Telegram 真的是一个加密应用吗？

作者：Matthew Green编译：Block unicorn

关于作者，Matthew Green是一名密码学家，也是约翰霍普金斯大学的教授。我设计并分析了无线网络、支付系统和数字内容保护平台中使用的加密系统。在我的研究中，我研究了使用加密技术保护用户隐私的各种方式。

这篇文章的灵感来自最近令人担忧的新闻，即 Telegram 的 CEO Pavel Durov 因未能充分监管内容而被法国当局逮捕。虽然我不清楚具体情况，但利用刑事指控来胁迫社交媒体公司是一种相当令人担忧的升级，事情看起来并不像表面那么简单。

但今天我并不想谈论这次逮捕事件。

我想要谈的是报道中的一个具体细节，特别是：几乎每一篇关于这次逮捕的新闻报道都将 Telegram 称为“加密应用”，以下是几个例子：



这种说法让我抓狂，因为从非常有限的技术角度来看，它并没有错。然而，在每一个重要的层面上，它基本上误导了人们对 Telegram 的认知以及它在实际中的工作方式。这种误导对记者和 Telegram 的用户，尤其是那些可能因此受到严重伤害的用户，都是不利的。

现在让我们来谈谈细节。

Telegram 到底有没有加密？

许多系统都会以某种方式使用加密，然而，当我们在现代私人消息服务的背景下谈论加密时，这个词通常有一个非常具体的含义：它指的是使用默认的端到端加密来保护用户的消息内容。当按照行业标准方式使用时，这一功能可以确保每条消息都使用只有通信双方才知道的加密密钥进行加密，而服务运营商无法获知这些密钥。

从你作为用户的角度来看，“加密的消息应用”意味着每次你开始对话时，你的消息只能被正在和你聊天的人读取。如果消息服务的运营商试图查看你的消息内容，他们看到的只会是无用的加密数据。同样的保证也适用于任何可能黑进提供商服务器的人，以及那些向提供商递交传票的执法机构，无论这种情况是好是坏。

Telegram 显然不符合这一更严格的定义，原因很简单：它并未默认启用端到端加密。如果你想在 Telegram 中使用端到端加密，必须手动为每个私人对话激活一个名为“加密聊天”的可选端到端加密功能。这个功能明确地并未为大多数对话启用，并且仅适用于一对一的对话，绝不会在超过两人的群组聊天中使用。

作为一种奇怪的“附加功能”，对于非专业用户来说，实际上激活 Telegram 的端到端加密功能非常麻烦。

首先，激活 Telegram 加密功能的按钮在主对话窗或主屏幕上是不可见的。要在 iOS 应用中找到它，我至少要点击四次——一次进入用户的资料页面，一次让一个隐藏菜单弹出显示选项，最后还要确认我想要使用加密。而且即便这样，我也无法真正开始加密对话，因为“加密聊天”功能只有在你的对话对象恰好在线时才会起作用。



在最新的 Telegram iOS 应用中开始与我的朋友 Michael 的“加密聊天”，从普通的聊天界面中，这个选项并不直接可见。激活它需要四次点击：

（1）进入 Michael 的个人资料页面（左图），

（2）点击“…”按钮以显示隐藏的选项集（中图），

（3）选择“开始秘密聊天”，

（4）在“您确定要继续吗”确认对话框中点击确认。之后，我仍然无法给 Michael 发送任何消息，因为 Telegram 的秘密聊天功能只有在对方也在线时才能启用。

总体来说，这与在现代行业标准的加密消息应用中启动新的加密聊天的体验大相径庭，后者只需打开一个新的聊天窗口即可。

虽然这看起来可能像是挑剔，但默认端到端加密与这种体验之间的差异可能非常显著。实际上，这意味着绝大多数一对一的 Telegram 对话——以及每一个群组聊天——可能都能被 Telegram 的服务器看到和记录，服务器可以查看并记录用户之间发送的所有消息内容。这对每个 Telegram 用户来说可能是个问题，也可能不是，但这显然不应该被宣传为特别安全加密的。

（如果你对详细信息感兴趣，以及对 Telegram 实际加密协议的一些进一步批评，我会在下面进一步说明。）

默认加密真的重要吗？

也许重要，也许不重要！可以从两个不同的角度来看待这个问题。

一个角度是，Telegram 缺乏默认加密对很多人来说完全没问题。现实是，很多用户根本不把 Telegram 作为加密的私人消息工具。对于许多人来说，Telegram 更像是一个社交媒体网络，而不是私人消息应用。

具体来说，Telegram 有两个受欢迎的功能使其非常适合这种用例。一个是创建和订阅“频道”的功能，每个频道都像一个广播网络，一个人（或少数几个人）可以向数百万读者推送内容。当你向成千上万的陌生人广播消息时，保持聊天内容的保密性并不是那么重要。

Telegram 还支持包含数千用户的大型公开群聊。这些群组可以对公众开放，也可以设置为仅邀请制。虽然我个人从未想过与成千上万的人共享群聊，但我听说很多人喜欢这个功能。在这种大型公开群体中，Telegram 群聊的未加密性其实也没那么重要——毕竟，在公共广场上谈话时，谁在乎加密性呢？

但 Telegram 不仅限于这些功能，很多加入这些功能的用户也会做其他事情。

想象一下，你在一个“公共广场”里进行大型群聊。在这种环境中，可能没有强隐私的预期，因此端到端加密对你来说并不重要。但假设你和五个朋友离开广场进行一个私密对话。这个对话是否值得强隐私保护？这并不重要，因为 Telegram 不会提供这种保护，至少在默认的加密中，它无法保护你免受 Telegram 服务器的内容共享。

类似地，假设你使用 Telegram 的社交媒体功能，主要是消费内容而不是生成内容。但有一天你的朋友也因为类似的原因使用 Telegram，发现你在平台上并决定给你发送私人消息。现在你是否担心隐私？你们是否会手动开启“加密聊天”功能——尽管这需要通过隐藏菜单进行四次明确的点击，并且如果其中一个人离线，它将阻止你们立即沟通？

我强烈怀疑，许多人可能是因为 Telegram 的社交媒体功能而加入，但最终也会用它来进行私人聊天。我认为 Telegram 知道这一点，并倾向于将自己宣传为“安全的消息应用”，并谈论平台的加密功能，正是因为他们知道这会让人们感到更舒适。但实际上，我也怀疑这些用户中很少有人真的在使用 Telegram 的加密功能。许多用户可能甚至不知道他们需要手动开启加密，可能以为自己已经在使用加密功能。

这引出了我接下来的观点。

Telegram 知道它的加密功能开启起来很困难，但仍然继续宣传自己的产品为安全的消息应用

自2016年以来（可能更早），Telegram 的加密功能就因我在这篇文章中提到的许多原因受到严重批评。事实上，其中许多批评是由包括我在内的专家在多年前与 Pavel Durov 在 Twitter 上的对话中提出。

尽管与 Durov 的互动有时比较尖锐，但那时候我仍然大多相信 Telegram 是出于善意。我认为 Telegram 正忙于扩大其网络，随着时间的推移，他们会改善平台的端到端加密的质量和可用性：例如，通过将其设为默认、支持群聊，并使得与离线用户开始加密聊天成为可能。我假设，虽然 Telegram 可能是一个追随者而不是领头者，但最终它会在加密协议上达到与 Signal 和 WhatsApp 相当的功能水平。当然，另一种可能性是 Telegram 会完全放弃加密，专注于成为一个社交媒体平台。

实际发生的情况让我感到更加困惑。

Telegram 的拥有者没有改善其端到端加密的可用性，自2016年以来，其加密用户体验几乎没有变化。尽管平台所使用的底层加密算法有一些升级，但2024年的秘密聊天用户体验与八年前几乎没有区别。尽管如此，Telegram 的用户数量在同一时期增长了7到9倍。

与此同时，Telegram CEO Pavel Durov 继续积极宣传 Telegram 作为“安全消息应用”。最近，他在个人 Telegram 频道上对 Signal 和 WhatsApp 进行了尖锐的批评，暗示这些系统被美国政府设置了后门，只有 Telegram 的独立加密协议才真正值得信赖。

如果这是在两个都支持默认端到端加密的平台之间进行的合理技术争论，这可能是可以理解的。然而，Telegram 在这一讨论中确实没有立足之地。看到 Telegram 组织鼓励用户远离默认加密的消息应用，而自己却拒绝实施那些能广泛加密用户消息的基本功能，已经不再觉得有趣。实际上，这开始显得有些恶意。

还有哪些加密细节呢？

这是一个加密学博客，所以如果我不花点时间讲解那些无聊的加密协议，那就有些不尽职了。我也会错过一个大好的机会来惊叹于 Telegram 加密的内部细节，每次我查看这些细节时，几乎都是目瞪口呆。

为了减少痛苦，我会在一段话中讲解这些细节，如果你不感兴趣，可以随意跳过。

根据我认为是最新的加密规范，Telegram 的秘密聊天功能基于一个名为 MTProto 2.0 的自定义协议。这个系统使用 2048 位有限域 Diffie-Hellman 密钥交换，群组参数（我认为）由服务器选择。（因为 Diffie-Hellman 密钥交换需要两个用户在线交互，所以如果一个用户离线时，加密聊天无法设置）MITM 保护由终端用户处理，他们必须比较密钥指纹。服务器提供了一些奇怪的随机非ces（随机值），我不完全理解其用途\*——过去这些随机数曾使密钥交换在恶意服务器面前完全不安全（但这一问题早已解决\*）。生成的密钥然后用于最令人惊叹的、非标准的认证加密模式——一种名为“无限混淆扩展”（IGE）的模式，它基于 AES，并使用 SHA2 处理认证。\*\*

注：在上面的段落中，每个我标记为“\*”的地方，是专家密码学家在类似专业安全审计的背景下会举手提问的点。我不打算深入探讨，可以说，Telegram 加密是非常不寻常的。

如果你让我猜测 Telegram 秘密聊天的协议和实现是否安全，我会说可能是安全的。老实说，但这并不重要，因为如果人们实际上不使用它，那再安全也没用。

Block unicorn注释：简单来说，Telegram 的加密系统使用了一些复杂的技术来保护信息，但在用户体验上，它的设置和使用都比较复杂。有些技术细节可能让人觉得不太透明，特别是随机数的使用和密钥的保护方式。

最后

尽管端到端加密是我们为防止数据泄露所开发的最佳工具之一，但这并不是故事的全部。消息传递中的一个最大隐私问题是大量的元数据——基本上是关于谁在使用服务、他们与谁交谈以及他们何时交谈的数据。

这些数据通常不会受到端到端加密的保护。即使在只有广播功能的应用程序中，如 Telegram 的频道，也有很多关于谁在收听广播的有用元数据。这些信息本身对人们很有价值，这一点从传统广播公司花费巨额资金收集这些数据中可以看出。目前，所有这些信息可能都存在于 Telegram 的服务器上，任何想要收集这些信息的人都可以获取。

我并不是专门批评 Telegram，因为几乎所有其他社交媒体网络和私人消息应用也存在同样的问题。但应该提到这一点，但我提到这些问题是为了避免让你觉得，只要有加密就足够了。