Sistemas Distribuídos 2016/2017

2º Semestre

Relatório de Segurança

https://github.com/tecnico-distsys/T13-Komparator.git

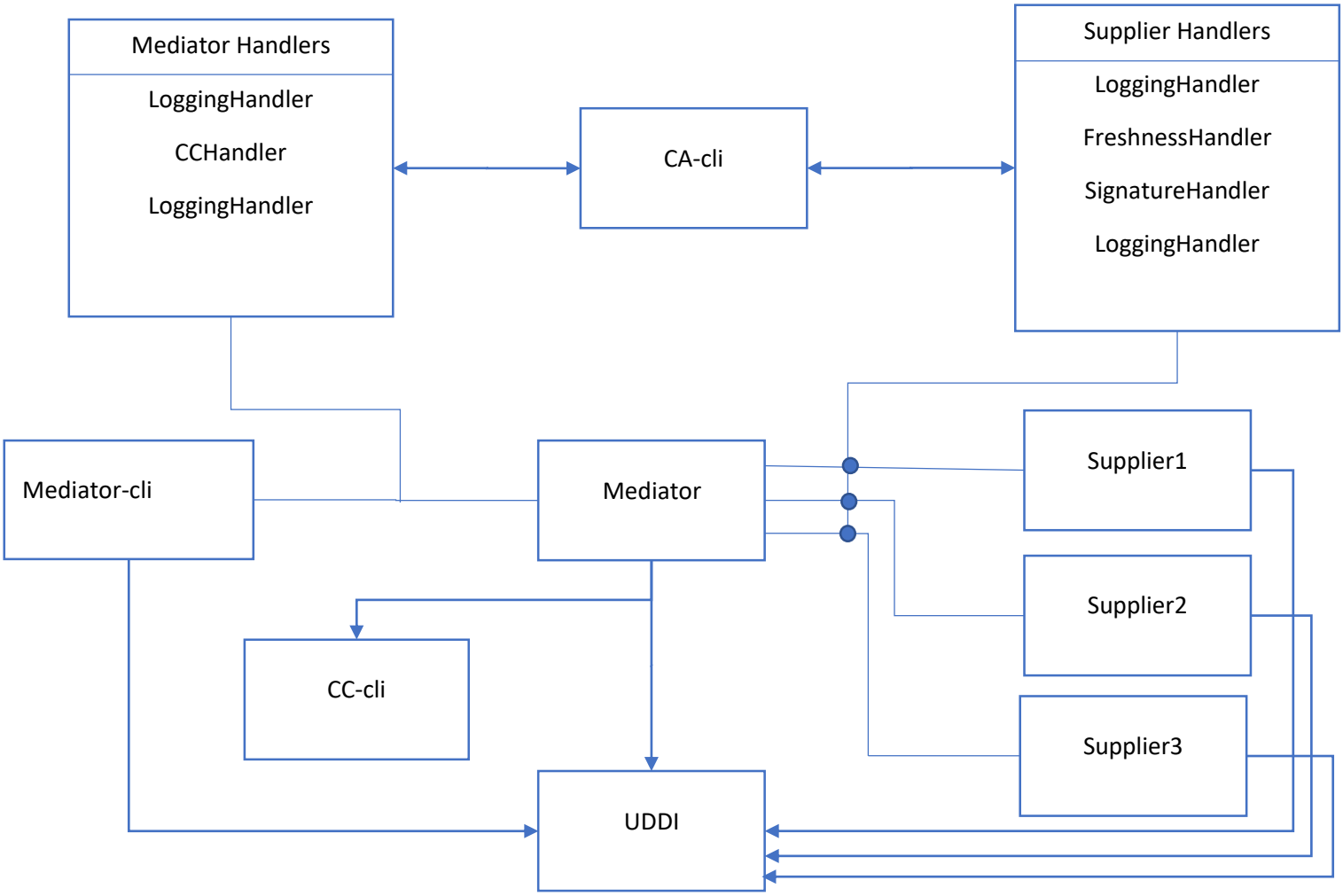
Grupo T13

52998
Rui Ferreira

63535
João Costa

65909
João Calado

Diagrama de Implementação



Descrição da Implementação

Os utilizadores interagem com a aplicação através do mediator que por sua vez interage com os vários suppliers existentes.

Ao iniciar os suppliers e o mediador, cada um faz uma chamada para o servidor de nomes UDDI de modo a registar-se para que os seus nomes sejam conhecidos na rede.

As chamadas aos métodos remotos são efectuadas por meio de mensagens SOAP.

Para evitar deturpações ou visualizações indevidas da informação trocada entre o cliente do mediador e o mediador criaram-se handlers para interceptar e proteger a informação antes de ser enviada para a rede, e para descodificar a mensagem recebida da rede à chegada.

Foi criado um handler para que no momento da compra do conteúdo de um carrinho de compras (quando é transmitido um número de cartão de crédito), esse número é cifrado e enviado ilegível pela rede. À chegada ao mediador, antes de ser entregue, o handler volta a tornar visível o seu conteúdo.

Fica ainda uma vulnerabilidade conhecida, uma vez que nao temos acesso à implementação da entidade dos cartões de crédito, codificando a informação à saída do mediador esta ficaria ilegível para o servidor da entidade dos cartões de crédito.

Entre o mediador, que implementa o cliente do supplier e os suppliers, a ideia é deixar a informação passar visível na rede, mas com a garantia que chegou ao outro lado sem ser alterada. Caso se detectem alterações, a mensagem é descartada. Assim, há um handler à saída que gera um timestamp e um token NONCE. Um outro handler faz um resumo do conjunto “mensagem + timestamp + token”, assina com a chave privada do mediador, coloca o resumo assinado no cabeçalho da mensagem SOAP e envia para a rede. À chegada ao servidor é verificada a assinatura com a chave pública do mediador, extraindo o resumo. A fim de comparar a integridade, cifra-se o resumo do conjunto “mensagem + timestamp + token”, com a chave pública do mediador e deve ser igual ao conteúdo do resumo decifrado à chegada.

Os tokens são guardados quando a mensagem chega ao receptor. Se o token for repetido, ou a assinatura for inválida, ou a data tiver uma diferença superior a 3 segundos da data atual, a mensagem é rejeitada.

Ataques

Entre o emissor e o receptor do mediador, pode ocorrer "replayattack", uma vez que não estamos a garantir a frescura das mensagens transacionadas.

O ataque "man-in-the-middle" foi tido em consideração uma vez que as chaves públicas são pedidas à CA, e é comparada a chave pública da CA com a chave pública guardada no módulo de segurança da aplicação. Caso alguem se tente passar pela CA, tem que ter uma chave privada compatível com a chave pública local.