白皮書

WPA3 與 ENHANCED OPEN：適用於新世代的安全 WI-FI

aruba
a Hewlett Packard Enterprise company

目錄

今日的 WI-FI 安全問題

IEEE 802.11i 工作小組自 2001 年開始制定後來成為 WPA2 的通訊協定。當時「Wi-Fi」尚未誕生，且 802.11 不像現今如此普遍。這對辦公室而言主要是第一站技術，而 Wi-Fi 介面採用 PCMCIA 卡 (即 PC 卡) 形式，需插入筆記型電腦中。此外，AP為獨立裝置 (控制器型架構尚不存在)，具備小型且容量有限的 CPU，無法執行複雜的密碼編譯作業。

IEEE 802.11i 標準最終在 2004 年取得核准，提供兩個明確制定的作業模式：一個使用預先共用金鑰 (PSK) 來驗證簡易的交握；另一個是 802.1X/EAP，會將驗證工作卸載至第三方伺服器。

IEEE 802.11i 完成後，Wi-Fi Alliance 便正式以 WPA2 標準認證實作。如果實作獲得 WPA2 認證，幾乎就能保證可搭配其他 WPA2 認證裝置使用。IEEE 802.11i 的 PSK 模式又稱為 WPA2-Personal (或是 WPA2-PSK)，IEEE 802.11i 的 802.1X/EAP 模式則稱為 WPA2-Enterprise。

這已經是超過 15 年前的事了 (在網際網路時代是很長一段時間)，而現在 IEEE 802.11i 已漸漸過時。

PSK 模式的問題

在 PSK 模式發佈的同時，就發現這個模式容易遭受攻擊。為了最大限度簡化 AP 的密碼編譯作業，在簡易輕量型驗證交握中使用的祕密金鑰，直接以預先共用金鑰為基礎。這導致此模式容易遭受離線字典式攻擊，攻擊者可以看到線上簡易交握的執行過程，然後取得交握訊息的副本並離線，嘗試使用所有想得到的密碼，直到找到可驗證該交握訊息的密碼。

這個過程其實沒有聽起來這麼費力，因為今日使用的大多數密碼通常都是數千組裡的其中一組，因此不需要執行太多運算工作，任何一般程度的攻擊者都能輕易找出密碼。此外，由於這是離線攻擊，因此攻擊者可將運算工作外包給他人進行。正因如此，即便使用高強度密碼，差別也只在於攻擊者成功找出密碼所需的時間長短。

事實上，這是實際發生過的情形：攻擊者使用以程式設計專門執行這類攻擊的大量 FPGA 陣列，每秒可測試數十萬個 PSK，在如此攻勢下，即使再長、再複雜的 PSK 都能輕易攻破。

問題在於，開發出這套通訊協定之時，AP 尚不具備所需的運算能力，無法實作高強度且安全的通訊協定，因此確保安全的重擔就落到使用者肩上。若要安全地使用 802.11i PSK 模式，必須採用複雜、混合大小寫，並以數字、字母和特殊字元組成的長 PSK。但是 PSK 越複雜就越難以管理，且正確輸入的機率就越低。

PSK 管理作業的人為因素，為以 802.11i PSK 管理的網路設下有效的複雜度上限。如此一來，某網路最終的安全性上限，將會影響所有使用者和裝置。

802.1X/EAP 的問題

為了防止 AP 須執行過多工作，同時確保仍可藉由 IEEE 802.11i 實現高強度密碼編譯驗證，而制定出 802.1X/EAP 作業模式。一般而言，此模式使用與用戶端和 AP 區隔開的獨立伺服器，這個伺服器採用可延伸的驗證通訊協定 (Extensible Authentication Protocol，EAP) 且會向用戶端驗證自己的身分，並可選擇性驗證用戶端。一旦 EAP 驗證交換交涉名為成對主鑰 (Pairwise Master Key，PMK) 的共用祕密，系統就會將這個金鑰從 EAP 伺服器傳送至 AP，而 AP 會執行輕量型驗證交握。

第一個 EAP 方法 LEAP 安全性極低，因此有關人士立即決定必須在 EAP 內採用傳輸層安全性 (TLS) 通訊協議，以增強連線的安全性。此後誕生的 PEAPv0、PEAPv1 和 TTLS，都是使用 TLS 執行驗證和建立金鑰的通訊協議。

驗證是運用這些 EAP 方法進行的雙步驟程序，首先伺服器使用 TLS 向用戶端驗證自己的身分，然後用戶端經由安全的 TLS 通道向伺服器驗證自己的身分 (通常需透過使用者名稱和密碼)。

設定 802.1X/EAP 相當困難，且須具備一般 Wi-Fi 使用者沒有的特殊知識。例如，一般使用者通常不知道「內部 EAP 方法」或「匿名身分」為何，更不用說該在這些欄位中填入什麼值。因此，只有當技術專精的 IT 部門能在連接網路前佈建好每一個用戶端，802.1X/EAP 部署才算真正完成。

802.1X/EAP 的這個重大問題是因為其眾多選項所導致。連線所用的組態也許表面上看似安全 (使用 SHA256 進行雜湊，或以 AES 和 128 位元金鑰加密)，但是實際上使用者控制範圍外的參數會導致安全性大幅降低。建立關聯時雖是與 AES-CCM-128 交涉，但最終的金鑰交換可能會產生具有約 60 至 80 位元安全性的金鑰。

舉例來說，交涉 EAP 內的以下任一個 TLS 加密套件，最終都會產生不適用 802.11 中任何未過時加密的對稱金鑰：

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_DH_DSS_WITH_AES_256_CBC_SHA

這是因為所用的雜湊函數為 SHA 或 MD5，或是使用了 RC4 加密。此外，若所用的 TLS 加密套件是透過具有 1024 位元 RSA 金鑰的憑證執行 RSA 金鑰交換，將會產生不適用 802.11 中任何未過時加密的對稱金鑰。問題在於用戶端無法以程式設計方式控制 TLS 加密套件在 EAP 內交涉的內容。

人們為了避免發生不相容的加密套件交涉所導致的連線問題，會以最簡單普遍的方式交涉，可想而知，這並非最安全的作法，而這個普遍作法加劇了此問題。

解決問題的常見使用案例

如上文所述，IEEE 802.11i 是在 Wi-Fi 普及之前所構思出來的。咖啡廳、旅館和餐廳當時不提供 Wi-Fi，如果曾有人預期我們今天所看到的部署，想必他們一定沒有參與 IEEE 802.11i 的開發過程。

Wi-Fi 開始普及時，整合無線電技術取代了筆記型電腦上的 PCMCIA 轉接卡，不久之後，在所有行動裝置上嵌入 Wi-Fi 無線電成為不可或缺的必需品。無論身在何處，人們都期望可使用 Wi-Fi，且有無 Wi-Fi 影響了他們決定要進入或離開某場所。為了吸引和並留住顧客，經營者會在營業場所安裝 AP 並提供免費網際網路服務。

然而，這些人並非經營提供網際網路服務的生意，而是販賣咖啡、司康、啤酒或大塊美味牛排的店家。他們對 Wi-Fi 安全所知甚少，老實說也沒有興趣知道。他們唯一可以確定的是，自己絕對不會購買、設定和維護 EAP 伺服器，然後要求來店的使用者嘗試設定 802.1X/EAP！

唯一的另一個選項為 PSK 模式。嘗試為每個顧客提供不重複的 PSK 是絕對不可能的，因此所有使用者必須共用一個 PSK。經營者為了提供網際網路讓顧客使用，並避免員工停下手邊工作來處理 IT 工作，便將 PSK 公開。實際上，現今的常見作法是將 PSK 寫在黑板或菜單上讓所有人都能看到，這是唯一可滿足這個使用案例的選項。

很遺憾，這個作法非常不安全。由於 PSK 就寫在黑板上，攻擊者甚至不需要執行字典式攻擊！既然已經知道 PSK，他們可以輕鬆擷取用戶端和 AP 必須參與的簡易輕量型交握，然後使用 PSK 來找出用戶端和 AP 所用的加密金鑰。

他們可以解密、修改、重播所有框架，也可以偽造框架。除此之外，由於攻擊者知道 PSK，因此可輕而易舉地建立惡意 AP 來吸引用戶端，然後便能攔截傳入和傳出用戶端的所有流量。共用和公開 PSK 實際的安全性就跟開放網路大同小異。

另一個不使用兩個 WPA2 模式的常見部署模型為網頁驗證入口。這是網際網路服務提供者 (ISP) 最常用作法適用的部署。用戶端連接 AP，然後系統將用戶端重新導向至伺服器，接著伺服器可以要求使用者確認條款與條件、觀看影片或使用信用卡，才能取得網際網路存取權。一旦使用者完成網頁驗證入口伺服器工作流程，系統就不會再將流量重新導向，並提供網際網路存取權給使用者。

由於這類網頁驗證入口部署使用第三方伺服器來處理使用者驗證作業，而這種驗證方式不需要事先佈建任何用戶端裝置，因此用戶端和 AP 之間的互動可無阻礙地進行。用戶端執行「開放性」802.11 驗證與關聯，且用戶端和 AP 互相傳送的框架並不安全。

缺點為網頁驗證入口在提供網際網路存取權給用戶端之前，通常會和用戶端進行密碼編譯交換，但是當用戶端完成網頁驗證入口驗證時，便不再具有密碼編譯狀態。任何鄰近用戶端和 AP 的人也可以偽造解除驗證框架，將使用者踢出網路，並篡奪用戶端的 MAC 位址以竊取網際網路存取權。

很明顯，以上是 WPA2 所導致的不良使用案例。

WPA3 登場解圍

上述每個問題都是經年累月以來所發現，而有關人士致力設計出可解決所有問題的適用通訊協議。最終制定出一系列適用的通訊協議，成為新的 Wi-Fi Alliance 認證計畫。從今往後，就交給 WPA3。

解決 PSK 問題

摩爾定律 (Moore's Law) 指出，積體電路上的電晶體數量每兩年會增加一倍。有些人由此推論，若非電晶體的尺寸會縮小一半，就是運算能力會加倍。摩爾定律對 AP 的影響，意味著 AP 用來執行高強度密碼編譯作業的運算能力，每兩年會增加一倍，再搭配效率更高的橢圓曲線密碼編譯技術，就表示執行高強度密碼編譯驗證的通訊協議和金鑰交換通訊協議，均可在 AP 上執行。最終 PSK 問題可迎刃而解。

對等實體同時驗證 (Simultaneous Authentication of Equals，SAE) 通訊協議在 2000 年代後期加入 IEEE 802.11s (網狀網路) 標準中。IEEE 802.11s 在 2012 年獲得認證。SAE 是 Dragonfly 金鑰交換的實例，使用零知識證明執行密碼驗證金鑰交換，兩方各自證明自己知道密碼，而不會暴露密碼或任何密碼衍生的資料。

若使用零知識證明技術，攻擊者就無法見證單一交換過程並離線破解 PSK。攻擊者確認密碼猜測是否正確的唯一方式，就是主動參與 SAE，每次主動式攻擊就猜測一次。若使用 SAE，所有專門用來破解密碼的 FPGA 陣列和彩虹表均徒勞無功。

零知識證明技術所帶來的影響，就是 SAE 可搭配傳統上視為低強度的密碼使用。WPA2-PSK 是安全性低的通訊協議，其彌補安全性的方式，是將安全責任丟給不應擔此重任的使用者，並對密碼設下要求，例如長度需為兩位數、混合大小寫、包含數字和特殊字元等。

這導致密碼複雜難記且輸入時容易出錯的情況，可想而知，人們因此需將密碼寫在某處，與原來提高安全性的目的背道而馳。若使用 SAE，對密碼唯一的要求只有難以猜測，例如從 1 到 10,000,000 中挑選一個數字。如果是搭配 WPA2-PSK 使用這個密碼，離線字典式攻擊可以在幾秒內找出密碼。但若搭配 SAE 使用同一組密碼，即使發動約 5,000,000 次主動式攻擊，成功機率也只能達到 0.5。主動式攻擊易於偵測和緩解。

802.1X 一致性

WPA3 為 802.1X/EAP 引入一個新組態選項，名為商業用國家安全演算法 (Commercial National Security Algorithms，CNSA)。CNSA 是由美國國家安全局 (NSA) 制定，目的為保護政府和軍事網路上的機密和最高機密資料。CNSA 可穩定提供一致的安全性，並將錯誤設定的可能性降為零，因此對資安有極高要求的企業 (例如金融機構) 均採用此演算法。

CNSA 建立的密碼編譯演算法套件中，每個演算法都提供具有約略相同的保護層級：用於雜湊的 SHA384、用於建立金鑰和數位簽名的 NIST p384 橢圓曲線，以及用於資料加密與驗證的 AES-GCM-256。若使用 CNSA，EAP 方法必須為 EAP-TLS，且交涉的 TLS 加密套件只能使用 CNSA 套件中的密碼編譯演算法。

這表示只要部署 CNSA，便可保證絕不會錯誤設定 802.1X/EAP、不可能以不安全的方式混合搭配演算法，且不可能不相容或加密降級，進而大幅簡化網路部署。

Enhanced Open：保護開放網路

咖啡廳和各種公共場所都想以簡單的方式為顧客提供表面上看似安全的網路。開放網路存在一些眾所詬病的問題，因此他們別無選擇，只好使用 WPA2-PSK 搭配共用和公開的 PSK。現在有一個新的解決方案，可提供比共用和公開 PSK 更優異的安全性：Wi-Fi CERTIFIED Enhanced Open™ 搭配機會性無線加密 (Opportunistic Wireless Encryption，OWE)。

OWE 是開放網路的替代選擇，具有相同的工作流程和使用者要求。基本上，只要按一下可用的網路即可連線。對使用者而言，OWE 網路看起來就跟開放網路一樣 (沒有鎖頭符號)，不過其優勢在於經過加密。OWE 會在用戶端與 AP 建立關聯時執行未驗證的 Diffie-Hellman，這個交換程序會產生一個金鑰，世界上只有用戶端和 AP 這兩個實體知道這個金鑰。系統可使用這個金鑰來衍生其他金鑰，用以加密傳出和傳入用戶端與 AP 的所有管理和資料流量。

雖然未驗證的 Diffie-Hellman 技術安全性不高，不過卻比搭配 WPA2-PSK 的共用與公開 PSK 安全，後者基本上是以「黑板上的密碼」作法提供網路存取權。因為 PSK 是公開的，所以位於 AP 涵蓋範圍內的任何人都能取得，且由於它是以共用方式提供，因此所有人都使用相同的 PSK。

這就表示，所有使用者都可以模擬 AP (用戶端無法驗證 AP)，且 AP 無從得知連線的對象 (AP 無法驗證用戶端)；基本上共用和公開 PSK 模式完全沒有經過驗證，就像 OWE 一樣。但 OWE 的不同之處在於，Diffie-Hellman 交換會提供真正成對的唯一金鑰給用戶端和 AP，也就是說其他任何人均無法竊聽連線。攻擊者不可能解密、偽造、修改或重播用戶端和 AP 之間傳送的任何框架。

若使用共用和公開 PSK，知道 PSK 的攻擊者 (每個人都知道！) 只要透過被動觀察 4 向交握，就能找出用戶端和 AP 使用的加密金鑰。OWE 為公共場所部署提供比 WPA2 層級更高的安全性。

針對網頁驗證入口部署，OWE 提供前所未有的安全性。在這些環境中，用戶端和 AP 會在網頁驗證入口啟動前執行 OWE 交換。包含重新導向至網頁驗證入口的框架在內的所有框架，都會受到從 OWE 交換衍生的成對唯一金鑰保護。網頁驗證入口可在加密的安全環境下執行本身的驗證工作：強制使用者按一下條款與條件、讓使用者觀看影片，或是請使用者提供信用卡資訊以取得網際網路存取權。

一旦網頁驗證入口授權用戶端，AP 便可允許用戶端的流量進入網際網路，並保留建立關聯時 OWE 所建立的金鑰。網頁驗證入口授權藉由 MAC 位址識別的使用者，並以相同的 MAC 位址識別 OWE 所建立的金鑰。由於 OWE 包含管理框架保護，因此攻擊者不可能偽造解除驗證框架來將有效的使用者踢出網路，並竊取其 MAC 位址。

總結

WPA3 和 Enhanced Open 代表著 Wi-Fi 安全遲來的改進。自 WPA2 發佈以來，網際網路和其使用方式發生劇烈變化，而與 WPA2 有關的問題和議題也浮上檯面。WPA3 可解決 WPA2 的缺點，且可處理 WPA2 無法處理的使用案例。

WPA3 很重要的特點為安全性提升，複雜度卻未提高。通常安全性提升會讓複雜度隨之提高，反而更難以獲得和實作安全性。使用 WPA3 的優勢在於工作流程或使用方式無任何改變、無需逐一孰悉新步驟，也不需要熟記注意事項。OWE 看起來與我們習慣的開放網路無異，按一下即可連線。此外，WPA3-SAE 看起來就像 WPA2-PSK 一樣，輸入密碼即可連線。最後，CNSA 消除了錯誤設定的可能性，且 802.1X/EAP 工作流程無任何變動。

參考資料

- D. Harkins 與 W. Kumari，《機會性無線加密》(Opportunistic Wireless Encryption)，RFC 8110，2017 年 3 月
- IEEE 802.11-2016，https://standards.ieee.org/standard/802_11-2016.html，2016 年 12 月
- D. Harkins，《Dragonfly 金鑰交換》(The Dragonfly Key Exchange)，RFC 7664，2015 年 11 月
- 美國國家安全局，《NSA Suite B 密碼編譯》(NSA Suite B Cryptography)，2009 年 1 月
- Wi-Fi Alliance，《裝置佈建通訊協議技術規格》(Device Provisioning Protocol Technical Specification) 0.2.8 版，2017 年 12 月
- D. Harkins，《公開金鑰交換》(The Public Key Exchange)，draft-harkins-pkex-05，2018 年 1 月
- F. Stejano 與 A. Ross，〈復活的小鴨〉(The Resurrecting Duckling)，《電腦科學演講筆記》(Lecture Notes in Computer Science)，1796 卷，Springer，柏林，海德堡，1999 年
- IEEE 802.11ai-2016，《修正案 1：快速建立初始連結》，2016 年

aruba
a Hewlett Packard Enterprise company

WP_WPA3EnhancedOpen_110118 a00059003enw