GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

TEMPEST And Electromagnetic Emanations Security: Is Not Only A Government Standard.

GIAC Security Essentials Certification (GSEC) Practical Assignment
Option One: Case Study in Information Security

Daniel Garlick
January 27,2005

Abstract

Electro-magnetic emanation interception security, or EMSEC for short, is a relatively new field of research that is only now becoming better known in the private sector. It has been, however, researched and examined for a long time by many governments, particularly by organizations that handle national security information. The US government has developed a complex set of classified policies, standards and physical security measures relating to electro-magnetic emanations and the associated risks that are called simply TEMPEST. This paper will look at TEMPEST standards and policies that can be of use to the information security managers of private sector organizations. We will discuss the threat at large and why security managers should harden their information systems and networks against this threat. There are a number of things that can be done to decrease emanations and prevent interception of clear text data. We will look at these countermeasures that can help managers and their organizations. The major difficulty is the fact that much of TEMPEST's technical specifications are still classified.

© SANS Institute 2005 Author retains full rights.

EMSEC

Computers have become ubiquitous in our society and are becoming increasingly common everywhere we look. Corporations have gone online building web portals for customers, partners and employees to use the power of the Internet to conduct business. Also, small and medium-sized companies have gone to an e-commerce business model and away from the brick and mortar framework. Education, finance, medicine, and government are all now big "net-centric" industries, and their information assets and resources are contained on distributed databases and the web. It is critical that these resources are kept safe and secure from those who do not have the right or privilege to access them.

Even as the Internet and computer networks have technologically progressed over the years, security has often been an area forgotten or marginalized by upper management in many organizations. Recently, security has become a touchstone for organizations that now understand the threat and risk to their vital information resources and assets. So now organizations are investing in stronger physical security techniques such as more rigorous authentication and/or more complex encryption algorithms. Also, organizations are spending more time in the area of logical security measures such as educating system users on how to protect their information assets properly. This education takes many forms such as teaching users to keep their workstations patched to not opening email attachments without first scanning them with a quality anti-virus product.

These measures and improvements have resulted in a vastly more secure environment for both public and private sector organizations as they carry out their activities. In the past, it was fairly easy for individuals to conduct successful attacks on the Internet-facing information systems and networks of organizations. Now, however, it has become much more difficult to be successful in cracking the defensive measures that firms and organizations are implementing to keep their information secure. One quality that hackers and other online attackers have shown is that they are generally very adaptive to technological advances in security tools and eventually find ways to circumvent these security solutions. The big question is the feasibility of these attack methods and the patience of the individuals using them. It is still a certainty that dedicated attackers who are set

on breaking into your system will continue to try until they have succeeded.

© SANS Institute 2005 Author retains full rights.

Due to the current effectiveness of information security measures and other types of technology being implemented in organizational networks, attackers will have to look to more and more technically sophisticated solutions to access the information assets they seek. Private firms and organizations need to exhibit greater concern about more sophisticated attacks. In the past, such technically advanced attacks fell primarily in the province of foreign governments since the cost of such attacks can be quite high.

The information available online and within corporate networks is now valuable enough to justify the initial investment for criminals. In addition, the prevalence of companies spying on competitors has increased significantly with the advent of the Internet. This is where the electro-magnetic emanations originating from computer monitors and other communication devices come into play. This is just one method that attackers WILL use to gain access to this wealth of valuable information." TEMPEST has been shrouded in secrecy. A lot of the mystery really isn't warranted though. While significant technical details remain classified, there is a large body of open source information, that when put together forms a pretty good idea of what this dark secret is all about." (McNamara,2004).

TEMPEST, which stands for Transient Electromagnetic Pulse Emanation , refers to a set of standards and countermeasures that was set up by the US Government to protect classified intelligence from being intercepted via spurious electromagnetic emissions from telecommunications equipment such as computers, scanners, printers, modems, and other telecommunications equipment. Everything that uses a transistor, microchip or other such device releases miscellaneous electromagnetic emanations. A circuit with a time varying current releases electromagnetic signals equal to the amplitude and its time rate of change. These signals go out as free space waves and as guided waves via conductors connected to the source. Now, if the time variations of the source are at all similar to the data in the signal, then it's also possible the electro-magnetic emanations will also be relative to the data.

So, what is the danger? The problem is that someone could sit in a parking lot 100 meters away and, with the right information-gathering equipment, could intercept, store and process this information back into another format that could be interpreted.

Generally, speaking the cost of electro-magnetic emissions interception and rebuilding data equipment can be found from $3000 up to $250,000 or more. Though some experts in the field of EMSEC have put together makeshift systems with a few hundred dollars worth of equipment purchased at their local Radio Shack and successfully reconstructed data. This can be a problem not

© SANS Institute 2005 Author retains full rights.

just for the government relating to national security information, but also for corporations trying to protect proprietary technology or other critical business data.

It should be noted that any discussion of TEMPEST will have to be somewhat general in nature. This is because much of the technical information related to TEMPEST issues is classified and controlled under a stringent US government need-to-know basis. Most EMSEC information, especially TEMPEST specific specifications, has been classified since 1995. This is primarily due to the fact if attackers had free access to the exact information included in the TEMPEST project, in particular the countermeasures, then the standard would be made largely ineffectual. This has limited the commercial applications of EMSEC technology and education in the private and educational sectors.

The history of TEMPEST goes back to 1918. During World War 1 the US government enlisted the help of Herbert Yardley to study how to detect and intercept signals from enemy's secure and combat telephones. However, Yardley's investigation uncovered that the Allies normal communications devices were allowing classified to be passed to the enemy. As a result, methods of decreasing signal emanations, such as using special shielding or the grounding of communications equipment cables, were implemented. Over the years, as technology advanced in both the telecommunications field and in signal interception, so to have the standards and countermeasures of EMSEC advanced in sophistication. EMSEC, or Emissions Security, has become the modern term for TEMPEST, which was more popularly used in the '60s and '70s.

The government has been approving TEMPEST certified equipment and devices that meet the strict standards of the TEMPEST program. These devices are tested and certified to their effectiveness in decreasing the emanations of the electromagnetic waves coming from them. If approved as TEMPEST compliant, the emanations from a device have been reduced by shielding or other technology so that it is relatively difficult to intercept signals and rebuild information screens. Currently, TEMPEST-approved devices are only sold through the government to contracted companies that work for or with the government handling classified information. There are claims by some hardware vendors that their products are TEMPEST compliant, but those are usually false claims since the TEMPEST standard is still just a US government program.

Electro-magnetic emanations security is still a fairly new field of study in which most IT professionals are unaware of the risks and preventive measures to take. Relatively few U.S. companies outside of defense-contractor circles appear to know much about the threat of computer-monitor surveillance or the government's Tempest program"(McCarthy,2000). Certain software methods can help to reduce the vulnerabilities caused by the miscellaneous release of

© SANS Institute 2005 Author retains full rights.

electro-magnetic emanations. Basically, software can transmit data in a format that is easy to collect and reconstruct into readable forms. However, if software is used to transmit information so that it will be much more difficult to recollect the data and reconstruct the data into screens again, security will be greatly enhanced.

Computers are a particularly rich source of electromagnetic emanations due to the types of signals they use .One new eavesdropping technique is an optical spying approach directed at computer CRT monitors and the light they emit. The technique involves observing the high-frequency variations in the emitted light. In many cases, enough of the original video signal remains. If these signals are intercepted, they can be used to rebuild readable text and screens from a CRT monitor. It is believed LCD screens eliminate this threat, but that is not true. They do reduce emanations, but do not eliminate them altogether.

Advances in state-of-the-art equipment design and signal processing techniques have intensified concerns about electromagnetic surveillance. While a few technologies such as fiber optics and multiplexing have made interception and analysis more difficult, the overall effect has been to open new opportunities for eavesdroppers (Pike, 2000). Projections for the immediate future indicate that this trend will continue. The only safe approach is a reasonable worst-case evaluation. It must be assumed that the opposition has the proper equipment to monitor all signals of significant amplitude in areas where access is uncontrolled.

EMSEC professionals are worried about electromagnetic emanations from all electronic devices and electronic surveillance. The concern stems from the fact that signal interception, gathering, and processing have greatly advanced as of late. Some new technologies such as multiplexing of network cables and fiber optic cables have made it somewhat more difficult to intercept and process data. Commercial organizations that have classified organizational information resources that need to be safeguarded must do as governmental agencies have done for decades under the TEMPEST program and assume that attackers have the means to attack. If private firms and other organizations have contingency plans in place for attacks, whereby attackers try to intercept and collect the electro-magnetic signals from computer monitors and other computer components, they will be far better prepared to deal with attacks when they do occur.

So what exactly can a private sector organization do to minimize their information assets vulnerability to this type threat agent? The main problem is the way a computer, or any electronics circuit for that matter, works in general. A circuit will usually use more energy than is needed because the electrons in the original current run into resistance in the form of protons or neutrons along the circuits path. To overcome this resistance, more energy is used; in the end some of this extra energy is released as heat or signal noise.

© SANS Institute 2005, Author retains full rights.

Sound waves are curved in their natural form, called sine waves. They are easily represented as a mathematical formula. Computers, however, use square waves that are known as digital signals. Since these square waves are not natural, they cannot be represented in any universal mathematical formula such as sine waves. Accordingly, if there is a change in the signal level, there is no way to show the change from one signal level to the next. Now each signal level can have different mathematical values, but not one value to represent all levels of changes between the levels. This causes some discontinuity in the signal. The problem also requires an increase in energy causing stronger signals.

A computer essentially requires more energy to overcome resistance build up and discontinuity in order to change state from one level to the next. Some of this additional energy, as mentioned earlier, is given off as heat or noise. However, most of this energy, in the form of organized noise, is thrown out of the circuit into the air like a radio signal. Two things determine the strength of the emanating signal. One is the time it takes to make the change: the shorter the time, the more energy required. The other is the difference in the levels corresponding to the amount of energy that will be required, with a bigger difference needing more energy. Also, electro-magnetic signal noise can emanate from circuits if the right conditions exist. The strength of the electromagnetic field generated is related to the magnitude of the signal and varies as the signal does.

There are a few specific measures that can be taken to reduce the threat of electro-magnetic emanations. One new technology that shows some promise in anti-eavesdropping is conductive concrete, which was designed to be an optional building material in very cold and snowy climates. The concrete is made with the additive coke breeze, which is coal that has been converted into a nearly-carbon material. This additive substance allows the concrete to conduct electricity that gives off heat and thus is perfect for cold climates. “But, this conductive concrete can also, be used to block computer equipment emissions”(Austen, 2002).

One of the most effective approaches to eliminating or at least substantially reducing electro-magnetic emissions is to use a faraday cage. A faraday cage is a five-sided steel box that usually encases the processor or other computer components to block and contain electrical fields. Most computer CPUs now run at well over 2 or even 3 GHZ, which means it has become much more difficult to contain electro-magnetic emanations. Computer manufacturers have tried to contain these increasing electrical fields and electro-magnetic emissions associated with them by reinforcing the computer frame and chassis, but this is not a financially feasible or entirely effective approach for private sector organizations. A better method would be to use a faraday cage to reduce these electrical fields.

© SANS Institute 2005 Author retains full rights.

One of the most important things to do is to first identify possible sources of extraneous noise. There a number of tools and methods to help identify noise sources. “Possible noise sources can be identified through technology roadmap analysis, product EMI history, and package and process review, among other analyses” (Raza, 2001). Once electro-magnetic sources have been discovered, then a faraday cage can be implemented. However, something to keep in mind is the difficulty in predicting where noise emissions will come from or how strong they will be until the entire system and all related components are up and running.

Once the system is approved and online, however, it is not practical cost-wise or an effective use of manpower to modify the system design. As a result, faraday cages have to be more or less ad hoc and implemented after the system is running. RF shielding is a refinement to the faraday cage method that was really designed for electrical fields more than electro-magnetic radiation. This shielding will absorb a significant portion of the emissions and contain more to help reduce the electro-magnetic emissions.

There are more than just technical measures that can combat these kind of advanced attacks. Policy is a tool that can greatly safeguard against EMSEC threats. The military uses a four-step COMSEC (communication security) policy that includes physical, emissions, transmission, and cryptography (Pike, 2000). COMSEC is an important idea even for private sector firms. It must be remembered that the security of information assets is a management problem as much if not more than a technological one. Management must look at this new type of sophisticated, aggressive attack and plan ahead.

Ultimately, we have to realize that there is no foolproof system of security, but we can minimize risks and vulnerabilities. If an organization plans in the design stage of a system or facility’s lifecycle, physical security concerns can be taken into consideration and some of the TEMPEST measures we have mentioned here such as shielding cables or Faraday cages can be incorporated. Also, firms can have equipment and cables separated according to the type of information they carry. The military does this with its black and red components model, where equipment is grouped physically together into two categories: red and black. Red

refers to anything that has to do with information that has national security value and therefore would be classified. Black relates to anything that does not have national security information, and is thus unclassified.

Many upper management and security managers may think they are safe since they encrypt their information with 3DES, IPSECv2 and so on. This is both true and false. They are correct in the fact that transmitted information is encrypted and fairly secure. However, this information has to be decrypted at its

© SANS Institute 2005 Author retains full rights.

destination, and this is where there is a window of opportunity for someone to intercept the screens (Murphy, 1997).

TEMPEST is a government and military standard, and so is difficult to impose on a private firm. There are lessons and guidelines, however, which firms can adopt from the government's TEMPEST standard. Another thing we have to do is weigh the costs and benefits. While some "hard" targets may justify a technical approach, traditional human intelligence (HUMINT) gathering techniques are without a doubt, used much more often than emanation monitoring (McNamara, 2004).

It should be noted that there are a few obstacles to the successful interception of an electro-magnetic signal. One has to be fairly close to the original source of the signal, and this can be both difficult and dangerous. First, many organizations are starting to build facilities that allow for more space between buildings and public areas such as parking lots. Also, organizations now frequently endeavor to locate computers with critical data well away from walls that are in close proximity to outside areas. The reason for these new preventive measures was primarily to deter war dialing associated with virtual private networks (VPN's). However, these steps have also decreased the likelihood of an attacker sitting in an adjacent parking lot and intercepting signals. In addition, since the interceptor has to be fairly close to the transmitting source, the chance of detection is greatly increased; this is especially true after the 9-11 attacks with the heightened sense of awareness.

In conclusion, the threat of electro-magnetic emanations interception is a real, but to date there have not been any confirmed cases or incidents of successful attacks in the private sector (to the extent of our current knowledge). This is most likely due to the time, cost and overall dedication required to carry out such activities. The chances of an individual attempting this type of activity against a given organization are most likely slim at best. Nonetheless, information security managers should be prepared for the worst, especially if they have information assets that need to be kept secure and confidential. Signal interception technology is increasing, and no one can say if this will soon allow for this threat to increase. As the old saying goes no one knows what the future holds.

© SANS Institute 2005, Author retains full rights.

References

1.Air Force Instructions 33-203.Emmissions Security. (1998). http://jya.com/afi33-203.htm

2.Atkinson James. (2002). TEMPEST 101: Debunking the Myth Web page. <http://www.tscm.com/TSCM101tempest.html>

3.Austen,Ian. "A Concrete That Percolates, Keeping Snow and Spies at Bay."new York Times. 21 March 2002. Retrieved on 22 November 2004: < http://www.nytimes.com/2002/03/21/technology/circuits/21NEXT.html?ex=1106888400&en=e918f9c634ffedf4&ei=5070&oref=login

4.Kuhn, Marcus."Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations." Retrieved 1 December 2004 : <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf

5.McCarthy Michael.(11 August 2000). "The Pentagon Worries That Spies Can See Its Computer Screens." Wall Street Journal. Retrieved 28 November 2004:< http://cryptome.org/tempest-fret.htm

6.McNamara, Joel. (2004) "The Complete Unofficial TEMPEST Information Page." Retrieved on 22 November 2004 :< http://www.eskimo.com/~joelm/tempest.html>

© SANS Institute 2005 Author retains full rights.

7.Murphy,Ian. (1997).”Who’s Listening?”IAM Secure Data Systems,Inc.< http://www.ravenswoodinc.com/captwhos.htm

8.Pike, John. 2000. Federation of Scientists:Intelligence Resource Program. Retrieved on 22 November 2004 :
< http://www.fas.org/irp/program/security/tempest.htm>

9.Raza, Ishfaqur. (2001) “Faraday Cage Enclosures and Reduction of Microprocessor Emissions.”Compliance Engineering.com. Retrieved 24 November 2004:
< http://www.ce-mag.com/archive/01/Spring/Raza.html>

10.Wim, Van Eck (1985) “Electromagnetic Radiation from Video Display Monitors: An Eavesdropping Risk”? Computers and Security Vol 4< http://jya.com/emr.pdf>

11. Wikipedia:TEMPEST page.< http://en.wikipedia.org/wiki/TEMPEST>

© SANS Institute 2005, Author retains full rights.