VaktBLE: Evaluating a Wireless Man-in-the-Middle Bridge against Malevolent BLE Connections

Geovani Benita Maldonado[1]
Leonardo Sestrem de Oliveira[1]
Matheus Eduardo Garbelini[1]
Sudipta Chattopadhyay[1]
Sumei Sun[2]
Ernest Kurniawan[2]

[1] Singapore University of Technology and Design (SUTD);
[2] Institute for Infocomm Research (I2R), A*Star.



VAKTBLE



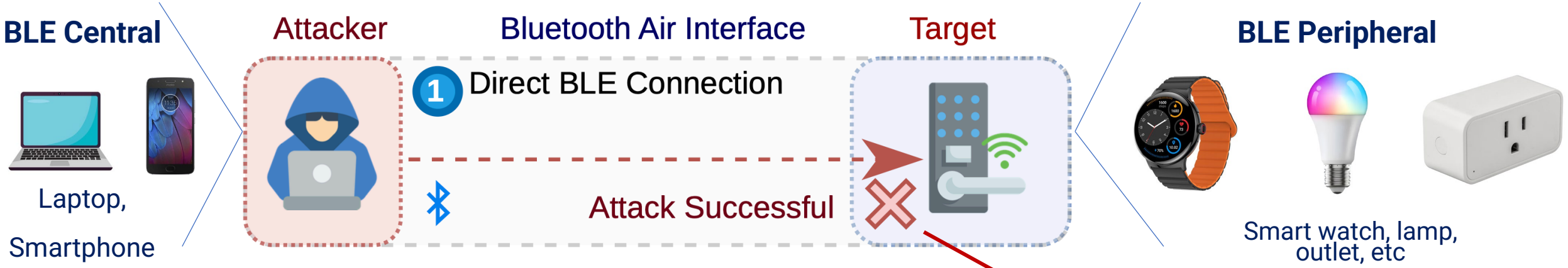




LASER Workshop 2024 – ACSAC 2024
2024 December 10, 2024
Honolulu, Hawaii, USA

VaktBLE: Introduction – Security Challenges in IoT

What is a Malevolent BLE connection (Attack)?



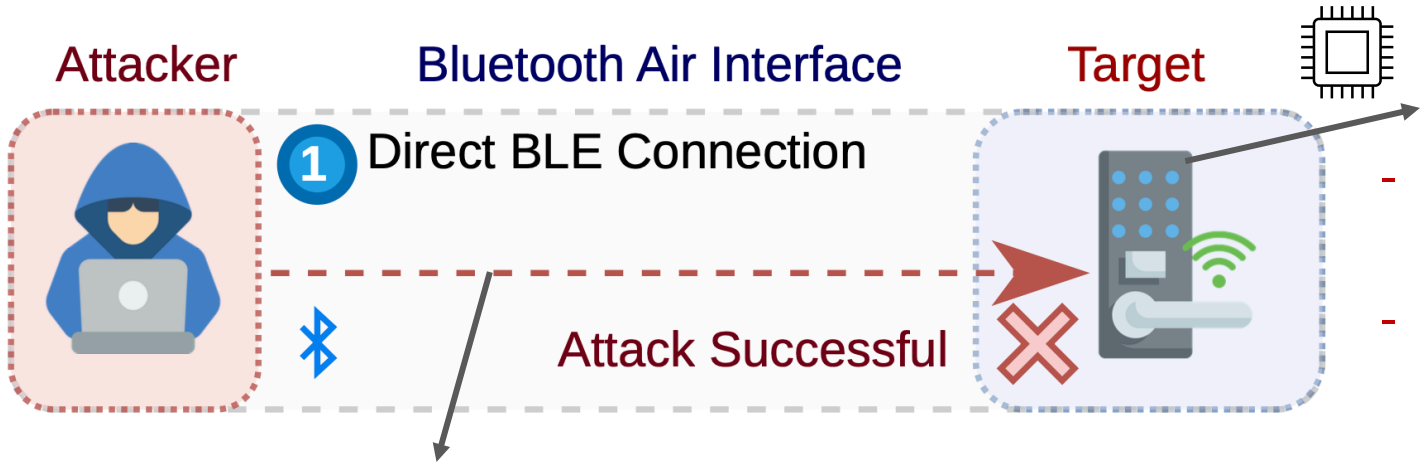
What we want?

- **Prevent** over-the-air (OTA) Attacks;
- Reduce time for end-users to receive patches.

What Attacks?

- Security Bypass
- Remote Code Execution
- Denial of Service (Hangs, Crashes, etc.)

VaktBLE: Introduction – Research Landscape



Over-the-Air (OTA) Intrusion Detection

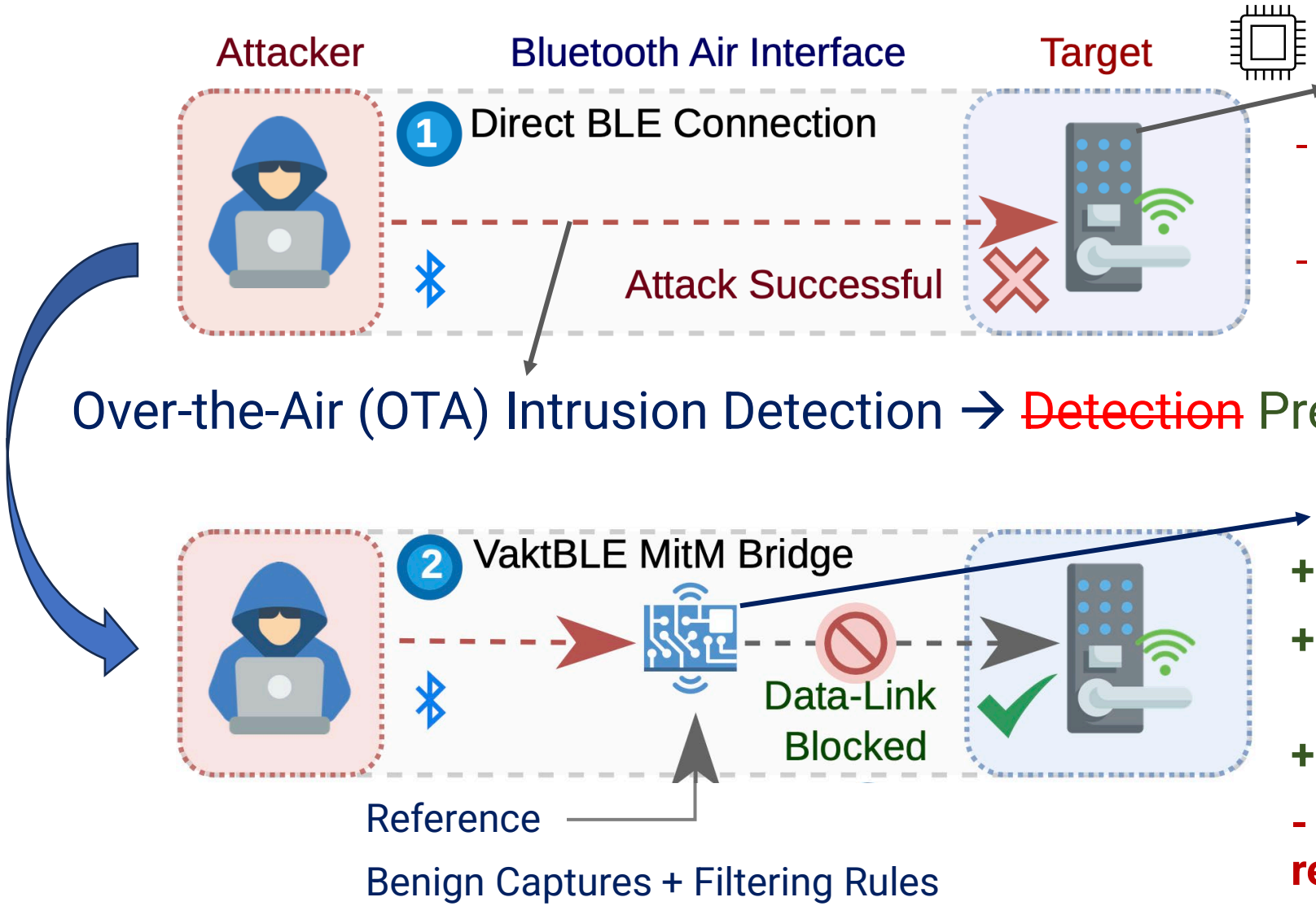
- Reactive
  (Does not prevent attacks in real-time)

Defense in the firmware

- Supports only certain devices
  (Less generic)
- Needs firmware patching
  (Not user friendly)

⚠ Lack of out-of-the box deployment solutions.

VaktBLE: Introduction – Why VaktBLE? (Use Case)



Defense in the firmware

- Supports only certain devices (Less generic)
- Needs firmware patching (Not user friendly)

VaktBLE

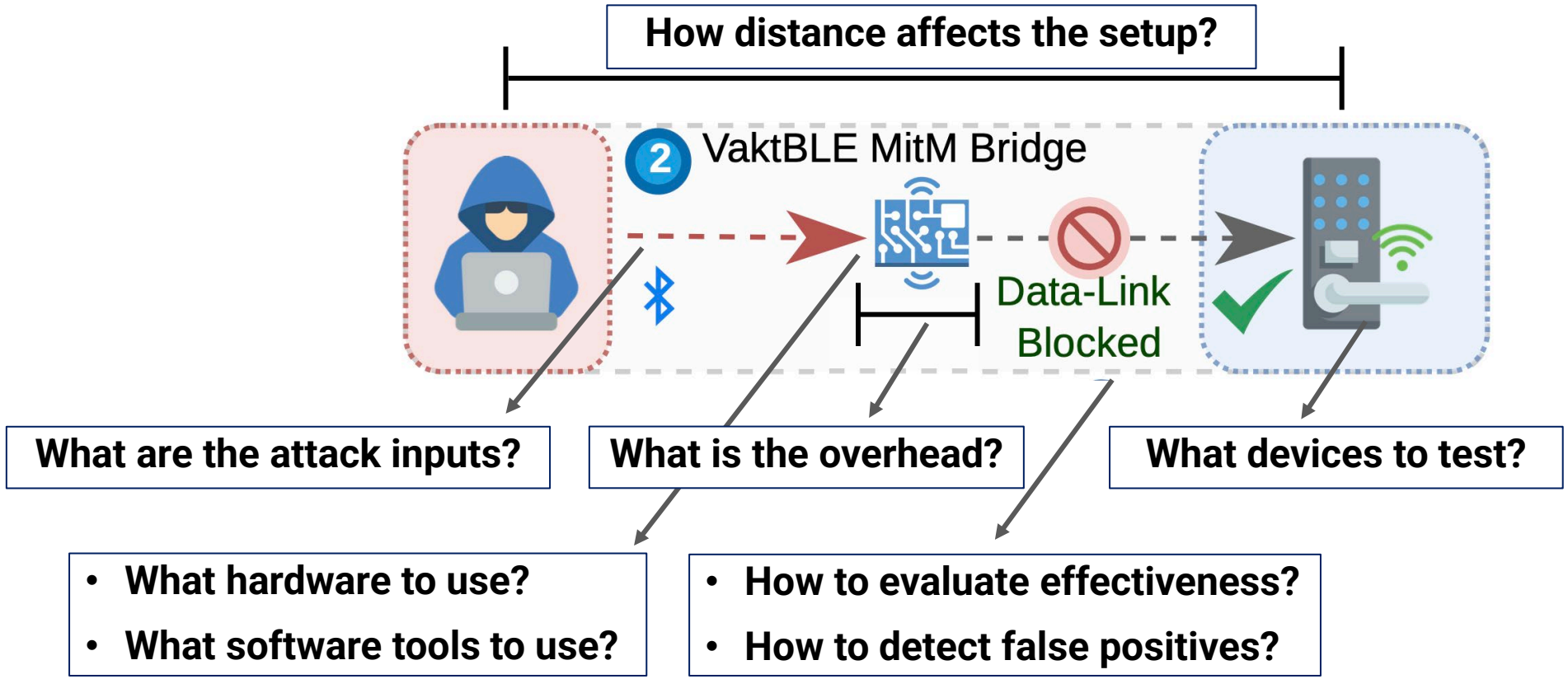
+ Actively prevent attacks

+ Supports any BLE device (More Generic)

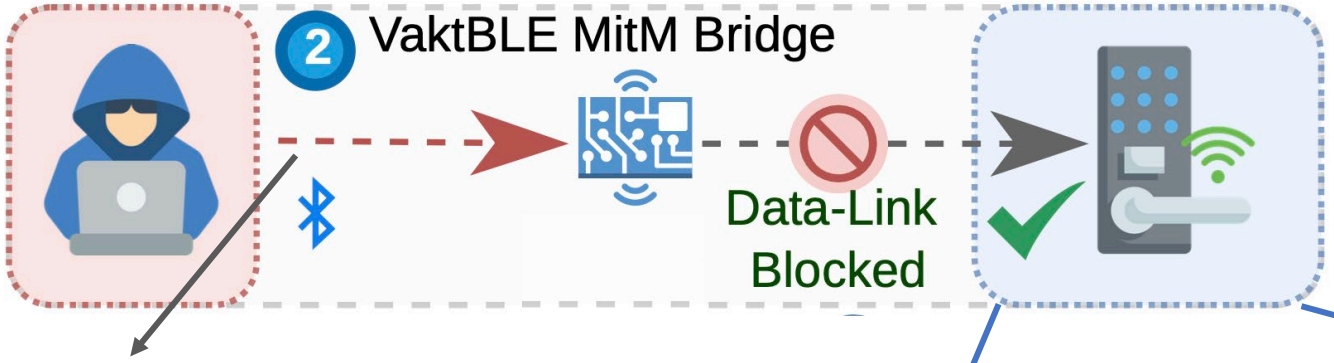
+ Used by non-expert users

- One-time collection of reference benign captures

VaktBLE: Evaluation Questions (How to Test This Thing??)



VaktBLE: Evaluation Methodology (Datasets Used)



What are the attack inputs?

Inputs = Attacker Actions

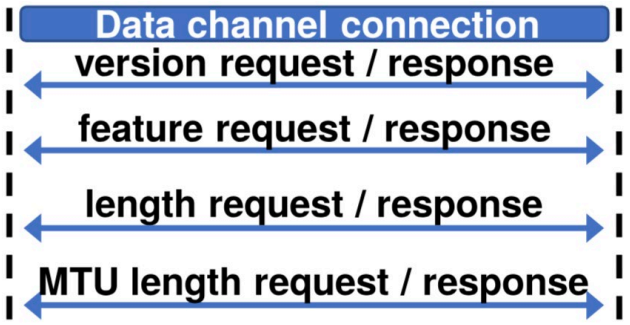
Vulnerable Software

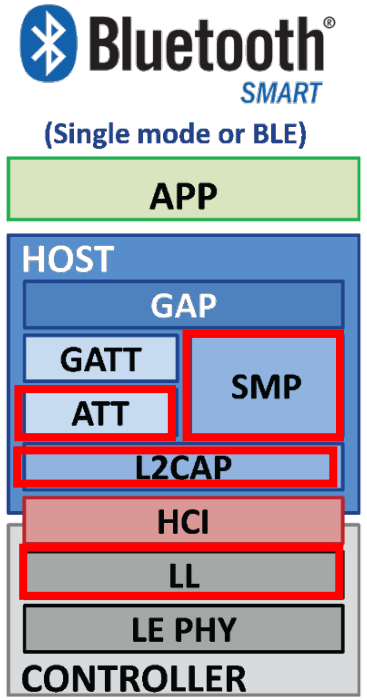
Inputs need to be realistic and practical!

Attacker Actions (Script)

- *Malformed Data fields*
- *Out-of-order messages*
- *Flooding*

Attack Surface (Message Exchange)



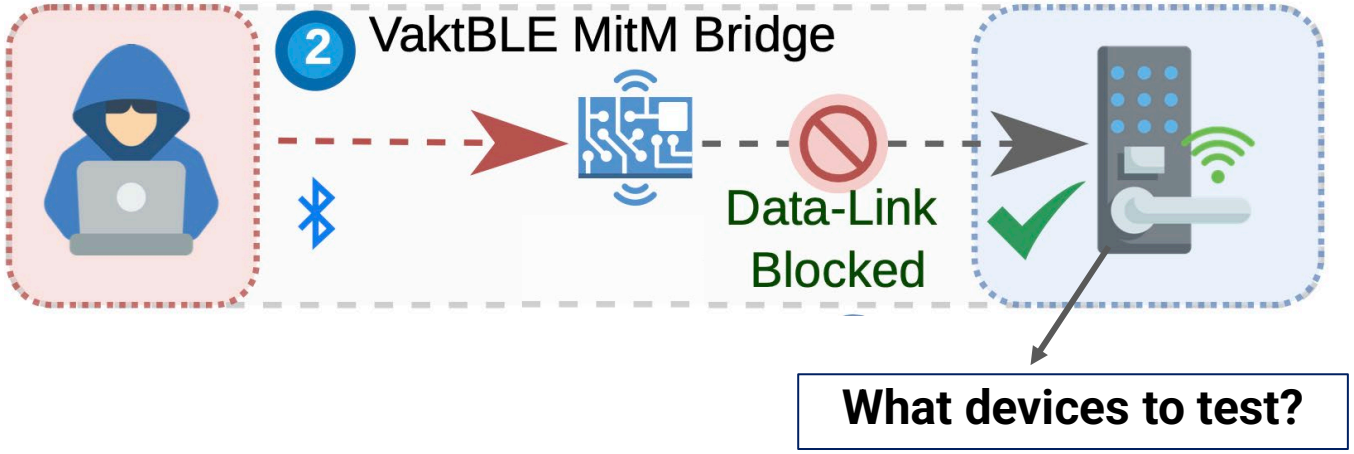


BLE Vulnerability families:

- *Sweyntooth*
- *CyRC*
- *InjectaBLE*
- *BLEDiff*

25+ BLE existing attacks

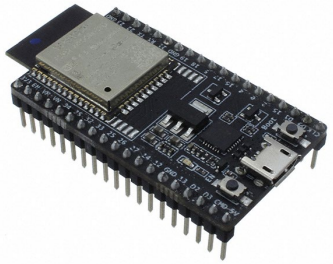
VaktBLE: Evaluation Methodology (Choice of Target Devices)



- Do we need different devices for every use-case?
- Hint: No, few representative devices are enough.
  (Approach can be validated regardless of exact BLE device)



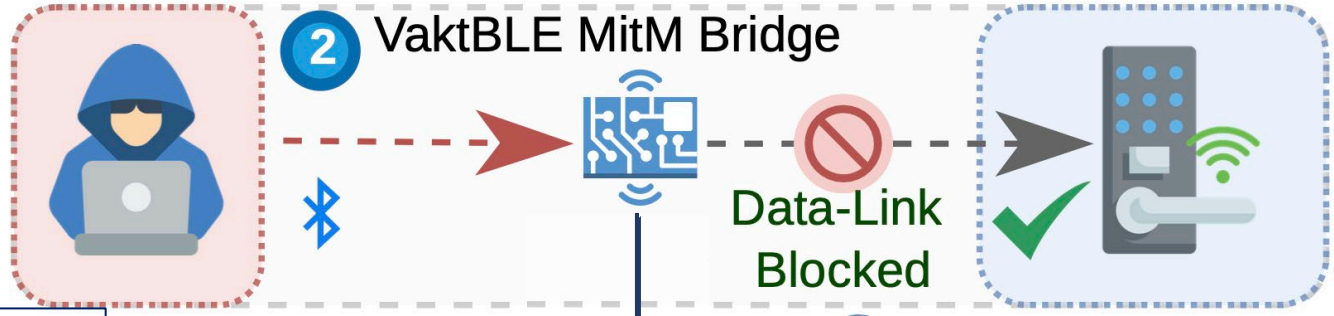
- Smartphone
  (MotoG 5s)



- Wireless BLE Module
  (ESP32-Dev-KitC)

+ Very Cheap (~5 USD)
+ Employed in many IoT products (smart power outlets, bulbs, alarms, etc)

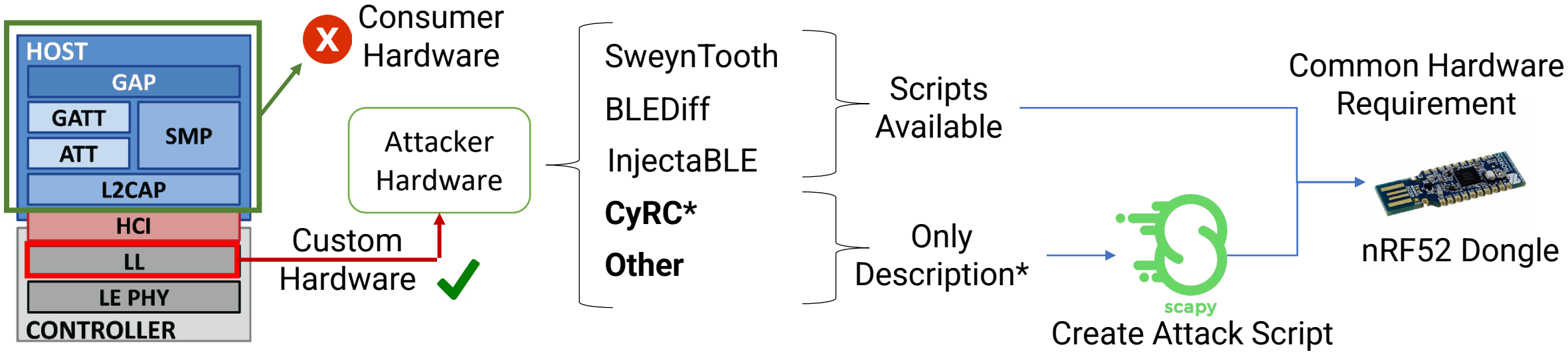
VaktBLE: Evaluation Methodology (Choice of Hardware & Software)



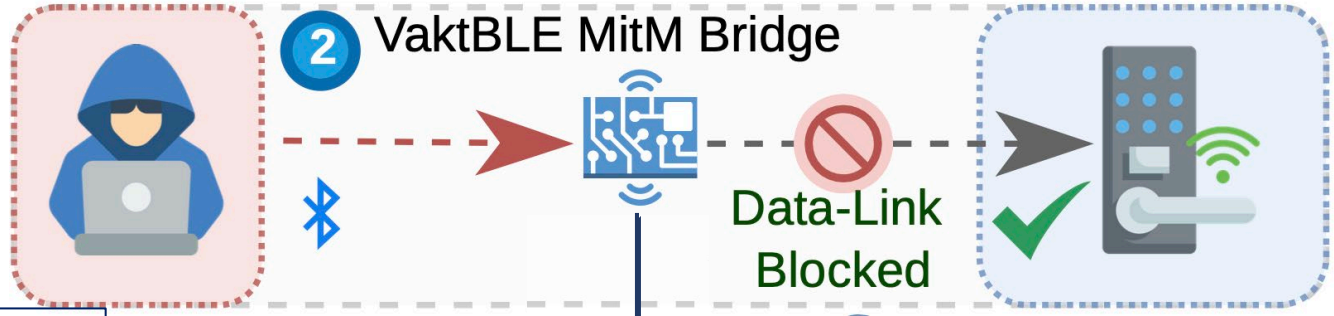
- **What hardware to use?**
- **What software tools to use?**

Need <u>hardware</u> for:

- **Launching attacks** – Reproduction of attacks requires use of specialized hardware (SweynTooth, BLEDiff)



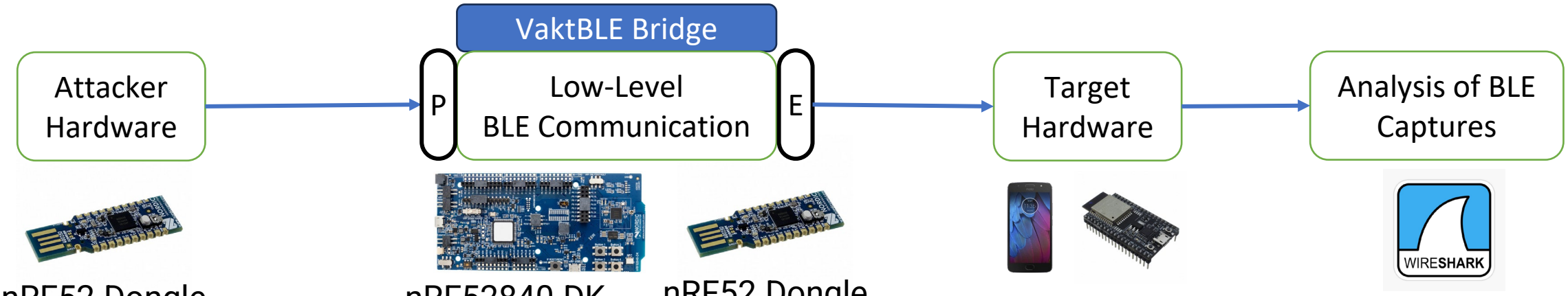
VaktBLE: Evaluation Methodology (Choice of Hardware & Software)



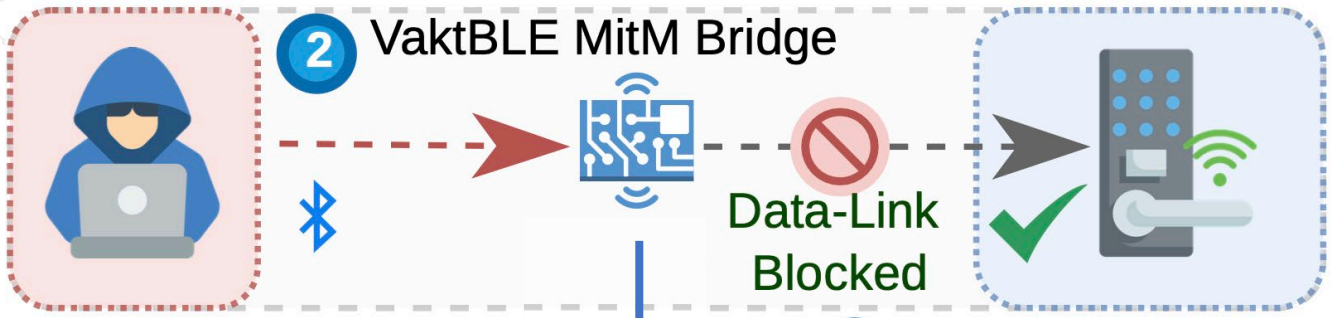
- **What hardware to use?**
- **What software tools to use?**

Need <u>software</u> for:

- **Low-level BLE communication** – VaktBLE Bridge (Inherits <u>SweynTooth</u> firmware requirements)
- **Parsing and Encoding of BLE packets** – <u>BrakTooth</u> for Parsing and <u>Scapy</u> for Encoding
- **Analysis of BLE communication** – <u>Wireshark</u> supports BLE Link Layer



VaktBLE: Evaluation Setup



Anchored setup

VaktBLE

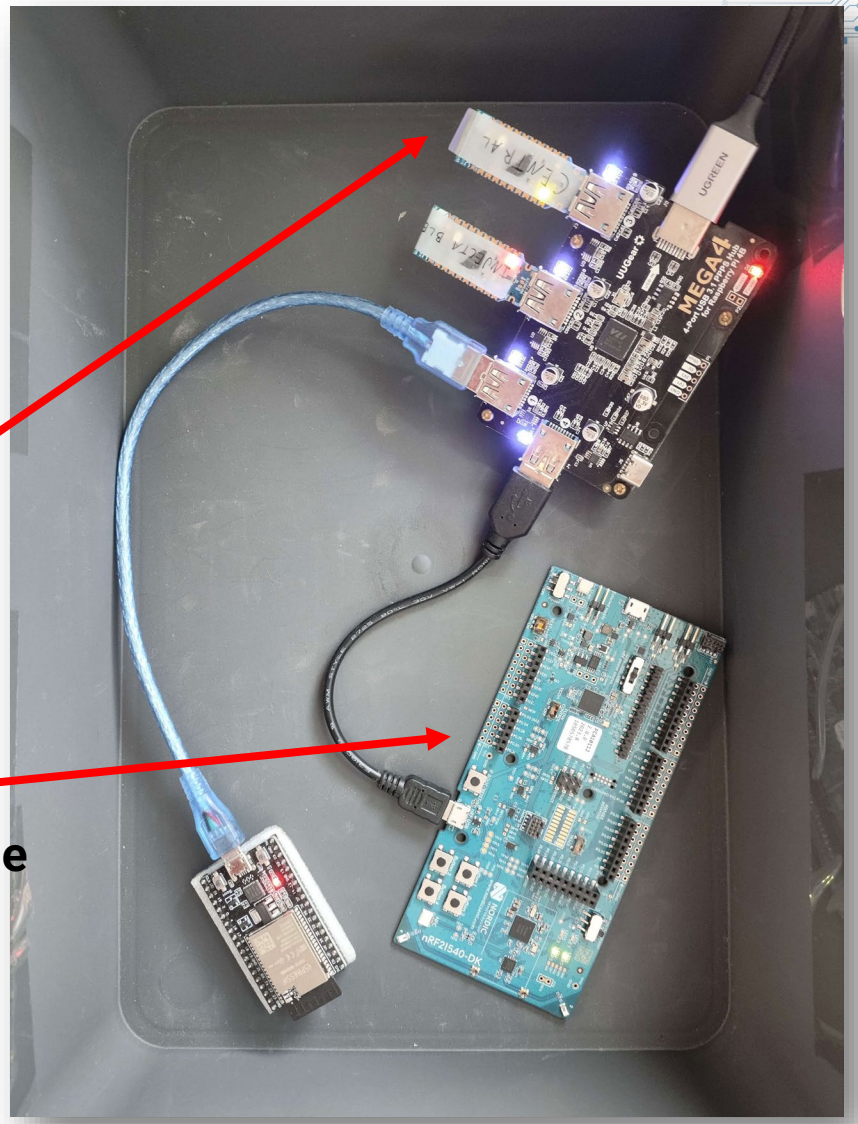
Validation Software

MitM Peripheral *(nRF52840-DK)*

MitM Central *(nRF52840-Dongle)*

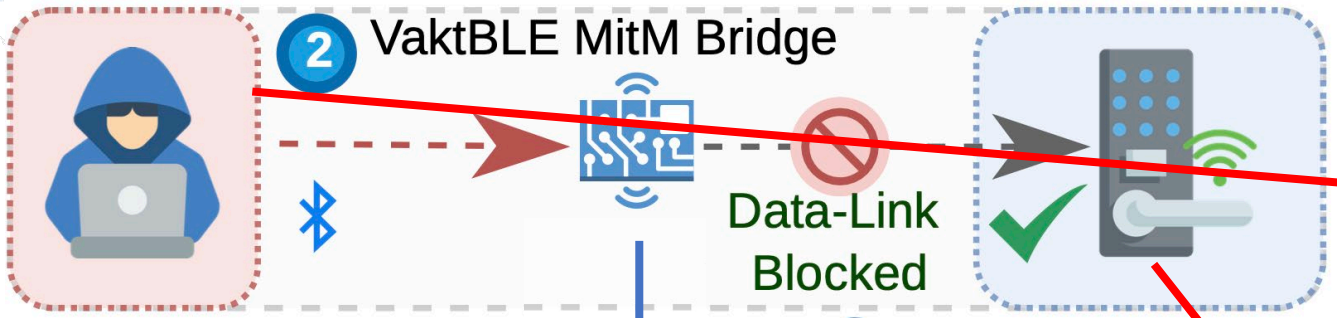
VaktBLE Bridge (Central)

VaktBLE Bridge (Peripheral)



Running on Intel i7-7700 CPU @3.60GHz with 64GB of RAM.

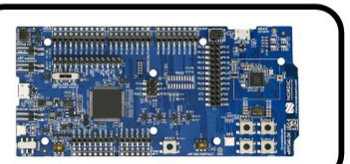
VaktBLE: Evaluation Setup



Anchored setup

VaktBLE

Validation Software

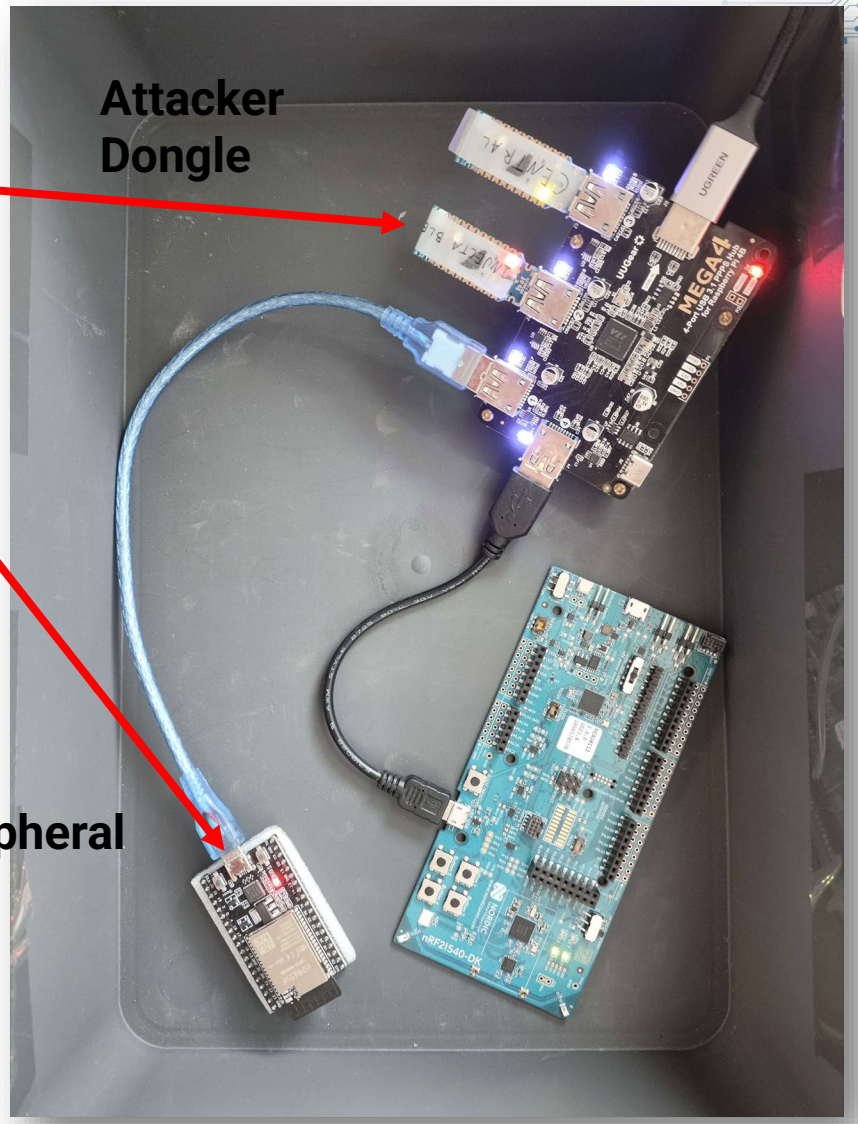


MitM Peripheral *(nRF52840-DK)*

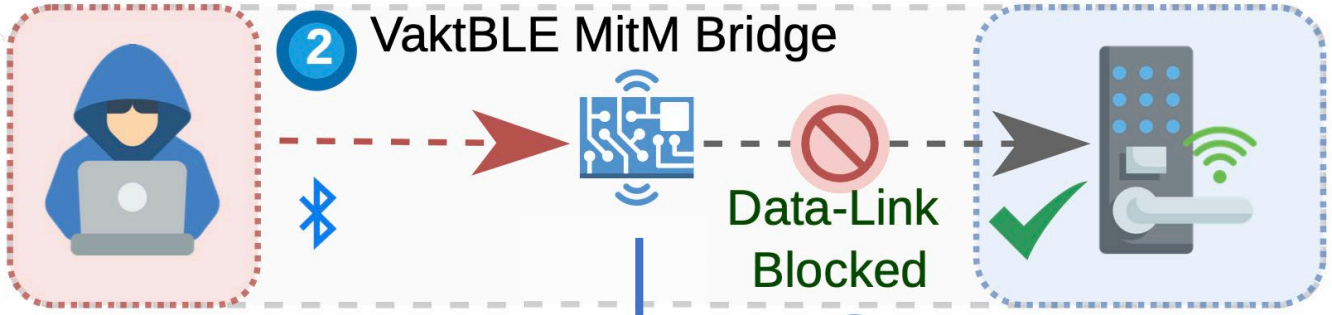


MitM Central *(nRF52840-Dongle)*

Running on Intel i7-7700 CPU @3.60GHz with 64GB of RAM.



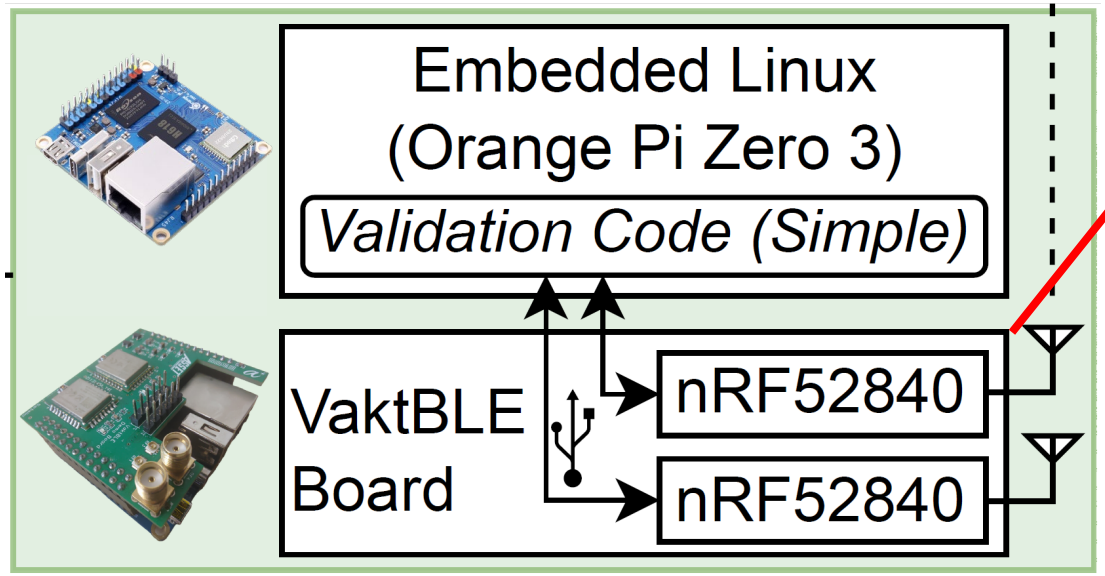
VaktBLE: Evaluation Setup



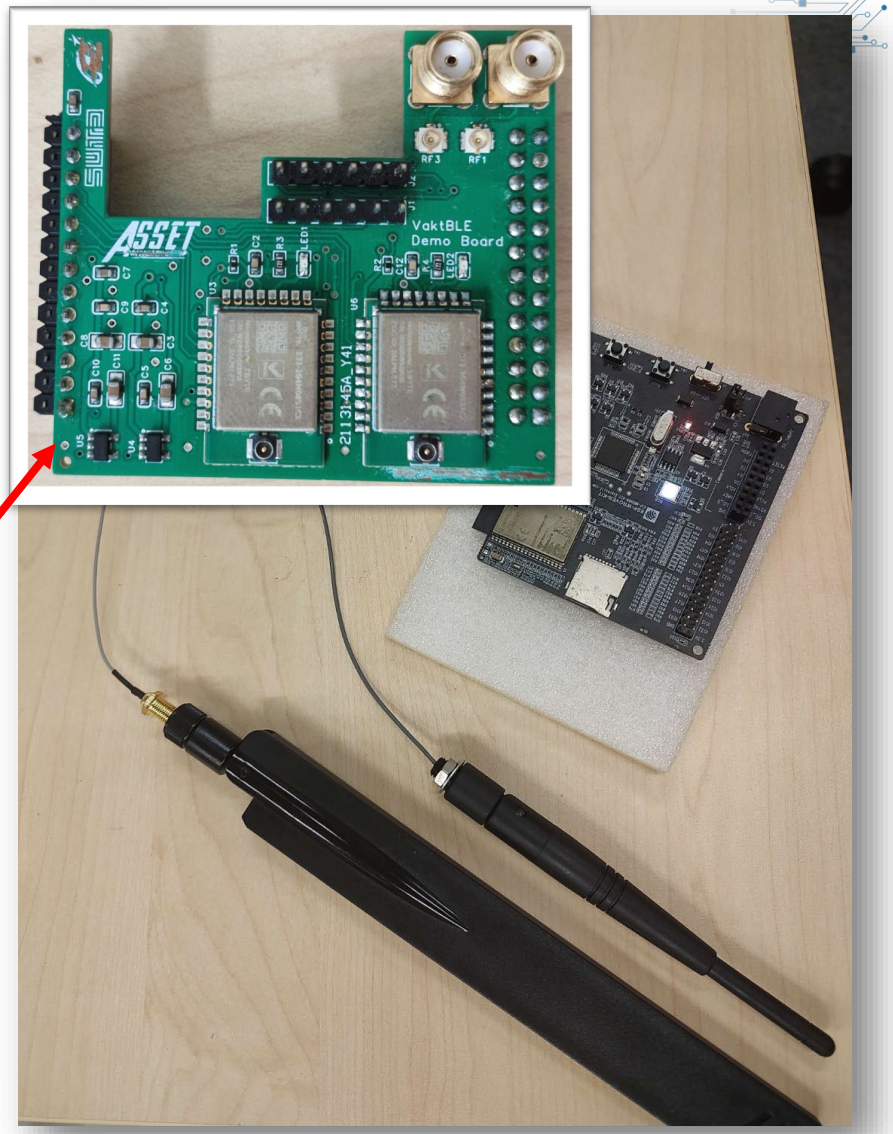
Portable setup

5.0x5.5cm

Running on Orange Pi Zero 3
ARM Cortex-A53
1.5Ghz 4GB RAM)



Open Hardware!
Facilitates Reproduction
by the community

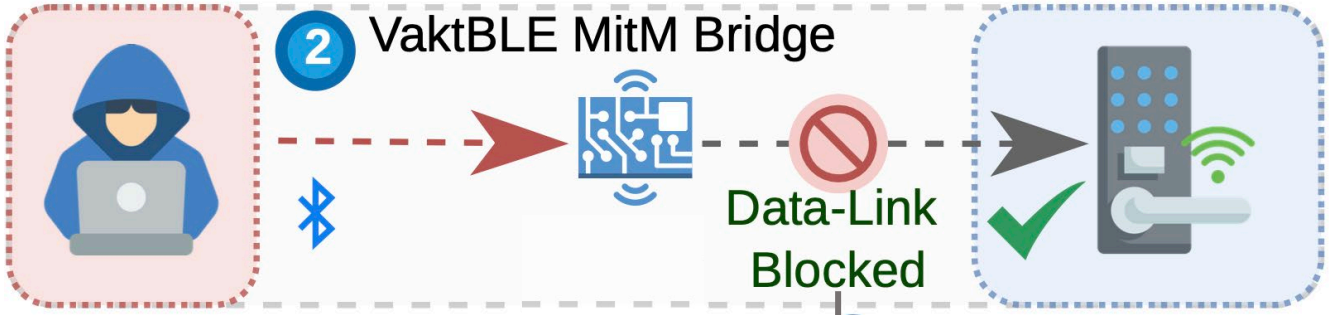


Demo Video: https://www.youtube.com/watch?v=RhDDp_HExsk

Demo Video: https://www.youtube.com/watch?v=RhDDp_HExsk

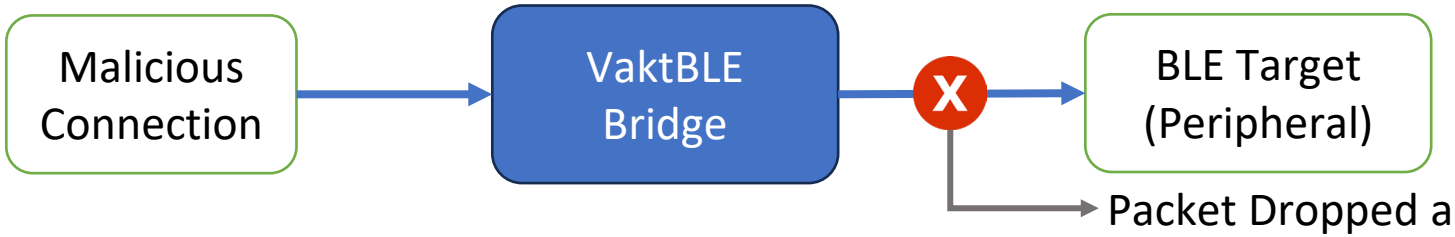
VaktBLE: Demo Video - Portable setup

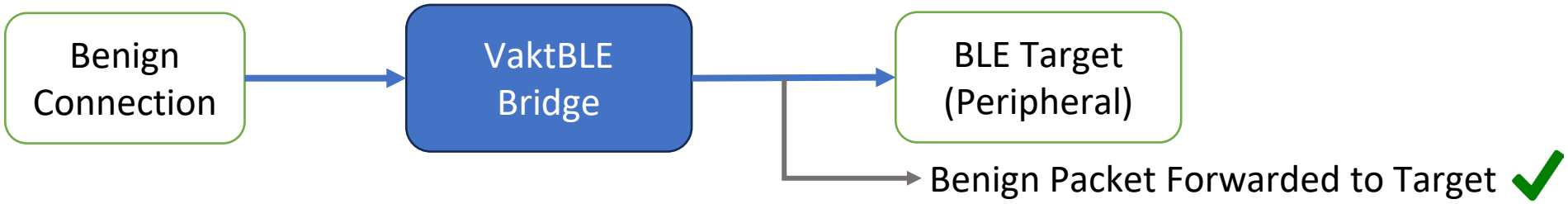
VaktBLE: Evaluation (Measuring Effectiveness)



- **How to evaluate effectiveness?**

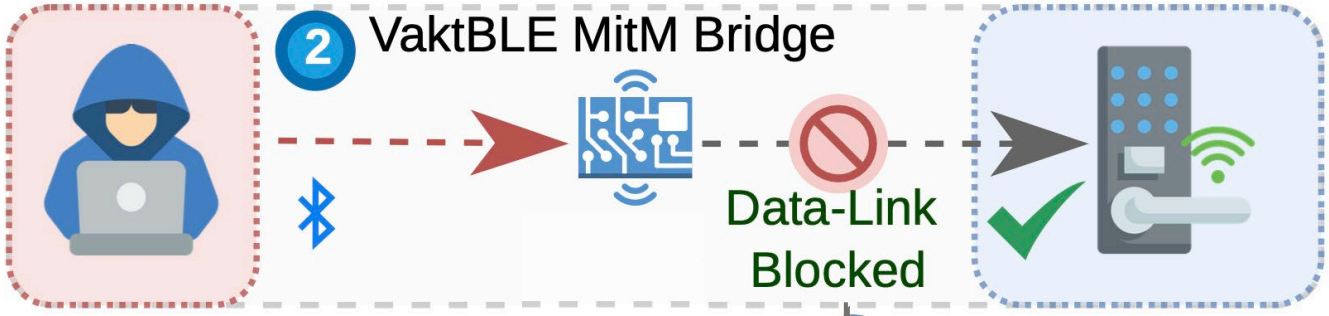
Successful Scenario





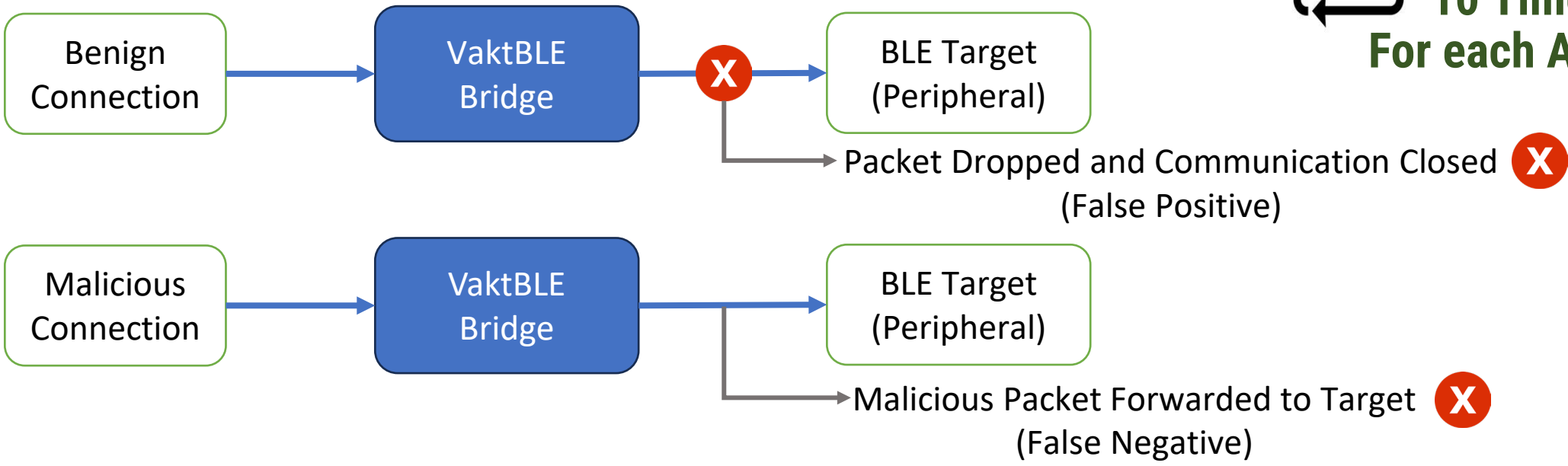
10 Times For each Attack

VaktBLE: Evaluation (Measuring Effectiveness)



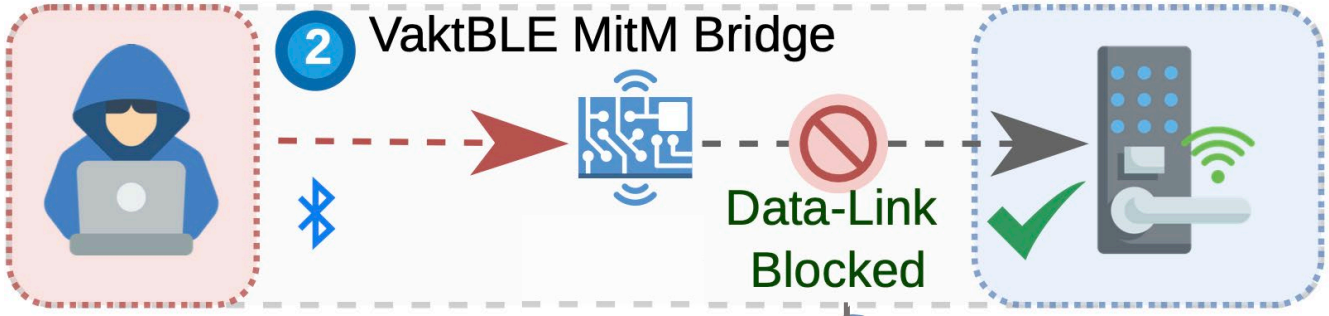
- **How to evaluate effectiveness?**
- **How to detect false positives?**

Failure Scenario



10 Times For each Attack

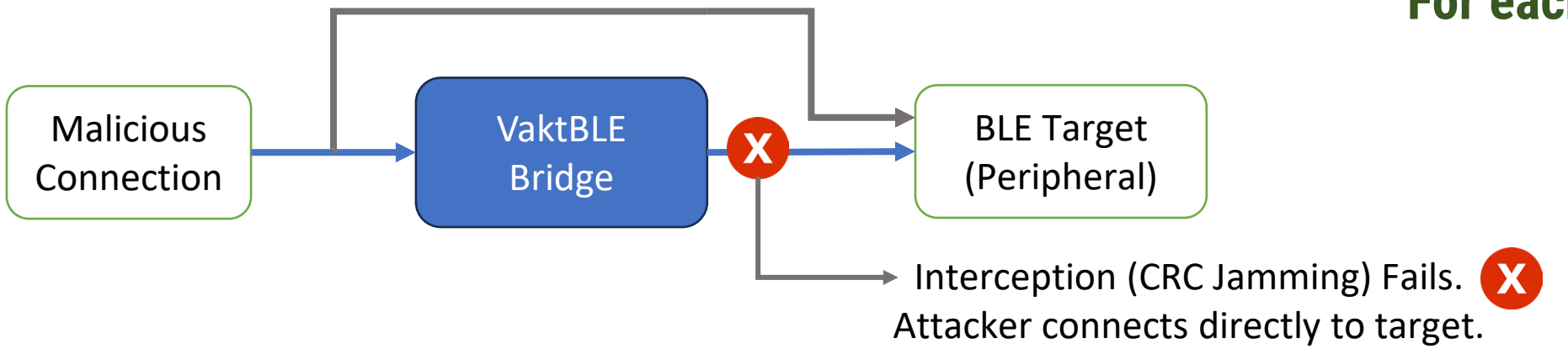
VaktBLE: Evaluation (Measuring Effectiveness)



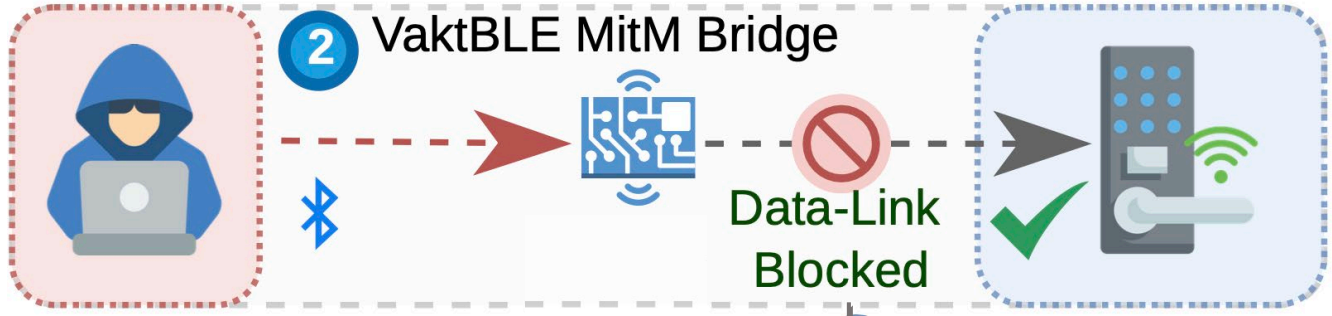
- **How to evaluate effectiveness?**
- **How to detect false positives?**

Failure Scenario (Continued)

10 Times
For each Attack



VaktBLE: Evaluation (Measuring Effectiveness)

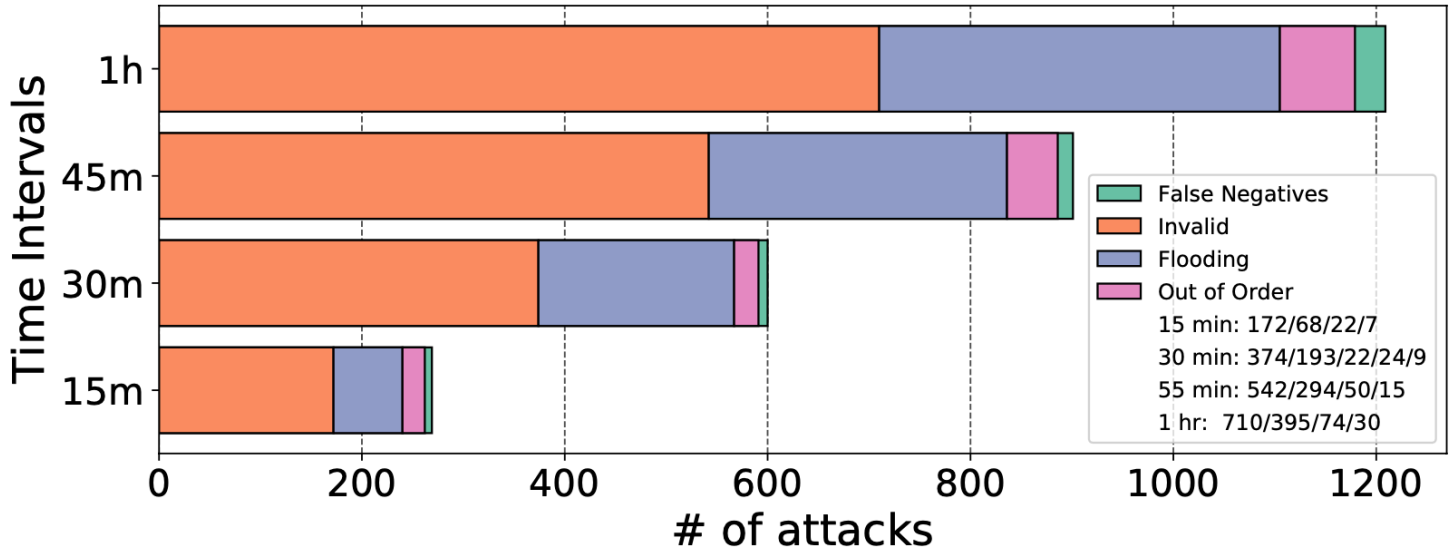


- **How to evaluate effectiveness?**
- **How to detect false positives?**

BLE Fuzzer
(As Attacker)

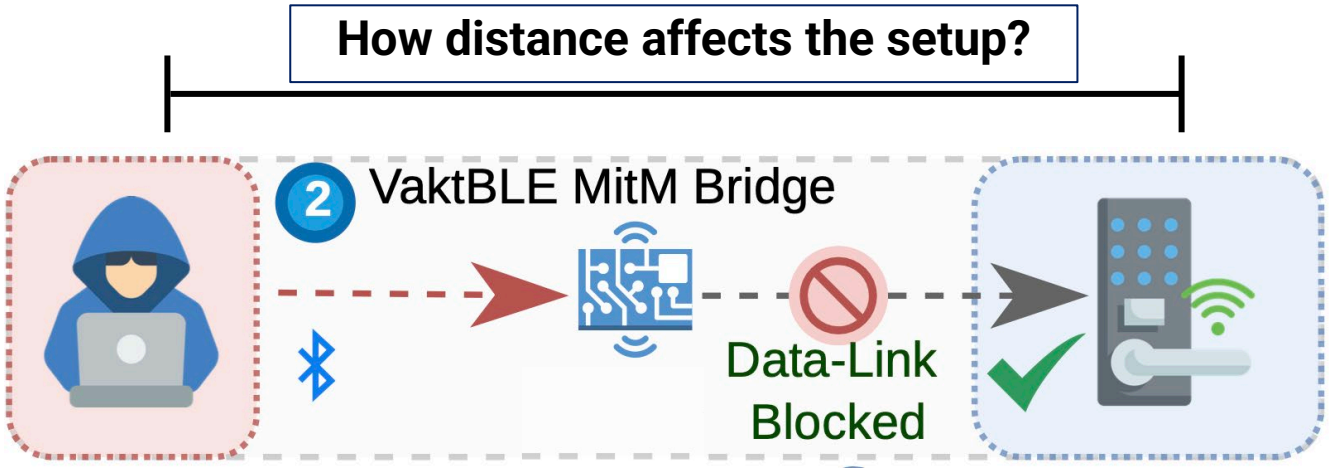
Fuzzer Actions

- *Malformed Data fields*
- *Out-of-order messages*
- *Flooding*

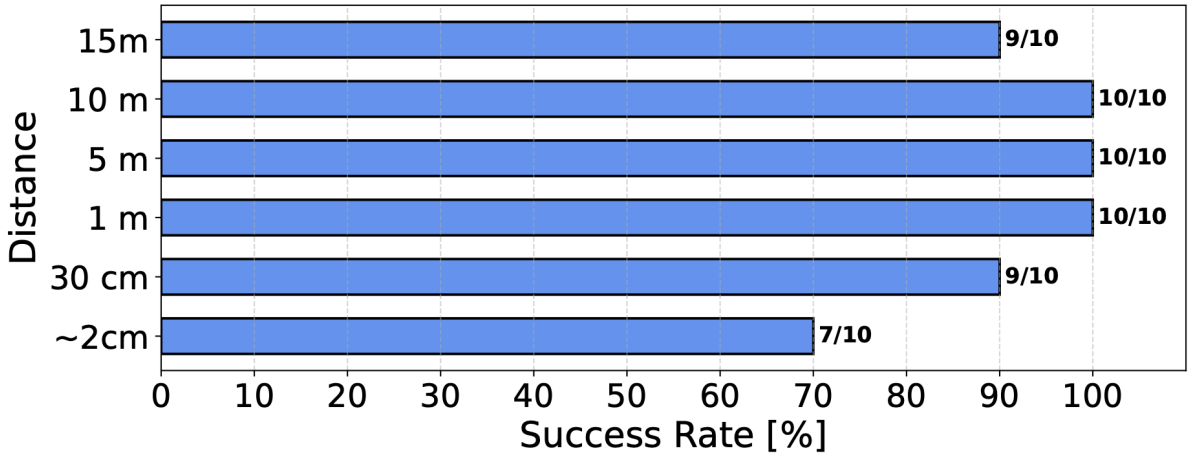


✓ Evaluated across automated testing tools (BLE fuzzer): Preventing ~97% of malicious packets.

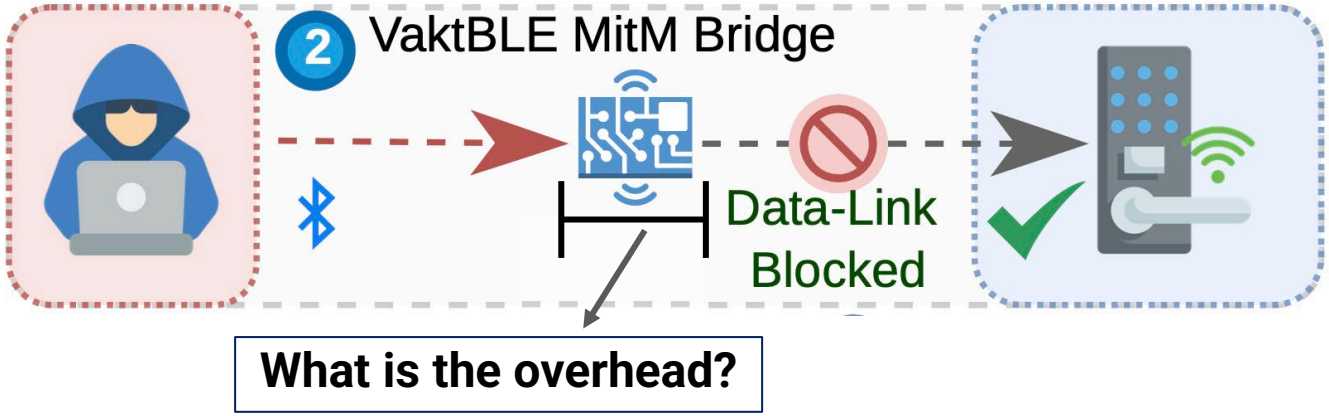
VaktBLE: Evaluation (Measuring Effectiveness)



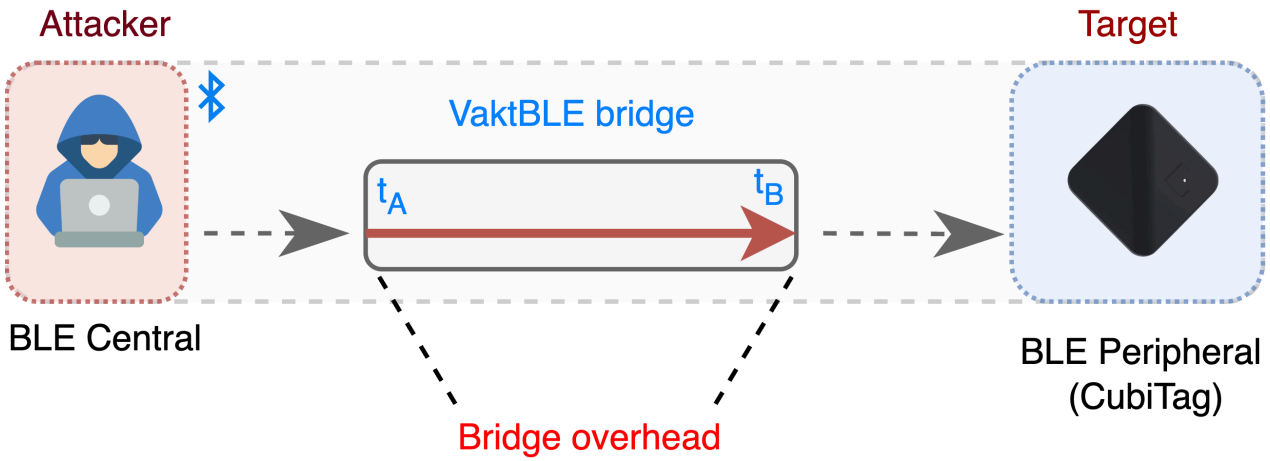
- ✓ Distance from VaktBLE to target needs to be very close!
- ✓ Evaluated attacker distance ranges from ~2cm to 15 m.



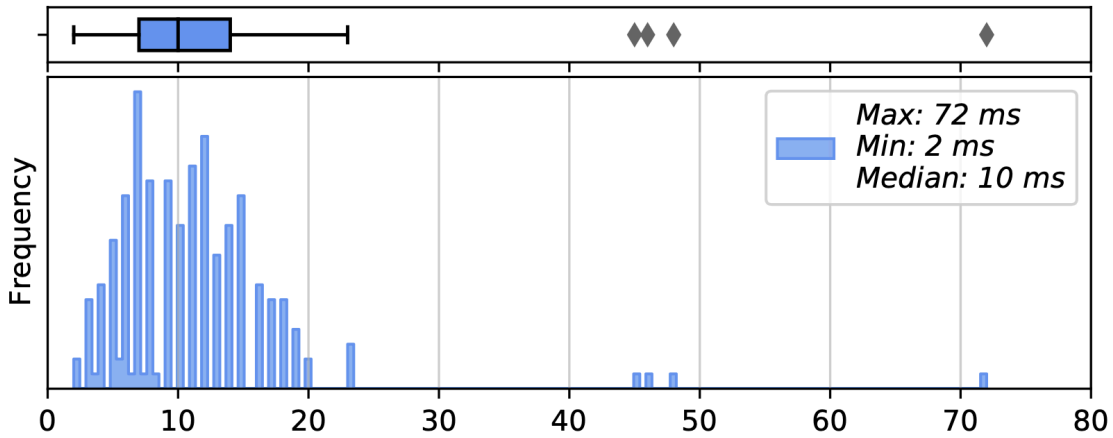
VaktBLE: Evaluation (Measuring Efficiency)



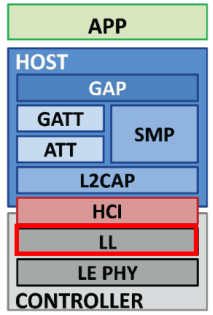
Measurement and Metrics



- ✓ Minimal **overhead** introduced within the range of BLE protocol (*10ms*) for Anchored Setup.
- ✓ Very low overhead (373µs) with Portable Setup.



Key Takeaways – Lessons Learned



1. Too many BLE vulnerabilities to reliably test against.
   We focused on low-level (Link Layer) attacks and reproducible scripts.

2. CVEs descriptions are not enough. Particularly if hardware is involved.

3. Noisy wireless environment makes evaluation more difficult.

4. Need for high quality artifacts. We adopted Open-Hardware and packaged prior work (attacks) to help in reproducibility (e.g., points 1 and 2).

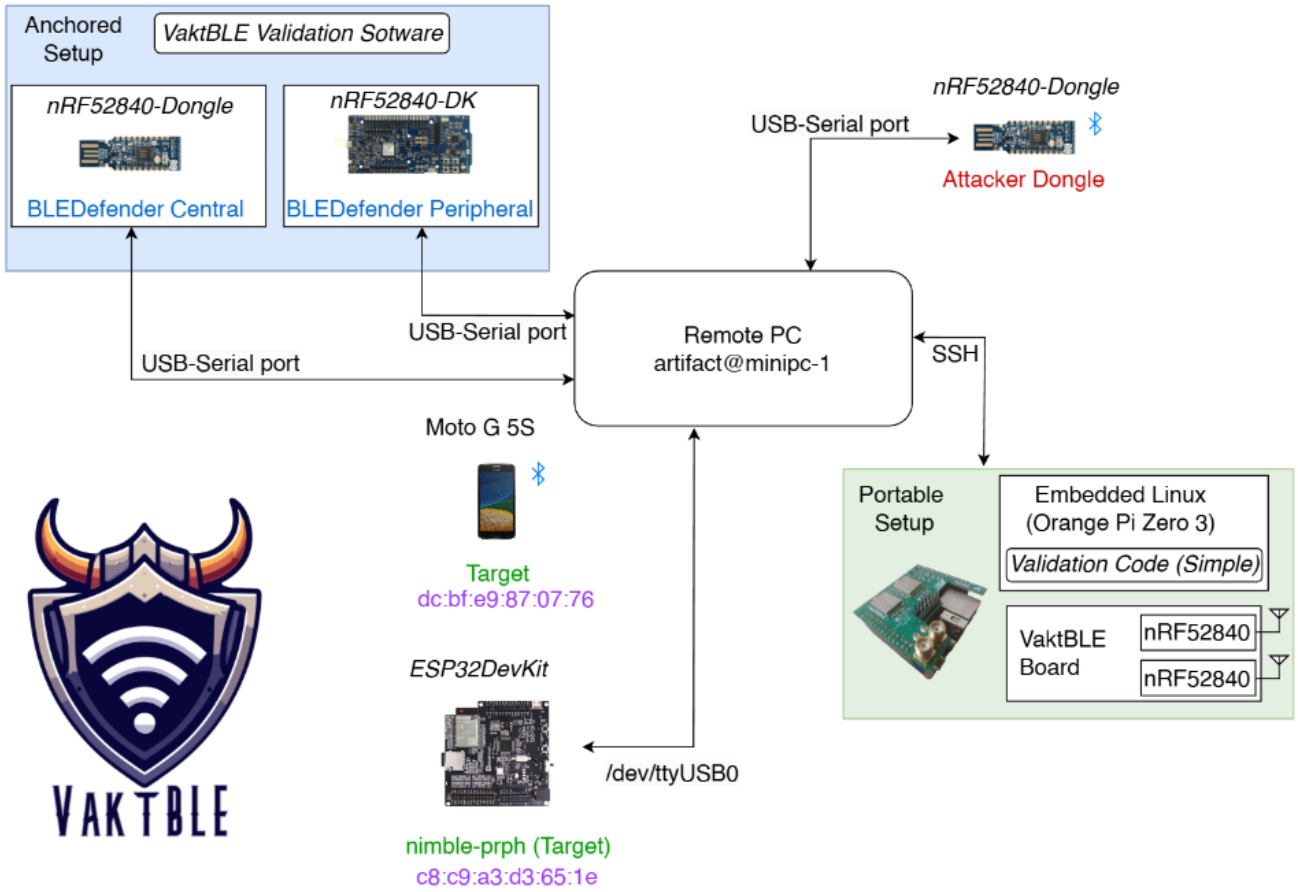
5. Wireless technology evolves fast. Support from the community is heavily appreciated.

Meta-Discussion - Recap

- Did you use any experimentation artifacts from the community?
  BLE Attack Scripts such as BLEDiff, CyRC, InjectaBLE.
- Did you attempt to replicate or reproduce earlier research?
  Yes, research on BLE attacks and closest related work (debloater).
- What challenges did you face, and how did you overcome them?
  Novel CRC Jamming, Comparing to related work and new BLE attacks
- What did you try that did not succeed before getting to the results you presented?
  Other BLE hardware, Jamming techniques, distance configuration
- Did you produce any intermediate or unsuccessful results?
  A. Comparison with closest related work failed for ESP32 (firmware)
  B. Some attacks cannot be defended by VaktBLE (not applicable)

Code & Experiments Artifact Availability

Github: https://github.com/asset-group/vakt-ble-defender/
Includes artifact documentation



Questions?

AnchoredSetup/docs/vaktble_documentation.pdf