对SSL流量的检测（使用受信任的证书模拟）---破坏ssl协议不可行

blindbox在对加密流量的检测上做出了贡献blindids也是其中一个发展

blindids：依然不解密流量，完善了blindbox在明文规则和大小上的不足

声称：第一个完整而正式的安全模型

四方：RG MB S R 结构与privdpi，spaBox相同

依然不考虑：S 和R都是恶意的情况。（即使在明文网络中这种通信也不能很好的识别）

【note】：s和r都是恶意（怎么定义恶意，对恶意者来说这次通信是善意的）

MB：定位依然是诚实而好奇

RG:不同之处：可能会在网络上监听有自己签名的数据包

论文设定：MB和RG不会联手的原因：市场声誉的限制

本文设定：发送者是恶意的，接收者善意（至少一个善意的）

模型：

（未加密的）规则 R 和一个检测算法，表示为 Detect，

将（未加密的）流量 T 和该集合 R 作为输入。在后文中，我们说该流

量是恶意的 iff Detect （T， R）=0。否则，流量是安全的，并且 Detect

（T，R）=1。在两种情况下，也可以提供一些辅助信息 aux作为检测算

法的输出。我

5过程：

setup：

每个人都有一个公钥（可以没有私钥），有公共安全参数生成的一些潜在key

RULEGEN：输入生成的一组公共安全参数，RG使用自己的私钥对rule进行加密，生成Brule，发送给MB

Send：使用公共参数，用自己的私钥和R的公钥发送Tmsg，Tmsg，加密后为Emsg

detect：检测;MB使用自己的公钥，加密Emsg，加密Brule，输出0、1 1match 0safe

recv：使用自己的私钥，Emsg作为输入。输出Tmsg

---------------------------------------------------------------------------------------------------------------

安全性

1.检测能力

2.流量的混淆能力

3.签名的不可分辨（针对RG的网络探测）

检测能力：图1假设A为敌手

流量的混淆能力：图2不可区分实验

规则不可区分：

=--===================================================================

解决的blindbox的不足：1.大小 2.明文规则 3.不使用sslKey

使用可解密的搜索加密Decryptable Searchable Encryption (DSE)一个工具

DSE：

关键字搜索属性指出给定密文 c 和关键字 w，测试密文是否

与关键字匹配是可行的。此功能对于解密密钥的所有者而言是显而易

见的，但也可以以关键字特定的陷门 T（w）的形式转移给任何人

KeyGen 是密钥生成算法，它以安全参数 A 为输入，并输出公共

密钥 pk ，解密专用密钥 sk和活板秘密密钥 tk 。

• Enc 是加密过程，输入关键字 w 和公共密钥 pk 作为输入。它输

出与 w 和 pk 有关的密文 c 。

• TrapGen 是陷阱门的生成，该陷阱门将 关键字 w 和陷阱门密钥 tk

作为输入，并输出陷阱门 T（w）。

• 测试 是一种测试算法。它以密文 c 和活板门 T（w）作为输入，

如果 c 是 w 的加密，则输出 1，否则输出 0。

• Dec是解密过程。它以密文 c 和私钥 sk 作为输入。它输出相关的

关键字 w。

具体算法p7

----------------------------------------------------------------------------------------------------

使用MB转发的方式，与spabox不同

S 和 R之间的流量使用DSE特定方式加密

原有的DSE有一个漏洞（4.3）修改了协议达到目的，使得其不能得到关键字的信息

----------------------------------------------------------------------------------------------------

开销不取决于规则的数量，使用的不是ssl学徒，需要握手

setup的开销转义到了MB的检测部分，DSE检测协议使用的检测时间比MB的检测时间更长，但是减少了内存的开销

blindbox的内存开销大小主要是为每个sender准备一个乱码电路，大小0.5M

BlindIDS也声称自己是第一个实现应用化处理的人，保持了各个方面的平衡

【note】：不适用ssl加密流量，而是使用一个DSE的工具加密流量。可能普适性差，且简单的setup导致MB的检测负担变大。