分布式系统中安全问题及对策

**1.1. 信息加密传送问题**

**问题陈述**：想象一下，你在一个充满数学家的食堂里，希望在没有任何人知道这个事实的情况下，向你的朋友发送消息。 您尚未通过指定协议传递消息，因此所有实施细节都必须向所有人公开声明。 可以怎么做呢？  
Chaum在1981年提出的这个问题的一个特别优雅的解决方案是让每个人都作为一个中继和一个接收者。 在这个方案中，参与者准备加密的消息，它们是数字等效的“包含信封的信封” - 向Alice发送消息，你会计算

|  |  |
| --- | --- |
| 1 | Enc(“T oBob 00 ||Enc(“T oAlice 00 ||Enc(message, Alice), Bob), Carol) |

并将该消息发送给Carol，他们将其解密并发送给Bob，Bob将其解密并发送给Alice。 为了防止流量分析，每个周期都会发送固定数量的消息。 为了处理返回地址，我们可以让Bob和Carol记住一个唯一的消息标识符，然后沿着这一条链路发送消息。  
对使用上述方法的系统特别重要的是共谋的可能性。 如果Bob和Carol合作，他们可能会决定谁发送给定的消息以及发送给谁的消息。

**1.3. 随机选择问题**

上述食堂问题陈述假定了一种向系统的每个其他用户发送消息的简单方法（例如，横跨自助餐厅）。为了实现最大限度地抵抗“共谋攻击”的Chaumian组合，我们需要能够从那些“真实”的中继节点中随机选择。无论何时加入或离开网络，都需要收到通知。不幸的是，在现实世界的P2P网络中，每个用户维护这样的列表将导致不可接受的网络流量（O（n 2）通知）。  
**问题描述**：我们如何维护所有当前“真实”中继节点的分布式列表，以最大限度地减少网络开销，并支持高效率的随机选择对等体？  
Chord [81]分布式哈希表（DHT）中可以找到一个特别优雅的解决方案。 在该方案中，对等体在大空间中分配唯一的地址，然后以在O（log（n））时间内执行查找的方式连接。 添加或删除用户只需要通知O（log（n））对等体。

### 2. 攻击

本文的大部分内容都是针对攻击预防，我们首先回顾一下关于这些攻击的文献对P2P网络尤其常见。

#### 2.1. 攻击目标

2.1.1. 信息收集  
兰花协议必须保卫的最大的攻击类型是 揭示有关其用户的信息。因为兰花被实现为现有互联网上的叠加层，一些信息不可避免地与一些同行共享。 在下面的列表中，这样的信息被标记为“\*”。任何未被明确列出的信息在本文档中不可避免地共享，但是发现了一种方法来发现信息被称为信息攻击，并被Orchid的White Hat Bug Bounty所覆盖。有关共享内容的更多信息，请参见第8节中的协议规范和第9.2节中的串通讨论以及网络参考实现[1]。  
被认为是攻击者感兴趣的数据的类型（永恒的）：

* 现实世界的身份信息。 如用户的姓名， SSN， 地址等。
* 网站帐户信息。用户帐户在特定的网站。 注意这可以查找不同现实世界身份信息。
* \*IP信息。 用户访问兰花网络的IP地址。 请注意，在某些使用场景中，这可能等同于知道“真实世界身份信息”。
* ethereum信息。 与用户钱包相关联的公钥和私钥。 请注意，在某些使用场景中，这可能等同于知道“真实世界身份信息”。
* 兰花网络信息。 与兰花网络上的节点当前业务相关联的密钥（公钥或私钥）。  
  被认为是攻击者感兴趣的行为信息的类型（时间和链相关联数据）：
* \*客户识别。 攻击者探悉客户的IP地址。
* \*中继识别。 攻击者探悉中继的IP地址。
* \*代理识别。 攻击者探悉代理的IP地址。
* \*链接识别。 攻击者探悉到在链中使用了两个IP地址。
* \*网站访问。 攻击者探悉到兰花网络进行了outbound连接到一个特定的网站。
* \*Web服务器访问。攻击者了解到，从兰花网络到特定的网络服务器（可能会托管多个网站）进行了出站连接。
* \*以太坊联系。 攻击者了解到，一个兰花用户持有一个Ethereum公钥。
* \*购买联系。 攻击者了解到两个交易共享一个付款人。
* \*购买信息。 攻击者了解通过链发送的带宽的数量和时间。  
  尽管上述行为信息在正常操作期间与兰花网络上的其他节点共享，如下所述，在大多数情况下，假设用户只有在行为信息收集时才会受到直接的伤害，如果攻击者可以快速探悉几条信息。例如，要说用户X访问了网站Y，攻击者将需要：买方识别，网站访问信息和几条链接标识。 因此，遵循参考规格的同行不会存储或共享上述任何信息，除非提供客户购买的服务所需。

#### 2.2. 经济攻击

与相关系统不同， 兰花协议必须关心支付机制的攻击。本文归纳两大类如下：  
-1. 经济利益。 有利的不良行为，例如用户提供“免费样品”带宽，允许用户专门使用免费样品带宽。  
-2. 经济拒绝服务（EDoS）。 使用付款来淹没兰花网络上的另一个节点进行购买，从而使其脱机。

#### 2.3. 服务质量攻击

一些对手可能会通过放慢兰花网络用户的系统性能来满足，从而潜在地减少使用。

#### 2.4. 中间人攻击

只有在两个互动方之间插入自己才能执行的操作统称为中间人攻击。可以记录加密的信息用于分析元数据（第2.8节），而非加密数据可能另外被更改为控制行为。如果密钥交换没有得到保障，中间人也可能会欺骗双方使其错误地认为攻击者的密钥是对方的密钥。

#### 2.5. 女巫攻击

伪装成多个用户执行恶意行为称为Sybil攻击，使被攻击者承受多方伪装用户的假冒数据。这种攻击的应用包括：

* 向Yelp, Amazon 等平台提供多个reviews。
* 通过假装是多个倾听者来实现BitTorrent从而可以快速下载[72]。

更多信息参见 <<女巫问题>>

#### 2.6. 日蚀攻击

在日蚀攻击中，攻击者的目标是隐藏系统的一部分。 采用的方法是一般网络相当于特权升级攻击：获得网络位置的控制权更多地控制网络，然后使用该控制来获取更多的控制权。

* 比特币的p2p，所有节点都是平等地位，端口数是有限制的，需要”51%”攻击的比特币网络把临近节点的端口数全被攻击者给占用，以致用小于51%的算力通过欺骗临近节点加入自己的网络，对比特币形成“51%“攻击。
* 通过接管与磁链接相关联的地址空间，从BitTorrent DHT中删除文件[83]。

#### 2.7. 拒绝服务攻击

拒绝服务攻击即是攻击者想办法让目标机器停止提供服务。 “意外”情况下的系统行为通常指定和测试不足。 DoS攻击对P2P网络中的节点进行去匿名化是非常有用的。

* 对特定目标DoS攻击结合女巫攻击来监测Tor的流量从而获悉匿名化的信息[53]。
* 只需要20个女巫节点，Dos就能 完全可以泛滥式攻击I2P的数据库使其脱机，从而对网络上的所有流量进行归档。

**更多信息参见《dos攻击》《非结构去中心化的P2P网络DDoS攻击的防御研究.pdf》文档介绍**

#### 2.8. 推理攻击

源于系统行为的统计建模的去匿名化被称为推理攻击或监视攻击。这些通常与精心制作或定时的“探测动作”相结合请求或其他攻击，例如DoS将特定对等体脱离网络并观察流量模式  
响应。

* 从SSL加密的Web流量推断医疗疾病、家庭收入和最终用户的投资选择[ 58 ]。
* 来自全球传输日志的Tor，I2P和兰花流量的分析去除匿名[60]。
* 通过时序分析学习OpenSSL服务器的私钥[55]。

#### 2.9. 黑客

通过将历史上可信赖的对等体转换为攻击向量，激励的攻击者可能会直接危及网络上的节点。当使用链部署带宽时，迭代黑客可能最终允许攻击者“回溯”连接。这种攻击具有重要的安全隐患，但不符合兰花网络的范围。 如果兰花网的设计达到目标，这将是对系统用户的主要攻击。

#### 对运行节点二进制程序，或者开发者插件进行签名验证，防止恶意代码加入节点运行

借鉴： 对于移动代码的攻击，在JVM中有不错的限制措施，代码运行在jvm中，下载过来的代码是不能直接访问本地类的，在这其中还要经过type-checking和code-validation字节码的有效性检测，防止非法访问地址。

#### 访问控制规则

访问控制的手段。这个在各大操作系统中已经被采用了，里面的2个小小的分类是一个叫protection domain保护域，还有一个叫ACL访问控制列表，二者的概念其实非常相像。

#### 授权访问

授权的概念，在系统中许多的资源访问需要对用户进行授权才能被访问到，但是授权容易，撤销权利就比较难了，一旦权利授权了恶意的用户，后果不堪设想。