- **Quais tipos de segurança para aplicação existem?**

- Segurança de Nuvem — busca proteger os servidores em nuvem e os dados armazenados nos sistemas distribuídos;
- Segurança de Rede — cuida dos equipamentos de rede e da comunicação da empresa com o mundo externo;
- Segurança do Parque — o que pode incluir cuidado com computadores alugados;
- Segurança Cibernética — protege os arquivos, as aplicações;
- Segurança de APIs — busca proteger as APIs;
- Cibersegurança — segurança especificamente no digital

- **Qual o tipo de segurança mais utilizada em projetos Java?**

Em projetos Java, a segurança é uma preocupação importante, e existem várias abordagens e tecnologias que podem ser usadas para implementar medidas de segurança. Algumas das tecnologias e práticas de segurança mais comuns em projetos Java são as seguintes:

1. Java Authentication and Authorization Service (JAAS): É uma API do Java que permite a autenticação e autorização de usuários em aplicativos Java. O JAAS fornece um conjunto de interfaces e classes que podem ser usadas para configurar e gerenciar políticas de segurança.

2. Java Secure Socket Extension (JSSE): É uma API do Java que oferece suporte a comunicações seguras por meio de protocolos criptográficos, como SSL (Secure Sockets Layer) e TLS (Transport Layer Security). O JSSE permite a criação de conexões seguras entre aplicativos Java por meio do uso de certificados digitais e criptografia.

3. Java Cryptography Architecture (JCA): É um framework fornecido pelo Java que oferece suporte à criptografia em aplicativos Java. Ele fornece uma API para criptografia simétrica e assimétrica, geração e gerenciamento de chaves, assinaturas digitais e outras operações criptográficas.

4. Java KeyStore (JKS): É um formato de arquivo usado para armazenar chaves criptográficas, certificados digitais e outras informações de segurança em Java. O JKS é frequentemente usado para armazenar certificados de servidor e clientes em projetos que envolvem comunicação segura.

5. Spring Security: É uma estrutura de segurança amplamente utilizada em aplicativos Java baseados em Spring. O Spring Security fornece recursos abrangentes para autenticação, autorização, prevenção de ataques comuns, proteção contra CSRF (Cross-Site Request Forgery) e muito mais.

- ## O que é criptografia?

A criptografia é um mecanismo de segurança e privacidade onde comunicações por texto, imagens, vídeo, etc, se tornam inacessíveis para quem não tem os códigos de tradução da mensagem.

Essa tecnologia utiliza cifragem dos dados para embaralhar as informações. Isso de forma que apenas aqueles que tenham a chave para descriptografar consigam acessar a informação original.

Ou seja, é a construção e análise de protocolos que impedem terceiros de lerem mensagens privadas.

Qual a importância da criptografia para o mundo digital?

A grande importância se dá pela proteção da identidade e dos dados de todos os usuários. Se ocorrer uma tentativa de invasão, a criptografia protege todas as informações importantes.

A grande necessidade de usar essa tecnologia está na proteção da identidade, se ocorrer uma invasão, o sistema irá proteger tudo, até mesmo mensagens trocadas.

Confira os principais tipos de criptografias:.

1. Chave simétrica

Esse é o tipo mais comum, onde uma mesma chave é utilizada pelo emissor e receptor da mensagem, seja para codificação ou decodificação dos dados.

O surgimento de outros modelos de criptografia se deu através da chave simétrica. Portanto, uma forma de entender o quanto ela é testada e aprovada por especialistas em segurança.

2. DES (Data Encryption Standard)

Modelo mais básico e um dos primeiros criados. Fornece uma proteção de apenas 56 bits, oferecendo até 72 quadrilhões de combinações.

Devido a isso, ela é considerada um método com segurança reduzida, porém não a torna irrelevante. Acontece que esse tipo de criptografia pode ser decifrada por meio de uma prática tecnológica conhecida como “força bruta”. Isso acontece porque um programa de computador fica testando diversas chaves sem parar, podendo passar várias horas nessa tentativa.

3. IDEA (International Data Encryption Algorithm)

Chave simétrica que opera em blocos de informações de 64 bits com chaves de 128 bits. Protege as informações confundindo as combinações.

4. AES (Advanced Encryption Standard)

Um dos mais seguros, utilizados pelo Governo dos Estados Unidos e por várias organizações de segurança. São chaves extremamente difíceis de serem quebradas em ataques cibernéticos.

Enquanto as duas últimas não passam de 70 blocos de informações, essa criptografia chega a operar com bloco de 128. Por isso, acaba sendo uma das mais seguras que existem.

5. Chave assimétrica

Trabalha de modo privado e público, com chaves secretas e codificações encaminhadas ao receptor para que assim tenha acesso ao conteúdo.

Devido a essa característica, essa criptografia também é conhecida como “chave pública”.

○ O que é autenticação?

A autenticação é um processo de segurança para verificar a veracidade e autenticidade de uma pessoa ou objeto. O tema da autenticação de um indivíduo, entidade ou objeto não é algo novo, dado que a palavra "autêntico" vem do grego "authentikos", que significa "original, genuíno". Portanto, a autenticação é baseada na comparação e correspondência para determinar se algo ou alguém é, de fato, o que ou quem afirmam ser.

Quais são os principais métodos de autenticação digital?

Token

O método por token é um padrão no mercado, utilizado em diferentes plataformas. Ele é bastante comum para fazer a autenticação de sistemas web em que há a relação entre quem utiliza e o servidor.

O token funciona da seguinte forma: o usuário coloca o login e a senha, e é gerado o token que dá a permissão para ele entrar no site ou aplicativo e utilizar os recursos em um tempo determinado, sem que precise fazer o login novamente.

Autenticação de chave pública e privada

É um tipo de autenticação dividida em duas partes ou duas chaves: uma pública e outra privada. Uma é usada para codificar e a outra é usada para decodificar — sendo a pública disponibilizada para qualquer usuário que está no sistema ou servidor. A privada fornece acesso apenas ao usuário, e só a ele pertence a criptografia dessa chave.

Suponha que uma pessoa mandou uma mensagem com a chave pública. O outro usuário deve usar a chave privada dele para receber o recado. Para responder, no entanto, ele terá que usar a chave pública.

Autenticação de chave simétrica

Nesse caso, é usada apenas uma chave para a autenticação. Ao contrário da anterior, é a mesma chave para codificar ou decodificar, o que pode ser uma desvantagem para acessar informações públicas, já que todos devem ter a chave.

Nesse tipo de autenticação, o usuário partilha uma chave com o servidor, então, quando há o envio de mensagem, ela é decodificada utilizando a mesma chave. Quando o servidor reconhece o padrão, ele autoriza o usuário.

Autenticação de identidade digital

Essa é uma das autenticações mais rigorosas, pois necessita de uma série de informações do usuário para confirmar o acesso. Geralmente, ela utiliza a combinação de dados, como localização, comportamento, dispositivo, endereço de e-mail e outros.

Por ser bastante exigente — já que é necessário confirmar que o usuário realmente é quem diz ser —, ela costuma ser bem segura, exigindo, inclusive, que o utilizador esteja em tempo real para responder às perguntas.

Autenticação contextual

Alguns sistemas podem ter uma configuração de acesso um pouco diferente. A maioria das plataformas exige algum tipo de senha colocada pelo próprio usuário para garantir o acesso. Na autenticação por contexto, a confirmação da identidade acontece de forma confidencial, com base em fatores como localização do dispositivo ou do endereço de IP.

Geolocalização

Outra ferramenta usada para a autenticação é a localização do usuário. Essa é uma forma de confirmação que funciona não só para indicar que a pessoa é quem diz ser, mas também que ajuda a definir informações importantes, principalmente quando se trata de uma troca de arquivos.

Se um documento foi gerado em um lugar e foi modificado em outro, é possível saber graças à verificação do local de armazenamento desse arquivo. Isso facilita a descoberta de um documento corrompido, por exemplo.

Certificado digital

Essa é uma forma de autenticação um pouco mais específica. O objetivo do certificado digital é checar se certo processo está de acordo com todas as diretrizes de segurança. Em muitos casos, ele pode ser visto como uma

espécie de identidade digital, sendo utilizado pelo indivíduo para ser reconhecido em outros sistemas e plataformas.

O certificado digital também fornece uma chave privada ao usuário, além de uma assinatura digital por meio de PIN, que autentica a assinatura de documentos.

Autenticação por SMS

Geralmente, esse é um tipo de autenticação de duas etapas. Primeiramente, o usuário faz o login para acessar a plataforma, e deve confirmar quem ele é por meio de um código numérico para concluir o login.

É um tipo de autenticação bastante comum quando o usuário esquece a senha ou precisa entrar em uma plataforma online.

Autenticação centralizada

Esse modelo não tem tanta relação com o meio, mas com a possibilidade de ingresso. Isso acontece porque a forma de o usuário ter acesso pode ser por senha ou token, mas essa autenticação garantirá que ele possa logar em uma série de outros serviços. Isso significa que o usuário não precisa de outro login para acessar.

É muito comum ver esse tipo de autenticação em redes sociais. A senha de uma pode ser usada para entrar em outros produtos da empresa, por exemplo — como é o caso do Facebook e do Instagram.

Outras plataformas

Esse é um tipo de autenticação que segue bem o princípio da centralizada, mas não é preciso que sejam os serviços da mesma empresa. Chamada de e-authentication, aqui a relação é entre o login e a senha de outras plataformas.

Por exemplo: alguns aplicativos podem proporcionar o cadastro de acesso e deixar que se use o login de uma rede social para entrar. Sendo assim, em vez do usuário criar uma nova identificação, ele pode entrar diretamente se já estiver logado na rede social.

Essa autenticação pode não ser tão segura, já que você fornece seus dados a outra plataforma, mas facilita o acesso, uma vez que não é preciso criar uma senha diferente.

Como ocorre o processo de autenticação?

Apesar de serem os mais comuns utilizados hoje no mercado, não quer dizer que eles são menos seguros ou que não resolvem bem a maioria das dores das empresas nesse segmento. Inclusive, alguns métodos tendem a ter a mesma estrutura, organizada de maneira diferente. Vamos ver alguns exemplos:

PINs ou senhas

Utilizados em praticamente todos os tipos de validação, os PINs e as senhas são números que, em tese, apenas o usuário legítimo conhece. De posse da sequência correta desses algarismos, o usuário consegue comprovar, em um

primeiro momento, que é ele que solicita o acesso, e não uma pessoa se passando por ele.

Biometria

A biometria é realizada por sistemas capazes de ler as características físicas únicas de cada usuário. Isso faz com que seja possível afirmar, com bastante efetividade, que o usuário é quem diz ser quando solicita um acesso.

Autenticação de dois fatores

A autenticação de dois fatores é uma camada extra de segurança para consumidores e empresas. É uma combinação dos métodos de autenticação citados anteriormente.

Também conhecida como 2FA, é uma etapa além da senha de usuário para garantir que uma pessoa, quando tenta o login em um ambiente protegido, realmente é quem diz ser — e não um fraudador tentando cometer um crime.

Os casos mais comuns de uso do segundo fator de autenticação são aqueles nos quais um SMS ou um código é enviado para um e-mail cadastrado pelo usuário, que tem a tarefa de acessá-lo e fazer a autenticação.

Essa ferramenta também é utilizada no mundo físico, como os caixas eletrônicos que pedem impressões digitais dos correntistas nos leitores biométricos, após a validação com senha.