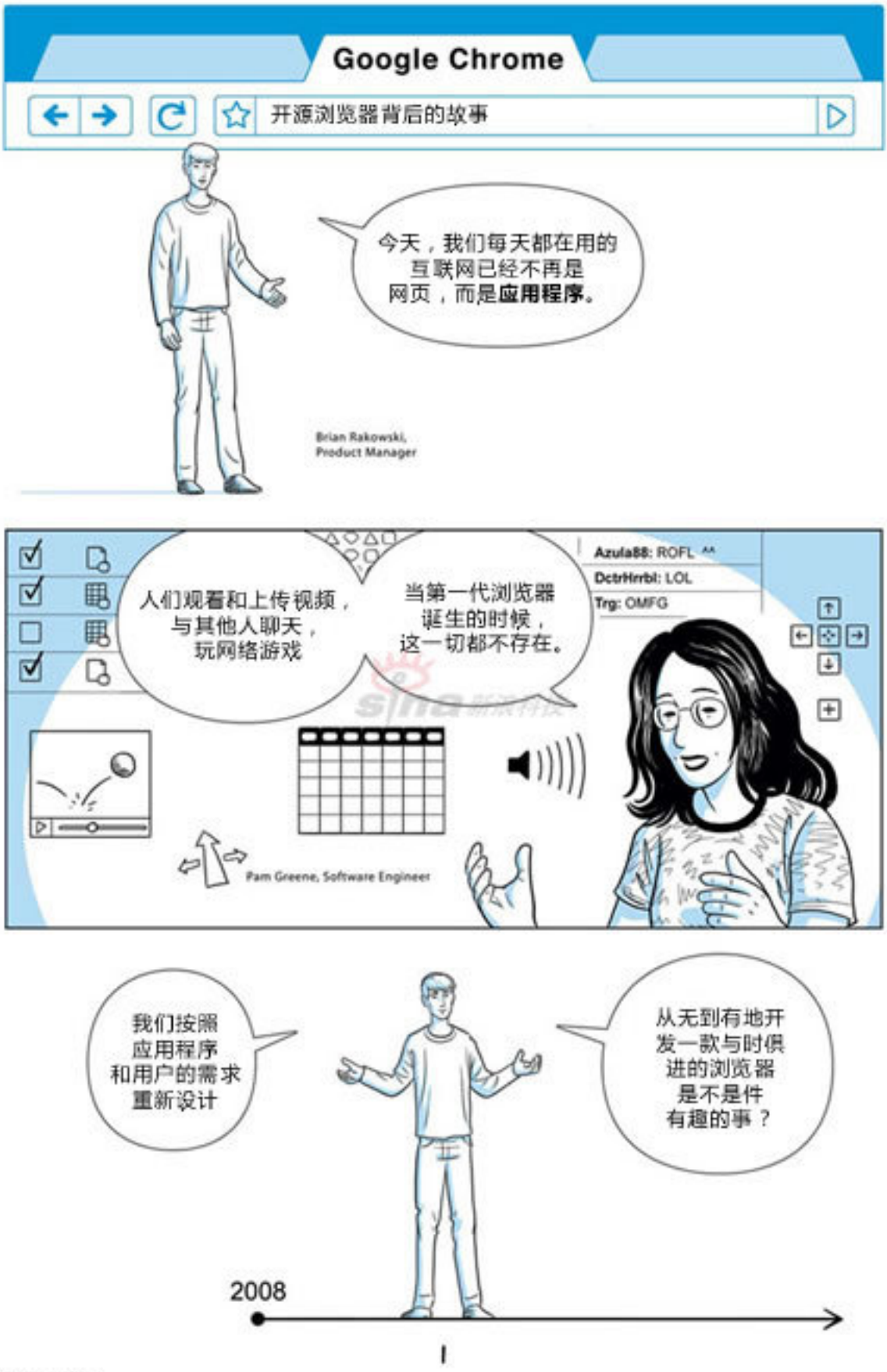
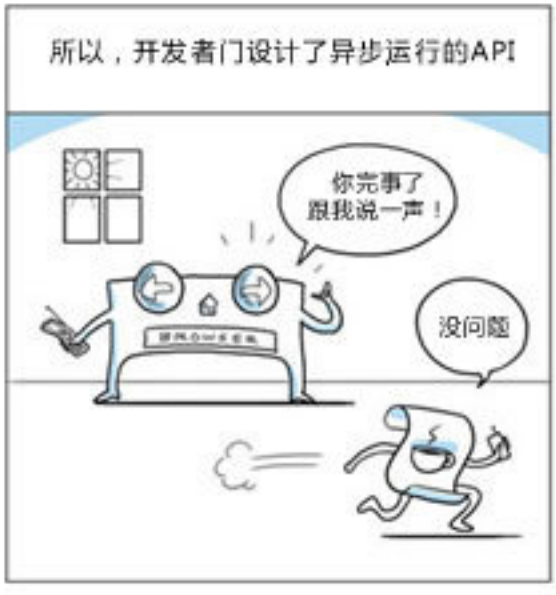
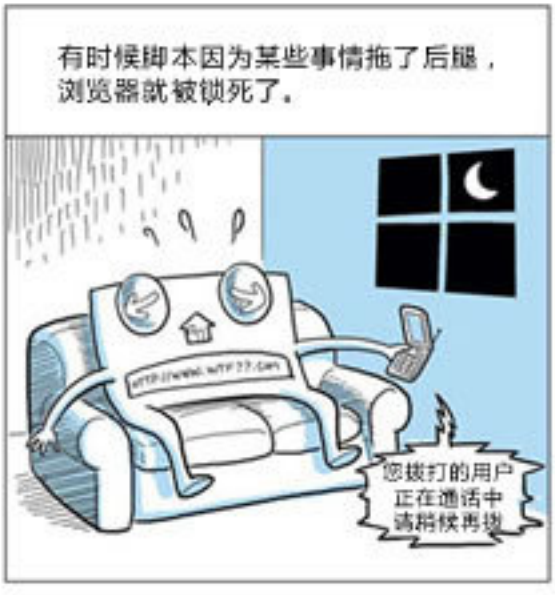

Google Chrome
开源浏览器背后的故事
今天，我们每天都在用的互联网已经不再是网页，而是**应用程序**。
Brian Rakowski, Product Manager
人们观看和上传视频，与其他人聊天，玩网络游戏
当第一代浏览器诞生的时候，这一切都不存在。
Azula88: ROFL ^^
DctrHrrbl: LOL
Trg: OMFG
Pam Greene, Software Engineer
我们按照应用程序和用户的需求重新设计
从无到有地开发一款与时俱进的浏览器是不是件有趣的事？
2008

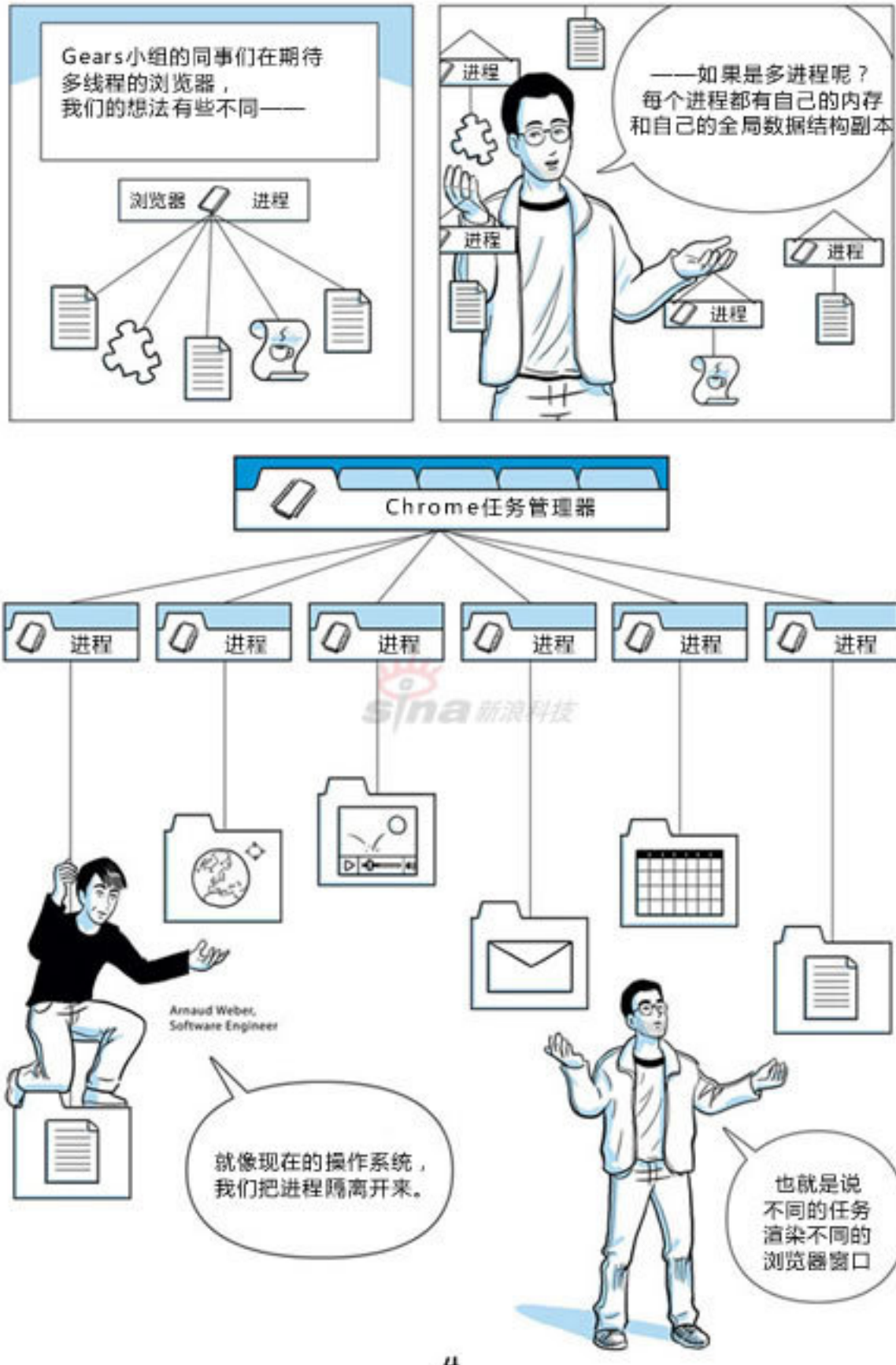

首先，浏览器需要更稳定。
当你在写重要邮件
或者编辑文档时，
浏览器崩溃可是大麻烦。
Darin Fisher, Software Engineer
浏览器还需要更快，
启动要更快，
打开网页也要更快。
而且，对于
网络程序来说，
Javascript脚本
也要更快。
Lars Bak,
Software Engineer
Kasper Lund,
Software Engineer
浏览器也得更安全，
根据现有的漏洞信息，
浏览器需要结构上的变化，
这样才能打击恶意程序。
Ian Fette,
Product
Manager
我们希望找到一个
功能和界面的平衡点，
为浏览器设计一个干净、
简单有效率的界面。
Ben Goodger,
Software
Engineer
最后，Google的Chrome
是一个完全开放源代码的
浏览器。
我们希望其他人
借鉴我们的想法
正如我们借鉴
其他人的好点子
一样。

翻译/制作：龚民

稳定性，严格和多任务构架





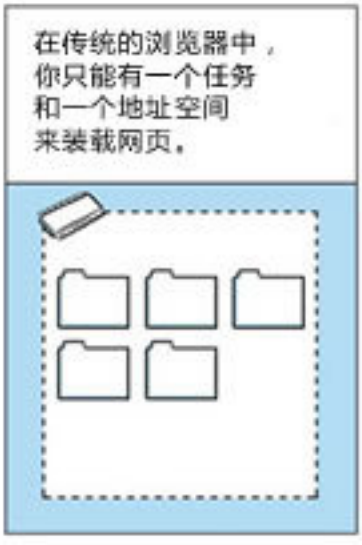

Gears小组的同事们在期待
多线程的浏览器，
我们的想法有些不同——
浏览器
进程
进程
——如果是多进程呢？
每个进程都有自己的内存
和自己的全局数据结构副本
进程
进程
进程
Chrome任务管理器
进程
进程
进程
进程
进程
进程
Arnaud Weber,
Software Engineer
就像现在的操作系统，
我们把进程隔离开来。
也就是说
不同的任务
渲染不同的
浏览器窗口

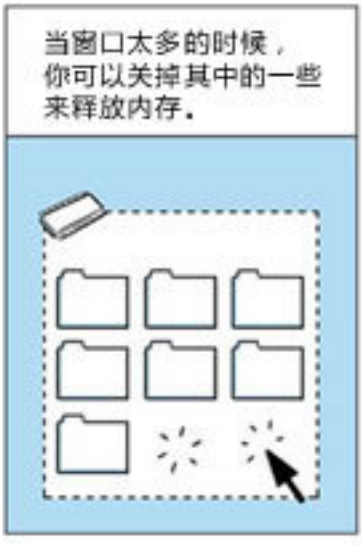

进程
进程
一个窗口也许在忙，
但其它的窗口
可以继续用。
这样
也有了单独的
Javascript
脚本线程

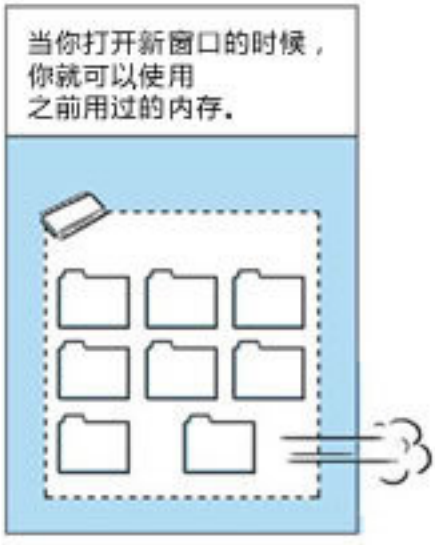

如果发现了浏览器Bug
（我们的经验是，
不可能除掉所有的Bug）
我们最多就是失去一个窗口而已。


一个窗口失去响应，
它会露出伤心的表情
但不会让整个浏览器崩溃。
是的，
它真的会伤心


多进程的设计也意味着
占用更多的内存。
每个独立的任务
都会增加一些成本。
但总的来说，
也意味着更少的
内存浪费。
LAUNCH


在传统的浏览器中，
你只能有一个任务
和一个地址空间
来装载网页。


当窗口太多的时候，
你可以关掉其中的一些
来释放内存。


当你打开新窗口的时候，
你就可以使用
之前用过的内存。

但随着时间的推移，
会出现一些内存碎片。
一些窗口虽然关闭了，
但内存仍然被占用。

我们也许会有
一块无法再次
利用的内存，
也许会有指针
指向一块
正在使用的内存。

Mike Belshe,
Software Engineer

当浏览器
打开一个新窗口时
原有的空间
就不够了——

THUNK!

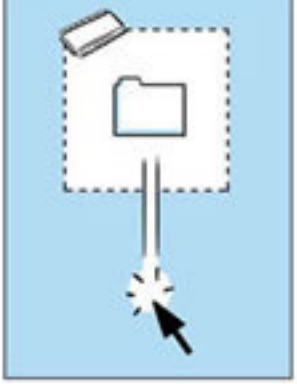
——所以，
浏览器会向
操作系统
申请更多的
内存空间。

这个问题每天都会发生，
尤其是浏览器一直开着的时候。

但如果在Google Chrome里，
关掉一个窗口，整个进程都被结束了。

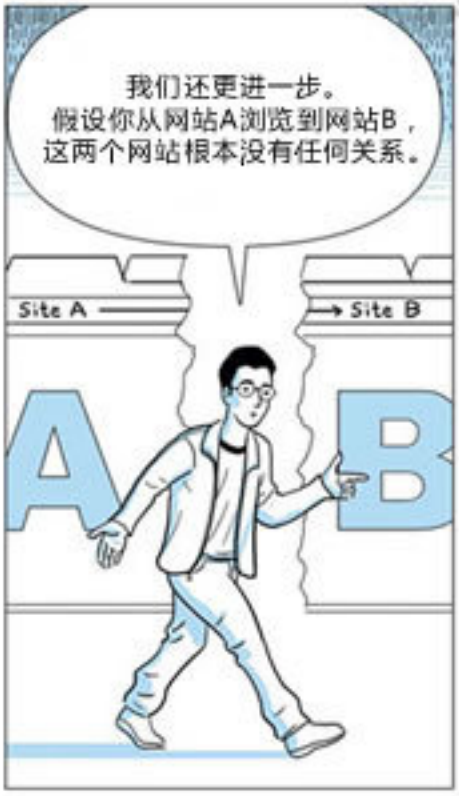
——而且，
所有的内存
都会被注销。

现在打开一个
新窗口，
就会启动一个
新进程。

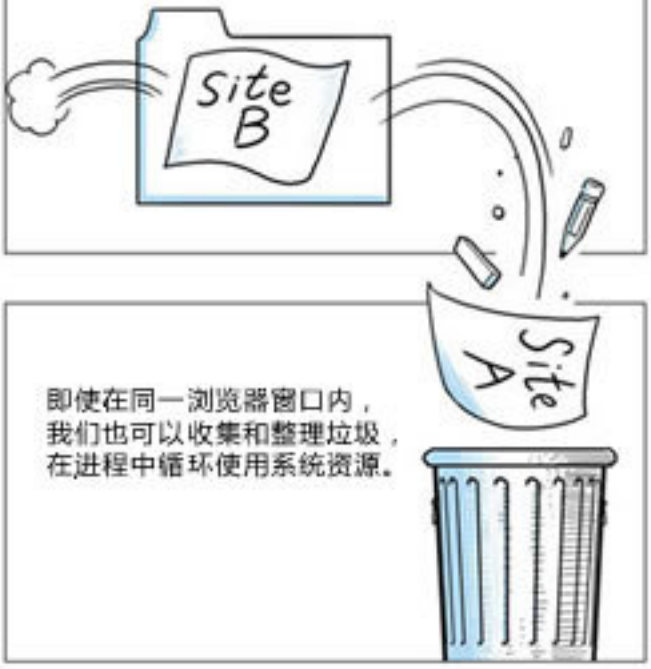


在你上网的时候，我们在不停地创建和删除进程。
如果出现了严重的内存溢出也不会困扰你太久，
因为你很有可能在某个时刻关掉一些窗口，
内存又会回来了。

我们还更进一步。
假设你从网站A浏览到网站B，
这两个网站根本没有任何关系。



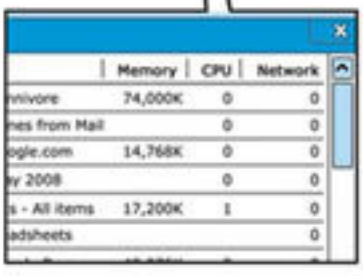
——所以这个时候，
我们可以扔掉旧的引擎，
旧的数据结构和旧的进程。



即使在同一浏览器窗口内，
我们也可以收集和整理垃圾，
在进程中循环使用系统资源。

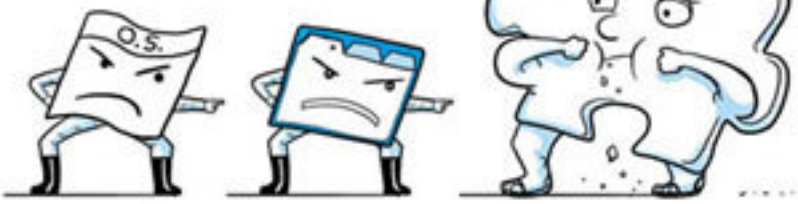
就像你的操作系统，
你可以通过Chrome
的任务管理器
查看背后的信息：
哪个网站用的内存最多，
用的带宽最大，
占用了太久的CPU

这个程序
要把整个互联网
都下载过来吗？



因为插件也会占用
一个单独的进程，
你甚至可以在任务管理器中
了解他们的工作状况。

所以当遇到麻烦的时候，
你可以找出谁不正常，
为什么不正常——



然后干掉他们

啪！

把你的批评
对准责任人。

翻译/制作：龚民

在浏览器编译之后20到30分钟内，我们可以调用上万个网页来测试它。

每周“Chrome 机器人”可以测试几百万个网页，并向工程师反馈早期的测试数据，而以前只能通过外部Beta测试获得。

十亿

当然，网上有上十亿的、甚至上万亿的网页。如果每次编译都需要测试一百万个网页的话，我们用**哪一百万**呢？

一百万

幸运的是，我们有一个特别的措施

Web Images

我们已为网页评分，根据大家的使用习惯找出访问更频繁的网页。

www.alreadyrank.com - Similar Pages

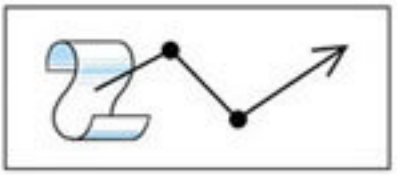
最坏的情况下，我们会保证这些常用的网页不出现显示错误。

www.attheverylast.com - Similar Pages

对于每次编译，我们都有几种测试的办法。可以单独测试部分代码——

——使用脚本模拟用户来动态测试UI。例如“点击后退按钮”或者“访问某个页面”……

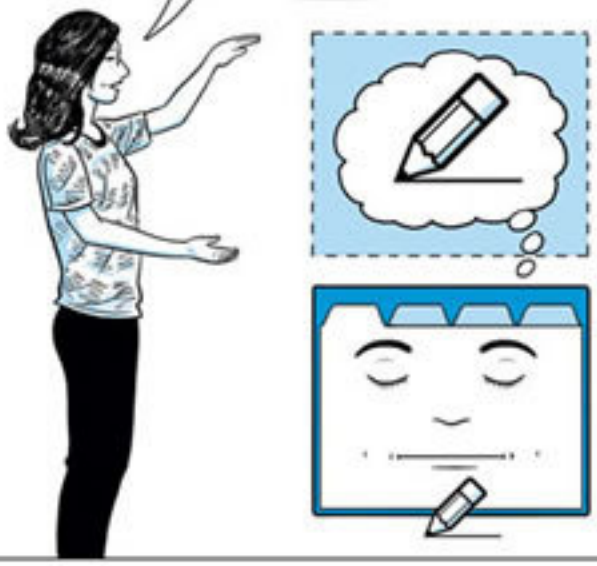
——甚至还有模糊测试：向程序发送随机数据。



Pam Greene, Software Engineer

翻译/制作：龚民

在输出测试中，我们发现更精准的测试办法。
我们让浏览器按照**自己的**算法生成一个网页概要，
而不是计算和对比截屏图片的哈希值。



当我们开始的时候，
我们已经通过了
23%的页面呈现测试。
而从23%到99%
这段路变成一个
有趣的、富有挑战的、
基于测试的设计工作。

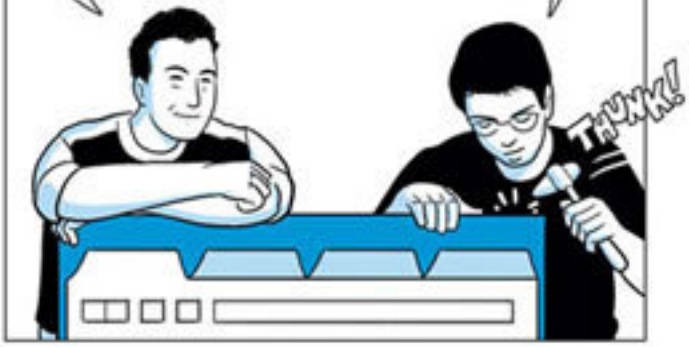
使用机器自动测试
也有不足之处。

比如说，
我们无法测试
需要登陆的网站。

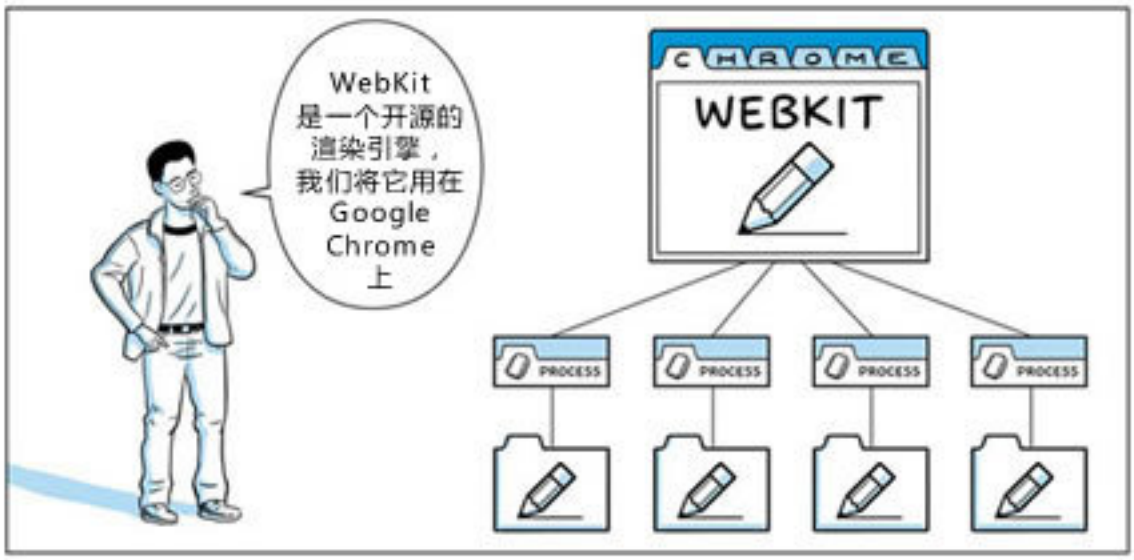
而且，这和人类滥用工具不一样，
我们是在使用浏览器，
只能按照当初设计的功能去用。

很难保证100%，
但这是我们的目标。

我不管它是否
有很酷的功能，
我只想它是一个
非常坚固的产品。

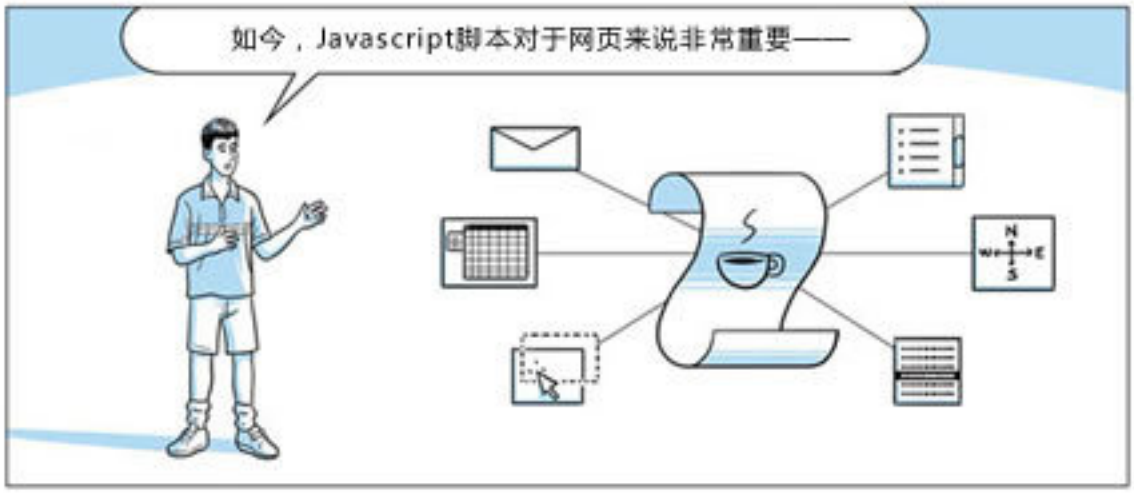



速度：WebKit和V8


WebKit
是一个开源的
渲染引擎，
我们将它用在
Google
Chrome
上
CHROME
WEBKIT
PROCESS
PROCESS
PROCESS
PROCESS


它的速度之快让我们印象深刻。


我们也知道
Google有一群人
在开发Android
我们问他们，
你们为啥
要用WebKit？
他们说，WebKit的
内存管理很优秀，
对于嵌入式设备来说
非常简单。而且，
浏览器开发的新手
也能够理解。
浏览器是很复杂的。
而WebKit做得很好，
它的一切都很简洁。


如今，Javascript脚本对于网页来说非常重要——


——我们觉得，
为Javascript脚本
开发一个虚拟机
也很重要
CHROME
WEBKIT


——这也是
位于丹麦的
V8小组
正在做的事情。
V8小组是虚拟机专家，
不管你想把什么语言
放在虚拟机里面，
他们都可以告诉你
如何做。


虚拟机带来了
安全和
跨平台的特性
但之前的Javascript虚拟机
是为小型软件开发的
它并不看重性能和
系统互动性。
他们只想
在网页上
运行一些
非常基本的
应用。
Lars Bak,
Software
Engineer, V8
Kasper
Lund,
Software
Engineer, V8

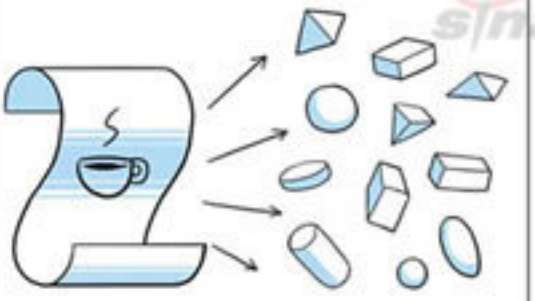
可是现在，
类似于Gmail这样的网络程序
几乎用尽了浏览器资源，
比如DOM操作和Javascript脚本

简单地去改进
Javascript引擎
已经不够了。

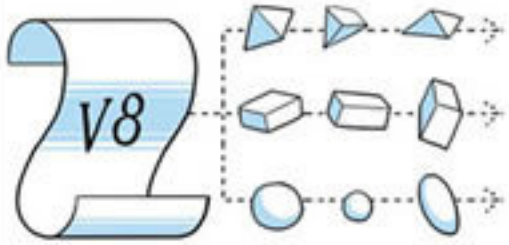
所以我们从零开始，
先想着怎么样才能
尽可能的快——

比如
引入**隐藏类转换**
的概念。

Javascript脚本本身没有类的概念。
你可以创建一个新的对象，
动态地为它添加属性。



但在V8中，程序运行之后，
同样属性的对象将共享同样的隐藏类。
基于此特性，我们可以做一些动态优化。

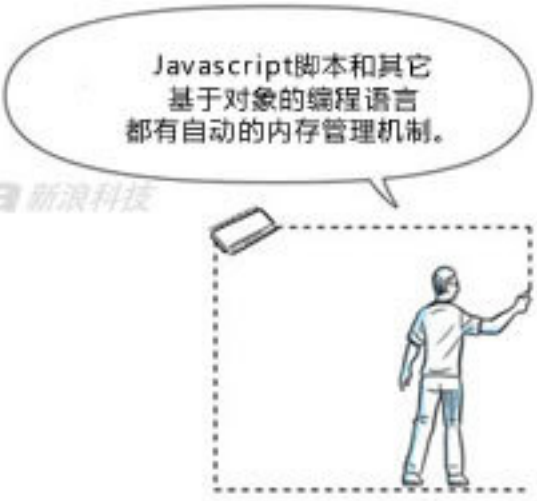


V8的速度还有
另外一个因素，
动态代码生成

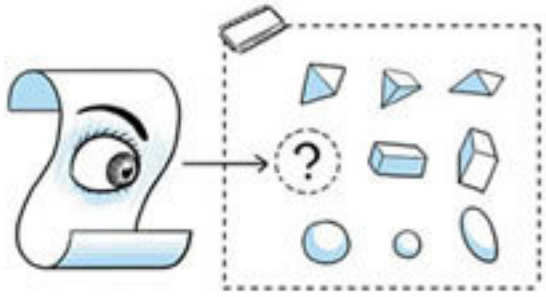
当其它的Javascript引擎运行的时候，
他们会先根据脚本源代码生成内部解释，
最后才会去执行。

Javascript脚本只需解释一次，然后编译成机器码，
接下来再也不需要解释，脚本就可以直接运行了。

1010001010001010100101010000101010000101

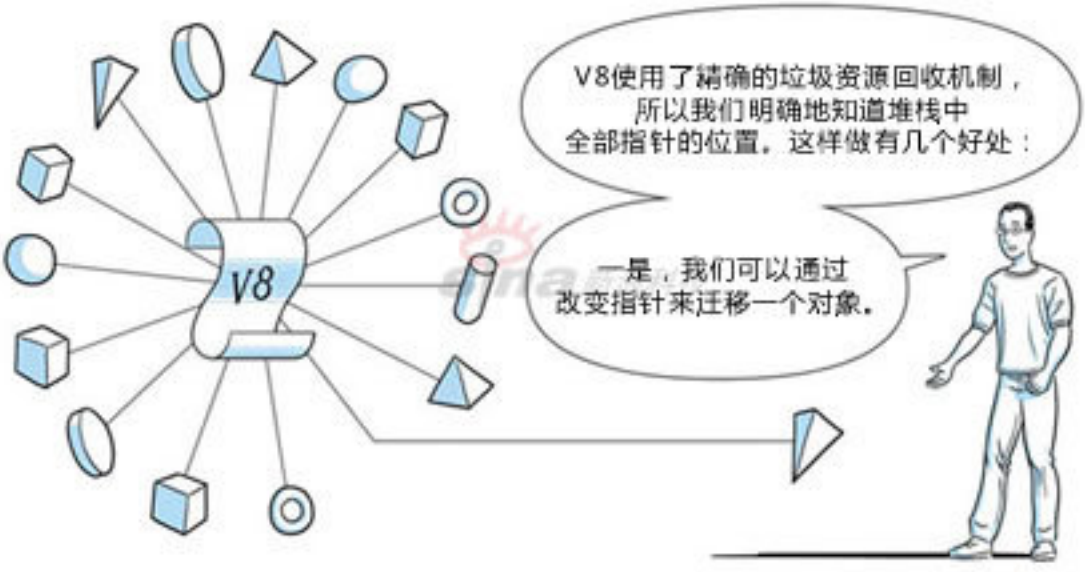


如果你不再使用一个对象，它所占用的
内存可以被系统收回。
这就是垃圾资源回收机制，
基本上是一个微不足道的过程。

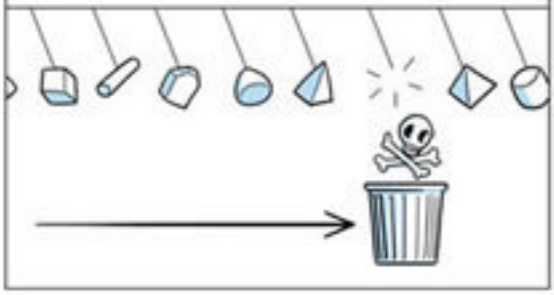


你就得在执行的堆栈中仔细地找，来看看哪句话像指针。

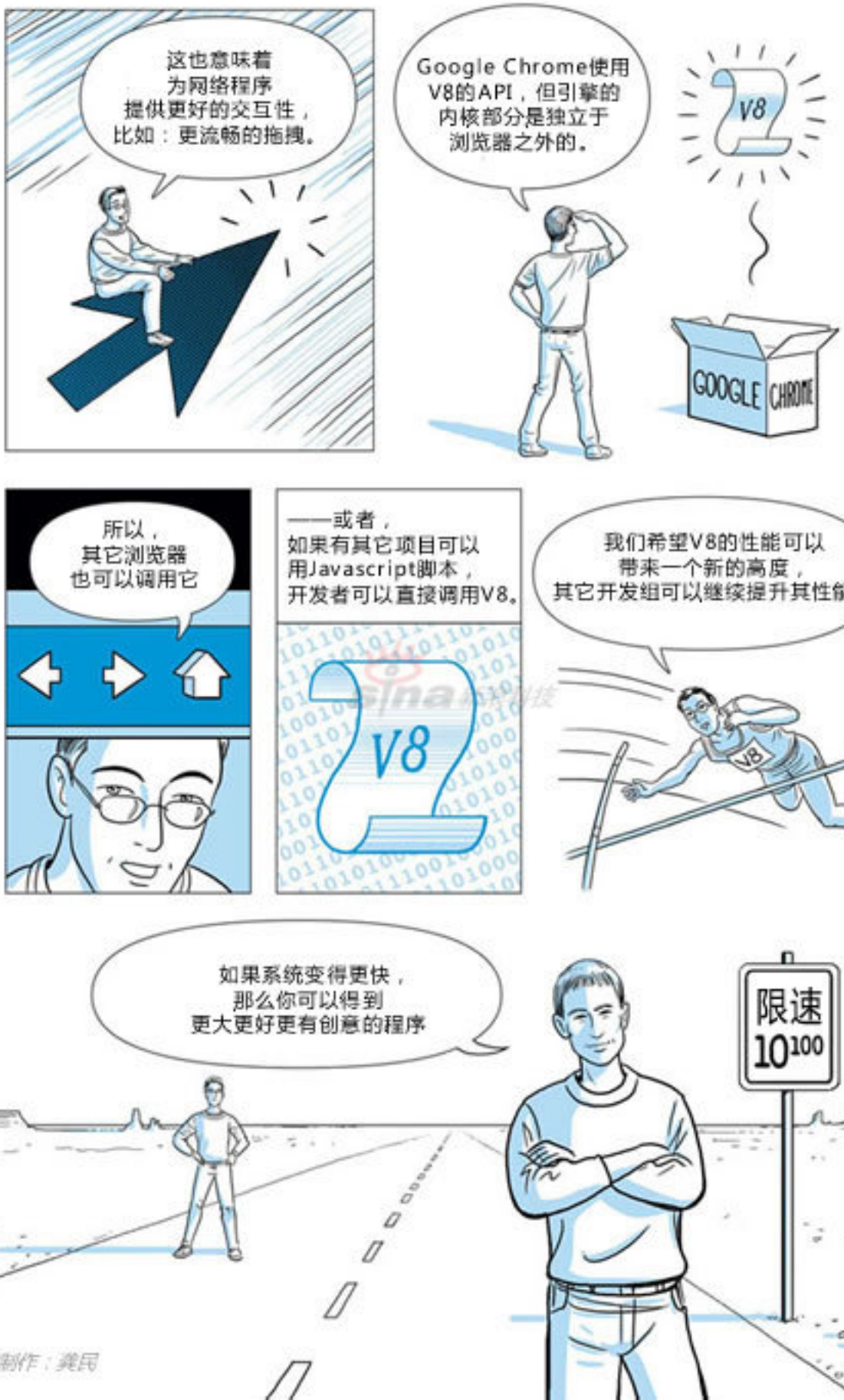
可是，那个看上去像像指针的家伙也许是个整型变量，它可能碰巧拥有同样的内存地址。

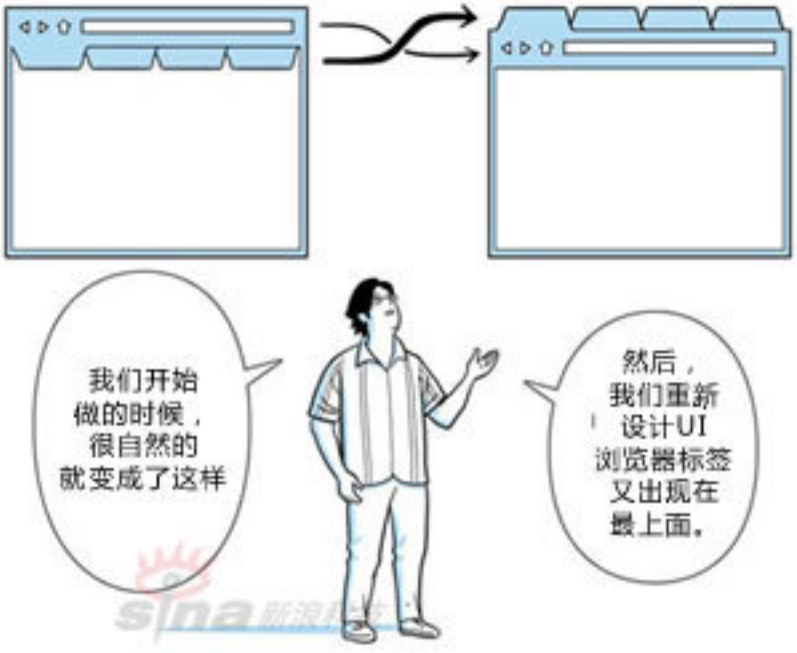


而且，因为我们知道所有的指针都在哪里，所以我们可以使用增量垃圾资源回收。

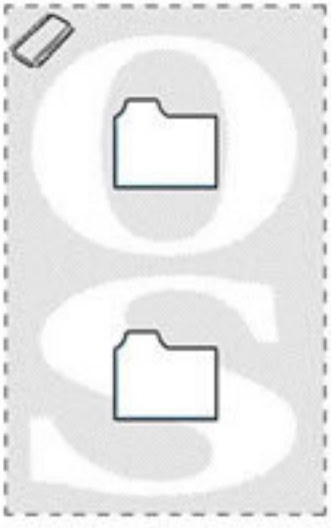


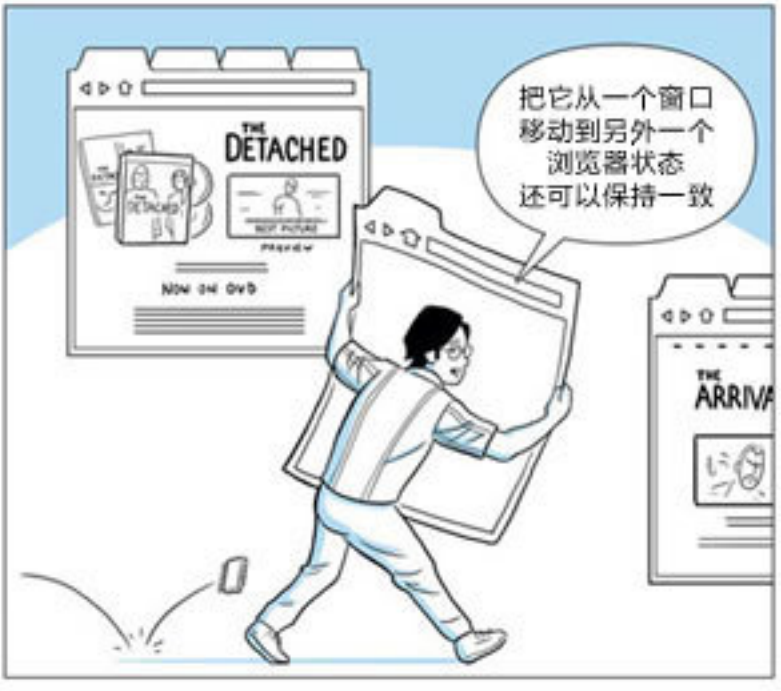
也意味着快速回收系统资源，处理100MB的数据仅需几微秒，不会造成浏览器假死。


这也意味着
为网络程序
提供更好的交互性，
比如：更流畅的拖拽。
Google Chrome使用
V8的API，但引擎的
内核部分是独立于
浏览器之外的。
V8
GOOGLE CHROME
所以，
其它浏览器
也可以调用它
——或者，
如果有其它项目可以
用Javascript脚本，
开发者可以直接调用V8。
V8
我们希望V8的性能可以
带来一个新的高度，
其它开发组可以继续提升其性能。
V8
如果系统变得更快，
那么你可以得到
更大更好更有创意的程序
限速
10100
翻译/制作：龚民



因为进程是分开的，
所以我们很容易
就可以把窗口独立出来






因为窗口标签是浏览器最重要的设计，
所以每个窗口都有自己的控制按钮。
还有自己的
地址栏。


这块区域，我们称之为“万能盒子”
cars


万能盒子处理的事情
可远不只网址……
它还可以提供
搜索建议，
您之前访问
较多的地址，
您未访问过的
但很出名的地址
还有更多……
cars
Search Google for cars
www.cars.com
Cars (2006)
Glen Murphy,
Software Engineer

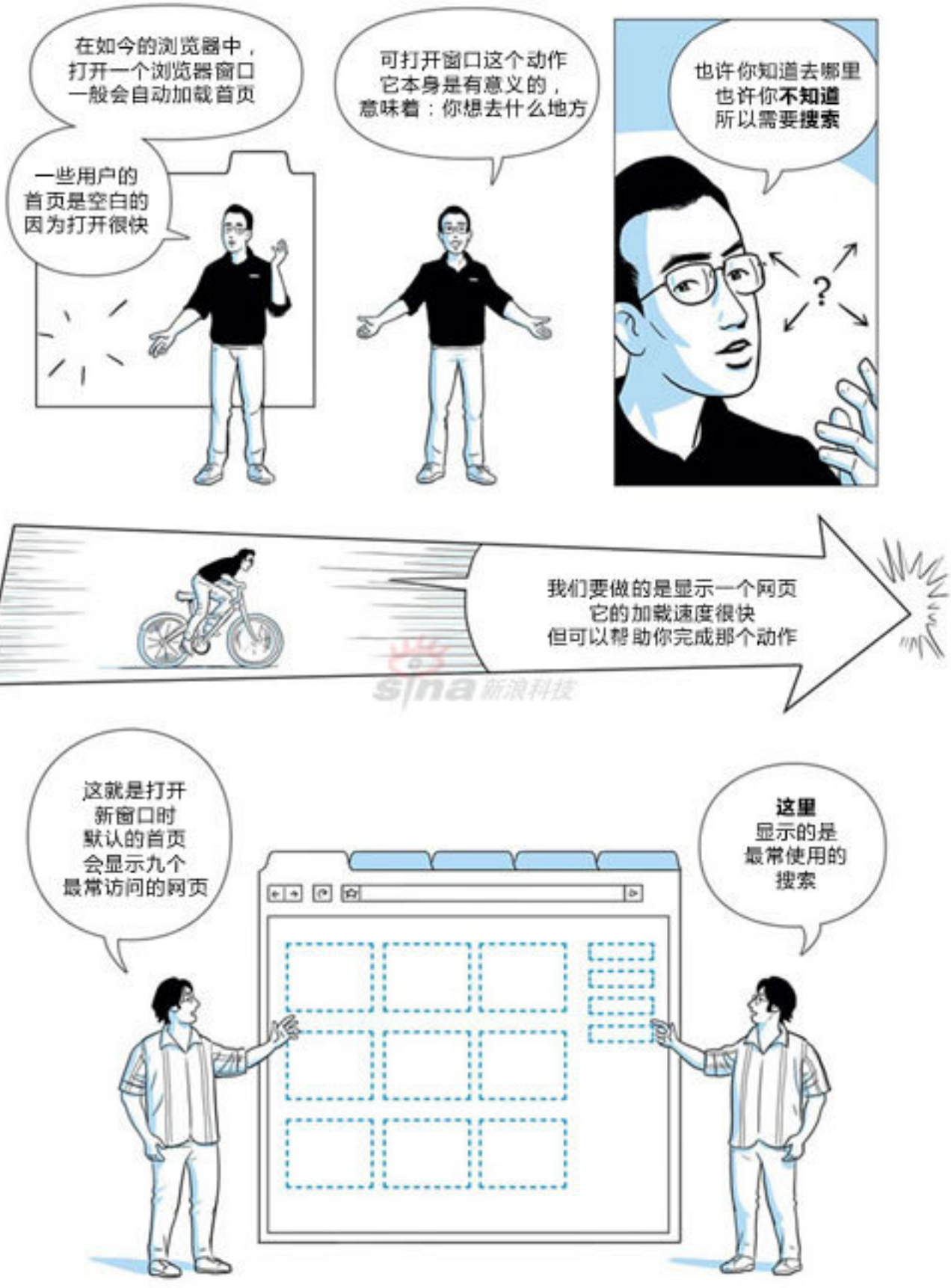

你可以全文搜索你的访问历史，
如果你昨天发现了一个
关于数码相机的好站点，
你无需加入收藏。
输入“数码相机”
四个字就
可以找回来。
digital camera
Search Google for digital came
www.digitalcamera.com
Nikon Digital SLR


当小组其它成员建议增加
“自动完成”的时候，
我说我不喜欢这个功能。
当我在地址栏输入的时候，
那些文字会自己蹦出来，
但哪一个都不是我需要的。
可是他们说，不不不，
请相信我，会很好用的。
然后，他们真的就
做出一个
令人称赞的功能。
自动完成功能决不会闪烁，
它非常完美，
非常艺术，
绝不分散注意力。


此外，它只会自动完成你以前直接输入过的网址。
输入 c 然后回车
很可能就会直接把你带入首页
cnn.com
TAP! TAP!
而绝对不会是……
cnn.com/2008/politics/07/27/campaign.wrap/index.html?iref=mp

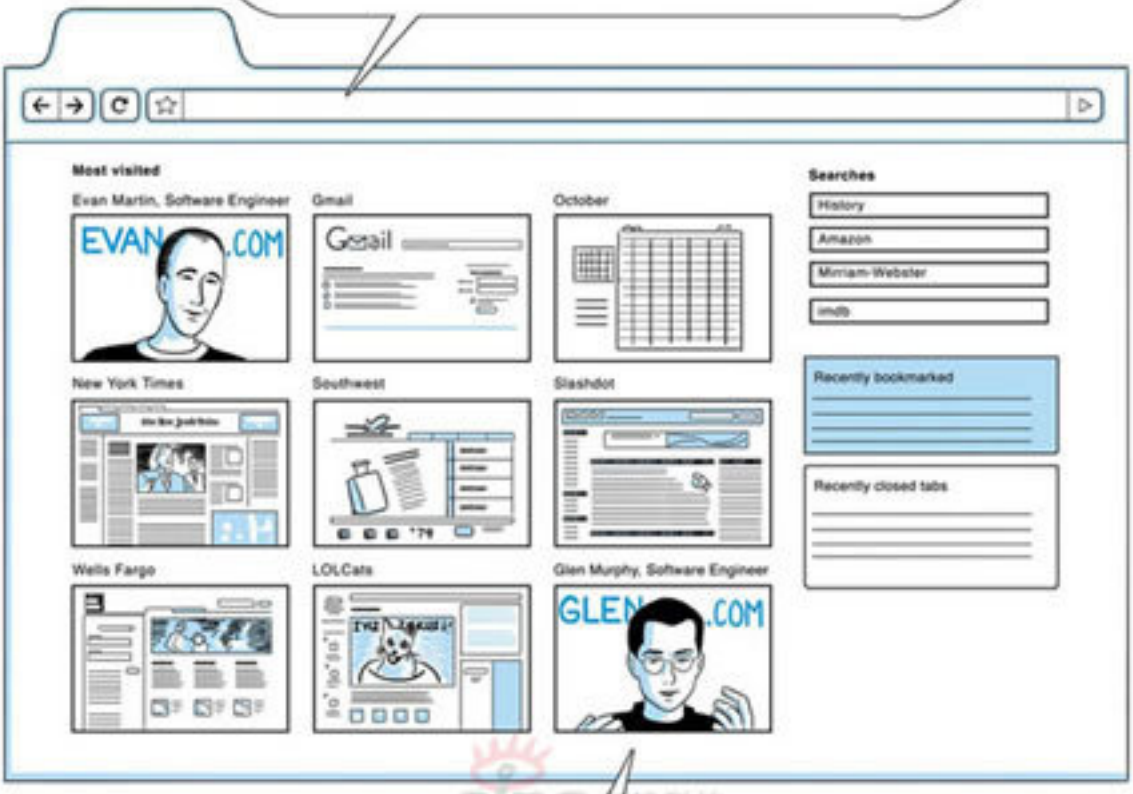

当你在亚马逊、维基百科
或者Google这样的站点搜索时——
Search
Books
Tufte
这些网页上的
搜索框会被
自动抓取到
你的系统里


这样一来，以后就可以在地址栏
使用自定义搜索，先输入站点的
名字，然后按下Tab键
a
tab
Search Amazon: Zamfir
CLICK!
回车



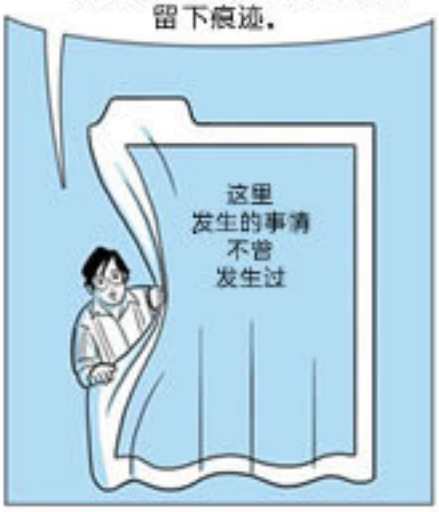
翻译/制作：美民

这就是你即将输入网址的页面，Google Chrome通过“万能盒子”来分析你的使用习惯，最终生成此页面。



你打开之后可能会想，我的网页干嘛都放在这里啊？
但过一阵子之后，你会发现这个页面真的成了**你的**浏览器。

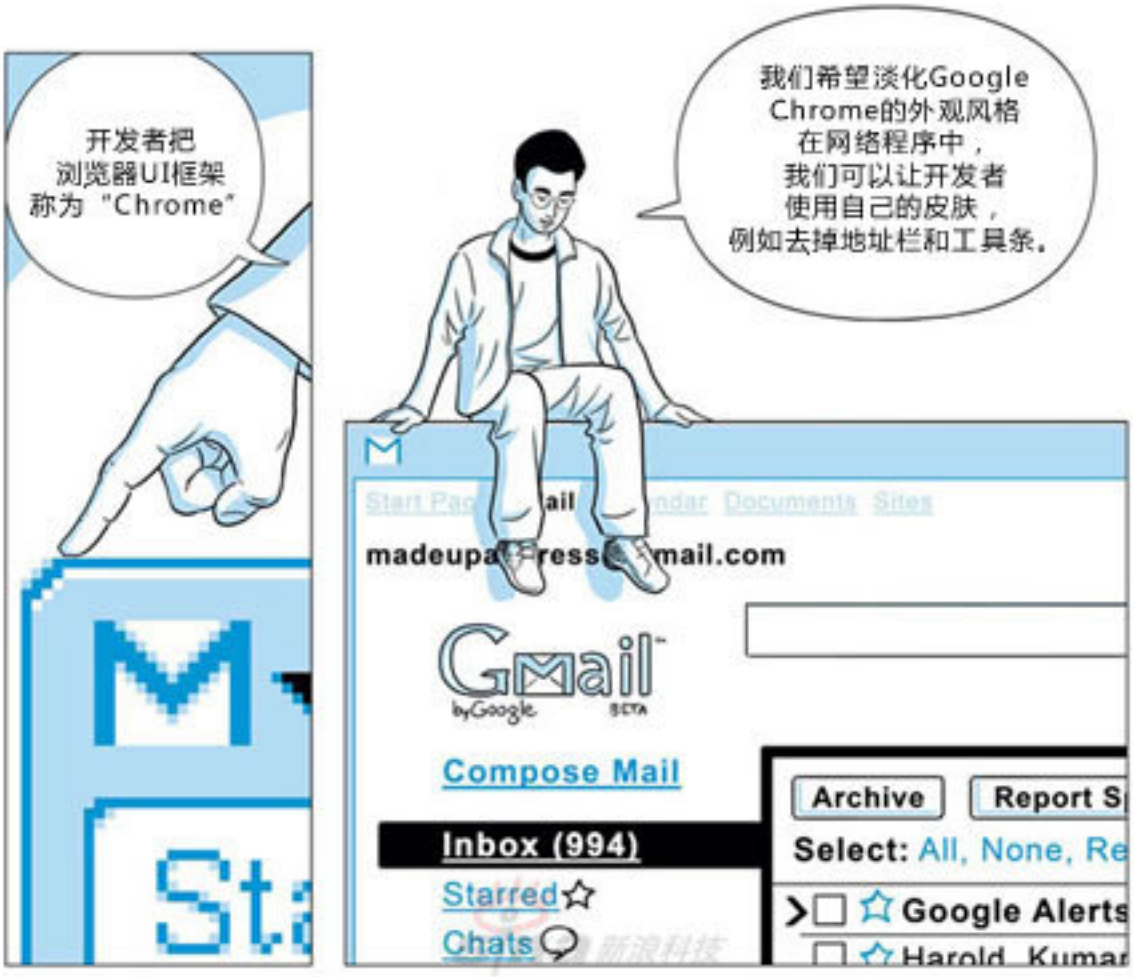
Google Chrome也有一种隐私模式，你可以创建一个“匿名窗口”。在这个窗口发生的一切事情都不会在你的电脑上留下痕迹。

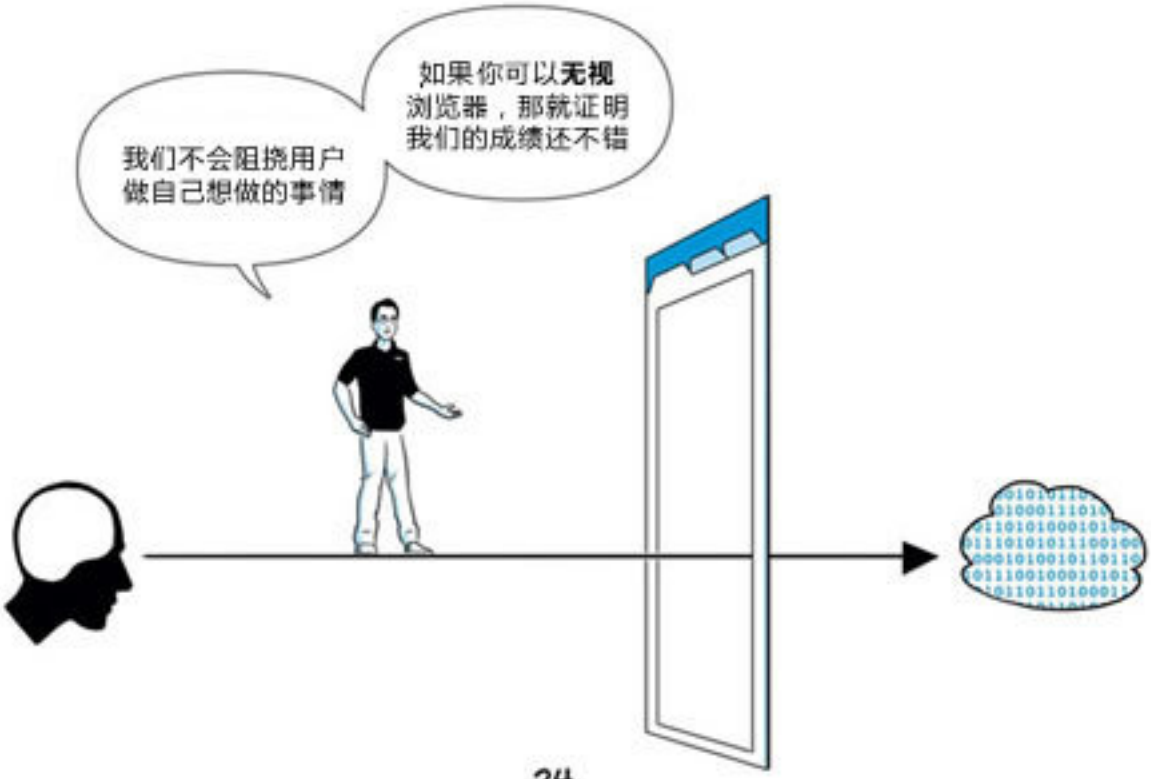


翻译/制作：龚民


你想让你的神秘礼物
继续成为惊喜吗？
也可以在其它窗口中
正常地浏览网页
在Chrome中
不会出现弹出窗口
Javascript没有
权限强制弹出
任何窗口
弹出窗口的
来源会显示
在页面中
EASY M
LOW! LOW RATES!
HOT! HOT! GIRLS!
BIG! BIG! BUKS!
而且会被
限制在这里
GULP!
假如这个窗口
是你想要的……
Audio Player
那就把它拖出来
它就会被升级成
一个新窗口。
BURP!

翻译/制作：龚民


开发者把
浏览器UI框架
称为 "Chrome"
我们希望淡化Google
Chrome的外观风格
在网络程序中，
我们可以让开发者
使用自己的皮肤，
例如去掉地址栏和工具条。
Gmail
Compose Mail
Archive
Inbox (994)
Starred
Chats
Google Alerts


我们不会阻挠用户
做自己想做的事情
如果你可以**无视**
浏览器，那就证明
我们的成绩还不错

翻译/制作：龚民


对于用户来说，
恶意程序和钓鱼程序是个大问题。
这影响了网上的信任度。
开始这个项目时，
我们面临了许多问题
其它浏览器都未曾经历过
Ian Fette,
Product Manager
John Abd-El-Malek,
Software Engineer


在那个时候，
浏览器的主要任务是
显示网页，
然后让那些
很酷的玩意儿
动起来。
没有金钱的获益，
没有人想在
用户的机器上
放置恶意程序。
Your 1998 Guide to HTML


现在完全不一样
恶意程序针对着
你的钱包而来
他们做的事情就是
盗窃你的密码
然后
把你的钱转走


在安全问题上，我们开始的时候
就假设浏览器并不安全
你最终一定会
遇到恶意程序
悲观主义者
Carlos Pizano,
Software Engineer

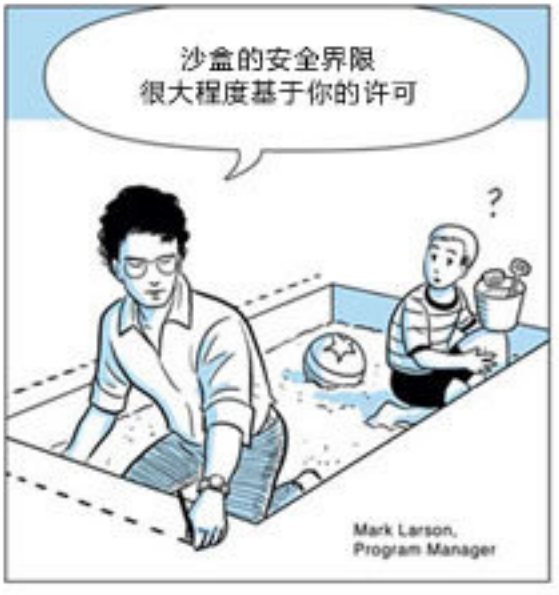

沙盒模式的目标是防止恶意程序安装到你的电脑中，
一个浏览器窗口中发生的事情不会影响到其它窗口。
所以，我们除去了
沙盒模式窗口的
所有权力。
他们可以运行，
但不能在你的硬盘上
写入任何数据。
也不能读取敏感
位置的文件。
例如：你的文档
和桌面。
CHROME PROCESS
PROCESS
PROCESS
PROCESS
PROCESS
或者
像沙盒模式小组
那样做——
PROCESS
我们把这个进程
放在一个盒子里
PROCESS
然后，
关入大牢！
SLAM!


也就是说
不会盯着你的
信用卡号码
不会
和鼠标互动
不会看着
你的退税记录
也不会让操作系统
在开机的时候
运行某个程序


也许窗口里也会运行
一些不好的东西
PROCESS


但只要关闭这个窗口
它就彻底不存在了
POP!
POP!


不会对你的电脑
产生影响
也不会对其它浏览器窗口
产生影响


沙盒的安全界限
很大程度基于你的许可
?
Mark Larson,
Program Manager


Vista使用修改版的BIBA安全机制
将行为分为三个级别
非常信任
一般信任
完全不信任
高
中
任
?

这个级别是
备份程序，升级程序
等等

高
中
低
?

这个级别是
其它所有正常的程序
包括：记事本、纸牌游戏、
计算器等等

高
中
低
?

读权限
的分配是
从低到高的

高
中
低
?

而**写**权限
的分配则是
从高到低的

高
中
低
?

一般来说，
接收和处理网络数据的程序
会被分配到较低的权限区

高
中
低
?

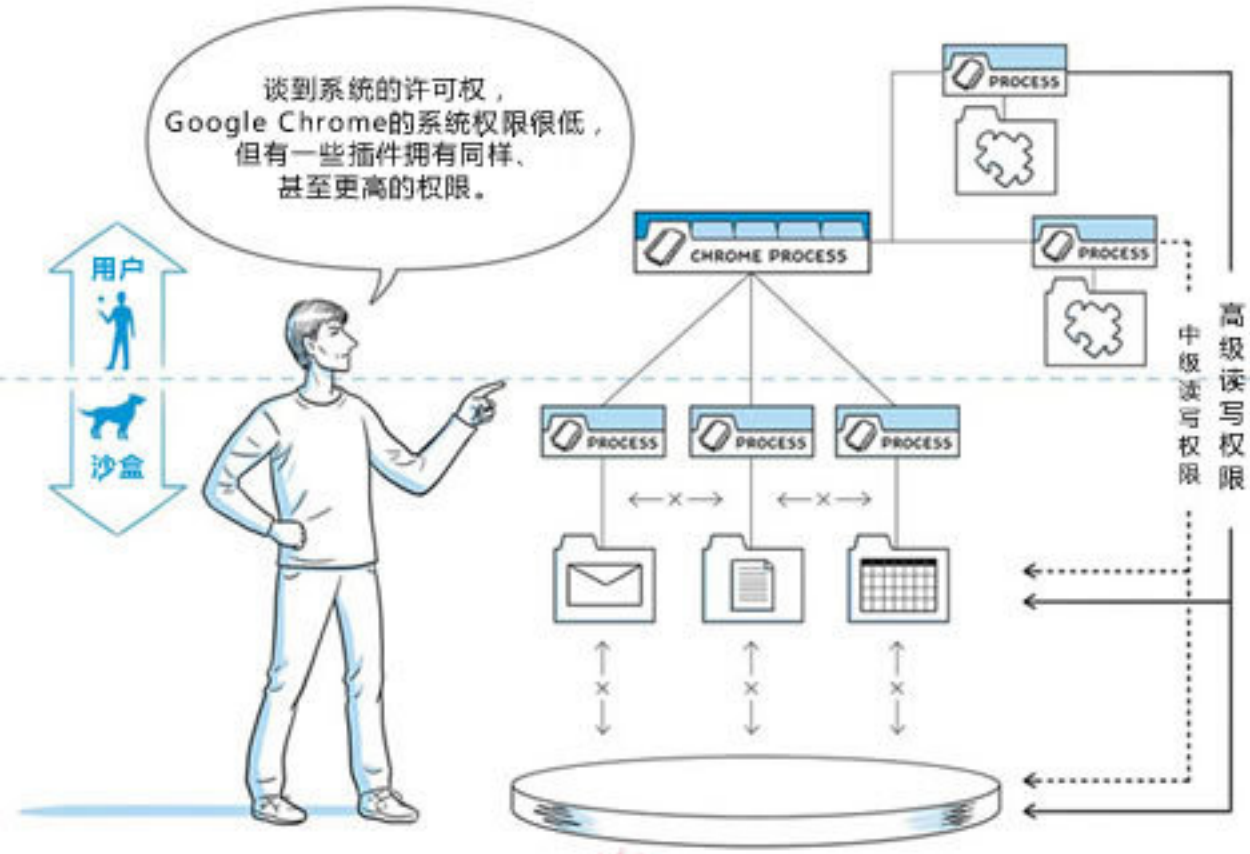
问题是，
与高级别权限不同
这里也有大量的敏感数据

高
中
低
?

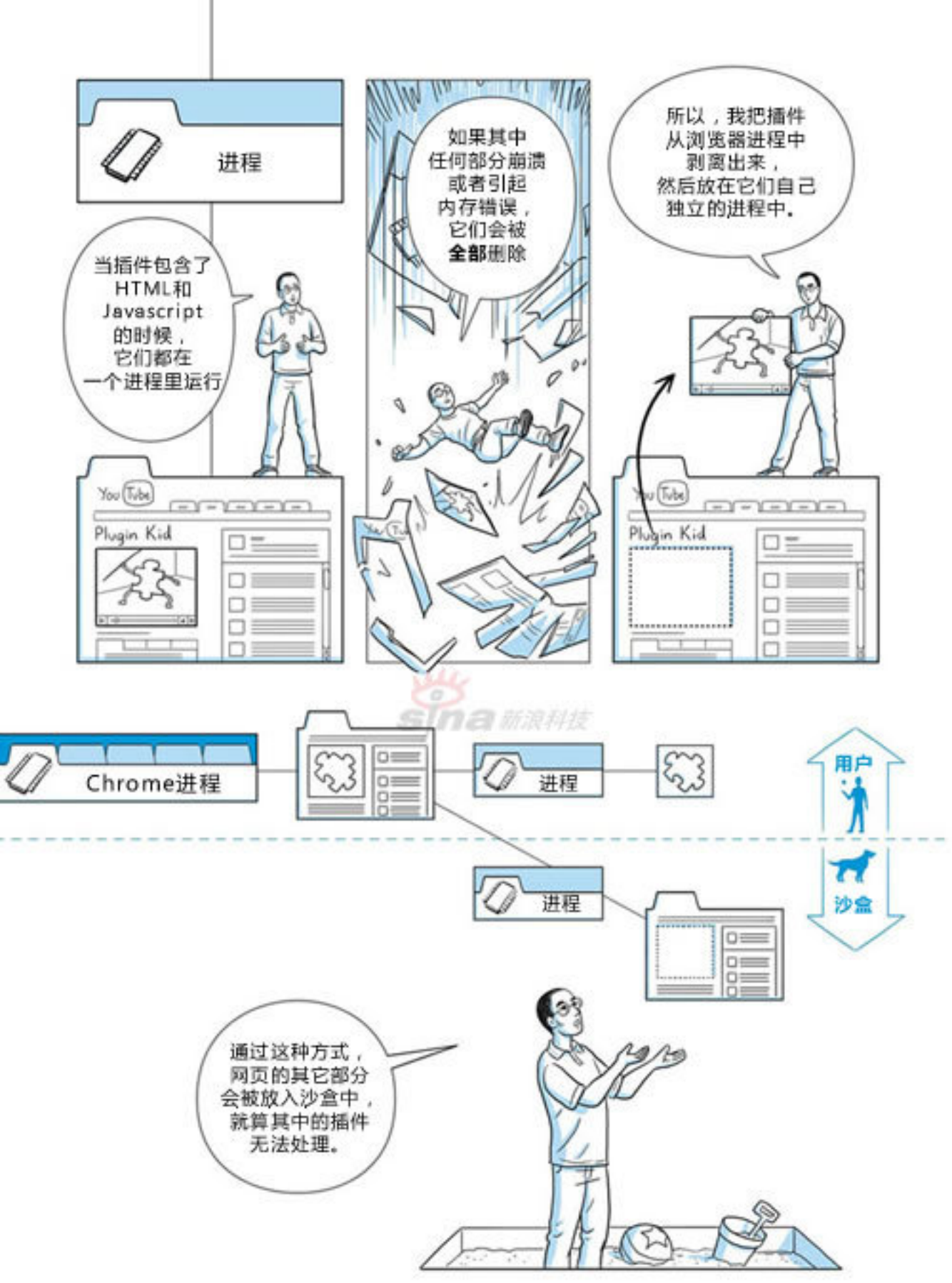
而这一级别的
程序
根本就**不能**
让它读取

高
中
低
?


在我们的模型中，
有**用户**，也有**沙盒**。
任何通信都**必须**由用户发起。
高
无
在这一边，**可以答复**
但无法接触到任何数据
除非用户自己提供
高
无
我们可以这么做，
因为所有的代码都是新的。
我们自己在写代码，
Google Chrome
拥有完全的控制权
HIGH
NONE
!SMASH!
只有一个例外
插件
因为网页
不仅仅是HTML和
Javascript



翻译/制作：龚民

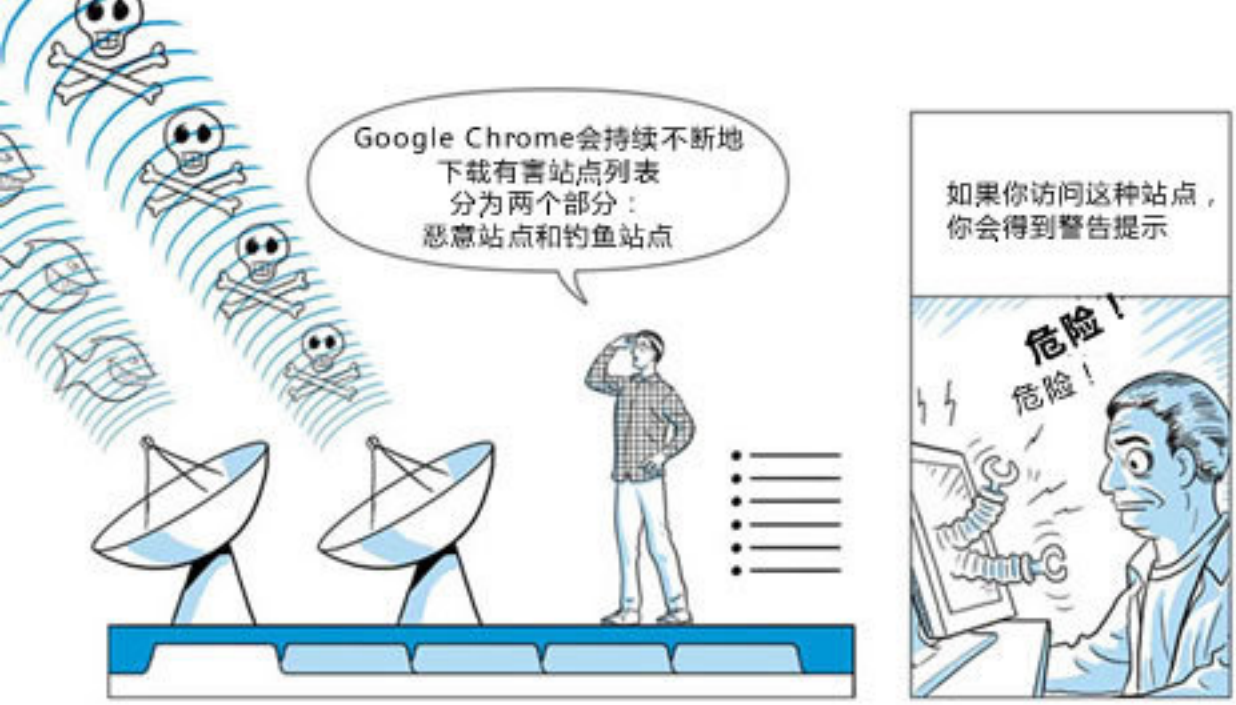

进程
当插件包含了HTML和Javascript的时候，它们都在一个进程里运行
Plugin Kid
如果其中任何部分崩溃或者引起内存错误，它们会被全部删除
所以，我把插件从浏览器进程中剥离出来，然后放在它们自己独立的进程中。
Plugin Kid
Chrome进程
进程
进程
用户
沙盒
通过这种方式，网页的其它部分会被放入沙盒中，就算其中的插件无法处理。


沙盒可以防止用户
遭受恶意软件袭击，
但无法防止
被**钓鱼软件**欺骗。
在典型的钓鱼案例中，
入侵者会发出邮件说“我是你的银行，
为确认你的身份，请提供帐号和密码”
等等……

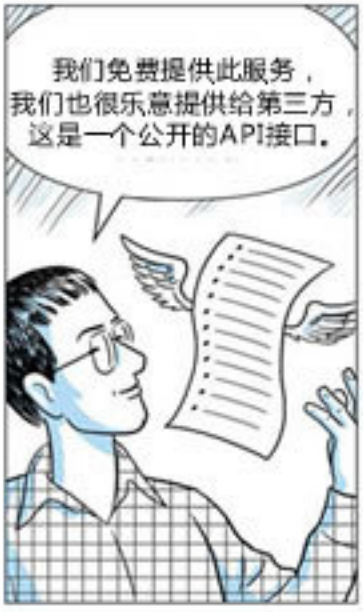

然后它们提供了一个不容易察觉的假网址，
并提供了几乎以假乱真的网页等着收集用户信息
http://www.(bank's name).com
View Your Accounts
Go to: Account Summary
Username:
http://www.(bank's name).login.com
View Your Accounts
Go to: Account Summary
Username:


很多钓鱼网站
在24小时内被关闭
但也有一些
得等上七天
才能被关闭


最难的部分在于
我们要在
零秒之内
找到它们
60


Google Chrome会持续不断地
下载有害站点列表
分为两个部分：
恶意站点和钓鱼站点

如果你访问这种站点，
你会得到警告提示
危险！
危险！

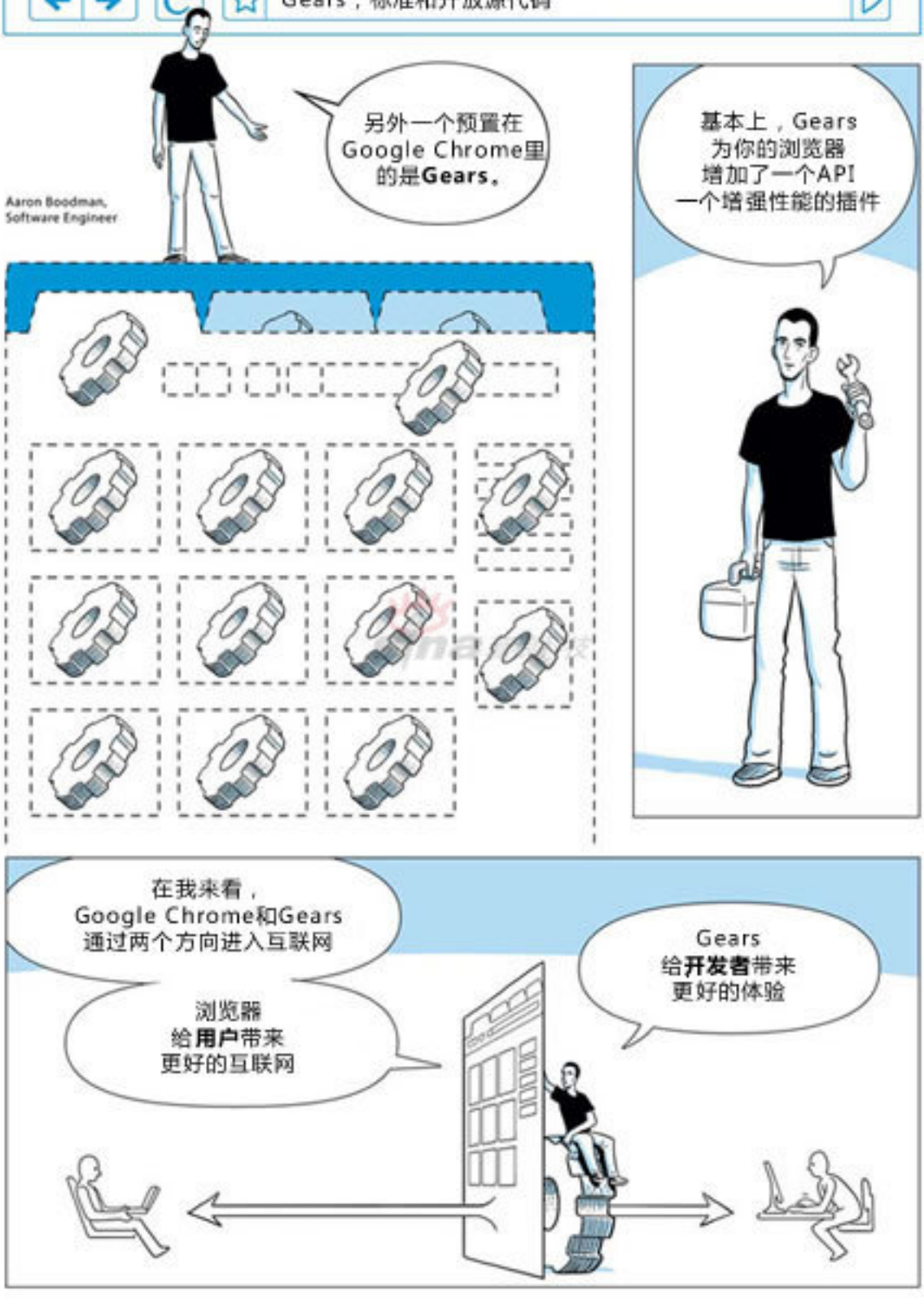

我们免费提供此服务，
我们也很乐意提供给第三方，
这是一个公开的API接口。


我们还有另外一个恶意软件列表。
包含了成千上万个对电脑有害的恶意软件信息。

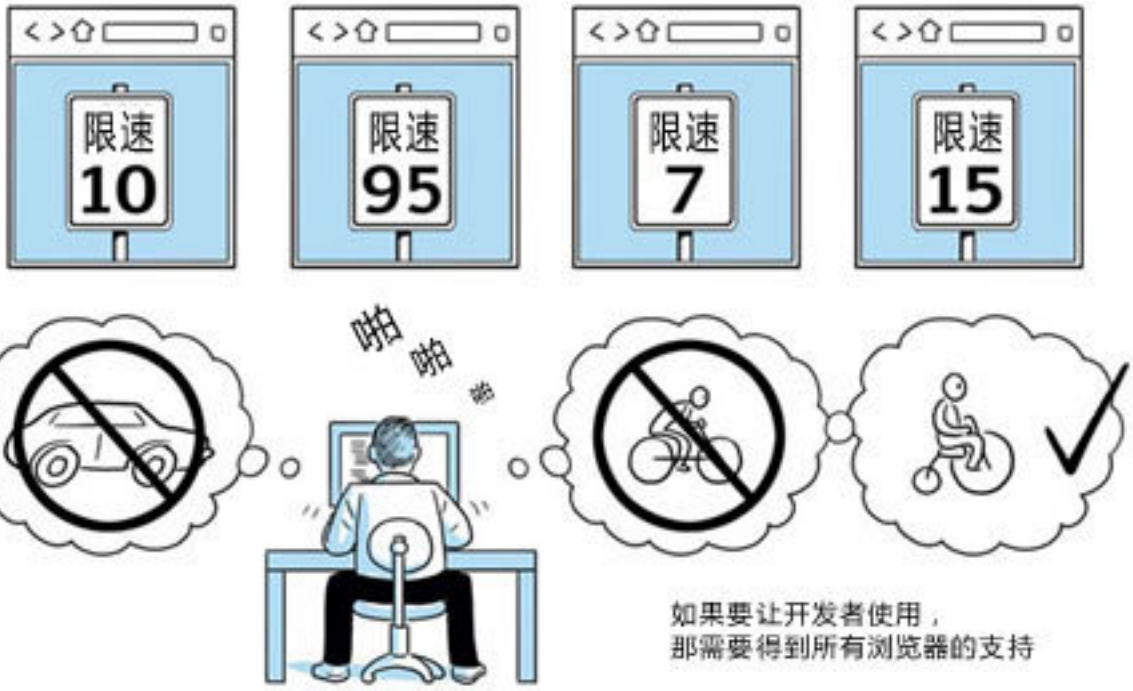

当我们发现
有害信息时，
我们会通知
网站的所有者。
通常都不是
他们故意这么做的，
而且
他们会很快
将这些有害信息
删除掉。
呃
？
啊，
抱歉！

翻译/制作：龚民

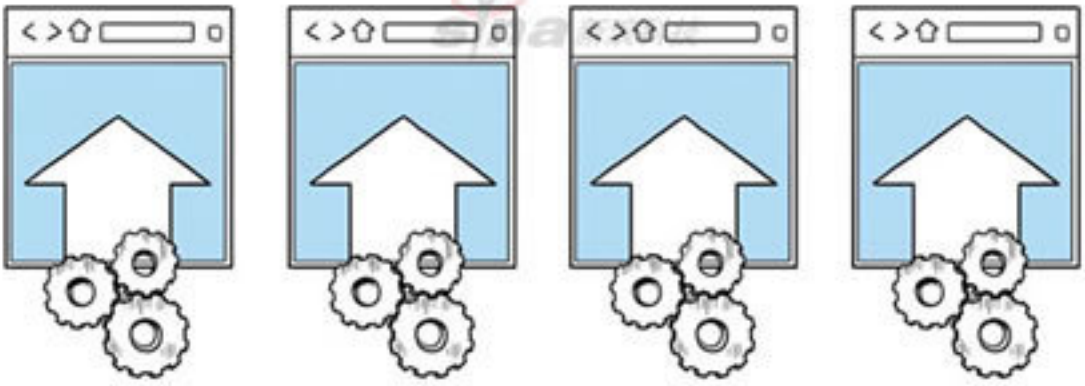
Gears，标准和开放源代码



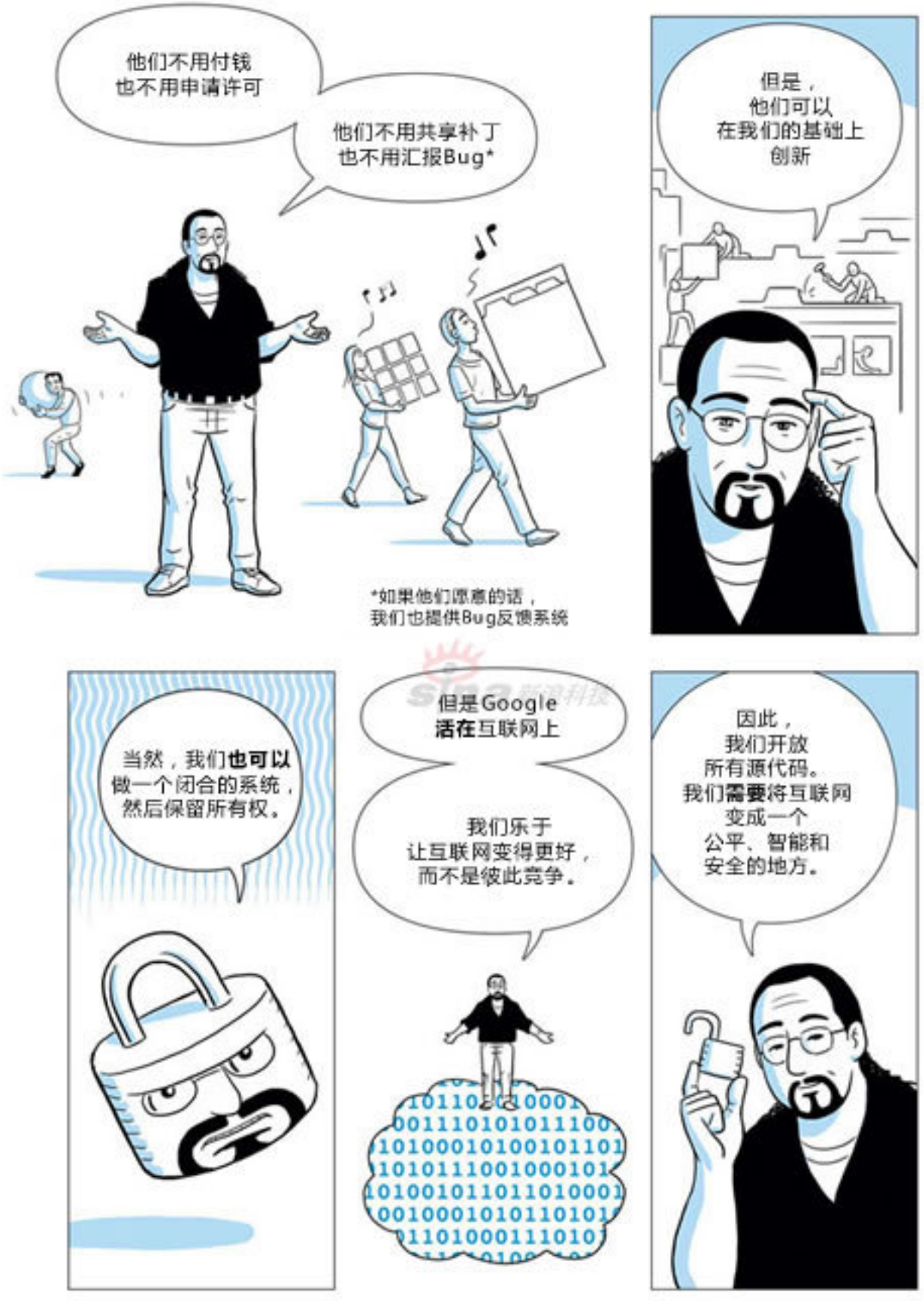
如今，基于浏览器的网络程序有很多局限，
每个浏览器都有自己不能做的事情，
如果一个很酷的功能只支持一个浏览器的话，那跟没有一样——



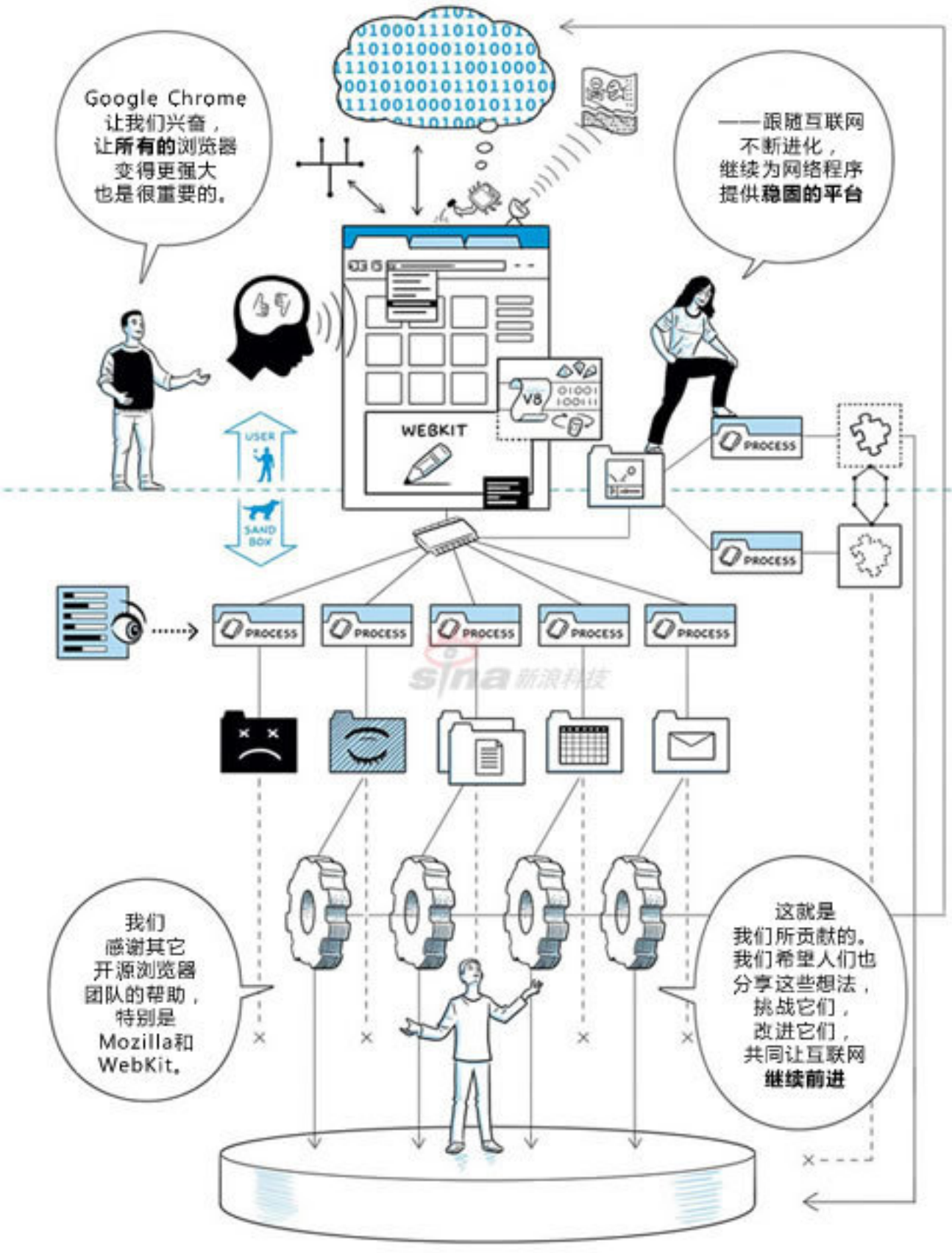
如果要让开发者使用，
那需要得到所有浏览器的支持




所以说，开放的标准
可以让浏览器更好
我们的团队已经做了
一些有趣的事情，
例如速度、稳定性、
界面和新的开始页
他们中的一些
将可能成为标准
有一些则不会
Chris DiBona,
Open Source Programs Manager
但是——
既然源代码
是开放的，
其它浏览器的
开发者也可以使用


他们不用付钱
也不用申请许可
他们不用共享补丁
也不用汇报Bug*
*如果他们愿意的话，
我们也提供Bug反馈系统
但是，
他们可以
在我们的基础上
创新
因此，
我们开放
所有源代码。
我们需要将互联网
变成一个
公平、智能和
安全的地方。
但是Google
活在互联网上
我们乐于
让互联网变得更好，
而不是彼此竞争。
当然，我们也可以
做一个闭合的系统，
然后保留所有权。

翻译/制作：龚民


Google Chrome
让我们兴奋，
让所有的浏览器
变得更强大
也是很重要的。
——跟随互联网
不断进化，
继续为网络程序
提供稳固的平台
WEBKIT
V8
USER
SAND BOX
PROCESS
PROCESS
PROCESS
PROCESS
PROCESS
PROCESS
PROCESS
我们
感谢其它
开源浏览器
团队的帮助，
特别是
Mozilla和
WebKit。
这就是
我们所贡献的。
我们希望人们也
分享这些想法，
挑战它们，
改进它们，
共同让互联网
继续前进

翻译/制作：美民

文案
Google Chrome团队

漫画
Scott McCloud