INSTITUTO INFNET
ESCOLA SUPERIOR DA TECNOLOGIA DA INFORMAÇÃO
CURSO DE ENGENHARIA DE SOFTWARES

Francisco Alves Camello Neto

TP 1 - Segurança, Monetização e Publicação de Aplicativos Android

Profº Denis Gonçalves Cople

Brasília
2022

SUMÁRIO

1ª - QUESTÃO

Quais são os três principais elementos da Arquitetura Android? Descreva cada um deles.

Resposta:

Integridade, confidencialidade e disponibilidade

2ª - QUESTÃO

Descreva três serviços do Google na nuvem que são voltados para a segurança do sistema Android.

Resposta:

VERIFY APPS

Atualmente com o nome Google Play Protect, este serviço faz uma verificação constante dos aplicativos de forma a detectar possíveis riscos, emitindo avisos, bloqueando instalações e removendo aplicativos nocivos.

SAFETYNET

Trata de um conjunto de APIs voltadas para a verificação da integridade de aplicativos e dispositivos, rastreando a presença de malwares e alterações efetuadas no sistema. Com a execução em background do programa snet, as informações são enviadas continuamente para o Google, permitindo que o Compatibility Test Suite (CTS) verifique qualquer tipo de modificação no sistema.

DEVICE MANAGER

Viabiliza ações de gerenciamento remoto do dispositivo, como bloqueio de funcionalidades, emissão de alerta, rastreio da localização, eliminação de dados, entre outros, tornando-se muito útil para os casos de perda ou roubo.

3ª - QUESTÃO

Suponha que você está desenvolvendo um aplicativo e deseja acessar as informações do cartão SIM do aparelho. Como é possível realizar essa operação?

Resposta:

Utilizando as permissões do grupo STORAGE, que ao concordar com o acesso, estaria permitindo os direitos de escrita e leitura simultaneamente.

4ª - QUESTÃO

Quais as formas de implementar IPC em um sistema Android?

Resposta:

O primeiro modelo é utilizado para serviços privados, executados no mesmo processo do cliente. Neste caso é criado um descendente de Binder, o qual é adotado como resposta ao método de vinculação do serviço.

No caso da comunicação entre processos distintos, a forma mais simples seria a adoção de objetos do tipo Message na comunicação. Neste caso, definimos uma interface para o serviço com o uso de Messenger e criamos um Handler para o tratamento das mensagens recebidas.

Quanto ao AIDL (Android Interface Definition Language), trata de um descritor de serviços próprio para o ambiente Android, devendo ser criados os arquivos com extensão .aidl para que as ferramentas do SDK se encarregam da implementação das classes abstratas necessárias para a comunicação.

5ª - QUESTÃO

O que é o sistema de permissões da plataforma Android?

Resposta:

O sistema de permissões do Android mantém todo o sistema consistente fazendo com que aplicativos que necessitem de acesso a dados, dados não produzidos por eles, ou necessitem de acesso a funcionalidades não disponíveis neles, que esses aplicativos definam permissões para que o acesso, consumo, seja possível.

6ª - QUESTÃO

Descreva pelo menos 5 permissões normais e as funções de cada uma delas.

Resposta:

Conexões Bluetooth

Aplicativos para transmissão sem fio exigem essa permissão, para que os seus arquivos possam ser transferidos através de Bluetooth, e também para que outros dispositivos possam ser encontrados e pareados. Normalmente, essa permissão é relativamente inofensiva, mas atualmente já sabemos sobre malwares que podem tomar controle do Bluetooth, e assim trocar arquivos com outros aparelhos próximos.

Status e acessos a Rede

Esta permissão informa o tipo de conexão a que você está conectado (Wi-Fi, 4G, etc.). É uma permissão relativamente inofensiva. Há também permissões que podem ver informações sobre a rede Wi-Fi em que você está conectado, e outras que podem até ligar e desligar seu Wi-Fi. Isso pode ser mais perigoso e é preciso ficar atento à rede em que seu smartphone está conectado. Uma outra pode modificar o tipo de rede que você está usando, ou seja, passar do Wi-Fi para o 4G e vice-versa.

Instalação de Packages (instalar aplicativos)

Com esta permissão, um aplicativo pode instalar outros aplicativos. Isso é importante para lojas alternativas à Google Play, como a Amazon, por exemplo.

Trava de modo ligado

Players de vídeo e outros aplicativos precisam desta permissão para impedir a sua tela de desligar enquanto você está assistindo a um vídeo ou jogando um jogo.

Configurações de sincronização

Isso permite que um aplicativo saiba se você tem sincronização de dados (para o Gmail ou para o Facebook, por exemplo) ligado ou desligado.

7ª - QUESTÃO

Descreva pelo menos 5 permissões perigosas e as funções de cada uma delas.

Resposta:

READ_CALENDAR / WRITE_CALENDAR, o aplicativo saberá tudo sobre sua rotina e talvez possa compartilhá-la com criminosos. Além disso, um aplicativo defeituoso pode acidentalmente apagar todas as reuniões importantes do calendário.

CAMERA, acesso à câmera deixa o aplicativo usar seu celular para tirar fotos e gravar vídeos. Um app pode gravar vídeos secretamente ou tirar fotos a qualquer momento.

READ_CONTACTS/WRITE_CONTACTS, um aplicativo pode copiar toda sua agenda. Esses dados são altamente atrativos para spammers e falsários. Essa permissão também garante acesso a lista de todos os contatos usados em aplicativos no dispositivo – Google, Facebook, Instagram, e outros.

ACCESS_COARSE_LOCATION/ACCESS_FINE_LOCATION, baseada em dados GPS. Por que é perigoso: o aplicativo sabe onde você está o tempo inteiro. Pode por exemplo, permitir com que um ladrão entre na sua casa enquanto você está ausente.

RECORD_AUDIO, o aplicativo pode gravar tudo que está sendo dito próximo ao seu celular. Todas as conversas. Não apenas quando você fala ao telefone, mas o dia inteiro.