一个 调查 的 隐私保护 技术 的 加密流量 检查通过网络中间盒

Geong Sen Poh
Dinil Mon Divakaran
勋卫离呒
geongsen.poh@trustwave.com
dinil.divakaran@trustwave.com
hoonwei.lim@trustwave.com
Trustwave

尖挺宁*
jtning88@gmail.com信息系统学院
新加坡管理大学，新加坡，178902

Achintya Desai *
achintya.desai@gmail.com国际信息技术研究所，海得拉巴
印度海得拉巴500032

抽象

中间件在一个计算机网络系统的检查和分析网络流量检测恶意通信，监控系统性能，并提供运营服务。然而，加密的流量，这已成为越来越普遍，阻碍了abil- 两者均的 中间件 来 执行 这样的 服务。 一个 常见的 在实践中 解决 这个 问题 是 由 采用 一个 “人在这方面的中间人” （MITM） 的方法， 其特征在于， 一个 加密的 业务 流 之间的 2端点 被 中断， 解密 和 分析 由 所述 中等框。 该 中间人 的做法 是 直接的 和 被 使用 的 许多组织， 但有是既 实用和 隐私 的担忧。实际上， 由于 到了 成本 的 在MITM 家电 和 的 延迟发生由于到的加密，解密过程， 企业 继续以 寻求 解决方案， 这是不太 昂贵和更少的计算密集型。目前 已经 还 了 讨论 上 的 许多 努力 需要 来配置MITM。 此外， MITM 违反 终端到终端的 隐私 瓜拉尼开球， 募集 隐私 担忧 和 潜在的 问题 上 遵守尤其是 与 在 上升的 意识 上 的用户 隐私。 此外，一些 中 的 MITM 实现 被 发现 到 被 有缺陷的。 CON- sequently，新的实践和隐私保护技术，这使检查过加密的流量被提出。

我们系统地检查了这些技术，以比较它们的优点，局限性和挑战。通过定义一个由系统架构，用例，信任和威胁模型组成的框架，我们将它们分为四个主要类别。这些是可搜索的加密，访问控制，机器学习和受信任的硬件。我们首先讨论的人在这方面的中间人的方式作为一个基线，然后讨论在细节每一个的他们，并提供了一个深入compar- isons 的 自己的 优点 和 局限性。 通过 这样做 ， 我们 描述了采用该技术的实际 限制， 优势 和 陷阱。继此，我们给出的见解上 该缺口之间的研究 工作 和 实际 执行 中 的 行业， 这导致 我们到了讨论上的挑战和研究方向。

CCS概念

· **安全 和 隐私 → 网络 安全**； **安全 协议**； *公共密钥（非对称）技术*; **对称 密码 和 哈希 函数**； *入侵 检测 系统*。

[*] w ^扫嘉莉d出来的时候的作者W ^ ê [R é附属d与该ñ美国Singtel的赛扬b呢硒安全实验室

,

。

关键词

加密 流量 分析， 深度 数据包 检查， 数据隐私， 中间盒

1 引言

包 检查 和 分析 已 被 用于 对 检测， 减轻和 阻止 可疑的 活动， 在 家庭 和 企业 网络。这是实现 通过 检查 的 报头 和 有效载荷 的 网络流量 的 实时 时间。 该 设备 部署 为 这个 目的 被 称为 中间件[1] 。 一个 中间设备 （MB） 提供 各种 服务 ， 在当今的计算机网络基础架构中 必不可少。一对的主要服务包括部署MB的系统和用户secu- RITY，用于例如，作为个人和组织的防火墙，入侵检测和预防系统，家长过滤，数据泄露检测系统，取证分析工具，如良好的恶意软件detec- 重刑 系统。 在 另外 对 安全性， 它 是 也 常见 到 部署 MB 的 性能 和 运营 服务。 这些 包括 服务于代理/高速缓存作为在内容分发网络（CDN），广域网优化，协议 加速， 访问 控制， 计费 和使用 监控， 和 网络 地址 翻译。 合规服务 是还 部署了 作为 一个 MB， 来 履行 义务， 这样 的 需要 ， 以 支持 合法 拦截 和 控制 的 非法 内容和 隐私。

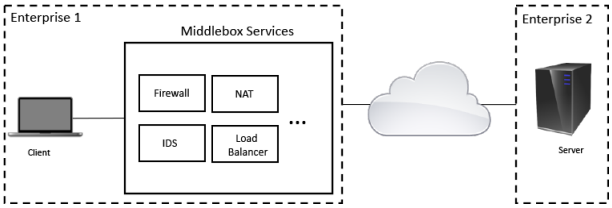

图 1： 传统 型-I [客户为本]： 客户端CON组nects到中间件服务为入站和出站NET-工作时，交通巡查

传统上， 宏块 被 部署 在 该 楼宇 的 企业 或客户网络。这些被称为“预置”的解决方案 （无花果URES 1和2）。 随着 中出现的 网络 功能 虚拟化

[1]个甲 中间盒， 也 被称为 作为 一 网络 设备 或 一个 网络 功能， 被 定义 在RFC 3234 作为 *任何 中介 框 执行 功能 除了从 正常的， 标准功能的 一个IP 路由器上的数据路径之间 一个 源主机 和 目标主机*[13]。一个 类似的 定义 是 还 提供 在 第一部分 我 的ETSI建议 在 中间盒 安全协议 和 企业 运输 安全 （ETS） [23]。

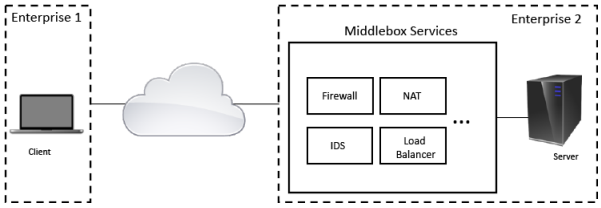

图2：传统模式-II [面向服务器]：服务器CON组nects到中间件服务为入站和出站NET-工作时，交通 巡查

（NFV）[30]，所述 依赖 于 专门的 和 昂贵的 硬件 部署 的 宏块 被 也 被 质疑，并且 存在 是 一个 明显转变 朝 部署 的 基于软件的 中间件 功能。在 其他 也就是说，我们 已经 开始 向 看到 的 外包 中 的MB 到的 云基 础架构，从 在 常见 的预置型 部署模型 [27， 37] （图3）。虽然 云计 算 基础架构 提供 了更大的灵活性 和 动态 可扩展性 不是 一个 基于硬件的 设备，他们 也 来 与 新 的挑战，尤其是 在 确保 安全和 隐私 的 这些 系 统 [8， 23]。

在 为了 以 使 服务 提到 上面 在 一个 有效 人为NER，中间件经常执行 网络检查和分析使用一个公认的技术公知为深包检查（DPI）[2] 。DPI 工具深入检查上的报头和有效载荷的网络数据包，在对比以 传统 包过 滤 是 检查 只有 数据包 报头。DPI 可以 是 有状态的，与不同的 有用 状 态 存储 期间 的分组 的处理， 例如 如流动 特性， 应用 状态， 等等 [33]。然而，目前87% 90%的所述网络通信量进行加密使用TLS [15， 40]。根据 对谷歌transparancy报告，为的年11月到2020 年81%， 98% 的 的 流量 使用 Chrome的 平台， 跨 不同操作系统 的系统 是HTTPS流量[48]。现有 DPI 技术即是仅能够的检查纯分组 属性 将是 的 有限 的使用 和 严重 影响 上 的 各个 网络服务 为 被 详述 通过 卡纳瓦莱 和范Oorschot在[19]。这种 手段的MB必须 制定 机 制能 的 分析加密 流量 中的 一个 方式 是 平衡 的 要求 的保密性， 实 用性 和 性能。

1.1 行业实践和新方法

两个常见的技术广泛地用于在该行业（在特定 于部署的MB在企业 [10]）来检查加密的流量是
（1）所述 的分裂TLS 技术，这 是 也 公知 为 一 人在the-中间 （MITM）的方法，和（2）键共享和委托。

MitM。 在 中间人，而不是的 建立 的 终端到终端的TLS会话 之间 的 客户端 ，并 在 服务器 的 客户端 建立 一个会话 使用 的 中间件。通 过这样做的话，加密 交通originat-荷兰国际集团从 所述 客户端 可以 被 解密， 检查 和 分析 由 MB。该 MB 重新加密 和 转发 所述 数据 到 所述 服务器上的 代表 的 的 客户端 经由 一个 第二， 新 TLS 会话 之间 的

[2] 根据国际电信联盟的建议 ITU-T Y2770 [33]，DPI是的 *分析，根据到该分层协议架构OSI-BRM [指定在ITU-T X.200] 的 有效载荷 和/或 数据包 属性 中列出 在 条款3.2.11]更深 比 协议 层2， 3 或4 报头 信息，以及 其它 数据包 的属性，以确定该应用程序 明确地。*

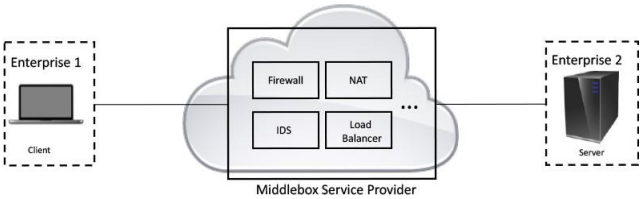

图3：外包模型：客户端或主机服务器订阅基于云的中间盒服务

MB 和 该 服务器。这 提供了 一个 切实可行 的解决方案 是 可以 被 部 署 ，而不 需要 任何 修改 到 了 TLS 协议，但 它 确实 需要 一个 客户端 来 安装 了 MB的 根 证书。该 根证书 使 所述 MB 到 呈现 自身 作为 所 述 服务器 （即 目的地 端点） 到 了 客户端 的 复制 和 签署 一个 新的 证书基础上的 凭据中的 服务器。在实际上，在MB假冒 的 服务器。这种 部署 是 安全 的 长 为 根 证书 被 安全地 存储， 跟上时代的 TLS 实 现的 使用， 以及 一个 可配置的 策略 引擎 是 使 的 管理- istrator到设 置一个白名单[3] 被提供。不幸的是， 一些的的部署 已经 被 示出 至是 不安全的，由于 对 的弱点 在其 执行 的 所述 底层 协议， 例如 作为 允许 弃用 密码 套件， 如 所讨论的 由Jarmoc [34]， 卡纳瓦莱和 甘露[18]， Durumeric *等。*[22]和Waked*等。*[58]。此外，基于 上 的 调查 进行 由 雪莉 *等人。*[51]，具有异构网络设备 的 大型 网络将需要许 多 经验丰富的管理员 来管理 它们。这带来了另一个隐私担忧时MITM 方法 被 使用时，因为许多的这些设备 可以 具有 接入 到 该 解密的 数 据。这 将 是 困难的 配置 这 是 该 设备 是 应该 有 访问 和 也对 跟踪 的 网络 流量。

密钥共享和委派。在这种方法中，企业分享他们的证书，或私 人密钥，以及客户共享会话密钥用的中间件。他们都支持通过行业 实际使用。对于例如，一个服务器共享其私有密钥与CDN，或者在 服务器共享静态密钥与中间件，如去尾中的企业运输安全（ETS） 标准化由ETSI [19]。问题与一些的这些方法包括不支持完美正 向 保密 （PFS），并因此将不兼容与TLS 1.3。详细的讨论上的 各种AP- proaches 和 问题 可以 是 在 [19]中找到。

双方的中间人，并重点分享的方法违反了最终 的端到端加密 和数据隐私保障的的所谓安全 两方 的通信，并且 可以 是 昂贵 和 困 难来实现。有是还的可能性，即一个MB存储 解密的 数据，这 打 开 了 另一 组 的 可能性 进行攻击 和 数据 泄漏。这 意味着 在 宏块 和 该 管理员 必须 完全 信任在这样 一个 环境。由于 到这些，US-CERT已 经 最近发出 的 警告 ，指出 该 使用HTTPS拦截变弱

[3] 一个 白名单 包含 的网站，其中 的 中间件 将 不会 检查 和 仅仅 转发 的 加密 流量。对 于 例如，加密的 流量 到 网上 银行 网站，和信用卡交易。

TLS安全性[17]，并在国家安全局（NSA）已经也发出了咨询的潜在内幕威胁上的使用的MITM [1]。

隐私保护 方法。 从该角度来看的革命制度党vacy，一调查上用户接受对加密的流量检查（即TLS）通过中间盒是进行由Ruoti *等人*。[50]。1976年参加者接受了调查。75 。8%表示对隐私和疑虑身份 盗窃 的 黑客，而 70 。9% 的 关注 有关 政府 监督。此外，使用中间人 和 键 分享 作为一个 工具 来 检查 网络 流量 可能 还 违反 保密 规定等 作为 对 最近 公布 的 欧盟 通用 的数据 保护 条例（GDPR）。对于 例如，明确 同意，从 一个 可能的消费者 被 要求 对 一个 第三方（例如，在 网络 安全 服务提供商 是 供应 和 管理 的 MBS）来 访问 的 数据， 和 83 。2% 的 参与者 在 Ruoti *等人*。的 调查 表明 是 他们 应该 首先 被 告知 或 同意。

这 是 因为 到 了 上述 担忧 新 方法 被 提出 由该研究团体。许多建议集中于该企业以上（例如，面向客户的和所讨论的环境 服务器-取向 设置 在 图 1 和 2 分别地）。一种 新的 方法 是 要 进行 加密的 流量 分析（ETA）基础上 机器学习 技术。一个 全面的 研究 可以 被 发现 在 该 ENISA最近的 报告[20]。该报告 调查了6用例是马茅根 学习 技术 是 很大程度上 有效， 即 应用识别，网络分析，用户信息识别，检测 的 加密的 恶意软件，指纹识别 和 DNS 隧道 检测。机学习技术，保护 隐私 是 他们 不 检查 的 （加密） 的有效载荷。然而，它被指出 的是 这种 技术 不能提供的相同水平的检查如在 正常 监控 的 未加密的 流量。

在 与 其他 手，另一个 新的 方法 是，以 设计 与隐私保护技术来检查加密的有效载荷没有缺陷 的 中间人。然而，该提议的方案要求无论是主动参与的双方的客户端和服务器端点，或 引入 问责制 的 两个 端点，以 允许 可视性 上 所有 的MB 是 坐 之间 的 客户端 和 该 服务器。在 实践中，根据 我们的 互动 与 该 行业，它 是 不是 可行，以 要求 所有端点 来 安装 或 坚持 到 这样 一个 建筑 的要求，如 在 还 指出 了 通过 卡纳瓦莱和范Oorschot [19]。例如，检测应被执行在一个方式即是不可知 到 了 目的地。一个 客户 机，为 的 源 端点 访问的Web 应用程序提供商，例如 如 谷歌，脸谱，亚马逊 或Instagram的。这 将 是 一个 重大的 事业 为 的 供应商 有 来 部署 类似 解决方案 的 那个 的 客户 来自 不同 企业 访问 其 站点。此外，如何 将 在 供应商 信任的企业 是要求以建立连接，以及什么是在激励中要通过的潜在昂贵的定制安装 成本是多少？我们相信这是一个的的障碍，在采用 现有的 隐私保护 方案 的 实际 实际部署。我们将在第 4节中详细讨论使用这两种方法的方案。

1.2 外包MB 服务

在 困难 的 给予 的 无数 设备 [51] 也 助长了 发展 的 新的 中间件 服务 是 的出发 从 该 传统 的本地 企业 中间盒 设置。该 emerg- ING 趋势 是 对 外包 MB 功能 到 基于云的 服务，这通常 称为 为 MB 作为 一个 服务。图 3 示出了 一个 总体结构 的 外包 的MB。它 减轻 了 企业 的 需要-荷兰国际集团，以 购买 相关 硬件，安装（包括 软件 和 硬件），配置，操作 和 维护 中间盒。因此MB的外包减少，或几乎消除，运营 成本，并 从而 使 该 企业 以 专注 于 它的 关键 业务。然而，外包 的MB 到 一个 第三方 供应商 加剧了 隐私 担忧 时 相比 于 在 内部部署 企业 SET-婷，因为现在数据即是 通常 检查 内部，具有 要被 路由 到 的 提供者 进行 处理。因此，许多研究工作 都 提出了 到 安全 MB 服务 中 的 云，其中包括隐私保护 检查 的 加密 流量。在 另外 到这一点，基于云计算的MB必须提供低延迟的操作，因为流量有到被重新路由到了云中。一个 例子 溶液 其能够保护隐私的检查用低延迟是出发，提出了 由 兰 *等人*。[37]。低延迟 是 实现 通过 一个架构 已知 作为 电器 为 外包 的MB 引入（安普仁）中[52]。在 一般的 想法 是 要 创建 一个 标记化 恩加密后 的流量 沿 的 TLS 流量。检索的 加密 方法被 用于 对 匹配 的 标记化 加密 通信 用 的 加密规则集 在 所述 MB，所有 的 这些 都 设置 在 所述 安普仁 AR-民族形式。

在 此外，许多 更 近 外包为主的 MB 建议开发 技术，这 是 基于 对 安全的飞地（即英特尔SGX）。这些 包括，为 例如，SafeBricks [46]，ShieldBox [56] 和SPlitBox [7]。在 一般的 想法 的 这些 技术 是 对 执行 数据包 检查，在 该 安全 飞地 这样 说 的 云 提供商也没有学习的内容中的加密数据包。我们将在第4.5节中更详细地讨论这些建议。

1.3 我们的 研究概述

在 本质上，一个 被 找 为 一个 最佳 的解决方案 之间 2个极端，（1）的 不 存在 能够 以 执行 深入 检查 由于该流量被加密的; 和（2）检查的解密 交通使用MITM和密钥 共享 的方法。许多 解决方案 已经 被提出 在 了 最近 几年 要 解决 这个 问题。我们将其归类为4类基础上的技术，他们使用。我们讨论这些技术在第 4，我们还包括了中间人的方式作为一个第五个类别中的开始的中讨论的比较。我们认为，在不同的设计和性能 的 成长名单的建议 应该被研究的 顺序，以清楚地 描述 自己的 优点 和 局限性。我们的 研究 提供了深入了解 的 安全 保证 和 性能 在 不同 使用情况下的场景，作为以及作为上诉的的技术，以真实世界的部署：

- 我们定义一个通用架构，标识的使用情况和他们的 约束（第2）。我们定义了3个系车型在规定的架构是说明了流量的网络流量通过的宏块。我们称之为他们面向客户，面向服务器和客户端-服务器负责设置。我们的模型提供了更多 细粒度 分类 和 增强 上 的一维 单面 和 双面 定义 中 的ETSI标准[23，25]。
- 我们定义了一个信任模型，该模型包含了包含MB的网络系统中的不同参与者（第3节）。它提供了一个

基础上，其安全模型可以被定义清楚。我们陈述 信任 的假设 基础上的架构和设置，即我们定义的，并确定威胁和安全要求，基于对这些假设。

- 我们分类现有的隐私保护技术为2类，*被动*和*主动*。这里，*被动*检查包括tech- niques该分析所加密的通信而无需解密或， MOD- IFY的流量的所述底层的协议。*主动*检查anal- yses的流量通过解密或修改的了基本协议。这些技术被分类为*访问控制*，*可搜索的加密*，*机器学习*和 *可信硬件*， 如 以及作为所述MITM方法用于比较（第4）。我们COM-削减的主要特点，优点和缺陷的每个类别。我们确定的研究挑战和讨论的潜在的研究方向 （第5节）。我们检查了当前的安全模型并分析了现有的攻击。这导致我们要 相信的是一些中的现有提议需要进一步的IM provements为行业收养。对于例如，一个协议，利用搜索加密机制将需要至 被 anal- ysed 对行之有效的 概念 的 信息 泄露 中的 字段。我们给出的见解，尤其是对的原因是exist- ING MITM 方法，用 组合 的 一个 配置的 策略引擎， 都仍首选中的行业。

作为一个边注，为实用和高效的部署与最优检测能力，它似乎解密的的加密的有效载荷是一个中的更好的方法。什么仍然要进行研究的是多如何加密数据应被解密，并透露给了以MB为单位为了要保护隐私。它是，我们相信，基于对这一事实，一个新的MB安全协议 （MSP）被提出和被接受的标准化工作[24]。它可能也是该情况下的是可信硬件的方法，例如如使用英特尔SGX，正在被开发，其中加密通信量被解密在一个办法保护通过硬件这样说的MB有没有访问到的解密数据。该技术和挑战的讨论在细节在第4和第5。

一个简短的调查有关，以该问题是我们研究的是提供 由王某*等人*。在[59]中。它研究的各种机制，为安全外包的宏块中一个普遍的方式，重点只在云基于MB。我们的工作补充他们的一个方式是我们提供 更广泛的调查，其中还涵盖了非外包的特定文献，因此我们定义了不同的系统模型和用例。在欧洲的联盟机构的网络安全 （ENISA）也公布一个调查上加密的流量分析[20]。该调查描述中详细地在特定6键的使用例 （即应用程序识别，网络分析，用户信息识别，加密的恶意软件，文件/设备/网站/位置手指甲的检测印刷和DNS隧道检测）和技术基于对机器学习。大多数近日，卡纳瓦莱和范Oorschot [19]提出了一个全面的调查上TLS拦截机制和动机，重点对实际的考虑之间的使用情况和奖励的的利益相关者。他们列出的19用例，其中接入到未加密的流量是至关重要的，在为了理解的动机中的各种建议在检查加密流量。其中的的关键见解，从他们的调查是在识别的差距之间的提议机制，使用情况和激励措施。大量细节上的各种MITM和关键shar-荷兰国际集团的技术进行了研究和比较。在这里，我们的重点是在用汇编隐私保护技术，分类的国家的最艺术，深入检查和比较这些不同的技术，它补充这些最近的调查。

2 系统模型和使用案例

我们现在描述的基本模式和使用情况。在不同的 模式是我们讨论在这里是基于上的设置提供由雪莉*等人*。（BlindBox）[53]，Canard*等*。（BlindIDS）[18]，Bhargavan*等*。[8]和ETSI标准I [23，25]。在为了要提供实用的见解，我们还存在使用案例场景对于每一个国防部-埃尔斯。图1， 2和3示出一个一般的高级别体系结构的MB的操作在一个计算机网络环境。我们描述了现有的和潜在的使用情况下，基于对这些架构。我们句话说它是常见的用于宏块，以充当直接到所述传递traf- FIC中的*带*中间盒设置，其中一个或多个中间盒被放置在线路之间的客户端和所述服务器。用于操作目的的常见用例包括内容交付网络（CDN），评估控制，计费和使用情况监视，资产跟踪，名称或标签解析和操作控制。这是也有可能在一定的使用情况下，该MB的存储的交通和分析他们在*出带外*设置。网络安全用例包括网络防火墙，应用程序防火墙，入侵检测系统（IDS）和入侵防御系统（IPS）。它是同时使用对于compli- ANCE义务，例如可用性/恢复能力，应急和公众安全通信，数据保留，身份管理，网络安全，内容控制，个人数据和隐私[23，25]。

2.1 客户端MB

我们首先描述了一个典型的面向客户的设置即是常见的企业网络。图1示出了一个高层次的模型的设置，其中，所述目标的所述中间件是对保护的clilent（多个），并且因此被经常置于更靠近于所述客户端（一个或多个）。在这里，一个客户端连接到一个服务器使用一个安全的信道。所述加密的流量流动，两者的入站和出站，被路由通过一个主机的MB的该检查的流量。MB接收来自多个客户端和服务器端点的入站和出站流量。它通常包括安装特定软件，或修改在连接在所述客户端设备中以便于使所述的MB来执行该检查。

用例。常见的使用案例包括防火墙，广告拦截，个人数据保护和匿名化的Informa的重刑[55， 62]。一个例子就是，保护的用户的隐私，而恩abling加密流量检查在一个计算机网络中的一个或-ganisation （例如一所大学，一个金融机构或一telecommu- nication公司）或由一个外包的中间件服务。雪利酒*等*。[53]描述一个场景，其中学生使用该大学网络安装的提出解决方案，以保护隐私的他们的数据尚未允许的系统（例如，一个安全解决方案），以检查加密流量。另一个使用的情况下，的亲滤波器，其中一个用户所预订的服务从一个ISP （因特网服务提供商）中也提出了。这2例优先考虑检查的OUT- 绑定流量从该客户端。Bhargavan*等*。[8]还指出，防火墙已部署在公司和教育机构到

保护电脑的恶意软件上都入站和出站流量，为例子。将最相关的部署方案，为企业是在面向客户的中间件。在这种情况下，一个企业部署的MB电器在其前提下，在对周边的的网络。该MB检查所有传入和传出通信（除了那些已列入白名单）从/向所述客户机，使用该先前提到的MITM方法。由于企业经常实施波利-资本投资者入境计划对员工的机器，在安装的根证书是允许的MB来解密和重新加密的流量是不是一个实际的问题。

2.2 面向服务器的 MB

甲面向服务器的MB是也常见于一企业网络（图2）。这是对安全的服务器托管在一个企业中，例如网络服务器。一个服务器在一个企业建立安全通道与请求的客户端那是经常之外的企业网络，在特别的互联网。该加密的流量从/在服务器端点都路由通过一个主机的宏块在服务器端（或外包给一个第三方服务提供商），其检查的加密流量。的主要技术在差异这一设置相比于在先前的一个是该连接的所有请求通过客户端，并且在一般的目的是要保证一个特定的服务器。面向服务器的MB被开发来保护服务器，例如作为网络服务器，数据库服务器，并因此上。甲典型的例子是一个网络应用防火墙该检查传入HTTP请求到一个网络服务器。由于该网站服务器本身已移动到云中，因为一个数年的现在，其面向服务器的宏块中的云是不鲜见，这些天[2]。

*用例。*一个常见的情况是，其中的内容交付网络（CDN）供应TLS交通上代表的客户的网站。在这种情况下，在重点是在检查的许多入站流量流入到该网站。另一使用情况下，被设置在所述ETSI标准[23，25]。它涉及到一个数据中心，这将需要检查的加密流量从不同的内部网络。这个装置之间的MB这些网络必须是能够向通信和检查的基础的加密通信。

3 信任 模型

在 至少 一个 的 的 2个 端点 必须 是 诚实的。 虽然去ploying一个传统的网络安全的解决方案，例如作为一个intru-锡永检测系统（IDS），它被假定的是任一个的所述端点必须是诚实[53，61]。否则，两个恶意端点可以达成共识在一个秘密密钥和加密的通信采用沿用已久的加密方案。Canard *等。*[18]描述的一个SCE-nario的，由此一个受感染的机器人所连接到的远程命令和控制服务器使用一个加密信道。检查将成为不可能时的交通流是加密。类似的假设是由在该情况下的宏块提供家长过滤和数据渗出检测[53]。在父母的过滤器，它是假定无辜的孩子会不会取代网络协议栈或安装隧道软件。数据漏出被假定到发生由于到意外传输的敏感数据。在其他词语，该情况下的一个用户（或一个对手即获得了控制上的装置）故意破坏一个设备到规避现有网络连接是不考虑在一些的所述建议[12，37，43，44，53]。

什么，如果这两个端点是恶意的? 鉴于在上述descrip-重刑，我们可以争论的共同假设是认为无论是在客户端还是在服务器必须是诚实的。然而，一个不能低估的攻击是故意修改一个用户的设备，用于例如，提取和发送敏感信息到一个恶意服务器。在事实上，一个方案是假设这样一个场景，其中两个在用户和服务器都是恶意的提议由Goltzsche *等人。*[29]。他们提出的解决方案利用安全的飞地，以防止一个恶意的客户端从操作的TLS流量。

从这些对比假设，在对下面我们定义在更清晰的细节，在信任的假设下的3个车型和使用情况是，我们已经讨论了。

3.1 假设

实体。三个主要的实体是参与在一个典型的设置。这是一个*客户端*，一个*MB提供商*和一个*服务器*。在一些的的方案中，一个第四实体可以是参与。对于例如，在对外包MB设置一个*云服务提供商*的主机的中间件。在其他SET-吊环，一个*设备*的行为作为一个值得信赖的政党在一个企业对寄存器-登记领或流量加密，或者一个*规则生成*共享/加密的规则集进行的中间件。一个实体可以是*诚实的*，*半诚实*，或*恶意*。通过*诚实的*，我们指的是一个实体遵循该协议的诚实和坚持到所有的安全要求和目标的的协议。在与其他手，一个*半诚实*实体fol-低点的协议诚实，但也将"等待"到了通信的顺序来尝试以提取或学习的内容中的信息从通讯。阿半诚实实体是还公知为一种*诚实但好奇*实体中的文献。一个*恶意的*实体是一个实体，是在除了要听来的通信，具有的能力，以改变该通信的顺序来，为实例，冒充一个的的合法实体和学习的基础消息被发送时，或假定控制的的合法实体。我们注意到的是它是可能的是一个客户端被感染的僵尸在企业网络（因此成为一个*恶意*实体），但该协议是不会受到影响。这是对说，在交通流仍路线通过的企业网络和的中间件。

相信。表1列出了信任的假设认为通过现有的方案。甲共同设置是其在中间盒是要么诚实（H）或半诚实（S），而无论是在客户机或所述服务器是诚实[4]。这是该案件的方案使用4项技术是我们讨论在第4，这些技术是人在这方面的中间人（MITM），检索加密（SE），访问控制（AC）和马折角学习（ML）的技术，如所示在列1-4中的表中。一个例外是一个方案叫EndBox[29]（行5），其中两个所述客户机和所述服务器可以是恶意的，尽管该MB被假定诚实。这是由可能通过部署可信的硬件（TH）等作为安全飞地（即英特尔SGX）在该客户端的设备。在这种方式的攻击者是不是能够对访问的方案，并修改了执行的的代码是被携带出里面的飞地。转播viously如果所有3个实体是恶意再有就是没有被保护。安全飞地是也使用在更多的最近亲提出的方案中的外包MB的场景。例子包括

[4]我们也不会考虑的情况下的半诚实的客户机/服务器，因为在原来打算的的通信是为双方的他们要发送/接收邮件，并因此他们学会了基本的内容呢。

SafeBrick [46]， ShieldBox [56] 和 SGX-Box [31]。 在这里，该服务提供商 托管 的 宏块 可以 是 恶意的，因为 执行 的 的 MB功能，包括 数据包 检查 的 执行中的安全飞地。这意味着一个恶意的服务提供商应该不会 是 能 要 了解 任何 信息 从 或 修改 该 执行的的 飞地。

在 术语 的 系统 模型，许多 的 的 方案 满足 了 客户端-定向 和 面向服务器的 设置 （CO 和 S-O）作为 所讨论的 第 2，这些 方案 可以 被 直接 地 部署 在 任一 客户端 的企业 网络，或者 在 该 服务器 （例如 网络 应用 程序提供商）。方案 基础 上 的 搜索 加密 （SE） tech- NIQUE例如 如 BlindBox [53] （CF第二行的表1），但是，还假设了存在的一个（半）诚实 规则 发生器在于 提供 规则集 到 MB。有 是 还 计划 是 迎合 了客户端-服务器的问责制 （CF排3），在这两个 端点有 知名度 的 的 MB的 部署，并 都 能够 对 这些认证的MB。上的其它一方面，EndBox [29]和SplitBox [7]焦点上面向客户端的模型，与 EndBox 提供 更强的 安全保证，其中 客户机 可以 是 恶意的。在 总结，有 有 2间主的信任 假设 认为 通过 的 现有 方案：

- **信托 假设 （TA） I：** 中间盒 （或 MB 提供商） 是 （半）诚实 和 一个 中 的 端点 （即 客户端 或 服务器）必须是诚实的。方案基于对这一假设在一般部署 MITM， SE，交流， ML技术。
- **信托 假设 （TA） II：** 云 服务 提供商 以及 之一的端点 （即客户端 或 服务器） 可以 是 恶意的。AL- ternatively， 两个 端点 可以 是 恶意的，但 在 MB提供商 是 诚实的。方案 基于 对 这一 假设 在一般 部署 TH 技术。

在讨论的方案包括只假设这涉及到了知觉的使用情况和场景。当然，也有明显的信任的组合 即 是 不是 可行的， 对于 例如：

- 在该 情况下，由此 所述 客户机和 所述 服务器 是 诚实然后 的MB 将 是 多余的。 该 客户端 与 该 服务器进行通信 直接 通过 加密的 流量。他们的主要安全需求将是，以防止外人从监听 或 修改 他们的 通信。
- 这 是 显而易见 的是，如果 所有 3个 实体 是 恶意 再 有 是 什么，以 保护 从。

新的 信任 假设 可能 被 要求 由于 对 新的 需求和 场景 即 是 没有 解决 由 现有的 研究。在这里，我们 给出 一个 例子， 在 该 可能性 的 接应 之间 的服务 提供商 托管 的 宏块 和 一个 中 的 终点，当我们 考虑 的 外包 MB 的场景。

共谋。 注意 的是，如果 MB 是 恶意的 （或 半诚实）， 并且无论 是 在 客户机 或 所述 服务器 为 恶意 （或 半诚实）， 所述网络 通信 量 被 暴露 到 的 MB 和 数据 可以 被 修改 或者查看 是否 在*2个 实体 串通*。这 是 该 情况，因为 无论是 客户端 还是 在 服务器 可以 共享 的 会话 密钥 用 的 MB。如果 存在 有 许多 MBS，以及 一 些 的 他们 是 恶意的 和 其他人 是 诚实的 ，那么我们可以把这个作为的情况下的诚信客户，诚实服务器 和 恶意 MB， 通过 假设 的 诚实 的MB 控股 的角色 的 客户端 或 服务器。在 第一 一眼，这 可能 不是 似乎 要 成为现实，因为它并没有 使 商业意义的一个 服务 提供商 要 以 学习 信息 从 该 用户 的 串通 与 在 其他 端点。然而，它可以是一个无良员工 的 的 服务 提供商 是 勾结，或 在 服务 提供商和 一个 中 的 端点 被 定向 到 提取 信息 下 一个政府 的监控 程序。

3.2 安全 要求

在主要目标的方案主张隐私保护检查 的加密 流量 是 要 保护 数据 隐私 的 的 加密的网络流量，同时保持类似的工具的检查，在普通的数据流量。在主要的安全要求是这样，以确保*数据 的隐私*， 在 这样 一个 方式 是 只有 在 端点 知道 的基本信息的 的 加密流量，而 在 实体 执行 的 检查 也 没有 学到 任何 信息， *这 是 不允许的，以学习*。 根据 有关 方案， 该 信息 是 了解 通过 该 检测 实体 可以 有所 不同。对于 例如，在 一个人为 在的中间人 （MITM） 的做法是解密 的网络流量是 能够 以 学习 所有 的 信息，如果 它 选择 到。

4 技术

我们调查了现有的用于加密网络流量的隐私保护检查的最新技术，这些技术已在上一节中进行了简要说明。

我们首先定义了2种的检查中使用的这些技术。

- *被动检查。* 一个 方案 提供 了 被动的 检查，如果 它
  (1) 不 不 修改 的 底层 协议 （即 SSL / TLS） 和
  (2) 不 未 解密 的 加密的 流量 在 顺序 来 执行 检查。
- *主动 检查。* 甲 方案 提供 活性 检查 如果 在底层协议 被 修改，和 /或解密 被 需要 在整个 或 部分 的 所述 加密的 通信。 它 可以 进一步 被 划分成两个 子类别：
  - *部分 检查。* 甲 方案 提供 活性 检验，但只 在 一个 受限制的 方式。对于 例如， 一个 几个 方案 基于 搜索的 加密 技术 使 仅 精确 匹配- ING，和 不 正规 表达式 类型 的 分析。
  - *全面 检查。* 甲 方案 提供 了 充分 的 活性 检查。这意味着 该 方案 使 所有 的功能 如 在 检查上 纯 数据。

4.1 中间人

的*人在这方面的中间人* （MITM） 技术 被 普遍 部署 在 enterpise 解决方案 用于 加密 的 流量 分析，对于 例如 作为 呈现 在[10， 18， 22， 58]。有 是 还 广泛 可用的 开源 工具，例如 如 MitMProxy [16]和 SSLSplit [49]。MitM的用途*主动检查*。的主要思路是，以使该中间件提供商，以 行动 为 在 服务器 端点 这样 认为 它 可以 解密， 检查 和 再重新加密的网络流量的的客户端。该业务被随后转发至该服务器端点。在 一般情况下，对于 一个 面向客户的 模式 （无花果URE 1）， 这 是 实现 由 第一 安装 一个 证书 的 所述 MB提供商 在 所述 客户端 设备 （例如， 受信任的 CA 存储 用于 浏览器）。 当 一个 客户端 发起 一个 安全的 会话 与 该 服务器 的 MB提供商 托管 的 宏块 截获 的 流量 和 伪造 一个 certifi- 美食 使用 该 服务器 证书。在 这种 方式 的 服务 提供者伪装为的服务器，设置一个会话使用的客户端，解密

表1：现有方案和解决方案的信任假设

方案	科技（第4节）	客户	兆字节	CSP	服务器	模型	备注
商业解决方案和具体技术[19]	米特	高/中	H	不适用	M / H	一氧化碳所以	通过白名单策略引擎保护隐私（例如，在线银行流量未解密）。
BlindBox [53]，SPABox [26]，BlindIDS [12]，踏上[37]，Yuan 等。[61]，SplitBox [7] PrivDPI [44]，松木[43]	东南	高/中	小号	不适用	M / H	一氧化碳所以	介绍（半）诚实 规则 生成器*。没有用于SplitBox的 规则 生成器，但是需要 多个云 提供程序。
mcTLS [42]，mbTLS [41]，maTLS [38] MSP [24]， Bhargavan等。[8]	交流电	高/中	-	不适用	M / H	CS	两个端点均可见的MB。
安德森等。[4-6] 山田等。[60]	ML	高/中	小号	不适用	M / H	一氧化碳所以	分析加密流量的元数据。
尾盒[29]	TH	中号	H	H	-	一氧化碳	在客户端上将安全区域作为MB部署。
SafeBricks [46]+，ShieldBox [56]+ SGX-Box [31]， LightBox [21]	TH	H 中号	中号 中号	中号 中号	中号 H	一氧化碳所以	服务提供商托管的MB可能是恶意的。MB中的安全区域检查代替。

H：诚实；S：半诚实；男：恶意；-：要么 H，小号 或 M. CO：面向客户; SO：面向服务器；CS：客户服务器 负责；MB：中间盒；CSP：云 服务提供商。
对于技术，MitM：中间人，SE：可搜索 加密，AC：访问控制，ML：机器 学习，TH：可信 硬件。每个技术 的 讨论 在细节在第 4。
*：Lan 等。（SafeBrick）提供 3个 不同的 规则 设置：（1）无论 客户端 和 MB 知道 的 规则；（2）只有 客户 应该 知道 的 规则。在 这种 情况下，客户端 加密 的规则集，并通过 他们 来 的MB；（3）只 MB应该 知道 的 规则。在这种 情况下，可信任 规则 生成器 是 必需的，以 生成 签名 上 的 规则，所以 说 的 MB 不能 简单地 生成 规则 来 匹配 任意 数据 从 该 加密的 流量。
+：外包MB服务的解决方案。云提供商可能是恶意的，但网络流量受到以MB实施的安全区域的保护。

并检查该数据。经过检查，该服务提供商ini- tiates上代表的的客户 一个 安全的 会话 与该 服务器。在一个企业网，安装的所述根证书上的每个客户端 设备 可以 被 执行 通过 所述 网络 管理员。 所述 检查可以被执行以MB的托管当地在该前提下 的企业 网络或者 通过外包MB服务。

在该面向服务器的 模型（图2），类似的方法可以被部署。然而，如果 该 服务器 订阅 到 一个 内容 deliv- ERY 网络（CDN），所述 常规 方法是，以通过 所述 服务器证书，一起与所述秘密密钥对所述CDN提供商[8]。在更近的方法，该秘密密钥是不给，而是一个程序接口 被 提供 给 该 CDN 提供商，以 具有 访问 到 的关键。这里有各种关键共享和内容授权办法 的 讨论 中[19]。Durumeric 等。[22]列出了一些商业解决方案 并 进行了探索 对 安全 问题 的 这些 解决方案。他们发现那几乎所有的解决方案，他们调查已经减少了连接的安全性和5的该解决方案包含严重vul- nerabilities。该 技术 可以 被 耦合 与 一个 策略 引擎，在其中 一 白名单 的 网站 可 被 创建 由 一个 管理员，以便 该这些 网站将不被检查 由所述的MB [54]。该服务 作为 一种 方法 来 减轻 隐私 的担忧，尤其是 对金融 交易，例如 如 网上 银行 和 购买。Nev- ertheless，该 管理员 具有 对 被 充分 信任 来 配置 的 策略 引擎 正确 而 诚实地。图4示出了MITM 设置 为 面向客户的 MB 模型 和 所述 面向服务器的 MB模型（对于 所述 的使用 例 涉及 内容 递送 网络）。在这里，我们使用的外包MB架构，因为它可以被用来为所有3种 系统的 机型 是 我们 已经 提出。此外，它是在新兴的 方向 在这两个 行业 和 研究。

在该以下我们讨论的主要优势和局限性的中间人的做法。

优点：

- *变化 给 TLS：* 该 技术 可以 被 部署straightfor- wardly没有改变的底层协议（例如，因为TLS）的服务提供商坐落在的中央和管理SE- 治疗 会话 之间 的 客户服务 提供商 和 服务提供商的服务器。

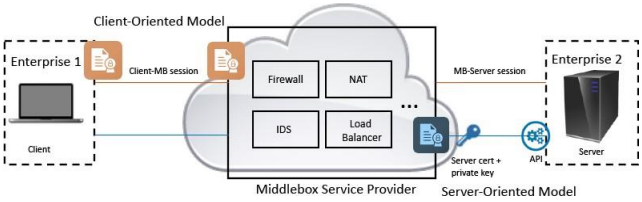

图4：MITM技术：（1）客户端面向：中间件服务提供商安装根证书上的客户端设备，以使中间盒以检查所述加密的流量；（2）服务器-定向在内容递送网络上下文：服务器共享证书和私有密钥与所述服务提供者，或提供一个程序接口为所述服务提供者访问的私人密钥。

- *功能：* 该 MB 解密 的 加密 流量。这个装置后的数据被解密，它是能够对运行类似功能 作为 在 该 情况下，其中 所述 流量 是 不 加密的。因此它保持 充分 的功能 为，如果该流量是不 加密的。
- *性能：* 它是相对高效相比于对其他需要额外的加密计算，技术，机器 学习 操作 或 计算 中 的 受信任的硬件。由于大多数 现代 的 CPU 支持 AES-NI 的指令，所述时间到加密 或 解密 一个 块 的 比特 采取3 μ小号每分组的1500 个字节。据 到[53]，所述 香草 TLS 设置阶段 花费 73ms 上一个 20 Mbps的吞吐量的网络。当然，这会带来更高的开销相比，以检验 对 普通 数据，因为该MB是必需的，以解密 和 重新加密 的 流量。对于 商业 解决方案，在中间件的等待时间即可是少比40 μ S，并根据上的装置变型中，TLS检查吞吐量达到250Mbps-10Gbps的范围。这些都是基于上

公开 可用的 信息，从 该 企业 是我们 调查的[9， 28]。

- 局限性：
  - *安全性：* 在 主要 问题 在 MITM 是 说 的 MB 提供 学习 的 内 容 中 的 交通 和 这 可能 引起 隐私问题，对于例如，对于一个 企业是订阅到一个 外包 MB 服务。另一个 问题 是 在于 我们 必须 信任 的MB 提供商 来 实现 的 底层 协议 正确地和 使用 的 最多的最 新 版本 的 所述 协议。作为 讨论在第1和第1.1，弱点被发现在 一些 的 解决方案，由于 要 执行 的 对TLS 使用协议的旧版本或 过时 的密码。在 另外 到 这个的 网关（或 该 服务 提供商） 变得 非常 有价值的目标 进行 攻击，并 在 管理员 必须 要 充分 信任。

4.2 可搜索的 加密

甲 第二 技术 那 被 提出 是，以 检测 恶意 流量经由令牌匹配，而不解 密 该 底层 加密流量。我们分类的技术，如 *可搜索 加密*（SE），因为 在 主要的 想法 是 对使用 搜索的 加密 方案 来映射之间的 加密 关 键字和该加密规则集。SE使用*主动检查*。**雪利酒 等。[53]**引入了 **BlindBox**，这是第一个使用SE 技术 的保护隐私的深层数据包检查 方案。在BlindBox，一个客户端发起一个TLS会话使用的服务器，作为 以及 作为 另一个 连接 的 令牌 匹配。双方 的连接 路线 通过 该 MB。在 一般的 想法 是 认为 该MB主机 规则集 是 被 加密 使用 一个 密钥 导 出从 会话 密钥 的 的TLS 会话。该 客户端 然后 标记化 和 烯隐窝 其 消 息 使用 的 相同的密钥，并发送所述标记化 的流量 通过 所述 第二 连接。该 MB 然后 尝试 以 匹配的 切分 流量 用 的 加密 规则集。如果 有 是 一个 比赛，在 交通 被 认为是 恶意的 和 阻断。图 5 示出了 一个一般 设置 为 基于SE- 方案。

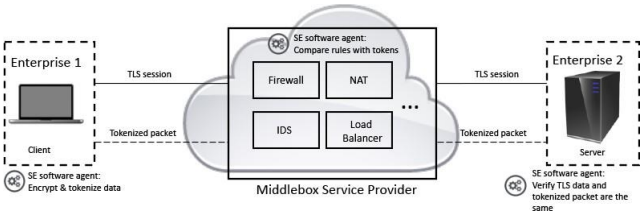

图 5： SE 技术： 所有 型号 都有 了 相同的 设置。的主要特点 是 其 存在 是2个 数据 流， 一个所述 TLS 会话 和 另一个 所述 记 号化 的数据。 MB 检查的 切分 数据而已，并转发该TLS会话到 服务器。服务器能够验证两个数据流是否相同，因为它 具有 的 会话 密钥 用于 对 加密 的 TLS 流量和切分 数据。

该 MB 应该 不 知道 该 键 使用，以 加密 的 规则集，并以生成的令 牌，因为如果这是的情况下，它是能够以解密所有令牌中的标记化 交通和学习的消息。这是类似于 到 具有 访问 到 的 明文。BlindBox 可 缓解 这个问题

通过 执行 加密 的 所述 规则集 通过 乱码 电路 和 不经意 传输 为 每个 会 话。此 装置 BlindBox 是计算上 昂贵，在 至少 在 所述 初始 握手 的 所 述TLS协议。此外，该方案必须是能够以验证是在 切分 流量 是 相同 的，以 该 TLS 会话。这 是 因为 客户端 可以 发送 恶意 消息 通过 的 标记 化 交通和 一个 良性的 一个 通过 的 TLS 会话， 从而 击败 了 IN- spection。在这里，核查 是 执行 由 该 服务器。所述 服务器接收到的 数据从两个连接，并且自所述服务器具有会话密钥，它可以解密的 TLS流量作为以及作为生成的 令牌，以 验证 该 的 内容 从 两个 连接 都 在 相同的。然而，检查基础上令牌匹配的的加密流量是相当有限的因 为它会不会是能够以迎合对常规 表情 检查。BlindBox 提出了 一个 可 能的原因 保密机制 来 缓解 这个 问题 通过 允许 解密 的 底层通信基础 上的会话密钥（没有透露该会话 密钥）。

所述 BlindBox 机构 被延伸到 所述 设置 的 外包MB 由 **兰 *等人。* [37]**。该 计划 被 称为 **Embark**。它 增强了令牌匹配技术，以包括前缀匹 配， 因为 还有不同的搜索加密功能迎合 specif- ically不同的MB的服 务，如IP防火墙，NAT，HTTP代理服务器，数据 渗透 和 入侵 检测。这 也 提出了 一个不同的，但 实际的 设置。在 为了 以 减轻 所述 运算 BlindBox，架空**鸭 *等。* [12]**提出了**BlindIDS**。它使用一个不同的方法 在该基于配对的公共密钥操作 是部署的令牌匹配，并针对该客户端， 以沟通 的 服务器 通过 的 MB。这 也 意味着 现有的 TLS亲母生育酚必 须进行更换与自己的方案。另一种方案是使用公共密钥操作是一个 方案，称为 **SPABox**通过**风扇 *等。* [26]**。在此相反，以BlindIDS，在 公共键操作基于同态加密 被 用于 只 向 执行 机学到，荷兰国际集团 基 于 检查。该 方案 还 使用 的Diffie-Hellman 基于不经意 伪随机 函数 用 于 加密 规则 的准备， 这 是 执行 交互 之间 的 MB 和 所述 服务器。对 于 正则 表达式 匹配， 该 方案 部署 一个 变体 乱码的 电路 那 是 更 有效 的 比 对 一般 建设。**Yuan *等。* [61]**提出了一种方案，该方案是比更有 效BlindBox 使用 一个 高性能的 加密 滤波器。 他们的 方案还 扩展 了 BlindBox的令牌匹配机制，以适用于多条件规则集。虽然高效，他们的 方案需要的 服务器，以 第一 注册 用 的 管理 服务 的 企业 托管 的客户 端。只有 那么 该客户端 可能会 发起 的TLS 会话 使用 的 服务器。 的 性能 的 BlindBox 被 的IM由显著证明**宁 *等。* [44]**在他们的方案中称为 **PrivDPI**。 的 计算 时间 期间 的 初始 握手被 大大 减少 时 相比 于 BlindBox，和一个可重用的混淆 机制 生成 中间 值，这些中间值 可在 后续会话中重复 使用以用于重复的令牌，这可以进一步加快令牌加密的 速度。的效率的PrivDPI是fur- 疗法 改善 在 一个 方案 叫 **松**，这 是 还 提出了 通过**宁 *等人。* [43]**。 在 此外，当中间 盒 服务 迁移 到 第三方 云 设置时，Pine启用了规则隐藏功能，因此规则隐私可能是 一个 问 题。 **任 *等人。*** 提出了 **EV-DPI [47]**。 EV-DPI 是 一个 双层次的架构 设计 和 被 部署 在 2 非勾结的服务器，以外包 的 中间设备。第一层 使用 编码的布隆过滤器过滤掉合法数据包。所述第二层支撑

确切规则匹配用于分组检查使用连接词搜索-能够 加密 方案 提出 通过 赖 *等人*。[36]。 该 方案允许 检查 结果 来 进行 有效 验证 使用 杜鹃哈希。 一个 相关的方案 是使用一个不同的方法下的云设置为 那非那韦 是SplitBox建议由Asghar *等人*撰写。[7]。他们建议在 使用的2个云系统，其中每一个规则的规则集 是XOR与一个 随机 字符串 ，并 分割 成 许多 块的 各个 宏块 居住 在一个 的 的 云 系统。 这两种 云系统 协同 计算 的 块 中 顺序 对 交通进行 检查。

优点：

- – *变化 到TLS：* 所述的主要 优点 的 这种 技术 是 该修改上 的 底层 协议 （即SSL / TLS） 是 不要求 （除了 用于BlindIDS其中提出 了一个 新的 协议，它 可以 替换 SSL / TLS）， 但 它 允许 隐私 保护检查。 一些 的 的 结构 可以 也 可以 有效地 在特定的场景。作 为一个 例子，假设一个 可信 规则 gen-爱适易 （这 是 该 情况下 为 一 小 的 的 方案 表示 在表1），加密的 所述 规则集 可以 被执 行有效如果 它 可以 被 假定 认为 所述 规则集 被 加密 由 所述 客户机 或另一个 值得信赖的 第三方 党 和 传递 来 的 MB。 Inspec-蒸发 散需要 只比较的规则集 用的 标记化数据， 并且 也 没有 需要 解 密 和 重新加密 为 在该MITM 方法。
  - – *安全性：* 它 提供了 更好的 安全 保障 比 的MITM 技术 和 对 访问 控制 技术 （第4.3） ，因为 检查 是 执行 不 解密 的 加密流量。 因 此， 在 MB 和 的 服务 提供商 将 不会 是能够 以 学习 的 内容 中 的 交通， 除外 对于 那些 记号是 相匹配 的 规则。 一个 例外 是 说 有 有计划，例如为BlindBox，PrivDPI和EV-DPI其中如下可能的 原因 隐私 其中 的 中间件 获取 到 看到 了 解密的流量，如果和仅 如果该流被视为到是可疑的。
- 局限性：
  - – *功能性：* 主要缺点是，实用程序可以是lim- 资讯科技教育 由于 以 简单 映射 的 加密 令牌 和 规则。这可能不是足够特别用于 检查需要正则表达式。一些方案解决这个prob- LEM通过允许的 MB来 解密 的 交通 时， 有 是 一个匹配。 或者， 计算密集型 原语 例如 如 HO- momorphic加密 被用来以使表达的检查。此外， 在 5月 的情况下 一个 单独的 信道 被 要求 进行通信 的 标记化的 交 通， 如 所示 在图5 对于所述 MB到是能够 对 检查 入站 和 出站 通 信， 既端点， 这意味着 在 客户端 和 该 服务器 必须 具备 的计划 安装。 这 是 在 对比 来 的 MITM 技术 （以及 为 在 机器 学习 和 值 得信赖的 硬件 的做法，这 我们 将 讨论 在 该 后续 章节）。
  - – *性能：* 在 该 客户端， 有 是 将 计算密集型过度 头 由于 到 的 附加 操作 的 标记化 和 烯crypting 的 数据 料流 相比 于 纯 TLS 连接， 并且 所述 MITM 技术。 在 该 MB，但是，只有在匹配执行。因 此，通常的设置相对于SE tech- niques 贡献 更多，以在整体 性 能 延迟 超过了 检查 阶段。 对于 BlindBox， 所述 设置 时间 是 97S为 3000分 的规则 和33 μ š用于检查1包用3000级的规则。 BlindIDS限制的设定时间到73ms ，但增加了inspec-重刑 时间 到 74S 为 相同的 设置。 通过 替换 乱码 带电路 可重复使用的 取幂 在基，PrivDPI准备3000条加密的规则在0.64s其是288倍更有 效的比BlindBox。 PrivDPI 还 减少 了 带宽 使用量 （从 GBs开始） 到KB） 由 替换 的乱码 表与可重复使用的obfus- cated 规则。 松 进一步 提高 了 一个全面 的连接与散列运算PrivDPI的时间。对 于SPABox， 缺乏硬件 支持 用于 操作 结果 在 较慢 （9 倍 比 BlindBox） 性能 用于 加密 一个 令牌 在 建立 阶段。然而， SPABox节省的平均29.5％时间在检查相比较，以BlindBox由 于到散列技术。

4.3 访问 控制

这 是 一个 技术 是 提倡 客户端 和 服务器 的问责，其中 的 客户端 ，并 在服务器都知道的所有的MB的部署中之间的2的他们。 此外， 他们被赋予的能力，以验证和分配访问权限给这些MB的。 因此， 术语 *访问控制* （AC） 。AC使用*主动检查*。图6示出了一个典型 的设置为基于AC-方案。

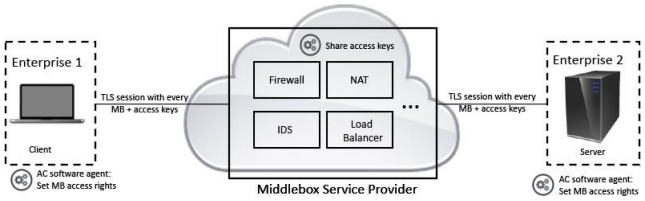

图 6：AC技术：所有型号都有了相同的设置。的主要特性是该MB的是可见的，以在端点和那的端点可以决定访问权限的的到的MB的加密流量。该访问权限的控制，我们-荷兰国际集团的读/写键

Naylor *等*。[42] 引入了 一个 方案 的 这种 类型， 称为 **mcTLS**。 它 会修改 现有的 TLS 协议 ，以 允许 在 客户端， 在MB的 和 的 服务 器 ，以 建立 安全 和 验证 通道， 交流 读取 和 写入 秘密 密钥 中 除了 到 的 会话密钥。 该 mcTLS 协议根据 最小特权MB访问策略对网络流量进 行 了 划分。每个MB被分配一个读取 和/或 一个 写密钥。这涉及到提 供不同级别的访问控制，以读和/或写上的加密通信。该加密的 流量 是 分区 这样 即 一些 部 的 所述 有效载荷 可以 被解密。 的好处 的 这样 一个技术是其存在是一个精细粒度控制和灵活性在维护 隐私上的 部分 的所述数据的是应不被解密。在其他词语， mcTLS仅部分地 保留 隐私 的 所述 底层的 有效载荷， 因为 一个 MB 具有的密钥来解密 所述部分的所述业务，其中授权被 给出。

的主要问题与mcTLS是说这是一个新的协议。对于adop-蒸发 散，现有TLS协议的是被广泛使用的必须的所有被取代与mcTLS。 **Naylor *等人***承认了这个问题。**[41]** 进一步提出了 另一种 方案， 称为 **mbTLS**。 它 也 不会 改变 的

底层TLS协议，除了在引入的扩展，可以被很容易地采用使用现有协议。它被设计成可伸缩的实施中的外包MB设置。在更多的细节，mbTLS考虑的问题的外包MB FUNC-蒸发散到多个第三方当事人。对于例如，有可能多MB的承包出去的一个客户端，在另外还有可以还存在一组的宏块进行的服务器，所有居住在不可信的云environ-换货。他们讨论了几个重要的特性所需的这样一个场景，并设计mbTLS，以满足一些的这种重要的特性。在mbTLS，一个不同的TLS会话存在之间每2个实体（客户机，MB，服务器），与每个会话的操作使用其自己的秘密密钥。这种设计是这样的是，该客户端是唯一知道的客户端的MB，并没有在该服务器端；和副反之亦然。该宏块中的云采用英特尔SGX来保护的数据和密钥，从该云基础架构提供商。所述初始控制消息之间的不同实体被复用在一个单TCP连接，从而增加无额外轮行程时间。在mbTLS， MB的是能够以查看的整个有效载荷，如在会议被交给了以参与实体。

Bhargavan *等*。[8]证实攻击上mcTLS，和亲构成一个正式的模型上进行分析的协议。在简单地说，一个的的攻击利用的事实是mcTLS并没有执行authentica-重刑，并在握手完成的消息对于在会议之间发起的客户端，并在MB，以及之间的MB和该服务器。由于到这一点，Bhargavan *等人*。进一步提出了一个协议，该地址会这些攻击下的安全模型是他们定义。它也不会要求任何修改到了TLS协议，在对比mcTLS。在响应到了攻击，在ETSI草案标准即是基于对mcTLS提出了一个修正到了mcTLS基础上mes-圣人验证码在他们的**MB安全协议（MSP）规范**[24]。在该时刻，它仍然要被看到怎样的行业将接受一个安全的，但MB友好新协议的加密交通，因为它可能意味着更换TLS与MSP。**Lee *等*。[38]**提出**maTLS**，一个中间盒感知协议来解决MITM陷阱。中间件是由可见光，从而该服务器可以被明确地验证，该加密参数使用可以被验证和是否消息被修改。每一个中间件是颁发一个证书由一个CA，并且该证书被记录在一个中间件透明度日志服务器。通过对日志服务器，一个中间设备证书是公开可验证的和可撤销的。然而，如在说明[19]，而在中间盒证书被审核通过的CA，客户（或最终用户）仍然需要来决定要接受这些证书。一个攻击者可以发起一个钓鱼攻击通过获得一个证书具有说服力的名字。

. 优点：
  - *安全性：* 在主提供的的交流技巧是在于它提供*的问责制*。这意味着该终端将是能够以验证的部署MBS，这是唯一以这种技术。
  - *性能：* 该技术并没有要求特殊crypto-图形元作为在SE和因此是更有效的。这是不太有效作为的MITM方法，但提供了更多的灵活性条款的保护隐私的的数据。它也没有需要安装的证书在该客户端，也不允许任何的所述宏块至解密和查看该充分有效载荷的所述流量。对于例如在mcTLS，所述性能期间握手亲母育酚取决于对数的上下文和中间盒。所需要的时间为在第一个字节，以达到该终点是400毫秒与10个上下文和560ms与14个上下文。
  - *功能：* 它提供了全面的功能为在该MITM技术。这是因为对于一个特定MB，例如作为一个IDS， 访问将被给出到解密的部分的所述加密的流量为所述IDS来执行的所需的检查。
. 局限性：
  - *变化给TLS：* 的主要缺陷的这种做法是它会要求所有各方，这意味着在2个端点和所有的宏块，以充分协同工作的顺序进行的方案来工作。这是因为在客户端，并在服务器必须知道该类型的MBS可以他们是与沟通。在客户端，在服务器和所有的宏块必须同意在该方案中，以被使用。它是还没有清除如何在客户端和所述服务器可以定义上下文（其部分的所述数据可被显示，以该MB），尤其是用于数据在不同的域和然后设置的访问策略对这些MB的。
  - *安全：* 联盟中的访问读取/写入密钥用于对其中的场景的MB被托管在该服务提供商将允许该服务提供商来解密最可能的所有部分中的加密流量。

4.4 机器学习

检查加密的通信基础上的机器学习（ML）tech- NIQUE代表一个理想的解决方案中的术语的安全性和applica- 重刑设置，因为它确实不要求任何修改，以在现有的设置。该想法是要分析的普通元数据和报头的协议，提取特征从所述加密的有效载荷，如以及分析遥测数据从所述网络流量。对于实施例，throgh观察行为特性（例如在圆形行程时间，数量的数据包发送），观察该加密的有效载荷，并观察附加信息，例如作为协议握手。它已经显示为是有效的特别用于使用情况下，例如作为业务聚类，应用类型和协议分类，异常检测和文件的识别[20]。在所有的技术，它的唯一的技术是使用*被动检查*。图7示出了一个高级别设置的所述ML技术。

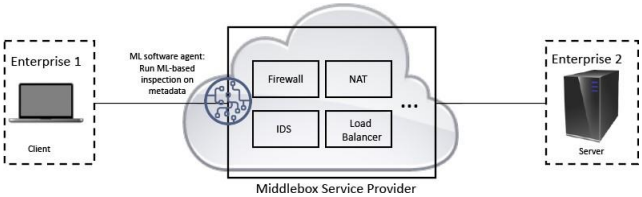

图7： ML技术： 所有型号都有了相同的设置。主要特性是无需更改即可在端点上进行工业部署。检查工作进行，而不需要到修改或解密的恩加密后的流量。

存在有许多建议使用ML技术用于使用例如用于应用类型和协议分类，异常detec-灰和文件标识。这些在[20]中进行了全面调查。另一个提案为异常检测是在提出的技术由**山田 *等人*。[60]**。其方案进行异常检测使用仅大小的数据和定时信息的加密的流量。更最近，**安德森 *等人*。[4-6]**提出的技术为恶意软件检测的是在另外的利用SE-quence的数据大小和定时，还采用了各种TLS报头信息和DNS数据。安德森 *等*。证明与企业网络流量相比，某些基于恶意软件的加密流量具有不同的特征。这些特性时结合与其他遥测数据，允许精确classifi-阳离子的的恶意软件的流量。他们都还表明该随机森林法优于其他方法的条款的分类恶意流量[5]。然而，通过仔细设计的的功能，在-结束性建议通过域名专家，线性回归使用更多的表现功能实际上优于随机森林方法。

有是还的技术是识别恶意软件的流量基础上的指纹。对于例如，**JA3 / JA3S**提出通过**Althouse *等*。[3]**生成的恶意软件指纹基于上的TLS的元数据（例如握手消息）。**安东[57]**提出了一个技术即创建规则由观察的分组字节流的创建指纹的流量。特定的恶意软件可以被检测到基于对所述独特数据包字节流发送从所述客户机向所述服务器。该技术是专门为与Suricata一起使用而创建的。无论上述建议可以被认为是基于签名的技术，并需要事先了解的该恶意软件。

- 优点：
  - *变化给TLS：* 将主要优势的的ML技术的COM缩减到所有的其他技术是那它确实不要求任何修改，以现有的加密流量的设置。没有modifica-重刑是需要在该客户或该服务器。该MB安装的ML模块等等那它是能够以分析的元数据的加密流量。
  - *安全性：* 由于没有变化的需要来的设置和对底层协议，它保留了安全保障的的原始设置。对于例如，使用ML技术保持端至端加密的一个TLS会话之间的客户端和服务器。这代表了另一个主要优势相比所有其他技术即需要改变到的协议（即，AC技术）或改变，以在客户端和服务器的设置（即MITM，SE，和可信硬件）。然而，我们此话是基于机器学习的分析和指纹识别技术可以也可以使用到学习信息关于一个用户。对于应试PLE，它是可能的一个攻击者向学习有关的一个网站，用户冲浪或找出来的文件，一个用户下载和共享，甚至尽管该业务被加密[20]。这是一个有趣的领域的研究是对如何普及ML技术可以也可以使用到学习有关一个实体，在相反于所述的技术被用来作为一个隐私保护方法用于分析加密的流量，而不知道该有效载荷。
- 局限性：
  - *功能：* 将主要关注的是是否该技术是足够全面，以涵盖大部分的的检测再执行安全功能的MB quirements。由于被指出在[20]，存在有固有限制到什么可以被分析基于对ML技术，和作为被讨论在[19]，还有的使用情况下这将需要检查上的有效载荷，不只是在标题和元数据。作为的现在，在最suc- cessfulML机制的安德森 *等人*。[4 - 6]仅迎合针对恶意软件的检测。所有的一切，该技术将需要以能够要迎合了不同类型的中间件服务。
  - *性能：* 它仍然要被看到怎样的性能的的技术，如相比于其他技术。培训必须执行之前的检测可以被进行了对实时数据。在及时的数据集和准确的的训练模式是区域要进行进一步的探讨。照原样讨论由安德森和麦格鲁[5]在他们的工作对恶意软件分类使用机器学习技术，它需要约200秒到训练和少比10秒至测试。这是对他们的最好进行随机森林算法上的增强功能。的定时是一个粗略的估计从图5在他们的工作中[5]。此外，解决方案基于对这种方法需要对连续供给的高逼真度标记的数据进行训练，这可能是很难获得。

4.5 可信硬件

可信硬件（TH）已也已部署了隐私保护的数据包检查。在新兴的做法是，以利用该安全飞地的的英特尔新交所信任的硬件。在一般的想法是对的客户端或在服务器到共享的会话密钥安全地与该飞地居住在该MB。所述解密，检查和再加密是执行中的飞地。该MB的和的服务提供商托管这些宏块是不能够来辨别或学习的数据和流程。的挑战是如何来实现中间件的功能有效和安全地以充分利用该能力的的信任硬件。我们可以归类此技术作为使用 *主动检查*，但该检查是隐藏从该视图的实体主机的可信的硬件。图8示出了一个高级别设置的所述TH技术。

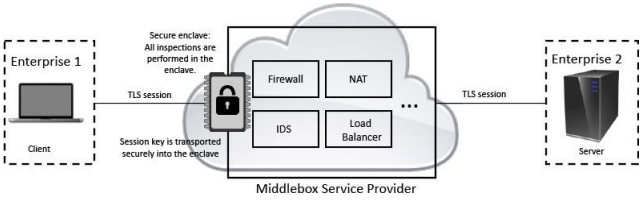

图8：TH技术：同样所有车型都有了相同的设置。任何改变都需要上的TLS协议。其主要特性是该解密的的流量是在执行的安全飞地。的主要要求是对安全运输的会话密钥到的飞地，要么通过客户端或服务器。

Han *等*。 [31] 提出了 一个 方案， **SGX盒**， 使用 这种 tech- NIQUE。在他们的方案中，该服务器共享的会话密钥与英特尔新交所的安全的飞地通过的出带外安全chan- NEL。他们 提出了 一个 高效的 执行 的 执行 的检查 中 的 安全 飞地。

它是也可能以推动所述MB功能到所述网络边缘（或到 所述 客户端的 装置）。这 是anologous 到 托管 的MB的 客户端， 除了 那个 检查 是 执行 中 的 安全 嵌入式飞地中的客户端设备。这是有利的，因为所有出站 流量被分析之前它被 发送从 所述客户端设备。入站流量 上 的 其他 手 被 证实 之前， 它 被 释放到 该 客户端 设备。 **EndBox**，由 **Goltzsche *等人*** 提出。**[29]**，提供了这样的解决方案。

有是也的作品是提出了全面的安全NET-工作功能虚拟化（NFV）系统使用TH technqiue。这些NFV系统提供检测的加密通信作为一个 的他们的 功能。 对于 例如， **SafeBricks** 提出 通过 **波达*等人*。** [46]。 SafeBricks提供MB作为一个云服务结构。它确保了云提供商只看到了加密的流量，其中， 所述 应用程序 报头 （通常 可见下TLS）是也加密 基于 上 的IPSec。 此外， 它 屏蔽 了 规则集 和 网络 功能 的代码 来自 的 云 提供商。 灯箱 进一步 完善了现有的基于TH-方案，包括 SafeBricks，在 术语 的 效率 和 性能。 对于 例如， 灯箱 addi-倚重 保护 隐私 的元数据 中的 业务，包括 数据包大小，计数 和 计时。两个相关的作品是 Trach *等人* 提出的ShieldBox 。[56] 和 Duan *等人* 提出的LightBox 。[21]。ShieldBox和灯箱提供安全中间件的功能通过 提供 的 NFV 系统 在 新交所。然而，这两个都面向朝着 高效 部署 的 宏块 的 不信任 云 提供商 和 将 需要 适应，以 专门 满足 对 加密流量 检查。

优点：

- – *变化 给 TLS：* 一个 优势 是 在于 它 确实 不 要求 改变，以在 底层 协议。但是，它必须是能够 对 运输 的 会话 密钥 来 对 信任 的 硬件 安全，无论是 通过 在 客户端 或者 在 服务器上。
  - – *功能性：* 另一个优点是它提供了MITM型全功能检查而不的缺点的的MITM AP- proach。 它 允许 一个 MB 到 检查 的 加密 流量 中的 一个屏蔽的 环境， 所以说 没有 解密的 数据包 被 泄露。 它 可能 代表 了 最 实用 的解决方案， 如果 硬件 去ployment，成本和安全的的信任硬件是不是一个 问题。
- 局限性：
  - – *安全性：* 在 当前 主要 关注的 是 该 安全 的 的信任 硬件 （即 英特尔 SGX） 是 仍然 是 积极 研究。由于 是 呈现 由 林德尔 [39]， 也 有 过 成功的侧面香奈儿 的攻击 对 英特尔 SGX。 它 仍然 要 被 看到 如何严重的这种 攻击是 在 实际 部署。
  - – *性能：* 它 是 较少 有效的 用于 检查， 在 至少 进行比较时， 以 SE方案如所讨论的在[37]。就拿SafeBricks的例子，它引入了16%的带宽开销时的COM缩减到踏上的21%的带宽开销。然而，SafeBricks也导致0-15%的吞吐量性能过头 在 该 中间件 由于 对 SGX 相比 于 可忽略不计 管理费用 的 踏上 和 BlindBox。然而，踏上（在栅极- 路） 和 BlindBox（在 客户端） 招致 高 等待时间 的 顺序 来进行加密的数据包在了终点，在那里SafeBricks并没有付出这样的代价。另一个 问题 是 对 可用性 的 的 硬件 和 成本。虽然 大多数 最近的 设备 会 有 一个 安全的飞地 嵌入 （即 英特尔 SGX），问题 仍然 对 那些 说是 没有， 特别是 遗留 系统。

4.6 比较

作为 一个 总结 的 东西，我们 已经 讨论了 这样远，表 2 提供了模型之间的比较，用例，特性 （如安全性，类型，型号，外包MB到云），在5个技巧和 表演。

4.6.1 安全性。 在 该 下面 我们 定义 3个 不同 级别的 安全性， 示于表 2 的 主要 目标 的 该 方案 是，以提供 数据 私密性 （如 表示 在 节 3.2）。在 其他 的话， 怎么多少 信息 被 泄露 给 了 对手， 这 可能 包括对 实体 托管 的 宏块。

- *完全显示（）。* 此装置的网络通信量或数据有效载荷是可见（或 解密 在 总计） 到 的 MB。 解决方案 基于 对 MITM 技术 都 在 此 范畴。
- *部分显示（，）。* 所述的这个装置只部分内容的网络 通信量 被发现 （或 局部 的解密 的 所述 有效载荷）到 所述 MB。 解决方案 基于 对 SE 和交流技术都在此 范畴。然而，存在是一个微妙差异之间的部分数据曝光之间的2层的技术。SE匹配加密规则与 所述 加密的 令牌 生成 从 所述 有效载荷， 并因此只有灵兽匹配结果。加密的有效载荷是不 匹配 任何 的 的 规则 保持 私有 从 该 视图 中 的 MB。 一个 例外 是 方案 是 揭示了 潜在的 数据 更多的 复杂的 检查 等 作为 常规 表达。在 另一方面， 方案 基于 对AC技术直接泄露的潜在 有效载荷 作为 长 作为 所述MB具有的 访问 权 到一些 部件的 所述 加密的 通信 数据。 通过 在 上述 的观察， 我们 可以说明的是SE技术的泄漏 更少的信息（ ）时比较，以AC技术（ ）。
- *隐藏（ ）。* 此 装置 的 网络 通信量 或 数据 有效载荷 被隐藏（或保持加密） 和所述MB具有无能见度到所述 底层的 内容。方案基础上ML和TH技术都在 此 范畴。注意 的是 这里 我们 假设 的 值得信赖的 硬件部署 在该方案被认为是安全的， 在那有是没有 信息 泄露，从 该 硬件 本身 在 执行该方案。这可以是一个强假设为存在是导通 去工作证明侧信道攻击，以这样的硬件实现 [39]。 它 仍然是 一个 研究 问题 作为 对 的影响 的 这样 的攻击 朝向 方案 使用TH技术。

4.6.2 实用程序。 在 术语 的 效用， 我们 定义 2级 宽 的类别，这 是 也 示出 和 描述 在 表 2中。

- *完整 功能（）。* 这 意味着 一个 方案 提供 检查实用工具 类似，以 该 的 检查 上 明文 流量。 MITM方法 都 在 此 范畴。
- *部分功能（，，）。* 这意味着方案仅提供部分 实用程序。 对于 例如， 解决方案基于对SE进行直接匹配和前缀匹配对预先定义的规则集。他们还需要特定的设置，例如 作为代号化的的消息

和一个单独的加密信道在除了到所述TLS通信。 因此 功能 用于 SE 技术 的 限制 时 相比 于其它技术 （ ）。基于ML- 解决方案 还具有 有限的监督 能力，为在前面讨论4.4，但他们并 没有 要求 任何 修改，以对 现有 设置并且可以被 部署直接 （ ）。解决方案 基于 对AC和TH在理论上可以实现全检公用事业如在中间人的做法。在AC背景和政策可以被设置到授权一个中间件，以具有完全控制上的流量（即解密，然后读取和写入上的消息），并在TH的原则可以解密和执行所有 类型 的 检查 下 的 安全 飞地。然而，在实际方面，所述主目标的所述AC技术是向限制 访问 到 的 加密的 净荷 依赖 于 所述 的要求一个 中间件。通过 做 这样 的 客户端 和 所述 服务器 可 控制 的 部分 的 所述 数据 即 是 允许 到 被 读取 或 修改由一个 中间盒。在 对比 来 的MITM 方法，该设置 是这样 的是 没有 一个 中间设备 是能够以解密的 完整信息，除了 用于 该 收件人。它会 还要求 新 设置 和配置 的 访问 方面 的 的 客户端 和 该 服务器。对于TH，在 安全的 飞地 提供了 有限的 存储/内存 和计算 能力。这 会 不会 是 实用的，以 执行 所有类型 的 检查 下 的 安全 飞地，在 至少 不 用于 在当前 TH 技术。因此，我们 表示 双方 的交流和TH技术作为实现部分但更好的功能（），因为 相比 于 在 SE 和 基于ML- 解决方案。

5 讨论

对于 所有 的 新 方案 是 已经 被 提出 来 至今，一个 ques-重刑 是 一个 可以问是 为什么 是 那多数 的 该 行业 仍然 喜欢和 部署 基于MITM- 解决方案。反之，如果 一个 基于MITM，所谓lution 被 设计 在 一个 谨慎 的方式，那 就是 用了最新的TLS配置和 政策 引擎，是 它 不是 足够 安全？在对其他方面，方案 基于 上 的 4项 技术 是 和 正在 不断地被提出来解决该问题与该中间人的做法，我。e。违反 的 端-端 加密，隐私 担忧 和 困难 或 缺陷 中 的 配置 和 设置。的 主要目标 是 主要 以 维持 端至端 安全 提供 由 所述底层 协议 例如 为 TLS，和 减少 的 信息 重新vealed 到 的 MB。其中 的 的 原因 是，以 减少 的 信任 放在 了 MB 提供商 所 以 这 一个 不会 不 依赖 于 该 供应商 以*设计 和 实施 加密 流量 检查 在 一个 仔细的 人为 NER*，这是总是不能够作为证实通过Jarmoc [34]，卡纳瓦莱和甘露[18]，和Durumeric *等人*。[22]。*所有的一切的 目的是 要取代的基于MITM，解决方案与任意的在其他4 技术 （或 组合 的 他们） 为 更好的 隐私 保护，同时保持在相似的效用和practicalility 部署。*

我们讨论的挑战中的技术讨论和伊赛格武功的研究方向。我们的讨论是基于对共同 的属性中的网络安全性的景观，那就是安全性，perfor-曼斯和效用。

5.1 安全性

信息 泄漏。 的主要挑战的方面的安全性 是泄漏的信息中的技术是我们已经讨论了。在 方案 基于 上 SE，令牌 匹配 可能 仍 泄漏 信息，如果 所述 客户机 或 所述 服务 提供商 （在 该 情况下 即 在 提供者 应该不知道的规则集）有背景信息的的基本规则集。这是一个合理的假设，因为那里是公开可用的规则集，例如作为该规则集提供的哼了一声。这种 关注 是 讨论 通过 波达 *等人*。[46]。此外，那里是这样的上搜索加密方案行之有效的攻击作为 推理 攻击 [32]，泄漏滥用 攻击 [14]，重建攻击 [35] 和 被动 攻击 [45]。同样的，进一步 的研究 是 需要 的 方案 是 使用 受信任的 硬件，由于 到了 最近的 攻击 基础上 侧 信息上的安全飞地，例如如在 攻击 讨论 中 [11]。

外包MB方案中的潜在 合谋。 在 条款中 的 外包 MB 模式，一个 的 的 挑战，这 也 没有 检查是对可能性的接应之间一个恶意的客户端或服务器，并在云服务提供商。该恶意客户端或服务器可以串通用的服务提供商通过提供所述会话密钥中以便为所述提供商来解密所述底层traf- FIC，从而绕过所述执行的所述方案，是它通过溶液基于上SE，AC， ML或TH。一个新的安全模型可以被要求到模拟这种情景和在那么问题将是这是否是一个实际的假设。对于例如，在对其中的场景的企业外包其内容管理到一个内容分发网络（CDN）提供商，该企业股票的证书私有密钥，或委托内容到的CDN提供商。假设说的CDN供应商使用其自己的云基础架构，也就是没有接应在这种情况下。在此相反，如果一个企业的外包网络威胁检测到一个托管服务提供商，其中的供应商使用一个第三方云提供商来托管其各种MB服务，然后在可能的勾结可能需要到被考虑到考虑。

挑战为ML技术。 ML技术使analy-SIS而不需要对变化和解密的现有加密网络设置（例如TLS）。这提供了最佳的解决方案，因为它可以被动地检查流量。然而，在一个挑战是是否该技术是足够全面以封面大多数的的检测要求的宏块进行安全功能。作为的现在，在最成功的ML机制的安德森*等人*。[4 – 6]仅迎合针对恶意软件的检测。此外，培训必须被执行之前的检测可以被进行了对实时数据。的及时的数据集和准确的的训练模式是区域要进行进一步的探讨。

5.2 性能

基于SE的方案可以保护隐私，但会产生巨大的开销。 方案 基于 对 SE 技术 要求 2个 的通信信道（例如 一个 用于 在 TLS 连接 和 一个 用于 所述 加密的令牌），该 生成 的 令牌 和 加密 的 规则集 （参见第 4.2节）。这意味着 基于SE的 方案 会产生 额外的 开销，在至少比到了中间人的做法。然而，它代表了一个有前途的技术，以私下巡视加密的有效载荷与-出需要任何专门的硬件作为在该基于TH- 解决方案。它也没有不露出部分的底层数据，作为在所述的情况下，基于AC- 溶液，除外当正则表达式类型匹配的是必需的。该挑战是然后以提高该effi- ciency上的当前计划尤其是在条款的规则集和加密，并匹配。一个问题是需要对被处理

表2： 加密流量检查的隐私保护技术：类型，技术和应用

方案	chg。TLS	种类		技术				Cl。	L.	实用程序	小学	组态			
		霸	法案。	交流电	东南	ML	TH					最初设定	前处理	加密/解密	匹配/检查
MitM方法	×		•						⊗ ◓	◆	证书 +政策	客户端安装根证书 服务器共享私钥	客户端/服务器共享会话密钥 服务器委托内容	MB解密 讯息	MB检查解密 有效载荷
mbTLS [42]	×		•	•			•	•	◓ *	◐	象征	客户端和服务器 同意MB清单	委托MB' 读/写键	MBs部分解密 通过读/写访问	MB检查解密 有效载荷
mcTLS [41]	✓		•	•					◓ *	◐	象征	与mbTLS @相同	--	--	--
MSP [24]	✓		•	•					◓ *	◐	象征	与mcTLS +	--	--	--
Bhargavan等。[8]	×		•	•					*	◐	象征	与mcTLS # 相同	--	--	--
maTLS [38]	×		•	•					⊗	◆	象征	MB从CA获得证书 （证书可公开验证）	MB共享密码套件 与客户一起设置	MB解密 讯息	MB检查解密 有效载荷
盲盒[53]	×		•		•				◐	◔	象征 + SMC	规则生成器准备和 标志规则	客户端标记邮件客户端和 MB共同加密 规则	客户端加密令牌	完全符合： 加密令牌与规则
登船[37]	×		•		•			•	◐	◔	象征	企业网关对规则进行加 密，传递 加密规则到MB	网关标记来自客户端的消息	网关加密令牌	完全匹配和前缀匹配： 加密令牌与规则
Yuan等。[61]	×		•		•			•	◐	◔	象征 + SC	服务器从客户端admin的 管理员那里获取密钥 加密规则，传递给MB	服务器/客户端标记 讯息	服务器/客户端加密 代币	准确及多-规则 匹配：加密令牌 与规则
BlindIDS [12]	✓ $		•		•				◐	◔	配对	服务器生成 密钥对 规则生成器/编辑器生成器。加密的 规则，将它们传递给MB	客户端标记消息	客户端使用服务器公钥加 密令牌	完全符合： 加密令牌与规则
SPA盒子 [26] a	×		•		•				◐	◔	DLP + HE	规则生成器准备规则	客户端标记消息，客户端与服 务器协商 DLP / HE参数	客户端加密令牌	完全匹配，正则表达式， ML：已加密 代币与规则/模型
PrivDPI [44] a	×		•		•				◐	◔	象征 + DLP	规则生成器准备和 标志规则	客户端共同标记客户端/ MB /服务 器的消息 gen。可重用的加密规则	客户端加密令牌	完全符合： 加密令牌与规则
松树[43] a	×		•		•				◐	◔	象征 + DLP	企业网关与规则生成器，规则共享 密钥 发电机准备并签署规则	网关共同标记来自客户端，网关/ MB的消息 gen。可重用的加密规则	客户端加密令牌	完全符合： 加密令牌与规则
EV-DPI [47]	×		•		•			•	◐	◔	象征 +高炉 + CH	企业网关加密规则，通过加密 MB的规则	网关标记来自客户端的消息	网关加密令牌	过滤条件和完全匹配： 加密令牌与规则
山田等。[60]	×	•				•			◆	◒	统计 分析	功能：数据大小，时间，HTTP 交通，访问频率	特征向量提取	Ñ /一	异常检测的IDS： 频率分析
安德森等。[4-6]	×	•				•			◆	◒	ML 分类器	功能：流元数据， TLS握手消息。等等	特征向量提取	Ñ /一	恶意软件流量 分类
SGX盒[31]	×		•				•	•	◆	◐	新交所	配置SGX，证明模块， 并更新服务器应用。	服务器安全共享 飞地的会话密钥	飞地解密 讯息	飞地检查 解密的有效载荷
尾盒[29]	×		•				•	边缘	◆	◐	新交所	配置SGX，证明模块，安全区安装 CA证书， 飞地 密钥对	客户端应用。安全股与飞地会 话密钥在 客户端（例如边缘设备）	客户端的飞地解密消息	客户飞地检查有效载荷
安全砖[46]	×		•				•	•	◆	◐	新交所	配置SGX，证明模块，嵌入网络功 能 在飞地	企业网关解密来自客户端，隧道的 TLS流量 通过IPSec迁移到云端	飞地云解密消息	云中的飞地检查有效载荷

“ chg。TLS“：要求改变以TLS，小学：原语，例如加密元或元数据，CL：云L：信息泄露的Util：实用，霸：被动，法：主动，AC：访问控制，SE：检索加密，ML：机器学习，TH：可信 硬件，符号：用于加密解密（即AES）的 对称 基元，SMC：安全 多方 计算，SC：秘密 共享，DLP：离散 日志/问题，HE：同态 加密，SGX：英特尔 实施 的 安全的 飞地，BF：布隆 过滤器，CH：杜鹃 哈希。

a：SpaBox，PrivDPI和松焦点上改善的性能的BlindBox与添加属性。SpaBox可实现更具表现力的匹配。PrivDPI推出可重复使用的模糊规则，所以是模糊的规则可以被重复使用在许多会议，因为相比于BlindBox这需要重新加密的规则 对于每个会话。松介绍 规则，躲在这样说的MB就没有学习的 规则，以及动态的另外的 规则。

$：BlindIDS提出了一种基于配对的新协议，该协议可以部署为SSL / TLS的替代协议

*：部分基础加密流量会根据访问权限进行解密。这意味着MB可以看到部分明文。

@：类似的 配置 与 mbTLS 但 该 协议 构造 是 一个 修改的 版本 的 所述 TLS 协议。在 此相反， mbTLS 只 需要 在 使用 的 TLS 扩展， 并 因此 也 不会 影响 现有的 TLS 实现。

+：修复mcTLS中的安全性问题。

#：可 被 实例化 与 未修饰的 TLS 1.3 草案 23. 构建 一个 可证明 安全的 协议。该 协议 是 不是 意味着 要 鼓励 采取 的 积极的 代理 ，但 要 证明 的 困难 的 构建 一个 安全 代理的终端到终端的安全 协议

是 该 在 的 情况下 ，其中 的专业 硬件 的 广泛使用，将基于SE方法 仍 然扮演 一个 角色 中提供 的检查加密的 流量 在 一个 私人 的方式？该 答案将是肯定的，如果 结合了 基于SE- 方法 和 在 TH 的方法 ，以 减少 对加工负荷的TH是相对更高效的比具有所有 加密的流量 被处理 在 所述 受信任的 硬件。

机器学习方法提出了理想的解决方案，但是效率低下？ 方案基 于对ML 表示 了 理想 的解决方案 ，因为 现有 的设置 是 不需要 对 被 改变。 然而，性能基础上ML匹配- 荷兰国际集团 可能需要 对 被 进一步 探索 尤其是 当相比 所有 的 其他 方法。

AC为主 的方案 作为 一个 替代 ，以 中间人？ 在 为了 要避免 的 安全 问题 的 的 基础MITM- 的解决方案， 根据方案的交流技术建议 方案是要求所有的MB到 是负责任之间 的客户端 和 该 服务器。如果 这 是 部署它意味着 在 客户端 和 该 服务器 是 能够 以 建立 一个 安全的 会话 与 每个 中 的 MB ，并 决定 哪些 数据 的 MB 被 允许 到视图。 的 性 能 会 然后 是 相似 于 一个 普通 MitM-基于 溶液 自 所述 MB 进行 解 密，检查和重新加密 作为 之前，但 在 该AC 设置。该 挑战 是 没有 这 么多 的 性能 在 此 情况下，但 安全性，配置和 实用，这 我们 讨论 中 的 其他 2个 部分。

移动 对 基于TH- 解决方案。 正如 每 我们的 观察上 的 最近期的 文 献中，新的 方案 正在 倾斜 ，旨在利用 值得信赖的 硬件 效率 等 作为 对 安全的 飞地技术 提供 由 英特尔 SGX 即 是 可 在 大多数 的 的 最新 英特尔 处理器。该 挑战 是 在 不断 的努力 在提高 了 性能 ，同时 在 该 同一 时间 最小化 无泄漏年龄 的 信息。这 是 至关重要的 ，因为 在 安 全的 飞地 可以被 认为是 资源有限的 设备 在 一个 特定的 意义，而不是 所有 的网络 流量 应该 被 路由 到 的 内存 或 存储空间 的 的 飞地 进行 处 理。 的 研究 方向 是 由此 检查 和 构建 高效的，但 私人 通信 亲母育酚 之 间 的 飞地 和 所述 MB （和/或 该 服务 提供者）。可替代地， 一个 方案 可以 构造 一个 秘密 共享 协议 的是利用 多个 飞地 该 分发 工作负载 之 间这些飞地 在 一个 安全的 方式。

5.3 实用程序

在 方面 的 效用，计划 基于 对AC和TH具有的capabil-，两者均以提 供完整的功能类似，以检查的明文数据。这是因为这两种技术，使 宏块到解密的潜在 流量。

无需客户端-服务器负责的完整功能。 的挑战为 方案 基于 对AC 技术是其是否它 是 可能的 ，以 实现 这样的 实用程序 ，而不 具有 向 一个 先验决定 和 认证 所述的MB 涉及 在 所述 之间的通信 的客户 机和 所述 服务器。这是不明确时，一个 新的 MB 是 引入，或在现有的一个 被 移除，如何在客户端和服务器更新他们的沟 通。此外，AC引入 的 概念 的 情况下，其中 的 客户端 ，并 在 服务器 具有 灵活 的 设置 一个 MB 访问 策略 对 他们的 数据。 这意味着 决 定 的 MB 是 可以 读取 和/或 写 一 特定部分 的 所述 加密 数据。 这 是 还没有 明确 如何 这 可能 是 执行 在 一个 系统 和 准确 的方式，特别是 存在 的信息 在 不同的 领域 是 5月 需要 特定的 访问的策略。 由于 被 指出 在 [19]， 解决方案 基 于 对AC技术需要的支持的该服务器和该客户端，这可能不是 可行 ， 因为 对于 例如 该 服务器 有 没有 兴趣 来 帮助 一个 客户 是 会 愿意 以 防止 恶意软件 下载。

扩展 功能 的 SE 和 ML 技术。 在 该情况下 ，其中 在部署 专门的 硬件 是 不 一个 选项， ES- pecially 与 遗留 系统中， 一个 可以 寻求 到 延伸 的 有限的基于SE和基于ML方法的功能性。在昼夜温差ficulty为 SE-技术是的并发症的延伸的TO- 肯 匹配 机制 不会 泄漏 大量 信息。 而 Embark [37] 和 Yuan *等人*。[61] 延伸 的 能力的 BlindBox [53]， 所述 匹配 仍然 没有 未 提供 充分 规则表达式 匹配。对于 基于 ML- 方案 的 挑战 是 要 构建 ML 算法 和 模型 是 使 检测 不同类型的 的 异 常 流量 ，而不 检查 所述 有效载荷。

6 结论

在 这个 工作 ，我们 提出 一个 全面的 调查 上 的 话题 的过度加密流量 隐私保护检查。我们定义一个信任 模型， 并根据 现有的最新方案 对不 同的网络设置进行分类。从我们的编辑，我们进一步归类的当前计划为 4种主要技术， 这 使 我们 对 展示 的 优势 和 局限性 的每一个 的 的 建 议。 这 给了 洞察 到了 合适 的 建议 ，以 待 部署 在 实践中，这 我们 也 讨论。主要的 困难 是 要 填补 的 缺口 之间的 实际 部署，其中非常多的 还是基于对的人在这方面的中间人的做法是不不 保留 隐私。为了这一 点，我们列出并讨论了许多 挑战，面临着 中 的 现有 技术 和 可能的 方 向进行 改进。

致谢

研究支持通过了国家研究基金会，总理大臣的 办公室，新加坡，根 据 其 公司 实验室@ 大学 计划，国立大学 的 新加坡，与 新加坡 电讯 有限公司

参考资料

[1] 国家安全 局。 2019年 交通运输 层 安全 Inspec- 重刑。https://www.us-cert.gov/ncas/current-activity/2019/11/19/nsa-releases- 网络咨询管理风险运输 层安全性。

[2] Akamai。于2020年 12月访问。Akamai Web服务安全。 https: //www.akamai。 com / us / en / resources / web-service-security.jsp。

[3] John Althouse，Jeff Atkinson和Josh Atkins。于2020年12月访问。使用JA3和 JA3S进行 TLS指 纹 识 别。ttps : //engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967。

[4] 布莱克 · 安德森 和 大卫 · 麦格鲁。 2016。 使用上下文流数据识别加密的恶意软 件流量。在 *诉讼 中 的2016 ACM 研讨会 上人工 智能和安全，AISec @ CCS 2016年，维也纳，奥地利，年10月28日，2016年*，大卫 · 曼德尔 · 弗里曼（David Mandell Freeman），阿卡特里尼 · 米特罗 科察（Aikaterini Mitrokotsa）和阿鲁涅什 · 辛哈（Arunesh Sinha）（编辑）。 ACM，35-46。https://doi.org/10.1145/2996758.2996768

[5] 布雷克 · 安德森 和 大卫 · 麦格鲁。 2017年 机器 学习 为 加密的恶意 流量 分类：会 计 的 嘈杂 标签 和 非平稳性。在 *诉讼 中 的 第23届ACM SIGKDD 国际 会议 上的 知识发现和数据挖掘，哈利法克斯，NS，加拿大，八月13日至17日，2017 年* 。 ACM ， 1723-1732 。 https://doi.org/10.1145/3097983.3098163

[6] 布莱克·安德森，苏巴西·保罗和大卫·麦格鲁。2018年。破译恶意软件对TLS的 使用（不解密）。 *J. 计算机 病毒学 和 黑客技术*14，3 （2018），195-211。 https://doi.org/10.1007/s11416-017-0306-6

[7] 哈桑 贾米尔 阿斯加尔，卢卡 梅利斯，西里尔Soldani，埃米利亚诺 德Cristofaro，钼HAMED阿里Kaafar，和劳伦Mathy。2016. SplitBox：迈向高效的专用网络功能 虚拟化。在 *诉讼 中 的ACM SIGCOMM 研讨会在中间盒和网络功能虚拟化，HotMiddle-热门话题箱@ SIGCOMM 2016年，弗洛里亚诺波利斯，巴西，八月，2016*，东塑 汉 和 丹尼拉兹 （编辑）。ACM，7–13。https://doi.org/10.1145/2940147.2940150

[8] Karthikeyan Bhargavan，Ioana Boureanu，Antoine Delignat-Lavaud，Pierre-Alain Fouque和Cristina Onete。2018年 一个 正式的 处理 的 负责任的 代理功能在TLS。在 *2018 IEEE 研讨会 上 的安全 和 隐私，SP 2018，圣 旧金山 美国加利福尼亚州，2018年5月21-23日*。IEEE 计算机 协会，339–356。

[9] Broadcom。进入 2020年，赛门铁克 SSL 可见性 设备。https：// docs。broadcom.com/doc/ssl-visibility-appliance-zh-CN。

[10] Broadcom。访问的 十二月 2020年 管理 加密的 流量 与 SSL 可视性 appli- ANCE。https://www.broadcom.com/products/cyber-security/network/encrypted- 交通管理。

[11] 乔凡Bulck，滨海Minkin，奥菲尔WEISSE，丹尼尔Genkin将，巴里斯Kasikci，弗兰克 Piessens，马克· 斯坦，托马斯 F. Wenisch，尤瓦 Yarom，和 拉乌尔 Strackx。2018年预示着：提取 的 钥匙 给 了 英特尔 SGX 王国 与 瞬态外的顺序 执行。在 *第27届USENIX 安全 研讨会上，USENIX Security 2018，巴尔的摩，MD，USA，年8月 15-17日 2018年*，威廉· 恩克 和 阿德里安娜 波特毛毡（编辑）。USENIX 协 会，991–1008。https://www.usenix.org/conference/usenixsecurity18 /演示/批量

[12] 塞巴斯蒂安·卡纳德（SébastienCanard），艾达·迪奥普（AïdaDiop），尼扎尔·凯尔（Nizar Kheir），玛丽·潘达德沃因（Marie Paindavoine）和 穆罕默德·萨伯特（Mohamed Sabt）。2017年 。BlindIDS：基于市场的，基于隐私的，对加密流量的入侵 检测系统。在 *诉讼 中 的2017年ACM 的 亚洲 会议 上 计算机 和 通信 安全，AsiaCCS 2017年，阿布·阿布扎比 联合 阿拉伯酋长国，2017年4月2 日至6日*，Ramesh Karri，Ozgur Sinanoglu，Ahmad-Reza Sadeghi，和迅毅（编辑）。ACM，561–574。https://doi.org/10.1145/3052973.3053013

[13] Brian Carpenter 和 Scott Brim。2002。中间盒：分类法 和 问题。RFC3234。https：//tools.ietf.org/html/rfc3234 。

[14] David Cash，Paul Grubbs，Jason Perry 和 Thomas Ristenpart。2015年 Leakage-滥用攻击反对检索加密。在 *诉讼中的第22届计算机与通信安全，科罗拉多州丹佛市，ACM SIGSAC会议 美国，2015年10月12日至16日*，Indrajit Ray，Ninghui Li和Christopher Kruegel（编辑）。ACM，668–679。https://doi.org/10.1145/2810103.2813700

[15] 思科。2018。加密的流量分析。https://www.cisco.com/c/dam/zh/us/ solutions / collateral / enterprise-networks / enterprise-network-security / nb-09- encrytd-traf-anlytcs-wp-cte-en.pdf。

[16] Aldo Cortesi，Maximilian Hils和Raum Fresser。2018.MitMProxy。https：//mitmproxy.org/。

[17] 网络安全 和 基础设施 安全 局 （CISA）。2017年HTTPS间ception弱化TLS安全。警报（TA17-075A），CISA，美国系的 国土 安全部。https://www.us-cert.gov/ncas/alerts/TA17-075A。

[18] 哈维尔·德·卡纳瓦莱·卡纳瓦莱特和穆罕默德·曼南。2016年。被 代理 杀死：分析客户端TLS拦截软件。在*23日AN- NUAL网络和分布式系统安全研讨会，NDSS 2016年，2016年2月21日至24日，美国加利福尼亚州 圣地亚哥*。在 互联网 Soci-ETY。http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/杀死代理分析客户端结束tls拦截软件.pdf

[19] 泽维尔 德 卡恩 德 卡纳瓦莱 和 保罗 C. 面包车 Oorschot。2020年 一个 调查 和分析 的 TLS 拦截 机制 和 动机。*CoRR Abs* / 2010.16388（2020）。arXiv：2010.16388 https://arxiv.org/abs/2010.16388

[20] 帕拉斯凯维 翟某，扬 Fajfer，尼古拉斯 穆勒，伊娃 Papadogiannaki，埃 Rekleitis，和FRANTISEK Střasák。2019。加密流量分析：用例和 安全 挑战。欧洲的 联盟 机构 的 网络安全（ENISA）。https://www.enisa.europa.eu/publications/encrypted-traffic-analysis。

[21] 华谊段，刘兴亮元，并聪王某。2017年。LightBox：SGX辅助的安全 网络 功能 以 接近本机的 速度运行。*CoRR* abs / 1706.06261（2017）。arXiv：1706.06261 http://arxiv.org/abs/1706.06261

[22] 扎基尔Durumeric，赞恩马，德鲁Springall，理查德巴恩斯，尼克沙利文，埃利Bursztein，迈克尔贝利，J.亚历 尔德曼，和维恩帕克森。2017年的安全 影响 的 HTTPS拦截。*2017年2月26日至3月 1日，在第24届 年度 网络 和 分布式 系统安全研讨会上，NDSS 2017，美国加利福尼亚州圣地亚哥*。互联网协会。https://www.ndss-symposium.org/ndss2017/ndss- 2017年计划/安全性影响-https-拦截/

[23] ETSI。2018.网络；中间盒 安全 协议；第1部分：配置文件 功能要求。ETSI TS 103 523-1 V0.0.13（2018-04）草案。

[24] ETSI。2018.网络；中间盒安全协议；第2部分：传输层MSP，简介为细晶访问控制。ETSI TS 103 523-2 V0.0.8草案（2018-04）。

[25] ETSI。2020年 。中间盒 安全 协议；第1部分：MSP 框架 和模板 要求。ETSI TS 103 523-1 V1.1.1（2020-12）。https://www.etsi.org/ 交付 /etsi_ts/103500_103599/10352301/01.01.01_60/ts_10352301v010101p.pdf。

[26] 靖远风扇，王朝文关，奎任，勇崔和刘春明巧。2017年SPABox：维护隐私在深度包检查，在一个中间设备。*IEEE / ACM Trans。网络* 25，6（2017），3753–3766。https://doi.org/10.1109/TNET。2017.2753044

[27] 尼克·费斯特（Nick Feamster）。2010。外包家庭网络安全。在 *诉讼中的2010 ACM SIGCOMM 研讨会上家庭网络（HomeNets '10）*。ACM，新

美国纽约州约克，37-42。https://doi.org/10.1145/1851307.1851317
[28] Gigamon。于2020年访问。 带有GigaSMART的Gigamon可见性和分析结构。 https://www.gigamon.com/content/dam/resource-library/english/feature-brief / fb-ssl-tls-decryption.pdf。
[29] 大卫Goltzsche，SIGNE RUSCH，曼努埃尔Nieke，塞巴斯蒂安Vaucher，尼科Weich- brodt，瓦莱里奥Schiavoni河，皮埃尔-路易Aublin，保罗·科斯塔，克里斯托夫·费兹，帕斯卡尔·费尔伯，彼得Pietzuch，并Rüudiger卡皮查。2018年ENDBOX：可扩展的 中间件功能 使用 客户端 可信 执行。在 *第48届IEEE / IFIP Interna-周志武 会议 关于 可靠 系统 和 网络的信息， DSN 2018， 卢森堡， 2018年6月25日至28日*。IEEE计算机 协会，1-12。
[30] 伯汉，维杰戈帕拉克里希南，芦笙姬，和Seungjoon利。2015年 网络功能 虚拟化：挑战 和 机遇 进行 创新。 *IEEE通信杂志*53，2（2015），90-97。 https://doi.org/10.1109/MCOM。2015.7045396
[31] Juhyeng汉，晟 敏 金，Jaehyeong哈，和 东苏 汉。2017年 SGX-Box：已 启用 能见度 在 加密 流量 使用 一个 安全 中间件 模块。在 *诉讼中的第一个亚太研讨会上网络，APNET 2017年， 香港地区， 中国， 年8月3-4级，2017年*，启辰和Jitendra Padhye （编辑）。ACM，99-105。 https://doi.org/10.1145/3106989.3106994
[32] 穆罕默德·赛义夫（Mohammad Saiful）伊斯兰教徒，穆罕默德·库祖（Mehmet Kuzu）和穆拉特·坎塔西奥乔（Murat Kantarcioglu）。2012年。关于可搜索加密的访问模式 披露：分枝，攻击和缓解 。在*2012年2月5日至8日于美国加利福尼亚州圣地亚哥举行的NDSS 2012第19届年度网络和分布式系统安全研讨会上*。在互联网所以- ciety。 https://www.ndss-symposium.org/ndss2012/access-pattern-disclosure- 可搜索的加密分支攻击和缓解
[33] ITU-T。2012年 需求 的 深层 数据包 检查 在 下一 世代NET-作品。 接下来 代 网络 - 安全性， 系列 Y： 全球 Infor公司MATION 基础设施， 互联网 协议 ASPECTS 和 下一步- 下一代网络，建议 ITU-T Y.2770建议书（11/2012）。 https://www.itu.int/ rec / T-REC-Y.2770-201211-I / zh。
[34] Jeff Jarmoc。2012年。 传递 信任： SSL / TLS 拦截 代理。 https：// www。 secureworks.com/research/transitive-trust。
[35] Georgios Kellaris，George Kollios，Kobbi Nissim和Adam O'Neill。2016年。对安全外包数据库的一般攻击。在 *诉讼中的2016 ACM SIGSAC 会议 对 计算机 和 通信 安全， 维也纳， 奥地利， 月24- 28年，2016年*，埃德加·R. Weippl，斯特凡Katzenbeisser，克里斯托弗Kruegel，安德鲁C.迈尔斯和夏嘉曦 Halevi （编辑）。ACM，1329年至1340年。 https://doi.org/10.1145/2976749。2978386
[36] 上汽赖，Sikhar Patranabis，阿明Sakzad，约瑟夫ḵ刘，Debdeep Mukhopad-hyay，罗恩·施泰因费尔德，石丰 太阳，东溪 刘，并 聪 左传·。2018。 结果模式 隐藏用于联合查询的 可搜索 加密。在 *2018年ACM SIGSAC计算机和通信安全会议的议事录中*。745-762。
[37] 常兰，海宁雪利酒，拉卢卡阿达波帕，西尔维亚Ratnasamy，和郅Liu发消息 2016年 踏上：安全地 外包 中间盒 到了云计算。在 *第13届USENIX网络系统设计与实现研讨会上，NSDI 2016，圣诞老人 美国 加利福尼亚州克拉拉，2016年3月16日至18日*，卡特琳娜·J·阿格里拉基（Katerina J.Argyraki）和丽贝卡·艾萨克斯（Rebecca Isaacs）（编辑）。USENIX协会，255-273。https://www.usenix.org/conference/nsdi16/ 技术会议/演讲/局域网
[38] Hyunwoo李，扎克 史密斯，Junghwan廉，Gyeongjae彩，塞林 淳，Tae-重 锺 和泰德Taekyoung权。2019年maTLS：如何以使TLS中间件感知？在 *第26届 年度 网络 和 分布式 系统 安全 对称- posium，NDSS 2019年，圣圣地亚哥 加利 福 尼亚州， 美国， 年2月 24-27日 2019*。该 互联网社会。 https://www.ndss-symposium.org/ndss-paper/matls-how-to-make-tls- 中 间盒感知/
[39] Yahuda Lindell。2018年 在安全 的 英特尔SGX的 重点 保护 和 数据 保密性的 应 用 。 https://cdn2.hubspot.net/hubfs/1761386/security-of- intelsgx-key-protection-data-privacy-apps.pdf。
[40] 玛丽·米克（Mary Meeker）。2019. 互联网趋势 2019.https ：//www.bondcap.com/report/ itr19 /。
[41] David Naylor，Richard Li，Christos Gkantsidis，Thomas Karagiannis和Peter Steenkiste。2017年 和 随后 有是更多：安全通信为更多 比二缔约方。在 *诉讼中的第13届国际会议上新兴的网络 试验 和 技术， CoNEXT 2017年， 仁川， 共和国 的韩国，2017年12月12日至15日*。ACM，88-100。 https://doi.org/10.1145/3143361。3143383
[42] 戴维·内勒，凯尔Schomp，利玛窦Varvello，伊利亚斯Leontiadis，杰里米·布莱克，迭戈R. 洛佩斯，Konstantina Papagiannaki，巴勃罗·罗德里格斯·罗德里格斯和彼得Steenkiste。2015。多上下文TLS（mcTLS）：在TLS中启用安全的网络内功能。在 *诉讼中的2015年ACM会议上的特别兴趣小组 上 数据 通信， SIGCOMM 2015年， 伦敦， 美国，英国， 年8月17-21日2015年*，史蒂夫尤利格，奥拉夫Maennel，布拉德·卡普，和Jitendra Padhye（编辑）。ACM，199-212。https://doi.org/10.1145/2785956.2787482
[43] 尖挺宁，新沂黄，GEONG森博爱医院，生民旭佳Ch'ng蕙，健 翁，和罗伯特H.邓。2020年松：启用隐私保护深层的TLS数据包检测与规则，隐藏和快速连接Establish-换货。在 *计算机安全方面-ESORICS 2020-第25届欧洲研讨会*

研究计算机安全，ESORICS 2020年，吉尔福德，英国，九月14-18， 2020年提起诉讼， 部分我 （演讲 笔记在 计算机 科学）， 利群 陈凝晖 李 开泰 梁，和 史 蒂 夫 A. 施 耐 德 （编 辑 。），卷 12308。施 普 林 格， 3–22。 https://doi.org/10.1007/978-3-030-58951-6_1

[44] 尖挺宁，GEONG森婆，佳Ch'ng洛，杰森嘉，和EE的简常。2019年 PrivDPI：隐私保护加密流量检测用可重复使用的 模糊处理 规则。在 *诉讼 中的2019 ACM SIGSAC 会议 上 COM的帕特 和 通信 安全， CCS 2019， 伦敦， 英国， 年11月11-15日 2019*，洛伦佐·卡瓦拉罗，约翰内斯·金德，王小峰和乔纳森·卡茨 （编辑）。ACM，1657–1670年。https://doi.org/10.1145/3319535.3354204

[45] 宁建廷， 徐佳， 梁开泰， 张凡和 张易建。2019。针对可搜索加密的被动攻击。 *IEEE Trans。 信 息 取 证 和 安 全* 14， 3 （2019）， 789–802。 https://doi.org/10.1109/TIFS.2018.2866321

[46] RISHABH 波达， 昌 兰， 拉卢卡 阿达 波帕， 和 西尔维亚 Ratnasamy。2018年 SafeBricks： 屏蔽网络功能中的云。在 *美国华盛顿州伦 顿 市举行的第15届 USENIX 网络系统设计与实现研讨会上，NSDI 2018 2018年4月 9日至11日*， Sujata Banerjee 和 Srinivasan Seshan （编辑）。USENIX Associa- 第 201–216 页 。 https://www.usenix.org/conference/nsdi18/presentation/poddar

[47] 郝任，红卫李，东晓刘，国文许，南承，和学民Sher- 人 沉。2020年。 保护隐私的 有效 可验证 深度 数据包 检查 适用于 云辅助的 中间盒。 *IEEE Transactions on Cloud Computing* （2020年）。

[48] Google透明度报告。[n。 d。]。网络上的HTTPS加密。 https：//transparencyreport.google.com/https/overview，将于2020年11月访问。

[49] Daniel Roethlisberger和贡献者。2018.SSLSpit。https://www.roe.ch/ SSL分割。

[50] Scott Ruoti，Jeff Andersen，Tyler Monson， Daniel Zappala 和 Kent E. Seamons。2018年 一个 比较 可用性 研究 的 重点 管理 的 安全 电子邮件。 在*马里兰州巴尔的摩市SOUPS 2018年第十四届可用隐私和安全性研讨会上， 美国， 年8月12-14日2018年*，玛丽·艾伦 Zurko 和 希瑟·里希特 Lipford （编辑）。USENIX协会，375–394。https://www.usenix.org/conference/soups2018/介绍/ ruoti

[51] 贾斯汀·雪莉。2016年 *中间盒作为一个云服务*。博士 论文。电的工程 与计算机 科学学院，大学 的 加利福尼亚州 的 伯克利。

[52] 贾斯汀· 雪莉 （Justine Sherry）， 沙迪 ·哈桑 （Shaddi Hasan）， 科林 ·斯科特 （Colin Scott）， 阿文德·克里希那慕尔 （ Arvind Krishnamurthy）， 西尔维亚· 拉塔萨米 （Sylvia Ratnasamy） 和维斯·塞卡 （ Vyas Sekar）。 2012年 制作 中间件 别人 别人的 prob- LEM： 网络 处理 作为 一个 云 服务。 在 *ACM SIGCOMM 2012 CON-扰， SIGCOMM '12， 赫尔辛基， 芬兰 - 年8月 13 - 17日， 2012*， 拉斯 埃盖特，约尔格 奥特，文卡塔 N. 帕德马纳班，和 乔治 Varghese分析 （编辑）。 ACM，13–24。 https://doi.org/10.1145/2342356.2342359

[53] 海宁 雪利酒，昌 兰，拉卢卡 阿达 波帕，和 西尔维亚 Ratnasamy。2015年 Blind-盒：深度 包 检测 过 加密的 流量。 在 *诉讼 中 的2015年ACM 会议 上的 特殊 利益 集团 的 数据 通信， SIGCOMM 2015年， 伦敦， 美国，英国， 年8月 17-21日 2015年*， 史蒂夫 尤利格， 奥拉夫 Maennel， 布拉德· 卡普，和Jitendra Padhye （编辑）。ACM，213–226。 https://doi.org/10.1145/ 2785956.2787502

[54] 赛门铁克。2018。加密的流量管理。https://www.symantec.com/ 产品/加密流量管理。

[55] T-Mobile。于2020年12月访问。T-Mobile安全网络。https：//networking.t-mobile。com / solutions / secure-web /。

[56] 博赫丹 泽， 阿尔弗雷德 Krohmer， 弗朗兹 格里， 谢尔盖 Arnautov， 普拉莫德 Bhatotia，和克里斯托弗费兹。2018年 ShieldBox：安全中间盒 使用屏蔽 Execu-重刑。在 *诉讼中的研讨会上SDN 研究，SOSR 2018年，洛杉矶 洛杉矶CA， 美 国 ， 2018 年 3 月 28 日 至 29 日* 。 ACM ， 2 ： 1–2 ： 14 。 https://doi.org/10.1145/3185467.3185469

[57] 安东 · 秋林。 2018。即使在TLS下也 检测 恶意 通信。苏里康 2018.https ：//suricon.net/wp-content/uploads/2019/01/SuriCon2018_Tyurin.pdf 。

[58] 路易 · 威克 （Louis Waked） ， 穆罕默德 · 曼南 （Mohammad Mannan） 和 阿姆 · 尤塞夫 （Amr M. Youssef）。 2018年 将 对不起 国家 TLS的 安全 在 企业 拦截 电器。 *CoRR* abs / 1809.08729 （ 2018 ）。 arXiv ： 1809.08729 http://arxiv.org/abs/1809.08729

[59] 王聪， 袁星亮，崔勇和奎仁。2018年。迈向安全 外包 中间盒 服务：实践，挑战 及 以 后 。 *IEEE 网 络* 32， 1 （2018）， 166–171。 https://doi.org/10.1109/MNET.2017.1700060

[60] 山田彰 （Akira Yamada），三宅裕 （ Yutaka Miyake），竹森 圭 辅 （KeisukeTakemori）， 阿伦 · 史都 （Ahren Studer） 和 阿德里安 · 佩里格 （AdrianPerrig）。2007。用于加密Web访问的入侵检测。在*21日的国际会议上先进的 信息 网络 和 应用程序 （AINA 2007），研讨会论文集，第1卷，2007年5月21-23日，加拿大尼亚加拉瀑布城*。电 气 工 程 师 学 会 计 算 机 学 会 ， 569–576 。 https://doi.org/10.1109/AINAW.2007.212

[61] 陈兴良元，新余 王，健胸 林，和 聪 王。 2016年。在外包中间盒中 保护隐私的深度 数据包 检查。在 *INFOCOM 2016年第35 届IEEE国际计算机通信年度会议上，San 美国加利福尼亚州弗朗西斯科，2016年4月10日至14日*。IEEE，1–9。

[62] Zscaler中，公司访问十二月2020 Zscaler中国综合安全解决方案由德国电信提供的。 https://www.zscaler.com/press/zscaler-powers-综合安全解决方案-offered-deutsche-telekom