

WPA prolomeno za 60 sekund

Vložil/a [cm3l1k1](#) [1], 7 Zář, 2009 - 13:06

- [Cracking](#) [2]
- [Encryption](#) [3]
- [Hacking](#) [4]
- [Security](#) [5]
- [WiFi & Wireless](#) [6]

Japonští "Networking nerds" vylepšily algoritmus kterým dokážou získat WPA klíč během jedné minuty.

Minulý rok v listopadu přišel Martin Beck a Erik Tews s útokem, díky kterému získali klíč během 12-15 minut, ale Japonští vědci tento nový útok pozvedli na novou úroveň.

Oba útoky jsou účinné jen v síti, kde se používá [TKIP \(Temporal Key Integrity Protocol\)](#) [7] algoritmus, takže nefunguje tam kde se používá WPA2 nebo WPA s algoritmem [AES](#) [8].

Info: <http://www.networkworld.com/news/2009/082709-new-attack-cracks-common-wi...> [9]

URL článku: <https://www.security-portal.cz/clanky/wpa-prolomeno-za-60-sekund>

Odkazy:

[1] <https://www.security-portal.cz/users/cm3l1k1>

[2] <https://www.security-portal.cz/category/tagy/cracking>

[3] <https://www.security-portal.cz/category/tagy/encryption>

[4] <https://www.security-portal.cz/category/tagy/hacking>

[5] <https://www.security-portal.cz/category/tagy/security>

[6] <https://www.security-portal.cz/category/tagy/wifi-wireless>

[7] http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[8] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[9] <http://www.networkworld.com/news/2009/082709-new-attack-cracks-common-wi-fi.html>