ESTI – ESCOLA SUPERIOR DA TECNOLOGIA DA INFORMAÇÃO

GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

BLOCO DE DESENVOLVIMENTO ANDROID

Segurança, Monetização e Publicação de Aplicativos Android

Assessment

Luiz Carlos de Souza Ardovino Ribeiro

Prof: Rafael

CPF:155.647.787-23

Santa Catarina, 06 de dezembro de 2022

Questão 1:

Explique como o Sistema Operacional Android protege os dados dos usuários de aplicativos de terceiros.

Resposta:

Além de oferecer isolamento de dados, compatibilidade com a criptografia para todo o sistema de arquivos e canais de comunicação seguros, o Android fornece diversos algoritmos para proteger dados usando a criptografia.

Questão 2:

Para que serve a camada HAL (Hardware Abstraction Layer) no sistema Android?

Resposta:

A camada de abstração de hardware (HAL) fornece interfaces padrão que expõem as capacidades de hardware do dispositivo para a estrutura da Java API de maior nível.

Questão 3:

O que são Certificados de Autoridade? Para que eles servem?

Resposta:

A Autoridade de Certificação emite certificados digitais que certificam a propriedade de uma chave pública. A CA é considerada um terceiro confiável e, portanto, o Android os reconhece como certificados confiáveis. Normalmente, uma CA é instalada ao mesmo tempo em que o certificado do cliente é instalado. Uma CA também pode ser instalada separadamente, mas pode ser necessária para verificar o certificado em relação ao dispositivo em que está. Essa medida ajuda a eliminar a ameaça de comprometimento de credenciais quando armazenadas em um cartão de armazenamento externo.

Os certificados digitais identificam computadores, smartphones e apps por motivos de segurança. Um certificado digital identifica seu smartphone e confirma que ele pode acessar algo.

Questão 4:

Descreva três serviços na nuvem relacionados à manutenção da segurança na plataforma Android.

Resposta:

- Backup do google drive: o Google implementou uma função para fazer o backup manual do seu dispositivo no Google Drive, ao menos para salvar os principais dados que estão contidos nele.

- O Dropbox é um serviço de armazenamento de dados em nuvem e sincronização que serve para salvar seus arquivos e fotos em servidores online.

- O OneDrive é o serviço de armazenamento de arquivos na nuvem da Microsoft, gratuito para Android, iOS, Mac e Windows. Nele é possível salvar conteúdo de vários formatos online e acessá-los de qualquer lugar.

Questão 5:

Qual é a diferença entre Permissões Normais e Permissões Perigosas?

Resposta:

Os grupos de permissão normais são permitidos por padrão, pois não representam um risco à privacidade. (Por exemplo, o Android permite que os aplicativos acessem à internet sem a sua permissão.) No entanto, os grupos de permissão perigosos podem fornecer aos aplicativos o acesso a informações, como seu histórico de chamadas, mensagens privadas, localização, câmera, microfone, entre outros. Portanto, o Android sempre solicitará que você aprove as permissões perigosas.

Questão 6:

Cite e descreva pelo menos duas boas práticas que devemos ter ao trabalhar com permissões de acesso aos componentes do dispositivo.

Resposta:

- Aumento na carga de transações:

É solicitado aos usuários que concedam acesso aos grupos de permissões individualmente, e não como um conjunto. Dessa forma, é extremamente importante minimizar o número de permissões solicitadas. Isso aumenta a sobrecarga do usuário para conceder permissões e, portanto, a probabilidade de pelo menos uma das solicitações ser negada.

- Permissões que precisam se tornar um gerenciador padrão:

Alguns apps dependem do acesso a informações confidenciais do usuário relacionadas a registros de chamadas e mensagens SMS. Se você quiser solicitar permissões especificamente para registros de chamadas e mensagens SMS e publicar seu app na Play Store, precisará solicitar que o usuário configure seu app como o gerenciador padrão de uma função principal do sistema antes de solicitar essas permissões de execução.

Questão 7:

Para que servem os componentes EncryptedSharedPreferences e EncryptedFile?

Resposta:

- EncryptedSharedPreferences: Encapsula a classe SharedPreferences e criptografa automaticamente as chaves e os valores usando um método de dois esquemas: As chaves são criptografadas usando um algoritmo de criptografia determinístico para que a chave possa ser criptografada e pesquisada adequadamente. Os valores são criptografados usando AES-256 GCM e não são determinísticos.

- EnryptedFile: Componente para criptografar e descriptografar um arquivo.

Questão 8:

Explique duas estratégias de monetização para aplicativos Android.

Resposta:

- Modelo de versões gratuita e paga do app

Uma das estratégias de monetização de apps mais utilizadas é oferecer duas versões do aplicativo: uma gratuita e uma paga. Com essa abordagem, os desenvolvedores limitam alguns recursos no app gratuito para "incentivar" o usuário a fazer um upgrade para o app pago, ou monetizam a versão gratuita com publicidade no aplicativo.

Essa estratégia traz dois benefícios. Por um lado, oferece uma opção grátis para os usuários conhecerem as funcionalidades básicas do app sem pagar nada. Por outro, permite que o desenvolvedor aumente a base de usuários para uma possível monetização com upgrades ou publicidade no aplicativo.

- Modelo de app gratuito com compras no aplicativo

Outra estratégia muito utilizada de monetização são as compras no aplicativo (IAP, na sigla em inglês). O app em si e as funções mais básicas são gratuitos. No entanto, se o usuário quiser recursos melhores, como ganhar vidas extras em um jogo ou ter acesso a recursos premium em um app de relacionamentos, ele precisará utilizar o modo pago.

Em alguns casos, os usuários ainda têm acesso a recursos premium sem pagar nada. Se eles forem pacientes o bastante para esperar que algumas funcionalidades sejam liberadas ou interagirem com o app com frequência, poderão usar a versão gratuita para sempre. Em outros casos, essas opções não estão disponíveis, e os desenvolvedores só liberam algumas funções sem custo, e outras são disponibilizadas via compra no aplicativo.

Questão 9:

Explique para que serve o parâmetro “Atualização Automática” ao cadastrar o bloco de anúncios no Google AdMob.

Resposta:

A taxa de atualização automática de um bloco de anúncios determina a frequência com que uma nova solicitação de anúncio é gerada para o bloco de anúncios em questão.

Questão 10:

O que é um bloco de anúncios premiado?

Resposta:

Um bloco de anuncio premiado da AdMob, você pode recompensar os usuários com itens no aplicativo em troca de interações com anúncios jogáveis e em vídeo, além de pesquisas.

Questão 11:

Descreva o processo, a nível de código, para liberar uma recompensa após a exibição de um vídeo.

Resposta:

Load a rewarded ad object

Set the FullScreenContentCallback

Show the ad

Ao exibir um anúncio premiado, você usará um objeto OnUserEarnedRewardListener para lidar com eventos de recompensa.

Questão 12:

Qual o procedimento para se cadastrar como desenvolvedor no Google Play?

Resposta:

Etapa 1: inscrever-se para uma conta de desenvolvedor do Google Play.

Etapa 2: aceitar o Contrato de distribuição do desenvolvedor.

Etapa 3: pagar a taxa de inscrição.

Etapa 4: inserir os detalhes da sua conta.

Questão 13:

Quais os requisitos necessários para preparar o aplicativo para publicação?

Resposta:

- Configurar o aplicativo para lançamento.

No mínimo, é necessário remover chamadas de Log e remover o atributo android:debuggable do arquivo de manifesto. É também preciso fornecer valores para os atributos android:versionCode e android:versionName, que estão localizados no elemento . Além disso, pode ser necessário definir diversas outras configurações para cumprir os requisitos do Google Play ou acomodar o método usado para lançar o aplicativo.

Se você está usando arquivos de compilação do Gradle, é possível usar o tipo de build release para definir configurações para a versão publicada do app.

- Criar e assinar uma versão de lançamento do aplicativo.

Usar os arquivos de compilação do Gradle com o tipo de build release para criar e assinar uma versão de lançamento do aplicativo. Consulte Criar e executar no Android Studio.

- Testar a versão de lançamento do aplicativo.

Antes de distribuir o aplicativo, é necessário testar minuciosamente a versão de lançamento em pelo menos um dispositivo celular de destino e um dispositivo tablet de destino.

- Atualizar recursos do aplicativo para lançamento

Todos os recursos do aplicativo, como arquivos multimídia e gráficos, precisam estar atualizados e incluídos no aplicativo ou organizados nos servidores de produção adequados.

Preparar os servidores e serviços remotos de que o aplicativo depende.

Se o aplicativo depende de servidores ou serviços externos, é preciso ter certeza de que eles são seguros e estão prontos para produção.

Questão 14:

Ao criar uma versão do aplicativo para publicação no Google Play Console, quais as características das faixas Alfa e Beta?

Resposta:

A API Google Play Developer permite fazer upload de novos APKs para seus apps e liberálos para diferentes faixas de lançamento. Isso permite implantar versões Alfa e Beta do seu app, que são disponibilizadas para usuários aprovados.

As versões Alfa e Beta do app são implantadas para os usuários que você atribui aos grupos de testes Alfa e Beta. Você atribui usuários a esses grupos usando o Google Play Console. As versões internas do app são implantadas nessa faixa, de acordo com a configuração no Google Play Console.

Questão 15:

Quais as desvantagens de publicar um aplicativo através de um site, no lugar do Google Play?

Resposta:

A principal desvantagem é a segurança, com o risco acentuado de contaminar o Android com algum malware.

A Google Play permite que seus usuários façam comentários e deem notas para o seu aplicativo, já um site não.