Stanford IM
(Instant Messaging)

Tech Briefing
September 11, 2009 – Turing Auditorium

www.stanford.edu/services/instantmessaging
What is Stanford IM?

- **Text-based Communication Tool**
  - Requested by stakeholders from across campus (and off-site) as part of the Work Anywhere initiative to allow University staff to conduct University business with their co-workers at Stanford
  - Uses SUNet ID
  - Uses SSL Encryption

- **Two supported open source instant messaging clients**
  - Adium (for Mac)
  - Pidgin (for Windows)
Benefits of Using Stanford IM

- Faster way of sharing encrypted business information
  - Clients across campus and Med School stay connected
  - Business offices that are off-campus can quickly share data
- Quick answers delivered to students
- Archive/Log your chat sessions (locally, on your computer)
  - You must install SWDE if archiving/logging chat sessions containing restricted or confidential data.
- Create Ad-Hoc Groups for multiple user conversation chats
- Centrally-funded service provided free-of-charge to the Stanford community
Encryption

A Crypto Nerd's Imagination:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Encryption

- What WILL be encrypted by the IM service:
  - the network connection between the desktop clients and the IM server
- What MAY be encrypted by the IM service:
  - the full conversation between the desktop clients (including on the server)
- What will NOT be encrypted by the IM service:
  - the logs of the conversations in the desktop clients (this is where you would need to consider SWDE)
How it works

Adium/Pidgin configured with Stanford Account

Jabber Server

encrypted

encrypted

Adium/Pidgin configured with Stanford Account
Unencrypted Session

Internet

Text transmits in the clear
What is OTR?

- Off The Record (OTR)
  - Encrypts the data on the server as well as in the “pipeline” to get to the server
  - You do not need OTR for Stanford to Stanford chats.
    - There is no logging of chat sessions on the Stanford server
    - The connection to the Stanford server is encrypted
  - The two clients involved in the chat are the only two who have a record of the content of the chat
- Stanford guarantees conversation between computer and server
- OTR guarantees conversation between the clients
- Do not use other services (e.g., Yahoo!, Gtalk, AIM) to chat about prohibited, restricted, or confidential data.
## Allowable Types of Data

### Data Classifications

<table>
<thead>
<tr>
<th>Types of Data</th>
<th>Prohibited (Not Allowed)</th>
<th>Restricted (Under Review)</th>
<th>Confidential (Allowed)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Social Security Numbers</td>
<td>Student Records</td>
<td>Fac/staff emp apps, personnel files, benefits info, salary, bdates, and contact information</td>
</tr>
<tr>
<td></td>
<td>Credit Card Numbers</td>
<td>Protected Health Information (PHI)</td>
<td>Admission apps</td>
</tr>
<tr>
<td></td>
<td>Financial Account Numbers, such as checking or investment account numbers</td>
<td>Passport and visa numbers</td>
<td>Donor info and gift amounts</td>
</tr>
<tr>
<td></td>
<td>Driver’s License Numbers</td>
<td>Research and other information covered by non-disclosure agreements</td>
<td>Privileged attorney-client communications</td>
</tr>
<tr>
<td></td>
<td>Health Insurance Policy ID Numbers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more info:  [www.stanford.edu/group/security/securecomputing/dataclass_chart.html](http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html)
Information Security Office (ISO)

- According to the ISO, at this time, the Stanford IM service is:
  - in the process of being reviewed for its security around handling restricted data.
  - only available for use with Confidential (and non-classified) data.

- Ongoing ISO requirements for a secure instant messaging service include:
  - that it not to be used to transmit prohibited data.
  - that it is limited to campus-only IP addresses (VPN in if off campus).
  - that it is limited for use with the approved clients (Adium and Pidgin).
  - that it is configured to require users to approve new buddies.
Logging of Chat Sessions

▪ No logging of chat sessions on the server
▪ Logging of chat sessions on your computer
  • Check your client’s Preferences
    • Adium—Adium Menu>Preferences>General
    • Pidgin—Buddy List>Tools>Preferences>Logging
▪ If your chat sessions are logged on your computer and contain non-public data:
  1. The log file must be encrypted. See the Data Encryption at Stanford web site to learn more
     http://www.stanford.edu/services/encryption/; and
  2. make sure that your computer is protected with a login password.
Download IM Clients

- **Download the recommended IM clients from their sites:**
  - Adium – adium.im
  - Pidgin – pidgin.im

- **These are the recommended clients because:**
  - They allow for Kerberos authentication
  - They allow for the SSL encryption
  - iChat does not meet these requirements

- **You must have an account on the service to chat with others on the same service. (i.e., Stanford, Yahoo)**
  - For Example, Stanford SUNetID to SUNetID.
  - You can not chat from your Stanford SUNetID to Yahoo IM account.
Adium—Mac Client

- Adium is a free instant messaging application for Mac OS X.
- Configure the client
  - Once downloaded follow the instructions to configure the client
    - im.stanford.edu
  - Most importantly, just remember:
    - Jabber ID = SUNetID@stanford.edu
    - No Password Required at installation
    - Security: Require SSL/TLS: checked
- You must authenticate to Kerberos.
  - Use Stanford Desktop Tools
    - ess.stanford.edu
Configure Adium

• Adium Menu>Preferences
• Click Accounts to display the Accounts window. If you are configuring Adium for the first time, select your user name and then click Edit.

• If you are configuring an existing Adium client, click the + in the lower-left corner and select Jabber.
Configure Adium

- Do **not** enter a password
- Do **not** click on Register New Account
- Click **Options**
Configure Adium

• Leave **Connect Server** blank
• Resource defaults to your computer’s name. Change if you prefer.
• Leave Port set to **5222**
• **Require SSL/TLS**
• Click **OK**

• If you are prompted to install Growl, it is a notification service that will inform you when people come on line or go off line.
• Adium developers recommend it.
Add a Group

- From the Contact Menu, select Add Group, enter group name and click Add.

Add a Contact (Business Contact) and place them into a group

- From the Contact Menu, select Add Contact.
- Jabber ID = SUNetID@stanford.edu
- Give your Contact an Alias
- Put that Contact in a Group, and click Add.
Adium – Group Chats

- Ad-hoc Group Chat
- Sessions are not logged on the server.
  - From the File Menu, select Join Group Chat.
  - Spaces are not allowed in the Chat Room Name
  - Server: conference.stanford.edu
  - List invitees as SUNetID@stanford.edu
  - Click Join.
  - Click Accept Defaults.
  - You may invite additional contacts after chat room is created.
Pidgin—Windows client

- Pidgin is a free instant messaging application for Windows users.

- You must obtain a Kerberos ticket to successfully log in to Stanford IM [www.stanford.edu/services/ess/pc/kfw.html](http://www.stanford.edu/services/ess/pc/kfw.html)

- Installation of Pidgin is simple.
  - Download the client from [www.pidgin.im](http://www.pidgin.im)
  - At the Welcome to Pidgin screen, click **Add**. In the Accounts window, click **Add** again.
    - if already installed, go to Accounts>Manage Accounts>**Add**
Configure Pidgin

• In the **Protocol** field, select **XMPP**
• In the Username field, enter your SUNetID
• Domain: **stanford.edu**
• Resource: leave blank or enter **Stanford IM**
• Leave Password field blank.
• Enter the user options of your choice
• Click **Advanced**
Configure Pidgin

- **Require SSL/TLS**
- Connect port: **5222**
- Connect server: leave blank.
- File transfer proxies: although not supported, leave as is.
- BOSH URL: leave blank
- Show Custom Smileys (optional)
- Do not check “Create this new account on the server.”
- Click **Proxy**
Configure Pidgin

- Proxy type: Use Global Proxy Settings
- Click Add.
Pidgin—Add a Group

**Add a Group**

- From the **Buddies Menu**, select **Add Group**, enter group name and click **Add**.

**Add a Buddy (Business Contact) and place them into a group**

- From the **Buddies Menu**, select **Add a Buddy**.
- Buddy’s username = **SUNetID@stanford.edu**
- Give your Contact an Alias
- Put that Contact in a Group, and click **Add**.
### Known Issues

<table>
<thead>
<tr>
<th>Known Issue</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate IM buddies may appear in the Pidgin Buddy List window. Deleting one entry may delete your own availability on that person's Buddy List window.</td>
<td>No workaround at this time. We have contacted the Pidgin developers about the problem.</td>
</tr>
<tr>
<td>Certificate warnings may appear as you sign in.</td>
<td>Accept the certificate.</td>
</tr>
<tr>
<td>Problems creating and joining permanent group chats.</td>
<td>Accept Group Chat preferences defaults.</td>
</tr>
<tr>
<td>iChat is not a supported IM client.</td>
<td>We are contacting the vendor.</td>
</tr>
<tr>
<td>On Windows, you will get an additional password prompt if you only have a WIN.STANFORD.EDU Kerberos ticket.</td>
<td>Install Stanford Desktop Tools.</td>
</tr>
<tr>
<td>If you do not have a Kerberos ticket, you will get a “500 internal server error”.</td>
<td>Obtain a Kerberos ticket by logging in to Stanford Desktop Tools or Network Identity Manager.</td>
</tr>
</tbody>
</table>
IM Etiquette

- Set your away status.
- Just because the other user didn’t set their presence (available/away) doesn’t mean they are available.
- If you don’t need an immediate response, use email.
- Always be polite.
- Keep it business related.
Keep in Mind

- Stanford IM is available to full-service SUNet IDs only
- No storage limitations
- File transfer using Stanford IM is **not supported** (or encrypted).
  - Use secure email for documents with classified data. [www.stanford.edu/services/secureemail/](http://www.stanford.edu/services/secureemail/)
- Newly activated SUNet IDs may have a lag time of 1 hour before they are active and therefore Stanford IM will not connect until the full service SUNet ID is active.
IM Tips

- To see if you are chatting with another Stanford IM user, hover over their name in the Contact/Buddy List. You should see their “@stanford.edu” address.
- When adding/requesting a contact, they will not appear active on your contact list until they accept your request.
- It is your responsibility to ensure that you are using the Stanford account when conducting business over a secure chat session.
Future Directions

- Integration with Workgroup Manager
- Web-based service
- Integration with Stanford Email and Calendar
Help and Support

- Stanford Instant Messaging Service Page
  - im.stanford.edu

- Need help with installation and/or configuration?
  - HelpSU: helpsu.stanford.edu
    - Request Category:
    - Request Type:

- Frequently Asked Questions
  - Stanford Answers: answers.stanford.edu