Potential Business –
IoT Risk Identification

Tego Chang

2022/08/26

Agenda

IoT Risk Identification
- Can it be a new business for the company?

Company's Strengths in IoT
- What are them?

Target Users in IoT
- Who are them?

Realize the Potential Opportunity
- Future work

Potential business?

YES

Target users?

Vendors of IoT devices and from cybersecurity (B2B2C)

Strengths?

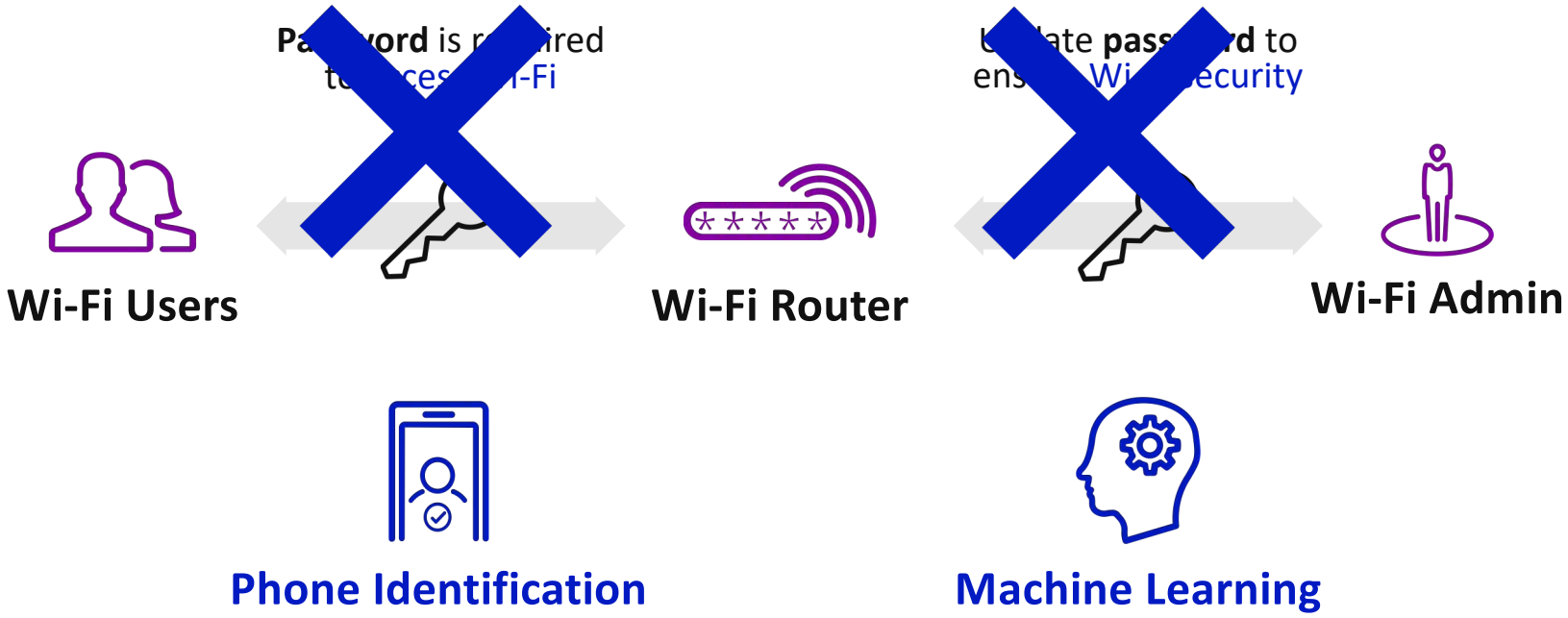
Utilization of phone (2FA) and data (Risk Prevention)

IoT Risk Identification

PoC from Entry of IoT –

Mobile Auth for Wi-Fi Access

Mobile Auth for Wi-Fi Access



Company's Strength in IoT

Two-factor Authentication &
A Risk Prevention Framework

Product Framework

- Risk assessment for Wi-Fi access – **IoT Risk Score** for each pair of phone number - mac address
- Scenarios: **Retails** and **Enterprise**

Wi-Fi Access Data

Applying customized router firmware to generate real world IoT data

- Modifying open-source router firmware, e.g., OpenWRT, DD-WRT, Tomato.
- Modify Hostapd, design, implement, and call TeleSign APIs.
- Partner with router vendors, e.g., Netgear, Google.

Synthesizing data

Lean toward the real-world situations
⇒ Applicability

The insights acquired from our model could speak for the Wi-Fi access of the target scenarios.

Settings

- Roughly 1000 pairs (phone-mac)
- 8 days, the first 7 days as history and the last one is considered today (happening now).
- 2FA timeout: 7 days

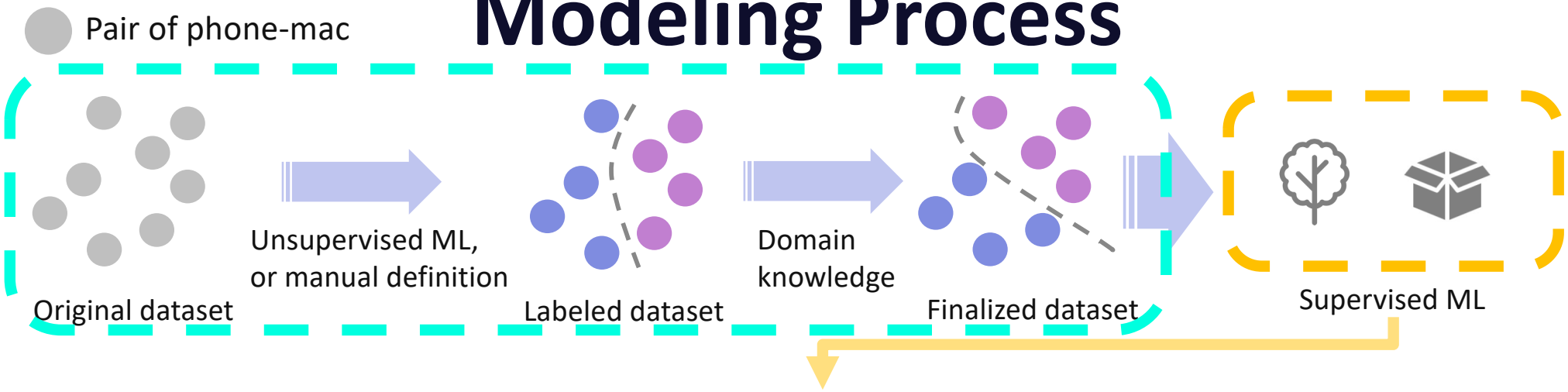
Logics

- Unless admin revokes the accept decision, a pair will no longer issue access request once being accepted.

Abnormal and Normal Labels

- When a pair's access records mees our predefined risky patterns, the pair will have a higher chance to be considered as abnormal, e.g., number of daily access request > 10.

Modeling Process



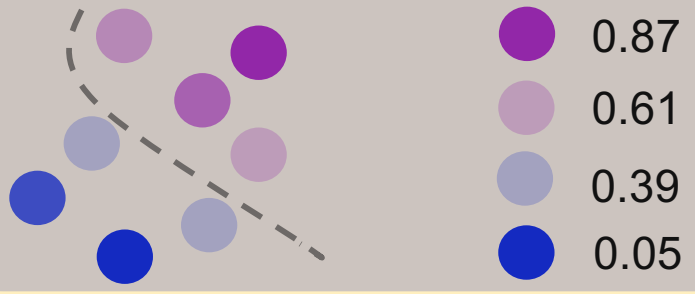
Model output aligns with our predefined risky patterns

⇒ Demonstrate data science methodologies can be applied to IoT risk assessment theoretically.

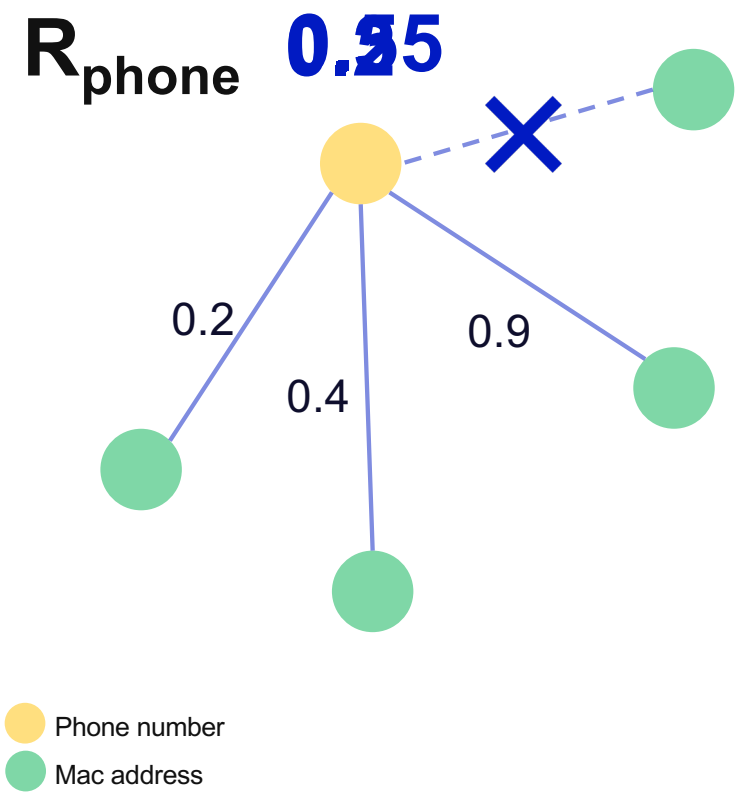
Interpret Patterns of Risk Behavior

- ***count_accessReq_1day*** – the count of daily access of an abnormal pair (18.72) is expected to be higher than that of the normal. (1.02)
- **5 of our 7 predefined patterns** can be perfectly explained by the model output.

Pair-wise Risk Score



Risk Prevention – Phone Number as an Identity



Update risk score for phone number, R_{phone}

- Calculated based on target scenarios, e.g., min() for retails or avg() of the top 3 pairs for enterprise.
- Daily updated and Initialized periodically, e.g., 3 months.

Phone Number Profiling

The more devices using a phone number for 2FA, the more the updated risk score of the phone number, R_{phone}, can represent its owner's risk level.

Target Users in IoT

Vendors from IoT Devices and Cybersecurity

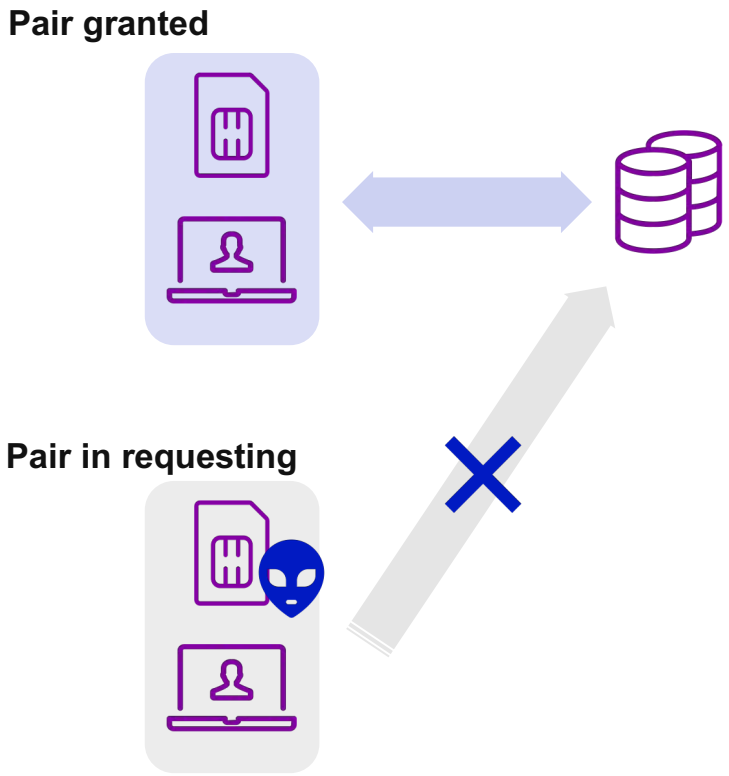
After Connected

What industry leaders have been working for long …

- Based on transmitted/received traffic patterns of the connected IoT devices to assess their potential risks.
  - One of the major Machine Learning applications in the current IoT industry.
  - Various OSI 7 layers' variables and patterns can be complicated, e.g., the UNSW-NB15 dataset comes with 300 features for network transmissions.

Do we really want to join this fight?

Business Strategy



Risk Identification Framework

Condition: integrating 2FA

1. Pair-wise risk score: **collaborate with cybersecurity vendors.**
2. Phone number profiling.

Risk Prevention

- More than existing risk detection.

Phone Number Profiling for IoT

- CDR records will help us identify the forged numbers during 2FA process.

Realize the Potential Opportunity

Future Work

Future Work

To pitch IoT vendor collaborations using Mobile Auth for Wi-Fi Access

Implementation

Apply customized router firmware to generate the real-world dataset to verify the conclusions from the synthetic dataset.

Collaboration/Competitor Analysis

More survey of the state-of-the-art solutions from cybersecurity vendors and Academic.

Marketing Analysis

Validate the existence of proposed target users – vendors who have security needs and integrating phone number 2FA is their option.

Reference

- IoT Risk Assessment – Palo Alto
  - https://docs.paloaltonetworks.com/iot/iot-security-admin/detect-iot-device-vulnerabilities/iot-risk-assessment
- UNSW_NB15
  - https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15
- Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey
  - Yongxin Liu, Jian Wang, Jianqiang Li, Shuteng Niu, and Houbing Song, *Senior Member, IEEE*
- Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction
  - Kazi Istiaque Ahmed and Abdul Ahad , Mohammad Tahir, Mohamed Hadi Habaebi, and Sian Lun Lau
- TOP 10 APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY
  - https://www.analyticsinsight.net/top-10-applications-of-machine-learning-in-cybersecurity/
- Top 5 Applications of Machine Learning in Cyber Security
  - https://www.geeksforgeeks.org/top-5-applications-of-machine-learning-in-cyber-security/

More Topics in
Authentication & Authorization (AA) for IoT

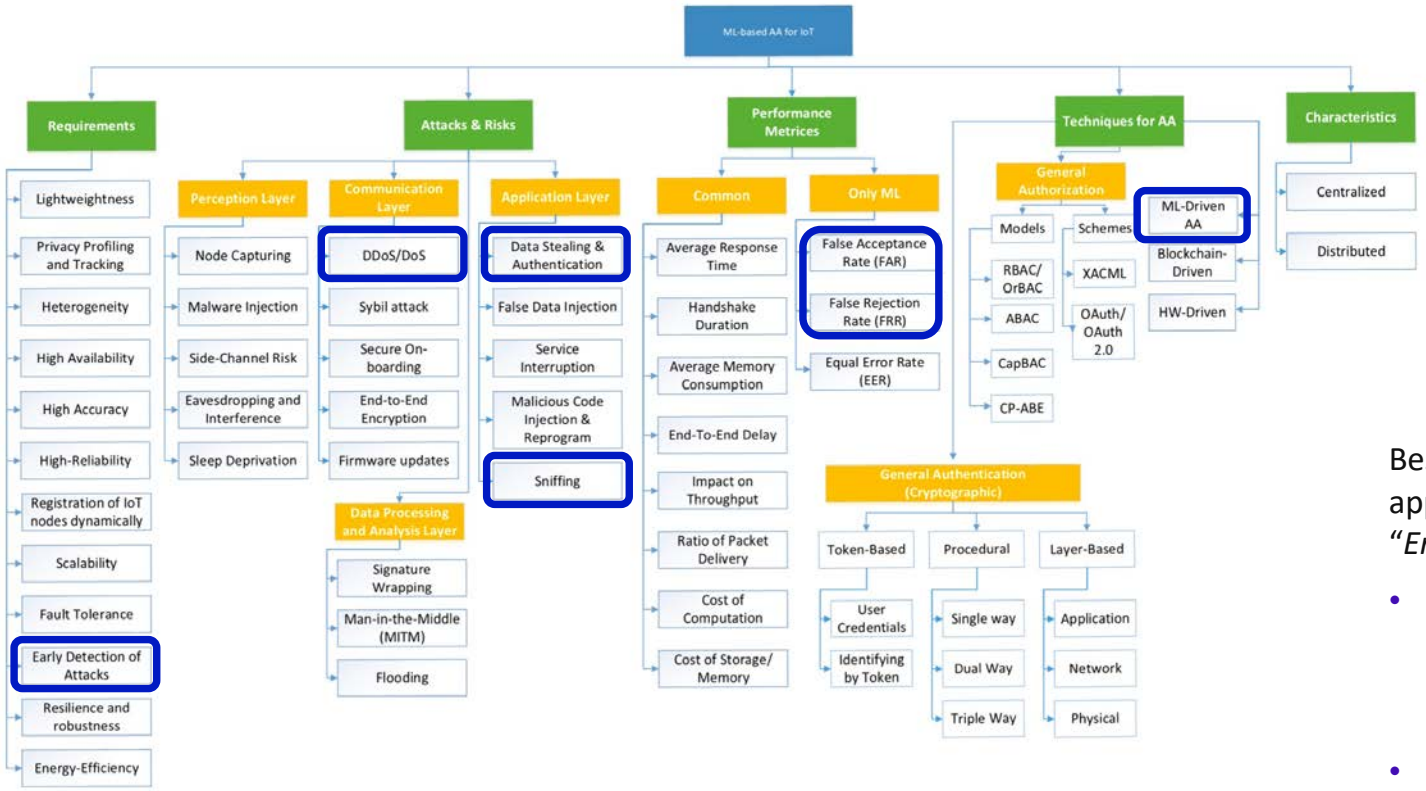


Figure 1. Taxonomy of ML-based AA for IoT.

Besides identifying cyber threats, some applications also overlap with the "*Enterprise Data Transmission*" proposal

- User behavior modeling
  - Confidential data leakage
  - Suspicious login/out patterns
- Phishing monitoring