2006

Electronic Protection / Chapter 77, The Handbook of Information Security

Rowe, Neil C.

Monterey, California. Naval Postgraduate School

Chapter 77 in the The Handbook of Information Security, H. Bidgoli, ed., New York: Wiley, 2006.
http://hdl.handle.net/10945/36447

Electronic Protection II-7

Neil C. Rowe
U.S. Naval Postgraduate School

INTRODUCTION
ELECTRONIC EMANATIONS FROM COMPUTER TECHNOLOGY
- The Physics of Electronic Emanations
- Electronic Eavesdropping Technology
- Points of Weakness for Electromagnetic Emanations in Computer Systems
- Error Correction

REDUCING THE THREAT OF ELECTRONIC EMANATIONS
- Electromagnetic Shielding
- Source Suppression
- Noise Generation and Encryption
- Signal Irregularity
- Deliberate Deception
- Bug Detectors

PROTECTING AGAINST OFFENSIVE SIGNALS
- Damage Mechanisms for Electromagnetic Signals
- Countermeasures for Damaging Electromagnetic Signals
- Electromagnetic Noise to Interfere with Computer Systems

CONCLUSIONS
Glossary
Cross References
References

Key words: Bug detectors, camouflage, eavesdropping, electromagnetic pulses electromagnetic radiation, electromagnetic shielding, emanations security, emissions security, encryption, high-power microwaves, information warfare, source suppression, TEMPEST.

Electronic protection involves methods of preventing spies from stealing secrets from the electromagnetic emanations of your information systems, as well as methods of preventing saboteurs from incapacitating or destroying your information systems using electromagnetic radiation. We discuss the kinds of threats and what can be done to reduce or prevent them. Particular weaknesses are video monitors, keyboards, and cables. Electromagnetic shielding is helpful, but requires special additions to computer hardware. Source suppression, noise generation, encryption, deliberate irregularity, and deliberate deception can also help against spies but require careful planning. Bug detectors can alert you to electronic devices that may be eavesdropping, but do not always work. As for electromagnetic sabotage, similar shielding methods can protect against it, but backup methods are important, including current limiters.

This is chapter 77 in the *The Handbook of Information Security*, H. Bidgoli, ed., New York: Wiley, 2006.

INTRODUCTION

The term *electronic protection* has been used inconsistently in the literature to mean several things related to information security. We interpret it here in the strict sense of methods of protecting information systems from attacks that do not require an electrical or software connection to the target but exploit electromagnetic effects of electronics. Unfortunately, electrical connections to a target system are not necessary to have serious security problems. We do not consider here other important aspects of this considered elsewhere in the *Handbook*, such as radio frequency and wireless communications security, wireless information warfare, hacking techniques in wireless networks, mobile devices and protocols, and smart card security. We also do not consider primarily nonelectronic physical attacks on computer systems and networks such as explosions of conventional munitions (see Physical Security Threats).

The two main threats addressed by electronic protection are people trying to steal your secrets (spies) and people trying to vandalize your hardware or prevent it from working (saboteurs). These threats are more associated with military information systems than civilian systems and are particularly serious in battlefield situations (Friedman, 1983), so much of the research has been done by military organizations. Spies in a military setting are trying to get intelligence, and if they get it from electronic signals, they are doing signals intelligence (SIGINT; Zorpette, 2002). But spying and sabotage are also an increasing problem for businesses; secrets of competitors can be worth considerable money and effort. Incidents may be underestimated because it is of little advantage for either the military or business to report them. Electronic spying and sabotage are usually illegal; in the United States, U.S. Code Section 2511 prohibits real-time acquisitions of electronic communications in transit, and many countries have similar laws. But this has not stopped determined spies when key government, military, or business secrets are at stake.

Like all security measures, electronic protection must be cost-effective. One needs to assess the likelihood of an attack and how serious the results of that attack might be. It is thus important to do a risk assessment (see Risk Assessment and Risk Management) before committing to the protection methods to be discussed.

ELECTRONIC EMANATIONS FROM COMPUTER TECHNOLOGY

We first consider the problem of leakage of information from a computer system or network through the electromagnetic radiation it produces. This has been termed *emanations security* or *emissions security* in the military literature.

The Physics of Electronic Emanations

It was discovered in the 19th century by Oersted, Faraday, and Henry and formulated in Maxwell's equations that changing electrical currents induce changing magnetic fields and magnetic fields induce changing currents. Computers use patterns in currents for operations and communication. These changes induce a changing magnetic field that propagates as an electromagnetic wave through surrounding space. This field can be picked up by electrical conductors in the vicinity, and in bad cases can impede operations of other electronic devices via *electromagnetic interference*. Thus an antenna with an amplifier can pick up a considerable amount of signal from a nearby computer and can reconstruct the generating electrical signals. Electromagnetic signal strength or intensity is the amplitude of the electromagnetic field waveform at some point in space (also called the electric flux density) and is the major factor affecting detectability of the signal. Signal intensity generally decreases as the square of the distance from the radiation source. Bugging devices within computers can pick up signals more successfully than remote ones can.

Electronic protection has not improved as the speed of computer technology has increased. With clock times now below nanoseconds, computers are radiating signals whose base frequencies are in the range of microwave radiation. As with microwave ovens, microwaves have good penetrating power for many kinds of materials. (The higher the frequency, the more energy the radiation has; however, penetration ability varies considerably with the chemistry of the material.)

Matters are made worse by the use of abrupt changes between two levels of voltage in digital hardware. The more abrupt a transition, the more high-frequency components in its spectrum. A sine wave has only one frequency; a square wave consisting of alternation between two voltages has a frequency spectrum of odd multiples of a base frequency where the amplitude of the components is inversely proportional to the frequency. High-frequency components of a waveform are refracted less by materials than low-frequency components, making them easier to detect if they are not absorbed. Furthermore, materials that one frequency poorly penetrates may be much more transparent to another?and the harmonics of an abrupt transition can be significant over quite a range of frequency. A spy may need only find one frequency to recognize the transition of a digital signal.

Several additional factors affect the intensity of signals emanating from a computer system:

- Higher currents produce stronger signals than lower currents. Most parts of computers run on relatively low currents, but an important exception is a cathode ray monitor, which requires hundreds of volts. Consequently, their screen images are easier to detect than most computer signals.
- Slower signals are often easier to detect than faster signals because they stand out better from the background noise. Therefore cables connecting to a modem are more susceptible to eavesdropping than a cable to a fast digital telephone line. However, faster signals may also radiate better.
- Periodic signals are easier to detect than irregular or one-time signals because signal energy can be summed for corresponding

parts of each period, greatly helping detection. Important periodic signals occur in many places in computers, especially in the central processing unit (CPU) cycle, the monitor screen refresh process, and the loop that monitors the keyboard for key depressions.

- "Unbalanced" signals are easier to detect than balanced signals. Signals are balanced when pairs of opposite currents occur on adjacent wires. Balance is a problem for some kinds of cables.
- Many sophisticated techniques from electrical engineering can help detect signals in the presence of noise, even nonrandom noise (Garth & Poor, 1994).
- Electronic circuits have resonant frequencies. An external signal can be broadcast to a computer system to induce it to resonate at one its natural frequencies. This has the effect of modulating normal signals of the computer, making them easier to detect by demodulation. However, the effect is weak and it is difficult to control what kind of information you obtain.
- If a spy can plant a Trojan horse on a computer system, it could deliberately create periodic loops in code to make stronger electromagnetic signals, providing a covert channel for transmission of information (see Side Channel Attacks).

Electronic Eavesdropping Technology

An electronic eavesdropper uses bugs consisting of the following:

- A device for picking up signals, as large as possible and as close as possible to the source while maintaining concealment; this can be an antenna at a distance or an induction loop around an electronic component
- An amplifier for the signals from the antenna
- A receiver (electronic filtering to extract the signal from the noise); the emanations of a computer are not designed for easy separation like radio stations are, but good filters can be effective
- Either a recording device (which may be hard to conceal given the amount of data recorded) or a retransmission device; retransmission is commonly by radio at a specific frequency, but could also be done by digitizing and connecting to a computer network (if the signal picked up is video, it could be retransmitted to another screen nearby)

Bug technology continues to decrease in size for the same performance (Murray, 2003). Intelligence agencies use bugs camouflaged as all kinds of everyday objects, so do not expect them to be easy to recognize. They may not need to be camouflaged much anyway? most people rarely look inside the cabinet of their computer. Even chips could be bugs because many computers leave empty slots during manufacture to permit later expansion. Good places to put bugs are on the display and keyboard drivers to enable reading of everything the user is doing. People who like to be suspicious have claimed bugs are widespread (Thomas, 2004), but one must be skeptical of much of what one reads about bugs on the Internet.

Points of Weakness for Electromagnetic Emanations in Computer Systems

We enumerate here some particular sources of signals that spies could exploit for electronic eavesdropping.

Cathode Ray Monitors

The traditional television-style monitor screen is a big source of emanations. Van Eck (1985) stimulated a great deal of interest by showing how easy it was to duplicate the display of a traditional cathode ray monitor on a nearby monitor using just the radiated signal. Reception is aided by high currents used by such devices. In addition, screen display follows a consistent periodic sequence: Each line of the screen is drawn from side to side, and the standard VGA format uses exactly 480 lines with exactly 640 pixels per line. This means one can reconstruct the screen signal by an easy guess as to the vertical sync (the time to draw all lines) and the horizontal sync (the time to draw one line) (Kuhn & Anderson, 1998). Liquid-crystal displays such as those found in most laptops do not use this mechanism but still give some weaker emanations nonetheless, especially the back-lit ones common today.

Keyboard

Another weakness is the keyboard-handling software. Usually the keys are sampled periodically by a keyboard driver to see if they have been depressed. This produces a near-periodic signal that can be compared between cycles to detect key depressions. However, it involves transitory changes and lower currents than those of the monitor.

Cables

Electrical cables connecting a computer to other devices can be a source of signal because of their similarity to antennas (which are long wires, too). Cables can use higher currents than CPUs because of the need to reduce transmission losses. Modem cables in particular are desirable targets because of their low data rates and the possibility of picking up passwords and keys in the clear. Furthermore, modems often use serial (one-at-a-time) character transmission, which reduces the number of signals that need to be distinguished by the eavesdropper.

Most cables are shielded to reduce the electromagnetic interference on their signal from other devices. (Exceptions include many telephone cables that are unshielded twisted pairs.) This means that the main conductor is surrounded but separated from an electrically conductive covering that carries the ground (or comparison) voltage. In principle, this should reduce emanations substantially. But in practice, not all cables are properly grounded (grounding can be difficult), not all shielding is effective (good cabling costs money), and there is a source of signal at each end where the cable connects to other electronics. Smulders (1990) showed a surprising ability to pick up signals from a modem cable with a standard radio receiver.

Power and Ground Voltages

Electrical devices using varying amounts of power create transients in the power and ground connections that they use. The effect is visible on any device sharing the same power connections, as within a building. This effect is often seen when large motors turn on and can be seen to a lesser extent with computer peripherals, especially a cathode ray monitor. But the signals produced are very noisy because everything attached to the power line or ground can also produce an effect.

Magnetic Disks

Magnetic hard disks rotate continually even when not being read. If the disk head remains over a particular track on the disk, it will generate a periodic signal representing the bits on that track. But this is uninteresting data most of the time, and the signal may be so weak because of shielding that it would be easier to directly connect to the associated computer system.

Optical Signals

Light is also electromagnetic and we need to prevent reading of computer screens through windows with telescopes. Just ensuring that the screen is unreadable at a reasonable distance is insufficient with cathode ray monitors, because the changes over time in the total diffused light from a monitor can carry enough information to enable reconstruction of characters (Kuhn, 2002). Many computers and peripherals also have light-emitting diodes (LEDs) intended to give operators a simple summary of what the devices are doing. However, LEDs can switch on and off at a rate up to 10 ns, far beyond what people can detect, and this could be a covert channel to signal information to a confederate (Loughry & Umpress, 2002).

Error Correction

Detected electromagnetic emanations have considerable noise, because the transmission of information is neither engineered nor intended. A variety of error-correction methods can be used by the eavesdropper. Conventional electronic filtering can be done when the signal has a primary frequency, or a strong known unwanted frequency can be filtered out. Video signals have a variety of specialized correction techniques that have been developed to aid copying of video. Research in optical character reading (Liu, Babad, Sun, & Chan, 1991) has developed a variety of robust techniques for correcting noisy images of characters.

As for digital data, error-correcting codes and checksums in network transmissions can be picked up by the eavesdropper to correct some reception errors (Forouzan, 2003). But even without such codes, a spy eavesdropping on text can exploit knowledge of an alphabet or language used to rule out most errors. For instance for English, 20,000 words is a common vocabulary size for a native speaker, and the average word is eight letters long. Yet there are 200 billion possible eight-letter words, so most of the one-character errors in interpreting an eight-letter English word are easy to correct. Kukich (1992) gives a comprehensive overview of algorithms for such corrections. For other kinds of data, knowledge of the typical symbols can be formulated from experience (Moulin & O'Sullivan, 2003).

The frequent predictability of software can be exploited by an eavesdropper. For instance, encryption algorithms often start execution with the same sequence of code; an eavesdropper could learn to recognize the signals corresponding to that code and then zero in on the plaintext key typed next. The eavesdropper could learn the necessary patterns by obtaining and running their own copy of the encryption software.

REDUCING THE THREAT OF ELECTRONIC EMANATIONS

In the face of these threats, several techniques can prevent or reduce eavesdropping, as summarized in Table 1.

Table 1. Summary of the Suitability of Electronic Protection Methods for Attack Targets

Threat	Monitor	Keyboard	Cables	Power and Ground	Disks	Optical Signals
Electromagnetic shielding	Yes	Yes	Yes	No	Yes	No
Source Suppression	Yes	No	Yes	Yes	No	Yes
Noise generation and encryption	Yes	Yes	Yes	Yes	Yes	Yes
Signal irregularity	Yes	Yes	Yes	Yes	No	Yes
Deliberate deception	Yes	No	Yes	No	Yes	Yes
Bug detectors	Yes	Yes	Yes	Yes	Yes	No

The most obvious techniques are concealment of the emanations themselves by reducing their intensity. This was the idea behind the TEMPEST standards adopted by the U.S. government in the 1960s to reduce emanations from their important computers (McNamara,

2004). Although the quantitative details of TEMPEST specifications are still secret (i.e., they are classified), the basic principles are available in the open literature. TEMPEST has not been as important since a 1991 report of the U.S. Central Intelligence Agency concluded it was not cost-effective, especially within the U.S. in protecting against foreign spies. TEMPEST hardware for computers, peripherals, and cables typically costs two to three times that of equivalent unprotected commercial hardware. There are so many software-based ways of stealing secrets that electronic eavesdropping is less threatening than it once was. Nonetheless, TEMPEST standards are still important for U.S. military and diplomatic computers that have important secrets.

Electromagnetic Shielding

Electromagnetic emanations can be reduced or even suppressed entirely by use of appropriate electromagnetic shielding. Gauss's law says the surface integral of a closed contour surrounding an object is only proportional to the charge enclosed. If that contour is unbroken and electrically conductive, an internal electrical field with no net charge will cancel itself out so there will be no net electrical field outside the contour. This also means that any electrical charge on a closed conductive surface resides entirely on the outside of the surface.

Therefore, to eliminate emanations, we should put computers in metal boxes (Faraday cages) made of conductive materials such as copper, aluminum, or steel. A variety of materials and forms (solid metals, conductive coatings, adhesive foils, conductively filled materials, etc.) suffice (Molyneux-Child, 1997). However, perfect protection assumes the conductive enclosure is unbroken. Because there usually must be gaps for ventilation, power lines, keyboards, and network connections, these gaps may permit signals to leak out (Warne & Chen, 1992). Consequently, significant gaps must be minimized. A key factor is the ratio of the diameter of the gap to the wavelength of the signal frequency one wishes to suppress (Hoffman Enclosures Inc., 2003). As a rule of thumb, it has been suggested this should be 1/10th or less to prevent significant radiation from escaping, and 1/100th to provide 60-db reduction (Molyneux-Child, 1997). Waveguides in the form of conductive pipes through the gaps can further reduce the emanations at these gaps, as can making the gaps into meandering channels. Power lines through these gaps can be filtered, and fiber optic cables through the gaps can supply communications signals without providing an electromagnetic channel. Monitor screens can be coated with a conductive film, but keyboards are tricky to protect. A number of vendors supply such specialized hardware. Such shielding is difficult to do on laptop computers, where weight and space are at a premium.

To simplify construction, the conducting box is often constructed with a grid of wires like a cage. This works well if the gaps between the wires fulfill the wavelength constraints, and it permits better ventilation than a closed surface. Rooms and even buildings can be built using these conductive grids (Hemming, 1992).

Cables provide special problems for shielding because an unshielded and unbalanced electrical cable can be much like an antenna.

Fiber optic cables are the best solution although they are more expensive per unit length than electrical cables. They have no electromagnetic emanations along their bodies because they are coated to prevent the escape of light. Their only weakness is on their ends where light is converted to and from electrical signals. Long fiber optic cables such as long-distance telephone lines also need to be periodically boosted electronically along their length, and the booster is susceptible to eavesdropping.

Optical signals from cathode ray monitors and LEDs can be suppressed by covering room windows and otherwise controlling their light, even the reflected light. Kuhn (2002) also suggests increasing light noise by using significant broad-frequency illumination for the computer room by incandescent or high-frequency fluorescent lights to cover the frequencies of the monitor light. Good design for LEDs should ensure they do not change any faster than humans can follow them.

Source Suppression

Another goal should be to reduce emanations from the computer itself. A good compact design of the machine will help. This means a relatively small chassis and short cables to reduce electrical dipoles that cause emanations. Devices used to measure electromagnetic interference can help locate possible emanation problems (Masuda et al., 2003). Generally speaking, the intensity of a signal decreases as the square of the distance from the source, so one can estimate how close an enemy must be to pick up a signal.

For conventional electrical cables of either the twisted-pair or coaxial type, ferrite beads or disks on the ends can reduce emanations. Ferrites are ferromagnetic materials that dissipate high-frequency magnetic fields as small amounts of heat with magnetic eddy currents. They are useful for frequency over 100 MHz, in the range of computer signals, but require some care to use effectively because they must be matched to appropriate electrical hardware. In-line capacitors can also achieve the effects of ferrite beads but can involve more power dissipation.

Because high frequencies tend to be easier to pick than low frequencies, it is desirable to lower the high-frequency emanations by slowing the switching times between low and high voltages in signals. This is difficult with the CPU but makes sense for the cables, particularly the video and keyboard cables that do not need fast transition times. This can be done by running the signals through a suitably designed low-pass filter, something done routinely to reduce electromagnetic interference. Kuhn and Anderson (1998) also designed special ?Tempest fonts? for monitor screen display that have reduced high-frequency components but are still legible, making them harder for an eavesdropper to pick up.

Another approach to source suppression is to move the source about as in a mobile device. That way any fixed-location eavesdropper cannot obtain all the information. But this is possible only with a few applications.

Noise Generation and Encryption

Another way to make eavesdropping more difficult is to broadcast noise at the same time. Noise can be just many signals at the same time. It is difficult to eavesdrop on a single computer in a busy office with many computers, and similarly, it is difficult to eavesdrop on the signals of a CPU because there are so many in a small space. Noise, however, can create electromagnetic interference if too strong. Realism requires that noise start and stop and eavesdropping could be done while it is off. Also, it is important to create sufficiently complex noise that cannot be easily filtered out. Analog white noise, for instance, noise of a uniform mixture of frequencies, is just added to the frequencies already present and its uniform height can be easily subtracted from the frequency spectrum. So digital noise is needed that looks like real computer operations from a number of simultaneous sources. Even noise sources that are obviously fake can create a difficult combinatorial problem for the attacker in assigning bits to each signal if the sources are located near one another.

The effect of noise can be created by omitting error-correcting bits transmitted in network protocols so attackers have a more difficult time fixing errors in reception. Because their error rate will be higher than that of the system they are monitoring, this creates added problems for them. However, this may give only a mild effect and also hurts the system if its own error rate is nonnegligible. So it is hard to justify against rare threats.

A systematic way to accomplish noise is to encrypt much of the digital activity of the computer. This is a good practice for files and network communications anyway when secrecy is important, so it can be extended to other aspects of the computer when electromagnetic emanations are a concern. Strong encryption methods are now easily available (see PKI and PGP). Unfortunately, the keyboard depressions and the monitor display cannot ultimately be encrypted, so other techniques are necessary for them. It will help to avoid displaying passwords and keys on the screen because the screen contents are easy to pick up. Steganography is not as useful as encryption because activities and files are difficult to conceal completely.

Even when data are encrypted, spies may learn something from when and where it is being used. Spies can do traffic analysis to determine the flow of information between sites; for a hierarchical organization, this may be sufficient to identify the flow of information. To prevent this, it is useful to send dummy (noise) messages periodically between sites; if an equal number of messages are sent between each pair of sites on the average, a spy cannot infer any structure of the sites.

Signal Irregularity

Because eavesdropping is easier with periodic signals, another idea is to insert deliberate random delays in transmission of signals to avoid periodicity. This can be done by changing the operation of the lowest layers of the OSI network transmission protocols

(Forouzan, 2003), the physical and data link layers. Because slow transmissions such as those with keyboards, monitors, and modems are the easiest to eavesdrop, and the EIA-232 (also called RS-232) protocol and associated cable hardware are used for these on most computers, it is desirable to add irregularity to that protocol. Transmissions with EIA-232 can be synchronous (with a clock signal) or asynchronous (without); synchronous transmissions are paradoxically best suited to creating irregularity because the clock signal can be supplied irregularly to indicate when the signal level should be sampled.

Irregularity can also be created at higher levels of network protocols. At the data link layer, gaps in time between bursts of data (frames) can be made random. Although bursts may be deciphered, it will be hard to string them into packets, particularly when similar signals on other electronic equipment are being generated at the same time. Buffering at the receiving end can regularize the data as needed to enable normal computer operations. Asynchronous transfer mode (ATM), important for the Internet, already supports irregular handling of its small packets.

Random delays can also be done in drawing the screen of the monitor. Also, the monitor does not need to draw the lines on the screen in vertical order but could draw them in an order determined by a secret time-varying key. Then an eavesdropper not knowing the key would see only a scrambled mess. But they could try orders at random until they hit on the right one because 480 lines in the standard VGA format is not many. Similarly, keyboard sampling to recognize key depressions could randomly delay between cycles and does not need to check the keys in the same order every time. Keyboard rates now are so slow compared to CPU processing times that a more complex keyboard-sampling method makes no difference to interaction speed. As for periodicity of a magnetic disk, the disk head can be moved when not in use to a blank portion of the disk.

Trojan horses that deliberately create periodic signals to facilitate eavesdropping can be found by the usual methods for finding Trojan horses (see Trojan Horse Programs) such as comparing checksums on executables to previous checksums and looking for statistically anomalous run-time behavior. Their broadcast may be detected by monitoring the emanations of the hardware for unusual frequencies.

Deliberate Deception

Deception is a classic military technique for exploiting modest resources for a major gain. Deception could be done in electronic emanations to plant disinformation with the eavesdropper. For instance, dummy computers could transmit false information made especially easy (in intensity or accessibility) for the eavesdropper to pick up. This is easiest if one can replay old signals that are no longer secret, with date and detail changes. Routine data such as transmission headers are easy to fake.

Deception can help confirm eavesdropping. One can plant some information and see if an eavesdropper reacts; if they do, then

deception can be tailored to them more specifically. Counterintelligence uses methods like these. Honeypots (see Use of Deception Techniques: Honeypots and Decoys) also use deception to collect information about attackers and their attacks. They can pretend to have resources that attackers want such as unencrypted (but ineffective) passwords to waste the time of the attacker. Deception can often be more effective than concealment because the enemy can recognize that you are concealing something and redouble his or her efforts to get it, whereas deception may make him or her go away.

Bug Detectors

If eavesdropping is suspected, one can try to locate the eavesdropping hardware and remove it (Ferrand, 1988; Tolces, 1986). If the countermeasures discussed have already been employed, any useful bug must be nearby. A variety of electronic bug detectors are available, but a purchaser must be cautious because there is much competition among vendors and little regulation. Some vendors promise more than they can deliver, and some are outright scams. Careful testing of products is essential.

There are two approaches to bug detection. One is to focus on the eavesdropping device itself. Because nearly all use electronics, one can exploit properties of electronics. For one thing, they dissipate some heat, so an infrared camera may be able to see bugging devices hidden unexpectedly in everyday objects such as light fixtures and telephones. Another idea is to take advantage of the nonlinearity of many transistors by irradiating the area with a strong microwave signal and looking for distinctive reradiation patterns at different frequencies than the excitation (Yost, 1985). This is usually what is meant by sweeping an area for bugs. It requires a very pure frequency generation because the detectable signals can be small, and good amplification for the sensitive signals after filtering out the excitation signal. Almost any bug will need to contain transistors, but this will not work for MOSFET circuits nor transistors with very small input leads. It will also not find bugs next to legitimate electronic hardware nor those electromagnetically shielded.

Another approach is to focus on bug transmissions. Because most bugs collect too much data to store at the bug (concealment is important, and the bug may need to remain untouched in place a long time to prevent suspicion), retransmission of data by electromagnetic waves to a more convenient location is usual. So frequency-scanning bug detectors, or frequency analyzers, look for unusual frequencies in the electromagnetic spectrum that could represent bug transmissions. It helps that it is easier for a spy to use off-the-shelf hardware for transmitters and receivers to take advantage of frequently used parts of the spectrum. These include the citizen's band at 25?50 MHz, the frequency modulation radio band at 88?120 MHz, the police band at 150?174 MHz, and the gap between UHF and VHF television at around 470 MHz (Yost, 1985); the antenna size required ranges from a few feet for the first to an inch for the last. So a bug detector frequency scanner should focus on those ranges. Techniques for detecting signals in nonrandom noise can help (Garth & Poor, 1994). Additional tricks may be necessary to detect signals of highly motivated adversaries such as military enemies (Stephens, 1996).

Spies can use several additional techniques to conceal bug transmissions: (1) a wide-spectrum broadcast, (2) frequency hopping in the broadcast, (3) double modulation using subcarrier frequencies, and (4) frequencies close to legitimate signals such as radio stations (?snuggling?). But each of these leaves clues in the frequency spectrum. Wide-spectrum and frequency-hopping behavior will give a distinctive ?smear? pattern; double modulation will give two equal peaks; and snuggling will give two distinct but very close peaks. It may help to keep records of the frequencies observed at a location to better notice changes created by new transmissions, analogously to using checksums for detecting changes to a file system. Frequency detection is not foolproof as it does not work when bug is turned off; a bug could be designed for only occasional transmissions.

Bugs can also be detected by nonelectronic inspection by noticing unusual changes to objects, such as repair work or abrasions where none should be expected, new objects or building materials, and so on. Counterintelligence training (Shulsky, 1993) provides many suggestions.

PROTECTING AGAINST OFFENSIVE SIGNALS

Now let us turn to the use of electromagnetic signals as weapons against computer systems for sabotage or harassment.

Damage Mechanisms for Electromagnetic Signals

A disadvantage of the decreasing size of computer and network hardware is that they are becoming increasingly vulnerable to electronic attacks as they become less able to dissipate large amounts of power. So a high voltage suddenly created within modern circuitry can more easily create permanent damage. High voltages induce high current flows that can melt electrical conductors, causing electrical breaks or shorts deep inside chips that are virtually impossible to repair. This heat can also melt the packaging and create toxic fumes or start fires. In addition, even moderate levels of heat can destroy the essential dielectric properties of the semiconductors that are the building blocks of integrated circuits, making them useless.

Several methods can damage circuitry without a direct electrical connection. High-frequency electromagnetic waves can be used that have powerful penetration capabilities. A short burst of such frequencies can be created by a nuclear explosion high in the atmosphere, an electromagnetic pulse (U.S. Government Printing Office, 1998). Such pulses are serious threats to international security because they can destroy digital hardware over a wide area. Smaller pulses can also be created from spark gaps, and they can be effective against specific targets.

Microwave radiation can also be used to attack computer hardware. Because microwave ovens can cook food, higher power microwaves can be focused to overheat particular targets. Such weapons can be either narrow band or broadband. Narrow band can be more effective if one knows the natural frequencies of an electronic device and can stimulate the device at those frequencies, amplifying the damage, but that requires detailed knowledge of the device. The former Soviet Union is alleged to have been the world leader in developing offensive electromagnetic weapons as an inexpensive way to attack the combat systems of the more technologically advanced West.

Countermeasures for Damaging Electromagnetic Signals

The same electromagnetic shielding discussed above as a protection against spying can also protect against electromagnetic attacks, as Gauss's law applies to both incoming and outgoing signals (Kopp, 1997; Podgorski, 1990). But for perfect protection, the device must be perfectly enclosed in a conductive material. If there are any gaps in the surrounding material, they will permit penetration by radiation of frequencies less than the width of the gap unless countermeasures are used. Centimeter-sized gaps are sufficient for microwaves, but not for the X rays and gamma rays that occur with a nuclear explosion. More complex shielding designs can address this. Press (1990) proposes convoluted corridors that twist and turn for the necessary gaps as a way to significantly attenuate radiation traversal.

Shielding can also be at the level of the integrated circuit. ?Radiation-hardened? integrated-circuit chips are available for military and space applications (Hughes & Benedetto, 2003) to protect against high-frequency radiation. They cost 10?1,000 times more than regular hardware because of their difficulty of manufacture but provide a number of techniques for protecting the chip. These include special thinness of the circuit layers (to reduce the effect of charged layers), extra width of critical electrical channels, fabrication at lower temperatures to reduce chemical weaknesses that radiation can exploit and more complex design methods. However, they are generally designed for continuous radiation (as in nuclear and space applications) rather than for the short pulses of radiation typical of an attack.

Traditional methods of electronic protection against voltage spikes (because of lightning, power problems, etc.) can also provide some protection for electronic circuitry if they are significantly upgraded from usual practice. Press (1990) recommends protection for up to 10,000 volts on power lines and 20,000 volts on phone lines (albeit for only a few nanoseconds); special devices such as varistors can accomplish that. A fuse is the oldest and most familiar method, but is no protection for a voltage surge over every conductor. Fuses must also be replaced once they have been blown and must be chosen to have a faster delay than the damage time of the circuit they are protecting. Circuit breakers involve a gap across which a high-voltage spike could jump, so they are not appropriate for powerful electromagnetic attacks. Fiber optic cables are useful along input lines because they cannot be overloaded.

Surge protectors and transient protection devices are another traditional way of protecting electronic equipment against current spikes on its power or signal lines. They use large resistors to dissipate energy as heat and capacitors to even out the current supplied to a device. However, capacitors become less effective the higher the frequency of the signal they are protecting against, and they cannot react effectively against a nuclear electromagnetic pulse. Surge protectors have a rated delay, and useful ones need to have delays on the order of picoseconds.

As with emanations protection, the danger decreases with the square of the distance from the source. Thus if you can keep your enemy outside a given perimeter around your computer systems, you can estimate the closest they could get, the strength of their electromagnetic weapons, the strength of your protections, and the possible damage.

Electromagnetic Noise to Interfere with Computer Systems

Another way to interfere with electronics is to deliberately produce electromagnetic interference to impede operations. Jamming is an example, where supplying a strong signal at the same frequency as a narrow band signal such as radio will prevent listeners from receiving the signal. Jamming works best with analog voltages, where adding to an existing signal changes the meaning of the signal. This could affect the video monitor of a computer or analog input devices. But it is less a problem for digital communications where there are only two voltage levels, because moderate noise does not increase ambiguity unless it changes the voltage enough to go from low to high or vice versa. This inherent noise protection is, in fact, a main justification for the shift from analog to digital electronics that has been occurring since the mid-1950s. Some protection against electronic noise can be obtained by filtering it out using appropriate circuitry. If the noise has distinctive frequencies, appropriate electronic filters can be designed, even automatically, in response to observed signals.

CONCLUSION

Electronic threats to computer systems and networks are often overlooked in the concerns over the myriad of security problems with the new software technologies. Nonetheless, electromagnetic threats remain serious problems for high-security systems, and everyone concerned with information security should be aware of them and the variety of measures available to combat them.

GLOSSARY

Bug Detector Electronic device for detecting electronic or audio eavesdropping devices.

Counterintelligence Methods used to impede the collection by your enemy of intelligence about you.

EIA-232 Commonly used physical-level network protocol and associated hardware specifications for slow communications like those for keyboards, monitors, and modems; originally called RS-232.

Electromagnetic Interference Electromagnetic waves that are sufficiently strong to induce significant voltages and thereby interfere with operations of electronic devices.

Electromagnetic Pulse A burst of high-voltage electromagnetic radiation, created by a special device or a nuclear explosion.

Electromagnetic Shielding Electrically conductive material placed around electronic devices to reduce their electromagnetic emanations and reduce their susceptibility to electromagnetic pulses.

Electronic Filter An electronic device that amplifies some frequencies more than others, useful in reducing electromagnetic emanations.

Emanations (Emissions) Security Issues in the protection of computers and networks from eavesdropping on the electromagnetic signals they inadvertently generate.

Faraday Cage Perfect electromagnetic shielding with no gaps.

Ferrites Ferromagnetic materials which can used for reducing high-frequency magnetic fields.

Ground The comparison voltage for electronic circuitry, usually electrically connected to the earth through an electrical plug and appropriate building wiring.

Intelligence Information about an enemy obtained by surreptitious means.

Signals Intelligence (SIGINT) Gathering of intelligence data by intelligence agencies from electromagnetic signals.

Source Suppression Reduction of electromagnetic emanations from a computer or network by reducing its generated signals.

TEMPEST Secret U.S. Government standards for computer hardware with reduced electromagnetic emanations, used for military and diplomatic systems.

Cross References

REFERENCES

Ferrand, M. K. (1988). Hidden electronics detection. *Proceedings of the Microwave Symposium Digest*, IEEE MTT-S International (vol. 2, pp. 1035?1038).

Forouzan, B. (2003). *Data communications and networking* (3rd ed.). New York: McGraw-Hill.

Friedman, R. S. (1983). Intelligence and the electronic battlefield. In W. V. Kennedy, *Intelligence warfare* (pp. 76?95). New York: Crescent.

Garth, L. M., & Poor, H. V. (1994). Detection of non-Gaussian signals: A paradigm for modern statistical signal processing. *Proceedings of the IEEE, 82*(7), 1061?1095.

Hemming, L H. (1992). *Architectural electromagnetic shielding handbook*. New York: IEEE Press.

Hoffman Enclosures Inc. (2003). *Electromagnetic compatibility (EMC)*. Retrieved June 11, 2004, http://www.hoffmanonline.com/PDFCatalog/SpecifiersGuide/ChAp20_22.pdf

Hughes, H., & Benedetto, J. (2003). Radiation effects and hardening of MOS technology: Devices and circuits. *IEEE Transactions on Nuclear Science, 50*(3), 500?521.

Kopp, C. (1997, February). *Information warfare?Part 2: Hardening your computing assets*. Asia/Pacific Open Systems

Review. Retrieved October 9, 2004, from www.globalsecurity.org/military/library/report/1997/harden.pdf

Kuhn, M.G., & Anderson, R. J. (1998). Soft TEMPEST: Hiding data transmission using electronic emanations. In D. Aucsmith (ed.), *Lecture in computer science, vol. 1525: Information hiding 1998* (pp. 124?142). Berlin: Springer-Verlag.

Kuhn, M. G. (2002). Optical time-domain eavesdropping risks of CRT displays. In Proceedings of the *IEEE Symposium on Security and Privacy* (pp. 3-18).

Kukich, K. (1992). Techniques for automatically correcting words in text. *ACM Computing Surveys, 24*(4), 377?439.

Liu, L.-M., Babad, Y. M., Sun, W., & Chan, K.-K. (1991). Adaptive postprocessing of OCR text via knowledge acquisition. In *Proceedings of the ACM Computer Science Conference* (pp. 558?569).

Loughry, J., & Umpress, D. (2002). Information leakage from optical emanations. *ACM Transactions on Information and Systems Security 5*(3), 262?289.

Masuda, N., Tamaki, N., Kuriyama, T., Bu, J. C., Yamaguchi, M., & Arai, K.-T. (2003). High-frequency magnetic near-field measurement using planar multi-layer loop coil. In Proceedings of the *IEEE Electromagnetic Compatibility Symposium* (vol. 1, pp. 80?85).

McNamara, J. (2004). *The complete, unofficial TEMPEST information page*. Retrieved June 8, 2004, from www.eskimo.com/~joelm/tempest.html

Molyneux-Child, J. W. (1997). *EMC shielding materials: A designer's guide* (2nd ed.). Boston: Oxford.

Moulin, P., & O'Sullivan, J. (2003). Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory, 49*(3), 563?593.

Murray, K. D. (2003). *Electronic eavesdropping and industrial espionage*. Retrieved June 11, 2004, from http://www.spybusters.com/mbsc3.html

Podgorski, A. (1990). Composite electromagnetic pulse threat. In *Proceedings of the IEEE Symposium on Electromagnetic Compatibility* (pp. 224-227).

Press, J. (1990). EMP response of a generic ground-based facility. In *Proceedings of the IEEE Symposium on Electromagnetic Compatibility* (pp. 74-79).

Shulsky, A. N. (1993). *Silent warfare: Understanding the world of intelligence* (2nd ed.). Washington, DC: Brassey's.

Smulders, P. (1990). The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers and Security, 9*(1), 53?58.

Stephens, J. P. (1996). Advances in signal processing technology for electronic warfare. *Proceedings of the IEEE National Aerospace and Electronics Conference* (vol. 1, pp. 129?136).

Thomas, K. (2004). *PROMIS and computer paranoia*. Retrieved June 11, 2004, from www.disinfo.com/archive/pages/article/id905/pg1/

Tolces, R. (1986, September). *Wiretap and bug detection*. California Association of Licensed Investigators Newsletter. Retrieved June 11, 2004, from www.bugsweeps.com/info/wiretap_detection.html

Van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers and Security, 4*(4), 269?286.

Warne, L. K., & Chen, K. C. (1992). A simple transmission line model for narrow slot apertures having depth and losses. *IEEE Transactions on Electromagnetic Compatibility, 34*(3), 173?182.

U.S. Government Printing Office. (1998). *Joint Economic Committee hearing: Radio frequency weapons and proliferation: Potential impact on the economy*. Retrieved June 10, 2004, from www.house.gov/jec/hearings/02-25-8h.htm

Yost, G. (1985). *Spy-tech*. New York: Facts on File.

Zorpette, G. (2002). Making intelligence smarter. *IEEE Spectrum, 39*(1), 38?43.
