
Google™
11
I/O

Taking Android to Work

#io2011 #Android

Gabe Cohen
Andy Stadler
Fred Chung @fredchung

Realtime Feedback: goo.gl/vdhGp

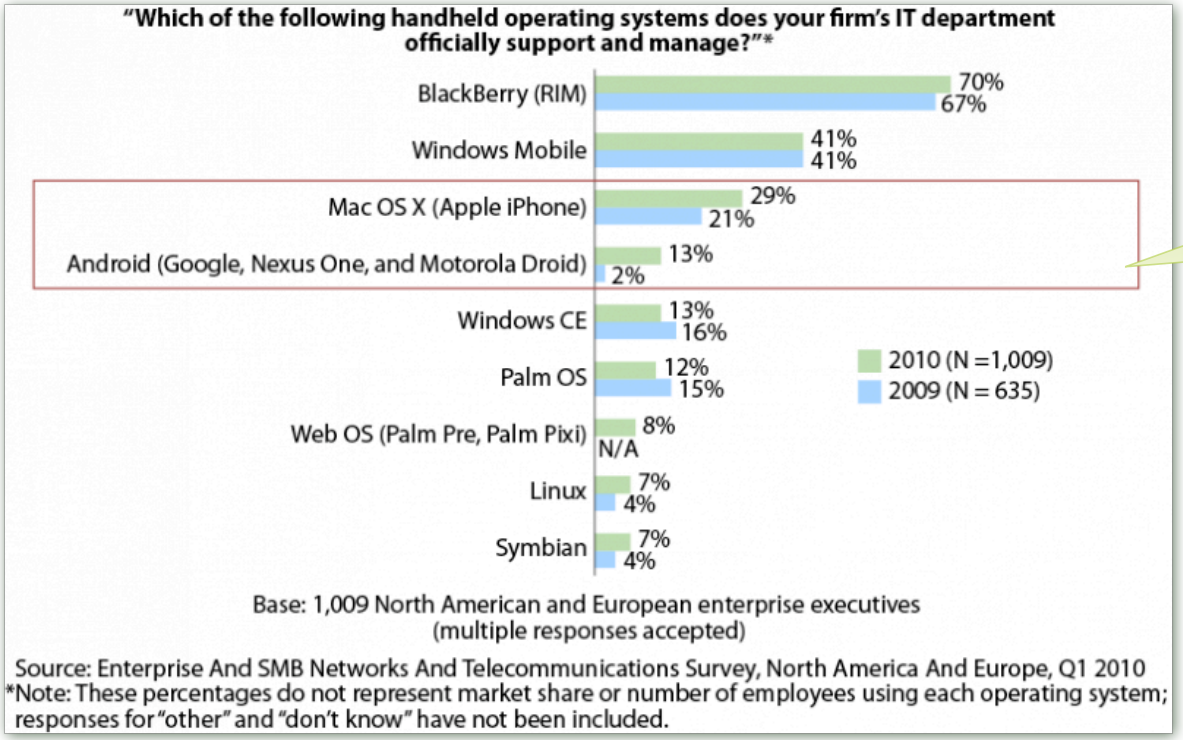
Questions: goo.gl/mod/uCeK

Android is Growing Fast

- 310+ devices, 215 Carriers, 96 countries, 400K daily activations

Android is Growing Fast...

at the workplace, too



Workplace acceptance of Android has gone from **2% in 2009** to **13% in 2010**

4 Source: http://blogs.forrester.com/reineke_reitsma/11-01-07-the_data_digest_which_mobile_operating_systems_do_enterprises_support

Who Wants to Carry Multiple Devices?

The CIO Perspective

iStockphoto®, ©RichVintage, Nerd Herd

6

The CIO Perspective

Security

iStockphoto®, ©RichVintage, Nerd Herd

6

The CIO Perspective

6

The CIO Perspective

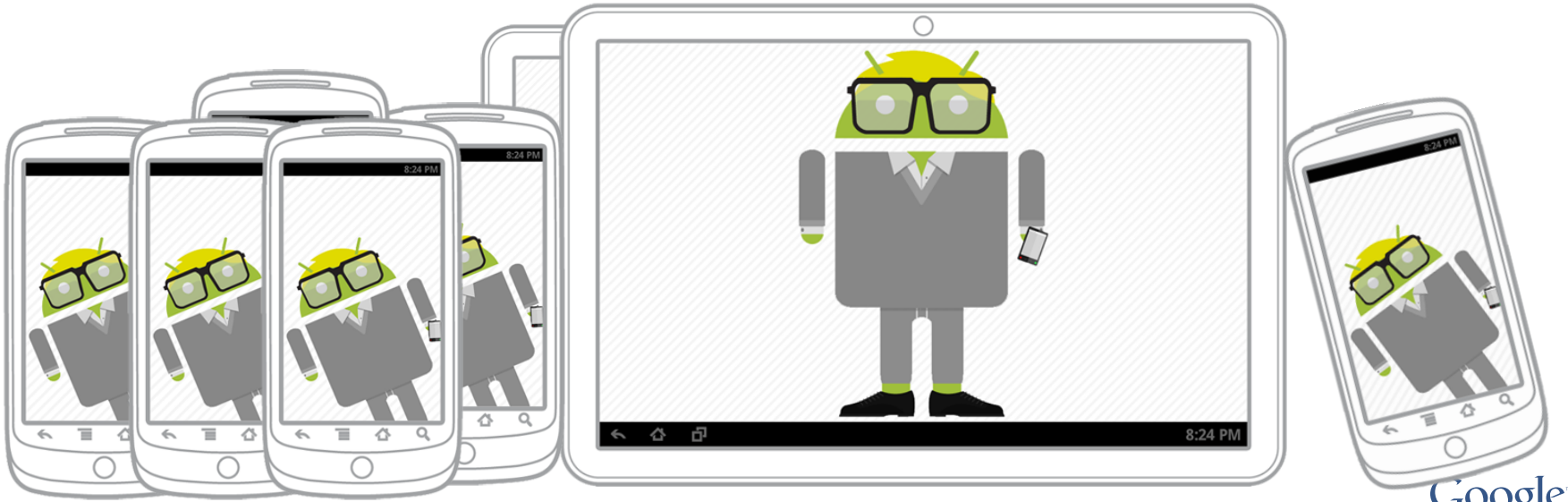
6

Data Security

- Protect against loss or theft
- Protect against interception
- Employees are the weak link
- Enforcement & crypto are key

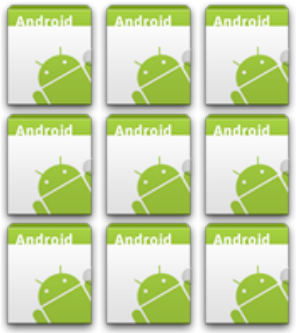
Device Management

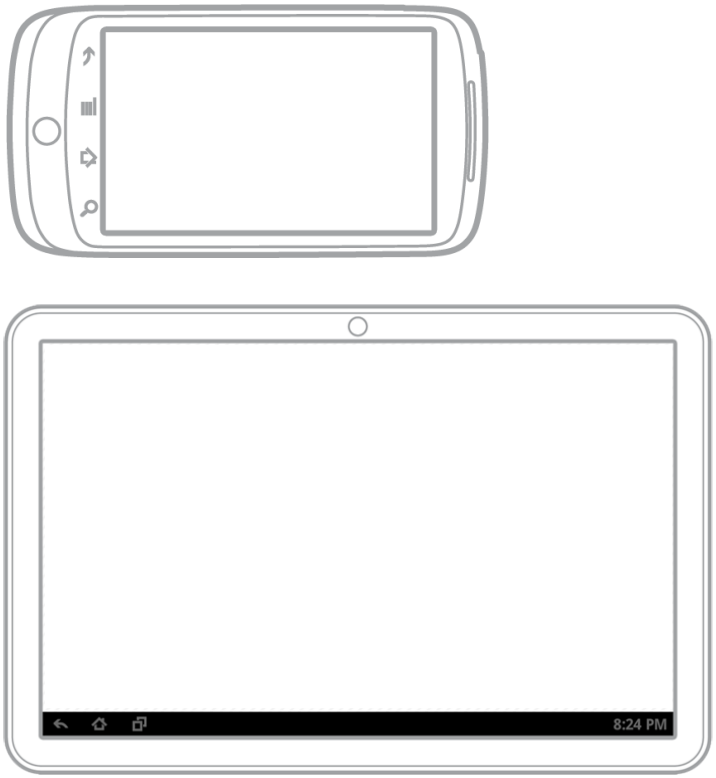
- Onboard the users
- Set up security and usage policies
- Supporting users
- Keep tabs on deployed devices



App Deployment & Management

- Determine key mobile apps
- Buy or Build
- Distribute apps to devices
- Manage updates
- Set app usage policies



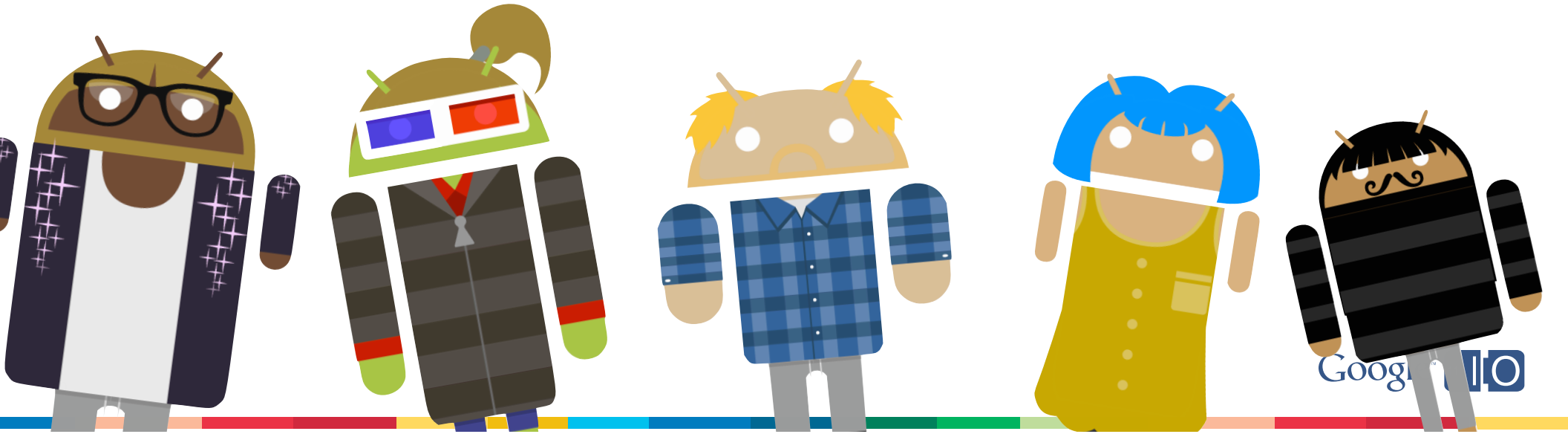


App Deployment & Management

- Determine key mobile apps
- Buy or Build
- Distribute apps to devices
- Manage updates
- Set app usage policies

Android's Approach

- Users come first
- Enterprise money is real
- Unlock dual use devices for our users
- Keep it open and let the ecosystem run



More Android Enterprise Support

Baked into every platform release

11

More Android Enterprise Support

Baked into every platform release

- Secure Wi-Fi
- VPN Support
- Exchange email and contacts
- Multiple overlay for email and contacts

- Password Lock
- PIN Support
- Device Policy Management 1.0
- Remote Lock API
- Remote Wipe API
- Screen Lock API
- Global Address List
- EAS Policy Support
- Exchange account auto-discovery
- Exchange calendar

- Calendar and event time zones
- Gmail Priority Inbox
- Gmail inline reply
- SIP calling support
- NFC Platform support for read, write, P2P

- More security: encryption, password rules
- Increased Exchange policy support
- Improved Email features
- Enhanced calendar features

Device Policy Management

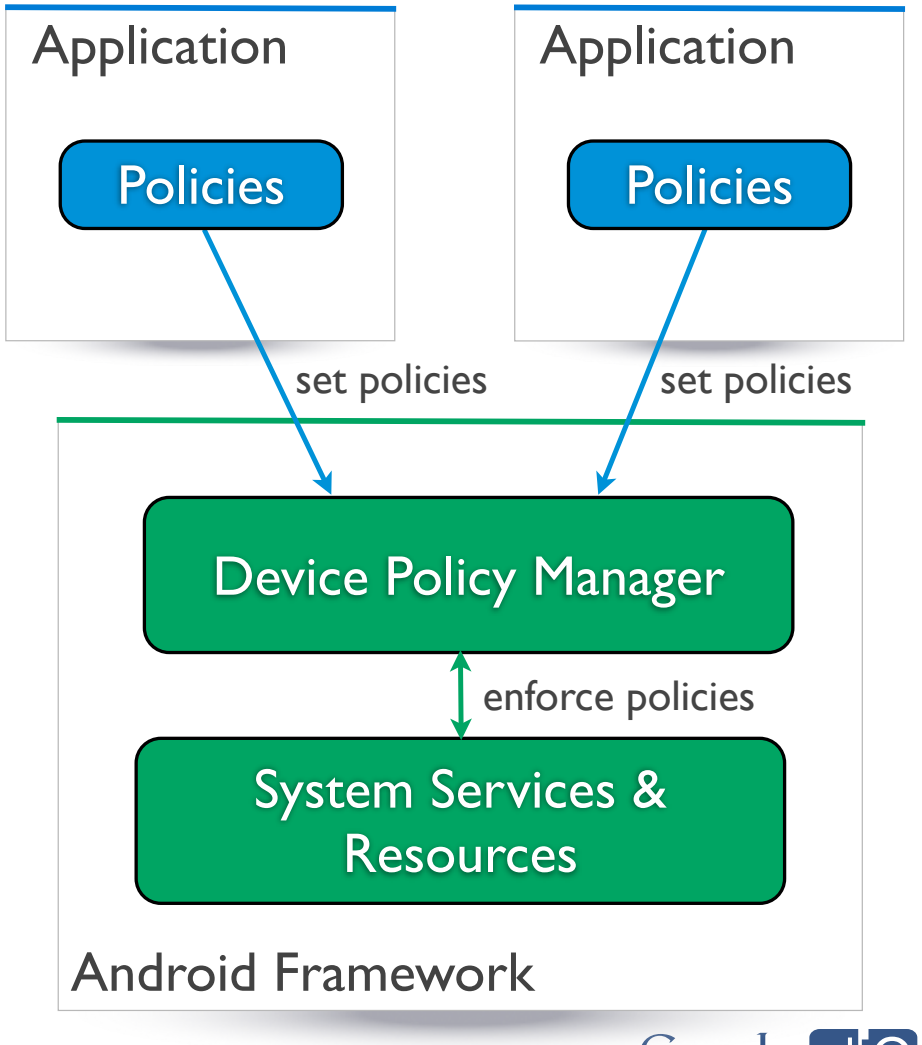
Policy Management Applications

Examples

- Account-Based fleet management
  - Google Apps Device Policy For Android
  - Microsoft Exchange ActiveSync
- Apps that manage or present secure data
  - Password locker
  - Confidential data lookup
- Apps that provide device security services
  - Find My Lost Device And Wipe It

Device Policy Management

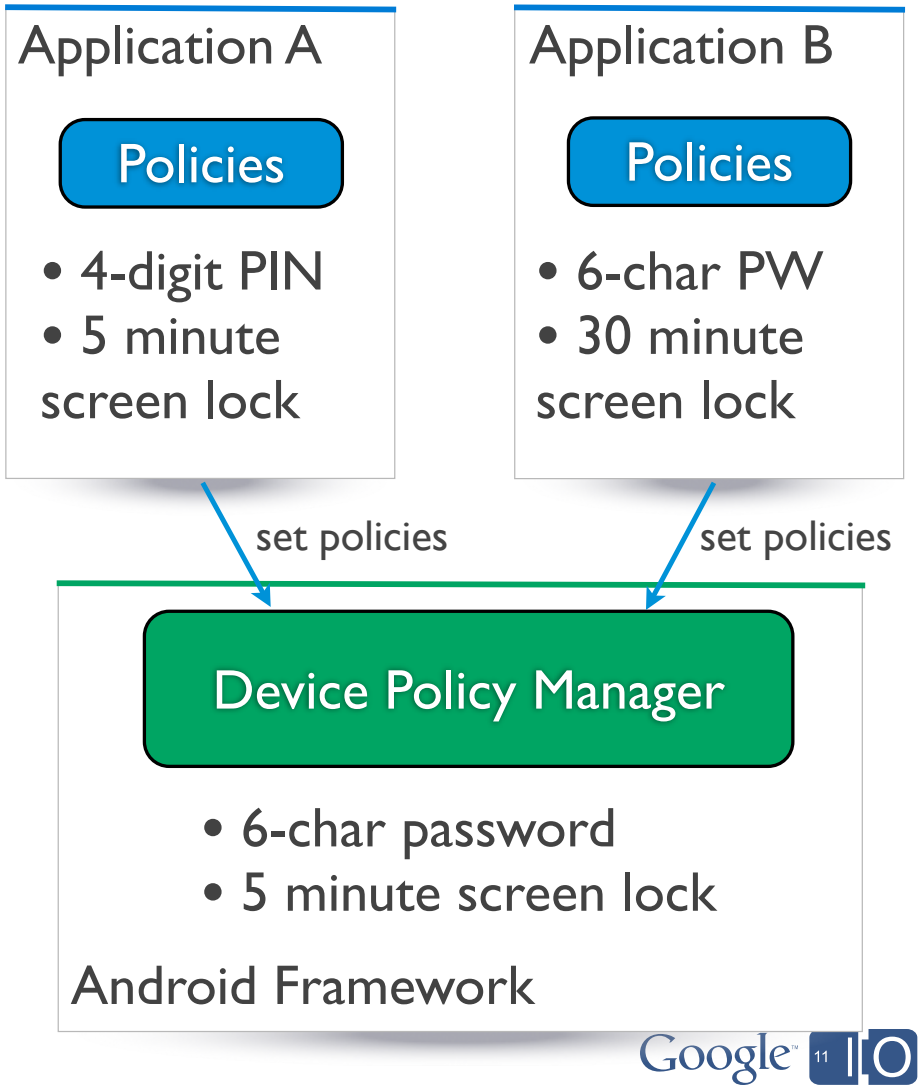
- The Android framework defines a set of policies around device security features
- Android applications use these policies to monitor & control device security
- Applications do this via the Device Policy Manager
  - An open API (available to any app)
  - Multiple applications can enforce security policies
  - Available since Froyo and continuously improved - each major release adds new policies to the list



14

Policies Always Increase Security

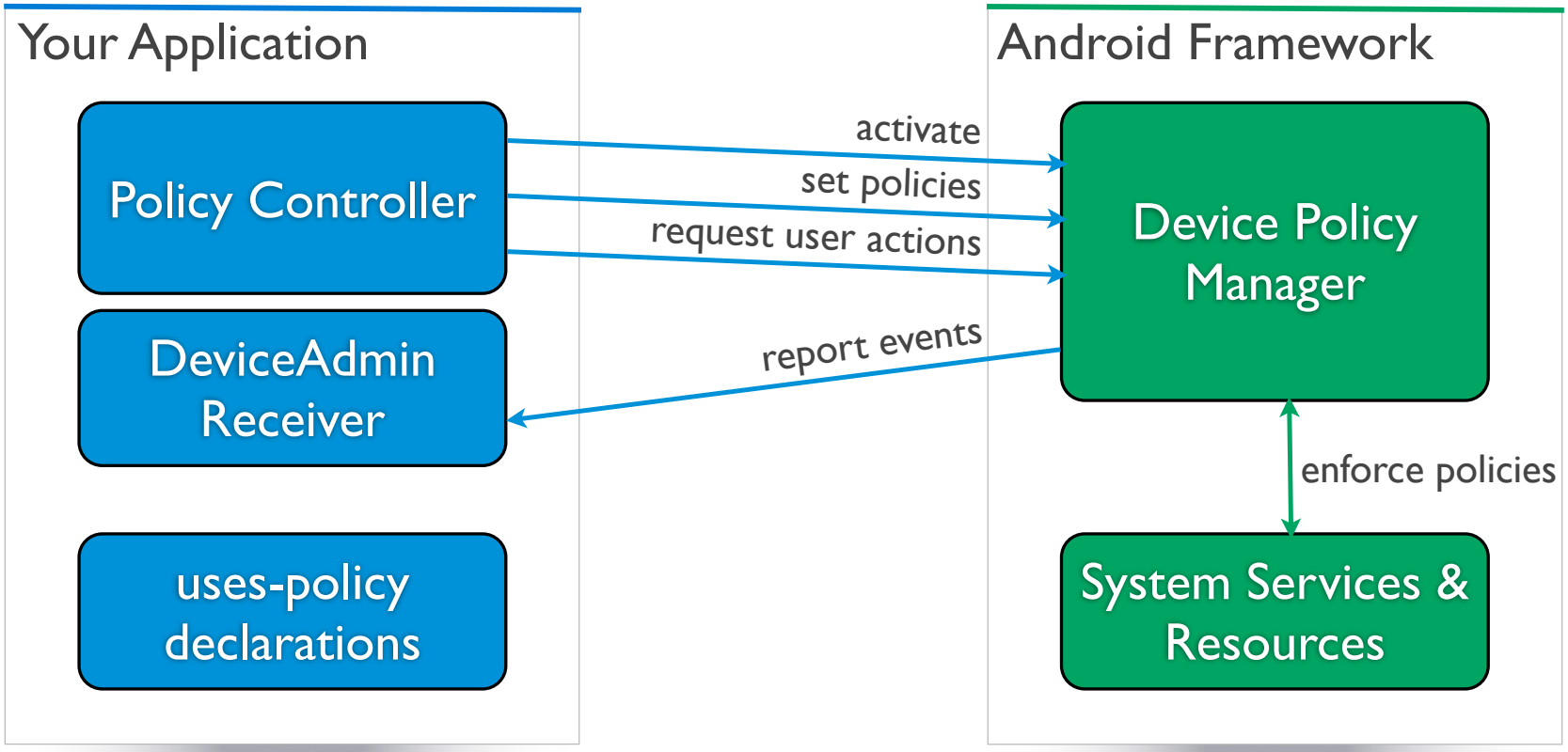
- More than one application can enforce policies
- For each policy, the strongest option is selected
- No application can reduce security



15

Policy Management Applications

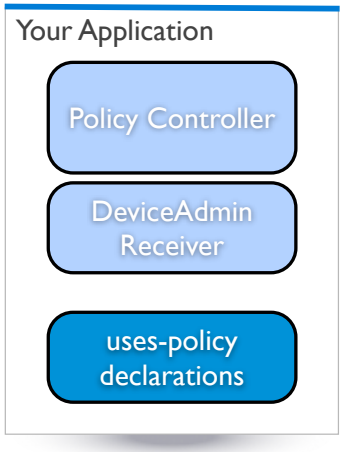
Required Elements - How It Works



Policy Management Applications

Required Elements - Policy Declarations

- An explicit list of policies that will be enforced by this application
- Stored as meta-data, referenced from application's manifest



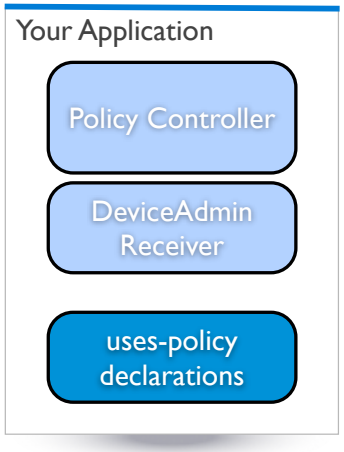

```
<device-admin
    xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-policies>
        <limit-password />
        <force-lock />
        <wipe-data />
        <expire-password />
        <encrypted-storage />
    </uses-policies>
</device-admin>
```


Google I/O 11

Policy Management Applications

Required Elements - Policy Declarations

- An explicit list of policies that will be enforced by this application
- Stored as meta-data, referenced from application's manifest



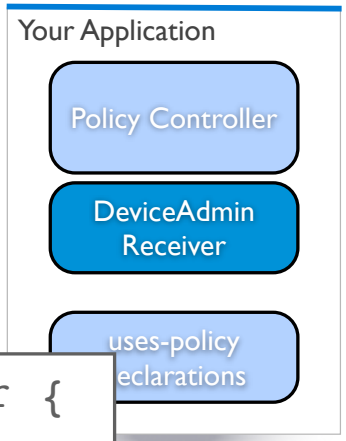

```
<device-admin
    xmlns:android="http://schemas.a
    <uses-policies>
        <limit-password />
        <force-lock />
        <wipe-data />
        <expire-password />
        <encrypted-storage />
    </uses-policies>
</device-admin>
```

```
public void setPasswordQuality(...)
public void setPasswordMinimumLength(...)
public void setPasswordMinimumNumeric(...)
public void setPasswordMinimumSymbols(...)
public void setPasswordHistoryLength(...)
etc.
```


18

Policy Management Applications

Required Elements - DeviceAdminReceiver



- Receives notifications of policy-related status changes

```
public static class PolicyAdmin extends DeviceAdminReceiver {

    @Override
    public void onDisabled(Context context, Intent intent) {
        BroadcastProcessorService.onDevicePolicyMessage(
            context,
            DEVICE_ADMIN_MESSAGE_DISABLED);
    }
}
```

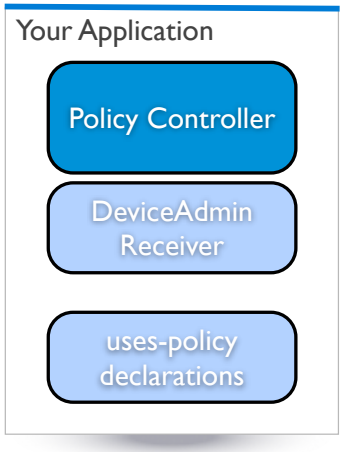
- *WARNING: Notifications are broadcasts on the UI thread. Recommend using an IntentService to handle them.*

Google I/O 11

Policy Management Applications

Required Elements - PolicyController

- Activate: First, check if already active...

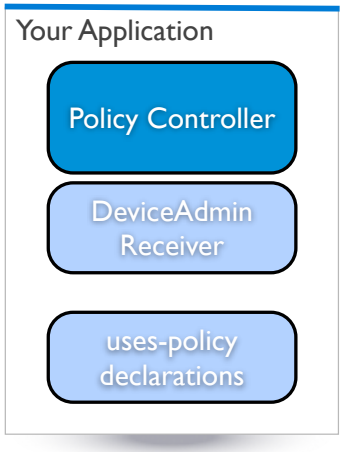



```
DevicePolicyManager getDpm() {
    return (DevicePolicyManager)
        mContext.getSystemService(Context.DEVICE_POLICY_SERVICE);
}

boolean isActive() {
    return getDpm().isAdminActive(myAdminReceiver);
```

Policy Management Applications

Required Elements - PolicyController

- Activate: If not already active, obtain user permission to assert policies...



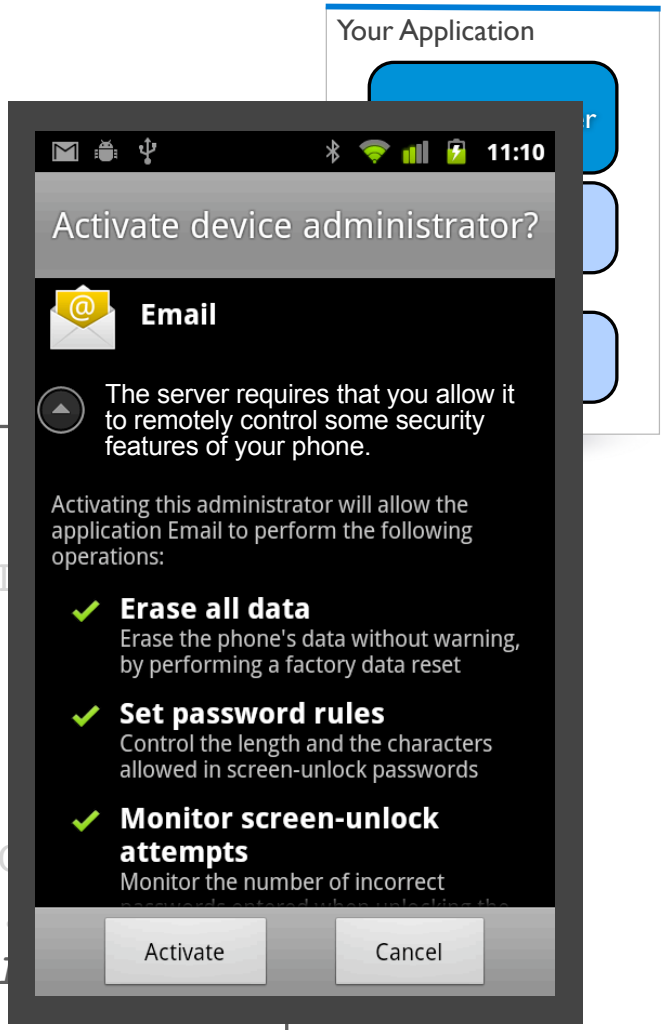

```
void activate() {
    Intent intent = new Intent(
        DevicePolicyManager.ACTION_ADD_DEVICE_ADMIN);
    intent.putExtra(
        DevicePolicyManager.EXTRA_DEVICE_ADMIN,
        myAdminReceiver);
    intent.putExtra(
        DevicePolicyManager.EXTRA_ADD_EXPLANATION,
        "The server requires that you allow it...");
    startActivityForResult(intent, REQUEST_ENABLE);
}
```

Policy Management Applications

Required Elements - PolicyController

- Activate: If not already active, obtain user permission to assert policies...

```
void activate() {
    Intent intent = new Intent(
        DevicePolicyManager.ACTION_ADD_DEVICE_AD
    intent.putExtra(
        DevicePolicyManager.EXTRA_DEVICE_ADMIN,
        myAdminReceiver);
    intent.putExtra(
        DevicePolicyManager.EXTRA_ADD_EXPLANATIO
        "The server requires that you allow it.
    startActivityForResult(intent, REQUEST_ENABL
}
```

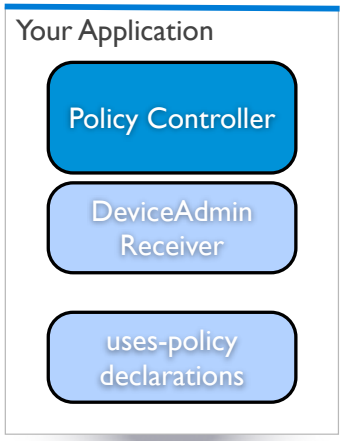


22

Policy Management Applications

Required Elements - PolicyController

- Policies: Next, check if required policies are satisfied...

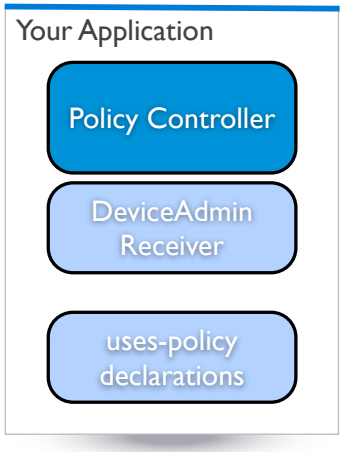



```
boolean arePoliciesSatisfied() {
    DevicePolicyManager dpm = getDpm();

    dpm.setPasswordQuality(myAdminReceiver,
        DevicePolicyManager.PASSWORD_QUALITY_NUMERIC);

    return dpm.isActivePasswordSufficient();
}
```

Policy Management Applications

Required Elements - PolicyController

- Policies: If policies not satisfied, set policies, and request user action...




```
void setPolicies() {
    DevicePolicyManager dpm = getDpm();

    dpm.setPasswordQuality(myAdminReceiver,
        DevicePolicyManager.PASSWORD_QUALITY_NUMERIC);

    if (!arePoliciesSatisfied()) {
        Intent intent = new Intent(
            DevicePolicyManager.ACTION_SET_NEW_PASSWORD);
        startActivity(intent);
    }
}
```

Policy Management Applications

Required Elements - PolicyController

- Policies: If policies not satisfied, set policies, and request user action...

```
void setPolicies() {
    DevicePolicyManager dpm = getDpm();

    dpm.setPasswordQuality(myAdminReceiver,
        DevicePolicyManager.PASSWORD_QUALITY_NUMERIC)

    if (!arePoliciesSatisfied()) {
        Intent intent = new Intent(
            DevicePolicyManager.ACTION_SET_NEW_PASSWO
        startActivity(intent);
    }
}
```

25

Policy Management Applications

Notes about application structure and business logic

Policy Management Applications

Notes about application structure and business logic

- User intervention is required to “bootstrap” a device into a fully-configured, secure configuration
  - Allow partial progress, and restarts
  - Use notifications & dialogs when restarting the security flow - tell the user what’s happening

27

Policy Management Applications

Notes about application structure and business logic

- User intervention is required to “bootstrap” a device into a fully-configured, secure configuration
  - Allow partial progress, and restarts
  - Use notifications & dialogs when restarting the security flow - tell the user what’s happening
- Consider your business logic / security rules when there are setbacks such as password expiration. In increasing order of strictness:
  - Prevent access to your app or your data
  - Delete your app’s sensitive data from the device
  - Wipe the device completely

Policy Management Applications

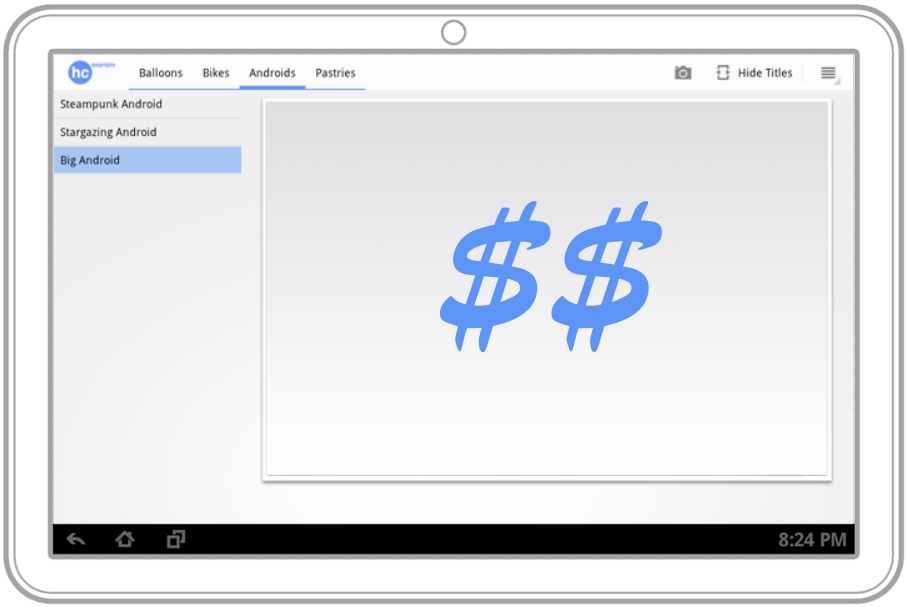
Notes about application structure and business logic

- User intervention is required to “bootstrap” a device into a fully-configured, secure configuration
  - Allow partial progress, and restarts
  - Use notifications & dialogs when restarting the security flow - tell the user what’s happening
- Consider your business logic / security rules when there are setbacks such as password expiration. In increasing order of strictness:
  - Prevent access to your app or your data
  - Delete your app’s sensitive data from the device
  - Wipe the device completely
- If mixing policies from multiple sources, apply principle of increasing security.

29

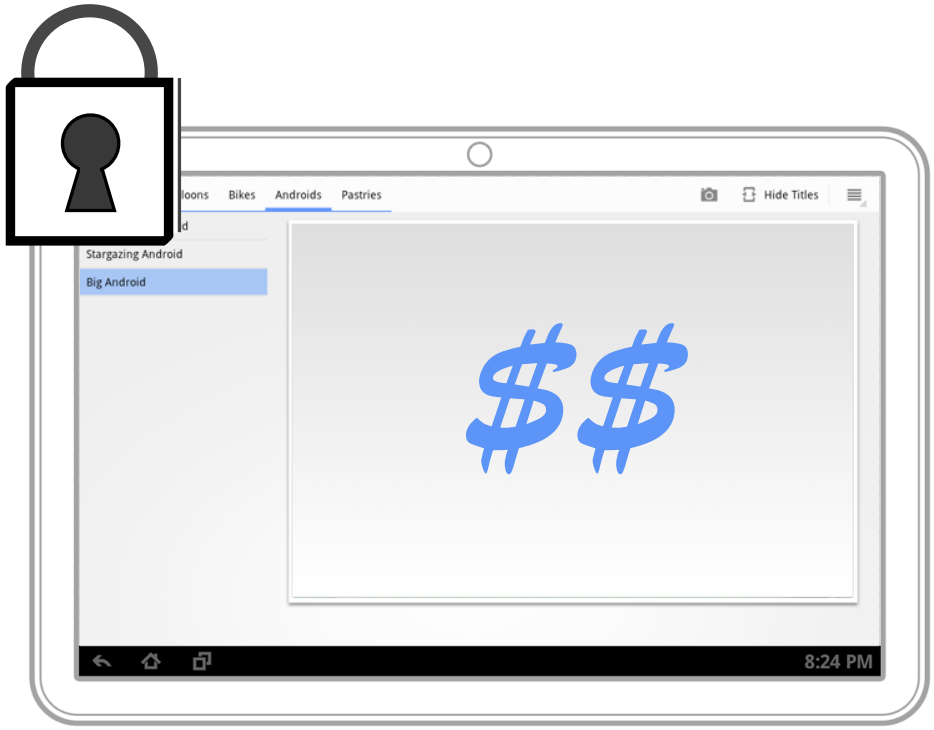
Demo

Demo


Balloons
Bikes
Androids
Pastries
Hide Titles
Steampunk Android
Stargazing Android
Big Android
$$
8:24 PM

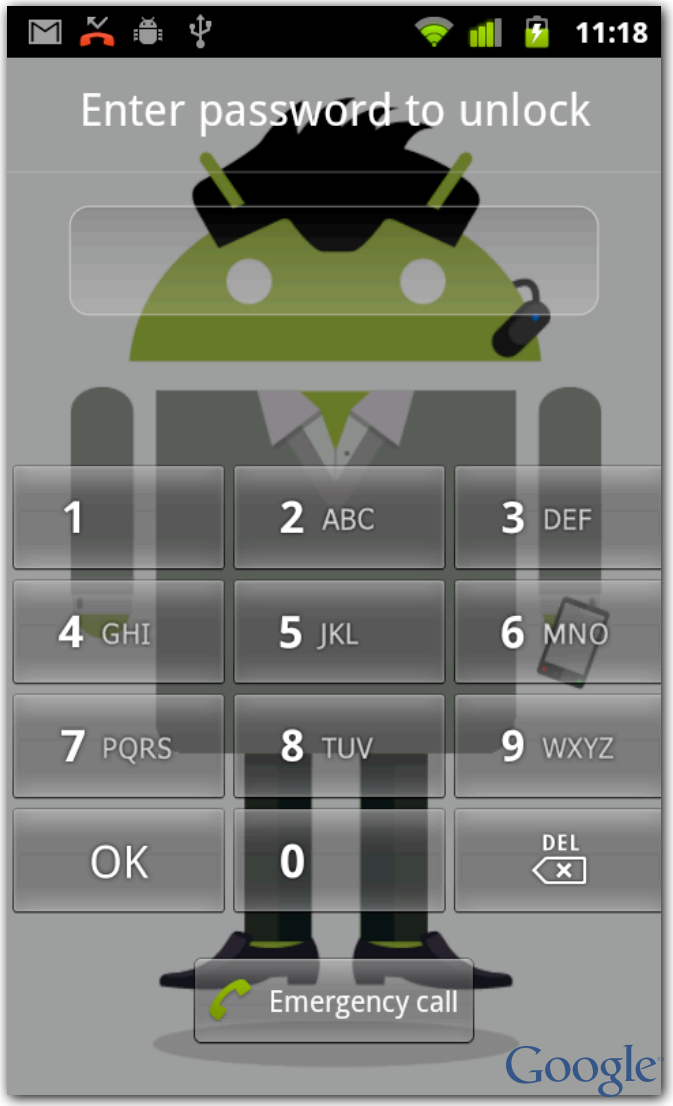
31

Demo


Bikes
Androids
Pastries
Hide Titles
Stargazing Android
Big Android
$$
8:24 PM

31

Screen-Lock Password, Anyone?

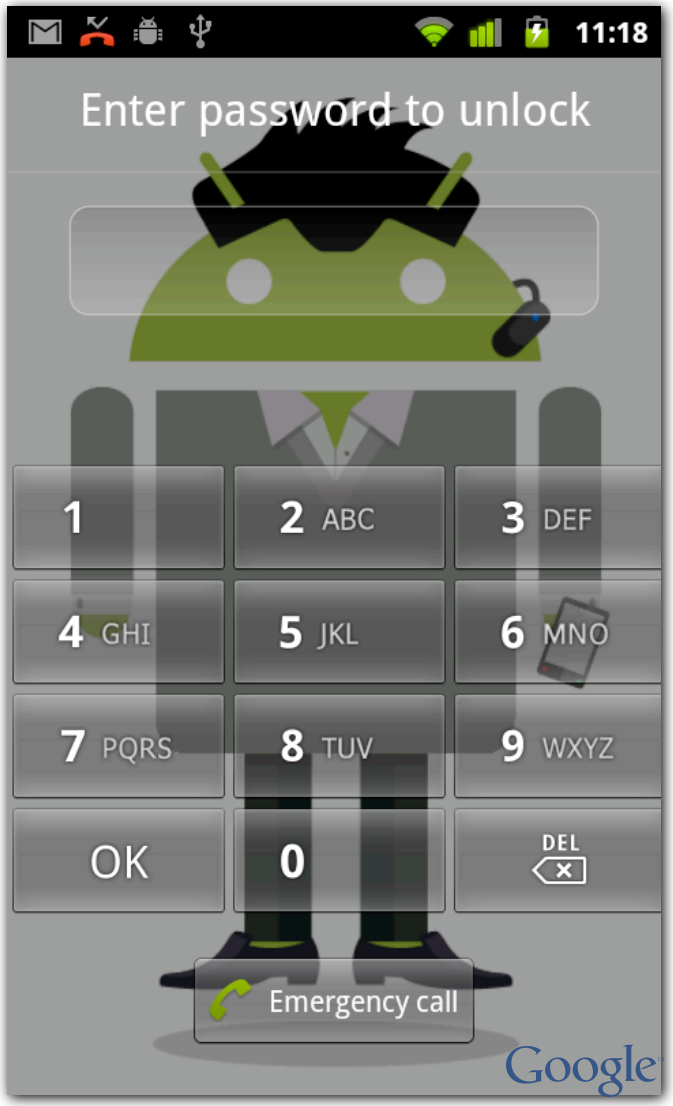


32

Screen-Lock Password, Anyone?

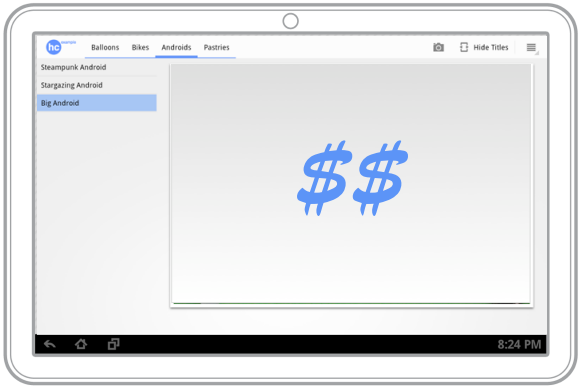
54% of smartphone users don't have a screen-lock password...

- Based on a survey conducted by Symantec

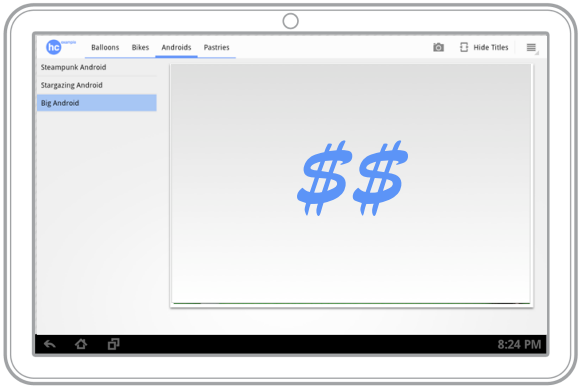


32

Device Management Demo for Android



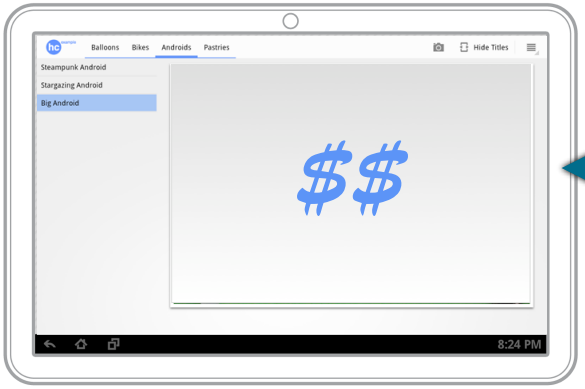
Device Management Demo for Android



Security policy:
pw type
pw quality...

33

Device Management Demo for Android



Security policy:
pw type
pw quality...

Source code available at:

goo.gl/tBwO4

http://code.google.com/p/device-management-demo-for-android

Internal App Distribution

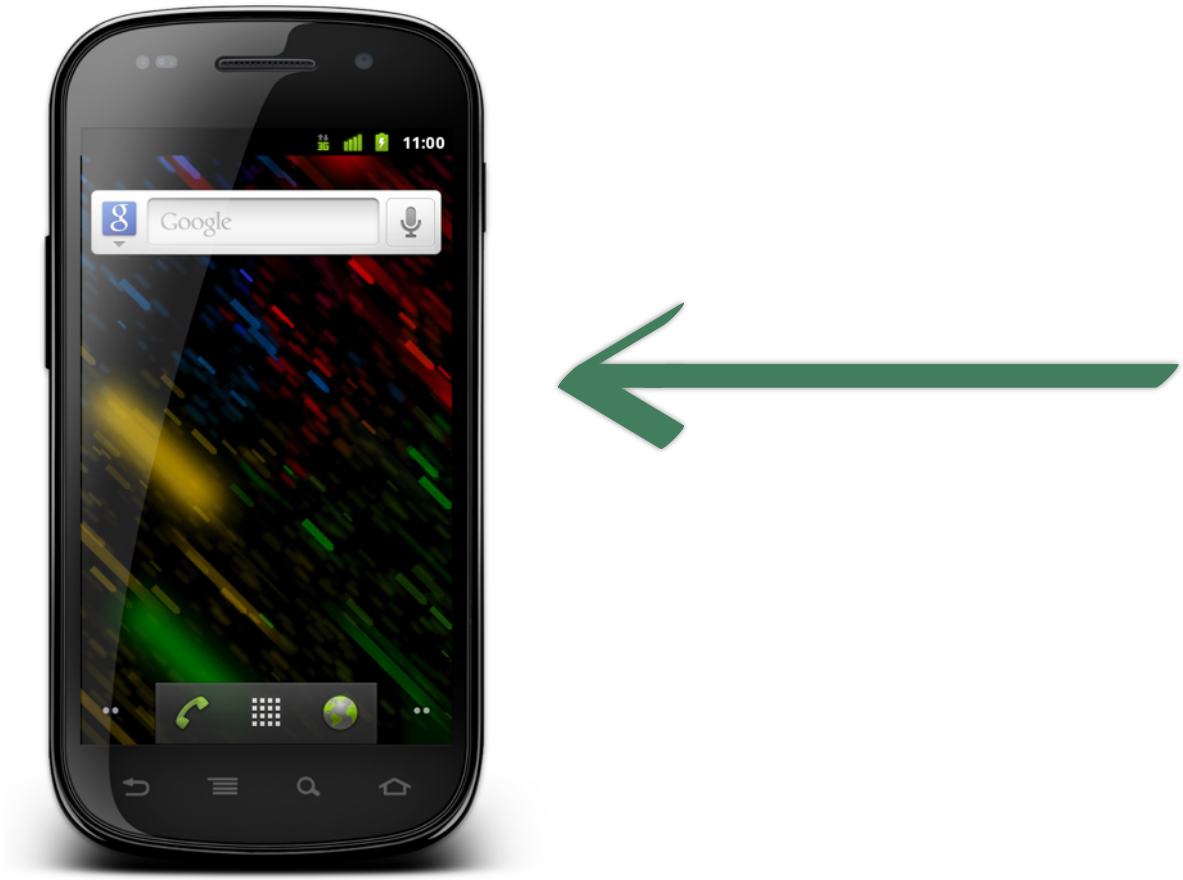
What about Android Market?

36

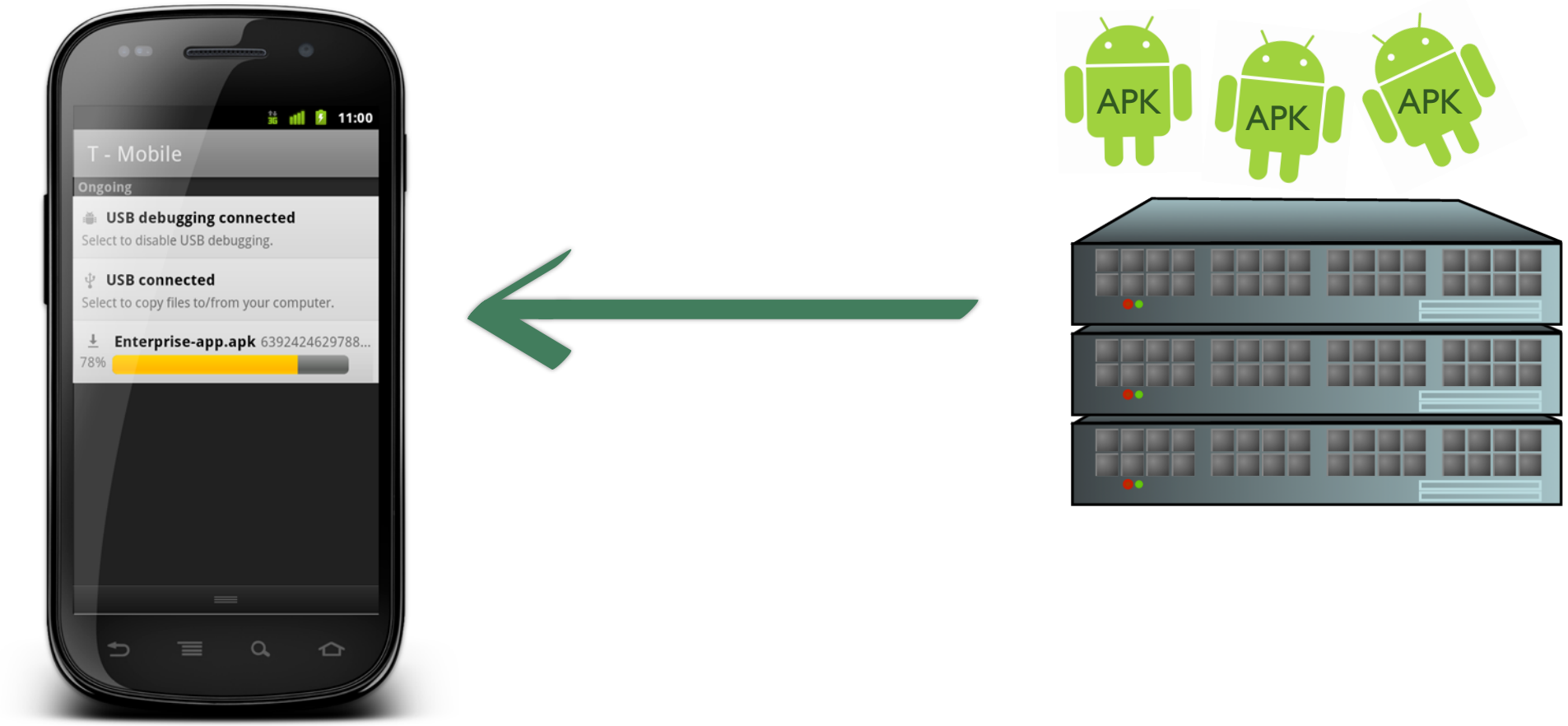
What about Android Market?

http://market.android.com?details=PACKAGE_NAME

Side-Loading



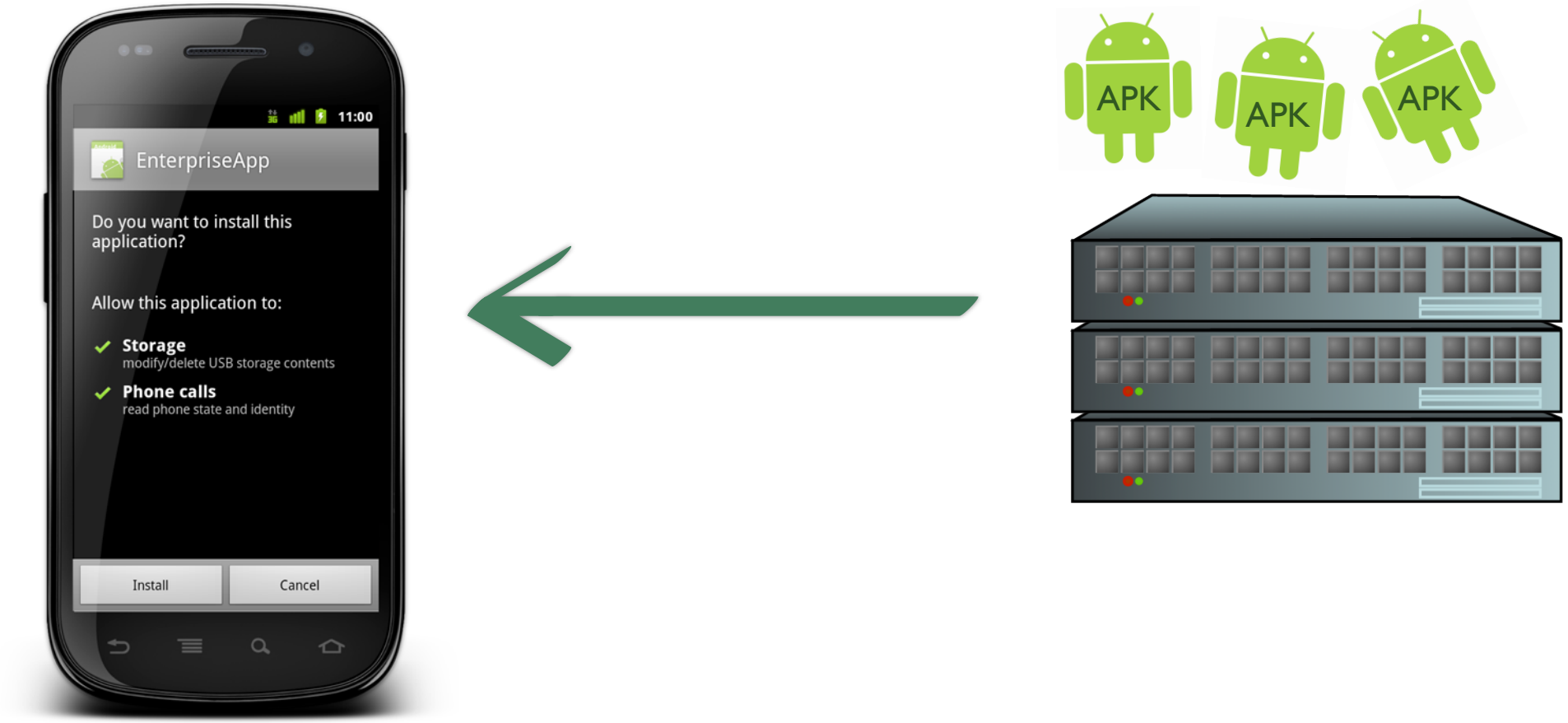
Side-Loading



Google I/O 11

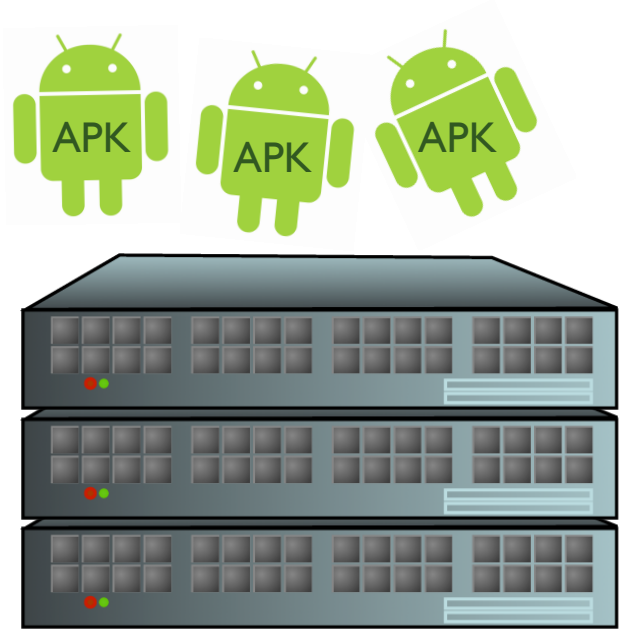
37

Side-Loading



37

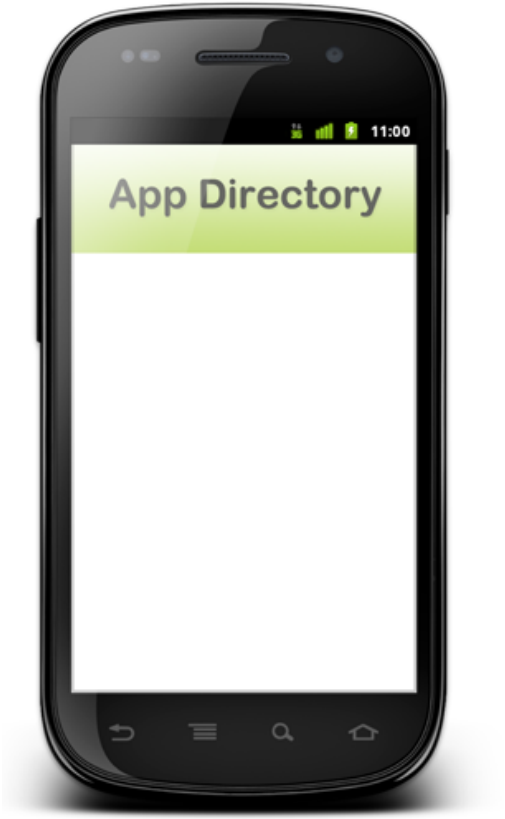
Side-Loading



37

Internal App Directory

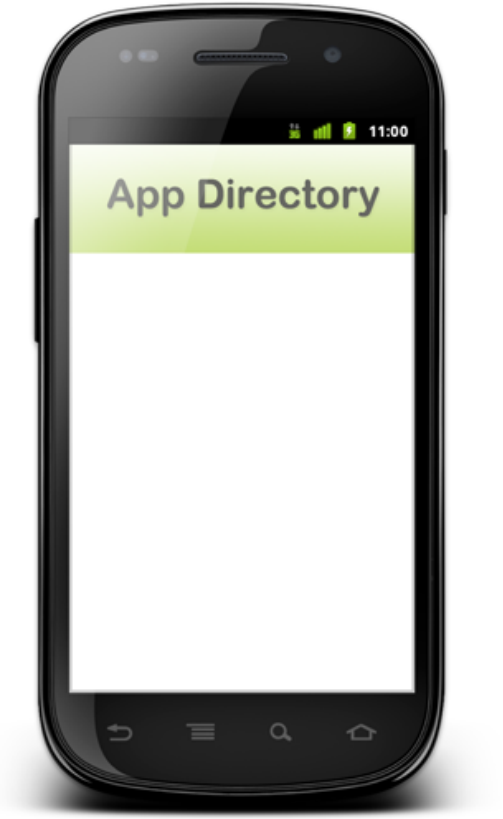
Overview

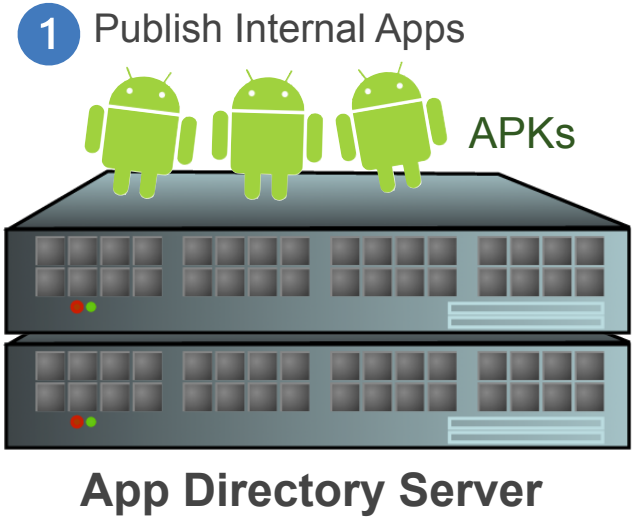


App Directory Server

Internal App Directory

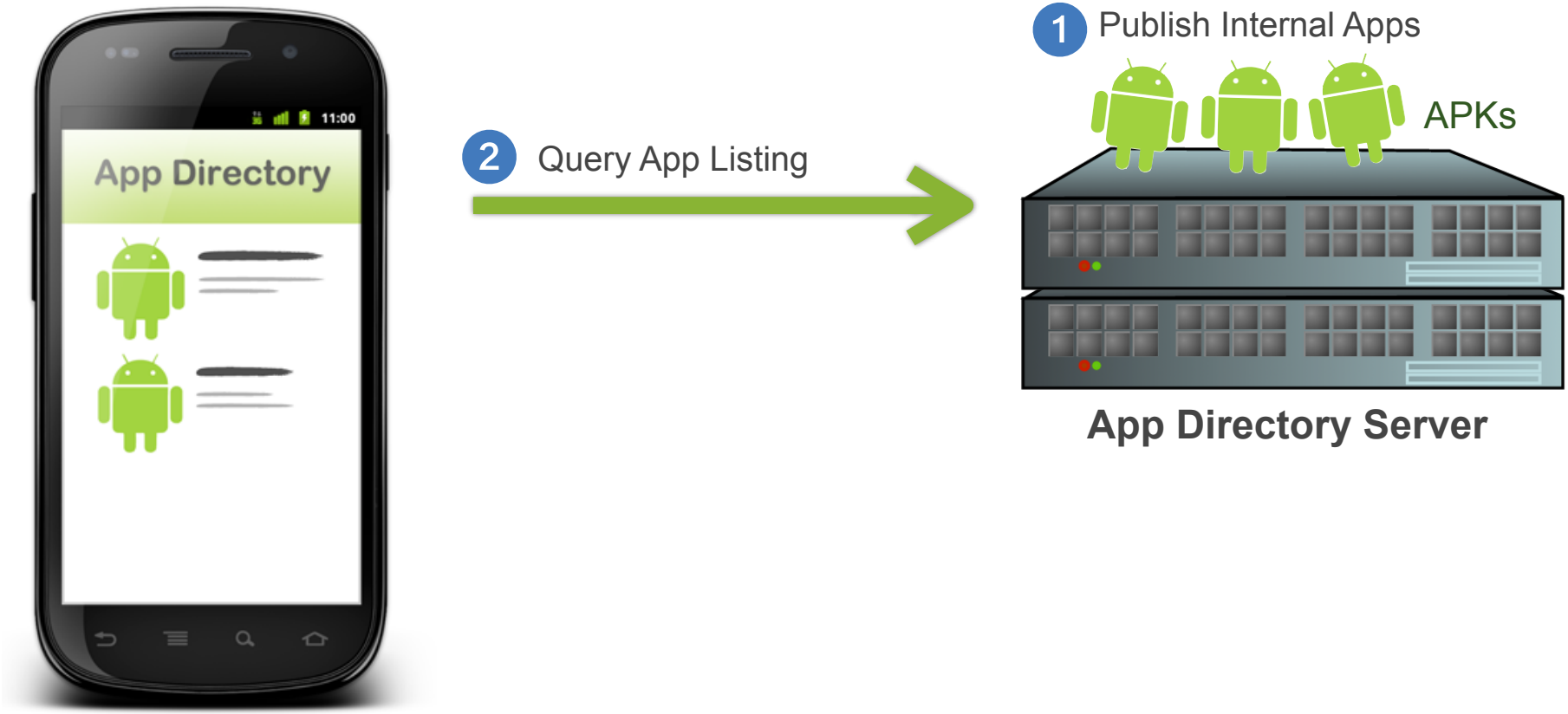
Overview





Internal App Directory

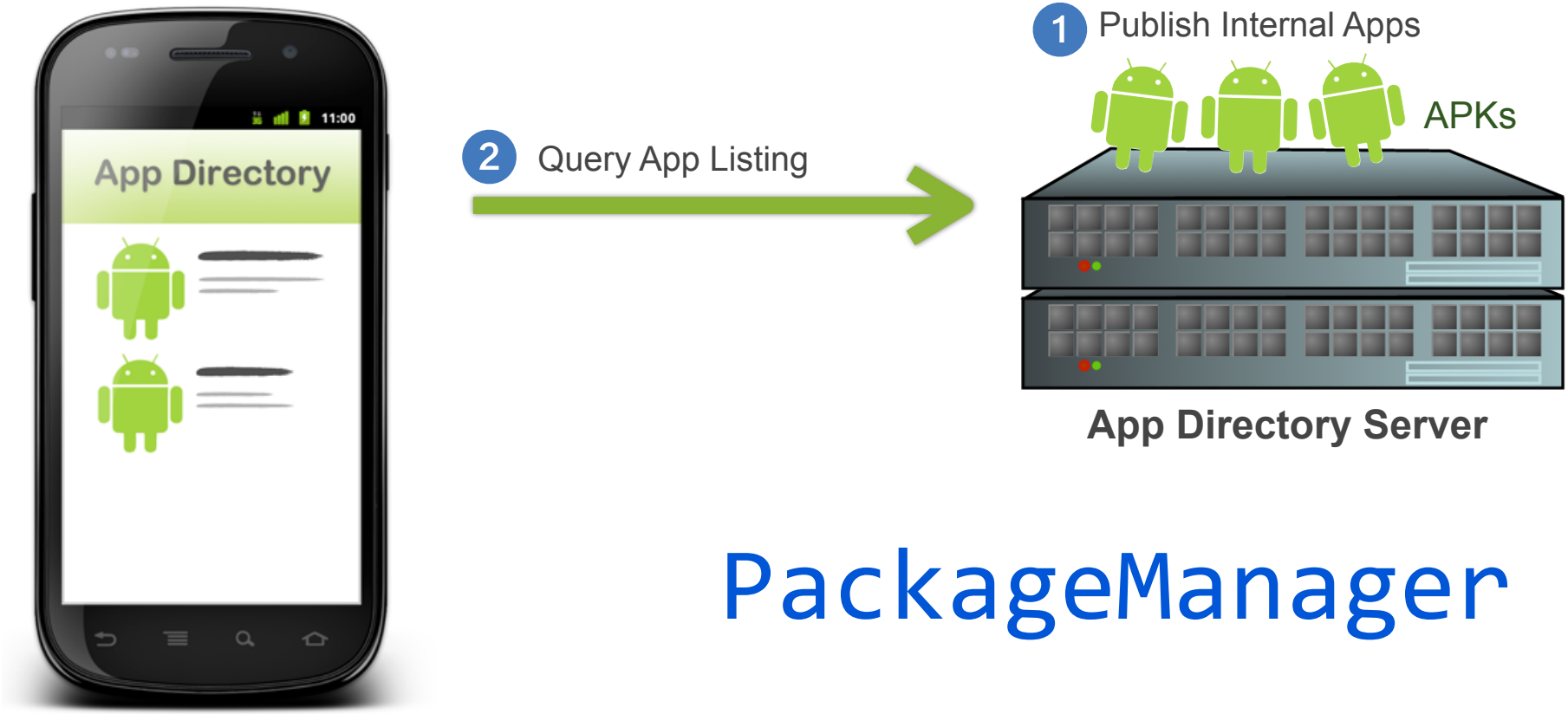
Overview



Google I/O 11

Internal App Directory

Overview

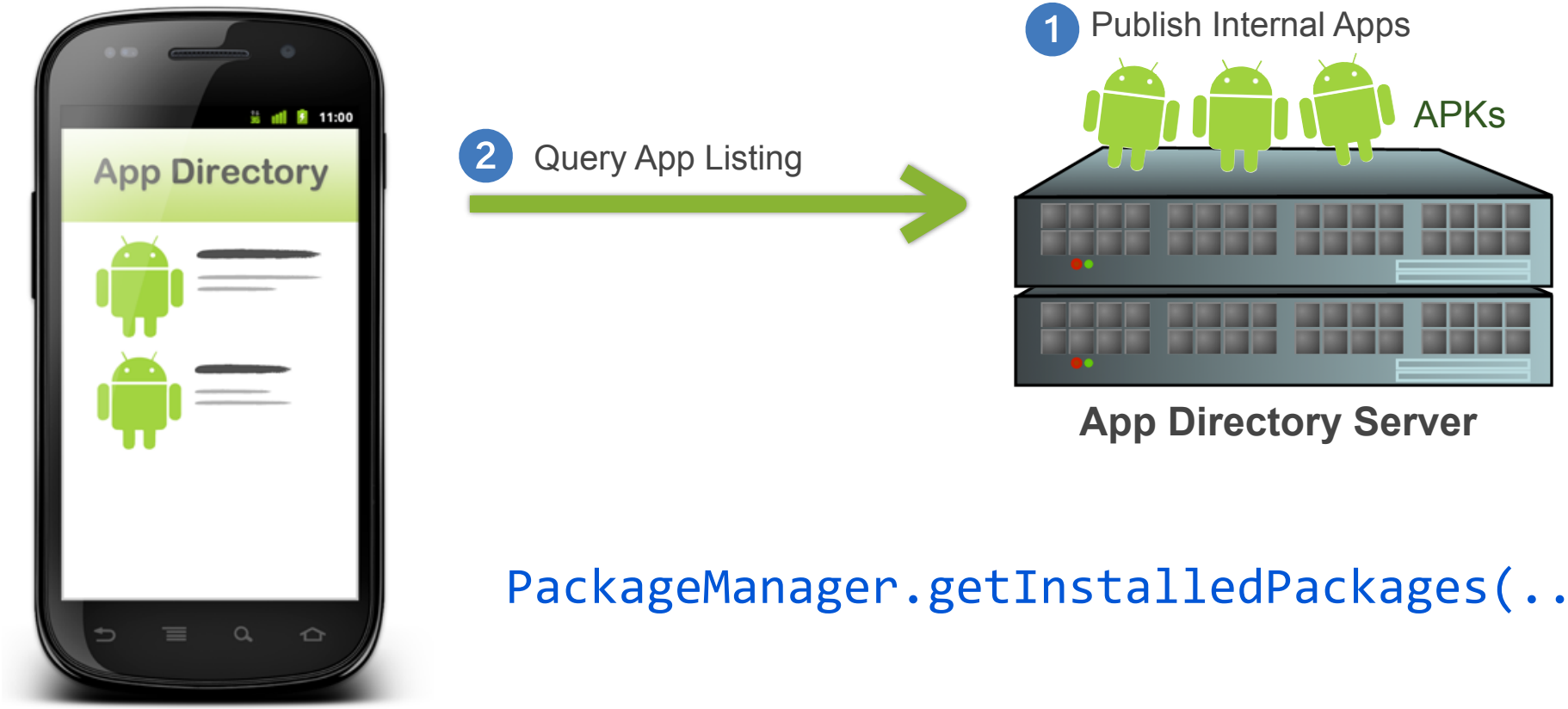


PackageManager

38

Internal App Directory

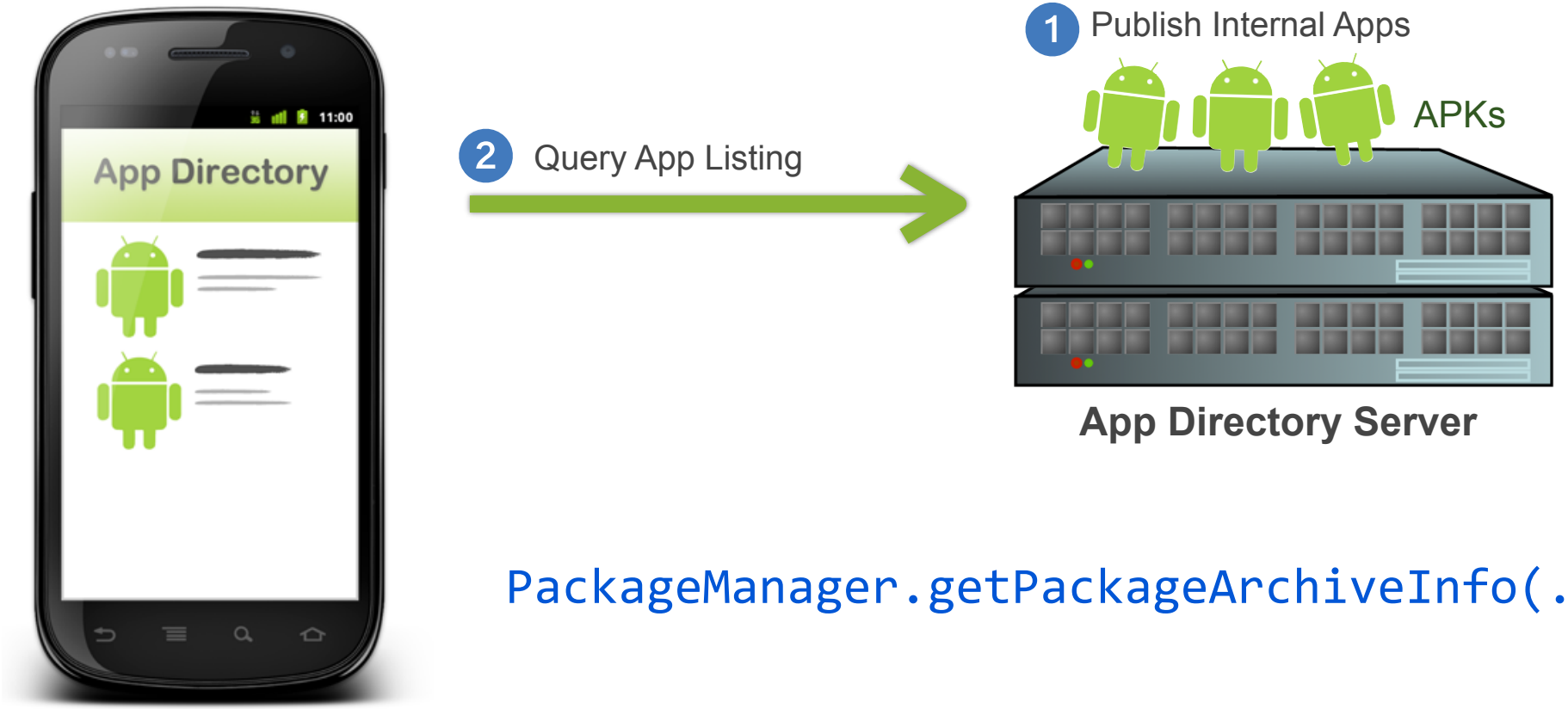
Overview




```
PackageManager.getInstalledPackages(...)
```

Internal App Directory

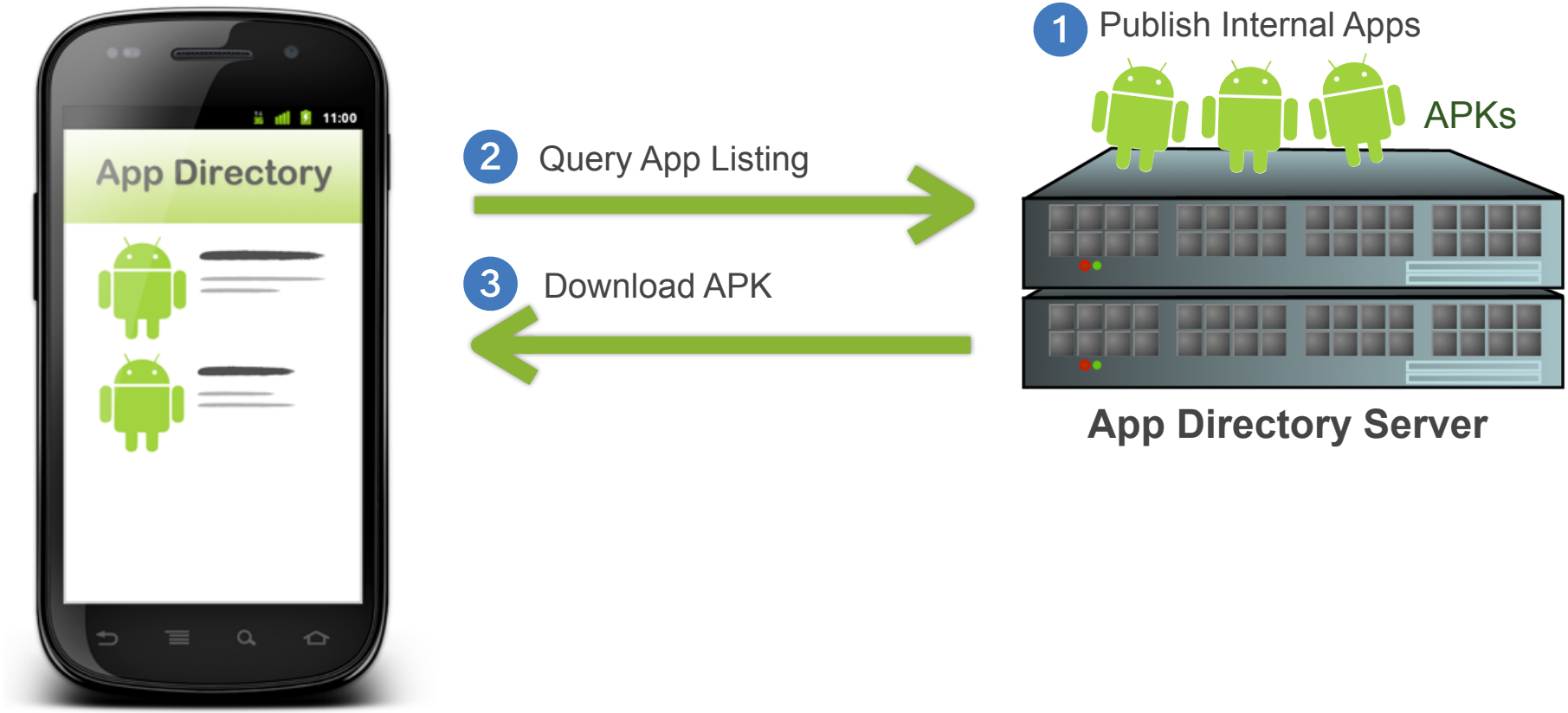
Overview




```
PackageManager.getPackageArchiveInfo(...)
```

Internal App Directory

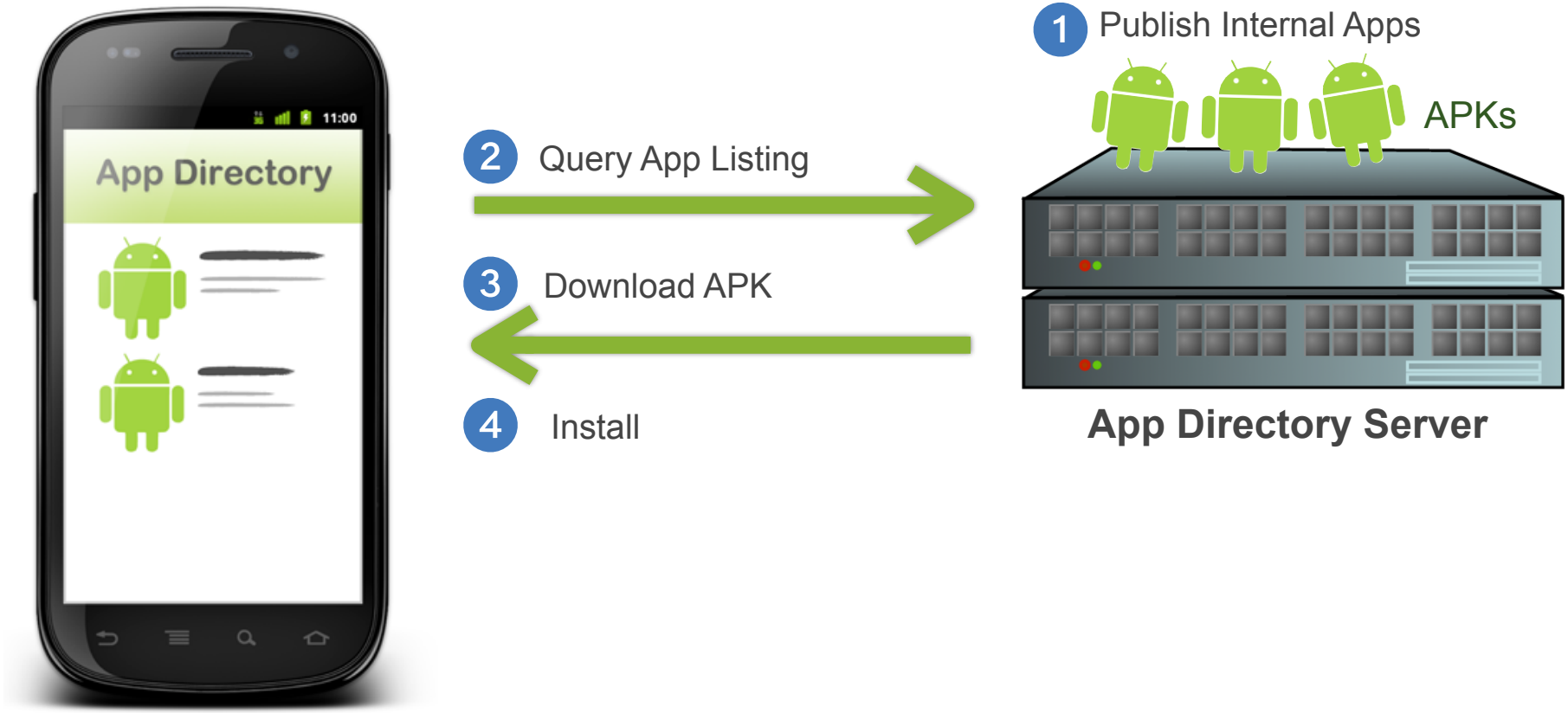
Overview



Google I/O 11

Internal App Directory

Overview



Resources

- Device Administration Overview
  http://d.android.com/guide/topics/admin/device-admin.html
- Device Policy Management API Docs
  android.app.admin package
- Device Management Demo for Android Source
  http://goo.gl/tBwO4
- Device Administrator Sample Code
  http://goo.gl/98mgz

Thank you!

Feedback: **http://goo.gl/vdhGp**

Q&A

goo.gl/mod/uCeK


Google™
11
I/O