DOI:10.16157/j.issn.0258-7998.2002.04.001

专家论谈

计算机电磁信息泄露与防护研究

中国科学院研究生院信息安全国家重点实验室北京 3908 信箱 DCS 中心（100039）
单国栋　戴英侠　王　航

摘　要：随着计算机安全技术的迅速发展，计算机电磁信息泄露问题已得到了广泛关注。本文对计算机电磁信息泄露进行了系统的分析，介绍了视频信息接收还原的原理，并详细说明了计算机电磁信息泄露的防护方法。

关键词：计算机安全　电磁辐射　信息泄露　TEMPEST

随着信息技术的发展和微型计算机的普及应用，计算机已成为目前应用最为广泛的信息处理和信息传输的电子设备。由于计算机的特殊构造方式与工作方式，它不可避免地会向空间辐射电磁波，这些电磁发射信号不但频谱成分丰富，而且携带信息，从而对某些处理的信息的安全性造成威胁。在信息安全领域，电磁信息辐射属于 TEMPEST 的研究范围。

TEMPEST，即“瞬时电磁脉冲发射标准”(Transient ElectroMagnetic Pulse Emanation STandard)或者“瞬时电磁脉冲发射监测技术”(Transient Electromagnetic Pulse Emanation Surveillance Technology)的英文缩写。据文献可查，该词最早出现在 1969 年美国制定的“EMC 计划”中。而美国早在二十世纪 50 年代就开始了计算机“泄密发射”(Compromising Emanations)的研究，并在 1981 年颁布了一系列 TEMPEST 标准；80 年代中期，英国和北约颁布了类似的标准，其它国家也制定了相应的研究开发计划，这些标准都是非常机密的，此方面的研究工作也都是秘密开展的。随着 TEMPEST 技术的发展，其研究范围又增加了电磁泄露的侦察检测技术，用于截获和分析对手的泄露发射信号。1998 年，英国剑桥大学的科学家 Ross Anderson 和 Markus Kuhn 提出了“Soft Tempest”的概念，即通过“特洛伊木马”程序主动控制计算机的电磁信息辐射，这标志着 TEMPEST 技术从“被动防守”到“主动进攻”的转变。

我国是从二十世纪 80 年代中期开始关注 TEMPEST 领域的，已经在计算机系统电磁信息泄露的安全防护方面取得了一些研究成果。但因为起步晚，许多课题尚有待深入研究、发展。

1　电磁信息泄露分析

1.1　电磁信息泄露的组成

麦克斯韦（James Clerk Maxwell）电磁场理论告诉我们：任何交变电磁场都会向四周空间辐射电磁信号，任何载有交变电磁信号的导体都可作为发射天线。计算机是采用高速脉冲数字电路工作的，因此，只要处于工作状态就会向机器外辐射含有敏感信息的电磁波。按照电磁辐射的内容，大致可以分为以下几种情况：

(1)无信息调制的电磁辐射。如计算机的开关电源、时钟频率、倍频和谐频等，这类电磁波辐射多数没有信息内容调制，个别的有 50Hz 交流电源或单一频率调制，不易造成敏感信息泄露。

(2)并行数据信息的电磁辐射。计算机系统内部的信息流主要有四个部分：数据总线、地址总线、控制总线及 I/O 输出。其中，前三个部分信息的共同特征是都是并行数据流（8 位、16 位、32 位、64 位等），这些并行的数据信息泄露后是极难还原的。这是因为：①并行的多位数据在时域上同步、频域上相关。从理论上讲，是难以将这些交织在一起的频谱信息分离开的。②这些并行的数据都是二进制编码。在不同的操作系统和不同的应用程序中，对同一组码的定义是完全不同的，因此很难确定某一组二进制码的确切含义。这类辐射信号的内容多数是反映计算机的运算过程，辐射频率主要集中在 2MHz~450MHz 内。

(3)寄生振荡。即计算机电子线路中的分布电容、布线电感在特定条件下，对某一频率谐振而产生的振荡。这种辐射的频率范围不规律，从几十 kHz 到上千 MHz 都有，辐射的能量也不相等，有的辐射信号理论上可以传播数公里。

(4) 计算机终端的视频信号辐射。计算机的 I/O 传输的数据一般是串行数据，如打印机、绘图仪、传真接口等，这些数据的速率低，其辐射信息容易还原。尤其是光栅扫描式阴极射线管显示器的视频信号辐射。由显示卡输出的视频信息经预处理、放大后加在显示器的阴极及控制栅极，信号的幅度高达 700Vpp，行、场信号经同步、放大后，形成上百伏的高电压，偏转线圈的电流可以达到安培级。这些串行特征的视频信号在大幅度、大电流的情况下是很容易造成电磁信息辐射的。形成此类电磁辐射的部分有：显示卡、连接线、CRT 视放电路等。

(5)计算机显示器阴极射线管产生的 X 射线。据报道，这种 X 射线也可以通过特殊的技术手段进行还原。

1.2 电磁信息泄露分析

计算机终端(CRT)上显示的任何信息都是由基本像素按行、场扫描排列而组成的。这些像素的视频信号是一个数字脉冲信号，像素的大小取决于终端的分辨率。也就是说，分辨率越高，视频信号脉冲的频率越高。

几年来，CRT 显示技术随着计算机的发展已有了很大的变化。早期的显示模式如 CGA、EGA 等的视频信号是 TTL 电平脉冲，显示分辨率较低，目前已基本淘汰。随着 VGA、SVGA、TGA 等扩展模式的不断推出，现在的计算机终端分辨率已大大提高，有的分辨率已达到 1800×1440 甚至更高，视频信号的脉冲频率也由早期的 25MHz 提高到 200MHz。由于信号幅度的大小变化更容易反映图像的灰度和颜色变化的微小区别，现在显示终端的视频信号已由 TTL 电平脉冲改变为 TTL 电平脉冲和模拟信号的混合方式。

直接计算 CRT 视频信息的功率谱密度是非常困难的，尤其是数字与模拟并存的情况。为了分析方便，我们仅仅考虑数字视频信号情况下的视频信号功率谱。设初始视频信号为 V(t)与一个方波信号(周期为 Tb)通过一个“与”电路产生的，其功率谱密度可近似地以下面的公式表示：

$$S_{xx}(F)=A\left(\frac{\mathrm{Sin}\,\pi fT_b}{\pi fT_b}\right)^2 \quad (V^2/\mathrm{Hz})$$

式中：T_b 是视频信号的一个比特脉冲宽度，A 是信号幅度相关的常数。

由于图象的随机性，决定了这些信号是非周期脉冲信号，信号每个脉冲的谐波与宽带电视信号的频谱有明显的相似之处。通过调幅解调方式，只要能够得到视频信号 $S(t)$的频域函数 $S_{xx}(f)$的一个旁瓣的信息，就可以恢复视频信号 $S(t)$。也就是说，$S_{xx}(f)$的一个旁瓣就提供了 $S(t)$足够的信息。这要求有一个较理想的滤波器，其带宽必须大于 $1/T_b$。由于 R、G、B 三色是并行传输，因此复原色彩信号是比较困难的，或者是不可能的。但是它们所组成的灰度变化信息是可以再现的。

1.3 电磁信息泄露的特点

在自然环境条件下，我们测量了数百台计算机系统的电磁辐射情况，包括早期的 AT，AXT 型以及目前的 PⅢ机，各种组装机和国内、外的品牌计算机。从中发现，所有计算机都存在一定的电磁信息泄露情况。从电磁辐射总的情况来看，品牌机要好于组装机，新机型好于老机型，新机型的电磁辐射频率一般高于老的机型。

另外，计算机的电磁辐射还具有以下特点：①电磁辐射信号多数为窄带信号；②辐射信号频率主要信号在几 MHz 到 500MHz 之间，100MHz 以下普遍存在较强的开关电源信号；③辐射频率分布在非常宽的频域范围内，这些频率多是谐波关系；④单个频率点一般只包含部分的视频信息。

2 视频信息的接收还原实验

计算机辐射信号与电视机接收广播电视信号有着很大的不同。电视信号有明显的同步信号，而计算机电磁信息泄露信号分布在非常宽的范围内，并且单个频率点往往只包含部分视频信息，同步信号往往不够完整。我们针对辐射较强的泄露信号，采用传统的接收方式进行了还原实验。

我们使用已有的高灵敏度专业接收机，从中分离出中频信号，通过一个宽带数字滤波器后，对信号进行解调、放大，并加入行、场同步信号，送往显示终端。其中，外加同步信号产生器用于产生行同步和场同步信号，且频率范围可调，分别为 50Hz~150Hz 和 15kHz~100kHz，以保证使图像处于稳定的状态。实验证明，使用这种简单的接收还原方法，可以在距离目标计算机 30 米的位置实现对辐射信号的完全恢复。

要将这些泄露信息还原到理想的结果，还需要做许多复杂的技术工作。首先，由于计算机视频信息电磁辐射属于无意发射，其发射强度和电台信号相比是非常弱的。还原接收的基本条件是接收机的灵敏度要足够高、中频通带要足够宽，并且有较宽的频率覆盖范围。而且，由于视频信号是基带信号，其泄露后的电波形式不同于电视台发射的电视信号的通带信号形式，视频信息高、中、低不同的谐波成分往往分布在非常宽的频域范围内。为了使接收还原出高质量的信息，接收设备必须有相当宽的视频通带。为尽一步提高接收效果，还应该具备强大的数字处理、软件分析等技术，包括高、低通数字滤波器、匹配检波器、图像复原技术等。这些技术是建立在超高速数据采集器、超大容量数据存储器及高速计算机之上的。

3 安全防护

为了尽量减少计算机视频信息电磁泄露的危险，必须采取安全防护措施。目前的防电磁信息泄露技术措施主要有三种：即信号干扰技术、电磁屏蔽技术和 TEMPEST 技术。

3.1 干扰技术

干扰技术又称为伪信息泄露防护技术，是指把干扰器发射出来的电磁波和计算机辐射出来的电磁波混合在一起，以掩盖原泄露信息的内容和特征等，使窃密者即使截获这一混合信号也无法提取其中的信息。

计算机电磁辐射干扰器大致可以分为两种：白噪声干扰器和相关干扰器。白噪声干扰器采用白噪声作为干扰源，对计算机辐射信号进行覆盖。此类干扰器的优点是结构简单、成本低，可以对放置在一起的多台计算机同时起到干扰作用。但存在以下不足：(1)干扰器的干扰信号和计算机的辐射信号之间没有相关联系。窃取者在接收这种白噪声干扰的混合信号后，仍然可以将噪声信号去除掉，从中提取出视频信息；(2)白噪声干扰器的辐

射功率一般比较高，会造成电磁环境污染。由于这些原因，白噪声干扰器目前正逐步被相关干扰器所取代。

计算机视频辐射相关干扰器模仿计算机的显示规律，生成的干扰信号和计算机视频辐射信号具有相同的频谱特性，使辐射信号和干扰信号在空间混合后形成一种复合信号，因而破坏了原辐射的信号形态，使窃收者无法还原其信息。在具体实现过程中，必须考虑以下基本要求：(1)干扰信号与辐射信号频域相同，即干扰信号时钟与信息像素时钟相同；(2)干扰信号与泄露信号时域相同，即有一定的帧周期重复特性；(3)干扰信号自身的保密性要高，信号结构不能是单一的简单模式；(4)能够自动跟踪显示模式的改变，自动适应各种不同模式下工作的显示终端；(5)干扰信号应该具有相当程度的隐蔽性和欺骗性；(6)在保证干扰信号强度符合电磁兼容标准的前提下，必须保证干扰信号有足够的幅度和足够的频率覆盖范围。

相关干扰器的特点决定了相关干扰器和要保护的计算机必须是一对一的配置关系。也就是说，一台相关干扰器只能对一台计算机的视频辐射起到相关保护作用，对于周围的其它计算机只相当于是不相关干扰。由于相关干扰采用的并不是高场强覆盖式原理，其干扰信号的场强值可以做的非常接近或略高于计算机辐射的最大场强值，因而相关干扰器一般不会影响其它电子设备的正常工作。

3.2 屏蔽技术

屏蔽室是一个导电的金属材料制成的大型六面体，它基于“法拉弟笼”的原理（即闭合导电球面体内电位差为零、电波的趋肤效应、反射衰减），能够抑制和阻挡电磁波在空中传播。它具有两种基本功能：(1)阻止外部电磁干扰进入屏蔽室。(2)使屏蔽室内的电磁能量不外泄。屏蔽技术是防止计算机信息泄露的重要手段，使用不同结构和材料制造的屏蔽室，一般可以使电磁波衰减 60~140dB。

屏蔽室的种类很多，按屏蔽材料分，有铜网式、钢板式、电解铜箔式等；按结构分，有单层钢板式、双层钢板式、多层复合式等；按安装形式分，有焊接式、组装式等。影响屏蔽室性能的因素有以下几个方面：(1)屏蔽材料，导电率高的金属材料有助于提高屏蔽室的屏蔽效能；(2) 拼接、焊接工艺，焊接的效果一般好于其它拼接方式；(3)通风窗和屏蔽室门，是屏蔽室的关键组件，直接影响屏蔽室的整体性能；(4)电源滤波器。妨碍屏蔽技术普遍应用的主要原因是造价太高、受安装场地等条件的限制。一般二、三十平方米场地的屏蔽室的造价即需几十至上百万元。因此屏蔽技术较为适用于重要的大型计算机设备或多台小型计算机集中放置的场合。

3.3 TEMPEST 技术

TEMPEST 技术即低辐射技术，是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取防辐射措施，从而达到减少计算机信息泄露的最终目的。目前广泛采用的 TEMPEST 技术有：

(1)屏蔽。屏蔽是 TEMPEST 技术中采取的基本措施。屏蔽的内容非常广泛，电子设备中每个零件、功能模块等都可以分别进行屏蔽。例如，使用屏蔽室、屏蔽柜对整个电子设备的屏蔽，使用隔离仓、屏蔽印制线路板对设备中容易产生辐射的元器件进行屏蔽。

(2)红、黑设备隔离。在安全通信和 TEMPEST 系统中，其基本单元可划为红设备和黑设备两个部分。其中，红设备是指处理保密信息、数据的设备，黑设备是处理非保密信息和数据的设备。红黑单元之间是绝对不允许进行数据传输的。通常是在两者之间建立红/黑界面，避免两单元的直接连接，仅仅实现黑到红设备之间的单向信息传输。

(3)布线与元器件选择。采用多层布线和表面安装技术，尽量减少线路板上走线和元器件引线的长度。尽量选用低速和低功耗逻辑器件，以减少高次谐波。

(4)滤波。使用合适的滤波器，减弱高次谐波，减少线路板上各种传输线之间的辐射和红/黑信号的耦合。

(5)I/O 接口和连接。在输入/输出接口上除了使用滤波器外，还要使用屏蔽电缆，尽量减少电缆的阻抗和失配；使用屏蔽型连接器，减少设备之间的干扰。

(6)TEMPEST 测试技术。即检验电子设备是否符合 TEMPEST 标准。其测试内容并不限于电磁发射的强度，还包括对发射信号内容的分析、鉴别。

生产和使用低辐射计算机设备是防止计算机电磁辐射泄密的根本措施。国外的一些先进国家对 TEMPEST 技术的应用非常重视，对使用在重要场合的计算机设备的辐射要求极为严格。如美国军队在开赴海湾战争前线之前，就将所有的计算机更换成低辐射计算机。国外已能生产出系列化的 TEMPEST 产品，这些产品的造价非常高，一台 TEMPEST 设备的价格往往是同样性能设备的 4~5 倍。

参考文献

1 Van Eck Wim. Electromagnetic Radiation from Video Display Units: And Eavesdropping Risk?, Computers & Security vol 4, 1985

2 Markus G. Kuhn and Ross J. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, University of Cambridge, David Aucsmith (Ed.): Information Hiding 1998

3 Cassi Goodman.An Introduction to TEMPEST,April, 2001

4 http://www.nsa.gov/sso/bao/tep.htm,TEMPEST Endorsement Program,Revised June 25, 2001

5 Mika St?hlberg. The TEMPEST Threat,Helsinki University of Technology,April, 2001

（收稿日期：2001-12-20）