E-fólio A | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

A preencher pelo estudante

NOME: José Manuel Valente Ribeiro

N.º DE ESTUDANTE: 1601792

CURSO: Engenharia Informática

DATA DE ENTREGA: 27 de novembro de 2023

Um sistema centralizado de controlo de versões (VCS - Version Control System) é uma ferramenta que permite rastrear as mudanças em arquivos e coordenar o trabalho entre várias pessoas num projeto. O principal objetivo é manter o histórico das alterações, facilitando a colaboração e a gestão eficiente de documentos. Em seguida, passo a explicar resumidamente os componentes deste serviço aos quais este trabalho irá focar. Este serviço é composto pelo repositório central que é o local central onde todas as versões dos arquivos e histórico de alterações são armazenados. Ele atua como o ponto central de coordenação para colaboradores. Tem o commit que representa uma mudança nos arquivos. Quando um utilizador realiza um commit, ele está a enviar as suas alterações para o repositório central. E tem o update que é o processo de sincronizar o código local de um utilizador com as alterações mais recentes do repositório central. Isso geralmente envolve receber as alterações feitas por outros utilizadores.

Enquanto responsável pela segurança deste serviço na minha empresa, foi-me encarregue desenhar uma solução de segurança e identificar os algoritmos criptográficos necessários à sua implementação. Adicionar segurança a um sistema centralizado de controlo de versões é crucial para proteger informações sensíveis, garantir a integridade dos dados e prevenir acessos não autorizados. É meu dever como responsável certificar que a segurança e qualidade do serviço sejam prioridades contínuas, implementando práticas robustas, políticas de acesso restrito e mecanismos de proteção, de modo a salvaguardar os dados sensíveis, promover a integridade das operações e garantir uma experiência confiável para os utilizadores.

Em primeiro lugar, para fortalecer a segurança de VCS, é crucial implementar iniciativas de educação e sensibilização. Pretendo oferecer regularmente formação prática, como workshops e treino de phishing (uma forma de fraude online na qual os criminosos tentam obter informações sensíveis, como senhas, detalhes de cartões de crédito e outras informações pessoais, ao se fazerem passar por entidades confiáveis) para capacitar os utilizadores na identificação de ameaças e na aplicação de práticas seguras. Pretendo também enviar comunicações periódicas com estudos de caso reais e a introdução de ferramentas preventivas. Para cultivar uma cultura de segurança, em segundo lugar, é essencial reconhecer boas práticas, criar fóruns de discussão, envolver os utilizadores na definição de políticas e realizar exercícios de simulação regulares.

Seguidamente irei abordar a segurança ao nível das comunicações entre utilizadores do serviço e o VCS. Existem imensas maneiras de fortalecer a segurança

nas comunicações do sistema centralizado do VCS. Eu optei pela aplicação do modelo de segurança com a utilização do algoritmo de hash SHA-256 para garantir a integridade e autenticação das mensagens. O algoritmo de hash SHA-256 (Secure Hash Algorithm 256 bits) é uma função criptográfica que transforma qualquer conjunto de dados em uma sequência fixa de 256 bits. Uma das suas principais propriedades é produzir uma saída única e irreversível para entradas diferentes, tornando possível verificar a integridade dos dados. Passo a explicar esse processo. Antes da transmissão, o remetente aplica o SHA-256 aos dados a serem enviados, gerando um hash único que representa a "impressão digital" dos dados. Esse hash é transmitido juntamente com os dados. No lado do destinatário, ao receber os dados e o hash correspondente, o mesmo conjunto de dados é submetido novamente ao SHA-256. O resultado é comparado com o hash recebido. Se os hashes coincidirem, isso indica que os dados não foram modificados durante a transmissão. A autenticação mútua é mantida por meio de certificados digitais (1). Cada parte (servidor e utilizadores) possui um certificado contendo uma chave pública. O remetente assina o hash SHA-256 com a sua chave privada, e o destinatário verifica a assinatura usando a chave pública do remetente. Para garantir não-repudiação, o remetente inclui uma assinatura digital baseada no hash SHA-256. A assinatura digital é um método de autenticação eletrónica que utiliza algoritmos de chave pública e privada. O signatário emprega sua chave privada para assinar digitalmente o documento, enquanto a chave pública correspondente possibilita a verificação da assinatura. Essa abordagem garante a integridade do documento, pois qualquer modificação não autorizada resultaria na falha da verificação da assinatura. Além disso, a autenticidade do signatário é assegurada, pois somente o detentor da chave privada associada à chave pública usada para verificar a assinatura pode tê-la gerado. Adicionalmente, a não-repudiação é estabelecida, impedindo que o signatário negue a autoria após a verificação bem-sucedida da assinatura. Esses princípios criptográficos tornam as assinaturas digitais essenciais para garantir a autenticidade, integridade e responsabilidade em contextos digitais. (1) O certificado digital é um documento eletrónico que contém informações sobre a identidade de uma entidade e é emitido por uma Autoridade Certificadora (AC) confiável. A chave pública, parte do certificado, é divulgada publicamente para cifrar mensagens destinadas ao titular. Além disso, o certificado inclui detalhes sobre a identidade do titular, como nome e organização, e possui um período de validade definido. Identificadores exclusivos, como número de série, são atribuídos ao certificado, e a autenticidade é verificada por meio de uma assinatura digital gerada pela Autoridade Certificadora.

Eu escolhi este algoritmo e não o SHA-512 por exemplo, devido ao facto de o SHA-256 ser geralmente mais rápido em termos de processamento computacional e ser mais compativel com um leque maior de sistemas e plataformas. Embora o algoritmo de hash SHA-256 seja amplamente adotado e reconhecido pela sua segurança, é importante reconhecer a existência de potenciais riscos. O avanço contínuo da capacidade computacional pode, teoricamente, aumentar a viabilidade de ataques de força bruta, nos quais um adversário tenta decifrar um input correspondente a um hash específico. No entanto, o SHA-256 tem uma excelente reputação pela sua robustez e considero ser uma escolha confiável.

Passo agora a abordar o processo para implementar a segurança do CVS, focando na integridade e confidencialidade dos dados armazenados no repositório. Neste ponto eu opto por utilizar a criptografia simétrica e assimétrica de forma complementar, pois cada abordagem oferece vantagens específicas que, quando combinadas, proporcionam uma solução de segurança robusta e eficaz. Por exemplo a criptografia simétrica utiliza algoritmos simétricos, como o AES (Advanced Encryption Standard) para encriptar os dados. Isso implica que a mesma chave seja usada tanto para encriptar quanto para desencriptar os dados. O AES, é eficiente em termos de desempenho e adequado para proteger grandes volumes de dados. Chaves AES de 256 bits são preferíveis para aplicações que demandam maior segurança, enquanto chaves de 128 ou 192 bits podem ser adequadas para casos específicos. Por outro lado, a criptografia assimétrica, que pode ser exemplificada pelo algoritmo RSA (Rivest-Shamir-Adleman), é um método onde um par de chaves é utilizado: uma chave pública, conhecida por todos, e uma chave privada, mantida em segredo. Essas chaves estão matematicamente relacionadas, mas a chave privada não pode ser derivada da chave pública. No contexto do serviço de controlo de versões, o RSA é empregado para cifrar a chave simétrica utilizada na criptografia dos dados. Isso permite que a chave simétrica seja compartilhada de maneira segura entre os utilizadores, garantindo a confidencialidade da transmissão e, ao mesmo tempo, tirando proveito da eficiência da criptografia simétrica para proteger os dados armazenados. Essa combinação estratégica de criptografias otimiza a segurança, garantindo integridade, confidencialidade e autenticidade no ambiente de controlo de versões. O tamanho da chave RSA influencia a segurança. Atualmente, tamanhos de chave de 2048 bits são considerados o mínimo para segurança de médio prazo, enquanto tamanhos de chave de 3072 bits ou mais são recomendados para segurança de longo prazo.

Em conclusão, como responsável pela segurança do serviço de controlo centralizado de versões, foi delineada uma abordagem abrangente para reforçar a segurança e atender aos requisitos específicos de confidencialidade, integridade, autenticação mútua e não-repúdio. Inicialmente, destaquei a importância da educação e sensibilização, implementando programas regulares de formação e promovendo uma cultura de segurança entre os utilizadores. Posteriormente, concentrei-me na segurança das comunicações, propondo a aplicação do modelo de segurança com a utilização do algoritmo de hash SHA-256 para garantir a integridade e autenticação das mensagens, bem como a autenticação mútua através de certificados digitais. Para fortalecer a integridade e confidencialidade dos dados armazenados, adotei uma abordagem combinada de criptografia simétrica e assimétrica. Utilizando o AES para a criptografia simétrica, garantimos eficiência e segurança na proteção de grandes volumes de dados. Com o RSA para a criptografia assimétrica, as chaves simétricas são seguramente compartilhadas, promovendo a confidencialidade da transmissão. A estratégia proposta assegura a integridade da informação e a identificação do utilizador responsável por cada atualização. A implementação destas medidas, combinadas com práticas de educação contínua, auditoria e monitorização, cria uma solução de segurança abrangente e eficaz para o serviço de controlo centralizado de versões. Cabe ainda ressaltar que o sistema foi concebido com flexibilidade para enfrentar desafios futuros, incluindo atualizações em algoritmos de segurança. Nesse sentido, está previsto um plano de migração para algoritmos mais avançados, assegurando a manutenção contínua da integridade e confidencialidade do serviço ao longo do tempo.

Referências bibliográficas:

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. 7th Edition (Global Edition), Prentice Hall:

Criptografia Simétrica, Chapter 3

AES, Chapter 6

SHA-256, Chapter 11

Critpografia Assimétrica e RSA, Chapter 9

Boson Treinamentos: https://www.youtube.com/watch?v=cWld3rMD7Wk&list=PLucm8g_ezqNred_fII4GzZxMi91PKbney

Version Control System:

https://en.wikipedia.org/wiki/Version_control

OpenAI. 2023. "ChatGPT." https://www.openai.com.