XIII Congresso 28 a 29 - setembro - 2005
Interno de Iniciação Científica da UNICAMP
Ginásio Multidisciplinar da UNICAMP

E298

**VERIFICAÇÃO FORMAL DE PROTOCOLOS CRIPTOGRÁFICOS**

Fabio Rogério Piva (Bolsista PIBIC/CNPq) e Prof. Dr. Ricardo Dahab (Orientador), Instituto de Computação - IC, UNICAMP

Com a expansão da Internet e o advento do comércio eletrônico, tornou-se necessário o desenvolvimento de novas técnicas para garantir a possibilidade de enviar e receber informação virtual de maneira segura. Os protocolos criptográficos têm por objetivo satisfazer requisitos de segurança. A verificação formal de protocolos criptográficos busca avaliar se os protocolos efetivamente satisfazem tais requisitos. Neste trabalho, foi desenvolvido um estudo sobre algumas técnicas de verificação formal, com um foco especial em métodos de prova de teoremas. Foram produzidas demonstrações nas lógicas BAN e SVO e na técnica de espaços de fitas de alguns protocolos de autenticação e estabelecimento de chaves, como Kerberos, Yahalom e Needham-Schroeder. Na etapa final do projeto foi investigada a aplicação da técnica de espaços de fitas a protocolos de trocas justas. Estes protocolos têm por objetivo permitir que dois ou mais usuários possam trocar conteúdo eletrônico sem que algum deles possa ter alguma vantagem ilegítima sobre os demais. Para verificar tais protocolos utilizando espaços de fitas, foi necessário um estudo preliminar das propriedades de trocas justas e o mapeamento destas propriedades em metateoremas de espaços de fitas.

Protocolos criptográficos - Verificação formal - Espaços de fitas