

# 关于计算机硬件设计安全问题的思考

马佳宾<sup>1</sup>, 郑云峻<sup>1</sup>, 武丹<sup>2</sup>

(1.山东濠鹏信息科技有限公司, 山东 济南 250101; 2.浪潮电子信息产业股份有限公司, 山东 济南 250101)

**摘要:** 进入信息化时代, 随着我国高科技手段的发展, 人们在注重生活质量的同时, 更加注重对个人隐私的保护。但是, 不断加强计算机硬件的信息化技术手段对于个人信息保护还远远不够, 黑客及其他病毒软件已经侵入人们的生活, 个人信息随时随地都可能发生泄露, 导致个人财产等造成一定的损失。因此, 计算机既要有硬件方面的保护, 也要有软件方面的保护。同时, 要进行多重防御和隐私加密, 提高计算机安全保护等级, 让计算机用户的信息更加隐秘, 避免被黑客窃取。

**关键词:** 计算机硬件; 设计安全; 思考

**中图分类号:** TP3

**文献标识码:** A

**文章编号:** 1674-1064 (2022) 04-085-03

**DOI:** 10.12310/j.issn.1674-1064.2022.04.029

## 1 计算机硬件安全发展现状

### 1.1 目前发展

计算机的安全主要体现在软件、硬件、通信三个方面, 如果从三个方面不断提高和创新, 那么在用户隐私保护方面就会取得很大的进步。计算机网络具有信息范围广的特点, 在信息化时代, 每一个角落都有可能存在用户的信息, 且信息非常零散, 很容易泄露, 计算机网络可以通过多种方式进行信息的传导、输入和输出, 在这些方面要对这些复杂的信息传导方式进行归类并提出合适的解决方法。在浏览网页的时候, 信息可能就会在不经意间泄露, 因此, 要不断提高计算机硬件的防御能力, 提高保密等级。

各国目前对软件的开发已经达到了一定的程度, 很难再得到提高, 软件也达到了比较高的保密等级, 因此, 对软件的开发可以稍微延缓, 对于硬件的开发则要不断创新, 才能不断提高硬件保密等级。因此, 提高计算机安全性的主要任务就落在了硬件方面<sup>[1]</sup>。

### 1.2 长远发展

计算机的发展是持续且快速的, 要从长远的角度考虑计算机硬件的安全设计。随着信息化时代的到来, 人们的信息通常在网上就可以简单查到, 因此, 更加注重信息安全。目前, 有许多防护软件出台, 从长远的角度考虑, 硬件是最基本、最重要且可以提高计算机的硬件安全性的一个方面, 需要不断创新和发展, 需要投入大量的设计性思维和设计人才, 许多人在使用计算机时, 由于操作不当, 可能导致木马病毒等病毒入侵电脑, 导致个人信息被木马病毒读取, 从未发生个人信息泄露问题。

操作计算机时, 在浏览网页或者下载软件的过程中, 导致木马病毒在间隙中入侵电脑, 长此以往会窃取个人信息, 在现阶段缺乏对计算机硬件方面的特殊保护, 导致其无法抵抗恶意攻击及非法拷贝等, 会导致信息泄露, 导致网络安全

性的不断降低。进入信息化的时代, 硬件的发展如果不能紧跟时代的发展, 那么传统的硬件设计思维必将被时代淘汰。因此, 硬件的发展必须具有创新性, 需要有大量创新型人才投入到硬件安全设计中, 推动计算机硬件得到快速发展和不断进步。

在信息化时代, 人们对自身信息化的要求越来越高, 需要更高的安全等级才能符合当今以及未来人们计算机的使用要求。但是, 由于信息泄露问题, 会导致一系列问题出现。在未来, 更加需要防护等级更高的计算机硬件, 才能适应社会的发展, 因此, 要从最基本的设计思路出发, 拓宽设计者的设计思路, 做好硬件设计创新, 符合未来计算机的设计要求, 才能在硬件方面实现技术性的快速提高, 进而提高硬件的防护等级, 保障未来电脑行业的发展。

## 2 加强计算机硬件设计安全的措施

### 2.1 加强硬件内置安全

硬件本身有一定抵抗病毒的作用, 但仍然会发生信息泄露。计算机硬件是安全防护的重要部分, 因此要在硬件设计过程中, 提高硬件抵抗外界信息侵袭的能力, 减少信息泄露。硬件设计要结合多种技术, 提高硬件的综合性, 能在外来病毒入侵时产生防御, 让病毒无法入侵, 硬件的内置安全还要与硬件的外置辅助硬件结合使用, 才会提高硬件的安全性。在内置的硬件在外来信息入侵时, 实现双重防御, 这样可以防止黑客以及病毒窃取用户信息, 提高硬件的安全性。当信息泄露时, 其他人可以利用用户信息进行非法的贷款以及实施其他违法行为, 这样就会导致个人财产的巨大损失以及个人身份信息泄露。

硬件作为计算机的主要组成部分, 对抵抗病毒以及黑客的入侵起到了至关重要的作用, 而硬件研发过程相对来说比较复杂, 由多个环节组成, 每一个环节的研发质量决定了硬件的最终的综合性能。因此, 在硬件研发过程中, 要加强对



图1 硬件研发环节



图2 计算机用户在网络上复制和传输信息示意图

硬件研发每一个环节的管控，从而保证硬件的质量。硬件研发环节如图1所示。

从基础上做好硬件研发，当硬件组装在计算机内的时候，要保证硬件可以充分发挥其防御病毒以及黑客入侵的作用，保护用户隐私和身份信息。当硬件研发完成后，要对硬件的安全性进行严格测试，保证硬件的设计没有瑕疵，既保证硬件的性能，又提高其防御病毒入侵的作用。在这一过程中，要对硬件整个研发过程进行综合评价，保证硬件的研发思路没有发生大方向的偏离，确保硬件的综合性能。当硬件大批量制造之后，还要对硬件进行逐个检测，排除瑕疵品，保证每一个硬件的质量，在安装在电脑上能够正常使用，保证电脑的综合性能。

如今人们发现，计算机用户的信息在网络上就可以进行简单的复制和传输，如图2所示。病毒和黑客可以通过各种渠道获取用户信息，不仅要通过软件进行防护，而且要通过计算机硬件进行防护。计算机硬件最根本的安全来自其内部硬件的安全设计，从内部出发可以解决其安全性能，但从内部出发需要极其复杂、极具创新性的结构才能保证安全性能得到提高，因此，硬件内置安全的设计相对来说是比较复杂的，长此以往，硬件内部的安全仍需要不断创新和发展，加强硬件内部安全设计是目前的首要任务<sup>[2]</sup>。

## 2.2 将安全设计融入硬件研发

硬件防护一般要通过内置和外置的硬件防护同时进行，这样的防护更加具有安全性，对硬件提出了更高的要求。在硬件的研发过程中，需要极高的制造技术，对硬件具有硬性要求，可以提高硬件质量，提高硬件的防护能力。在这一过程中，在硬件无法突破瓶颈时，要将硬件设计的安全理念与硬件技术相结合，提高硬件的制造水平和硬件的防护功能。

为了实现硬件与软件同时抵抗网络上的病毒与黑客入侵，首先要提高设计人员的安全意识。现阶段，设计人员更加注重硬件的设计性能，在信息化飞速发展的时代，只有具有高性能的硬件设施，计算机才会表现得更好。在这一基础上，要对硬件设计人员进行严格的培训，增强他们对硬件安全理念的重视，关注硬件安全性设计。

设计理念决定了硬件发展的长远道路，先进的设计理念要与硬件制造相结合，将硬件安全融入硬件设计，进一步提高硬件安全性能。在计算机发展中，对计算机的硬件要求极其严格，一味地提高计算机的硬件性能会在很大程度上忽视硬件的安全性，因此，在提高计算机硬件性能的基础上，应更加侧重于提高计算机安全性，使其不仅具有极其强大的性能，更具有极其强大的安全性能，不断完善计算机的发展。

现阶段，一些硬件设计依然沿用传统的安全思维，导致

硬件不能防护病毒以及不能避免窃取用户信息的问题。硬件设计如果不融入安全设计思维,那么在硬件的使用过程中就会出现一定的问题,不能很好地维护用户信息安全。安全思维则是建立在用户信息上的设计思维,防止用户在浏览网页以及黑客入侵的情况下出现信息泄露问题。为提高硬件的安全性能,要将安全设计思维融入设计,保障硬件设计具有更高的防护等级,防止信息泄露和黑客入侵。因此,将安全思维融入硬件设计是必然趋势,也是未来计算机长期发展中对硬件的必要要求<sup>[3]</sup>。

### 2.3 硬件安全技术创新

计算机硬件安全方面存在很多的漏洞需要填补,但是传统方法只能解决简单的技术漏洞,抵御简单的病毒和部分黑客的入侵,信息泄露问题仍然会出现,进而导致一系列问题的发生。因此,传统的计算机硬件设计思维要及时更新,使之符合当今信息时代的发展。

在硬件安全先进技术的引进方面,要结合多种硬件的安全技术设计思路综合考虑,提出一条综合性能良好、安全性能得到显著提升的设计思路,因此,要结合各种品牌的硬件研发技术,拓展更加先进的研发思维,保证硬件安全的技术能够得到显著突破。与此同时,需要引进先进技术人才,在硬件研发上不断创新,提出新方法、新举措,硬件安全技术的创新需要大量的先进人才付出更多的努力,以往传统的设计思维已经不适用于当今时代的发展,需要更加先进的思维,不断创新,不断进步,这样才能满足新时代硬件发展的新要求。

对此,首先应查找出现漏洞的原因,并进行全面分析,需要先进的人才进行创新研究。信息泄露的原因非常复杂,很多因素都会导致信息泄露,因此,要对漏洞进行全方位检测,使用先进技术、引进先进人才是硬件创新并提高安全性的主要方法。为改变传统的硬件安全设计思维方法,需要培养出具有创新性的人才投入到安全技术创新中,促进硬件安全技术得到快速发展和提高。

硬件在目前传统的设计思路,不能满足未来计算机的发展需求。为保障计算机使用的安全性,就会导致传统的硬件研发技术停滞不前,因此,要加强硬件研发,不断创新技术,在目前的基础上转变和提高硬件设计创新思维,才能符合未来计算机的发展。硬件的安全性不仅取决于硬件本身的质量,而且取决于设计人员的设计思维及设计方法。因此,要不断研发硬件制造材料,在此基础上持续创新,并在提高硬件质量的同时,改变传统的设计方法及研究方法,由此,才能提高硬件安全性,为硬件的长期发展奠定基础<sup>[4]</sup>。

### 2.4 培养人才,提高设计水平

硬件的安全性及硬件设计的根本动力来源于人才,硬件生产的每个环节都融入了设计人员的设计思路。因此,需要

我国高等院校加大投入力度,加强计算机专业的研发力度,加强专业人才的培养,提高设计人员的技术水平,帮助他们培养和创新硬件安全设计的思路。

安全思维是从思维水平上进行发展和研究的,因此,为了推动高校加大人才培养力度,国家要及时出台各种支持政策,以学科发展特点和学生学习特点为基础,通过各种创新性活动,提高学生的思维高度,把学生培养成具有独立思考、创新思维的人才,进一步提高高校培养人才的质量,提高计算机硬件安全水平。

与此同时,各计算机生产企业、研发机构也应提高设计人员的设计思维,进一步提高计算机硬件的安全性能。在招聘专业人才时,要注重创新设计理念和思路,由企业举办专业技术培训,让设计人员明确企业需要什么样的人、需要怎样的硬件设计,确保符合未来计算机硬件安全性的设计要求。同时,为计算机产业的发展做好人才资源储备。

随着科技的不断创新,人才储备量越来越大,但是高质量人才相对来说不能满足市场的需求,研发机构需要从各个高校以及社会上招聘高质量人才。在这样的情况下,加快解决计算机硬件设计安全问题,只有拥有充足的人才储备,拥有更加强大的研发团队,才能保证硬件安全设计思路不断创新和进步,从而有效解决计算机硬件安全问题。

## 3 结语

计算机硬件包括多个方面,硬件类型比较复杂,包括内部硬件以及外部硬件的辅助检测,因此,硬件创新非常重要但极具难度。计算机硬件设计与技术创新必须紧跟时代发展步伐,否则,信息泄露情况会变得越来越严重。基于此,在提高和创新计算机硬件安全的研究道路上,不仅要加强计算机硬件技术设计创新,而且培养大量的创新型人才投入到硬件设计中,通过硬件设计安全与软件设计安全相结合,提高计算机的安全性能和运行质量,确保计算机硬件安全,推动计算机产业不断创新发展。

## 参考文献

- [1] 马伟勃.计算机硬件设计安全问题的若干研究论述[J].科技创新与应用,2016(31):110.
- [2] 刘宁.计算机硬件设计安全问题及对策探究[J].科学中国人,2016(4z):14.
- [3] 毕海嘉.网络环境下计算机硬件安全保障及维护策略的思考[J].电子世界,2018(12):88-89.
- [4] 戴金.计算机硬件设计安全问题研究[J].计算机产品与流通,2019(9):23.