Projeto - Sistema de Leilões

Universidade de Aveiro
Segurança Informática nas Organizações
2018/2019

84793 Daniel Nunes
84921 Rafael Direito

Proteção (Encriptação, Autenticação e Integridade) das Mensagens Trocadas

- **JSON**
- **Cifras Híbridas** (Certificado + AES-CCM) - Cliente - Repositório
- **TLS com Autenticação Mútua** - Repositório - Leiloeiro

84793 Daniel Nunes | 84921 Rafael Direito

Proteção das *Bids* até ao Fim do Leilão

- **Cifra Híbrida**
- **Chave Pública RSA** criada pelo criador do leilão
- **Chave Simétrica** (AES-CCM) criada pelo leiloeiro

84793 Daniel Nunes | 84921 Rafael Direito

Identificação do Autor de cada *Bid* com o Cartão de Cidadão

- Cliente **assina** cada *bid* que envia com o cartão de cidadão

- Cliente cifra o seu **certificado** e coloca-o no Bloco que contém a *bid* - permite verificar a autenticidade do autor de uma *bid*

84793 Daniel Nunes | 84921 Rafael Direito

Validação das *Bids* com Recurso a Código Dinâmico

84793 Daniel Nunes | 84921 Rafael Direito

- Cliente cria um **ficheiro python** no seu diretório
- Conteúdo do ficheiro é enviado e **reconstruído** no leiloeiro
- Utilização do comando **exec(...)** para executar o código enviado

Modificação das *Bids* com Recurso a Código Dinâmico

- Após validação do leiloeiro
- Mesmo mecanismo explicado anteriormente
- Pode ser usada para manipular a dificuldade do *cryptopuzzle* enviado a cada cliente

84793 Daniel Nunes | 84921 Rafael Direito

Construção da *Blockchain* Associada a um Leilão

- Conjunto de blocos ligados entre si
- Permite verificar a autenticidade, validade e integridade de cada *bid* (bloco na cadeia)
- Um cliente pode verificar a integridade desta a qualquer momento
- Deteta se qualquer bloco foi alterado após as sua inserção na cadeia

84793 Daniel Nunes | 84921 Rafael Direito

Deployment dos *Cryptopuzzles*

- **Desafio** enviado para o cliente, pelo servidor

- Cliente necessita de **calcular uma solução do puzzle** com base num *nonce random* e enviá-la ao repositório (coloca-a no bloco que recebeu)

- Repositório valida a solução que, se for correta, leva a que bloco seja inserido na *blockchain* associada ao leilão.

84793 Daniel Nunes | 84921 Rafael Direito

Validação de um Leilão Fechado

84793 Daniel Nunes | 84921 Rafael Direito

No final do leilão, cada utilizador poderá validar:

- **Autenticidade de cada bid** - através das assinaturas
- Soluções dos **cryptopuzzles**
- **Ordem das bids**

Extras

- **Autenticação de 2 fatores** - Utilização de uma *OTP*
- **TLS com autenticação mútua** entre o repositório e o leiloeiro.
- **Encriptação de ficheiros** - com recurso ao 7zip
- **Leilões** guardados em **disco** - com recurso à biblioteca *pickle*
- **Leilão *single bid***

84793 Daniel Nunes | 84921 Rafael Direito

Questões ?