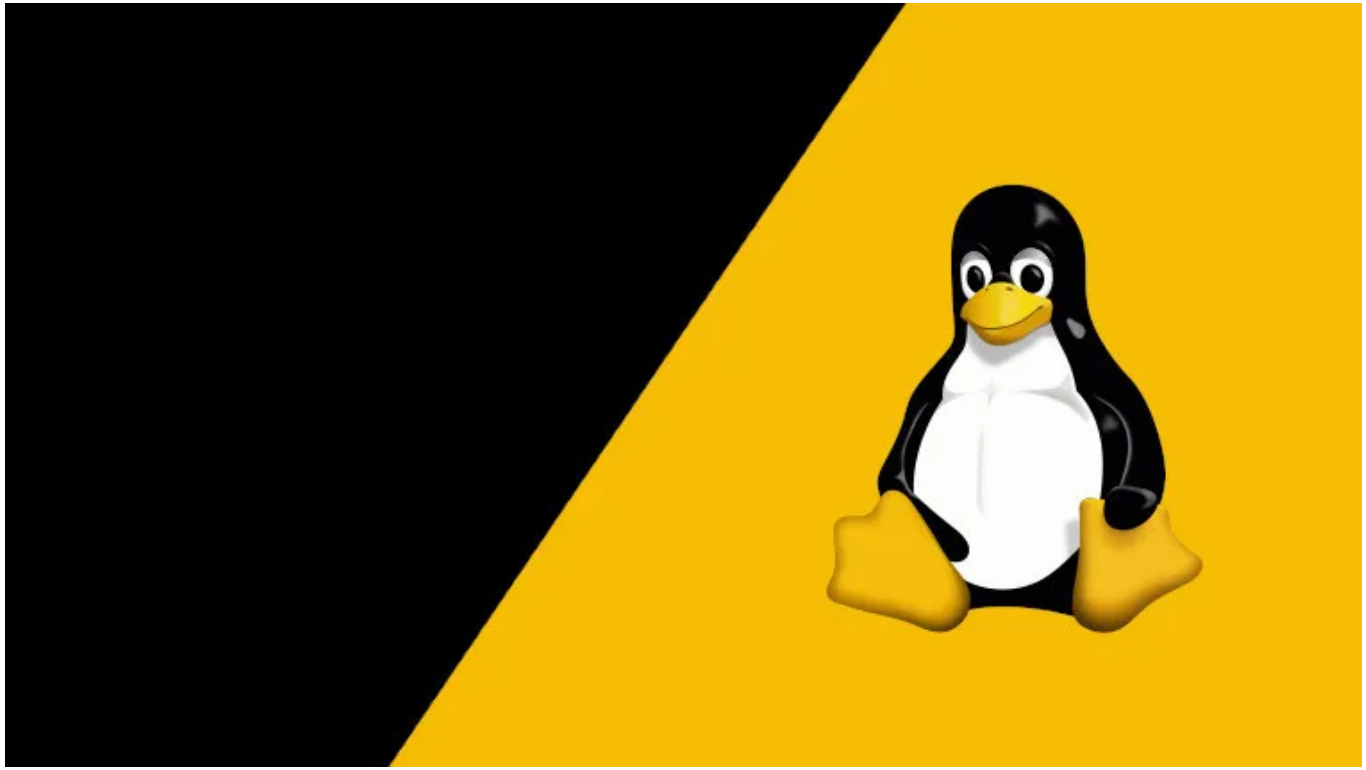
為寫論文，華人學者向Linux提交200多條「惡意代碼」，結果整個大學都被Linux封了

計算機視覺Daily 昨天

本文轉載自：機器之心 | 編輯：杜偉、陳萍

> 為了寫論文，明尼蘇達大學的研究者竟然向Linux 內核發送了200 多個有漏洞的代碼，結果惹怒了Linux 社區，不僅禁止整所大學向Linux 提交代碼，還將該校提交的代碼還原。

近日，國外學術圈出現了一件「新鮮事」，明尼蘇達大學的兩位華人研究者在寫論文時嘗試將壞補丁（bad patch）放入Linux 內核中作為「測試」，用於研究開源社區的漏洞。但當他們繼續貢獻「帶bug 代碼」的時候，卻發現Linux 內核管理員Greg Kroah-Hartman 終結了他們的行為，並將整個明尼蘇達大學拉入了Linux 黑名單。



事情究竟是怎樣的呢?

此前，明尼苏达大学计算机科学与工程系博士生 Qiushi Wu 及其导师助理教授 Kangjie Lu 合作写了一篇《On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits》论文，尝试将 UAF（Use-After-Free）漏洞放入 Linux 内核。通常来说，这种 Red Team 安全检测很常见，并且该论文已经被 2021 IEEE 安全与隐私研讨会接收。

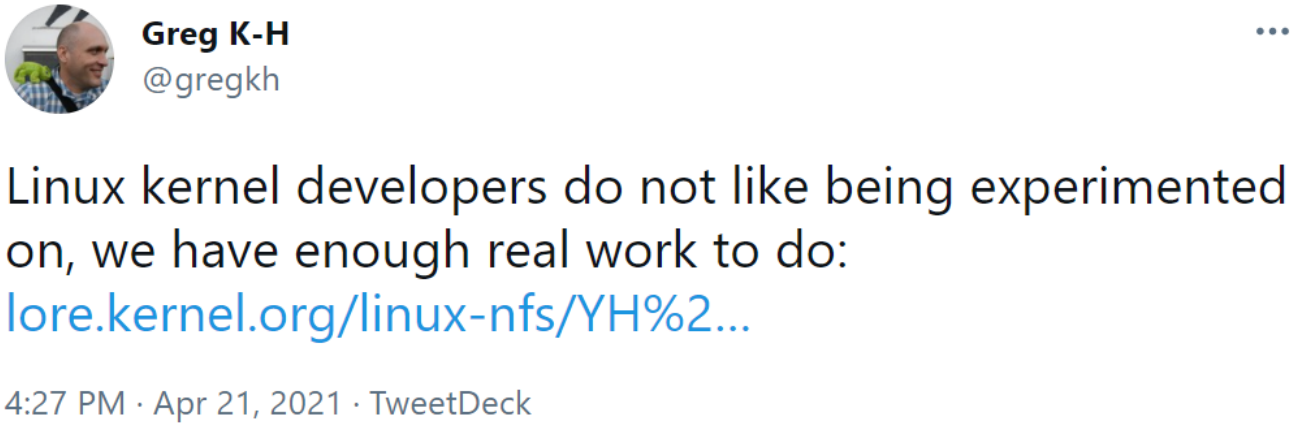
但当他们再次尝试提交代码时，却发现 Linux 内核管理员 Greg Kroah-Hartman 已经将整个明尼苏达大学「拉黑」了。

On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits

Qiushi Wu and Kangjie Lu
University of Minnesota
{wu000273, kjlu}@umn.edu

论文地址：https://github.com/QiushiWu/QiushiWu.github.io/blob/main/papers/OpenSourceInsecurity.pdf

Greg Kroah-Hartman 是备受尊敬的 Linux 内核开发者之一，他在推特回复称：「Linux 内核开发者不喜欢『被实验』，我们要做的事情本来就够多了。」

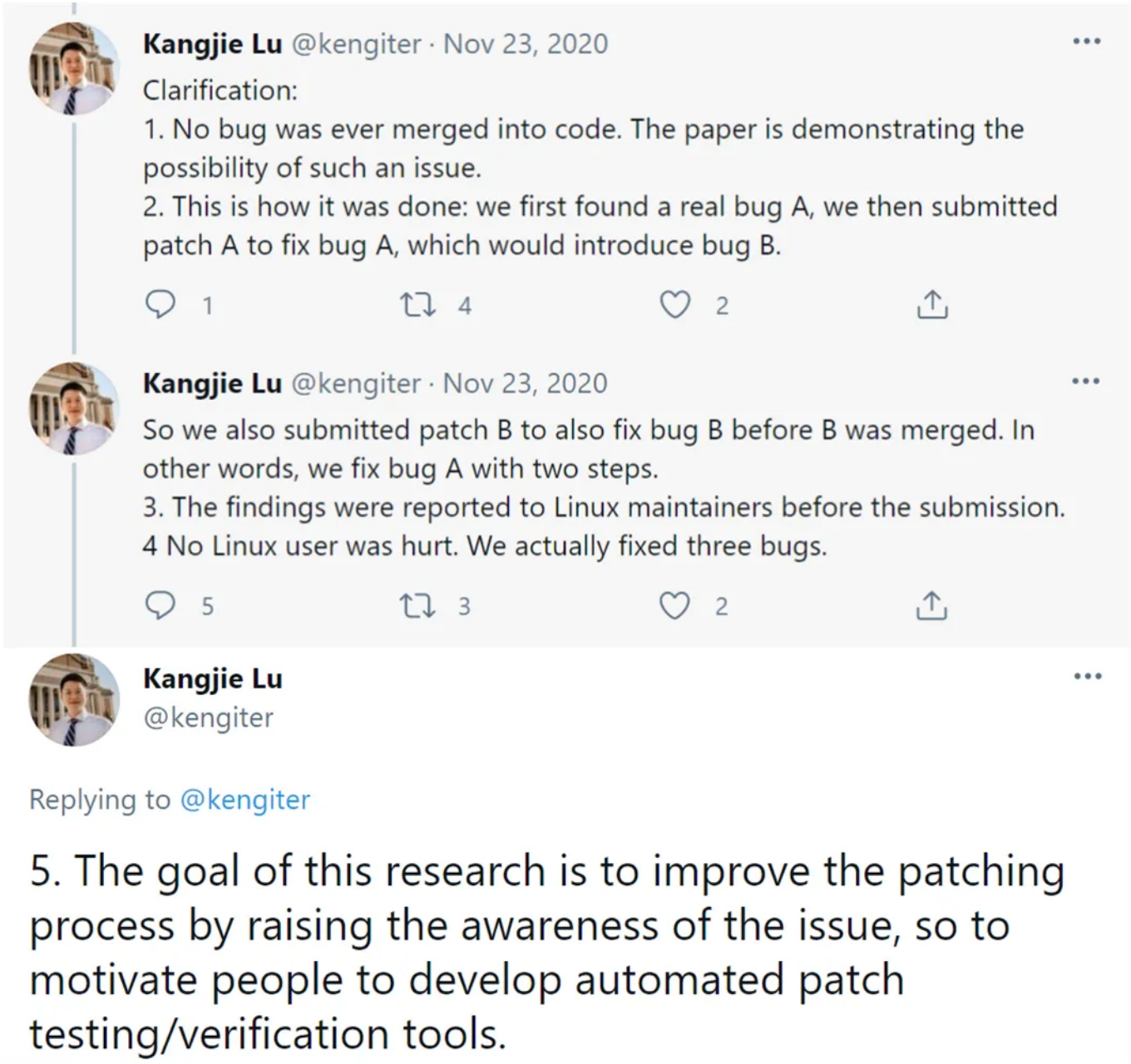


在 Linux 内核邮件列表（LKML）中，当研究者再次尝试提交虚假补丁时，Kroah-Hartman 更清楚地表达了他的态度，「请停止提交已知无效的补丁，不要想着为了完成论文而在审核过程中捣鬼，这种做法是不对的，浪费我们的时间。我们将不得不再次向贵校知会这件事情。」

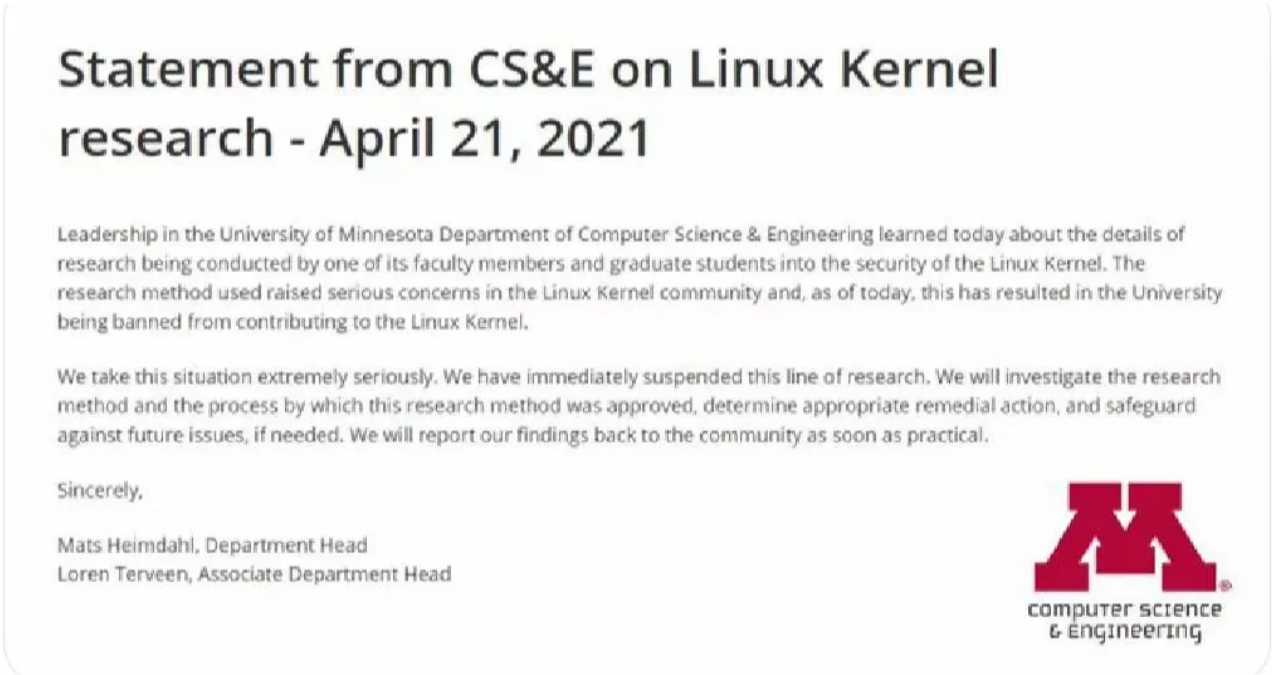
Linux 内核高级开发人员 Leon Romanovsky 也解释道：「他们是故意将 bug 引入内核，这在任何开源社区都是大禁忌。在 Linux 内核社区中，开发者之间的信任是开发过程中至关重要的一部分。」

这两位研究者是不是故意为之呢？又会不会对 Linux 造成损害呢？Kangjie Lu 教授之前已经对自己的研究做出了以下声明：

一，我们从来没有在提交的代码中合并 bug，论文证明了这类问题存在的可能性；
二，我们的做法是这样的：首先发现真正的 bug A，然后提交补丁 A 来修复 bug A，这也将引入 bug B；所以，我们也会在合并 bug B 之前提交补丁 B 来修复它。换句话说，我们通过两步来修复 bug A。
三，这些发现在提交前已经报告给了 Linux 管理员；
四，我们不会对任何 Linux 用户造成伤害，并修复了这些 bug；
五，这项研究旨在通过提高人们对这类问题的认知来改进修补过程，激励人们开发自动补丁检测和验证工具。


Kangjie Lu @kengiter · Nov 23, 2020
Clarification:
1. No bug was ever merged into code. The paper is demonstrating the possibility of such an issue.
2. This is how it was done: we first found a real bug A, we then submitted patch A to fix bug A, which would introduce bug B.
1
4
2
Kangjie Lu @kengiter · Nov 23, 2020
So we also submitted patch B to also fix bug B before B was merged. In other words, we fix bug A with two steps.
3. The findings were reported to Linux maintainers before the submission.
4 No Linux user was hurt. We actually fixed three bugs.
5
3
2
Kangjie Lu
@kengiter
Replying to @kengiter
5. The goal of this research is to improve the patching process by raising the awareness of the issue, so to motivate people to develop automated patch testing/verification tools.

双方各执一词。不过，明尼苏达大学计算机科学与工程系官方在获知这件事情之后，表示「两位研究者的研究引发了 Linux 内核社区的广泛关注，并导致 Linux 拉黑了整所大学。**我们非常严肃地处理整件事情，并已经立即终止了这项研究。我们还将追查两位研究者采用的研究方法以及该方法的批准流程，确定适当的补救措施，并为将来出现的其他问题做好准备。**」



Statement from CS&E on Linux Kernel research - April 21, 2021

Leadership in the University of Minnesota Department of Computer Science & Engineering learned today about the details of research being conducted by one of its faculty members and graduate students into the security of the Linux Kernel. The research method used raised serious concerns in the Linux Kernel community and, as of today, this has resulted in the University being banned from contributing to the Linux Kernel.

We take this situation extremely seriously. We have immediately suspended this line of research. We will investigate the research method and the process by which this research method was approved, determine appropriate remedial action, and safeguard against future issues, if needed. We will report our findings back to the community as soon as practical.

Sincerely,

Mats Heimdahl, Department Head
Loren Terveen, Associate Department Head

computer science & engineering

或许是校方的「不作为」导致自己被拉黑

Kangjie Lu 教授的另一位博士生（Aditya Pakki）提交了一个一共只修改 / 增加了两行的小补丁：

```
Signed-off-by: Aditya Pakki <pakki001@umn.edu>
---
 net/rds/message.c | 1 +
 net/rds/send.c    | 2 +-
 2 files changed, 2 insertions(+), 1 deletion(-)

diff --git a/net/rds/message.c b/net/rds/message.c
index 071a261fdaab..90ebcfe5fe3b 100644
--- a/net/rds/message.c
+++ b/net/rds/message.c
@@ -180,6 +180,7 @@ void rds_message_put(struct rds_message *rm)
                    rds_message_purge(rm);

                    kfree(rm);
+                   rm = NULL;
            }
 }
 EXPORT_SYMBOL_GPL(rds_message_put);
diff --git a/net/rds/send.c b/net/rds/send.c
index 985d0b7713ac..fe5264b9d4b3 100644
--- a/net/rds/send.c
+++ b/net/rds/send.c
@@ -665,7 +665,7 @@ static void rds_send_remove_from_sock(struct list_head *messages, int status)
 unlock_and_drop:
                    spin_unlock_irqrestore(&rm->m_rs_lock, flags);
                    rds_message_put(rm);
-                   if (was_on_sock)
+                   if (was_on_sock && rm)
                            rds_message_put(rm);
            }
```

由于这个补丁很简单，而且似乎改善了代码的质量，它最初得到了一些成员的支持，但后来受到质疑。而在 4 月 19 日，资深的内核贡献者 Al Viro 斥责该贡献者提交了一个「没有修复任何东西的补丁。」

Aditya Pakki 提交的另外一个补丁：

```
1.          }
2.  -       gss_release_msg(gss_msg);
3.  +       if (gss_msg)
4.  +               gss_release_msg(gss_msg);
5.   }
```

Linux 内核开发者之一 Greg Kroah-Hartman 警告称，不要浪费内核维护者的时间提交这种补丁。显然，这不是唯一引起争议的补丁请求。还有 3 个这样的补丁来自同一个研究人员，并认为这些补丁增加了安全漏洞。

面对这些公开抨击，Aditya Pakki 认为自己是受害者，指责内核维护者的态度，「我恭敬地请你停止和停止作出近乎诽谤的野蛮指控。」他还声称「这些补丁是作为我写的一个新的静态分析器的一部分发送的，它的灵敏度显然不是很高。我发送补丁的目的是希望得到反馈。我们不是 Linux 内核方面的专家，反复发表这些言论让人听了很反感。」Pakki 说：「我不会再发补丁了，因为这种态度不仅不受欢迎，而且会让新手和非专业人士感到害怕。」

这激怒了 Kroah-Hartman 并回复道：

> 你和你的团队公开承认发送了已知的错误补丁，以查看内核社区对它们的反应，并发表了一篇基于这项工作的论文。现在你又提交了一系列明显错误的补丁，我该怎么看待这种事情？[这些新的补丁] 显然不是由一个有智慧的静态分析工具创造的，因为它们都是完全不同的模式的结果，而且所有这些补丁显然根本没有修复任何东西。那么，除了你和你的团队继续通过发送这种无稽之谈的补丁来对内核社区的开发者进行试验之外，我还能想到什么呢？

> 当提交由工具创建的补丁时，每个这样做的人都会提交类似「found by tool XXX, we are not sure if this is correct or not, please advise」的语句。为什么在这里你们就没执行这样的操作。你不是在寻求帮助，你声称这些是合法的修复，但你知道这是错误的。

> 任何对 C 语言有一定了解的人都可以看到你提交的补丁根本没有任何作用，所以认为一个工具创造了它们，然后你认为它们是一个有效的 「修复」，这完全是你的疏忽，不是我们的。你才是有错的人，我们的工作不是成为你创造的工具的测试对象。

> 我们的社区欢迎那些帮助和增强 Linux 的开发者，但并不是你们尝试做的事情，所以请不要试图用这种方式来破坏它。我们的社区不欢迎被试验，也不欢迎通过提交已知的补丁被测试，这些补丁要么是故意不做什么，要么是故意引入 bug。如果你想做这样的工作，我建议你找一个不同的社区来做你的实验，你在这里是不受欢迎的。

这些开发者不会再回来了。而且，因为明尼苏达大学在受到警告后没有阻止他们，Kroah-Hartman 表示现在不得不禁止明尼苏达大学今后提交任何代码，并将以往提交的代码还原。

大多数 Linux 内核开发人员和其他程序员都同意 Kroah-Hartman 的观点。Linux 内核高级开发人员、谷歌工程师 Ted T'so 指出，尽管负责这个项目的助理教授 Kangjie Lu 过去做过一些有用的安全工作：

> 问题在于，Lu 教授和他的团队在关于什么是道德的以及内核开发社区可接受的行为方面有一些非常偏颇的想法。并且，明尼苏达大学机构审查委员会（IRB） 认为 Lu 教授所做的研究不在正常实验范围内，这意味着**明尼苏达大学没有任何机构对这种行为进行控制**——这大概就是 Linux 禁掉整所大学的原因所在。

此外，两位研究者在他们的论文中声称，他们的补丁没有一个真正进入任何 Linux 代码库，它们只是出现在电子邮件中，而不是成为任何 Linux 内核分支的 Git 提交。然而事实并非如此。

另一位 Linux 内核高级开发人员 Romanovsky 对此表示，他已经查看了 Pakki 提供的四个已被接受的补丁，其中三个添加了各种严重性的安全漏洞。Linux 内核驱动程序和 Debian 开发人员 Sudip Mukherjee 也表示，很多补丁已经到达 stable tree。

所以，这些研究人员不仅浪费了 Linux 提交者的时间，而且他们实际上把坏代码引入了 Linux 内核。

参考链接：

https://www.neowin.net/news/linux-bans-university-of-minnesota-for-sending-buggy-patches-in-the-name-of-research/

https://www.zdnet.com/article/greg-kroah-hartman-bans-university-of-minnesota-from-linux-development-for-deliberately-buggy-patches/

https://linux.cn/article-13320-1.html

神经网络绘图神器下载

后台回复：**绘图神器**，即可下载绘制神经网络结构的神器！

PyTorch 学习资料下载

后台回复：**PyTorch资料**，即可下载访问最全的PyTorch入门和实战资料！

CVPR 2021论文合集下载

后台回复：**CVPR2021**，即可下载CVPR 2021论文和代码开源的论文合集

推荐下载

82页《现代C++教程》：高速上手C++ 11/14/17/20（附中文PDF下载）
豆瓣评分9.4！《统计学习导论》现在有了Python版（附PDF和代码下载）

计算机视觉Daily
一个专注于计算机视觉开源项目的公众号，涵盖CV、传统图像处理、OpenCV、深度学习、机器学习代码实战和相关资料等内容

7篇原创内容

公众号

▲点击上方卡片，关注我们

整理不易，请给点赞和在看！

喜欢此内容的人还喜欢

微软终于对JDK下手了！

OSC开源社区

Ubuntu 21.04將Home目錄默認設置為私有

腳本之家

微軟發布自己的OpenJDK，真是對Java又愛又恨

碼農小胖哥