ANDROID FOR WORK
Lecture 15b

COMPSCI 702
Security for Smart-Devices

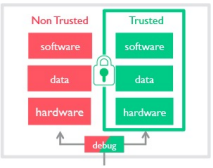
Nalin Asanka Gamagedara Arachchilage

Muhammad **Rizwan** Asghar

April 1, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

SECURE OS SERVICES: TRUSTZONE



- TrustZone technology can support a full Trusted Execution Environment (TEE),
  - Runs in a special CPU mode called Secure Mode
- Memory for secure mode and security functions can be hidden from “normal world”
- Using this technology, Android vendors can supply many secure features
  - E.g., secure boot and DRM

CRYPTO AND DATA PROTECTION

- Cryptography is used throughout Android to ensure confidentiality and integrity
- Google supports most of the industry-standard algorithms
- The major uses of cryptography in Android are:
  - Device encryption
  - App signing
  - Network connectivity and encryption including SSL, WiFi, and VPN

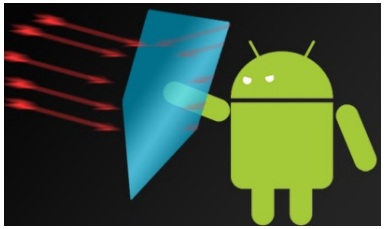
DEVICE ENCRYPTION

- Process of encoding user data on an Android device using an encryption key
- If device encryption is enabled, all user-created data is automatically encrypted before storing on disk
- All reads automatically decrypt data before returning it to the calling process
- Android disk encryption is based on *dm-crypt*
- Android uses Advanced Encryption Standard (AES) for device encryption

APP SECURITY

- App sandboxing and permissions
- Security Enhanced Linux (SELinux)
- App signing
- Google Play App review
- Google Play Protect

NETWORK SECURITY



- Android provides secure communications over the Internet by supporting TLS/SSL
  - E.g., for web browsing, email, instant messaging, and other Internet applications

- TLS/SSL vulnerabilities/misconfigurations
  - The Android Security team has developed a tool called *nogotofail*
  - *nogotofail* provides an easy way to confirm that devices or applications are safe against known TLS/SSL vulnerabilities and misconfigurations

DEVICE AND PROFILE MANAGEMENT

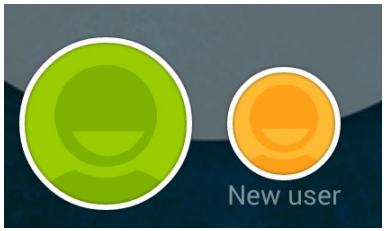
- Android 5.0 supports enterprise use cases
- There is also a concept of multiuser Android

BRING YOUR OWN DEVICE (BYOD)

- BYOD refers to the policy of permitting employees to bring personally owned mobile devices to their workplace

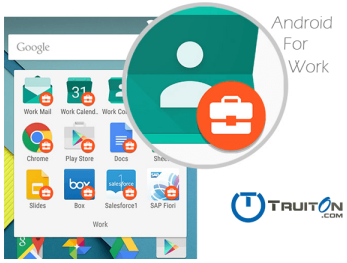
- These devices are used to get access to privileged corporate information and apps

ANDROID USERS



- Primary user
  - The first user added to a device
  - Cannot be removed, except by factory reset
  - This user also has special privileges
  - The primary user is always running
- Secondary user
  - Any user added to the device other than the primary user
  - A secondary user can be removed by the primary user
  - Less powerful than a primary user

MANAGED PROFILE



- Work profile
  - Work profile is a separate Android user
  - All data within this profile is managed separately by the enterprise
- Profile owner
  - The one who can manage the corporate space on a user's personal device to support the BYOD use case
- Device owner
  - Like a profile owner, but scoped to the whole device
  - The device owner is the device admin in the corporate-owned device use case

APP MANAGEMENT

- Google Play for Work
  - Offers APIs used by Enterprise Mobility Management (EMM) vendors to allow them to manage apps
    - An IT admin can **remotely install or remove** apps on managed Android for Work devices via the EMM's app
    - An IT admin can define **which users** should be able to **see which apps**
    - Enterprise admins can see **which users have apps** installed

APP MANAGEMENT

- Google Play for Work
  - Private apps
    - Apps can be published by an enterprise customer and targeted privately
    - There are two modes of delivery for private apps
      - Google-hosted
      - Externally-hosted
    - Apps must comply with all Google Play policies in all cases
  - Managed app configuration
    - An app could allow an IT admin to remotely control the availability of features or configure settings

RESOURCES

- **TrustZone**
  http://www.arm.com/products/processors/technologies/trustzone/index.php

- **Android for Work:**
  Android Security White Paper
  https://static.googleusercontent.com/media/www.google.co.il/iw/IL/work/android/files/android-for-work-security-white-paper.pdf

- **Android for Work**
  Applications Overview
  https://static.googleusercontent.com/media/www.google.co.nz/en/NZ/work/android/files/android-for-work-apps-guide.pdf

Questions?

Thanks for your attention!