CROWDED SPACES CAN BE HOTBEDS FOR OVER-THE-AIR SMARTPHONE ATTACKS

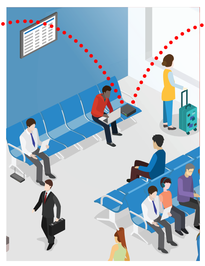
By simply walking through a high-traffic area with a powered-on smartphone, one can fall prey to a variety of radio-based attacks.

CELLULAR

Key threat: IMSI catcher (fake cell tower)

An IMSI catcher uses various techniques to mimic a real cell tower and force a smartphone to connect to it. After capturing the phone's IMSI (the SIM card's ID number), the IMSI catcher situates itself between the phone and cellular network.

Risks: Location tracking | Leakage of certain types of data | Malware infection



WIFI

Key threat: Rogue access point (Karma attack)

Because a smartphone broadcasts its preferred network list when looking for a WiFi network, a rogue access point can assign itself an SSID (WiFi network name) from the list to trick the phone into thinking it's reconnecting to a familiar network.

Risks: Leakage of sensitive information (like passwords) | Malware infection

BLUETOOTH

Key threat: Bluetooth exploit

Working from a laptop, a threat actor can locate a smartphone with an active Bluetooth signal in the vicinity, obtain the phone's MAC address and then send out an exploit tailored to the device's operating system.

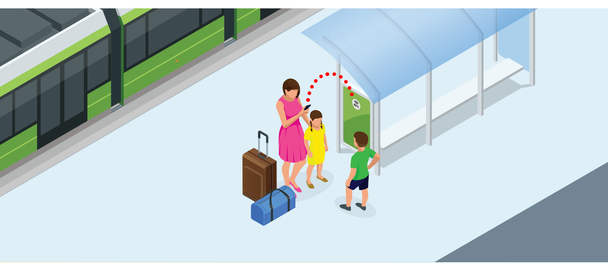
Risks: Leakage of sensitive information | Malware infection

NEAR-FIELD COMMUNICATION (NFC)

Key threat: Malicious NFC tag

After a smartphone user inadvertently bumps their device into a malicious NFC tag that's been placed in an inconspicuous location, the NFC tag opens – automatically or with social engineering prompts – a malicious site in the user's browser.

Risks: Malware infection



PRIVORO®