EM-Whisperer: A Voice Injection Attack via Powerline for Virtual Meeting Scenarios

Jiachun Li*, Yan Meng*‡, Le Zhang*, Fazhong Liu†, Haojin Zhu*‡
* Department of Computer Science and Engineering,
School of Electronics, Information and Electrical Engineering (SEIEE), Shanghai Jiao Tong University, Shanghai, China
† School of Cyber Science and Engineering, SEIEE, Shanghai Jiao Tong University, Shanghai, China
{jiachunli, yan_meng, sj-16-zl, liufazhong, zhu-hj}@sjtu.edu.cn

***Abstract*—The rapid development of virtual meetings brings much convenience to the user. Due to the limited battery size of smart devices, it is quite common to attend meetings while charging. However, the interface of charging also opens the door to performing audio injection attacks, which may cause series results in the meetings. In this study, based on this insight, we propose a voice injection attack for daily meetings, which is named EM-Whisperer. By modifying simple Commercial-Off-The-Shelf (COTS) devices, the attacker can inject the malicious voice stealthily and remotely with the assistance of the Frequency Modulated (FM) electromagnetic wave. For the designation of EM-Whisperer, we set up two phases: the content based analysis and the voice injection implementation. The content based analysis can be utilized for the selection of the attacking malicious words. After this phase, we can perform the proposed voice injection attacks. Finally, We implement EM-Whisperer for various virtual meeting scenarios in which users utilize various smart devices, including smartphones, laptops, and personal computers. It can achieve more than 90% in attack success rate when facing various impact factors, which proves the superiority of the proposed attacks among existing works.**

***Index Terms*—voice injection, powerline, FM signal, virtual meeting**

I. Introduction

Virtual meetings are regarded as a promising solution when facing COVID. It is so popular that the participants can interact with each other conveniently online, like sharing the screen, presenting slides, and playing games. It is reported that the market for virtual meetings is estimated to grow with a compound annual growth rate (CAGR) of 14.2% [1], which may reach 27.19 billion by 2028.

Despite the great benefits of virtual meetings, there is a severe problem with battery energy when attending meetings online. Since most of the smart devices are battery constrained [2], and the virtual meeting application is of high energy cost, it is very common to attend the meeting and use the voice interface (*e.g.*, give a speech, free chat) when charging by powerline. As the charging interface is integrated with the audio interface currently, this phenomenon opens a door for the *voice injection attack*. Specifically, as the voice interface is integrated with the charging interface in the Type-C port instead of using the 3.5 mm port [3], the attacker can leverage the habit of talking while charging to launch the voice injection attack.

There are a number of researchers that have investigated the inaudible voice injection attacks on smart devices. [4], [5], [6] utilize the wireless signal (*e.g.*, ultrasonic wave) to carry the malicious voice command to perform the aforementioned attacks. Furthermore, the most relevant work [7] considers using Bluetooth (*i.e.*, distance of about 30 cm) to inject malicious voice commands on smartphones when charging, which easily raises suspicion from the victim. In summary, existing works pay less attention to the vulnerability of the charging interfaces when attending the meetings, and also face several limitations (*e.g.*, transmitting distance, specific types). Thus, it is important to present a stealth, remote, effective method for voice injection, which can pose a threat to charging interfaces, especially for virtual meeting scenarios.

In this study, to overcome the aforementioned challenges when applying existing methods, we design EM-Whisperer, a novel voice injection attack via a powerline for various meeting scenarios. Firstly, the attack is easy to be launched with little modification on the Commercial-Off-The-Shelf (COTS) devices, which is in a small size for the consideration of stealthiness. Secondly, the attacker can perform the attack in a remote location with the carrier of Frequency Modulated (FM) electromagnetic wave. Finally, the proposed attack is robust and effective when applied in various meeting scenarios.

However, it is still challenging to build an aforementioned attack with the advantages of stealthiness, remoteness, and effectiveness. Particularly, we should address the following challenges: (i) Concerning the characteristics of virtual meeting (*e.g.*, noisy background), how to launch the attack stealthily and conveniently? (ii) How to overcome the challenge of distance with the size limited device? (iii) How to verify the usability and effectiveness of the proposed attacks in real world environments?

In this paper, we address the aforementioned challenges in detail. Firstly, for challenge 1, to fit the characteristics of the meeting scenario, we design a content based analysis module and trigger the attacking phases, which can assist to discover the malicious words appropriately. Then, to reach the goal of being stealthy and convenient, we utilize the COTS device in small size to inject the malicious voice. Secondly, for challenge 2, to improve the distance of the transmission, we establish an FM transmitter and receiver model in this study, which leverage the advantages of FM electromagnetic wave.

‡ Yan Meng and Haojin Zhu are corresponding authors.

Finally, for challenge 3, we implement EM-Whisperer in the real world and evaluate the impact factors (*e.g.*, the distance, the mobility). Furthermore, to address challenge 3, we evaluate EM-Whisperer on various meeting scenarios, which contain most types of smart devices.

Concerning the performance of EM-Whisperer, it can achieve an attack success rate of 97% when deploying on types of smart devices, including smartphones (*e.g.*, Mi 9), laptops (*e.g.*, Lenovo Xiaoxin Pad 2022), and personal computers (*e.g.*, Lenovo Legion Y7000 2020). According to the experimental results, the performance of EM-Whisperer is superior to existing works. The contribution of this work is summarized below:

1) We propose a novel voice injection system, EM-Whisperer, which is a stealth, remote, effective method for virtual meeting scenarios. Note that, it is convenient and stealth only by the usage of COTS devices in small sizes.
2) We design two phases for the attack. For phase 1, we conduct case studies to discover the appropriate malicious words for meetings. In phase 2, we design an FM radio and inject the malicious voice command by it into the charging powerline.
3) To address the usability of the proposed attack, we evaluate the attacking performance of EM-Whisperer on various meeting scenarios, including smartphones, laptops, and personal computers. EM-Whisperer achieves the attack success rate of 97%. It also gets good results when changing various impact factors.

The remainder of this paper is organized as follows. The background and the related works are introduced in Section II. We elaborated the designation of the proposed attack in Section III. In Section IV, the details of EM-Whisperer are introduced, which is followed by the discussion, the conclusion in Section V, Section VI respectively.

II. Background and Related Works

In this subsection, we introduce the integrated interface of Type-C, which is in charge of the charging function and the audio interaction. After elaborating on this insight, we show the related works in this section.

A. The Charging Interface in Type-C Port

Recently, it is a common trend that the developer integrates the charging interface and the audio interface together recently. As a result, it also opens a door for the voice injection attack when charging.

When the user is charging the smart device in the virtual meeting, the charging process can be shown as follows: Firstly, the charging system conducts the detection of plugging, in other words, checking the downstream/upstream facing port. After that, it utilizes the CC port to check the flipped issue, which is followed by the shifting of the current mode, and the recognition of port configuration. Finally, the data can be transmitted via the USB 2.0 port (*e.g.*, A6, A7) while charging adaptively.

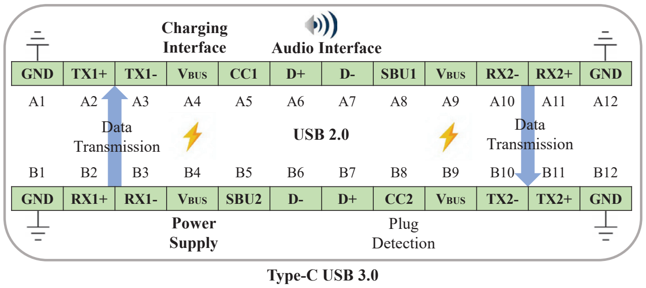


Fig. 1: The charging interface in USB Type-C.

Then, we introduce the function of each port in Fig. 1. In Type-C powerline, it maintains the function of USB 2.0 and adds some useful ports, A2, A5, and A9. Port D+ and port D-, which is A6, and A7 as shown in Fig. 1 can be utilized to transmit the voice command. Moreover, fast data transmission can be conducted in ports A2, A3, A10, and A11. The power energy is supplied in V_{BUS} at ports A9 and B4.

Thus, since the charging interface and the audio interface are both open when charging the smart device, it is possible for the attacker to inject the malicious voice by powerline (*i.e.*, the charging interface), when the victim is attending the meeting by the charging device.

B. Related Works about Voice Injection

In this subsection, we introduce the existing works of attacking charging interfaces and the inaudible attacks.

Existing works pose threats to the charging interface. [8], [9] can perform the juice jacking attack [10], which can inject the malicious application and the malicious command (*e.g.*, AT command) into the smart devices while charging. [11] shows that the charging curve can be exploited to perform the side channel attack, which can infer user privacy (*e.g.*, the preference of websites, and applications). Similar to the aforementioned works, [12], [13] discover the vulnerability of wireless charging, which performs side channel attacks from the software side and the hardware side. [14] present jamming attacks targeting the charging system of vehicles. In summary, the aforementioned works pay less effort into the injection of voice when charging, which motivates our work.

According to state-of-the-art works, inaudible attacks can threaten the security of smart devices. For instance, [4], [5], [6] leverage the wireless media to inject the malicious voice into smart devices. Moreover, [15] utilize the light to carry the malicious command for injection to control the voice assistants in smart homes.

In particular, [7] proposes a voice injection method on the charging interface of smart devices. Different from this work, our work is designed for various meeting scenarios (*i.e.*, smartphones, laptops, personal computers) which are used in virtual meetings, especially considering the malicious words. We also extend the attacking distance with the assistance of FM electromagnetic waves.

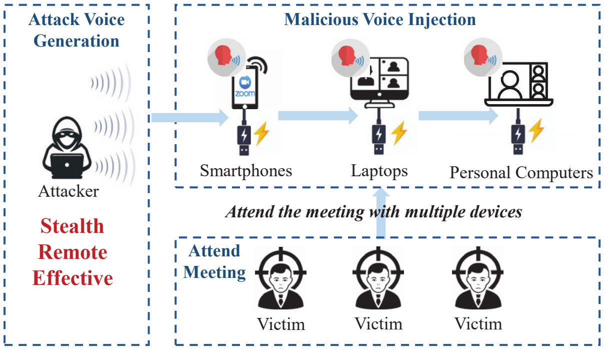


Fig. 2: The threat model of this work.

III. System Design

In this subsection, we propose the voice injection attacking system, EM-Whisperer. In particular, we introduce the threat model, the system overview, and the designation of the proposed system.

A. Threat Model

In this study, we assume the attacker can modify the charging powerline with small modifications. The modified powerline can be rented by the victim when they attend the virtual meeting in public places, like the airport, or the train station. After that, it is reasonable to assume the victim opens the interactive audio interface to talk in the meeting scenarios while charging.

B. Overview of EM-Whisperer

In this subsection, firstly, we elaborate on the motivation of the designed attacking system, EM-Whisperer. Then, we show the overview of EM-Whisperer.

The motivation of EM-Whisperer is that, since the charging interface and the audio interface is integrated into Type-C, when the victim is participating in the meeting and using the audio interface while charging, the attacker can inject the malicious voice with wireless media according to this phenomenon.

Based on this motivation, as shown in Fig. 3, we design EM-Whisperer, which consists of two phases: the content based analysis and the voice injection implementation. As for the overview, the attacker can first generate the malicious words and analyze them by the content based module to select an appropriate one. Then, EM-Whisperer will start injecting the malicious voice into the charging powerline via FM electromagnetic wave and change the attacking parameters according to the feedback results.

C. System Designation

In this subsection, we elaborate on the details of the proposed system, which consists of the selection of the malicious words, and the malicious voice injection implementation. For the two aforementioned phases, we design the content based analysis, and the frequency modulated based attacking schemes respectively.

TABLE I: Case study when changing the attacking malicious words.

Device	Smartphones:Mi 9				Laptops:Lenovo Xiaoxin Pad			
Malicious Words	**Okay**	**Hi**	**Okay Okay**	**Hi Hi**	**Okay**	**Hi**	**Okay Okay**	**Hi Hi**
ASR	95%	92%	96%	92%	96%	94%	96%	94%
RR	99%	99%	98%	99%	100%	99%	99%	99%

1) Malicious words selection by content based analysis: To improve the injection performance of EM-Whisperer, it is important to select an appropriate malicious word for preparation. In order to select this word, we conduct a case study named content based analysis as follows:

Inspired by [16], we select some malicious words from some popular voice recognition systems. In this study, we evaluate the performance of “Okay”, “Hi”, “OkayOkay”, and “HiHi”, which are in various richness and content. Then, we perform the transmission process as shown in Fig. 3. To evaluate the performance, we recruit 10 users to transcribe the received voice. Then, we can select the appropriate words among the aforementioned malicious words.

In this study, we choose the attack success rate (ASR), and recovery rate (RR) to evaluate the performance of EM-Whisperer. For the definition of the attack success rate, if the injected voice appears in the meeting, we calculate the ASR as the ratio of the time period of the injection voice and the overall time. As for the recovery rate, we recruit 10 users to transcribe the injected voice simultaneously. Thus, the RR is calculated as the ratio of the correct recovered words and the overall words in the meeting.

According to the results of the case study, it is observed that for the two given smart devices (*i.e.*, smartphones, laptops), when we select “OkayOkay” as the malicious word before the malicious voice injection, the performance is the best one. Thus, in this study, we leverage the malicious word “OkayOkay” as the prefix frame in the malicious injection voice.

2) Frequency modulated based attacking implementation: After the selection of the malicious word for attacking, to overcome the limitation of transmission distance in existing works, we design a Frequency Modulated (FM) based attacking method. Specifically, it leverages the advantages of Frequency Modulated electromagnetic waves, which can be transmitted over a long distance and overcome the impact of obstacles. The details are shown as follows.

As mentioned in Section III, the injected voice can be represented as $v_m = [v_w, v_r]$, where v_w denotes the malicious word, v_r is for the designed injecting voice in the virtual meeting. Furthermore, v_m is the combined injected voice in this study.

Nonlinearity effect. Since the attacking voice sample is from the attacker’s voice command, which is pre-collected by the audio recorder, it will face the challenge of the nonlinearity effect. Let the input voice as v_m, and the generated output signal v_{out} is:

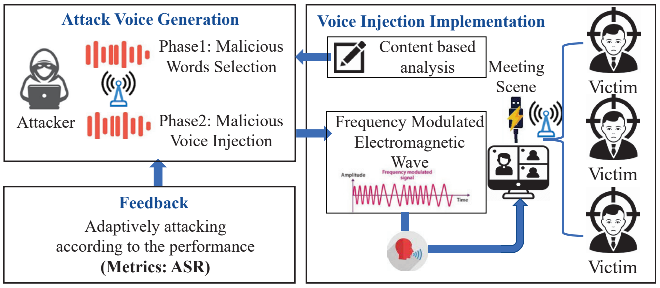

Attack Voice Generation
Attacker
Phase1: Malicious Words Selection
Phase2: Malicious Voice Injection
Voice Injection Implementation
Content based analysis
Meeting Scene
Frequency Modulated Electromagnetic Wave
Amplitude
Frequency modulated signal
Time
Victim
Victim
Victim
Feedback
Adaptively attacking according to the performance
(Metrics: ASR)

Fig. 3: The system designation of EM-Whisperer.

$$v_{out} = A * v_m + B * v_m^2, \tag{1}$$

where A and B are the gain of the channel. For instance, if the voice signals like a simple tone signal (*i.e.*, $cos(2\pi f_m t)$ is transmitted on a carrier with the central frequency f_c, it will generate many high frequency components (*e.g.*, $f_m, f_c - f_m, f_c + f_m, 2f_c$) due to this issue. To address this, EM-Whisperer implements the low pass filter in this study.

Then, after introducing the solution of the nonlinearity effect, we elaborate on the details of modulation and demodulation of the voice injection part.

Modulation process: For a malicious input signal $v_m = [v_w, v_r]$, to improve the transmitting distance, we design an FM based modulation scheme to transmit it over the air. Specifically, the modulated FM electromagnetic wave embed with the malicious voice is sent by the transmitting antenna. And the modulated signal $V_{FM}(t)$ is shown as:

$$V_{FM}(t) = A_n \cos\left(\omega_c t + K_{FM} \int v_m(t)dt\right), \tag{2}$$

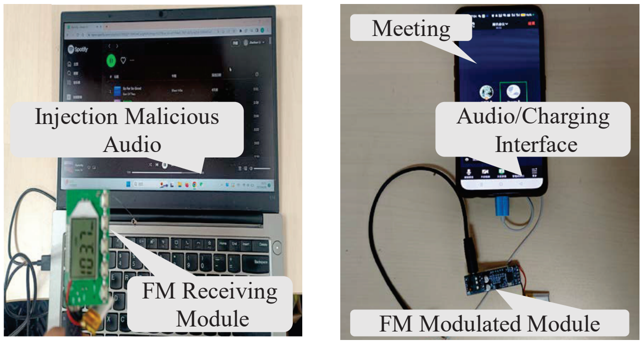
where A_n is the amplitude of the carrier wave, ω_c is the angular frequency of the carrier wave, which is calculated as $2\pi f$. K_{FM} represents the frequency sensitivity of the FM modulator.

According to the aforementioned equation, the modulation process is as follows: firstly, the input signal will be given to an integrator to generate $\int v_m(t)dt$. A carrier oscillator is utilized for generating a carrier wave, which is $cos(\omega t)$. Then, the phase modulator can modulate the processed input signal into the carrier, and generate the modulated signal $V_{FM}(t)$.

Since the voice signal $v_m(t)$ can be simplified as a simple tone signal for a given time period, which is $v(t) = \cos(2\pi f_m t)$. To simplify the derivation, the following part of modulation and demodulation is all based on a simple tone signal. Thus, we can derive the modulated signal $V_{FM}(t)$ as:

$$V_{FM}(t) = A_n \cos\left(\omega_c t + \frac{K_{FM}}{2\pi f_m}\sin(2\pi f_m t)\right). \tag{3}$$

Then, the modulated signal will be received by the receiving antennas in the demodulation part, which can recover the malicious input signal and inject it via the charging interface when meeting.



Attacker Side **Victim Side**

Fig. 4: The experimental setting of EM-Whisperer.

Demodulation process: After receiving the modulated FM signal over the air from the receiving antennas, the demodulation part is utilized to recover the malicious injection voice v_m and inject it into the charging interface. The detailed process is as follows:

Firstly, the received signal $V_{FM}(t)$ will be given to a frequency detection discriminator (*i.e.*, differentiator), which can generate an FM amplitude modulation wave as:

$$\begin{aligned} \frac{dV_{FM}(t)}{dt} = & A_n\left(2\pi f_c + K_{FM}\cos(2\pi f_m t)\right) * \\ & \sin\left(2\pi f_c t + \frac{K_{FM}}{2\pi f_m}\sin(2\pi f_m t)\right). \end{aligned} \tag{4}$$

Then, the phase shifter can transform the subpart $\sin\left(2\pi f_c t + \frac{K_{FM}}{2\pi f_m}\sin(2\pi f_m t)\right)$ into cosine function. After that, the envelope detector and the debiasing module can collaborate to generate the malicious injecting voice v_m and inject it into the charging interface.

Furthermore, to ensure the performance of voice injection, EM-Whisperer also design a feedback module to change the parameters adaptively, for example, the orientation of the antennas, and the amplitude of the signals.

In summary, with the collaboration of the designed schemes (*i.e.*, content based analysis, voice injection implementation), the malicious voice can be injected into the charging powerline when the victim is attending the meeting.

IV. Evaluation

In this subsection, we evaluate the performance of the proposed attacking system, EM-Whisperer. Moreover, to evaluate the usability of the attacks, we implement EM-Whisperer on various meeting scenarios, including injecting malicious voice on smartphones, laptops, and personal computers. Furthermore, we also measure the impact of various factors (*e.g.*, the distance, the mobility) on this attack to show the attacking effectiveness.

A. Experimental Settings

As shown in Fig. 4, we set up the attacking system, EM-Whisperer based on the COTS devices in small size, which can be embedded into the powerline.

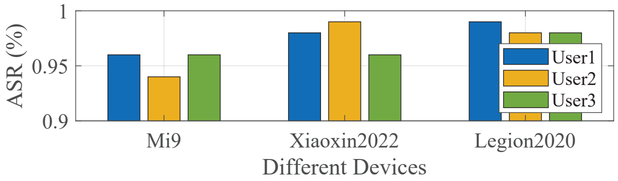


Fig. 5: Overall performance of EM-Whisperer (ASR metrics).

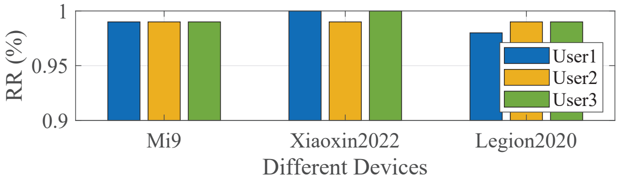


Fig. 6: Overall performance of EM-Whisperer (RR metrics).

1) For the attacker side, we play the malicious voice by the personal computer, which is the combination of the attacking words and the malicious command from the pre-collected audio. For the transmitter, EM-Whisperer modifies the TEA5767 [17] to send the FM electromagnetic wave.
2) For the victim side, the victim is deceived to use the modulated audio/charging cables. The designed receiving module we selected is the chip QN8035 [18]. In the meeting scenario in Fig. 4, to further investigate the integration of the audio interface and the charging interface, we also utilize ALC5686 [19] audio chip in this study.

The data collection process is as follows. we select a 30 second malicious voice for injection. 3 recruiters are required to attend a meeting on various meeting scenarios when charging. Then, we run the attacking system, EM-Whisperer. Then, we capture the meeting audio and detect whether the malicious voice is injected.

B. Overall Performance

Firstly, as defined in Section III, we utilize the attack success rate (ASR) and the recovery rate (RR) to depict the performance of EM-Whisperer. In the overall evaluation, we evaluate EM-Whisperer with 3 users on various meeting scenarios (*i.e.*, smartphones, laptops, personal computers). The detailed results are shown in Fig. 5 and Fig. 6.

It is observed that EM-Whisperer can achieve an average attack success rate of 98% among the 3 users. The RR is also above 98% in this study, which proves the effectiveness of EM-Whisperer. In summary, the attacking system EM-Whisperer poses the vulnerability of charging interfaces of smart devices.

C. Impact of Various Factors on EM-Whisperer

In this subsection, we evaluate the impact of various factors on EM-Whisperer, which contains: the impact of transmission distance, the impact of the obstacle, and the impact of mobility.

Impact of transmission distance: To demonstrate the advantages of the proposed FM based transmission, we evaluate the performance of EM-Whisperer in various distances with no obstacle. The transmission distance is selected as 1 meter, 3 meters, 5 meters, 10 meters, and 15 meters in this study.

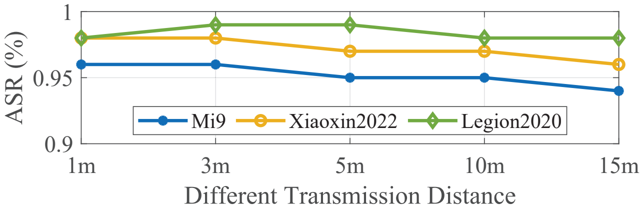


Fig. 7: The impact of the distance on EM-Whisperer.

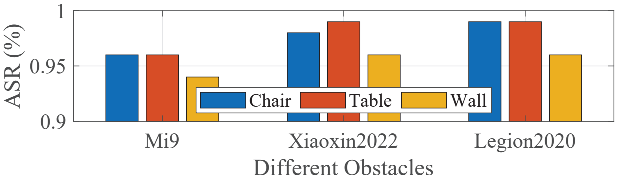


Fig. 8: The impact of obstacles on EM-Whisperer.

As shown in Fig. 7, when the transmission distance increases, the performance of EM-Whisperer decreases simultaneously. However, the ASR is still around 95% and the RR is above 98%, which proves the usability of the proposed attacks.

Impact of obstacle: To explore the impact of existing obstacles on the transmission distance, we set the transmission distance at 3 meters and change the obstacles in the transmission path. In this study, the obstacle is set as a chair, a table, and a wall.

As illustrated in Fig. 8, when the transmission distance is set as 3 meters, the obstacles in the path is of little impact on the performance of voice injection. Even if the attacker is across the wall, the performance of voice injection can still achieve above 95% in ASR, which proves the stealthiness of our work.

Impact of mobility: Since it is reasonable that the victim may attend the meeting while charging in a moving scenario, for instance, walking, jogging, or driving a vehicle. Thus, we evaluate the impact of mobility in this study. Specifically, the mobile speed of the attacker and the victim is set as 0.5m/s, 1m/s, 3m/s, 5m/s, and 10m/s, which is designed to simulate the conditions of walking, jogging, driving, *etc*.

It is observed in Fig. 9 that when the moving speed of the attacker and the victim increases, the performance of EM-Whisperer will decrease due to the loss of message. However, the ASR and the RR can still achieve 94% and 95% in the driving condition, when the moving speed is set above 5m/s. Thus, the experimental results show the robustness of EM-Whisperer.

In summary, the performance of the designed attacking system EM-Whisperer is still of high effectiveness when changing different impact factors, which proves the superiority of our work.

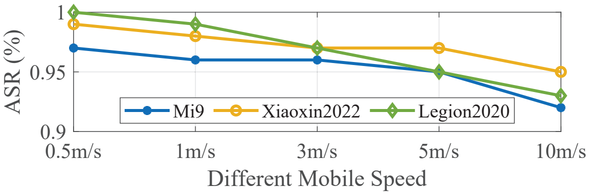


Fig. 9: The impact of mobility on EM-Whisperer.

V. Discussion

In this subsection, we introduce the limitation of EM-Whisperer, which contains the scale of the attacking device, the stability of the modification, and the orientation of the antenna.

A. Scale of the Attacking Devices

In this study, we conduct some modifications based on the Commercial-Off-The-Shelf (COTS) device, which is in small size. However, it still faces some difficulties when embedding the small attacking device in a charging powerline for the victim side. Thus, it is still under research to improve the scale of the attacking device.

B. Stability of the Modification

Since we conduct some modifications in the charging powerline, which is shown in Fig. 4, it is required to keep EM-Whisperer in a stable posture. Thus, for future work, we will design more advanced equipment to optimize this issue and fix the challenge of stability.

C. Orientation of the Antenna

As we all know, if the transmitter antenna and the receiving antenna are calibrated correctly, the performance of signal transmission will be the best in all conditions. In this study, we have to calibrate the orientation antennas several times to ensure the best performance of voice injection, which is an open question. Furthermore, to improve the performance of EM-Whisperer, we will also consider the impact of the multipath effect [20] in future work.

VI. Conclusion

We propose a novel voice injection system, EM-Whisperer, which is a stealth, remote, effective method for virtual meeting scenarios. It is based on the integration of the charging interface and the audio interface. Specifically, for a meeting scenario while the smart device is charging, EM-Whisperer selects the appropriate malicious words targeted for the meeting. Then it modulates and transmits the malicious voice for injection through the FM radio. Finally, it can inject malicious voices into the charging interface. In the evaluation part, EM-Whisperer is easy to be deployed since it leverages the COTS devices in small sizes. Furthermore, according to the experimental results, EM-Whisperer can achieve good attacking performance in a long distance with the assistance of FM radio. Also, the proposed attack is also effective when we change the impact factors (*e.g.*, the distance, the mobility) in environments.

Acknowledgment

This research was supported by National Natural Science Foundation of China under Grants No. 62132013.

References

[1] B. Consulting, “Virtual meeting software market to grow at a cagr of 14.2%, during forecast period — blueweave consulting.” https://www.globenewswire.com/en/news-release/2022/09/29/2525431/0/en/Virtual-Meeting-Software-Market-to-Grow-at-a-CAGR-of-14-2-during-Forecast-Period-BlueWeave-Consulting.html, 2023.

[2] D. Minoli, K. Sohraby, and B. Occhiogrosso, “Iot considerations, requirements, and architectures for smart buildings-energy optimization and next-generation building management systems,” *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 269–283, 2017.

[3] Frobes, “Why apple was right to remove the iphone 7 headphone jack.” https://www.forbes.com/sites/jvchamary/2016/09/16/apple-iphone-headphone-jack/, 2022.

[4] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, “Dolphinattack: Inaudible voice commands,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 103–117. [Online]. Available: https://doi.org/10.1145/3133956.3134052

[5] H. Abdullah, W. Garcia, C. Peeters, P. Traynor, K. Butler, and J. Wilson, “Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems,” in *Network and Distributed System Security Symposium (NDSS)*, 2019.

[6] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, “Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves,” 01 2020.

[7] Y. Wang, H. Guo, and Q. Yan, “Ghosttalk: Interactive attack on smartphone voice system through power line,” *CoRR*, vol. abs/2202.02585, 2022. [Online]. Available: https://arxiv.org/abs/2202.02585

[8] B. Lau, Y. Jang, C. Song, T. Wang, P. H. Chung, and P. Royal, “Mactans: Injecting malware into ios devices via malicious chargers,” *Black Hat USA*, vol. 92, 2013.

[9] D. J. Tian, G. Hernandez, J. I. Choi, V. Frost, C. Raules, P. Traynor, H. Vijayakumar, L. Harrison, A. Rahmati, M. Grace, and K. R. B. Butler, “ATtention spanned: Comprehensive vulnerability analysis of AT commands within the android ecosystem,” in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 273–290.

[10] Wikipedia, “Juice jacking attacks,” https://en.wikipedia.org/wiki/Juice_jacking, 2023.

[11] P. Cronin, X. Gao, C. Yang, and H. Wang, “Charger-Surfing: Exploiting a power line Side-Channel for smartphone information leakage,” in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 681–698.

[12] A. S. La Cour, K. K. Afridi, and G. E. Suh, “Wireless charging power side-channel attacks,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’21, 2021, p. 651–665.

[13] Y. Wu, Z. Li, N. Van Nostrand, and J. Liu, “Time to rethink the design of qi standard? security and privacy vulnerability analysis of qi wireless charging,” in *Annual Computer Security Applications Conference*, 2021, pp. 916–929.

[14] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, “Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging,” in *Network and Distributed System Security Symposium (NDSS)*, 02 2022.

[15] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, “Light commands: Laser-based audio injection attacks on voice-controllable systems,” ser. SEC’20. USA: USENIX Association, 2020.

[16] R. He, X. Ji, X. Li, Y. Cheng, and W. Xu, “”ok, siri” or ”hey, google”: Evaluating voiceprint distinctiveness via content-based profile score,” in *USENIX Security Symposium*, 2022.

[17] Sparkfun, “Tea5767hn: Low-power fm stereo radio for handheld applications,” https://www.sparkfun.com/datasheets/Wireless/General/TEA5767.pdf, 2023.

[18] Datasheet, “Qn8035 receiver datasheet: Single-chip low-power fm receiver,” https://datasheetspdf.com/datasheet/QN8035.html, 2023.

[19] Reddit, “Datasheet for alc5686,” https://www.reddit.com/r/Realtek/comments/r66ilz/datasheet_for_alc5686/, 2023.

[20] H. Zhao, M. Huang, and Y. Shen, “High-accuracy localization in multipath environments via spatio-temporal feature tensorization,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 12, pp. 10 576–10 591, 2022.