Deteção de Tráfego Cifrado Gerado por Aplicações da Rede eDonkey Usando Métodos de Inspeção Profunda de Pacotes

Proposta de Projeto de Licenciatura

Orientador: Mário Freire

1. Objetivos

Os sistemas P2P (Peer-to-Peer) de partilha de ficheiros apresentarem benefícios para algumas aplicações, também podem conduzir a uma degradação da produtividade das organizações, nomeadamente, em situações em que estas aplicações afectam o desempenho de servidores, serviços ou aplicações críticas das organizações ou tarefas dependentes da rede. Nesta situação, um administrador da rede informática de uma instituição pode necessitar de impor limitações ao tráfego P2P, através da limitação da taxa de transmissão, diferenciação de serviços ou mesmo bloqueio da ligação, para assegurar um bom desempenho das aplicações da instituição, e/ou forçar regras corporativas para regulamentar a utilização de sistemas P2P. Sem a capacidade para identificar e limitar o tráfego P2P, a tomada de medidas do tipo acima referido por parte do administrador de redes pode conduzir a uma degradação do desempenho da rede, afectando todo o tipo de tráfego na rede, incluindo o das aplicações críticas das empresas. Por outro lado, a maior parte das aplicações de partilha de ficheiros entre pares permite cifrar o tráfego por elas gerado, tentando evitar a detecção do tráfego P2P. A presente proposta de projecto é dedicada ao problema da detecção de tráfego cifrado gerado por aplicações de partilha de ficheiros da rede eDonkey, recorrendo a técnicas de inspecção profunda de pacotes.

A solução a desenvolver será baseada num sistema de detecção de intrusos em rede, com regras adequadas para a detecção de tráfego cifrado gerado pelas aplicações aMule, eMule e Shareaza nas configurações com ou sem *Tracker* e com ou sem *protocol obfuscation*.

2.Tarefas

São propostas as seguintes tarefas para a execução do trabalho de investigação e de desenvolvimento subjacente ao projecto:

- Tarefa 1. Estudo dos principais conceitos subjacentes às aplicações de partilha de ficheiros entre pares;
- Tarefa 2. Estudo da classe de métodos de inspecção profunda de pacotes e respectiva aplicação para detecção de tráfego cifrado gerado por aplicações de partilha de ficheiros entre pares;
- Tarefa 3. Instalação de um testbed para detecção de tráfego gerado por aplicações de partilha de ficheiros entre pares, o qual deve incluir um sistema de detecção de intrusos em rede;
- Tarefa 4. Definição e implementação de regras para a detecção de tráfego P2P cifrado;
- Tarefa 5. Escrita do relatório de projecto.

3. 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 uma cruz (x).

Tarefa/mês	Fevereiro 2011	Março 2011	Abril 2011	Maio 2011	Junho 2011
Tarefa 1	x				
Tarefa 2		x			
Tarefa 3		x	x		
Tarefa 4			x	x	
Tarefa 5				x	x

4. Requisitos Técnicos

Domínio da língua inglesa.

5. Requisitos Académicos

Tecnologias Multimédia, Redes e Serviços Internet, Segurança Informática.

6. Grau de Dificuldade

Difícil.

7. Resultados esperados

- *Testbed* experimental para detecção de tráfego cifrado gerado por várias aplicações eDonkey.
- Relatório de projeto.

8. Contactos

Mário Freire (mario@di.ubi.pt)