ChemTracker Security Overview

System Architecture
The ChemTracker client application is a commercial Java applet running in an internet browser on client workstations. This applet is unsigned and has no execution or access rights on the client workstation outside of the default “sandbox”. Java interpreted code is obfuscated such that decompilation yields nearly incomprehensible source code. Original source code is not exposed to end user nor is it available to ChemTracker development staff. Communication between the client application and the middleware tier employs a proprietary data marshalling and encryption scheme embedded in a SSL (Secure Socket Layer) protocol wrapper. The client application contains only user interface display and navigation functionality, all business logic is contained within the database layer.

The middleware tier consists of a proprietary Java application middleware / security layer (JML) operating in conjunction with a commercial “Presentation Server” (PS) executing in a Tomcat application container on Windows 2003 servers. The JML authenticates user logins, establishes user sessions, verifies user request authenticity, decodes client application requests from the PS and passes them to the database layer, and formats data returned by the database to be sent by the PS back to the client application. Communication between the PS and the JML is via direct Java object method calls as both execute in the same Tomcat Java application container. In some cases where special processing is required (structure searching, spreadsheet upload, etc.) additional Java servlets (EXternal Procedures or EXP) are used, that while not part of the JML or PS, run in the same application container. JML and EXP to Oracle database communication utilize the Oracle 10g JDBC “Thin Client” driver.

Data tier is housed in Oracle 10g Database Servers running under the Linux operating system. All ChemTracker business logic is implemented within the database layer itself as Oracle PL/sql stored procedures. Each ChemTracker member organization’s data is kept in a separate Oracle tablespace and account, with unique database usernames and passwords. Only Stanford ITS (central computing) personnel who maintain the system have access to database system administration and “root” accounts. ChemTracker development staff has access to only application level database account credentials.

Application Security Considerations
Each member organization’s ChemTracker user passwords are stored in their respective database account tables in encrypted format, using a proprietary encryption algorithm. These passwords are not “human readable” by persons having root or development level access to the database, nor can they be copied between user account records at the database level. Database level passwords are stored within the JML on the application servers.

Passwords may be retrieved by users if forgotten, by supplying either a valid account username or email address. Upon receipt of a password request, the application checks a user profile table for a matching record. If the user supplied a user name, the user name and password specified in the profile record
matching the user name is sent to the email address of that matching record. If the user supplied an email address, the user name and password specified in the profile record matching the email address is sent to the email address of that matching record. This approach prevents unauthorized discovery of a password; either the account information is sent to the rightful user, the requestor receives their own account information, or the request is denied because no matching profiles were found in the database.

User access is controlled by profiles that limit both the chemical inventory a user can view or change, and what program functionalities they may use. A user must be authorized to access both the storage location (building or building and room) and owner (PI, Lab Manager, etc.) of record for a particular inventory item in order to gain access to that item. Furthermore, a user’s ability to modify inventory items (add, edit, delete), run regulatory reports, modify buildings and rooms, create and modify chemical owners, create and modify application users, etc. is by default not allowed unless specifically granted by an “Administrative” user. To avoid uncontrolled creation of administrative users, these are only created by ChemTracker Technical Staff upon request from an organization’s approved EH&S or inventory project manager.

When a user accesses their organization’s ChemTracker link, either from the ChemTracker member’s access page or from a saved bookmark, a “Java Server Page” (JSP) based user login page is presented by the Tomcat application container hosting the PS and JML. If the user is able to successfully authenticate to the system by supplying a valid username and password, two user sessions are established within the application container, one each for the PS and JML. The session IDs for each session, along with the user’s ID and organization ID are recorded in a table in a central shared database instance (session log). Subsequent user requests are internally validated against both the PS and JML session IDs. Requests to EXPs activate a lookup of matching session IDs in the session log, and a comparison of user and organization information in the log to that contained in the current session. If the information does not match, the EXP performs no additional processing and returns no results.

**Infrastructure**

Data Storage Facility: ChemTracker data is stored in an Oracle 10g database located in a seismically secure computing facility equipped with multiply-redundant cooling and electrical systems. The data center is staffed 24x7x365 and is designed to be physically locked down in the event of a major emergency, and contains sufficient food, water, facilities and supplies to maintain staff for up to two weeks without outside support. This facility houses almost 80% of all other Stanford systems data, including Stanford’s financial and academic records, and is staffed exclusively by members of Stanford’s Information Technology Services group (ITS) and the Stanford University Department of Public Safety (police) and other security departments.

Database Servers: Housed in the above-described facility, database server configuration is Dell PowerEdge 1850, 3.6GHz CPU, 8 GB RAM, running Linux RedHat Enterprise 4 Kernel 2.4.21-37.ELSMP. For patch management and update, servers are registered with rhnsat.stanford.edu which provides “up2date” service, used to distribute patches to OS-level software and tools. Servers backed up to tape on an IBM ADSM/TSM Robot Tape Library using BMC DataTools for Oracle Backup, from 12:30 – 3:00am daily (PST). This backup contains all data and database structures required to completely rebuild the database. A “data only” export is also taken at 12:00pm daily.

Application Servers: Also housed in the above-described facility and backed up as described above. Application server configuration is Dell PowerEdge 2850, 3.20GHz CPU, 6 GB RAM.
Additional
Written requests for additional ChemTracker security information will be considered, as will recommendations for implementation of additional security measures.