“Powers of Tau”活动教程

你想参与 **Powers of Tau** 活动吗？此文是引导你完成参与相关步骤的一个指导，同时首先了解为什么需要这个活动，什么是威胁模型等问题也是非常重要的。

* **为什么需要这么一个活动？** 我强烈建议阅读我们的[博客文章](https://z.cash.foundation/blog/powers-of-tau/)来理解活动的目的。简而言之,虽然 zk-SNARKs 非常棒，但是目前它们的参数设置非常贵并且存在一定的风险。Powers of Tau 是一个活动仪式，为了所有人的便利，通过执行一个单一的，巨大、公共的活动，取消了参数设置中最困难最贵的部分。从而使单个参数设置更容易，并且更具伸缩性。

* **什么是威胁模型？活动如何算成功？** 只要有一名参与者成功地破坏了他们曾经参与的一些随机信息，这个活动就成功了。因此，威胁模型就是一个能够让每个参与者陷入风险的攻击者，或者每个参与者都是不诚实的，互相勾结。为了减少攻击者针对每个参与者的破坏方式，确保每个参与者采取不同的方法是至关重要的。

* **那么哪些人可以参与？** 每个人都可以！我们活动将持续到2018年2月，以便让更多的人参与此次的活动。活动每次只能有一个参与者， 有时候这个过程需要几个小时，所以我们需要仔细安排大家参加的时间。另外，因为我们正努力争取在二月份的某个时候"完成"工作，如果要求参与的人比较多，我们将优先考虑那些信誉良好的参与者。
* **如何参与？** 活动目前由 Sean Bowe 协调。如果你感兴趣，你可以在 [zapps-wg 邮件列表](https://lists.z.cash.foundation/mailman/listinfo/zapps-wg) 上公开要求参与。也可以私下联系肖恩（sean@z.cash）请求参加。

参与的步骤?

当轮到你的时候，你会收到一个大小为 1.2 GB 的 `challenge` 文件。你需要运行一个[用 Rust 编写的程序](https://github.com/ebfull/powersoftau)来使用这个 `challenge` 文件。这个程序将随机抽取一些信息(称为有毒废物) ，执行计算后输出一个 `response` 响应文件。然后，你必须将这个 `response` 文件上传给我们。收到文件的同时我们也会发送此操作的指南给你。

只要至少有一个人的有毒废物被破坏，活动就成功了。一些参与者可能认为，破坏这个信息仅仅通过重新启动他们的计算机就可以了。其他的人可能会做更多的尝试：

* 你可能想在之后破坏电脑。
* 你可能想使用 DVD 与机器进行交互。
* 您可能想使用一个可审计的流程对您的 `response` 文件进行运算，这样可以减少机器被植有木马后门的风险。
* 你可能想用其它人的代码。举个例子，可以看看 devrandom 的 powersoftau 代码的构建过程，它使用了一个纯 C 编译的旧版本的 Rust 编译器。

当然，如果你认为你的机器没有受到威胁，你也可以简单的运行代码，然后发送 `response` 文件后重启动您的计算机。重要的是，人们采取的方法是多样化的，从而使攻击者破坏每个人的贡献的方法更少。

我们要求参与者事后写一份描述他们做了什么以及涉及的文件或代码的相关哈希证明，推荐使用 PGP 签名并在 zapps-wg 邮件列表上发表。

代码是如何工作的?

假设你已经收到了 `challenge` 文件。程序代码存放在 [github](https://github.com/ebfull/powersoftau) 上，下载文件，并把 `challenge` 文件存放在此下载目录中。

代码是用 Rust 编写的，所以要编译它，需要一个 [Rust 编译器](https://www.rust-lang.org/)。一旦有了编译器，就可以在 `powersoftau` 目录中运行此命令：

```
cargo run --release --bin compute
```

程序会首先要求您提供一些额外的随机信息，以提高你的电脑样本的私密随机性。然后它将会进行一个非常大的运算，有可能需要一个小时或更长的时间。

当计算完成，它会输出一个 `response` 响应文件，以及响应文件的对应的哈希值。这个哈希值非常重要：这是你(或其他人)证明你参加了活动的唯一方法。你最好在完成参与后公开发布这个哈希值。

你还需要在完成后将 `response` 响应文件上传给我们。`response` 和 `challenge` 件不是私密的，所以你可以自由公布，我们也将会备份保存你上传的文件。

在这一点上，你的工作是确保破坏机器中有毒废物。所以，做任何让你感觉舒服的事情吧！

虚拟的 challenge 文件

如果你想用一个虚拟的 challenge 文件来测试整个过程，你可以运行`cargo run --release --bin new` 来新建一个。但是不要忘记在你真正参加活动之前删除 `challenge` and `response` 文件。

我什么时侯能拿到 challenge 文件

我们会为你安排时间。一种方法是发送到我们的[邮件列表](https://lists.z.cash.foundation/pipermail/zapps-wg/)并要求参与。
填上你大概估计能参与的时间。如果你不愿意这样做，你也可以私下要求参与：给 `sean@z.cash` 发一封电子邮件，附加一个要求参与的时间段。

当轮到你的时候，你就会收到一个 `challenge` 文件和一个在完成后上传 `response` 传响应文件的方法。

感谢[ebfull](https://github.com/BlockchainTranslator)翻译