

- Filename: eccouncil-ceh31250-v11-17-1-1-mobile-hacking-basics.md
 - Show Name: CEHV11 (312-50)
 - Topic Name: Mobile Platform, IoT, and OT Hacking - Hacking Mobile Platforms
 - Episode Name: Mobile Hacking Basics
- =====

Mobile Hacking Basics

Objectives:

- Mobile Attack Surfaces
 - Mobile Device itself
 - Bluetooth
 - Bluesnarfing
 - Attacker is able to connect to victim without auth to see contacts, email, calendars, text messages, pictures, etc
 - Bluebugging
 - Similar to Bluesnarfing
 - 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 - Outdated protocol providing interoperability between providers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
 - Official app stores have been infiltrated from time to time
 - Web
 - VPN
- OWASP Top 10 Mobile Risks
 - <https://owasp.org/www-project-mobile-top-10/>
- Other Mobile security issues
 - Sandbox bypass/escape
 - Mobile Spam
 - SMSHING
 - Vishing
 - NSO Group (Pegasus/Darknet Diaries)