

使用 HTML5 进行硬件指纹识别

加比·纳基布利、吉拉德·谢莱夫、施兰·尤迪列维奇
以色列理工学院计算机科学系。

摘要—网络上的设备指纹识别已获得Windows 注册表值、屏幕分辨率和驱动程序 enu-

受到研究界和公司的广泛关注综合考察所使用的功能
商业市场也是如此。几乎所有的指纹识别功能

迄今为止提出的解决方案取决于设备上运行的软件。所有这些功能都
可以由用户更改，从而泄露设备的指纹。在本立场文件中，我们认为

要对设备进行指纹识别，请参阅 [1]。所有这些功能都是基于软件
的，也就是说，这些功能只能使用软件进行设置或更改。因此，它
们可以很容易地

HTML5 标准的出现催生了新的由用户更改。例如，只需更改

基于指纹特征的硬件浏览器访问网站时，用户可以挫败许多
设备的这些特征很难被掩盖或改变这些指纹特征。

从而提供更高的指纹置信度。我们提出了几种可能的指纹方法，允
许 HM

Web 应用程序来识别设备的硬件。我们还预
对设备 GPU 进行指纹识别的初步实验。

在本立场文件中，我们认为，最近出现的 HTML5 标准 [9] 催生了一
类新的指纹识别特征，这些特征基于时长日一个埃硬件设备本身
并不一定依赖于设备上安装的软件。这些功能更难实现

我引言

识别用户 - 无需其明确合作 - 只要用户使用相同的设备，他们就会提供

浏览网页是网站管理员梦寐以求的目标，它提高了设备 指纹的可信度。用户访问的网页。识别访问用户允许网站硬件功能可分
为两个子类：

打击欺诈行为并检测违反网站条款的行为。f us

另一方面，它可以用来损害某人的隐私

通过跟踪用户并识别他的浏览习惯，

历史。这最常用于投放广告

为用户量身定制。在大多数情况下，识别用户 wuittho

他的合作仅限于识别其所使用的设备

浏览网页。追踪

设备使用 HTTP cookies。这允许网站

将状态存储在用户的设备上，然后将其发送回
网站。

在过去的几年里，越来越多的病例被发现

HTTP cookies 被滥用来追踪用户及其

浏览历史[1]。这提高了用户社区

意识到 HTTP cookie 所带来的隐私威胁。

澳大利亚最近的一项研究[2]表明1在3用户数

在访问网站后的一个月删除 cookie。

此外，还有众多插件和浏览器扩展

允许用户监视其设备上设置的 Cookie，从而创建更复杂、更吸引人的 Web 应用程序

(例如 [3])。此外，大多数浏览器允许阻止在浏览器上运行的第三方应用程序。为了允许这些新功能和 Cookie (由未在列表中
列出的网站设置的 Cookie)，

地址栏，通常嵌入在页面上的广告

网站) [4], [5]。

这种普遍的 cookie 不可用促使广告依赖于系统底层硬件功能和跟踪器来寻找新的方式来跟踪用户及其浏览

历史。如今，有许多商业公司允许访问设备的硬件，这些公司通过提供“无 cookie”的设备识别

- 网站根据设备的硬件特性对设备进行指纹识别

尽管很少有研究涉及硬件指纹识别[6]-[8]，这些研究显示设备可以识别 HTML5，但有强烈的迹象表明

根据浏览器和操作系统打印功能

最值得注意的功能包括插件枚举、len

浏览器功能、User-Agent HTTP 标头、字体检测、查看网络上的设备指纹相关工作。

是可行的。

dab 本文的结构如下：在第二部分中，我们

在第三部分我们介绍了几种可能的硬件数据库
指纹识别方法可以通过网络使用，使用相机捕捉图片或视频。在第四部分中，我们展示了我们进行的初步实验的结果
如 [19] 所示，相机光学传感器的每个像素都有
根据设备的 GPU 特征对设备进行指纹识别。偏差很小但可测量。该偏差是本文第五节总结的线性函数。
照射到像素上的光的实际强度 I_e 。有少数研究利用像素偏差进行相机识别。文献 [20] 提出了一种确定相机

二、R 兴高采烈西兽人

有许多研究使用相机拍摄的 300 张照片来探索指纹参考偏差的方法。此网络客户端。如上所述，这些研究的绝大部分都为相机提供了独特的指纹。结果表明，基于软件的指纹识别方法能够以很高的概率将新照片的相关特征（主要是浏览器的特征）与拍摄该照片的相机相关联。

系统和驱动程序。参考文献 [7] 表明，参数 α 系统 $c)$ 扬声器/麦克风 [21]：主要规格
屏幕分辨率、浏览器插件、麦克风和扬声器等配置是频率响应图。系统字体以及 HTTP 标头的内容 A – 麦克风的频率响应是其标准化的输出 User-Agent 和 Accept – 允许对设备进行指纹识别。其他工作提出了更多的指纹识别方法，这些方法依赖于浏览器功能，例如历史记录和文件缓存 [10]，JarivpatScover 给定的频率范围。典型的麦克风或扬声器性能 [11]，以及与 JavaScript conforncmea 的偏差，其响应曲线在不同频率测试中有所不同 [12]。

此外，过去几年中已经证明
许多网站根据“麦克风或 cookie 的每个实例的超高频响应”来识别网络客户端。这些标识符存储在 locsaleaker 上，即使它们是同一型号，也不相同。主机以各种持久的方式不受 ab 的控制
因此浏览器无法对其施加标准限制
使用 HTTP cookies。这也是一种基于软件的方法。商品麦克风和扬声器 ± 2 db。它有
据我们所知，只有 [22] 中的两篇论文指出，频率的这种变化旨在根据 Web 客户端的硬件特性对其进行指纹识别。
参考文献 [14] 提出了使用渲染文本和 WebGL 的方法，该技术可以使用设备的场景在 HTML5<canvas> 元素上播放特定频率的音调，同时测量扬声器，同时使用画布的像素图记录播放的音频。不同的浏览器使用不同的麦克风。这允许网页以不同的方式测量文本和图形。差异源于扬声器和麦克风的频率响应。这种差异来自软件（浏览器和驱动程序）和硬件的混合

该方法同样可以适用于台式计算机。
– GPU – 配置。所提出的方法不 $d)$ 运动传感器 [23]：许多移动设备都打算通过配备加速度计和陀螺仪来区分两个 Web 客户端。这两个传感器
相同的软件和硬件配置，即使用 im
硬件功能。
参考文献 [15] 是我们知道的唯一一篇旨在哦是传感器的灵敏度和偏移量。理想情况下，为了根据隐式参数值区分两个 Web 客户端，参数值应该年代
硬件特性。建议的方法是测量偏差，例如，偏差可能由于制造商的不同而不同
web 客户端的 CPU 时钟偏差。测量结果并无差异。此外，除了形式之外，其他缺陷
使用 JavaScript 代码定期将时间戳和敏感度发送回服务器，可能会因不一致而产生误差。这项工作的灵感来自 [16]，其中展示了设备的时钟偏差可以对设备进行指纹识别。网页可以从这些传感器读取测量结果，从而可能计算出

三、H 硬件一个中远海运能源服务有限公司乌唱歌 HTML5

下面我们列出了网页上的硬件模块 $e)$ 全球定位系统 [25]：GPS 接收器对位置进行三角测量
可以使用 HTML5 直接或间接访问。对于每个设备，通过计算其与至少 3 个 GPS 站点的距离。我们参考用于访问的 API 文档，这些距离是通过测量信号发射的时间来计算的
硬件模块。并且对于每个设备，我们提出可能的
指纹识别方法的说明。
 $a)$ GPU [17]：现在所有的现代浏览器都是“硬件-先前的研究 [16] 表明，时钟的偏差可以识别
加速”，这意味着渲染图形可能会
使用设备的 GPU。various 的渲染延迟
图形可用于对 GPU 的时钟频率进行指纹识别，理论上，时钟的偏差不会影响计算和偏斜。在下一节中，我们将描述我们的初步实验
使用此指纹方法。

¹这种线性偏差通常称为模式噪声。

位置。尽管如此，在预定义的时间间隔内，屏幕上仍有许多错误来源。计算接收器位置时，此测量构成了 GPU 指纹的基础。假设我们的效应和多路径效应。此类错误不会在指纹测试中发生，指纹测试是占用 GPU 的唯一过程

在位置确定过程中的计算结果，并且隐含地表示渲染帧的数量在很大程度上取决于时钟偏差导致的误差。因此，GPU 的参数（例如时钟频率、核心数量）可能导致位置计算中时钟偏差

以及其他影响 GPU 性能的参数。没有完全纠正。我们假设，采取多重措施，但是，允许访问 GPU 的软件 – GPS 的位置测量可能会暴露这种偏差。浏览器和 GPU 驱动程序——也有一定的影响

f) 电池[26]: 随着时间的流逝，电池会逐渐消耗 GPU 性能。渲染帧数并且其容量会下降。这种情况发生的速度也受时钟偏差的影响，但影响程度要小得多，取决于许多因素，例如气候、使用情况和 GPU 的充电情况。请注意帧模式的时间间隔 [27]。容量损失会影响使用 CPU 时钟测量渲染速度的速度。

可以充电或放电。因此，每个设备都有 S 由于每秒渲染帧的速率有一个最大值。充电/放电率是其独有的。电池充电/放电率的值为 60（这是计算机常用的刷新率），设备（即智能手机、平板电脑显示器）必须渲染复杂的图形，而笔记本电脑则需要渲染这些图形）。...。

当然，充电/放电速率并不
不仅取决于电池容量，还取决于 cturren

A. 实验

设备上的活动性能和过程剧院在我们的实验中，我们制作了一个显示当前在其上运行的 3D 的网站。一个成功的指纹识别方法分为三个阶段。每个阶段显示增加的单个
需要找到一种方法来消除这些因素。

复杂的图形。每个阶段持续 15 秒。在此期间，我们测量了三个 5 秒间隔内渲染的帧数。渲染过程执行

IV. F 印记鸟唱图形处理器

下面我们介绍使用 requestAnimationFrame() API 进行 fingerprtrin 的初步尝试。此 API 发出信号设备使用其 GPU 进行渲染。尽管结果令人鼓舞，但动画过程应该被调用，但我们的目的不是在此展示设备显示屏下一次刷新前的完整 GPU 渲染。动画

方法，而是提出这样的方法

修改过程本身会调用此 API，因此必须

是可能的。我们的目标是定期基于显式特征对 GPU 进行指纹识别。实验网站可以在这里找到：特征 – GPU 时钟频率 – 以及基于隐式特征：. herobo.com。我们计算平均值

特征——GPU 时钟偏差。后者需要对每个相位进行 3 次测量。从而通过 [16] 中提出的时钟偏差方法获得指纹。在本文中

为每个设备的每个阶段进行指纹识别。我们为 130 台设备进行了指纹识别

一台计算机正在利用其 CPU 时钟偏差进行指纹识别。IDNEVICES；其中 34 个被多次指纹识别。对于这种方法，许多带时间戳的数据包被定期发送，为了简化分析，我们将实验限制在仅由设备进行。另一台计算机拾取了这些数据包，

Desktop 和笔记本电脑。

计算了第一台计算机的 CPU 偏差。更准确的

，电话乙是。结果

该方法测量了第一台计算机的 CPU 的偏斜相对

第二个的 CPU 偏差。正如人们所预料的那样，我们首先测量了每台计算机和每个阶段吨时他 95

两台计算机之间的网络抖动有显著影响。两次测量值之差的百分位数

对倾斜测量的影响。为了平均 0（即每 5 秒渲染的帧数）。我们使用

95 百分位数，而不是最大差异

这种抖动必须发送许多带有时间戳的数据包，因此

延长指纹识别过程。尽管如此，sendhineg tdiscriminator 仍会忽略任何异常值，这些异常值最显著地是由

时间戳到另一台计算机对于此手指尖nrgin浏览器窗口离开焦点并且不显示在

方法，因为不能用 osuctreen 测量时钟的偏差。95 百分位数差异计算为

另一个参考时钟。5 帧。然后我们为每个阶段绘制了

我们的指纹识别方法的基本思想是使用宽度为 5 帧的箱体进行简单的相位测量。我们利用 HTML5 来使用设备的 CPU，直方图如图 1 所示。在测量设备 GPU 时钟指纹分布时，参考时钟的熵可以在表中找到

偏差。也就是说，我们努力通过测量来对设备进行指纹识别。从图 1 和表 1 中可以明显看出，随着设备 CPU 和 GPU 的相对时钟偏差，下划线图形更复杂，指纹允许

不幸的是，与 CPU 不同，没有 JavaScript API 可以更好地区分不同的计算机。

合作plex 阶段能够产生 5.14 的指纹熵

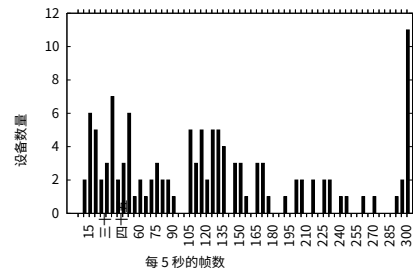
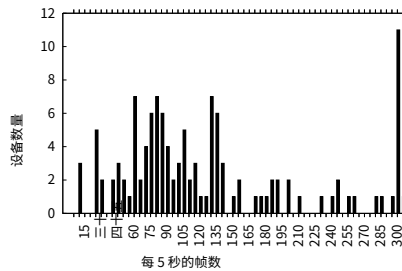
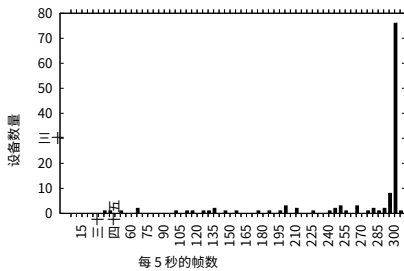
获取 GPU 时钟的时间戳。因此，我们必须

间接方法来测量 GPU 的时钟 skebwi.ts。我们怀疑更复杂的图形会产生

我们采用的指纹识别方法很简单，熵值较高。

我们使用 WebGL [28] 在 2 在这种情况下，浏览器会自动减少

HTML5 画布。我们测量渲染的帧数r埃nd每秒所需的帧数。



(a) 第一阶段结果（最不复杂的图形） (b) 第二阶段结果（中等复杂图形） (c) 第三阶段结果（最复杂的图形）

图 1. 渲染帧数分布

第一阶段	第二阶段	第三阶段
2.8	5.03	5.14

表一

电视阶段的指纹熵[息税前利润]

200	236	234
249	177	195
182	190	232

表二

弗阶段期间测量的印记值三为了9不同的
具有相同硬件和软件的计算机
规格

请注意，这个初始实验实际上测量的是 GPU 的性能。如上所述，尽管影响这一性能的最重要因素是硬件

GPU 的效率。使用 GPU 的软件效率Web 2.0 时代”，2009 年。GPU（浏览器和 GPU 驱动程序）也会影响其性能[。7] P. Eckersley，因此，可能需要进行更复杂的指纹测试来消除软件的影响。

我们还在 9 台具有相同硬件和软件配置的台式计算机上运行指纹测试3蒂奥内
指纹图谱结果见表 2。指纹图谱[10] A. Juels、M. Jakobsson 和 T. Jagatic，在每个计算机的多个实验中都保持一致。结果令人鼓舞，表明 GPU 指纹识别
允许区分具有相同硬件的计算机和软件配置。fingerp 的差异实际上比我们最初预期的要宽。似乎除了 GPU 时钟偏差之外，同一型号的 GPU 之间还有更多因素不同。成功的指纹识别方法需要考虑到这一点。

V、C 结论

在本文中，我们指出了最近[1吨5]D.-J. 黄K.-T. 杨，C.-C. Ni, W.-C. 滕，T.-R. H 答案和 Y.-J. Lee，HTML5 的出现使基于特征的一类新的强大的指纹识别功能成为可能

设备硬件而不是软件[1它6] T. Kohno、A. Broido 和 K. Claffy，“远程物理骰子手指运行。这样的硬件功能不仅可以区分具有不同硬件配置的设备之间[你17]W3C，“HTML Canvas 2D 上下文”，http://www.w3.org/TR/2dcontext/。

3 电脑型号：HPZ220，显卡：Nvidia Quadro 60S0；，W dows 7 SP1，浏览器：Firefox。

还可以区分具有相同硬件配置的设备。我们介绍了一些硬件指纹识别的想法。并展示了使用其 G.PU 对设备进行指纹识别的初步实验的令人鼓舞的结果

R 参考文献

- [1] N. Nikiforakis、A. Kapravelos、W. Joosen、C. Kruegel、P 菲埃森斯以及 G. Vigna，“无 Cookie 怪物：探索生态系统 网络-基于设备指纹识别” 安全与隐私 (SP)，2013 IEEE 研讨会.IEEE，2013 年，第 541-555 页。
- [2] comScore，“删除 Cookie 对网站服务的影响 广告服务器澳大利亚的气候指标”，2011 年 1 月。
- [3] “Lightbeam：照亮那些在看着你的人”，http://www.mozilla.org/en-US/lightbeam/。
- [4] “禁用 第三者 曲奇饼 在 火狐 到停止 一些 跟踪类型 经过 广告商”，http://support.mozilla.org/en-US/kb/disable-third-party-cookies。“Chrome 帮助 - 管理您的 cookie 和网站数据”，https://support.google.com/chrome/answer/95647?hl=en。
- [5] JR Mayer，“任何人.....小册子作者：互联网中的
- [6] “你的网络浏览器有多独特？” 磷在隐私增强技术Springer，2010，第1-18页。
- [8] T. Yen、Y. Xie、F. Yu、R. Yu、和 M. Abadi，“网络上的主机指纹识别和跟踪：隐私和安全影响” 磷我mNDSS 会议记录，2012 年。
- [9] R. Berjon 等。等人，“HTML5 - 词汇表和关联A 培训绩效指标 HTML 和 XHTML”，http://www.w3.org/TR/html5/，2014 年。“Cache Cookoiersbrfowser 身份验证”，安全与隐私，IEEE 研讨会，2006 年 5 月。
- [10] K. Mowery、D. Bogenreif、S. Yilek 和 H. Shacham，“Feinrg 印刷 javascript 实现中的信息，”我西 n2SP，IEEE 计算机社会，2011 年 5 月。
- [12] M. Mulazzani 等人，“使用 JavaScript 引擎指纹识别实现快速可靠的浏览器集成”，西 n2SP，IEEE 计算机学会，可能 2013 年。
- [1d3] M. Ayenson、D. Wambach、A. Soltani、N. Good 和 C. Hoaogflne，“Flash cookies 和隐私 ii：现在有了 html5 和 etag resn 片吧”可在 SSRN 1898390 获得，2011 年。
- [14] K. Mowery 和 H. Shacham，“像素完美：html5 中的指纹识别画布”，2012 年 5 月。
- [15] K. Mowery 和 H. Shacham，“基于时钟偏差的克隆环境中的客户端设备识别”。艾娜、L. Barolli、T. Enokido、F. Xhafa 和 M. Takizawa，编辑。IEEE，2012 年，第 526-533 页。
- [16] “可靠和安全计算，IEEE 交易，第 2 卷，第 2 期，第 93-108 页，2005 年。
- [18] 一，“HTML 媒体捕获”，http://www.w3.org/TR/html-media-capture/。
- [19] G. 霍尔斯特，CCD 阵列、相机和显示器。SPIE 光学工程出版社，1998 年。

- [20] J. Lukás、JJ Fridrich 和 M. Goljan, “数字摄像机 航空识别来自传感器模式噪声我, 埃” *EE 信息取证学报* 和安全, 第 1 卷, 第 2 期, 第 205-214 页, 2006 年。
- [21] W3C, “Web 音频 API”, <http://www.w3.org/TR/webaudio/>。
- [22] “智能手机加速度计ID”[http://www.sfgate.com/technology/](http://www.sfgate.com/technology/dotcommentary/article/AcceleromeID) 秒”, tesr-智能手机-秒-4885.7p1h1p, 2013。
- [23] W3C, “设备方向 事件 规格,” <http://www.w3.org/TR/orientation-event/>。
- [24] S. Dey 等人, “AccelPrint: 乙酰胆碱计的缺陷使智能手机可追踪”, 否 n.决策支持系统. ISOC, 2014 年。
- [25] W3C, “地理定位 API 规格,” <http://www.w3.org/TR/geolocation-API/>。
- [26] —, “电池状态API”, <http://www.w3.org/TR/battery-status/>。
- [27] R. Spotnitz, “锂电池容量衰减模拟 o-ni 电池” *电源杂志*, 第 113 卷, 第 1 期, 第 72-80 页, 2003 年。
- [28] khronosgroup, “WebGL规范”, <http://www.khronos.org/registry/webgl/specs/01/>。