brightsight®

the number one
security lab
in the world

Android Security

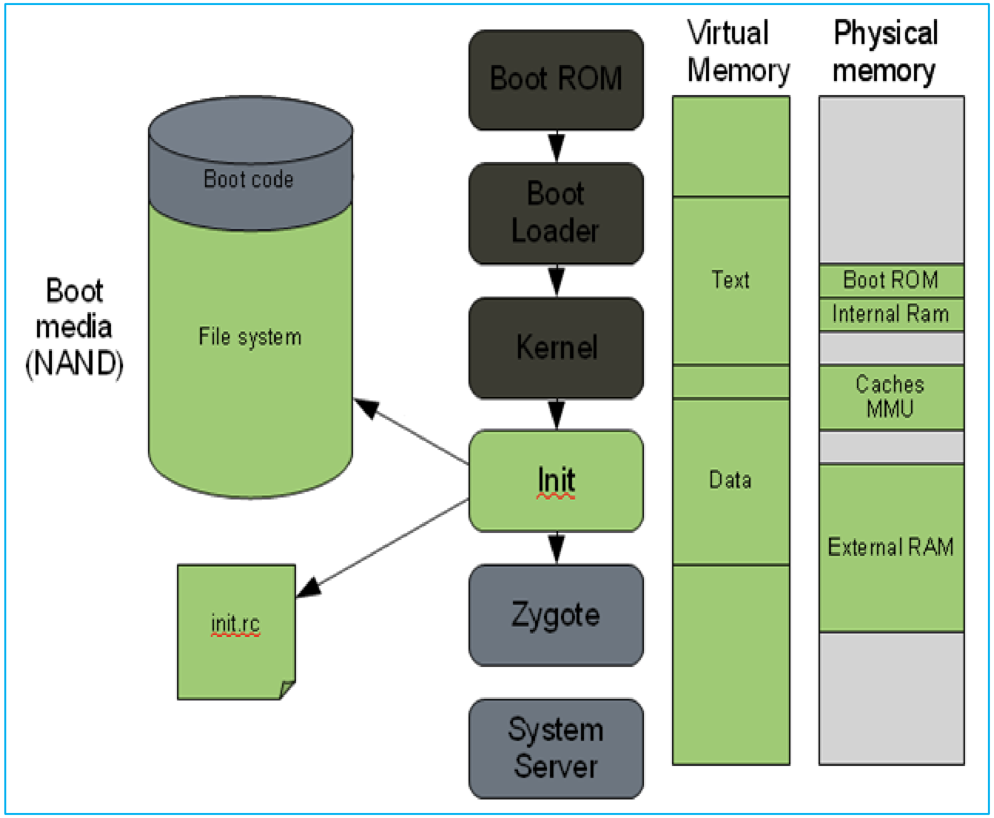
Secure and Minimized Configuration (B18)

Shiqi Li / Brightsight

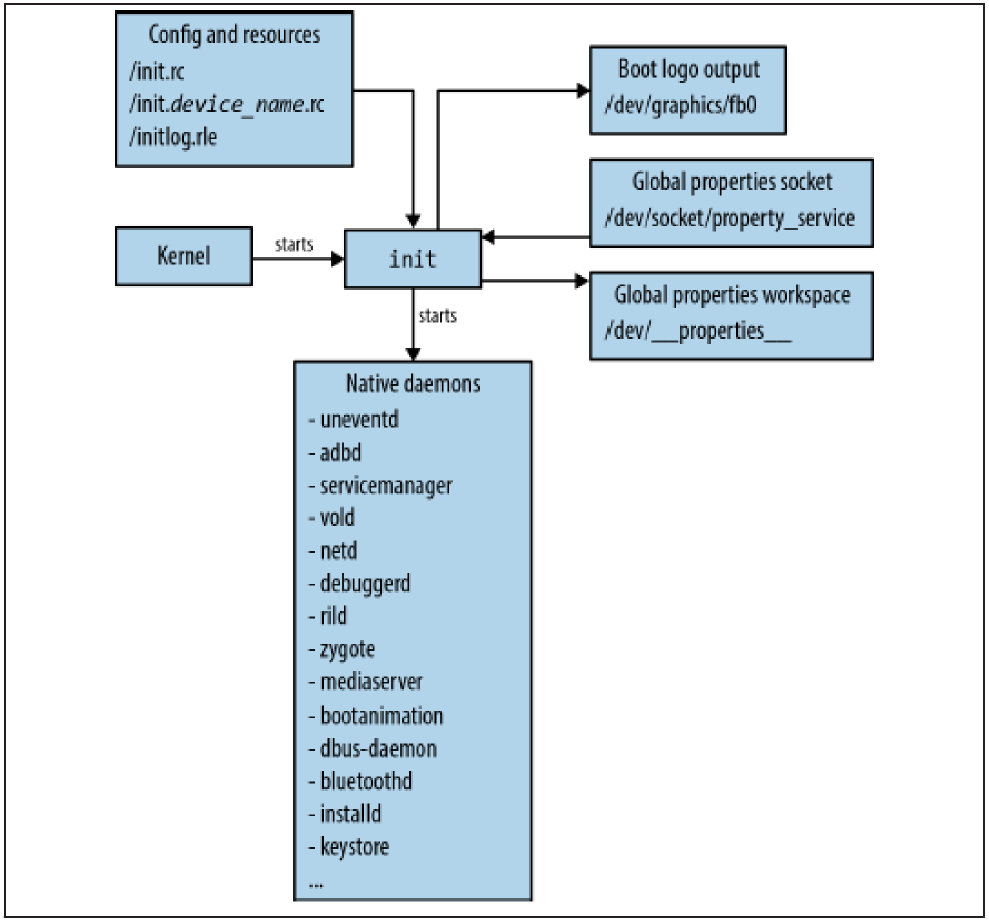
Outline

- ❑**Secure Configuration**
- ❑Remove dangerous staff

init process (1)



- init process is the “mother” of all processes
- it is launched first and killed last
- PID = 1
- Reads
  - init.rc and
  - init.<device_name>.rc files



After getting started by the kernel:

1. it essentially reads its configuration files
2. prints out a boot logo or text to the screen
3. opens a socket for its property service, and
4. **starts all the daemons and services that bring up the entire Android user-space**

Properties files

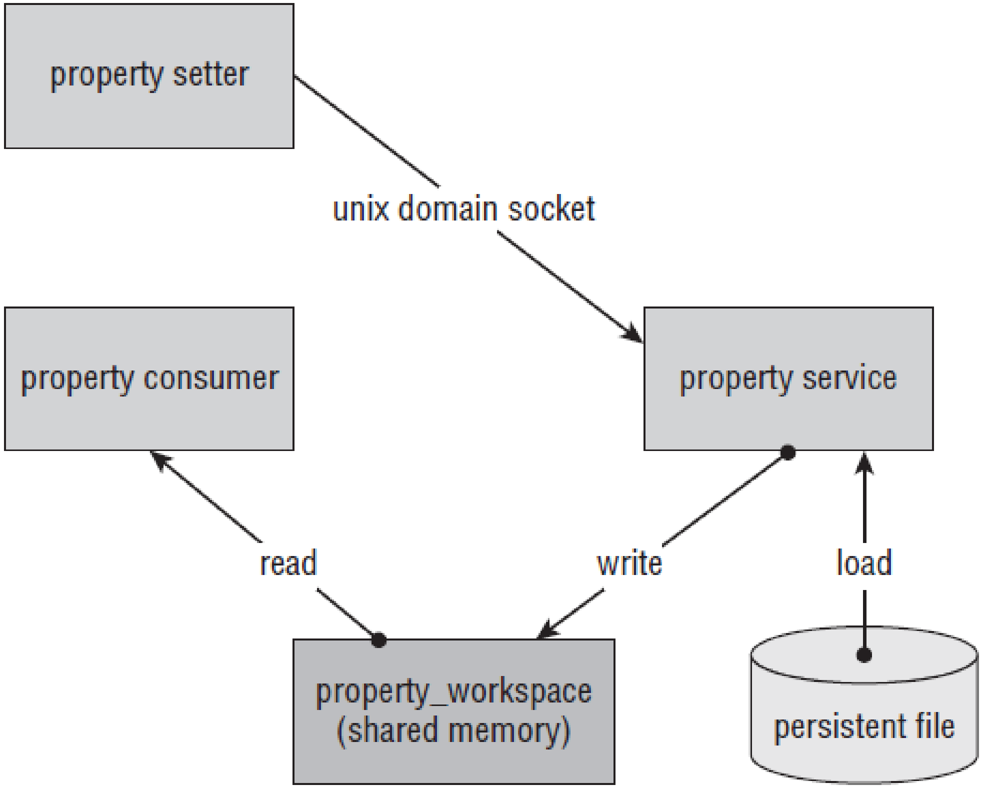


Figure 2-2: The Android Property Service

- A Property is a key / value pair
- Many android apps and libs refer to properties to determine their runtime behavior
- Init process loads:
  - /default.prop
  - /system/build.prop
  - /system/default.prop
  - /data/local.prop

Security Concerns

The evidences shall show that:

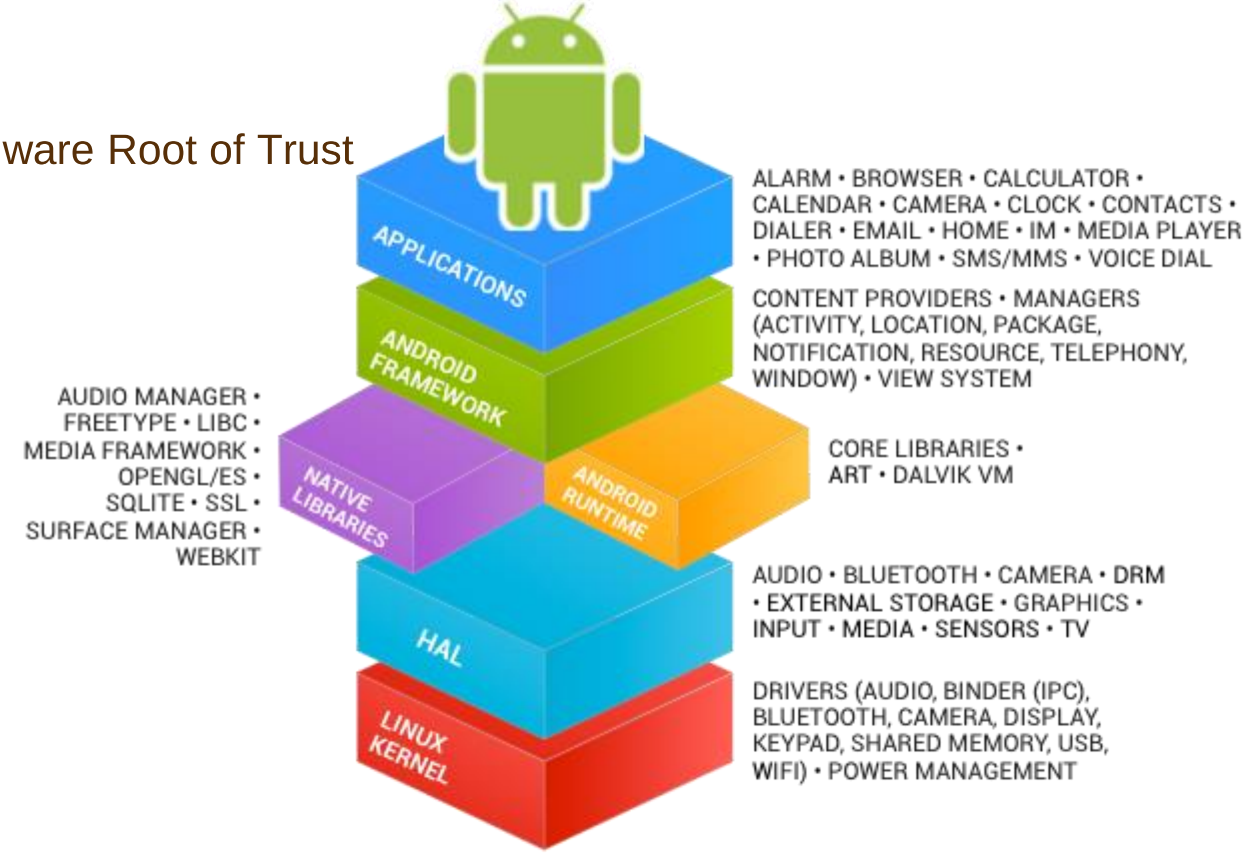
- Proper privilege settings for filesystem image, folder, keystore, device nodes, init.rc, .prop, other security relevant settings in /etc folder
- Proper setting for SUID programs
- Proper setting for permissions (e.g. key service, Virtual PINPAD service…)
- Poper Access Vector rules of the SELinux

Outline

- Secure Configuration
- **Remove dangerous staff**

Security measures in Android

- SEAndroid with MAC and MMAC (enforcing mode)
- Configuration
- Policy
- Permissions
- Most important: Hardware Root of Trust


APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL
ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM
NATIVE LIBRARIES
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT
ANDROID RUNTIME
CORE LIBRARIES • ART • DALVIK VM
HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV
LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Things to Remove

- There are no inherently dangerous things
- It’s all about configuration:
  - Include only modules that are required
  - Might need new **payment device** branch
  - Configure those modules correctly
- ADB support:
  - Disabled in user builds (normal behavior)
- WebView:
  - Remove web browsers
  - Do not use webview < 4.4
- Pre-Installed Apps:
  - Web browser, email client
  - Remove Unnecessary Privileges
- Default (Google) Certificates

Patches

- **Important for vendors:**
  - **Update** to most secure OS
  - Create an **payment device** branch
  - Apply **patches** in a timely manner

Hardening Checklist (1)

- **Basic Security**
  - □ Update Operating System to the Latest Version
  - □ Do Not Root the Device
  - □ Do Not Install Applications from Third Party App Stores
  - □ Enable Device Encryption
  - □ Disable 'Developer Actions‘
  - □ Enable Android Device Manager
  - □ Erase All Data Before Return, Repair, or Recycle

Hardening Checklist (2)

- **Authentication Security**
  - □ Set a PIN and Automatically Lock the Device When It Sleeps
  - □ Set an Alphanumeric Password
  - □ Set Auto-Lock Timeout
  - □ Disable 'Make Passwords Visible‘
  - □ Erase Data upon Excessive Passcode Failures

Hardening Checklist (3)

- **Network Security:**
  - □ Turn Off Bluetooth When Not in Use
  - □ Disable Network Notification
  - □ Forget Wi-Fi Networks to Prevent Automatic Rejoin

Hardening Checklist (4)

- **Additional Security Settings:**
  - □ Turn off Location Services
  - □ Use a Third Party Application to Password Protect Applications with Sensitive Data
  - □ Limit the Number of Text (SMS) and Multimedia Messages (MMS) Saved
  - □ Disable JavaScript
  - □ Use TextSecure to Encrypt SMS Messages

Evaluation Concerns

- Vendor provides hardening documentation
- Everything on the above list must be in vendors list. If not:
  - Very good reasoning why
  - Protection mechanisms
  - In depth code review
- Verify with Makefiles and other Build Configuration:
  - PRODUCT_PACKAGES
  - LOCAL_REQUIRED_MODULES

PCI PTS security concerns

DTR B18:

The evidences shall

- Any API and software component not required for specific functionality are removed/disabled
- intended system configuration is maintained
- All public available vulnerabilities in public domain were analyzed and fixed
- System configuration is consistent with the documented configuration

Questions?