华为专题前沿论文最新进展 14 篇
2018.11.04 方建勇

提示：采用手机 safari 微软翻译技术

1. **5gperf: 5g 的信号处理性能**

   作者:g. haains, w. suijlen, w . liang, z. wu

   文摘: 5gperf 项目由**华为**研究团队于 2016–17 进行。它关注 5g 基站原型信号处理算法的加速问题。它改进了已经优化的 simd 并行 cpu 算法，并设计了一种新的软件工具，在将 matlab 代码转换为优化的 c 时提高程序员的工作效率

   2018 年 10 月 25 日提交;最初宣布 2018 年 10 月。

2. **超越谷歌游戏：中国安卓应用市场的大规模比较研究**

   作者:王浩宇, 刘哲,梁景岳,纳塞奥·瓦利纳–罗德里格斯, 姚国,李丽, 胡安·塔皮多尔, 曹景村, 徐国爱

   摘要: 中国是世界上最大的 android 市场之一。由于中国用户无法访问谷歌游戏购买和安装 android 应用，一些独立的应用商店已经出现，并在中国应用市场上竞争。一些中国应用商店是预安装的供应商特定的应用市场（如**华为**、小米和 oppo），而其他应用商店则由大型科技公司（如百度、奇虎 360 和腾讯）维护。这些应用商店的性质和通过它们提供的内容差别很大，包括它们

的可信度和安全性保证。截至今天，研究界还没有深入研究中国安卓生态系统。为了填补这一空白，我们推出了第一个大规模的比较研究，涵盖了从 16 个中国应用市场和谷歌 play 下载的 600 多万个 android 应用。我们的研究重点是跨应用商店的目录相似性、它们的功能、发布动态以及各种形式的不当行为（包括存在假的、克隆的和恶意的应用）的普遍程度。我们的发现还表明了跨应用商店的异构开发人员行为，包括代码维护、第三方服务的使用等。总体而言，中国应用市场的表现要严重得多，因为中国的应用市场采取了积极措施，保护移动用户和合法的开发者免受欺骗和虐待行为者的侵害，其现状明显高于 google play。少

2018 年 9 月 26 日提交;**最初宣布** 2018 年 10 月。

3. **基于图形的推荐系统的中毒攻击**

作者:方明红,杨国雷，龚振强,刘佳

摘要: 推荐系统是许多 web 服务的重要组成部分，可帮助用户找到符合其兴趣的项目。几项研究表明，推荐系统容易受到中毒攻击，攻击者将假数据注入给定的系统，以便系统根据攻击者的需要提出建议。然而，这些中毒攻击要么与推荐算法无关，要么经过优化，推荐不基于图形的系统。与基于关联的规则和基于矩阵因素的推荐系统一样，基于图形的推荐系统也在实践中部署，例如 ebay、**华为**应用商店。然而，如何为基于图形的推荐系统设计

优化中毒攻击仍是一个悬而未决的问题。在这项工作中，我们对基于图形的推荐系统的中毒攻击进行了系统的研究。由于资源有限，为了避免检测，我们假设可以注入系统的假用户数量是有限制的。关键的挑战是如何将评分分数分配给假用户，以便向尽可能多的普通用户推荐目标项目。为了应对这一挑战，我们将中毒攻击作为一个优化问题来解决，它决定了假用户的评分分数。我们还提出了解决优化问题的技术。我们评估我们的攻击，并将它们与白盒（建议算法及其参数已知）、灰盒（推荐算法是已知的，但其参数未知的）和黑盒（推荐算法是已知的）下的现有攻击进行比较未知）使用两个实际数据集的设置。我们的结果表明，我们的攻击是有效的，并且优于现有的基于图形的推荐系统的攻击。例如，当 1% 的假用户被注入，我们的攻击可以使目标项目推荐到 580 倍以上的正常用户在某些情况下。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

4. **基于 csi 的大型 mimo 户外本地化：一种学习方法的实验**

作者:亚历克西斯·德克恩格、路易斯·加西亚·奥尔多涅斯、保罗·费朗、何高宁、李伯杰、张伟、 maxime guillaud

摘要: 我们报告了使用基于学习的方法推断蜂窝网络的移动用户在单元中的位置的实验结果，对于 5g 型大规模多输入、多输出（mimo）系统。我们描述了如何使用从 csi 计算的样本空间协方

差矩阵作为学习算法的输入，该算法试图将其与用户位置相关联。我们讨论了几种学习方法，并深入分析了极端学习机器在定位问题上的应用，这些机器有理论上的近似性能基准。利用**华为** 5g 试验台上收集的实验数据验证了该方法的有效性，提供了一些性能和鲁棒性基准，并讨论了在 5g 网络中部署这种技术的实际问题。少

2018 年 6 月 19 日提交;**最初宣布** 2018 年 6 月。

5. **面向移动设备的高性能视频对象检测**

作者:朱希洲,戴继峰,朱兴奇,魏一晨,陆元

摘要: 尽管最近在桌面 gpu 上成功地检测了视频对象，但它的体系结构对于手机来说仍然太重了。稀疏特征传播和多帧特征聚合的关键原则是否适用于非常有限的计算资源也尚不清楚。本文提出了一种用于手机视频对象检测的轻量级网络体系结构。在稀疏关键帧上应用轻量级图像对象检测器。一个非常小的网络，光流，是为建立帧之间的对应而设计的。设计了一个流导向 gru 模块，以有效地聚合关键帧上的特征。对于非关键帧，执行稀疏特征传播。整个网络可以端到端进行培训。该系统在手机上的 map 得分达到 60.2，速度为 25.6 fps (如**华威** myt 8)。少

2018 年 4 月 16 日提交;**最初宣布** 2018 年 4 月。

6. 深度 fm: 用于 ctr 预测的端到端宽和深度学习框架

作者:郭惠峰,唐瑞明,叶云明,李振国,何秀强,董振华

摘要: 了解用户行为背后复杂的功能交互对于最大限度地提高推荐系统的点击率至关重要。尽管取得了很大进展，但现有方法对低阶或高阶交互有强烈的偏见，或依赖于专业知识特征工程。本文证明了建立一个强调低阶和高阶特征交互的端到端学习模型是可能的。在新的神经网络体系结构中，拟议的深度 fm 框架结合了用于推荐和深度学习的因子化机器的功能，用于特征学习。与谷歌最新推出的宽深模型相比, deepfm 对其 "宽" 和 "深" 组件都有共享的原始功能输入，除了原始功能外，不需要功能工程。deepfm 作为一个通用的学习框架，可以将各种网络架构整合到其深层组件中。本文研究了深 fm 的两个实例，其 "深" 成分分别为 dnn 和 pnn，我们将其称为 deepfm-d 和 deepfm-p。在基准数据和商业数据上，进行了全面实验，以证明 deepfm-d 和 deepfm-p 相对于现有的 ctr 预测模型的有效性。我们在**华为**应用市场进行在线 ab 测试，发现与工程良好的 lr 模型相比，deepfm-d 在生产环境中的点击率提高了 10% 以上。我们还介绍了在**华为**应用市场部署我们的框架的相关实践。少

2018 年 5 月 16 日提交;**v1** 于 2018 年 4 月 11 日提交;**最初宣布** 2018 年 4 月。

7. 移动应用的 gui 设计违规的自动报告

作者:kevin moran, boyangli, carlos bernal-carrdenas, dan jelf , denys poshyvanyk

摘要: 移动应用的初始化通常采用图形用户界面（gui）的模型形式，表示为静态图像，描绘了满足要求的 gui 小部件的正确布局和样式。在这个初始模型之后，设计工件就会传递给开发人员，开发人员的目标是在代码中准确地实现这些 gui 和所需的功能。考虑到模型和代码之间存在巨大的抽象差距，开发人员通常会引入与 gui 相关的错误，这些错误可能会对应用在竞争激烈的市场中的成功产生负面影响。此外，这样的错误在快速变化的应用的进化背景下很常见。这导致设计团队的耗时和费力的任务，以验证应用程序的每个屏幕是否按照预期的设计规范实现。本文介绍了一种新的自动化方法来验证移动应用的 gui 是否按照其预期的设计实现。我们的方法解决了已实现的应用程序和模型中与 gui 相关的信息，并使用计算机视觉技术来识别移动 gui 实现中的常见错误。我们在一个名为 gvt 的工具中实现了 android 的这种方法，并与华为的设计师和开发者进行了有控制的开源应用经验评估以及**行业**评估。结果表明, gvt 解决了一个重要的、困难的、非常实用的问题，具有显著的效率和准确性，从工业设计师和开发人员的角度来看，具有一定的实用性和可扩展性。该工具目前被**华为**的一千多名工业设计师和开发商使用，以提高移动应用的质量。少

2018 年 4 月 5 日提交;**v1** 于 2018 年 2 月 13 日提交;**最初宣布** 2018 年 2 月。

8. **路由协议实现的形式化黑匣子分析**

作者:adi sosnovich, orna grumberg, gabi

摘要: 互联网基础设施的路由协议完全依赖于开放标准。但是，互联网上的大多数路由器都是闭源。因此，没有简单的方法来分析它们。具体来说，不能很容易地识别路由器的路由功能与路由协议的标准的偏差。这种偏差（有意或无意）尤其需要识别，因为它们可能会降低网络的安全性或弹性。基于模型的测试程序是一种技术，它允许基于要测试的系统模型系统地生成测试;从而发现系统中的偏差与模型的比较。但是，将这种方法应用于复杂的多方路由协议需要数量高得令人望而却步的测试，以涵盖所需的功能。我们针对针对路由协议分析而定制的基于模型的测试程序提出了高效、实用的优化方案。这些优化允许设计一种正式的黑盒方法来发现闭源路由协议实现中的偏差。该方法只依赖于测试目标协议实现和观察其输出的能力。偏差的识别是完全自动的。我们针对互联网上复杂且广泛使用的路由协议之一 ospf 来评估我们的方法。我们在思科的 ospf 实施中寻找偏差。我们的评估发现了许多重大偏差，这些偏差可能被滥用于损害网络的安全。这些偏差得到了思科的证实。我们还使用我们的方法来分析 quagga 路

由套件的 ospf 实现。分析显示了一个重大偏差。在披露偏差后，ibm、联想和**华为**也在自己的产品中发现了其中的一些偏差。少

2017 年 9 月 23 日提交;**最初宣布** 2017 年 9 月。

9. **海豚攻击：听不到的语音命令**

作者:张国明,陈燕,季晓宇,张泰民，张天辰,徐文元

摘要: 语音识别（sr）系统（sr），如 siri 或 google now，已成为一种越来越流行的人机交互方法，并将各种系统转变为语音可控系统（vcs）。之前攻击 vcs 的工作表明，人们无法理解的隐藏语音命令可以控制系统。隐藏的语音命令，虽然隐藏，但仍然可以听到。在这项工作中，我们设计了一个完全听不到的攻击，海豚攻击，调节超声波载波（例如，f & gt; 20 千赫）上的语音命令，以实现听不到。通过利用麦克风电路的非线性，可以成功解调、恢复，更重要的是由语音识别系统进行解释。我们验证海豚攻击流行的语音识别系统，包括 siri，谷歌现在，三星 s 语音,**华为** hivoice，cortana 和亚历克莎。通过注入一系列听不到的语音命令，我们展示了一些概念验证攻击，其中包括激活 siri 在 iphone 上启动 facetime 通话，激活 google now 将手机切换到飞行模式，甚至操纵导航在奥迪汽车的系统。我们提出硬件和软件防御解决方案。我们通过使用支持的向量机（svm）对音频进行分类来验证

检测海豚攻击是可行的，并建议重新设计语音可控系统，以抵御听不到的语音命令攻击。少

2017 年 8 月 30 日提交;最初宣布 2017 年 8 月。

10. **对信任区的降级攻击**

作者:岳晨,张玉龙,王志,陶伟

摘要: 安全关键任务需要与不受信任的软件进行适当隔离。芯片制造商设计并在其处理器中包含受信任的执行环境（tee），以确保这些任务的安全。软件在受信任环境中的完整性和安全性取决于系统的验证过程。我们发现了一种可以对广泛部署的 arm 信任区技术的当前实现执行的攻击形式。攻击利用了信任（ta）或 trustlet os 加载验证过程可能使用相同的验证密钥的事实，并且可能缺乏跨版本的适当回滚预防。如果利用漏洞适用于过期版本，但在最新版本上对此漏洞进行了修补，则攻击者仍然可以使用相同的漏洞将软件降级到较旧的可利用版本来破坏最新的系统。我们在市场上的流行设备上做了实验，包括谷歌、三星和**华为**的设备，发现所有这些设备都有受到攻击的风险。另外，我们还展示了一个利用高通 qsee 的现实案例。此外，为了找出哪些设备图像共享相同的验证密钥，对不同供应商的模式匹配方案进行了分析和总结。少

2017 年 7 月 18 日提交;**v1** 于 2017 年 7 月 17 日提交;**最初宣布** 2017 年 7 月。

11. **双镜头智能手机肖像的高质量对应和分割估计**

作者:沈晓勇,高红云,新涛,周超,贾佳佳

摘要: 估计两个图像之间的对应关系和提取前景对象是计算机视觉中的两个挑战。随着 iphone 7plus 和**华为** p9 等双镜头智能手机进入市场，两张观点略有不同的图像为我们提供了统一这两个主题的新信息。我们提出了一种通过联合完全连接的条件随机场（crf）框架同时解决这些问题的联合方法。区域对应用于处理无文本区域的匹配，并使我们的 crf 系统在计算上具有效率。我们的方法评估了超过 2，000 对新的图像对，并产生了有希望的结果，具有挑战性的肖像图像。少

2017 年 4 月 7 日提交;**最初宣布** 2017 年 4 月。

12. **基于图形的推送服务平台**

作者:郭惠峰,唐瑞明,叶云明,李振国,何秀强

摘要: 众所周知，在今天的信息爆炸环境中学习客户的偏好并向他们提出建议是至关重要的，也是不平凡的。推荐系统有两种不同的模式，即拉模式和推模式。大多数推荐系统是拉模式，仅在用户进入应用程序市场时才向用户推荐项目。而推模式更积极地工

作，以增强或重建应用程序市场和用户之间的连接。作为最成功的手机制造商之一,**华为**应用商店（又名 hispace store）的用户和应用数量都大幅增加，到 2016 年为止，华为拥有约 3 亿注册用户和 120 万个应用。其用户数量正在高速增长。针对实际场景的需要，我们在 hispace store 中建立了一个推送服务平台（简称 psp），通过另外一组贴有标签的应用（通常大约在 10 个应用）中自动从 web 规模的用户操作日志数据中发现目标用户组。在本工作中，psp 包括分布式存储层、应用层和评估层。在应用层中，我们设计了一种实用的基于图形的用户群发现算法（a-parw），它是部分吸收随机游走的近似版本。基于 a-parw i 模式，与在应用层中使用个性化 pagerank 的系统相比，该系统的有效性有了显著提高。少

2016 年 11 月 29 日提交;最初宣布 2016 年 11 月。

13. **检查和平衡：用于 comp 的低复杂性高增益上行电源控制器**

作者:陈艳洲,孙音, 秦一平,坎尔·科克萨尔

摘要: 协调多点（comp）承诺为下一代蜂窝系统带来可观的吞吐量。然而，实现这种增益在飞行员和回程带宽方面是昂贵的，并且可能需要对物理层硬件进行大量修改。针对高效吞吐量增益，我们为上行蜂窝网络开发了一种新的协调功率控制方案，称为 "检查和平衡（c & amp; b)"，该方案可检查一个用户的接收信号强

度及其对邻近基地产生的干扰站，并平衡这两个。c & amp; b 有一些非常有吸引力的优势: c & amp; b (i) 可以很容易地在软件中实现, (ii) 不需要升级非 comp 物理层硬件, (iii) 允许为每个用户设备 (ue) 完全分布式实现 (ue), (iv) 不需要额外的飞行员或回程通信。我们在与**华为**仔细校准的上行 lte 系统级仿真平台上评估 c & amp; b 的吞吐量性能。仿真结果表明，与几种广泛使用的功率控制方案相比, c & amp; b 实现了更好的吞吐量性能。少

2016 年 10 月 26 日提交;**最初宣布** 2016 年 10 月。

14. **拥有您的家庭网络: 重新审视路由器安全**

作者:marcus niemietz, joerg schwenk

摘要: 本文研究了几个 dsl 家庭路由器的 web 接口，这些路由器可用于通过 web 浏览器管理其设置。我们的目标是通过使用主 xss 和 ui 调整攻击来更改这些设置。本研究评估来自 10 个不同制造商 (tp-link、netgear、**华为**、d-link、linksys、logilink、belkin、buffalo、fritz!盒子和阿苏斯)。我们能够规避他们所有人的安全。为了演示所有设备是如何受到攻击的，我们演示了如何快速进行指纹攻击。此外，我们还提供了对策，使管理接口更加安全，从而使路由器的使用更加安全。少

2015 年 6 月 12 日提交;**最初宣布** 2015 年 6 月。