《计算科学导论课程总结报告》

### 一、引言

随着互联网的高速发展，计算机的地位也不断提高，这也是我在高考后选择计算机科学与技术作为我的专业的主要原因。

在炎热的8月，我收到了中国石油大学（华东）计算机科学与技术专业的录取通知书，从那开始，我也踏上了这条光明的道路。

九月是一个令人激动的日子，我踏入了我为此奋斗了三年之久的高校校园。不久后，开始了我的学习。

我十分幸运，遇到了孙运雷副教授，第一次上计算机科学导论课，我昏昏欲睡，我实在不理解计算机为何会跟哲学扯上关系。随着进一步的学习，我慢慢地发现，孙运雷副教授是一位知识渊博的老师，他了解哲学、历史和文学，当然还有必不可少的计算机知识。我现在依然清楚地记得，我被孙教授抽到回答的第一个问题：“为什么书禁锢了人的思想，我们却还要读书？”，我也尝试从孙教授的角度去思考，他究竟要我们回答什么？慢慢的，我知道了，他要的从来就不是什么标准答案，他要的是我们会独立思考，拥有自己的思想，还有科学严谨的学习、科研态度。

在接触了孙教授后，我明显地感觉到，我有很大的进步，不是技术，而是思想。结课后，我也了解了计算机的基本概念和知识，脑海里也浮现了许多疑问，这将是接下来我们要讨论的。

### 二、认识与体会

为了更加准确地认识计算科学导论，我查阅了许多资料[1-2]。计算科学是对描述和变换信息的算法过程，包括其理论、分析、设计、效率分析、实现和应用的系统研究。全部计算机科学的基本问题：什么能有效地自动进行，什么不能有效地自动进行。现在，计算已成为继理论、实验、之后的第三种科学形态。作为计算机科学与技术专业的入门课程，高层次抽象是本课程的特点，本课程将本专业的各门主干课程，如操作系统、数据结构、汇编语言、编译原理、数据库系统和计算机网络等内容“浓缩起来”。其特点是概括性极强，对于学生，特别是本科生来说，入门具有一定难度。所以教授的教学方式十分重要，若偏向于理论，学生课能难以接受；若偏向于技术，又没有必要。所以两者之间的权衡是十分重要的。本课程的主要目的有两方面，一是让学生了解本专业的发展历程以及先辈们做出的杰出贡献，了解计算科学的本质问题；二是介绍计算机科学与技术专业的现状以及发展趋势，让本专业学生了解应该掌握哪些知识，应该具备什么样的知识结构与能力。

种种迹象表明，全球信息化的发展，正在从基于计算机科学向着基于计算科学转变。计算科学与计算机科学虽密不可分，但是一字之差，内涵上却有重大的差异。《信息化:从计算机科学到计算科学》中指出，计算科学是融合性科学，它融合了三个不同的元素：1.算法、建模和模拟软件；2.计算机与信息科学；3.计算的基础设施。它们都在不同的领域中发挥着重要的作用，提升了各个行业的科学水平和发展速度。著名计算机科学家艾兹赫尔·戴克斯特拉曾经指出：“计算机科学并不只是关于计算机，就像天文学并不只是关于望远镜一样。”而计算机科学有四个主要领域：计算理论，算法与数据结构，编程方法与编程语言，以及计算机组成与架构。与计算科学不同的是，计算机科学更加偏向于与计算机，而计算科学更加偏向于计算，即数学。但二者都毫无疑问地促进了信息发展。

在《计算科学导论》中，有关于高级语言的内容，其主要阐述了高级程序设计语言地发展历程、现状以及未来趋势，并未涉及任何具体的技术与方法，与课程程序设计不同的是，程序设计更加偏向与相关高级语言的技术与方法，而计算科学导论只是给我们构建一个框架，让我们理解高级语言的内涵及历史。若只是浮于表面，学习其语法特性，那将与小学生无异。

总而言之，计算科学导论是容易被许多学生忽视，但是必不可少的一门课程。

### 三、对于杀毒软件进一步的思考

#### 3.1 杀毒软件的现状

杀毒软件[4]使用于侦测、移除电脑病毒、电脑蠕虫和特洛伊木马程序。杀毒软件通常含有即时程序监控识别、恶意程序扫描和清除和自动更新病毒数据库等功能，有的杀毒软件附加损害恢复等功能，是电脑防御系统（包含杀毒软件，防火墙，特洛伊木马程序和其他恶意软件的防护及删除程序，入侵防御系统等）的重要组成。

国内的安全厂商有火绒安全、奇虎360、金山毒霸、瑞星、江民科技和微点等等。目前为止，奇虎360是功能最完善，最受用户欢迎，杀毒效果最好，同时误杀率最低的杀毒软件之一。

国外的安全厂商有卡巴斯基、比特梵德、ESET、诺顿、Avast、趋势科技、Avira、迈克菲和AVG等等。2019年，卡巴斯基产品共计参加86次独立评测。我们的产品荣获64次第一名，并取得70次前三名的佳绩­[5]。比特梵德连续多年在国际权威测评机构AV-Test和AV-Comparatives的测试中排名第一。经过本人的使用（使用时间长短不一，并未带着可以测评的心理使用），得出以下结论：卡巴斯基在18年以前占用系统资源较多，18年后经过优化有很大改进，查杀率高，误报率较低；比特梵德占用系统资源较多，查杀率高，误报率较低；ESET是目前我使用过的最安静的杀毒软件，查杀率一般，误报率低。但是国外杀毒软件都存在一个普遍问题：面对国内的一些病毒或木马程序往往不会有反应。

目前反病毒公司普遍采用的反病毒技术是特征值扫描技术，即从病毒代码中人工提取出该病毒的特征值，该特征值就代表了该系列病毒，反病毒公司再将该特征码上传入自家的病毒库中，用户使用时，反病毒软件会将扫描对象与病毒库中事先提取出的病毒特征值进行比对，若比对成功，则将该对象视为该类病毒。

传统反病毒技术处于“病毒出现---提交---分析---升级---再出现---提交……”的循环之中[7]，始终无法及时查杀新病毒。除此之外，若反病毒公司的病毒库并没有某病毒的特征代码或用户并未及时升级病毒库，那么杀软遇到该病毒也将无法识别。病毒方面，越来越多的不法分子对恶意代码使用变形技术来躲避杀毒软件的查杀，对反病毒公司的病毒库升级工作带来了巨大压力。

#### 3.2 发展趋势

##### 3.2.1 云安全

云安全是指基于云计算商业模式应用的安全软件、硬件、用户、机构、安全云平台的总称。云安全通过网状的大量客户端对网络中软件的行为进行监测，获取互联网中木马、恶意程序的最新信息，并发送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

随着信息时代的发张，病毒种类越发繁多，病毒的数量也与日俱增。病毒库的大小也不断上升，病毒库更新速度也越来越快，用户可能会反感更新。采用传统杀毒方式不仅速度越来越慢，面对一些新病毒也无能为力。所以仍然只通过传统杀毒技术来保护用户的计算机安全是远远不够的。此时云安全诞生了。

云安全的技术特点有[8]：查杀效率更高并且查杀能力更强。通过对已经接入互联网的终端中的所有软件进行分析并监测，获取病毒的最新情况，并实时将解决方案发到客户端上进行防护。省去了传统杀毒技术的病毒提交、人工提取病毒特征码等繁琐步骤，大大提升了病毒查杀效率和速度。

云安全将使得每一台计算机都可以称为病毒的监测点[9]，客户端甚至不需要包含完整的病毒库，杀毒厂商只需要将病毒库设置在服务器，杀毒软件将可疑代码或软件提交至服务器进行比对，若计算机处于非联机状态，可将可疑代码或软件隔离，待用户手动操作，或联机后自动提交至服务器进行分析。

目前，趋势科技推出了PC-cillin 2021云端版，其采用了全球独家主动式云端防病毒技术，让电脑无负担更轻快，将80%的病毒特征码移入云端，大幅减少了电脑或手机因为更新病毒库所带来的负担。

##### 3.2.2 大数据的建设与共享

中国最大的网络安全公司360集团董事长兼CEO周鸿祎6日接受《环球时报》记者专访时表示，伴随着5G、工业互联网、车联网等新技术的应用，有国家背景的黑客组织发起的网络战已经成为中国面临的头等安全威胁。他认为，这类网络战的威胁甚至比核战争更大。

周鸿祎介绍说，数字时代下网络战成首选，其第一个特点是不宣而战。“网络战每天都在发生，不需要等到两国宣战。别国如果某天宣布对中国发起网络攻击，相关的潜伏、渗透工作之前就已经完成。”其次，新型网络战已经具备实体攻击能力，新型网络战的第三个特点是极其隐秘。

如何应对这样的网络战？周鸿祎建议说，大数据是看见网络战和APT（高级可持续威胁攻击）的基础，所以一定要重视网络大数据的建设。第二，目前的物联网设备相互独立，需要像部队作战的数据链，要建立发现漏洞和打补丁的情报标准，将发现的各种敌情通过数据链让所有安全厂商实现信息互通。

总而言之，在万物互联的时代，网络安全就是国家安全，为了保障国家安全，最好的做法之一就是重视大数据的建设，注重积累网络攻防知识。共享漏洞与补丁，避免传统网络安全防御思路“头痛医头，脚痛医脚”给网络安全甚至国家安全带来重大隐患。

##### 3.2.3 机器学习识别技术[10]

在我们小组的演讲中提到，利用人工智能技术实现对病毒的防控，并且我在答辩中也阐述了较为详细的操作：机器学习识别技术既可以做静态样本的二进制分析，又可以运用在沙箱动态行为分析当中，是为内容/行为+算法模式。伴随着深度学习的急速发展，各家厂商也开始尝试运用深度学习技术来识别病毒特征，如瀚思科技中的基于深度学习的二进制恶意样本检测[11]。具体内容在参考文献[11]中已经阐述得非常清楚，我就不做赘述。以下是我的适当总结。

运用深度学习技术有许多好处：1.效果足够好。2.样本性质适合。3.样本量够多。4.避免人工特征选取。但是，就目前而言，运用深度学习技术做静态样本的二进制分析也有许多难题，例如将输入的图像，或是语言，或是文字如何转化为二进制文件？选取什么样的网络结构？不过我相信，瀚思科技一定会突破重围，掌握杀软的新科技。

##### 3.2.4 主动防御技术[7]

主动防御技术是近几年来网络安全领域新兴的一个技术，它根据程序的行为来判断该程序是否为病毒或蠕虫等，从而进行防御，这种技术不需要传统杀毒技术所依赖的“病毒特征码”。

早在2004年，国外杀毒软件厂商Panda就已经推出了一款具有主动防御技术的软件：Truprevent，这一款软件也让Panda公司成为了欧洲第一位计算机安全产品公司同时也是世界上在计算机安全领域成长最快的公司。国内的主动防御技术起步较晚，国内民用级最早的主动防御技术是东方微点开发的，是刘旭先生（曾经微星的总工程师）带头开发的，历经三年磨难，于2008年6月25日正式上市。[12]目前拥有较为成熟的主动防御技术的安全厂商有卡巴斯基、赛门铁克、比特梵德等等，其中卡巴斯基的HIPS（基于主机的入侵防御系统）较为出色。

传统杀毒技术是通过识别程序的特征码来判断该程序是否为病毒的，而目前许多病毒都会使用加壳技术（可以理解为对执行文件进行了加密）来逃避杀软的查杀。而此时，主动防御技术就能对传统杀毒技术的不足做一个补充，但是由于技术和病毒特性的原因，还不能做到完全取代。所以目前市面上大多民用杀毒软件都同时包含传统杀毒技术和主动防御技术。但是主动防御技术以后或许将取代传统杀毒技术，成为主要的杀毒技术。

### 四、总结

通过一个学期的学习，我对计算科学有了大致的了解，同时我也对计算机科学与技术专业的学习方向、学习方法以及学习内容也有了一定的了解。

我认为，通过演讲和写报告的方式对计算科学导论学习评分是非常好的，这给我们提供了在大学为数不多的演讲机会和团队合作机会，同时也让我们学会辨别文献，什么是权威的文献，什么是没有意义的文献，以及查找文献的途径。

在上课时，你会偶尔向我们提问，而我，也能从这学到东西，面对一个问题，我们首先要思考的不是它的正确答案是什么，因为在这个世界上，有正确答案的问题也许不是那么多，我们首先要思考的，是这个问题的真实性和存在性，以及存在的条件（这是我从我被第一次叫起来提问中总结出来的），我愿意称这些为“问题的限制条件”，在思考完这些“限制条件”后，我们心中往往就有了一个答案，这个答案也许不是正确的，但至少对自己来说是有意义的，是经过自己思考后得出的相对比较严谨的答案。

在我上完这门课后，确实实现了计算科学导论的目的，我已经被计算机科学与技术专业深深吸引，而我也对未来有了一定的想法与规划（这将在我的职业规划中详细说明），并且也对计算机科学与技术专业学习路径有了一定的框架，相信在未来的学习中，我会因此更加轻松，更急热爱计算机科学与技术专业。

### 五、参考文献

[1] 赵致琢.计算机科学导论[M].科学出版社

[2] 唐培和.计算学科导论研究[A].高等教育研究学报

[3] 周宏仁.信息化:从计算机科学到计算科学[J].中国科学院院刊

[4] <https://zh.wikipedia.org/zh-hans/%E6%9D%80%E6%AF%92%E8%BD%AF%E4%BB%B6>

[5] <https://www.kaspersky.com.cn/top3>

[6] <http://www.bitdefender-cn.com/>

[7] 向林泓.主动防御技术的研究和实现[D].电子科技大学

[8] 郭思梦.网络时代的云安全技术分析[A].中国新通信

[9] 任翔.基于云安全技术的防病毒软件商业模式的分析与研究[D].北京邮电大学

[10] <https://zh.wikipedia.org/wiki/%E6%9D%80%E6%AF%92%E8%BD%AF%E4%BB%B6>

[11] <http://wurui.cc/tech/malware-detection-by-deep-learning/>

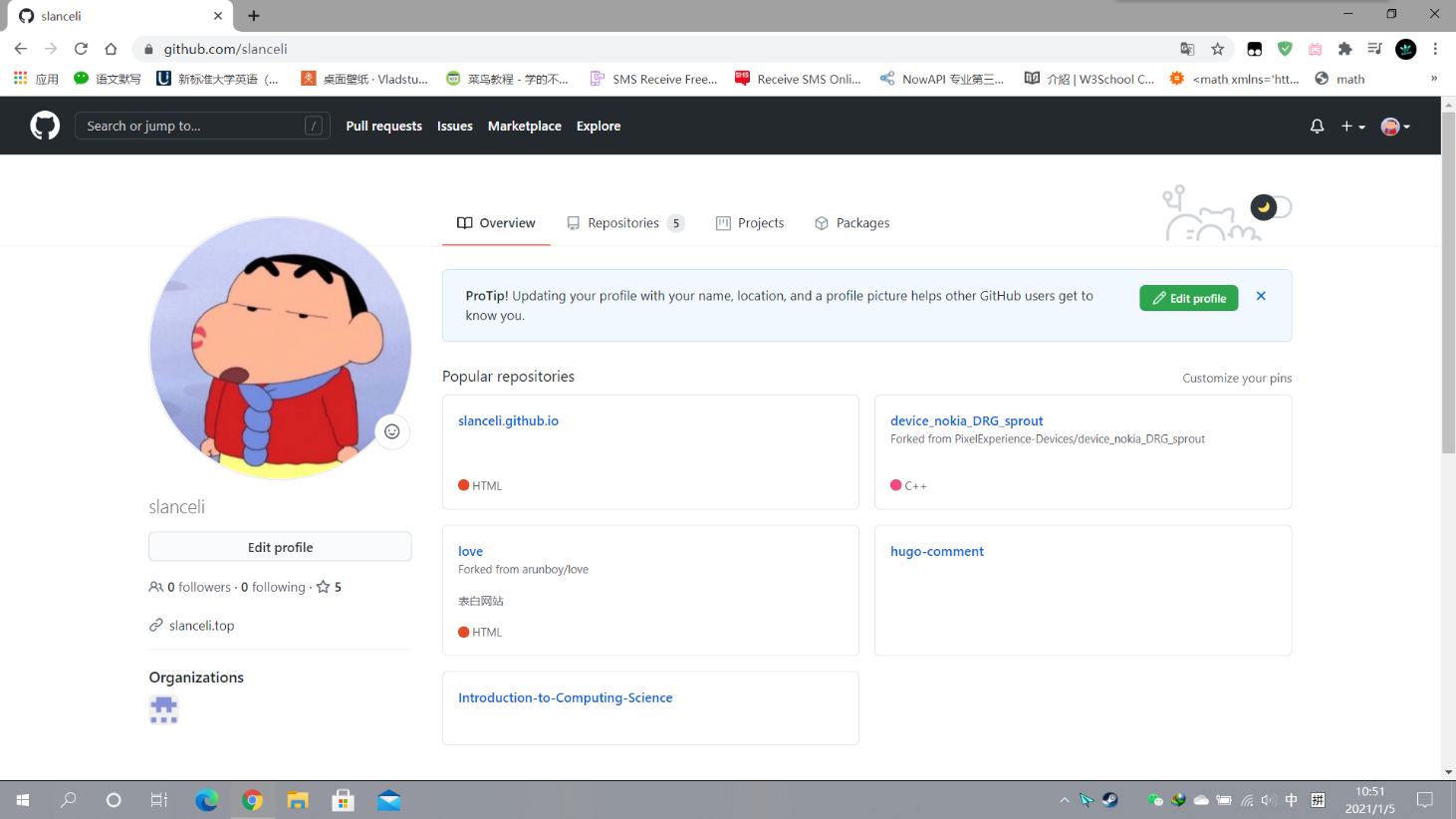
[12] <http://bbs.micropoint.com.cn/showthread.asp?tid=35868>

### 六、附录

#### 6.1 Github

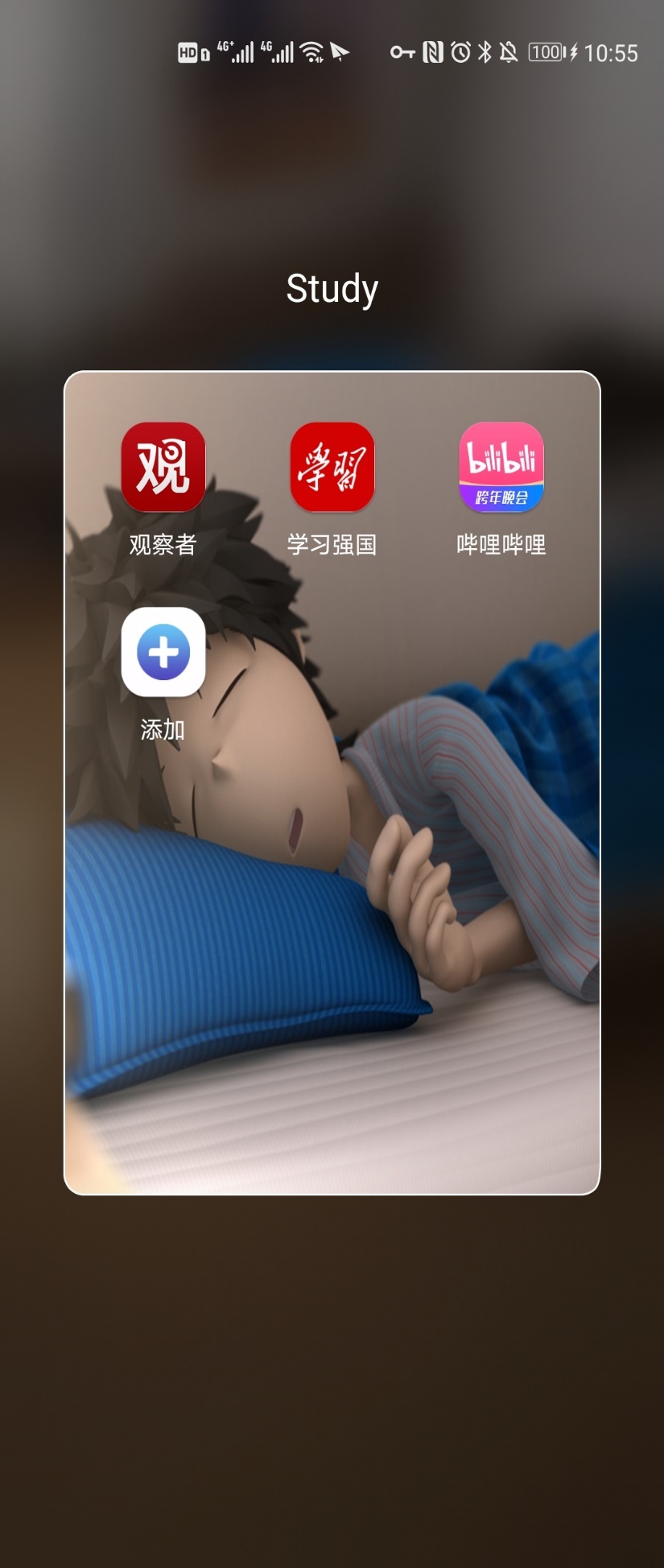
网址：<https://github.com/slanceli>

截图：



课程相关资料网址：<https://github.com/slanceli/Introduction-to-Computing-Science>

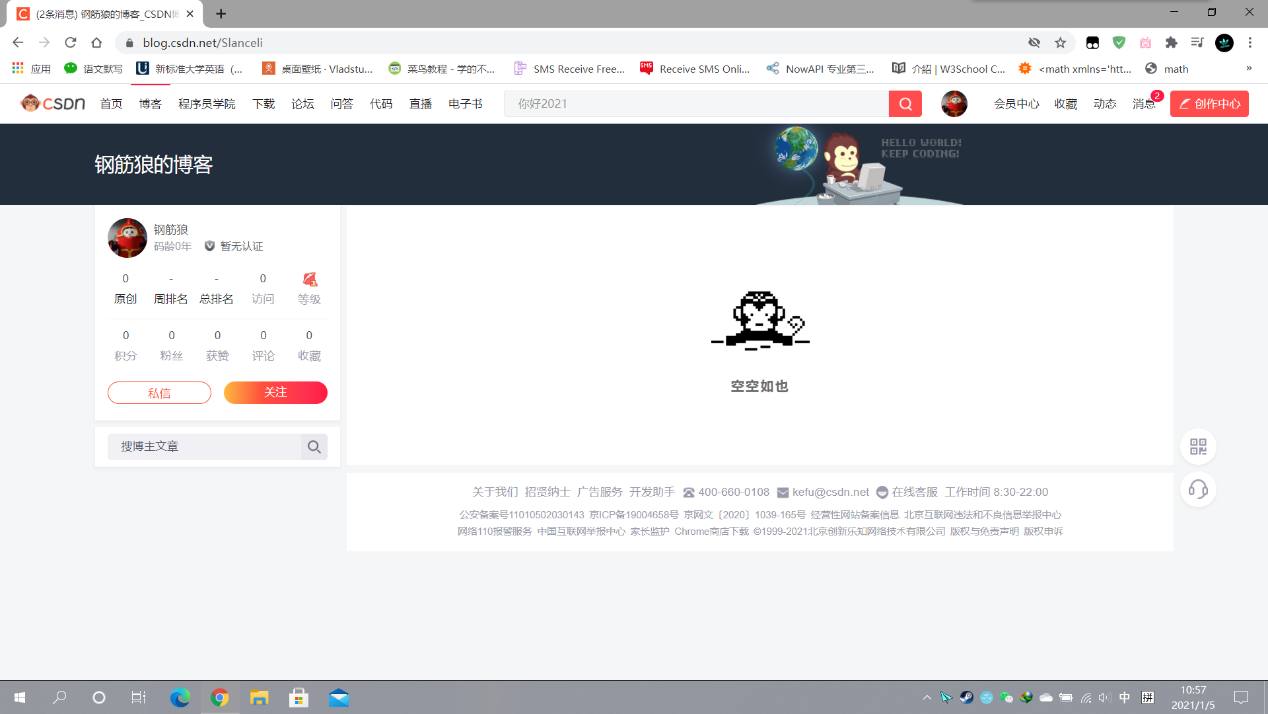
#### 6.2 观察者、学习强国、Bilibili的APP截图



#### 6.3 CSDN

网址：<https://blog.csdn.net/Slanceli?spm=1000.2115.3001.5343>

账户：钢筋狼

截图：

#### 6.4 小木虫

网址：<http://muchong.com/bbs/index.php>

截图：

