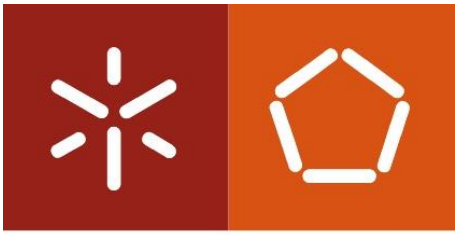

Universidade do Minho

Departamento de Informática

Mestrado em Engenharia Informática

Criptografia e Segurança de Informação

Engenharia de Segurança
Projeto de Desenvolvimento 2 - Utilização/integração de ferramentas disponibilizadas no âmbito do Digital Signature Services (DSS)

Grupo Nº 3

Ariana Lousada (PG47034) Luís Carneiro (PG46541)
Rui Cardoso (PG42849)

20 de junho de 2022

Resumo

O presente documento descreve sucintamente os objetos de avaliação e de análise ao longo do segundo projeto de desenvolvimento inserido na unidade curricular Engenharia de Segurança, pertencente ao perfil de Criptografia e Segurança da Informação inserido no Mestrado em Engenharia Informática da Universidade do Minho. O presente projeto teve como principal objetivo a utilização/integração de ferramentas disponibilizadas no âmbito do Digital Signature Services (DSS).

Conteúdo

Capítulo 1

Alterações efetuadas

1.1 Transpor as alterações efetuadas para a nova versão

De modo a transpor as alterações efetuadas para a nova versão, a versão mais recente do repositório foi obtida através do seu repositório no GitHub. De seguida, os *commits* do projeto do ano passado foram percorridos um a um (através do link https://github.com/uminho-miei-engseg-20-21/Grupo3/commits/) e o código correspondente inserido no projeto atual.

A razão pela qual não poderíamos simplesmente fazer "copy paste"dos ficheiros do projeto do ano passado é simples - se entretanto esses ficheiros tivessem sido modificados, essas alterações perdiam-se, pelo que fomos "obrigados"a proceder desta forma.

Reparamos ainda que apenas as três pastas da dss-demonstrations atualmente presentes na nossa entrega (dss-demo-bundle, dss-demo-webapp e dss-mock-tsa) são precisas para compilar e executar a versão web desta ferramenta, pelo que as restantes foram apagadas. Adicionalmente, a meio da realização deste projeto foi preciso alterar a versão de certos ficheiros de 5.10.1 para a 5.10 devido a estes terem sido apagados no repositório DSS.

1.2 Adicionar interface de autenticação inicial

Para este ponto não é preciso apenas acrescentar a interface em si, é também preciso intercetar os pedidos de forma a que o utilizador tenha de estar "logged in"para aceder às páginas oferecidas pelo serviço. Caso contrário, a autenticação seria inútil. Para este propósito, foi utilizado o Spring Security, juntamente com uma base de dados *in-memory*, de forma a validar a implementação (da interceção e do processo de autenticação e logout em si).

Em suma, enquanto que o utilizador não está autenticado e tenta aceder a uma página qualquer, este é redirecionado para uma página simples de login, onde insere o seu *username* e *password*. Depois de estar autenticado, pode navegar sem restrições pelo serviço. Para fazer logout, basta clicar no botão correspondente que aparece no fundo de todas as páginas que visita. Foi ainda implementado uma página de registo, onde o utilizador indica um *username* e *password* para (caso estes sejam válidos) de seguida se poder autenticar. Ambos estes campos são validados, isto é, o *username* tem 5 a 20 carateres e a *password* tem 8 a 25 carateres, com pelo menos uma letra e um número.

Como seria de esperar, a *password* é guardada cifrada, neste caso com o algoritmo bcrypt.

1.3 Adicionar área de utilizador

Tal como o enunciado indica, é necessário implementar uma base de dados para poder guardar o número de telemóvel inserido pelo utilizador, assim como o apresentar quando este acede à sua área de utilizador.

Foi utilizado a base de dados MySQL com uma tabela "accounts", que guarda o *username*, *password* e número de telemóvel de cada utilizador. Naturalmente, este último campo está vazio quando o utilizador se regista.

Quando o utilizador visita a sua área de utilizador, o número de telemóvel é buscado à base de dados e, se existir, é apresentado no ecrã. Depois, é possível inserir um novo número para ser guardado na base de dados.

O número de telemóvel tem de ter o indicativo do país (por exemplo, +351), um espaço opcional e o número em si (9 dígitos).

1.4 Utilização do número de telemóvel guardado na área do utilizador

Para este requisito foi preciso alterar o código no controlador do formulário apresentado quando o utilizador quer efetuar uma operação com a sua Chave Móvel Digital.

Antes deste ser apresentado, o número de telemóvel é buscado à base de dados, tal como é feito no ponto anterior.

Falta ainda alterar o JavaScript, pois este por defeito escreve o "+ 351"no campo do formulário correspondente se não tiver nenhum número guardado na *Local Storage*. A única alteração foi que o JavaScript apenas escreve esse texto por defeito caso o número não tenha sido definido pelo controlador (ou seja, caso o utilizador ainda não o tenha definido na sua área de utilizador).

Apêndice A

SAMM (Software Assurance Maturity Model)

A.1 Pergunta 2.1

Identifique a maturidade de três práticas de segurança (à sua escolha) que utiliza

Foram escolhidas as práticas de segurança cuja pontuação de maturidade atual seja a menor e, como tal, precisem mais urgentemente de serem melhoradas, ou seja, a *Governance*, *Construction* e *Verification*. A pontuação é, respetivamente, 1.24, 1.24 e 1.39.

A.2 Pergunta 2.2

Para cada uma das práticas de segurança identificadas na pergunta anterior, estabeleça o objetivo para a mesma (Fase Set the Target do SAMM), i.e., o nível de maturidade pretendido;

O objetivo será chegar à pontuação de 1.5 para cada prática de segurança mencionada (isto é, da *Governance*, *Construction* e *Verification*).

A.3 Pergunta 2.3

Desenvolva o plano para atingir o nível de maturidade pretendido

O plano, que pode ser visto em mais detalhe no ficheiro excel e PDF anexado, consiste em definir passos incrementais em cada fase, de modo a dividir o trabalho ao máximo e chegar ao objetivo pretendido.

Para a prática de segurança da *Governance*, isto traduziu-se na melhoria de 2 atividades nas duas primeiras fases, e na melhoria de 1 atividade por fase nas últimas duas fases, de modo a atingir uma pontuação final de cerca de 1.51.

Para a *Construction* melhoraram-se, respetivamente, uma, duas, uma e duas atividades em cada fase, com a pontuação final de 1.52.

Finalmente, para a *Verification* foram melhoradas uma atividade por fase durante as três primeiras fases, com a pontuação final de 1.51.

Apêndice B

RGPD (Regulamento Geral de Proteção de Dados)

B.1 Pergunta P1.1

O ARTICLE 29 DATA PROTECTION WORKING PARTY publicou o Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 em que indica os nove critérios que devem ser considerados para avaliar se o processamento de dados pessoais irá resultar num risco elevado, devendo ser efetuado um DPIA sempre que o processamento satisfizer dois desses critérios.

1. Identifique os nove critérios.

Os nove critérios são aplicados caso os dados:

- forem utilizados para avaliar, caraterizar ou prever o utilizador, especialmente sobre aspetos do seu desempenho no trabalho, situação económica, saúde, preferências pessoais ou interesses, fiabilidade ou comportamento, localização ou movimentos;
- forem utilizados para efetuar uma tomada de decisão automática, com consequências legais ou semelhantes (por exemplo que levem à exclusão ou discriminação de certos indivíduos);
- sejam o resultado de uma monitorização sistemática do(s) sujeito(s), pois os sujeitos podem não saber quem a faz nem para que é feita;
- contenham dados sensíveis ou de natureza altamente pessoal (por exemplo qual a opinião pessoal política do sujeito);
- sejam processados numa grande escala (que apesar de subjetiva, pode ser melhor classificada através do número de sujeitos envolvidos, do seu volume ou da sua duração ou permanência);
- sejam utilizados para corresponder ou serem combinados com *datasets* existentes;
- se apliquem a sujeitos vulneráveis (por exemplo crianças, visto que por norma não têm consciência nem consentem que os seus dados sejam processados);
- sejam utilizados de uma forma nunca antes vista em soluções tecnológicas ou organizacionais novas, já que este novo uso pode acarretar novas formas de coleção de dados com um risco maior de infringir os direitos e liberdades pessoais dos indivíduos;
- e o seu respetivo processamento previnam os sujeitos de exercer um direito ou usar um serviço ou contrato.

2. Verifique como é que o PD2 (projeto de desenvolvimento 2, no âmbito da avaliação prática 2) que está a efetuar para esta UC se enquadra nesses nove critérios.

Achamos que nenhum destes critérios se aplicam à versão online do PD2, visto que tal como a demonstração online indica (em https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/home), nenhum dos ficheiros submetidos é guardado (e a submissão dos ficheiros é da única responsabilidade do utilizador). Ou seja, como não é guardada nenhuma informação, não pode ser extraída qualquer informação ou dados.

Já para o PD2 em si, o *username*, a *password* (cifrada) e número de telemóvel são guardados na base de dados. No entanto, não consideramos o número de telemóvel como dado sensível, já que nesta categoria estão incluídas opiniões políticas ou os dados médicos do sujeito, e, comparativamente, o número de telemóvel parece-nos bastante mais banal. De qualquer maneira, é recomendado que o utilizador não submeta dados sensíveis.

B.2 Pergunta P1.2

O CNIL (Commission Nationale de l'Informatique et des Libertés) disponibilizou uma ferramenta open-source para ajudar no Data Protection Impact Assessment (DPIA) em https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

1. Instale a ferramenta (disponível para Linux, Windows e MacOS) que se encontra em https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

2. Utilize a ferramenta para o DPIA do seu PD2 (projeto de desenvolvimento 2, no âmbito da avaliação prática 2), preenchendo sucintamente (pode preencher em português) todas as componentes pedidas, indicando como o seu projeto responde aos vários requisitos.

3. No final do preenchimento e validação, vá ao dashboard e escolha a apresentação em lista, selecione "Display PIA"e imprima para ficheiro PDF.

O ficheiro PDF pode ser consultado no ficheiro de entrega do trabalho prático.