

# **The (in)security of Omegle**

## **What Omegle users should know.**

**By Valentin Höbel. Mail to [valentin@xenuser.org](mailto:valentin@xenuser.org)  
(February 2010)**

- I. What is this document about?**
- II. About Omegle**
- III. Introduction**
- IV. Understanding Omegle**
- V. Summary**
- VI. Sources and other stuff**

### **I. What is this document about?**

When I first heard of Omegle I was fascinated from it's idea and simple usage. This service seems to promise a lot of fun and interesting conversations.

In January 2010 I started to get interested in the details: How does Omegle work and is this service secure?

Sadly it didn't take long until I found out that Omegle comes along with some serious security issues.

Since I did not find many articles about this I decided to write this document and explain to normal Omegle users why they should be concerned about their privacy.

In this document, most things are based on the stuff Bear24rw (Max Thrun) found out. I just put the pieces together and explain why Omegle should be enjoyed with caution.

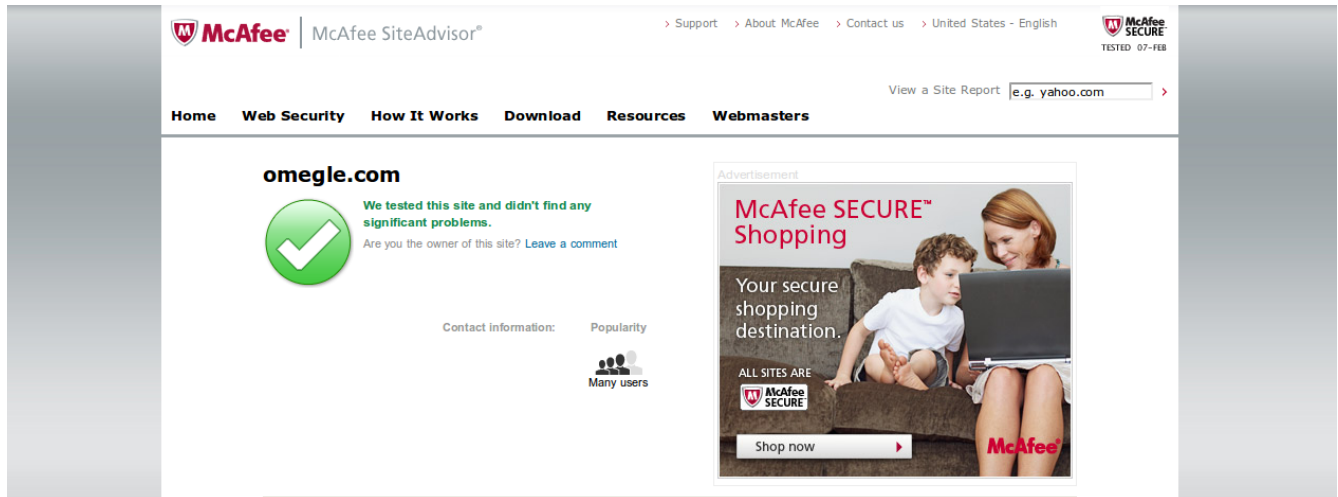
### **II. About Omegle**

“Omegle is a brand-new service for meeting new friends. When you use Omegle, we pick another user at random and let you have a one-on-one chat with each other. Chats are completely anonymous, although there is nothing to stop you from revealing personal details if you would like.” [1]

This service has become very popular and is used by thousands of people all over the world.

### III. Introduction

When you enter the chat room and talk to a stranger you disclosure your information to the Omegle server. In general when using such a service you can thrust the company or private individual running this service. You rely on their competence and feel secure since everything should be secure and encrypted. Right?



The screenshot shows the McAfee SiteAdvisor interface for the website omegle.com. At the top, there is a navigation bar with links for Support, About McAfee, Contact us, and United States - English. The main content area features a green checkmark icon and the text: "We tested this site and didn't find any significant problems. Are you the owner of this site? Leave a comment". Below this, there is a section for "Contact information:" and "Popularity:" with a "Many users" icon. To the right, there is an advertisement for McAfee SECURE Shopping, featuring a woman and a child sitting on a couch with a laptop. The ad text includes "Your secure shopping destination." and "ALL SITES ARE McAfee SECURE". A "Shop now" button is visible at the bottom of the ad.

In this case you may be wrong putting your trust into this service. Various things indicate that Omegle is very open and not secure at all.

Being interested in the way Omegle works, I started Wireshark (sniffer tool) and watched the packages scrolling down my screen while I was chatting with some stranger.



**Talk to strangers!**

You're now chatting with a random stranger. Say hi!

**Stranger:** asalamualikum

**You:** huhu

Your conversational partner has disconnected.

[Start a new conversation](#) or [save this log](#) or [send us feedback](#)

Well, this was a short conversation. Let's see what wireshark is saying:

```
▼ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Transfer-encoding: chunked\r\n
    Date: Sun, 07 Feb 2010 14:37:39 GMT\r\n
    Content-type: application/json\r\n
    Server: TwistedWeb/8.1.0\r\n
    \r\n
  ▸ HTTP chunked response
▼ Line-based text data: application/json
  [["gotMessage", "asalamualikum"]]
-----
0050  4b 0d 0a 54 72 61 6e 73 66 65 72 2d 65 6e 63 6f  K..Trans fer-enco
0060  64 69 6e 67 3a 20 63 68 75 6e 6b 65 64 0d 0a 44  ding: ch unked..D
0070  61 74 65 3a 20 53 75 6e 2c 20 30 37 20 46 65 62  ate: Sun , 07 Feb
0080  20 32 30 31 30 20 31 34 3a 33 37 3a 33 39 20 47  2010 14 :37:39 G
0090  4d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 74 79 70 65  MT..Cont ent-type
00a0  3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73  : applic ation/js
00b0  6f 6e 0d 0a 53 65 72 76 65 72 3a 20 54 77 69 73  on..Serv er: Twis
00c0  74 65 64 57 65 62 2f 38 2e 31 2e 30 0d 0a 0d 0a  tedWeb/8 .1.0....
00d0  32 31 0d 0a 5b 5b 22 67 6f 74 4d 65 73 73 61 67  21..["g otMessag
00e0  65 22 2c 20 22 61 73 61 6c 61 6d 75 61 6c 69 6b  e", "asa lamualik
00f0  75 6d 22 5d 5d 0d 0a 30 0d 0a 0d 0a  um"]].0 ....
```

Bingo! See the text at the bottom right of the picture? It seems that Omegle still sends data unencrypted.

I am not the only one who found this out. Actually Bear24rw already described this issue in a blog entry [2]. Omegle communicates the data the following way:

```
You: POST omegle.com/start
Omg: HTTP "123456" <-- random 6 digit 'username' (a-z A-Z 0-9 _ -)
You: POST omegle.com/events?id=123456
Omg: HTTP [["connected"]]
You: POST omegle.com/send?msg=hello&id=123456
Omg: HTTP win <-- funny
You: POST omegle.com/events?id=123456
Omg: HTTP [["gotMessage", "hey"]] <-- message from other person
...
You: POST omegle.com/disconnect?id=123456 <-- quit the chat
```

Some new facts just popped up. Omegle gives every use a random ID (containing of 6 digits), Omegle uses the “events”-script and uses the POST-method for communication.

We now know enough to go further...

#### **IV. Understanding Omegle**

We now know that Omegle uses some script called “event” to handle the data. It doesn't take a high IQ to guess that the Omegle service also contains some sort of queue which stores the users (e.g. the users waiting for a chat partner) and the messages.

This should look like this:

Client1 <--send/receive data--> Server <--send/receive data--> Client2

Based on this assumption, Bear24rw described a scenario where man in the middle attacks would make it possible to send messages to users who don't have a clue that you are here. Another idea would be to even link dozens of chatters together in one single chat room.

Another Omegle user who already looked at the security of this service also developed some ideas about how to have some more fun.

John Sichi published his man in the middle script here [3].

#### **V. Summary**

The fact that manipulating the chat sessions is possible makes this service highly insecure when you keep in mind that some people reveal their personal data to other chatters and think that this information is “safe”.

The private individual running Omegle should already be aware of this issue and make some changes so using this service is more secure.

Anyway, I think it is a great achievement that someone that young (as far as I know this guy is 18/19 years old) develops such a great idea and service. Omegle is very fun and should be developed further.

#### **VI. Sources and other stuff**

[1] Description taken directly from omegle.com

[2] <http://bear24rw.blogspot.com/2009/11/omeglecom-man-in-middle-attack.html>

[3] <http://thinkwaitfast.blogspot.com/2009/09/i-should-really-get-job-soon.html>

Thx going out to Max Thrun alias Bear24rw for his thoughts about Omegle and the security issues.

You may publish this document and copy stuff in any way you like.

Valentin Höbel

valentin@xenuser.org

<http://www.xenuser.org>