Bezpečnost bezdrátových sítí

Milan Radojčić

SSPŠaG – KBB

8. dubna 2026

Hlavní body

WEP

WPA

WPA2

WPA3

Hlavní body

WEP

WPA

WPA2

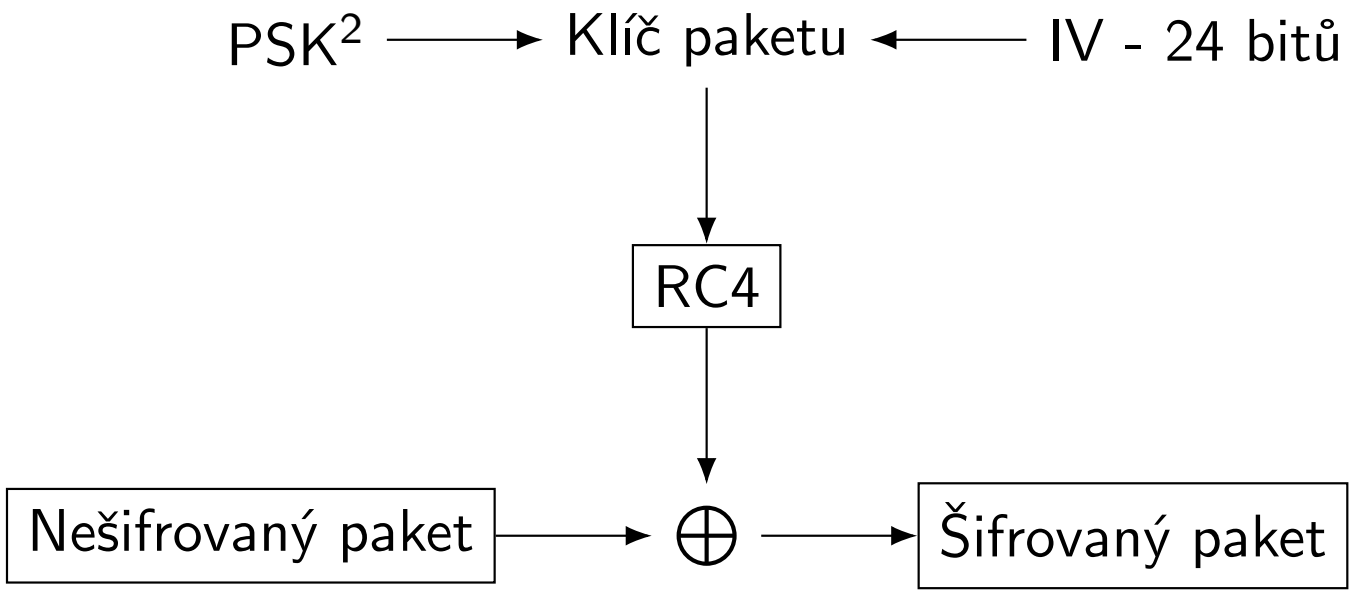
WPA3

WEP

- Standard pro zabezpečení bezdrátových sítí.
- Publikován v roce 1997.
- V roce 2001 byl prolomen.[1]

[1] Weaknesses in the Key Scheduling Algorithm of RC4 – Fluhrer; Mantin; Shamir (2001)

Šifrování paketu



[2]PSK – Pre-Shared Key = heslo

Bezpečnost WEP

- IV je moc malý (24 bitů), brzo nastanou kolize.
- Lze pomalu odchytávat provoz a statisticky odvodit klíč.
- Pomocí technik jako jsou deauth a ARP replay útoky lze vytvářet „falešnou komunikaci“, která ale bude obsahovat nové IV.

Hlavní body

WEP

WPA

WPA2

WPA3

WPA

- Přechodný standard, který opravuje některé základní chyby ve WEP.
- Problém WEP: slabá šifra a heslo přímo použito v klíči.
- K odvozování klíčů používá protokol TKIP.
  - Přidává pořadové číslo, aby nešlo replayovat pakety.
  - Šifrovací klíč je odvozen z PSK (heslo), pořadového čísla a MAC adresy.

Hlavní body

WEP

WPA

WPA2

WPA3

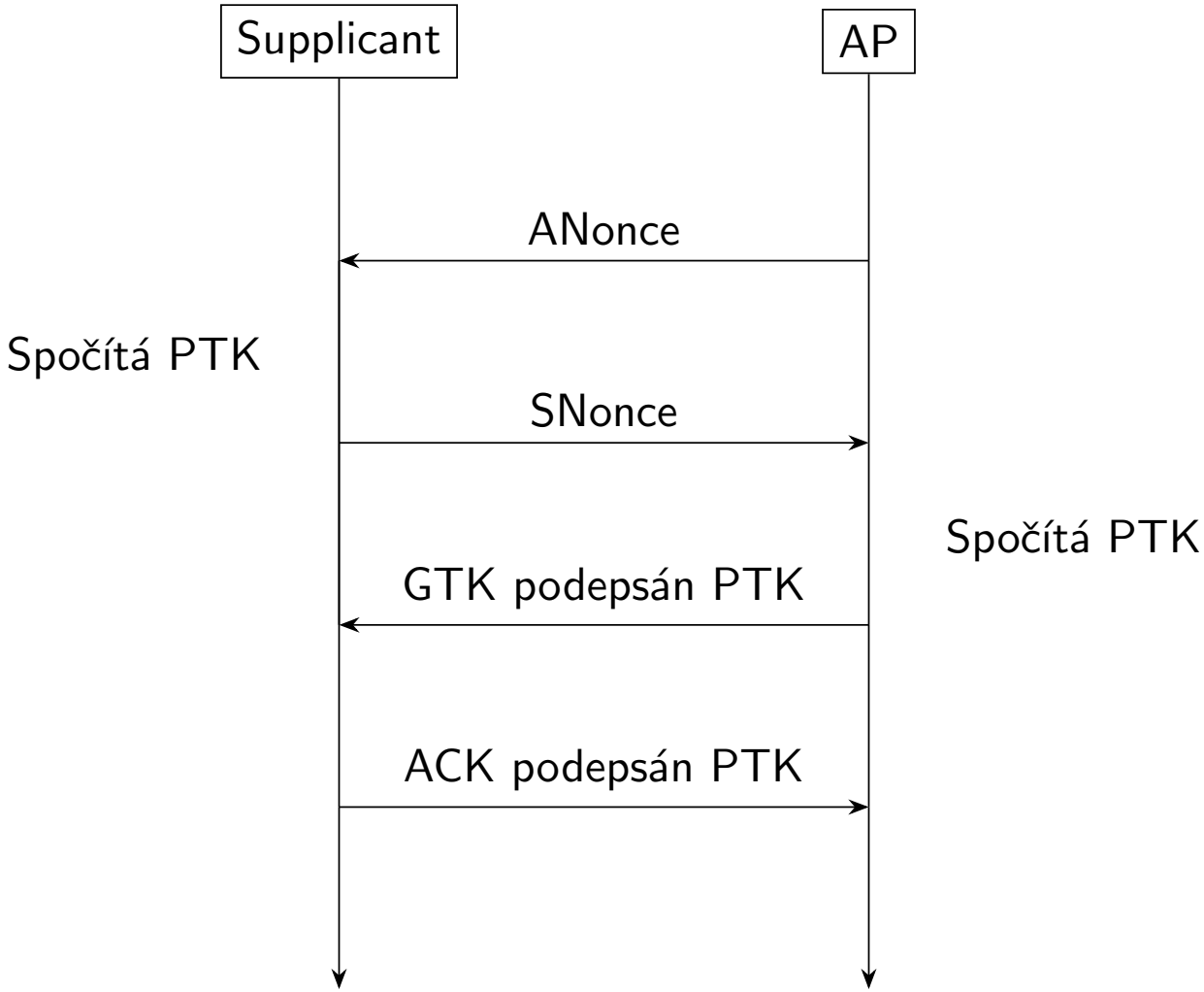
Značení a klíče

- PTK – Pairwise Transient Key
  - Používá se k šifrování.
  - Odvozuje se z PMK.
- PMK – Pairwise Master Key
- PSK – Pre-Shared Key
  - Při použití WPA2 Personal je PSK = heslo.
- KDF – Key Derivation Function
  - Bývá založená na heších.
  - V PBKDF2 bývá použitý HMAC.

WPA2

- WPA2 používá AES pro šifrování.
- Při připojení nového zařízení se provede handshake, při kterém se vytvoří PTK.
- PTK = PBKDF2(PMK, AP MAC, Supplicant MAC, ANonce, SNonce)
- PMK je odvozen z PSK.
- Při použití WPA2 Personal je PMK = PSK = heslo.

Handshake


Supplicant
AP
ANonce
Spočítá PTK
SNonce
Spočítá PTK
GTK podepsán PTK
ACK podepsán PTK

Crackování handshaku

- Při použití WPA Personal je PTK odvozen z PSK.
  - PTK = PBKDF2(PMK = heslo, AP MAC, Supplicant MAC, ANonce, SNonce)
- 3. a 4. zpráva v handshaku jsou podepsány PTK.
- Možnost odhadu PSK a porovnání s podpisem.

Hlavní body

WEP

WPA

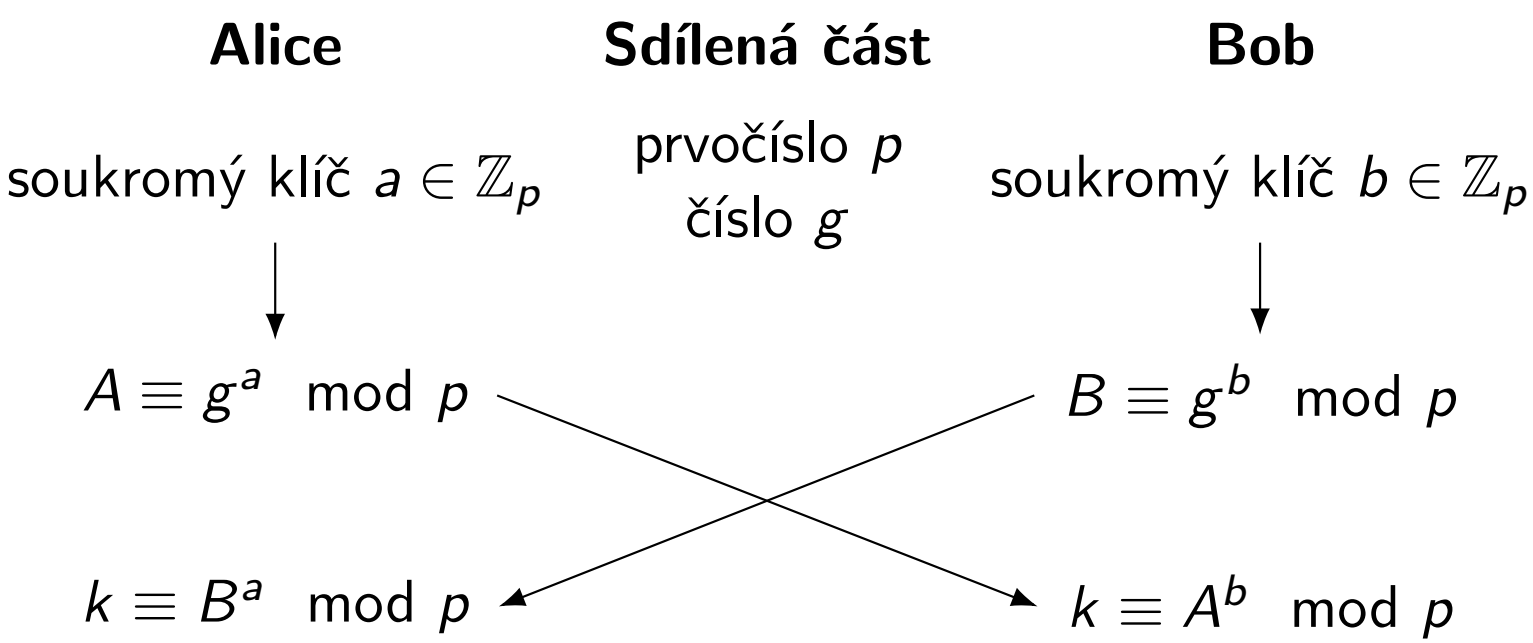
WPA2

WPA3

WPA3

- Představen v roce 2018.
- Řeší největší problém WPA2: crackování handshaků.
- Používá protokol SPEKE (Simple Password Exponential Key Exchange) ke generování klíče, který nezávisí přímo na hesle.

Opakování DHE



$$k \equiv A^b \equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv B^a \pmod{p}$$

SPEKE

1. Alice a Bob se dohodnou na prvočíslu p a hašovací funkci H. Oba předem znají sdílený klíč S.
2. Oba spočtou $g = H(S) \mod p$
3. Alice vybere náhodné číslo $a \in \mathbb{Z}_p$ a Bob náhodné číslo b.
4. Alice spočte $A = g^a \mod p$ a Bob $B = g^b \mod p$, tyto čísla si vymění.
5. Alice spočítá společný klíč jako: $k = B^a \mod p$ a Bob jako $k = A^b \mod p$.