Inducing Wireless Chargers to Voice Out

Donghui Dai, Zhenlin An, Lei Yang
Department of Computing, The Hong Kong Polytechnic University
{dai,an,young}@tagsys.org

ABSTRACT

Recent advances have demonstrated that voice assistants or speech recognition systems can be manipulated by malicious and inaudible voice commands. However, the previously proposed attacks require an acoustical generator (e.g., a speaker or a capacitor) to trigger mechanical vibrations at a microphone diaphragm. In this work, we investigate a new type of inaudible command attack using wireless chargers. Specifically, the magnetic interference generated by a wireless charger can induce an inaudible sound at a nearby microphone, without triggering any mechanical vibrations, even if the microphone is equipped with a Faraday cage and an internal electromagnetic interference filter already. By taking advantage of this new insight, we will present a novel inaudible command attack demo that can inject inaudible voice commands into smart devices that are being charged or near to a charger. We conduct extensive experiments with 17 victim devices (iPhone, Huawei, Samsung, etc.) and six types of voice assistants (Siri, Google STT, Bixby, etc.). Evaluation results demonstrate the feasibility of the proposed attack with commercial charging settings.

CCS CONCEPTS

• **Networks** → **Mobile and wireless security**.

KEYWORDS

Malicious Voice Commands, Wireless Charging, Electromagnetic Interference

ACM Reference Format:
Donghui Dai, Zhenlin An, Lei Yang. 2022. Inducing Wireless Chargers to Voice Out. In *The 28th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '22), October 17–21, 2022, Sydney, NSW, Australia.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3495243.3558763

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9181-8/22/10…$15.00
https://doi.org/10.1145/3495243.3558763

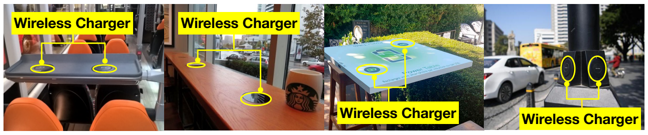


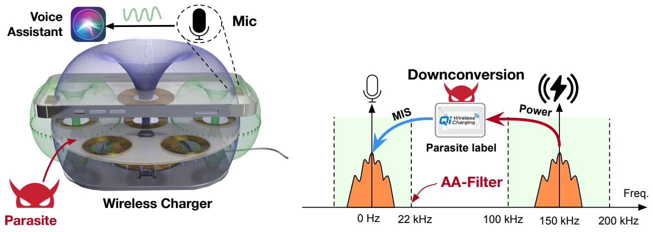
Fig. 1: Illustration of wireless charging services in public. As the fast spread of wireless charging technology, wireless chargers are becoming free and public facilities everywhere.

1 INTRODUCTION

Voice assistants have become an increasingly popular human-computer interaction approach in smart devices (e.g., smartphones or wearables) with the recent incredible advances achieved in the field of speech recognition. For example, Apple Siri [1] and Google Now [2] allow users to initiate phone calls and launch apps through their voices; With the spread of voice assistants, a built-in microphone has become a new vulnerability under sneaky and malicious *inaudible voice attacks*; in these attacks, inaudible voice commands, which are unintelligible and unnoticeable to human listeners, can take control of the victim devices [3]. The known voice command attacks can be initiated via different types of inaudible media, such as the ultrasound [3–8], laser [9], and RF signal [10–12].

In this demo, we explore a new type of inaudible voice attack through the wireless chargers, which produce the well-modulated magnetic interference to inject the voice commands into the microphones as if they were recorded from a physical sound. Wireless charging delivers power from an energy supply to smart devices without contact. Wireless charging is becoming a de facto power supply solution for a vast number of smart devices, especially for wearables (such as Apple Watch or AirPod). Fig. 1 shows some typical public wireless charging stations, where numerous free wireless chargers are deployed in public everywhere and hundreds of millions of people are benefiting from them every day. Nevertheless, these public wireless chargers are becoming potential security breaches according to our insight.

Achieving magnetic-inductive sound (MIS) at microphones is very challenging because there exists an about 80 kHz frequency gap between microphones and chargers. Specifically, a microphone can only record the voice below 22 kHz where higher frequencies will be completely filtered out, whereas a wireless charger produces magnetic fields at 100 to 200 kHz. To address this issue, we propose a novel attack approach. We envision that an adversary attaches small and thin accessory equipment called *parasite* onto a public wireless charger, as shown in Fig. 2. The parasite can use an RX coil to "steal"



(a) Parasite Attack (b) Frequency Domain

Fig. 2: Parasite Attack. (a) show the magnetic field of parasite attack and (b) show how it downconverts the high-frequency magnetic-inductive sound into the audible spectrum.

power from the host charger and drives one of the TX coils to generate the magnetic-filed in the voice frequency, which further produces MIS at microphones.

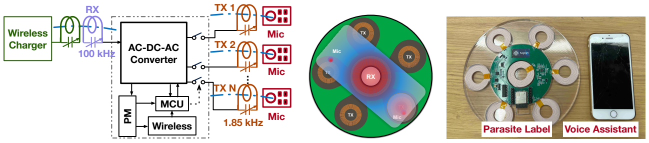
We have tested the attack on 17 smart devices, which involve six voice controllable or speech recognition (SR) systems. Each attack is successful on at least one SR system. The attacking demos can be found at [13]. We believe this list is by far not comprehensive. Nevertheless, this study serves as a wake-up call to consider the security breach caused by the magnetic interference and reconsider what functionality shall be introduced in voice assistant systems. More details can be found in our full paper in IEEE S&P 2023 [14].

2 DESIGN OF PARASITE ATTACK

Parasite attack launches the attack through accessory equipment called parasite. The battery-free parasite is as thin and small as an NFC tag. The adversary adheres to the parasite on the top of a charger and disguises it as a sticker by printing some signs, e.g., “Free Charging”, which mislead users to view a parasite label as a part of the actual wireless charger. The parasite presents between the host wireless charger and the smart device as shown in Fig. 2(a). We design the parasite as a battery-free device to be small, compact, and not eye-catching. Fig. 3 shows the architecture of a parasite. Specifically, a parasite label is composed of an inner RX coil and several outer TX coils. After the power transfer contract is established, the parasite uses the inner RX coil to steal power from the underneath charger and boosts the attack with outer TX coils. The center of the RX coil is empty without a ferrite shield such that the magnetic field created by the host charger can reach the RX coil of the victim device with minimal attenuation. Multiple TX coils are deployed on a ring to ensure at least one TX coil is located nearby the victim’s microphone even if the device’s posture is uncertain. The key module of the parasite label is the power converter between the RX coil and Tx coil, that is, the AC-DC-AC converter. It has two purposes: first, it can rectify AC to DC for powering up the MCU and the communication; second, it also converts the high-frequency current at 100 kHz harvested from the RX coil down to a low-frequency voice signal for TX coils. In such a way, the parasite exactly transmits the voice in the operating range of a microphone.

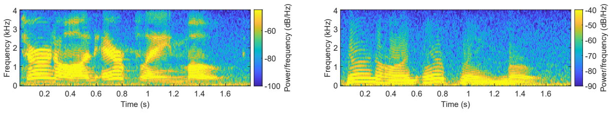
Table 1: Experimental devices and speech recognition results.

Model	SR	Recog.	Model	SR	Recog.
V9 Pro	Xiaoai	✓	GT2 Pro	Xiaoyi	✓
V11	Xiaoai	✓	Watch 7	Siri	✓
Mate 20 Pro	Xiaoyi	✓	iPad(6th)	Siri	✓
Honor V30 Pro	YOYO	✓	iPad Air 4	Siri	✓
iPhone 8	Siri	✓	iPad mini 6	Siri	✓
iPhone 11	Siri	✓	ADMP401	Google	✓
iPhone 12	Siri	✓	SPH0690LM4H-1	Google	✓
Galaxy 21	Bixby	✓	KY-037	Google	✓
Galaxy Watch 4	Bixby	✓			



(a) Schematic (b) Top view (c) Prototype

Fig. 3: Architecture of a parasite label and its prototype. (a) shows the schematic of the parasite label. (b) show the top view of a parasite label. (c) show the prototype of parasite label.



(a) Original TTS voice (b) Magnetic-inductive sound

Fig. 4: Spectrum comparison. (a) and (b) show the voice recorded by iPhone 8 but injected by a speaker and a TX coil, respectively.

3 DEMO: PARASITE ATTACK

As shown in Fig. 3(c), we prototype the parasite label using an annular PCB, which holds the main circuits (e.g., MCU, rectifier, and inverter). We test our attacks across eight types of smartphones, three types of smartwatches, and tablets respectively. We also test three types of add-on microphones, which are the most popular components for developing smart wearables. We connect these microphones to an Arduino for voice recording. Table 1 summarizes the experiment results. The attack is viewed as a “success” (ticked with √) once the SR system can successfully recognize the short wake-up voice commands (e.g., “Hey Siri", “Hey Google" and “Hi Xiaoai") recorded by the microphones under attacks. Overall, regardless of the types of models, manufacturers, and SR systems, the commercial off-the-shelf devices all fail to defend against the proposed attack. Fig. 4 compare the spectrum between the original and parasite-injected voice. The test voice clip is “turn on airplane mode”. Clearly, the parasite-injected voice exhibit similar patterns as the original voice.

Acknowledgement. This study is supported by NSFC Excellent Young Scientists Fund (Hong Kong and Macau) (No. 62022003), NSFC Key Program (No. 61932017), NSFC General Program (No. 61972331), UGC/GRF (No. 15204820, 15215421), and National Key R&D Program of China 2019YFB2103000.

REFERENCES

[1] "Apple Siri," https://www.apple.com/siri/, 2017.

[2] "Google Now," https://www.androidcentral.com/google-now, 2016.

[3] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proc. of ACM CCS*, 2017, pp. 103–117.

[4] N. Roy, H. Hassanieh, and R. Roy Choudhury, "Backdoor: Making microphones hear inaudible sounds," in *Proc. of ACM MobiSys*, 2017, pp. 2–14.

[5] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, "Inaudible voice commands: The long-range attack and defense," in *Proc. of NSDI*, 2018, pp. 547–560.

[6] C. Yan, G. Zhang, X. Ji, T. Zhang, T. Zhang, and W. Xu, "The feasibility of injecting inaudible voice commands to voice assistants," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[7] M. Zhou, Z. Qin, X. Lin, S. Hu, Q. Wang, and K. Ren, "Hidden voice commands: Attacks and defenses on the vcs of autonomous driving cars," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 128–133, 2019.

[8] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, "Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves," in *Network and Distributed Systems Security (NDSS) Symposium*, 2020.

[9] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.

[10] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

[11] C. Kasmi and J. L. Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.

[12] Y. Wang, H. Guo, and Q. Yan, "Ghosttalk: Interactive attack on smartphone voice system through power line," *arXiv preprint arXiv:2202.02585*, 2022.

[13] "Magsound Project Website," https://anplus.github.io/magsound/, 2022, Last accessed August, 2022.

[14] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2023.