Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Electromagnetic Attack: Is Your Infrastructure and Data at Risk?

You have worked hard to secure your network and data. You've got intrusion detection systems (IDS), backups, corporate firewalls, personal firewalls, honey pots, bullet-proof armoring and centralized logging. You've eliminated or minimized single point failures, installed redundant systems and are a believer of defense in depth. Your security policies and procedures are in order, and you have corporate or institutional buy-in as a reward. You are aware that the most important aspect of data and network securi...

Copyright SANS Institute

Author Retains Full Rights

AD

August 10, 2001

Electromagnetic Attack: Is Your Infrastructure and Data at Risk?
Michael B. Hayden

Introduction

The general population's fascination with esoteric, state-of-the-art weapons is quite real. The movies are full of ray guns, phasors, disintegration rays real and imagined. Recently email, eHeadlines and even spam promise a variety of new futuristic ways to attack the infrastructure, network and your data security. Do It Yourself (DIY) books are available and describe the construction of ion weapons, lasers and particle beam weapons that promise destruction at a distance.

You have worked hard to secure your network and data. You've got intrusion detection systems (IDS), backups, corporate firewalls, personal firewalls, honey pots, bullet-proof armoring and centralized logging. You've eliminated or minimized single point failures, installed redundant systems and are a believer of defense in depth. Your security policies and procedures are in order, and you have corporate or institutional buy-in as a reward. You are aware that the most important aspect of data and network security is physical security, so you keep things properly buttoned up behind locked doors and you control physical access.

But now you hear the bad guys have RFWs, HPMs, TEDs, UWBs, EMPs , EMI, HEMPs and more. Is this stuff for real? And if it is, can you protect yourself and your systems from damage or total destruction from a perpetrator outside your perimeter defenses? It's time to think about these things before you fall victim to your own technology.

Definitions – Get Familiar

We are no strangers to acronyms, but some of these devices, jargon and technologies may be new to many of us. Let's take a moment to explore their meaning before we proceed.

RFWs – Radio Frequency Weapons, some varieties of which are called Radio Frequency Munitions or RFMs. These are devices that generate intense pulses of electromagnetic energy in the radio portion of the spectrum[1]. Narrowly directed energy so generated can be directed over a large distance to a point target, or more widely transmitted to attack a broad target.

Radio Frequency (RF) weapons can be categorized into two main groups, High Power Microwave (HPM devices or Ultra Wide Band (UWB) systems. Their purpose is to introduce abnormally high levels of RF (Radio Frequency) energy into the target's electronics, thereby destroying or degrading it. HPMs and UWBs look like radio transmitters. They must include a power source, amplifier and antenna system.

[1] http://www.ntia.doc.gov/osmhome/allochrt.pdf

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

TEDs – Transient Electromagnetic Devices. A TED is another form of directed energy weapon, different from a HPM in that instead of generating a continuous train of energy as a HPM does, it creates a spike-like form of energy for a fleeting amount of time. By analogy, the electrostatic discharge (ESD) you cause from shuffling across a carpet on a dry day and then touching delicate electronics is similar. Both the TED and the ESD generate a very brief, very high voltage discharge that can momentarily break, and perhaps irreparably damage the functionality of sensitive electronic circuits, memory, CPUs and various semiconductors.

EMPs – Electromagnetic Pulse. EMP as a destructive force was first notice during the early testing of high altitude airburst nuclear weapons. Although the detonation of the weapons occurred high in the atmosphere where the ground affects of the physical blast were minimal, these airbursts were found to generate an intense electromagnetic pulse in the vicinity of the detonation. The generated electric field on the ground, though transient, can be intense and amount to thousands of volts. This is plenty sufficient to be of military significance in that exposed electrical conductors and unprotected electronic components can be irreversibly damaged or ruined. A variety of non-nuclear methodologies have been substituted to create EMPs. For instance it is possible to use a conventional explosion to rapidly compress a magnetic field in a carefully designed device. The intense magnetic field generated by such a device can create peak currents upward to a million amps, with energies measures in the mega joule range. Such devices are not yet particularly small, self contained or convenient to transport and position.

EMI – Electromagnetic Interference. Most electronic devices are susceptible to degradation or malfunction if too much unwanted electromagnetic energy is coupled into them. Our Government recognizes this vulnerbility, and has established guidelines[2] limiting the magnitude of interference emitted by consumer electronic devices so they don't interfere with other electronics and communications services. These guidelines are frequency specific. Once emission limits by frequency are established, manufactures of new equipment can and often do "harden" their equipment to function properly when exposed to at least these levels of EMI . It can be costly to so, however, and manufacturers of all but the most critical of electronic hardware to not tend to over protect their designs. The Government's position in this is that if they set absolute quantitative levels of unwanted emissions from different forms of user electronics, and the manufacturers of devices provide a reasonable immunity to these interference levels, the rest of the solution comes from separation distance.

Since electromagnetic energy falls off as the square of the distance between the interfering and interfered with devices, sufficient physical separation can help mitigate the affects of EMI. This is why your radio might pick up noise from your computer when placed side-by-side, but that same radio works fine from across the room.

[2] US Code of Federal Regulations, CFR 47 Telecommunications, Part 15 "Radio Frequency Devices"

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Educated Garage Mechanic
Can these esoteric radio wave devices be constructed? Given sufficient time money and size, the current state of technology suggests they not only can be, they have been.

The literature is full of accounts both in the form of expert testimony[3] [4], and anecdotal reports[5] [6] that suggest proof of concept devices have been constructed and tested. The more important issue is the probability that an antagonist who is constrained by size, money or materials could construct such a device. The possibility cannot be ruled out.

In declarations before the Joint Economic Committee of the US Congress in 1998, experts in the field are of the opinion that a damaging device can be constructed with parts available for purchase at a hardware store using tools common in an average machine shop. Quoting Mr. Schriner's testimony from that presentation

"The net result of all this design, experimentation, fabrication and measurement proves that such a weapon system could be made by anyone with an engineering degree or even a bright technician with good hardware experience. … The materials needed are nothing special, and if the effort is made, advanced concepts can be made using everyday hardware such as automotive ignition systems."

The commonness of the devices that could be improvised in the creation of such a device are such that, should there be a need, tracing them would be all the more difficult. This is another attractive characteristic of currently available technology.

Is this a Potent Security Threat?
If we presume that such a device can be built at reasonable cost by a properly educated and motivated individual, what might its efficacy be against your network infrastructure, computer hardware and data?

Quite literally, the mileage may vary. The idea that such a weapon or device would be capable of destroying vulnerable hardware depends entirely on how much energy can be coupled into your equipment/electronics. Estimates of the currents and energies generated from specially designed test hardware ranges from 100s upwards to 1000s of amperes . Lightening by comparison can represent 20,000 to over 100,000 amperes[7]. These carefully constructed prototypes might induce voltages of one or two thousand volts into a target.

---

[3] Dr. Ira W. Merritt before the Joint Economic Committee, United States Congress, Wednesday, February 25, 1998 "Proliferation and Significance of Radio Frequency Weapons Technology".
[4] Statements of Gen. Robert T. Marsh, Chairman of the President's Commission on Critical Infrastructure Protection before the House of Representatives, Committee on National Security, Military Research and Development Subcommittee, Wednesday, July 16, 1997.
[5] New Face of Terrorism: Radio Frequency Weapons by Eric Rosenberg, c. 1977 Hearst Newspapers
[6] Mr. David Schriner before the Joint Economic Committee, United States Congress, Wednesday, February 25, 1998 "The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods"
[7] http://home.earthlink.net/~jimlux/lfacts.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Swedish scientists are claimed to have successfully built an RF based device that in experiments was able to stop a running car at 100 yards[8]. There are reports of those same scientists claiming RF weapons have been directed against their financial institutions. There are unsubstantiated claims that similar weaponry has been used against unnamed British banking and financial institutions, supposedly reported by the London Times.

Here on the east coast of the US, I recall seeing a "news" clip on the television in early 2001 of what appeared to be a mobile device used by the Los Angeles Police Department to stop vehicles trying to evade the law. A device carried aboard and fired by the squad car was said to emit unspecified energy that disrupted a target car's computer control causing it to stall out. I presume your restored '57 Chevy would have continued to run normally due to its lack of fancy electronics.

Still, with the current state of the art and the fact that effectiveness is sensitive to separation distance and the degree of electromagnetic coupling, it seems that today's devices are very much limited in their range and effectiveness.

Effectiveness can be enhanced by building bigger devices, along with super-sizing their power supplies, but my research suggests that any sufficiently powerful device would occupy considerable volume – perhaps truck sized. Such a device would have a range measured in feet and likely be a one shot device if it was intended to destroy electronic devices rather than just temporarily interfere with them.

I can find no concrete evidence that a sufficiently powerful device can be built today (Summer 2001), much less than built into a suitcase and carried into a building to wreak havoc on network devices.

EMI and EMP pulses generated as a result of nuclear weapon airburst are hundreds of times larger and would cause significant destruction of unhardened electronics resulting from EMP. Fortunately for the vast majority of civilian system administrators, a cooked server is of little practical concern if a nuclear bomb has just been detonated over their heads.

No one really knows how susceptible commercial electronic systems might be to a concerted EMI based attack tomorrow as technology advances and more experimentation takes place by a breed of radio savvy black hats.

Vulnerability Estimate

So what are the chances you are vulnerable to such a designer weapon? We can attempt an order of magnitude calculation using reasoned guesses. So let's define the following parameters and then assign them estimated values. These are my estimates, modify them to your liking:

[8] "RF Weapons and the Infrastructure", by Robert Schweitzer, submitted to the House Joint Economic Committee on June 17, 1997.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Probability that you'll be the target (A)
Probability that Bad Guys can get in range of the target (B)
Probability that sufficient unwanted energy can be coupled into your system (C)
Probability that the attack will destroy the target (D)
Probability of a RF weapon of some type is used (E)
Number of attacks a year

What is the likelihood that you will be a target and not the guy/gal next door? We need to make some reasonable assumptions. Are you a Fortune 500 company? Military or Government institution? There are about 1200 government agencies[9]. There are over 5.5 million businesses in the USA (1998)[10]. Let's say there are 5000 worthwhile, high visibility targets that are worth the risk. Your chances are 5000/5,500,000 or about 0.000909 (0.0909%). So let A = 0.0009

Can an attacker get a big enough device near enough to you to do damage? In the places I have worked, my hardware has been as close as 20 feet from a driveway (but inside a building), and as far as a ten minute walk up many flights of stairs or horizontally. On average, I would say that any target of mine is perhaps 200 feet away from a place where a truck could be parked. If an effective range of a truck-sized device is 50ft (a reasonable guess), and it's effectiveness is diminished as the square of the distance separating us because of spreading losses, the probability my equipment might be damaged 200 ft away (four times the sure-kill distance) is about (1/4^2) or 1/16 = 0.0625 (a bit over 6%). So let B = 0.06

What are the chances enough energy can be transferred into your equipment? This is a function of the device and what is connected to it. We use a lot of cable, and cables act as antennas to RF energy. 10 Base T wire, power lines, phone cables and the like make us pretty vulnerable. Are you shielded? You may be in pretty good shape if you are the military or the Government. But most of the rest of us are using COTS (Commercial Off the Shelf) hardware and don't give it another thought, relying on manufacturing standards - where they exist - as our only means of protection. The probability may be about 0.8 that you are under protected, so C = 0.8 (80%).

If energy can be coupled into your electronics, will it destroy them? You could experience a range of damage. There could be no discernible affect, impairment or outright destruction. Induced currents generate heat. High currents could dissipate significant thermal energy inside the hardware. MOS devices (typically transistors, IC and chips) may be damaged by high electric fields. Yet, practical experience tells us that the likelihood of damage may be small. Your electronics are not always destroyed by a proximity lightening strike, and they are significant events compared to the estimated power from an RF attack. Let's guess that a kill likelihood is only 0.05 (5%) so D=0.1 or one in 20.

[9] http://www.lib.lsu.edu/gov/fedgov.html
[10] http://www.census.gov/csd/susb/usst98.xls

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The probability that your attacker will be using a state of the art RF weapon is low. Other attack schemes are more likely: viruses, Trojans, worms, break-in, social engineering and such. Will 1 in 1000 be willing to give it a try? Maybe 1 in 10,000? The latter is probably closer, so E = 1/10000 or 0.0001 (0.01%).

Finally, how many attacks are you likely to suffer a year? From all attack sources, maybe a few a day? We are electronically pounded relentlessly where I work. Let's say 500 times a year? So let F = 500.

Probability Estimate

Mathematically, the combined probability of things that are independent of one another is the multiplication of the individual probabilities, or Pr[A and B] = Pr[A] x Pr[B]. Extend this to our situation and multiply by the number of expected attacks, or

P = F (A x B x C x D x E)

Where P is the probability you will get hit by a destructive RF device in the next year.

P = 500 (0.0009 x 0.06 x 0.8 x 0.05 x 0.01)
P = 1.081E-5
P= 0.0000108, or roughly once per 100,000 incidents.

What can you do?

Countermeasure do exist and some are deceptively simple. Distance is a good countermeasure to this type of attack mechanism, so placing critical equipment a good distance from possible attackers is wise. Since power flux density deceases proportional to the distance squared, a modest increase in distance provides a substantial increase in protection.

Proper grounding of equipment is essential. Whenever possible, a solid earth ground should be used, arranged in a star configuration. Rather than individually grounding all chassis, it is better to run each to a single ground system. Always be mindful of local building code requirements before you install a new ground system or modify one that already exists. You may unwittingly make your system more prone to damage if your grounding solution is not properly engineered and implemented.

Adequate shielding is important for sensitive installations. Induced EMF is coupled into electronic equipment by direct conduction through attached wires and cables. The use of shielded cables where possible will minimize pickup of unwanted energy. So will careful use of line filters and surge suppressors on AC power lines. The effect you want to block is similar to the surge and impulses you see with a close in lightening strike, so similar methods are useful here. Data, power, telephone and fixed electrical wiring are among the conductors that can pick up potentially damaging impulses. Physically disconnecting

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

cables from sensitive equipment when not in use can be considered in special cases, or when there is time to react to an imminent threat.

Radio frequencies and EMF can enter equipment through ventilation holes, electrical interfaces and the gaps between metal panels. These apertures can admit energy and direct energy into your equipment as an aperture or slot antenna depending on their physical size, geometry and the wavelength (related to the frequency) of the electromagnetic interference.

Fiber optics are immune to most of the EMF pulse interference likely to be generated by RF attacks and can be used to replace copper cable in many installations. Fiber optics are not a viable option for power supply lines, so they would remain vulnerable without other appropriate protection. If copper is replaced en mass with optical fiber the infrastructure would be significantly more robust against electromagnetic attack, particularly for a distributed computing topology.

For very delicate or sensitive electronics, Faraday shielding may be appropriate and it can be highly effective. Faraday shielding involves placing the equipment to be protected in a fully enclosed metallic screen room or electrically conductive enclosure. All openings and doors to such a Faraday cage must be properly gasketed with conducting seals and care must be exercised to insure cables entering the room are properly shielded and grounded as mentioned above. A properly engineered and constructed Faraday shield, RF cage or conductive screen room will safeguard electronics within because externally generated electromagnetic fields that could cause damage cannot penetrate it. The mechanism involved is the same as the one that keeps occupants relatively safe in an automobile or aircraft struck by lightening[11]

With centralized computing you are more likely to be able to properly protect your systems, in that you need harden only your computer operations center against attack. But as Mark Twain reported once said, "If you put all your eggs in one basket, you'd better watch that basket."

On the other hand, decentralization of your computer network presents a major vulnerability to electromagnetic attack. But, it reduces the effectiveness of an actual physical attack that could cripple your network.

Summary and Conclusions

Attack of the infrastructure by way of radio frequency devices is technically possible and has been demonstrated on a small scale. The equipment needed to build and experiment with such devices is modest, and the materials and technology are easily obtainable. The expertise level necessary to experiment and perhaps build a device with a reasonably effective range is not great, and is certainly within the capabilities of an enthusiast trained in engineering or electronics.

[11] Gabrielson, B.C., The Aerospace Engineers Handbook of Lightening Protection, Don White Publishing, Gainesville VA, 1986.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Current state of the art, however, suggests that any such device or weapon would necessarily be large, given materials available off the shelf and the power requirements of such a unit. At this point in time, it appears unlikely such a device could be easily concealed or positioned in a way that would guarantee its effectiveness against electronic devices without being detected.

Because of the many shapes and forms an attack against your infrastructure can take, the probability is very low that an effective attack would be waged using an RF device.

Nevertheless, diligence is appropriate and complacency is your enemy. Precautions can and should be part of your overall defense in depth strategy. Cost effective countermeasures exist in the form of shielding and properly engineered systems. Effective shielding and grounding reduces your exposure to RF attacks, as well as lightning. The damage mechanism is similar.

You may rest easy for the moment knowing that the likelihood of damage due to EMF attack is very low. A bi-annual review and threat reassessment of the state of RF attack technology is recommended.

References:

1. http://www.ntia.doc.gov/osmhome/allochrt.pdf
2. US Code of Federal Regulations, CFR 47 Telecommunications, Part 15 "Radio Frequency Devices"
3. Dr. Ira W. Merritt before the Joint Economic Committee, United States Congress, Wednesday, February 25, 1998 "Proliferation and Significance of Radio Frequency Weapons Technology".
4. Statements of Gen. Robert T. Marsh, Chairman of the President's Commission on Critical Infrastructure Protection before the House of Representatives, Committee on National Security, Military Research and Development Subcommittee, Wednesday, July 16, 1997.
5. New Face of Terrorism: Radio Frequency Weapons by Eric Rosenberg, c. 1977 Hearst Newspapers
6. Mr. David Schriner before the Joint Economic Committee, United States Congress, Wednesday, February 25, 1998 "The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods"
7. http://home.earthlink.net/~jimlux/lfacts.htm
8. "RF Weapons and the Infrastructure", by Robert Schweitzer, submitted to the House Joint Economic Committee on June 17, 1997.
9. http://www.lib.lsu.edu/gov/fedgov.html
10. http://www.census.gov/csd/susb/usst98.xls
11. Gabrielson, B.C., The Aerospace Engineers Handbook of Lightening Protection, Don White Publishing, Gainesville VA, 1986.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced