计算机硬件设计安全问题研究

钱 凯 黄 敏
中国电子科技集团公司第五十二研究所 浙江杭州 310013

摘 要：随着时代的发展，信息逐步走进每个人的生活，与人们的生产与生活息息相关，在信息时代下计算机也在迅猛发展，但是随之暴露出来的问题也是不容忽视的，重点引起人们关注的问题就是计算机硬件设计安全问题，因为这关系到人们信息的安全。本文从计算机硬件发展和生产过程中存在的安全问题出发，详细的阐述了计算机硬件的现状，并在内置安全和外置辅助的基础之上提出了一些改善策略。

关键词：计算机硬件；内置完全；外置辅助

Research on the security of computer hardware design

Kai Qian, Min Huang
The 52nd Research Institute of China Electronics Technology Corporation, Hangzhou, Zhejiang 310013

Abstract: With the development of the times, information has gradually entered everyone's life, which is closely related to people's production and life. In the information age, computers are also developing rapidly, but the problems exposed can not be ignored. The key problem that attracts people's attention is the security of computer hardware design because it is related to people's information security. Starting from the development of computer hardware and the security problems existing in the production process, this paper expounds on the current situation of computer hardware in detail and puts forward some improvement strategies based on built-in security and external assistance.

Keywords: computer hardware; Built-in complete; External auxiliary

引言：

计算机是由硬件和软件两个部分组成的，它们保障了计算机的各种功能的实现，硬件和软件二者缺一不可。近几年来，在计算机的技术发展之中，技术人员关注的焦点多是软件开发，而对于硬件的发展则少了许多，这体现出了一定的不平衡性。在计算机技术中，要想取得长足的进步，就不能只注重单方面的发展，硬件的发展应该要跟上软件的开发步伐。硬件方面的发展重要的部分就是安全问题，做好硬件安全的设计工作，是目前摆在计算机技术人员面前的至关重要的一个难题。

作者简介：
钱凯，1985，浙江龙游，汉，本科，工程师，浙江科技学院，电子硬件；
黄敏，1980.8，浙江临海，汉族，男，硕士研究生，杭州电子科技大学，机械电子技术。

1 计算机硬件安全的基本概述

关于计算机的硬件安全领域存在一个特有技术，那就是“加固技术”。我们所用的计算机应用了加固技术以后就可以加强计算机的防腐蚀、防盐雾、防潮、以及抗震的功能。经过加固后的计算机就可以在野外各种恶劣环境中正常工作了，因此加固技术在硬件安全中也是很重要的。计算机除了自己内部硬件产生问题影响安全外，还会有其他的因素对安全问题造成影响。比如：CPU一般都会有一系列的集成性的指令代码，即使这些代码是保密的，但是不能保障是一定安全的。如果计算机的CPU中有着病毒的指令代码或者说陷阱类的代码，其他的设备就可以通过使用无线代码来控制CPU中的这项指令。这样就造成了计算机内部的文件、资料的泄漏，结果往往也是毁灭性的。计算机的系统一时间也会被攻击，内部硬件信息也会被泄密，变得不安全。而最终的硬件泄密还会间接影响到电源的安全，也就有了电源泄密的情况。计算机是由一个个的零部件构成的，其中每一个

零件都是可以被操作的。那么也就有下面的可编程控制芯片，一但这种芯片被他人操作控制，那么计算机也就可以被完全操控。因此目前我们就要保障芯片的安全问题，以此来更好地保护计算机硬件的安全，也使得硬件设计更加安全化[1]。

2 计算机硬件的组成

计算机的硬件部分指的是计算机体系中通过电子、机械和光电元件等等构成的种种物理装置的综合名称。把上述物理的装置依据系统的结构通过规范组合出一整个有机的部分，是计算机的软件运行供给物质的基础。从一个容易理解的方面来说，计算机的硬件功能为输入并且存储程序与数据，同时执行的程序要把数据加工成能够运用的样式。从外在具体的形象方面来说，电脑由主机箱与外部设备组成。主机箱里面的构造主要包括CPU、内存、主板、硬盘驱动器、光盘驱动器、各种扩展卡、连接线、电源等等；外部的设备就包括鼠标、键盘等等。当对于计算机的硬件各个部分设备具有一定的认识后，设计人员才可以在实际的计算机硬件设计过程中对于安全问把握一定的方向，构造出合理的设计方案。

3 计算机硬件的设计安全发展现状

计算机系统中有各种各样的元件，这些构件组合起来构成了物理部件，也就是所谓的计算机硬件。根据分析调查得出，现阶段，计算机硬件发生的安全问题基本上可以分为三种，相应的产生问题的原因也大概能分为三种，包括输入设备、储存介质、输出设备。首先，就输入设备来说，以它为源头产生的计算机硬件安全问题大致有两种，一种是所输入的信息资料、数据资料存在问题引发安全威胁，一般情况下发生这种情况是因为输入的信息存在木马病毒，从而导致计算机系统信息数据安全受到一定程度的威胁。另一种是在输入过程中没有依法进行运作而造成安全问题爆发，一般情况下发生这种情况都会导致计算机内部信息数据被破坏与泄露，后果严重。其次，就储存介质来说，以它为源头产生的安全问题主要是计算机系统内部的储存介质没有给信息资料、数据资料提供安全保障，安全保护层没有搭建起来就会导致信息数据在面临被破坏以及非法拷贝时毫无抵挡之力。最后，就输出设备来说，以它为源头产生的计算机硬件安全问题主要是输出设备自身具备的记忆性能会导致信息数据输出时的操作动作留下痕迹被复制下来，这在一定程度上使得信息数据处于危险状态下。

4 提升计算机硬件安全的具体措施

4.1 确认内置安全

为了提升计算机整体的安全特性，要从计算机硬件的质量方面出发，比如说在新片方向上的设计等等方面，具体而言，可以从下面几个方面着手：在使用芯片之前往往需要对其进行测试，在测试过程中可以在电路上设计一个密钥技术，这种技术不仅可以用于芯片测试，还可以用在芯片的设计中。二是为了保证计算机的整体安全，可以在总线上采取措施，比如设置一些上锁环节。三是当今的PUFID已经得到了广泛的运用，我们可以将它和芯片的设计进行融合，基于此设计出功能性更佳的芯片。四是可以添加一个AES算法，这种加密算法能够提升计算机的严密性，也可以合理的运用这种算法，投入到芯片的设计当中去。

4.2 硬件系统设计的安全方案

第一，在计算机硬件系统中内置安全确认程序。在计算机硬件系统，比如说芯片制造中，可以采用EPIC技术，在芯片的电路中加设密钥，也可以启用加密锁，解锁的形式，以此来达到对于硬件地址的有效保护。结合EPIC技术以及物理不可复制技术，能够实现对计算机安全系统的重要防护。需要将硬件系统经过原始设计以后，通过工具进行编译，然后借助于FUF技术实现有效的复制，对于原始芯片数据进行修改，能够获得安全性能比较高的地址信息。这些地址信息能够和版权之间的信息相互融合，再利用加密算法形成密钥，做好加密模块的建设，对于版图能够做到有效的防护[2]。第二，外部设置的辅助性安全检测措施。对于计算机硬件系统的外置辅助性检测一般采用固定机制，这种机制能够通过信任的密钥，能够通过私人密钥与公共密钥之间形成可信任的连接关系。可以在公共密钥中设置芯片，该芯片是通过加密的信息，能够将这种加密信息储存在计算机硬件系统的集成电路中，形成一种集成信息回路。在计算机硬件系统安全性检测中，外置辅助性设备主要包括验证的芯片以及密钥的存储设备，它能够保证密钥的安全性。在外置辅助验证设备进行运行时，需要利用IFID技术获得内部的回路信息，同时有安全信息芯片进行验证，这样就能够有效保证计算机芯片硬件的安全性能[3]。

4.3 研发时注重安全设计

计算机硬件设计安全问题是多方面存在的，所以在进行计算机安全设计的整个过程里不仅仅需要加强对技术领域的监管检测，还需要关注多方面，避免因为设计方案、设计想法、设计工作者以及实施工作时的重点这些因素产生计算机硬件设计安全问题。除此之外，现阶段存在的一个问题是计算机硬件的设计研发工作者不够

了解计算机硬件，认识计算机硬件的程度不深，所以还需要提高他们对计算机硬件的了解与认识，与此同时，还需要更加注重计算机硬件的设计安全功能。总之，在设计研发中要注意内置以及外置，搞好设计安全，制定计算机硬件设计安全检测制度以及相关检测程序，除此之外，还要注意评估输入设备、储存介质与输出设备，以便发现问题、解决问题。

4.4 服务器设计

计算机系统的正常运行离不开服务器的运行，服务器在运行过程中需要许可身份证。服务器认证需要通过设计伺服框架来实现，这种框架基本上采用多线程方式处理，能够实现伺服进程。只有多线程作业才能够实现服务器功能。需要将多线程进行分解，转化成为多个字线程，有效调整子线程的数据处理的顺序，受到攻击时，能够重新分配，最终达到提升安全性的要求。因此在进行服务器设计时，对于伺服系统可以设定最大的子线程数量，这样做的目的是防止由于子线程系统过多，而对于服务器伺服性能产生不良影响，这也能够防止非法程序利用子线程来对于计算机硬件系统进行攻击。

4.5 检验外置辅助安全

芯片虽然在计算机的整体构件中占比很重，但是仅仅提升芯片的质量还不足以解决计算机的硬件安全问题，这就需要添加外置辅助进行更加深入的研究，而RAS便是这方面的关键技术之一，并且由于这种技术的自身优势，可以在芯片的检验方面起到至关重要的作用，甚至可以将之称为密钥技术的核心内容，它的作用不光是体现在设备的监测方面，还体现在芯片的验证方面[4]。

4.6 研发过程要注重创新

针对于目前出现的计算机硬件设计的安全类问题还在于现代技术水平没有达到所需的要求。因此，要想真正的解决此类安全问题，就要在研发的过程中进行创新，来完善目前有缺陷的计算机硬件的安全设计技术。

5 结束语

经过以上对计算机硬件方面存在的问题进行了讲述，总结出计算的硬件安全对计算机和互联网的信息安全具有重要意义，它的安全直接关系到计算机运用等多个方面的发展，也对人们的日常生活具有很大的影响。虽然近些年来我国在这方面投入了较大的精力，但是整体效果却是微乎其微，这就意味着需要这方面的相关工作人员加大计算机硬件安全的维护力度，使得计算机能够得到安全、快速的发展。

参考文献：

[1]苏云飞.计算机硬件设计安全问题研究[J].计算机产品与流通，2019（01）：25.

[2]唐淑珍.计算机硬件设计安全问题研究[J].信息与电脑（理论版），2017（20）：26-28.

[3]鲍静.计算机硬件设计安全问题分析[J].中国安全防范认证，2017（04）：50-54.

[4]徐敏.计算机硬件设计安全问题研究[J].工程技术：文摘版，2016（8）：00104