Área: *CIÊNCIA DA COMPUTAÇÃO*

Título : ***MODELO DE AGENTES MÓVEIS PARA UM SISTEMA DE DETECÇÃO DE INTRUSÃO***

Autor(es): *EMMANUELE SANABRA MORAES SILVA; RENATO BOBSIN MACHADO; FENG CHUNG WU; HUEI DIANA LEE E JOYLAN NUNES MACIEL.*

E-mail Apresentador: *emmanuele_s@yahoo.com.br*

Orientador(a): *RENATO BOBSIN MACHADO*

E-mail Orientador(a): *renato@unioeste.br*

Instituição: *LABORATÓRIO DE BIOINFORMÁTICA - LABI/ UNIOESTE - FOZ*
INSTITUTO DE TECNOLOGIA EM AUTOMAÇÃO E INFORMÁTICA - ITAI

Resumo:

A tecnologia de agentes móveis consiste em um novo paradigma de sistemas distribuídos, que envolve a migração de toda unidade de execução entre servidores, possuindo autonomia e flexibilidade para realizar tarefas, comunicar-se e acessar recursos. Neste trabalho apresenta-se um modelo para leitura, decodificação e distribuição de logs de auditoria, mecanismo de persistência e processos relativos pertencentes a um Sistema de Detecção de Intrusão (SDI). O ambiente foi desenvolvido utilizando a plataforma Grasshopper 2.2.4, que atende à padronização de agentes móveis. Esse modelo é formado por uma região, composta por uma agência de origem e por um número configurável de agências de destino. Na origem, um agente estático é responsável pela leitura e decodificação dos logs. Esse agente é configurado por um arquivo de iniciação, contendo informações relativas ao tipo de log, ao itinerário a ser percorrido e ao nome e diretório do arquivo monitorado. Esse agente monitora permanentemente o arquivo de log e ao detectar uma nova entrada, instancia um novo agente móvel com informações relativas ao itinerário e ao log decodificado. O agente móvel percorre, por meio de socket, todas as agências de destino armazenando o log no banco de dados de cada uma delas. Na primeira agência de destino, o agente móvel avalia o tipo de log. Caso seja interpretado como ataque, esse agente envia um e-mail para o administrador notificando-o e um agente móvel é criado para registrar a violação na agência de origem. O modelo implementa um sistema de backup, de modo que, na ocorrência de exceções no processo de migração, o agente armazena as informações em um banco de dados local, as quais são mantidas em todo o itinerário após o restabelecimento do serviço de comunicação. Para a otimização do sistema, avaliou-se duas técnicas de interação do agente móvel com o banco de dados das agências de destino. Na primeira, o próprio agente é responsável pela conexão e desconexão com o banco de dados enquanto na segunda, o agente móvel atribui a tarefa para um agente estático com conexão permanente. A primeira técnica apresentou melhor eficiência, validando-a para compor o processo de distribuição dos logs no sistema. A partir dos experimentos realizados em laboratório, o sistema de agentes contribuiu na persistência e distribuição dos dados, na performance, nos níveis de redundância, além de possuir componentes essenciais para um SDI, tais como: confidencialidade, distribuição e transparência.

Palavras-chave: *DISTRIBUIÇÃO DE LOGS; DETECÇÃO DE INTRUSÃO E APLICAÇÕES DE AGENTES MÓVEIS.*

Modalidade de atuação: *UNIOESTE - FOZ*