

Secure Chat Sessions Using Pidgin with OTR For Encryption

Wednesday, 12 September 2007

Chatting on AOL Instant Messenger (also known as AIM) is a convenient way to communicate. Many people are unaware of an interesting fact: using the AIM program from AOL is NOT required. It is possible to log on to the AIM network using alternative software such as Pidgin. Pidgin does not have annoying advertisements or excessive features. In fact, you can start with a minimal set of features and add more as you go along by using what are called plug-ins.

The Pidgin OTR plug-in uses encryption to create a secure chat environment between two people. The only requirement is that both people are using OTR. Encryption essentially scrambles the text of the conversation with complicated mathematical algorithms. This prevents nosy hackers (which there are more of than most people think) from being able to read conversations should they attempt to "sniff" data being sent over the network. These packet sniffing attacks are more common than people expect, and are completely untraceable since they occur over the network and not directly on the computer. Even if someone assumes they are not likely to be attacked this way, they would not know if the person who they are chatting with is being watched. It could come from prying hackers or even the IT department at their job. In the U.S., it is currently legal for employers to monitor their employees on-line activity in the office without giving notice.

Here are step-by-step instructions for downloading and installing Pidgin as well as instructions for downloading and installing the OTR plug-in:

- Download Pidgin [here](#) and install it.
- After installing, run Pidgin.
- The first time you run it, it will show you a list of your AIM accounts and ask you which ones you want to import. Select the account(s) you intend on using for Pidgin. Each one you select will ask you for the password and if you want it to remember the password or not. Which one you choose is up to you. Enter your password and choose if you want it to be remembered or not. Click "OK".
- After selecting the accounts you want, click "Close". Pidgin will now log you in automatically. You will see your buddy list.

- Close Pidgin now. This is important to do before the next step.
- Download OTR (Win32 installer for pidgin) and install it.
- After installation, run Pidgin again and log in. Click "Tools" to pull down the Tools menu, then click "Plugins".
- Scroll down the list of plug-ins until you see "Off-the-Record Messaging" and click the empty box to the left of it so that a checkmark appears.
- Click "Configure Plugin" at the bottom of the window. This will open up a window with some options.
- Under "My private keys:" where it says "Key for account:", use the pulldown menu to select which account you want to use for encrypted chat.
- Click the button that says "Generate" and wait patiently for your private key to be created.
- When it is finished, click "OK". Never give this key to anyone.
- Click "Close" on the OTR preferences window.
- Click "Close" on the Plugins window.

From now on OTR will automatically detect if a person you start a chat with is also using it. This automatically creates a secure connection without you having to do anything to start it. If you found this article useful, show it to anyone else you want to have secure chat sessions with.

For added privacy, configure Pidgin to use a SSH SOCKS proxy tunnel.