을 각각 $(\mathrm{mod}\ 36)$을 하여 얻은 값을 정수로 변환한다. 그림 4은 숫자(10개), 영문자(26개)로 이루어진 조합된 형태이다.

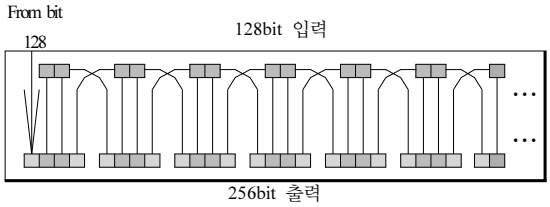
[그림 4] Image 배열

③ 숫자 $13(00001101_2)$을 그림 5의 이미지 배열에서 14번째 이미지 D를 선택한다. 나머지 배열도 동일한 방법을 수행하여 선택한다. 그림 5과 같이 Alice와 Bob은 동일한 이미지를 얻는다.



[그림 5] 이미지 추출

④ Alice와 Bob은 그림 5과 같이 추출된 이미지를 128비트의 입력값을 확장된 P-Box를 통해 256비트의 확산된 출력값을 생성한다. 그림 6와 같은 과정을 통해 얻어진 출력값을 세션키로 사용한다.



[그림 6] Expansion P-box

⑤ Alice는 평문, 쪽지·채팅에 필요한 세션키를 이용하여 암호화하고 Bob에게 송신한다. Bob은 동일한 세션키를 이용하여 복호화한다.

4. 프로토콜 분석

본 논문에서 제안한 프로토콜에 대하여 분석한다. 기존 방식은 사용자의 개인정보를 서버의 데이터베이스에 저장을 하기 때문에 내부자 공격에 취약하고, 클라이언트 간의 통신 내용도 그대로 송·수신되었다. 이러한 정보 노출 문제점을 해결하기 위해 제안한 프로토콜을 스니핑과 다양한 공격에 대한 안전성에 대하여 알아본다.

4.1 스니핑 분석

본 논문에서 제안한 프로토콜은 회원가입 단계, 로그인 단계, 쪽지·채팅에 필요한 난수 생성 및 전송 단계, 이미지 배열을 통한 세션키 생성단계 등으로 구성된다. 이러한 구성 단계별로 스니핑에 대하여 분석한다.

ㅇ 회원가입 단계

제안한 프로토콜에서는 회원가입 단계에서는 Alice의 아이디를 해시한 값과 패스워드를 해시한 값을 배타적 논리합으로 계산한 값을 해시함수를 통해 얻은 P_A를 공격자가 스니핑을 시도하여도 암호학적 해시함수의 일방향성 때문에 Alice의 패스워드 값 PW_A를 알아내지 못한다. 그러므로 Alice의 비밀정보인 SI_A를 계산할 수가 없다. 따라서, Alice의 회원가입 정보를 알 수 없다.

ㅇ 로그인 단계

공격자는 스니핑을 통해 로그인 정보를 획득할 수 있다. 하지만 Alice는 서버의 공개키로 M_{A1}을 암호화하여 보낸다. 그러므로 공격자는 서버의 비밀 키 d_S를 모르기 때문에 계산할 수 없다.

ㅇ 쪽지·채팅에 필요한 난수 생성 및 전송 단계

쪽지·채팅에 필요한 난수 생성 및 전송단계에서 Alice는 Bob의 공개키를 서버를 통해 수신하고 Alice는 Bob의 공개키를 이용해 난수 N_A을 Bob에게 암호화하여 보낸다. 공격자는 스니핑을 통해 수신자로 전달되는 패킷을 획득하더라도 Bob의 개인키를 알 수 없기 때문에 Bob에게 송신된 난수 N_A를 알 수 없다.

ㅇ 세션 키 추출 단계

Alice와 Bob은 서로 공유한 난수로 이미지를 생성하고 확장된 P-Box를 통해서 생성하고 생성된 세션 키 값은 총 16글자로 구성된다. 이미지 배열에 있는 이미지는 숫자(10개), 영문자(26개)로 조합된 형태이다. Alice와 Bob은 쪽지·채팅에서 사용되는 세션키는 256비트 길이를 가진다. 세션키의 경우의 수는 36^{16}개이다. 만약 공격자가 쪽지·채팅에 사용되는 256비트 길이의 세션키를 알아낸다 하더라도 그 다음 쪽지·채팅에서 사용되는 난수를 새로 생성하여 다른 세션키를 사용하기 때문에 안전하게 메시지를 송·수신 할 수 있다.

4.2 다양한 공격에 대한 분석

다음은 본 논문에서 제안한 프로토콜에 대하여 내부자 공격(Insider Attack), 재전송 공격(Replay Attack), 중간자 공격(Man in the Middle Attack), 전방향 안전성(Forward Secrecy)에 대해 분석한다.

ㅇ 내부자 공격(Insider Attack)

기존의 메신저는 서버관리자가 데이터베이스에서 악의적인 의도를 가지고 메신저 사용자의 주민등록번호, 집주소, 전화번호 등을 모두 알 수 있었다. 하지만 제안한 프로토콜은 회원가입 단계에서 최소한의 사용자 정보 MI_A만을 서버에 공개하고 중요한 개인정보 SI_A는 사용자의 PW_A를 SHA-1을 사용하여 생성된 다이제스트 값을 키로 사용하여 암호화하기 때문에 안전하고, 서버로 전달되는 패스워드는 해시함수를 거쳐서 전달되기 때문에 안전하다. 즉, 암호학적 해시함수의 일방향성 때문에 서버관리자라 하여도 사용자의 패스워드나 사용자의 개인정보를 추측 하거나 알 수 없기 때문에 내부자 공격에 안전하다.

ㅇ 재전송 공격(Replay Attack)

A와 B가 서버로부터 인증을 받은 올바른 사용자라고 가정하자. 재전송 공격은 이전의 A와 B사이의 정상적인 프로토콜에서 전송되었던 정보를 공격자가 가지고 있다가 나중에 A 또는 B에게 다시 보내서 프로토콜을 진행하려고 하는 공격이다. 제안한 프로토콜에서 재전송 공격에 대하여 분석한다. 만약, Alice가 서버에 회원가입 시 Eve가 M_{A3}정보를 가로채서 M_{A3}에 있는 T_A를 변경하여 서버에게 전송한다. 서버는 수신한 M_{A3} 정보로부터 첫 번째로 $T_S - T_A \cong \triangle T_S$를 계산하여 검증을 한다. 두 번째로 $M_{A2} = h(M_{A1} \| SI_A \| T_A)$의 정보에도 T_A를 포함하였기 때문에 T_A 변경 시 첫 번째 검증에 통과하더라도 두 번째 검증 M_{A3}에 있는 정보 M_{A1}, SI_A, T_A를 이용하여 서버는 $M_{A2}' = h(M_{A1} \| SI_A \| T_A)$를 계산한다. 따라서, $M_{A2}' \cong M_{A2}$가 성립하지 않는다. 위와 같은 두 가지 검증으로 메시지 재전송 공격에 안전하다.

ㅇ 중간자 공격(Man in the Middle Attack)

중간자 공격이란 공격자가 수신자와 송신자 사이에서 송신자에 대해서는 수신자처럼, 수신자에 대해서는 송신자처럼 행세하는 공격이다. 만약, Alice와 Bob은 쪽지·채팅을 위해서 로그인을 하여야 한다. 로그인이 성공하면 Alice와 Bob은 $L_A = h(PW_A)$과 같이 패스워드를 해시하여 $L_{A2} \equiv L_{A1}^{e_S} \pmod{n_S}$로 서버의 공개키로 암호화하여 서버에 송신한다. 서버는 무결성 및 유효성을 검증하고, 통과되면 서버의 개인키 (d_S, n_S)로 $L_{A1} \equiv L_{A2}^{d_S} \pmod{n_S}$를 복호화하여 데이터베이스에서 Alice와 Bob의 아이디를 찾아서 ID_A , ID_B를 배타적 논리합하여 $P_A = h(h(ID_A) \oplus L_A)$ 값을 검증한다. 로그인을 통해 인증을 통과하여야 쪽지·채팅을 할 수 있기 때문에 재전송 공격에 안전하다.

ㅇ 전방향 안전성(Forward Secrecy)

A가 서버로부터 인증을 받은 올바른 사용자라고 가정하자. 공격자가 A의 개인키나 패스워드를 알아냈다고 해도 이전에 A가 사용했던 어떠한 세션키도 알 수 없을 경우 프로토콜은 전방향 안전성을 만족한다고 한다. 제안한 프로토콜에서는 이전에 사용한 공개키나 세션키의 정보를 저장하지 않고, 한 세션 마다 서버를 통하여 클라이언트간의 난수를 생성하고 난수를 분배하기 때문에 안전하다. 또한, 생성하는 난수는 ANSI x9.17 알고리즘을 이용한 강력한 난수를 제공한다. 그러므로 현재의 공개키로 이전의 세션 키를 계산한다는 것은 불가능하다.

제안한 프로토콜에서는 회원가입 시 5회의 해시함수 연산과 2회의 지수연산 필요하다. 해시함수의 연산은 10만 번 연산 시 0.1㎲~0.2㎲의 시간이 걸린다. 그리고 1024비트로 RSA의 암·복호화 시간을 측정한 결과 암호화 시간은 0.0014002㎲로 나왔고, 복호화 시간은 0.0412006㎲로 비교적 빠른 시간으로 암·복호화를 하였다. 위 결과를 볼 때 로그인 단계와 쪽지·채팅 단계도 1초 미만으로 문제가 되지 않는다. 회원가입 후 사용자가 로그인을 하게 되면 서버는 사용자의 공개키, 사용자는 서버의 공개키를 가지게 된다. 로그인 단계에서 지수연산은 2회에 0.05㎲이다. 현대 컴퓨팅 기술에서는 연산속도에 영향을 미치지 않는다.

5. 결론

기존 네이트온는 사용자의 개인정보를 서버의 데이터베이스에 저장을 하기 때문에 내부자 공격에 취약하고, 클라이언트간의 통신 내용도 그대로 송·수신되었다. 이러한 정보 노출 문제점을 해결하기 위해 새로운 프로토콜을 제안하였다.

본 논문에서 제안한 프로토콜에서는 서버에게 사용자의 최소한의 개인정보만을 공개하고 중요한 개인정보는 사용자만 알고 있는 패스워드로 암호화되어 서버 데이터베이스에 저장한다. 개인정보는 사용자의 패스워드로 암호화되기 때문에 서버관리자 또는 제3자는 악의적인 의도로 사용자의 중요정보를 알 수 없다. 또한 네트워크상에 노출되었던 클라이언트간의 통신내용도 송·수신 시 암·복호화 되어 안전한 통신을 할 수 있다. 본 논문에서 제안한 사용자간의 안전한 통신을 위한 메신저 프로토콜에서는 개인정보유출을 보호하는 다양한 응용분야에서 효율적으로 사용할 수 있을 것이다.

참고문헌

[1] 신동휘, 최윤성, 박상준, 김승주, 원동호,“네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석”, 성균관대학교 정보통신공학부 정보보호연구소, 2007.

[2] 전웅렬, 원동호, 김승주, “국내 상용 제품의 인증 취약성 분석”, 한국정보보호학회, 2009.

[3] 윤영준, 표경환, 신승수, 한군희, “사용자 사이의 안전한 통신을 위한 메신저 설계”, 한국산학기술학회 춘계학술대회 논문집, 2010.

[4] D. Weinshall and S. Kirpatrik,「Passwords You'll Never Forget, but Can't recall」, In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI), pp.1399-1402, 2004.

[5] T. Calentine,「An evaluation of the Passface personal authentication system」, Technical Report, Goldsmiths College, University of London, 1998.

[6] 양대헌, 강전일, 맹영재, 조형상, 니영청, “안전한 패스워드 이용을 위한 키보드 입력 패스워드 대체방안 연구”,인하대학교, 2009.

[7] “네이트온 본인 인증 서비스 실시와 문제점", http://hummingbird.tistory.com/1698.

신 승 수(Seung-Soo Shin) **[정회원]**

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 무선 PKI, 네트워크 보안, USN, 스마트카드,

한 군 희(Kun-Hee Han) **[종신회원]**

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
암호프로토콜, 네트워크 보안, 영상처리