Wireless Charging Power Side-Channel Attacks

Alexander S. La Cour, Khurram K. Afridi, and G. Edward Suh

Cornell University, Ithaca, NY

*Presented at: ACM CCS, **2021***

Can a Wireless charger reveal private information?

- Yes, It can.. It can profile user activities
- No sophisticated equipment needed
- No User permission needed

Contributions

- Wireless charging power side channel for website fingerprinting
- Compares wired and wireless charging and shows they basically leak same amount of information
- Amount of information leakage depends significantly on battery level

Threat Model

Side-channel attack : Acquire sensitive information through **unintended secret-dependent** variations **in physical behaviors.**

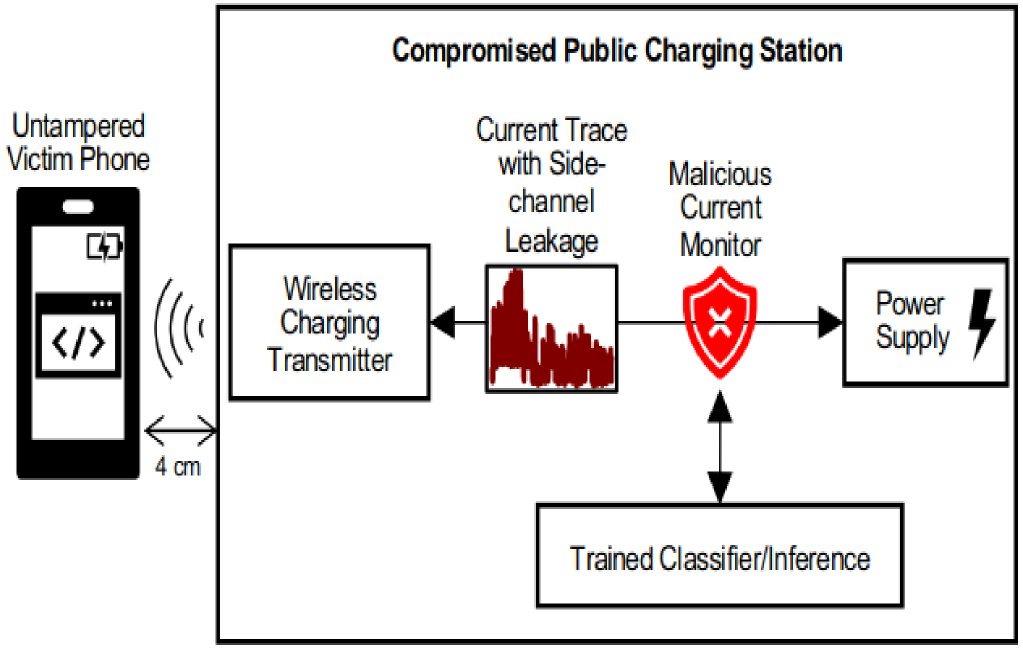

Compromised Public Charging Station
Untampered Victim Phone
4 cm
Wireless Charging Transmitter
Current Trace with Side-channel Leakage
Malicious Current Monitor
Power Supply
Trained Classifier/Inference

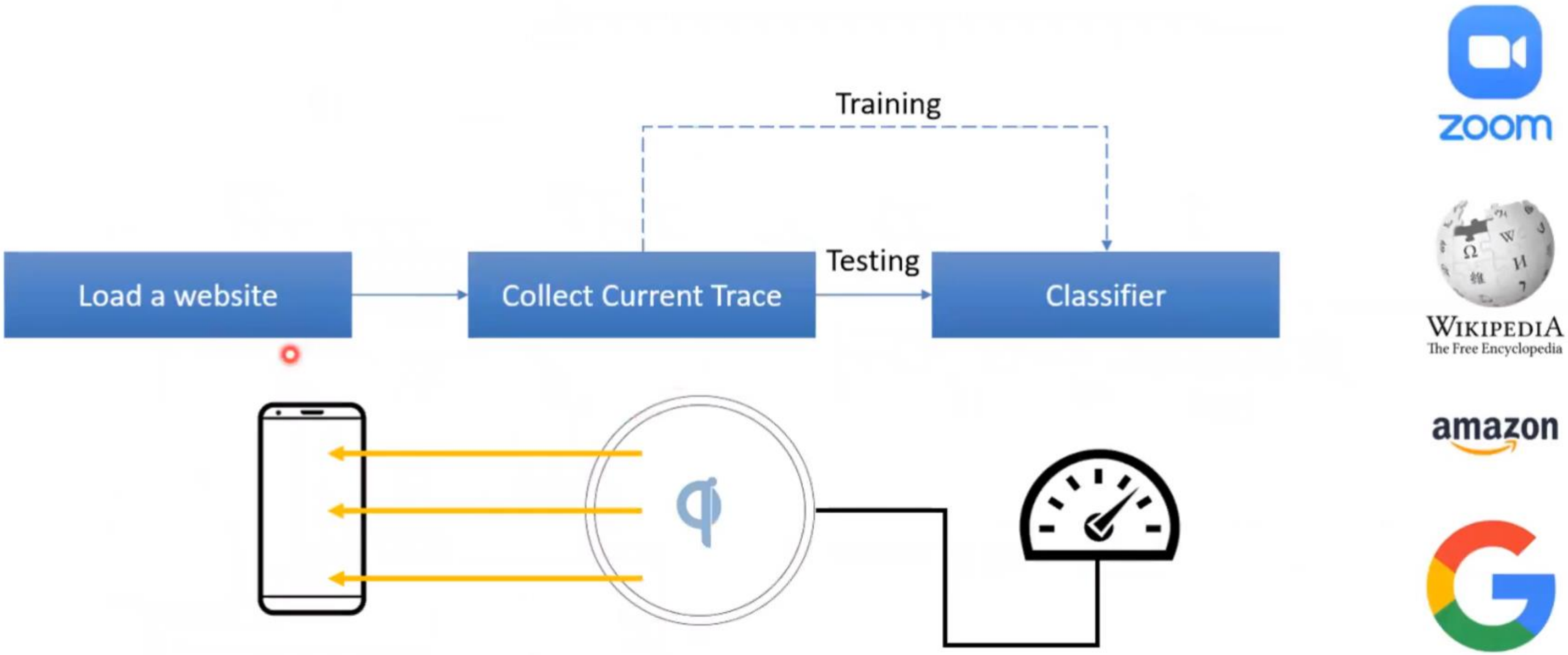
Figure 3: Threat model demonstrating a power side-channel attack by a compromised public charging station.

Attacker

Action: monitor and record the amount of power delivered to untampered transmitter

Goal: Infer the events or data on target device by analyzing the recorded power traces.

Attack Overview



Training

Load a website

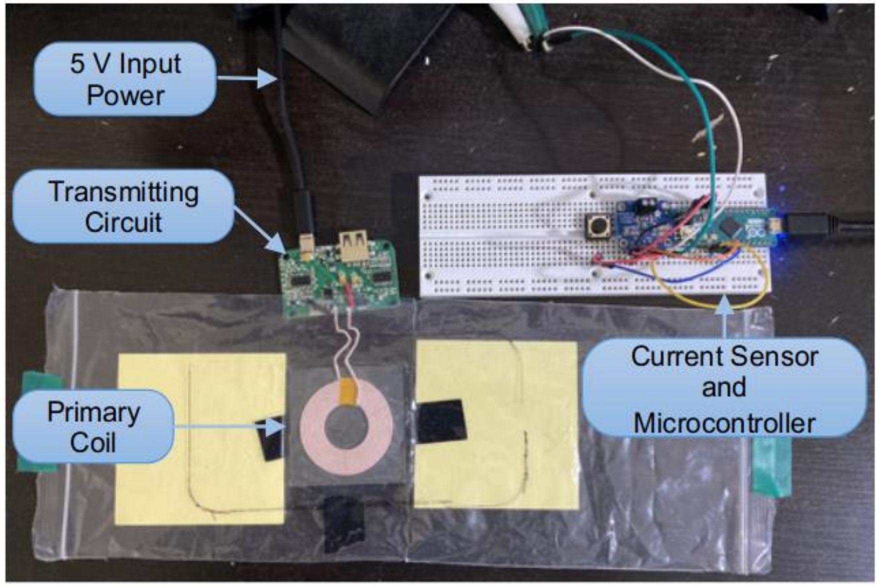
Collect Current Trace

Testing

Classifier

Central Idea!!

- Power consumption varies with requested traffic
- Develop a ML-classifier(CNN+LSTM) for website fingerprinting



(b) Photo of setup with the Adafruit 5 W transmitter.

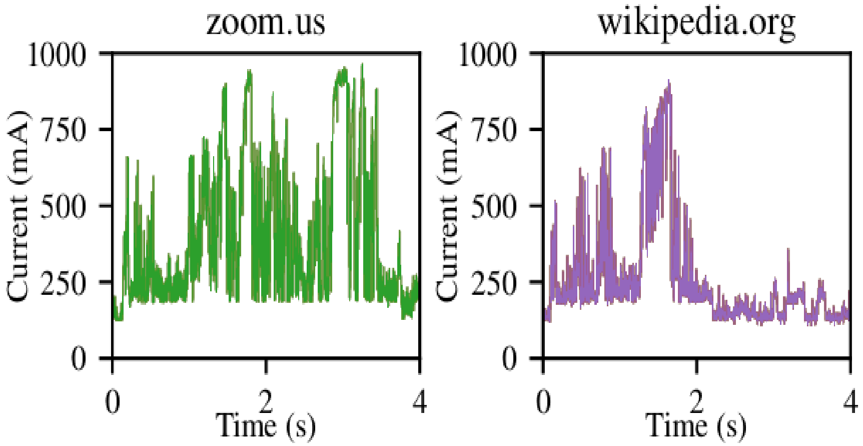


Figure 2: A wireless charger draws a varying amount of current as mobile webpages are loaded on the charging phone.

How current battery charge affects the attack success?

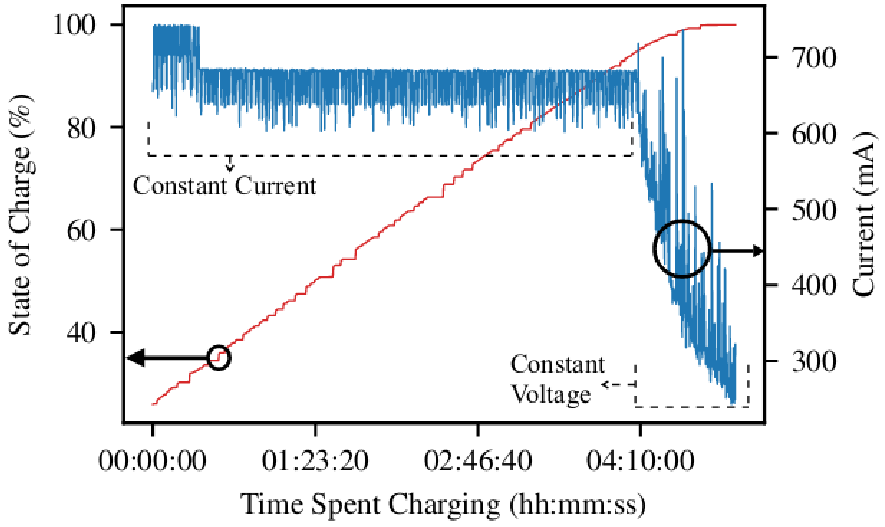


Figure 6: Current delivered by a 5 W Qi charger/battery state of charge vs charging time for an iPhone 11. The constant current and constant voltage charging stages are identified.

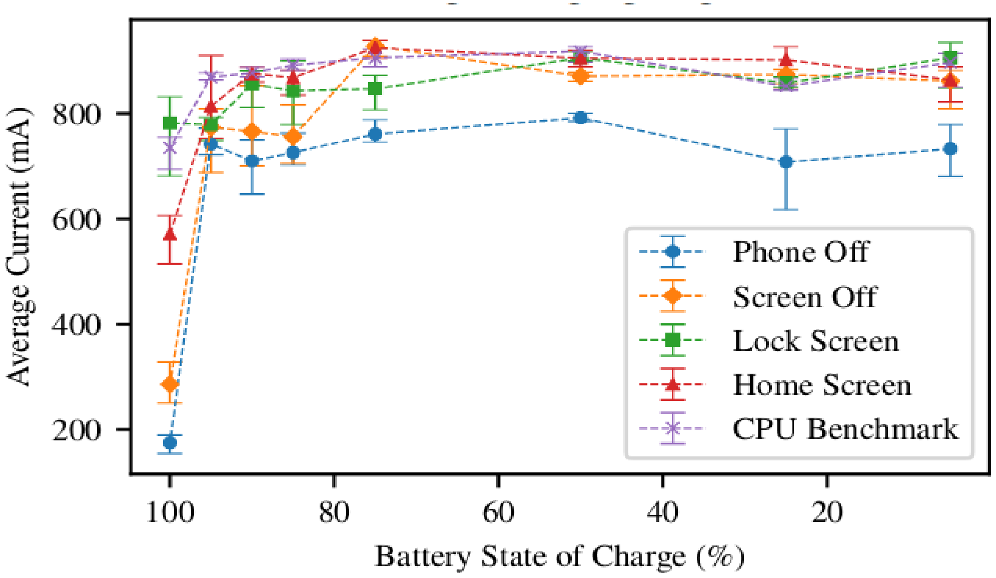


Figure 7: The average current consumption vs iPhone 11 state of charge for five different activities.

Observation:

1. The higher the battery level, the more suspectable the user to the attack.

2. Little information leaks when the battery level is below 80%.

Evaluation

Metrics:

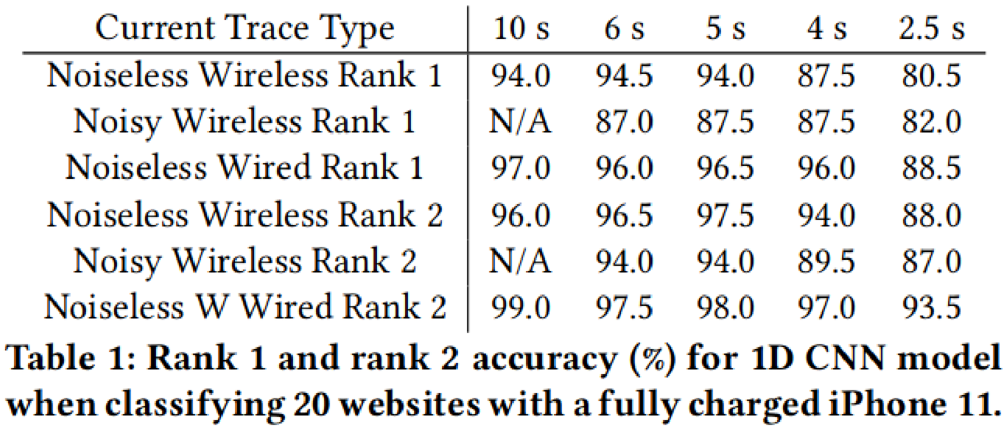
- Rank-1 accuracy: website with highest score is correct
- Rank-2 accuracy: website with highest and second-highest score is correct

Experiments w.r.t :

- Device manufacturer
- Different device for training and testing
- Different charger for training and testing
- Aging of training traces
- Battery state of charge

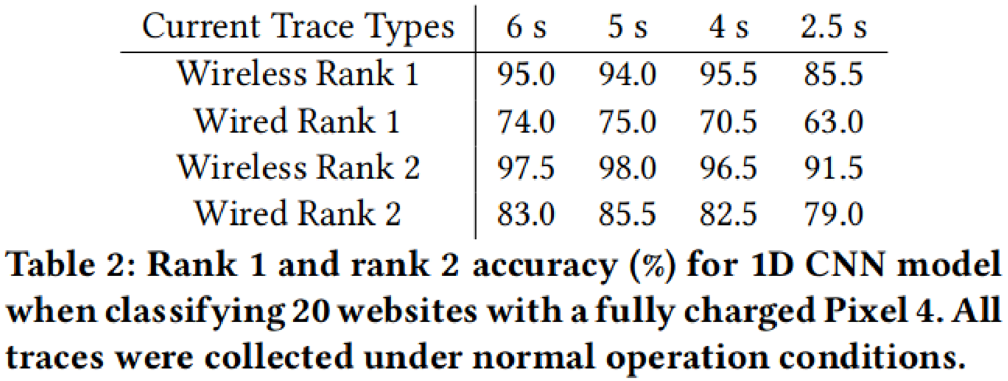
Results

iPhone 11 vs Pixel 4



Current Trace Type	10 s	6 s	5 s	4 s	2.5 s
Noiseless Wireless Rank 1	94.0	94.5	94.0	87.5	80.5
Noisy Wireless Rank 1	N/A	87.0	87.5	87.5	82.0
Noiseless Wired Rank 1	97.0	96.0	96.5	96.0	88.5
Noiseless Wireless Rank 2	96.0	96.5	97.5	94.0	88.0
Noisy Wireless Rank 2	N/A	94.0	94.0	89.5	87.0
Noiseless W Wired Rank 2	99.0	97.5	98.0	97.0	93.5

Table 1: Rank 1 and rank 2 accuracy (%) for 1D CNN model when classifying 20 websites with a fully charged iPhone 11.



Current Trace Types	6 s	5 s	4 s	2.5 s
Wireless Rank 1	95.0	94.0	95.5	85.5
Wired Rank 1	74.0	75.0	70.5	63.0
Wireless Rank 2	97.5	98.0	96.5	91.5
Wired Rank 2	83.0	85.5	82.5	79.0

Table 2: Rank 1 and rank 2 accuracy (%) for 1D CNN model when classifying 20 websites with a fully charged Pixel 4. All traces were collected under normal operation conditions.

Training and Testing on Different Devices

- **Trained on iPhone:**
  - Rank 1: **4.2%**
  - Rank 2: **12.1%**

😍

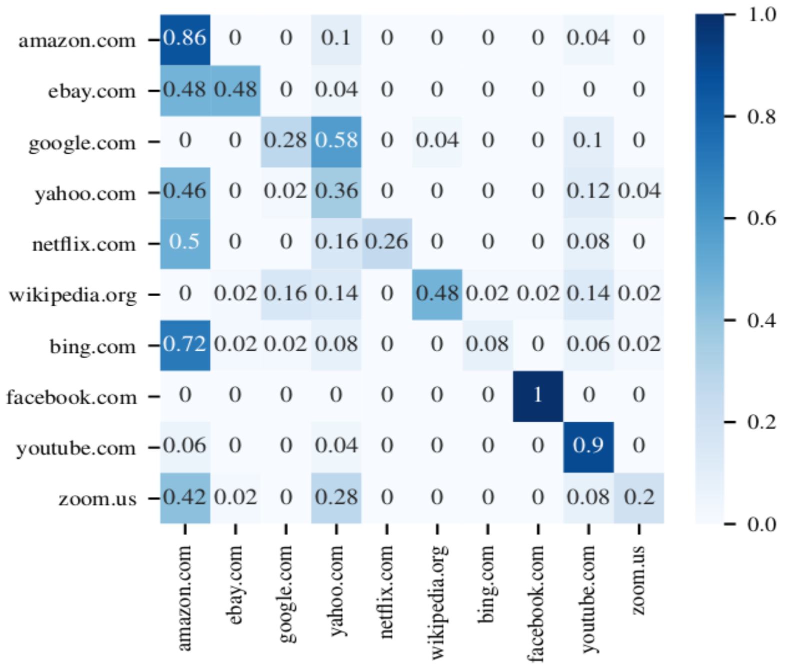
- **Trained on Pixel 4:**
  - Rank 1: **5.7%**
  - Rank 2: **11.6%**

Result: Unable to identify traces form different device at all

Results(cont..)

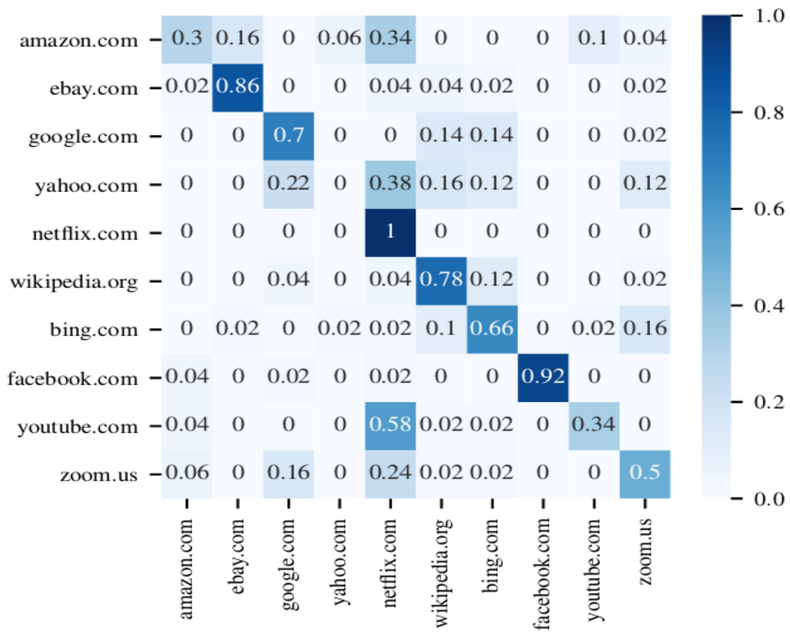
Training and Testing on Traces from Different Chargers

- **Target:** Impact of different chargers without retraining the classifier
- **Result:** leakage from wireless is comparable to wired charging



(a) Training on wireless traces, testing on wired traces.

Train on wireless, test on wired



(b) Training on wired traces, testing on wireless traces.

Train on wired, test on wired

Results(cont…)

Aging of Training Traces

Method: test new traces 9 months after the training traces were collected

Result: accuracy significantly lowered due to dynamic content

Impact of Battery State of Charge

Result: information is revealed when battery state reaches **95%(wired) 90%(wireless)**