The Impact of Electromagnetic Radiation Considerations on Computer System Architecture.

Carlo Kopp and Ronald Pose.

Dept of Computer Science,
Monash University,
Clayton, Victoria, 3168,
AUSTRALIA
Email: {carlo, rdp}@cs.monash.edu.au

Abstract. This paper will discuss the typical damage effects produced by various types of electromagnetic weapons, and review a range of possible measures in electrical and system design of computer systems, which can be used to defend against electromagnetic attack. The paper states the need for the definition of a standard with electromagnetic hardness ratings for equipment and sites.

1 Introduction

Computer systems are being applied in very sensitive installations. The sensitivity may be commercial or industrial as in a bank or factory whose whole operation is critically dependent on the correct and continuous operation of its computer systems, and it may be military or government sensitivity where economic or even physical security is at risk.

The risks involved are two-fold. First, there is the reasonably well studied risks of sensitive information leaking out of the computer system. Second there is the relatively unstudied risks of disruption of computer system operations though external influences.

In the case of information leaking out of computer systems much effort has been expended on various operating system security measures and on various forms of encryption and authentication technology. There have also been some studies done [VECK85] on the interception of electromagnetic radiation from computer systems. In the case of disruption of normal computer system operations, once

again a great deal of work has been done in increasing the security of operating systems and critical application programs, mainly through various authentication and encryption techniques. However relatively little has been done in the way of studying threats to the physical operation of computer systems.

This paper is essentially a position paper which seeks to raise these important issues, and it also provides outlines of possible approaches to tackling the problems identified. The issues being considered are the ones directly affecting the computer systems hardware and its operation, hence what is being proposed is an approach to computer systems architecture which seeks to minimize the risks.

For a comprehensive solution one must consider the computer system as a whole. The system is only as strong as its most vulnerable component. This means that one must consider, not only the computer, but also its networking, infrastructure, its peripherals, and even its power supply. In fact it turns out that the interconnections between the various components which make up a modern computer system are the weakest points.

Computers are being used in more and more critical applications. At the same time the techniques available and known to those who may like to intercept data or disrupt computer system operations, are becoming more numerous and more powerful. We are aware and are actively taking steps to deal with so-called hackers and others who work through weaknesses in the computer system's software. WHat we examine here are the possibilities and defences against those who may choose to attack the computational machinery itself.

We are not talking here about increasing the physical security of the computer installation. That goes without saying. Of course the computer system should have adequate protection against unauthorised physical access. Here we consider the threats that may be present even without physical access to the computer system components, the invisible but insidious threats which may be propagated through electromagnetic waves. Surprisingly the technology required to attack a computer system electromagnetically is very cheap; far cheaper than that required to phsically blow things up. While the technology does require some engineering expertise, it is based on well-known physical principles, hence will inevitably become available to the next generation of 'hardware hackers'.

As computer system architects we must be aware of the threats and methods of dealing with them. While retrofitting protective measures to existing systems is very difficult and expensive, it is not so very difficult or necessarily expensive to design new computer systems which are not very susceptable to electromagnetic attack.

Interestingly, if one does a good job of protecting against electromagnetic disruption of the operation of computer systems, one automatically gains excellent immunity to eavesdropping on the operation of the computer system and the possiblilty of sensitive information being leaked.

The remainder of this paper concentrates on the vulnerability of computer systems to electromagnetic attack. It looks at the means and motivation for such attack, and it looks at possible defensive and protective measures. The military and defence establishments are beginning to take matters such as these very seriously. Given countries' economic dependence on computer systems operation, the economic and commercial implications are even more vital, and deserve serious consideration by government, commerce and industry.

2 Electromagnetic Attack on Computer Systems and Networks

A recent conference convened on the subject of Information Warfare ran with the theme of the "Convergence of the Military and Civilian Electronic Infrastructures". Whilst this effect may not be readily apparent, it should come as no surprise. Since the early 1990s and the post Cold War scaling down of military force sizes worldwide, we have seen a growing trend for governments to subcontract substantial portions of their electronic infrastructure support and communications traffic carriage to private industry or civilian government utilities. Another important trend has been the strong shift in purchasing behaviour away from expensive, limited production volume Milspec equipment, to standard Commercial Off The Shelf (COTS) computer systems identical to those used in the civilian community.

Another factor is exerting an influence in this area, and this factor is the increasing dependency of private industry, government and military forces upon increasingly complex networks of computers. Traditionally, military planners have regarded fundamental infrastructure as legitimate targets in times of war. The information handling infrastructure has now become a prime target. The destruction of such a critical component of a target system will paralyse that system, or render it significantly dysfunctional. The Allied effort during the 1991 Gulf air war is a good case study.

Few organisations today in the OECD nations, government, military or private industry, could truthfully claim to be immune from the effects of depriving them of their information handling infrastructure. Organisations in the finance industry, government taxation offices and military air defence systems are all examples of organisations which cannot function without their computing infrastructure.

The first question we must ask now is what is the likelihood of an attack upon an organisation's information technology infrastructure ? If the organisation handles large amounts of money, or its activities clash with the agendas of special interest groups, then the likelihood is significant. Whether we are dealing with a bank being extorted by criminals, a mining company being harassed by militant

environmentalists, a food manufacturer being persecuted by militant animal rights supporters, or a government under attack by a terrorist group financed by another government, the motive to attack exists and a corresponding vulnerability to attack exists. It is not difficult to conclude that a genuine problem will develop over the coming decade.

Information Warfare theorists typically identify the following categories as potential threats against the information infrastructure:

Luddites, militant labour organisations, political special interest groups, environmental radicals, Third World governments, Criminals (extortion), Special Forces ie the wartime threat of commando attack, and finally direct attack by air or strategic missile forces equipped with electromagnetic bombs.

This is indeed a broad spectrum of parties who may have much to gain from taking down an organisation's infrastructure.

Government organisations therefore need to consider the vulnerability of their fundamental infrastructure to electromagnetic attack to ensure that vital services are provided to the population at all times. Private industry needs to consider both the potential financial losses directly incurred as a result of a successful third party electromagnetic attack, as well as the potential follow-on losses to be incurred in litigation by customers or shareholders, who may have experienced losses through the unavailability of a contracted service. Private industry must also consider the longer term implications of high insurance premiums which would have to be paid, to provide protection against litigation.

3 An Overview of Electromagnetic Weapons and Damage Effects

A wide range of device types exists which may be employed to damage electronic equipment. In principle, any device which can cause semiconductor devices within equipment to be exposed to unsafe electrical voltages or power levels could be used as an electromagnetic weapon.

Electromagnetic weapons fall into two broad categories in terms of scale of attack and delivered power, these are the category of special forces and terrorist weapon which have low emitted power and coverage, vs the categories of strategic and tactical military systems which are built to destroy whole sites. The ultimate electromagnetic strategic weapon is the high altitude air-burst nuclear EMP bomb.

In assessing the effects of an electromagnetic weapon, we identify the terms "Soft Kill" and "Hard Kill". A soft kill is achieved when the effects of the weapon cause the target to crash or reset, lose data or get into an unrecoverable state requiring a reboot. Once the electromagnetic weapon ceases to affect the target system, and it is rebooted, normal operation can resume. The effect of soft kill is

therefore to disrupt operations, causing downtime and preventing the organisation from performing its assigned task.

A hard kill is achieved when sufficient energy is delivered into the target system, such that it is permanently electrically or physically damaged and thus can no longer perform its function. The objective of a hard kill attack is to inflict attrition upon the victim's electronic assets. A victim subjected to sustained hard kill attacks will eventually lose the capacity to perform functions reliant upon electronic infrastructure.

3.1 Terrorist and Special Forces Weapons

Terrorist and special forces weapons are the most likely threats which we can expect to see used. These are typically designed to destroy a single machine, workgroup of machines, or disable the networked systems in a single building. Such weapons are used from very short distances, if not requiring direct physical contact with the equipment.

3.1.1 HERF and HPM Guns

The High Energy Radio Frequency (HERF) gun is is a generic term which can be applied to any device which can emit and focus a high power beam of RF energy. Because of the need to focus the effect of the weapon, and provide the operator with a reasonably focussed beam, we can expect most HERF guns to operate at frequencies above 100 MHz. Power levels need to be sufficient to produce standing wave amplitudes of at least hundreds of Volts on the wiring or interconnecting cables associated with the victim system.

Should a HERF gun operate at microwave frequencies, and deliver hundreds of kiloWatts of peak power, then it qualifies as a High Power Microwave (HPM) gun. Such weapons damage targets not only through back door coupling of standing waves on cabling, but also by directly coupling into equipment chassis through ventilation holes and poorly secured panels.

The Tesla coil is a non-directional equivalent to a HERF gun, operating at frequencies of tens to hundreds of kiloHertz. A Tesla coil can be used as a service denial weapon, concealed within the vicinity of a victim system and left to operate unattended.

The primary damage effect of HERF guns is that of exposing semiconductors to RF voltages which are unsafe and cause breakdown of MOS gates and BJT PN-junctions. HERF guns may be pulsed or continuous wave, the latter also constituting a significant health hazard to operators and bystanders alike.

3.1.2 Man Portable Explosive Flux Compression Generators

Explosively pumped flux compression generators are the preferred power source for strategic and tactical military electromagnetic weapons. The generator device itself can produce MegaGauss magnetic flux levels at very short distances. As a result, it is expected that such generators, packaged suitably, will be used as the electromagnetic equivalent of a man portable demolition mine or charge.

Such a device would be emplaced several metres from a victim site, for example against the outside wall of a computer centre machine room, and then left to detonate under timer control. The the result will be the production of a ramping pulse of up to MegaAmps of current within the generator, with a duration of several hundred microseconds. Cables and wiring exposed to the generators field will have a single high voltage pulse coupled into them. This pulse can punch through transformers and destroy semiconductors.

3.1.3 Tazers and Power Line Spiking

Devices such as the Tazer stun gun can be used to damage network interfaces across large numbers of machines, by injecting voltage pulses of kiloVolts of magnitude into network cabling. The user of the Tazer will require physical access.

Any device which can produce a very rapid short circuit, and then open circuit, can be used to “spike” mains power lines. Such sharp transients travelling along power cables can penetrate power supplies to damage components, as well as damage datacomm interfaces differential earth potentials. Spiking of power lines also requires physical access, although this may be outside the security perimeter of a site.

3.2 Strategic and Tactical Military Weapons

Strategic and tactical military electromagnetic weapons are at this time immature but growing in importance. Such devices are specifically designed to destroy a wide range of electronic equipment over footprints of up to hundreds of metres of diameter. While an unlikely threat in the short term, such devices have been described as the “Nuclear weapons of the Information Age”, and may be commonly used in future military operations, punitive strikes and high calibre terrorist operations.

Two technologies are at the core of such weapons. The explosively pumped flux compression generator, capable of producing currents of up to tens of MegaAmps and energies of tens to hundreds of MegaJoules. It may be used as a

weapon in its own right. Alternately, it may be used to drive a High Power Microwave tube and produce a single pulse of of tens of GigaWatts.

3.2.1 Low Frequency (EMP) E-Bombs

An air delivered bomb containing a pure flux generator warhead is termed an LF E-bomb. Is primary effect is to produce an intense magnetic field in the near vicinity of the bomb which will inductively couple into wiring, producing a single high voltage pulse, possibly with a ringing transient decay.

3.2.2 HPM E-Bombs

An air delivered bomb containing a flux generator powered HPM warhead is termed a HPM E-bomb. Its primary effect is to produce microwave field strengths of between kiloVolts to hundreds of kiloVolts per metre, in a footprint of hundreds of metres of diameter with a duration of up to several microseconds. The microwave radiation may be circularly or linearly polarised, and will produce high voltage standing waves on wiring and cables, as well as directly penetrate through holes in shielding.

3.2.3 Combined Effects E-bombs

A Combined Effects E-bomb is a HPM E-bomb which uses an oversized FCG to produce a combination of HPM and LF damage effects. Such a weapon will be effective against any target vulnerable to either HPM or LF weapons.

3.2.4 High Power Microwave Directed Energy Weapons (HPM DEW)

The HPM DEW is the large scale military equivalent of the HPM/HERF gun. Because it will deliver peak powers of GigaWatts and average powers of hundreds of KiloWatts, it can produce damage through high voltage as well as thermal effects.

Such weapons are also extremely dangerous to personnel and subject to wavelength of operation, may be capable of penetrating many miles of rain or cloud to damage or destroy a target.

4 Coupling Modes and Damage Effects

The primary target of any electromagnetic weapon are semiconductor devices. Bipolar devices are damaged by causing breakdowns in reverse biased PN junctions, which may be then subjected to thermal damage due the direct effects of the weapon, or thermal damage through the action of the equipment's power supplies. Because most computer or other digital equipment has a substantial amount of fast capacitance attached to the power supply rails as bypass capacitors, in addition to typically substantial power supply capacitors, discharge currents can be substantial enough to destroy most semiconductor devices.

Field Effect Transistors, be they MESFET or MOSFET, are damaged by causing very high electric fields to punch through the Gate dielectric. Such damage can either cause gate leakage, degrading performance, or permanent breakdown. In the latter instance the transistor is destroyed. Again, the equipment power supply may contribute to the damage effects.

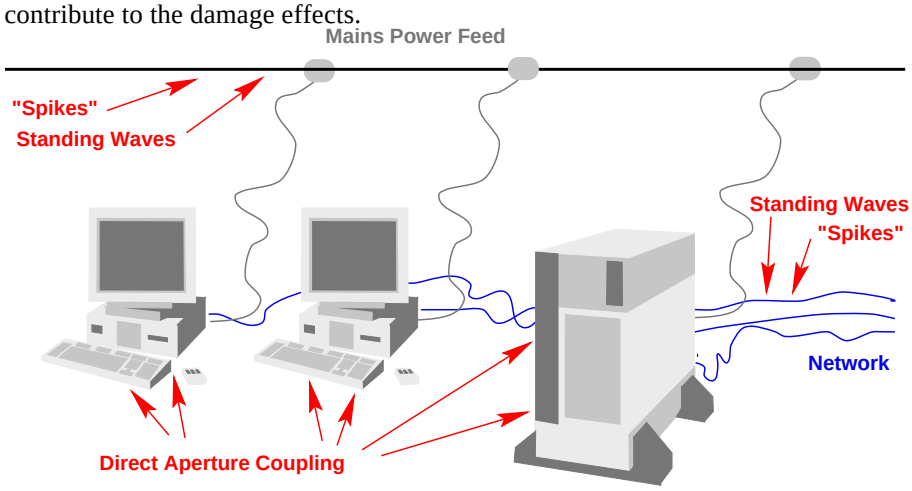

Fig.1 System Level Susceptibility

Two principal coupling modes are recognised in the literature. Front Door coupling occurs through antennas and destroys the RF semiconductors in receivers and transmitters. Back door coupling occurs through power and data cables and wiring, and can damage both power supplies, data receiver and transmitter devices, and if propagated into the equipment any other devices exposed.

4.1 Low Frequency FCG Effects

Low frequency weapons will damage their targets primarily through back door coupling into power and data lines. The high voltage pulse will damage power

supplies, punch through isolation transformers on data lines, and cause common mode breakdowns on receivers and transmitters on data lines.

4.2 HERF Gun Effects and HPM Standing Waves

A HERF gun will damage its target by primarily through back door coupling into power and data lines. Significantly, circuits which may exhibit low impedance behaviour at lower frequencies may present a higher impedance at RF frequencies and thus sustain exposure to high voltages induced as standing waves on cables and wiring. This may be particularly true of HPM sources.

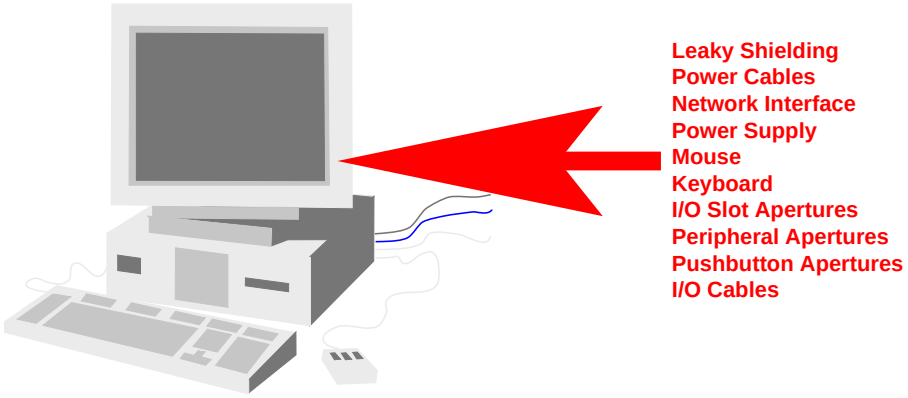

Fig.2 Host Level Susceptibility

Moreover, with HPM sources, standing waves on wiring which enters equipment cavities may contribute to exciting spatial resonances within the equipment cavity itself.

4.3 HPM Cavity Resonances

HPM radiation has the ability to directly couple into shielded equipment cavities through ventilation holes, and poorly sealed panels. Gaps or holes can behave as slot radiators providing that they are comparable in size to the wavelength of the radiation. Panels which are not conductively sealed about their edges may also resonate when excited by microwave radiation and directly couple energy into the cavity. The spatial standing wave pattern will exhibit potentially large field strengths at its antinodes, and semiconductor components exposed to such fields may be damaged or destroyed.

5. Hardening Strategies

Defending against electromagnetic attack may be simple conceptually, but may add significant costs to equipment as well as site installations.

The starting point for any hardening measures is fundamental reliability theory. If we assume a non-redundant system, which is a very reasonable assumption for most types of computer or communications equipment, then Lusser's product law applies. This rule states that the probability of system survival is the product of the probabilities of survival of all system components.

If follows therefore that partial hardening is not a viable measure. Equipment or sites must be comprehensively hardened. Because the threat may be operating within a frequency band spanning tens of kiloHertz to tens of gigaHertz, implementation can be quite expensive.

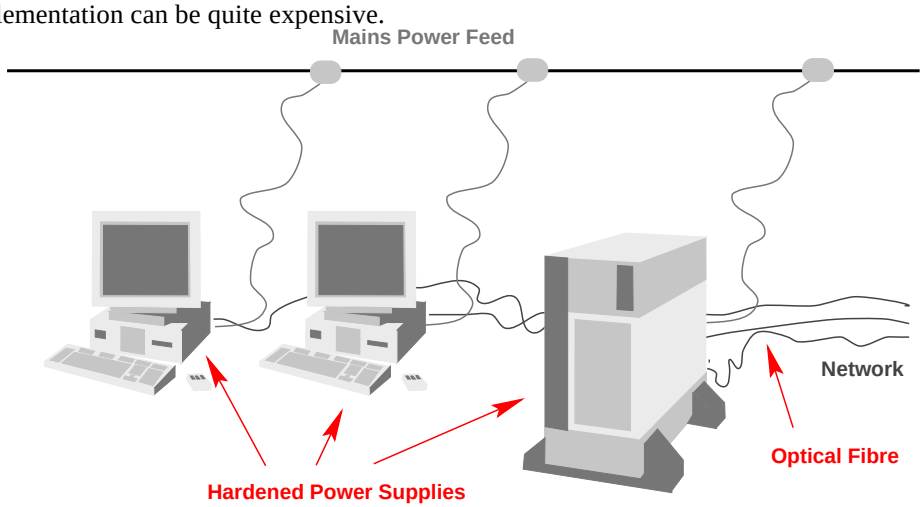

Fig.3.1 I/O and Power Interface Hardening

A very robust strategy is to use a layered defence, where the damaging radiation or voltages must penetrate several design features specifically built to defeat its effects or absorb its energy in a repeatable fashion.

Diversity in space and equipment types can contribute to system level reliability, as significant physical and electrical separation of equipment may prevent a single attack from destroying items other than those directly exposed, as well various manufacturers' equipment types may exhibit various degrees of "hardness" to attack.

At an electrical level, two fundamental strategies exist which may be used. The first strategy is that of dissipation of effects. This is accomplished by using either passive networks, gas discharge devices, or fast switching protection diodes, all of which are intended to dissipate the coupled wave or pulse to a level where it will not damage exposed semiconductor devices. this strategy is designed to defeat back door coupling through power, and particularly data lines. The drawback of this

approach is that it provides a degree of protection, beyond a certain power level the dissipative device will fail. The advantage of this strategy is that it can be often retrofitted to equipment, by placing connectors with protection devices between equipment and their cables.

An alternate, more robust strategy for protection exists, but can be significantly more expensive. This is a strategy of exclusion of electrical effects. This is achieved by using comprehensive shielding of sensitive components, in effect producing a Faraday cage around sensitive components, and by using non-electrical channels for the transfer of data and power. In this fashion, no path exists via which damaging voltages or radiation can enter the equipment.

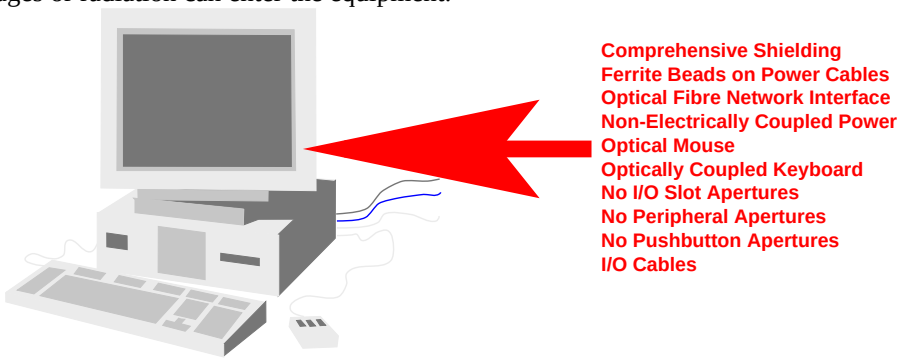

Fig.3.2 Comprehensive Host Hardening

A site or equipment item hardened in this fashion can withstand significantly higher field strengths than equipment or sites defended by dissipative techniques. Indeed, should the task be performed very thoroughly and a non-electrical external source of power be used, then the equipment or site may become virtually immune to attack. Only weapons capable of physically damaging the Faraday cage or producing extremely high magnetic fields within the enclosure can defeat this scheme.

5.1 Site Level Hardening

Site level hardening of whole buildings or rooms in buildings can be performed by turning buildings or rooms into Faraday cages and using the previously stated schemes for data and power transfer. Inside such sites, unhardened equipment may be safely used.

Another issue will however then arise, which is site security and physical access control. A malicious party with a portable HERF or HPM gun can defeat this scheme once inside the facility.

The principal drawback of this strategy is cost, as the refitting of a substantial building or site will cost easily millions or tens of millions of dollars. Moreover, it

is not a strategy which can be applied incrementally, The whole site must be done at once. As noted earlier, since partial hardening is of little value, the benefit of site hardening will not be seen until the site is completely done.

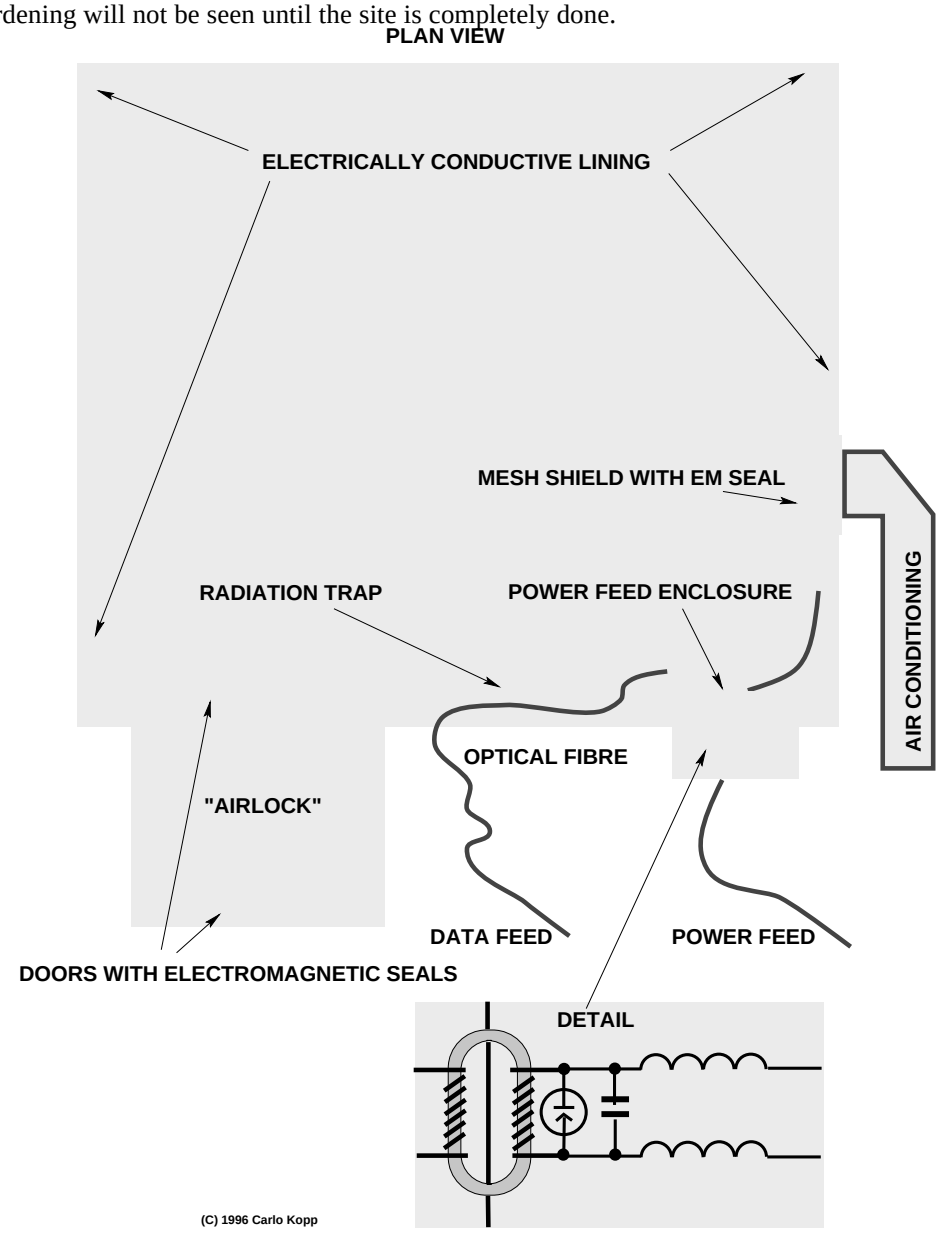

FIG.4 COMPUTER ROOM HARDENED AGAINST EM ATTACK

One element of site level hardening can however be justified whether or not the intent is to shield the whole building. This element is the comprehensive use of

optical fibres for internal networking inside the site. Because conventional LANs may propagate damaging electromagnetic power levels throughout a building, they constitute a potential single point of failure for the whole site, as well as being a single point via which most computers in the building may be attacked and damaged.

5.2 System Level Hardening of Computer Systems

Hardening of individual items of computer equipment may initially appear to be a difficult task to perform economically, and hence one which can significantly impact the cost of a larger installation. This is not entirely true however, in that designing equipment for a high level of electromagnetic hardness can be achieved with only modest penalties in cost. With high volume production techniques it should be possible to manufacture equipment with very good resilience to high field strengths, providing it is designed from the outset for economical production.

The starting point for any hardening effort is the choice of preferred strategy. We will choose a strategy of exclusion, as this is the most robust approach to solving the problem.

The general approach we will follow is that the equipment chassis will be a Faraday cage, the electrical power supply will use non-electrical means to feed power into the Faraday cage, and finally optical fibres or direct optical transceiver links will be used to interconnect equipment components, such as the keyboard, the monitor or LCD display, the mouse and external peripherals such as disks or magnetic tapes.

The comprehensive shielding of the equipment chassis is not a technologically difficult task, and much off the shelf hardware exists which can be applied to this task. Access into the Faraday cage should exist only for optical cables and the non-electrical power feed, and one or two large panels with electromagnetic seals should be used to access the internals. The conventional strategy of having multiple I/O adapter boards with individual back panels exposed on the rear of the chassis is not acceptable, as each panel is a potential failure point in the shielding system.

5.3 Power Supplies

The power supply problem is one which requires further effort. The problem can simply be defined as one of how to most efficiently transfer power into a Faraday cage without an electromagnetic path between the interior and the exterior of the cage.

An example of such a scheme could be a modular power supply in a form factor identical to current Personal Computer PSUs. This supply would however employ a simple and robust squirrel cage electrical motor on the exposed or “hot” side of the supply, to produce both airflow for cooling and hydraulic fluid pressure and flow. Power would be coupled into the Faraday cage through closed cycle hydraulic fluid flow, the fluid passing through mesh shields or sintered blocks conductively embedded in the Faraday cage wall.

On the protected or “cold” side of the supply, the hydraulic fluid would drive a small impeller or other torque generating device, which would drive a low voltage alternator. The alternator windings would be appropriately tapped so that the downstream linear regulators are fed with appropriate voltages, the main +5V DC rail would be regulated by electrical control of alternator output duty cycle. The supply would be built in two separate sections, to allow the rapid replacement of a damaged “hot” side.

Another viable alternative is the use of a compact electrical motor / generator arrangement. A simple and robust squirrel cage motor can be used on the hot side of the supply to convert mains electrical power into torque on a shaft which runs between the hot and cold portions of the supply enclosure. The motor would be intentionally designed with heavier wire than would typically be used, to avoid thermal damage effects from sustained or repeated exposure. A flywheel could be added to the motor to provide energy storage to defeat short duration dips in the mains power feed. As well, the shaft could carry a fan to provide cooling airflow through the enclosure.

On the cold side of the supply, a small alternator could be used to generate the voltages required to drive the +5V, +12V, -12V and any other required supply rails. The alternator would have windings tapped for each rail, thereby avoiding the need for transformers. The alternating output from the windings would be rectified and filtered, and if necessary run through a linear regulator chip. As with the previous example, the main +5V rail would be regulated by manipulating the current through the rotor winding, as is done with automotive alternators.

Mechanical power transfer schemes may be simple and robust, but do suffer eventual wearout of their bearings, causing a loss in efficiency and finally failure. Another alternative which should be considered is the use of a closed cycle fuel cell scheme. In such an arrangement, the incoming mains power is rectified by suitable means to electrolyse the working electrolyte, the propellant and oxidiser (eg hydrogen and oxygen) are then fed into the cold side of the supply to drive a fuel cell which generates a very smooth and stable DC voltage. The depleted working electrolyte or oxidation product is then cycled back to the hot side of the supply for further energy transfer. A fuel cell based system has some very nice attributes, as it has no moving parts it is silent and does not suffer mechanical wearout, moreover, if it is built with additional chemical storage tanks it can also function as an uninterruptable power supply. The disadvantage of a chemical fuel cell scheme is

likely to be initially cost, as well as the potential hazards of storing flammable or corrosive propellants and oxidisers. Energy density and size will also be an issue, and this is why a fuel cell scheme is likely to be most suitable for large installations or computer room hardening.

Should we choose a strategy of dissipation rather than exclusion in the power supply design, then we will have to accept lower limits on ultimate performance. However this may be achieved at a substantially lower cost and thus should not be disregarded from the outside. Many low power threats may be readily defeated by this technique.

5.4 Networking

Optical variants of Ethernet have been used widely for many years. Optical variants of most networking protocols are widely established, indeed FDDI is primarily an optical medium.

The importance of optical networking should not be understated. Whereas power supplies are built from low density and usually electrically robust components which usually require substantial energy to damage, conventional networking interfaces are built from much higher density components with an inherently lower tolerance to electrical damage. Because networking cables interconnect most systems on any given site, a damaging electrical signal which enters the network at any given physical point can be propagated to most systems in that site. Because networks operate at tens to a hundred Megabits/s clock speeds, they typically use low loss and electrically fast cable types, thereby providing an excellent propagation environment for sharp spikes, VHF, UHF and microwave signals. The qualities which make such a cable a good performer in transmitting intended signals also make it a good medium for an attacker.

Because networking cables usually cover distances of tens to hundreds of metres, following corridors and risers, they have both the length and geometry to act as effective antennae and thus can provide excellent coupling of incident radiation. The proliferation of 10 and 100 Base-T is of particular concern, as the cable is typically unshielded and thus efficient at coupling energy to signal lines. Typical 10 Base-T hardware employs miniature coupling transformers which exhibit substantially higher impedances than the nominal 100 Ohms at frequencies above 10 MHz, thereby providing a coupled signal with a high impedance load against which a substantially higher peak voltage may be attained.

The comprehensive use of optical fibre for local areas networks removes this fundamental vulnerability of the basic networking infrastructure. Placing hubs, repeaters, bridges, switches and routers into Faraday cages with protected power supplies allows a significant improvement in electromagnetic hardness at a very modest cost.

Mobile networking schemes intended to allow systems to be moved within buildings should employ infra-red optical links rather than RF links. The latter will become another vulnerability to electromagnetic attack if it proliferates significantly in the marketplace.

5.5 External Storage and Multiple Chassis Systems

Large and small computer systems are often packaged into multiple chassis, which are interconnected by bus cables. The most popular example would be SCSI bus peripherals, where a parallel electrical interface using TTL-like signalling is used to carry data between chassis.

Such bussing presents another vulnerability to electromagnetic attack, for the same reasons why networking cables produce a vulnerability to attack. Again, a damaging voltage introduced into one equipment item can be propagated into another.

Fortuitously for the defending side, the SCSI-3 standard includes an optical interface, which was introduced for reasons of performance and reliability. As with the instance of networking, fibre SCSI should be used exclusively for new installations.

Peripherals with removable media should employ doors or covers over entry apertures, which are spring loaded and equipped with an electromagnetic seal. Otherwise the risk is always present that radiation from a microwave weapon could couple into the peripheral and cause damage.

5.6 Other Peripherals.

The largest proportion of computers in use today are single user desktop or deskside systems. All such systems will use a keyboard, a monitor and usually a mouse. In conventional designs, all of these items are connected to the system via copper cables, which carry TTL, analogue signals and in input devices, +5V DC power to the devices.

These copper connections all constitute potential vulnerabilities. All could be replaced with optical fibres, or free space optical transceivers. The simplest near term strategy for resilient keyboard and mouse design is to use low power CMOS logic internally in such devices, shield them well and power them by battery and optionally photo-voltaic (eg solar) cells.

In the instance of keyboards and mice, these could also be built as wholly optical devices, with a low power semiconductor eyesafe laser driving optical power out to the device through a large numerical aperture optical fibre. An optical

transducer in the keyboard or mouse would then appropriately manipulate the optical signal, a proportion of which would be routed back to the system via another fibre.

Monitors based upon CRT technology can be easily adapted by adding an optical receiver board with three, four or five channels to accept video and sync from the host system. Optical receivers and transmitters can be built with excellent linearity, arguably much better than that achieved in the video channels of consumer quality CRT monitors.

Whereas CRT monitors which are bulky can easily accommodate a protected power supply within their existing volume, monitors based upon LCD technology cannot. Whilst these may be easily fed with video, as in the preceding example, their power consumption would most likely be too great for compact battery power and thus repackaging may be required to a larger degree than with CRT technology.

6 Priorities and Cost Issues in Hardening

The fundamental question is how much hardening at what cost ? How many defensive layers are required ? Are purely electromagnetic defensive techniques adequate ? Must we move to optical communications ?

In hardening a site we must first identify what we perceive to be the most likely threats, and the worst case threat we can expect to see. This will set bounds upon the level of hardening required.

A good starting point for system and site hardening is networking, as it is ubiquitous and capable of propagating damaging energy throughout a site. Once networking has been addressed, they we must deal with power. We then move to improve the quality of individual equipment shielding, and finally move to optical connections between peripherals.

The cost issue in host systems and peripherals is incremental, in that equipment types known to be more robust can be phased in as existing equipment is phased out. With the life cycle of a typical desktop system today being 18 months to three years, this means that an incremental cost penalty will be incurred until the whole population of devices is replaced. Only should immediate replacement of a whole population be required would this incur a significant cost penalty.

Sites with well established copper networking infrastructure may incur significant costs should they move over to fibre, as they will need to recable as well as replace network adaptors on hosts. This is an inevitable consequence of an established technology base being no longer suitable for environment it exists in.

Converting computer rooms or sections of buildings into Faraday cages will be expensive and difficult. Arguably this aspect of hardening is the most difficult, and should be implemented only after a careful risk assessment. Low power threats may

be defeated by using lesser measures, and a comprehensive Faraday cage shield may not always be justifiable.

A important point to stress in this context is that Lusser's product law of system reliability does apply, and thus incomplete hardening may not improve the survivability of a site. It is therefore imperative that a careful assessment of risks be carried out before committing to a specific plan for site and equipment hardening.

Conclusions

First, the existing electronic infrastructure is highly vulnerable to properly thought out electromagnetic attack. This vulnerability in turn will create opportunities for criminals, political movements, Luddites, terrorists and info-terrorists and finally, military powers with an interest in strategic power projection.

For commercial sites, hardening of some type will be required to defend against liability claims by consumers or corporate customers. Some interesting legal issues may arise in relation to the provision of proper care in safeguarding both shareholder and customer data and services.

Government sites will require comprehensive hardening to defend against military threats as well as lower grade threats. A citizen unhappy with his tax return or a speeding ticket may feel compelled to test his homebuilt HERF gun with possibly expensive consequences for the community at large.

A unclassified and publicly available electromagnetic hardening standard with "hardness ratings" for equipment and sites will be required, and will need to be widely adopted by manufacturers and end user sites. Given the vulnerability of the basic civilian infrastructure to such attack, there is no military advantage to be had in restricting access to such information.

Researchers in academia and industry should also consider exploring techniques for making equipment and sites more resilient to such threats.

A final note is that the implementation of comprehensive electromagnetic hardening would have a very interesting side effect, that being a substantial reduction the levels of EMI produced by computer and networking equipment. This would both improve the quality of the electromagnetic environment, as well as reduce opportunities for eavesdropping Van Eck (TEMPEST) radiation, thereby enhancing privacy and security. The adoption of a comprehensive EMI control regime has been resisted by much of the marketplace, many regarding the cost penalties of shielding as exceeding the potential costs of RF pollution and compromised security. The threat of electromagnetic attack should add a final and decisive reason to this argument.

In conclusion, we have examined the problems of computer system security and vulnerability to electromagnetic eavedropping and more importantly,

electromagnetic attack. The means and methods of such attack have been outlined, as have some defensive measures.

Computer systems architects should be aware of these issues and should design systems which deal with such threats. It is only a matter of time before even commercial systems will demand immunity to attack of this kind.

Apart from the technical content of this paper, we have identified an aspect of computer system architecture which has been largely ignored, partly though ignorance. There will, in the near term, be lucrative niche markets for computer systems designed to cope with electromagnetic attack. Initially the markets will be military, but very quickly economically vital industries and government will take these matters seriously. Here is an opportunity for Australian computer architects to be at the leading edge,

in an area which is bound to attract significant funding in the near future.

References

CAIRD85 - Caird R.S. et al, Tests of an Explosive Driven Coaxial Generator, Digest of Technical Papers, 5th IEEE Pulsed Power Conference, pp.220, IEEE, New York, 1985.

FANTHOME89 - Fanthome B.A., MHD Pulsed Power Generation, Digest of Technical Papers, 7th IEEE Pulsed Power Conference, pp.483, IEEE, New York, 1989.

FLANAGAN81 - Flanagan J., High-Performance MHD Solid Gas Generator, Naval Research Lab, Patent Application 4269637, May 1981.

FOWLER60 - C. M. Fowler, W. B. Garn, and R. S. Caird, Production of Very High Magnetic Fields by Implosion, Journal of Applied Physics, Vol. 31, No. 3, 588-594, March, 1960.

FOWLER89 - C. M. Fowler,R. S. Caird, The Mark IX Generator, Digest of Technical Papers, Seventh IEEE Pulsed Power Conference, 475, IEEE, New York, 1989.

GLASSTONE64 - S. Glasstone, Editor, The Effects of Nuclear Weapons, US AEC, April, 1962, Revised Edition February, 1964.

GOFORTH89 - Goforth J.H. et al, Experiments with Explosively Formed Fuse Opening Switches in Higher Efficiency Circuits, Digest of Technical Papers, 7th IEEE Pulsed Power Conference, pp.479, IEEE, New York, 1989.

GRANATSTEIN87 - Granatstein V.L., Alexeff I., High Power Microwave Sources, Artech House, Boston, London, 1987

HERSKOVITZ96 - Herskowitz D., The Other SIGINT/ELINT, Journal of Electronic Defence, April, 1996.

HOEBERLING92 - Heoberling R.F., Fazio M.V., Advances in Virtual Cathode Microwave Sources, IEEE Transactions on Electromagnetic Compatibility, Vol. 34, No. 3, 252, August 1992.

KOPP92 - Kopp C., Command of the Electromagnetic Spectrum - An Electronic Combat Doctrine for the RAAF, Working Paper No.8, Air Power Studies Centre, Royal Australian Air Force, Canberra, November 1992.

KOPP93 - Kopp C., A Doctrine for the Use of Electromagnetic Pulse Bombs, Working Paper No.15, Air Power Studies Centre, Royal Australian Air Force, Canberra, July 1993.

KOPP96 - Kopp C., The E-bomb - A Weapon of Electrical Mass Destruction, Proceedings of the InfoWarCon V Conference, September, 1996, National Computer Security Association, Washington, DC

KRAUS88 - Kraus J.D., Antennas, Second Edition, McGraw-Hill, 1988.

MICRON92 - Micron DRAM Data Book, Micron Technology Inc, Idaho, 1992.

MOTO3 - Motorola RF Device Data, Motorola Semiconductor Products Inc, Arizona, 1983.
NATSEMI78 - CMOS Databook, National Semiconductor Corporation, Santa Clara, 1978
NPI93 - NPI Local Area Network Products, SMD Transformers, Nano Pulse Industries, Brea, 1993.
RAMO65 - Ramo S. et al, Fields and Waves in Communications Electronics, New York, John Wiley & Sons, 1965
REINOVSKY85 - Reinovsky R.E., Levi P.S. and Welby J.M., An Economical, 2 Stage Flux Compression Generator System, Digest of Technical Papers, 5th IEEE Pulsed Power Conference, pp.216, IEEE, New York, 1985.
SANDER86 - Sander K. F. and G.A.L. Reed, Transmission and Propagation of Electromagnetic Waves, Cambridge University Press, 1986.
STAINES93 - Staines, G.W., High Power Microwave Technology - Part IV, Military Applications of High Power Microwaves, Salisbury, DSTO ERL, EWD, 1993, draft paper.
TAYLOR92 - Taylor C.D., Harrison C.W., On the Coupling of Microwave Radiation to Wire Structures, IEEE Transactions on Electromagnetic Compatibility, Vol. 34, No. 3, 183, August 1992.
THODE87 - Thode L.E., Virtual-Cathode Microwave Device Research: Experiment and Simulation, Chapter 14 in High Power Microwave Sources, 1987.
VECK85 - van Eck W., "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk", Computers and Security, 1985, pp. 269.
WHITE78 - The EMP - A Triangular Impulse, 2.29, A Handbook Series on Electromagnetic Interference and Compatibility, Don White Consultants, Maryland, 1978.