PAPER 论 GNU/Linux

摘自:
2019 11 月下,P17-18
12 月下,2020 1 月上,P20-22

近期中帝当局的一系列“网络安全”法律所蕴含的强盗逻辑以及我们该如何应对

(编者按:如果 1+1=2 会妨碍资本家获取利润，那么资产阶级一定会想尽一切办法禁之而后快。中帝当局所出台的各类网络安全法律便是这个极度夸张例子的现实体现，如果资产阶级发现哪种科技的发展会威胁到其统治地位进而威胁到其安心剥削，那么显然，其当然会毫不犹豫地阻止这种科技发展。)

这几日，特色当局先是放出个《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，其中说：

“可以认定行为人明知他人利用信息网络实施犯罪……（包括：）频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的（属于犯罪）”；

然后又放出个《中华人民共和国密码法》规定：

“第二十七条法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

……

第三十七条关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。”

如果资产阶级发现哪种科技的发展会威胁到其统治地位进而威胁到其安心剥削，那么显然，其当然会毫不犹豫地阻止这种科技发展。

公然垄断对于密码研究与测试的权利，没有资质的个人甚至会因为评估某密码协议的安全性而因此犯法。

这一系列事件，从科学性的角度看待，无疑是反科学的；而从革命活动的观点看待，也正体现了网络为革命的准备所提供的便利已经影响到特色的反动统治。

概括来说，由于革命准备活动与网络的结合使得特色政府不得不采取反科学的做法。

这一系列法律规定所体现的强盗逻辑

这次“两高”关于网络犯罪的司法解释，公然把为提供加密通讯这一很正当的行为说成犯罪，已经到了反智的地步了。

不错，利用加密通讯是能犯罪，但在资产阶级民主的范畴内，保护个人的隐私权也是重要内容。不让提供加密通讯，那么我们的通讯就只能暴露在特色的眼睛里。不说革命，将单纯不想让第三者知道的事情经加密后发出，这种行为天然地具有正当性。而不让提供加密通讯，那么是不是说我们大家的所有思想都要受当局审核，我们就毫无隐私权可言了？这分明就是强盗逻辑！

据我推测，真正让特色当局采用这一流氓司法解释的原因无非只有一个——这几年的人民自发反抗的运动让他们害怕了，以至于连“人民民主”的门面也丢掉不要了。

还有什么为他们提供加密通讯技术也是犯罪。有程序员因为开发了渗透软件，并将它发布在互联网上，他本人只是做了开发工作，并没有用它来做不符合特色法律的事情，然而，有不法分子用它来盗取他人的信息，于是把这程序员也判了刑。

针对此，我们是不是可以同理得出一下结果，有专家写了一本人体结构的书，犯罪分子拿它来研究如何杀人并真的杀了人，因此这专家也算同伙；汽车厂的工人生产了一辆汽车，犯罪分子用汽车去压人，所以工人也是同伙；世上的父母亲生下的新生儿都自带能打人的拳头和能强奸人的生殖器，那么假如这些新生儿长大犯了罪，那么他们的父母也是同伙。这是何等的荒诞！就像孔老二再传弟子孟轲说的那样：“此何异于杀人而曰：‘非我也，兵也’”。然而这样荒诞的法律被如此荒诞的运用，不也说明了反动势力所依靠的真是反动的东西吗？

几天后通过的密码法则更是为了镇压人民的反抗、防备革命而将反科学精神发挥到了极致。

众所周知，只有公开研究，公开讨论的东西才有可能是科学，那些闭门造车，一言堂的东西多半是神学。特色当局正是要在科学的领土上传播他们的神学思想。

他们口口声声说什么“科教兴国”，可是却连科学精神也做不到，这同时已经连资本主义的自由竞争都达不到了，要知道在美国 DSA 等密码协议都是技术公开允许私人研究破解甚至攻击的。

于是，这条法律最后无非会有两种结局：要么这条法律在科学规律面前显得螳臂当车；要么科学研究的进展被这法律严重阻碍。

无论那一种都无法回避一个事实，即反动的特色当局试图以反科学的态度对抗日益高涨的自发反抗运动，这注定会是失败的。

我们该做些什么

我们该做些什么？是坐以待毙，空口抱怨；还是仅仅留于谴责层面？

我相信作为当代的革命者，这两种态度都不是我们该选择的。

技术的事情应该交给技术来解决，这是我们这个时代一一信息时代所不同于以前的资本主义时代的方面。

众所周知，美国的棱镜门丑闻正是利用技术手段来监控各国尤其是各国对于美国当局的不利情况的。但是，大家所不知道的是，没有谷歌等大公司的参与没有微软等大企业的开放后门，美国政府不可能或者说所费代价将高到他们难以接受。也就是说，正是在软件领域的私有制度，才是美国政府所能凭借的把手，正是商业资本家和官僚资本家的通力合作才能达到如此全面的监控。

但是，世界上不是所有的软件都掌握在资本家手里，二十世纪八十年代以来以理查德·斯托曼为代表的自由软件运动参与者，正用自己的心血去实现他们的自由软件理念，并为之开发了大量的自由软件，其中涉及很多可以保护个人安全的软件，如 GNU/linux 系统、GPG 等，它们能充分利用现代信息技术的成果为我们的革命事业服务。

想要在私有软件上进行革命的准备工作是不可能的，因为微软公司、腾讯公司等商业公司和特色国安部门、美国 NSA 等政府情报部门可以随时调取你的使用记录，让你无处可逃，更不用说集流氓之大成的“血洗强国”了。

从现在开始，逐步摆脱对于私有软件的依赖，用自由软件和自由软件运动武装自己。

全世界的无产者，通过马列毛主义，运用自由软件，联合起来！

二十世纪八十年代以来以理查德·斯托曼为代表的自由软件运动参与者，正用自己的心血去实现他们的自由软件理念，并为之开发了大量的自由软件

1. 自由操作系统的重要性

——在谈论线上秘密工作前，我们应该遵守的大前提

（编者按:我们此前委托熟悉技术的同志们写一些工作指南性的文章，这是第一个成果，我们衷心感谢同志们的辛劳付出。如果要领导推翻资产阶级统治的运动，那就必须学会秘密地工作，这是列宁同志在《怎么办》中明确指出的。在当代，学会使用安全的工具是学会秘密工作的重要组成部分，必须学会使用之。如果能够学会使用安全的工具，那么这将为线上与线下的秘密工作提供更加安全而坚实的物质基础。）

各位读者看到这篇文章时，我猜你们一定会想这篇文章大概会介绍哪些加密通讯软件，哪些文件加密软件等等，但笔者并不打算一上来就介绍这些具体的应用软件，我想从操作系统谈起，因为没有自由的操作系统，就没有秘密的线上工作。

读者一定遇到或听说过这些情况：今天早上说要买零食，下午逛手机淘宝时就自动推荐了许多零食呢；随便在 QQ 危信上说了点“过激”的话，第二天警察就找上门了。

过去我们往往把这些现象归咎于某个 app 的过度索取权限，可是正如社会领域的问题一样，app 们肆意妄为也得有一个根本背景，这就是私有操作系统，为什么这么说呢，因为一切应用都需要与操作系统进行交互。

许多私有 app 过度索取用户信息，其背后离不开私有操作系统的原因。

X 光下，人的骨骼可以被看得一清二楚，这和穿没穿衣服并无关系。

各位一定在使用 M$WIN(我们对 windows 系统的蔑称)10 时遇到过以下问题:为什么我的系统不受我的控制自动“升级”了？为什么“我的电脑”里有那么多无法访问的文件？为什么系统越“升级”越不稳定，越使用效率越低？

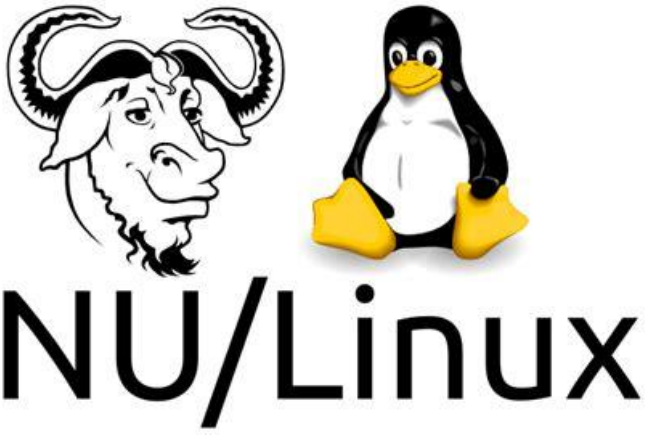
你的机器并不像你想象得那样听你的话，计算机在安装私有操作系统的情况下，就已经是资本家对你的监视工具了，如果不仅安装了私有操作系统又充满了其他私有软件的话，它们将彻底受制于资本家，成为囚禁你让你无处可藏的圆形监狱。原因很简单，信息技术产品区别于传统产品的地方在于它们靠代码运行，而且靠代码就可以自动运行，因而也有完全脱离用户的掌控而自动运行的可能，只要具备运行条件（比如设备有电、联网等等），这就为监视行为打开了大门。

此外，私有操作系统与私有应用的开发者沆瀣一气，他们共享着剥削用户的利益，私有操作系统诱导用户下载安装私有应用，私有应用要求用户的操作系统也是私有的，举个例子，许多游戏应用只能在 M$WIN 下运行，而不是自由的操作系统，而 M$WIN 或者原厂 android 的应用商店及 apple store 又源源不断地向用户推荐着私有软件，而不是自由软件，这就使得用户无法接触到自由软件，更不用说自由软件哲学，进而只能囚禁在私有软件的牢笼里。

因而，才像我开头提到的那样：没有自由的操作系统，就没有秘密的线上工作。在私有操作系统

下进行所谓秘密工作就如同在 x 光下穿着衣服不让人们看到你的骨骼，并且他们还不断诱惑你让体验 ct、b 超，进而套取你的数据，然而你在这些仪器下本质上已和裸体的结果并没有任何区别，更不用说源源不断泄漏着自己的信息这一点了。

那么有没有什么可以被我们利用的自由的操作系统呢？有的。在电脑端上有已经成熟的各 GNU/Linux 发行版本，在手机上有自由的 android 发行版本，例如 lineageos、RRos 等。离开这些自由的操作系统谈论秘密线上工作无异于是天方夜谭。



GNU/Linux，自由软件运动的伟大产物。

那么为什么说私有软件不可靠，而自由软件可靠呢？对于私有软件，其罪恶，其危害随意在互联网上搜索就可以找到一大堆，今天脸书泄漏个用户数据啊，明天各个原厂 android 又发现什么“漏洞”啊，后天微软向美国国家安全局提供用户数据啊，比比皆是，它们是资本家为了从用户那里榨取更多利益而监视甚至控制用户的禁脔。

而自由软件不同，它是自由软件运动，这一旨在实现“自由软件，自由社会”理念的伟大社会运动的产物。自由软件运动的领袖——理查德·斯托曼（Richard Stallman）及其他发起者为了实现用户对软件的绝对控制这一目标，提出了自由软件应该具备的四大自由：

用户可以按照自己的意愿使用的自由（自由之零）；用户可以自由修改该软件使得能更好地为用户所用的自由。为此用户有权查看软件源代码（自由之一）；用户有传播该软件副本的自由（自由之二）；用户有传播用修改后的软件副本的自由（自由之三）。

facebook 多次发生过泄露用户数据的事件，其依赖的服务系统正是私有网络和私有软件。

由此，他们为这个世界编写了琳琅满目的自由软件。另外，为了利用美国的版权法来保护自由软件运动的成果，理查德·斯托曼先生和他的伙伴，编写制定了 GPL 软件发布协议，凡是在这一协议下发布的软件，必然符合这四大自由（自由许可协议并不只有 GPL 一种，但只有左版的许可协议才能保证其所有衍生作品仍然是自由的）。通过保障实现四大自由的 GPL，软件的安全性被极大地保证了，恶意代码将无处可逃，因为它的源代码是开放的所有做的手脚都能被发现，而且都能被及时修改。

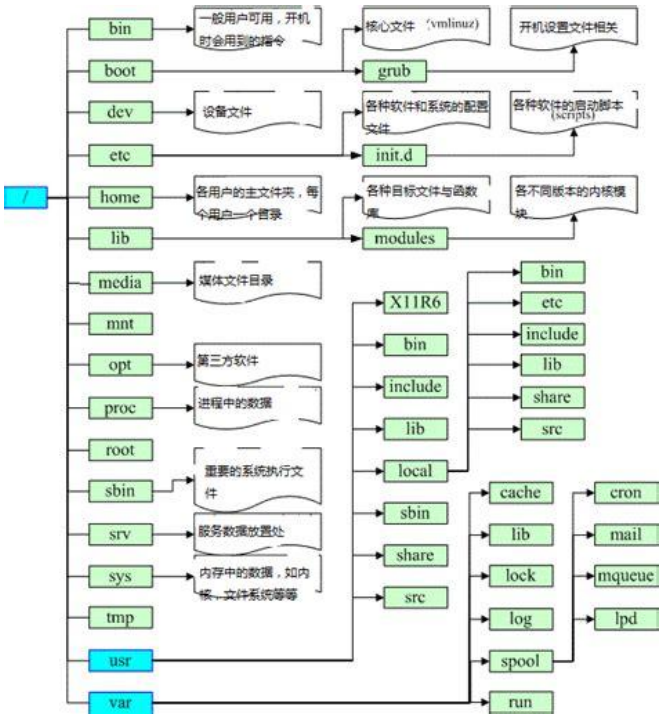
让我们说回操作系统。实际上，操作系统也是软件，但是它是最接近硬件，也就是所谓的“底层”的软件，一切应用软件都需要在操作系统之上运行，都需要与操作系统进行交互，这样实际上应用是受制于操作系统的。而且，如果系统千疮百孔，那又怎能保证恶意程序不去侵害用户的隐私呢？而 M$WIN 就是这样一款千疮百孔的操作系统，它文件系统混乱，只是简单地分了个 C、D、F 盘，每个盘下的软件可以随意安放，用户等级模糊，导致误操作很容易导致系统崩溃，而在这种乱七八糟的编排之下，很容易藏几个恶意程序。

GNU/Linux 系统不同，根目录下每个目录都有具体的分工，管配置的就管配置，管硬件的就管硬件，管命令的就管命令，在这样井井有条的分类之下，植入恶意程序恶意代码的可能性就大大下降了。

当然自由只是隐私的前提，假如你自己不注重保护自己的隐私，那么秘密仍然也无法谈起，毕竟即使小声说话被他人听见也算泄密。

为此我们必须增强保密意识，意识到我们保护我们秘密的重要性。这在线下可能有些人做得已经很好了。比如，外出会关好家里的窗户并将房门反锁，不想让他们知道的事情就不告诉不靠谱的等等。可是，在线上，很多人只是感觉自己很保密，其实对于隐私的重视完全不足。比方说，有的人为了所谓财产“安全”，用移动支付代替现金支付，孰不知当你一笔一笔地用着移动支付的时候，移动支付软件便一笔一笔地记下你的交易记录，并将它们发送到资本家手中。先不说这样是否会泄露其他信息，单是你每一笔交易的情况都反馈这一点，资本家都完全可以通过大数据技术，分析出你的种种情况，比如贫富、喜好等等。而且别忘了移动支付都是实名的，这直接可以通过分析你的交易记录来判断你到底是个怎么样的人，这样下去，哪天你登录手机淘宝，人家给你推送“革命者应该使用的武器”，你也不要惊呼“事情败露了”。这对于其他领域也是一样的，依赖危信 QQ 等集中构架的即时通讯软件宣传革命无异于当着习近平的面说什么“我要刺杀你”，因为你的一言一行全部都收录在资本家的数据库里，要调起来很容易。

自由软件运动之父——理查德·斯托曼



这就是 GNU/Linux 系统的文件系统目录树，其中每一项都是一个目录，大的目录中有小的目录，它们都是有自己的明确的作用的。

保密意识绝对不容半点妥协。为什么这么说？机密只有在它没有泄漏时才是机密，一旦泄漏就不再是了。私有的操作系统也是如此，还记得前面提到的 M$WIN10，提到的种种怪异举动吗？既然 M$WIN10 不受你控制，那么自动升级一定是微软给它的指令，微软既然可以在你不许可的情况下就“升级”系统，那么为什么不可以在你不许可的情况下检查你磁盘上的文件，并把它们泄漏给政府呢？资本家都是追求利润的，今天他能为了利润狠心压榨工人，明天就能为了利润，贩卖你的数据。

杜绝资本家的窥视的唯一办法就是使用自由的操作系统，为什么？因为你能彻底地掌控他们，根据你自己的需要来调整他们，假使有漏洞你也可以自己想办法修补，不用考虑私有软件修补漏洞后，带来了更大的副作用。

保密并不是一个点，它是一个面，不，一个体，一个四面透风的房子谈不上保密，因为路人也可以看得一清二楚；一个遮风挡雨的房子才能保密，因为窗帘一拉谁也看不见了，只要你能保证外人进不来。对于我们来说，只是务求几个保密软件来实现秘密工作是不可能的，只有把保密换成一个体系，一个线上的从计算机到网络连接全是安全的情况下，保密才谈得上。

另外，在不彻底改变自己机器上的私有操作系统的基础上，而使用所谓“秘密软件”，这同时也是一种妥协，类似于改良主义的那种妥协，那种不触动资本主义根本只进行局部改良的妥协。我想作为一个立志成为革命者的人来说改良主义绝对不是一个需要考虑的选择，因为显而易见，妥协只对资本家有利。

尽快掌控自己手中的设备吧，离开了自由，秘密将荡然无存。

4.GNU/Linux 基础

——在谈论线上秘密工作前，我们应该遵守的大前提

(编者按:这是线上安全工作指南系列文章的第二篇，此篇文章开始切实地讲解技术问题。我们委托作者同志尽可能简单易懂地讲解技术问题，以便为我们的读者带来学习上的便利。再一次地，我们衷心感谢我们同志的付出。)

上一章，我们初步提到了 GNU/Linux，从这一章开始，我们将开始讲解什么是 GNU/Linux，以及如何安装并使用它，在安装并使用 GNU/Linux 之前，先让我们了解一下 GNU/Linux 到底是什么。

Linux 内核之父——林纳斯·托瓦兹

首先，先了解一下 GNU 和 Linux 分别是什么。

简单说来，GNU 是理查德·斯托曼等自由软件运动的发起者于 20 世纪八十年代开始研制的自由的操作系统。Linux 是林纳斯·托瓦兹（Linus Torvalds）于二十世纪九十年代与许多程序员共同开发的操作系统内核。

以上叙述可以看出，GNU 与 Linux 是两个工程，那么它们又是如何结合到一起去的呢？九十年代时，GNU 操作系统的基本架构已经开发完毕，仅仅差一个内核，而 GNU 的开发者们开发的内核——hurd 由于其开发难度超出了设想导致不能实际使用，但这个时候林纳斯·托瓦兹等程序员开发了 Linux 内核并在开发完毕后的第二年使它成为了自由软件，于是 GNU 结合 Linux 内核成为了 GNU 的一个发行版本即 GNU/Linux。①。

GNU 与 Linux 内核的结合是自由软件运动历史上的大事

GNU 操作系统与 Linux 内核的结合是自由软件运动历史上的大事。它表明自由软件运动有了自己独立的操作系统，从而可以将大量自由软件整合起来并且能更大地发挥它们的作用，进而大大促进自由软件运动的发展。

以上便是 GNU/Linux 的历史。

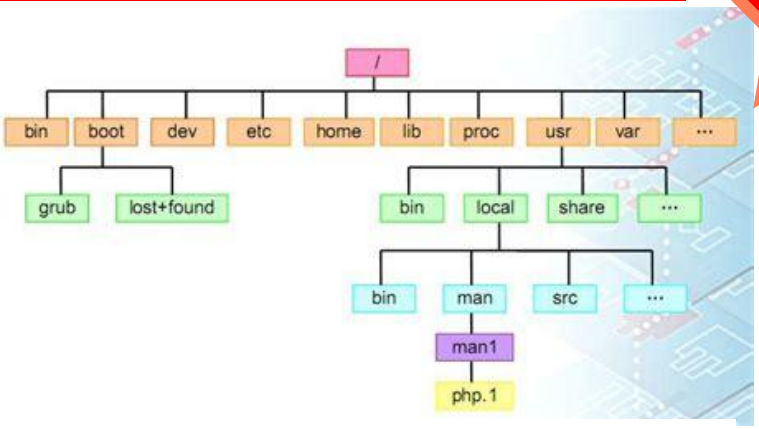
顺便说一句，有很多人将 GNU/Linux 仅仅称作 Linux，这背后体现的其实是资本家对于自由软件思想的抵触，他们无法接受自由软件思想，他们妄图通过抹杀 GNU 让用户忘记 GNU/Linux 是自由软件运动的产物。②

GNU/Linux 的历史想必大家已经有所了解了

那么我们接下来讲讲，GNU/Linux 的基本概念。

一切皆是文件。一切皆是文件，这是什么意思，相信每一个看到这句话的读者一定有些不明所以，不过，其实它很好理解，简单来说，在 *nix （或称“类 unix”）操作系统中，不但程序配置用人类

可读的文本储存于典型文件中，就连磁盘分区、通信接口，甚至网络套接字都“表现为文件”，以类似典型文件的方式去访问。用文本文件保存程序配置的好处是便于管理与控制计算机，因为进行配置就是在编辑文件。而后者的实质是用读写文件的操作统一抽象任意输入输出操作，这种统一可以大大拓展应用程序的适用范围。但同时用户如果缺乏运用 *nix 系统的知识或者因为失误进行了误操作，将会危害计算机，因此 GNU/Linux 系统下存在严格的权限隔离机制。

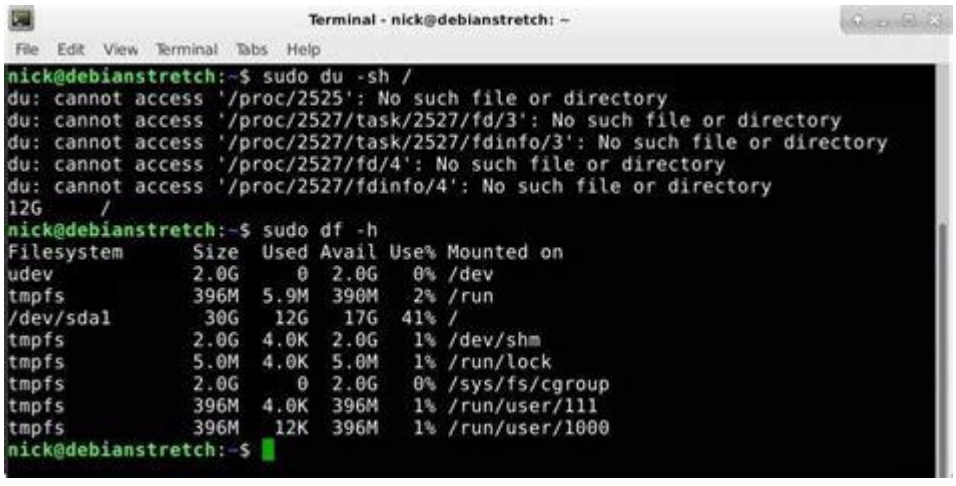


这就是 GNU/Linux 系统的目录树

权限隔离。GNU/Linux 系统的权限隔离体现为不同账户对同一（广义）文件的访问权限的区别。*nix 系统中任何权限主体（用户和组）对任何文件系统对象均有读、写、执行三种访问权限。*nix 系统中普遍存在 root 账户，又称超级用户，它有权更改文件系统中的任何文件和目录的访问权限，故可以通过修改操作系统上的文件进而控制住计算机；而非 root 的普通账户就是通常情况下用来启动操作系统的账户，其权限只是 root 账户权限的子集，只能更改属于自己的文件和目录的权限。每个普通用户被（root 用户）创建时都会分配一个 /home/<用户名>/ 目录（被称为该用户的“主目录”或“家目录”）归其所有。因此使用它仅可以自由支配自己的主目录下的文件，甚至不可以下载安装软件（因为普通用户没有主目录以外范围的写权限）。通过这种分明的权限隔离，普通用户就无法对自己的主目录以外的文件进行编辑修改（有的甚至还不能读取），这样可以保证多用户并存的时候，不会因为乱动别人的文件而互相干扰，这体现了其多用户操作系统的特点。

GNU/Linux 的软件依赖关系。GNU/Linux 下的软件能合理处理软件依赖关系。什么叫软件依赖关系呢？一个软件往往能运行需要其对应的运行环境，比如 a 软件要运行，它可能需要 b 软件作为其运行环境，这时如果 c 软件要运行也需要 b 软件，那么就可以说 a 和 c 都依赖 b，b 与 a 和 c 形成依赖关系。这在 M$WIN 下处理得并不好，比方说，还是 a 软件依赖 b 软件，c 软件也可以依赖 b 软件，但是 c 软件的软件包里又包含了 b，这样就会浪费空间，原因就是 M$WIN 没有统一的包管理器；但在 GNU/Linux 下由于存在统一的包管理器，软件依赖关系处理良好，往往 b 就是 b，不会多出个和 b 功能重复的软件，这样可以减少相同功能程序的存在，节约磁盘空间。

目录树。GNU/Linux 对于文件系统的划分方法不同于 M$WIN 下那种 C、D、E 盘的模糊分法，它是通过目录树组建起文件系统的。首先一切目录都挂载在“/”根目录下，而根目录下的每个目录都有它的作用。例如，“/home”存储各个用户的家目录，个人帐户的文件都存储在这里，这也是未取得 root 密码的用户所唯一能修改的文件的存储地；“/etc”，用于存储程序所需的全局配置文件，如 sudo 的配置文件 sudoers 就存储在这里。而子目录下又会包含二级子目录，如“/home”家目录下包含的具体的用户目录。这样就构成了目录树。③



Linux 的命令行，比 loosedows 的 cmd 不知道强到哪里去了

命令行。GNU/Linux 下许多软件都需要通过命令行界面的形式使用，GNU/Linux 的命令行强大无比，可以进行网络通信可以压缩可以写文章可以编程，总之基本涵盖了计算机使用的方方面面。在命令行界面里，我们通过输入字符命令来进行操作，这虽然一开始会比较难，但是随着熟练程度的加深，你会渐渐发现很多时候命令行的效率要高于图形界面。④

以上就是在安装前，关于 GNU/Linux 的基础知识，

那么使用 GNU/Linux，除了它是自由软件安全性较高以外，还有什么好处呢？

笔者根据以上特点总结了以下三点：

1. GNU/Linux 下一切皆是文件，这和 M$WIN 这种充斥着注册表和设备专用工具的系统不同，可以更加方便地管理系统和电脑。

2. GNU/Linux 下用目录树安排磁盘，可以更有效率地利用资源，做到井井有条。

3. GNU/Linux 下命令行界面强大无比，可以节约很多图形化所需的时间并实现自动化，提高效率。

注释：

①GNU libc 至少可以对接三种内核、hurd、linux、还有 freebsd 的内核，从而分别构成 GNU/Hurd、GNU/Linux 和 GNU/kFreeBSD，其中 GNU/Hurd 前面提过因为技术不成熟，GNU/kFreeBSD 因为支持的硬件少且用户体验和 GNU/Linux 相差不大，因而使用的人数非常少。

②这也和“开源”运动有一定关系，至于开源软件和自由软件的区别以后会提到。

③目录树的知识具体会在接下来几章详细讲解。

④M$WIN 也有它的命令行终端 cmd，但是很不好用。

这个样子可爱的小机器人（android 意为“机器人”）承载了多少罪恶

附加：

前面，我们提了那么多，为什么没有提到手机端呢？现在手机不是更普及吗？我想，你们一定有这样的疑惑。然而其原因却是不言而喻的，手机端所受的限制远大于电脑端，不仅仅是操作系统构架如此，甚至连硬件本身对软件的支持上来说都是如此。

apple 远不如它声称的那么安全，恰恰相反，一个用户掌握不了的设备不可能安全

在手机端，操作系统基本为 Mandroid（对 android 的蔑称）和 IThing（对 ios 以及一切苹果公司的产品的蔑称）所垄断，后者干脆搞封闭，尽管用户可以通过“越狱”获得很大的权限，但仍不能完全掌控设备，并且它完全不给用户留一点自主选择第三方 rom 包的机会；前者倒是大谈“开源”，可是又狡猾地绕开了左版（copyleft）的限制，成为一个对用户限制重重的操作系统，尽管它是基于 Linux 内核开发的。

尽管 Mandroid 可以通过刷相对自由的第三方 rom，如 lineageos，rros 等，但是即便如此它的框架仍然是 google 设定的，只是少了例如谷歌框架等侵犯用户隐私的东西罢了。

那么手机端的 GNU/Linux 操作系统呢？手机端的 GNU/Linux 系统确实存在（例如 sailfish os），但是配适的应用软件非常少，可用性不足。而想要在 Mandroid 中把 Linux 内核解放出来，也不是一个轻轻松松的事情。

不过 Mandroid 用户为了隐私安全还是建议各位刷入相对自由的第三方 rom，但这并非每一款 android 手机都可以，只有部分可以“解锁”，且 开发出相应 rom 的手机才能，这个以后我们也会讲到。至于 ITing 用户，我们只能建议您卖掉自己的苹果设备。

因此，总的来说想要从事真正的线上秘密工作，一台电脑（苹果电脑除外）是必不可少的。