HubBub: Contention-Based Side-Channel Attacks on USB Hubs

Junpeng Wan[1], Yanxiang Bi[2], Han Gao[1], Dave (Jing) Tian[1]
[1]Purdue University, [2]The Chinese University of Hong Kong

Background

- Hardware sharing exposes attack surface for side-channels, e.g.
  - Flush+Reload [1] (Memory)
  - Prime+Probe [2] (LLC)
  - TLBleed [3] (TLB)
  - SMoTherSpectre [4] (CPU ports for execution units)
  - MeshUp [5] /Lord or Ring [6] (CPU interconnects)
  - Invisible Probe [7] (PCIe switch/PCH)
  - .....

Background

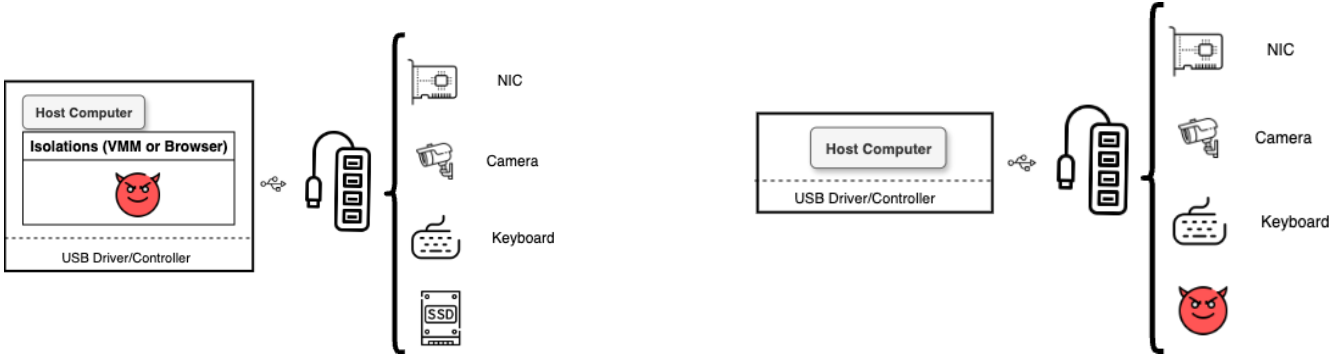
- USB hubs
  - Present a hardware-sharing scenario
  - Widely used in our daily life
    - Especially on recent laptops with fewer USB ports
  - Multiple downstream ports
    - USB type-A/type-C
    - HDMI
    - NIC
    - USB PD
    - .....

HubBub

- A new class of side-channel attacks based on USB hub contention
- Explores potential information leakage
  - On USB 2.0/3.0/3.1 Hubs
- Leaks information from 3 USB peripherals
    - NIC
    - Camera
    - Keyboard

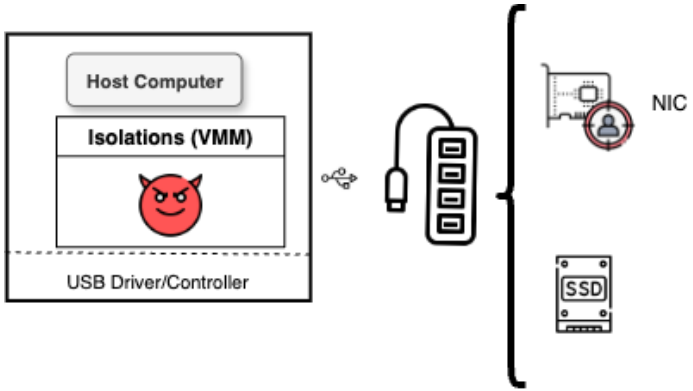
HubBub Threat Model

- Several USB devices share a USB hub
- The attacker can take two forms:
  - A program accessing a USB device within an isolated environment like a VMM or browser
  - **Or** a malicious USB device



Example (Attack A): Website Fingerprinting

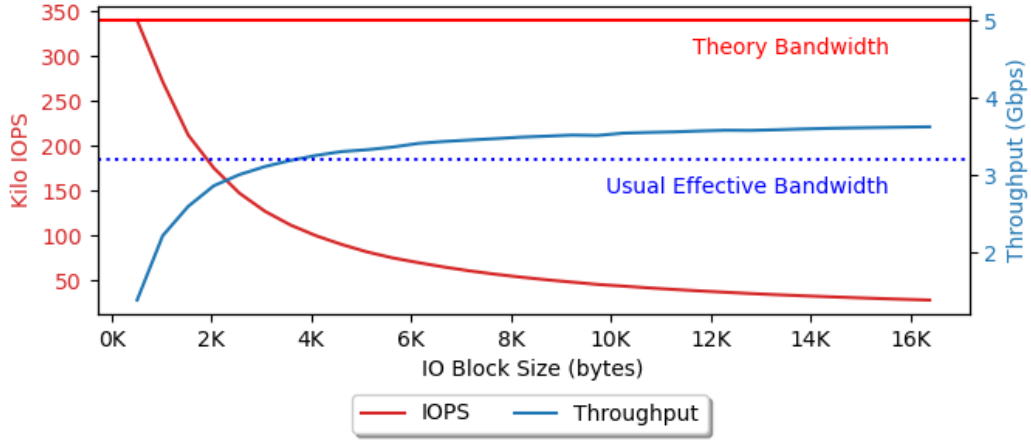
- Goal: Infer the website visited by the victim
- Setting
  - A USB NIC and a USB SSD are connected to the same USB hub
  - An attacker-controlled program has access to the USB SSD
  - Victim is browsing websites



Example (Attack A): Website Fingerprinting

Procedures

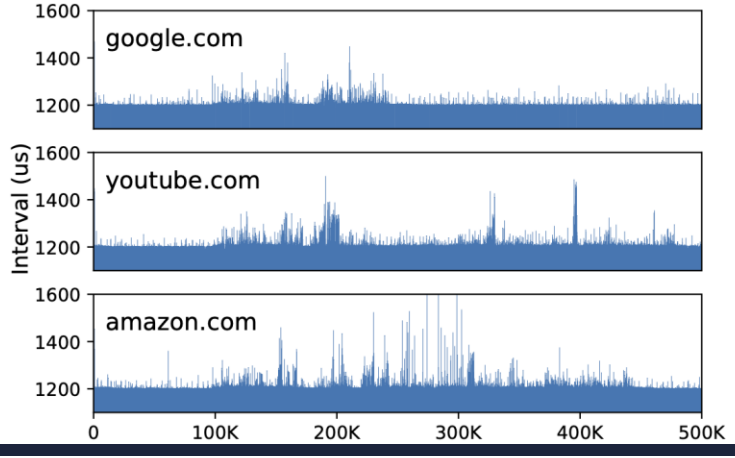
1. Saturate the USB hub bandwidth
    - Utilize **io_uring** to perform high-speed SSD accesses



Example (Attack A): Website Fingerprinting

Procedures

1. Saturate the USB hub bandwidth
2. Record timestamp for each I/O and calculate the Intervals
   - RDTSCP
   - Traces →



Example (Attack A): Website Fingerprinting

Procedures

1. Saturate the USB hub bandwidth
2. Record timestamp for each I/O and calculate the intervals
3. Preprocess Traces & Train ML/DL classifier
    - to distinguish which website the victim accessed

Example (Attack A): Website Fingerprinting

Evaluation (on 1 USB 3.0 hub)

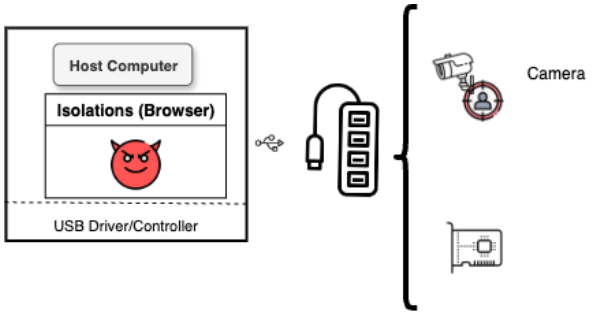
- Select top-100 websites and collect 537 traces for each website.
- Dataset split: 80% Training/20% Testing
- Model: GRU + Attention
- Accuracy: 98.84% Top-1/99.53% Top-3

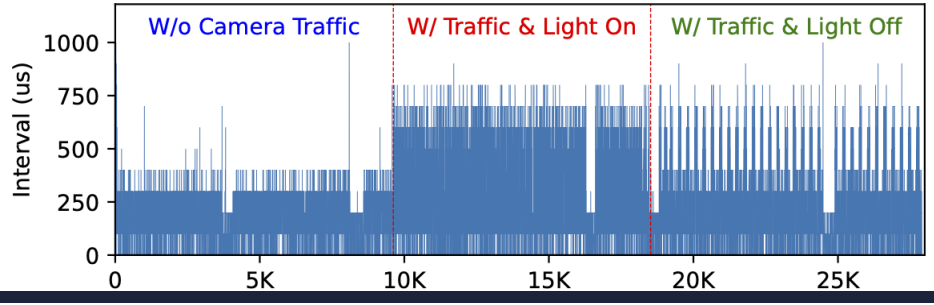
Example (Attack A): Website Fingerprinting

- Also works on
  - 10 USB 3.0 hubs
  - 4 USB 3.1 Hubs
  - 1 USB 2.0 hub
  - 1 Internal Hub
  - 1 Monitor
- Further evaluations
  - Transferability on different USB hubs/hosts
  - ……

Attack B: Camera Activities

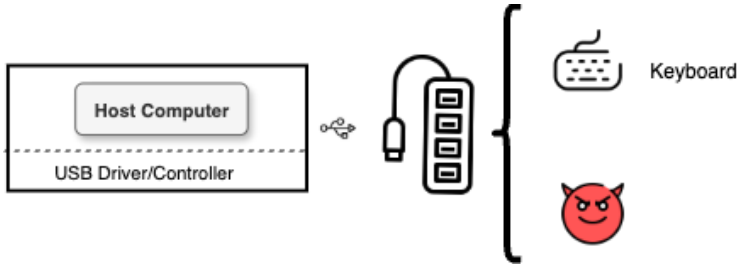
- Goal: Infer activities captured by the webcam
- Setting
  - A USB NIC and USB webcam connected to a shared hub
  - Attacker is a JavaScript program embedded in a webpage
  - Webcam activated, monitor a room

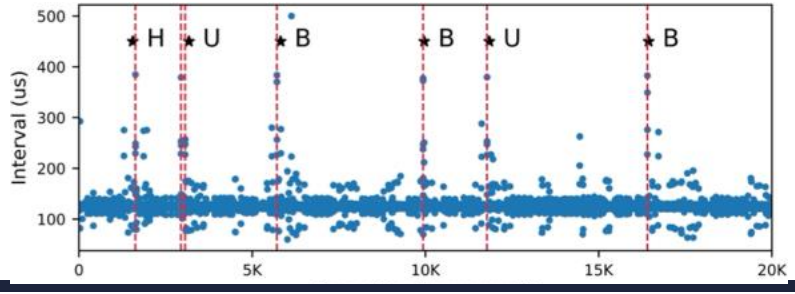




Attack C: Keystrokes

- Goal: Capture keystrokes of sensitive text
- Setting
  - A USB keyboard and the attacker USB device are connected via a shared USB hub
  - User types sensitive text on the USB keyboard





Thank you!

Reference

- [1] FLUSH+RELOAD: A high resolution, low noise, l3 cache Side-Channel attack
- [2] Last-Level Cache Side-Channel Attacks are Practical
- [3] Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks
- [4] Smotherspectre: exploiting speculative execution through port contention
- [5] MeshUp: Stateless cache side-channel attack on CPU mesh
- [6] Lord of the ring (s): Side channel attacks on the CPU On-Chip ring interconnect are practical
- [7] Invisible probe: Timing attacks with pcie congestion side-channel