Segurança de Redes e Sistemas de Computadores 2017/2018
Trabalho Prático nº 2 (v1.0), 15/Maio/2018)

Background do TP2 e indicações iniciais sobre entrega

Referências iniciais a ter em conta:
SRSC-TP2 Background (bem como materiais e referencias constantes neste documento).
Apresentação TP2-Initial-Overview.ppt (apresentação em aula prática)

A - Contexto e *background* inicial do trabalho TP2

Este trabalho será realizado em grupo, podendo integrar até quatro participantes. Assim, a partir dos grupos inicialmente registados podem opcionalmente juntar-se em equipas maiores (2+2 ou 3+1), de modo a poderem beneficiar de maior capacidade de implementação e massa crítica para implementarem uma melhor solução em extensão e sobretudo em qualidade.

A implementação do trabalho fará uso do conhecimento prático sobre programação com técnicas, métodos e algoritmos criptográficos (com suporte em JAVA / JCE), explicados, demonstrados ou clarificados nas aulas práticas (ver o material nas aulas práticas – pacotes *lab*) e tendo em vista as construções criptográficas requeridas para a concepção e realização da plataforma, usando nomeadamente:

- Algoritmos criptográficos simétricos: implementação com o suporte Java/JCE
- Algoritmos de sínteses de segurança (*secure hashing*): implementação com o suporte Java/JCE
- Algoritmos criptográficos assimétricos: implementação com o suporte Java/JCE
- Assinaturas digitais de chave pública: implementação com o suporte Java/JCE
- Certificados de chave pública: implementação com o suporte Java/JCE e ferramentas auxiliares associadas
- Estabelecimento de segredos (ou chaves) criptográficas com base num acordo Diffie-Hellman: implementação com o suporte Java/JCE
- Comunicação baseada em TLS e respetivas parametrizações de detalhe de *endpoints* TLS (implementação com base em Sockets TLS e suporte de programação Java JSSE ou, alternativamente, invocações REST/TLS).

Para preparação inicial da plataforma (cuja arquitetura de referência se encontra apresentada no documento TP2-Initial-Overview.ppt), os grupos deverão proceder à montagem do ambiente de desenvolvimento e *deployment*), pelo que deverão ser tidos em conta:

- A clarificação da arquitetura geral de referencia da plataforma (conforme introduzida e discutida em aula prática), de acordo com apresentação disponibilizadas no documento TP2-Initial-Overview.ppt.
- Os materiais e componentes para montagem da plataforma incial, conforme descrito no material das aulas práticas (ver TP2 em asc.di.fct.unl.pt/~hj/srsc/aulas-praticas).

Assim, o primeiro passo para realização do trabalho será proceder a montagem da arquitetura de referencia, a partir do *background* das aulas e das anteriores linhas de orientação. A partir dos materiais disponibilizados, cada grupo deverá discutir e clarificar (entre o grupo e com o docente) as opções de implementação, de acordo com o quadro de referencia genérico nas seguintes secções deste enunciado.

Desenvolvimento do trabalho após SETUP dos componentes da platafora

Após a preparação da plataforma inicial far-se-ão os seguintes desenvolvimentos do trabalho, de acordo com os requisitos indicados. Cada grupo e os respetivos membros podem e devem organizar-se de acordo com a metodologia de desenvolvimento e o escalonamento de atividades de desenvolvimento que considerem melhor para o seu caso, tendo em conta os prazos para finalização e entrega do trabalho. A clarificação ou a especificação de detalhe da implementação, a partir do quadro de referencia do presente enunciado, deverá ser encetada por cada grupo, tendo em conta a sua implementação concreta.

Assim, o refinamento de detalhe ou as opções específicas de implementação por parte de cada grupo, a partir

do quadro de referencia do presente enunciado, será um factor de avaliação. Os grupos podem e devem discutir as suas opções e hipóteses de trabalho com o docente. Deste modo poderão validar as suas opções complementares ou as suas soluções específicas de implementação. Propositadamente as especificações de referência do trabalho deixam vários aspectos em aberto para que os grupos possam conceber e implementar soluções específicas, por si concebidas a partir dos requisitos iniciais.

B - Entrega e submissão do trabalho

Data de entrega:
O trabalho poderá ser entregue a partir de 6/JUNHO/2018 e com data-limite de entrega em 12/JUNHO/2018.

Sugere-se que os grupos organizem as agendas de trabalho de modo a conciliarem essa agenda de forma a atenderem a data de entrega que for mais favorável aos elementos de cada grupo.

Materiais a entregar. Os alunos receberão oportunamente (via CLIP) indicações específicas complementares para entrega do trabalho. Resumidamente, como rindicação inicial, a entrega envolverá os seguintes elementos:

- O projeto do TP2 com os componentes de implementação deverá estar num repositório GITHUB ou BITBUCKET na data de entrega. Na entrega do trabalho os alunos deverão submeter o URL para clonagem e inspeção a partir do respetivo URL do projeto indicado na mensagem de entrega. No momento da clonagem serão verificadas as datas de modificação do repositório, pelo que o seu conteúdo não pode ser alterado depois de 12/Junho/2017. Para partilha com o docente devem ser usados os seguintes identificadores:
    - hj@fct.unl.pt no caso do GitHub
    - henriquejoaolopesdomingos no caso do BitBucket

- Os alunos deverão incluir no repositório uma diretoria (docs) contendo o relatório do trabalho (designado por TP2-REPORT.pdf). O *template* de referência para este relatório será disponibilizado no sistema CLIP oportunamente, sendo comunicado aos alunos.
- No repositório do projeto, deverá ainda ser incluída toda a informação (README) como todas as indicações relevantes para inspeção, correção ou teste do trabalho.
- A entrega far-se-á assim com um simples envio (entre 6/Junho e 12/Junho) de uma mensagem de correio electrónico para o endereço hj@fct.unl.pt, identificando o grupo e seus elementos bem como o URL para efeitos de acesso e clonagem do repositório. Nesta mensagem o grupo deverá estar corretamente identificado e o URL deverá estar corretamente indicado e acessível para o efeito, sob pena de não ser o trabalho considerado entregue.
- De forma semelhante à entrega do trabalho prático nº 1, na realização do teste nº 2, os alunos serão chamados a indicar ainda o URL do projeto do grupo (na folha de respostas do teste). Assim, os alunos deverão fazer-se acompanhar do referido URL (correto para acessibilidade ao repositório do projeto) no momento de realização do teste 2.

Após análise das implementações e respetivo *reporting*, podem haver trabalhos e grupos selecionados para discussão/demonstração. Neste caso isso será comunicado aos grupos em causa para efeito de agendamento de datas de discussão e demonstração, o que será combinado grupo a grupo.