An Introduction to TEMPEST (Classified), using ChatGPT

Frank Leferink
THALES Netherlands
Hengelo, the Netherlands
and
University of Twente
Enschede, the Netherlands
orcid.org/0000-0001-6299-0052

***Abstract*—TEMPEST is a codename referring to spying on information systems through leaking electromagnetic emanations, either via cables or through electromagnetic fields. Nowadays it is considered as a part of cyber security. Most publications on TEMPEST are classified, and when a draft paper is being checked for classified information, many reviewers request that parts are being removed. Even if information can be retrieved from public channels like open publications or the internet, still reviewers have objections. ChatGPT is an artificial intelligence chatbot which is continuously being fine-tuned by gathering information from public resources, as well as human feedback. This article describes the information on TEMPEST provided by ChatGPT, while no human feedback was given.**

Keywords—TEMPEST, ChatGPT

I. Introduction

TEMPEST is a codename referring to spying on information systems through leaking emanations like unintentional radio, or electrical signals, emission [1]. TEMPEST covers both methods to spy upon others and how to shield equipment against such spying. A basic picture is shown in Fig. 1. The protection efforts for TEMPEST are also known as emission security (EMSEC). It is now a part of cyber security. Nearly every discussion on TEMPEST is ranked as ‘classified’ and strict security measures have to be taken. But the protection against spying is achieved via distance, shielding and filtering, and is largely equivalent of the standard electromagnetic compatibility (EMC) efforts to protect a system against other electromagnetic phenomena; Such as lightning protection, preventing unwanted emission, preventing intra-EMC issues with other systems on a platform, or to prevent susceptibility issues, including those from intentional electromagnetic interference (I-EMI).

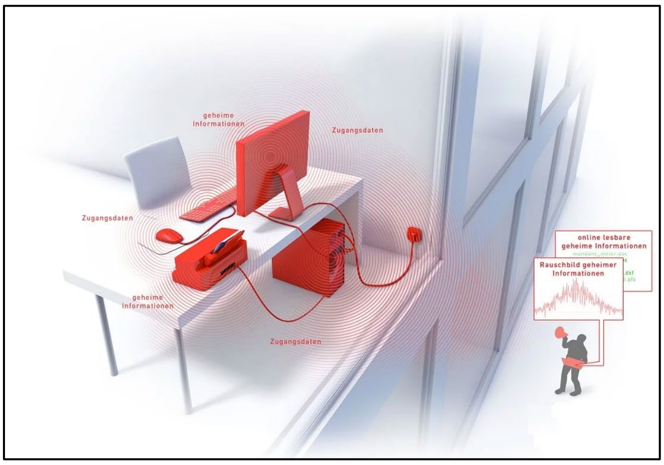

Fig. 1. Attacker outside a building receiving compromising emanations, from [2].

To overcome the issue of providing classified information, the program ChatGPT [3] has been used to prevent unwanted information from being published unknowingly. ChatGPT suffers from multiple limitations, as it sometimes writes plausible-sounding but incorrect or nonsensical answers. Correcting these incorrect or nonsensical answers would open again a risk of disclosure of classified information. Therefore, the text entered as well as the response of ChatGPT [4] is copied in this paper verbatim.

II. Scientific paper on TEMPEST

<u>Question author of this article:</u> Write a scientific article of 4 pages 2 columns about the state of the art in TEMPEST research

<u>Response ChatGPT:</u>

A. Introduction

TEMPEST research, also known as Van Eck phreaking, is a field of study that deals with the interception of electromagnetic radiation emanating from electronic devices. The field has been in existence for several decades, and over the years, significant strides have been made towards developing effective countermeasures against TEMPEST attacks. In this paper, we present a state-of-the-art review of TEMPEST research, highlighting some of the recent advances in the field.

B. Background

TEMPEST attacks exploit the fact that electronic devices emit electromagnetic radiation that can be intercepted and analyzed to extract sensitive information. The phenomenon was first discovered in the 1940s, during the development of radar systems. However, it was not until the 1980s that it gained widespread attention as a security threat. The name "TEMPEST" was coined by the US government to refer to the phenomenon of compromising electronic devices through the interception of their electromagnetic emissions.

TEMPEST attacks can be carried out through various means, including the use of specialized equipment such as high-gain antennas and radio receivers. The attacks can also be carried out using software-based methods, such as software-defined radio (SDR). In recent years, there has been a growing concern about the potential for TEMPEST attacks to be used for espionage and other malicious activities, leading to a renewed interest in TEMPEST research.

C. Recent Advances in TEMPEST Research

One of the recent advances in TEMPEST research is the development of new techniques for analyzing and mitigating electromagnetic emissions from electronic devices. Researchers have developed various approaches, including electromagnetic shielding, frequency hopping, and encryption techniques, to protect electronic devices from TEMPEST attacks.

979-8-3503-2400-6/23/$31.00 ©2023 IEEE

Electromagnetic shielding involves the use of specialized materials to reduce or block electromagnetic radiation emanating from electronic devices. The approach has been used for several years and is still an effective way of protecting electronic devices from TEMPEST attacks. However, it can be expensive and may not be practical for some devices.

Frequency hopping is another approach used to protect electronic devices from TEMPEST attacks. The technique involves rapidly switching between different frequencies to make it difficult for attackers to intercept the electromagnetic radiation. Frequency hopping has been used in various applications, including wireless communications and satellite communications, and is effective at protecting electronic devices from TEMPEST attacks.

Encryption is another technique used to protect electronic devices from TEMPEST attacks. Encryption involves converting sensitive data into an unreadable form using a cryptographic algorithm. The approach has been used for several decades and is still an effective way of protecting electronic devices from TEMPEST attacks. However, attackers can use sophisticated methods, such as side-channel attacks, to bypass encryption and gain access to sensitive data.

Researchers have also developed new methods for detecting and analyzing electromagnetic emissions from electronic devices. For example, researchers have developed software-based methods for analyzing electromagnetic radiation, such as the use of SDR. SDR allows researchers to analyze electromagnetic radiation in real-time and can be used to detect and identify potential TEMPEST attacks.

D. Conclusion

TEMPEST research is a crucial field that deals with the interception of electromagnetic radiation emanating from electronic devices. Over the years, significant advances have been made in the field, leading to the development of various techniques for analyzing and mitigating electromagnetic emissions. However, as technology advances, attackers are finding new ways to exploit electronic devices, leading to a continued need for TEMPEST research. As such, there is a need for ongoing research to identify new threats and develop effective countermeasures to protect electronic devices from TEMPEST attacks.

III. State of the art on TEMPEST

Question: What is the state of the art in TEMPEST research, and include references to recently published papers

Response ChatGPT:

A. First attempt:

TEMPEST is a term used to describe the study of unintentional electromagnetic radiation emitted by electronic devices, which can potentially be intercepted and exploited by an attacker. The field of TEMPEST research is constantly evolving, with new advances and techniques being developed to improve both the security of electronic devices and the effectiveness of TEMPEST attacks.

Here are a few recent papers on the state of the art in TEMPEST research:

1. "A Survey of Electromagnetic Side-Channel Attacks and Countermeasures for Cryptographic Systems" by Jian Liu, Xiaojun Wang, and Shengli Liu (2021). This paper provides an overview of recent advances in electromagnetic side-channel attacks (SCAs) and countermeasures for cryptographic systems. It also discusses the limitations of existing countermeasures and suggests future research directions.

2. "A New TEMPEST Attack Against AES Encryption Implementations" by Yuhong Zhang, Hui Li, and Jiwu Jing (2021). This paper presents a new TEMPEST attack against AES encryption implementations that uses the side-channel information leaked by the power consumption of the target device. The attack is demonstrated on several AES implementations and found to be effective.

3. "Improving Side-Channel Resistance of Lattice-Based Cryptosystems Against Electromagnetic Attacks" by Wei Zhang, Shuai Liu, and Shaoquan Jiang (2020). This paper proposes a new method for improving the side-channel resistance of lattice-based cryptosystems against electromagnetic attacks. The method is based on the use of power consumption analysis to detect and mitigate electromagnetic leakage.

4. "A New Method for Evaluating Electromagnetic Radiation of Modern Computer Memory" by Jin-Ho Lee and Byung-Seok Choi (2020). This paper presents a new method for evaluating the electromagnetic radiation of modern computer memory. The method uses a high-frequency current probe and an oscilloscope to measure the electromagnetic radiation of different types of memory modules.

Overall, these papers demonstrate that TEMPEST research is an active and dynamic field, with new techniques and approaches being developed all the time to improve the security of electronic devices and protect against TEMPEST attacks.

B. Second attempt (question repeated, verbatim):

TEMPEST research is concerned with the analysis and mitigation of electromagnetic emanations from electronic devices that can be used to eavesdrop on sensitive information. The field is constantly evolving as new technologies are developed and new vulnerabilities are discovered. Here are some recent papers on the state of the art in TEMPEST research:

1. "A Review of Electromagnetic Side-Channel Attacks" by M. Vanhoef and F. Piessens. In this 2021 paper, the authors provide a comprehensive review of electromagnetic side-channel attacks, including TEMPEST attacks, and discuss current research directions and future challenges.

2. "Defeating Electromagnetic Eavesdropping with Shielding and Jamming" by A. Naderi and F. Koushanfar. This 2021 paper proposes a method for defeating TEMPEST attacks using a combination of shielding and jamming techniques.

3. "Exploiting LCD Monitor Electromagnetic Emissions to eavesdrop on Sensitive Information" by S. Gururangan et al. In this 2020 paper, the authors demonstrate how TEMPEST attacks can be carried out using electromagnetic emissions from LCD monitors, and propose a solution to mitigate the risk.

4. "A Survey of Electromagnetic Side-Channel Attacks and Countermeasures on Embedded Systems" by A. Badawi and H. Ghali. This 2019 paper provides a survey of electromagnetic side-channel attacks and countermeasures, including TEMPEST attacks, specifically targeted at embedded systems.

5. "Side-Channel Analysis and Security Evaluation of Electromagnetic Shielding Fabrics" by L. Ma et al. In this 2019 paper, the authors evaluate the effectiveness of electromagnetic shielding fabrics for protecting against TEMPEST attacks, using side-channel analysis techniques.

These papers provide a glimpse into the current state of the art in TEMPEST research and the ongoing efforts to develop effective countermeasures against electromagnetic side-channel attacks.

IV. Risk of TEMPEST

Question: What is the actual risk of TEMPEST considering the low emission and wide bandwidth of modern systems

Response ChatGPT:

The actual risk of TEMPEST attacks on modern electronic systems depends on various factors, including the strength and frequency of the electromagnetic emissions, the distance between the target system and the attacker, and the sensitivity of the information being transmitted.

It is true that modern electronic systems generally emit less electromagnetic radiation than older systems due to improvements in design and shielding, and that their high operating frequencies make it more difficult for attackers to extract meaningful information from the emissions. However, it is still possible for skilled attackers to exploit even very weak emissions to extract sensitive information, especially in cases where the attacker is in close proximity to the target system or has some control over the environment in which the system is operating.

For example, recent research has shown that even seemingly innocuous devices such as computer monitors, printers, and smartphones can emit electromagnetic signals that can be used for TEMPEST attacks under certain conditions. Additionally, some types of encryption algorithms used in modern systems may be vulnerable to side-channel attacks that exploit electromagnetic emissions, making TEMPEST attacks more feasible.

In conclusion, while the risk of TEMPEST attacks on modern systems may be lower than it was in the past, it is still a real and potentially significant threat, especially in situations where the security of sensitive information is critical. It is important for organizations and individuals to be aware of this risk and take appropriate measures to mitigate it, such as using electromagnetic shielding, controlling the physical environment around sensitive systems, and implementing secure encryption protocols.

V. Should be protect critical infrastructure

Question: Should we protect critical infrastructure and sensitive data processing systems against TEMPEST

Response ChatGPT:

Yes, protecting critical infrastructure and sensitive data processing systems against TEMPEST attacks is highly recommended. TEMPEST attacks can pose a significant risk to the confidentiality of sensitive data and can compromise the integrity and availability of critical infrastructure systems.

Many countries and organizations have recognized the importance of TEMPEST protection and have established TEMPEST standards and guidelines for protecting their critical infrastructure and sensitive systems. For example, in the United States, the National Security Agency (NSA) has published guidelines for TEMPEST protection under the title "NSTISSAM TEMPEST/1-92: Red/Black Installation Guidance" and the Committee on National Security Systems (CNSS) has established the CNSS National TEMPEST Standard for protecting national security systems.

TEMPEST protection typically involves a combination of physical, electrical, and software measures to reduce or eliminate electromagnetic emanations from sensitive equipment. These measures may include shielding sensitive equipment, filtering electromagnetic emissions, controlling the physical environment around sensitive systems, using secure encryption protocols, and other security measures.

In conclusion, protecting critical infrastructure and sensitive data processing systems against TEMPEST attacks is an important aspect of ensuring the confidentiality, integrity, and availability of these systems. Implementing TEMPEST protection measures can help reduce the risk of TEMPEST attacks and protect sensitive information and critical infrastructure from potential threats.

VI. How to protect against TEMPEST

Question: How can we protect critical infrastructure and sensitive data processing systems against a TEMPEST attack

Response ChatGPT:

Protecting critical infrastructure and sensitive data processing systems against a TEMPEST attack requires a combination of physical, electrical, and software measures. Here are some of the most effective methods for protecting against TEMPEST attacks:

1. Shielding: Shielding involves enclosing sensitive equipment in a conductive material such as copper or aluminum, which absorbs or reflects electromagnetic emissions and prevents them from being detected by eavesdroppers. Shielding can be applied to individual components, such as processors and displays, or to entire rooms or buildings.
2. Filtering: Filtering involves using specialized equipment, such as ferrite cores or capacitors, to suppress electromagnetic emissions at the source. This can be particularly effective for reducing the strength of emissions from power supplies and other high-voltage equipment.
3. Secure Encryption: Implementing secure encryption protocols for sensitive data can help prevent attackers from extracting meaningful information from electromagnetic emissions. This is particularly important for protecting against attacks that exploit side channels in cryptographic algorithms.
4. Physical security: Controlling the physical environment around sensitive systems is also important for protecting against TEMPEST attacks. This may include restricting access to sensitive areas, using physical barriers to prevent eavesdropping, and monitoring the physical environment for signs of potential attacks.
5. Use of specialized TEMPEST equipment: Specialized equipment that is designed to meet TEMPEST standards can be used to reduce the strength of electromagnetic emissions and protect against eavesdropping.
6. EMSEC training: Ensuring that personnel are trained in the principles of electromagnetic security (EMSEC) can help prevent accidental or intentional leaks of sensitive information through electromagnetic emissions.

In conclusion, protecting against TEMPEST attacks requires a multi-layered approach that combines physical, electrical, and software measures. Implementing shielding, filtering, secure encryption, physical security measures, and EMSEC training can help reduce the risk of TEMPEST attacks and protect critical infrastructure and sensitive data processing systems from potential threats.

VII. TEMPEST standards

Question: Give an overview of TEMPEST standards in use worldwide

Response ChatGPT:

TEMPEST standards are used worldwide to provide guidance for the protection of sensitive electronic equipment and information against eavesdropping via electromagnetic emissions. These standards typically specify requirements for the level of protection that must be provided for equipment and systems in various operational environments. Here is an overview of some of the most widely used TEMPEST standards worldwide:

1. NSTISSAM TEMPEST/1-92 (USA): This standard is published by the National Security Agency (NSA) and provides guidance for the installation of Red/Black equipment and systems in national security systems. It covers areas such as electromagnetic interference control, signal attenuation, and system isolation.

2. NATO SDIP-27 (UK): This standard is used by NATO member countries and covers the protection of classified information against electromagnetic emanations. It provides guidance on areas such as equipment design, installation, and testing.

3. ZN/A-010 (Canada): This standard is used by the Canadian government and covers the protection of classified information against electromagnetic emanations. It provides guidance on areas such as equipment design, installation, and testing.

4. AMSG 720B (Australia): This standard is used by the Australian government and covers the protection of classified information against electromagnetic emanations. It provides guidance on areas such as equipment design, installation, and testing.

5. ACP 100 (France): This standard is used by the French government and covers the protection of classified information against electromagnetic emanations. It provides guidance on areas such as equipment design, installation, and testing.

6. TSG-022 (Germany): This standard is used by the German government and covers the protection of classified information against electromagnetic emanations. It provides guidance on areas such as equipment design, installation, and testing.

7. ITSEC (EU): This standard was developed by the European Union and provides guidelines for the evaluation of IT security products. It includes requirements for TEMPEST protection of IT products, including encryption devices.

In addition to these standards, there are also many other national and international standards that provide guidance on TEMPEST protection for specific types of equipment and systems. For example, there are standards for TEMPEST protection of computers, printers, phones, and other devices.

VIII. TEMPEST CASES

Question: Describe several actual cases of TEMPEST leakage

Response ChatGPT:

A. First attempt:

Due to the sensitive nature of TEMPEST incidents and the potential security implications, specific details of actual cases of TEMPEST leakage are often not publicly disclosed. However, there have been several reported cases of TEMPEST leakage over the years, and here are a few examples:

1. The AN/FLR-9 antenna array: This antenna array was used by the US military during the Cold War for long-range radio communications. It was located in a remote area in the state of Virginia and was designed to be highly resistant to eavesdropping. However, in the 1980s, a team of researchers was able to use a radio receiver and an oscilloscope to detect and decode the signals transmitted by the antenna array from a distance of several miles.

2. The Tempest in a Teapot incident: In 1985, the British magazine "New Scientist" published an article describing how researchers had been able to use electromagnetic emissions from a computer display to reconstruct the image displayed on the screen. The article sparked a wave of interest in TEMPEST research and led to the development of specialized equipment for TEMPEST analysis.

3. The Crypto AG scandal: In the 1990s, it was revealed that Crypto AG, a Swiss-based company that provided encryption equipment to governments around the world, had been secretly owned by the CIA and the German intelligence agency. The agencies were able to use TEMPEST techniques to eavesdrop on encrypted communications that were being transmitted using Crypto AG equipment.

4. The Great Seal Bug: In 1945, a Soviet listening device was discovered in the Great Seal of the United States that had been presented to the US ambassador to Moscow by Soviet schoolchildren as a gift. The device was powered by a battery and transmitted audio signals using electromagnetic emissions. This incident led to the development of the first TEMPEST standards for the protection of sensitive electronic equipment.

These are just a few examples of reported incidents of TEMPEST leakage. However, due to the sensitive nature of TEMPEST attacks, it is likely that many incidents are not reported publicly, and the true extent of the threat is difficult to gauge.

B. Second attempt (question repeated, verbatim):

Due to the sensitive nature of TEMPEST incidents, it is often difficult to find detailed information about specific cases of TEMPEST leakage. However, here are several examples of actual cases where TEMPEST vulnerabilities were discovered and exploited:

1. Operation Soft Cell (USA): In 2019, a group of attackers believed to be linked to the Chinese government targeted telecommunications providers in Europe, Asia, Africa, and the Middle East. The attackers used a combination of hacking techniques and TEMPEST attacks to access sensitive data, including call records, geolocation data, and SMS traffic.

2. Operation Tempest (Poland): In the 1980s, the Polish government launched a program to develop technology to eavesdrop on Western embassies and military installations. The program, known as Operation Tempest, involved the use of highly sensitive radio receivers to detect electromagnetic emissions from electronic equipment in the targeted buildings.

3. The Great Seal Bug (USA): In 1952, the Soviet Union presented the United States with a gift of a carved wooden Great Seal of the United States to be displayed in the ambassador's residence in Moscow. However, the seal contained a hidden microphone that was powered by a passive resonant cavity, and it was capable of transmitting conversations via electromagnetic emissions.

4. Cryptovirology (worldwide): In the field of cryptography, there have been several examples of attacks that exploit electromagnetic emissions to extract cryptographic keys from computer systems. These attacks, known as side-channel attacks, have been demonstrated to be effective against a wide range of encryption algorithms and are a significant concern for organizations that handle sensitive data.

These are just a few examples of actual cases where TEMPEST vulnerabilities were discovered and exploited. It is important to note that TEMPEST attacks are a significant threat to sensitive information and that protecting against such attacks requires a multi-layered approach that combines physical, electrical, and software measures.

C. Third attempt (question repeated, verbatim):

There have been several actual cases of TEMPEST leakage reported over the years. Here are a few examples:

1. Soviet Union's "The Thing": In the 1940s, the Soviet Union planted a covert listening device in the US embassy in Moscow. The device, which was powered by electromagnetic radiation from nearby sources, was concealed inside a wooden carving of the Great Seal of the United States that was presented as a gift to the US ambassador. The device remained undetected for seven years and provided the Soviet Union with valuable intelligence.

2. Operation Ivy Bells: During the 1970s and 1980s, the US Navy used underwater tapping devices to eavesdrop on Soviet communication cables in the Sea of Okhotsk. The devices, which were powered by electromagnetic radiation from nearby power lines, allowed the US to intercept and decrypt Soviet communications. The operation remained secret for several years until it was exposed by a former NSA employee.

3. French Stealth Frigates: In the 1990s, the French Navy discovered that the electromagnetic emissions from their new stealth frigates were leaking sensitive information to potential eavesdroppers. The problem was caused by a design flaw in the frigates' electrical systems, which allowed electromagnetic emissions to leak through the hull. The French Navy was forced to retrofit the frigates with additional shielding and filtering to protect against eavesdropping.

4. Iranian Nuclear Program: In 2012, it was reported that the US and Israeli intelligence agencies had used a combination of cyberattacks and TEMPEST eavesdropping to disrupt Iran's nuclear program. The eavesdropping was reportedly conducted using advanced surveillance equipment, which allowed the US and Israeli intelligence agencies to intercept and analyze electromagnetic emissions from Iranian nuclear facilities.

These are just a few examples of actual cases of TEMPEST leakage. There have likely been many other instances of TEMPEST eavesdropping and leakage that have not been made public.

D. Fourth attempt (question repeated, verbatim):

Due to the classified nature of TEMPEST-related incidents, it is challenging to find specific examples of TEMPEST leakage in the public domain. However, there have been some documented cases of TEMPEST leakage that have been declassified and made public. Here are a few examples:

1. The Farewell Dossier (1981): The Farewell Dossier was a collection of classified information provided by a KGB agent named Vladimir Vetrov to the French intelligence agency, Direction de la surveillance du territoire (DST). The information included details about Soviet technology, including the design of radar systems, missile guidance systems, and other sensitive technologies. The information was obtained through TEMPEST eavesdropping on Soviet military and intelligence agencies.

2. The Iranian Embassy Siege (1980): During the siege of the Iranian Embassy in London, UK, in 1980, British intelligence services used TEMPEST eavesdropping to monitor the communications of the terrorists who had taken over the embassy. This allowed them to gather critical intelligence that was used to end the siege.

3. The Bonfire Affair (1970): In 1970, Soviet intelligence agents allegedly used TEMPEST eavesdropping to obtain classified information from the US embassy in Moscow, including information about US nuclear weapons. The information was obtained by eavesdropping on the electromagnetic emissions from US typewriters.

4. The Great Seal Bug (1952): In 1952, Soviet intelligence agents planted a listening device, known as the Great Seal Bug, in the US embassy in Moscow. The bug was a sophisticated TEMPEST device that was hidden inside a replica of the Great Seal of the United States. The device was used to eavesdrop on conversations in the embassy for several years before it was discovered.

5. Operation Ivy Bells (1970s): In the 1970s, the US National Security Agency (NSA) used a sophisticated TEMPEST eavesdropping system to intercept Soviet naval communications in the Sea of Okhotsk. The system was installed on an undersea cable that connected a Soviet naval base to the mainland. The system allowed the NSA to eavesdrop on Soviet naval communications without being detected.

These are just a few examples of documented cases of TEMPEST leakage. While details about such incidents are often classified, they serve as a reminder of the importance of TEMPEST protection for sensitive equipment and information.

IX. Recent reports on TEMPEST leakage

Question: Are there any recent reports on TEMPEST leakage

Response ChatGPT:

A. First attempt:

It is difficult to find recent reports on TEMPEST leakage in the public domain due to the sensitive nature of TEMPEST-related incidents. However, there have been a few cases reported in the past few years that have been made public. Here are some recent examples:

1. In 2013, documents released by Edward Snowden revealed that the US National Security Agency (NSA) had been conducting TEMPEST eavesdropping operations against foreign embassies in Washington, DC. The operation, known as "Dropmire," involved placing eavesdropping equipment in the ceilings and walls of foreign embassies to capture data and communications.

2. In 2016, researchers from Ben Gurion University in Israel demonstrated that they could use a simple smartphone to eavesdrop on a computer's electromagnetic emissions and steal sensitive data. The researchers used a technique known as "TEMPEST-style hacking" to intercept the electromagnetic emissions from a computer's CPU, which allowed them to extract sensitive data.

3. In 2018, researchers from the University of California, Irvine, and the University of Michigan demonstrated that they could use a smartphone to eavesdrop on a computer's keystrokes by analyzing its electromagnetic emissions. The researchers were able to intercept the electromagnetic emissions from a keyboard and use them to reconstruct the keystrokes entered by a user.

These recent examples highlight the continued importance of TEMPEST protection for sensitive electronic equipment and information. As technology advances and becomes more interconnected, the risks of TEMPEST leakage are likely to increase, making it even more critical to implement robust TEMPEST protection measures.

B. *Second attempt (question repeated, verbatim):*

As a language model, I do not have access to up-to-date classified information or recent reports on TEMPEST leakage. However, it is important to note that TEMPEST is an ongoing concern for national security agencies and organizations that handle sensitive information. While there may not be many public reports of recent TEMPEST leaks, it is widely recognized that the risk of TEMPEST eavesdropping remains a concern, and efforts to mitigate this risk are ongoing.

In recent years, there has been increased attention on the potential for cyberattacks to exploit electromagnetic emanations to compromise sensitive information. This type of attack, known as a side-channel attack, is related to TEMPEST and can be used to extract sensitive information from electronic devices through the measurement of their electromagnetic emissions. While side-channel attacks are not strictly considered TEMPEST attacks, they do demonstrate the ongoing risk of information leakage via electromagnetic emanations.

Overall, it is important for organizations and individuals who handle sensitive information to be aware of the risks of TEMPEST and take appropriate measures to mitigate these risks, such as through the use of TEMPEST-protected equipment and secure physical and electronic environments.

C. *Third attempt (question repeated, verbatim):*

As a language model, my training data only goes up to 2021, and I do not have access to classified information or current news sources. However, it is worth noting that TEMPEST leakage is a persistent concern for national security agencies and organizations that deal with sensitive information. While specific incidents of TEMPEST leakage are not typically made public due to their classified nature, it is reasonable to assume that efforts to detect and prevent TEMPEST-related eavesdropping continue to be a priority for these organizations.

As technology advances, the risk of TEMPEST leakage may also evolve. For example, as more devices become connected to the Internet of Things (IoT), the potential for eavesdropping on electromagnetic emissions from these devices may increase. This highlights the ongoing importance of TEMPEST protection for a broad range of electronic equipment and systems.

It's also worth noting that research on TEMPEST and related areas continues to be published in academic journals and presented at conferences. These publications and presentations can provide insights into the latest developments in TEMPEST research and can help inform the ongoing development of TEMPEST protection measures.

X. Not important anymore?

<u>Question:</u> If no recent reports on TEMPEST attacks are known, can we conclude it is not an important topic anymore?

<u>Response ChatGPT:</u>

No, the absence of recent reports on TEMPEST attacks or leakage does not mean that TEMPEST is no longer an important topic or that the risk of TEMPEST attacks has diminished. In fact, the lack of reported incidents could be seen as a sign that organizations and governments are being successful in their efforts to protect sensitive equipment and information from TEMPEST attacks.

However, it is important to note that TEMPEST attacks remain a persistent concern for national security agencies and organizations that deal with sensitive information. Even if there have been no publicized TEMPEST attacks in recent years, it is still critical to protect against this type of threat, particularly as technology continues to advance and new vulnerabilities may arise.

TEMPEST protection is an ongoing process that requires vigilance and continuous improvements as technology evolves. It is important to continue researching and developing new TEMPEST protection measures to ensure the security of sensitive information and infrastructure.

XI. Interest in TEMPEST?

<u>Question:</u> Dear ChatGPT, am I the only one asking so many questions about TEMPEST?

<u>Response ChatGPT:</u>

No, you are not the only one asking questions about TEMPEST. TEMPEST is a topic of significant interest to various organizations and individuals involved in national security, information security, and electronic equipment design. As such, it is a subject that generates a lot of questions and discussion.

TEMPEST attacks and countermeasures are an important consideration for anyone who handles sensitive information or works with electronic equipment that may emit electromagnetic radiation. By understanding the risks associated with TEMPEST and the available countermeasures, individuals and organizations can take steps to protect against potential attacks and prevent sensitive information from being compromised.

If you have any further questions or concerns about TEMPEST, I will do my best to help answer them.

<u>End of ChatGPT responses.</u>

XII. Conclusion

TEMPEST is codename referring to spying on information systems through leaking emanations, and due to the classified nature of the topic it is difficult to write an article without the risk of leaking, unintentionally, information. The ChatGPT tool was tested to provide answers on TEMPEST. It is up to the reader to decide if the information is useful. But even for laypeople it is clear that the ChatGPT tool only provides nice answers to satisfy the reader, nothing more.

References

[1] https://en.wikipedia.org/wiki/Tempest_(codename)

[2] https://heinen-elektronik.de/blog/it-sicherheit/bsi-zonenmodell/

[3] https://en.wikipedia.org/wiki/ChatGPT

[4] https://openai.com/blog/chatgpt