On Electromagnetic Attacks

Abstract

Electromagnetic pulse attacks, even if not new, are not very well known are rarely considered. Still they are getting easier to implement and at the same time more difficult to defend against. These attacks require often the proximity of the attacker to the target device, but the implementation of the attack can go completely unnoticed. ICT systems and devices, and in general electronic circuits which by now are present in almost all devices, can be forced to malfunction, stop working or even destroyed. In this article we discuss the relevance of this threat from the point of view of ICT security.

When considering the security of ICT systems, we are used to consider the contribution of two fields: physical security and proper ICT (or logical) security. Physical security deals with controlling the access to the hardware used by ICT systems on top of all other aspects of physical security required by the environment in scope. ICT security deals mainly with the security of the execution of applications (programs) on the ICT hardware devices, that is mostly what it is called "logical" security.

But there is another kind of threat which is not usually considered by either fields, and this threat is electromagnetic attacks (see eg. [1] and [2]). Physical security usually does not consider this threat because electromagnetic radiation are not "physical" in the usual sense adopted here: you cannot stop it by putting a gate, and it is not "physical" for the human senses.

Moreover, physical security is usually not specifically targeted to ICT, but it is a generic security field which protects also ICT devices. Instead electromagnetic attacks are specially targeted to ICT devices, any kind of them: large, small, embedded, portable etc.

ElectroMagnetic (EM) Attacks

But what are electromagnetic attacks? We have plenty of examples of these attacks in very well known movies like for example the following two:

- in “Ocean's Eleven” the criminals use an electromagnetic weapon to blackout for a few minutes a portion of Las Vegas
- in James Bond's “GoldenEye” a satellite electromagnetic weapon destroys a Russian radar station and threatens to do the same to London.

These two movies already give us the first classification of EM attacks: they can either *disrupt* or *damage* a target electronic system. The two type of attacks are quite different both for the attacker and for the target to defend itself.

Disruption, like in “Ocean's Eleven”, is typically an interference which induces some anomalies in the electronic system, up to the point of forcing it to stop working for a limited amount of time, but no damage to the hardware is done. This a different kind of “Denial of Service” attack.

Damage instead is applied to the hardware so that it is fully or in part permanently destroyed, like the radar in the James Bond's “GoldenEye” movie.

Damaging EM attacks

There are various ways in which an electromagnetic pulse can destroy a electronic system, but the most common way is to pour so much energy, carried by the electromagnetic pulse, in the circuits that they breakdown. The breakdown is usually due either to over-heating and meltdown (the energy has to go somewhere and in electronic circuits, excess energy is usually disposed through heat, but if the heat is excessive, the circuits melt) or by electrostatic breakdown of device junctions, that is a short-circuit due to the excess current.

Building a EM weapon to damage or destroy electronic circuits is not easy: typically these weapons are either very small range or very directional, and they are extremely dangerous to use if the operator is near to the device due the induced local EM fields. There exists also a well-known long range and non directional weapon which has an EM component, the nuclear bomb, which, on top of all nuclear devastation, produces also a huge EM pulse.

In practice, outside military and similar applications, there are only a couple of damaging EM

attacks that we should consider.

The first class of attacks is actually represented by a very well-known natural phenomenon: *lightning*. Defences against lightning are well known and they rely mostly on *grounding* the EM flow. This is actually the main defence to all EM types of attacks. With lightning we need to shield our EM devices and make sure that all the energy is safely grounded. As easy as it looks, making all direct and indirect earths correctly electrically bonded is often quite expensive and difficult to achieve. Usually houses and offices are not correctly connected and damages can happen.

Other well-known phenomena which give rise to EM attacks are the solar storms (or solar flares). These sun phenomena produce very violent emissions of EM radiations which can cause serious disruptions. There have been solar storms which have disabled or damaged satellites and spacecraft electronics, and they can be harmful to the health of astronauts. They have been able to knock out terrestrial electric power grids for extended periods of time and to disturb the operation of radars and air traffic, wireless communication and the GPS system.

But the point, as usual in a security scenarios, is to consider which threats we want to address and evaluate the cost-effectiveness of the defences or counter-measures. In most scenarios of EM damaging attacks, defences will just be too expensive, and the best approach besides the standard precautions, is to rely on off-site backups, business continuity plans and insurance.

But there is another damaging EM attack scenario which should be considered: targeted short-distance attacks. In this scenario, an attacker with a EM portable weapon enters the facilities and is able to activate the EM weapon at short distance from the ICT systems she/he wants to destroy. She/he can do that either by sending EM radiation through an antenna or connecting directly the weapon to the ICT system cabling (network or power). In this case the security approach is to rely on classical physical security measures to prevent the access of the weapon to the building or to the vicinity of the ICT systems.

EM weapons

But what are EM weapons? Is it difficult to build them?

Actually it is quite easy to build very rough EM weapons. Browsing on the web [3] one can find many Do-It-Yourself descriptions on how to build them. The basic components are: a power source (typically a battery or a small generator), some circuitry (microwave ovens give some interesting

suggestions) and an antenna or a hard-wired connection to the target. The full kit can fit a large bag or a small van (if the antenna is inside the van, better have the side panels made of fibre-glass which does not block the radiation).

Of course DIY EM weapons do not typically have the power and precision to damage and destroy the target, but they are able to disrupt their functioning. Some of these weapons have been able to shutdown a car at considerable distance.

But these weapons are extremely dangerous, often more dangerous for the attacker who uses them than for the target of the attack. Typically the operator of such weapons is not protected from the generated fields and she/he is the one suffering the most consequences also for her/his own health. One should remember the skull which appears on all high voltage electrical power transmission lines, it applies also in this case to the operator of the weapon.

EM disrupting attacks

The most interesting and real attacks, are the disrupting ones. This is because:

- it is much easier and less costly to build a EM weapon to interfere with the working of electronic circuits
- it is much safer for the health of the attacker
- it is much easier to implement the attack, and in most cases even to go undetected
- it can also happen as an unintended consequence of using not-shielded EM devices (a microwave oven or even a mobile phone are the first examples) in the proximity of electronic circuits and ICT systems.

The attacks can be in general of two kinds: targeted (narrowband) in which case one is aiming to disrupt a specific well-known circuit using a specific frequency, or generic (wideband) in which case many different frequencies are used hoping to find one to which the targeted circuit responds.

Today the attacks to electronic circuits are easier than a few years ago because old circuits worked at higher voltage and lower frequencies. Current electronic circuits work at lower voltage and higher frequencies and it is easier to attack these circuits by sending very short pulses (from 100ns to microseconds) high in voltage. The attack is successful if (at least one of) the frequency of the EM matches the resonance pattern of the target electronic circuit. In this way, energy is transferred

from the EM radiation to the electronic circuit. This energy appears in the circuit typically as extra current which disrupt its normal functioning.

The attack can be implemented mainly in three ways:

1. remotely (eg. from outside the building) by means of an antenna
2. connecting to the power or network connectivity of the building
3. directly connecting to the power or the network connectivity of the electronic circuit.

Case 3. requires direct access of the attacker to the target system, which can be prevented by traditional physical security.

The first two cases instead pose quite new challenges. To understand these challenges let consider the case of a typical desktop computer in the following scenario (we'll consider servers later on): a desktop computer on a desk facing a window on a street. In the street there is the attacker with the EM weapon sitting for example in a van or in a car. The attacker aims the EM weapon antenna at the building and fires. The PC which is behind the window starts crashing and even rebooting is difficult until the attack is ongoing.

Defending against EM attacks

How can we protect the PC? The main approach to protect from EM radiation goes back to the English scientist Michael Faraday, who in 1836 invented what is known as a Faraday cage [4]. In theory a Faraday cage is simply a complete enclosure by a (grounded) conducting material. Faraday cages can give rise to quite impressive experiments, like those of people suspended in a Faraday cage surviving completely untouched a lightning. The problem with a Faraday cage is that it works if it is completely closed and the mesh of the insulation has holes which are smaller than the wavelength of the radiation that we want to stop. So we cannot build a real Faraday cage around a normal PC, but better EM shielding 'a la Faraday cage' can reduce or dump the effects of the EM attack.

One of the biggest problem in shielding a PC and in general an electronic device, is the fact that as of today to work it has to be connected to the power and to the network. Both of these connections are easy channels which allow an EM pulse to reach the device. From this point of view, portable devices with batteries are more protected, but still one should prevent wireless communication and

standard copper Ethernet connections. The best protection could be achieved by a battery powered PC (recharged only when it is off) with optical fibre connection (with cables without copper, metal reinforcement and metal junctions).

Since a Faraday cage works in both direction, we can look at this also from the opposite point of view. The best shielded devices are those which have been built to *prevent* EM radiation to leave them, typically for health reasons. Think for example of the hospital's rooms where there are RMI machines, or to our mobile/smart-phones. The enclosure of the mobile phones is designed to protect our heads from EM radiation, which make at the same time the phone more protected from external EM attacks.

So we have very little possibility to directly protect our PC from the external EM attack, unless we buy some military grade devices tested for warfare and we connect them only with optical fibres, we run them only with batteries and enclose them within a grounded metal wired mesh.

But we can do something to the room or the building to protect all what it is contained from an outside EM attack. First of all, concrete walls typically contain steel which already give some level of protection. Windows should not be present or if there are they should be covered with a metal screen. Better still, all walls, floor, ceiling and doors should be completely covered with a (grounded) metal shield. In this way it is quite possible to make a Faraday cage room. Communication with the outside must be implemented with optical fibre connection (with cables without copper, metal reinforcement and metal junctions). The only difficult point is how to make electric power get in the room. It is possible, though quite expensive, to connect power lines safely by adding power surges, filters etc. so to guarantee that the power line cannot bring in EM pulses, but better still it is to install inside the room a full UPS system which regenerates the power feed from outside or generates it directly inside the room.

Making again a reference to a movie, in “Enemy of the State”, Gene Hackman has a server room insulated in a Faraday cage, all contained. In the movie one thing is not very clear: at some point Hackman connects his machines to the CIA servers, how does it do that? Should we assume that he has an optical fibre connection to an outside network?

It is obvious that the shielded room solution is too expensive for a common office, but it could be worth to consider it for computer / server rooms where most of the required components are already in place.

Summing up

Defending against EM pulse attacks is very difficult and expensive. We should consider anyway that:

- attacks, in particular disruptive attacks, are getting all the time easier and cheaper to implement;
- attacks can be unintentional, for example by using not-shielded devices in the proximity of the ICT devices or by works on the power or communication lines;
- "attacks" can have natural causes, like lightning.

Still, this threat is only of the "Denial of Service" type, no information, data, device is stolen or divulged.

This implies that the best approaches to counter this threat are probably those related to *physical security* and *business continuity*.

Still we can do something to reduce or prevent these attacks, in particular:

- shield appropriately all server rooms;
- adopt optical fibre cables where possible, and be sure that the UPS filters power surges both for power and communication (Ethernet) cables;
- check shielding characteristics of electronic devices before buying them;
- make known to HW manufacturer that better shielding and EM pulse resistance is valued, making them interested to improve on them;
- be sure that your business continuity plan, disaster recovery plan and backup procedures consider the threats of EM pulse attacks (also for media storage).

References

[1] William A. Radaski, "Electomagnetic Warfare is here", IEEE Spectrum, August 2014, http://spectrum.ieee.org/aerospace/military/electromagnetic-warfare-is-here

[2] Report by the "Commission to assess the threat to the United States from Electro Magnetic

Pulse (EMP) Attacks", http://www.empcommission.org/index.php

[3] For example Google for "HERF Weapon" for a list of recipes (HERF stands for High Energy Radio Frequency)

[4] See eg. https://en.wikipedia.org/wiki/Faraday_cage

Andrea Pasquinucci (PhD CISA CISSP)