(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/android11&usg=ALkJrhhs8nKw3csOUu_Eut-M1lPPuR9Bvg)
em 3 de junho!

Definir uma permissão de aplicativo personalizado

Este documento descreve como os desenvolvedores de aplicativos podem usar os recursos de segurança fornecidos pelo Android para definir suas próprias permissões. Ao definir permissões personalizadas, um aplicativo pode compartilhar seus recursos e recursos com outros aplicativos. Para obter mais informações sobre permissões, consulte a Visão geral
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/permissions/requesting&usg=ALkJrhjGZq3i_VVNjAN5jr_keoe7FZIuZA)
das permissões
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/permissions/requesting&usg=ALkJrhjGZq3i_VVNjAN5jr_keoe7FZIuZA)
.

fundo

O Android é um sistema operacional separado por privilégios, no qual cada aplicativo é executado com uma identidade distinta do sistema (ID do usuário Linux e ID do grupo). Partes do sistema também são separadas em identidades distintas. Dessa forma, o Linux isola aplicativos um do outro e do sistema.

Os aplicativos podem expor sua funcionalidade a outros aplicativos, definindo as permissões que esses outros aplicativos podem solicitar. Eles também podem definir permissões que são disponibilizadas automaticamente para outros aplicativos assinados com o mesmo certificado.

Assinatura de aplicativo

Todos os APKs devem ser assinados com um certificado cuja chave privada seja mantida pelo desenvolvedor. Este certificado identifica o autor do aplicativo. O certificado *não* precisa ser assinado por uma autoridade de certificação; é perfeitamente permitido e típico que aplicativos Android usem certificados autoassinados. O objetivo dos certificados no Android é distinguir os autores do aplicativo. Isso permite que o sistema conceda ou negue aos aplicativos acesso a permissões no nível da assinatura
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA#plevel)
e conceda ou negue à solicitação de
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/manifest-element&usg=ALkJrhhPv1AKdzJBf66pl4VubAAKC8KELg#uid)
um aplicativo a mesma identidade Linux
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/manifest-element&usg=ALkJrhhPv1AKdzJBf66pl4VubAAKC8KELg#uid)
que outro aplicativo.

IDs de usuário e acesso a arquivos

No momento da instalação, o Android fornece a cada pacote um ID de usuário Linux distinto. A identidade permanece constante durante toda a vida útil do pacote nesse dispositivo. Em um dispositivo diferente, o mesmo pacote pode ter um

UID diferente; o que importa é que cada pacote tenha um UID distinto em um determinado dispositivo.

Como a imposição da segurança ocorre no nível do processo, o código de dois pacotes normalmente não pode ser executado no mesmo processo, pois eles precisam ser executados como usuários diferentes do Linux. Você pode usar o atributo sharedUserId (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/manifest-element&usg=ALkJrhhPv1AKdzJBf66pl4VubAAKC8KELg#uid) na tag de manifesto (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/manifest-element&usg=ALkJrhhPv1AKdzJBf66pl4VubAAKC8KELg) do `AndroidManifest.xml` de cada pacote para atribuir o mesmo ID de usuário. Ao fazer isso, por questões de segurança, os dois pacotes são tratados como sendo o mesmo aplicativo, com o mesmo ID de usuário e permissões de arquivo. Observe que, para manter a segurança, apenas dois aplicativos assinados com a mesma assinatura (e solicitando o mesmo sharedUserId) receberão o mesmo ID do usuário.

Todos os dados armazenados por um aplicativo receberão o ID do usuário desse aplicativo e normalmente não poderão ser acessados por outros pacotes.

Para mais informações sobre o modelo de segurança do Android, consulte Visão geral da segurança do Android (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://source.android.com/tech/security/index.html&usg=ALkJrhh-6qJkpb2nwQnVO3Rsj0mpEEoEHQ)

Definindo e aplicando permissões

Para impor suas próprias permissões, você deve primeiro declará-las no seu `AndroidManifest.xml` usando um ou mais elementos `<permission>` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA)
.

Por exemplo, um aplicativo que deseja controlar quem pode iniciar uma de suas atividades pode declarar uma permissão para esta operação da seguinte maneira:

```
<manifest
  xmlns:android="http://schemas.android.com/apk/res/android"
  package="com.example.myapp" >

    <permission
      android:name="com.example.myapp.permission.DEADLY_ACTIVITY"
      android:label="@string/permlab_deadlyActivity"
      android:description="@string/permdesc_deadlyActivity"
      android:permissionGroup="android.permission-group.COST_MONEY"
      android:protectionLevel="dangerous" />
    ...
</manifest>
```

Nota: O sistema não permite que vários pacotes declarem uma permissão com o mesmo nome, a menos que todos os pacotes sejam assinados com o mesmo certificado. Se um pacote declarar uma permissão, o sistema não permitirá que o usuário instale outros pacotes com o mesmo nome de permissão, a menos que esses pacotes sejam assinados com o mesmo certificado que o primeiro pacote. Para evitar colisões de nomes, recomendamos o uso de nomes no estilo de domínio reverso para permissões personalizadas, por exemplo `com.example.myapp.ENGAGE_HYPERSPACE` .

O atributo `protectionLevel` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA#plevel) é necessário, informando ao sistema como o usuário deve ser informado sobre aplicativos que exigem a permissão ou quem tem permissão para detê-la, conforme descrito na documentação vinculada.

O atributo `android:permissionGroup` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-group-element&usg=ALkJrhjLXjraroxitzEhsUH4i2iSF_Vgbg) é opcional e usado apenas para ajudar o sistema a exibir permissões para o usuário. Na maioria dos casos, você deve configurá-lo como um grupo de sistema padrão (listado em `android.Manifest.permission_group` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/reference/android/Manifest.permission_group&usg=ALkJrhhCILAuAzO_GeEcVCUrbCfFZVXZkg)), embora você mesmo possa definir um grupo (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/permissions/defining.html&usg=ALkJrhh6YD8_hTcseNJNxdpjN7P8LV4Q7Q#groups). É preferível usar um grupo existente, pois isso simplifica a interface do usuário de permissão mostrada ao usuário.

Você precisa fornecer um rótulo e uma descrição para a permissão. Esses são recursos de sequência que o usuário pode ver quando está visualizando uma lista de permissões (`android:label` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA#label)) ou detalhes em uma única permissão (`android:description` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA#desc)). O rótulo deve ser curto; algumas palavras que descrevem a parte principal da funcionalidade que a permissão está protegendo. A descrição deve conter algumas frases descrevendo o que a permissão permite que um detentor faça. Nossa convenção é uma descrição de duas frases: a primeira frase descreve a permissão e a segunda frase avisa o usuário sobre o tipo de coisas que podem dar errado se um aplicativo receber a permissão.

Aqui está um exemplo de rótulo e descrição para a permissão `CALL_PHONE` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/reference/android/Manifest.permission&usg=ALkJrhgKfYoGw1W6kyJpC7zVBeKhlcmUMw#CALL_PHONE):

```
<string name="permlab_callPhone">directly call phone numbers</string>
<string name="permdesc_callPhone">Allows the app to call
    phone numbers without your intervention. Malicious apps may
    cause unexpected calls on your phone bill. Note that this does not
    allow the app to call emergency numbers.</string>
```

Crie um grupo de permissões

Conforme mostrado na seção anterior, você pode usar o atributo `android:permissionGroup` (https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-group-element&usg=ALkJrhjLXjraroxitzEhsUH4i2iSF_Vgbg) para ajudar o sistema a descrever permissões para o usuário. Na maioria dos casos, você deseja definir isso como um grupo de sistema padrão (listado em `android.Manifest.permission_group`

(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/reference/android/Manifest.permission_group&usg=ALkJrhhCILAuAzO_GeEcVCUrbCfFZVXZkg)
), mas também pode definir seu próprio grupo com `<permission-group>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-group-element&usg=ALkJrhjLXjraroxitzEhsUH4i2iSF_Vgbg)
.

O elemento `<permission-group>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-group-element&usg=ALkJrhjLXjraroxitzEhsUH4i2iSF_Vgbg)
define um rótulo para um conjunto de permissões - aqueles declarados no manifesto com elementos `<permission>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA)
e os declarados em outro lugar. Isso afeta apenas como as permissões são agrupadas quando apresentadas ao usuário.
O elemento `<permission-group>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-group-element&usg=ALkJrhjLXjraroxitzEhsUH4i2iSF_Vgbg)
não especifica as permissões que pertencem ao grupo, mas fornece um nome ao grupo.

Você pode colocar uma permissão no grupo atribuindo o nome do grupo ao atributo `permissionGroup`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA#pgroup)
do elemento `<permission>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-element&usg=ALkJrhj4ac6ukVp6YOicCg7CSg7n-3a1ZA)
.

O elemento `<permission-tree>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/permission-tree-element&usg=ALkJrhgjBB6PyP-Lu2EAsqziaMrqpMsNwQ)
declara um espaço para nome para um grupo de permissões definidas no código.

Recomendações de permissão personalizadas

Os aplicativos podem definir suas próprias permissões personalizadas e solicitar permissões personalizadas de outros aplicativos, definindo os elementos `<uses-permission>`
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/uses-permission-element&usg=ALkJrhj4l1f3G2cvKvDa3m_qHF3GFh37iw)
. No entanto, você deve avaliar cuidadosamente se é necessário que seu aplicativo faça isso.

- Se você estiver projetando um conjunto de aplicativos que expõem funcionalidade um ao outro, tente projetar os aplicativos para que cada permissão seja definida apenas uma vez. Você deve fazer isso se os aplicativos não estiverem todos assinados com o mesmo certificado. Mesmo que todos os aplicativos sejam assinados com o mesmo certificado, é uma prática recomendada definir cada permissão apenas uma vez.
- Se a funcionalidade estiver disponível apenas para aplicativos assinados com a mesma assinatura que o aplicativo fornecido, você poderá evitar definir permissões personalizadas usando verificações de assinatura. Quando um de seus aplicativos faz uma solicitação para outro, o segundo aplicativo pode verificar se os dois aplicativos estão assinados com o mesmo certificado antes de atender à solicitação.

Continue lendo sobre:

<uses-permission>
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://developer.android.com/guide/topics/manifest/uses-permission-element&usg=ALkJrhj4l1f3G2cvKvDa3m_qHF3GFh37iw)

Referência da API para a tag de manifesto que declara as permissões de sistema necessárias do seu aplicativo.

Você também pode estar interessado em:

Visão geral da segurança do Android
(https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-BR&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://source.android.com/devices/tech/security/index.html&usg=ALkJrhhsyaEVCZQSwNUcgpsz775yRnzsIA)

Uma discussão detalhada sobre o modelo de segurança da plataforma Android.

Anterior
← Permissões usadas apenas em manipuladores padrão