- Filename: eccouncil-ceh31250-v12-17-1-1-mobile-security-basics.md
- Show Name: CEHv12 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - Hacking Mobile Platforms
- Episode Name: Mobile Hacking Basics
  ==

Mobile Security Basics

Objectives:

- List common attack surfaces of mobile devices
- List common threats and vulnerabilities of mobile devices

- Mobile Attack Surfaces, Vulnerabilities, and Threats
  - Mobile Device itself
    - Android and iOS are constantly being patched and updated due to security issues
  - Malware
    - Malware Zoo: https://github.com/ytisf/theZoo/tree/master/malware/Binaries
  - Bluetooth
    - Bluejacking
      - Old bluetooth specs allowed for data transfer to unpaired devices
    - No authentication
    - No encryption
    - No need to confirm by target user
      - Sent Spam, phishing, viruses, etc
    - Bluesnarfing
      - Same problem as Bluejacking
      - Attacker is able to connect to victim without auth to see contacts, email, calendars, text messages, pictures, make phone calls, etc
    - Bluebugging
      - Similar to Bluesnarfing
    - Blueborne
      - https://www.armis.com/research/blueborne/
  - Wifi
  - Telco (cellular)
    - SS7 (Common Channel Signaling System No.7)
      - Outdated protocol providing interoperability between providers
        - Services
          - SMS
          - Billing
          - Call waiting/forwarding
      - Attacker can tap into this network using a laptop and the SS7 SDK
        - Attacker can then eavesdrop on conversations
  - App Stores/Apps
    - 3rd-party app stores can host malware apps
      - https://f-droid.org/en/
    - Official app stores have been infiltrated from time to time
  - Web

    - VPN
    - Weak/No Encryption

- OWASP Top 10 Mobile Risks

    - https://owasp.org/www-project-mobile-top-10/

- Other Mobile security issues

    - Sandbox bypass/escape
    - SIM Hijacking
    - Mobile Spam

        - SMShing
        - Vishing

            - NSO Group (Pegasus/Darknet Diaries)

    - Theft