2. Přednáška: Bezpečnostní testování bezdrátových sítí

Bezpečnost ICT 2

Zdeněk Martinásek

Vysoké učení technické v Brně
martinasek@vut.cz

2022

Informační bezpečnost

Úvod do bezpečnosti bezdrátových sítí

- **Signál přenášen volným prostorem** nejčastěji pomocí elektromagnetického vlnění (výjimečně pomocí světla v oblasti infračervené části spektra),
- stejně jako kabelové počítačové sítě dělíme bezdrátové dle dosahu WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) a WWAN (Wireless Wide Area Network),
- v kurzu se zaměřujeme na dnes nejrozšířenější WLAN a to technologii IEEE (Institute of Electrical and Electronics Engineers) **802.11** známá pod komerční zkratkou **WiFi** (Wireless Fidelity).

Úvod do bezpečnosti bezdrátových sítí

- Existuje řada rozšíření původní normy 802.11,
- obecně **cílené na rozšíření funkcionality** např. zvyšují přenosové **rychlosti** (802.11a, 802.11b, 802.11g ...), přidávají podporu v **nových frekvenčních pásmech** (802.11n) atd.,
- jedním z rozšířeních je doporučení **IEEE 802.11i**, které se komplexně zabývá zabezpečením (WPA2),
- pozn. rozdíl **autentizace** X **asociace**.

Proč bezdrátové sítě zabezpečit?

- U klasických kabelových sítí se šíří signál s přenášenou informací po jasně stanovené trase,
- u bezdrátových sítí jsou data **přenášena volným prostorem a kdokoli v dosahu sítě je může odposlechnout**,
- jinými slovy, v bezdrátových sítích nelze dostatečně omezit přístup k fyzickému médiu,
- tento negativní a podstatný nedostatek je nutné eliminovat **implementací bezpečnostních mechanizmů** (kryptografie),
- také použití systému WIPS/WIDS (Wireless Intrusion Prevention Systems) - `Kismet`.

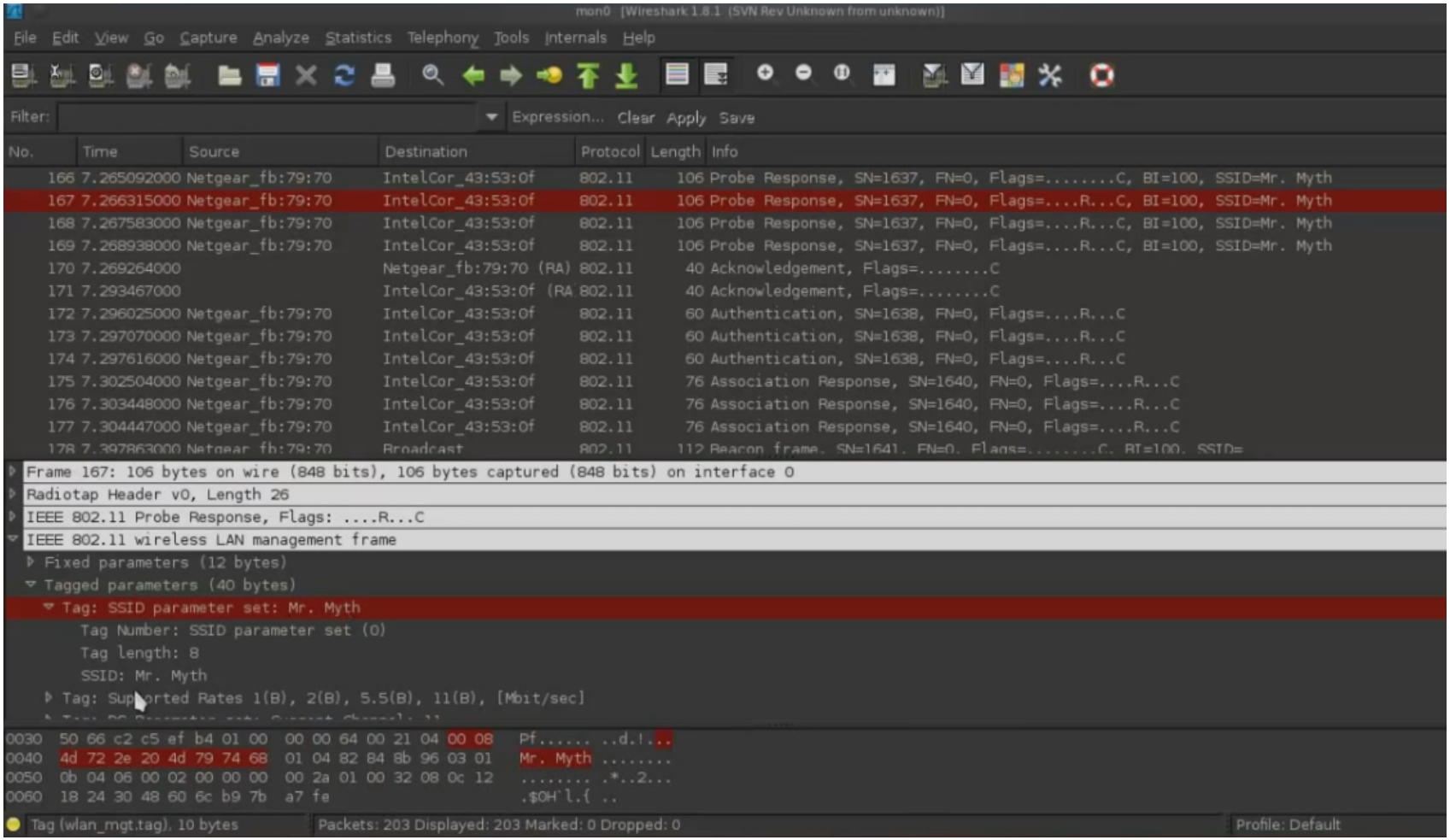
Cíle zabezpečení v bezdrátových sítích?

- Implementované kryptografické prostředky poskytují k zajištění bezpečnosti u bezdrátových sítí tyto služby:
  - **autentičnost** (authentication) - příjemce je schopen ověřit autora zprávy,
  - **důvěrnost** (confidentiality) - utajení informace před neoprávněnými uživateli,
  - **integritu dat** (integrity) - příjemce dokáže jednoznačně rozpoznat zda byla zpráva během přenosu modifikována,
  - nepopíratelnost (non-repuditation) - odesílatel nemůže popřít, že danou zprávu odeslal.

„Zabezpečení“ - skrytí SSID (Service Set Identifier)

- Jedním z jednoduchých způsobů „zabezpečení“ je skrytí identifikátoru sítě (SSID, ESSID - Extended SSID),
- předpoklad, **bez znalosti tohoto identifikátoru se do sítě nemůže nikdo připojit**,
- tento předpoklad je **velký omyl** (existuje několik způsobů),
- běžně dostupné síťové karty + software (Wireshark) stačí k odhalení SSID,
- skrytí SSID přináší uživatelům (správci) jen obtíže a NE bezpečnost.

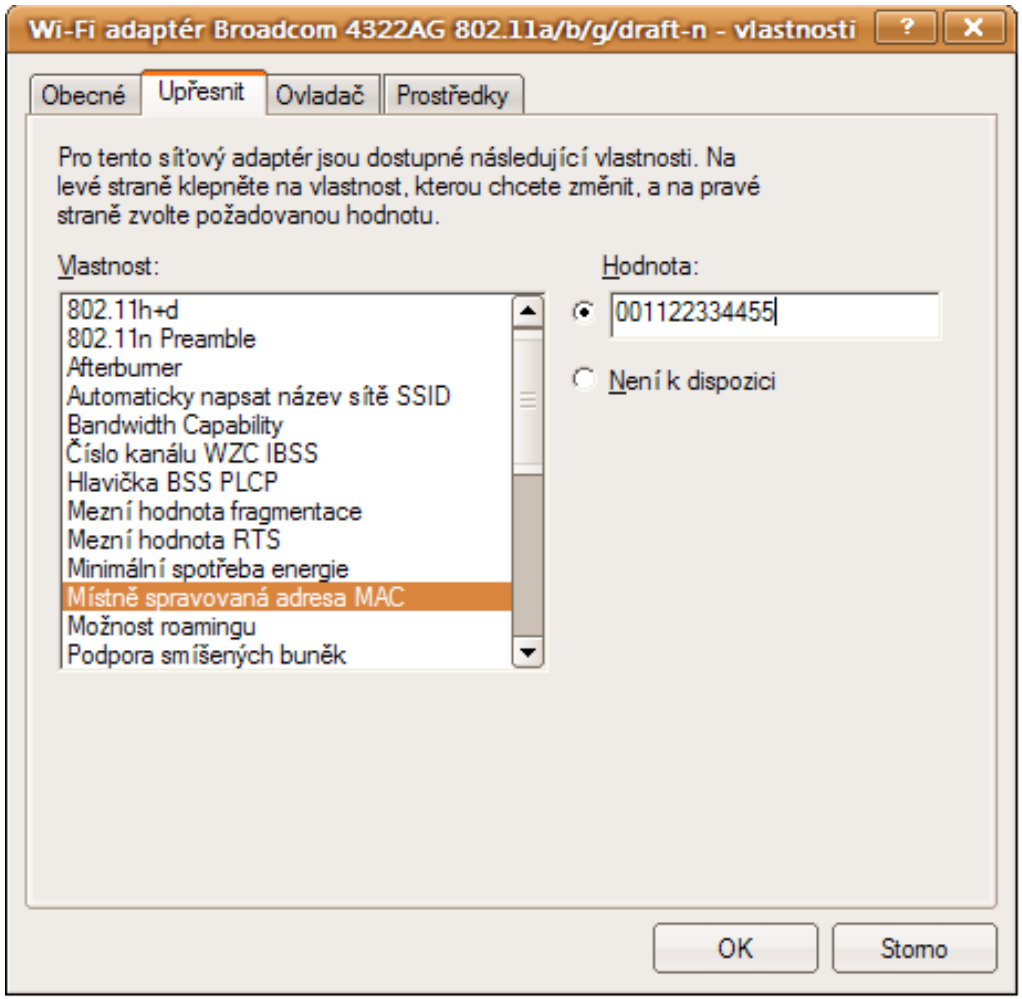
„Zabezpečení“ - skrytí SSID



„Zabezpečení“ - MAC (Media Access Control) filtr

- Dříve používaný způsob „zabezpečení“ založený na **filtrování MAC adresy klientů**,
- na AP (Access Point) je vytvořen seznam povolených MAC adres, které se smějí do sítě připojit,
- obdobně jako v předchozím případě jde tento způsob **snadno obejít** pomocí běžně dostupných síťových karet a softwarového vybavení,
- navíc **přináší nevýhody pro uživatele** (správce) při změně koncových stanic,
- praktické demonstrace viz laboratorní úlohy,
- správný způsob zabezpečení WiFi spočívá v **implementaci kryptografických mechanizmů**.

„Zabezpečení“ - MAC filtr



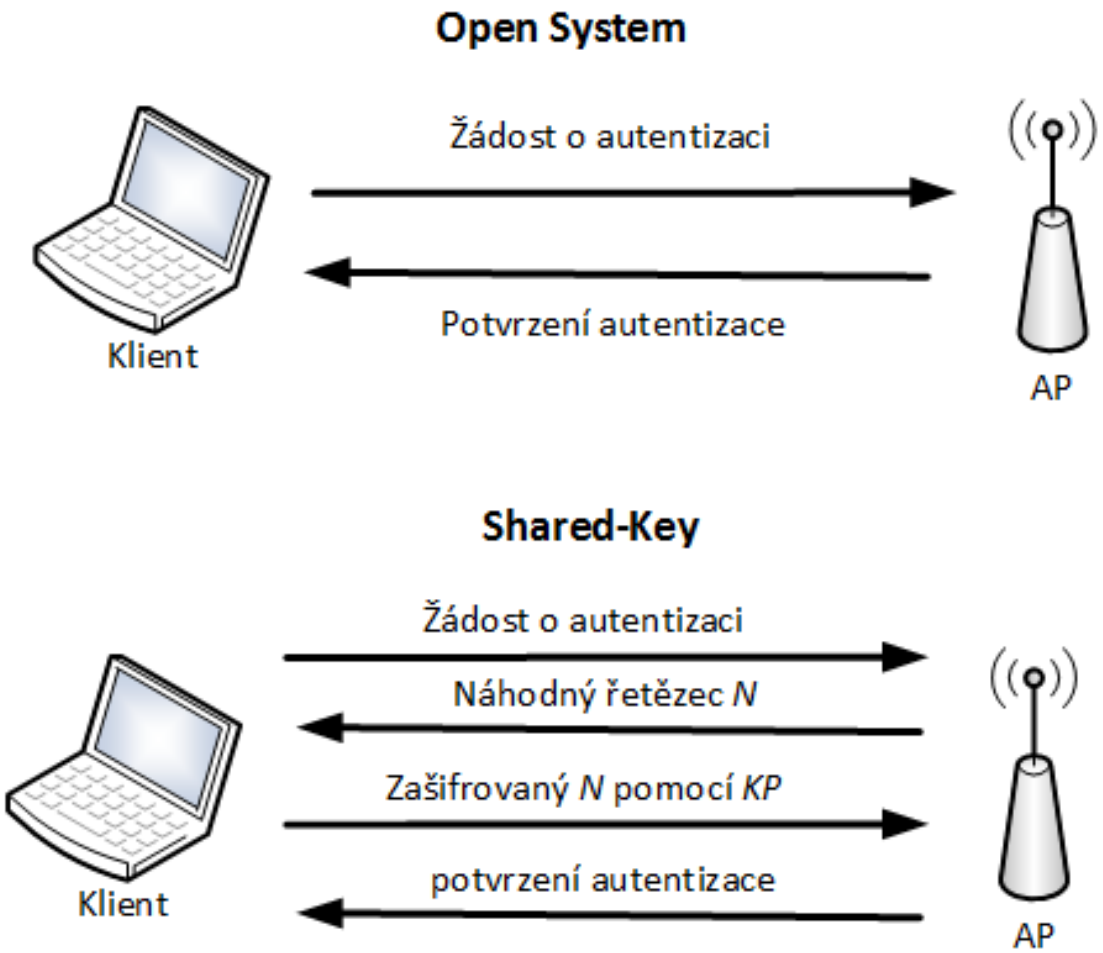
WEP - Wired Equivalent Privacy

- Protokol WEP byl prvním **volitelným** způsobem zabezpečení přítomným již v původním doporučení IEEE 802.11 [**?**],
- dle názvu měl poskytnout uživatelům bezpečnost na stejné úrovni jako v pevné LAN (metalické, optické),
- realita - **snadno prolomitelný** díky,
  - nevhodné implementaci šifrovacího algoritmu,
  - chybějícímu managementu klíčů,
  - předvídatelnosti obsahu.

WEP - autentizace

- Protokol WEP podporuje dva typy autentizace:
- **Open System** - dvoucestná výměna (2-way handshake), kdy je autentizován uživatel, který pošle požadavek na autentizaci se správně vyplněným identifikátorem sítě (SSID).
- **Shared-key** - čtyřcestnou výměna (4-way handshake), účastník odešle požadavek na autentizaci, AP v odpovědi odešle náhodně vygenerovaný řetězec, který účastník zašifruje sdíleným WEP klíčem. Následnou odpověď AP dešifruje a porovná řetězce.

WEP - autentizace



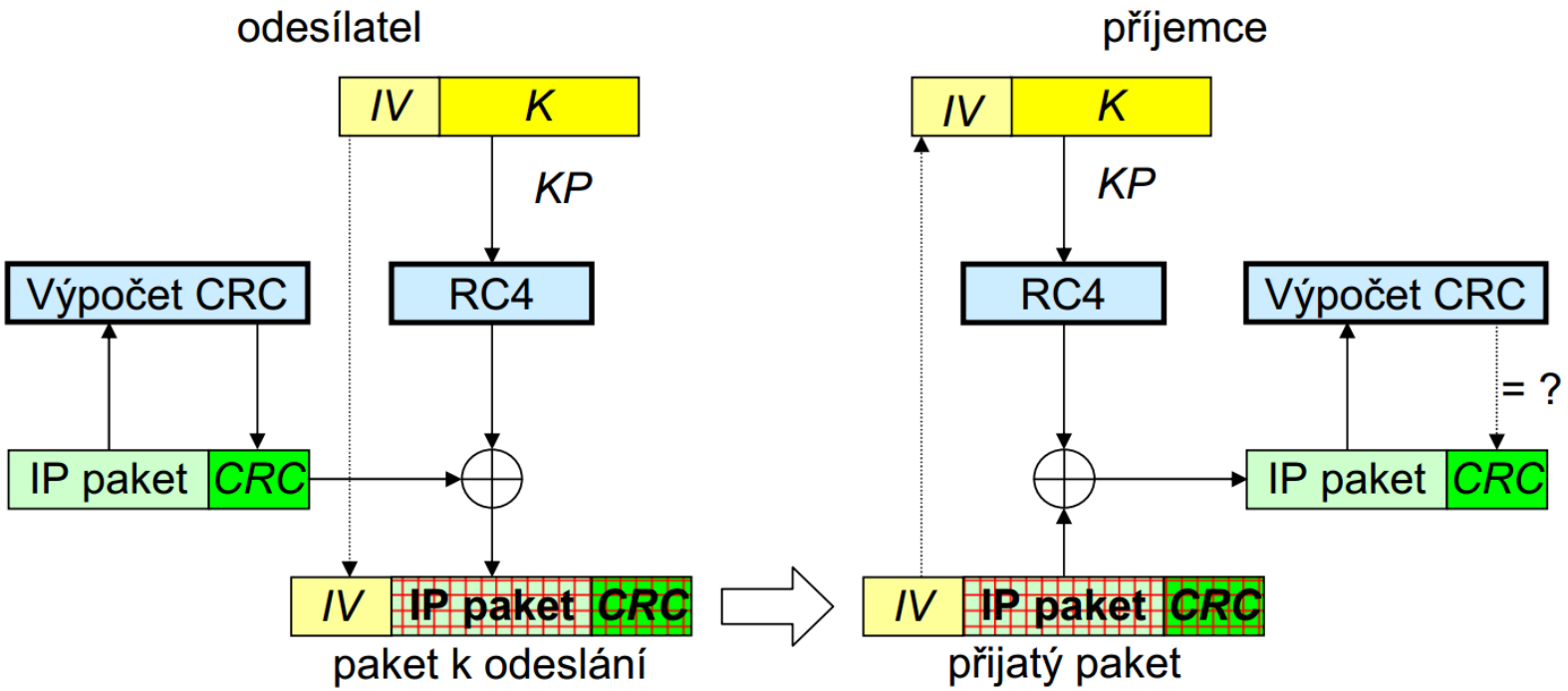
WEP - autentizace slabiny

- Autentizace **jednostraná** (pouze strana uživatele),
- prakticky je autentizováno zařízení ne uživatel (odcizení PC),
- hlavní slabinou je možnost zachycení **výzvy a odpovědi během autentizace**,
- útočník má pak k dispozici otevřený text a zašifrovaný, ze kterého určí kryptoanalýzou tajný klíč K protokolu WEP,
- ztohoto důvodu možná volba **Open system** :).

WEP - důvěrnost

- Paket je šifrován **proudovou šifrou RC4** klíčem $KP = IV||K$,
- IV (24 bitů) se generuje pro každý paket (připojeny v otevřeném tvaru, pořadí paketů),
- tajný klíč K se do stanice a AP vkládá zpravidla ručně,
- původně norma 802.11 definovala **WEP klíč délky 64 bitů s efektivní délkou 40 bitů**, protože úvodních 24 bitů tvoří IV,
- později se objevili varianty s délkou klíče 128 nebo 256 (resp. s efektivní délkou 104 a 232 bitů).

WEP - důvěrnost



[?]

WEP - důvěrnost slabiny

- Autorem algoritmu **RC4** (někdy označované jako Ron's Code) je **Ron Rivest** z RSA Laboratories,
- proudová šifra má jednoduchou strukturou, kterou lze velmi efektivně softwarově i hardwarově implementovat,
- základním požadavkem na bezpečnost: nesmí nastat situace aby **IV plus klíč (KP)** byly stejné pro dvě zprávy to je **velký problém**),
- WEP **nespecifikuje změnu IV**, délka jen 24 bitů (kombinace 2^{24}) $\longrightarrow$ porušení bezpečnostního požadavku RC4,
- klíče jsou zadávány staticky.

WEP - integrita dat

- zajištěna polem ICV (Integrity Check Value)[1],
- použito „zabezpečení“ pomocí **CRC-32** (Cyclic Reduntant Check),
- data nejsou chráněna proti **úmyslné modifikaci** (útočník modifikuje data a následně přepočítá CRC),
- CRC kódy slouží k detekci chyb vzniklých během přenosu nebo zpracování.

[1] Na obrázku znázorňující princip WEP označeno CRC.

WEP - slabiny shrnutí

- protokol WEP je odstrašující příklad **nekompletní implementace kryptografických technik**,
- klíče se vkládají ručně (statické) a neexistuje mechanismus distribuce klíčů (všechny stanice identický klíč, **všichni mohou dešifrovat**),
- efektivní délka klíče 40 bitů je **zcela nedostatečná**,
- autentizace je jednostranná (autentizuje se stanice k AP),
- při odchycení **výzvy a odpovědi lze získat klíč**,
- není specifikováno jak se generuje *IV* (opakování IV, útok lze realizovat vždy, **nutné jen odchytit dostatek dat**),
- zajištění integrity pouze pomocí CRC aj.

WPA - WiFi Protected Access

- **Mezikrok** mezi starým a nebezpečným protokolem **WEP** a zcela novým komplexním doporučením **IEEE 802.11i**,
- schvalování standardu dlouhý proces (schváleno až 2004),
- bezpečnostní rizika protokolu WEP dobře známa,
- na přelomu 20. a 21. století k masivnímu rozšiřování technologie IEEE 802.11,
- nebylo možné čekat na schválení konečného standardu,
- **říjen 2002 došlo k publikování vybraných** částí popisu zabezpečení bezdrátových sítí nazvaný WPA (3. pracovní návrhu standardu IEEE 802.11i) pod hlavičkou organizace WiFi Alliance,
- řešil největší problémy WEP při zachování **zpětné kompatibility**.

WPA - základní vlastnosti

- **autentizace** pomocí IEEE 802.1x nebo pomocí PSK (Pre-Shared Key),
- **důvěrnost** přenášených dat, šifrování pomocí protokolu TKIP (Temporal Key Integrity Protocol),
- zajištění **integrity** dat pomocí algoritmu MIC (Message Integrity Code),
- **kompatibilita** se stávajícími zařízeními (podporu WPA lze přidat pomocí upgrade firmwaru zařízení)[2],
- brát v úvahu řešení **firemní** X **osobní** (malé sítě).

[2] Výpočetní náročnost RC4 vs AES.

WPA - pracovní režimy

Režim	Wi-Fi Protected Access – WPA	
	Autentizace	**Šifrování**
Enterprise Mode (firemní mód)	802.1x / EAP	TKIP / MIC
Personal Mode (osobní mód)	PSK	TKIP / MIC

[?]

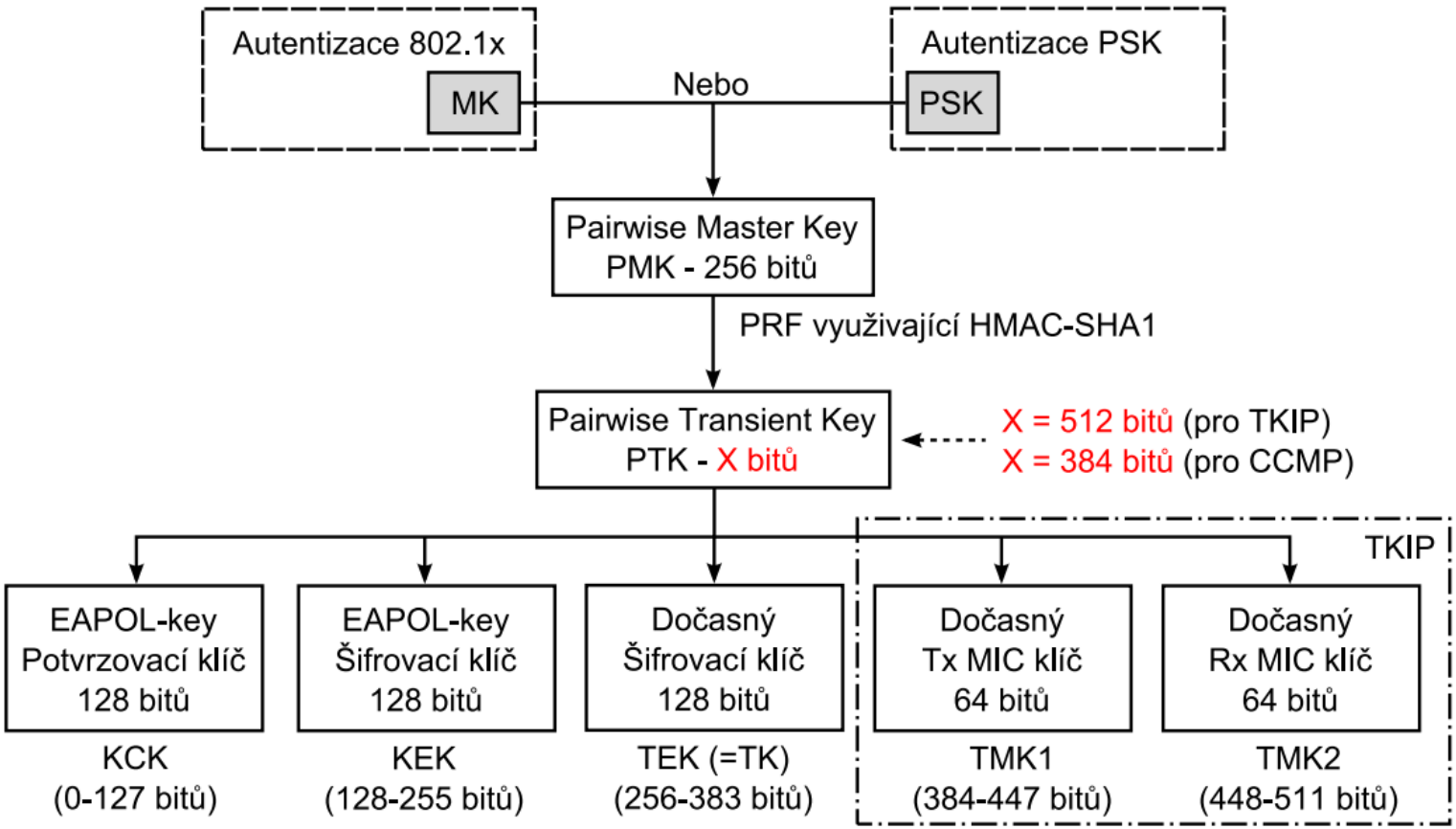
WPA - Hierarchie a distribuce klíčů

- WPA využívá několik klíčů (kolekce klíčů),
- **základem** pro klíče je **výstup úspěšné autentizace**, který je indikován získáním hlavního klíče **PMK** (Pairwise Master Key),
- získání klíče PMK je závislý na použité metodě autentizace,
  - u 802.1X je klíč získán z autentizačního serveru (odvozen z MK, Master Key),
  - u PSK platí **PMK = PSK** (viz následující text),
- další potřebné klíče jsou pak **následně derivovány z hlavního PMK** (pomocí hašovací funkce).

WPA - Hierarchie a distribuce klíčů

- PMK klíč se nikdy nepoužije k procesu šifrování nebo kontroly integrity,
- generuje se z něj dočasný šifrovací klíč PTK (Pairwise Transient Key),
  - **KCK** – (Key Confirmation Key), využití pro autentizační zprávy (MIC) během čtyřcestné výměny tzv. 4–Way Handshake,
  - **KEK** – (Key Encryption Key), využívá se k zajištění důvěrnosti dat (šifrování) během 4–Way Handshake,
  - **TK** – (Temporary Key), využívá se k šifrování dat (používaný TKIP a CCMP),
  - **TMK** – (Temporary MIC Key), určen k autentizaci dat, přičemž je využíván pouze algoritmem Michael s TKIP.

WPA - Hierarchie a distribuce klíčů



[?]

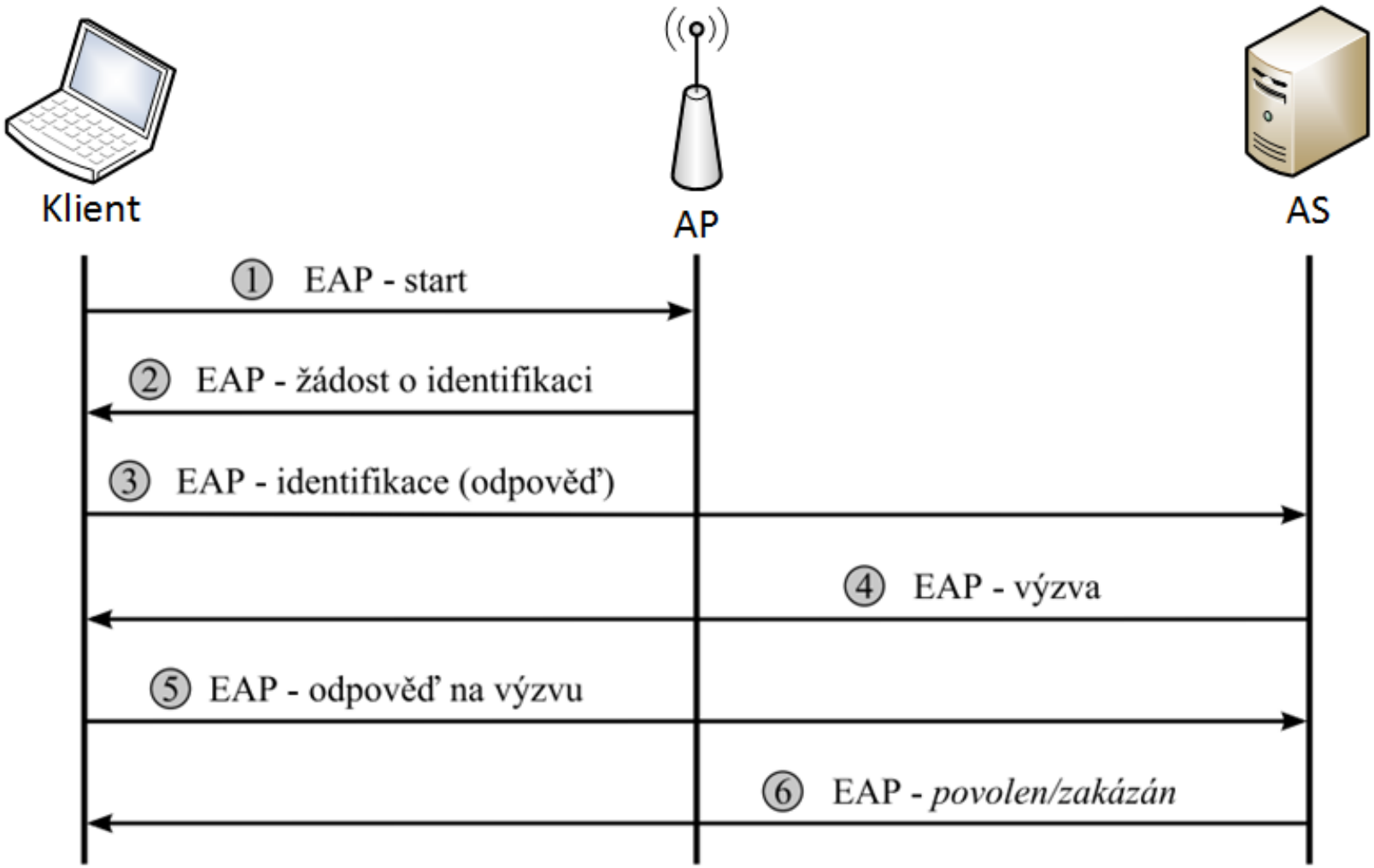
WPA - autentizace IEEE 802.1x

- 802.1x (Port Based Network Access Control) týkající se řízení přístupu do sítě **prostřednictvím autentizace na portech** [**?**],
- bezpečnostní rámec pro autentizaci **v metalických LAN**,
- nejčastěji se dnes používá v bezdrátových sítích WiFi,
- cílem je zamezit (blokovat) přístup do LAN, Internetu uživatelům bez patřičného oprávnění,
- vhodné pro firemní sítě (viz následující vlastnosti).

WPA - autentizace IEEE 802.1x

- Při **autentizaci AP zprostředkovává** spojení mezi **uživatelem a autentizačním serverem** AS (RADIUS nebo Kerberos),
- celkem tři entity (žadatel = uživatel, autentizátor = AP, Autentizační server = RADIUS (Remote Authentication Dial In User Service)),
- jádro 802.1x je tvořen protokolem EAP (Extensible Authentication Protokol),
- podpora EAP na všech zůčastněných entitách.

WPA - autentizace IEEE 802.1x



WPA - autentizace IEEE 802.1x

1. Posláním startovacího rámce (žadateli je umožněna pouze komunikace přes EAP, zbytek **blokován**!),
2. autentizátor pošle žadateli rámec s žádostí na identifikaci,
3. odpověď, rámec se svými identifikačními údaji,
4. na základě identifikačních údajů AS pošle výzvu,
5. žadatel odpovídá na výzvu příslušnými údaji,
6. AS ověří správnost odpovědi, následně AP přenastaví řízený port (přístup povolen X odepřen) - poz. **EAP-TLS** [3].

[3] V posledních zprávách potvrzující autentizaci je předán MK, MK = haš(PMS, SNonce, ASNonce).

WPA - autentizace PSK

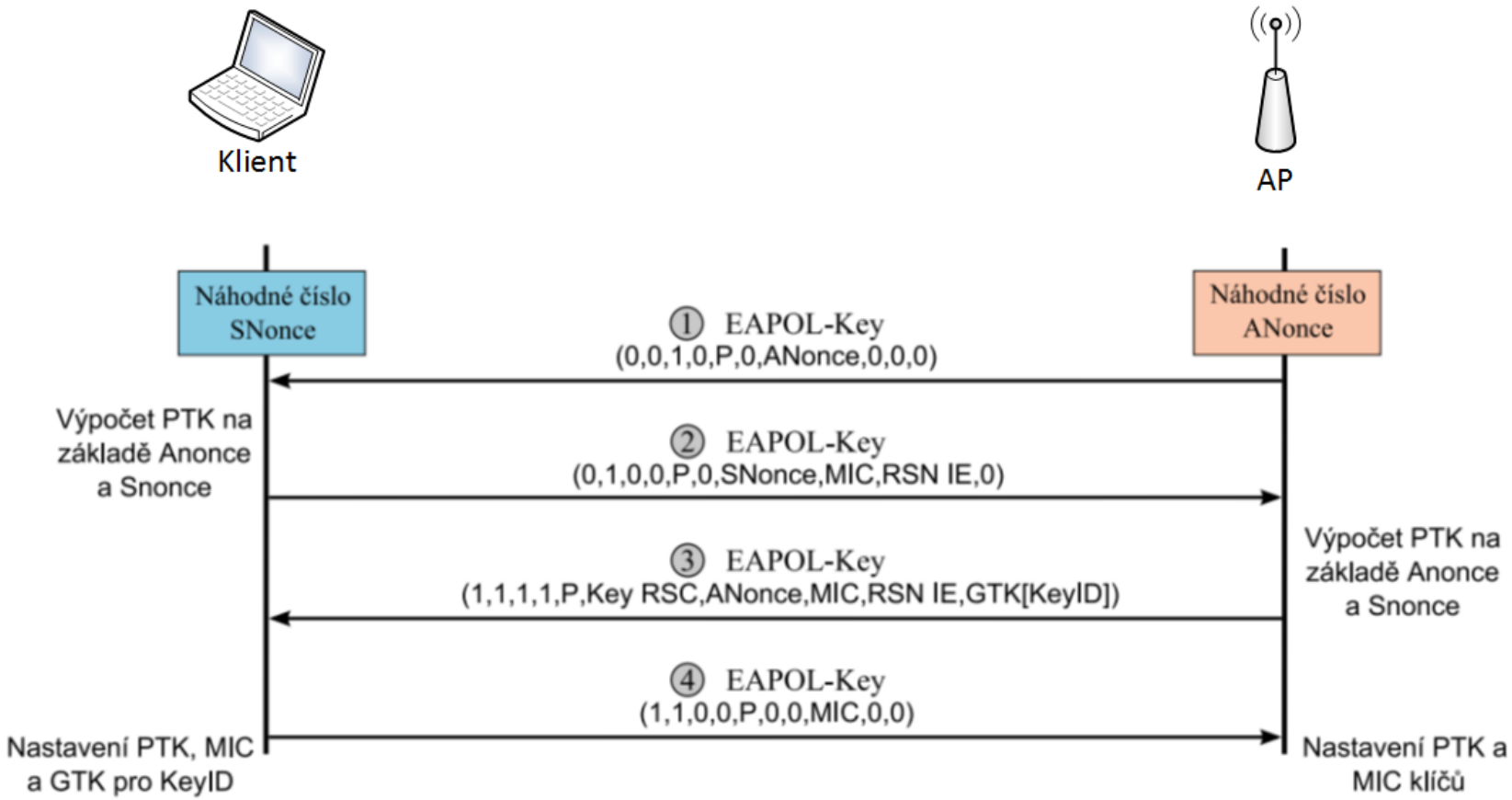
- V AP a v klientských stanicích je umístěn 256-ti bitový klíč (PSK),
- v dalších fázích protokolu má funkci **PMK** (Pairwise Master Key),
- PSK se nezadává přímo, ale místo něj se **zadá heslo** (passphrase) délky 8 až 63 znaků, které se převádí na PSK (resp. PMK) pomocí vztahu:

$$PSK = PBKDF2(passphrase, SSID, SSIDlength, 4096, 256)^{4},$$

- PBKDF2 (Password-Based Key Derivation Function) je hašovací funkce definovaná v PKCS#5 2.0 a RFC2898,
- autentizace *4–Way Handshake*.

[4] 4096 počet hašování, 256 délka výstupu

WPA - autentizace PSK, *4–Way Handshake*



WPA - autentizace PSK, *4–Way Handshake*

1. AP vygenerováno náhodné číslo ANonce, které je zasláno k žadateli (otevřeně),
2. uživatel generuje náhodné číslo SNonce, provede výpočet PSK-PTK a odvodí dočasné klíče, s využitím klíče KCK posílá k AP zprávu obsahující číslo SNonce a MIC (otevřeně), AP příjme zprávu, využije čísla SNonce k výpočtu PTK spolu s dočasnými klíči, vypočte MIC a ověří shodu (autentizace uživatele, passphrase),
3. AP zasílá klientovi zprávu s GTK zašifrované pomocí KEK, uživatel ověří MIC (autentizace AP),
4. závěrečná zpráva od uživatele k AP potvrzuje dokončení 4–Way Handshake.

WPA - TKIP obecné vlastnosti

- Protokol TKIP navržen k **řešení známých nedostatků** WEP,
- využito **proudové šifry RC4** (zpětná kompatibilita),
- implementace je více propracovaná (snížení výkonnosti přibližně o 10% - 15%),
- TKIP tvořen několika prvky, které odstraňují slabiny WEP,
  - MIC - eliminuje manipulace zprávy (nahrazení CRC),
  - IV (generování) - nedefinovaný způsob generování,
  - Mixování klíče pro každý paket - statické klíče, FMS
  - Distribuce a správa klíčů - přímé použití klíče.

WPA - TKIP - integrita dat pomocí MIC

- MIC (Message Integrity Check)[5],
- jednocestná **hašovací funkce** označovaná *Michael* [**?**],
- **kompromis mezi bezpečností a náročností** (bitové posuny a XOR),
- výstupem hašovací funkce je 64-bitový kontrolní součet MIC:

$$MIC = H(TMK, DA, SA, priorita, payload),$$

- kde H - hašovací funkce, TMK - dočasný klíč, DA/SA - cílová/zdrojová MAC adresa, priorita - rezerva, payload - datová část.

[5] U WPA a WPA2 MIC představuje o MAC (Message Authentication Code).

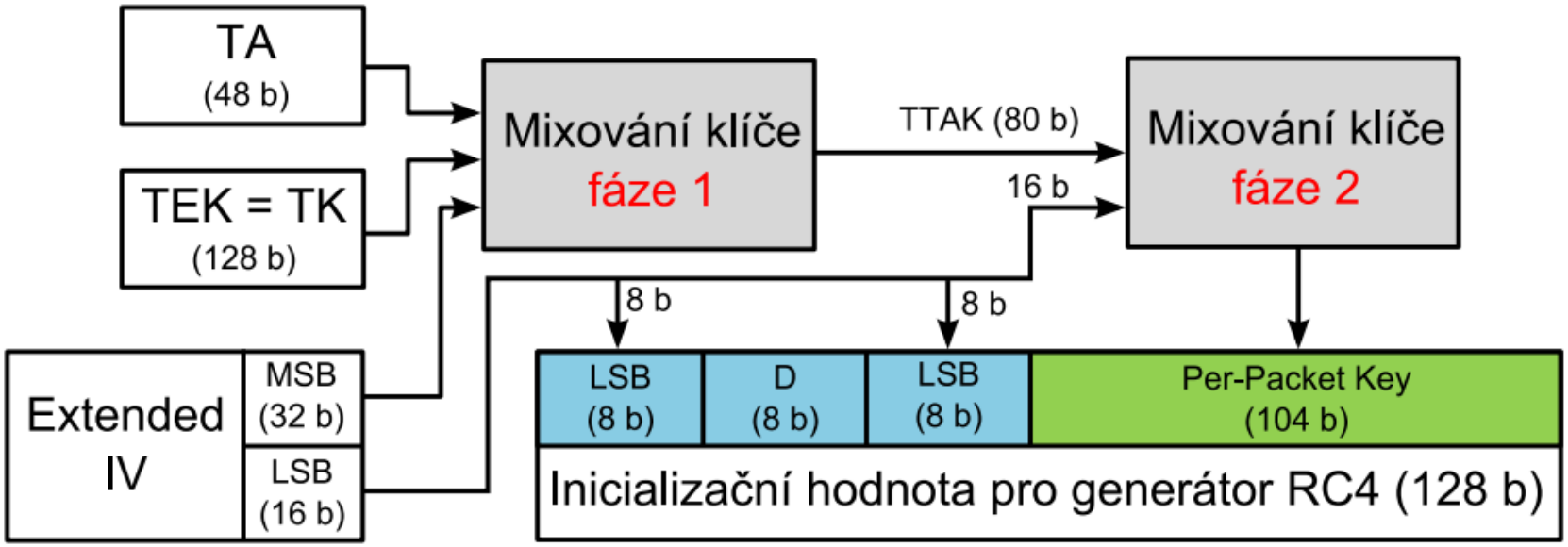
WPA - TKIP - Generování a použití IV

- prodloužený IV (ExtIV, Extended IV),
- **délka je 48b** (dvě části 16 b a 32 b),
- TKIP využívá opět mechanismu RC4 generátoru,
- IV je použit jako sekvenční čítač (TSC, TKIP Sequence Counter),
- eliminuje možnost příjmu rámce s jinou než očekávanou hodnotou.

WPA - TKIP - mixování klíčů

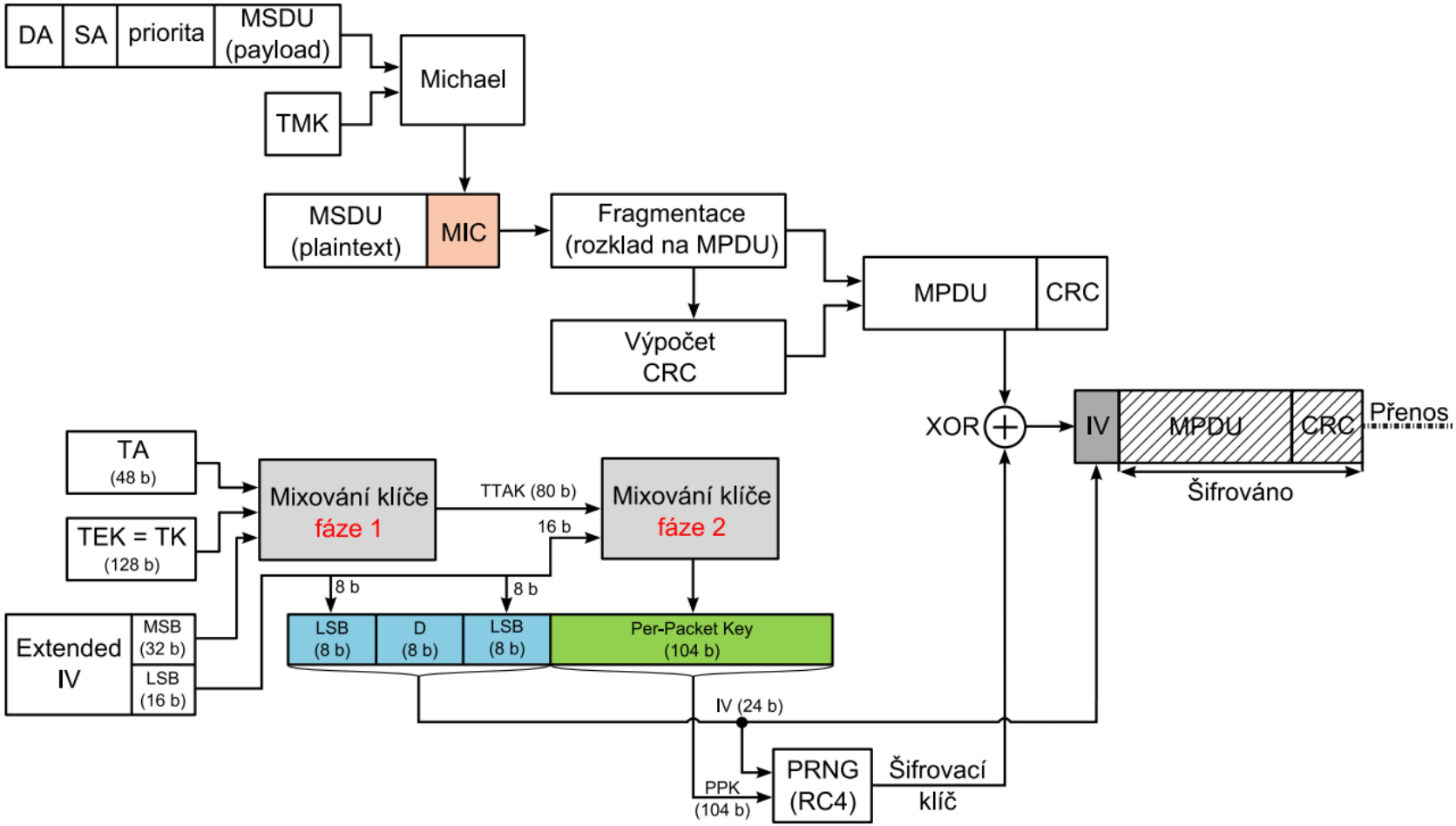
- pro každý vyslaný paket byl využit jiný šifrovací klíč (Per-Packet Key Mixing),
- v prvním kroku je promíchán 128bitov TKIP klíč s 48bitovou MAC adresou a 32 bity IV,
- v druhé fázi je k výsleku operace přimíchán opět 128 bitový TKIP klíč a zbylých 16 bitů IV,
- promíchání je realizováno nelineární substitucí (S-box).

WPA - TKIP - mixování klíčů



[?]

WPA - důvěrnost



[?]

WPA - slabiny

- Použití před-sdíleného klíče PSK lze vypočíst ze znalosti „**passphrase**“,
- po odchycení 4–Way Handshake hádáme „passphrase“ a kontrolujeme se symetrickým podpisem,
  - odchytnu NONCE, hádám heslo **PSK** $\rightarrow$ **PMK** $\rightarrow$ **PTK**,
  - následně **ověří MIC druhé zprávy**, pokud najde shodu nalezl PTK,
- pozn. přenáší se důležité hodnoty v otevřeném tvaru (první dvě zprávy NONCE),

802.11i (WPA2) - základní vlastnosti

- Komplexní zajištění informační bezpečnosti pro bezdrátové sítě (IEEE 802.11b/g/a/h/n),
- **navazuje na WPA** proto asociace Wi-Fi Alliance označuje WPA2,
- hlavní **rozdíl je v použitém šifrovacím algoritmu**,
- RC4 byla nahrazena algoritmem **AES** (Advanced Encryption Standard),
- algoritmu MIC vypuštěn, pro zajištění integrity pomocí režimu CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

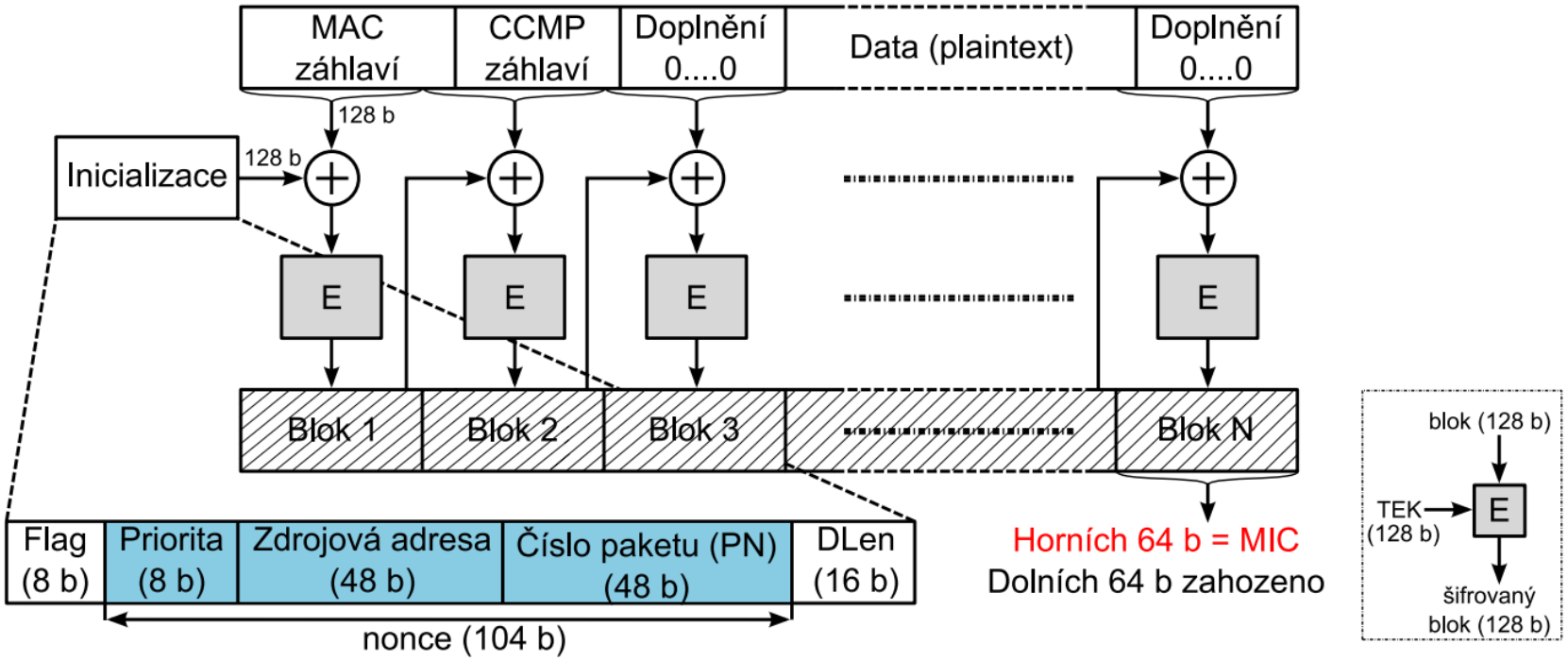
WPA2 - hierarchie a distribuce klíčů

- Hierarchie a distribuce klíčů stejná jako u WPA,
- **rozdílná je délka PTK** (paradoxně kratší),
- Pairwise Temporal Key (PTK) – KCK (128 b), KEK (128 b), TK (128 b),
- WPA2 **dva režimy** (Personal a Enterprise), pro které jsou typické příslušné autentizační mechanismy,
- **PSK** nebo **802.1x** (EAP).

WPA2 - pracovní režimy

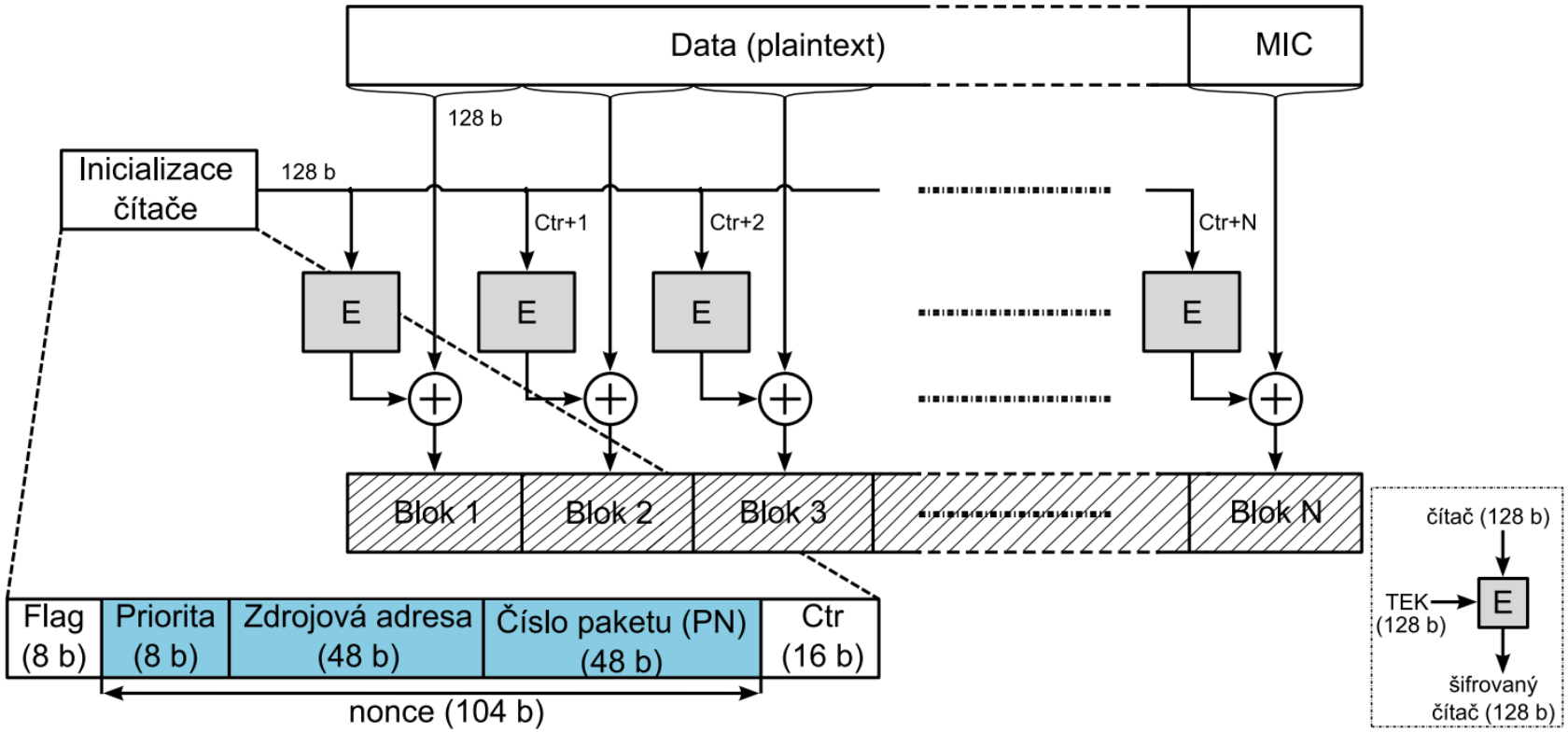
Režim	Wi-Fi Protected Access 2 – WPA2	
	Autentizace	**Šifrování**
Enterprise Mode (firemní mód)	802.1x / EAP	CCMP – AES
Personal Mode (osobní mód)	PSK	CCMP – AES

802.11i -Výpočet MIC pomocí CBC-HMAC

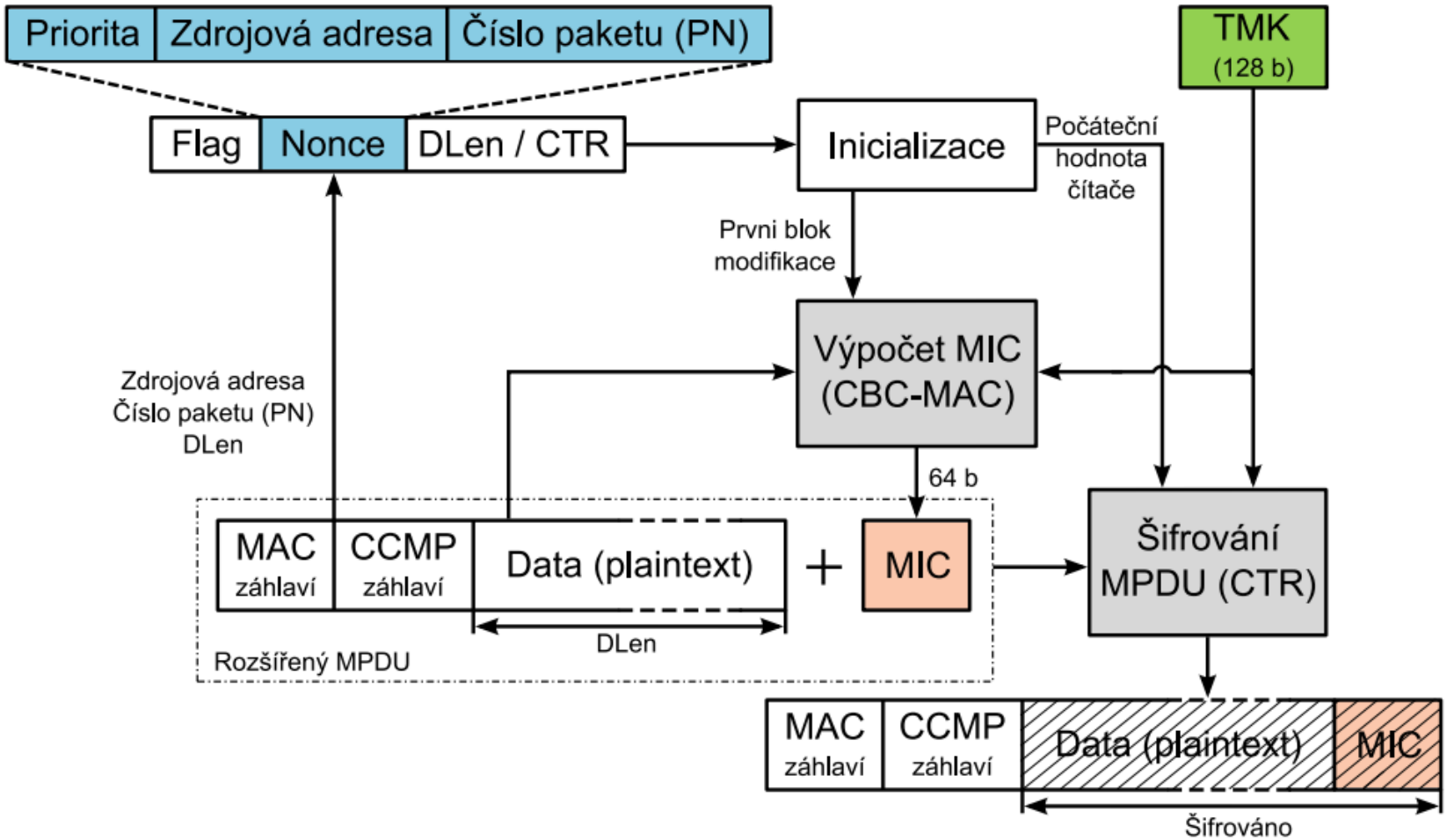


[?]

WPA2 - šifrování v CCM CTR-AES



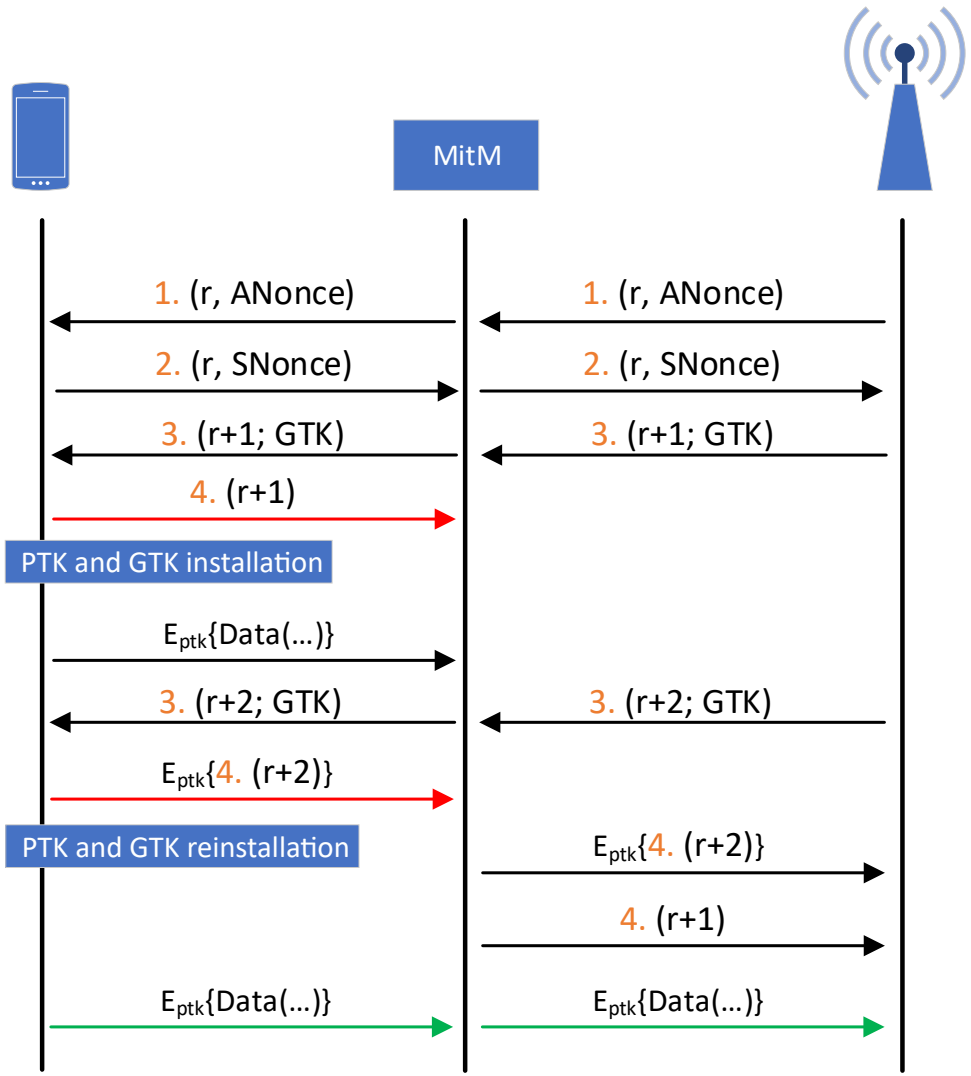
WPA2 - Zjednodušeně



WPA2 - slabiny

- **Problematika hesla** je stejná pro WPA i WPA2,
- slabina v podobě útoku na chybně zvolené heslo,
- dodržení bezpečnostních zásad tzn. volba dostatečně silného a nepředvídatelného hesla, které nepatří mezi běžně používaná hesla (slovníkové útoky),
- problem podpory WPS (Wi-Fi protected setup),
- díky jádru AES nejsou známé útoky,
- KRACK - Key Reinstallation Attack.

WPA2 - slabiny - KRACK



WPS - Wi-Fi protected setup

- Většině nových bezdrátových routerů je do firmware zapracována funkce WPS (2004),
- cíl -zjednodušit nastavení zabezpečení bezdrátové sítě,
- pokud znáte PIN (8 místné číslo), zadáte jej do klientského zařízení, to pak získá od routeru heslo k šifrované síti,
- náchylný na útoky „brute force“ - útočník zkouší veškeré možné kombinace PINu.

WPS - slabiny

- Osmičíselný kód pro útočníka představuje sto miliónů různých kombinací,
- pokud routeru pošlete špatný kód, odpoví vám, že první či druhá půlka byla správně, a tím výrazně snižuje počet potřebných kombinací.
- poslední číslo tvoří pouze kontrolní součet předchozích sedmi
- ve výsledku tak útočník musí poslat na směrovač maximálně 11 000 pokusů,
- rozlousknutí hesla je tedy v řádu hodin (3s na pokus cca 4,5 hod).

WPA3

- Nejnovější bezpečnostní standard (IEEE 802.11ac)
- Nová správa klíčů - bezpečnější SAE (Simultaneous Authentication of Equals) handshake - Handshake Dragonfly
  - Využívání eliptických křivek (ECDH, ECDSA)
  - Odolný proti slovníkovému útoku - sdílené dopředné tajemství (heslo změněno na vysoce entropický klíč)
  - WPA3 Personal 128 bit SAE, WPA3 Enterprise 192 bit SAE
- Šifrování – AES GCMP (Galois/Counter Mode Protocol)
- Dostupnost na standardech 802.11ac/ax

WPA3 - slabiny

- Dragonblood, složen z:
  - Dragonslayer: útočí proti EAP-pwd, vyžaduje pouze platné uživatelské jméno
  - Dragondrain: provádí DoS pomocí handshake
  - Dragontime: provádí časovací útok proti handshake
  - Dragonforce: experimentální nástroj, který zjišťuje heslo z postranních kanálů
- Downgrade attack - zneužití přechodového režimu (přechod na WPA2)
- Postranní kanály - časování, mezipaměť
- Zranitelnost v Braipoolových eliptických křivkách

Shrnutí

WEP	WPA	WPA2	WPA3
RC4	RC4 TKIP	AES CCMP	AES GCMP
WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
CRC-32	MIC	CBC MAC	BIP-GMAC-256
–	4-way Handshake	4-way Handshake	Dragonfly Handshake ECDH, ECDSA

Testování bezpečnosti

- WEP - útoky využívají slabinu IV
  - pasivní - pasivní odposlech komunikace (z pohledu útočníka není tak nápadný), airodump-ng
  - akrtivní - aktivní generování provozu obsahující IV (ARP dotaz) aireplay-ng (Chopchop attack, Caffe Latte attack atd.)
- WPA - útoky využívající slabé heslo
  - hádání hrubou silou (airodump-ng, aircrack-ng),
  - slovníkový útok,
  - Rainbow tables popř. GPU (hashcat) - zrychlení výpočtu hašování PBKDF2 (WPA2 sůl v podobě SSID - předpočteno pro nejvíce používané SSID) ,
  - WPS zranitelnost (reaver, pixiewps).

Testování bezpečnosti

- WPA - zmatení uživatele (SE)
  - naslouvání provozu a vytvoření falešného AP,
  - vyzrazení hesla.
- Celkové testování - automatické nástroje
  - wifite a fluxion.

Závěr

- Jak nastavit zabezpečení bezdrátové sítě?
- Osobní X firemní mód,
- filtrování a skrytí SSID nevhodné,
- dostatečná délka hesla (náhodné znaky),
- vypnutí podpory WPS.

Reference I

Děkuji za pozornost!
Dotazy ?

martinasek@feec.vutbr.cz