

Exploiting Instant Messengers

Błażej Miga

<blazej.miga@man.poznan.pl>

Jarosław Sajko

<jaroslaw.sajko@man.poznan.pl>

Who are we?

- Security Team of PSNC
- Gadu-Gadu, Tlen, WPKontakt
 - December 2004
- Security audits, code analyses, security systems
- Research projects: SGIGrid, Clusterix, Unizeto, Progress
- Homepage: <http://security.psnc.pl>
- Valkyrie IDS developers



Motivation

- To present our research results in the field of the instant messengers security
- To prove that the instant messenger can be a serious threat
- To prove that exploiting the instant messengers bug can be a really trivial
- To increase the consciousness level of the instant messengers users

Presentation outline

for vulnerability in vulnerabilities:

1. describe a vulnerability
2. present the Proof-Of-Concept
3. discuss prevention methods

Vulnerability Set

- Scripting vulnerability
- Direct connections misdesigns & vulnerabilities
- Simple stack based buffer overflow

Tools

Tools, exploits, etc. needed for this tutorial can be downloaded from our website:

<http://security.psnc.pl/>

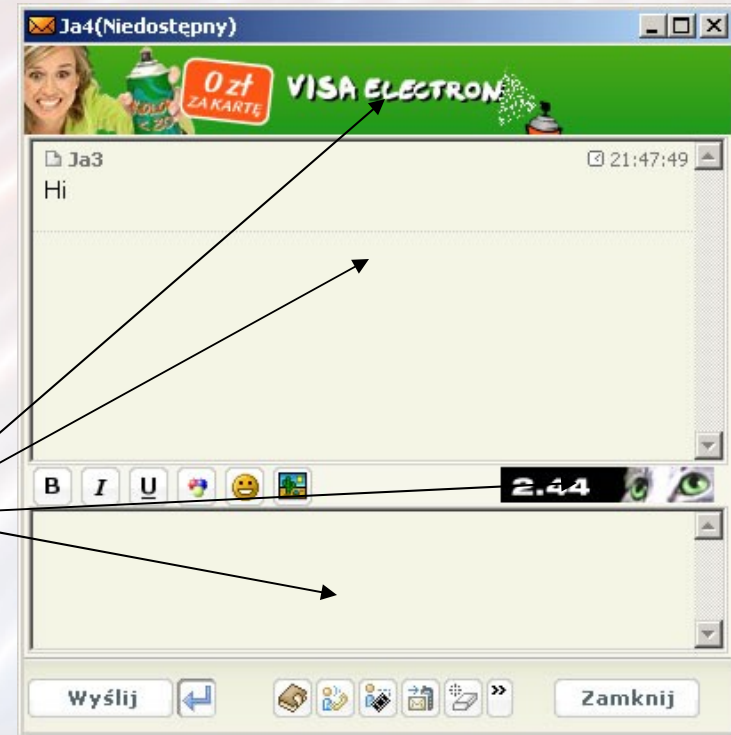
Just a text message (1)

Everybody knows that web browsing is relatively insecure. The web is vast, there is a lot of space for the nasty pages. Not everybody knows that many of the most popular instant messengers are built on the strength of the Internet Explorer. Indeed your chat window is often the Internet Explorer instance.

Just a text message (2)

Gadu-Gadu (a popular Polish instant messenger) chat window

Internet_Explorer_Server component



Just a text message (3)

That „just a text message” is in fact the html page. The text displayed in the chat window is delivered by the user from the second end. It should be carefully parsed and checked for presence of malicious tags and formatting statements.

Writing secure parser is non-trivial

Just a text message (4)

During an audit of the Gadu-Gadu application code many parser bugs were revealed. One of them was the security bug which was chosen for the purpose of this presentation.

„Parsing error. We can send a malicious string which has an url inside. This url can be a javascript code for example or a reference to such a code. Code will execute when the window with message pops up. The code will execute in LOCAL ZONE! „

```
www.a" style=background-  
image:url(JaVaScRiPt:document.write('%3cscript%3ealert%28  
%22you%20are%20owned!%22%29%3c%2f script%3e'));" .pl
```

Just a text message (5)

Go for it!

Just a text message (6)

- Step 1 (optional)
 - Download and install the Python interpreter
- Step 2 (optional)
 - Download and install the GG application (build 154)
 - Create an account for testing purposes

Just a text message (7)

- Step 3
 - Download the gg-scripting.py exploit
- Step 4
 - Launch the exploit and watch for results:

```
gg-scripting.py <your uin> <your pass> <victim's uin>
```

Just a text message (8)

How to prevent?

- Lower or customize your Internet Settings
- Don't talk to the strangers
- If your IM „executes” messages in the Local Zone, use another one
- Unpatched web browser equals vulnerable IM

Direct Infections (1)

Many Instant Messengers have the direct connections feature. Voice and video connections and file transfer are the most usual examples of direct connections usage. In most cases the proprietary protocol is used for such purpose.

It is non-trivial to design a safe and secure protocol.

Direct Infections (2)

Gadu-gadu allows to interchange the files between users even if they are behind the NAT. How do they do that?

It is simple. Each user can ask the other user to connect to the given address. It is assumed that this is the external address of the asking user (ie. firewall address used for port forwarding). But in fact it could be any address. Moreover, the asked user is never prompted to accept the connection request. The whole process goes behind him/her.

Direct Infections (3)

There are more weak points:

- Undocumented protocol codes – strange feature like banner sharing. A possibility of silent transfer banners between the application clients.
- The protocol is stateless and has many misdesigns – we can send an error message again and again and the error box pops up each time.

Direct Infections (4)

Just do it!

Direct Infections (5)

- Step 1
 - Download the gg-dccthief.py exploit

- Step 2
 - Launch the exploit and watch for results

```
gg-dccthief.py <your uin> <your pass> <victim's uin> <filename>
```

Direct Infections (6)

How to prevent?

- (Re)consider using the direct connections
- Tighten your personal firewall policy
- If your IM's DC functionality is working in the unclear way, use another IM or don't use DC.

Where is the firewall? (1)

Firewall is a nice tool which can be helpful if we want to secure our network. But if we are using instant messengers we have to allow outbound connections to the instant messenger server. If the instant messenger protocol is proprietary it is hard to inspect and filter its content. Especially if the content is ciphered (ie. tunneled over the SSL). Thereby if we have the vulnerability within the instant messenger the firewall can become pretty useless.

Where is the firewall? (2)

During an audit of the Gadu-Gadu application several buffer overflows were revealed. One of them was the stack based buffer overflow. That vulnerability was posted to the vendor about a year ago. Today another similiar buffer overflow exists in the newest version of that instant messenger.

This BO concerns image sending. The file name of the image simply can overrun the buffer.

Where is the firewall? (3)

**Let's check where
the firewall is!**

Where is the firewall? (4)

- Step 1
 - Download the gg-imaging.py exploit
- Step 2
 - Launch the exploit and watch for results

```
gg-imaging.py <your uin> <your pass> <victim's uin>
```

Where is the firewall? (5)

How to prevent?

- Using non-exec page protections can eliminate the attack vector, but not the vulnerability itself.
- One can minimize the functionality of the instant messenger application but this is not the way.
- You can take care about the quality of software which you use and this is the best you can do.

Conclusions and Questions

- Instant Messenger can be a serious threat
- The firewall is not always a solution
- The icon in the tray is small, but if it is there, we have the doors open

Thank you very much!