情報保護學會論文誌
第17卷 第1號, 2007. 2

네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석

신동휘, 최윤성, 박상준, 김승주‡, 원동호
성균관대학교 정보통신공학부 정보보호연구소

Cryptanalysis on the Authentication Mechanism of the NateOn Messenger

Donghwi Shin, Younsung Choi, Sangjoon Park, Seungjoo Kim‡, Dongho Won
Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University

요 약

네이트온 메신저는 국내에서 가장 많은 사용자를 확보하고 있는 메신저이다. 메신저는 메일, 쪽지, 싸이월드 그리고 SMS 서비스 등의 많은 기능을 제공하고 있다. 본 논문에서는 네이트온 메신저 프로그램의 인증 트래픽을 분석하여 악의적으로 획득한 개인 인증 정보를 재전송 공격함으로써 이를 통해 공격자가 불법적으로 인증될 수 있다는 것을 설명한다. 또한 네이트온 메신저 이외에 타 국내 메신저들 또한 이와 유사한 방법으로 공격될 수 있음을 보인다.

ABSTRACT

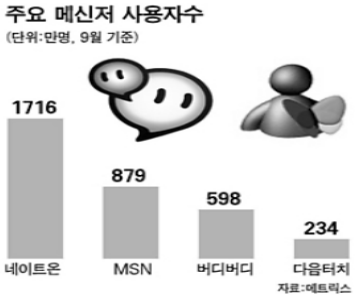
Nateon Messenger, which has the most number of users in Korea, supports many services such as E-mail, note, Cyworld, SMS, etc. In this paper, we will analyse the authentication traffic which is transmitted and received by the Nateon Messenger. Through performing the replay attack with the authentication information, we will show that an attacker can be authenticated illegally. Furthermore, we will show that other domestic messengers have similar security problems.

Keywords : *Messenger, Replay Attack, Password*

Ⅰ. 서 론

네이트온 메신저는 [그림 1]에서와 같이 국내에서 가장 많은 사용자를 확보하고 있는 메신저이다.

이 메신저를 통해 사용자는 메일을 확인할 수 있으며 친구들과 대화도 할 수 있고 SMS(Simple Message Service) 또는 MMS(Multimedia Messaging Service)



[그림 1] 주요 메신저 사용자 수

접수일: 2006년 10월 10일; 채택일: 2006년 11월 28일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.
(IITA-2006-C1090-0603-0028)
‡ 교신저자, skim@security.re.kr

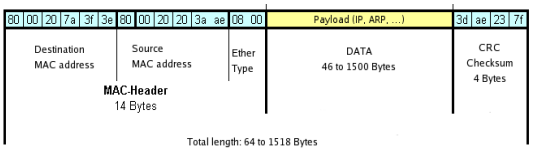
[표 1] 국내 메신저 연동 서비스

국내 주요 메신저	연동 서비스
네이트온 v3.5.15.0(600)	네이트 메일/클럽 서비스, 네이트 닷컴 서비스 싸이월드 미니홈피, 싸이월드 클럽
버디버디 v5.8	버디버디 클럽
터치(다음) v5.06101300	다음 메일/클럽 서비스
타키(세이클럽) v2.9.5	세이클럽 메일, 피망
MSN v8.0(8.0.0812.00)	MSN 닷컴, Hotmail 서비스

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.

현재 국내에서 가장 많이 사용되고 있는 네이트온 메신저의 인증 메커니즘은 사용자의 정보들이 암호화되어 전송되도록 하고 있다. 그러나 네이트온 메신저 프로그램이 인증 정보를 만들 때 동일 사용자에 대해서는 항상 동일한 인증정보를 생성한다. 그 결과 공격자가 임의의 사용자에 대한 인증 정보가 네트워크로 전송되는 것을 확인할 수 있다면 공격자는 그 인증 정보를 가지고 재전송 공격(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. 공격자가 이와 같은 공격을 성공하면 네이트온 메신저에서 제공하는 서비스들을 통해서 본래 사용자의 메일을 열람할 수 있으며 싸이월드에서 도토리와 같은 것을 사용할 수도 있게 된다.

본 논문의 2장에서는 공격을 위한 스니핑이라는 기법과 스니핑을 위한 다른 기법들에 대해서 살펴보겠다. 3장에서는 네이트온 메신저 프로그램이 사용자 인증을 위해 사용하는 비공개 인증 메커니즘을 상세히 분석하고, 이를 통해 발견된 취약점을 분석하겠다. 4장에서는 취약점을 바탕으로 재전송 공격 시나리오를 만들고 공격 프로그램을 구현하여 재전송 공격을 통해 사용자의 친구목록 정보를 얻는 과정에 대해 설명한다. 또한 인증 정보에서 사용자의 패스워드를 추출하는 과정에 대해 설명한다. 5장에서는 타 회사의 메신저 인증 메커니즘의 문제점에 대해 정리하고 마지막으로 6장에서 결론을 맺는다.



[그림 2] Ethernet Frame

Ⅱ. 스니핑(Sniffing)과 스니핑을 위한 공격기법

본 장에서는 네트워크를 통해 전송되는 패킷들을 열람할 수 있는 스니핑이라는 기술에 대해 언급한다. 그리고 공격자가 스니핑을 하기 위해 필요한 부가적인 기법들에 대해 간단히 설명한다.

2.1 정의 및 원리

해킹기법으로서의 스니핑은 네트워크를 통해 전송되는 패킷들을 훔쳐보는 것을 말한다. 다시 말해 공격자가 악의적인 목적으로 갖고 네트워크 트래픽을 도청하는 것을 스니핑이라고 한다. 그리고 스니핑을 할 수 있도록 해주는 툴들을 스니퍼(Sniffer)라고 한다.

스니핑의 원리는 다음과 같다. 이더넷은 로컬 네트워크에서 모든 호스트들이 선을 공유하도록 되어 있다. 그러므로 동일 네트워크에 속해 있는 호스트들은 통신하는 모든 트래픽을 볼 수 있는 것이다. 하지만 모든 트래픽들을 일반 호스트가 받아서 처리한다는 것은 상당히 비효율적이며 각 호스트들의 네트워크 성능은 크게 저하될 것이다. 그러므로 각 호스트들에 설치되어 있는 NIC(Network Interface Card)는 이더넷 프레임의 내용 중에 MAC(Media Access Control)주소를 확인하여 자신의 MAC주소와 동일한 트래픽만을 받아들이고 그렇지 않은 트래픽들을 무시하는 필터링 기능을 수행하게 된다. 이와 같은 내용은 이더넷 프레임의 구조([그림 2])를 보면 알 수 있다. 하지만 NIC에서 이와 같은 필터링 기능을 수행하지 않고 Ethernet상에서 모든 트래픽들을 볼 수 있도록 하는 설정할 수 있는데 이것을 “Promiscuous Mode”라고 한다. 호스트에 설치된 NIC를 Promiscuous Mode로 설정해 놓으면 앞서 설명한 필터링 기능을 수행하지 않고 Ethernet상의 모든 트래픽을 받아들이게 된다.

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 모두 열람할 수 있었다. 하지만 인터넷이 TCP/IP 프로토콜을 기반으로 하여 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.

2.2 스푸핑(Spoofing)

스푸핑이란 공격자 자신의 신분을 위장하여 공격 대상이 되는 호스트가 보내는 패킷들을 공격자를 통해서 전송되게 하거나 공격 대상 서버가 공격자를 다른 사용자로 인식하도록 하는 것들을 의미한다. 스푸핑의 종류에는 IP 스푸핑, ARP 스푸핑, 쿠키 스푸핑 등의 기법들이 있으며, 최근 많은 문제가 되고 있는 피싱(Phishing) 또한 스푸핑의 일종이라고 할 수 있다.

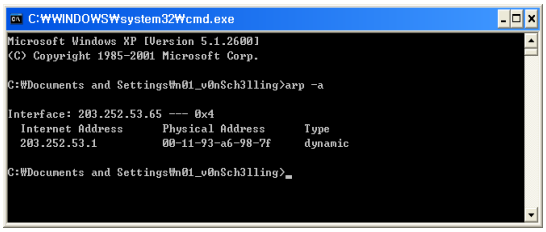
본 장에서는 ARP 스푸핑을 가지고 스푸핑에 대해서 설명하겠다. 2.1에서 언급하였듯이 이더넷에서는 NIC의 MAC주소를 가지고 각각의 호스트들을 인식하고 통신하게 된다. 그렇기 때문에 각각의 호스트들은 MAC 주소를 관리하기 위해 ARP Table([그림 3])을 관리한다. 이더넷에서 통신을 하기 위해 호스트는 자신의 ARP Table을 확인하여 통신하고자 하는 호스트의 MAC 주소 정보가 ARP Table에 있는지 확인한다. 통신을 원하는 호스트의 MAC 주소 정보가 ARP Table에 있다면, 호스트는 해당 MAC주소를 가져와서 이더넷 프레임을 구성한다. 만약 원하는 호스트의 정보가 없다면, 호스트는 네트워크에 있는 라우터에게 ARP 쿼리를 보내 통신하고자 하는 호스트의 MAC 주소 정보를 가져와서 이더넷 프레임을 구성한다.

임의의 공격자는 ARP 스푸핑을 통해 대상 호스트의 ARP Table의 내용을 수정하여 ARP Table에 저장되어 있는 MAC 주소를 공격자의 MAC 주소로 변경한다. ARP 스푸핑 공격을 당한 호스트가 인증서버로부터 인증을 받기 위해 인증정보가 담긴 이더넷 프레임을 만들면 이더넷 프레임의 Destination MAC Address 부분은 공격자의 MAC Address가 된다. 그러므로 ARP 스푸핑 공격을 당한 호스트에서 전송되는 이더넷 프레임은 공격자에게 전송되게 된다. 그리고 공격자는 스니퍼를 통해 들어오는 모든 패킷들을 보게 된다. 위의 설명을 그림으로 도식화 하면 [그림 4]와 같다.

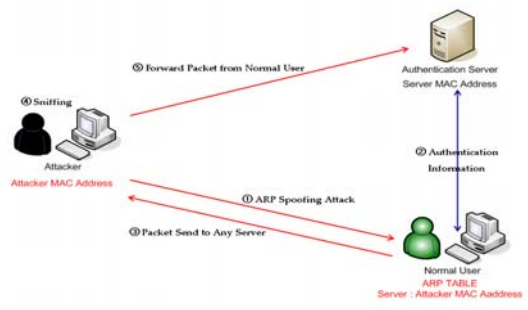
2.3 프록시 서버(Proxy Server)

프록시 서버는 인터넷의 보안을 위해 침입 차단 시스템에서 사용되었다. 웹 브라우저에서 프록시 서버를 설정해 놓으면, 사용자가 요구하는 웹 페이지의 정보를 해당 웹 서버로 직접 요청하는 것이 아니라 프록시 서버에 요청하게 된다. 프록시 서버는 해당 웹 페이지의 내용을 가지고 있다면 사용자에게 응답을 주게 되고, 그렇지 않다면 사용자의 요청을 웹 서버로 넘겨주고 웹 서버에서 오는 응답을 다시 사용자에게 넘겨주게 되는 된다.

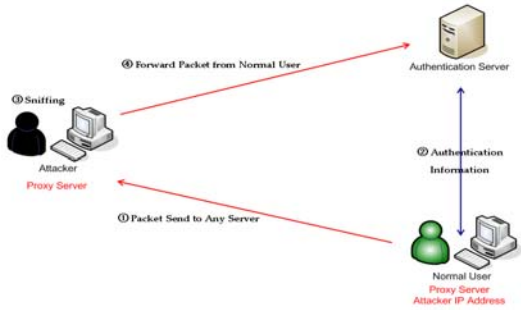
하지만 공격자는 이러한 프록시 서버의 기능을 악용할 수 있다. 공격자가 자신의 PC를 프록시 서버로 만들고, 자신의 IP 주소를 프록시 서버의 주소라 하고 인터넷에 뿌리게 된다. 그렇게 되면 인터넷상의 임의의 사용자가 공격자가 프록시 서버의 주소라고 뿌린 공격자의 주소를 프록시 서버로 설정하게 된다. 그러면 임의의 사용자가 통신하는 모든 트래픽은 공격자의 호스트를 거



[그림 3] ARP Table



[그림 4] ARP Spoofing Attack



[그림 5] Proxy Server

쳐서 웹 서버와 통신을 수행하게 된다. 여기서 공격자는 스니퍼를 통해 들어오는 모든 패킷들을 보게 된다. 이와 같은 방법을 통해 공격자는 무작위로 패킷을 수집하고, 많은 패킷들 중에서 공격자가 원하는 패킷들만을 잡기 위해서 스니퍼의 필터링 기능을 가지고 원하는 패턴의 패킷만을 수집할 수 있게 된다. 위의 설명을 그림으로 도식화 하면 [그림 5]와 같다.

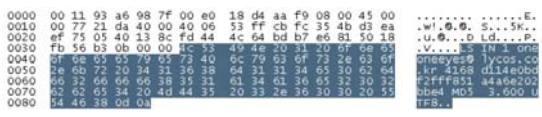
Ⅲ. 네이트온 메신저의 인증 메커니즘

본 장에서는 국내에서 가장 많은 사용자를 확보하고 있는 네이트온 메신저의 비공개 사용자 인증 메커니즘을 분석한다. 이 분석을 통하여 네이트온 메신저 인증 메커니즘의 취약점을 지적하도록 한다. 인증 메커니즘 분석을 위해 Ethereal Packet Capture 프로그램을 사용하였다.

3.1 네이트온 메신저 인증 메커니즘 구조 분석

사용자가 네이트온 메신저 로그인시 네이트온 메신저 프로그램이 서버로 보내는 인증정보를 담은 패킷을 수집해 보았다. 인증정보를 담은 패킷은 [그림 6]과 같이 로그인하고자 하는 사용자의 이메일주소와 암호화된 256비트 문자열을 포함하고 있다는 것을 알 수 있다.

인증정보를 담은 패킷에는 앞서 언급했던 사용자 이메일주소와 암호화된 256비트 문자열과 함께 MD5라는 문자열이 포함되어 있었다. 그러므로 암호화된 문자



[그림 6] 네이트온 메신저 인증 패킷

[표 2] 네이트온 메신저 인증정보

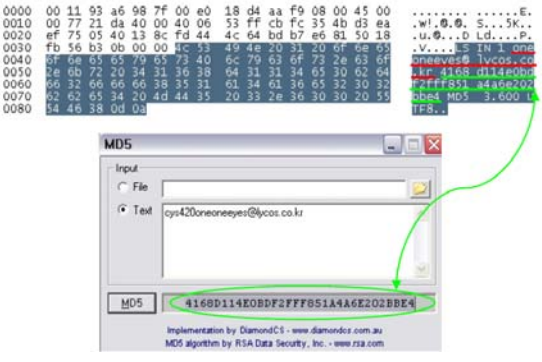
구 분	인증정보
네이트닷컴 이메일 사용자(xxx@nate.com)	MD5(Password ‖ xxx)
타 회사 이메일 사용자(xxx@abc.com)	MD5(Password ‖ xxx@abc.com)

열의 구성을 살펴보기 위해 MD5 해시함수를 통해 분석해 보았다. 분석 결과 사용자의 인증정보는 사용자의 ID(또는 E-Mail주소)와 패스워드의 단순 조합만으로 생성된다는 것을 알 수 있다.([표 2]) 이때 사용자의 네이트온 ID에 사용되는 이메일 주소에 따라 2가지의 경우로 나누어진다. 네이트온 ID가 네이트닷컴의 이메일 계정인 경우, MD5 해시함수의 인자로 사용자 패스워드와 @nate.com을 제외한 사용자 ID만이 입력된다. 그리고 네이트온 ID가 타 회사의 이메일 계정인 경우 [그림 7]과 같이, MD5 해시함수의 인자로 사용자 패스워드와 사용자 전체 이메일주소가 입력된다.

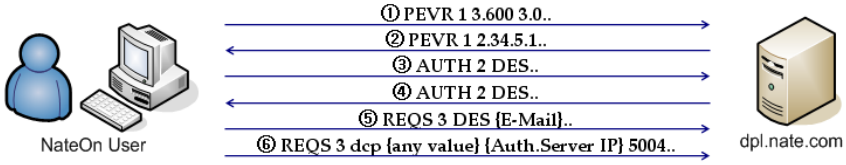
3.2 네이트온 메신저 인증 메커니즘 세부 구조 분석

네이트온 메신저 로그인시 전송되는 패킷들의 분석을 통해 네이트온 메신저 프로그램의 비공개 인증정보 생성 메커니즘을 분석했다. 이제부터는 네이트온 메신저 프로그램이 생성한 인증정보를 가지고 어떠한 절차로 사용자 인증을 수행하는지 알아보겠다.

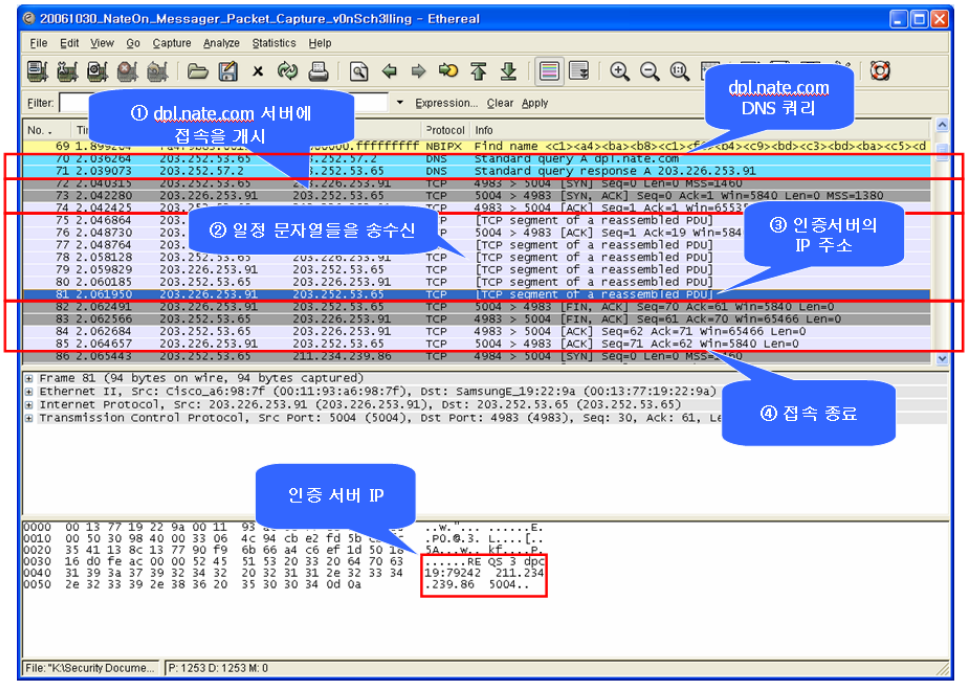
네이트온 메신저 프로그램은 사용자가 인증을 받아야 하는 인증서버의 IP주소를 받기 위해 dpl.nate.com:5004 서버로 접속을 시도한다. dpl.nate.com:5004로 접속하기 위해 DNS서버를 통해서 dpl.nate.com의 IP주소



[그림 7] 네이트온 ID가 oneoneeyes@lycos.co.kr인 경우



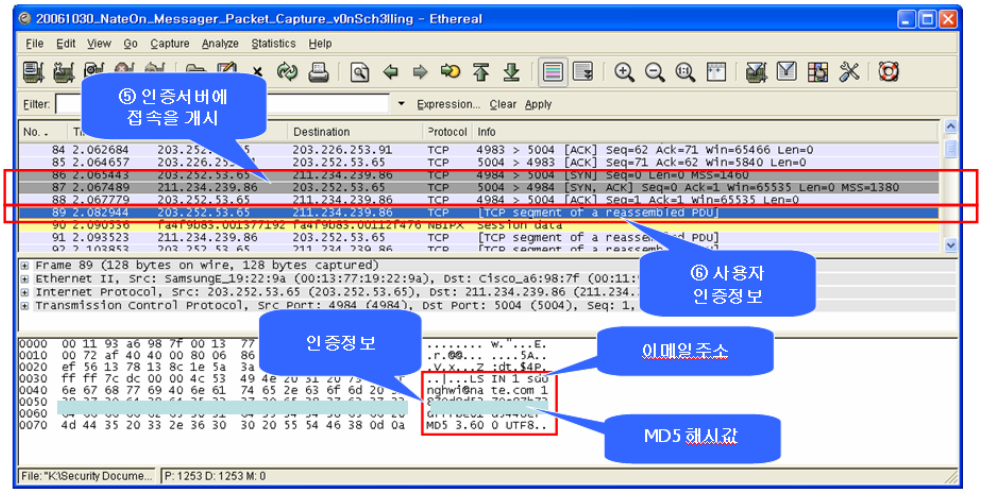
[그림 8] dpl.nate.com:5004 서버와 송수신하는 문자열



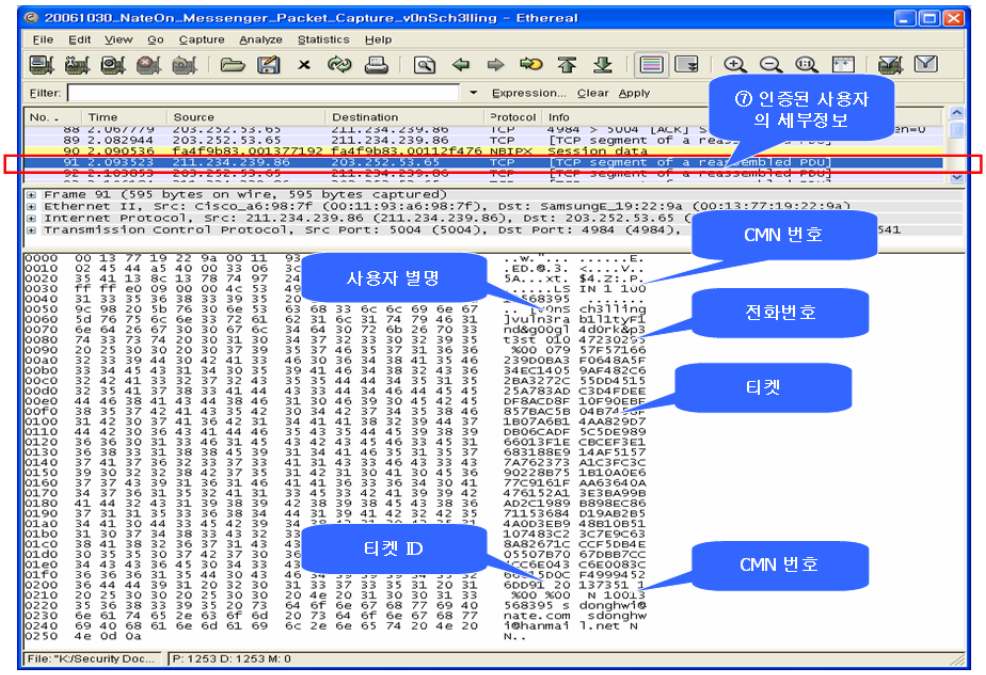
[그림 9] 네이트온 메신저 프로그램과 dpl.nate.com:5004와의 통신

를 얻은 네이트온 메신저 프로그램은 DNS서버로부터 얻은 IP주소를 가지고 사용자 PC와 dpl.nate.com:5004 서버 사이에 TCP Connection을 성립시킨다. 이것은 사용자 PC와 dpl.nate.com:5004가 3-Way Handshake를 위해 송수신되는 패킷을 통해 알 수 있다. 네이트온 메신저 프로그램이 dpl.nate.com:5004 서버에 접속하면 상호간에 데이터들을 송수신할 수 있고 네이트온 메신저 프로그램은 [그림 8]과 같이 dpl.nate.com:5004 서버와 3번의 문자열을 송수신한다.

[그림 8]에서 첫 번째부터 네 번째까지의 문자열들은 네이트온 메신저 프로그램이 dpl.nate.com:5004서버와 송수신하는 정해진 문자열이다. 다음으로 네이트온 메신저 프로그램이 다섯 번째로 송신하는 문자열을 살펴보자. “REQS 3 DES {E-Mail Address}”에서 “REQS 3 DES”는 항상 동일한 문자열이고 {E-Mail Address} 로그인하고자 하는 사용자의 이메일 주소이다. 네이트온 메신저 프로그램이 “REQS 3 DES {E-Mail Address}” 문자열을 송신한 뒤에, “REQS 3 dpc{any value} {Auth.Server IP} 5004..”라는 문자열을 수신한다. 이 문자열에서 any value는 “xx:xxxxx” 형식을 갖고 있으며 이는 dpl.nate.com:5004에서 보내는 임의의 값이다. 수신된 문자열에서 중요한 부분은 “{Auth.Server IP} 5004”이다. Auth.Server IP는 네이트온 메신저 프로그램이 사용자 인증을 받아야 하는 서버의 IP주소를 나타낸다. 위 사실은 세 번째 응답으로 문자열을 받은 이후에 사용자 PC가 Auth.Server IP로 접속하기 위해 3-Way Handshake를 하고 인증 정보를 전송한다는 것으로서 알 수 있다. 위의 사실들을 종합해보면 3번의 문자



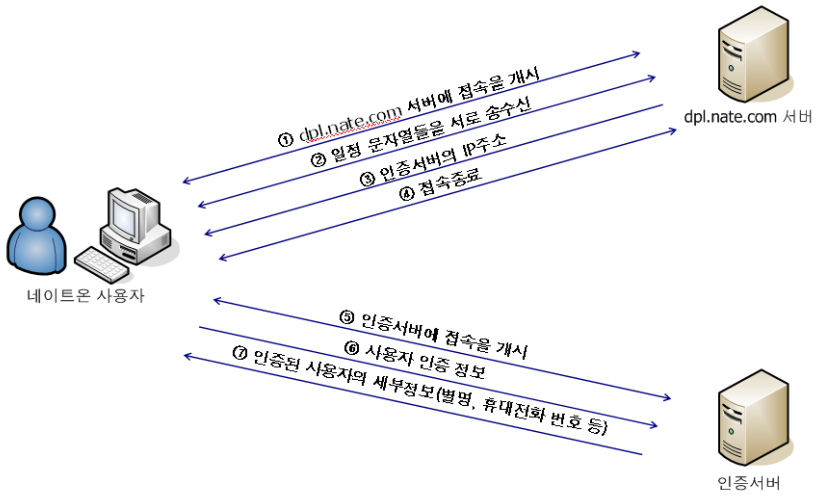
[그림 10] 네이트온 메신저 프로그램과 인증서버와의 통신



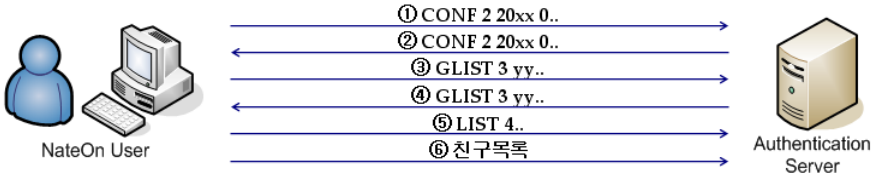
[그림 11] 인증서버와의 통신내용 Ⅰ(사용자 인증 이후)

열 송수신 과정을 통해 네이트온 메신저 프로그램은 어떤 사용자가 인증을 시도할 것인지 dpl.nate.com:5004 서버에게 알려주고 dpl.nate.com:5004 서버는 해당 사용자가 인증을 받아야 하는 인증 서버의 IP주소를 네이트온 메신저 프로그램에게 알려주는 것이다. 위의 과정을 모두 마치고 나면 dpl.nate.com:5004에서 FIN Flag가 설정된 TCP 패킷을 보내 dpl.nate.com:5004와 네이트온 메신저 프로그램과의 TCP Connection을 종료하게 된다. [그림 9]는 정상적인 네이트온 메신저 사용자가 dpl.nate.com:5004와 로그인하기 위해 통신하는 패킷들의 정보를 Ethereal로 잡아서 분석한 것이다.

이제 인증서버의 IP주소를 얻어왔으므로 네이트온 메신저 프로그램은 사용자 인증을 시도할 것이다. 네이트온 메신저 프로그램은 인증서버의 IP주소와 3 Way



[그림 12] 네이트온 메신저 프로그램 인증 절차



[그림 13] 인증서버와 송수신하는 문자열

Handshake를 통해 TCP Connection을 맺게 된다. 성공적으로 접속이 완료되면 네이트온 메신저 프로그램은 사용자가 입력한 인증 정보들을 3.1에서 설명한 정해진 암호화 방법을 통해 암호화시키고 전송한다. [그림 10]은 정상적인 네이트온 메신저 사용자가 인증서버에서 인증을 받기 위해 보내는 인증정보 패킷을 Ethereal로 잡아서 분석한 것이다.

이제 네이트온 메신저 프로그램이 인증서버에 사용자 인증정보를 보냈으므로 인증서버로부터 인증된 사용자 정보를 받는다. 인증 정보를 인증서버에게 보낸 이후, 인증서버는 사용자의 별명, 전화번호, 티켓, 티켓ID, CMN 정보를 포함한 인증된 사용자의 세부정보를 담은 패킷을 보내준다. [그림 11]은 정상적인 네이트온 메신저 사용자가 인증을 받은 이후의 패킷들을 분석한 내용이다.

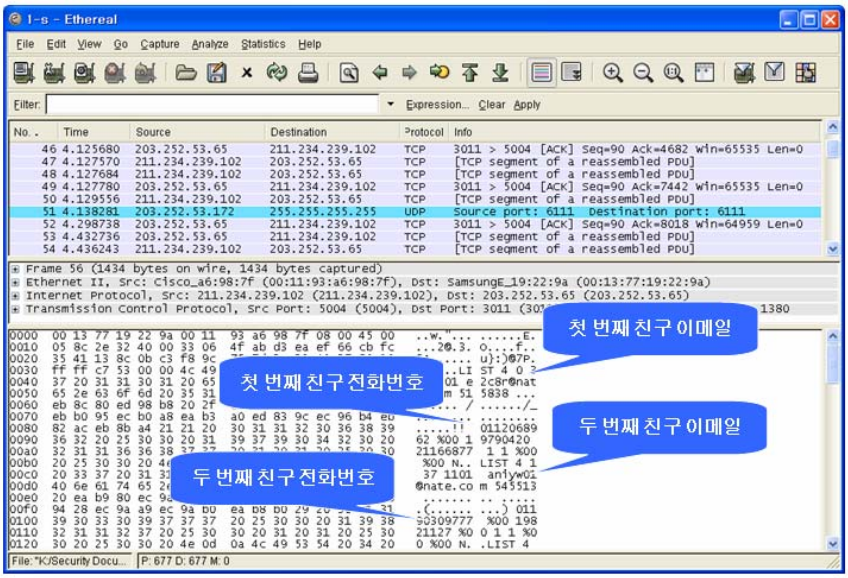
지금까지 설명한 사용자 인증 메커니즘을 종합해보면 [그림 12]와 같다.

이후 네이트온 메신저 프로그램은 로그인한 사용자가 등록한 친구 목록을 받기 위해 인증서버사이에 정해진 문자열들([그림 13])을 송수신하게 된다. 이 문자열들을 송수신한 뒤에 인증서버는 로그인한 사용자가 등록한 친구 목록의 정보([그림 14])를 보내준다.

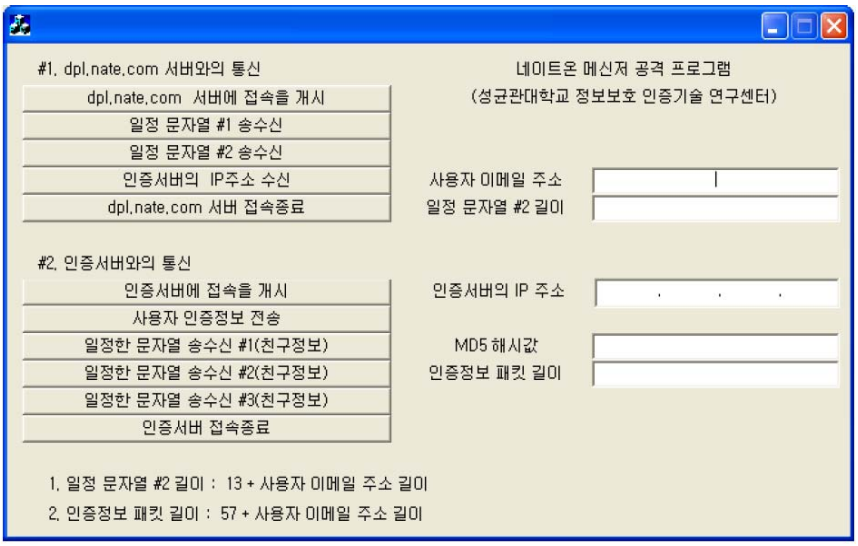
3.3 네이트온 메신저 인증 메커니즘 취약점 분석

네이트온 메신저 프로그램과 인증 서버와의 통신을 지속적으로 살펴보면, 네이트온 메신저 프로그램은 3.1에서 설명한 인증정보 생성 방법에 따라 사용자별로 다른 MD5 해시 값을 전송하겠지만 MD5 해시 함수의 인자로 고정된 문자열인 사용자 패스워드와 사용자 ID 또는 E-Mail 주소만 사용하기 때문에 동일한 사용자에 대해서는 항상 동일한 MD5 해시 값을 인증정보로 보내게 된다. 그러므로 공격자가 임의의 사용자에 대한 MD5 해시 값을 얻을 수만 있다면, 공격자가 3.2에서 언급한 것과 같은 방식으로 통신하여 인증 서버의 IP주소를 얻고 획득한 사용자의 MD5 해시 값을 가지고 재전송 공격이 가능하다.

뿐만 아니라, 공격자는 스니핑을 통하여 얻은 사용자



[그림 14] 네이트온 메신저 프로그램과 인증서버와의 통신



[그림 15] 네이트온 메신저 재전송 공격 프로그램

의 E-Mail 주소와 인증정보인 MD5값(패스워드|E-Mail 주소)을 이용하여 사용자의 패스워드를 검출할 수 있다. 즉 유추된 패스워드와 사용자의 E-mail를 MD5 함수에 입력한 후, 그 출력 값을 스니핑을 통해서 얻은 MD5 값과 비교하여 일치하면 해당하는 패스워드가 사용자가 사용하는 패스워드인 것이다. 이때 사용하는 MD5 해시 함수는 속도가 빠르다고 검증된 프로그램이다. 따라서 MD5 값을 유추된 패스워드와 사용자의 E-mail에 대한 MD5 함수 출력 값을 스니핑을 통해서 얻은 MD5 값과 비교하는 모든 과정도 빠르게 구현될 수 있다.

Ⅳ. 네이트온 메신저 공격

본 장에서는 네이트온 메신저를 공격하기 위해 만든 프로그램을 바탕으로 실제 재전송 공격을 해보겠다. 그리고 재전송 공격과정에서 문제가 되는 송수신 패킷과

정상적으로 통신할 때의 패킷을 비교해보고 로그인한 사용자가 등록한 친구 목록을 받아오도록 하겠다. 재전송 공격의 내용을 보다 자세히 분석하기 위해 Comm-View Packet Capture 프로그램을 사용하였다. 또한 MD5 해시 값을 가지고 사전공격을 통해 패스워드를 추출해보겠다. 사전공격을 이용하여 패스워드를 검출하기 위해서 상용 프로그램인 Passwordspro를 이용하였다.

4.1 네이트온 메신저 재전송 공격

공격자는 네이트온에 로그인하는 사용자의 인증정보

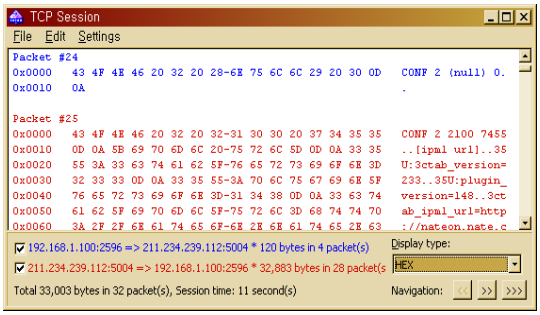


그림 16. "CONF 2 (NULL) 0.."

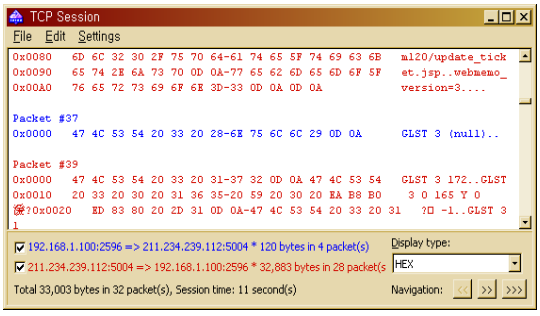


그림 17. "GLIST 3 (NULL).."

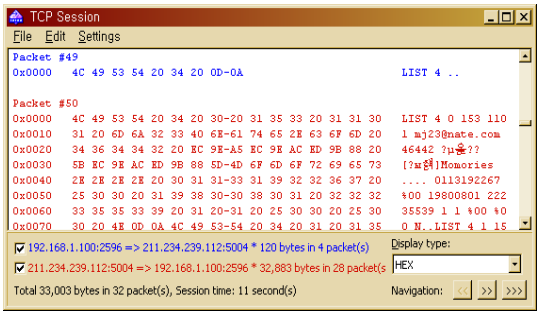


그림 18. "LIST 4 .."와 친구정보

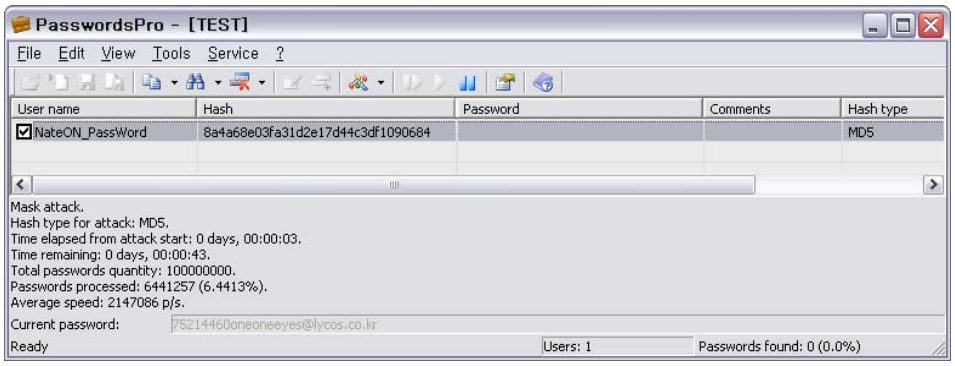
를 네트워크를 통해 획득한다. 그리고 4장에서 설명한 절차에 따라서 재전송 공격을 위한 프로그램([그림 15])을 작성해 보았다.

위의 공격 프로그램을 구현할 때에, dpl.nate.com:5004서버와의 통신에는 아무런 문제가 없었다. 재전송 공격 프로그램이 네이트온 메신저 프로그램과 송수신하는 문자열과 동일한 문자열을 송수신하도록 구현하면, dpl.nate.com:5004서버는 사용자가 인증 받을 인증서버의 IP주소를 보내준다. 그리고 재전송 공격 프로그램이 dpl.nate.com:5004 서버로부터 받은 인증서버 IP주소로 사용자 인증정보를 정해진 문자열에 맞추어 보내면 사용자 인증이 완료된다. 하지만 문제는 로그인한 사용자가 등록한 친구목록을 받아오는 부분을 구현하는데 있었다. [그림 13]을 보면 네이트온 메신저 프로그램은 인증서버에게 "CONF 2 20xx 0.."이라는 문자열을 전송하는데 "xx"부분에 들어가는 숫자가 매번 바뀌게 된다. 이때 만일 재전송 공격 프로그램이 "xx"라는 숫자에 임의의 값을 넣거나 방금 전에 로그인할 때 사용했던 값을 넣고 전송하게 되면, 인증서버는 아무런 반응을 보이지 않게 된다. 또한 "xx"에 들어가는 숫자에 대한 정보는 앞에서 송수신하는 패킷들로부터 찾아낼 수 없으며, "GLIST 3 yy.."에 들어가는 숫자 "yy"에 대한 정보도 찾을 수가 없다.

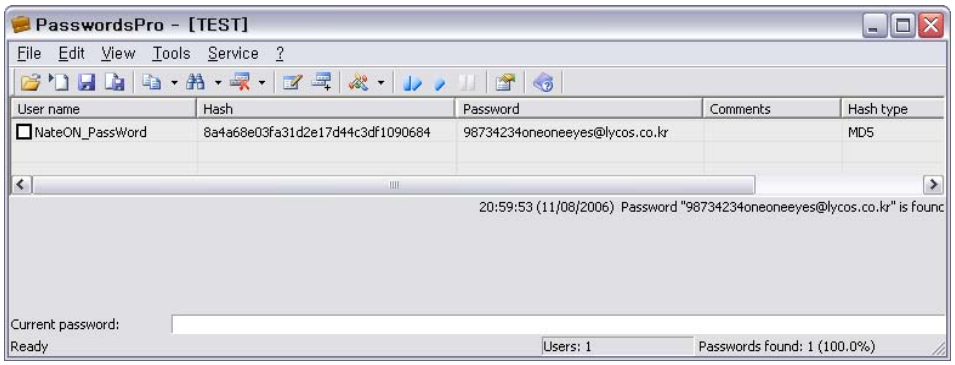
그러나 현재 PC에 설치되어 있는 네이트온 메신저 프로그램에서 처음 로그인하는 사용자의 패킷을 살펴보면 문제를 해결할 수 있다. 정상적으로 로그인할 때 사용되는 패킷들을 분석한 결과 "GLIST 3 yy.."에서 "yy"는 로그인한 사용자가 등록한 친구의 수를 나타내고 있다. "GLIST 3 yy.." 문자열은 네이트온 메신저 프로그램이 먼저 송신하는데 처음 로그인한 사용자의 경우에는 네이트온 메신저 프로그램이 사용자가 등록한 친구의 수를 알고 있을 수가 없다. 그렇기 때문에 처음 로그인하는 사용자의 경우, 네이트온 메신저 프로그램은 "GLIST 3 (NULL).."이라는 문자열을 보내게 된다. 그러므로 "CONF 2 20xx 0.."에서 "20xx"부분을 "(NULL)"로 ([그림 16]) "GLIST 3 yy.."에서 "yy"부분을 "(NULL)" ([그림 17])로 바꾸어 전송하게 되면 [그림 18]과 같이 친구정보를 받아올 수 있다.

4.2 MD5 해시 함수를 이용한 패스워드 검출

상용 프로그램인 Passwordpro를 이용하면 네이트온



[그림 19] 숫자로만 구성된 8자리 패스워드의 검색



[그림 20] Passwordspro를 이용한 네이트온 사용자 패스워드의 검출

메신저 사용자의 패스워드를 검출할 수 있다. 특히 Passwordpro의 옵션에는 dictionary attack과 mask attack(패스워드의 형태를 지정한 후 검색) 기능이 있는데 이 두 기능을 이용하면 효과적으로 패스워드를 검출할 수 있다. 본 실험에서는 옵션 중에서 mask attack을 이용하였다. Passwordpro 프로그램 인터페이스 중 User name은 사용자 이름을 명시하는 부분인데 MD5를 이용한 패스워드 검출에는 영향을 주지 않는 부분이다. Hash 부분에는 스니핑을 통하여 획득한 사용자 인증정보 중 MD5 값을 입력한다. Password 부분에는 프로그램이 실행된 뒤 정확한 패스워드가 검출되면 해당 패스워드가 출력되는 부분이다. Comments 부분은 프로그램에 추가적인 설명을 붙이는 부분인데 이것 역시 MD5를 이용한 패스워드 검출에는 영향을 주지 않는 부분이다. 여기서는 Passwordpro 프로그램이 검색하는 패스워드의 형태를 추가적인 설명으로 넣었다. Hash type 부분은 Passwordpro가 지원하는 여러 해시 함수 중에 사용자가 선택한 해시 함수 형태를 보여주는 부분이다. [그림 19]는 숫자로만 구성된 8 자리의 패스워드 형태의 패스워드들 중 사용자의 네이트온 패스워드가 있는지 검색하는 과정을 보여주고 있다. 그리고 그림 20은 Passwordpro 프로그램이 사용자의 패스워드가 98734234인 것을 검출해내는 모습이다.

패스워드의 구성 형태를 알고 있고 Passwordpro 프로그램의 Mask attack 공격을 이용할 때, 본 프로그램의 검출 속도는 [표 3]과 같다. [표 3]은 해당 구성 형태의 모든 패스워드를 검색하는데 걸리는 시간을 보여주고 있으며, 패스워드 형태가 선정된 기준은 다음과 같다.

미국 컴퓨터보안연구소인 SANS (SysAdmin, Audit, Network, Security)에서 안전한 패스워드를 생성하기 위한 패스워드 정책과 마이크로소프트의 패스워드 설정 원칙 및 미국 NIST 전자인증 가이드라인 등을 참조하여 강한 패스워드의 기준을 선정하였다. 선정된 강한 패스워드의 기준은 다음과 같다.

- 다양한 문자(영소문자, 영대문자, 숫자, 특수문자)의 포함한 패스워드
- 적어도 8자리 이상의 길이를 가진 패스워드
- 단순한 패턴이 없는 패스워드.(예를 들어, aaa1122,

b1234567, ccc000, 등)

- 국내/외국어 사전에 포함된 단어로 이루어지지 않은 패스워드

사용자가 패스워드를 기억하기 싶게 하기 위해서 위 기준을 지키지 않고 약한 패스워들 사용하게 되는데, 강한 패스워드를 선정하는 참조한 자료들과 선정된 강한 패스워드 조건을 기초로 하여 사용자들이 주로 사용하며 취약한 패스워드 조건을 기준하였다. 선정된 주로 사용되고 약한 패스워드의 기준은 다음과 같다.

- 특정 문자로만 이루어진 패스워드
- 8자리보다 짧은 패스워드
- 단순한 패턴으로 구성된 패스워드(예를 들어, aaa1122, b1234567, ccc000, 등)
- 국내/외국어 사전에 포함된 단어들로 이루어진 패스워드

본 실험에서는 국내/외국어 사전에 포함된 단어들로 이루어진 패스워드는 배제하고 보다 일반적이고 포괄적인 실험데이터의 산출을 위하여 다음과 같은 [표 3]과 같은 기준으로 실험을 진행하였다. [표 3]의 결과로는 특정 문자로만 이루어진 패스워드 및 사용 가능한 모든 문자를 사용한 패스워드(단순한 패턴이 없는 패스워드는 뜻도 포함), 6~8자리 길이의 패스워드, 단순한 패턴을 가진 패스워드에 대한 분석이 가능하다.

그리고 해당 프로그램의 속도는 실행되는 컴퓨터의 기본적인 속도 및 실행 환경 조건(타 프로그램의 실행 여부, CPU 점유율 등)에 따라서 유동적이지만 대략적인 패스워드 검색 시간을 알아보는 것에는 도움이 된다. 해당 프로그램이 실행된 컴퓨터의 환경은 CPU : 펜티

[표 3] 패스워드의 형태와 검출 시간

No	문자 구성	경우의 수	자릿수	총 경우의 수	검색 시간
1	· 숫자	10	6	1,000,000	최대 약 2초
2	· 숫자	10	7	10,000,000	최대 약 5초
3	· 숫자	10	8	100,000,000	최대 약 50초
4	· 숫자	10	10	10,000,000,000	최대 약 1시간 30분
5	· 영소(대)문자 1 ‖ 숫자 5	26 ‖ 10	6	2,600,000	최대 약 3초
6	· 영소(대)문자 1 ‖ 숫자 6	26 ‖ 10	7	26,000,000	최대 약 12초
7	· 영소(대)문자 1 ‖ 숫자 7	26 ‖ 10	8	260,000,000	최대 약 2분
8	· 영소(대)문자 2 ‖ 숫자 4	26 ‖ 10	6	6,760,000	최대 약 3초
9	· 영소(대)문자 2 ‖ 숫자 5	26 ‖ 10	7	67,600,000	최대 약 31초
10	· 영소(대)문자 2 ‖ 숫자 6	26 ‖ 10	8	676,000,000	최대 약 5분 10초
11	· 영소(대)문자 3 ‖ 숫자 3	26 ‖ 10	6	17,576,000	최대 약 7 초
12	· 영소(대)문자 3 ‖ 숫자 4	26 ‖ 10	7	175,760,000	최대 약 1분 30초
13	· 영소(대)문자 3 ‖ 숫자 5	26 ‖ 10	8	1,757,600,000	최대 약 15분 30초
14	· 영소(대)문자	26	6	308,915,776	최대 약 2분 30초
15	· 영소(대)문자	26	7	8,031,810,176	최대 약 1시간 10분
16	· 영소(대)문자	26	8	208,827,064,576	최대 약 1일 10시간
17	· 영소문자, 영대문자	52	6	19,770,609,664	최대 2시간 30분
18	· 영소문자, 영대문자	52	7	1,028,071,702,528	최대 6일 20시간
19	· 영소문자, 영대문자	52	8	53,459,728,531,456	최대 약 280일
20	· 영소문자, 영대문자, 숫자	62	6	56,800,235,584	최대 약 7시간
21	· 영소문자, 영대문자, 숫자	62	7	3,521,614,606,208	최대 약 20일 3시간
22	· 영소문자, 영대문자, 숫자	62	8	218,340,105,584,896	최대 약 1,120일
23	· 영소문자, 영대문자, 숫자, 특수문자(32개)	94	6	689,869,781,056	최대 약 3일 15시간
24	· 영소문자, 영대문자, 숫자, 특수문자(32개)	94	7	64,847,759,419,264	최대 약 370일
25	· 영소문자, 영대문자, 숫자, 특수문자(32개)	94	8	6,095,689,385,410,816	10,000일 이상

[표 4] 타 회사 메신저 인증정보 전송방식

구분	인증정보 전송방식	공격방법
버디버디 v5.0.6.101200	동일한 사용자에 대해 동일한 인증정보 전송	재전송공격
버디버디 v6.8	패스워드 평문 전송	스니핑
파키(세어클럽) v2.05	패스워드 평문 전송	스니핑

엄 4 2.4C, 메모리 : 1 GB, OS : Window XP 이다. 컴퓨터의 기본적인 속도 및 실행환경조건이 더 좋아지면 패스워드를 검색하는 시간도 더 빨리질 것이다. [표 3]의 -문자 구성- 이란 패스워드 한 글자를 구성하는데 사용되는 문자의 종류를 뜻한다. 예를 들어 문자의 구성이 [영소(대)문자] 이면 영소문자로만 이루어진 패스워드라는 뜻이다. 영대문자로만 이루어져도 영소문자로만 이루어진 것과 같은 결과가 나와서 [영소(대)문자]라고 표현하였다. 그리고 [영소(대)문자 1 ‖ 숫자 7] 란 패스워드의 총길이는 8자리이며, 패스워드 첫 번째 자리는 영소문자이며 2~8번째 자리는 숫자로 이루어진 패스워드라는 뜻이다. 그리고 -경우의 수- 는 패스워드 한 글자를 구성하는데 사용되는 문자 종류의 수를 뜻한다. 예를 들어 [영소문자, 영대문자, 숫자, 특수문자(32개)]는 영소문자 26개, 영대문자 26개, 숫자 10개, 특수문자 32개로 패스워드 한 글자를 구성하는데 94가지 문자가 사용된다. -자리 수-는 패스워드의 총 길이를 뜻하며, -총 경우의 수- 해당 패스워드가 가질 수 있는 패스워드 총 종류의 개수를 뜻한다. -검색 시간- 은 Passwordpro 프로그램이 해당 총 경우의 수 만큼의 개수를 가지는 패스워드 형태 모두를 검사하는 걸리는 대략적인 시간을 뜻한다. 이 값은 Passwordpro 프로그램이 실행되는 PC의 기본적인 속도 및 실행환경조건에 따라서 유동적이다.

[표 3]의 No.23의 경우와 같이 6 자리의 패스워드는 영소문자, 영대문자, 숫자, 특수문자 모두를 혼합하여 복잡하게 구성되어 있더라도 최대 약 3일 15시간 안에 패스워드를 검출해 낼 수 있다는 걸 알 수 있다. 그리고 No.19와 같이 영소문자로만 이루어진 경우는 8 자리로 패스워들 설정하더라도 최대 약 1일 10시간 안에 패스워드가 검출됨을 알 수 있다. 특히 No.3과 같이 숫자로만 이루어진 경우는 8 자리라도 최대 약 50초 안에 패스워드가 검출 가능하다. 숫자로만 구성된 패스워드는 No.5에서 알 수 있듯이 10 자리의 패스워드라도 최대 약 1시간 20분 안에 검출 가능하다.

Ⅴ. 타 회사 메신저 문제점

메신저 인증 메커니즘의 문제는 네이트온 메신저만의 문제는 아니다. 타 회사 메신저의 인증 메커니즘도 [표 4]와 같이 유사한 문제점들을 갖고 있었다.

Ⅵ. 결 론

지금까지 네이트온 메신저의 인증 트래픽 분석을 통해 네이트온 메신저의 사용자 인증 메커니즘에 대해 자세히 알아보았다. 그리고 분석 결과로부터 네이트온 메신저가 재전송 공격과 사전공격에 취약하다는 것을 알 수 있었다.

현재 대부분의 포털사이트에서 제공하고 있는 메신저를 통해 사용자는 포털사이트가 제공하는 서비스로 연결될 수 있다. 포털사이트의 인증은 이전에 비해 많이 개선되었지만 메신저 서비스를 통해서 다시 보안에 구멍이 생긴 것이다. 그러므로 메신저 서비스를 제공하고 있는 포털사이트들은 웹사이트에서 제공하는 보안접속의 기능을 메신저에도 적용해야 본 논문에서 설명한 것과 같은 취약점을 막을 수 있을 것이다.

참고문헌

[1] Chin-Chen Chang, Tzong-Chen Wu and Chi-Sung Laih, Cryptanalysis of a password authentication scheme using quadradic residues. Computer communications, Vol. 18 No. 1, January 1995, pp 45-47.

[2] C.S. Laih, L. Harn and D. Huang, Password authentication using public-key encryption, Proceeding of 1983 International Carnahan Conference on Security Technology, Zurich, Switzerland, October 1987, pp 35-38.

[3] Chin-Chen Chang, Wen-Yuan Liao, Remote password authentication scheme based upon ElGamal's signature schemem, Computers & Security, Vol. 13, No. 2, Apr, 1994, pp 137-144.

[4] Chun-Li Lin, Tzonelih Hwang, A password authentication scheme with secure password updating, Computers and Security, Vol. 22 No. 1, 2003, pp 68-72.

[5] Lei Fan, Jian-Hua Li, Hong-Wen Zhu, An enhancement of timestamp-based password authentication scheme, Computers and Security, Vol. 21 No. 7, 2002, pp 665-667.

[6] A. Menezes, P. Van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. Boca

Raton, FL: CRC Press, 1997.
[7] 원동호, 현대암호학 2004년 3월
[8] 정보보호진흥원 암호인증기술팀, SEED 알고리즘을 이용한 개인키 암호화 기술규격[v1.00], 정보보호진흥원, 2004.
[9] The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt
[10] PasswordsPro, Inside Pro, http://www.insidepro.com/eng/passwordspro.shtml
[11] 마이크로소프트의 패스워드 설정 원칙, http://www.microsoft.com/athome/security/privacy/password.mspx
[12] 미국 NIST 전자인증 가이드라인 표준, NIST Special Publication 800-63 - AppendixA http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
[13] The SANS Institute, Password Protection Policy Standards Organization, http://www.sans.org/resources/policies/Password_Policy.pd

<著者紹介>

신 동 휘(Donghwi Shin) 학생회원
2002년 2월: 성균관대학교 자연과학부 물리학과(이학사)
2002년 2월: 성균관대학교 전기전자컴퓨터공학부(공학사)
2002년 3월~2002년 9월: 성균관대학교 일반대학원 물리학과 석사과정
2006년~현재: 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 네트워크보안, 침투테스트, 정보보호 응용

최 윤 성(Younsung Choi) 학생회원
2006년 2월: 성균관대학교 정보통신공학부(공학사)
2006년~현재: 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 디지털 포렌식, 정보보호 응용, PKI, 보안성 평가

박 상 준(Sangjoon Park) 종신회원
1986년 2월: 한양대학교 수학과 석사
1999년 2월: 성균관대학교 정보공학과 박사 (암호전공)
1986년 1월~1999년 12월: 한국전자통신연구소 부호기술부 선임연구원
2000년 1월~2000년 10월: 국가보안기술연구소 책임연구원
2000년 11월~2005년 5월: (주)비씨큐어 부사장
2005년 7월~현재: 성균관대학교 정보보호기술연구소 연구교수
<관심분야> 암호 알고리즘, 키 분배, 인증 및 서명, 암호분석

김 승 주(Seungjoo Kim) 종신회원
1994년 2월～1999년 2월: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월～2004년 2월: 한국정보보호진흥원(KISA) 팀장
2004년 3월～현재: 성균관대학교 정보통신공학부 교수
2001년 1월～현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월～현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 7월～현재: 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호(Dongho Won) 종신회원
1976년～1988년: 성균관대학교 전자공학과(학사, 석사, 박사)
1978년～1980년: 한국전자통신연구원 전임연구원
1985년～1986년: 일본 동경공업대 객원연구원
1988년～2003년: 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년～1998년: 국무총리실 정보화추진위원회 자문위원
2002년～2003년: 한국정보보호학회장
현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호 인증기술연구센터 센터장, IT보안성평가연구회 위원장
<관심분야> 암호이론, 정보이론, 정보보호