



Prof.^a Ana Cristina Barreiras Kochem Vendramin

Universidade Tecnológica Federal do Paraná (UTFPR), Câmpus Curitiba
Engenharia de Computação, Sistemas de Informação
Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Departamento Acadêmico de Informática (DAINF)

Avaliação (valor 2,0)

Arquitetura de Processos Pares, Comunicação em grupo e Segurança.

Siga as instruções abaixo para desenvolver e testar um sistema que permita o compartilhamento de notícias entre um grupo pequeno de usuários:

1. Considere um conjunto mínimo inicial de três processos que desejam compartilhar notícias em uma arquitetura *peer to peer* (P2P).
2. Utilize a comunicação em grupo (*multicast*) para que os processos se conheçam e troquem suas chaves públicas. O sistema deve permitir a entrada e saída de pares da rede durante o funcionamento da aplicação. Quando um novo par entrar na rede ele deverá se anunciar (*multicast*) e fornecer sua chave pública aos demais. Os demais nós enviarão a esse novo nó sua chave pública por *unicast* (valor 0,5).
3. As notícias serão enviadas por *multicast*. Ao receber uma notícia, um nó pode caracteriza-la como falsa enviando um alerta para o grupo. Crie uma forma de manter localmente uma lista com a reputação de cada nó no grupo com base nas notícias que ele enviou e nas suas verificações da veracidade das notícias (valor 1,0).
4. O sistema deve evitar que um processo mal-intencionado assuma o papel de um par escolhido, envie uma notícia falsa e prejudique a reputação do par escolhido. Empregue chaves assimétricas (chave pública e privada) para assegurar a cada par que o par escolhido é o processo que está enviando o arquivo em questão. Todo envio de arquivo deve ser criptografado com a chave privada do par que está enviando o arquivo em questão (valor 0,5).

Obs: Utilizar sockets. Qualquer linguagem de programação. É obrigatório documentar todo o código e a equipe é de dois programadores.