KRACK破解WPA2

林宜進

大綱

- KRACK介紹
- 攻擊分析-四向交握為例
- 預估受害範圍
- 對應方法
- 補充資料
- 參考資料

KRACK介紹

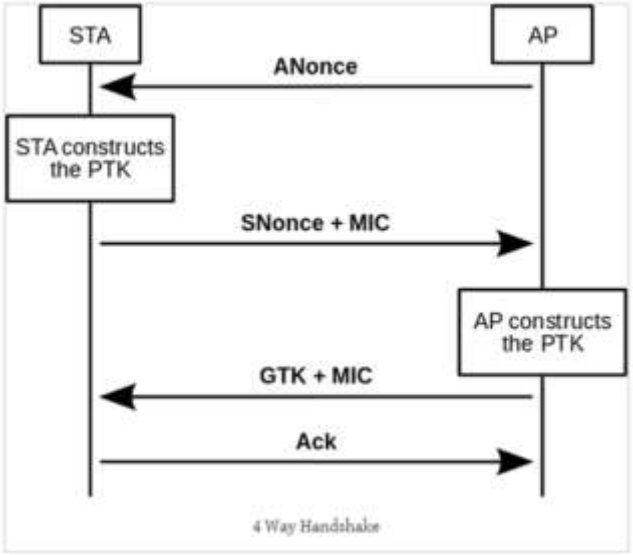
- KRACKs（Key Reinstallation AttaCKs）是一系列WPA2 (Wi-Fi Protected Access 2)協定漏洞的總稱
- 比利時研究人員在今年5月就發現了這一系列漏洞，並於10/16公布細節，以及概念驗證(見補充資料1)。
- 與此相關CVE漏洞有10項(見補充資料2)
- 這是一種不需要依靠密碼猜測的 WPA2 協定攻擊手段

攻擊分析
四向交握為例

1. 四向交握介紹
2. 技術原理

四向交握(4-WAY HANDSHAKE)介紹

- 第一步(Msg1)，AP會傳送一組初始化向量（ANonce）給客戶端裝置(STA)。
- 第二步(Msg2)，STA接到ANonce，會產生一組PTK（Pairwise Transient Key）和另一個初始化向量（SNonce）發給AP，並且使用了名為 MIC（Message Integrity Code）的檢驗碼。
- 第三步(Msg3)，AP收到SNonce後，也會導出一組PTK，並發送密鑰GTK給STA。
- 第四步(Msg4)，STA在安裝本身PTK和GTK之後回復訊息(Ack)給AP。



技術原理

- 利用Wi-Fi握手協議漏洞，在四向交握中客戶端沒有收到AP的訊息時，會要求訊息重傳。
- 當客戶端收到AP發來的訊息(Msg3)後將會安裝PTK和GTK，用於加密正常的封包。但因為Msg3可能丟失或者被丟棄，AP沒有收到回應(Msg4)的話，AP將會重新傳輸Msg3。
- 客戶端每次收到Msg3都會重新安裝加密key，從而重置nonce和replay counters 。而攻擊者可以收集和重新發送四向交握中的Msg3強制重置nonce，從而成功攻擊加密協議，解密客戶端發送的封包，截獲敏感信息。

技術原理-(圖)

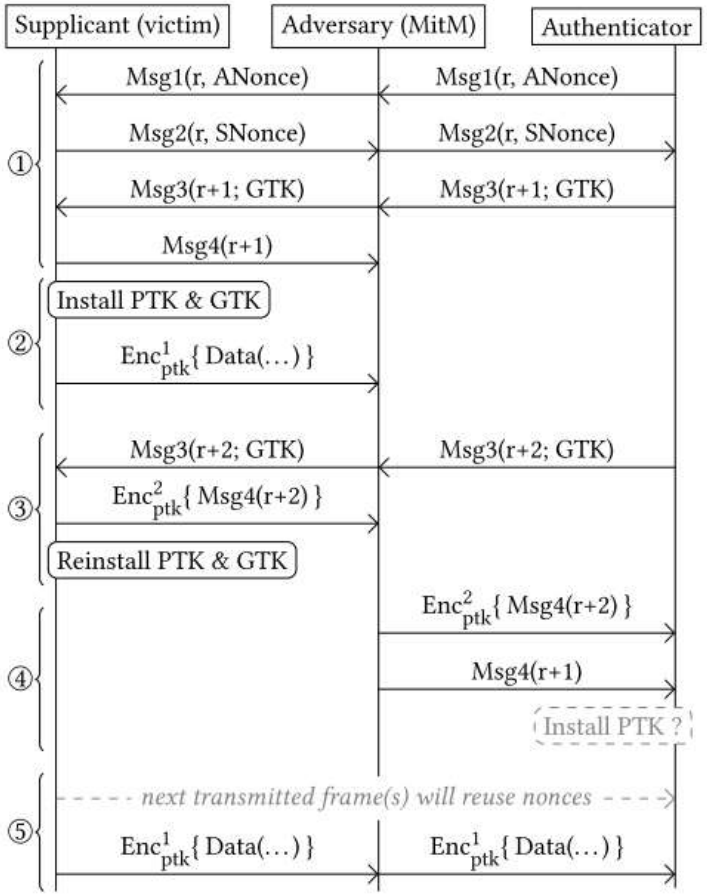


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

預估受害範圍

- 10/16之前尚未修正此漏洞的裝置，例如:
  - 作業系統
    - Microsoft、masOS、使用wpa_supplicant 2.4、2.5版本的Linux系統等等
  - 移動裝置
    - Android 6.0及之後的版本
    - Android Wear 2.0
  - 無線AP
    - 不論何種標準(WPA/WPA2)和任何加密方式(AES/TKIP)都會被破解

對應方法

一. 使用者應盡量瀏覽採用 HTTPS 的加密網站，確保使用者瀏覽網頁時的安全性。

二. Wi-Fi AP 未修補此漏洞前，儘量避免傳送個人相關的機密資料。

三. 使用者連網設備的作業系統，包括電腦、手機作業系統的安全性更新，應儘速更新至最新版本。

四. Wi-Fi AP 的韌體儘速更新到最新版本。

五. 盡量減少使用公共Wi-Fi (如果使用者有行動網路的話)

六. 暫時關閉802.11r（fast roaming）來減少遭攻擊的機率

補充資料

1) KRACK DEMO
2) CVE相關漏洞
3) 廠商修補進度

KRACK DEMO

- 影片 連結:

https://www.youtube.com/watch?v=Oh4WURZoR98

- 額外解說影片 (CVE漏洞):

http://blog.mojonetworks.com/wpa2-vulnerability

CVE相關漏洞

① CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.

② CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.

③ CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.

④ CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.

⑤ CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.

⑥ CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.

⑦ CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.

⑧ CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.

⑨ CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

⑩ CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

廠商修補進度

- 多數廠商在10/16發布此重大漏洞後，才趕緊釋出更新
- 更新部分進度如下(10/19節錄自iThome)

廠商名稱	WPA2弱點修補進度	更多資訊	進度更新
Microsoft 微軟	已在10/10的10月例行更新中修補WAP2（包括Windows和Windows Server各支援版本），10/16對外公告	參考連結	10/16
Google	10/16，發言人透露Pixel手機將率先於11/6修補，其餘Android OS則在數周內修補	非正式公告	10/16
Apple	10/17 蘋果對分析師證實，已在iOS、tvOS、watchOS和macOS目前beta版本中修補了WPA2漏洞。	非正式公告	10/17
Aerohive	10/16公布受影響產品，將先釋出8.1r2a版修補，6.5r9和6.7r4還在開發中。10/18釋出6.5r8a和6.7r2a修補版本	參考連結	10/18
Aruba Networks	已釋出更新（ArubaOS,Aruba Instant,Clarity Engine,501 Wireless Client,AirMesh MSR）	參考連結	10/16
Asus	10/17在用戶論壇中回覆正在處理中	參考連結	10/17
Buffalo/MELCO	先公布受影響產品，正在調查中	參考連結	10/18
Broadcom	受影響，但官方尚無公告		10/18

參考資料

1. KRACK Demo: Critical Key Reinstallation Attack Against Widely-Used WPA2 Wi-Fi Protocol : https://thehackernews.com/2017/10/wpa2-krack-wifi-hacking.html
2. Key Reinstallation Attacks: https://www.krackattacks.com/
3. 廠商更新資料來源
   A. https://github.com/kristate/krackinfo
   B. https://www.ithome.com.tw/news/117532
   C. http://www.kb.cert.org/vuls
4. Key Reinstallation Att acks: Forcing Nonce Reuse in WPA2 論文連結: https://papers.mathyvanhoef.com/ccs2017.pdf
5. 【安全報告】密鑰重載攻擊：強制WPA2重用Nonce: https://www.iread.one/3385707.html
6. 【安全報告】WPA2 KRACK Attacks 分析報告: https://www.iread.one/3372849.html
7. Discovering Logical Vulnerabilities in the Wi-Fi Handshake Using Model-Based Testing 論文連結: https://lirias.kuleuven.be/bitstream/123456789/572634/1/asiaccs2017.pdf