213 **SISTEMA DE CONVERSAÇÕES SEGURAS NA INTERNET.** *Alejandro Olchik e Raul Weber*. (Instituto de Informática, UFRGS)

O Sistema de Conversações Seguras na Internet (SISCON) é um sistema cliente servidor totalmente escrito em Java. Este sistema permite que usuários distribuídos pela Internet utilizem seu browser para estabelecer uma conversa on-line. O sistema apresenta um esquema de segurança robusto, garantindo a autenticidade dos participantes na conversa e a sigilosidade das mensagens trocadas entre os mesmos. Antes de poder utilizar o sistema o usuário deve pedir para o administrador cadastrar o seu nome e a sua senha no servidor. Utilizando o seu browser, então, o usuário está apto a carregar a aplicação cliente. Esta aplicação cliente consiste de uma applet que é carregada automaticamente quando o usuário carrega a página HTML hospedeira. A aplicação cliente, depois de carregada, estabelece uma conexão criptografada com IDEA, utilizando uma chave de 128 bits. Para estabelecer esta chave é utilizado o algoritmo de chave pública RSA, com chave de 512 bits. Após o estabelecimento da chave o usuário fornece o seu nome e a sua senha para ser autenticado. O servidor, por sua vez, armazena um hash MD5 da senha do usuário, evitando que a informação nele contida não possa ser acessada por terceiros.