「クラウドGPUサービスを活用した2段階EvilTwin攻撃の実装と評価」による無線セキュリティの向上を目指して

“2-Step EvilTwin Attack Using Cloud GPU Service” to Improve Wireless Security

信州大学大学院　青山 諒仁
Akihito Aoyama, Graduate School, Shinshu University
ORCID ID : https://orcid.org/ 0009-0003-9628-8351

国立情報学研究所特任准教授　鈴木 彦文
Hikofumi Suzuki, Project Associate Professor, National Institute of Informatics
ORCID ID : https://orcid.org/ 0009-0003-2467-1634

信州大学大学院准教授　岡崎 裕之
Hiroyuki Okazaki, Associate Professor, Graduate School, Shinshu University
ORCID ID : https://orcid.org/ 0009-0000-1022-361X

【紹介論文】
「クラウド GPU サービスを活用した 2 段階 EvilTwin 攻撃の実装と評価」
青山 諒仁（信州大学），鈴木 彦文（国立情報学研究所），岡崎 裕之（信州大学）
学術情報処理研究 ,vol.28,No.1,pp,23-29,2024.

1. はじめに

このたびは，機関誌「AXIES Trajectory」に論文誌「学術情報処理研究」に掲載された我々の論文について，紹介の機会を与えていただき，関係者の方々に深く感謝申し上げる．

本論文の基礎となった研究は，家庭のみならず大学などの研究機関，企業，公共の場などの様々な環境において無線 LAN を用いる機会が増えたこと，そのセキュリティについて具体的にはどのような脅威が発生するのかを検証することで，より安全な無線ネットワーク環境の構築に寄与できるのではないかという点に着想を得て開始したものである．

2. 本論文の概要

近年，公衆無線 LAN や Cityroam [1]，eduroam [2] などのローミングサービスが普及し，無線 LAN 利用機会が増加している．特に eduroam は国内 423 機関が参加し，多くの大学や高専で利用されており，学術機関以外の施設でも提供が進んでいる．このような無線 LAN の利用にはセキュリティ対策が重要であり，eduroam や Cityroam は IEEE802.1X 認証を用いた WPA2（3）-Enterprise 方式を採用している．この方式ではユーザごとに異なる認証情報を用いて RADIUS サーバで認証するため，なりすましを防ぎやすく，無線 LAN 利用権の管理も容易である．

しかし，WPA2-Enterprise 方式にはサーバ証明書の設定不備が問題として挙げられる．証明書の設定に不備があると，正規ユーザへのなりすましが可能になる．この問題を検証するため，脆弱な証明書を使った 2 段階 EvilTwin 攻撃を実験し [3]，短いパスワード長におけるパスワード解析の脆弱性が確認された．しかしながら，CPU 解析では限界があり，より長いパスワードには GPU 解析が必要であると考えられる．そこで本研究ではクラウドサービスを用いたパスワード解析と，異なるページ遷移を利用したフィッシングサイトでの攻撃実験を行い，WPA2-Enterprise の安全性，適切なパスワード設定，ユーザが注意すべき点について考察した．

3. 筆者の従来の研究

筆者らはこれまで EvilTwin 攻撃をベースとした攻撃検証環境を構築してきた．特に実際に攻撃するケースを想定し，従来研究より可搬性を重視した研究を実施してきた [3]．図 1 はその際に用いた実験装置である．

図 1 に示すように基本的な構成としてはノート PC と RaspberryPi を用いているため可搬性が高い．本論文 [4] に示したように，本研究では WPA2-Enterprise 方式に対する EvilTwin 攻撃を行うため，正規 AP に接続する認証情報が必要となる．そのため認証情報を取得しパスワード解析を行う 1 段階目，取得した認証情報

図 1　2 段階 EvilTwin 攻撃実験で実際に使用した装置 [3]

を利用する 2 段階目という 2 段階の攻撃手法を提案した．従来研究における端末構成を図 2 に示す．攻撃者の端末として RaspberryPi と，仮想環境上に Kali Linux をインストールしたノート PC を準備した．また被害者の端末としてクライアントとなる PC やスマートフォンと正規 AP を準備した．攻撃の詳細な流れを説明する．攻撃の流れを図示したものを図 3 に示す．

4. クラウドリソースを用いたEvilTwin攻撃

本研究では，サイバーキルチェーンモデル [5] に基づき，攻撃者の目的がマルウェアによる金銭要求や情報収集であると仮定し，その前段階でユーザの認証情報を”偵察”として取得することを目指すと考えた．EvilTwin 攻撃は近距離のユーザを対象とし，RaspberryPi による可搬性で様々な場所での攻撃が可能となる．本研究の攻撃手法は，2 段階 EvilTwin 攻撃にクラウドサービスの Amazon EC2 [6] を活用し，図 4 に示す端末構成で行う．また，攻撃の流れを図 5 に図示する．airgeddon を使用するため操作が簡便で，GPU を用いたパスワード解析により解析時間の短縮が可能となり，解析できるパスワードも増加する．さらに，この 2 段階攻撃により認証情報の窃取量が増え，アカウントリスト攻撃へと発展できる．改良点として，高度なフィッシングサイトを作成し，認証情報入力後に正規サイトへリダイレクトすることで，ユーザが偽サイトであると気づきにくくした．認証情報をサーバ上に保存することで，攻撃者がアカウントリストを簡単に作成できるようにした．

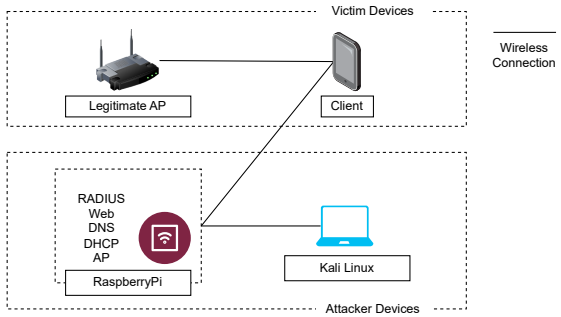

図 2　筆者の従来研究における 2 段階 EvilTwin 攻撃の概要図 [3,4]

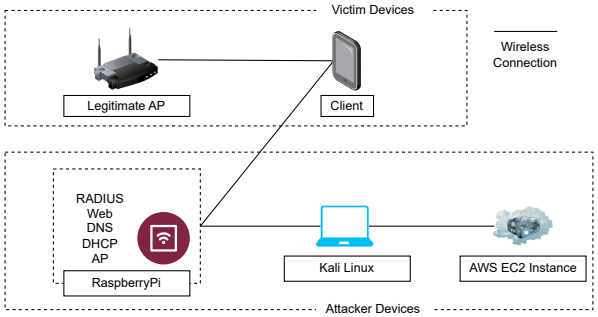

図 4　本研究における 2 段階 EvilTwin 攻撃の概要図 [4]

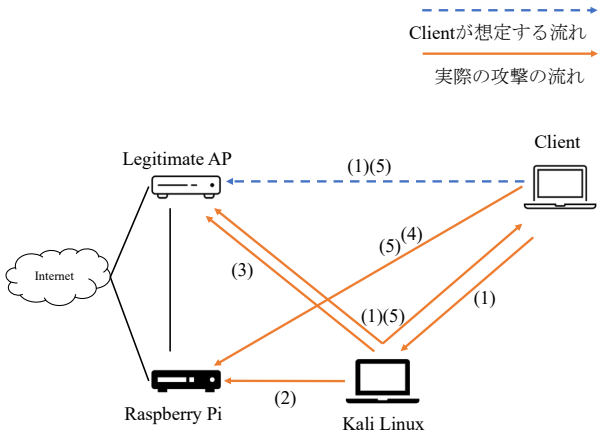

図 3　筆者の従来研究における 2 段階 EvilTwin 攻撃のフロー図 [3,4]

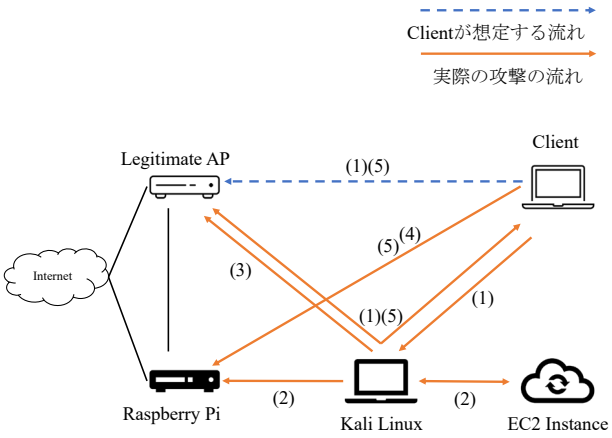

図 5　本研究における 2 段階 EvilTwin 攻撃のフロー図 [4]

5. EvilTwin攻撃結果の考察

本研究 [4] の結果の考察については，次のようにまとめられる．

まず，EvilTwin 攻撃単体について考える．公共施設や教育機関での攻撃を想定すると，ユーザの無線 LAN 利用時間は 1 時間程度あると見込まれる．その前提で考察すると，パスワード解析時間を除いた EvilTwin 攻撃自体の所要時間は 5 ～ 6 分と短く，滞在時間に対して攻撃が迅速に完了する．また，フィッシングも正常に動作していた．攻撃者がサイバーキルチェーンに沿って攻撃を行う場合には，フィッシングサイトの代わりにマルウェアをダウンロードさせる Drive-By-Download 攻撃 [7] が適用される可能性もある．本攻撃手法では可搬性に優れた RaspberryPi を利用することで，様々な環境での攻撃が考えられるが，性能面で大量のユーザを処理する際のサーバ可用性が課題となり得る．しかし一般的な AP のユーザ数であれば，どのネットワークでも本攻撃が可能と考えられる．

EvilTwin 攻撃の対策として，DoS 攻撃に用いられた Deauthentication Attack は，IDS/IPS やモニターモードを用いた検出方法 [8,9] が有効である．

次にパスワード解析について考える．本研究のパスワード解析は，従来研究と比較し，GPU を用いた hashcat によって実施した．従来は CPU で John the Ripper を使用し，5 文字解析が数分程度，6 文字解析に約 2 時間を要したが，本研究では 6 文字の解析が 10 秒程度で完了し，従来より数百倍の速度である．本実験でのパスワード解析では，パスワード長による解析時間の差はあるが，文字種による違いは見られなかった．これは，ブルートフォースによる探索が文字種によらず均等に探索を行うためと考えられる．記号なし 8 文字の解析には 20 分以上かかり，9 文字では全数探索に約 5 日かかるため，EC2 インスタンスの GPU 性能では 8 ～ 10 文字程度が解析の限界である．一般的な 10 文字以上のパスワードや記号付きには本手法が適用できないケースが多いと推測される．本攻撃手法は，ユーザ数が増えても対応可能であり，パスワード長が 8 文字以下の場合にはユーザ数の増加は影響しないと考えられる．

6. むすび

本研究では，クラウドサービスを利用したパスワード解析を用いて 2 段階 EvilTwin 攻撃の提案と実験を行い，WPA2-Enterprise 方式でも脆弱な設定ではなりすましが可能であることを確認した．ただし，適切な設定が施されていれば，この攻撃は防げることも示された．また，今後の課題として，WPA3-Enterprise の登場が挙げられる．WPA3 では Protected Management Frames（PMF）が必須となり [10]，Deauthentication Attack が困難になるため，新たな攻撃手法による安全性の検証が必要である．詳細は本稿で紹介した論文を参照されたい．このような研究を実施することで，無線 LAN におけるセキュリティが向上することを期待する．

2024 年 12 月 16 日

参考文献

[1] NGHSIG: Cityroam. https://cityroam.jp/（2024.12.03 参照）
[2] NII: eduroam. https://www.eduroam.jp/（2024.12.03 参照）
[3] 青山諒仁，鈴木彦文，岡崎裕之：WPA2-Enterprise に対する RaspberryPi を用いた 2 段階 EvilTwin 攻撃の提案. 研究報告インターネットと運用技術（IOT），第 2023-IOT-61 巻，pp. 1-7, 2023
[4] 青山諒仁，鈴木彦文，岡崎裕之：学術情報処理研究, Vol.28, pp. 1-7（2024）, DOI: 10.24669/jacn.28.1_1
[5] Lockheed Martin: Cyber kill chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html（2024.11.07 参照）.
[6] Amazon Web Services. Amazon EC2 P3 インスタンス. https://aws.amazon.com/jp/ec2/instance-types/p3/（2024.12.03 参照）.
[7] Marco Cova, Christopher Krügel, and Giovanni Vigna: Detection and analysis of drive-by-download attacks and malicious javascript code. In The Web Conference, 2010. https://api.semanticscholar.org/CorpusID:3018093（2024.12.03 参照）.
[8] Mayank Agarwal, Santosh Biswas, and Sukumar Nandi: Detection of de-authentication denial of service attack in 802.11 networks. In 2013 Annual IEEE India Conference（INDICON）, pp. 1-6. IEEE, 2013.
[9] Haitham Ameen Noman, Shahidan M Abdullah, and Haydar Imad Mohammed: An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks. International Journal of Computer Science Issues（IJCSI）, Vol. 12, No. 4, p. 107, 2015.
[10] Wi-Fi Alliance. Discover wi-fi security. https://www.wi-fi.org/discover-wi-fi/security（2024.12.03 参照）.

【著者略歴】

青山 諒仁

2023 年信州大学卒業．同年同大学大学院修士課程入学，情報セキュリティに関する研究に従事．

鈴木 彦文

1992 年信州大学工学部情報工学科卒業．1994 年同大学大学院博士前期課程修了．1997 年同大学大学院博士後期課程単位取得退学. 修士(工学)．1997 年長野工業高等専門学校 電子情報工学科助手．2003 年東京大学大学院新領域創成科学研究科基盤情報学専攻助手．2005 年信州大学総合情報処理センター准教授．2009 年信州大学総合情報センター副センター長准教授．2023 年信州大学情報基盤センター副センター長准教授．2023 年より国立情報学研究所学術基盤推進部学術基盤課学術認証推進室特任准教授，認証の高度化，ネットワーク，情報セキュリティ，情報教育，Ad-Hoc ネットワークの研究に従事．情報処理学会，電子情報通信学会，教育システム情報学会各会員．

岡崎 裕之

1999 年京都工芸繊維大学電子情報工学科卒業．2004 年京都工芸繊維大学大学工芸科学研究科博士後期課程修了．博士（工学）．2005 年信州大学大学院助手．2007 年信州大学大学院助教．2021 年より信州大学大学院准教授．情報処理安全確保支援士（登録番号 018816）. 情報セキュリティ，特に暗号理論，形式検証などの教育・研究に従事．日本応用数理学会，電子情報通信学会，日本ソフトウェア科学会，情報処理安全確保支援士会，各会員．