SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

WPA2/WPA3 無線 LAN 機器に対する新たな DoS 攻撃とその効果
New DoS attacks against WPA2/WPA3 wireless LAN devices and their effects

西井 大智 * 中嶋 祥吾 † 白石 善明 † 森井 昌克 †
Daichi Nishii Shogo Nakajima Yoshiaki Shiraishi Masakatu Morii

キーワード 無線 LAN，DoS 攻撃，WPA2，WPA3

あらまし

2017 年に無線 LAN セキュリティプロトコルである WPA2 には脆弱性が発見された [1]．その後，後継プロトコルとして 2018 年に WPA3 が発表されたものの，この WPA3 に対してもが Vanhoef らによって，Dragonblood と称される攻撃方法が提案された [2]．Dragonblood は WPA3 特有の脆弱性を利用した攻撃の総称であり，ダウングレード攻撃やサイドチャネル攻撃等が提案されている．

2020 年，著者の一人ら [3] は CSA(Channel Switch Announcement) を利用して，アクセスポイントとクライアントの通信を交互に遮断・接続さることによって，一部の OS に対して，クライアント全体および特定のクライアントに対して，通信を遮断できることを示した．特に特定のクライアントのみに攻撃できることは，攻撃の発見を困難にする極めて有効な攻撃方法と考えられる．

本研究では特定のクライアントに対して，通信を遮断できるだけでなく，通信速度を制御し，著しく通信速度の低下を促し，DoS 攻撃の発見を困難，より継続性のある，かつ効果的な攻撃法を提案し，その実証を行う．実際の環境に即した実験環境を提示するとともに，改ざんビーコンによってチャネルを切り替えることによって，クライアント側の通信速度を通常の 1/10 以下に制御出来ることを示した．本攻撃方法はさらなる発見を困難にする攻撃方法であり，より継続的な攻撃を可能とすることから大きな現実的な脅威となり得る．

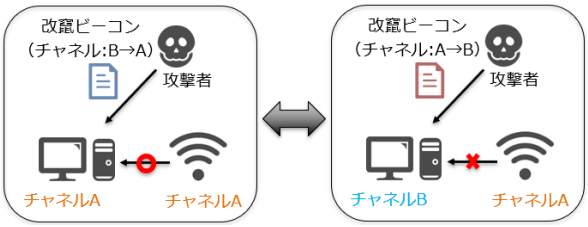

図 1: WPA2/WPA3 無線 LAN 機器に対する新たな DoS 攻撃

謝辞

本研究は，総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」 の成果である．

参考文献

[1] Mathy Vanhoef and Frank Piessens,“Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,In ACM SIGSAC CCS 2017, pp. 1313–1328. ACM, 2017.

[2] Mathy Vanhoef and Eyal Ronen.“Dragonblood: A Security Analysis of WPA3’s SAE Handshake”. IACR Cryptology ePrint Archive, p. 383, 2019.

[3] 窪田恵人，五十部孝典，森井昌克.“WPA2/WPA3 無線 LAN 機器に対する有効な DoS 攻撃とその対策”．コンピュータセキュリティシンポジウム 2020 論文集,pp. 826-831, 2020.

* 神戸大学, 兵庫県神戸市灘区六甲台町 1 − 1 , Kobe University, 1-1 Rokkodai-cho, Nada-ku, Kobe-shi, Hyogo
† 神戸大学大学院, 兵庫県神戸市灘区六甲台町 1 − 1 , Kobe University Graduate School,1-1 Rokkodai-cho, Nada-ku, Kobe-shi, Hyogo