E0325

VERIFICAÇÃO DE PROTOCOLOS DE TROCAS JUSTAS UTILIZANDO O MÉTODO DE ESPAÇOS DE FITAS

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

Os protocolos criptográficos de trocas justas propõem-se a permitir que dois ou mais usuários possam trocar conteúdo eletrônico sem que algum deles possa ter nenhuma vantagem sobre os demais. O método de espaços de fitas é uma técnica de verificação formal de protocolos que baseia-se na formulação e prova de teoremas que refletem as propriedades intencionadas pelo protocolo. Adaptando o método de espaços de fitas às propriedades de trocas justas propostas por Asokan, podemos verificar a segurança provida por estes protocolos às aplicações de comércio eletrônico que os implementam. Neste trabalho introduzimos uma maneira de utilizar o método de espaços de fitas na análise de protocolos de trocas justas, bem como teoremas gerais que representam suas propriedades. Utilizando a adaptação proposta, produzimos demonstrações de dois protocolos otimistas de certificação de correio eletrônico: o protocolo FPH (Ferrer-Gomila et al. 2000) e o protocolo ZDB (Zhou et al. 1999). As demonstrações reproduziram ataques previamente documentados, bem como um ataque desconhecido até o momento.

Verificação formal - Espaços de fitas - Trocas justas