网络环境下计算机硬件安全保障及维护策略分析

张岩　于翠迪　王珏
齐齐哈尔医学院附属第一医院

[摘　要]随着社会经济的快速发展，计算机已广泛应用于各行各业，成为人们生产生活中不可缺少的一部分。然而，由于网络的高度共享性和开放性，导致了网络环境的复杂性和计算机安全问题，所以必须采取科学有效的措施来维护其安全。

[关键词]网络环境；计算机硬件；安全保障；维护策略
【DOI】10.12252/j.issn.2096-6288.2021.10.1677

在网络环境运行背景下，要想为计算机硬件提供安全保障，在实际工作中应使用安全微处理器。同时，对于内存部分，应运行隔离模式，以防止病毒等的侵入。在对硬盘进行加密时，保护计算机所含信息的安全性能，最终为计算机在网络环境中稳定运行提供重要契机，使人们的生活及工作得到有力支撑。

一、网络安全对计算机硬件的重要作用

为保证计算机硬件安全，必须有一个安全的网络环境。然而，网络安全一直未得到重视。直到现代网络的迅速发展和普及，通讯保密也进入了公众的视野。在当今社会，计算机硬件的使用、安全和维护受到了极大的重视，它影响着人们的社会安全、财产安全和个人生活等，所以有很多地方需人们去防范，比如黑客行为、电子谍报、计算机犯罪、信息丢失、网络协议、信息战等。计算机安全不但影响着社会生产及人们生活，还会对国家安全、国防军事、国家政治外交、机关单位的正常运转产生重大影响。如今，作为一个国家经济、政治、文化和社会活动的神经中枢及基本平台，计算机系统一旦遭到破坏，无法运转，将对国家产生重大影响，如国防能力下降、通信系统中断、国家金融体系瘫痪等，严重时甚至导致国家经济崩溃、政治动荡、社会秩序混乱等，后果难以想象。

总之，日常生活中所涉及的计算机硬件面临着严重的威胁，主要来自网络环境。在这种环境下，计算机硬件系统包括处理器、硬盘、路由器等，这些硬件的安全运行保证了计算机的正常工作。一旦计算机在网络环境中处于较低安全状态，就无法保证计算机的安全运行。因此，对硬件来说，网络环境的安全具有重要价值及意义。

二、网络环境下计算机硬件存在的问题

1、计算机病毒。计算机硬件的一个较严重问题是病毒问题，在目前的网络环境下，病毒监控系统还不够完善，对病毒的认识也非常有限，病毒防控需进一步加强。在这方面，计算机病毒监控中心缺乏对全网计算机病毒的统一监控和管理，不可避免地会受到计算机病毒的侵袭。此外，计算机硬件系统无完善的信息安全管理体系。由于网络的重要性，它是一个物理上与外界网络隔离的专用网络。目前，我国整体上缺乏成熟的安全结构体系，相应的安全标准和条例也跟不上，网络信息安全管理还存在一些漏洞，基础设施相对薄弱。网络的安全使用和保护留下了巨大的潜在隐患，可能导致网络病毒的传播，并为计算机外部系统入侵提供机会。

2、安全意识薄弱。互联网和计算机的发展速度远超过了人们的预期，所以在实际使用中，很多人员由于缺乏一定的安全意识，使用计算机时易被不法分子侵入计算机内窃取信息。目前，互联网技术被用于购物、工作、学习和获取资料等，但许多人并未对自己的计算机硬件进行日常维修检查。另外，连接网络时，未养成良好的使用习惯，未经允许下载一些带有木马或病毒的软件，随意点开弹窗，这些行为易触碰到网络病毒，从而威胁到自身计算机硬件的安全。许多计算机用户在使用计算机时未及时发现存在的病毒，因此不会采取有效措施去排除，这是由于许多用户在使用计算机时缺乏一定安全意识造成的。

3、运行环境。自然环境和设备使用条件是计算机硬件需注意的问题。事实上，环境对计算机设备的影响较突出，包括电磁波干扰、磁场干扰、空气湿度干扰等。温度过低和过高会导致硬件设备驱动满及电路板烧毁。此外，湿度也是硬件系统必须注意的问题，潮湿的空气会损坏硬件电路板并烧毁电线。电磁波和电磁场会使计算机硬件无法正常运作。

三、计算机硬件层面的安全保障

1、设计的安全性保障。设计是计算机硬件系统的源头，因此先要从设计角度对计算机硬件的安全性进行分析讨论。设计领域的防护措施包括检测木马系统、不可信任工具、版权集成电路等。木马系统可借助合法程序外衣进入硬件系统，篡改内部芯片系统数据，导致计算机硬件系统瘫痪，大量数据流失。在计算机硬件电路设计中，若增加门电路，在安全检测中会发现一些无法识别的攻击，从而加剧了木马程序对系统的攻击性，严重危及计算机硬件系统的安全。

在正常情况下，攻击计算机硬件系统的木马程序只有在硬件系统进入运营到相关状态下，才能对系统发挥破坏作用，包括改变硬件功能、占用内存资源、复制和传输硬件信息，导致信息数据泄漏。例如，使用A作为硬件木马程序，由简单电流触发，可能包括and门和nand门，还包括电容与xor门。当长期充电条件充足时，该硬件木马程序能在短时间内进入高电平区，主要是激活内置的木马程序功能，改变信息系统的传输信号。对于该木马程序的入侵，可采用反向木马检测技术，比如，功能检测技术（主要是故障测试机）可用于向芯片添加激励电流，并通过检测输出电流来查看内部是否存在硬件木马。

2、合理隔离内存区域。内存是计算机硬件应用的重要组成部分，也是计算机数据存储的主要设备类型。维护内存应用的安全能保证数据的安全性，有效提高计算机系统的安全性。这就需对内存数据进行合理划分，并根据其重要性对内存数据进行隔离处理，以确保数据的安全稳定性。同时，将一些重要且敏感的隐私数据与外界隔离，以避免外部环境的干扰。对于每个内存区域，可设置相应的访问权限设置，只有经授权的用户才能访问内存某一区域，这样能有效控制网络危险环境的因素，尽可能降低内存中数据安全泄漏的风险。

3、做好加密技术。密匙可用来加密整个计算机硬件数据系统，从而保证数据安全性。由于使用加密技术需更多的技巧性，其投入成本也相对较高。此外，还可采用全加密硬盘形式，即对系统的硬盘数据进行加密，可有效防止硬件上非法程序的入侵，保证计算机网络硬件系统的安全运营。然而，全加密硬盘无法加密所有数据，因此这种加密形式需改进。

使用加密技术能将计算机数据转换成相应的密码形式，通过加密技术的算法，这些密码可被再次读取并恢复到原始数据的状态，从而有效保证数据的准确性和安全性。若非法程序被嵌入到传输数据的系统中，可能只会得到一些加密数据，无法获得数据的原始效果，从而提高计算机系统的安全性。目前，有两种形式的加密技术，即对称及非对称。对称是指加密和解密使用同一个系统，无需额外转换，从而实现高效的加密和解密；非对称是指使用两种不同类型的密匙进行加密和解密，此外，计算机硬盘还可创新字符和数字的组合形式，增加密码长度，不断改变交错规律，有效防止硬盘受到干扰。

四、计算机硬件安全维护策略

1、处理器维护。处理器是计算机硬件系统的核心部件，其性能和稳定性直接影响到计算机系统的运行能力。同时，处理器也是保证计算机硬件安全的核心部件，处理器将对工作中的每一步进行加密解密，提高了系统的安全性能，因此，保证计算机处理器的安全稳定工作对保证整个计算机硬件系统的安全非常重要。对处理器来说，极端的温度环境将直接影响其稳定性及运行性能。在正常情况下，处理器的使用易受到高温的影响。尤其在夏季，处理器的发热更为严重，若散热风扇的散热能力不足，易因温度过高而降低使用寿命，甚至损坏处理器。对那些有独特要求、硬件配置高的计算机，由于处理器承担的任务繁重，单位时间内的运行速度较快，处理器会产生大量的热量，必须确保有一个良好的散热系统。可通过构建水冷式散热系统来散热，因这种散热方法比其他散热方法更安静且可循环，还能为机箱中的其他硬件设备提供散热支持，对提高计算机硬件的整体散热起到很好的作用。高压环境也易导致处理器烧毁，这在雷击电流冲击下通常较明显。因此，计算机设备间必须采取防雷措施，并配备专用UPS稳压，以确保处理器稳定安全运行。此外，处理器还可提取和处理加密操作码，以防止外来入侵，提高处理器的安全性。

2、主板的维护。计算机主板是整个计算机硬件系统的基础，是各硬件模块间的沟通桥梁，实现了各硬件模块间的指令交换操作。目前，影响计算机主板安全的问题是静电和形变。主板由电路板、芯片、晶体管组成，并通过自身接口连接各种硬件设备。主板在运行时可能会产生静电，静电不仅会影响主板使用稳定性，还会影响硬件设备的使用寿命，甚至损坏主板中的电路元件。因此，要对计算机采取接地措施，以便主板上的静电电流能及时释放到大地。此外，若主板在外力作用下变形，可能会影响主板的整体物理结构，导致主板损坏。因此，安装主板时，需将其稳定地固定在主机机箱上。安装其他硬件组件时，应控制用力。后期使用时，还应确保机箱不受大的振动和高处跌落等，以确保主板使用的稳定性。

3、硬盘的维护。硬盘是计算机存储器的重要组成部分，属于外部存储器，大部分数据存储在硬盘上。目前，大多数计算机仍使用HDD硬盘，HDD硬盘由机械结构构成，整个机械系统较复杂和精密，因此对外部干扰非常敏感。当受到一定程度的振动时，容易导致磁头碰到盘片，造成磁盘表面损坏，最终损坏硬盘，导致硬盘数据丢失。此外，随着硬盘技术的发展，SSD硬盘也越来越普及，SSD硬盘由电路板、存储颗粒、芯片、电阻元件等组成。因此，对工作环境要求较高，主要是防止静电对电路元件的影响，所以确保接地措施非常重要。无论使用何种类型的硬盘，在硬盘移动中都应尽可能轻拿轻放，避免外力对硬盘内部结构的影响，确保硬盘的使用寿命及稳定运行，确保计算机数据的安全。为防止网络入侵，可加密硬盘中的每个字节。

总之，当前社会在不断发展，国家的进步和经济的发展推动着我国科技的不断创新。正因如此，我国不断地向信息时代迈进，网络系统在当今社会已实现了大面积的覆盖，信息系统已开始应用于各个行业。无论是政府、国有企业还是私营企业都已开始建立自己的信息系统。因此，在目前的形式下，网络环境下计算机硬件的安全保障及防护显得尤为重要。

参考文献

[1]朱泓.网络环境下计算机硬件安全保障及维护策略[J].网络安全技术与应用，2020（09）：7-8.

[2]尹锦屏.网络环境下计算机硬件安全保障及维护策略探讨[J].电脑知识与技术，2020，16（12）：54-55.

[3]郭香柏.基于网络环境下计算机硬件的安全保障和维护策略[J].中国新通信，2019，21（21）：135.