DEFCON 18

Electronic Weapons

Tim Otto, aka mage2

10th year of DEFCON, and I am finally giving some back in the form of a talk. I noticed a few things over the years of coming here. One thing is that most talks are from the point of the software engineer, the coder, the exploit artist, etc. I also noticed that recently there has been a push for us geeks to dig more into the hardware side of things. This is bad ass. I want to support that, so here I am. I am going to cover a wide range of devices. I am going to focus on things like EMP and RFI. What is it? How does it work? These are some of the questions I will answer.

Disklamer: Mucking about with the things covered in this could have a few consequences that you might not want. I am not responsible for any of the consequences that you might encounter while mucking about in this or any other realms. So as the saying goes "kids don't try this at home".

This talk will cover devices that target electronic devices, then if there is time we will quickly go over some of the new high-tech weapons that target humans. These are not exactly electronic weapons but are more high-tech weapons.

* EMP, electro-magnetic pulse - damage by generating voltage spike via RF energy.
* Electromagnetic interference - covering the signal with noise.
* projectile based, eg. railgun, coil/gauss gun, etc. I wont be covering these in much depth.
* lasers or to quote a talk last year "freaking laser beams"
* ones designed for human targets eg. heat-rays, sonic attacks, light attacks.

EMP/RFI Basic Concepts

* All conductive material can act as an antenna, this includes wires, ground planes, chassis, etc
* Modern electronics are sensitive to voltage spikes.
* Most communication based electronics run on relatively low power signals. < 1W
* Atomic and Nuclear weapons are not the only sources of EMP.
* Voltage is based on the potential difference between the source and the ground.
* Ohms law , learn it love it. V over IR squared.
* We all know computers and all digital electronics run on binary signals.
* In most systems this is represented as a square wave between 0v and either 3.3v or 5v
* These systems there is a threshold of what the hardware expects to see as a high or a low.
* Most electronics run on either 5v (TTL) or 3.3v (CMOS)
* When using transformers , you will trade current for voltage.
* RF power diminishes over distance, closer = better.

* Most of these run on the principle of large amounts of energy discharged in a short time.

How do we do that you ask..

Many of the devices that fall under this topic are energy hogs, they require huge amounts of energy and require it to be delivered quickly. Currently in the realm of energy storage there are really only two options that will work, coils and capacitors. Quick rundown on what they are.

Capacitors are devices that come in more than a few form factors. They all work on the same principal, the are 2 conductive plates separated by a non-conductive material. When power is applied it it stores some of that energy in an electric field. As for caps, they are the bread and butter of the quick discharge of energy world, but they come in ranges and types. For most high power discharge you are going to be mucking about with electrolytic caps, these are somewhat special in the fact that they are polarized. You plug them in backwards to get a good pop, depending on the cap of course. There are others but for high voltage + lots of storage you cant go wrong with a coke can sized electrolytic.

Coils are actually a little more simple, it stores the energy in a magnetic field. As most high school dropouts know, if you apply current to a wire coil you get a electromagnet, what they don't know is that when that current is stopped and the magnetic field collapses it generates current. Thus coils store the energy in magnetic fields.

The coils and caps will fuel your mad scientist plans for world domination.

Lets start with Denial Of Service, AKA RFI

Electromagnetic interference, swamping out the signal with noise.

I will try to show a simple RFI demo

RFI is Radio Frequency interference. By generating a signal on the same frequency as your target you can cover the target signal with noise, or with your signal. One way of accomplishing this would be a spark gap transmitter. Sparks can create large amounts of RF over a large frequency range and have a large amount of power output. Another option is to build a transmitters that is tuned to emit energy on or in a specific frequency/frequency range. Both of these possibilities would work on the same idea but the tuned transmitter is more precise . This could be as simple as a FM transmitter overpowering a radio station, to your cordless phone causing your Wifi troubles. Transmitter design is almost magical, but lucky for you there are plenty of resources around that will help you get started such as google, ARRL handbook, TI data sheets, etc.

EMP or Electro-Magnetic-Pulse

EMP works by utilizing the wires/traces as an antenna and injecting a voltage spike into a circuit, where RF interference usually targets some type of receiver. An EMP can affect any electronic devices. The fast rise time of the pulse in a electronic device can cause the damage.

As much as I would like to, I am not going to demo a EMP here today.

@ Low Powers -
At low powers this will be noise on the wire. Low power would cause computers to crash/reboot, calculators to freak out, devices to act strangely. This would all be because the circuit is getting anomalous signals. When the device expects a 0 or a 1, (0V or 5V), and it gets a 3V signal or a 10V signal it doesn't know what to do. There is a threshold when working with digital devices.

@ High Powers -
At higher powers instead of injecting noise into the signals, the RF would cause a high power pulse, instead of the circuitry getting 3.3v or 5v it gets hit by 100V or even a 1000V. This would cause physical damage to the chips.

IC's are much more susceptible to damage than passive components.

Examples:?

There are lucky for us very few examples and none that are common.

There has been much talk about building a EMP bomb, most are total bullshit. But there have been a few that could create enough energy for a low range EMP effect. The one that I am most interested in is a copper tube surrounded with a high order explosive, copper wire is wrapped around this copper tube and is energized with a high power energy source, at the same time the explosive is initiated and it causes the crushes and vaporizes the tube and coil to compress the magnetic field and amplify the current. This could cause a EMP type of effect, its range would still be shorter than a nuclear one. This is lovingly called a EPFCG (Explosively pumped flux compression generator).

Insert diagram

There does seem to be a good amount of doomsday worries about EMP weapons, and some with good reasons. While a EMP would not most likely not directly kill you. It would cause lots of problems. If a nuclear weapon was detonated high in the atmosphere, the EMP resulting from that blast could affect a large part of a country. It would most likely severely damage the infrastructure we all depend on.

Protection from EMP and RF interference:

There are ways to protect from EMP and RFI attacks. Things like shielding the devices with grounded cases, shield the wires, or go to an extreme and use a Faraday cage. Also the use of Frequency hopping and/or spread spectrum will help negate RFI attacks.

A powerful EMP will require a good Faraday cage and a little luck.

Projectile based

These include coil (Gauss) and rail guns both of these utilize large amounts of energy discharged to create magnetic fields, and use those fields to propel items. So far these are not efficient enough for use outside of labs but they do show much promise.

Coil/Gauss gun:

A coil gun uses a coil to create a strong magnetic field to pull a ferrous projectile toward it, the more advanced use more than one coil and use some type of sensor to control the firing of the coils to get the best acceleration on the projectile. This device has a few hurdles that so far have kept the overall power of the projectile limited. The coils must energize very quickly, alas much of the energy put into the coils is converted into waste heat. At high powers the coils have a tendency to fail under the power of their own magnetic fields. Also the projectile must be magnetic, the magnetic flux can cause the projectile to be saturated by magnetic energy that will cause heating of the projectile.

Railgun:

A railgun uses no coils but it energizes the rails that the projectile rides on . This creates a strong magnetic field because of the blah blah fucking physics. Because of the energy levels used many times some of the projectile is converted at least partly into plasma. There have been many successful projects for both of these weapons, the main stumbling block currently is energy storage and powering these beasts.

Lasers:

I assume we all know what lasers are, if you do not well you have other problems. Lasers cause damage by heating the target. I will cover a few of the positives and negitives of lasers as weapons.

Let us start with the negative side of things.

* Energy storage, again these are power hungry monsters, meaning they are tied to large power grids. the larger the laser the more power needed. This makes mobility a large issue.

* After energy storage we run into the fact that we are using light, so we will need collating lenses, these lenses would keep the beam from dispersing.

* We are also going to have to deal with water vapor, dust, etc in the beam path all of these will affect the amount of energy that reaches our target.

* Lasers will impart their energy to the target as heat, a reflective target would be much more difficult to damage with a laser.
* Because we will be heating up the target we will need to track the target. tracking optics for high power will be heavy, costly, and sensitive to damage.

* Line of sight. There will be difficulty in lobbing photons over the hill

Now for the positive points.

* Extremely long range.
* Ability to bring a lot of energy to the party
* Already tested at powers levels needed to be a real weapon

The most powerful military laser that has been made public is the MIRACL laser that is currently based out of White Sands missile range in New Mexico. (anyone up for a road trip?)
It is able to produce a beam that is 5.5 in square and can pack ~1MW of power for more than 60 seconds. Also the navy just completed shooting down a another unmanned drone with a laser.

Now to cover some devices and components that will help you to create the havoc.

Tesla coil,

A Tesla coil is really a simple device. It is a tuned transformer. They can create extremely high voltages but at low currents. The sparks generated will create lots of RF noise and could affect items that are sensitive to RF noise that's nearby. A few things to know though, they are not quiet they have a high current spark gap to drive the primary coil and its a noisy beast, so a fail on stealth. And with the output being low current its RF output is limited on power.

Marx generator:

A Marx generator is a cap based circuit where you charge the cap bank in parallel and discharge it in series. when working with caps its good to know that when caps are connected in parallel, you will increase the energy storage, when discharged in series you increase the voltage. Using one of these its possible to use off the shelf caps, and generate thousands of volts. more than enough to create a arc. Each cap will need to be able to handle the total output voltage.

Flyback transformers:

these are the transformers that power old CRT monitors, i am going to group these with all other standard transformers, ignition coils ect. they all work on the same idea and are good for generating HV arcs.

Voltage multipliers:

Using caps and diodes you can turn a AC voltage into a HV DC output.

Passive components:

Resistors:

They resist the flow of energy.

Coils:

Coils are covered up above.

Capacitors:

Also covered above.

Diodes:

Allow energy to flow in one direction only.

Transistors:

Are electronic switches, used in amplifiers, and radios.

MOSFET

Also electronic switches, can handle higher powers than transistors but at lower freq.

Humans as targets (less than lethal)

There recently has been more than a few advancements that allow real energy weapons to be used on humans, from flashing lights to sonic attacks.

What are less than lethal weapons?

These are devices that are designed for crowd control and for stopping an aggressor without having to use lethal weapons. The cause discomfort in different ways and different intensities.

Sonic Cannon:

These can use a wide range of sound frequencies at high db levels to cause pain and discomfort. These are currently being used for crowd control.

They utilize both low (infra-sound) and high (ultra-sound) frequencies. Low frequencies at high power levels are known to cause nausea and vision problems, high freq will cause headaches and loss of focus.

"Heat Rays"

Use high frequency microwaves to make the target feel heat on the exposed skin. This is also being planned for crowd control. It is currently truck mounted but they are working on more mobile versions. This device is labeled the ADS (Active Denial System)

Strobe Lights aka sea sickness strobe,

uses flashing bright lights flashing with a random pattern to cause nasusa and disorientation. could also cause seizure in those that are predisposed.

This was created for the DOD by a subcontractor for military applications and crowd control, and was recreated by Adafruit for "fun and testing"

In closing, if you have read this far, my hats off to you. The presentation will I hope have a good QA session at the end and will spark some offline discussion. If you have any questions please feel free to contact me. Later.