xahive

Your Cybersecurity Partner

CYBERSECURITY CYBER-ATTACK SERIES

SIDE CHANNEL – TEMPEST Attacks

Prepared by David Mohajer

What is a TEMPEST attack?

Technical:

"*TEMPEST is the name of a technology involving the monitoring (and shielding) of devices that emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. The term's origin is believed to simply be a code word used by the U.S. government in the late 1960s, but at a later stage it apparently became an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Some sources insist that it is an acronym for Transient Electromagnetic Pulse Emanation Standard*" (An Introduction to TEMPEST, 2016).

English:

A TEMPEST attack is a method of listening to electronic devices remotely and without needing to actually "hack" into the device or otherwise interact with it directly.

Policy:

"The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. To counter this vulnerability, the US Government has long required that electronic equipment used for classified processing be shielded or designed to reduce or eliminate transient emanations. An alternative is to shield the area in which the information is processed so as to contain electromagnetic emanations or to specify control of certain distances or zones beyond which the emanations cannot be detected. The first solution is extremely expensive, with TEMPEST computers normally costing double the usual price. Protecting and shielding the area can also be expensive. While some agencies have applied TEMPEST standards rigorously, others have sought waivers or have used various levels of interpretation in applying the standard. In some cases, a redundant combination of two or three types of multilayered protection was installed with no thought given either to cost or actual threat" (The Complete, Unofficial TEMPEST Information Page, 1999).

(U.S.) Main Office & Mailing Address: 347 Fifth Avenue, Suite 1402-285. New York, New York, 10016, USA
(U.S.) 2nd Office Location: 326 Broad Street, Utica, New York 13501, USA
(Canada) Mailing Address: PO BOX # 47056. 2638 Innes Road. Ottawa, Ontario. K1B5P9 CANADA
(Canada) Office Address: 255 Centrum Blvd., Suite 102, Ottawa, ON, K1E 3W3 CANADA
T: 646-205-2246 **T2:** 613-286-6484 **URL:** www.XAHIVE.com, **Email:** sem@xahive.com

But this is just spying and nation state activity right?

Not anymore.

Due to the complexity and specialized equipment needed to conduct a TEMPEST attack – it has been a Nation-State level cyber attack for most of its existence (1960s).

Only recently has this become something that enterprising Cyber Criminals can consider as a tool in their kit for certain types of TEMPEST attacks with prices running around $200 USD to setup shop with modern (~2012+) era equipment available off-the-shelf (Genkin, Pachmanov, Pipman, & Tromer, 2015).

Types of TEMPEST Attacks

Looking at your monitor
TEMPEST attacks can be used to remotely view the activity of your CRT, LCD and Viewscreen **(Introduction to TEMPEST Attacks, 2005)**.

Learning Encryption Keys from your CPU activity
Do you like using encryption? The emanations of the CPU and other devices in your computer might be giving away enough information to reconstruct encryption and decryption keys for secure protocols **(Schneier, 2015)**.

Watching your internal network
It is possible to read activity of certain types of copper Ethernet cables as they too have emanations that contain useful information.

This means that air-gapped (for security) internal networks might be vulnerable to unauthorized data exfiltration if not properly configured.

Listening to your phone conversations
Hacking into a mobile network is not easy, and ISPs don't like to give access. It is much easier to listen to the electromagnetic emanations coming from devices using TEMPEST and reconstructing the audio or video **(Lee, 2014)**.

More
Pretty much anything electronic is susceptible to TEMPEST.

Is this happening to my business?

Maybe. If you are a large organization with trade secrets so valuable that patents or copyrights would reduce your economic advantage over your competitors – rest assured that HUMINT style infiltration mixed with TEMPEST will occur.

"*The main difficulty in tracking instances of emanation monitoring is because it's passive and conducted at a distance from the target, it's hard to discover unless you catch the perpetrator*

red-handed […] Even if a spy was caught, more than likely the event would not be publicized, especially if it was corporate espionage. Both government and private industry have a long history of concealing security breaches from the public" **(The Complete, Unofficial TEMPEST Information Page, 1999)**.

Preventing a TEMPEST attack

Faraday Cages
The first thought that probably comes to mind for many Sci-Fi geeks are Faraday Cages. Guess what? They are a viable method of protecting yourself against TEMPEST (The Complete, Unofficial TEMPEST Information Page, 1999).

Unfortunately, Faraday Cages are not cost-effective or simple to build nor are they readily available to private organizations as a purchasable product (Genkin, Pachmanov, Pipman, & Tromer, 2015).

You can, however, make your own Faraday Cage – all you need to do is ensure that one side of the cage has a positive charge and the other is negative; then you ground the entire structure. Also a Faraday cage requires there to be no gaps in the structure in order to be effective. There are limitations on the ability to protect against energy emission/detection based on the conductivity of the material used, the thickness of material and the coverage of the actual structure itself. A good technical reference for faraday cages and how they work and could be designed is this YouTube video: https://www.youtube.com/watch?v=t23iXhEiQUc uploaded by Professor Walter Lewin of MIT.

Encryption is key
"*On the software side, it is also advisable to encrypt any data that you send from your computer systems so that even if the emanations were captured, they won't be easily reconstructed into anything meaningful*" (An Introduction to TEMPEST, 2016). This isn't a sure-fire way to protect against TEMPEST. But it is the most cost-effective.

Network cables
Fiber optic networking is a safe, but not so cost-effective way to traverse long distances without risk of emanations.

Additionally, switching your existing copper cable to shielded twisted pair (CAT-STP) can very cost effectively improve security and reduce emanations as well without requiring infrastructure changes.

Infrastructure analysis
The copper pipes in your building might be used as conduits for signal emanations. So, even a secure room inside a facility can leak information through the plumbing! (Schneier, 2015).

Hiring a consultant to do an analysis of your site to determine where the “safe” areas might be for signal emanations is prudent for handling critical data.

These thoughts should also guide the design, installation, and security classification of your data centres.

Further thoughts
Most of the TEMPEST protection equipment prepackaged and ready for sale is not available to private organizations. However, nothing stops a private individual or organization from developing and installing their own TEMPEST protections.

Works Cited

An Introduction to TEMPEST. (2016, September 21). Retrieved from SANS Institute: https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981

Backes, M., Chen, T., Durmuth, M., P.A. Lensch, H., & Welk, M. (2009, January 1). *Tempest in a Teapot: Compromising Reflections Revisited*. Retrieved from mia.uini-saarland.de: http://www.mia.uni-saarland.de/Publications/backes-sp09.pdf

Genkin, D., Pachmanov, L., Pipman, I., & Tromer, E. (2015, September 1). *Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation*. Retrieved from tau.ac.il: http://www.tau.ac.il/~tromer/radioexp/

Introduction to TEMPEST Attacks. (2005, January 1). Retrieved from SuraSoft: http://www.surasoft.com/articles/tempest.php

Lee, J. (2014, January 14). *NSA TEMPEST Attack can remotely view your computer and cell phone screen using radio waves!* Retrieved from CV News: https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/

Schneier, B. (2015, June 29). *TEMPEST Attack*. Retrieved from Schneier on Security: https://www.schneier.com/blog/archives/2015/06/tempest_attack.html

The Complete, Unofficial TEMPEST Information Page. (1999, December 4). Retrieved from jammed.com: http://www.jammed.com/~jwa/tempest.html