Global Information Assurance Certification Paper

TEMPEST

Gary Kelly

November 13, 2000

I. Introduction

Ever seen a James Bond movie? More than likely you have. What do you like best? The action? The women? How about all those nifty gadgets? Well a Tempest device could be in a James Bond film. It is a gadget or rather a classification of gadgets. Of course Hollywood has the best gadgets because they don't really need to function. But the same type of creativity that generates those films is out there making some extremely good surveillance products.

All electronic devices emit electro-magnetic radiation. The radiation can travel through mediums such as air or conduit. This is where it gets interesting. There exist devices capable of reading/displaying/recording this information. For example, the monitor sitting on your desk, a device could be used to perfectly mimic your displays contents at a distance. 007 would be proud. The NSA has recently de-classified some information on these wondrous devices, or more specifically warnings on how to protect assets from them. The Internet has provided us with information to infer how these devices work and what countermeasures maybe applied.

II. Description

What is Tempest? Officially Tempest is not the tool it's the protection, or rather a code name of these protection standards. Much like a Di-lithium crystal or flux-capacitors, a device with tempest emblazoned across its side does not exist. Tempest is actually the government standards to reduce the emission or likelihood that those emissions can be intercepted of electronic devices. These standards are not unique to the USA. Several European countries have agencies and guidelines to protect against emanation snooping. As we speak Tempest has undergone some changes. Tempest appears to have become EMSEC or Emanation Security.

The theory is that any electronic device creates electromagnetic emissions. These emissions can be detected. If the listening device is sophisticated enough and the operator is skilled enough, the information can be intercepted. Most people will associate information and electronics to computers. Computers are a primary candidate for snooping. However it is not the only device that holds risk. Simple office electronic hardware can be intercepted such as fax machines, printers, and input devices. If someone could intercept messages from a fax machine what could they see? In some ways that maybe more damaging than having a computer hacker invade your network.

Tempest is merely a listing of guidelines for defense against electronic eavesdropping. The defense includes shielded devices, shielded structures or perimeter zones. Tempest shielding is basically the "armoring" of a device or location by using highly conductive materials such as copper tubing. Since most emanation attacks must be physically close to a source, a large enough perimeter may be enough to defend against some eavesdropping. Think about this: humans by their very nature can only decrypt the most basic of information. For instance your eyes view light radiation and you see, your inner ear vibrates just right and you hear. Get hit by bright light or a loud noise and those functions are lost. When we encrypt information we are basically simulating the bright light or loud noise over data by using mathematics. Now to bring it together: when you are viewing a monitor screen it can't easily be encrypted because you will no longer be able to interpret the screen with your basic vision. One more step: if the information that you can interpret with your rather unsophisticated decryption devices (eyes and ears) is freely available to the airwaves how long do you think it would take to decipher? Rather than investing in supercomputers to decrypt information why not just listen harder for unencrypted information?

This topic tends to remind me of the guy sitting on a park bench wearing dark sunglasses and reading an upside down newspaper: The clichéd stakeout guy. What's bad about this situation is that the stakeout guy could be a kid roller-blading past your office or a bum loitering a block away. The traditional cloak and dagger surveillance that you see in cop shows and spy movies does not apply. I can't describe what one of these devices looks likes, how much it weighs or what its capabilities. A large portion of this topic is still classified. What we can tell is what is being demonstrated to us by the Governments actions. Do I think a roller-blader could carry an antenna big enough to intercept a monitor's content at a distance, probably not. From my research that antenna may be the size of a motor home, but again specifics are just not available.

iii. History

Emanation security is not a new concept. The government documentation indicates that the government was developing standards back in the 1950's. As I have discovered Tempest security levels have been present in the military for decades. The two departments with the most input appear to be the NSA and the Department of Defense. I have also discovered that the cost of Tempest shielded equipment is high. With cutbacks and so on it looks like the government has broken their electronic devices into two categories: the RED and the BLACK. The RED devices contain highly sensitive information; the black devices may not contain overly sensitive information but still need secured.

Shielded devices actually hold patents, by companies such as IBM. This is a good indication that a significant investment has been required to secure electronic

assets.

iv. Securing Devices

The security of electronic devices involves several techniques. There are two basic categories: secure the site or secure the device.

To secure the site the walls can be shielded using blocking materials such as conductive metal. Windows can be ordered that block RF transmissions. Grounding techniques and isolated shielded cabling can also reduce emissions. Building layout and design can have a great impact. By increasing the distance to target, the size and sophistication of the listening devices must be greatly increased and the risk of data capture is greatly reduced. Some of my research indicates that there may exist devices that produce emissions that block or impair the interception of the target emissions.

Securing the device is just that. By wrapping the device in conductive materials the emissions are absorbed. Not being that technically inclined my interpretation of an "emission" is a collateral signal that is not being completely absorbed by the target. The term errant was used. Therefore if the shielding is inadequate the errant signal could escape and still be intercepted. It is therefore necessary to layer your defenses. Secure each component with shielded materials. Secure power to the device. Use shielded cables wherever possible. It has been indicated that a lot of shielded devices are developed using trial and error. In other words add this capacitor and check to see if the emissions are reduced. Another source indicated using a simple AM radio as an antenna around the device to detect increased amounts of static, which would represent emissions. There also appears to be specific fonts that are vulnerable to interception.

V. Conclusion

This topic is like an episode of X-files. The truth is out there. What I hoped to accomplish was to inform people in the private sector of this topic and stimulate interest. Because of the highly secretive nature of this information, discerning hard data from Internet Sources is a risky business. If there is additional information or corrections to my laymans attempt at the description of this topic please feel free to contact me and I will correct them. I would also like to say thanks to people who take an active role in gathering information about this seldom heard of topic.

The security of emissions has received a little public scrutiny. Their costs however are very significant. It appears that the government has released only what it had to protect its resources. Can you risk leaving assets un-protected against these devices?

References:

1) McNamara, Joel. "The Complete, Unofficial TEMPEST Information Page". 2 October 2000. URL: http://www.eskimo.com/~joelm/tempest.html

2) Murphy, Ian A. "Who's listening?" copyright 1997. URL: http://www.ravenswoodinc.com/captwhos.html

3) Hesseldahl, Arik, Forbes.com. "The Tempest Surrounding Tempest". 10 August 2000. URL: http://www.forbes.com/2000/08/10/mu9.html

4) Gabrielson, Bruce C. "What is Tempest". September 1987. URL: http://206.102.92.130/ses/papers/TEMPEST/Whatis.html

5) Smith, Jeffrey H. "Redefining Security". 28 February 1994. URL: http://cryptome.org/jcs.html