国際会議 ACM-WiSec2024 & WiseML2024 参加報告

櫻井　幸一 [1,*]

概要：2024 年 5 月ソウルで開催の The 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2024) と併設の The ACM Workshop on Wireless Security and Machine Learning (WiseML) 2024 の参加報告を行う。

キーワード：ワイヤレスセキュリティ, モバイルネットワーク、プライバシー、機械学習

ACM-WiSec2024 & WiseML2024 participation report

Kouichi SAKURAI [1,*]

Abstract: This reports the author's participation in the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2024) and ACM Workshop on Wireless Security and Machine Learning (WiseML) 2024, held in Seoul in May 2024.

Keywords: Wireless Security, Mobile Networks, Privacy, Machine Learning

1. はじめに

2024 年 5 月ソウルで開催された 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2024) と併設アークショップ ACM Workshop on Wireless Security and Machine Learning (WiseML) 2024 の参加報告を行う。

今年で 17 回を迎える WiSec は、アジアでは初めての開催であった。隣国ではあったが、日本からは、下名一人の参加であり、もう一人の日本人は、オランダからの発表者であった。情報提供の意味でも、下名がここに参加報告を行う。

2. 歴史

現在は、WiSec: ACM Conference on Security and Privacy in Wireless and Mobile Networks となっている。ただし、これは 2011 年の第5回以降の名称である。初回から第4回までは、WiSec: ACM Conference Wireless Network Security であった。また、初回 WiSec2008 はそれまでの三つのワークショップ

[1]ESAS (European Workshop on the Security of Ad Hoc and Sensor Networks) 2004-2006 International Conference on Wireless Internet (WICON) と併設。

[2]SASN (ACM Workshop on the Security of Ad Hoc and Sensor Networks) 2003-2006 ACM CCS と併設

[3]WiSe (ACM Workshop on Wireless Security) 2002--2006 ACM MobiCom と併設

が統合された会議としての発足であった。

また、Wisec と併設の ACM Workshop on Wireless Security and Machine Learning (WiseML)は、2019 より開催され、今回で 第6回目である。

3. 会議の運営

諮問委員会(Steering Committee)は、2024 年現在は、以下6名の構成員である

Panos Papadimitratos
(KTH Royal Institute of Technology, Sweden (chair))
Kevin R. B. Butler (University of Florida, USA)
René Mayrhofer (Johannes Kepler University Linz, Austria)
Guevara Noubir (Northeastern University, USA)
Yongdae Kim (KAIST, South Korea)
Christina Poepper (NYU Abu Dhabi, UAE)

会議運営は、ほとんどが欧米の研究者主導である。しかし、2022 年に韓国の Yongdae KIM 教授(KAIST)が PC 長を演じ、2023 年から諮問委員会に参画、2024 年には、会議長として、韓国での開催誘致に成功した結果の今回ソウル開催の WiSec2024 であった。

YouTube では、2017 年ごろからから断片的な配信があり、2020 年にはほぼ全てが online 配信されている。しかし、今回の 2024 は、会場でも録画されてはいなかったと記憶する。

4. 投稿/査読と参加状況

冒頭での PC 長からの報告がなされた。

論文投稿：25 カ国から 144 件の投稿あり

北米：53，欧州 49，アジア 27，オセアニア 5，アフリカ 2

参加者：28カ国

韓国 111 米国 26，ドイツ 7、中国 5、フランス5、(中略)、、

1 九州大学 Kyushu University
* sakurai@inf.kyushu-u.ac.jp

日本1名（下名）

投稿と査読は、2023 年より、秋と春の2回に分けて行われている。
国際会議レベル：シンガポール工科大学は J.Zhou 作成のサイバーセキュリティトップ会議ランキング一覧によると、WiSec は 19 位である（http://jianying.space/conference-ranking.html)。

5. 発表概要（その１）基調講演

基調講演二つ
Quantum Computing and TelCo Security Jean-Pierre Seifert (TU Berlin, Germany) 下名が依頼を受けて、座長した。

Agenda:
(1)A quick intro into Quantum Computing
(2) Is it interesting for the TelCo world?
(3) PQC securing the SUCI
(4) Quantum cryptanalysis of AKA (Milenage)
(5) ETSI and its view on QC

アルゴリズム MILENAGE（"mi- le-nahj"）に対する最近の量子攻撃と、それに対する ETSI からの対応する回答を紹介していた。また、通信会社の暗号化領域における"まれな"公開鍵暗号(PKC)利用についても説明し、さらに、TelCo 暗号化におけるこのようなまれな PKC の使用法に関する PQC の状況に関する意見も述べていた。後半は、WiSec2022 で発表した自身の論文[A Post-Quantum Secure Subscription Concealed Identifier for 6G]の紹介であった。

Ref[https://arxiv.org/pdf/2404.10602]
Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design

Shor と Grove の量子解読法を勘案し、共通鍵に関しては、鍵長の長い AES の安全性と、NIST 候補の公開鍵暗号系の利用とその注意点を論じていた。特に、解読技術としては、現在の量子計算機で扱える計算ビット長に加えて、エラー処理の課題を重視しての、量子計算効率の評価である。

When Wireless Protocols Meet New Threat Models, Mathy Vanhoef (KU Leuven University, *Belgium)*

スライドは [https://secappdev.org/2024/sessions/when-network-protocols-meet-new-threat-models/]より入手可能
@[https://secappdev.org/2024/speakers/]

過去の（無線）プロトコル攻撃のいくつかは、脅威モデルについて創造的に考えることによって発見されたことを論じていた。これは、KRACK や FragAttacks のような Wi-Fi 攻撃や、BEAST や HEIST のような過去の HTTPS 攻撃を事例に説明される。発表ででは、このことが防御者と攻撃者にどのようなインスピレーションを与えることができるかについても議論していた。
鍵となる主張(キーポイント):

攻撃対策は、新たな欠陥を見つけるか、
新たな脅威モデルを導入することによって、
より見通し良くなる。

6. 発表概要（その 2）Vison 講演

昨年は、Industry and Academic Collaboration in Cellular Security Research と題したパネルが行われたが、今年は Vison として、3件の講演が、毎日一つづつ行われた

Security & Privacy Issues of Electric Vehicles and Batteries
Privacy by Birth: Protecting Data from the Source in AIoT Era
Quo Vadis Bluetooth? Security by Transparency

なお、Mauro Conti の講演は Vision Talk のプログラムでは、"Security & Privacy Issues of Electric Vehicles and Batteries"となっているが、本番では"The Power and the Security of Wireless Power Charging" に変更されていた。EV へ充電する部分を Attack Surface にする着眼点が興味深いと評価できる。

7. 発表概要（その 3）一般講演と論文賞

一般講演を含むプログラムは付録(1)に付す。ここでは、特に注目したセッション 5: 攻撃（I）の２つの研究を紹介する。

Keyless Entry: Breaking and Entering eMMC RPMB with EMFI Aya Fukami 1 and Richard Buurke 2
1 University of Amsterdam, Netherlands Forensic Institution 2 Netherlands Forensic Institution
最新のストレージシステムであるリプレイ保護メモリブロック(RPMB)は、認証によってデータの整合性が確保される安全な領域を提供している。このブロックは、潜在的な攻撃者による変更から保護する必要がある重要な情報を格納するために、スマホや PC などのデジタルデバイスで使用される。本研究では、大手メーカーの 3 つの異なる eMMC における RPMB の認証方式を対象とする。実験では、ターゲットチップに電磁パルスを送ることでグリッチを注入した。RPMB 認証は正常にグリッチされ、2 つのターゲット eMMC に保存された情報は、他のデータの整合性に影響を与えることなく、任意のデータで上書きされた。発表では通信環境下でデモも行われた。
特筆すべきは、講演者の一人は、日本人である[https://orcid.org/0000-0002-6393-5888]。

続く発表は、今回の論文賞を受賞している WiFi への攻撃に関する研究であり、著者の一人は基調講演者でもある：
[Short Paper] SSID Confusion: Making Wi-Fi Clients Connect to the Wrong Network
Héloïse Gollier 1 and Mathy Vanhoef 1 (1 DistriNet, KU Leuven)

SSID の混乱： Wi-Fi クライアントを間違ったネットワークに接続させる攻撃

WPA2 や WPA3 などの保護された Wi-Fi プロトコルを使用する場合、接続するアクセス ポイントはクライアントによって認証される。これにより、敵対者が Wi-Fi ネットワークの不正なクローンを作成するのを防ぎ、SSID と呼ばれるネットワークの名前をスプーフィングできないことを意味している。しかし、この論文では、クライアントがだまされて、接続を意図したものとは異なる保護された Wi-Fi ネットワークに接続する可能性があることを示す。つまり、クライアントのユーザー インターフェイスには、接続されている実際のネットワークの SSID とは異なる SSID が表示される。根本的な原因は、IEEE 802.11 標準の設計上の欠陥であり、SSID が常に認証されるとは限らない。本研究では、この攻撃の実際的な影響を実証し、テストされたすべてのデバイスが攻撃に対して脆弱であることを発見し、下位互換性のある防御と標準の更新を提案する。

この WIFI への攻撃は、国内ベンダーでも深刻な課題であるということ。各ベンダー毎に、応急修正で対応できてはいる。しかし、互換性を考えると、規格の修正が待たれている現状にある、ということ。

8. 発表概要（その 3）ポスター＆デモ

5件のポスターと1件のデモは、初日夕方のレセプションと並行して行われた。

Five Posters
Never Gonna Give You Up: Exploring Deprecated NULL Ciphers in Commercial VoWiFi Deployments
Gabriel K. Gegenhuber1, Philipp È. Frenzel2, and Edgar Weippl1
1 University of Vienna. 2 SBA Research

Testing network-based RTK for GNSS receiver security
Marco Spanghero1 and Panos Papadimitratos1
1 KTH Royal Institute of Technology

5G Puppeteer: Chaining Hidden Command and Control Channels in 5G Core Networks
Julian Sturm1, Daniel Fraunholz1, Oliver Zeidler2, Katharina Schaar1, and Wolfgang Kellerer2
1 ZITiS. 2 Technical University of Munich

Fundamental Investigation of Speech Sound Leakage Using Optical-Vibration Analysis
Aditya Srivastava1, Long Huang1, and Chen Wang1
1 Louisiana State University

Experimentation platform for repeatable security analysis in IoT heterogeneous environments
Florent Galtier1, Paul L. R. Olivier1, Guillaume Auriol1, Romain Cayre2, and Vincent Nicomette1
1 LAAS-CNRS. 2 EURECOM

One Demos
RTKiller - controlling GNSS rovers by RTK base spoofing
Marco Spanghero1 and Panos Papadimitratos1
1 KTH Royal Institute of Technology

9. WisecML 体制

諮問委員会 Steering Committee
Dr. Wenjing Lou, *Virginia Tech*
Dr. Sennur Ulukus, *University of Maryland*
Dr. K.P. (Suba) Subbalakshmi, *Stevens Institute of Technology*
Dr. Aylin Yener, *The Ohio State University*

WS 長
Minhoe Kim Korea University Seoul, South Korea
Gihyuk Ko KAIST Daejeon, South Korea
Yalin Sagduyu Virginia Tech Blacksburg, VA, USA
Yi Shi Virginia Tech Blacksburg, VA, USA

TPC18 名は、欧米勢と韓国2名、中国一名（日本からはゼロ）

10. WiseML 基調講演

基調講演二つ
Reinforcement Learning Methods for Secure Computing
Joongheon Kim （Korea University, *Seoul, South Korea*）
強化学習の基本理論の解説、続けて、最新の計算プラットフォームにおける多様な応用を紹介していた。後半では、現在および将来のセキュア コンピューティングの観点からの議論として、量子学習系の主要成果を紹介していた。
特に講演者は、8 月開催の IJCAI ワークショップで、
1st International Workshop on Quantum Algorithms, Optimization, and Artificial Intelligence (QAI 2024)
[https://sites.google.com/view/qai2024ijcaiworkshop]
を企画(会議長(兼)プログラム長)しており、その開催も案内もしていた。

Sensing the Future: Unveiling the Benefits and Risks of Sensing in Cyber-Physical Security
Jun Han （KAIST), South Korea
講演では、センサー データを活用した IoT/CPS シナリオのセキュリティとプライバシー保護を提供する方法を紹介し、さらに、同様のセンサーデータから生じる新たなセキュリティ脅威についても紹介していた。具体的には、さまざまな IoT 設定での攻撃と防御にセンサー データを活用する最近のプロジェクトのいくつかを取り上げ、また、スマートホーム、建物、車両などの新しい分野からの予期せぬセキュリティ課題の特定と防御など、今後の研究の方向性についても議論していた。

講演者は、ACM MobiSys 2024/2022 や ACM Sensys 2021 などで、自身の成果を発表している。ちなみに、ACM MobiSys 2024(第22回) は、7 月に東京で開催され、講演者は、ワークショップ長の一人を務めて，11 ワークショップ中、5 個は ＡＩ系であった（https://www.sigmobile.org/mobisys/2024/wsl.html）

11. WiseML 一般講演

付 録 (2) https://wisec2024.kaist.ac.kr/wiseml2024/program/ https://wisec2024.kaist.ac.kr/wiseml2024/program/に記載する。

12. おわりに

次回 Wisec2025 は、ワシントン D.C で 6 月あたりでの開催を検討中とのことである（@YD KIM より)。

謝辞 準備講演を ATR は 5GBeyond プロジェクトの場で行った。頂いた質疑やコメントを参考に草案を改善できた。参加頂いた横山所長を初め、プロジェクト構成員の方に感謝する。 論文賞の WiFi 攻撃に関する現場の声は、PicoCELA 株式会社の大森洋一氏による。

付録

付録 A.1 WiSec2024 のプログラム
[https://wisec2024.kaist.ac.kr/program/]

付録 A.2 WiseML のプログラム
[https://wisec2024.kaist.ac.kr/wiseml2024/program/]