WPA3 – řešení nebo promarněná příležitost?

Od WPA2 se 14 let v oblasti bezpečnosti Wi-Fi sítí zdánlivě nic nedělo. A znenadání je zde WPA3. Co přináší?

Termín WPA (Wi-Fi Protected Access) neoznačuje, jak se často mylně soudí, konkrétní bezpečnostní standard nebo protokol pro zabezpečení Wi-Fi sítí, nýbrž certifikační program Wi-Fi Alliance[1]. WPA3 z ledna letošního roku označuje nový certifikační program, který nahrazuje WPA2 z roku 2004. Od tohoto roku Wi-Fi sítě doznaly masového rozšíření a bylo nalezeno několik závažných zranitelností.

WPA2 – předchůdce WPA3

Certifikace WPA2 (Wi-Fi Protected Access 2) je založena na plné implementaci standardu IEEE 802.11i a existuje ve dvou variantách: WPA2-Personal (neboli WPA2-PSK), kde všichni klienti využívají stejné sdílené heslo lokálně uložené v přístupovém bodu, a WPA2-Enterprise, která vyžaduje RADIUS server.

Pokud pomineme přechodná řešení, WPA2 používá protokol CCMP (Counter Mode CBC-MAC Protocol), šifruje data

[1] Wi-Fi Alliance je obchodní sdružení, které od roku 1999 certifikuje jednotlivé Wi-Fi produkty. Označení „Wi-Fi Certified“ získají produkty testované z hlediska kompatibility, přizpůsobivosti a výkonu.

Použité zkratky BOX 1

BIP-GMAC-256	Broadcast/Multicast Integrity Protocol Galois Message Authentication Code
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode CBC-MAC Protocol
DPP	Device Provisioning Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GTK	Group Transient Key
HMAC-SHA1	Keyed-hash Message Authentication Code – Secure Hash Algorithm 1
KEK	Key Confirmation Key
MIC	Message Integrity Control
MitM	Man in the Middle
NFC	Near Field Communication
OWE	Opportunistic Wireless Encryption
PBKDF2	Password-Based Key Derivation Function 2
PMK	Pairwise Master Key
PMKID	Pairwise Master Key Identifier
PSK	Pre-shared key
PAKE	Password-Authenticated Key Exchange
PKCS	Public-Key Cryptography Standards
PTK	Pairwise Transient Key
SAE	Simultaneous Authentication of Equals
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

pomocí šifry AES a k ověření autentizace využívá provozní režim CBC-MAC. Klíčový management u varianty WPA2-PSK probíhá ve dvou krocích:

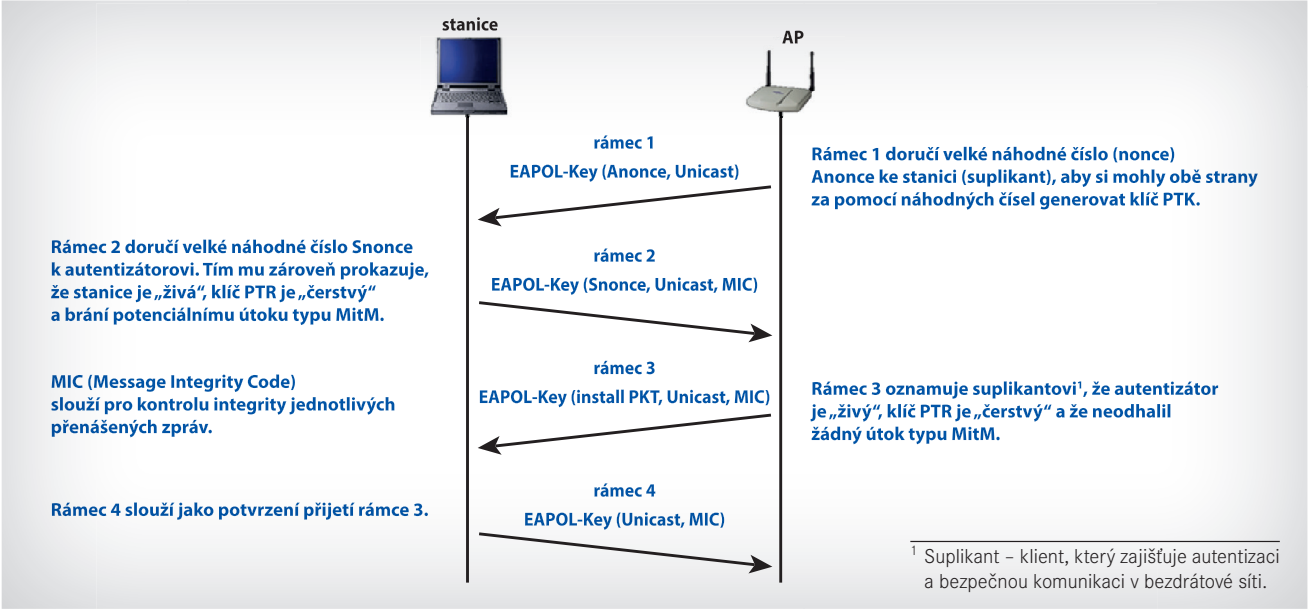
1. Výpočet sdíleného klíče PSK (Pre-shared key) pomocí funkce PBKDF2[2]: PSK = PBKDF2(HMAC-SHA1, heslo, SSID, 4096, 256), kde 4096 je počet iterací a 256 je velikost výstupu v bitech.

2. Výměna čtyř zpráv (čtyřfázový handshaking), během kterých se klient a AP vzájemně dohadují na šifrovacích klíčích PTK (Pairwise Transient Key) a GTK (Group Transient Key) a ověřují si, že jsou na obou stranách stejné (pro dohadování klíče PTK viz obr. 1).

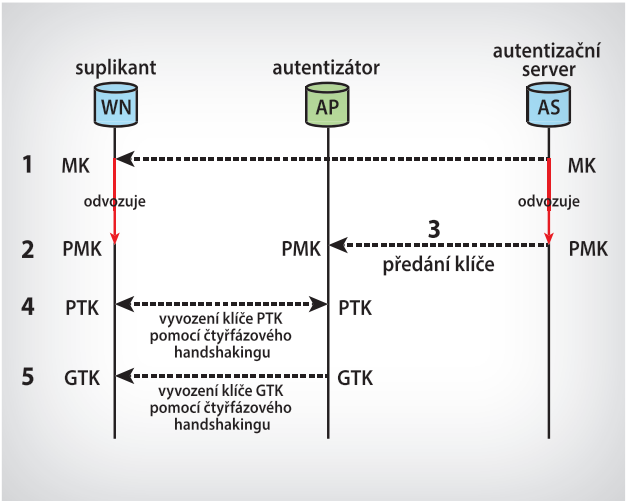
U WPA2-Enterprise (podnikové sítě) jsou v souladu se standardem IEEE 802.11i (viz obr. 2) u autentizátoru (RADIUS serveru) a suplikantu (program v klientském zařízení) uloženy Master Key (MK), z kterých si obě strany vygenerují Pairwise Master Key (PMK). RADIUS server poté předá klíč PMK autentizátoru (Access Point) a ten si spolu s klientem z PMK odvodí pomocí popsaného handshakingu klíče PTK a GTK (viz obr. 2). Klíč PTK je následně „nakrájen“ na další klíče: klíč KCK (Key Confirmation Key) sloužící ke kontrole integrity EAPOL rámců[3], klíč KEK (Key Encryption Key) zajišťující důvěrnost výměny EAPOL rámců a na další dva dočasné klíče.

Postupně byla publikována řada útoků na procesy autentizace a šifrování na protokoly WPA (předchůdce WPA2) i na samotný WPA2, včetně útoků na PSK i GTK. Např. zatímco útoky na klíče PTK lze detekovat, GTK tuto vlastnost nemá. Útoky s využitím této zranitelnosti popsal v roce 2010 na konferenci Defcon Md Sohail Ahmad [7], který ji nazval „Hole 196“[4].

Další významná zranitelnost byla v roce 2017 nalezena v autentizaci, kdy lze ve třetí zprávě klíč poslat vícekrát, přičemž při opakování je znovu nastavena počáteční hodnota nonce, a tím jsou získány různé texty zašifrované stejným klíčem[5] – zranitelnost byla nazvána KRACK (Key Reinstallation Attack).



Obr. 1: Výměna zpráv při dohadování klíče PTK [3]



Obr. 2: Management klíčů, jejich distribuce a hierarchie v souladu se standardem IEEE 802.11i [11]

[2] PBKDF2 je součástí standardu PKCS #5 v2.0 (Public-Key Cryptography Standards) tehdejší společnosti RSA Security (dnes součást EMC Corporation). V roce 2000 PKCS #5 vyšlo jako RFC 2898.
[3] EAPOL (Extensible Authentication Protocol Over LAN) je síťový protokol určený pro 802.1X autentizaci.
[4] Zranitelnost je důsledkem zjednodušeného postupu uvedeného na str. 196 popisu standardu IEEE 802.11, z čehož plyne název zranitelnosti. Blíže se tomuto typu i dalším útokům aktuálním v dané době věnuje článek Petra Hanáčka a Mateje Kačice „WPA2: Útoky z vnútra siete“, který vyšel v DSM 2011/4.
[5] Účelem náhodných čísel nonce je eliminovat opakované šifrování stejným klíčem.

Řada výrobců hardwaru i tvůrců softwaru už vydala opravy, přesto si někteří uživatelé hlídají své sítě pomocí KRACK detektoru.

U WPA2-Enterprise sítí mohou být úspěšné útoky pouze zevnitř, o to jsou však zákeřnější. Jejich uživatelům však chybí silnější kryptografické algoritmy adekvátní komplikovanému řešení.

Pro domácí použití se ukázal postup dle WPA2 jako poněkud těžkopádný, proto byl již v roce 2007 doplněn protokolem WPS (Wi-Fi Protected Setup), kdy pro připojení do dalšího zařízení do existující Wi-Fi sítě stačilo místo dlouhého hesla (přesněji tzv. passphrase) uvést definovaný osmibitový PIN nebo ho automaticky vygenerovat stlačením tlačítka (PBC – Push Button)[6]. U zařízení některých výrobců je tato vlastnost nastavena jako defaultní. Toto řešení se ukázalo jako citlivé na útok hrubou silou a všeobecně se doporučuje je vypnout, což ovšem u některých výrobků nebylo možné. Výrobci cílení na podnikový trh raději WPS mód nepodporují.

Co nového přináší WPA3

Certifikační kritéria WPA3 byla vytvořena se třemi základními cíli [10]:

- Výběr přirozeného hesla: Umožnit uživatelům zvolit si taková hesla, která se lépe pamatují.
- Snadnost použití: Poskytnout zvýšenou ochranu beze změny způsobu připojení uživatelů k síti.
- Forward secrecy[7]: Ochrana přenášených dat i v případě, že je privátní heslo dané strany prolomeno.

Uvedených cílů by mělo být dosaženo pomocí následujících technických opatření:

a) Bezpečnější handshaking

Bezpečný handshaking je zajištěn pomocí protokolu SAE (Simultaneous Authentication of Equals), který je variantou handshakingu zvaného Dragonfly (RFC 7664). Původně byl navržen pro sítě[8] typu mash a je součástí standardu 801.11s vyvíjeného v letech 2003 až 2012. Založen je na výměně klíčů podle algoritmu Diffieho-Hellmana z roku1976 používajícího konečné cyklické grupy nebo eliptické křivky[9]. Je zde třeba řešit problém, že ačkoli algoritmus zabraňuje slovníkovým útokům [6], sám o sobě nezajišťuje vzájemnou autentizaci, a tím pádem je zranitelný útoky MitM (Man in the Middle).

Handshaking SAE časově předchází tradiční čtyřfázový handshaking a zajišťuje vygenerování čerstvých klíčů PMK. Je odolný vůči slovníkovým útokům i za situace slabých hesel. Byl publikován matematický důkaz jeho bezpečnosti, není však garantována odolnost handshakingu proti útokům skrytými kanály.

b) Nahrazení WPS protokolem DPP

Protokol DPP (Wi-Fi Device Provisioning Protocol) umožňuje bezpečné připojení k síti dalšího zařízení za použití QR kódu, hesla, technologie NFC (Near Field Communication) nebo Bluetooth. DPP identifikuje a autentizuje zařízení za pomoci veřejného klíče. V první fázi DPP zvané bootstrapping probíhá mezi oběma zařízeními výměna „surových“ (neověřených) veřejných klíčů a vzájemné ujištění, že klíče patří k jejich identitě (použit je zde protokol PKEX [4]). Ve druhé fázi zvané authentication and provisioning jsou tyto klíče použity pro vzájemné ověření a ve třetí fázi zvané network access phase jsou algoritmem Diffieho-Hellmana vygenerovány klíče relace – výhodou je, že je nelze odvodit z veřejných klíčů, tudíž je nelze použít k odposlechu dalších zpráv (forward secrecy). DPP ale nebude součástí certifikace WPA3.

c) Neautentizované šifrování

Cílem tohoto šifrování je zajistit bezpečnost otevřených sítí (hotspoty atd.). Předpokládá se zde použití mechanismu zvaného Opportunistic Wireless Encryption (OWE) [5]. Toto opatření sice znemožní odposlech přenášených zpráv, nezabrání však takovým útokům, jako je falešný přístupový bod AP.

Po technické stránce vyjednává handshaking OWE nový klíč PMK v rámci výměny klíčů pomocí algoritmu Diffieho-Hellmana. Potřebné údaje jsou zapouzdřeny v informačních prvcích (IE – Information Element) rámců (re)association request a response. Výsledný klíč PMK se používá ve čtyřfázovém handshakingu, který vyjednává a instaluje šifrovací klíče rámce.

d) Silnější kryptografické algoritmy

Z hlediska kryptografie Wi-Fi Alliance nemusela jít daleko a převzala řadu algoritmů, které jsou součástí Commercial National Security Algorithms (CNSA) Suite. S jejich pomocí budou zabezpečeny následující oblasti:

- *Autentizované šifrování:* 256bitový protokol GCMP-256 (Galois/Counter Mode Protocol).

[6] V roce 2014 byla ještě doplněna možnost bezkontaktní komunikace NFC (Near Field Communication).
[7] Server pro každé spojení používá nový pár klíčů. Ani kompromitace privátního klíče nevede ke kompromitaci klíče spojení.
[8] Typu „každý s každým“, vždy peer-to-peer, žádný server ani klient.
[9] Na https://www.cloudshark.org/captures/3638626f4551 je ukázka odchyceného souboru pcapng.

- *Vyvozování klíčů a jejich potvrzování:* 384bitový HMAC-SHA384 (Hashed Message Authentication Code with Secure Hash Algorithm).
- *Výměna klíčů a autentizace:* algoritmy ECDH (Elliptic Curve Diffie-Hellman) a ECDSA (Elliptic Curve Digital Signature Algorithm) za použití eliptické křivky 384 bitů.
- *Robustní ochrana řídicích rámců:* sada protokolů BIP-GMAC-256 (Broadcast/Multicast Integrity Protocol with Galois Message Authentication Code) s 256 bity[10].

Závěr

Při diskuzi ke článku [8] na ROOT.CZ jeden z diskutujících napsal: „Pak tedy vyvstává otázka, proč tu ještě nemáme Open Wi-Fi šifrovanou klíčem vytvořeným přes Diffie-Hellman výměnu.“ A je to tady. Že je na čase, o tom svědčí další významná zranitelnost WPA2, kterou jako vedlejší efekt při hrátkách se svým nástrojem Hcxdumptool objevil Jens (Atom) Steube v srpnu letošního roku [1, 2] (viz Box 2).

Mathy Vanhoef, objevitel slabiny KRACK, označil certifikaci WPA3 pro její polovičatost za ztracenou příležitost [9]. Když se probral vágními informacemi na stránkách Wi-Fi Alliance, došel k závěru, že jediné, co je u certifikace WPA3 skutečně povinné, je SAE (dragonfly handshaking). Delší klíč je požadován jen u certifikace WPA3-Enterprise. Ostatní novinky se stanou součástí jiných certifikací – protokol DPP součástí certifikace Wi-Fi Easy Connect a mechanismus OWE součástí certifikace Wi-Fi Enhanced Open. Dovoluji si dodat: A Wi-Fi Alliance bude vybírat další certifikační poplatky.

[10] Tato ochrana již byla u WPA, ale jen jako volitelná možnost.

Nový útok na WPA/WPA2 s použitím PMKID **BOX 2**

Tato metoda útočí na klíč PMKID (Pairwise Master Key Identifier) obsažený ve volitelném poli RSN IE (Robust Security Network Information Element) třetí zprávy protokolu EAPOL v rámci čtyřfázového handshakingu zobrazeného na obr. 1. V rámci tohoto volitelného kroku obě strany prokazují znalost párového Master klíče (PMK) zahešovaného do podoby identifikátoru klíče PMKID (Pairwise Master Key Identifier).

Hodnota PMKID je vypočtena zahešováním klíče PMK spolu s řetězcem znaků názvu master klíče, MAC adresy Access Pointu a MAC adresy stanice klienta:

PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)

Předchozí útoky byly založeny na odposlechu čtyřfázového handshakingu, takže útočník musel čekat na přihlášení klienta, mít k dispozici nástroj pro odposlech jeho komunikace se serverem a být vhodně dislokován pro jeho použití. Jens (Atom) Steube zjistil, že stačí, aby se útočník sám autentizoval, odchytil rámec EAPOL, v něm našel identifikátor klíče PMKID a z něj vyvodil klíč PMK. Pro WPA3 je útok přes PMKID bezpředmětný, protože čtyřfázovému handshakingu předchází v rámci protokolu SAE bezpečná výměna klíčů PMK podle algoritmu Diffieho-Hellmana.

Podívejme se ale na problém ze strany výrobců: musí zajistit zpětnou kompatibilitu a ne vždy mohou dělat zásadní výrobní změny ze dne na den. Na nově certifikované produkty si určitě alespoň rok počkáme.

Jaroslav Dočkal
jdockaldsm@gmail.com

Doc. Ing. Jaroslav Dočkal, CSc.

Absolvent VDU Martin a VAAZ, v současnosti vyučuje kybernetickou bezpečnost na Střední škole informatiky, poštovnictví a finančnictví. Externě přednáší na Masarykově univerzitě, je lektorem Cisco akademie a členem redakční rady DSM.

POUŽITÉ ZDROJE

[1] ATOM. New attack on WPA/WPA2 using PMKID. Dostupné z: https://hashcat.net/forum/thread-7717.html
[2] CERT-EU Security Advisory 2018-019, Aug 07. New attack on WPA/WPA2 using PMKID18 – v1.0. Dostupné z: https://cert.europa.eu/static/SecurityAdvisories/2018/CERT-EU-SA2018-019.pdf
[3] FRANKEL, S., EYDT, B., OWENS, L., SCARFONE, K. Networks: A Guide to IEEE 802.11i Establishing Wireless Robust Security. Recommendations. NIST Special Publication 800-97. February 2007. Dostupné z: https://csrc.nist.gov/publications/detail/sp/800-97/final
[4] HARKINS, D. Public Key Exchange. draft-harkins-pkex-05, January 24, 2018. Dostupné z: https://tools.ietf.org/html/draft-harkins-pkex-05
[5] HARKINS, D., KUMARI, W. Opportunistic Wireless Encryption. RFC 8110, March 2017. Dostupné z: https://tools.ietf.org/html/rfc8110
[6] LANCRENON, J., ŠKROBOT, M. On the Provable Security of the Dragonfly Protocol. In: Lopez, J., Mitchell, C. J. (eds.) Information Security – 18th International Conference, ISC 2015, Trondheim, Norway, September 9–11, 2015, Proceedings. LNCS, vol. 9290, pp. 244–261. Springer (2015)
[7] MD AHMAD, S. WPA Too! Dostupné z: https://www.defcon.org/images/defcon-18/dc-18-presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too-WP.pdf
[8] NOVÁK, M. Odposlouchávání a prolamování Wi-Fi sítí zabezpečených pomocí WPA2. ROOT.CZ, 4. 1. 2017. Dostupné z: https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/
[9] Vanhoef, M. WPA3: A Missed Opportunity. Dostupné z: https://www.mathyvanhoef.com/2018/06/wpa3-missed-opportunity.html
[10] Wi-Fi CERTIFIED WPA. Wi-Fi Alliance. Dostupné z: https://www.wi-fi.org/discover-wi-fi/security
[11] 802.11 Tutorial. Yoe 10 June 2005. Dostupné z: https://spacehopper.org/mirrors/www.geocities.com/backgndtest/wlan_tut.html