네이트온 인증 방식의 보안 취약점에 대한 대응 방안

노재민, 문정일, 임동현, 김미지, 박혜림

건국대학교 컴퓨터응용과학부

A method for improving security of the NateOn authentication scheme

Jae-Min Noh , Jeung-Il Moon, DongHyoun Lim, MiJi Kim, HyeLim Park

Department of computer science

Konkuk university

요 약

네이트온 메신저는 현재 국내에서 가장 많은 사용자가 이용하고 있는 메신저이다. 그러나 이 메신저에도 사용자를 인증하는 과정에서 보안문제의 취약점이 존재 하였다. 본 논문에서는 네이트온 메신저 프로그램의 인증방식과 그에 따른 취약점을 살펴보고 이를 바탕으로 새로운 인증 제안 프로토콜을 제안하여 문제점을 극복하고자 한다.

Abstract

Nate-on is one of the most widely used messenger system in Korea. A recent research, however, shows that Nate-on messenger has some security vulnerabilities in its mechanism for user authentication. From the present paper found on which the certify method of nate-on messenger program and its weakness. This paper aims to propose new certified protocol and find a solution to the problems that it has by reviewing the way to authenticate the nate-on messenger program and its weak points. In this work, we present a new authentication protocol designed to resolve the security problem with the Nate-on system.

1. 서론

네이트온 메신저는 국내에서 가장 많은 사용자를 확보하고 있는 메신저이다.[1] 이 메신저를 통해 사용자는 메일을 확인할 수 있으며 친구들과 대화도 할 수 있고 SMS(Simple Message Service) 또는 MMS(Multimedia Messaging Service)를 통하여 핸드폰으로 메시지를 전송할 수 있다. 또한 네이트온 메신저에서 제공하는 SSO(Single Sign On) 기능을 통하여 싸이월드와 연동하여 사용할 수 있는 등의 수많은 서비스들을 제공하고 있다.

그러나 네이트온 메신저 프로그램은 인증 정보를 만들 때 동일 사용자에 대해서는 항상 동일한 인증정보를 생성한다.[2]

그 결과 공개 네트워크상에서 전송되는 사용자의 인증 정보를 공격자가 획득하게 되면 공격자는 그 인증 정보를 가지고 재전송 공격(replay attack)을 할 수 있다. 이를 통해 공격자는 다른 사용자로 가장 할 수 있게 된다. 또한 공격자는 획득한 인증정보에서 사전공격(dictionary attack)을 통해 직접 사용자의 패스워드를 추출할 수도 있다. 공격자가 이와 같은 공격에 성공하면 네이트온 메신저에서 제공하는 서비스들을 통해서 본래 사용자의 메일을 열람할 수 있으며 또한 싸이월드에서 도토리와 같은 것을 사용할 수도 있게 된다. 따라서 본 논문에서는 위와 같은 네이트온 인증 방식의 보안 취약점을 살펴보고, 이에 대한 대응 방안으로 새로운 사용자 인증 및 키 교환 프로토콜을 제안한다.

2장에서는 네이트온 메신저 인증 메커니즘 구조에 대하여 살펴보겠다. 3장에서는 네이트온 메신저 인증 메커니즘의 2가지 취약점에 대해 설명하고, 4장에서는 취약점을 바탕으로 개선책을 제안하겠다. 마지막으로 5장에서 결론을 맺고자 한다.

2 .네이트온 메신저 인증 메커니즘

네이트온 메신저의 인증방식은 먼저 사용자가 네이트온 메신저 프로그램에 인증정보를 입력하고, 이 인증정보로부터 메신저 프로그램이 인증패킷을 구성하여 이 패킷을 인증서버에 전송함으로써 시작된다.이때 사용자가 입력한 인증정보는 사용자 ID와 패스워드로 구성되는데. 메신저 프로그램의 이러한 사용자 인증정보를 입력으로 하여 MD5 해쉬값을 계산하게 된다. 표1은 메신저 프로그램이 MD5 해쉬함수의 입력은 사용자의 네이트온 ID에 이메일 주소의 성격에 따라 나뉘어 진다.

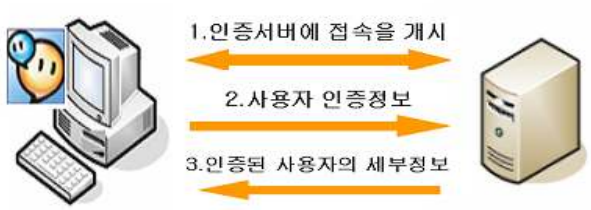
즉, 네이트온 ID가 네이트 닷컴의 이메일 계정인 경우와 네이트온 ID가 타 회사의 이메일 계정인 경우로 다르게 처리된다.

(표 1) 네이트온 메신저 인증정보

구분	인증정보
네이트닷컴 이메일 사용자(XXX@nate.com)	MD5(Password||XXX)
타 회사 이메일 사용자(XXX@abc.com)	MD5(Password||XXX @abc.com)

네이트온 메신저 프로그램은 네이트온 인증서버로의 접속을 위해 dpl.nate.com 서버를 통해 네이트온 인증서버의 IP 주소를 획득한다. 이후 네이트온 메신저 프로그램은 획득한 IP주소를 통하여 인증서버에 접속을 개시한다. 프로그램은 이때 사용자가 입력한 정보를 바탕으로 표1과 같이 MD5해쉬값으로 변환 후 인증서버에 인증정보를 전송한다.

인증서버는 수신한 인증정보를 토대로 올바른 인증정보가 전송됨을 확인 후 로그인을 허가하고 사용자가 이전에 저장했던 여러 가지 사용자의 세부정보를 담은 패킷을 반환한다. 위에서 설명한 사용자 메커니즘을 간략히 그림으로 나타내자면 그림1과 같다.



(그림 1) 네이트온 메신저 프로그램 인증 절차

3.네이트온 메신저 인증 메커니즘 취약점

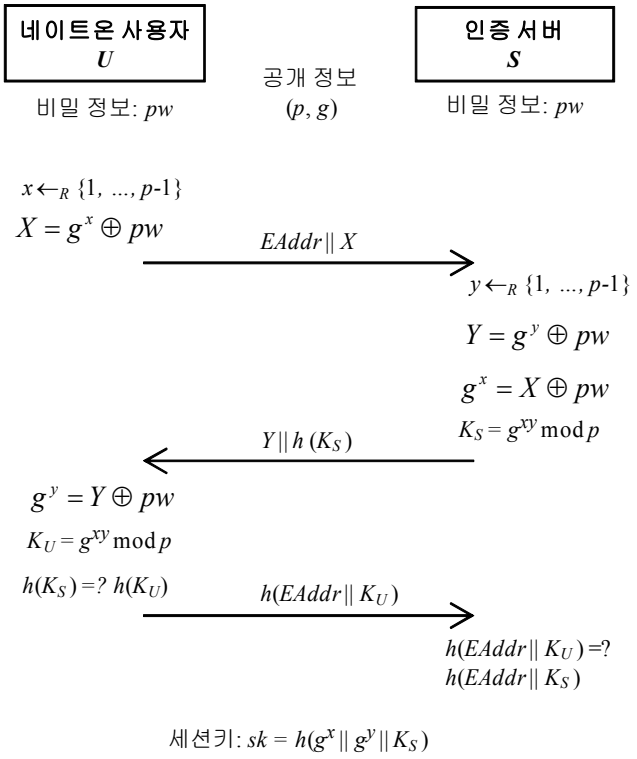
네이트온 메신저 프로그램은 인증정보 생성방법에 따라 사용자별로 다른 MD5 해쉬값을 전송하겠지만 동일한 사용자에 대해서는 항상 동일한 MD5 해쉬값을 보내게 된다. 따라서 공격자가 사용자에 대한 MD5 해쉬값을 얻을 수 있다면 이 값을 가지고 재전송 공격이 가능하다. 뿐만 아니라 공격자는 스니핑을 통하여 얻은 사용자의 E-Mail 주소와 인증정보인 MD5 해쉬값을 이용하여 사용자의 패스워드를 얻어낼 수 있다.

3.1 재전송 공격(Replay Attack)

네이트온 메신저의 인증방식에서 사용자는 인증서버에 접속을 개시한 이후 사용자의 인증정보 MD5(Password||XXX)또는 MD5(Password||@abc.com)를 인증서버에 전송한다. 이때 이 정보는 사용자의 E-Mail 혹은 ID와 Password의 MD5 해쉬값 이다. 즉, 사용자 인증정보는 E-Mail과 Password 외 다른 값을 가지고 있지 않다. 이와 같이 네이트온 사용자는 항상 같은 MD5 해쉬값을 인증서버에게 전송한다는 것을 알 수 있다. 만약 공격자가 이러한 인증정보를 얻을 수 있다면 별다른 어려움 없이 인증서버에 재전송만으로도 사용자의 정보를 획득 및 정당한 사용자로 가장할 수 있게 된다. 따라서 네이트온 메신저는 재전송 공격에 취약하다고 할 수 있다.

3.2 사전 공격(Dictionary Attack)

위에서 언급한 바와 같이 인증서버로 전송되는 인증정보는 사용자의 ID와 Password의 단순 조합으로 구성됨을 알 수 있다. 따라서 공격자는 인증정보를 얻어 낼 수 만 있다면 일반적으로 공개된 사용자의 ID외에 Password 부분을 다음과 같은 사전공격으로 알아낼 수 있다.



(그림 2) 패스워드 기반 인증 및 키 교환 프로토콜

PW = 원래의 패스워드
PW' = 패스워드의 추측값
C = MD5($pw||XXX$)
C' = MD5($pw'||XXX$)

1. 공격자가 C를 획득한다.
2. 공격자는 PW'을 해쉬함수에 대입한다.
3. 위에서 얻어낸 C'을 C와 비교한다.
4. 두수가 일치하지 않으면 다시 2단계로 돌아간다.
5. 두수가 일치한다면 C'에 대입한 PW'이 용자의 PW임을 알아낸다.

길이가 짧거나 다양한 문자를 사용하지 않은 Password 일수록 더욱 짧은 시간 내에 원래의 패스워드를 알아낼 수 있다.

4. 네이트온 인증 방식 개선 방안

4.1 제안프로토콜

본 장에서는 앞서 살펴 본 네이트온 인증방식의 보안 취약점을 개선하기 위한 새로운 인증 및 키교환 프로토콜을 제안한다. 그리고 재전송 과 사전 공격 측면에서 제안 프로토콜의 안정성에 대하여 분석 하겠다.

● Notation

U : 네이트온 사용자
S : 인증서버
pw : 공유한 패스워드
h : 일 방향 해쉬 함수
sk : 세션 키

● 설정단계

U와 S는 사용자 패스워드 pw 와 공개 파라미터 p, g를 공유한다.

● 실행단계

① U는 1부터 $p-1$까지의 수에서 랜덤하게 x를 생성한다. x를 이용하여 $g^x \oplus pw$를 계산하여 X를 생성한다. 그런 후, $EAddr$ 주소와 X값을 S로 보낸다.

② U로부터 메시지 $EAddr \| X$를 받은 S는 1부터 $p-1$까지의 수에서 랜덤하게 y를 생성하고, $Y=g^y \oplus pw$ 와 $g^y=X \oplus pw$를 계산한다. 그리고 S는 $k_s = g^{xy} \bmod p$를 계산하여 Y와 $h(k_s)$를 U에게 전송한다.

③ S로부터 메시지 $Y \| h(k_s)$를 받은 U는 $Y \oplus pw$를 계산하여 g^y를 만든다. U는 g^y를 이용하여 $g^{xy} \bmod p$를 계산하여 세션키 k_u를 생성한다. 생성한 k_u값과 S로부터 받은 k_s값을 h에 넣는다.

U는 $h(k_u)$와 $h(k_s)$을 비교하여 값이 동일한지 확인한다. 동일한 값으로 확인이 되면 $h(EAddr \| k_u)$를 S에게 전송한다.

④ U로부터 $h(EAddr \| k_u)$를 전송받은 S는 $h(EAddr \| k_u)$와 $h(EAddr \| k_s)$의 값이 동일한지 검증을 한다. 동일한 값으로 검증이 되면 사용자 U의 로그인을 허용한다.

U와 S는 세션키 $sk = h(g_x \| g_y \| k_s)$를 생성하여 이후의 통신을 보호하는데 사용한다.

4.2 안전성 분석

앞서 제안된 인증 및 키교환 프로토콜을 이용하여 사전공격과 재전송 공격에 안전하다.

4.2.1 사전 공격 안전성

사전 공격은 패스워드 추측에 필요한 정보를 얻은 다음에 임의의 패스워드를 대입하여 획득한 정보와 비교하여 패스워드를 알아내는 공격 방식이다. 본 논문에서 제안된 프로토콜에서 공격자는 메시지 X 또는 Y를 획득하여 사전공격을 시도 할 수 있다. 하지만 이는 이산대수 문제의 어려움에 부딪히게 된다. 또한 임의의 난수 x와 y는 랜덤하게 생성되는 값이므로 알 수가 없게 된다. 때문에 사전공격은 불가능하게 된다.

4.2.2 재전송 공격 안전성

U와 S사이에 이미 주고받은 정보를 다시 보내는 형태이다. 하지만 앞에서 제안된 프로토콜은 랜덤값 x와 y를 이용하여 매번 다른 g^x와 g^y의 값을 사용하게 된다. 따라서 같은 정보를 다시 보내는 재전송 공격은 불가능함을 쉽게 알 수 있다.

4. 결론

본 논문에서는 네이트온 메신저의 인증방식의 취약점을 해결하기 위한 새로운 프로토콜을 제시 하였다. 기존의 인증방식은 간단한 구성으로 이루어졌기 때문에 사전공격과 재전송공격에 취약하였다.

우리가 제시한 새로운 제안 프로토콜은 Diffie – Hellman을 이용하였는데, 이는 패스워드 기반의 사용자 인증 및 키 교환 프로토콜을 이용한다. 이 제안 프로토콜은 이산대수 문제의 어려움을 이용하여 사전 공격과 재전송 공격에 안전하도록 하며, 효율성과 안정성을 높인다.

[참고문헌]

[1] 네이트온 http://nateonweb.nate.com/

[2] 신동휘, 최윤성, 박상준, 김승주, 원동호, "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석", 情報保護學會 論文誌 第17卷 第1號, pp 68-80, 2007.2

[3] 해킹과 보안, 김승현 윤청원 공저, 영진닷컴, 2003

[4] 현대 암호학, 원동호 저, 그린,2004

[5] Data communications and networking, Behrouz A. Forouzan, McGraw-Hill, 2005

[6] william stallings “Network Security Essentials" Prentice Hall, pp75-78, pp81-126

[7] 강유의 해킹&보안, 강유 저, 에이콘출판사, 2003