

## Re: Secure chat

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2005-09/0109.html>

---

**From:** Juergen Nieveler ([juergen.nieverer.nospam\\_at\\_arcor.de](mailto:juergen.nieverer.nospam_at_arcor.de))

**Date:** 09/14/05

Date: 14 Sep 2005 13:02:26 GMT

Volker Birk <[bumens@dingens.org](mailto:bumens@dingens.org)> wrote:

>> *As I see it, that leaves only two things open: The amount of traffic  
>> going over my TOR connection, and the fact that the Jabber-server will  
>> know who I send messages to. The first can be taken care of by creating  
>> random traffic over the TOR link when not chatting.  
>> Is there such a thing as Onion-Routing-Messaging, or a Mixmaster-like  
>> Jabber system to take care of the second issue?*  
>  
> *The random traffic is needed to avoid knowing anybody, when you're  
> communicating.*

Yes, but that only takes care of wiretaps on your own end. Anybody with access to the server will be able to see who you send messages to, as all messages are routed through the server. Hence the idea of a Mixmaster-like messaging system – you send an encrypted IM to a random contact, who decrypts it and receives instructions to pass the message on to the next recipient. As it's encrypted, he doesn't know whether it's the final recipient or just another forwarder.

Hang on... technically, one wouldn't even need to install this on the server end, would one? This could be handled exclusively on the client side, and it could be built into a client as default. As the "Mixmaster" – messages are encrypted, it doesn't matter whether the client sees the messages. Therefore, if you build a "Mixmaster" into every IM client, to send non-traceable messages all you need to do is choose a recipient at random from all the clients that are online at that time. The client would decrypt the message, and if it's destined for him, he'd show it to the local user. If not, he'd pass it on to the next hop...

Any takers? Does this sound like a workable concept?

Juergen Nieveler

--

Speed-optimizing the code?!? Don't you have a PENTIUM PRO??!!