



T1457

DETERMINAÇÃO DO PERFIL DE ATAQUES A REDES DE COMPUTADORES

Michelle Marques Pfeifer (Bolsista PICJr/CNPq), Daniele Stradioto Ortolan (PICJr), Mayara Marssal Costa (PICJr) e Prof. Dr. André Franceschi de Angelis (Orientador), Faculdade de Tecnologia - FT, UNICAMP

As redes de computadores são essenciais ao mundo atual e mantê-las em bom funcionamento é um desafio permanente para administradores e estudiosos. Abordagens proativas tentam detectar problemas na rede antes da sua ocorrência, de maneira a permitir uma intervenção que justamente os impeça de se manifestar, evitando apenas ações corretivas em resposta a falhas ou degradação dos serviços das redes. Tais abordagens proativas majoritariamente baseiam-se em técnicas estatísticas e, dentre elas, o uso de cartas de Controle Estatístico de Processos (CEP). Pesquisas em andamento na FT propuseram cartas CEP sofisticadas para monitoramento de redes, tais como as de Média Móvel Exponencialmente Ponderada (MMEP). No estágio atual dos trabalhos, está em aberto calibrar a sensibilidade destes instrumentos estatísticos para detecção correta de ataques sem a geração de falsos alarmes. Este projeto, iniciado em junho/2012, visa aos primeiros esforços no sentido de determinar o perfil estatístico dos ataques mais frequentes, de forma a gerar subsídios para calibração de modelos e ferramentas de gerenciamento proativo das redes. O objetivo específico consiste em determinar a variação do comportamento estatístico da variável 'número de pacotes IP (*Internet Protocol*) trocados entre duas máquinas' na ocorrência de ataques do tipo 'negação de serviço' para calibração de cartas de controle Média Móvel Exponencialmente Ponderada.

Redes de computadores - Ataques - Detecção de intrusos