Gaim.

É il servizio multi-protocollo di Intant Messaging che abbiamo scelto di installare sulle macchine del Bugslab e che consigliamo di installare anche sui vostri computer perché permette di essere configurato in modo da garantire un buon grado di sicurezza e di privacy.

Gli utenti di Gaim possono utilizzare contemporaneamente diversi account su diversi Network (ad esempio Msn sul network della Microsoft piuttosto che Jabber sul network di Autistici), ma questa versatilità presenta comunque degli aspetti secondari da valutare con attenzione.

Sottolineamo infatti che, qualora non configurato correttamente, il software farà sì che tutte le nostre comunicazioni avvengano *in chiaro* e come tutte le nostre discussioni siano potenzialmente leggibili (con una facilità estrema !) dai gestori del network che stiamo utilizzando o da chiunque riesca ad accedere al traffico tra noi e il server del network stesso (con attacchi conosciuti in ambito informatico come *sniffing* e *man in the middle* alla portata oramai di un utente tecnicamente preparato poco più della media).

Evidenziamo, inoltre, che il gestore del network è in grado di risalire, analizzando l'ip con il quale ci connettiamo, alla nostra effettiva localizzazione fisica e alla nostra identità (qualora fosse in grado di incrociare ulteriori informazioni prelevate da altri servizi che il network stesso mette a disposizione, come è il caso di Msn con MySpace piuttosto che Jabber con GoogleMail).
Fondamentale in questo senso utilizzare delle tecniche di anonimizzazione del traffico come Tor.

Una ulteriore precisazione è che alcuni protocolli che prevedono la possibilità di registrare i propri *contatti* (Msn ovvero Jabber ad esempio) permettono al server di gestione del network di costruire banalmente la rete delle nostre conoscenze, che è oggigiorno una informazione anche più preziosa della nostra effettiva identità.

Chiaramente, come al solito, ci sentiamo di consigliare l'utilizzo di reti gestite da realtà come quella di Autistici/Inventati che hanno a cuore allo stesso modo del Bugslab le tematiche di sicurezza informatica e di privacy dei propri utenti, anche se non ci stancheremo mai di dire che *per quanto ci è possibile, non dobbiamo mai demandare ad altri la tutela della nostra riservatezza.* (per approfondire questo argomento puoi cercare informazioni in rete su cosa sia successo con il caso del *crackdown di Autistici*)

Passiamo quindi a una configurazione passo-passo di un account su Gaim. Per affinità con quanto detto finora illustriamo le operazioni necessarie ad un utenza che utilizzi il protocollo Jabber sul network di Autistici, per gli altri protocolli il discorso è comunque similare.

- Selezionare la voce Accounts dalla barra principale del menu di Gaim e cliccare su Add/Edit.
- Nella finestra di gestione degli account cliccare sul pulsante Aggiungi e, nella nuova finestra che si aprirà, dovremo inserire le informazioni della nostra utenza, che nel caso di Autistici corrispondono in gran parte a quelle della casella di posta.
- Dal menu a tendina Protocollo: selezioniamo Jabber
- Nella casella di testo Screen Name: dovremo inserire il nome utente
- Nella casella di testo Server: dovremo inserire autistici.org
- Nella casella di testo Risorsa: dovremo inserire marte
- La casella di testo Password: possiamo lasciarla tranquillamente in bianco, ci verrà chiesta al momento della sincronizzazione con il server
- Nella casella di testo Alias: dovremo inserire il nome che vogliamo i nostri contatti vedranno visualizzato sul loro client

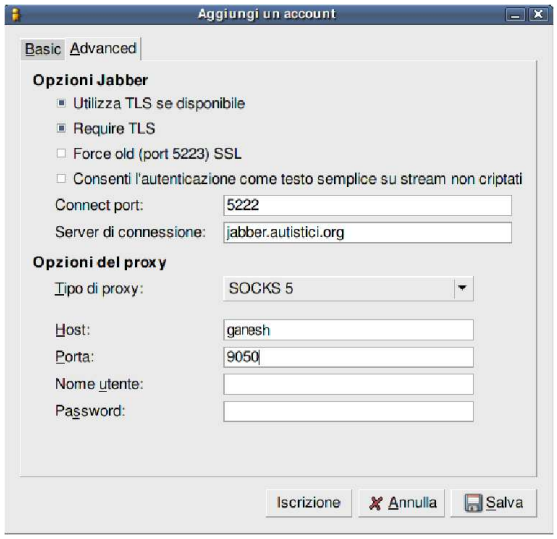
A questo punto selezioniamo la tab in alto *Advanced*

- Lasciamo selezionate le voci Utilizza e Require TLS, mantenendo invariata la porta 5222
- Come server di connessione impostiamo *jabber.autistici.org*

La sezione Opzioni del proxy ci permette di configurare Gaim in modo che utilizzi il Tor client per nascondere al server di Autistici l'ip dal quale ci stiamo connettendo.

- Come tipo di proxy selezionare SOCKS 5
- Nella casella di testo Host: inserire *ganesh*
- Come porta inseriamo la 9050 che è quella di default del Tor client

Salviamo le impostazioni.

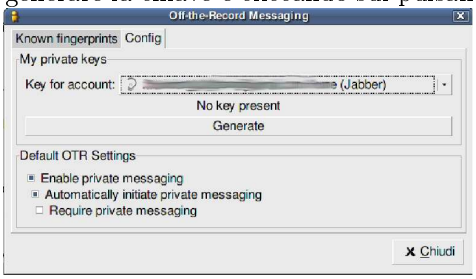


In questo modo Gaim è configurato in modo che non sia banalmente identificabile il nostro ip e la nostra connessione al server è crittata con SSL.

Non è ancora tutto. Noi vogliamo che solo la persona con la quale stiamo parlando conosca il contenuto della nostra conversazione. La nostra connessione al server è su un canale sicuro e crittato con SSL. Supponiamo che anche la connessione tra il contatto col quale stiamo parlando e il server sia su un canale sicuro e crittato con SSL. Ciò non è ancora sufficiente. Un eventuale curioso che abbia accesso al server che gestisce il protocollo (è proprio quello che è successo durante il crackdown di Autistici dove la polizia postale ha avuto accesso fisicamente alla macchina del server, e quindi a tutti i servizi che essa gestiva) avrebbe la possibilità di leggere la nostra conversazione nel momento in cui passa da un canale all'altro.
Per evitare questo tipo di attacco (detto *sniffing* del traffico), utilizziamo *OTR*, un plugin di Gaim che abbiamo installato sulle macchine del Bugslab, o che vi suggeriamo di installare qualora decidiate di usare Gaim sulla vostra macchina.

Generazione della chiave privata (questo paragrafo può essere saltato in quanto la chiave privata verrà generata automaticamente al momento necessario).

Cliccando con il tasto destro sulla tray icon di Gaim selezionare la voce Plugin dal menù a tendina. Selezionare il plugin *Off-the-Record Messaging* e cliccare sul pulsante *Configure Plugin*. Si aprirà una finestra che ci presenterà l'elenco di tutti i *fingerprint* conosciuti. Per *fingerprint* si intende una stringa di caratteri identificativa di una chiave crittografica associata ad un contatto e noi dovremmo generare la nostra selezionando la tab Config, selezionando l'account del quale vogliamo generare la chiave e cliccando sul pulsante *Generate*.



Possiamo chiudere tutte le finestre di configurazione di OTR e, avendo generato la nostra chiave, possiamo già stabile una sessione di chat crittografata con un contatto che abbia fatto altrettanto.
Cliccando con il pulsante destro del mouse su un contatto comparirà una voce che ci permette di modificare i settaggi di OTR, come ad esempio disabilitare di default la connessione privata con quel particolare contatto.

La prima volta che ci si mette in contatto con qualcunaltro che utilizza come noi OTR, apparirà una finestra informativa con la richiesta di accettare il fingerprint del nostro interlocutore. Se lo accettiamo come valido (e il nostro interlocutore farà lo stesso) la nostra conversazione avverrà su un canale

privato crittografato. Notiamo come sia presente un pulsantee ci permette di gestire la comunicazione attraverso OTR. É possibile in ogni momento passare tra una connessione in chiaro e una crittografata con OTR cliccando sul pulsante. Quando la comunicazione è in chiaro il testo sul pulsante sarà *OTR: Not private*, mentre quando sarà crittografata il testo sarà *OTR: Unverified*.

Il testo *Unverified* è indicativo del fatto che la nostra connessione sta avvenendo su un canale crittografato tra noi e il nostro contatto, ma noi non possiamo essere effettivamente sicuri che il fingerprint che abbiamo utilizzato per stabilire la connessione appartenga effettivamente al nostro interlocutore. Questo è il tipico scenario di un attacco informatico della tipologia *man in the middle* in cui un elemento invisibile si frappone fra gli utenti che stanno mantenedo la comunicazione e in questo caso invia ad entrambi i contatti che vuole spiare il proprio fingerprint fingendosi il corrispettivo interlocutore.
Se ad esempio Bob (che ha il fingerprint xxx) volesse comunicare con Alice (che ha il fingerprint zzz) ma nel mezzo si inserisse Mallory con il suo fingerprint, lo scenario schematizzato potrebbe essere il seguente :

Bob (xxx) —— (yyy) Mallory (yyy) —— (zzz) Alice

in cui Bob interloquirà con Alice convinto che il suo fingerprint sia yyy.
Ma Alice stessa sarà convinta che il fingerprint di Bob sia yyy.
In realtà il fingerprint yyy appartiene a Mallory, dunque il canale sarà crittografato tra Bob e Mallory e tra Mallory e Alice : Mallory sarà in grado di leggere l'intera conversazione.
É fondamentale in questo senso utilizzare un canale diverso da quello di Gaim che sia sicuro (come una telefonata ad esempio) per verificare che effettivamente il fingerprint che utilizziamo per instaurare la comunicazione appartenga realmente al nostro interlocutore.
Il plugin OTR mette a disposizione la possibilità di informare Gaim che il fingerprint è stato verificato correttamente, da quel momento in poi la conversazione potrà svolgersi *privatamente* (ce ne accorgiamo perchè la scritta sul bottone cambierà in *OTR: Private*. Per verificare un fingerprint clicchiamo con il tasto destro sul bottone *OTR: Unverified* e comparià un menu a tendina dal quale selezioniamo *Verify fingerprint*. La finestra che ci verrà proposta da OTR ci chiede di verificare che la parte in neretto corrisponda a quella che ci comunicherà il nostro interlocutore, mentre noi dovremo comunicare la parte scritta normalmente e il nostro interlocutore verificare che corrisponda alla sua parte scritta in neretto. Ripetiamo, è estremamente importante che questa verifica venga fatta comunicando su un canale sicuro !!
Completata la verifica selezioniamo dal menu a tendina *I have* verified ... e clicchiamo su OK. Da questo momento possiamo dialogare col nostro contatto con un pizzico di privacy in più.

Per ulteriori informazioni potete scambiare quattro chiacchiere con i ragazzi che gestiscono i servizi del Bugslab.