1. Software-implemented security
    - Linux Native Permissions
        - AID ranges
        - Treble and the return of passwd/group files
    - SELinux
    - SECCOMP-BPF
    - Android Runtime permissions
    - Appops

2. Hardware-backed security
    - TrustZone
        - Theory & Design
        - Vendor Implementations:
            - Qualcomm: QSEE/QHEE
            - MTK/Older Samsung: Mobicore
            - Samsung: TEEGRIS
            - Google: Trusty
    - Beyond Trustzone: Hardware Security Modules
        - Titan M/M2
        - Qualcomm SPU

3. Authentication subsystems
    - The Lock Screen (`lock_settings` service)
    - The `auth` service
    - The `biometric` service
    - Face authentication (The `face` service)

4. Encryption facilities
    - DM-Crypt
    - Ext4Crypt
    - Keystore
    - Linux keyrings
    - Gatekeeper

5. Integrity & Attestation
    - Android Verified Boot
        - AVB 1.0
        - AVB 2.0
        - AVBMeta tool
    - DM-verity
    - 11: App Integrity, File Interity (fs-verity)
    - Samsung TIMA & Knox
    - Google SafetyNet

---

6. Introduction/Threat Modeling Android
   Lorem ipsum
    - Threat Modeling
    - Attack classes
        - ..
        - ...
    - Android Security Model

7. Rooting
   Rooting Android using boot-to-root methods

  - Prerequisite: OEM unlocking
    - Android IOEMUnlock interface
    - ...
  - Case Study: Magisk
  - Malware Case Study: Intellexa's "Alien"

8. Vulnerability/Exploit case studies:
   (Jury's still out on which of those I'll use - comments/suggestions welcome)
   - Linux Kernel: CVE-2021-1048 (epoll) or CVE-2022-0847 (Dirty Pipe)
   - AOSP Linux Kernel: Bad Binder (CVE-2019-2215) and/or num_not_so_valid CVE-2020-0041
   - Vendor: Pixel 6 - Samsung's MFC
   - TrustZone: likely Trusty
   - AOSP: (still looking for something nice here)
   - Vendor: MTK-su and/or Boot chain vulnerability?
   - Baseband: Samsung Exynos (Shannon) VoLTE/SIP vulns

9. Appendices:
   - Android App Hardening Guide
   - Android System Hardening Guide