Poster Abstract: Security and Privacy in the Age of Cordless Power World

Yi Wu
University of Tennessee
Knoxville, TN, USA
ywu83@vols.utk.edu

Zhuohang Li
University of Tennessee
Knoxville, TN, USA
zli96@vols.utk.edu

Nicholas Van Nostrand
University of Tennessee
Knoxville, TN, USA
nvannost@vols.utk.edu

Jian Liu
University of Tennessee
Knoxville, TN, USA
jliu@utk.edu

ABSTRACT

In this work, we conduct the first study to explore the potential security and privacy vulnerabilities of cordless power transfer techniques, particularly Qi wireless charging for mobile devices. We demonstrate the communication established between the charger and the charging device could be easily interfered with and eavesdropped. Specifically, through stealthily placing an adversarial coil on the wireless charger, an adversary can hijack the communication channel and inject malicious data bits which can take control of the charging process. Moreover, by simply taping two wires on the wireless charger, an adversary can eavesdrop Qi messages, which carry rich information highly correlated with the charging device's activities, from the measured primary coil voltage. We examine the extent to which this side-channel leaks private information about the smartphone's activities while being charged (e.g., detect and identify incoming calls and messages from different apps). Experimental results demonstrate the capability of an adversary to inject any desired malicious packets to take over the charging process, and the primary coil voltage side channel can leak private information of the smartphone's activities while being charged.

CCS CONCEPTS

- **Security and privacy**;

KEYWORDS

Wireless charging, side-channel attack, man-in-the-middle attack

ACM Reference Format:
Yi Wu, Zhuohang Li, Nicholas Van Nostrand, and Jian Liu. 2020. Poster Abstract: Security and Privacy in the Age of Cordless Power World. In *The 18th ACM Conference on Embedded Networked Sensor Systems (SenSys '20), November 16–19, 2020, Virtual Event, Japan.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3384419.3430416

SenSys '20, November 16–19, 2020, Virtual Event, Japan
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7590-0/20/11…$15.00
https://doi.org/10.1145/3384419.3430416

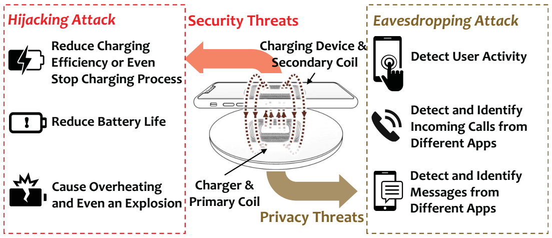

Hijacking Attack
Reduce Charging Efficiency or Even Stop Charging Process
Reduce Battery Life
Cause Overheating and Even an Explosion
Security Threats
Charging Device & Secondary Coil
Charger & Primary Coil
Privacy Threats
Eavesdropping Attack
Detect User Activity
Detect and Identify Incoming Calls from Different Apps
Detect and Identify Messages from Different Apps

Figure 1: Illustration of the discovered security and privacy threats of Qi wireless charging.

1 INTRODUCTION

With the ever-growing development of wireless charging techniques, traditional wired charging solutions have gradually become a past tense in our daily lives. Among different wireless charging standards, Qi [2], which provides 5-15 watts of wireless power transfer to portable mobile devices, has become the dominant one on the market. As illustrated in Figure 1, a primary coil is embedded in the charger (e.g., a charging pad), while the charging device (e.g., a smartphone) contains a secondary coil. During the charging process, the primary coil generates an electromagnetic field that induces a current in the secondary coil to transfer energy. To allow the charging device take control of the charging procedure, Qi specifies interoperable data communication between the charger and the charging device. However, no encryption scheme has been used to secure the communication channel, making the transmitted data bits (a.k.a., Qi messages) susceptible to being interfered with or eavesdropped. We describe how the adversary can inject malicious Qi messages to control the charging process, as well as detect and identify the charging device's activities using the eavesdropped Qi messages and the primary coil voltage of the charger in the prospectives of security and privacy threats as follows:

Security Threats. We show the potential of hijacking the communication channel by stealthily placing an adversarial coil between the charger and the charging device. Through a well-crafted alternating current acting on the adversarial coil, the adversary can inject malicious data bits to the communication channel. The adversary can further extend the data bits to complete Qi messages so as to take control of the charging process. As a consequence, the adversary can largely reduce the charging efficiency or directly terminate the power transfer. Moreover, the adversary can make the charger transmit an excess amount of power, leading to overheating, battery life reduction or even an explosion.

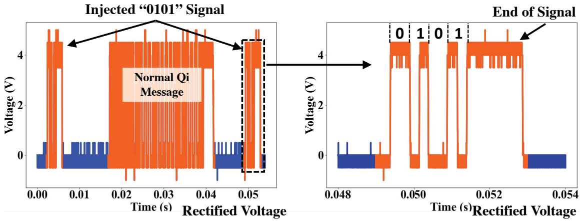


Figure 2: Illustration of injecting "0101" signals.

Privacy Threats. We show that the non-encrypted Qi messages could be easily eavesdropped through measuring the primary coil voltage of the charger. More importantly, some of these messages (i.e., *Control Error* messages) indicate the difference between the actual amount of power received and the device's desired one, which would change significantly when the charging device changes its status or is triggered by an activity such as turning on/off the screen, receiving an incoming phone call or a message from an app. Leveraging this side channel, we demonstrate an adversary could detect and identify the incoming phone calls and messages from different apps, as well as the moment where the user manually turn on the screen of the smartphone.

2 HIJACKING & EAVESDROPPING QI COMMUNICATION CHANNEL

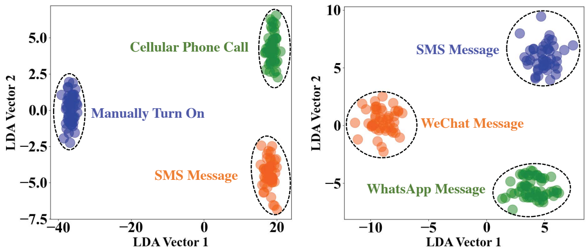
2.1 Hijacking via Malicious Message Injection

We followed the procedure of encoding and modulation specified in Qi to regulate the voltage on the adversarial coil to inject binary data bits. Specifically, we placed the adversarial coil between the wireless charger (i.e., EVALSTWBC-EP board [1]) and the charging device (i.e., a LG G7 smartphone). We used a Keysight 33522B waveform generator to produce the well-crafted alternating signal on the adversarial coil.

Qi messages are bi-phase encoded, AM modulated binary data bits with the modulation frequency set as 2 kHz, while the modulation depth is set to be at least 200 mV [2]. Through adding a 80 kHz sinusoidal wave with a 20 V peak-to-peak voltage on the adversarial coil, we observed that the primary coil voltage can be increased up to 3 V, which satisfies the requirement. By switching off the signal, the primary coil voltage would return to its original level. Thus, to inject manipulated Qi messages, the adversary can follow the bi-phase encoding mechanism to regulate the voltage of the adversarial coil (i.e., switching between LOW and HIGH states).

2.2 Eavesdropping via Primary Coil Voltage

In order to isolate Qi-message-relevant signals, we first apply a moving-max filter and a low-pass filter to extract amplitude modulated signal and eliminate irrelevant frequency components, respectively. In order to derive the bi-phase encoded data bits, we further leverage the transition points between the LOW state and HIGH state. Given that each bi-phase bit has a period of 0.5 ms, the possible distance between two adjacent transition points should be 0.25 ms (stands for a "ONE") or 0.5 ms (stands for a "ZERO"). We used the EVALSTWBC-EP board [1] and a smartphone (i.e., LG G7) as the charger and charging device, respectively. We used an oscilloscope to sample the primary coil coltage, and extensive experiments involving over 100,000 Qi messages show that Qi messages can be correctly derived with a success rate of over 99%.



(a) Three types of activities (b) Three apps of *Message*

Figure 3: Illustration of the extracted features to distinguish different activities.

3 PRELIMINARY EVALUATION

3.1 Hijacking via Malicious Message Injection

Figure 2 shows the primary coil voltage and rectified voltage when we injected "0101" signals in intervals into the communication channel. The rectified voltage is measured using the test point provided by the wireless charger board, which can better visualize pre-demodulated Qi messages to verify whether the signal is successfully injected. We can observe the bi-phase encoded "0101" signal (the following High voltage represents the end of the injected bit sequence that added by us intentionally) from the rectified coil voltage clearly, which confirms our hypothesis that an adversary can inject any malicious communication packets to control the charging process by using an adversarial coil. Through injecting *End Power Transfer (EPT) Packets*, the adversary can directly stop the power transfer, while through injecting *Control Error Packets* with different values, the adverary can reduce the charging efficiency or make the charger provide an excess amount of power.

3.2 Eavesdropping via Primary Coil Voltage

We collected the primary coil voltage and the corresponding demodulated control error sequences when the smartphone (i.e., LG G7) was triggered 100 times by (1) three types of activities: receiving a cellular phone call, a SMS message, and manually turning on the screen; and (2) three apps of the same activity (i.e., receiving messages): SMS message, WeChat message, and WhatsApp message. We then extracted 128 statistical time-frequency domain features (e.g., variance, skewness) from both the voltage signal and the decoded control error sequence which stands for each activity. We applied linear discriminant analysis (LDA) for dimensionality reduction and plot the extracted features in a 2-dimensional domain as shown in Figure 3. It's obvious to observe that different activities and apps can be easily distinguished as collected samples of each activity are densely clustered. This opens a new side channel for an adversary to infer the user's privacy while the smartphone is being wireless charged.

REFERENCES

[1] ST Microelectronics. 2020. EVALSTWBC-EP: Qi MP-A15 15W wireless charger TX evaluation kit based on STWBC-EP. https://www.st.com/content/st_com/en/products/evaluation-tools/solution-evaluation-tools/psu-and-converter-solution-eval-boards/evalstwbc-ep.html. Accessed September, 2020.

[2] Dries Van Wageningen and Toine Staring. 2010. The Qi wireless power standard. In *Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*. IEEE, S15–25.