Wi-Fi CERTIFIED Enhanced Open™
技术概述

2018 年 6 月

为开放式网络环境提供更好的保护

用户在所有地方都要使用 Wi-Fi 网络：在家中、办公室、酒店、购物中心、公共交通中心和市政服务处。在这类地方使用不安全的网络是有风险的，个人数据可能被窃取，这也是为什么 Wi-Fi Alliance 强烈建议，只要可能，用户就应确保使用安全的、要求身份验证的网络。然而，在有些情况下，开放式 Wi-Fi 网络是惟一可行的选择。虽然世界各地很多消费者使用开放式网络都没有遇到任何问题，但重要的是，要意识到开放式网络是有风险的，要尽力保护用户数据。为了向网络管理员提供另一种无论用户在哪里连接网络都能保护用户数据的工具，Wi-Fi Alliance 开发了一种有利于开放式 Wi-Fi 网络用户的解决方案。

Wi-Fi CERTIFIED Enhanced Open™是 Wi-Fi Alliance 的一项认证计划，在保留开放式网络使用便利这一特点的同时，降低了访问不安全的网络带来的某些风险。Wi-Fi Enhanced Open™网络无需进行身份验证，就为用户提供数据加密，这对根本不提供任何保护的传统开放式网络而言，是一大改进。利用 Wi-Fi Enhanced Open 技术，Wi-Fi 网络服务提供商可以：

- 保持开放式网络的用户体验不变，不要求用户输入密码；
- 为最终用户提供对数据和管理帧的保护；
- 保持部署的简便性，因为不存在需要维护或分享的网络证书；
- 保持与传统开放式网络的互操作性，包括那些采用“强制主页（captive portal）”的传统开放式网络。

本文概述 Wi-Fi Enhanced Open 计划以及该协议的主要组成部分。

开放式网络的风险

无论何时，只要可能，网络拥有者都应该实现 Wi-Fi 安全性，但是在有些部署情况下，人们不希望分发网络证书，或分发网络证书是不切实际的（参见“用例”一节）。无论在什么位置，也无论出于什么原因，开放式网络都有安全风险，尤其是对于不太明白安全问题及安全浏览方法的用户而言，更是这样。

目前有若干种方法利用开放式网络或无需进行身份验证的网络发起攻击，其中包括数据包捕获、数据包注入和建立中间人位置。数据包捕获又称为数据包嗅探，这种方法收集通过开放式网络传送的数据，类似于窃听别人的谈话。然后，分析或梳理这些收集到的数据，以获得敏感信息，例如电子邮件地址、家庭住址或账号。数据包注入又称为数据包欺骗，这种方法在开放式网络上注入数据包，并让这些数据包看起来就像是从另一个合法方传送过来的一样。数据包注入常常用来支持以下攻击：取消身份验证风暴攻击，或在第二层将数据注入不安全的“超文本传输协议（HTTP）”会话中。中间人攻击方法在开放式网络或无需进行身份验证的网络上收集、注入或修改数据，攻击者秘密地转发并有可能更改两方的通信内容，而通信双方都认为他们在相互直接通信。这些攻击可能涉及一些社交工程技巧，例如显示假冒登录页面，以诱导最终用户向攻击者泄漏敏感信息，例如上网密码。

采用 HTTPS（Hyper Text Transfer Protocol Secure）的网站降低了数据包捕获、数据包注入和中间人攻击的风险，HTTPS 是互联网通信的一种加密形式。然而，HTTPS 并不针对用户设备可能在开放式和未加密环境中传送的所有网络信息加以保护，而且用户也并不总是会留意其浏览器中是否出现的是 HTTPS。

Wi-Fi Enhanced Open 在开放式网络中保护用户数据

传统的开放式网络容易遭受被动型攻击，窃听者能够获得未采用 HTTPS 或虚拟专网（VPN）等方法保护的用户信息。开放式网络还容易受到简单的数据包注入攻击。当攻击者尚未建立中间人位置时，Wi-Fi Enhanced Open 通过防止被动型数据包嗅探或数据包注入，切断了攻击路线。这种保护方法对用户而言是透明的，因为该技术无需用户输入密码就可保护数据。

“机会性无线加密”

Wi-Fi Enhanced Open 技术基于“互联网工程任务组（IETF）”在 RFC8110 规范中定义的“机会性无线加密（Opportunistic Wireless Encryption，简称 OWE）”协议，在与 Wi-Fi 网络的关联之上增加了 Diffile-Hellman 密钥交换。Diffie-Hellman 密钥交换在双方之间建立一个共享密钥，用来进行加密通信，同时通过公共网络交换数据。OWE 采用 Diffie-Hellman 的一种变体，即基于先进的椭圆曲线加密方法的“椭圆曲线 Diffie-Hellman（ECDH）”。ECDH 更加高效，能够以更少的计算量提供足够安全的密钥。

OWE 不提供身份验证，因此不针对中间人攻击提供保护，这种攻击引诱客户端设备连接到一个假冒的接入点（AP）上。不过，OWE 确实针对被动型窃听以及简单的数据包注入提供保护，例如取消身份验证风暴攻击或在第二层将数据注入不安全的 HTTP 会话这类数据包注入。采用 OWE 可以得到一个共享、成对、独一无二并用来协商会话密钥的密钥，从而可利用“Wi-Fi 受保护的管理帧（Wi-Fi Protected Management Frames，简称 PMF）”来保护单播数据帧和单播可靠管理帧（robust management frames）。

向“机会性无线加密”网络过渡

网络运营商开始部署 Wi-Fi Enhanced Open 网络时，可以利用 Wi-Fi Alliance“机会性无线加密规范”中定义的 Wi-Fi Enhanced Open“过渡模式（Transition Mode）”。这种“过渡模式”容许逐步向 Wi-Fi Enhanced Open 网络迁移，同时保持与传统设备的互操作性，且不会干扰到用户。支持 Wi-Fi Enhanced Open 的客户端设备将在不知不觉中受益于该技术提供的新的保护功能，因为这种技术无需任何额外的用户配置。

“过渡模式”中 Wi-Fi Enhanced Open AP 采用两种不同但有关的“服务集识别符（Service Set Identifiers，简称 SSID）：一种用于 Wi-Fi Enhanced Open，另一种用于传统的开放式网络。

开放的“基本服务集（Basic Service Set，简称 BSS）”广播一个 OWE“过渡模式”信息元，以提供成对的 Wi-Fi Enhanced Open BSS 的“基本服务集识别符（Basic Service Set Identifier，简称 BSSID）”和 SSID。

Wi-Fi Enhanced Open 客户端设备通过仅列出针对开放 BSS 的 SSID，禁止在 Wi-Fi Enhanced Open AP 上显示 Wi-Fi Enhanced Open BSS SSID。这就为用户提供了一致的体验。

Wi-Fi Enhanced Open 客户端设备与 Wi-Fi Enhanced Open 网络无缝关联，该网络连接到用户选择的开放式网络上。

以 Wi-Fi Enhanced Open“过渡模式”运行的 AP 可以在开放式网络和 Wi-Fi Enhanced Open 网络之间传递广播或组播信息，以支持网络管理目标，例如当处于 Wi-Fi Enhanced Open“过度模式”时支持设备发现。

以 Wi-Fi Enhanced Open“过度模式”运行的 AP 采用与 Wi-Fi Enhanced Open 和开放 SSID 相同的运行政策，例如客户端隔离。

Wi-Fi Enhanced Open 用例

咖啡店和餐馆

咖啡店和餐馆通常提供免费 Wi-Fi 服务，因为客户喜欢去有 Wi-Fi 的地方，而且提供 Wi-Fi 接入符合很多人的期望。店主们提到，如果提供免费 Wi-Fi，他们的客户往往停留更长时间，并有可能购买更多食物。Wi-Fi Alliance 建议，为客户提供安全的、进行身份验证的网络。然而，有些店主喜欢提供不必维护和分享网络证书的 Wi-Fi，或者不想让客户增加额外的输入网络证书的步骤。有些全功能公共 Wi-Fi 解决方案的部署或维护可能还需要 IT 专长。当店主不想限制网络接入，希望最大限度降低部署复杂性时，Wi-Fi Enhanced Open 具有很大的优势，可针对被动型窃听提供保护，并提供无缝的客户体验。

有“强制主页”的顾客网络

在机场、体育馆和其他公共场所提供高速互联网接入的服务提供商常常采用“强制主页”作为授权顾客接入的惟一方法。在“强制主页”中，客户端设备与可用的 SSID 相关联，并被重新导向到一个 HTTPS 站点。如果服务是免费的，例如在机场提供的服务，那么在获得网络授权接入互联网之前，常常提示用户输入某些信息，也可能是观看一个广告，并读取使用条款。在付费服务情况下，被重新导向到 HTTPS 门户的用户必须选择他们想要的 Wi-Fi 服务包，并输入信用卡信息。有时，即使通过“强制主页”完成了身份验证，在开放式网络上仍然要额外传送元数据。

采用“强制主页”控制网络接入的网络运营商可以利用 Wi-Fi Enhanced Open 针对被动型窃听提供保护，同时尽可能最大限度降低部署复杂性。因为 Wi-Fi Enhanced Open 是一项 Wi-Fi CERTIFIED™计划，所以该技术与传统网络是兼容的，甚至那些采用“强制主页”的传统网络。希望部署全功能身份验证和设备配置解决方案的网络运营商，应该考虑采用 Wi-Fi CERTIFIED Passpoint®等方法。

部署时需要考虑的因素

仅 Wi-Fi Enhanced Open 并不能兼顾所有部署情况下需要考虑的全部安全因素，但是该技术为网络运营商降低风险提供了又一种工具。网络管理员可以非常有把握地阻断开放式网络上可能出现的被动型窃听攻击，不过对于更改网络上所传送信息的流氓 AP 和主动型攻击者，他们必须保持警觉，时刻加以监测。

在公共网络中，也有某些类型的“内部人”攻击，例如那些基于“地址解析协议（ARP）”进行欺骗的攻击，这种攻击是由连接在网络上的恶意客户端设备发起的。在 Wi-Fi Enhanced Open 网络上，通过将网络配置为使所有客户端设备相互完全隔离，可以降低这类攻击的风险。隔离措施可能包括对帧进行过滤，如果不过滤，这些帧就会由一个客户端设备转发或路由到另一个客户端设备，还可能包括，通过防止客户端设备利用分组密钥相互直接通信来降低风险。

当 Wi-Fi Enhanced Open 在用户群中的渗透率达到足够高的水平时，网络管理员就应该禁用 Wi-Fi Enhanced Open “过渡模式”了。

总结

Wi-Fi Enhanced Open 网络和设备提供了传统开放式网络目前不能提供的保护。凭借 OWE 技术，Wi-Fi Enhanced Open 无需特殊配置、维护或用户互动，就能提供更强的保护。这种保护对用户而言是透明的。Wi-Fi Enhanced Open 提供数据加密的同时，可保持开放式网络的易用性，因此有利于用户，该技术还有利于网络提供商，因为没有需要维护、分享或管理的公共密码。

如需了解更多有关 Wi-Fi Enhanced Open 的信息，请访问：https://www.wi-fi.org/discover-wi-fi/security。

关于 Wi-Fi Alliance®

www.wi-fi.org

Wi-Fi Alliance®是全球联网的企业共同为您提供 Wi-Fi®服务。我们的合作论坛成员来自整个 Wi-Fi 生态系统，秉承共同的“随时随地、连通一切、连接所有人”的企业愿景，同时提供最佳的用户体验。自 2000 年以来，Wi-Fi Alliance 已经认证了超过 40,000 多项产品，带有 Wi-Fi CERTIFIED™批准印章的产品均符合互操作性、兼容性和最高的行业标准安全保护措施。如今，在不断扩张的各种应用程序中，Wi-Fi 承载着一半以上的互联网流量。数十亿人每天都依赖于 Wi-Fi，Wi-Fi Alliance 将继续推动它的普及和发展。