FACULDADE ENGENHARIA
Departamento de Informática

Sistema de Autenticação com Recurso a Meio Físico e Utilizando *Zero-Knowledge Proof*

Proposta de Projeto

Orientador: Bernardo Sequeiros (jbfs@ubi.pt)
Coorientador: Pedro Inácio (inacio@di.ubi.pt)

Objetivos

A autenticação com recurso a uma palavra-passe remonta a milénios passados, sendo ainda hoje o método mais comum para autenticação que utilizamos no dia-a-dia. O factor *something you know* permite a alguém autenticar-se perante outra entidade, que tem em si guardada esse mesmo factor. No entanto, as palavras-passe são hoje um ponto comum de falha por parte dos utilizadores. A utilização repetida destas, em diferentes serviços, ou a utilização de palavras-passe simples de adivinhar, para facilitar a memorização destas, levam a que sejam plenamente exploradas como vector de ataque em múltiplos sistemas. Mais recentemente, os protocolos criptográficos *zero-knowledge*, que permitem provar a uma outra entidade algo, sem que para isso seja necessário revelar algo mais do que a prova em si, ou seja, é feita a prova sem revelar qualquer informação ou aspeto desta, têm ganho relevância como mecanismos alternativos de autenticação, ao removerem da equação a necessidade de um dado factor estar presente de ambos os lados, de quem se tenta autenticar, e de quem verifica a autenticação

Este projecto tem como objectivo o desenvolvimento de um mecanismo de autenticação utilizando *zero-knowledge proofs*, que irá incorporar uma variável física (um factor *something you own*) como factor de autenticação que permitirá a realização da prova. O mecanismo desenvolvido deve garantir as três propriedades essenciais destes mecanismos, completude, solidez e zero conhecimento, e deve permitir a autenticação, sem que do lado do validador seja armazenada qualquer informação relevante para o processo de autenticação do utilizador. Deve ser demonstrada a funcionalidade do mecanismo com uma implementação prototipada numa aplicação para este efeito.

Dada a natureza deste projeto, requerem-se conhecimentos sólidos principalmente em Programação, Programação Orientada a Objetos, Segurança Informática. O(a) estudante terá assim a oportunidade de solidificar os seus conhecimentos nas várias áreas abrangidas por este projeto.

Requisitos Técnicos / Académicos

Conhecimentos sólidos principalmente em Programação, Programação Orientada a Objetos, Segurança Informática.

Tarefas a Realizar e Cronologia

Segue-se uma planificação preliminar do projeto em termos de tarefas e sua duração:

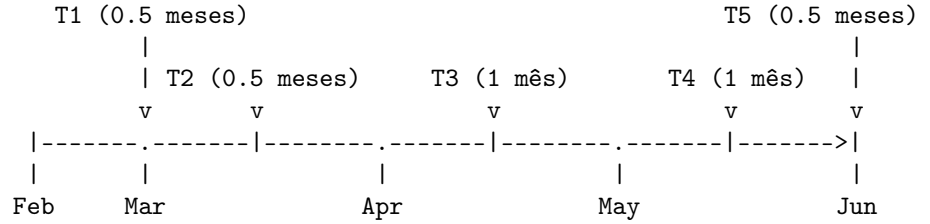
T1 Contextualização com os objetivos propostos; preparação do ambiente de trabalho, e seleção e familiarização com as tecnologias a utilizar (0,5 meses);

T2 Desenvolvimento do primeiro protótipo e das principais funcionalidades da aplicação (0,5 meses);

T3 Desenvolvimento de funcionalidades mais avançadas. Testes pontuais (1 mês);

T4 Finalização da aplicação. Testes e aprimoramento (1 mês);

T5 Escrita do relatório de projeto (0,5 meses) [1].



Elementos de Avaliação a Entregar

Para além do relatório, o(a) estudante deverá entregar todo o código e elementos associados relativos à aplicação.

Resultados Esperados

Os principais resultados esperados para este projeto são:

* Aplicação;
* documentação da aplicação;
* 1 relatório de projeto [1, 2].

Referências Bibliográficas

[1] C. Collberg and S. Kobourov, "Self-plagiarism in Computer Science," Communications of the ACM, 48(4): 88 - 94, 2005.

[2] Universidade da Beira Interior, "Código de Integridade da UBI," Julho, 2018. [Available online: `https://www.ubi.pt/Ficheiros/Entidades/91363/codigo_integridade.pdf`.]