

Proposta para Dissertação de Mestrado em Engenharia Informática

Título:

Proteção Contra Ataques de Low-rate Distributed Denial of Service a Serviços Cloud

Orientador:

Mário Freire (email: mario@di.ubi.pt; página web: <http://www.di.ubi.pt/~mario/>)

Sumário

A computação na cloud inclui um ambiente de execução onde os utilizadores podem executar as suas aplicações. Contudo, o interesse na utilização destes serviços pode trazer problemas adicionais de segurança. Os ataques avançados de Distributed Denial of Service (DDoS) do tipo low-rate, que tentam imitar comportamentos de utilizadores legítimos, constituem uma das principais ameaças para aplicações neste tipo de ambientes, podendo ter um impacto significativo no negócio de uma empresa que baseie o seu negócio em serviços cloud. Nesta dissertação pretende-se desenvolver um mecanismo de proteção ao nível da camada de aplicação contra ataques avançados do tipo low rate em ambientes cloud.

Objetivos

O principal objetivo desta dissertação consiste na definição e implementação de um mecanismo de proteção ao nível da camada de aplicação contra ataques avançados do tipo low rate DDoS em ambientes de serviços cloud. O mecanismo de proteção ao nível da camada de aplicação deve incluir um método para deteção de ataques low rate baseados em entropia, o qual deverá permitir distinguir tráfego legítimo e tráfego ilegítimo, devendo o mecanismo de proteção rejeitar o tráfego identificado como ilegítimo.

Tarefas a Realizar

São propostas as seguintes tarefas para a execução do trabalho de investigação e de desenvolvimento, conducente à elaboração da dissertação de mestrado:

- Tarefa 1. Estudo dos principais conceitos subjacentes aos modelos de serviços na cloud, estudo dos principais conceitos subjacentes à deteção de ataques do tipo Distributed Denial of Service e levantamento do estado da arte na deteção de ataques avançados do tipo Distributed Denial of Service.
- Tarefa 2. Estudo e comparação dos métodos existentes para deteção de ataques do tipo low-rate e implementação de um método existente para deteção de ataques do tipo low-rate DDoS.
- Tarefa 3. Especificação e implementação da arquitetura de um mecanismo de proteção ao nível da camada de aplicação contra ataques avançados do tipo low-rate em ambientes de computação na cloud, a qual inclui o método implementado na tarefa anterior para deteção de ataques do tipo low-rate DDoS.
- Tarefa 4. Execução de testes e validação experimental do mecanismo de proteção ao nível da camada de aplicação contra ataques avançados do tipo low-rate DDoS em ambientes de computação na cloud.
- Tarefa 5. Elaboração de estudos de desempenho do mecanismo de proteção ao nível da camada de aplicação contra ataques avançados do tipo low-rate DDoS em ambientes de computação na cloud.
- Tarefa 6. Escrita de um artigo científico sobre o trabalho de investigação realizado e escrita da dissertação de mestrado.

Cronograma

A tabela seguinte representa a calendarização prevista para a execução das tarefas, em que a execução de uma dada tarefa num determinado mês é assinalada com um x.

Tarefa/mês	Set 17	Out 18	Nov 18	Dez 18	Jan 18	Fev 18	Mar 18	Abr 18	Mai 18	Jun 18
Tarefa 1	x									
Tarefa 2		x	x							
Tarefa 3			x	x						
Tarefa 4					x					
Tarefa 5						x	x			
Tarefa 6								x	x	x