**洋葱路由 VS美国国家安全局**

Nicky van Rijsbergenand Kevin Valk

Radboud University Nijmegen (s4062833)

[n.vanrijsbergen@student.ru.nl](mailto:n.vanrijsbergen@student.ru.nl)

Radboud University Nijmegen (s3052273)

[evin@kevinvalk.nl](mailto:evin@kevinvalk.nl)

摘要：

政府和强大组织的数字间谍已经被隐私倡导者警告了许多年了。然而，被美国国家安全局泄露项目的规模还是相当可怕的，即便是专家的项目。

Edward Snowden告诉我们，美国国家安全局正积极地收集尽可能多的信息，并且用任何可能的方法来实现这个目标。他们确实这么做了，例如，努力地影响各种公司的实现和标准来确保后门和弱点会存在。在被Snowden揭露之后，许多人寻求一种方法来保护隐私。然而，鉴于最近发生的事，我们又能相信什么工具呢？

在本文中我们研究了匿名工具洋葱路由。我们观察了对抗NSA这样强大的对手，洋葱路由能提供多少隐私。我们观察了洋葱路由的可用攻击以及NSA能如何使用这些攻击。我们也调查了NSA暴力破解洋葱路由的密码的可能性。为了找到答案，我们假设了NSA有多么强大，并给出了确定的假设。

关键字：TOR,AES,RSA,ECC,NSA

1. **介绍**

在理想的情况下，每个人能决定他们是否希望自己的隐私被泄露。在这种情况下，人们至少应该意识任何侵犯他们隐私的情况，并能随时制止这些侵犯。每个人能控制自己的隐私，并能信任任何人及他人的隐私。这种情况是理想的，因为隐私是每个人的权利，更重要的是，隐私对于所有人来说都是重要的。

不幸的是，现实不是这样理想的情况。由于揭发者Edward Snowden，NSA正以许多人们没想到的方法来从公民身上搜集情报的事已越发明了。起初，人们没意识到这是一种隐私侵犯。但现在，他们明白了，他们试图夺回一部分他们的隐私，但经常不知道该去怎么做。其中一个原因就是因为不清楚NSA的能力。一个许多人试图夺回隐私的方法是用匿名工具；举个例子来说就是洋葱路由，它有超过三百万的用户，是最多被使用的匿名工具。

为了让现实与理想状况更像相似，我们研究了对抗NSA这样强大的对手，洋葱路由是否能够提供隐私。我们提出了以下的问题：对抗NSA洋葱路由能提供怎样程度的保护？

为了得到这个问题的答案，我们首先研究了NSA。NSA已显露的能力是什么（他们已经做了什么）以及NSA预期的能力（他们还可能做什么）。被Edward Snowden揭露的事提供了很大的帮助。我们调查了NSA能做什么来对抗洋葱路由。NSA可以用两种方法来攻击洋葱路由的用户，一是有针对性的，主要是当他们有理由去怀疑某个人，二是通过群众监督，当NSA只是想收集信息。我们已经研究了洋葱路由存在的几个NSA能有针对性性攻击利用的漏洞。我们也观察了洋葱路由的密码系统是否有能力承受得住NSA的攻击。

本文如下组织。第2段给出洋葱路由的介绍。第3段给出对于NSA的全球性看法，以及解释NSA为什么被看作一个敌人。第4段会描述目前已知的对于洋葱路由的攻击，本段也会给出一个关于洋葱路由使用的密码的看法，以及一份这些密码的安全性的详细分析。第5段会总结本文。

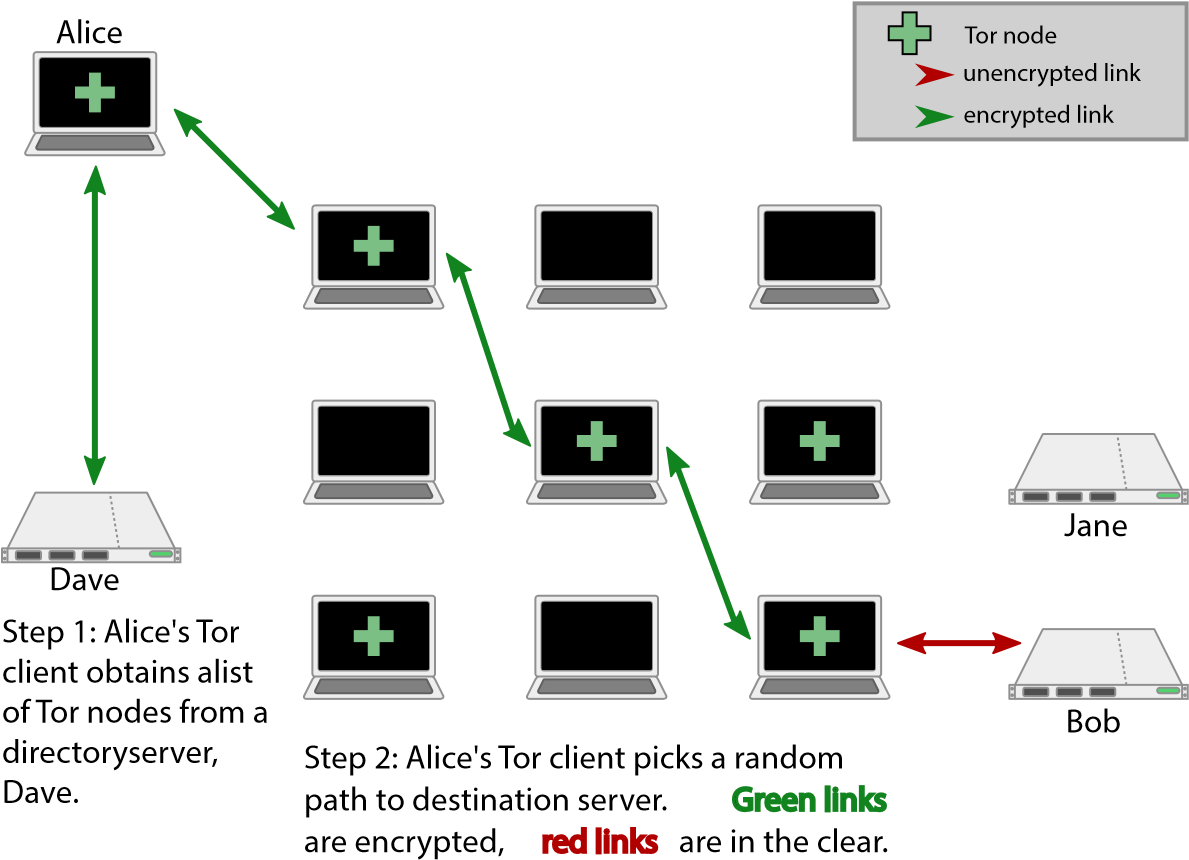
1. **洋葱路由**

洋葱路由是一个开源软件，可以在使用互联网时保持匿名。洋葱路由最初是作为海军研究实验室第三代洋葱路由项目被设计、实施和部署的。记者、军人、政治活动家、举报者、罪犯和普通人现在都可以使用它了。洋葱路由有超过300万的用户。Tor被美国海军研究实验室开发，目前由多家公司和超过4600个个人捐助者赞助。

Tor反弹通过Tor网络的交通来隐藏真正的发送者。外部人员只能看到一个大的Tor网络，但他们并不知道数据包是从哪个网络来的。

* 1. **Tor的全球概述**

Tor通过路由用户通过几个Tor节点（通常是三个）的流量来提供匿名。Tor节点是运行Tor软件的电脑。每个Tor节点都不知道消息的起始点或目的地，或者都不知道。入口节点知道发起者是谁，出口节点知道接受者是谁，中继节点发起者和接受者都不知道。路径的端点（即Tor网络中的发送和结束的点）用X层的加密算法来加密初始的数据包。其中，X相当于路径的长度。这是Tor被叫做洋葱路由的主要原因。因为只有端点知道原始的内容。Tor过去使用RSA加密算法，但是最新版本的Tor使用的是ECC椭圆曲线加密算法。为了提高效率，Tor客户端对发生在每十分钟之内的连接使用相同的路径。之后的请求就会被给予一个新的路径，为的是防止敌人把你早期的操作连接到一个新的路径上。



图一：Tor的概述(来自Justin Findlay(2013)[16]）

Tor也让用户在提供各种服务的同时能够隐藏他们的位置，例如web的发布或者一个即时消息服务器。

**·对于Tor攻击的景象**

Tor只专注于保护数据的传输，所以基本上防止了让外部人员知道他在与谁交谈。Tor不能 提供完全的隐私。当一个对象使用发送包含身份验证的消息，却不使用端到端的加密软件时，Tor仍然会显示关于这个对象的信息。

Tor最近发布了0.2.4版本，它使用了256位的ECC加密算法作为标准，而不是老版本中的RSA-1024算法。原因是因为RSA-1024算法已经不再被认为是安全的了。然而，不是所有Tor客户都更新到最新的版本了，这意味着这些Tor的老客户端可能是脆弱的。

其他针对于Tor的攻击也是存在的。例如，用于关联两个已知的端点的流量/时序分析攻击。坏苹果攻击是另外一个例子，这些例子使用会显示用户信息（例如公共IP地址以及Tor将一个用户的所有流放在同一个电路上的事实）的不安全应用程序。最终，如果敌人控制了N个节点，那么他就可以关联（M/N）2的流量。

1. **国家安全局**

美国国家安全局是美国信号和情报的中央生产者和管理者。据估计，NSA是人事和预算方面美国最大的情报机构之一。对于NSA能够做什么和它已经做了什么有很多的猜测。

由于Edward Snowden，我们不再需要将我们的信息基于关于NSA的谣言。Edward Snowden目前为止大约已经泄露了来自NSA的50~200万份秘密文件，不仅如此，以后还会有更多。这些文件描述了NSA做过的许多间谍活动。这些间谍活动的一部分例子如下：

* 通过影响标准来获得大量数据
* 接受能帮助NSA的所有公司的互联网流量副本，例如AT&T
* 使用大规模监控设备来检测互联网流量
* 对法国、英国、墨西哥等友好国家进行间谍
* 窃听35个世界领导人
* 通过PRISM访问Google和Yahoo的数据库

这些只是NSA到目前为止被揭露了的间谍活动的一部分，许多这些活动违背了欧洲隐私权规定

举报人Edward Snowden唤醒了我们，并让我们意识到了NSA正把矛头指向公民和盟友们，这意味着NSA是我们应该注意的对手。

另外一个NSA应该被看做Tor的敌人的原因，是NSA把Tor看做是一个最高优先的目标。这从Edward Snowden泄露的最高机密幻灯片中可以清晰地看出。这些幻灯片描述了NSA是怎样计划攻击Tor的。

·NSA的黑色预算

NSA不用改被认为只是一个对手，由于他们巨大的黑色预算，更是一个非常强大的对手。他们2013年的黑色预算估计有108亿美元。黑色预算是一个国家用来分配给机密和其他秘密操作使用的。总额中大约有56亿用于数据收集，数据处理和开发以及分析。此外，估计总额中的10亿美元投资在了密码分析和开发。

NSA另一项主要的支出是2013年建立完成的一个大型的数据中心。这个数据中心被叫做“犹他数据中心”，但也被称为“智能社区综合国家网络安全倡议数据中心”。这个数据中心大约100万平方英尺，并且能给NSA 3到12EB的存储容量。

这个数据中心的主要目标当然是未知的，可能是用来存储和处理大量数据。由于Edward Snowden，对于这个数据是什么我们有一个笼统的概念。

1. **Tor vs NSA**

在本节中，我们将会看一看在文献中描述的几次对于Tor的攻击。我们也会看一看NSA怎样才能使用这些攻击来废弃Tor提供的匿名化。最后我们将会分析Tor使用什么样的密码，以及这些密码当前被认为有多强。

* 1. **攻击Tor**

Tor有一些未解决的弱点，我们将在接下来的小章节总结最紧迫的问题。

* + 1. **攻击Tor**

如果两个端点都已知，则会进行流量分析攻击。如果敌人正观察Tor路径的两个端点，那么他介意知道双方是否在跟对方交谈。这意味着如果敌人正在观察Alice（或者路径中的第一跳）和Bob（或路径中的最后一跳），那么这个敌人通过利用统计可以知道Alice和Bob是否正在交谈。例如，敌人可以简单地对Alice发送给Tor网络的数据包进行计数，以及Bob从Tor网络接收到了多少数据包。敌人也可以跟踪Alice发送消息的时间和Bob在什么时候接收到的（又称作时间分析攻击），在一段时间后，敌人将会知道Alice和Bob是都在交谈。开始监控流量的好地方是互联网交换，因为有很多Tor电路只使用一个。

如果对手实际上控制着入口和出口的节点，那么他可以发起一个标记攻击。这基本上意味着他标记了进入Tor网络的数据，并试图找到曾经到达了被他所控制的出口节点的标记。已经被测试过的标记攻击的一个例子，是在Tor使用计数器模式AES的协议级别。敌人可以用正常计数器中断的方法来改变消息。只要信息到达了出口节点，出口节点将会出现解密问题，因为计数器已经不再是正确的了。如果敌人控制着出口节点，他将会注意到这一点。

然而，标记攻击对于敌人来说也是有风险的，因为这会使敌人被注意到的几率更高，这是因为他在数据流中进行了实际的改动，而被动的数据分析则不会。另外，标记攻击被认为是不那么有效的，例如定时攻击。定时攻击的结果导致怀疑这两个人是不是正在与对方交流，这是经常会有的情况。换句话来说，定时攻击几乎没有误报。

NSA可以使用这种攻击，但是他们将会手动地进行，假设NSA没有控制任何Tor的节点。他们需要怀疑这两个人是否真的是在与对方交谈，并且这个攻击将会验证这两个人是否真的在与对方交谈。