DCC Deep Web

Introdução

Neste trabalho iremos desenvolver uma plataforma de *roteamento cebola*. Estas plataformas permitem que clientes se conectem a servidores sem revelar sua identidade para os servidores e para nós intermediários. Um exemplo deste tipo de aplicação é o Tor.[1]

Nossa plataforma irá permitir que vários clientes se conheçam, estabeleçam túneis para roteamento cebola, e comuniquem dados com um servidor de forma (pseudo-)anônima.[2] Imagine que dispositivos enumerados D_1, D_2, ..., D_n integram nossa plataforma de roteamento cebola. A comunicação anônima é estabelecida seguindo os seguintes passos:

1. O dispositivo D_i envia uma requisição para o dispositivo D_{i+1} para estabelecer um túnel (T1). Esta requisição estabelece a comunicação entre D_i e D_{i+1} para este túnel (T2).

2. Se D_i e D_{i+1} forem não forem os dois últimos dispositivos no túnel (T3), voltamos à etapa anterior para construir o resto do túnel (fazendo $i \leftarrow i + 1$). Se D_i e D_{i+1} forem os dois últimos dispositivos no túnel, passamos para a etapa seguinte.

3. O último dispositivo no túnel deve finalmente abrir uma conexão com o servidor para repassar os dados (T4).

Dispositivos recebem dados e repassam para o próximo dispositivo no túnel. O último dispositivo no túnel repassa os dados para o servidor. Depois de receber a resposta do servidor, o último dispositivo no túnel repassa os dados de volta no túnel até o dispositivo de origem.

Protocolo

A primeira parte do trabalho é especificar um protocolo de comunicação que os dispositivos irão utilizar para interoperar. Este protocolo será proposto e utilizado por todos os grupos. **Esta parte do trabalho vale 5 pontos e deverá ser entregue até o dia 28 de maio.**

[1] `https://www.torproject.org/`

[2] A comunicação não será totalmente segura pois não iremos criptografar os dados.

O protocolo deve especificar como as tarefas T1, T2, T3 e T4 do processo de formação de túneis e será implementado. Em particular:

T1, T3 O protocolo deve especificar o formato, a codificação, e as informações presentes numa requisição de formação de túnel. A mensagem de requisição deve conter todas as informações necessárias para decidir se um enlace é o último do túnel ou não.

T2 O protocolo deve especificar como a comunicação entre dois dispositivos no túnel é realizada (e.g., através de um soquete TCP).

T4 O protocolo deve especificar qual a conexão entre o último dispositivo do túnel e o servidor (i.e., IP do servidor, porta e tipo do protocolo).

O protocolo também deverá especificar as mensagens que os dispositivos usarão para anunciar sua participação na rede. Em particular, pelo menos quatro mensagens devem ser especificadas:

1. Mensagem de chegada na rede.
2. Mensagem de transmissão de integrantes da rede.
3. Mensagem de teste para ver se um membro ainda está presente.

Note que para as mensagens de participação, os alunos podem assumir que o computador `george.dcc.ufmg.br` sempre irá participar da rede utilizando a porta 80.

Implementação e avaliação

Este trabalho deve ser realizado em grupo de até quatro alunos. Os grupos deverão implementar o protocolo descrito acima e formar uma rede de roteamento cebola. Seu cliente deve interoperar com outros clientes (teste com clientes dos colegas), inclusive com o cliente de referência a ser implementado pelo professor. O cliente pode ser implementado em Python, C, C++ ou Java, mas deve interoperar com clientes escritos em outras linguagens.

A avaliação do código será feita através de demonstração de uma rede formada pelos programas de todos os grupos. Além disso, cada grupo deverá entregar documentação em PDF de *até* 4 páginas (duas folhas), sem capa, utilizando fonte tamanho 10, e figuras de tamanho adequado ao tamanho da fonte. A documentação deve discutir desafios, dificuldades e imprevistos de projeto, bem como as soluções adotadas para os problemas.