메신저의 통신 구조 분석 및 사용 차단 방식의 제안

안규성 최진구

한국산업기술대학교 컴퓨터공학과
{dksrbtjd, jkchey}@kpu.ac.kr

The proposal of access blocking methods in messenger

KyuSung Ahn Jinku Chey
Dept. of Computer Engineering, Korea Polytechnic University

요 약

기업 내에서 메신저 사용으로 인한 정보유출이나 근무태만에 대하여 대처하기위해 메신저 사용을 차단하는 방법은 제안한다. 차당방법을 제안하기에 앞서 현재 범용의 메신저를 실제 IP 스니핑을 통한 테스트로 구조를 분석하고 그 분석된 구조를 바탕으로 메신저 차단 제어의 3가지 방법을 제안 한다.

1. 서 론

메신저란 인터넷에서 실시간으로 메시지와 데이터를 주고받을 수 있는 소프트웨어이다. 메신저는 E-mail과 다르게 등록되어 있는 수신자들의 상태(On/Off-Line)를 알 수 있어 실시간으로 대화할 수 있다. 이런 메신저의 실시간성과 신속성 등의 장점 때문에 메신저 사용자수는 2001년에 소개 된 이후 꾸준히 늘어 현재 우리나라의 인터넷 사용자의 48.5%가 메신저를 이용할 정도로 보급이 널리 되어 있다.[1] 이런 높은 보급률과 장점 때문에 기업에선 업무의 효율성을 높이고자 메신저를 사용한다.

하지만 이런 기업 내에서 메신저의 사용은 업무의 효율성을 높이는 긍정적인 부분이 있는 반면에 또한 기업의 정보누출의 가능성과 메신저 사용자가 근무시간에 사적인 용도로 사용하여 근무태만이 되는 문제도 있다. 때문에 기업 내에서의 메신저 사용을 필요에 따라 제재할 필요성이 있다. 본 논문에선 메신저 통신 구조를 분석하고 분석한 내용을 토대로 메신저 사용을 차단 할 수 있는 방법을 제시한다.

2. 관련연구

2.1 메신저 통신 구조

메신저 통신구조는 크게 Client-Server, P2P, 혼합 구조로 나누어 볼 수 있다.

2.1.1 Client - Server 통신구조

메신저(Client)가 메신저 서버(Server)에 접속하여 모든 정보를 주고받는 방식이다. 대부분의 메신저는 이 방식을 기반으로 구현되어 있다. 인증, 친구리스트, 채팅 등의 데이터 모두 메신저 서버에게 보내고 받는다. Client-Server로 통신하는 상황에서는 내 PC가 오로지 메신저 서버와 통신하게 되므로 친구로 등록되어 있는 다른 사용자의 IP 주소를 얻을 수 없다.

2.1.2 P2P (Peer To Peer) 통신구조

메신저(Peer : Client 의 다른 이름)가 다른 사용자의 메신저(Peer)와 직접 연결하여 정보를 주고받는 방식이다. 메신저의 대용량 파일전송의 기능은 대부분 P2P 로 구현되어 있다. P2P 통신이 진행 중인 상태에서는 내 PC가 상대방의 PC와 직접 통신하게 되므로 상대의 IP주소를 얻을 수 있다.

2.1.3 혼합 통신구조

현재 NateOn, MSN 메신저는 Cilent - Serve 방식과 P2P 방식을 혼합하여 사용하고 있다. 사용자 인증과 대화, 저용량 파일 전송은 Client - Server 방식을 사용하고 있고 대용량 파일은 P2P 방식을 사용하고 있다.

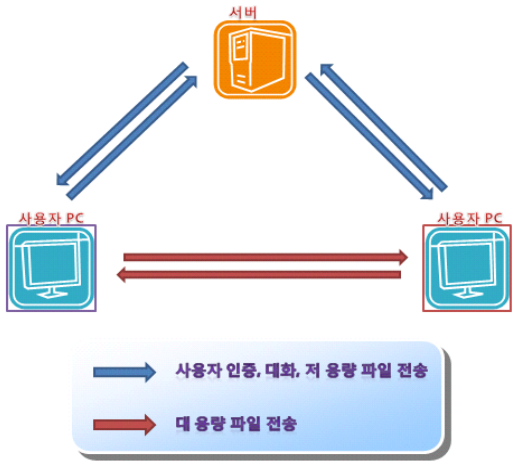


그림 1. 혼합방식의 메신저 통신 구조

3. 본 론

3.1 IP 스니핑을 통한 실제 통신 구조 분석

2대의 PC를 사용하여 대화 시, 파일 전송 시에 어떻게 동작하는지 분석하였다. 2대의 PC의 IP 주소는 다음과 같다.

A PC : 10.60.1.105

B PC : 10.60.1.177

분석한 메신저는 NateOn, Msn, BuddyBuddy 이다. 분석 툴은 Microsoft Network Monitor 3.3을 사용하였다.

3.1.1 서버 접속 시(로그인 시)

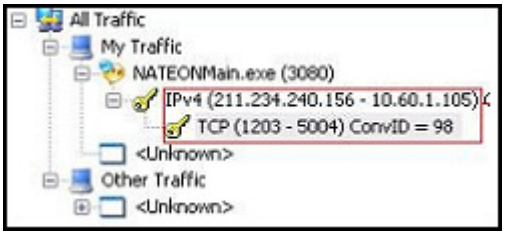


그림 2. 처음 서버에 접속했을 때

[그림 2]와 같이 처음 접속을 하면 포트가 하나 열리는데 이 포트(5004)로 통신을 하면서 대화 상대방들의 접속 여부에 대해서 알려준다. 대화 상대가 접속하거나 접속을 끊게 되면 서버에서 이 포트를 사용하여 정보를 전송한다.

3.1.2 대화를 하기 위해 대화창을 열었을 때

다음은 A PC에서 B PC로 대화를 신청하는 상황이다.

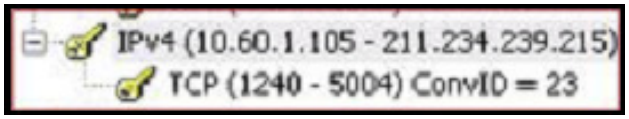


그림 3. A PC에서 B PC로 대화신청 했을 때

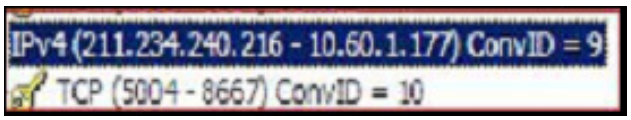


그림 4. B PC에서 대화신청을 받았을 때

[그림3,4]에서 앞의 IP가 source IP 이며 뒤의 IP는 Destination IP이다.

[그림3]과 같이 A PC에서 B PC로 대화를 신청할 시에 열리는 포트의 Destination IP 가 B PC의 IP가 아닌 NateOn 서버 IP임을 알 수 있다. 또한 B PC에서도 Source IP가 대화상대인 A PC의 IP가 아닌 NateOn 서버의 IP 임을 알 수 있다. 이와 같이 대화 구조를 보면 (A PC - Server - Server - B PC) 의 구조로 이루어져 있다. 이로써 NateOn 메신저의 대화 구조는 Client - Server 구조로 되어 있음을 알 수 있다.

3.1.3 파일 전송 시

다음은 A PC에서 B PC로 100MB 이상의 파일을 전송하는 상황이다.

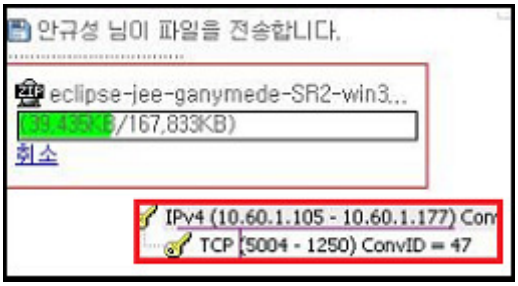


그림 5. A PC에서 B PC로 대용량 파일을 전송 할 때

Destination IP, Source IP를 보면 A PC와 B PC가 서버를 거치지 않고 직접 연결되어 있음을 알 수 있다. NateOn은 대용량 파일 전송은 Peer To Peer 방식을 사용하고 있다는 것을 알 수 있다. (저용량 파일은 서버를 경유하여 전송이 이루어진다).

3.1.4 테스트 결론

테스트 결과 NateOn, MSN 메신저는 사용하는 포트, IP만 다를 뿐 기본적인 구조는 대화 시엔 Server - Client 방식 대용량 파일 전송 시에는 Peer To Peer 방식을 사용하고 있고 BuddyBuddy는 대용량 파일 전송 시에도 Peer To Peer 방식이 아닌 Server - Client 방식을 사용하고 있다.

3.2 메신저 서버 간 통신 구조

메신저는 Dispatch Server, Notification Server, Switchboard Server로 구성되어 있다.

3.2.1 Dispatch Server

사용자가 처음 접속 시 사용자 인증을 위해 접속하는 서버이다. 사용자 인증이 완료되면 Notification Server의 IP를 전송해 준다.

3.2.2 Notification Server

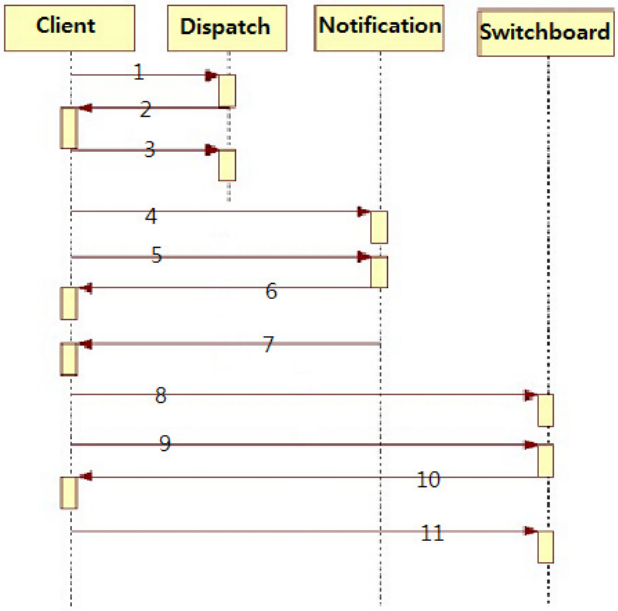
인증 완료 후 Dispatch Server에서 전송받은 IP로 접속한 서버가 Notification Server이다. Notification Server는 Session 확립과 Switchboard Server의 IP, PORT를 알려주는 역할을 한다.

3.2.3 Switchboard Server

사용자간의 대화나, 파일 전송 시 연결을 해주는 역할을 한다.

3.2.4 서버 간 통신 구조

[그림 6]과 같이 Client 는 Dispatch Server로 인증을 하고 Notification Server와의 지속적인 통신을 통해 친구로 등록된 사용자들의 상태와 대화를 요청하고 대화를 수락하기 위한 정보를 송수신한다. 그리고 상대방과 대화를 하거나, 저용량 파일을 송수신 할 때 Switchboard Server를 경유하여 정보를 송수신 한다.



1. 사용자가 인증을 한다.
2. Dispatch Server가 Notification Server의 IP, PORT정보를 Cilent에게 전송한다.
3. Dispatch Server와의 연결을 종료 한다.
4. Dispatch Server에서 받은 Notification Server의 IP, PORT로 접속을 시도한다.

5,6. Sesseion을 확립하고 인증을 한다.

7. Switchboard Server의 IP, PORT 정보를 Client에게 전송한다.
8. Switchboard Server와의 연결을 시도한다.

9,10. Messege를 송/수신한다.

11. Switchboard Server와의 연결을 종료한다.

* 이 때 Notification Server와의 Session은 계속 유지한다.

그림 6. 메신저 서버 간 통신 구조

3.3 차단방법

3.3.1 IP 차단방법 (IP Table 확립)

가장 기본적인 차단방법이다. 메신저 서버의 IP 정보를 IP Table에 확립한 후 서버로 나가는 모든 패킷을 차단하는 방식이다. 주기적인 IP Table의 무결성(완벽히 차단이 되는지) 검사와 업데이트가 필요하다. 밑의 [표1]에 명시된 IP를 차단하면 해당 메신저의 사용을 차단할 수 있다.

	Messenger		2009.8.27
	NateOn	Msn	BuddyBuddy
차단 IP	***211.234.240.****	***64.4.9.****	***211.115.122.****
	203.226.253.*	***207.46.125.****	
		64.4.15.*	
		64.54.239.*	
		207.46.107.*	
		64.4.34.*	

표1. IP Table

Messenger Service 측에서 Dispatch Server로 가는 IP를 변경할 경우 IP Table을 업데이트하기 전까지 차단이 풀려버린다. 그러므로 주기적인 차단 테스트와 IP Table의 Contents의 주기적인 관리가 필요하다.

3.3.2 프로세스 차단방법

메신저 소프트웨어의 실행 자체를 차단하는 방법이다. 메신저 프로세스의 실행을 차단함으로써 메신저 사용을 차단한다. API Hooking 이나 윈도우즈의 방화벽 같은 여러 가지 접근 방법으로 차단이 가능하다. 프로세스의 실행파일 이름을 근거로 차단을 했을 경우 실행파일의 이름만 바꾸어주면 우회가 가능하기 때문에 메신저 수정을 할 수 없는 프로세스의 클래스 네임이나, 컨트롤 텍스트를 근거로 하여 프로세스를 차단하는 방식도 병행되어야 한다.

3.3.3 메신저 프로세스에서 사용되는 패킷 차단방법

메신저 프로세스에서 사용되는 모든 패킷을 차단하는 방법이다. IP 차단방법과 다른 점은 차단하는 패킷의 근거가 다른데 IP 차단방법은 Destination IP(Dispatch Server IP)를 인식하여 차단하는 방식이며 메신저 프로세스 패킷 차단 방식은 해당 패킷이 차단된 프로세스에서 사용되는 패킷이면 차단하는 방법이다.

각각의 차단방법에는 우회방법이 존재하거나 취약한 부분이 있으므로 3가지 방법을 병행하여 취약한 부분을 보완할 수 있다.

4. 결 론

본 논문에서는 기업 내에서 메신저 사용으로 인한 정보유출이나 근무태만에 대하여 대처하기위해 메신저 사용을 차단하는 방법은 제안했다. 차당방법을 제안하기에 앞서 현재 범용의 메신저를 실제 IP 스니핑을 통한 테스트로 구조를 분석하고 그 분석된 구조를 바탕으로 메신저 차단 제어의 3가지 방법을 제안했다. IP차단, 메신저 프로세스 차단, 메신저 프로세스에서 사용되는 패킷 차단의 3가지 방식은 각각의 우회 방법이 존재한다. 예를 들어 IP 차단방법 같은 경우 대기업에서는 라우터를 통하여 메신저 접속을 금지시키는데 이는 IP만 우회시키면 접속이 가능하기 때문에 iloveim과 같은 사이트에서 실제로 IP를 우회시켜 메신저를 사용할 수 있게 해주는 서비스를 제공한다. 이와 같이 하나의 방법만 사용할 경우 신뢰성이 크게 떨어지므로 3가지 방법을 병행, 조합하여 사용함으로써 차단의 신뢰성을 높인다.

끝으로 메신저 차단에 대한 연구는 차단을 해제 하려는 악의적인 사용자들이 계속해서 다른 방법으로 시도하려고 하기 때문에 이에 발맞추어 지속적으로 연구가 이루어져야 한다.

5. 참고문헌

[1] 인터넷진흥본부 '2009년 7월 미국과 한국의 인터넷 이용을 비교한 한국과 미국의 인터넷이용실태비교 보고서'

[2] 신동희 'Cryptanalysis on the authentication mechanism of the NateOn Messenger'

[3] 양대일 '정보 보안 개론' 한빛미디어

[4] James F.Kurose, Keith W.Ross 'Compurter Networking 4th' pearson

[5] 김희정 '직장인 79%, 근무 안하고' 한경뉴스