SEGURANÇA EM REDES E COMPUTADORES | 21181

Período de Realização

Decorre de 2 de novembro a 27 de novembro de 2023

Data de Limite de Entrega

27 de novembro de 2023, até às 23:59 de Portugal Continental

Temática / Tema / Conteúdos

Métodos criptográficos para a comunicação de informação.

Objetivos

Deve demonstrar:

- Conhecer e compreender as diferentes técnicas criptográficas;
- Saber aplicar os princípios fundamentais da criptografia a sistemas de comunicação Internet;
- Demonstrar ter o conhecimento para desenhar uma solução de segurança para um serviço, por forma a implementar um conjunto de requisitos de segurança.

Trabalho a desenvolver

Considere um sistema centralizado de controlo de versões, ilustrado na Fig. 1. Este tipo de sistema é comummente utilizado no suporte à gestão de informação centralizada de grupos de trabalho, por exemplo: gestão central documental ou do código desenvolvimento por programadores, numa empresa. Neste tipo de sistema, os vários utilizadores identificam-se perante o serviço central (repositório ou base de dados) e sincronizam a sua informação com a disponível na base de dados do serviço. Tal como ilustra a figura, as operações de commit permitem enviar alterações para a base de dados, ao passo que as operações de update permitem receber atualizações do servidor. Desta forma, os vários utilizadores do sistema de controlo de versões podem sincronizar, a qualquer instante, a informação partilhada, com recurso ao serviço.

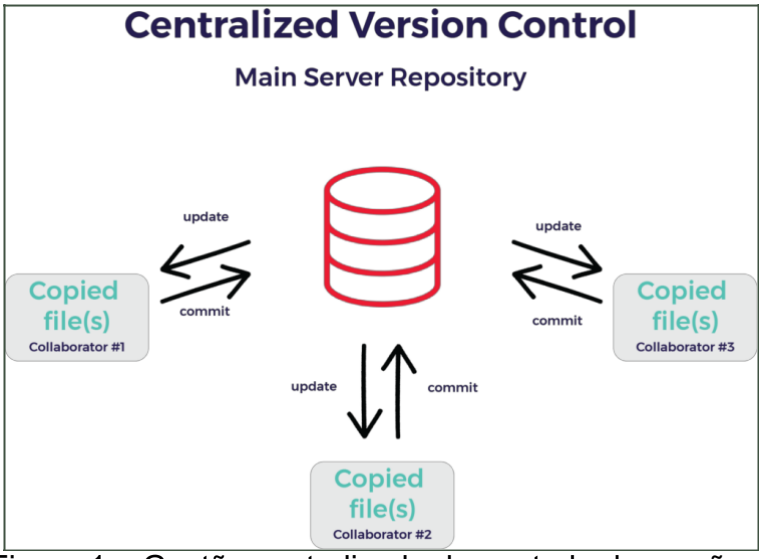

Figura 1 – Gestão centralizada de controlo de versões

No cenário atrás descrito, considere que, enquanto responsável pela segurança deste serviço, é confrontado com a necessidade de adicionar segurança ao mesmo, pelo que deverá desenhar uma solução de segurança, bem como identificar os algoritmos criptográficos necessários. Considere igualmente que se trata de um sistema desenvolvido na empresa, embora sem quaisquer funcionalidades de segurança. A seguir descrevem-se em maior detalhe os objetivos do trabalho, com este objetivo em vista.

Tal como discutido anteriormente, o objetivo do trabalho é delinear uma estratégia para adicionar segurança ao serviço de controlo centralizado de

versões anteriormente descrito. Os requisitos de segurança para o serviço são os seguintes:

- Ao nível das comunicações entre utilizadores do serviço e o serviço de controlo de versões:

a) Confidencialidade e integridade em todas as mensagens (commit e update) trocadas entre os utilizadores e o serviço.

b) Autenticação mútua entre os utilizadores e o serviço.

c) Não-repudiação nas mensagens (commit e update) trocadas entre os utilizadores do serviço e o serviço.

- Ao nível do armazenamento da informação na base de dados do serviço de controlo de acessos:

a) Integridade da informação armazenada.

b) Considere que o serviço dispõe da capacidade de armazenar, para além da versão mais recente da informação partilhada, também versões anteriores. Para todas as versões da informação partilhada, o serviço deverá garantir integridade da informação, bem como a identificação do utilizador responsável por cada atualização (com o comando commit) da mesma.

O relatório a entregar deverá apresentar a solução proposta para adicionar segurança ao sistema de controlo de versões, focando os seguintes aspetos fundamentais:

a) Propor um modelo de segurança para o serviço.

b) Identificar os algoritmos criptográficos a utilizar para cumprir os requisitos descritos anteriormente, juntamente com informação relevante para cada algoritmo (por exemplo, o modo de aplicação do algoritmo e o tamanho da chave recomendada).

c) Outros aspetos que considerar relevantes, particularmente ao nível do enquadramento da solução.

Algumas notas: - Atenção à estrutura do documento e respetivo conteúdo; - Atenção ao nível do português utilizado; - Atenção às referências bibliográficas; - Atenção aos erros ortográficos; - Atenção à reutilização de código obtido diretamente na web (nota: eu também conheço essas fontes!); - Atenção às "reutilizações" de textos de livros, artigos, outros trabalhos ou ChatGPT. Plágios serão penalizados!

Recursos

Utilize os recursos à sua disposição, nomeadamente:

1. Fórum específico do eFolio A
2. Manual recomendado

Critérios de avaliação e cotação

Na avaliação do trabalho serão tidos em consideração os seguintes critérios e cotações:

1. Segurança proposta ao nível das comunicações entre utilizadores do serviço e o serviço de controlo de versões = 1,5 pontos.
2. Segurança proposta ao nível do armazenamento da informação na base de dados do serviço de controlo de acessos = 1,5 pontos.
3. Qualidade do conteúdo do relatório, quer em termos técnicos, quer em termos de justificação das opções tomadas = 1,0 ponto.

Total: 4 pontos = 4 valores

Normas a respeitar

Deve redigir o seu relatório na Folha de Resolução disponibilizada na turma e preencher todos os dados do cabeçalho.

Todas as páginas do documento devem ser numeradas.

O seu relatório não deve ultrapassar 4 páginas A4 (excluindo a folha de rosto) redigidas em Arial, tamanho de letra 11. O espaçamento entre linhas deve corresponder a 1,5 linhas.

Nomeie o ficheiro com o seu número de estudante, seguido da identificação do E-fólio, segundo o exemplo apresentado: 000000efolioA.

Deve carregar os ficheiros para a plataforma no dispositivo E-fólio A até à data e hora limite de entrega. Evite a entrega próximo da hora limite para se precaver contra eventuais problemas. O ficheiro a enviar não deve exceder 8 MB.

Votos de bom trabalho!

Henrique S. Mamede