

Forum:[Hack Forums](#)

Thread: [WPA1 and WPA2 current working HACKs](#)

MPdqz63 - July 12, 2024, 2:47 pm

Hello everyone,

what's the current working technique to penetrate a WPA1 and WPA2 ?

All I know about WPA is that you can do PMKID attack and it seems to work nowadays but is there any other technique working currently ?

KRACK is outdated isn't it ?

Thanks for clearing this fog subject !

DramaKing - July 13, 2024, 12:28 pm

(Jul 12, 2024 02:47 PM)MPdqz63 Wrote: [\[CITE\]](#) Hello everyone,

what's the current working technique to penetrate a WPA1 and WPA2 ?

All I know about WPA is that you can do PMKID attack and it seems to work nowadays but is there any other technique working currently ?

KRACK is outdated isn't it ?

Thanks for clearing this fog subject !

Sometimes PMKID is broadcast. If I remember right, it's used to authenticate during AP roaming. WPS PIN has virtually disappeared. KRACK was patched about six years ago with the introduction of WPA3. There is also no POC, and it would not be trivial to exploit. It's merely an encryption exploit, anyway.

MPdqz63 - July 14, 2024, 8:41 am

(Jul 13, 2024 12:28 PM)DramaKing Wrote: [\[CITE\]](#) Sometimes PMKID is broadcast. If I remember right, it's used to authenticate during AP roaming. WPS PIN has virtually disappeared. KRACK was patched about six years ago with the introduction of WPA3. There is also no POC, and it would not be trivial to exploit. It's merely an encryption exploit, anyway.

So the only attack available nowadays for WPA2 is the PMKID attack ?

What about WPA1 and WPA3 ?

What about social engineering attacks ?

Sorry if I ask dumb questions but I wanna be clear on the subject of WiFi hacking

DramaKing - July 14, 2024, 8:52 am

(Jul 14, 2024 08:41 AM)MPdqz63 Wrote: [\[CITE\]](#) So the only attack available nowadays for WPA2 is the PMKID attack ?

What about WPA1 and WPA3 ?

What about social engineering attacks ?

Sorry if I ask dumb questions but I wanna be clear on the subject of WiFi hacking

I assumed that capturing WPA/WPA2 handshakes went without saying. WPA3 had Dragonblood, but SAE/Dragonfly is secure.