No Free Wireless Charge: Covert Channels via Wireless Charging on Mobile Devices

Wei-Yang Chiu, Weizhi Meng and Brooke Lampe
SPTAGE Lab, Department of Applied Mathematics and Computer Science,
Technical University of Denmark, Denmark

***Abstract*—Manufacturers and users have embraced the shift from wired to wireless technologies—a shift that promises convenience, reduced cabling, and modernization. Manufacturers cut costs by cutting down on wiring; meanwhile, users experience increased accessibility and mobility on their wireless devices. Naturally, wireless media does not come with wires, but it does come with strings attached. In a wireless world, when device A talks to device B, communication is no longer physically constrained to the two of them. Instead, the communication channel is shared by many devices, opening up avenues for eavesdropping and interception.**

Wireless charging, which has become de facto functionality on many types of smart devices, is not immune to this phenomenon. Qi, the leading standard in this domain, provides a communication protocol that is unencrypted and insecure. In fact, the Qi standard enables several new means of wireless charging attack. In this paper, we propose three novel attacks on wireless charging stations, named LeakyCharge, SneakyCharge and CheatyCharge. Two are supply chain attacks, while the third would allow an adversary to perform random attacks.

***Index Terms*—Blockchain, Decentralized application, Aircraft maintenance, Smart contract, Record and data integrity**

I. Introduction

Wireless charging for mobile devices has been under development for many years. During the early phases of its adoption, there was a general lack of standardization, which, in turn, led to a general lack of compatibility. Proprietary implementations of wireless charging are either stuck in the pilot testing phase or are commercially available with limited functionality. Manufacturers are eager to claim that their devices support wireless charging, but the truth is that many of them are simply incompatible. Users are forced to purchase either (1) charging base stations developed by the device manufacturer or (2) tailor-made stations designed specifically for the device.

Compared with the standardization of USB charging—especially since the wide adoption of USB-C—wireless charging struggles to compete. Lack of standardization is particularly problematic for public charging stations, which are intended to serve many types of devices. Both private companies and public institutions—libraries, airports, etc.—have come to view public wireless charging as an effective business practice. Wireless charging services continue to grow in popularity and usage. Unfortunately, when new technologies and services become widely known and widely used, they become targets for all types of cybercriminals. Wired charging is arguably more secure than its wireless counterpart, yet it has been threatened by various side-channel attacks and abuses of the debug port [1]. Wireless charging, inherently less secure, may soon face pervasive attacks.

978-1-6654-9538-7/22/$31.00 ©2022 IEEE

A. Related Work

Nohl and Lel (2014) of SRLabs implemented a DHCP override attack on smartphones via USB [2]. They devised a spoofed USB Ethernet adapter, which acted as a typical network card; when devices connected to the spoofed adapter, a "connected media" connection was established. From the user's perspective, she is merely plugging her phone to a typical USB charging cable; however, the adversary can intercept her connection and perform man-in-the-middle (MITM) attacks.

In 2015, USB was once again exploited as an attack interface for the smartphone. The Kali NetHunter [3] demonstrated a new tactic: tricking the target device into thinking that the attack device is a human interface device (HID). They crafted a device that would be recognized by target devices as an HID (e.g., keyboards and touchpads). The device had preprogrammed key commands that could be sent to the charging smartphone directly. Later, in 2016, Meng *et al.* [4] developed an automatic juice filming charging attack. During charging, the attacker records the screen of the charging device via the cable's video output. The attack is enabled by (1) the device's video output capability and (2) a misconfiguration of the device.

Yu *et al.* [5] developed an intelligent attack specific to directional wireless charging. Given a collection of directional wireless chargers and directional rechargeable devices, an intelligent adversary can compromise the directional chargers in order to disrupt or destroy the rechargeable devices. In this scenario, the adversary can manipulate the transmission power, directional angle, etc. of the directional chargers. For the rechargeable devices, the consequences may include disruption, malfunction, damage, or even destruction due to too much or too little power. In 2022, Conti *et al.* [6] crafted a novel relay attack against Vehicle-to-Grid (V2G) infrastructure. This relay attack would enable an adversary to charge an electric vehicle while an unsuspecting victim is stuck with the payment.

Further, several inexpensive power banks have been exposed as threat installation mediums for smart devices, especially smartphones [7].

B. The Qi Standard

With Qi emerging as the de facto wireless charging standard, such functionality is no longer reserved for high-end flagship devices. According to Strategy Analytics, wireless charging-enabled devices should have hit the one billion mark by the end of 2021. Further, Strategy Analytics anticipated that public and private forces would converge to drive the evolution and popularization of wireless charging.

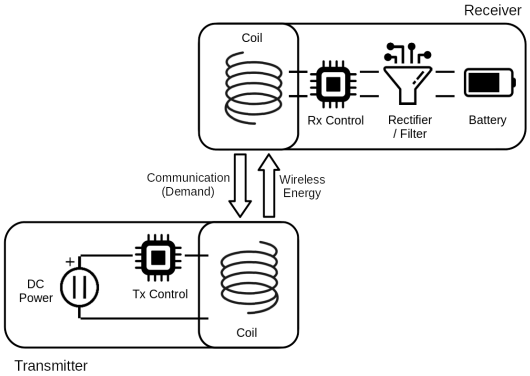

Fig. 1. A simple diagram of Qi Wireless Charging

Qi's wireless charging standard and diagram indicates that, unlike USB, wireless charging has limited data transmission capability, since it was designed to deliver energy, not data (see Figure 1). The data communication flow in Qi, before the development and release of the extended standard, was unidirectional. The device sent commands to the charging base station, and the station reacted accordingly [8][9].

This inherent limitation can partially decrease the possibility of an attack—at least compared to a USB charging solution. However, the unidirectionality of Qi does not guarantee that it is secure.

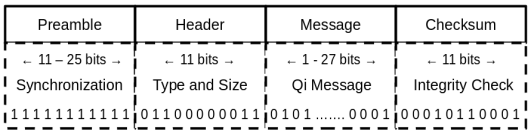

Fig. 2. Qi Message Packet

Though the extended Qi protocol has been released, it is not widely implemented; as such, many Qi charging stations are confined to unidirectional data and command flow. Generally, unidirectional wireless charging is safer than bidirectional wired USB charging (if the data lines in the USB cable have not been severed). The bidirectional flow of data and commands during USB charging enables adversaries to deliver exploits to the phone. In the unidirectional context of wireless charging, such an attack is all but impossible.

That said, communication in the Qi protocol is not purely unidirectional. Qi charging stations can still function as data receivers. The Qi message protocol allows additional information to be encoded in packets and sent to charging stations, such as the 0x25 Auxiliary Data Transfer Request in the specification [8].

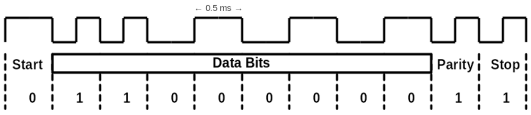

Fig. 3. Qi Message Encoding

Though the Qi protocol's data signal encoding scheme may not be the most efficient (see Figure 2 and Figure 3), it can still achieve data transfer speeds of around 90 bytes per second. Such speeds would be more than sufficient to transfer sensitive information, such as credentials (e.g., digital credit cards and authentication tokens). If we assume a typical charging time of approximately one hour, then the Qi protocol could transfer 324 kilobytes of data.

Furthermore, if combined with additional wireless mediums, the wireless charger itself could be converted into a distributing platform rather than a simple data collector.

C. Our Contributions

By exploring the wireless charging standard and channels, we identify three novel and feasible attacks, such as LeakyCharge, SneakyCharge and CheatyCharge, as below:

1) Compared to normal USB charging, the unidirectional nature of a wireless charger's data channel means that it is all but immune to attacks such as payload injection and debug port abuse (e.g., juice filming charging attack [4]). However, our *LeakyCharge* attack demonstrates that wireless charging itself can constitute a privacy threat.
2) From a data transmission perspective, the de facto standard of wireless charging precludes data transmission from the charging station to the device. However, we identify a side-channel attack—*SneakyCharge*—which sends charging pulses back to the device and, thus, breaks the protection barrier of wireless charging.
3) Lastly, we demonstrate that the wireless charging station itself can be exploited as a threat distribution center. The *CheatyCharge* attack, or a variation of that attack, would be much more effective at distributing malicious content than a USB.

For the rest of this work, Section II explains each attack type and some constrains, and Section III concludes our work.

II. Potential Wireless Charging Attacks

In this section, we demonstrate three possible attacks, each of which can be conducted via publicly available wireless charging stations. The first and second attacks necessitate supply chain access, while the third attack could be executed by anyone.

A. *LeakyCharge - Leak your data as you charge*

According to the Qi Message Packet, it has a dedicated header `0x25` to set the packet as an auxiliary data packet. If we are able to capitalize on this functionality, we could conceivably leverage it for data transfer attacks. Currently, we are constructing two modified devices: one Qi transmitter and one Qi receiver.

When the modified transmitter detects the existence of the receiver, it will begin a normal Qi conversation. Later, the modified transmitter will continue to masquerade as a normal transmitter—awaiting and reacting to commands—while secretly outputting any data through the serial bus when the data packet header is `0x25`.

The transmitter cannot send any data back to the receiver under normal circumstances. As such, one of the receiver's key responsibilities is to send the `0x25` data packet once the normal Qi conversation is complete.

Phones contain many types of sensitive data, so the LeakyCharge attack could have dire consequences for the individual victims. A user's credentials and credit cards would be obvious targets for financially-motivated attacks, but an adversary could also steal personal data for the purposes of blackmail. If the malicious charging station is used by many people, as is typical in public places, then the number of victims could be quite high.

A model of our proposed LeakyCharge attack is illustrated in Figure 4.

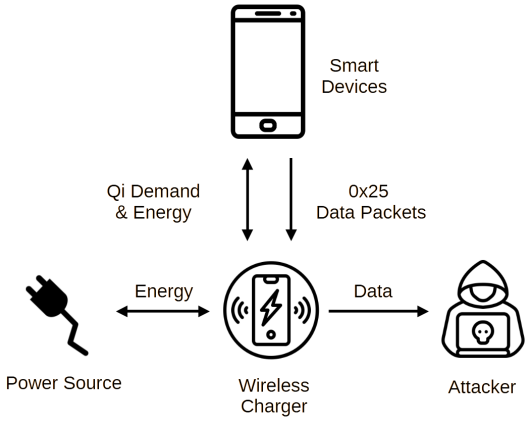

Fig. 4. LeakyCharge Model

a) Limitation: Although the LeakyCharge attack is theoretically feasible, it is currently unavailable on most smartphones. Upon review of the Android Developer Guide and the Android Developer Reference, we have not yet identified a method to inject data messages during Qi charging. Up to Android API 17, there is exactly one attribute related to wireless charging, the `BATTERY_PLUGGED_WIRELESS` attribute, which lives in the `BatteryManager` class. If the device is engaged in wireless charging, it will report a constant integer `0x4` to the application [10].

However, as the extended Qi charging standard gains traction, the establishment of bidirectional communication during wireless charging may very well involve the upper software stack rather than a dedicated subsystem.

B. *SneakyCharge - Infect your device as you charge*

SneakyCharge is essentially a reversal of the LeakyCharge attack, as shown in Figure 5. LeakyCharge leaks data through Qi protocol, meaning that the data flows from the phone to the charging station, whereas SneakyCharge applies a different method to communicate a smaller amount of information in reverse.

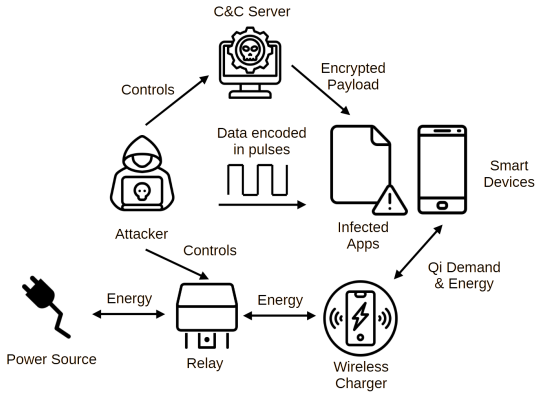

Fig. 5. SneakyCharge Model

Without the extended Qi specification, no simple exploit can force the Qi protocol to send data from the charging station to the charging device. However, we can still achieve this behavior in a creative way. We do not even need to disturb or disassemble the charging device. Instead, we use the USB power control to turn the charging station on and off, simulating "pulses." These "pulses" encode the data we want to send to the charging device.

This solution is viable, but it can be impractical when sending substantial amounts of data. That said, it is more than sufficient when sending a few numerical digits. We recognize that the simulated "pulses" will disrupt the device and the charging process, since they require repetitive on and off power switching. Therefore, we minimize the disruption by encoding each digit of the numerical value in a single pulse over a ten-second period. The digit is determined by timing: if the pulse occurs during the seventh second of the ten-second period, then the digit will be seven (as shown in Figure 6).

An infected app—or an app with an infected library—will collect the information transmitted by the charger and, subsequently, contact a C&C server for the encrypted payload. The numerical value transmitted by the charger will be the extraction key for the encrypted payload.

For the SneakyCharge attack, the potential impacts would generally depend upon the nature of the malicious payload. Mobile malware can exfiltrate credentials, credit card information, and personal data (e.g., photos). Additional possibilities include wiretapping and ransomware.

b) Limitation: The behavior of the phone and user interface when the charging process is disrupted varies from

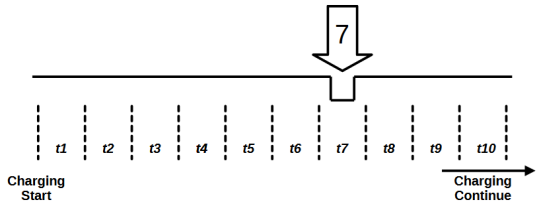

Fig. 6. SneakyCharge Data Pulse

one operating system to the next, from one manufacturer to the next, and even from one model to the next. On devices running iOS, users would be unlikely to notice the unusual charging behavior, as iOS merely changes the battery indicator in the upper right-hand corner of the screen from not charging to charging—and vice versa. For Android devices, charging behavior varies widely: some devices will display a full-screen notice that the device is charging (see Figure 7), while others are more similar to iOS—small, subtle indicators.

Fig. 7. Full-screen charging notice

Full-screen notices are far more likely to draw a user's attention to his phone, and at that point, the repeated power disturbances might prompt the concerned user to remove his phone from the charger.

To overcome this issue, we are devising methods to communicate information by controlling power output to the device. By manipulating the power output without disrupting the charging process, we can achieve the SneakyCharge attack without catching the user's attention.

C. CheatyCharge - Phish your credential as you charge

CheatyCharge leverages the wireless charger as an intermediary; behind the scenes, the NFC sticker facilitates the attack (see Figure 8).

A phishing website URL link is embedded within the NFC sticker. When a user puts her phone on the charger, the phone will immediately open up the phishing website (see Figure 9 and a short demo[1]).

Originally, we were concerned that the NFC stickers might not work as expected due to the magnetic field that the wireless charger creates; however, we have experimented with several phones and encountered no issues—the phones are perfectly capable of engaging in wireless charging and NFC tag reading at the same time.

[1]https://youtu.be/aklQ5FQHp8

Fig. 8. CheatyCharge - Modified wireless charger with NFC sticker pasted inside the charger

This type of attack promises ease of implementation and ease of installation. It is inexpensive both in terms of effort and money, and it can be conducted out of sight of the user. Moreover, this type of attack can be extended beyond the phishing example described here: system exploits and online threats are also possible. Compared to the previous two wireless charging attacks, CheatyCharge is much more flexible. As such, the impact of CheatyCharge on victim devices would depend on the goals of the phish or exploit—and the user's awareness. Some users might be more trusting—and, thus, more vulnerable—than others.

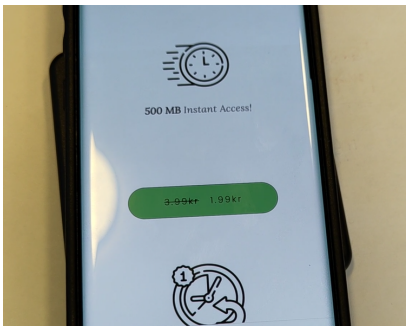

Fig. 9. CheatyCharge opens up phishing website as soon as the user starts charging her phone.

III. Conclusion

In this paper, we briefly introduced the trend toward wireless media, and we outlined the Qi wireless charging protocol. Next, we explored related work in smartphone charging attacks, and we saw that many attacks exploit the bidirectional capabilities of USB.

Though the data flow in the Qi wireless charging protocol is unidirectional, we identified three plausible attacks. The first attack exploits the protocol itself, the second attack involves energy supply disturbances, and the third attack leverages the charging station as an intermediary to perform an out-of-band attack. Some of the proposed attacks have several limitations which interfere with practicality. However, we seek to enhance the practicality of our wireless charging attacks during our ongoing work.

ACKNOWLEDGMENT

This research has received funding from the European Union's Horizon 2020 EU Research & Innovation program under Grant Agreement No. 952696 (ASSURED Project).

REFERENCES

[1] N. Nissim, R. Yahalom, and Y. Elovici, "Usb-based attacks," *Computers & Security*, vol. 70, pp. 675–688, 2017.

[2] S. Blanchet, "Badusb, the threat hidden in ordinary objects," 2018.

[3] R. Kernel, Apr 2019 (access on 1 February 2023). [Online]. Available: https://github.com/offensive-security/kali-nethunter/wiki\#60-kali-nethunter-attacks-and-features

[4] W. Meng, W. H. Lee, S. Murali, and S. Krishnan, "Juicecaster: towards automatic juice filming attacks on smartphones," *Journal of Network and Computer Applications*, vol. 68, pp. 201–212, 2016.

[5] N. Yu, X. Wang, H. Dai, and G. Chen, "A novel strategy under charger capture attack in wireless rechargeable sensor networks," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2020.

[6] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack onelectric vehicle charging system," in *Computer Security – ESORICS 2022*, V. Atluri, R. Di Pietro, C. D. Jensen, and W. Meng, Eds. Cham: Springer International Publishing, 2022, pp. 488–508.

[7] R. Spolaor, L. Abudahi, V. Moonsamy, M. Conti, and R. Poovendran, "No free charge theorem: A covert channel via usb charging cable on mobile devices," in *Applied Cryptography and Network Security: 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings 15*. Springer, 2017, pp. 83–102.

[8] W. P. Consortium, "The version 1.3 qi specification." [Online]. Available: https://www.wirelesspowerconsortium.com/knowledge-base/specifications/download-the-qi-specifications.html

[9] D. Van Wageningen and T. Staring, "The qi wireless power standard," in *Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*. IEEE, 2010, pp. S15–25.

[10] Google, Apr 2012. [Online]. Available: https://developer.android.com/reference/android/os/BatteryManagers