実環境を想定したKr00kの評価実験とその改良案

窪田 恵人[1,a)]　白石 善明[1]　森井 昌克[1]

概要：2020 年，無線 LAN に対する新たな攻撃として Kr00k が提案された．Kr00k は，無線 LAN 機器が送信予定のパケットを記憶しておくバッファと，通信で用いる暗号鍵に関する仕様を悪用して一部パケットの復号が可能となる攻撃である．一部の Wi-Fi チップセットでは無線通信が切断された場合であっても，バッファ内のパケットを送信することがある．また，通信が切断されると通信に用いられる暗号鍵がクリアされ，すべて 0 となる．結果として，一部のチップセットにおいて通信が切断されると，バッファに残ったパケットがすべて 0 の暗号鍵で暗号化されて送信されることがわかった．これを利用して送信予定であったパケットの復号を試みるのが Kr00k である．この攻撃は登場して日が浅く，発見者ら以外による評価に乏しい．そこで，我々は実環境を想定したうえで Kr00k の評価実験をし，その実現可能性と影響について調査した．結果として，いくつかの端末で攻撃が成功することが確認できた．しかしながら，実際に利用される環境を想定した場合，Kr00k の実現は非常に困難であり，現実的ではない．我々は実際の利用環境に即した，攻撃難易度の低い新たな攻撃法を提案し，有効であることを実証する．本攻撃法は，Kr00k の改良となっている．

キーワード：Kr00k, 無線 LAN,IEEE802.11

Evaluation of Kr00k in the Real Environment and Its Improvements

Keito Kubota[1,a)]　Yoshiaki Shiraishi[1]　Masakatu Morii[1]

Abstract: In 2020, Kr00k was proposed as a new attack on wireless LANs, which enables a wireless LAN device to decrypt some packets by abusing a buffer that stores the packets to be sent and the specifications of the encryption key used in the communication. Some Wi-Fi chipsets may send packets in the buffer even if the wireless communication is disconnected. When the communication is disconnected, the encryption key for the communication is cleared and becomes all zero. As a result, when the communication is cut off in some chipsets, all the remaining packets in the buffer are encrypted with all zero encryption key and sent. Kr00k tries to decrypt these packets. This attack is still young and has not been evaluated well by those who did not discover it. Therefore, we conducted evaluation experiments of Kr00k under real environment to investigate its feasibility and impact. As a result, we confirmed that the attack was successful on some terminals. However, we also found that the attack is very difficult to perform in a real environment. Based on the results of the experiments, we discussed a plan to improve Kr00k to reduce the attack difficulty.

Keywords: Kr00k,Wireless LAN,IEEE802.11

1. はじめに

近年，モバイル機器の普及に加えて，リモートワークを実現する手段として，無線 LAN の需要が高まっている．しかし，データの送受信に電波を使用する Wi-Fi は盗聴が容易であり，安全なデータのやり取りには通信の暗号化が必要不可欠である．現在，Wi-Fi の暗号化方式として最も広く用いられているものが WPA2 である．

2017 年，WPA2 に対して KRACKs（Key Reinstallation AttaCKs）と呼ばれる攻撃が提案された [1]．この攻撃は WPA2 のセキュリティプロトコルの脆弱性を利用するもの

[1] 神戸大学
Kobe University
[a)] kubota@stu.kobe-u.ac.jp

であり，攻撃者は特定のパケットを遮断することで暗号化された通信を復号するヒントを得られると言われている．我々はすでに KRACKs について実環境上での実現可能性や影響について評価実験を行っている [2]．この実験の結果，KRACKs は実環境上での影響は非常に小さく，暗号化されたパケットを復号して情報を得ることは非常に難しいという結果が得られた．しかし，KRACKs の脆弱性を有するクライアントの中でも，Ubuntu など一部 OS では暗号鍵がすべて 0 になる脆弱性が見つかっていた．実験の結果，これらの OS では実環境上でもパケットの復号が容易に可能であり，早急なアップデートが必要であった．

2020 年に ESET の研究者らが Kr00k と呼ばれる，WPA2 に対する新たな攻撃を公表した．この攻撃は，KRACKs によって鍵がすべて 0 で暗号化される脆弱性について調査している中で発見されたものである．Kr00k では，一部の Wi-Fi チップセットにおいて送信予定のバッファにたまったパケットが通信切断後も送信されること，通信切断時に暗号鍵がすべて 0 にクリアされることを利用している．攻撃者はクライアントを故意に通信切断させることでバッファにたまったパケットをすべて 0 の暗号鍵で暗号化して送信させる．これらのパケットは暗号鍵がわかっていることから，攻撃者であっても容易に復号可能であるため，一部通信の傍受が可能となる．

Kr00k は今年になってから発表された攻撃であり，まだまだ実環境での評価に乏しい．無線 LAN を安全に使っていくうえでも，Kr00k を正しく評価し，実際の影響について調査することは不可欠である．我々は Kr00k の実環境上での影響について評価するために，実際に攻撃を実装して評価実験を行った．結果として，いくつかの端末では実際に攻撃が成功し，通信を復号することに成功した．本稿ではこれらの実験とその結果について紹介する．また，実験の結果から実環境上での Kr00k の実現可能性や問題点について考察を行う．最後に，これらを踏まえたうえで，実際の利用環境に即した，安定して通信を傍受するための Kr00k の改良案をいくつか提案する．

2. 予備知識

本章ではまず無線 LAN 機器における通信開始までの手続きとセキュリティプロトコルについて説明する．その後，本稿で評価実験をする Kr00k について説明する．

2.1 アクセスポイントへの接続

クライアントが無線 LAN を利用して通信を開始するためには接続手順に従ってアクセスポイントと接続しなければならない．接続手順は 3 つの手続きからなる．本節ではこれら 3 つの手続きについて説明する．また，Kr00k で利用される切断に関するフレームについても述べる．

まず最初の手続きとして，クライアントがアクセスポイントと接続するためには通信可能なアクセスポイントを見つける必要がある．これには静的スキャンと動的スキャンの 2 種類の方法がある．アクセスポイントは自分の存在を周辺のクライアントに知らせるために自分が使用しているチャネルでビーコンと呼ばれるパケットを定期的に送信している．静的スキャンでは，クライアントは様々なチャネルでビーコンを受信していくことでアクセスポイントを見つける．動的スキャンではクライアントはプローブ要求と呼ばれる呼びかけをブロードキャストで送信する．プローブ要求を受信したアクセスポイントはそのクライアントに対してプローブ応答を送信する．プローブ応答にはビーコンと同じような情報が含まれており，これによってクライアントはアクセスポイントの存在を認知する．

次にクライアントは見つけたアクセスポイントの中から接続したいアクセスポイントを選択し認証手続きに入る．現在では認証手続きは形だけのもので特に情報などは交換されない．ただし，クライアントが WPA3 を用いて通信する際は認証手続きの前に SAE ハンドシェイクによって事前共有鍵から一時的なマスター鍵を生成する．

その後，アソシエーション手続きに入る．ここでもビーコンやプローブ応答と同じような情報やさらに詳細な通信方式の情報がアクセスポイントからクライアントに送られる．接続しようとしているアクセスポイントが WPA2 を採用している場合はアソシエーション手続きの後に 4 ウェイハンドシェイクと呼ばれる鍵生成・共有プロトコルによって暗号鍵の生成と共有を行うことで接続が完了する．

ここで，上記手順はアクセスポイントとクライアントが接続するための手順であるが，何らかの理由によりアクセスポイントとクライアントが切断する場合は Deauthentication フレームや Disassociation フレームが利用される．クライアントがこれらをアクセスポイントから受信した場合，クライアントは切断に向けた処理に入り，パケットの送信を止めたうえで暗号鍵のクリアを行う．

2.2 無線 LAN のセキュリティプロトコル

無線 LAN 通信は電波を用いて通信をするため盗聴が容易である．攻撃者によって盗聴され情報が漏れることを防ぐためにも通信の暗号化が不可欠である．無線 LAN では通信の暗号化について定めたセキュリティプロトコルがいくつか存在する．現在，主に用いられているのが 2004 年に発表された WPA2（Wi-Fi Protected Access 2）である．WPA2 では接続手順のアソシエーション手続きの後に 4 ウェイハンドシェイクによって鍵の生成と共有をし，標準では AES 暗号をカウンターモードで利用して通信を暗号化する．WPA2 は発表以来安全なプロトコルとして広く利用されてきた．しかし 2017 年に KRACKs と呼ばれる 4 ウェイハンドシェイクの脆弱性を利用した攻撃が提案された [1]．我々は以前の研究で KRACKs が実環境上で大きな

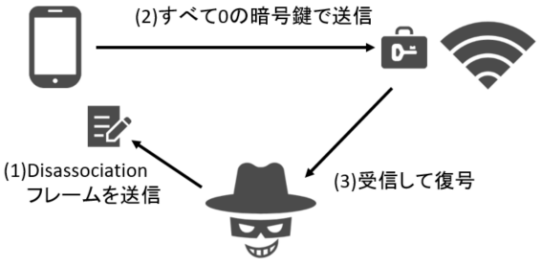

図 1　Kr00k の攻撃概要

影響を与えることは少ないということを示した [2]．ただし，Ubuntu など一部の OS では KRACKs 実行時に暗号鍵がすべて 0 になることが発見されている．この場合，攻撃者は容易に通信を復号可能であるため，アップデートを行うなどの対策が必要であった．

WPA2 ではクライアントとアクセスポイントが接続するたびに 4 ウェイハンドシェイクによる鍵生成が行われるため，同じ鍵が二度利用されることはない．また，この仕様を実現するうえで，通信時以外は通信に利用した暗号鍵を記憶しておくことはセキュリティリスクとなりうるため，多くのクライアントではアクセスポイントと切断されるたびに暗号鍵をクリアしている．

2.3　Kr00k

Kr00k は 2020 年に ESET によって発表された無線 LAN の送信バッファと暗号鍵の保存に関する脆弱性およびそれを利用した WPA2 に対する攻撃である [3]．この脆弱性は通信切断時のクライアントにおける送信バッファと暗号鍵の扱いの齟齬に由来している．2.1 節で述べた通り，アクセスポイントがクライアントと切断するとき，アクセスポイントはクライアント側に特定のパケットを送信する．ここで，本来であればクライアントはこれらのパケットを受け取った時点で送信バッファに残っている送信予定のデータを送信してはいけないはずである．しかし，一部の Wi-Fi チップセットでは切断用のパケットを受信したあとであっても，バッファ内にあるパケットを送信してしまうことが発見された．また，切断用のパケットを受信したことでクライアントは暗号鍵をクリアしてしまい，すべて 0 の鍵がセットされた状態になってしまう．結果として，アクセスポイントから切断されたクライアントはバッファ内に残っているパケットをすべて 0 の鍵で暗号化されたうえで送信される．これが Kr00k で述べられている脆弱性である．

攻撃概要を図 1 に示す．攻撃は以下の手順で行う．

(1) 攻撃者はアクセスポイントからクライアントに向けた Disassociation フレームを偽造して送信する
(2) クライアントは通信を切断し，バッファに残ったパケットをすべて 0 の鍵で暗号化して送信する
(3) 攻撃者はクライアントが送信したパケットを受信し，復号することで通信を傍受する

表 1　実験に使用した機器

攻撃者	Xubuntu(VMware)
	Wi-Fi アダプタ A
アクセスポイント	Ubuntu20.04
	Wi-Fi アダプタ A
クライアント	Raspberry Pi 3B（Raspbian June 2019）
	Raspberry Pi 3B+（Raspbian June 2019）
	ノートパソコン A（Ubuntu18.04）
	ノートパソコン B（Ubuntu18.04）
	iPhone7（iOS13.1.2）

3.　Kr00k の評価実験

我々は 2.3 節で述べた Kr00k について，実環境上での影響を評価するために，攻撃を実装したうえで実験を行った．本章ではその実験結果および考察について述べる．3.1 節では実験に用いた端末，および実験方法について説明する．3.2 節では実験結果を示す．3.3 節では実験結果をもとにした Kr00k についての考察を行う．

3.1　実験方法

攻撃に使用したツールは，チャネルベース中間者攻撃と呼ばれる無線 LAN に対する中間者攻撃を行うためのツール [4] の一部を書き換えて作成した．このツールは攻撃対象となるクライアントが接続しているアクセスポイントと同じ MAC アドレスになりすまし，任意のタイミングで偽造した Disassociation フレームを送信することができる．ツールは Xubuntu のコマンドライン上で実行可能である．

実験で使用した機器は表 1 の通りである．攻撃者は VMware 上で立ち上げた Xubuntu であり，偽造した Disassociation フレームを送信するために USB 接続の Wi-Fi アダプタ A を接続した．アクセスポイントとしては Ubuntu20.04 のホットスポット機能を使って立ち上げたものを利用した．通信用の Wi-Fi アダプタとして Wi-Fi アダプタ A を利用しており，Kr00k を再現するためにセキュリティプロトコルは WPA2 を採用した．攻撃対象のクライアントには，Kr00k の脆弱性があると公式で発表されている Raspberry Pi 3B および Raspberry Pi 3B+に加え，二種類のノートパソコンと iPhone7 を使用した．それぞれのクライアントについて，Kr00k に対するパッチが配布されているものについては，パッチを適用していない状態のもので実験を行った．

表に示した各クライアントに対して，2.3 節の手順で攻撃を行い，Disassociation フレーム送信後のクライアントから送信されたパケットを解析することで Kr00k が成功しているかを調べる．なお，パケットの解析には PCAP ファイルから暗号鍵がすべて 0 で暗号化されているパケットを抽出できるツールを利用した [5]．

表 2　結果（速度テスト時）

クライアント	攻撃
Raspberry Pi 3B	成功
Raspberry Pi 3B+	成功
ノートパソコン A	失敗
ノートパソコン B	失敗
iPhone7	成功

表 3　結果（通常の通信時）

クライアント	攻撃
Raspberry Pi 3B	失敗
Raspberry Pi 3B+	失敗
ノートパソコン A	失敗
ノートパソコン B	失敗
iPhone7	失敗

3.2　実験結果

まず，確実に送信バッファにパケットを保存させた状態での攻撃可否を調べるため，各クライアントでインターネット速度テストを利用しつつ実験を行った．本実験ではインターネット速度テストとして Google で”internet speed test”と検索することで実行可能であるものを利用した．これはクライアントとアクセスポイントの双方向からパケットを送信することで通信速度を測定するものであり，30 秒ほどで約 4.4MB のデータがやり取りされる．各クライアントがインターネット速度テストを実行している途中で Disassociation フレームを送信し，その後のパケットを解析することで Kr00k が成功するかを調べた．

実験の結果を表 2 に示す．脆弱性があると言われていた Raspberry Pi に加え，iPhone7 でも攻撃に成功した．これらの端末では何度攻撃を行っても，平均 2,3 個のパケットが通信切断後にすべて 0 の暗号鍵で暗号化されて送信されていた．なお，これらの端末は現在ではパッチによる対策がなされており，最新状態にアップデートすることで攻撃を防ぐことができる．ノートパソコン A およびノートパソコン B では攻撃に失敗した．これらの端末では通信切断後にパケットが送信されておらず，そもそも Kr00k の脆弱性が存在していなかったと考えられる．以上の結果から，新たに iPhone7 が Kr00k の脆弱性を有していたことがわかり，脆弱性を有している端末では攻撃に成功すれば容易に一部通信を復号できることがわかった．

次に，より実環境に近い環境での攻撃評価を行うために，各クライアントで普段想定されるようなペースでウェブサイトを移動しつつ適当なタイミングで Kr00k をすることで復号可能なパケットが受信できるかを調べた．各クライアントで任意のサイトからページ内のリンクを使った別のページへの移動を繰り返し，その途中で Disassociation フレームを送信し，通信切断後のパケットを観測した．

実験の結果を表 3 に示す．インターネット速度テストを利用した実験で成功した端末も含め，実験で用いたすべての端末で複数回実験を行っても通信切断後にパケットが送信されておらず，攻撃に失敗した．これは通常の通信においてクライアント側からアクセスポイント側に多くのパケットを送信する状況があまり多くはないため，バッファにパケットがたまったタイミングを狙って通信を切断させることがきわめて難しいためであると考えられる．

3.3　考察

3.2 節の結果から，実環境上での Kr00k の実現可能性や影響について考察する．まず，実験の結果からクライアントがアクセスポイントに向けて大量のパケットを送信するような状況であれば Kr00k は容易に成功するが，一般的な通信時ではバッファにパケットがたまっているタイミングで攻撃することが非常に難易度が高いため，実環境上での一般的な通信時に攻撃を成功させることは容易ではないと考えられる．一般的なユーザーがクライアントからアクセスポイントに向けて大量のパケットを送信するような状況はビデオ通話などのストリーミング時やアクセスポイントと接続した直後の IP 通信に関する情報を多くやり取りするときに限定される．以上より，例えばホテルやカフェといった公共の場で Kr00k を用いて通信の傍受を狙うことは非常に難しいと考えられる．しかし，必ず通信内容が流出しないという保証はなく，前述のとおりクライアント側が多くのパケットを送信するような状況では一度の攻撃で複数のパケットがすべて 0 の暗号鍵で暗号化されており，ある程度の情報を得ることができる．また，アクセスポイントと接続した直後のタイミングで攻撃を行うことで，攻撃対象のネットワークに関する情報が得られる可能性もある．以上のように重要な情報が流出する可能性ももちろん存在するため，Kr00k に対するパッチがリリースされている端末では確実にアップデートをしておくことが重要である．

4.　Kr00k の改良案

3 章の結果から，通常の通信時では送信バッファにパケットがたまったタイミングで通信切断を狙うことは難しく，Kr00k の実現可能性は低いことがわかった．そこで，我々は他の無線 LAN に対する攻撃と組み合わせることで送信バッファにパケットをためさせ，復号可能なすべて 0 の暗号鍵で暗号化されたパケットの送信を狙いやすくする改良案について考察した．これらの改良案によって，アップデートをしておらず脆弱性を有している端末に対してではあるが，攻撃の実現可能性を上昇させ，より大きな影響を与えることができると考えられる．本章では改良案について，利用する攻撃とそれを用いた攻撃手法を説明する．4.1 節では無線 LAN に対するジャミングを利用した手法について述べる．4.2 節では無線 LAN に対する中間者攻撃を利用した手法について述べる．4.3 節では Channel Switch Announcement（CSA）と呼ばれる信号による DoS 攻撃を利用した手法について述べる．4.4 節では 3 つの方法について比較していく．

4.1　Continuous Jamming を用いる手法

4.1.1　Continuous Jamming

Continuous Jamming は 2014 年に Vanhoef らによって提案された無線 LAN に対するジャミング手法である [6].

この手法では無線 LAN における衝突回避のプロトコルである CSMA/CA の仕様を悪用することでジャミングを行う．無線 LAN 機器は通信開始前に同一チャネル上に現在通信している端末が他にいないかを確認し，他に通信している端末がいない場合に限りランダム時間だけ待機した後にデータを送信する仕様となっている．この手順の間に他端末からのデータ送信を検知した場合はデータ送信を中止して待機状態に遷移する．Continuous Jamming において攻撃者は攻撃対象とするチャネル上で Wi-Fi アダプタを利用してランダムなデータを送信し続ける．この際，通常であれば利用される Ack や衝突回避などをすべて無効化することでほぼ確実に攻撃者がデータを送信できるようにしてある．正規端末は攻撃者のランダムなデータが同一チャネルに流れていることから CSMA/CA によって衝突回避を行う．結果として，正規端末はほとんどデータ送信ができなくなり，ジャミングされた状態となる．

4.1.2 改良案

Continuous Jamming を用いることで攻撃者は任意のチャネルのクライアントの通信を大幅に制限することができる．したがって，クライアントは送信したいパケットがあった際にも，通常の通信時のようにすぐに送信することができず，送信予定のパケットが送信バッファにたまるようになると考えられる．すなわち，クライアントからアクセスポイントに対して常時多くのパケットを送信するような状況でなくともクライアントのバッファをためさせることができ，ここで Disassociation フレームを送信することで，攻撃者はより高い確率ですべて 0 の鍵で暗号化されたパケットを送信させることができるようになる．この手法は従来の Kr00k に Wi-Fi アダプタを追加するだけで比較的容易に実行可能であり，なおかつ攻撃の成功確率を大幅に上げて実現可能性が上昇すると考えられるので，Kr00k に対する改良案として有効であると考えられる．

4.2 チャネルベース中間者攻撃を用いる手法

4.2.1 チャネルベース中間者攻撃

チャネルベース中間者攻撃は Wi-Fi 機器に対する中間者攻撃の一種として，2014 年に Vanhoef らによって提案された [6]．中間者となることで攻撃者は通信の遮断や改ざん，また再送が可能になる．

まず，攻撃者は攻撃対象となる正規のアクセスポイントのチャネルをジャミングする．クライアントはジャミングによってビーコンやプローブ応答などを遮断され，正規のアクセスポイントの情報を得ることができなくなる．さらに，攻撃者は正規のアクセスポイントの代わりに同じ MAC アドレス，SSID でチャネルのみ異なる不正アクセスポイントを設置してビーコンを送信し，クライアントのプローブ要求に答える．その結果，クライアントが正規のアクセスポイントに接続しようとすると，意図せず攻撃者が設置した不正アクセスポイントに接続してしまうことになる．その後，攻撃者は妨害を停止して正規のアクセスポイントと接続し，双方からのパケットを転送することで中間者になることができる．

また，2018 年には Vanhoef らによってジャミングの代わりに CSA と呼ばれるチャネルを切り替えさせる信号を利用した新たな中間者攻撃の手法も提案されている [7]．

4.2.2 改良案

チャネルベース中間者攻撃を行うことで，クライアントとアクセスポイントの間の通信を遮断したり遅らせることが可能となる．これを利用して，まず攻撃対象となるクライアントに対してチャネルベース中間者攻撃を行い，クライアントからアクセスポイントに向けたパケットをあえて遮断したり，逆にアクセスポイントからクライアントに向けたパケットをいくつかためて一斉に送ることで，クライアントに送信予定のパケットを複数ためさせることができると考えられる．多くのパケットをためさせた状況を作り出し，そのタイミングで Disassociation フレームを送信することで，通常の Kr00k による攻撃に比べて成功確率を上昇させられると考えられる．

4.3 CSA を利用した DoS 攻撃を用いる手法

4.3.1 CSA を利用した DoS 攻撃

CSA はアクセスポイントがクライアントに対して通信に使用するチャネルの変更を通知する信号であり，IEEE802.11h で定義されている [8]．CSA を受け取ったクライアントはチャネルを変えて通信を続けるか別のアクセスポイントに接続するかを選択し，通信を続ける場合はアクセスポイントのチャネルが変わり次第チャネルを切り替えて通信を再開する．なお，CSA はビーコンなど特定のフレームに挿入して送信することができる．ビーコンに挿入する場合は，ビーコン自体が暗号化や改ざん検知が利用されていないため，容易に偽装可能となる．

我々は以前の研究でこの CSA を利用した DoS 攻撃を提案している [9]．攻撃の流れを以下に示す．

(1) 攻撃者はアクセスポイントからビーコンを受信し，そのビーコンに存在しないチャネルへ切り替えさせる CSA を挿入して送信する
(2) 改ざんビーコンを受け取ったクライアントは指示されたチャネルへ切り替える
(3) 攻撃者も同じチャネルに切り替え，元のチャネルへ切り替えさせる CSA を挿入したビーコンを送信する
(4) クライアントは元のチャネルに戻る
(5) 攻撃者も元のチャネルに戻り，(1) から繰り返すことでチャネルを切り替えさせ続ける

ここで，クライアントが存在しないチャネルに切り替わったときは通信不可能となるが，元のチャネルに戻ったタイミングではアクセスポイントと通信をすることが可能とな

る．したがって，この攻撃では，脆弱性を有するクライアントに対して従来の DoS 攻撃と異なり通信切断が起こらないまま通信速度を低下させることが可能となる．

4.3.2 改良案

CSA を利用した DoS 攻撃も 4.2 節のチャネルベース中間者攻撃と同じく，アクセスポイントから切断させることなくクライアントの通信をある程度遮断させることができる．したがって，クライアントは送信予定のパケットがバッファにたまる確率が高くなると考えられるため，4.2.2 節と同様に，ある程度通信を遮断させたうえで Disassociation フレームを送信することで従来の手法に比べて高い確率ですべて 0 の鍵で暗号化されたパケットを送信させることができると考えられる．

4.4 改良案に関する考察

これまでに述べた 3 つの改良案について比較していく．まず攻撃の難易度であるが，どの改良案も既存の無線 LAN に対する攻撃を利用したものであり，基本的には Wi-Fi アダプタがいくつかあれば実現可能な攻撃であるため難易度は高くない．しかし，チャネルベース中間者攻撃は途中で通信が切断して攻撃が失敗することがある．したがって安定して攻撃を実行可能であるのは他の 2 つになる．

攻撃の実現可能性に関しては Continuous Jamming を利用した手法が一番高いと考えられる．これは，他の手法がパケットの遮断によって送信したいパケットを再度バッファにためさせることを狙うのに対して，そもそも送信しようとしたパケットを送信待ちの状態でバッファにためさせることができるため，確実にパケットを送信バッファにためさせることができるためである．

最後に攻撃対象について比較する．Continuous Jamming は特定のチャネルに対する攻撃であるため，攻撃対象となるクライアントと同じチャネルで通信をしているすべての端末がジャミングの影響を受ける．これは攻撃範囲が広くなってしまい攻撃が気づかれやすくなるため短所といえる．これに対して，他の攻撃は宛先アドレスによって最初から攻撃対象を一つのクライアントに絞ることができるため，比較的攻撃に気づかれにくい．

5. むすび

本稿では，2020 年に発表された WPA2 に対する新たな攻撃である Kr00k について，実環境上での評価実験を行った．また，評価実験の結果から Kr00k の実現可能性や問題点について考察を行い，既存の無線 LAN に対する攻撃を組み合わせることで，実際の利用環境に即した，攻撃難易度をさげる改良案をいくつか提案した．

実験の結果，Kr00k に対するパッチが適用されていない状態で脆弱性がある端末ではパケットの復号が可能であることがわかった．ESET の発表では言及がなかった iPhone7 であってもパッチが当たっていない状態では復号可能であった．しかし，提案されている手法では脆弱性がある端末であったとしても，クライアントからアクセスポイントに向けて多くのパケットが送信されている状態でなければ攻撃は成功しなかった．これは送信バッファにパケットが残っているタイミングで通信を切断させることが非常に難しいからであると考えられる．すなわち，通常の通信をしている環境で Kr00k を行ったとしても攻撃が成功する確率は極めて低く，特定の環境以外では攻撃難易度は極めて高い．いずれにしても，現在では多くのクライアントで Kr00k に対するパッチがリリースされているため，各クライアントを適切にアップデートすることが重要である．

さらに，実験の結果を踏まえて，攻撃難易度を低下させるための Kr00k の改良として，クライアントの送信バッファにパケットをためさせる手法をいくつか提案した．なかでも Continuous Jamming を利用した手法では，同一チャネル内の他の端末もジャミングされるというデメリットがあるものの，攻撃対象のデータ送信を妨害することで送信バッファにパケットをためさせることができ，非常に有効な改良案である．

本稿では Kr00k の改良案に関しては考察にとどまっており，実装や評価実験は行えていない．今後，これら改良案の有効性を検証するために検証実験を進めていきたい．

謝辞

本研究は JSPS 科研費 20K11810 の助成を受けたものです．

参考文献

[1] Vanhoef, M. and Piessens, F.: “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, *ACM SIGSAC CCS 2017*, ACM, pp. 1313–1328 (2017).
[2] 窪田恵人，小家　武，船引悠生，藤堂洋介，五十部孝典，森井昌克：“実環境を想定した WPA2 に対する KRACKs の評価実験”，コンピュータセキュリティシンポジウム 2018 論文集，pp. 561–568 (2018).
[3] URL: `https://www.eset.com/int/kr00k/`.
[4] URL: `https://github.com/vanhoefm/modwifi`.
[5] URL: `https://github.com/hexway/r00kie-kr00kie`.
[6] Vanhoef, M. and Piessens, F.: “Advanced Wi-Fi attacks using commodity hardware”, *ACSAC 2014*, ACM, pp. 256–265 (2014).
[7] Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I. and Piessens, F.: “Operating Channel Validation: Preventing Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks”, *ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec , 2018*, ACM, pp. 34–39 (2018).
[8] IEEE-SA: “802.11h-2003 - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications”.
[9] 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”，暗号と情報セキュリティシンポジウム論文集 (2020).