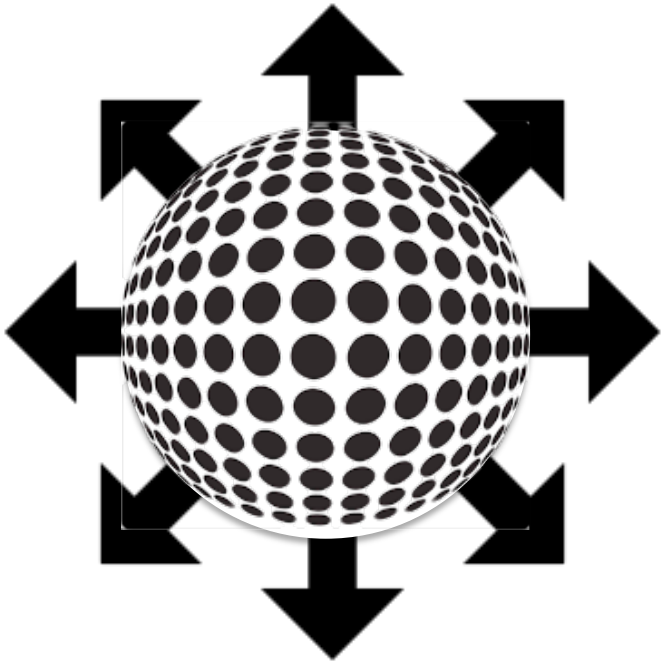
93rd IETF Prague
July 19 – 24, 2015



分布式拒绝服务开放威胁信令（DOTS）工作组

操作要求

Chris Morrow <morrowc@ops-netman.net>
网络安全工程师, Google

Roland Dobbins <rdobbins@arbor.net>
首席工程师 , Arbor Networks

介绍和背景

分布式拒绝服务背景

什么是分布式拒绝服务（DDoS）攻击？

- 尝试消耗有限的资源，利用软件设计或实施中的弱点或利用基础设施容量不足
- 针对计算和网络资源的可用性和实用性
- 攻击几乎总是分布得更明显 (i.e., DDoS)
- 攻击造成的附带损害可能与攻击本身同样严重，甚至更严重
- 分布式拒绝服务攻击会影响可用性！没有可用性，没有应用程序/服务/数据/互联网！没有收益！
- 分布式拒绝服务攻击是针对容量和/或状态的攻击！

三种安全特性

- 安全的目标是维持这三个特征

三种安全特性

- 分布式拒绝服务防御的主要目标是面对攻击时保持可用性

协同DDoS防御的现实

当今互联网安全状况的普遍认识

当今互联网防御的实际状况

谁可以帮助您？

您的ISP或MSSP！

您今天如何寻求帮助？

罗伯特·胡克（**Robert Hooke**）于**1667**年率先采用的技术仅略有改进！

寻求帮助很难！知道如何帮助更加困难！

- 大多数最终客户不知道其正常的互联网流量是什么样子，更不用说进行分布式拒绝服务（甚至知道自己受到攻击了！）时的实际情况。
- 许多ISP / MSSP并未为其终端客户详细配置分布式拒绝服务防御。在许多（大多数）情况下，最终客户无法明确说明需要保护哪些服务器/服务，应制定哪些网络访问策略，等等。
- 这样会大大减慢反应/缓解时间。
- 这大大阻碍了反应/缓解功效。
- 这会导致更长的服务中断，收入损失，最终客户（和这些最终客户的客户）沮丧。

如今，存在自动分布式拒绝服务攻击通知方法

- 但是它们是专有的！
- 最终客户不能混合搭配供应商，ISP分布式拒绝服务云缓解提供商，MSSP分布式拒绝服务云缓解提供商。从所有实际目的出发，在攻击过程中进行有效协调是不可能的。
- 作为分布式拒绝服务目标的服务器/服务/基础设施设备即使能够检测和分类分布式拒绝服务攻击也无法发出缓解信号（请考虑使用Apache mod_security / mod_evasive，BIND RRL）。
- 当共同努力减轻分布式拒绝服务攻击时，ISP / MSSP必须手动协调（严重，低效）。
- 随着攻击者转移分布式拒绝服务媒介/资源，严重的延迟，防御者之间常见的误用。
- 存在网络门户；它们特定于供应商/ ISP / MSSP，具有不同程度的缓解配置（大多数最终客户不知道要配置什么），并且在攻击期间将IDC和客户端局域网传输合并在一起时可能很难访问。

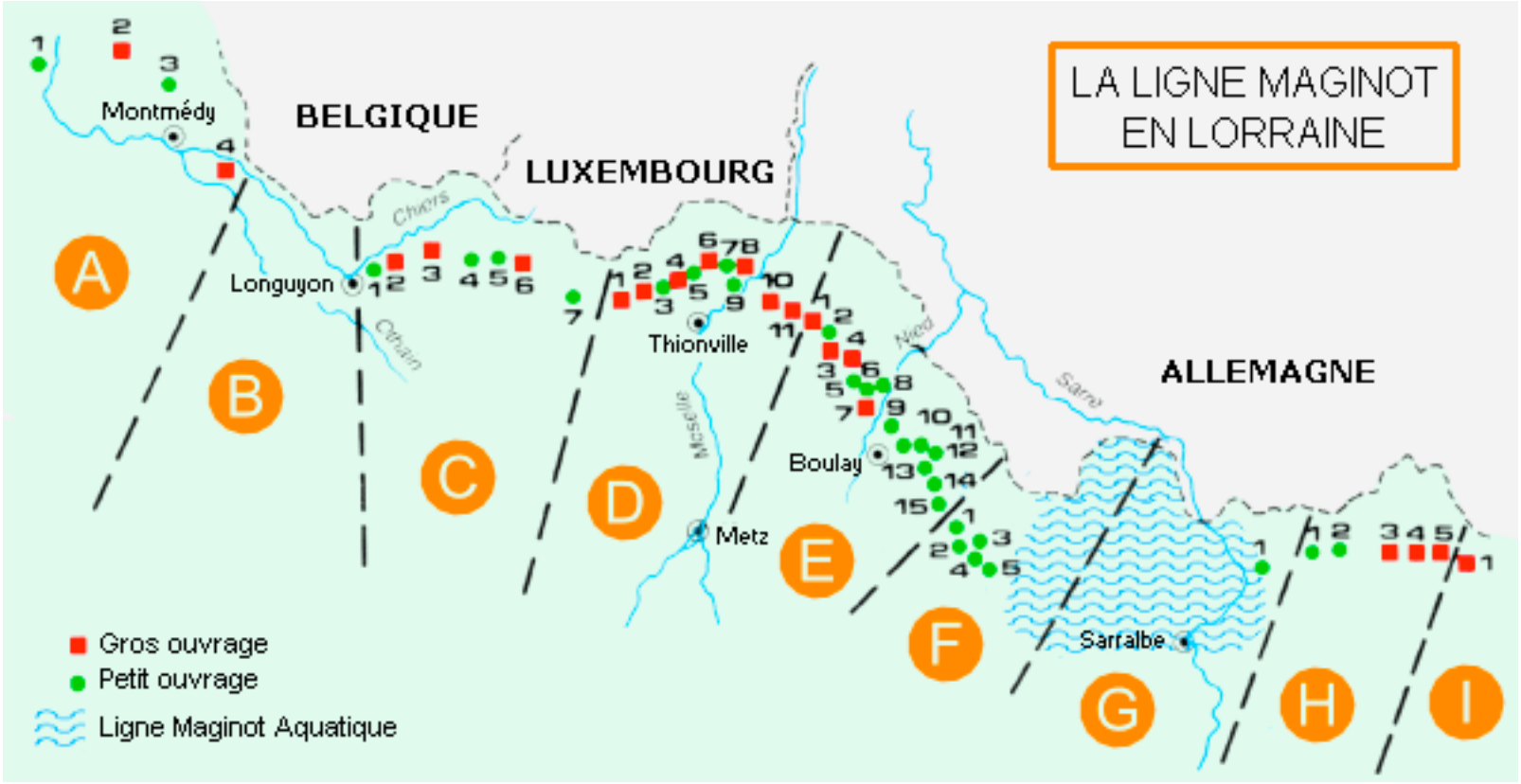
分布式拒绝服务防御成为打字竞赛。 。 。

攻击者。

分布式拒绝服务防御成为打字竞赛。 。 。

防御者。

大型静态，低敏捷防御。。。


LA LIGNE MAGINOT
EN LORRAINE
BELGIQUE
LUXEMBOURG
ALLEMAGNE
Montmédy
Longuyon
Thionville
Boulay
Metz
Sarralbe
Chiers
Crusnes
Moselle
Nied
Sarre
A
B
C
D
E
F
G
H
I
Gros ouvrage
Petit ouvrage
Ligne Maginot Aquatique

。 。 。导致可预测的结果。

分布式拒绝服务防御协调，大约1995年。

```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

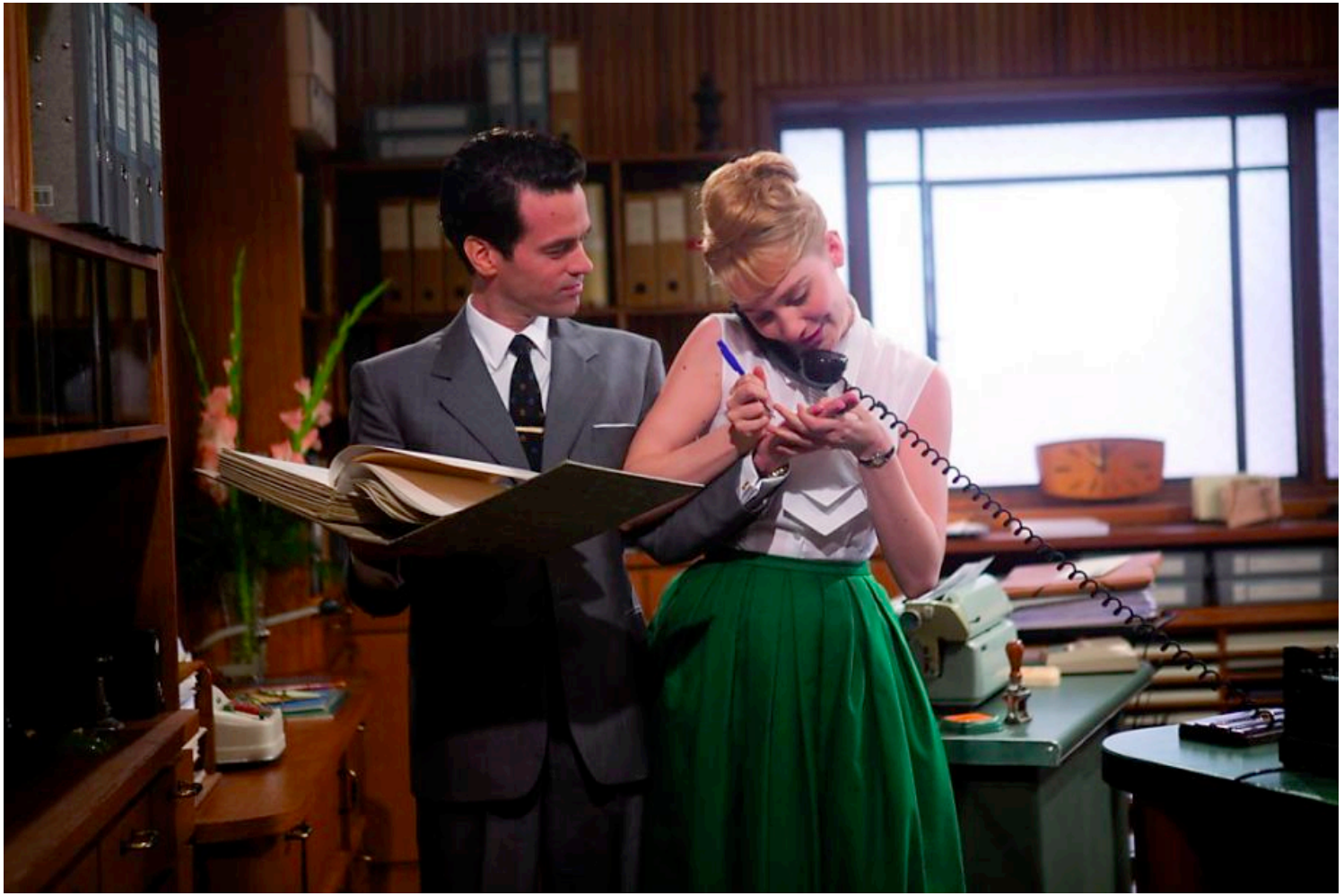
分布式拒绝服务防御协调，大约2005年。

```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

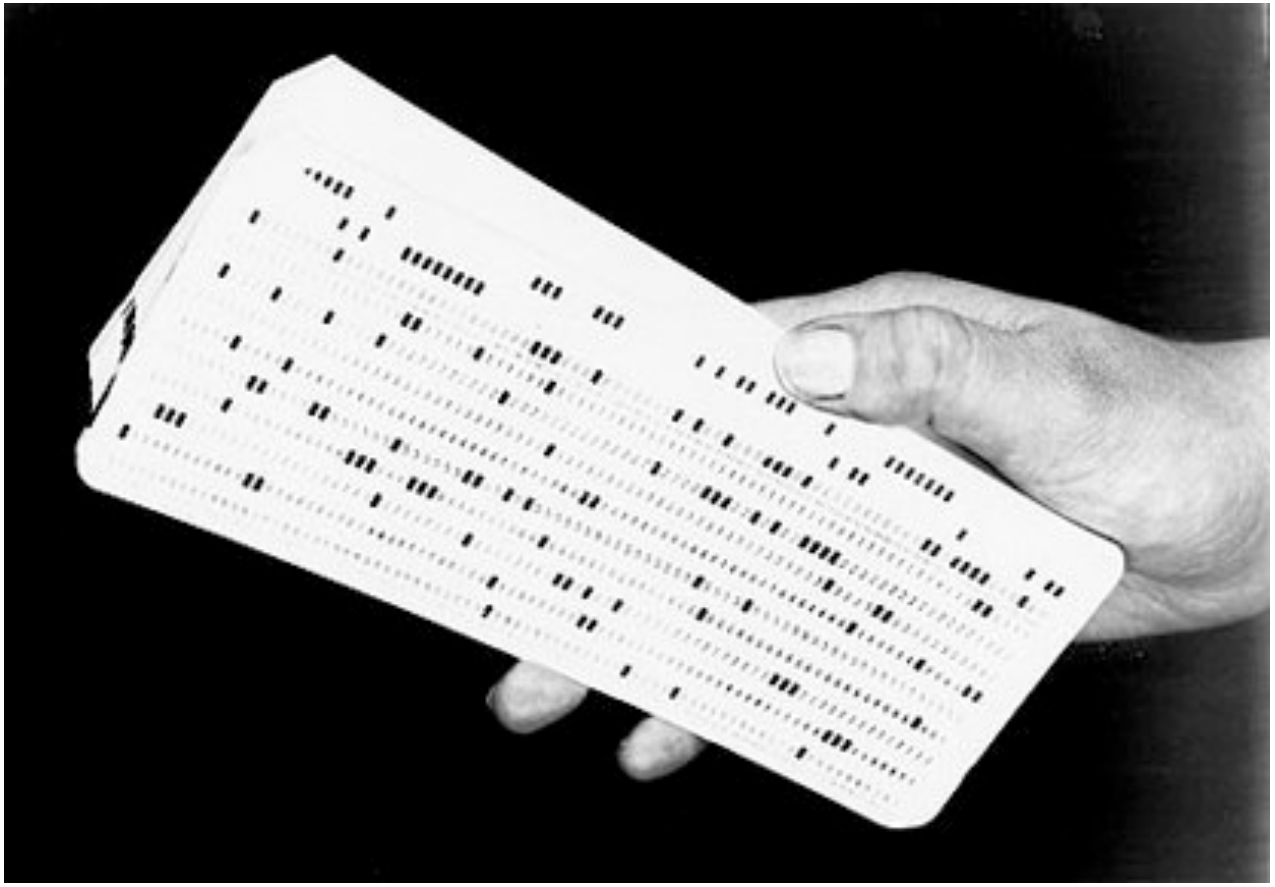
分布式拒绝服务防御协调，大约2005年。

```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

我们可以并且必须做的比这更好！



我们需要标准化的信息共享途径。 。 。



。 。 。跨越快速，低延迟，不可靠的传输。 。 。

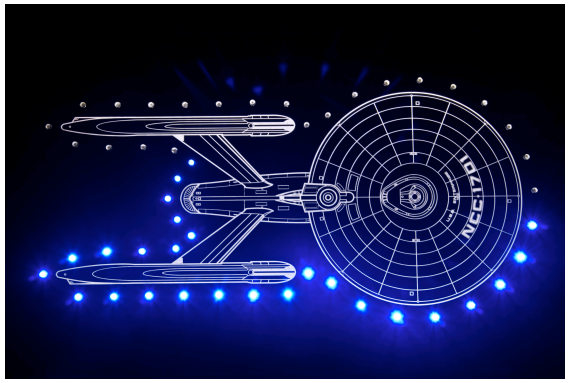
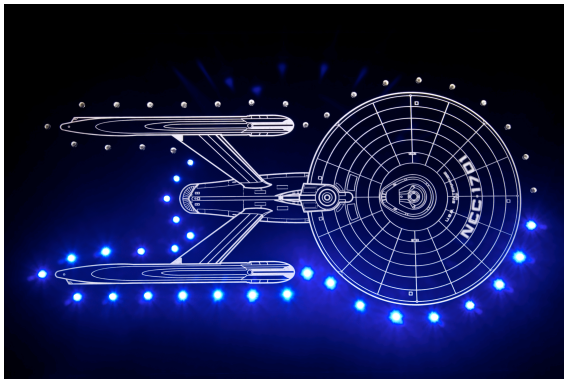
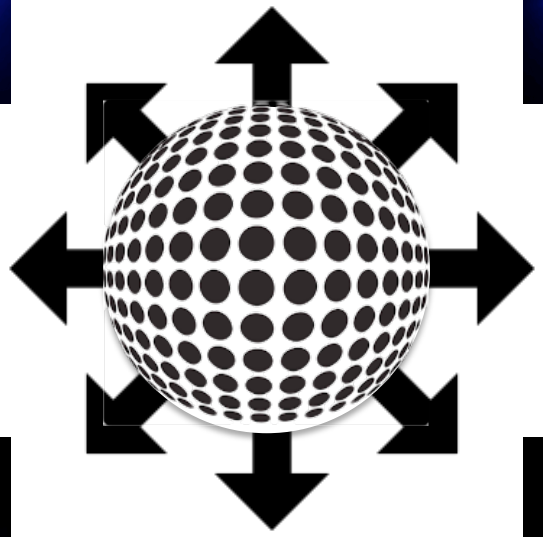
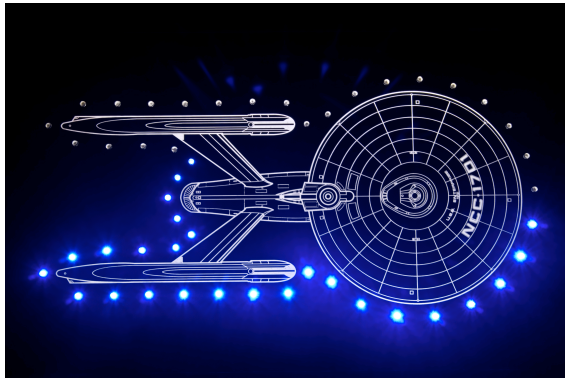
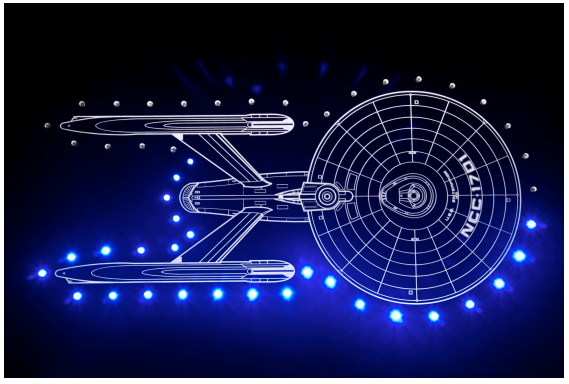
。 。 。跨越可靠的运输，通过政策来实现。 。 。

。 。 。告诉我们有关自身，问题和所需措施的信息。 。 。

。 。 。可以根据需要在内部和外部中继。 。 。

。 。 。网络上的每个人都能参与。 。 。

。 。 。在协作式按需分布式拒绝服务防御中。

DOTS操作要求摘要

DOTS操作要求

- 基于标准的分布式拒绝服务攻击和缓解信息交换。
- 不得承担请求者的有机检测/分类功能。
- 必须跨通用的不可靠和可靠的传输方式工作。
- 必须支持双向身份验证和可选加密。

DOTS操作要求（续）

- 必须描述遭受攻击的目标（IP地址范围，在目标上运行的端口/协议/服务等）。
- 必须以一般术语（阻止，重定向，清理，速率限制等）描述所需结果。
- 必须用实施的操作和状态更新请求方，请求方必须执行相同的操作和状态。
- 必须支持组织内和组织间中继。

DOTS操作要求（续）

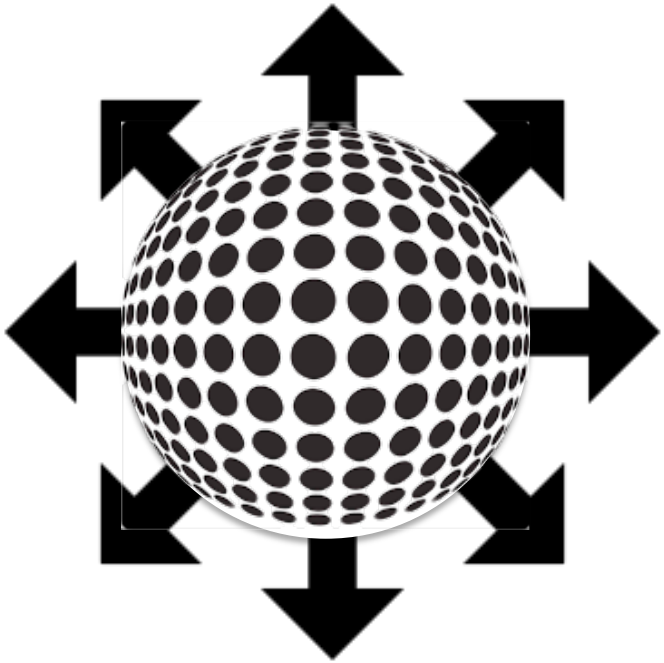
- 必须支持基于策略的操作/结果过滤和转换。
- 必须是可扩展的。
- 首先必须专注于分布式拒绝服务，后来可能会用于其他用途。
- 必须最小化实现和节点交互的复杂性。

DOTS操作要求（续）

- 必须包括“心跳”功能。
- 必须与检测/分类/缓解技术无关。
- 必须支持允许的分发范围（TLP？）。
- 应在任何可能的地方，酌情利用现有的协议和信息模型。

本演讲 – http://bit.ly/1l2lVrF

93rd IETF Prague
July 19 – 24, 2015



分布式拒绝服务开放威胁信令（DOTS）工作组

谢谢！

Chris Morrow <morrowc@ops-netman.net>
网络安全工程师, Google

Roland Dobbins <rdobbins@arbor.net>
首席工程师 , Arbor Networks