Investigating Android Devices

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

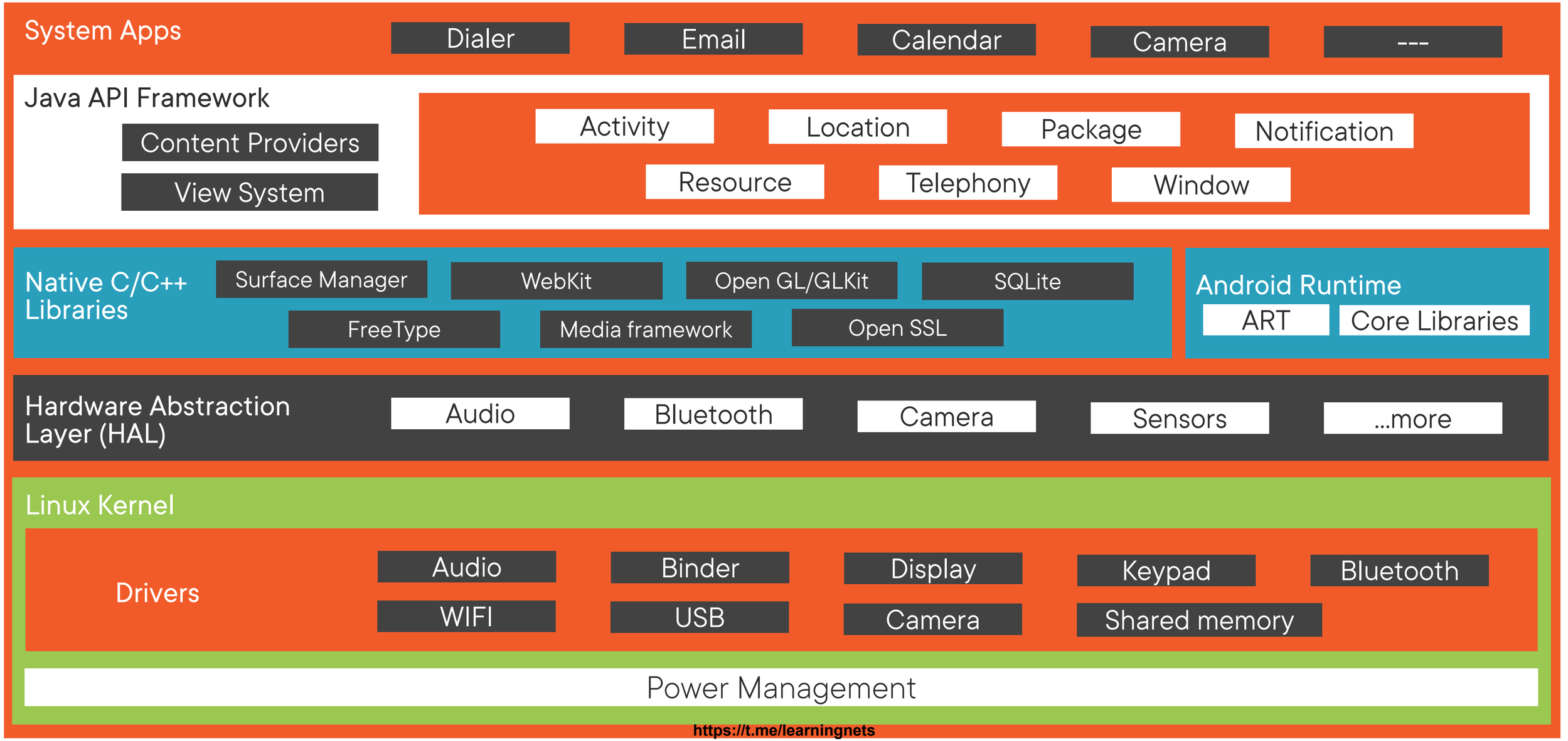
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

“It’s not about being smart, it’s about being smarter than the attacker.”

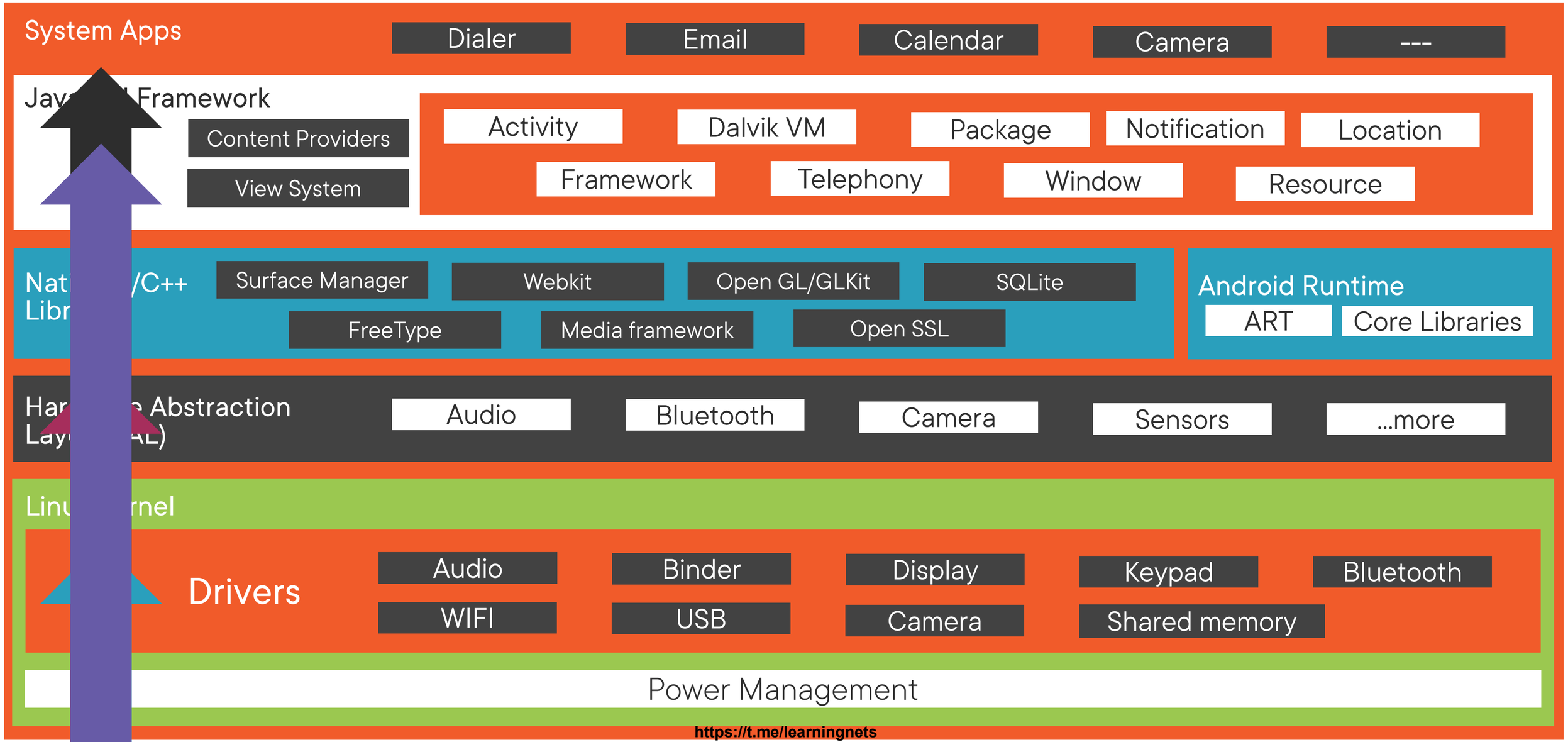
Harper Reed & Dale Meredith

Android Security

The Architecture



The Architecture



Rooting

Rooting

Modify or delete system files

Remove bloatware

Low-level access to hardware

Improve performance

Wi-Fi and Bluetooth tethering

Installing applications on SD card

Improve user interface and keyboard

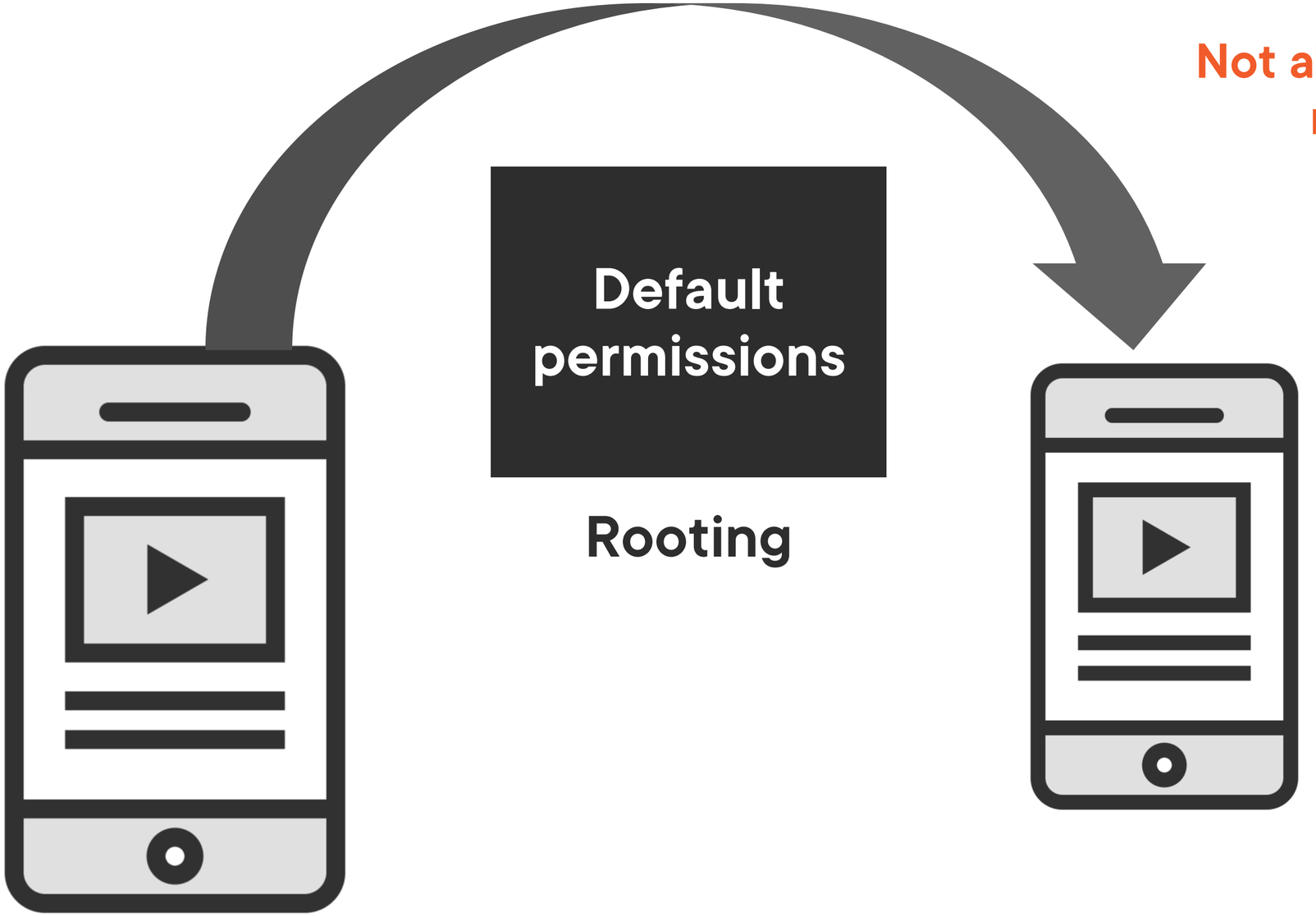
Security Risks

Voiding your phone’s warranty

Poor performance

Malware infection

Bricking the device



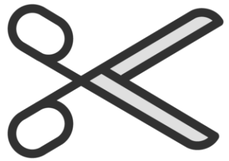
Not all applications will use root level access

Applications are restricted by the security model

Tools

KingoRoot

TunesGo Root Android Tool



One Click Root

Android Debug Bridge (ADB)

Phonesploit

Android-based Sniffers

FaceNiff

Packet Capture

tPacketCapture

Android PCAP

Testeldroid

Demo

Using dozer to scan for vulnerable apps

Demo

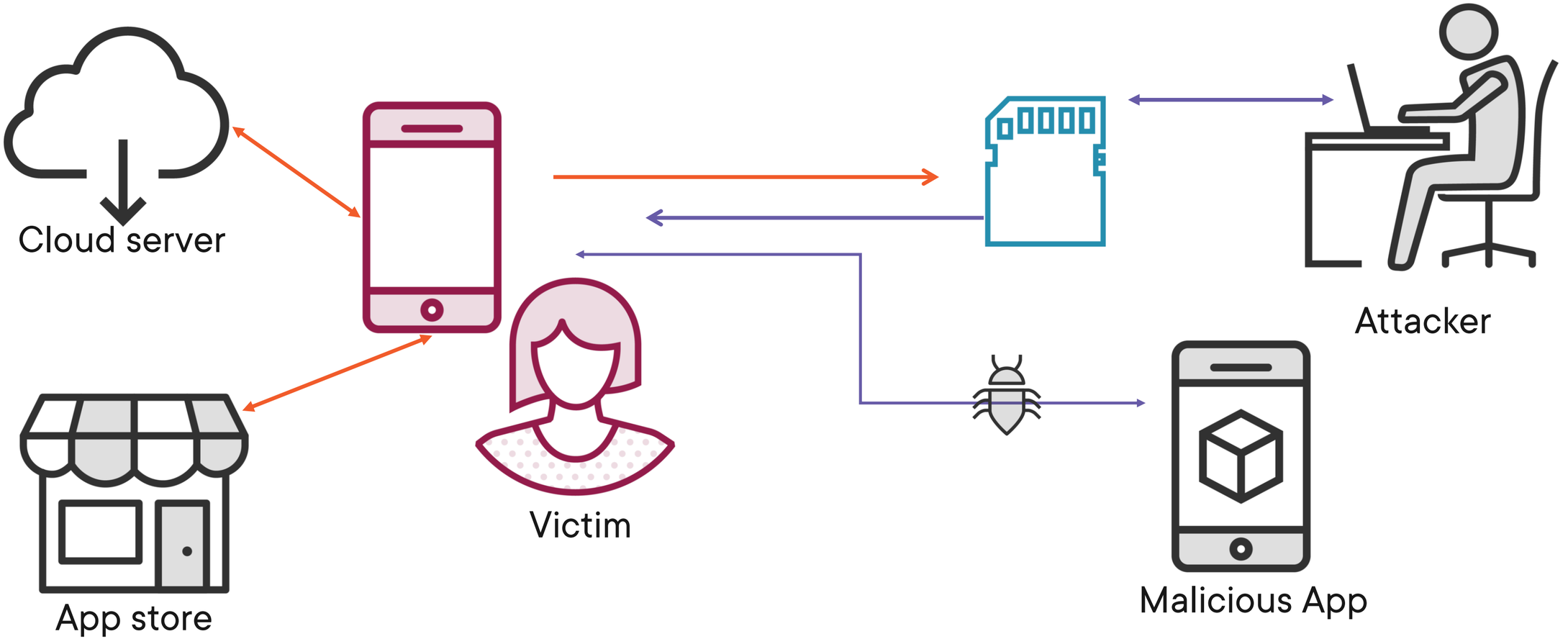
Hacking a device using PhoneSploit

Demo

Analyzing a suspicious app

Other Hacking Techniques

Man-in-the-Disk Attack (MITD)



User app fetches the tampered code

Spearphone Attack

Markie

Voice call

Ramon

Ramon is communicating via speaker phone

Ramon's phone generates speech vibrations

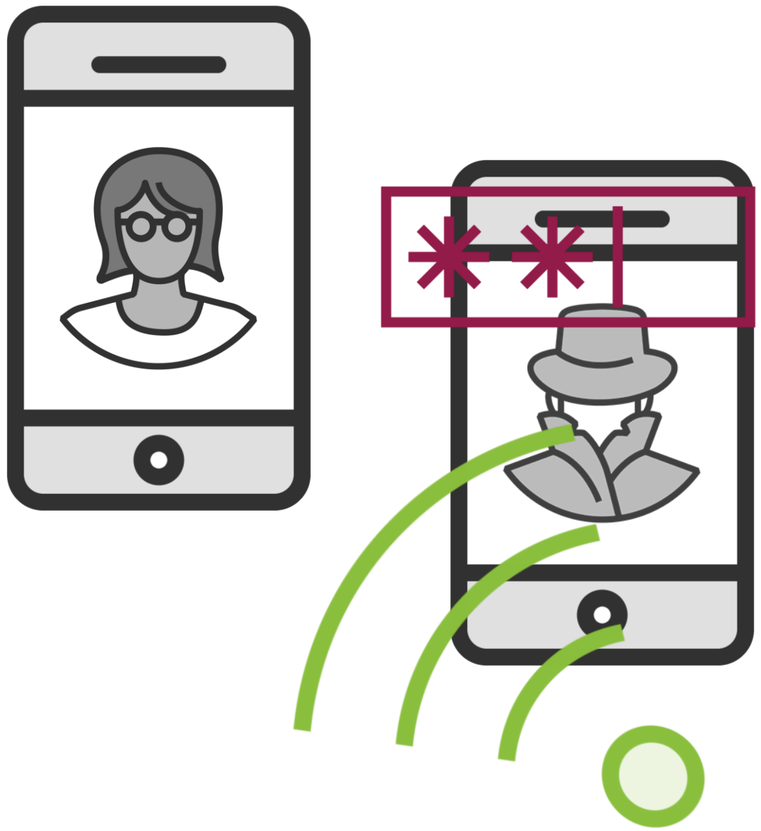
Spearphone exploiting accelerometer output

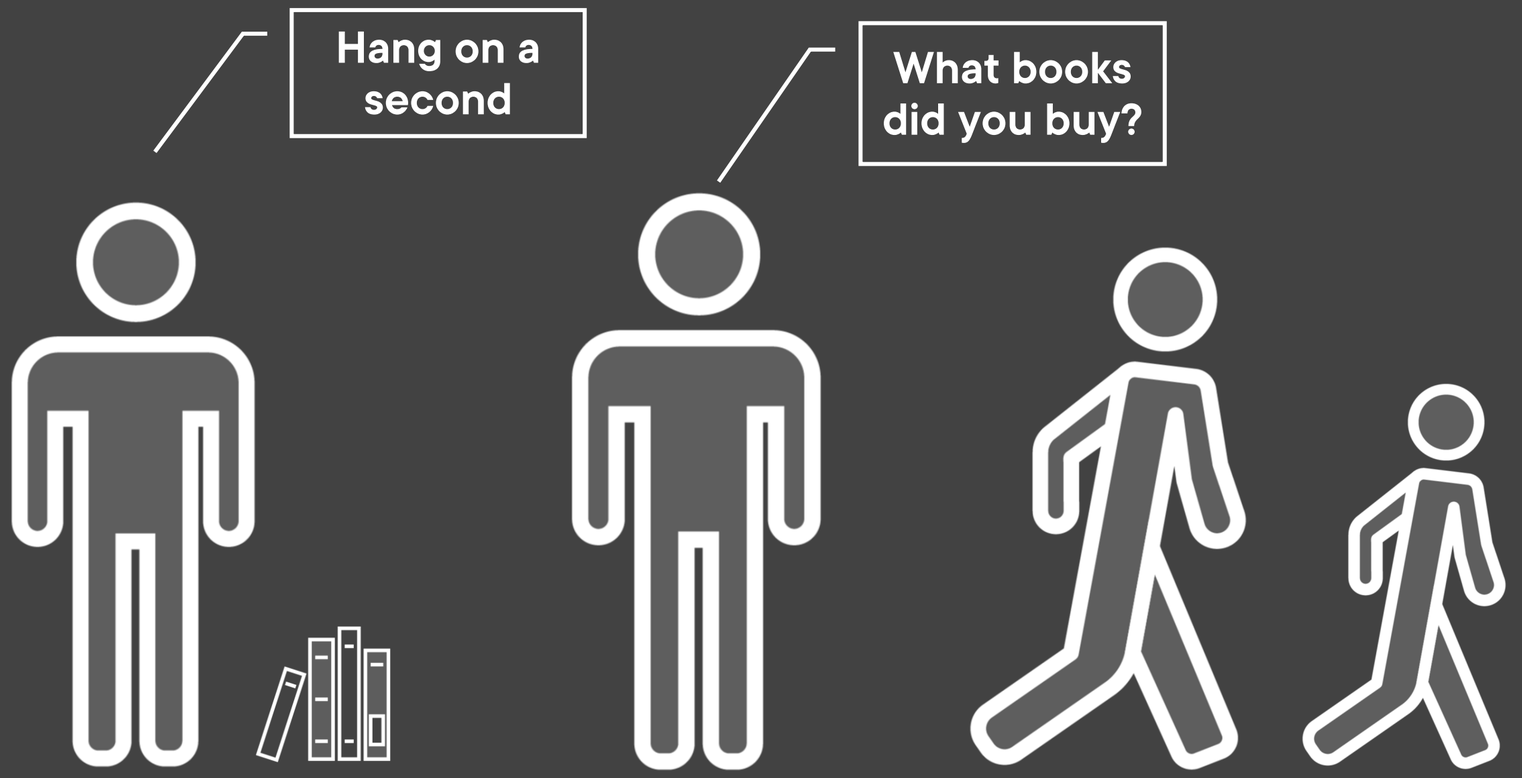
Spearphone transmits accelerometer log to the attacker

Performs gender/speaker/speech classification from received log

Tap ‘n Ghost Attack

Uses near-field communication to get your PIN from your phone





Demo

Using Fing to identify devices

Locking down Android Devices

Protecting Android Devices

Enable screen locks

Update the operating system

Download official Android market apps only

Use a protector app to assign passwords

Update device with Google Android antivirus software

Customize the locked home screen with user information

Protecting Android Devices

- **Use** Anti-Virus or malware protection
- **Use** multiple accounts if your device is shared with others
- **Use** a VPN when not on your network

Protecting Android Devices

Encrypt the device

Disable Wi-Fi

Uninstall unused apps

Use a password manager

Enable two-factor authentication

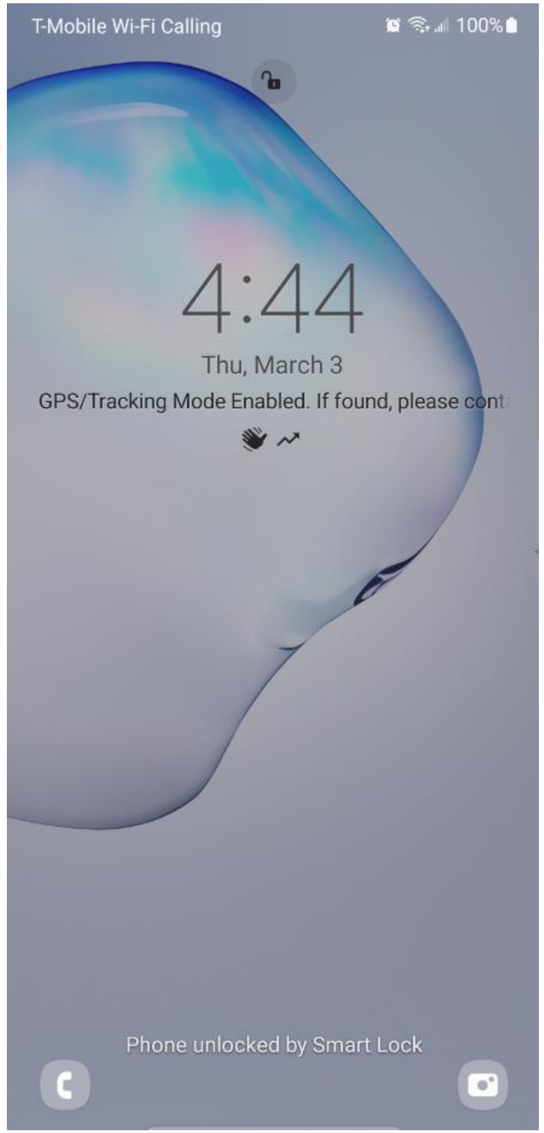
Add user information to your lock screen

Protecting Android Devices

Encrypt the device

Disable Wi-Fi

Uninstall unused apps



Protecting Android Devices

- **Avoid** rooting your android device
- **Avoid** giving permissions that aren’t needed
- **Avoid** downloading Android package files (APK)

Older devices can pose a significant threat to your infrastructure

Learning Check

Learning Check

Up Next: