pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.5.223

A Study on Countermeasures against Messenger Phishing using ARIT Technique

Sung Kyu Cho† · Jun Moon Seog††

ABSTRACT

With the rapid development of IT technologies, many people talk to each other in real time on-line using messenger or use the messenger to share files for work. However, using this convenience, phishing crimes occur: e.g. demanding money, and if a criminal uses a bypassing technique like proxy in order to hide the IP address the criminal has used to log on, it is in fact, difficult to find the criminal's real IP address. This paper will propose a plan to measure against messenger phishing that may occur in advance by collecting the IP address with which a user has used in a dual channel mode and the real IP address obtained by ARIT Agent using ARIT technique, going through a separate identification process and deciding whether the user has accessed in a normal method.

Keywords : Massenger, Phishing, IP Traceback, Proxy

ARIT 기법을 이용한 메신저 피싱 대응방안에 관한 연구

조 성 규† · 전 문 석††

요 약

IT기술의 급속한 발전으로 인해 인터넷 상에서 많은 사람들이 메신저를 이용해 실시간으로 대화를 나누거나 업무처리를 위한 파일 공유 등에 메신저를 사용하고 있다. 하지만 이런 편리성을 이용해 금전 요구 등의 메신저 피싱 범죄가 발생하고 있으며, 범죄자가 자신이 접속한 IP 주소를 은닉하기 위하여 Proxy와 같은 우회기법을 사용할 경우 범죄자의 Real IP 주소를 확인하는 것은 어려운 실정이다. 본 논문은 ARIT 기법을 이용해 2채널 방식으로 접속 IP 주소와 ARIT Agent를 이용해 얻은 Real IP 주소를 수집하여 별도의 확인 과정을 거친 후, 사용자가 정상적인 방법으로 접속했는지 여부를 판단하여 사전에 발생할 수 있는 메신저 피싱에 대응할 수 있는 방안에 대해 제시하고자 한다.

키워드 : 메신저, 피싱, IP 역추적, 프락시

1. 서 론

인터넷을 사용하고 있는 많은 사용자들은 이메일보다 메신저를 이용해 실시간으로 대화를 하거나 업무처리를 위한 파일 공유 등에 메신저를 사용하고 있다. 이러한 메신저의 편리성 때문에 우리나라 인터넷 사용자의 48.5%가 메신저를 사용하고 있으며[1], 포털 사이트 및 기업에서도 그들만의 자체 메신저를 개발하여 보다 효율적으로 업무가 이루어질 수 있도록 이용하고 있다.

근래에는 이와같이 편리한 메신저의 기능을 범죄자들이 악용하여, 타인의 정보를 이용해 메신저에 접속한 후 등록된 지인들에게 부당하게 돈을 요구하거나 신용카드정보, 비밀번호 등을 요구하는 피싱 공격이 빈번히 늘어나고 있는 실정이다[2].

국정감사 자료에 의하면 2010년~2011년 7월말까지 메신저 피싱 범죄는 총 2,171건이 발생한 것으로 나타났으며, 한달 평균 74.8건, 하루 평균 3.7건이 발생하였다[3].

또한 범죄자들은 자신의 접속 IP 주소를 속이기 위해 불상의 방법을 통해 접속하기 때문에 범죄자의 Real IP 주소를 알기가 어려우며, 범죄가 발생하여도 검거하는데 많은 어려움이 따른다. 그러므로 사전에 이와같은 범죄가 발생하지 않도록 차단하는 것이 무엇보다 필요한 상황이다.

본 논문에서는 ARIT(Agent-based Real IP Traceback)를 통해 범죄자의 Real IP 주소를 추출하고 메신저 피싱을 사전에 탐지하는 방안에 대해 제시하고자 한다.

본 논문의 구성은 2장에서 메신저의 구조와 기능 및 메신저 연결방식에 대해 살펴보고, 3장에서는 Real IP 추출기법

† 준 회 원 : 숭실대학교 컴퓨터학과 박사과정
†† 종신회원 : 숭실대학교 컴퓨터학과 교수
논문접수 : 2013년 2월 4일
수 정 일 : 1차 2013년 3월 18일
심사완료 : 2013년 3월 18일
* Corresponding Author : Sung Kyu Cho(flashbit@naver.com)

에 대해 설명한다. 4장에서는 실제 실험을 통한 메신저 피싱에 대한 탐지기법 적용 결과를 제시하며, 5장에서 결론을 맺는다.

2. 관련 연구

2.1 메신저의 구조와 기능

메신저는 일반적인 P2P(Peer-to-Peer) 방식과 다르게 하나의 메신저 서버를 통해 동작한다. 현재 사용되고 있는 메신저는 다양한 기능을 제공하고 있다. 즉 다자간 채팅과 음성채팅 등을 지원하면서, 대용량의 동영상 파일 전송과 이동전화 및 문자 메시지 교환 등의 기능도 제공하고 있다. Fig. 1은 사용자가 메신저 서버로 접속 시 이루어지는 절차를 도식화 한 것이다[4].

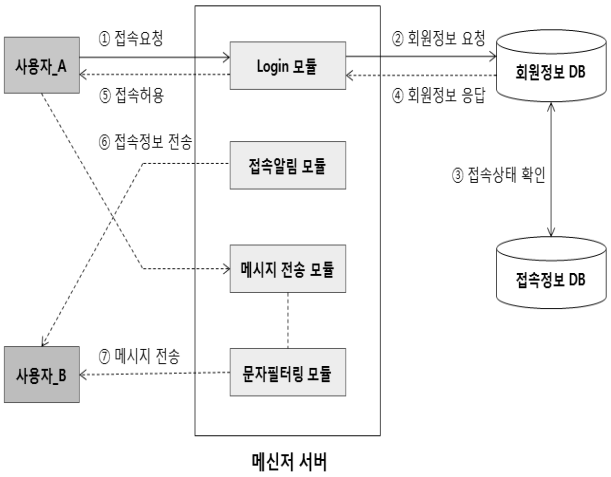

Fig. 1. General messenger access structure

① 사용자 A가 아이디와 패스워드를 입력 후 메신저 서버로 접속 요청을 한다.
② 메신저 서버는 사용자가 입력한 아이디와 패스워드가 일치하는지 확인하기 위해 회원정보 DB를 검색한다.
③ 회원정보 DB를 검색 후 아이디와 패스워드 정보가 일치한 경우, 접속정보 DB를 이용해 동일한 아이디를 사용하여 현재 접속된 상태인지 확인한다.
④ 아무런 문제가 없는 경우 Login 모듈로 정상적으로 접속 할 수 있다는 응답 메시지를 전송한다.
⑤ Login 모듈은 접속정보 DB로부터 수신 받은 정보를 이용해 사용자 A가 로그인할 수 있도록 허용한다.
⑥ 사용자 A에 등록된 지인들에게 사용자 A가 접속한 것을 알려주기 위해 접속 알림 모듈을 이용해 다른 사용자들에게 접속 정보를 전송한다.
⑦ 메신저를 통해 사용자 A와 사용자 B가 실시간으로 대를 주고받을 때 문자필터링 모듈은 통장계좌 및 카드번호 등 위험성이 있는 메시지가 검색될 경우 사용자에게 주의 메시지를 전송하게 된다.

2.2 메신저 연결방식

메신저는 보다 안정적으로 관리하고 보안을 강화하기 위해 여러 개의 서버들과 접속하게 된다. 각각의 서버들은 수많은 사용자를 처리할 수 있도록 역할을 하므로 분리된 서버를 거쳐 사용자가 접속하기 때문에 다른 프로토콜들에 비해 접속 속도가 비교적 느리다.

1) Dispatch Server

Dispatch Server(DS)는 사용자가 메신저로 접속할 수 있도록 처리해 주는 역할을 한다. 사용자가 메신저로 로그인을 시도할 경우 가장먼저 접속하는 서버가 DS이다. DS는 Notification Server(NS)들로 접속할 수 있는 정보들을 보유하고 있으므로 DS는 NS의 상태를 보고 사용자가 접속할 수 있도록 적당한 NS의 IP 정보와 Port 번호를 사용자에게 알려주는 역할을 한다.

만약 사용자가 사전에 알고 있는 NS의 IP 주소와 Port 번호가 있을 경우 DS를 통하지 않고 바로 NS로 접속하는 것이 가능하다.

2) Notification Server

Notification Server(NS)는 사용자가 DS로 부터 수신한 NS의 IP 주소와 Port 번호를 이용해 접속한 사용자 인증과정을 확인한 후 정상적으로 사용자 인증이 이루어질 경우 NS로 접속하게 된다.

3) Switchboard Server

Switchboard Server(SS)는 대화하기 위해 사용자들이 직접 세션을 만들 수 있도록 하는 컴포넌트(Component)이다. SS는 같은 대화세션에 참여하고 있는 사용자에 한해 서로 간의 메시지 교환을 할 수 있도록 한다.

2.3 Proxy 접속방식

IP 주소는 인터넷에 연결된 모든 통신망과 서로 통신할 수 있도록 부여되는 고유의 식별번호이므로 범죄자는 자신이 사용하고 있는 IP 주소를 외부로 유출하지 않도록 다양한 우회기법을 통해 웹사이트, E-Mail, 메신저 등을 이용한다.

Proxy 서버는 사용자가 요청한 정보를 대신해 다른 네트워크 서비스로 접속할 수 있는 간접적인 역할을 수행한다. 즉 서버와 클라이언트 사이에 중계기 역할을 해 사용자가 요청한 정보를 대신 목적지로 전달하고 목적지로부터 수신한 정보를 다시 사용자에게 전송하게 된다.

초기 Proxy 서버는 사용자가 요청한 정보를 캐시 메모리에 저장한 후 동일한 정보를 다시 요청할 경우 캐시 메모리에 저장된 정보를 빠르게 전송함으로써 네트워크 속도를 향상시키는 역할로 사용했지만 IT 산업이 급속도로 발전하면서 초고속 인터넷이 일반화된 지금은 Proxy 서버를 통해 정보를 요청하는 것보다 직접 목적지로 정보를 전송하는 것이 훨씬 빠르므로 현재는 많이 사용하지 않는다[5]. Proxy 서버는 Transparent, Anonymous, High Anonymity 유형이 존재한다.

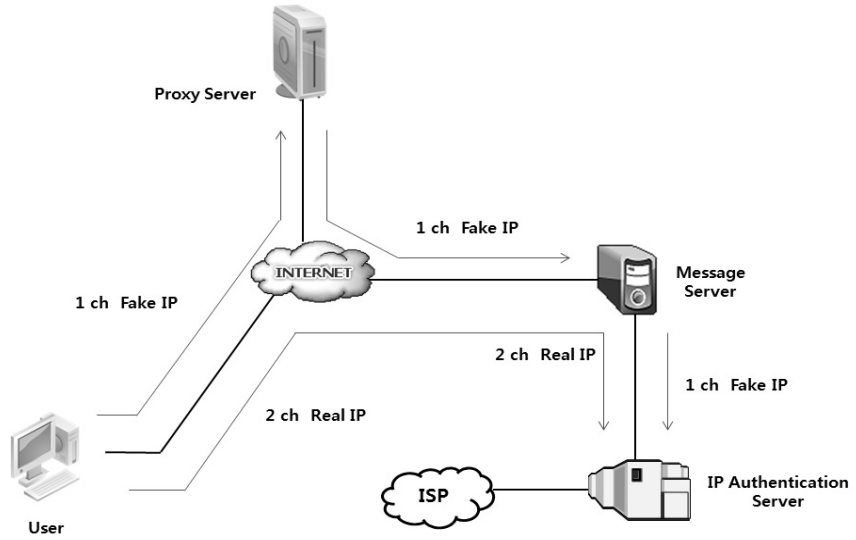

Fig. 2. Checking accessor location

1) Transparent

Transparent는 순수하게 캐시 서버나 사용자가 요청한 정보에 대해 대행해 주는 서버로 동작한다. 즉 Transparent는 클라이언트의 모든 정보를 서버로 전송하므로 Proxy Server를 통해 정보를 수신하는 것을 제외하면, 사용자가 직접 정보를 목적지로 전송하는 것과 큰 차이가 없다. 사용자가 Transparent 유형으로 Proxy 서버를 통해 접속할 경우 패킷 헤더를 통해 사용자의 Real IP 주소를 확인할 수 있다.

2) Anonymous

Anonymous 유형은 Transparent 처럼 사용자의 IP 주소가 패킷 헤더에 기록되지 않으므로 IP 주소를 숨길 수 있다. 하지만 패킷 헤더 정보를 이용해 Proxy 서버를 통해 접속했다는 사실을 확인할 수 있다.

3) High Anonymity

High Anonymity는 패킷 헤더에 어떤 정보도 포함되지 않기 때문에 Proxy 서버를 통해 접속했다는 사실을 확인할 수 없다. 결과적으로 자신의 IP 주소를 속이기 위해 가장 좋은 방법이라고 할 수 있으며, 범죄자들이 가장 많이 사용하고 있는 방법 중 하나이다.

3. Real IP 추출

메신저 피싱은 타인의 메신저 아이디를 도용해 로그인한 뒤 등록된 지인에게 금전을 요구하는 행위 등을 의미하며, 접속된 IP 주소를 추적해 보면 대부분 Proxy 서버 또는 제3의 방법을 이용해 접속하므로 범죄자를 검거하기는 매우 어렵다. 본 논문에서 제시한 ARIT 기법을 적용할 경우 기존 방법보다 쉽고 정확한 IP 주소를 추출할 수 있으며, 사전에 발생할 수 있는 메신저 피싱을 차단 할 수 있다.

3.1 Real IP 주소 수집

ISP(Internet Service Provider)는 IP 주소 블록을 할당받고 최종 사용자에게 IP 주소를 분배한다. IP 주소는 서로 중복될 경우 문제가 발생할 수 있기 때문에 각 기관은 IP 주소를 할당할 때 어떤 사용자가 IP 주소를 사용하고 있는지 모든 정보를 기록하게 된다.

인터넷을 통해 검색할 경우 사용자가 이용하고 있는 IP 주소의 위치를 확인해 근거리의 관련 정보를 보여주는 것처럼 메신저 상에서도 상대방이 어느 지역에서 접속했는지 확인할 수 있다. Fig. 2 처럼 사용자가 Proxy 서버를 통해 접속 시 본 논문에서 제시한 기법인 2채널 방식을 통해 Fake IP 주소와 Real IP 주소를 수집한 후, IP 인증 서버를 통해 ISP로 전송하여 사용자 위치를 실시간으로 확인할 수 있다. 접속한 사용자의 Real IP 주소를 추출하기 위해서 사용자가 메신저를 이용하는 컴퓨터에 Plug-in 방식으로 역추적 에이전트 모듈을 설치한다[6].

Fig. 3은 클라이언트가 사용하고 있는 IP 주소를 추출하기 위한 알고리즘을 보여준다.

```
Regex regex = new
Regex(@"^(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\
d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\
d|25[0-5])$");

foreach (System.Net.IPAddress ip in
System.Net.Dns.GetHostEntry(System.Net.Dns.GetHostName( )
).AddressList)
{
if (regex.IsMatch(ip.ToString()))
{
return ip.ToString();
```

Fig. 3. IP address extracting algorithm

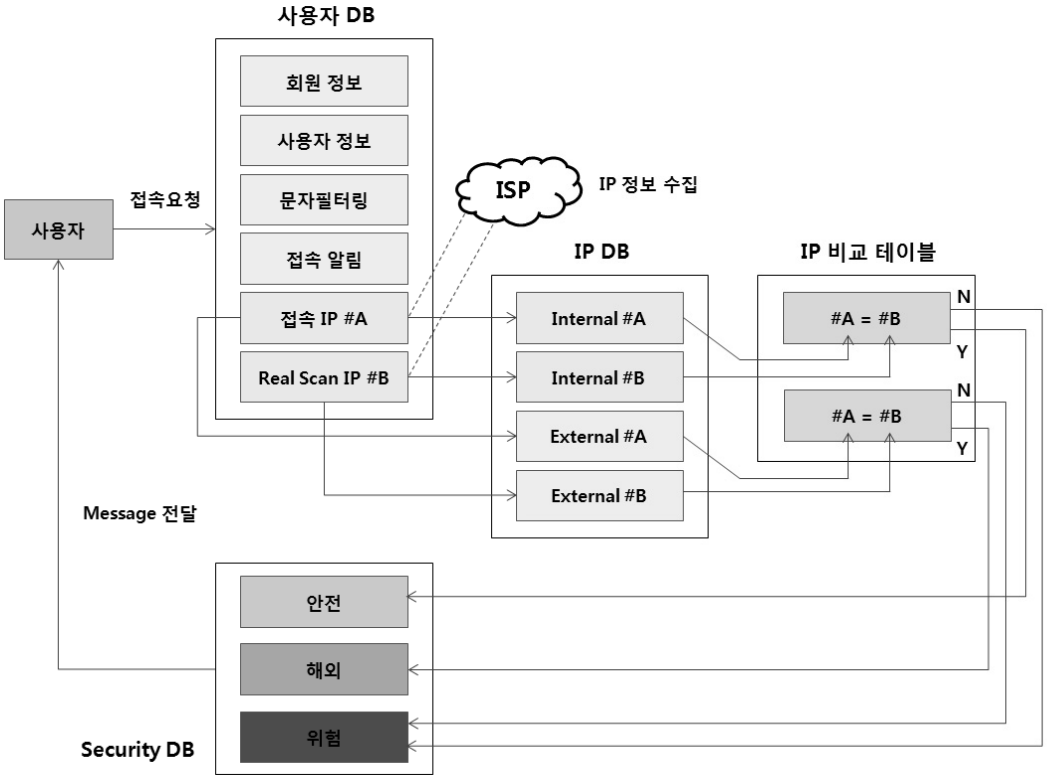

Fig. 4. IP address authorization

3.2 IP 주소 인증

IP 주소를 인증하기 위해 사용자가 접속한 IP 주소와 ARIT를 통해 수집한 IP 주소를 ISP로 전송해 해당 IP 주소의 위치를 확인해 다른 사용자에게 안정성 여부를 알려주어야 한다.

Fig. 4은 사용자가 메신저 서버로 접속 시 사용자 DB는 아이디와 패스워드를 정상적으로 입력했는지 확인한 후 해당 아이디를 통해 접속된 사용자가 있는지 확인하고 사용자가 정상적인 방법으로 접속했는지 또는 비정상적인 방법으로 접속했는지 확인하여 메신저에 등록된 지인들에게 안전성 여부를 알려주는 구조이다.

1) 사용자 DB

사용자 DB는 접속자 관련 정보들을 관리하는 데이터베이스이다.

a) 회원 정보: 사용자가 자신의 아이디와 패스워드를 입력할 경우 회원정보 데이터베이스를 통해 인증한다.
b) 사용자 정보: 메신저에 등록된 지인들에 대한 정보들을 관리하는 데이터베이스이다.
c) 문자필터링: 등록된 지인들과 실시간 대화를 주고받을 때 위험성 문장이 탐지될 경우 경고성 메시지를 전송하기 위한 데이터베이스이다.
d) 접속 알림: 메신저에 등록된 지인들에게 사용자의 메신저 접속사실을 알려주기 위한 데이터베이스이다.
e) 접속 IP #A: 사용자가 메신저 서버로 접속할 때 사용한 IP 주소를 ISP로 전송해 해당 IP 주소가 사용되고 있는 곳이 어디인지 확인한 후 ISP로부터 수신한 정보를 IP DB로 전송하기 위한 데이터베이스이다.
f) Real Scan IP #B: Real IP Scan으로 부터 수집한 IP주소를 ISP로 전송해 해당 IP 주소가 사용되고 있는 곳이 어디인지 확인한 후 ISP로부터 수신한 정보를 IP DB로 전송하기 위한 데이터베이스이다.

2) IP DB

IP DB 테이블은 접속 IP와 Real IP 주소에 대한 정보를 관리하는 데이터베이스이다.

a) Internal #A: 접속 시 사용한 IP 주소가 ISP로부터 국내에서 사용되고 있는 IP 주소로 인증된 경우 관리하는 데이터베이스이다.
b) Internal #B: Real IP Scan으로부터 수집한 IP 주소가 ISP로부터 국내에서 사용되고 있는 IP 주소로 인증된 경우 관리하는 데이터베이스이다.
c) External #A: 사용자가 메신저 서버로 접속한 IP 주소가 ISP로부터 해외에서 사용되고 있는 IP 주소로 인증된 경우 관리하는 데이터베이스이다.
d) External #B: Real IP Scan으로부터 수집한 IP 주소가 ISP로부터 해외에서 사용되고 있는 IP 주소로 인증된 경우 관리하는 데이터베이스이다.

3) IP 비교테이블

IP 비교테이블은 IP DB로부터 받은 정보를 이용해 접속한 IP 주소와 ARIT로 수신한 IP 주소를 비교해 정상적인 방법으로 접속했는지 확인하기 위한 데이터베이스이다. 즉, Internal #A, Internal #B 및 External #A, External #B로 부터 수신한 IP 주소를 비교해 사용자가 접속한 IP 주소와 ARIT로 수집한 IP 주소를 서로 비교해 같은 IP 주소인 경우 Security DB로 전송해 메신저 서버에 등록된 지인들에게 "안전"하다는 메시지를 전송하고 만약 서로 다른 IP 주소인 경우 메신저 서버에 등록된 지인들에게 "위험"하다는 메시지를 전송하게 된다.

사용자가 접속한 IP 주소와 Real IP Scan으로 수집한 IP 주소가 모두 해외 IP 주소인 경우 비교테이블에서 Security DB로 전송해 사용자에게 "해외"에서 접속한 사용자라는 사실을 알리게 된다.

3.3 Application 인증

Fig. 5는 사용자가 메신저 프로그램을 통해 접속할 경우 메신저 서버는 ARIT Agent가 정상적으로 설치되었는지 확인한 후 정상적으로 설치되어 있지 않은 경우 ARIT Agent를 설치할 수 있도록 하는 과정을 보여준다. 이후 아이디와 패스워드를 통해 메신저로 로그인할 경우 사용자가 접속한 IP 주소와 ARIT Agent를 통해 수신한 IP 주소를 통합정보 DB로 전송해 위치기반 서비스를 이용하여 IP 주소를 확인 후, 로그인할 수 있도록 하고 분석 모듈을 통해 분석하게 된다. 이후 IP 인증 모듈을 통해 접속한 IP 주소와 ARIT Agent로 수신한 IP 주소를 확인 후 Security DB로 전송해 최종적으로 사용자에 대한 안정성 여부 메시지를 전송하게 된다.

4. 실험 및 분석

실험을 통해 본 논문에서 제안한 모델에 대해 ARIT 기법을 이용하여 Real IP 주소를 정상적으로 수집하는지에 대한 기능을 검증하고, 비정상적인 방법을 통해 접속한 사용자에 대해 경고메시지를 전송하는지에 대해 확인하였다.

4.1 실험환경

본 논문의 실험 환경은 ARIT Agent 기법이 적용되지 않는 상태에서 우회기법을 이용하여 메신저 서버로 접속할 때와 본 논문에서 제안한 기법을 적용한 후 우회기법을 통해 접속했을 때 정상적으로 Real IP 주소를 추출하여 다른 사용자에게 접속자 위치를 알려주는지 확인하였다. 또한, 메신저를 통해 기능의 정상적인 동작을 확인하기 위하여 간단한 기능의 메신저를 개발하여 실험하였다[4, 7, 8].

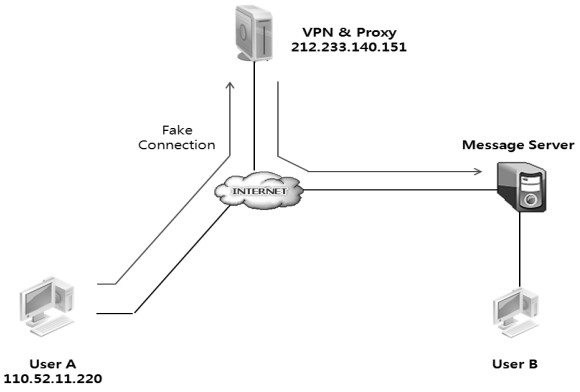

Fig. 6. Messenger access using a proxy server

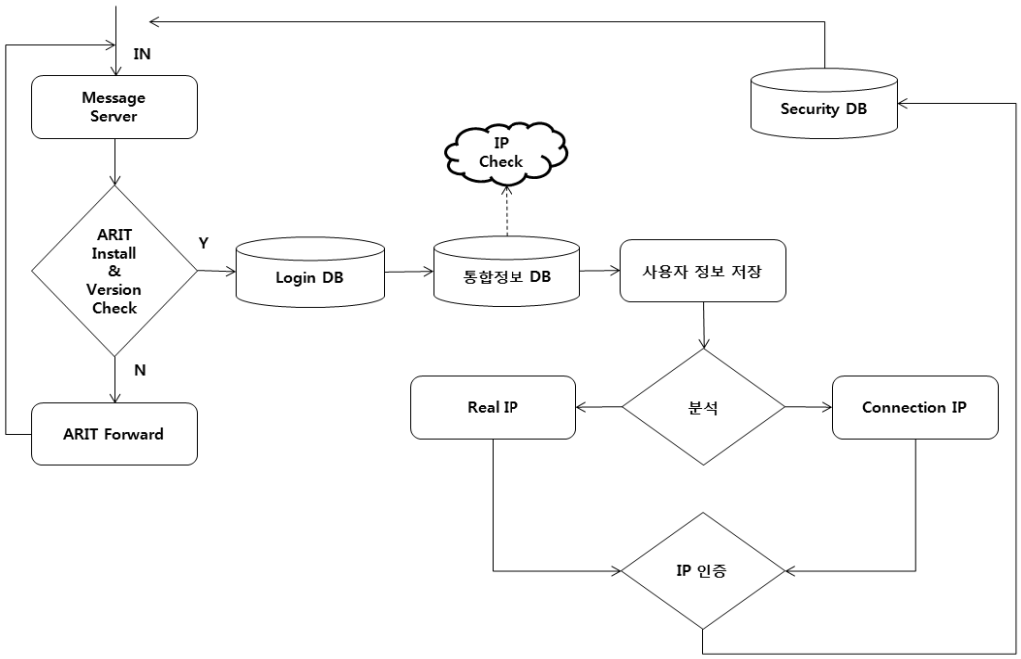

Fig. 5. Application Architecture

```
mysql> select * from Real_IP;
+----+----------+---------------+----------+--------+--------+
| No | Date     | Real_ip       | Proxy_ip | Vpn_ip | Status |
+----+----------+---------------+----------+--------+--------+
|  1 | 20130126 | 212.233.140.151 |          |        |        |
+----+----------+---------------+----------+--------+--------+
1 row in set (0.00 sec)
```

Fig. 7. DB breakdown of the results of connections to which ARIT is not applied

4.2 ARIT 적용 전

Fig. 6는 사용자 A가 타인의 정보를 이용해 Proxy 서버를 통해 접속할 경우 메신저 서버와 사용자 B는 사용자 A가 정상적인 방법으로 접속을 시도했는지의 여부를 알 수 없다는 것을 확인하였다.

위 접속 내역을 확인해 보면 사용자 A가 사용하고 있는 IP 주소가 110.52.11.220이며, 접속된 정보를 확인해 보면 212.233.140.151로 기록되어 있는 것을 확인할 수 있다. 즉 사용자 A가 불상의 방법을 이용해 우회기법을 적용하여 접속한 사실을 알 수 없다는 것을 확인하였다.

4.3 제안기법 적용

Fig. 8은 사용자가 타인의 정보를 이용해 메신저 서버로 접속해도 본 논문에서 제시한 ARIT 기법을 이용하여 우회기법을 통한 접속자의 실질적인 Real IP 주소를 모두 추출한 후, Security DB에서 접속한 IP 주소와 ARIT로 부터 수신한 IP 주소를 비교하여 사용자에게 위험성 여부를 알려주는 것을 확인하였다.

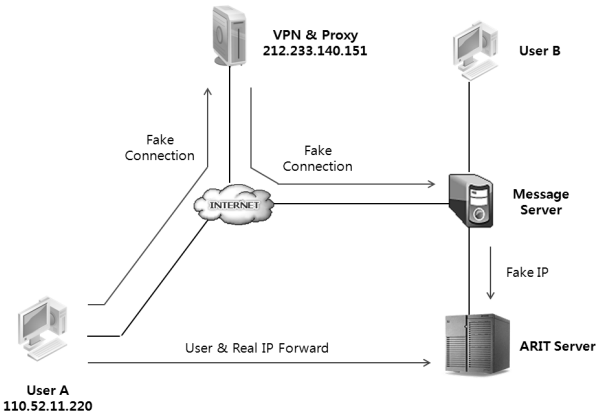

Fig. 8. Check abnormal access

Fig. 9의 접속내역을 살펴보면 사용자 A가 사용하고 있는 Real IP 주소와 사용자가 우회기법을 통해 접속한 IP 주소를 정상적으로 수신한 것을 확인할 수 있으며, 비정상적인 방법으로 접속했다는 정보도 기록되어 있는 것을 확인하였다. Fig. 10는 본 논문에서 제시한 기법을 이용해 메신저 프로그램을 통해 접속했을 때 정상적으로 위험성 여부를 알려주는 것을 보여주고 있다.

```
mysql> select * from Real_IP;
+----+----------+---------------+---------------+--------+---------+
| No | Date     | Real_ip       | Proxy_ip      | Vpn_ip | Status  |
+----+----------+---------------+---------------+--------+---------+
|  1 | 20130126 | 212.233.140.151 |               |        |         |
|  2 | 20130126 | 110.52.11.220   | 212.233.140.151 |        | Warning |
+----+----------+---------------+---------------+--------+---------+
2 rows in set (0.01 sec)
```

Fig. 9. DB breakdown of the results of connections to which ARIT is applied

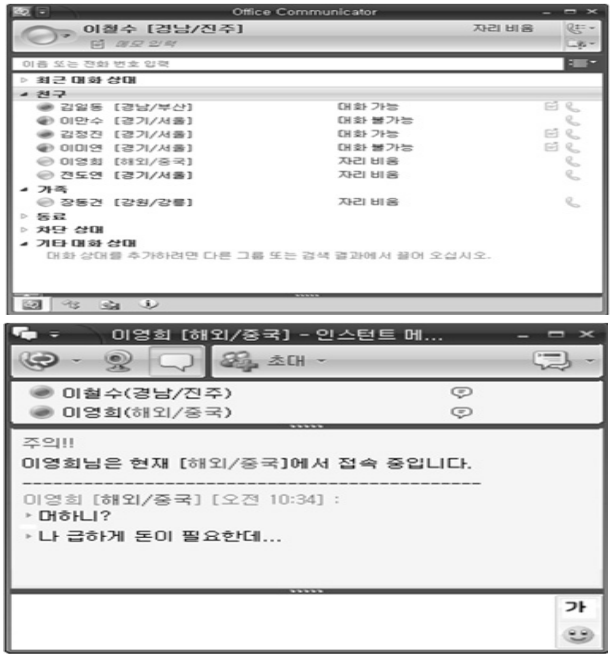

Fig. 10. Sending warning messages through messenger

4.4 IP 역추적 기법 비교

지금까지의 실험 결과를 바탕으로 기존에 나와 있는 대표적인 IP 역추적 기법인 Backscatter, Link-testing traceback의 특징 및 단점과 ARIT 기법과의 비교를 통해 ARIT 기법의 우수성에 대해 살펴보도록 한다.

Table 1에 기술한 것처럼, ARIT 기법을 이용할 경우 기존의 방식들에 비해 불필요한 작업을 최소화 할 수 있으며, 공격지 주소를 변조한 패킷의 실제 IP주소를 효율적으로 얻을 수 있는 장점을 가지고 있다.

또한, 현재 범용적으로 사용되고 있는 네이트온 메신저의 경우 사용자에게 피싱 공격의 위험성을 경고하기 위해 같은 아이디로 동시 접속 시 다중접속 알림 기능, 대화 상대방의 본인 인증 서비스 기능, 금전과 관련된 문구가 대화에 포함될 경우 경고 메시지 생성 및 신고하기 기능 등을 지원하고 있다. 하지만 이와 같은 네이트온의 피싱 경고 기능은 공격자가 자신의 접속 IP주소를 은닉하기 위한 공격을 시도하는 것은 탐지하지 못하므로, 기존에 네이트온 등의 메신저에서 지원하는 피싱 경고 기능과 함께 본 논문에서 제시하는 기

Table 1. Comparison of IP traceback techniques[9, 10]

IP 역추적 기법	특징 및 단점	
Backscatter	특징	출발지 주소를 Spoofing한 패킷을 라우터가 Drop할 경우, ICMP unreachable 패킷을 패킷의 발신지 쪽으로 보내게 되며, ICMP unreachable 메시지는 거의 랜덤하게 흩어져서 되돌려지게 (Backscatter) 된다. 이 때 대규모 IP 영역을 Shinkhole 네트워크로 지정하여 대규모 네트워크에서 공격의 진입지점을 찾아내는데 활용할 수 있다.
	단점	· Sinkhole 라우터는 가능한 충분한 대역폭을 확보해야 함 · 합법적인 트래픽도 서비스 거부 결과를 가져올 수 있음
Link-testing traceback	특징	Hop-by-Hop 단위로 작동하는 기법이다. Link Testing 기법은 현재 존재하고 있는 프로토콜을 응용하여 구현될 수 있으며 각 라우터에서 링크를 조사하여 특정 패킷이 어떤 링크로 유입되었는지 결정한다. 이러한 정보를 통해 공격자로부터 공격 대상까지의 통신 체인을 결정한다.
	단점	· 많은 시간과 자원 필요 · 통신 체인에 포함되는 모든 인터넷 사업자(ISP)의 협조 필요 · 역추적이 끝나는 시점까지 공격이 이어져야 함
ARIT	우수성	· 패킷의 경로 보다 실제 패킷이 출발한 근원지의 IP주소를 알 수 있음 · 불필요한 대규모의 네트워크 트래픽을 유발하지 않음 · ISP 협조, 자원 이용 등이 최소로 소요됨 · 연결이 끊어져도 공격지의 IP 주소를 확보할 수 있음

능들을 함께 적용한다면 좀 더 효율적으로 불법적인 피싱 공격에 대한 대응이 가능하여 질 것이다.

5. 결 론

메신저를 이용한 피싱 등이 발생할 경우, 사용자가 접속한 IP 주소만을 추출하거나 에이전트를 통해 사용자 컴퓨터에 적용된 IP 주소만을 추출하는 방식으로는 실질적으로 IP 주소를 역추적해도 근원지를 찾을 수 없는 경우가 많다. 또한 IP 주소를 역추적해 근원지를 찾는다 해도 해외 IP 주소로 확인되는 경우가 많기 때문에 범죄자를 검거하기는 어려운 실정이다.

하지만 본 논문에서 제안한 ARIT 기법은 2 채널 방식으로 사용자가 자신의 접속 IP 주소를 속이기 위해 우회기법을 이용해도 Real IP 주소를 추출해 사전에 발생할 수 있는 메신저 피싱을 탐지하여 이용자들에게 경고 메시지를 전송함으로써, 금전사기 등의 피해를 사전에 방지할 수 있는 기능을 제공하는 것이 가능하다.

참 고 문 헌

[1] Kyu-Sung Ahn, Jin-Ku Chey, “The proposal of access blocking methods in messenger”, Paper Collection of the Korea Information Science Society, Vol.37, No.1, pp.94-96, 2010.

[2] JuHyun Kim, YoungJae Maeng, DaeHun Nyang, KyungHee Lee, “Cognitive Approach to Anti-Phishing and Anti-Pharming”, The Korea Institute of Information Security and Cryptology, Vol.19, No.1, pp.113-124, 2009.

[3] TaeWon Kim, Messenger phishing occured 3.7 times a day[Internet], http://ktw.or.kr/contents/bbs/board.php? bo_table=AOA&wr_id=492.

[4] Geum-wuk Seo, “Messenger Structure Design using WCF”, Micro Software, pp.320-326, 2007.

[5] Shin-Beom Kang, Sang-Jin Lee, Jongin Lim, “A Study on the Criminal Threat and Privacy Protection with a Proxy Service”, Vol.22, No.2, pp.317-326, 2012.

[6] Ji-won Gang, “IP Back-tracking Model using improved BPbT Technique”, Doctoral Dissertation in Kyonggi University, 2012.

[7] Yoeung-Jun Yoon, Kyoung-Hwan Pyo, Seung-Soo Sin, Kun-Hee Han, “Desing of Messenger for Secure Communication between Users”, Spring Symposium Paper Collection of the Korea Academia-Industrial Cooperation Society, Vol.1, pp.81-84, 2010.

[8] Bo-go Jung, Gwang-soo Rhee, “A Design and Implementation of Secure Instant Messenger”, Journal of the Information Processing Society of Korea, Vol.8, pp.213-220, 2001.

[9] Byung-yun Park, “Even Correlation Analysis with Traceback for Network Security”, Doctoral Dissertation in Kongju University, 2010.

[10] Tae-soo Kim, “A Study on Design Analysis System for Analyzing DDoS Attack and IP Traceback on All-IP Network”, Masteral Dissertation in Hanshin University, 2010.

조 성 규

e-mail : flashbit@naver.com
1998년 성결대학교 컴퓨터공학과(학사)
2002년 숭실대학교 컴퓨터학과(석사)
2005년~현 재 숭실대학교 컴퓨터학과 박사과정
관심분야 : 네트워크 보안, 개인정보보호, 암호학, 인증

전 문 석

e-mail : mjun@ssu.ac.kr
1981년 숭실대학교 컴퓨터학과(학사)
1986년 University of Maryland 전산과(석사)
1989년 University of Maryland 전산과 (Ph. D.)
1989년 Morgan State University 전산수학과 조교수
1991년~현 재 숭실대학교 컴퓨터학부 정교수
관심분야 : 정보보호, 전자여권, 전자상거래, 암호학