SGC Challenge 2020 Report

Pedro Henrique Dadalt de Queiroz

Florianópolis - 4 May 2020

Sobre o Desafio

Neste desafio foi proposto e simulado um modelo de assinaturas múltiplas. O caso específico é um onde múltiplos operadores de uma usina nuclear devem assinar digitalmente um documento para aprovar o desligamento da usina. Neste relatório será apresentado este modelo.

O Modelo

Para modelar o cenário descrito cada operador que deve assinar o documento é visto como um agente. Para simular um cenário realista, após um operador (classe **NuclearOperator**) ser construído ele deve pedir o seu *Certificado Digital* para uma *Autoridade Certificadora* (classe **AC**) confiável. A Autoridade Certificadora assina e devolve um Certificado Digital que contém informações do operador, sua chave pública e informações da Autoridade Certificadora e sua chave pública.

No modelo um operador master (classe **MasterOperator**) é responsável por buscar o arquivo a ser assinado, pedir a assinatura dos diversos operadores (o operador master incluso) e verificar as diversas assinaturas. Para isso ele utiliza de uma interface entre a estrutura de dados e as operações de assinatura e verificação a serem executadas (a classe **MultiSignRequest**). As múltiplas *Assinaturas Digitais* dos operadores são calculadas individualmente utilizando um hash criado do documento a ser assinado e suas chaves privadas. Para verificar as assinaturas basta descriptografar a assinatura com a chave pública do operador e comparar com o hash de origem. As *Assinaturas Digitais* assim criadas são armazenadas em uma lista. Por serem calculadas e armazenadas dessa maneira, não importa a ordem em que são feitas as assinaturas. Na simulação as assinaturas são realizadas de modo síncrono, mas da mesma maneira poderiam acontecer de maneira assíncrona, aonde o pedido de assinatura é enviado a todos os operadores e eles respondem em ordem aleatória e em intervalos de tempo aleatórios.

Para verificar as assinaturas basta verificar se para todos os operadores para os quais foi enviado um pedido de assinatura existe uma assinatura correspondente no documento. No código enviado esse problema (verificar todos os operadores vs assinaturas) não foi resolvido da forma mais eficiente, mas para poucos operadores não é um grande problema.