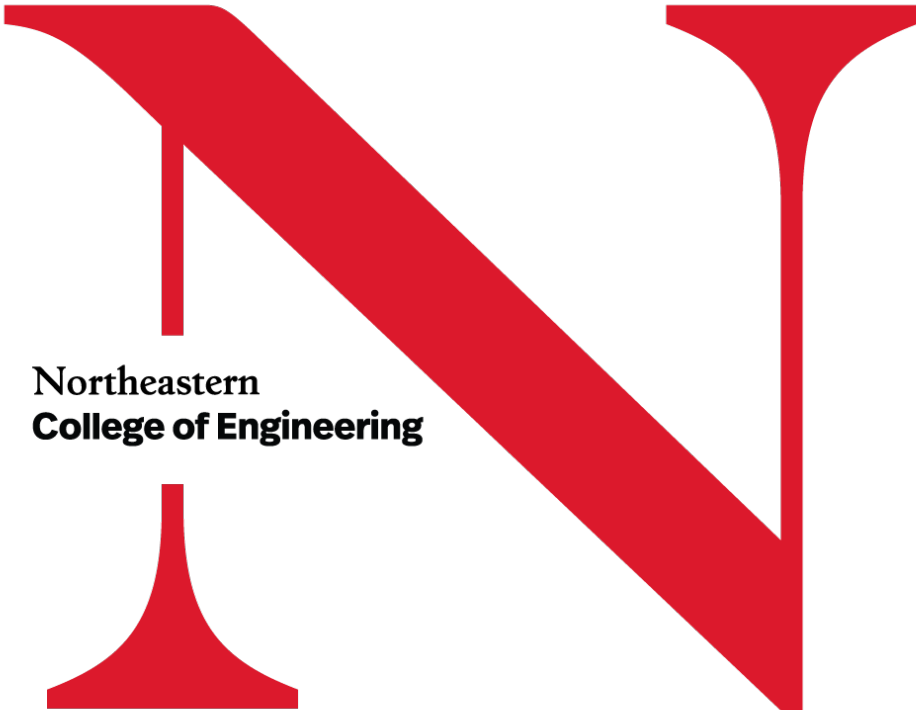
USBSnoop – Revealing Device Activities via USB Congestions

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

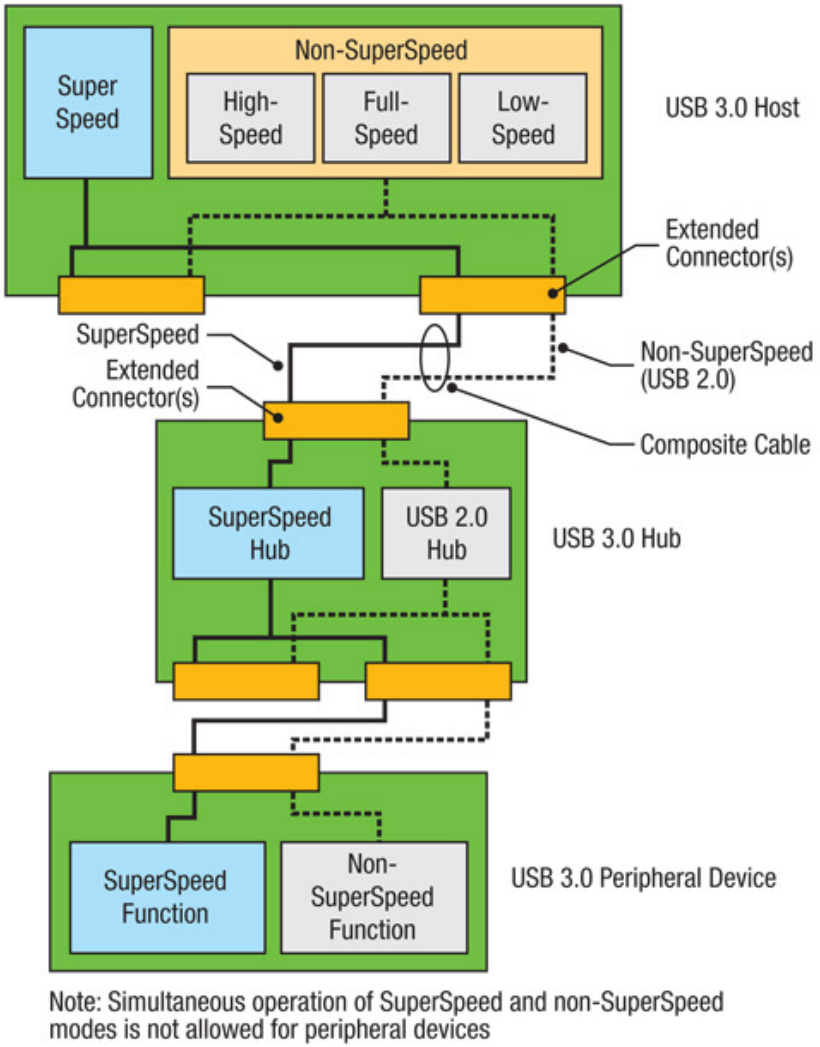


Introduction

USB is Universal

USB is Shared

USB is Vulnerable



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

Background

Splitting Bandwidth ≠ Privacy

Hubs are Integral to USB

Sources of Private Information

- Keyboards
- Mice
- Network Adapters

Threat Model

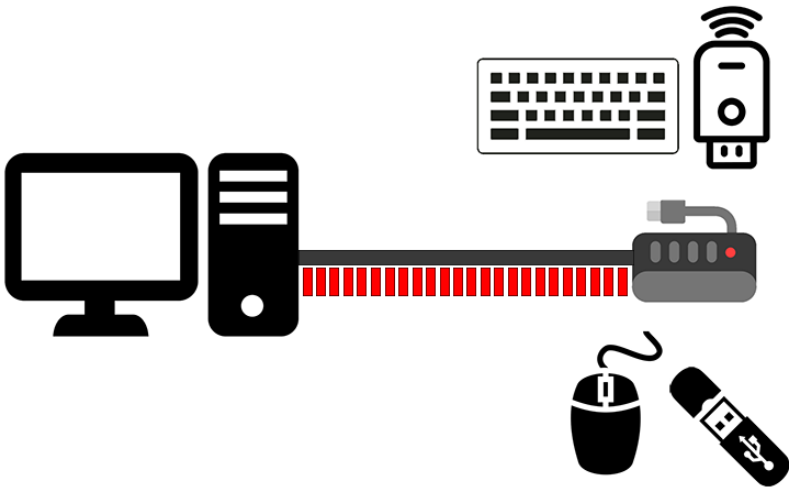
Devices can spy on each other

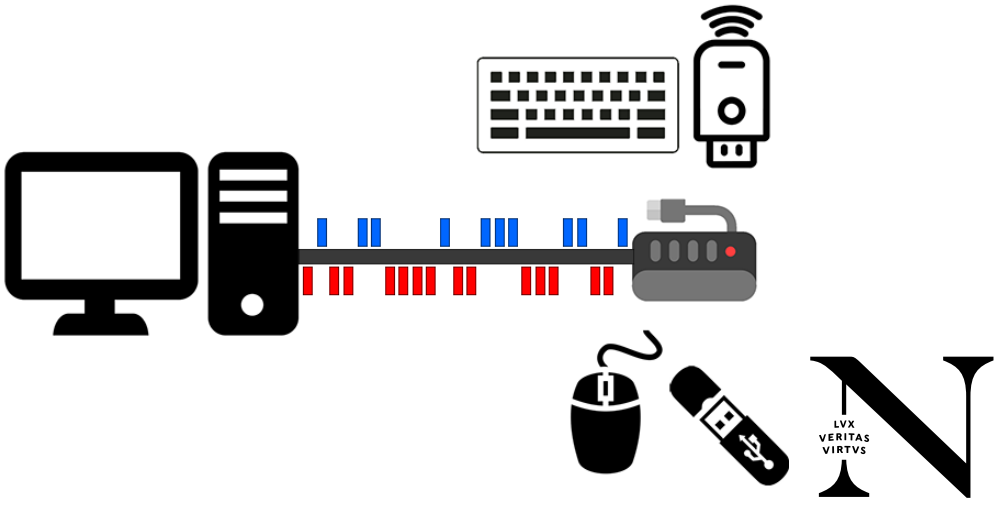
Attack #1

- Mouse spying on a keyboard

Attack #2

- External disk spying on a network adapter





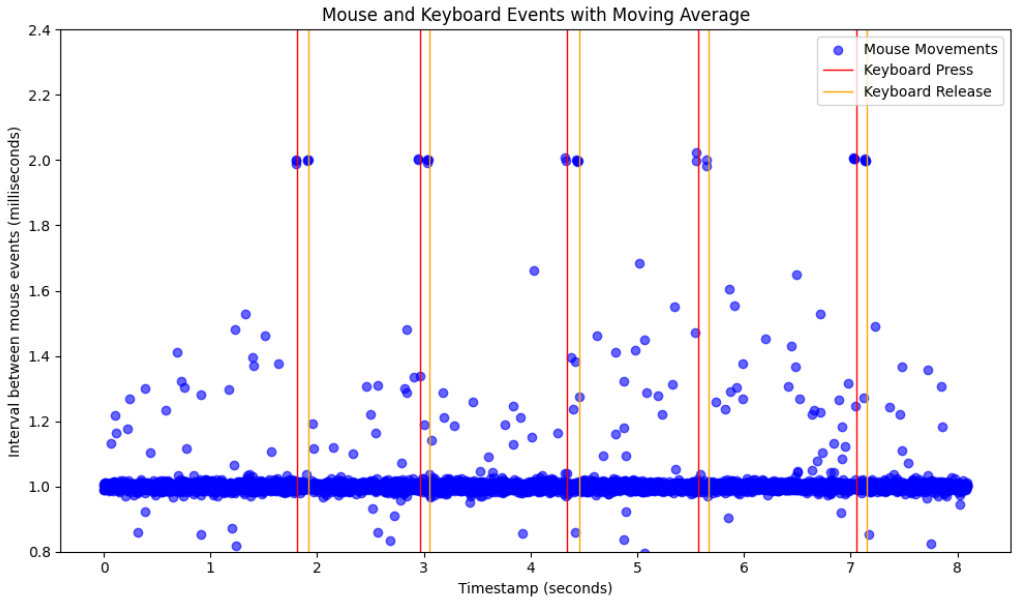
Attack

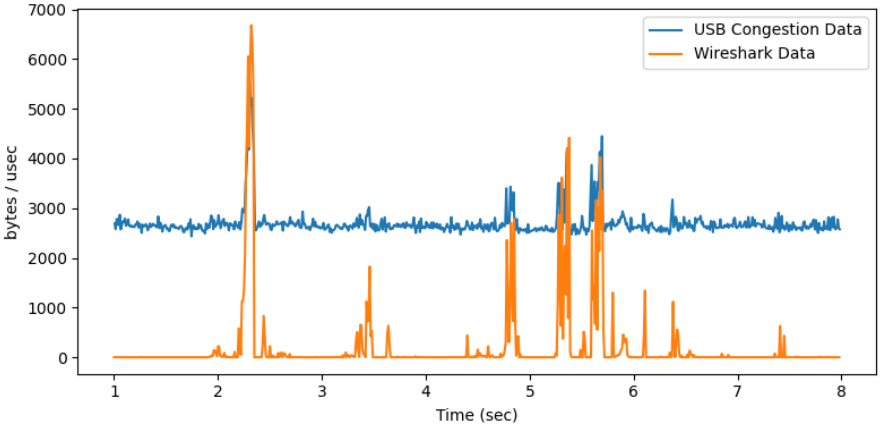
Attack #1 – Recovering Keystrokes

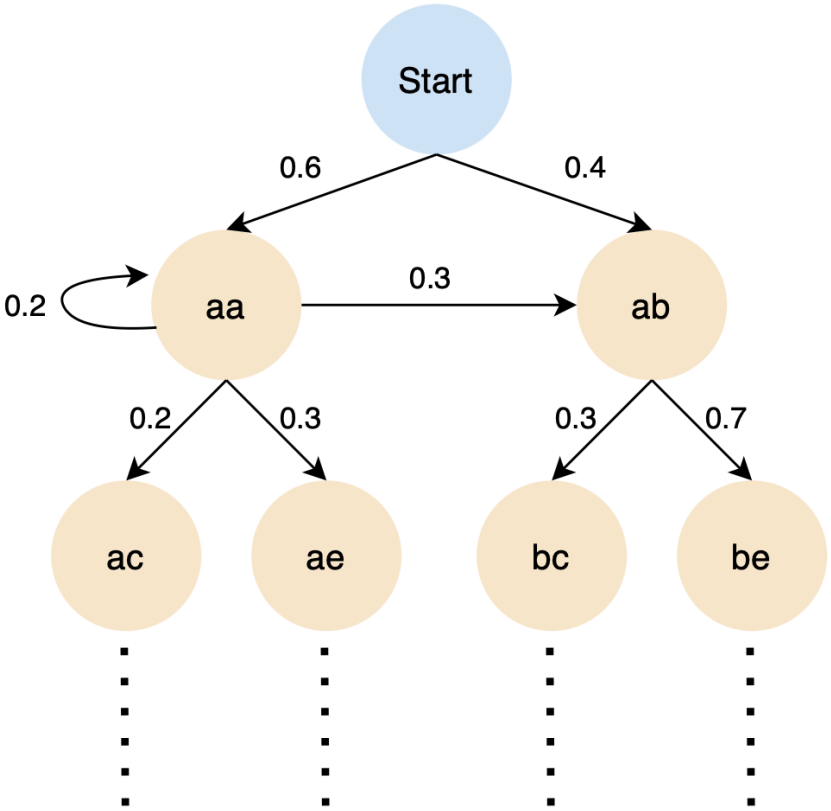
- Mouse updates conflict with keyboard updates

Attack #2 – Recovering Web Traffic Patterns

- Data transfer from USB drive saturates full bandwidth



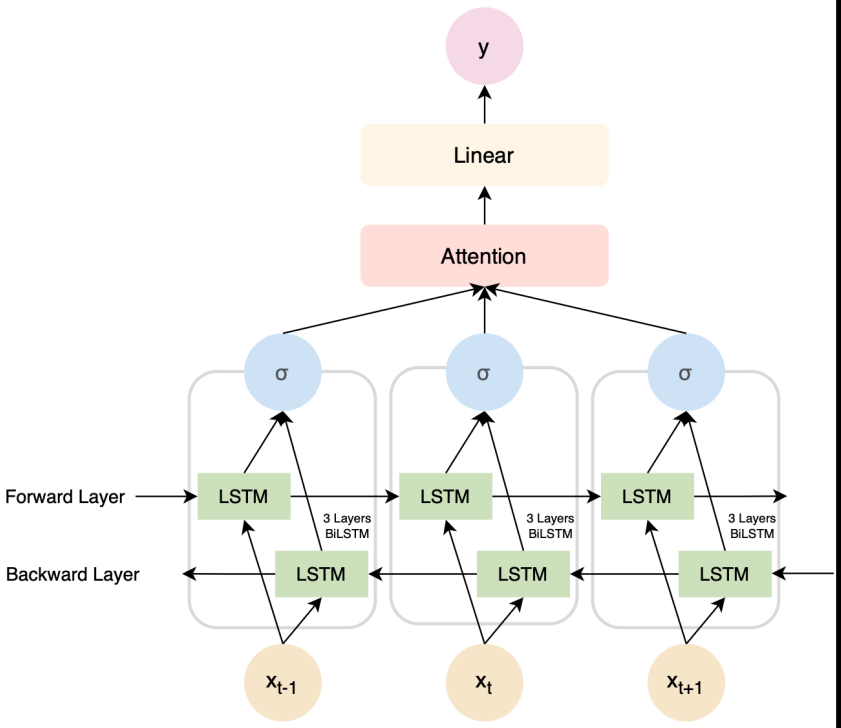




Results – Keyboard Attack

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 Hidden Markov Model (HMM)



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 browsed websites using Attention-Based Long-Short-Term-Memory (LSTM) Model