今天我讲的论文是Eclipse Attacks on Bitcoin's Peer-to-Peer Network
Bitcoin被认为只要百分十51的算力是可信的，那么系统就是安全的。
但是前提是需要所有参与方都可以看到有效交易块。Bitcoin依赖点对点网络传递信息。
因此如果能够控制点对点网络，就可以控制信息流，进而控制区块链。
eclipse攻击就是利用这种方式影响Bitcoin安全的。

先讲什么是eclipse攻击，能用它做什么坏事。
然后讲如何进行eclipse攻击以及需要的资源。
最后提出我们的对策，以及如何在Bitcoin系统上进行部署。

在将攻击之前，先解释一下比特币的点对点网络。
这些是比特币网络的节点，对于该目标节点来说。默认最多有8个TCP传出连接。
最多有117个TCP传入连接。这些链接可以形成点对点的gossip网络。来扩散比特币的交易块。
最下方是一个节点，它发送一个交易块。一旦有节点发现它，就把交易块向其他节点发送。

本文的攻击目标是接受传入连接的比特币节点，不是所有节点都接受传入连接的。
information eclipse 攻击就是：在点对点网络中控制节点的信息获取。
如果目标节点连接上的都是攻击者的节点。
攻击者就可以阻止交易块的扩散。使得目标节点和整个网络孤立开来。
一般来说攻击者是无法使目标节点的所有链接都指向它的。
后面会提到攻击者如何造成这样的局面。但首先我们来讲一下，攻击成功能造成危害。

将这张图重新绘制一下，使得攻击者处于目标节点和P2P网络之间。
eclipse 攻击可以做什么。
只要具有40%的算力，就可以实现51%攻击。

这张图里面，攻击者有40%的算力，目标节点有30%的算力，剩余网络有30%的算力。

首先攻击者要做的是孤立挖矿者，这样他们就不能在其他交易块上进行挖矿了。

攻击者然后拥有的算力就比这两方单体来说都多了。

攻击者可以产生比挖矿者更长的链。而比特币总是使用更长的那条链。

那么攻击者的链就成为了主链。这种攻击方式和51%攻击是等价的。

因为攻击者可以保证只有自己的块，可以被链接到主链上。攻击者可以选择停止打包所有比特币上的交易。
比特币就停止工作了。攻击者也可以篡改区块历史。等等。
我们假设攻击者不仅有攻击能力，也有挖矿能力。

第二个例子是，N块确认的双花攻击。
这里假设攻击者没有任何挖矿能力。
我们在这里加入了一个商店。目标节点和商家共享一个区块链状态view。

攻击者想进行一个双花攻击。攻击者把一个币花了两遍。它把比特币给了商家，在P2P网络中又把币重新转给自己。

攻击者已经把P2P网络分割了。因为商家和目标节点看到了同样的区块链状态。目标挖矿者就把交易打包了，并且之后也链接了确认块。

剩下的网络也这样做，看到交易，打包，确认。

但是双方都不知道还有另一条链存在。

因此商家在看到三个块确认了交易之后，就发货给攻击者。

当攻击者停止操纵块后，孤立算力的区块链就作废了。攻击者也拿回了自己的钱。

这样的攻击者并不具备挖矿的算力，但是它操纵了第三方的算力。

下面介绍如何实现eclipse攻击。
首先攻击者加入P2P网络。
需要将目标节点的peer table 都变成攻击者的IP。
目标节点然后重启并失去了所有现在的传出连接。
节点从peer table中取得IP，所有新的链接都指向攻击者IP。

然后讲peer表如何工作。节点选择邻接节点的IP是从两张表中选择的。

一个是new table。是节点曾经 听说过，但是没有连接过的IP。
还有一个是tried table，里面是节点曾经连接过的IP。
表里面有bucket，里面装着IP。

还包括IP的时间戳。在tried table时间戳是该IP最后一次连接节点的时间。

如果节点想建立一个传出连接。先要决定是从new 表还是tried表里面选。
挑定表之后，它倾向于选择更新鲜的IP。
然后就尝试和那个IP建立传出连接。攻击者希望让表里面充满攻击者的IP。
攻击者会让他的IP更新鲜，所以更容易被选到。

传入连接的IP都会加到tried里面，所以攻击者就连接该节点。

当连接建立后，攻击者就发送大量IP。这些IP会被加到new表里面。实际上他可以一次性发送上千个IP。
通过不断的链接，表里面就回充满攻击者的IP。

然后攻击者就等待节点重启。
重启后，节点的所有传出连接都指向攻击者IP。

那它还有传入链接怎么办。很简单，就通过一个IP，跟他建立117个传入链接。
这里考虑到nat网络地址转换的设计，所以实际上是允许这样做的。

那如何使节点重启呢。比如更新补丁需要重启。dos攻击可以使他重启。还有电力的中断。
P2P网络的安全性，不应当依赖节点百分之百的在线。

然后讲一下IP填入bucket的细节。他将IP的前半部分作为group。哈希后可以确定四个bucket。
后半部分IP哈希后，确定4个bucket到底放哪个。这使得攻击者需要使用不同group的IP。
要不就是有很多IP，要不就是用僵尸网络实现IP group的多样性。

因为tried表倾向于选择新鲜的IP。所以只要多花点时间进行攻击。就可以使诚实IP过期。攻击者IP新鲜。
如果bucket满了，就需要丢弃IP。随机选4个，丢弃最旧的，插入新IP。

因为是随机选取的，所以一个漏洞就是攻击者可以无限重用他们被丢弃的IP。
另一个漏洞是前面提到的新鲜性倾向。

第三部分攻击建模和实验。他们用概率统计建模，蒙特卡洛仿真。
利用模型找到关键攻击要素。在真实的Bitcoin节点上做实验。
最坏的情况下，不论tried表里有什么，攻击者都可以赢。
在攻击开始前，人为的把tried表填满，百分之99都是诚实IP。
用了4600个IP，每个group有2个IP。用了5小时，将节点tried表中98.8%变成了攻击者IP。
做了60次实验，成功率是100%。他们又查找了一般僵尸网络的大小，那么攻击中用到的资源，比起现实中的僵尸网络来说还是很小的。

第二个实验是，实际运行的节点。
一个已经运行43天以上的节点，tried表中有300个诚实IP。
用400个来自400个group的IP，花1小时进行攻击。在攻击后，虽然tried表还是很空，但57%的IP是攻击者的。
做了50次实验，成功率为84%。有一个叫carna的僵尸网络是可以满足IP要求的。
最后他们提出了该攻击的对策。他们建议去掉对于IP新鲜度的偏好。

在丢弃IP的设计上也有漏洞，因为可以重复发送IP将bucket填满，
绿色的线是未改变丢弃原则前的，大概4000个IP前能线性地把攻击IP填入bucket，
他们建议IP在bucket里面的位置也应该固定。
这样bucket被填满的时间会比较慢，如红色线所示。

他们还建议了一种连接探测器，这样new表就可以更快地填充tried表。
建议在丢弃IP之前先测试能否建立连接，如果可以就不丢弃。
Bitcoin的开发团队采取了他们126的建议。60%的节点都部署了。
作者团队对34做了补丁。在比特币团队进行更新后，最坏的情况攻击IP需要原来的9倍的IP，成功率在50%。
存活节点也是如此。作者自己的补丁，在丢弃前进行IP连接测试。在tried表满的情况下，攻击不会发生。

他们希望使得比特币P2P网络更加健壮。
总结一下，eclipse攻击可以造成双花攻击，51%攻击需要的算力更少了。
他们用很少的僵尸网络IP就可以攻击节点。也提出了相应的对策，为系统打上补丁。