Is Broken Cable Breaking Your Security?

Md Faizul Bari, Meghna Roy Chowdhury, Shreyas Sen
Elmore Family School of Electrical & Computer Engineering, Purdue University, West Lafayette, USA
Emails: {mbari, mroycho, shreyas}@purdue.edu

Abstract*—Traditional methods of repairing a broken cable focus on restoring electrical connectivity and mechanical integrity, ignoring the electromagnetic aspects of it. Most of these repairing methods create a small monopole antenna as a byproduct which affects its electromagnetic compatibility (EMC). Switching activity in the transmitted signal through the wire creates an unintentional emission, called emanation, according to Maxwell's equations. This emanation is usually weak and suppressed to conform to EMC requirements. However, the monopole antenna of the repaired cable helps transmit it better, increasing the SNR of the emanation and extending its detection range significantly. This creates a serious security issue as emanations contain a significant correlation with the source signal and can be exploited for information extraction. In this work, the electromagnetic aspects of the broken cable repairing process have been explored in detail. We have applied the most commonly used cable repairing methods (twisting, soldering, and butt connector) to 3 types of widely used cables (USB, power, and HDMI cable) which are broken intentionally for experimental purposes. Collected data shows that the emanation SNR increases significantly due to the repairing process with -47 dBm power at a 20 cm distance. Although emanation power varies from cable to cable, it remains detectable even at >4 m distances. This strong emanation can penetrate through obstacles and remain detectable up to ~ 1 m distance through a 14 cm thick concrete wall. Along with exploring the vulnerability, a possible remedy, external metal shielding, has been explored in detail. This work exposes a new dimension of information leakage.

***Index Terms*—emanation, broken cable, cyber-physical systems, vulnerability, eavesdropping, information leakage**

2023 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-6654-5109-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISCAS46773.2023.10181751

I. Introduction

Electrical cables are as important as electronic devices to ensure proper power supply and data transfer. However, the quality of insulation and internal conducting material degrade over time, resulting in frayed or broken cable as shown in Fig. 1(a). Other causes behind frayed cables are bending, frequent twisting, heat, excessive tensile force, squeezing by heavy objects (e.g., chair, table, etc.), chewing by pets, etc. In most cases, one or more of the internal wires get broken and can be repaired easily by following 3 simple steps: (1) cutting off the damaged portion, (2) attaching the conductive part by twisting it together (and soldering, if possible), and (3) adding proper insulation by electrical tapes or heat shrink tubes. These approaches have two major goals: ensuring electrical connectivity through the wires and insulating the wires properly. However, they ignore the change in the electromagnetic emission from the cable and any possible violation of the EMC (electromagnetic compatibility) regulations introduced by the repairing process.

When a broken wire is twisted and soldered to repair, it forms a tiny monopole antenna as shown in Fig. 1(b) and (c). This is not an efficient antenna as it is a byproduct of the repairing process, not an intentionally designed one. The antenna length is seldom $\frac{\lambda}{4}$ and there is also no dedicated ground plane with a radius $>\frac{\lambda}{2}$. However, the earth acts as the ground plane for it and this inefficient monopole antenna causes weak emission. But what exactly does it radiate? It radiates electromagnetic emanation which is unintended emission from electronic devices and connecting wires due to electrical signal switching. It contains a significant correlation with the data being processed in the device, leading to information leakage. It can bypass physical and cryptographic access-to-data control methods at hardware and software levels; forming a 'side-channel' for the attackers and leading to several vulnerabilities such as *side-channel attack (SCA)* [1]–[3].

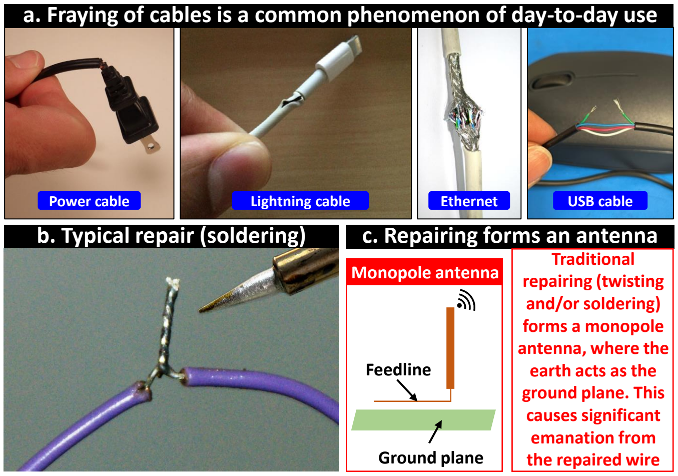
a. Fraying of cables is a common phenomenon of day-to-day use
Power cable
Lightning cable
Ethernet
USB cable
b. Typical repair (soldering)
c. Repairing forms an antenna
Monopole antenna
Feedline
Ground plane
Traditional repairing (twisting and/or soldering) forms a monopole antenna, where the earth acts as the ground plane. This causes significant emanation from the repaired wire

Fig. 1. (a) The condition of electrical cables deteriorates over day-to-day use and often breaks due to bending, frequent twisting, heat, excessive tensile force, squeezing by heavy objects, etc. It is a common phenomenon and typically it is much more economical to repair them. (b) Traditional repairing involves twisting to join severed wires or soldering them. (c) These repairing methods form a monopole antenna as a byproduct. Due to the switching activity in the transmitted signal, cables already have unintentional, weak electromagnetic emissions called emanation which is an information leakage source. Now the presence of an antenna makes the emission even stronger. The increased SNR of the emanation renders the whole system vulnerable.

Electromagnetic emanation is considered a data leakage source. Emanation has been used to detect keystrokes from keyboards [4], recover screen text and images [5], [6], monitor USB device activity [7], covert communication [8], detect DNN architecture [9], monitor smartphone camera activity [10], etc. Since electrical cables carry data streams, they emanate. In most cases, the cables are shielded internally to suppress the compromising emanation. However, with the

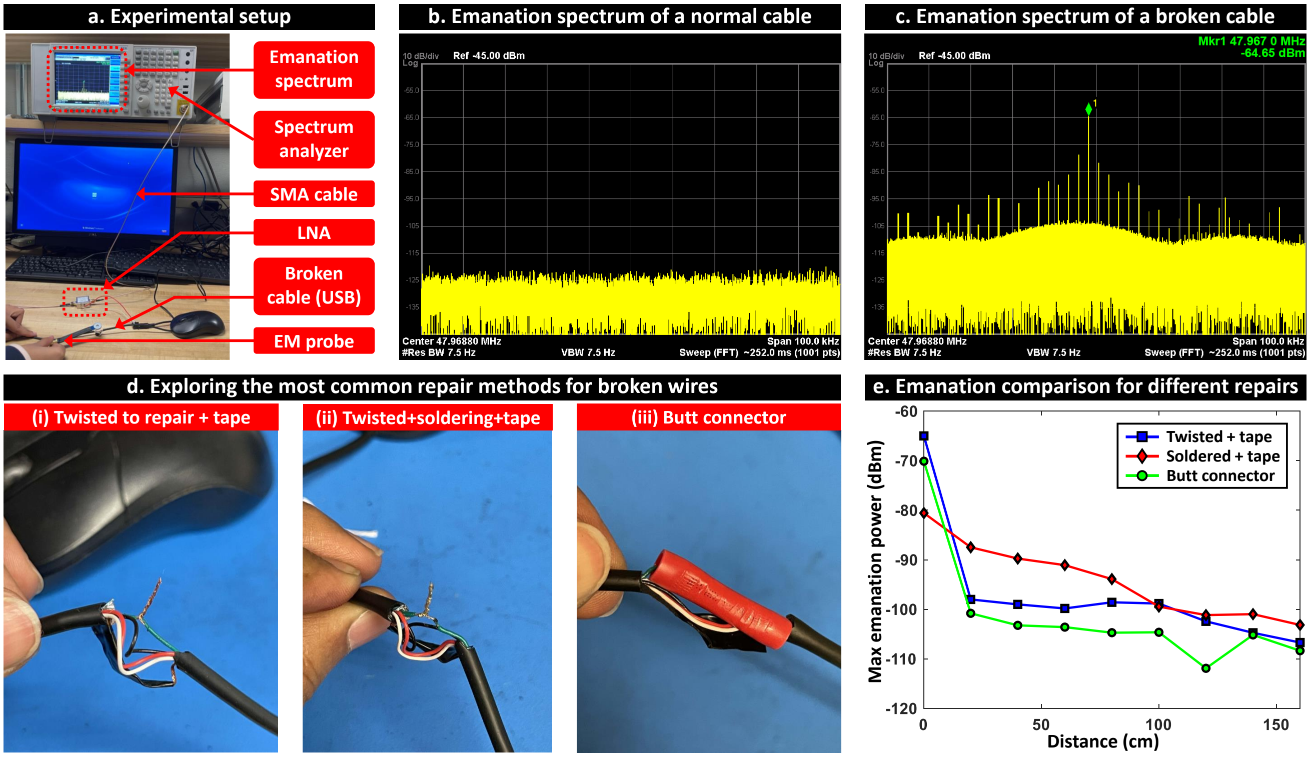

Fig. 2. (a) Physical experimental setup shows emanation data collection using EM probe. (b) and (c) Emanation spectrum from normal and broken USB cables respectively. It is observed that the normal cable has no significant emanation, while the repaired cable is much louder. (d) Most commonly used repairing methods: twist to join, soldering, and using butt connector. All these methods have been used in this work. (e) Comparison of maximum emanation power from the same USB cable, but repaired using 3 different methods. The plot shows that soldering method renders slightly higher SNR emanation.

monopole antenna in place (due to the repair process), the radiated emanation power becomes significantly higher. This emanation can be picked by an attacker to perform information recovery. In addition to the security issues, this unwanted emission causes electromagnetic interference (EMI) to nearby electronic equipment, leading to EMC compliance violations.

In this work, we have explored the electromagnetic aspects of the repair processes of broken cables. We have repaired the 3 most commonly used cables (USB, power cable, and display cable) by employing the most commonly used repairing processes: twisting, soldering, and using butt connectors [11]–[13]. Collecting data using an EM probe, we have shown that the repaired cable causes significantly louder emanation compared to its normal counterpart. The emanation power can be as high as -47 dBm at 20 cm, which can be detected even at >4 m distance. In addition to that, it is detectable even through a 14 cm thick concrete wall up to a distance of ~ 1 m. Our specific contributions are as follows:

- We have repaired the 3 most commonly used cables (USB, power cable, and HDMI) using traditional repairing methods (twisting, soldering, and employing butt connector) and collected emanation data from them. *For the first time, we have shown that the traditional repair process creates a monopole antenna as a byproduct which makes the electromagnetic emanation from the cable much stronger*, leading to a security vulnerability.
- Analyzing our collected data, we have shown that emanation power can be as high as -47 dBm at 20 cm for the HDMI cable. Although emanation power varies among cables, it can be detected even at >4 m distance for all of them. It can be even detected up to a distance of ~ 1 m through a 14 cm thick concrete wall. These results show that the broken cable creates a strong leakage source that can be exploited even from outside of a room.
- As a probable solution, we have applied an external shielding consisting of 8 layers of aluminum foil. Experimental data show that it reduces emanation power up to 30 dB, but cannot suppress it completely.

II. Relevant Works

'Twisting wires to repair' essentially creates a small monopole antenna. A brief theory and operation of monopole antenna can be found here [14], [15]. This unintentional antenna helps emanation transmit better. Emanation is present even without the antenna, it just becomes stronger due to it. Compromising emanation has been exploited widely for eavesdropping purposes by military organizations [16]. The first unclassified research paper on emanation was published by Wim van Eck in 1985 [17]. He demonstrated that the screen content of a display unit can be successfully reconstructed at a long range using very cheap equipment. Electromagnetic emanations are sometimes called 'van Eck radiation' after him

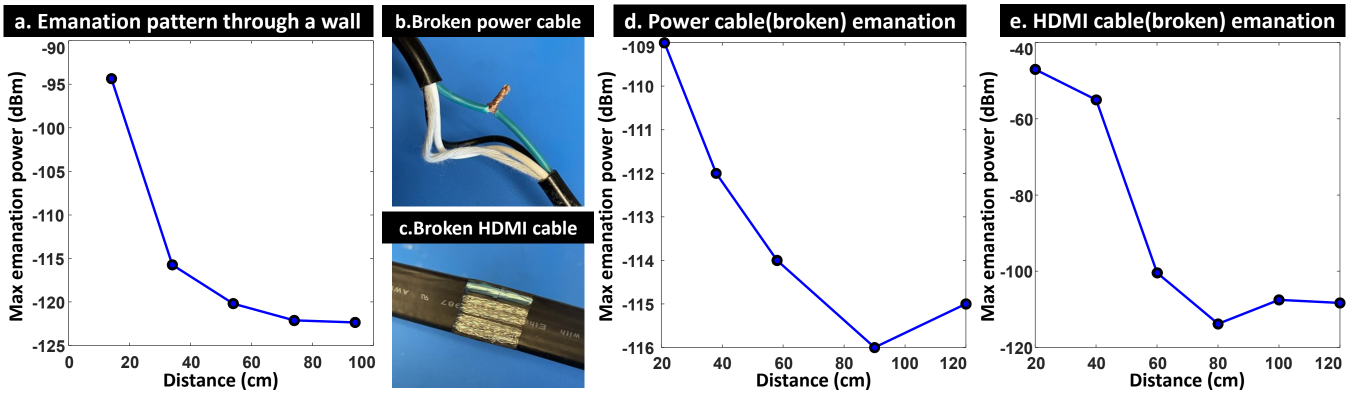

Fig. 3. (a) Emanation pattern of a USB cable detected through a 14 cm thick concrete wall. (b) A broken power cable has been twisted to repair. (c) A broken HDMI cable with internal metal shielding was removed. (d) Emanation pattern of a repaired power cable. (e) Emanation pattern of a broken HDMI cable.

[16]. In 2002, a detailed investigation on monitor emanations and screen text reconstruction was performed by Markus G. Kuhn in his doctoral dissertation [18]. Since then, a lot of studies have focused on the on-screen image and/or video reconstruction. In [5], the authors have reconstructed a grayscale image containing text and geometric shapes both. The same authors recently succeeded in reconstructing a grayscale image containing text and a human face [6].

Emanations from USB devices have been used for versatile information extraction. In [4], the authors have recovered the keystroke on both wired and wireless keyboards (both USB and PS2) with high accuracy (>95%). Emanations can couple and propagate through the powerline as well. Authors in [19] have proposed an attack that uses power lines to extract data from air-gapped computers. They have developed malware that modulates CPU core utilization, which is propagated through the power supply. A major attack using emanation is a ‘side-channel attack’ (SCA) where the attacker recovers the private key using collected traces from the victim device [1], [2]. In [3], the authors have demonstrated a cross-device, deep learning-based side-channel attack with $> 99.9\%$ accuracy.

Emanation from data storage devices has been used to monitor and classify its activity (reading, writing, or silence) [7]. In [9], authors have exploited GPU emanation to detect DNN architecture. In [10], emanations from smartphones are used to detect the camera status (both front and rear). In a very recent work [20], the authors have characterized emanations from an off-the-shelf PC. One interesting phenomenon was frequency shifting with the execution of different programs. This temporal behavior has been exploited in another recent work [8] to provide FSK-modulated data for covert communication. These information leakage examples show why the circuit and system designers try to suppress emanation as much as possible.

III. Data Collection

A. Experimental Setup

Fig. 2(a) shows our experimental setup in our lab. An EM probe is used as a sensing device to collect emanation data from the target (broken cable). The EM probe is connected to a 32 dB low-noise amplifier (LNA) which amplifies the signal and sends it to a spectrum analyzer where the signal is collected and analyzed. We have intentionally broken different types of cables by stripping off their external plastic layer and cutting either the data wire or the power-carrying wire. Then the cables are repaired using different methods described below in section III-B. Fig. 2(b) and (c) shows the emanation spectrum from the normal and repaired cable (USB) respectively.

B. Repairing Methods

There are many different methods to fix the broken wires inside a cable [11], [12]. The most common method involves scraping off a portion of insulation from the severed wire to expose the metal strings and twist them together as shown in Fig. 2(d)(i). After joining them, electrical tape or a heat shrink tube is used to restore insulation. Fig. 2(d)(ii) shows a modified version of this method where the broken pieces of the wire are soldered together before applying insulation. Another method is to use a butt connector [13] which is a plastic tube with a hollow metal tube inside. The broken pieces of wires are inserted in it from both sides and then the connector is pressed hard so that the internal metal tube gets squeezed and holds the wires firmly together. Fig. 2(d)(iii) shows the use of a butt connector. In this work, we have applied all these repair methods.

IV. Results

A. Emanation from USB Cable

To test emanation from USB cables, a USB mouse was taken. It was USB 2.0 which supports 12 Mbps data rate at full speed. Hence, 12 MHz and its harmonics were our primary targets. The strongest emanation was found at the 4^{th} harmonic (48 MHz) which is shown in Fig. 2(c). Data were collected from the nearest position to the cable up to 4 m, in 20 cm steps. Fig. 2(e) shows the maximum emanation power versus distance plot for up to 160 cm for USB cables with 3 types of repairing process (twisting, soldering, and using

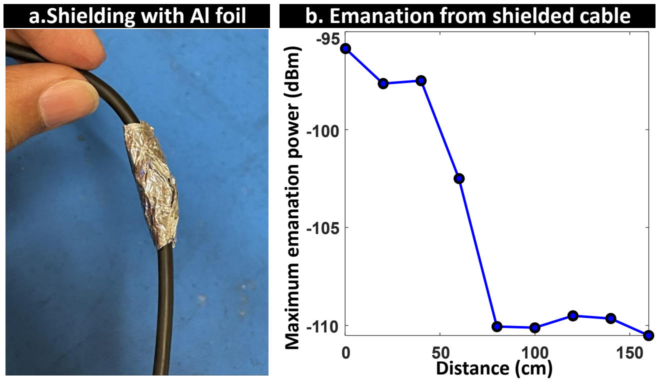

Fig. 4. (a) A 'broken and twisted to repair' USB cable is externally shielded with 8 layers of aluminum foil. (b) The emanation pattern of the shielded cable shows reduced emission power.

butt connector). The soldered wire seems to have a slightly stronger emanation compared to the other two. However, for all 3 cases, emanation is > -110 dBm at $>$1.5 m. This shows the extent of leakage caused by the monopole antenna.

B. Detection through Obstacles

Next, the detection is performed through a concrete wall to imitate an eavesdropper outside of the facility. For that purpose, the broken cable is kept outside of the experiment room while the emanation signal is collected from inside. Fig. 3(a) shows collected emanation power through the wall versus distance (includes wall thickness). The wall causes $\sim$20 to 30 dB loss. However, it is still detectable even at $\sim$1 m distance. This means that sensitive data can be stolen even from outside the room.

C. Emanation from Power Cable

After exploring USB cables, we focus on other cables and check if the same phenomenon occurs for them. Fig. 3(b) shows a broken and repaired power cable. The cable was supplying power to a desktop to which the mouse was connected. The desktop contains an intel® core^{TM} i7-6700 microprocessor and $8\,\mathrm{GB}$ RAM. For this power cable, we found the strongest emanation at $120\,\mathrm{MHz}$. Fig. 3(d) shows the maximum emanation power vs distance for the broken power cable. Here, the emanation follows a similar pattern as in the case of the USB cable, but weaker.

D. Emanation from Display Cable (HDMI)

Next, emanations from a display cable (HDMI) are tested. Fig. 3(c) shows a broken HDMI cable with internal shielding removed. Emanation from the HDMI cable is the strongest and unlike the other two cables, HDMI has detectable emanation even without breaking the cable. However, broken cable makes the emanation even stronger. On top of the cable, the strongest detected emanation was $\sim$-20 dBm. Even at 20 cm, it was -47 dBm. Fig. 3(e) shows the maximum emanation power vs distance. As mentioned in section II, emanations from regular HDMI cables and monitors have been exploited to reconstruct screen images and texts. Broken cable only makes it worse, making reconstruction easier with higher emanation SNR.

V. Prevention of Leakage - External Shielding

Shielding is commonly used inside a cable to reduce emanation power. But how effective is external shielding on a broken cable? To answer that, an external shielding is attached to the top of a repaired USB cable. This shielding contains 8 layers of aluminum foil. Fig. 4(a) shows the shielded cable. Next, emanations from the cable are measured following our earlier method. Fig. 4(b) shows the maximum emanation power over distance. A comparison of Fig. 2(e) and Fig. 4(b) shows that shielding decays emanation to some extent (up to $30\,\mathrm{dB}$), but can not suppresses it totally. However, this suppression reduces the maximum detection range and renders eavesdropping or exploitation of emanation harder. So, traditional repairing methods can be augmented with an extra layer of shielding and insulation (e.g. heat shrink tube) for better protection against EM leakage.

As an extra precaution, electronic equipment and the corresponding cables should be placed toward the center of the room. This effectively sets a control perimeter within which the emanation signal decays significantly. However, for an extremely sensitive facility, the best approach is to replace the damaged cable and recycle it.

VI. Conclusion

In this work, we have explored the electromagnetic aspects of traditional repair methods for broken cables. We postulated that the repairing process creates a monopole antenna which will increase the SNR of the compromising emanation. Employing 3 types of most commonly used repair methods (twisting, soldering, and butt connector) on different cables (USB, power cable, and HDMI), we have proved our hypothesis experimentally. Our results show that even at a $20\,\mathrm{cm}$ distance, emanation power can be as strong as $-47\,\mathrm{dB\,m}$ for HDMI cable. For all types of cables, emanation is detectable at >4 m distance. It is so strong that it can penetrate a concrete wall and remains detectable up to ~1 m distance through a $14\,\mathrm{cm}$ thick concrete wall. We have explored a possible remedy, external shielding using metal foil which suppresses the emanation to some extent but cannot block it completely. This work exposes a previously unexplored security vulnerability that may go unnoticed and affect an otherwise secure cyber-physical system.

Acknowledgment

This research was supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via contract: 2021-21062400006. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes not withstanding any copyright annotation thereon.

REFERENCES

[1] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, “Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 163–177, doi: 10.1145/3243734.3243802.

[2] J. Danial et al., “EM-X-DL: Efficient Cross-Device Deep Learning Side-Channel Attack with Noisy EM Signatures,” ACM Journal on Emerging Technologies in Computing Systems, 2020, vol. 18, no. 1, pp. 1–17. doi: 10.1145/3465380.

[3] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury and S. Sen, “X-DeepSCA: Cross-Device Deep Learning Side Channel Attack,” 2019 56th ACM/IEEE Design Automation Conference (DAC), 2019, pp. 1-6, doi: 10.1145/3316781.3317934.

[4] M. Vuagnoux and P. Sylvain, “Compromising electromagnetic emanations of wired and wireless keyboards,” in USENIX security symposium, vol. 1. 2009.

[5] H. S. Lee, D. H. Choi, K. Sim and J. -G. Yook, “Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment,” in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1098-1106, Aug. 2019, doi: 10.1109/TEMC.2018.2855448.

[6] E. Lee, D. -H. Choi, T. Nam and J. -G. Yook, “A Quantitative Analysis of Compromising Emanation From TMDS Interface and Possibility of Sensitive Information Leakage,” in IEEE Access, vol. 10, pp. 73997-74011, 2022, doi: 10.1109/ACCESS.2022.3184294.

[7] B. Liu, Y. Xu, W. Huang and S. Guo, “Detecting USB Storage Device Behaviors by Exploiting Electromagnetic Emanations,” ICC 2022 - IEEE International Conference on Communications, 2022, pp. 4980-4985, doi: 10.1109/ICC45855.2022.9839155.

[8] M. Hegarty, Y. E. Sagduyu, T. Erpek and Y. Shi, “Deep Learning for Spectrum Awareness and Covert Communications via Unintended RF Emanations.” In Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning, pp. 27-32. 2022.

[9] S. Liang, Z. Zhan, F. Yao, L. Cheng and Z. Zhang, “Clairvoyance: Exploiting Far-field EM Emanations of GPU to “See” Your DNN Models through Obstacles at a Distance,” 2022 IEEE Security and Privacy Workshops (SPW), 2022, pp. 312-322, doi: 10.1109/SPW54247.2022.9833894.

[10] B. B. Yilmaz, E. Mert Ugurlu, A. Zajić and M. Prvulovic, “Cell-Phone Classification: A Convolutional Neural Network Approach Exploiting Electromagnetic Emanations,” ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020, pp. 2862-2866, doi: 10.1109/ICASSP40776.2020.9054006.

[11] “6 Ways to Fix Broken Wires - Beginner Through Pro,” www.youtube.com, https://www.youtube.com/watch?vx̄Mqt5AoWPyI &ab_channel=LRN2DIY (accessed Oct. 22, 2022).

[12] D. Farquhar, “How to fix a broken wire,” The Silicon Underground, Dec. 04, 2019. https://dfarq.homeip.net/how-to-fix-a-broken-wire/ (accessed Oct. 22, 2022).

[13] “How to Strip and Connect Wires With a Butt Connector,” Instructables. https://www.instructables.com/How-to-strip-and-connect-wires-with-a-butt-connect/ (accessed Oct. 22, 2022).

[14] P. J. Bevelacqua, “The Monopole Antenna,” antenna-theory.com. https://www.antenna-theory.com/antennas/monopole.php (accessed Oct. 22, 2022).

[15] “Monopole antenna,” Wikipedia, Jan. 09, 2021. https://en.wikipedia.org /wiki/Monopole_antenna

[16] “Tempest (codename),” Wikipedia. https://en.wikipedia.org/wiki/Tempest _(codename). (Accessed: 07-Oct-2022).

[17] W. Van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?,” Computers & Security 4, no. 4 ,1985, 269-286.

[18] M. G. Kuhn, “Compromising emanations: eavesdropping risks of computer displays,” (Doctoral dissertation, University of Cambridge), 2002.

[19] M. Guri, B. Zadov, D. Bykhovsky and Y. Elovici, “PowerHammer: Exfiltrating Data From Air-Gapped Computers Through Power Lines,” in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1879-1890, 2020, doi: 10.1109/TIFS.2019.2952257.

[20] M. F. Bari, M. R. Chowdhury, B. Chatterjee and S. Sen, “Detection of Rogue Devices using Unintended Near and Far-field Emanations with Spectral and Temporal Signatures,” in IEEE/MTT-S International Microwave Symposium - IMS, 2022, pp. 591-594, doi: 10.1109/IMS37962.2022.9865347.