Radio Frequency Interference and its Use as a Weapon

Helen Gantt

East Carolina University – DTEC6870 – Advanced Network Security

Abstract

Electromagnetic radio frequency emitters are common and are used legitimately in everyday applications such as wireless communications and Global Positioning Systems. It is also common that the electromagnetic energy that RF emitters produce will affect other electronic devices, called electromagnetic interference (EMI). An example is using a walkie talkie near a television. The signal is picked up by the television's antenna and distorts the picture. If RF emitters are used to purposely disrupt electronics, they then become a weapon. They are more powerful and therefore cause more damage than ordinary RF emitters. In this paper, I will discuss this type of weapon further, how it might be used, and why an attacker would consider this technology as a weapon. This discussion will be limited to the security threats of everyday private sector systems, and will not delve into the realm of its use for the purpose of war.

Radio Frequency Interference and its Use as a Weapon

Introduction

The complexity of technology today accelerates in sophistication at a great pace, much faster than what seems only a few years ago. There are so many conveniences and opportunities that continue to emerge, easily passing you by if you don't wade in that steadily increasing stream of information. At my age, I'd call it a category four. But with all the good, there's always someone there to mess it up. Waiting, crouching, hiding, calculating. It all starts with means and motivation. All that's left is finding the opportunity.

Radio Frequency Interference

Radio frequency is a type of electric current on a wireless network, which emits an electromagnetic field when alternating current is applied to an antenna. Similar to waves that result from a rock thrown into water, radio waves are altered when obstructions appear, and may reflect or scatter for example, depending on their interactions with each other. (Shimonski, 2002) Wave fronts are generated when the waves become reflected. So from a receiver's perspective, the wave fronts may be in or out of phase with the main signal as they reach the receiver at different times. If the peak of one wave is added to the peak of another, they are in phase and the wave will be amplified. If the peak of one wave comes in contact with the valley of another, they are out of phase, and the wave is eliminated.

Radio Frequency Interference occurs "when a signal radiated by a transmitter is picked up by an electronic device in such a manner that it prevents the clear reception of another and desired signal or causes malfunction of some other electronic device (not simply a radio or television receiver)." (Brock, Fall 1998) RFI can be induced intentionally, or unintentionally.

Unintentional RFI

RFI affects many electronic devices, not just computers, telephones, TVs and radios, and also includes audio systems, kitchen appliances such as the microwave, automatic garage-door openers, fluorescent lights, and security systems. Common forms of RFI consist of unwanted signals not being filtered or rejected by home electronic equipment, such as no reception on certain TV channels, an obtrusive station replacing the expected program on a channel, reduced quality or hearing other conversations on the telephone, or a baby monitor.

In heavily populated areas, escalating cell phone use is causing RFI problems for police officers and firefighters. They use the same 800MHz broadcast spectrum as cell phones and it is hindering their ability to communicate. In one instance, while responding for a fight in a Boston suburb, an officer had to walk to the other side of a high rise apartment to be able to call for backup. In another, responding to a burglar alarm, an officer couldn't call for help as he approached the building. (Salant, 2004) Throughout cities as well as rural areas, cell phone companies disperse large antennas to provide the signals necessary. There are a limited number of frequencies, which poses a problem in densely populated areas to meet the needs of those individuals to make phone calls. If the network is congested, the network will be too busy to handle additional calls. Service providers counter this by dividing cities into cells, each with a diameter of a few miles. To prevent RFI, different frequency ranges are used for adjacent cells. (Chandler, 2005) However, this problem was serious enough among first responders that they urged the FCC to split the 800 Mhz band, with one segment going to the public safety exclusively. The FCC began the first wave of the 800 MHz band reconfiguration 5/27/2005, and the effort is ongoing. (800 MHz Band Reconfiguration, 2004)

RFW is Intentional RFI

Simply put, a radio frequency weapon (RFW) is a device that produces and transmits electromagnetic energy with the intent of destroying or damaging the electronics that are targeted. RFWs are categorized by the type of beam they create, which is wideband or narrowband. Wideband devices work in the low frequency ranges (10MHz to 1 GHz), create short pulses and are called Ultra-Wideband (UWB) weapons. Narrowband devices operate at a single frequency (1 – 35 GHz), create longer pulses, and are called High Power Microwave (HPM) weapons. (Brunderman, 1999) However, HPM has been known to describe microwave weapon technology as a whole. These weapons can create currents sufficiently high enough to melt circuitry, or low enough to cause temporary disruption. They are considered non-lethal, and can be used without people even knowing they've been hit.

Considered a narrow-band weapon, an Electromagnetic Pulse (EMP) creates an electromagnetic shockwave and can emit currents between 10 to 1000 times greater than lighting. (Overholt & Brenner, unknown) Although EMP was first conceptualized over a hundred years ago, its effects and hazards were first realized during nuclear testing in the mid-20th century and WWII. Additionally in 1962, as part of a US military test, a nuclear bomb was detonated 250 miles above the earth. The resulting EMP damaged electrical equipment 800 miles away in Hawaii, and damaged satellites. (Webb, 2004). The E-bomb is the non-nuclear version of this weapon, and is a Flux Compression Generator (FCG). They are made of a copper cylinder packed with explosives, and surrounded by a coil that carries current. Upon detonation, the explosion short-circuits the coil, and compresses the magnetic field forward as the number of turns in the coil is reduced. (Abrams, unknown) The E-bomb is relatively inexpensive to make, and parts can be found at most hardware stores. Depending on the desired output, the power supplied for detonation can be as small as a few D-cell batteries, a car battery, or electrical outlet.

(Webb, 2004) It is not very efficient however, because you have to blow it up, and the strength of the shock dissipates quickly, requiring the explosion to occur fairly close to the target, making it possibly lethal and most certainly detectable.

Another narrow-band weapon is the High Energy Radio Frequency (HERF) gun, and directs a radio signal at the intended target in order to disrupt it. While an E-bomb covers a wide radius, the HERF gun can be aimed, by tuning in to the frequency of their target. The potential for damage relies upon the power used, obstructions in the line of sight, and the target itself. Parts to build a HERF gun are as easily obtainable as the E-bomb. The cost of a signal generator depends on the frequencies available, from AM to 6.4 GHz and up, and range from ~$200 to over $50,000. The cost of the power source goes up as the wattage goes up, and can weigh as little as five pounds. If a highly directional antenna is not desired, a satellite dish can be converted as an alternative. (Webb, 2004)

Considered an Ultra-wideband weapon, the Transient Electromagnetic Device (TED) has been referred to as the "weapon of choice to the modern cyber or infrastructure RF warrior". (Schriner, 2006) The TED produces a spike of energy, much like electrostatic discharge (ESD) that occurs when you touch something after rubbing your feet on the carpet. While narrowband devices are limited to a single frequency, TEDs do not have a definable frequency, and occupy a very large spectrum. Narrowband devices only affect the systems that operate at their tuned frequency, but TEDs can disrupt systems without previous knowledge of the frequencies they are vulnerable to. TEDs are attractive because they don't require as much skill to build, the power supplies require less power and therefore are smaller in size, and the parts and information to build them is readily available.

Advantages

The most significant advantage of RFWs is they travel at the speed of light. This greatly

reduces the chance that a target can evade interception, or that an obstruction will have time to get in the way. Also, since the beams lack any mass, they are immune to gravity, and are free from aerodynamic constraints. They are relatively cheap, and can be created on a variety of power levels. (Spencer & James Jay Carafano, 2004) When RFWs are properly adjusted, they are non-lethal to humans. Attacks are difficult to detect when explosive devices are not used, and are therefore useful for covert operations. (Schriner, 2006)

Disadvantages

A disadvantage to RFWs is that damage assessments will be difficult since not all devices will behave the same way when subjected to the same amount of energy. Also, there will be no signs of whether the objective was accomplished or if they're "playing possum". (Dr. Robert Cooper, Estes, III, Dr. Delores Etter, General Ronald Fogelman & Kaminski, 2003) To have a higher likelihood of the intended effect, the RFWs will need to be built a size larger. Conversely, because they can also be smaller in size, weapons can be hidden in a briefcase or vehicle and disrupt computer networks and electronic equipment. Virtually any electronic equipment that is unprotected is at risk. (Beehner, unknown)

How we're Vulnerable

As the features of semiconductors continually shrink, cutting edge semiconductor components are becoming increasingly vulnerable to RF energy. Metal oxide semiconductors are in heavy use in the microelectronics industry, which are tested for failures to the point when their dielectric strengths are exceeded by voltage, or an RF pulse melts the device from heating by current. Designers of these circuits primarily focus on FCC limitations, and it is not known how susceptible commercial systems could be to an electronic attack. (Merritt, 1998) In addition, other than backups, almost no major corporations have a defense against an RF attack.

Commercial systems include the banking industry, telecommunications, oil, gas distribution, and transportation systems. It is unknown what the effects would be from an attack, even though these systems are designed for worst case scenarios. And although military aircraft have hardened electronics to withstand a nuclear EMP, commercial aircraft remain unprotected. (Webb, 2004) Additionally, the US is one of the most advanced electronically, and the largest user of electricity. There's also the trickle down effect, because 90% of military communications occur over public networks. If an RF weapon were to take down the main communications, all communications would suffer. (Merritt, 1998)

RFI Countermeasures

To counter RFI effects on electronic devices and communications systems, there are several countermeasures that can be put in place. If it is possible to find the source, eliminate it. Although it may not be feasible in most cases, it is the most effective. A common ground for devices will provide some protection from noise and interference. Adequate grounding is required for certain electronic equipment to operate properly. Additionally, the conductor for grounding the equipment should be as short as is necessary to ward off a ground loop condition. Using a filter will allow the desired frequencies through to the dev ice, and will reject all other frequencies that are not a part of the filter specifications. To minimize and possibly eliminate EMI is to shield them to avoid any contact with electromagnetic energy. It is often expensive and challenging to shield a device fully, because the equipment will have to be enclosed completely with a conductive material. (Burrell, 2003)

Conclusion

It has been said by officials that since the Cold War, the nation's military infrastructure has been carefully protected by the US government. But precautions in the private sector have

largely been ignored, and businesses could be vulnerable to attack. Technology's accelerating complexity and rate of change adds to the arena of concern. They are designed by the commercial industry that is primarily concerned with meeting FCC standards. We revel in technology's advances, but we take it for granted. If something happened and it was taken away by an adversary, would be prepared to go on without it? Would we be able to fight back? Would we be able to recover quickly? That remains to be seen.

References

*Brunderman, J. A. (1999, December). *High Power Radio Frequency Weapons: A Potential Counter to U.S. Stealth and Cruise Missile Technology*. Retrieved May 26, 2006, from Air University Research Web site: http://https://research.au.af.mil/papers/ay2000/awc/brundeman.pdf

Abrams, M. (unknown). *The dawn of the E-Bomb*. Retrieved May, 2006, from IEEE Spectrum Web site: http://www.spectrum.ieee.org/archive/1543

*Dr. Robert Cooper, Estes, G. H. M., III, Dr. Delores Etter, General Ronald Fogelman, & Kaminski, D. P. G. (2003, February). *Directed-Energy Weapons: Technologies, Applications, and Implications*. Retrieved May, 2006, from Lexington Institute Web site: http://www.lexingtoninstitute.org/docs/321.pdf

Beehner, R. (unknown). *Simple RF Weapon Can Fry PC Circuits*. Retrieved May, 2006, from PC World Web site: http://pcworld.about.com/news/May022001id49048.htm

*Burrell, J. (2003, April). *Disruptive Effects of Electromagnetic Interference on Communication and Electronic Systems*. Retrieved July, 2006, from National Aviation Reporting Center on Anomalous Phenomena Web site: http://www.narcap.org/Jim-Burrell-April-2003.pdf

Merritt, D. I. W. (1998, February 25). *Proliferation and Significance of Radio Frequency Weapons Technology*. Retrieved May, 2006, from Joint Economic Committee Web site: http://www.house.gov/jec/hearings/radio/merritt.htm

Overholt, M., & Brenner, S. (unknown). *Overview of Cyber-Terrorism*. Retrieved May, 2006, from Susan Brenner Web site: http://cybercrimes.net/Terrorism/overview/page3.html

800 MHz Band Reconfiguration. (2004, November 22). Retrieved July 14, 2006, from Federal Communications Commission Web site: http://wireless.fcc.gov/publicsafety/800MHz/bandreconfiguration/index2.html

Chandler, N. (2005, July). *Wireless 101: How Digital Devices Drop Their Wires*. Retrieved July 13, 2006, from Sandhills Publishing Company Web site: http://www.pctoday.com/editorial/article.asp?article=articles/2005/t0307/16t07/16t07.asp&GUID=

Salant, J. D. (2004, April 7). *Call Waiting: Cell Phone Interference Disrupts Some Police, Fire Radios*. Retrieved July 14, 2006, from FireRescue1.com Web site: http://firerescue1.com/products/communications/interoperability/articles/5151/

*Schriner, D. (2006, February 25). *The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods*. Retrieved May, 2006, from Joint Economic Committee Web site: http://www.house.gov/jec/hearings/radio/schriner.htm

Shimonski, R. J. (2002, December 16). *Wireless Security Primer 101*. Retrieved July 10, 2006, from WindowSecurity.com Web site: http://www.windowsecurity.com/pages/article_p.asp?id=1108

*Brock, R. H. (Fall 1998). *The Ghost in the Computer: Radio Frequency Interference and the Doctrine of Federal Preemption*. Retrieved July 13, 2006, from Computer Law Review and Technology Journal Web site: http://www.sbot.org/docs/RFI.pdf

*Webb, C. (2004). *Radio Frequency Weapons*. Retrieved July, 2006, from Cybersecurity '04 Web site: http://www.ncc-cybersecurity.net/workingCopy%20BLUE/WCSU1.html

*Spencer, J., & James Jay Carafano. (2004, August 2). *The use of Directed-Energy Weapons to Protect Critical Infrastructure*. Retrieved May, 2006, from The Heritage Foundation Web site: http://www.heritage.org/Research/NationalSecurity/bg1783.cfm