Sistemas de Elevada Confiabilidade

Highly Dependable Location Tracker

2º Semestre de 2020/2021

Grupo 15:
Francisco Silva, nº 98848
Guilherme Cardoso, nº 98495
Tiago Domingues, nº 88045

16 de abril de 2021

Design do sistema

Todas as comunicações efetuadas entre as diferentes partes do sistema são realizadas através da utilização da tecnologia de gRPC. Desta forma, foram utilizados três contratos de RPC diferentes:

- Contrato para a comunicação entre os utilizadores;
- Contrato para a comunicação entre cada utilizador e o servidor;
- Contrato para a comunicação entre o utilizador especial (*Healthcare Authority*) e o servidor.

A comunicação entre os diversos utilizadores não é confidencial e os dados das mensagens circulam em *plaintext*. Por outro lado, todas as comunicações realizadas entre os utilizadores (incluindo a *Healthcare Authority*) e o servidor são confidenciais.

Posto isto, quando um utilizador se junta ao sistema, ele interage com o servidor para gerarem uma chave simétrica que será usada para cifrar os dados transmitidos nas comunicações futuras. Para garantir confidencialidade na geração da chave simétrica, é utilizada criptografia assimétrica. Por simplicidade, assumiu-se a existência de uma infraestrutura que realiza a distribuição das chaves públicas por todos os intervenientes do sistema.

Ameaças e Garantias de integridade

Durante a implementação do sistema, foram tidas em consideração as suposições enumeradas no enunciado. Desta forma, um *byzantine user* pode tentar realizar os seguintes ataques contra o sistema e os seus utilizadores:

1. Criar uma (falsa) prova de localização em nome de outro utilizador;
2. Criar uma falsa prova da sua própria localização;
3. Obter informação do servidor acerca de outros utilizadores;
4. Ataques de *Man-in-the-Middle*;
5. Ataques de *replay* (de mensagens);

O primeiro ataque é facilmente prevenido através da utilização de criptografia. Como já foi referido, quando um utilizador se junta ao sistema, utiliza criptografia assimétrica para comunicar de forma segura com o servidor e geram uma chave simétrica que será utilizada para cifrar as comunicações seguintes. Desta forma, um atacante não conseguiria enviar uma mensagem ao servidor fazendo-se passar por outro utilizador, dado que não tem acesso à chave simétrica do mesmo. Se o atacante simplesmente usasse a sua chave simétrica para cifrar uma mensagem de prova de localização de outro utilizador, o servidor seria capaz de detetar essa ação e não o iria permitir.

Um atacante também não consegue criar uma falsa prova da sua própria localização, dado que se assume que existem sempre mais utilizadores corretos do que

utilizadores bizantinos perto de um determinado utilizador (incluindo o atacante). Por esta razão, não é possível que um grupo de atacantes crie uma falsa prova de localização. Por outro lado, um atacante também poderia tentar fazer-se passar por outro utilizador para verificar o seu próprio pedido de localização (falsa). Contudo, isto também não é possível visto que as provas de localização são assinadas digitalmente pelos utilizadores e, não tendo acesso às chaves privadas de cada um deles, o atacante não o conseguiria fazer.

Naturalmente, nenhum utilizador consegue obter informação do servidor sobre a localização de outros utilizadores durante *epochs* passados porque o servidor apenas permite que os utilizadores obtenham os seus próprios dados. Como já foi referido, o utilizador especial (*Healthcare Authority*) é a exceção a esta regra.

No que toca aos ataques de *Man-in-the-Middle*, um atacante que consiga intercetar as mensagens dos utilizadores para o servidor não consegue obter os dados nela contidos, dado que os mesmos se encontram cifrados com uma chave simétrica. Por sua vez, essa chave simétrica gerada quando o utilizador se junta ao sistema também circula cifrada com a chave pública do utilizador. Desta forma, o atacante também não consegue obter a chave simétrica porque não tem a chave privada do utilizador.

Para além disso, o *Man-in-the-Middle* também pode tentar alterar *bytes* da mensagem que intercetou. No entanto, quando a mesma chegar ao servidor, esta ação será detetada (porque o conteúdo da mensagem deixa de fazer sentido) e é retornada uma mensagem de erro para o utilizador.

Por fim, um atacante pode ainda tentar fazer *replay* de mensagens (suas ou até de outros utilizadores). Contudo, sempre que o servidor recebe um relatório de localização de um utilizador, verifica se, para aquele *epoch*, já tinha recebido alguma mensagem. Se sim, o servidor não processa o relatório e envia uma mensagem de erro para o utilizador. Desta forma, o envio de mensagens repetidas não permite alterar os dados armazenados no servidor.

Existem ainda outros acontecimentos que podem ocorrer e colocar em causa a integridade e a confiabilidade do sistema, apesar de se considerar que o servidor e os utilizadores corretos são honestos. Por exemplo, existe a possibilidade de, por algum motivo, o servidor sofrer um *crash*. Deste modo, é necessário assegurar que o servidor possa ser reiniciado com garantias de recuperação do estado em que se encontrava antes do *crash*. Ou seja, é preciso garantir que os dados armazenados pelo sistema não são perdidos nem corrompidos. Para isso, o servidor armazena em disco todos os dados acerca da localização dos utilizadores em cada *epoch*, bem como as chaves simétricas que utiliza para comunicar com cada um deles.

Para além disso, o sistema assegura não-repudiação dos relatórios e das provas de localização. Relativamente aos relatórios, esta propriedade é garantida pelo simples facto de a mensagem ser cifrada com uma chave simétrica única, à qual apenas o utilizador tem acesso. Relativamente às provas de localização, esta propriedade é garantida através de assinaturas digitais: quando um utilizador valida a localização de outro utilizador, a prova é assinada digitalmente e, consequentemente, o *proofer* não pode negar que tenha validado determinada localização.