Universidade de Brasília – UnB

Departamento de Ciência da Computação - CIC

Disciplina: Segurança Computacional – 2025/1

Professora: Lorena Borges

Seminário

O seminário é uma atividade avaliativa que tem por objetivo verificar a capacidade do aluno em estudar um assunto, relacionado ao tema de segurança computacional e algoritmos criptográficos. Ao final, será realizada a apresentação em sala de aula dos projetos desenvolvidos e análises do relatório.

O seminário englobará como tarefas:

- O desenvolvimento de um projeto com codificação para entrega de um sistema que aborde os temas sugeridos neste roteiro ou outro tema sugerido pelos alunos, mediante aprovação do docente.
- Apresentação em sala de aula pelo grupo (máximo de três integrantes) dos resultados obtidos, com demonstração dos programas codificados.

Temas do Seminário

1. **Sistema de Assinatura e Verificação de Documentos Digitais:** Desenvolvimento de uma aplicação desktop ou web onde os usuários possam carregar um arquivo (PDF, TXT, DOCX) e gerar uma assinatura digital, permitindo que terceiros façam a verificação da autenticidade e integridade do documento.
2. **API Segura com Autenticação de Mensagens:** Criação de uma API RESTful onde cada requisição sensível (ex.: envio de dados confidenciais, pagamentos, comandos críticos) inclui uma assinatura digital da carga (payload).
3. **Sistema de Mensageria Segura com Assinatura:** Aplicativo de troca de mensagens (CLI ou web) onde cada mensagem enviada inclui uma assinatura digital do conteúdo e o receptor verifica a integridade e autenticidade da mensagem.
4. **Blockchain Privado com Validação de Transações via Assinatura:** Desenvolvimento de uma blockchain simplificada, onde cada transação é assinada digitalmente pelo remetente e os nós da rede verificam a validade da assinatura antes de incluir no bloco.
5. **Sistema de Votação Digital Seguro:** Plataforma de votação onde cada voto é assinado digitalmente pelo eleitor com sua chave privada. A apuração verifica as assinaturas antes de contabilizar os votos.

Composição dos Grupos

Será possível fazer o **trabalho em trio**. Os grupos e os temas escolhidos deverão ser postados no respectivo fórum no Aprender. O mesmo tema só poderá ser escolhido por no máximo quatro grupos. As datas previstas serão nos dias: **07/07, 09/07, 14/07 e 16/07.**

Cada grupo terá 15 minutos para realizar a apresentação, em formato de slides. O tempo de apresentação é reduzido, por isso, será avaliada a capacidade de síntese e apresentação geral.

Avaliação

A avaliação do seminário será composta por duas etapas: material a ser entregue e a apresentação em sala de aula.

Os alunos poderão utilizar os algoritmos de assinatura digital desenvolvidos no TP3 ou outros algoritmos criptográficos, de maneira complementar, para aumentar a qualidade e segurança das soluções.

Material Entregue – Além dos slides utilizados na apresentação, deverá ser entregue um relatório em PDF, apresentando e analisando em mais detalhes o tema escolhido. Deverá constar no relatório os nomes dos integrantes do grupo, com a devida formatação, em um máximo de 10 páginas. Apenas um integrante do grupo precisa enviar a entrega do trabalho.