Secure Instant Messaging / Chat

Michael Chesbro, Ph.D., CCIA, CCIP

February 15, 2014

Many people use instant messaging (IM) / chat programs to communicate with their friends and family on-line. IM is a convenient, effective, and even fun way to stay in contact with others, no matter where they may be – as long as they have an Internet connection. There are several IM programs available. Just a few of these programs are: AIM, Google, ICQ, IRC, and Yahoo. Unlike posts to social media sites (i.e. a post to your Facebook Timeline), IM tends to be used for more personal and private communication; a conversation between just the people chatting, not an announcement posted for everyone to see.

Unfortunately most IM is not really private. It is a trivial matter for someone with good computer skills to monitor your IM. Using IM over a public WiFi network (such as at a coffee shop or hotel) increases your risk of being monitored and having your private conversations spied on. Service providers (i.e. Google and Facebook) can also, of course, monitor and record any non-encrypted traffic on their networks.

If you regularly use IM to communicate with your friends and family on-line, you should consider installing Pidgin (https://www.pidgin.im) on your computer. Pidgin is a universal chat client that brings all of your IM programs together in one place. Pidgin is not an IM / chat program itself, rather it allows you to run all of your chat programs (AIM, Facebook, Google, Yahoo, etc.) from within one program. If you run the MAC Operating System, download Adium (https://adium.im), a version of Pidgin for MAC OS X. You need to have at least one IM account, such as AIM, Facebook, Google, or Yahoo, to use Pidgin / Adium.

Having all of your IM programs conveniently located in one place would be in and of itself a good reason to use Pidgin, but for the security-minded person there is even a better reason. Using the "Off The Record (OTR)" plugin with Pidgin / Adium you can encrypt all of your on-line chats with anyone else using the same program and a compatible IM client.

Once you have downloaded and installed Pidgin, you will also need to download and install OTR. The OTR download page is located at https://otr.cypherpunks.ca For Adium the OTR plugin comes pre-installed. In addition to encryption, OTR allows for user authentication, perfect forward secrecy so that if your encryption key ever gets compromised previous messages are still safe, and deniability. It should be noted that OTR is different from Pidgin-Encryption which is a different plugin that provides encryption and authentication, but not deniability or perfect forward secrecy.

Security and Privacy

Plugin Name	Website	Short Description
Advanced Auto Auth	Go	auto accept cert and auth requests in perl, only win32
Authorization Blocker	Go	The plugin blocks the first authorization request of a contact and answers with the order to ask for authorization again. This helps to prevent spam on ICQ accounts.
bOt_tOOls	Go	Configurable plugin for auto-ignoring yahoo spammers
Bot Sentry	Go	Stop spam bots
IM of Trust	Go	Pidgin IM of Trust blocks authorization requests based on online lists.
Off-the-Record Messaging (OTR)	Go	Encrypts conversations and provides security even when keys are compromised
Pidgin-Encryption	Go	Encrypts conversations using stored RSA keys
pidgin-gnome-keyring	Go	Stores account passwords in the Gnome Keyring instead of as plaintext.
Pidgin-GPG	Go	Pidgin GPG/OPENPGP (XEP-0027) Plugin
Pidgin-Paranoia	Go	Encrypts conversations using one-time pads
Pidgin-privacy-please	Go	Stop spam bots
pidgin-wincred	Go	Save passwords as windows credentials instead of as plaintext.

Once you and your friends have OTR installed, your on-line chats can be encrypted. Someone trying to monitor your encrypted IM cannot read anything you have written during the chat. Only someone with a compatible encryption key will be able to read what you have written.

Although Pidgin / Adium with the OTR plugin installed provides perhaps the best all-around security for IM, there are other options available for securing your on-line chat sessions.

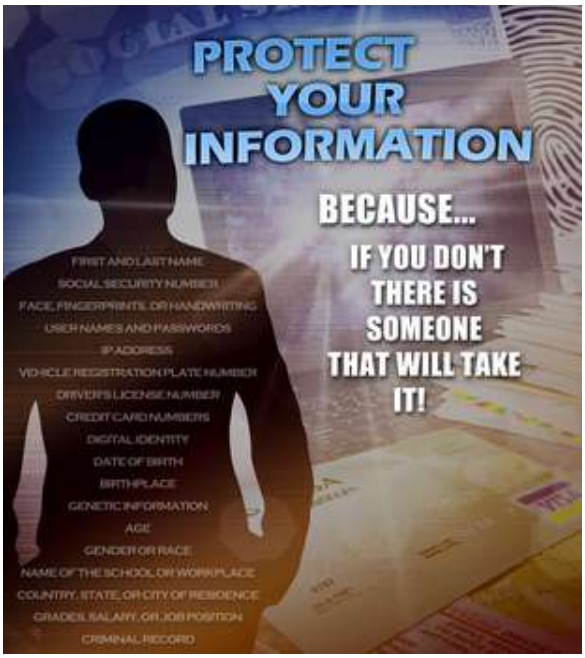
Cryptocat

Cryptocat (https://crypto.cat) is a browser plugin / add-on for Chrome, Firefox, Safari, and Opera that provides encrypted chat sessions for users based on a common conversation name. Once you have Cryptocat installed in your browser you simply choose a conversation name and a nickname (your name in the chat room) and then click the connect button. Cryptocat creates an encrypted chat session. Anyone who knows the conversation name and has Cryptocat installed in their browser can join the encrypted chat session. When the last person leaves the chat session Cryptocat deletes all record of the chat from their servers. At the time this paper was written Cryptocat was hosted on the servers at the Bahnhof Data Center in Pionen, Sweden.

Chatcrypt

Another option for secure chat is Chatcrypt (http://www.chatcrypt.com/). Chatcrypt is a web-site that creates encrypted chatrooms based on a name and password provided by the users. To use Chatcrypt you go to the Chatcrypt web-site, enter a room name, user name, and password in the fields provided and click on the "Secure Chat" button. Chatcrypt opens a chatroom, and uses AES-256 encryption (with the password as the encryption key) to secure your conversation. If anyone enters the chatroom (chooses the same room name) but does not have the correct password, all they will see is encrypted text. A WHOIS search showed that the Chatcrypt domain was registered in Budapest, Hungary.

Conclusions



There is a very real threat from cyber-criminals, stalkers, and identity thieves. The need for privacy and security in our on-line communications should not be minimized or overlooked. The tools that we use to protect our personal privacy also serve to create a more secure on-line community in general.

Pidgin/Adium with the OTR plugin, Cryptocat, and Chatcrypt all help make you a little safer on-line, and all help keep your private conversations a little more private.