ARTIFACT EVALUATED
usenix ASSOCIATION
AVAILABLE

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

PURDUE UNIVERSITY

香港中文大學
The Chinese University of Hong Kong

CERIAS

PurSecLab

Background

- Hardware sharing exposes attack surfaces 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

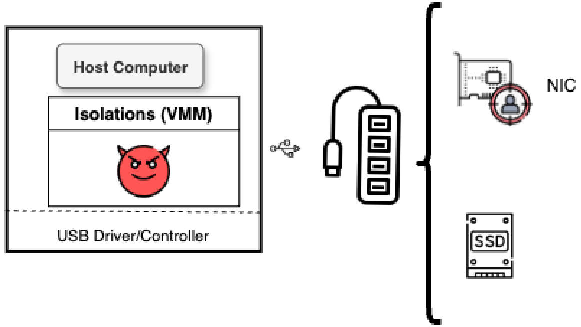
- USB hubs
  - Present a hardware-sharing scenario
  - Widely used in our daily life
    - Especially on recent laptops with fewer USB ports
  - Multiple downstream ports
    - USB type-A/type-C
    - HDMI
    - NIC
    - USB PD
    - ……

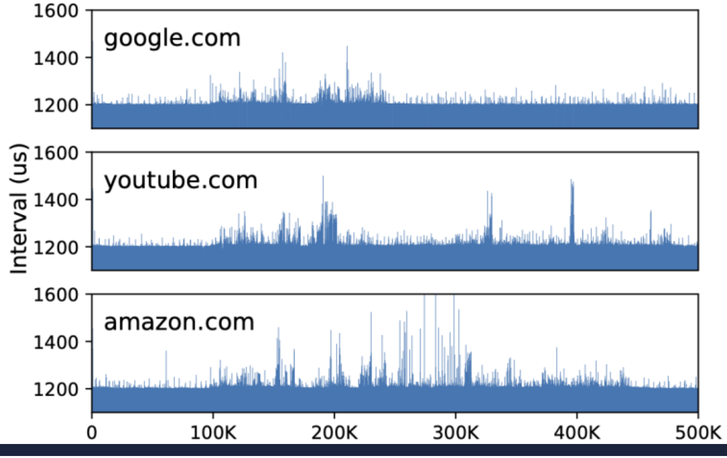
HubBub

- 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

Attack A: Website Fingerprinting

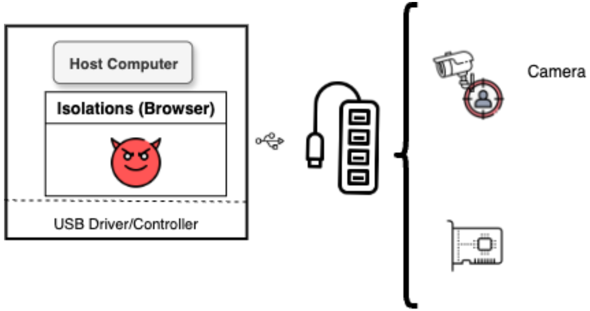
- Goal: Infer the website visited by the victim
- Setting
  - A USB NIC and a USB SSD are connected to the same USB hub
  - Attack Program congests the USB hub via SSD and measures timing variations
  - Different patterns for each website

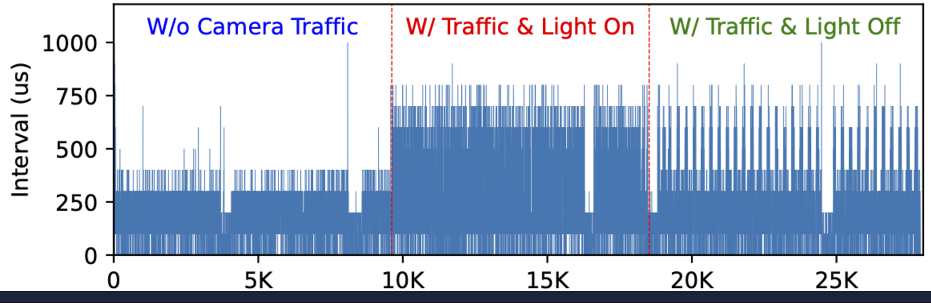




Attack B: Camera Activities

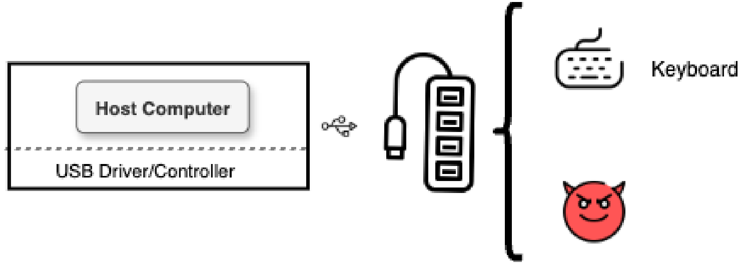
- Goal: Infer activities captured by a webcam
- Setting
  - A USB NIC and USB webcam connected to a shared hub
  - Attacker is a JavaScript program embedded in a webpage
  - Webcam activated, monitor a room

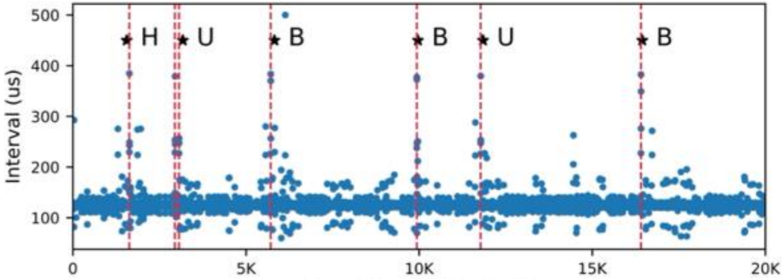




Attack C: Keystrokes

- 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