USBSnoop – Revealing Device Activities via USB Congestions

Davis Ranney, Yufei Wang, A. Adam Ding, Yunsi Fei

Northeastern
College of Engineering

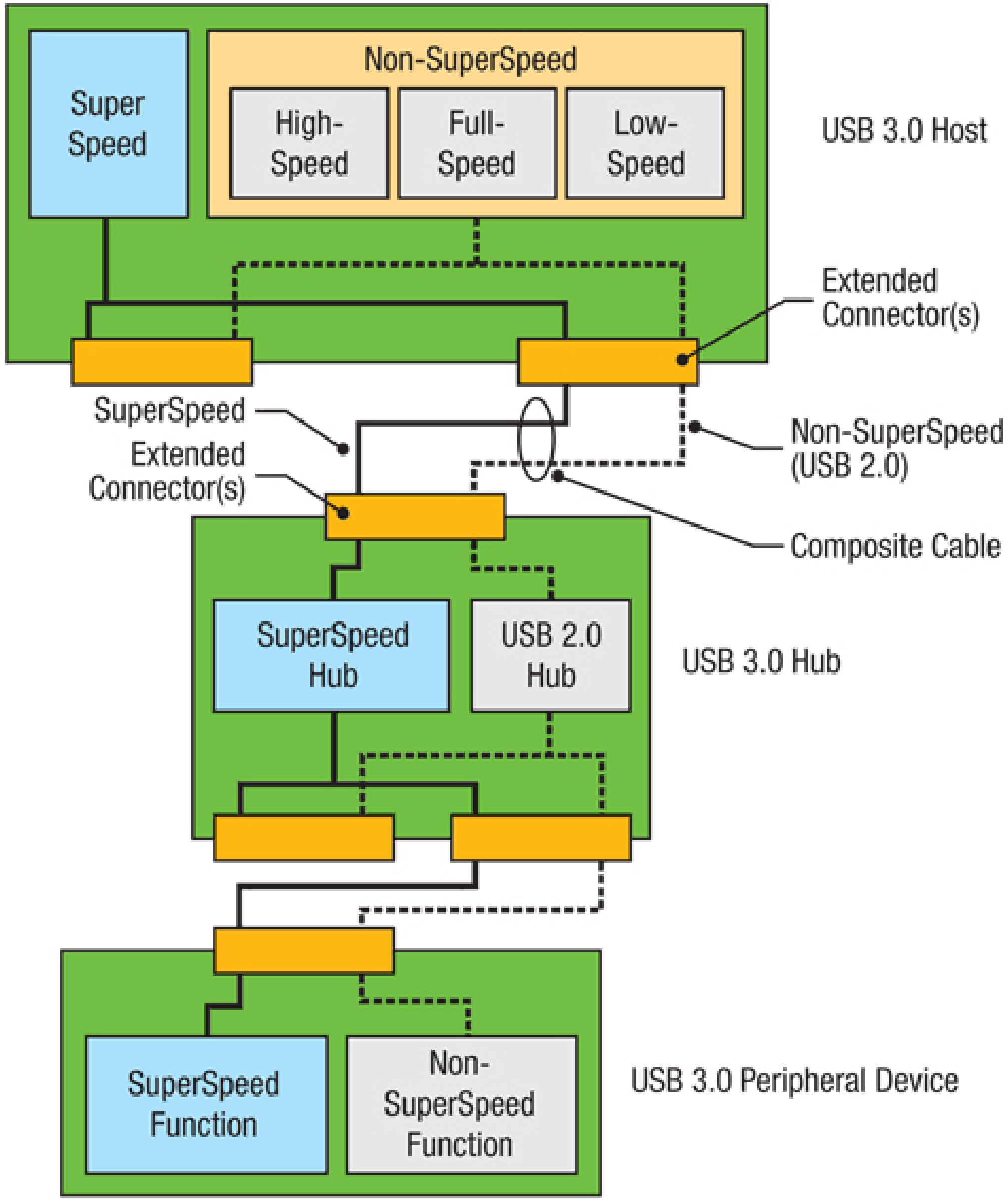
Introduction

USB is Universal

USB is Shared

USB is Vulnerable

- BadUSB & USB Drop Attacks
- Hardware keyloggers
- EM Crosstalk



Note: Simultaneous operation of SuperSpeed and non-SuperSpeed modes is not allowed for peripheral devices

Background

Splitting Bandwidth ≠ Privacy

- Invisible Probe – Exploiting PCIe Congestion

Hubs and bandwidth sharing are integral to USB

Sources of Private Information

- Keyboards
- Mice
- Network Adapters

Threat Model

Devices can inadvertently spy on each other

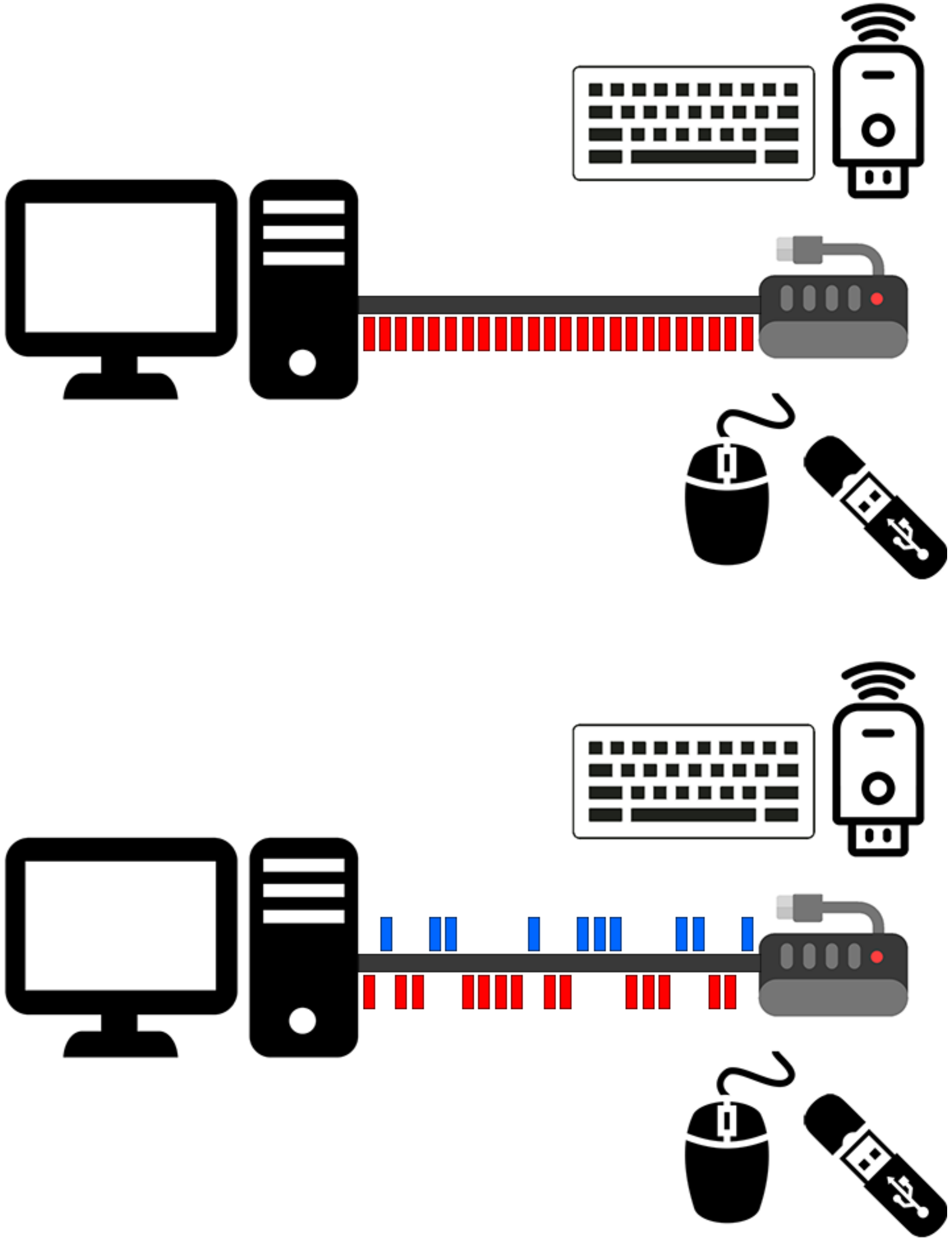
- No direct intrusion
- No man-in-the-middle

Attack #1 - Mouse spying on a keyboard

- Recover typed keystrokes from timing information

Attack #2 - External disk spying on a network adapter

- Recover web traffic activities from changes in the bandwidth



LVX
VERITAS
VIRTVS

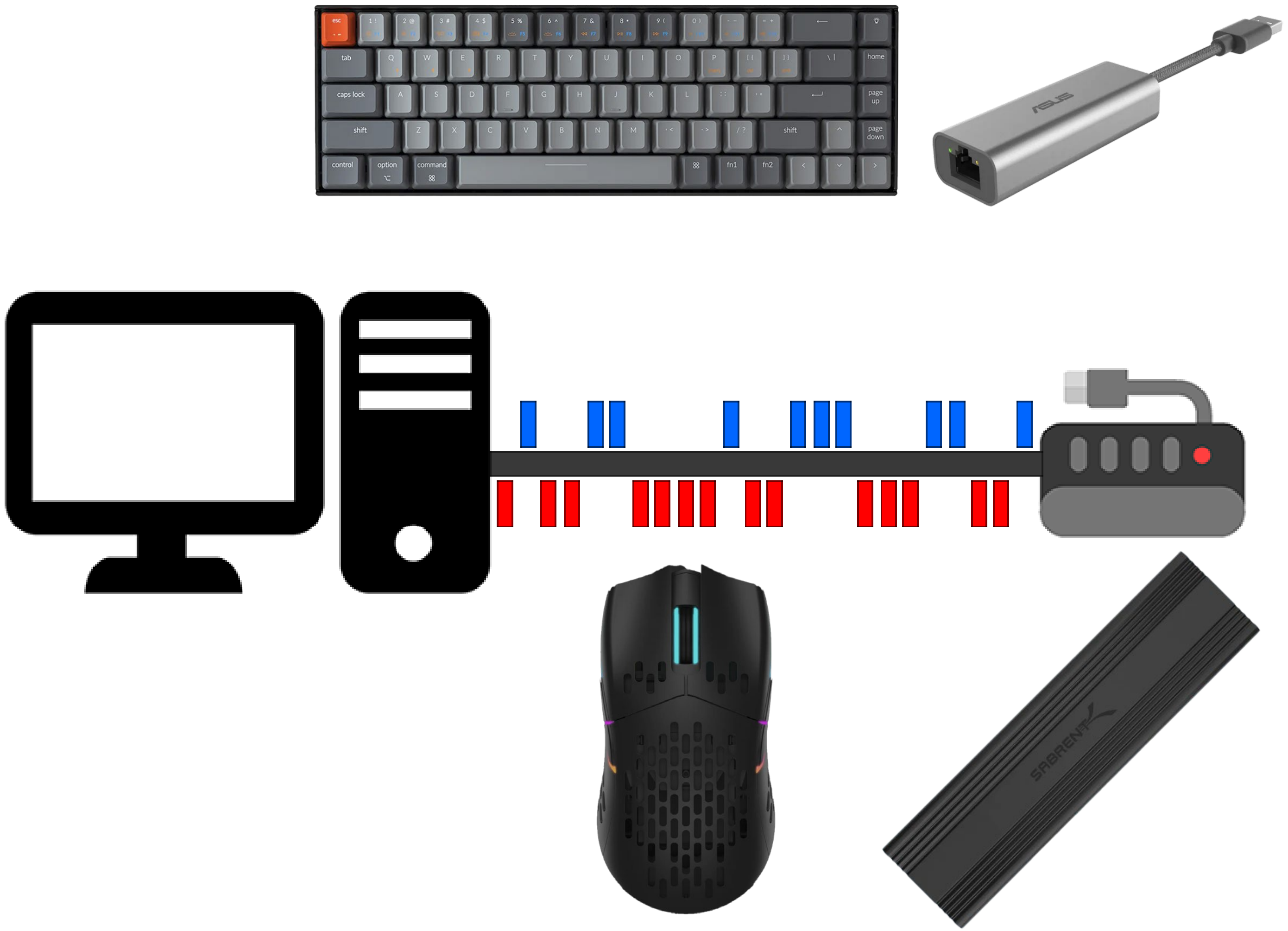
Experimental Setup

Mouse spying on a keyboard

- Inland 4 Port USB 2.0 Hub
  - Keychron M1 mouse
  - Keychron K6 keyboard

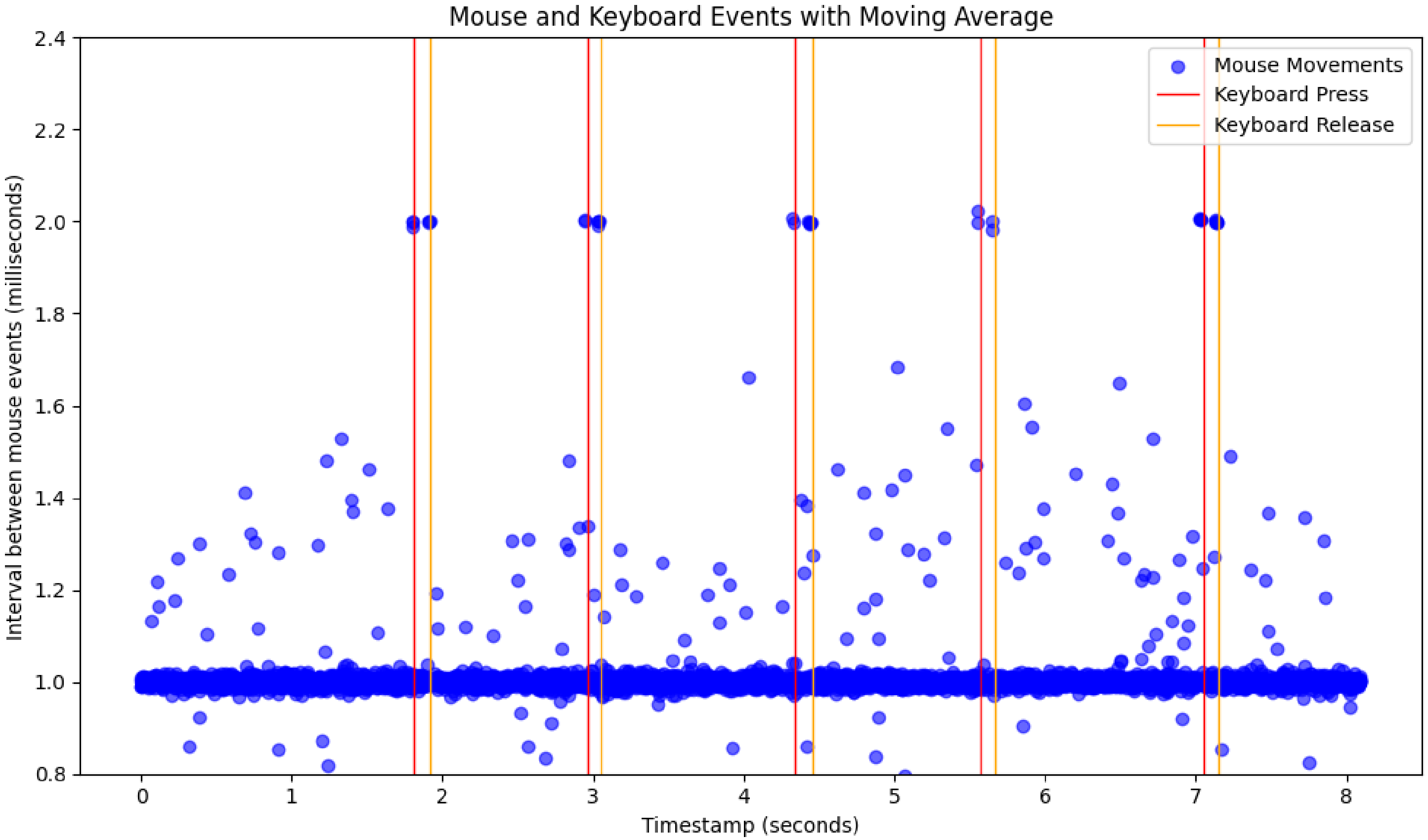
External disk spying on a network adapter

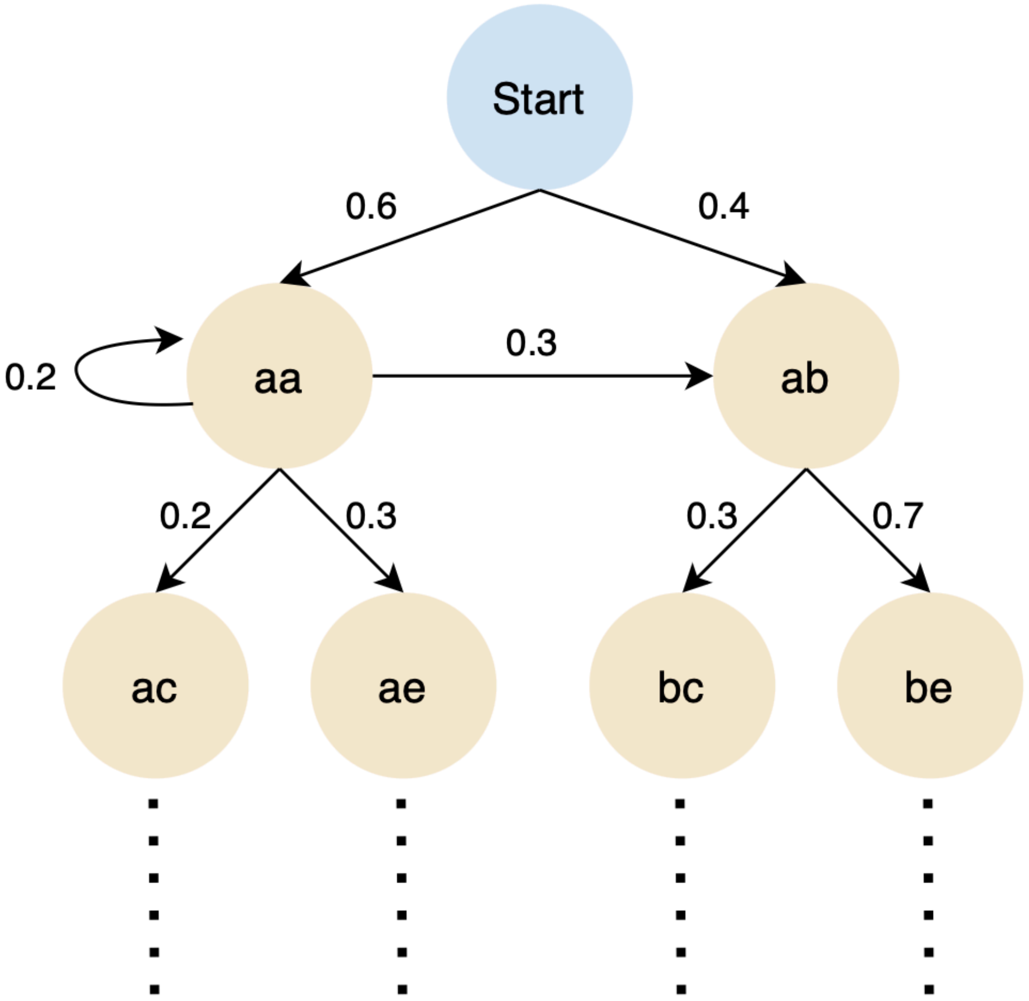
- Inland 4 Port USB 3.0 Hub
  - Sabrent USB 3.2 NVMe Enclosure
  - ASUS USB 3.2 Wired Networking Adapter



Recovering Keystrokes

1. Mouse device constantly sends input updates to host
   a. Can be imperceptible to the user
2. Keyboard is utilized as normal
   a. Congestion occurs with each character typed
3. Timing side-channel of keystrokes to recover the inputted characters





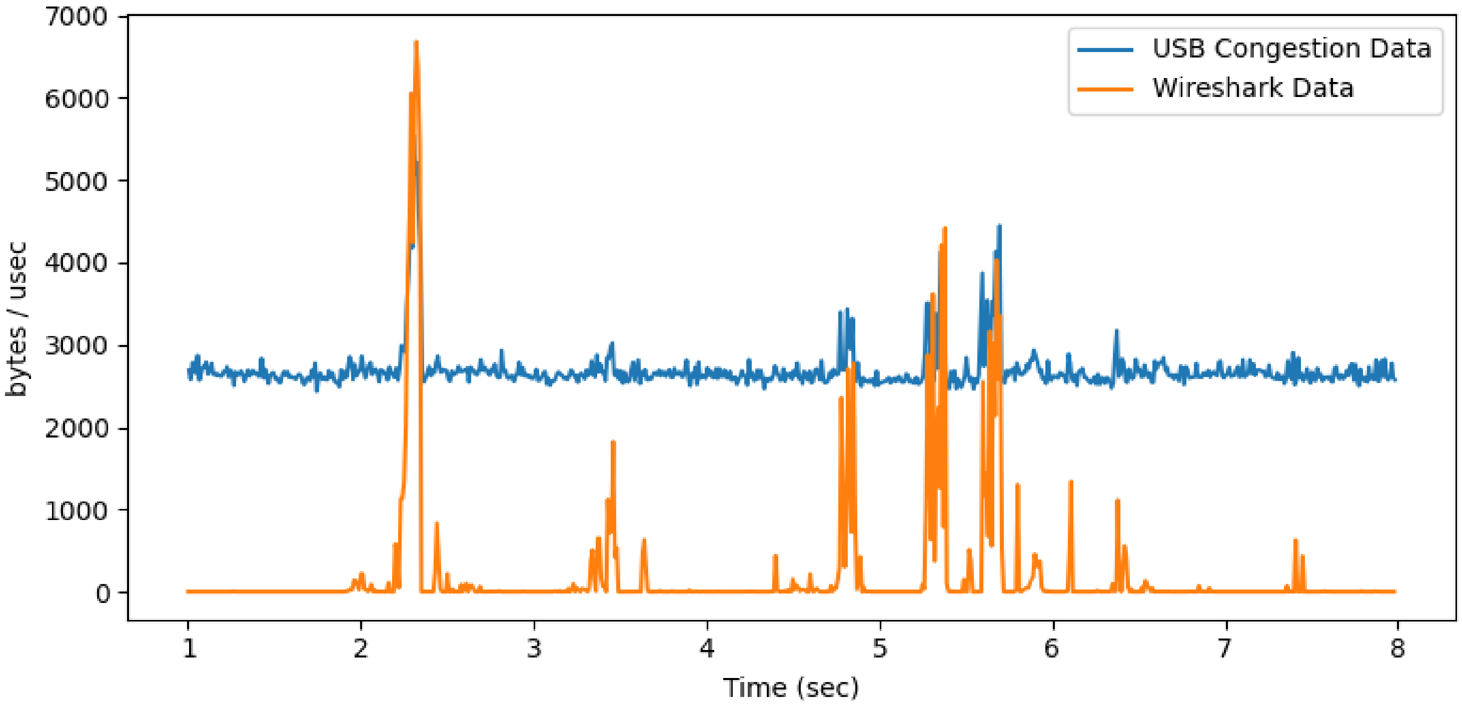
Results – Keyboard Attack

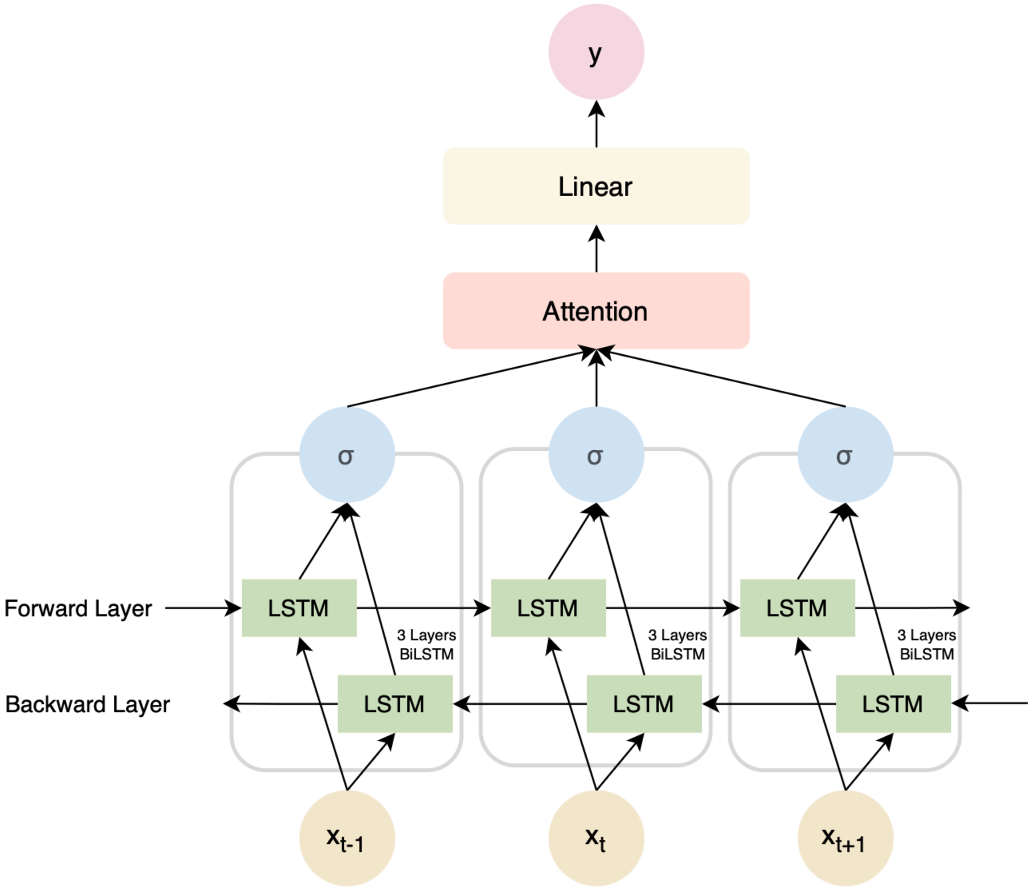
Dataset	Side Channel	Top-10 Accuracy	Top-50 Accuracy
7658 Words 26 Letters	USB (Our Work)	36.3%	89.3%
1000 Words 10 Letters	USB (Our Work)	66.7%	95.3%
	PCIe (Invisible Probe)	69.2%	96.4%
4500 Words 15 Letters	USB (Our Work)	38.0%	86.0%
	Network Traffic (Peeping Tom)	55.8%	93.2%

Recover keystrokes using a Hidden Markov Model (HMM)

Recovering Websites

1. USB drive is induced with constant data reading
   a. Can be executed remotely
2. USB network adapter is utilized to browse websites
   a. Congestion is proportional to website file sizes
3. Timing and bandwidth information can be used as fingerprints for websites





Results – Network Adapter Attack

Dataset	Top-1 Accuracy	Top-3 Accuracy
USB 2.0 Hub – Trained Network	83.4%	89.2%
USB 3.X Hub – Trained Network	81.1%	88.9%
USB Type C Hub – Trained Network	80.6%	87.9%
USB 2.0 Hub – Untrained Network	78.2%	84.7%
USB 2.0 Hub – Untrained VPN Network	70.7%	78.2%
USB 2.0 Hub – Trained VPN Network	81.1%	87.9%

Fingerprint top-100 websites using an Attention-Based Long-Short-Term-Memory (LSTM) Model

General Attack Design

Attackers distribute or hack USB devices with added functionality

- Induce congestion via emulated mouse and disk

Collect data on users’ web history and keystrokes

- Can collect informed data on what usernames and passwords are used on specific websites

Difficult to mitigate because devices seem benign

- Stop USB trust-by-default, must authorize new devices
- Change the USB bandwidth sharing paradigm

Thank You

Northeastern University
College of Engineering

References

- J. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates, and K. Butler, “SoK: “Plug & Pray” Today – Understanding USB Insecurity in Versions 1 Through C,” in 2018 IEEE Symposium on Security and Privacy (SP), May 2018, pp. 1032–1047, iSSN
- K. Nohl and J. Lell, “BadUSB - On Accessories that Turn Evil,” Aug. 2014. [Online]. Available: https://www.youtube.com/watch?v=nuruzFqMgIw
- M. Tan, J. Wan, Z. Zhou, and Z. Li, “Invisible Probe: Timing Attacks with PCIe Congestion Side-channel,” in 2021 IEEE Symposium of Security and Privacy (SP). San Francisco, CA, USA: IEEE, May 2021, pp. 322–338.: 2375-1207.
- K. Zhang and X. Wang, “Peeping tom in the neighborhood: keystroke eavesdropping on multi-user systems,” in Proceedings of the 18th conference on USENIX security symposium, ser. SSYM’09. USA: USENIX Association, Aug. 2009, pp. 17–32.
- Q. Yang, P. Gasti, K. Balagani, Y. Li, and G. Zhou, “USB side-channel attack on Tor,” Computer Networks, vol. 141, pp. 57–66, Aug. 2018.
- J. Hardwick, “Top 100 Most Visited Websites (US and Worldwide),” Oct. 2023. [Online]. Available: https://ahrefs.com/blog/most-visited-websites/