Sprint 1

Hijacking Attack:

Overview:

An adversary can hijack the Qi communication channel by injecting adversarial magnetic signals using a disguised adversarial coil to alter the power transfer process.

By modulating the alternating current flowing through the adversarial coil, the coil will produce magnetic signals to disrupt the electromagnetic field between the power transmitter and receiver

Assumptions:

* Adversary is able to place coil between charging pad a target device

Supplies Needed:

* Oscilloscope (might be able to do waveform generation)
* Software to interact with the oscilloscope?
* Dedicated laptop for oscilloscope readings?
* Adversarial coils
* Wireless charging pad (victim)
* Phones (differing makes and models but Qi compliant)
* Keysight 33522B Waveform Generator to produce alternating signal <https://www.keysight.com/us/en/support/33522B/waveform-generator-30-mhz-2-channel-arb.html>

Setup/Initial Steps

* Wireless charger -> adversarial coil -> smartphone
* Connect Oscilloscope to the primary coil?
* Connect Oscilloscope to laptop to acquire data readout?
* Connect Waveform generator to adversarial coil

Actions:

* Generate malicious Qi packets for hijacking (End Power Transfer and Control Error Packet)

Proof of Concept Experiment (verify adversarial coil can inject):

* Requires perceived am modulated signal to change significantly in the primary coil voltage (>200mV)
* Injecting “0101” signal
* Add a 80 kHz sinusoidal wave with a 20V peak-to-peak voltage on the adversarial coil -> observe primary coil voltage change
* Turn off the signal and observe if primary coil voltage returns to its original level
* Adversary can follow the bi-phase encoding mechanism to regulate the voltage of the adversarial coil (switch LOW and HIGH)

Eavesdropping Attack:

Overview:

An adversary can observe a victim’s actions on a phone by observing the control error messages sent between a device and a wireless charger.

These messages can be demodulated by the adversary to observe patterns specific to different actions performed by the user. This information can be used to gain personal information and track habits of the user.

The “control error” message to the charger adjusts the transmit power density – different activities rely on different amount of power consumption Should produce an identifiable pattern on the control error sequences as well as the induced voltage

Assumptions:

* Adversary can place adversarial coil near enough to the primary coil to achieve a reading
* Some form of back-end data logging

Supplies Needed:

* Oscilloscope (serves as our data logging backend)
* Software to interact with the oscilloscope?
* Dedicated laptop for oscilloscope readings?
* Adversarial coils
* Wireless charging pad (victim)
* Phones (differing makes and models but Qi compliant)
* Keysight 33522B Waveform Generator to produce alternating signal <https://www.keysight.com/us/en/support/33522B/waveform-generator-30-mhz-2-channel-arb.html>

Setup/Initial Steps

* Place adversarial coil near primary coil (can be underneath surface about 3.2cm)
* Connect Oscilloscope to the primary coil
* Connect Oscilloscope to laptop to acquire data readout
* Connect Waveform generator to adversarial coil

Actions:

* Measure induced voltage on adversarial coil when phone actions take place
* Decode the control error sequences
* Trigger Actions
* Receiving a cellular phone call, a SMS message, manually turning off the screen (50 times for each activity)
* 14 time domain features for both the voltage signal and decoded control error sequence on each activity segment
  + Length, min, max, median, variance, std, abs-mean, skewness, kurtosis, first quartiles, second quartiles, third quartiles, inter quartile range)
* Proof of concept, iPhone messages/Phone calls