The Impostor Among US(B): Off-Path Injection Attacks on USB Communications

Robbie Dumitru[*†], Daniel Genkin[‡], Andrew Wabnitz[†], and Yuval Yarom[*§]

[*] THE UNIVERSITY of ADELAIDE

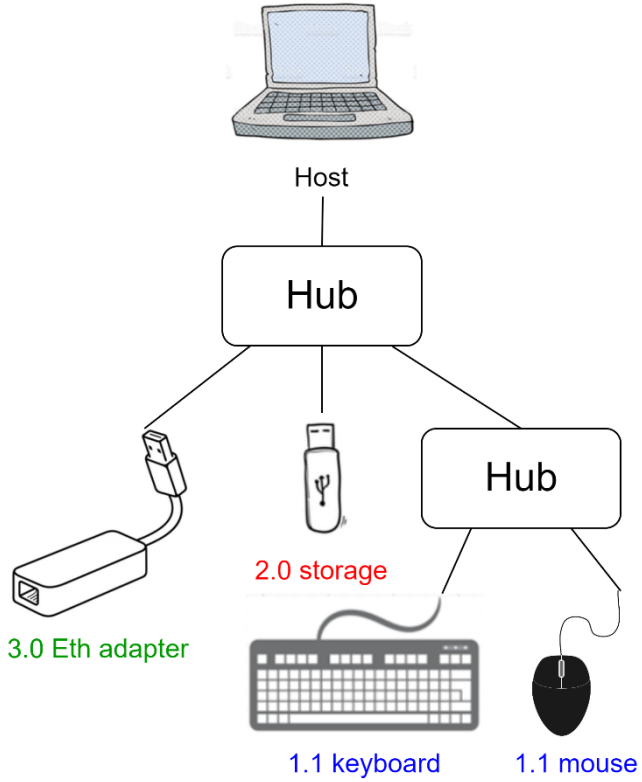
[†] Australian Government Department of Defence Science and Technology

[‡] Georgia Tech

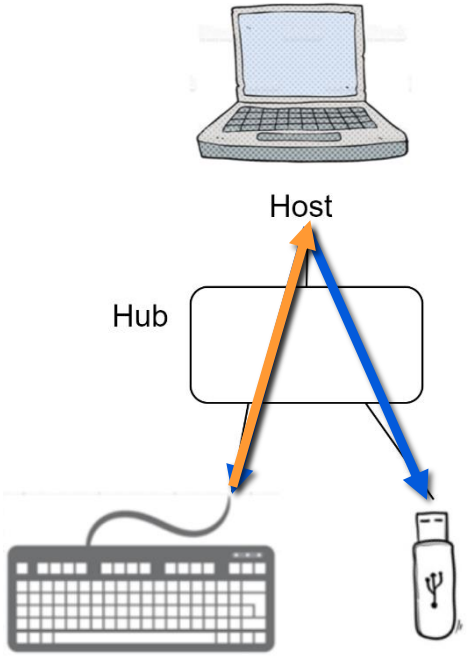
[§] RUB

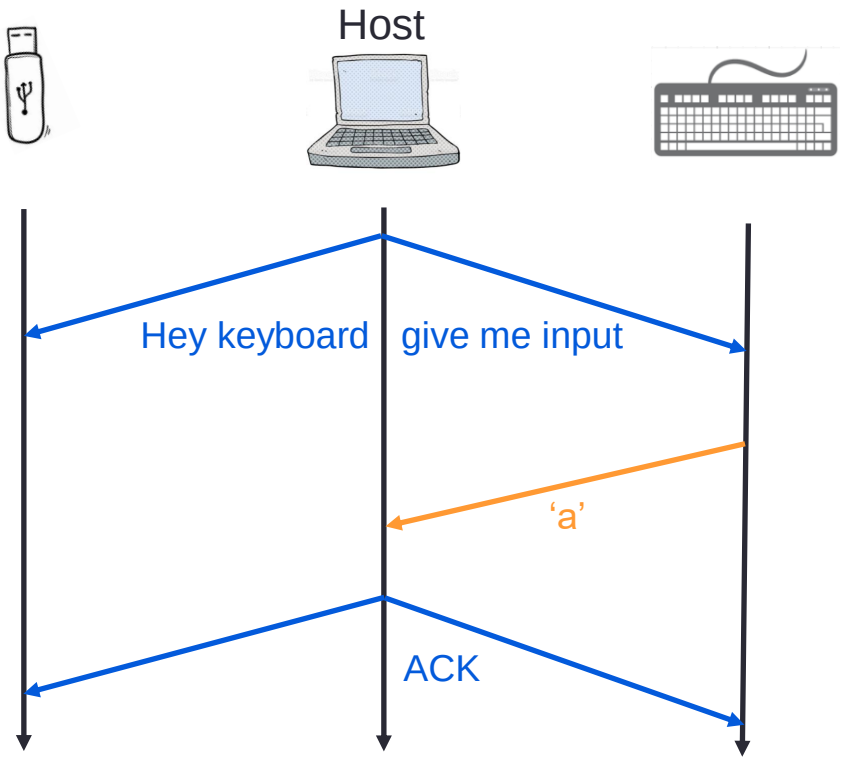
USB Overview

- USB 1.0 (1996), …, USB4 (2019)
- Various speed modes, electrical interfaces & connector types
- Tree topology:
  - host = root
  - hubs = nodes
  - devices = leaves
- Backward compatibility built-in
- Host-arbitrated shared bus



USB 1.1 & 2.0 Communication Model

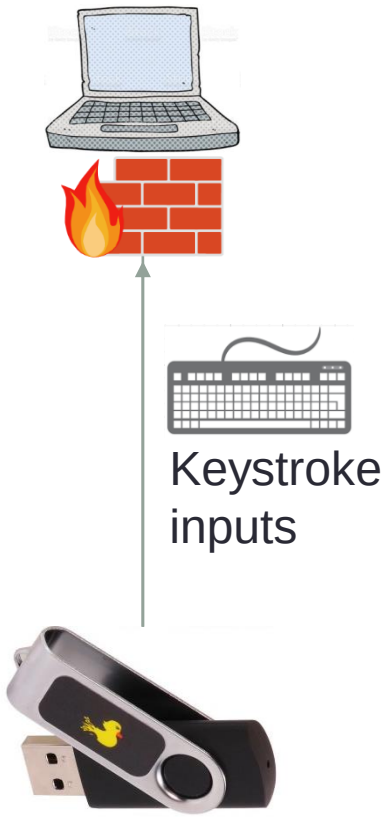




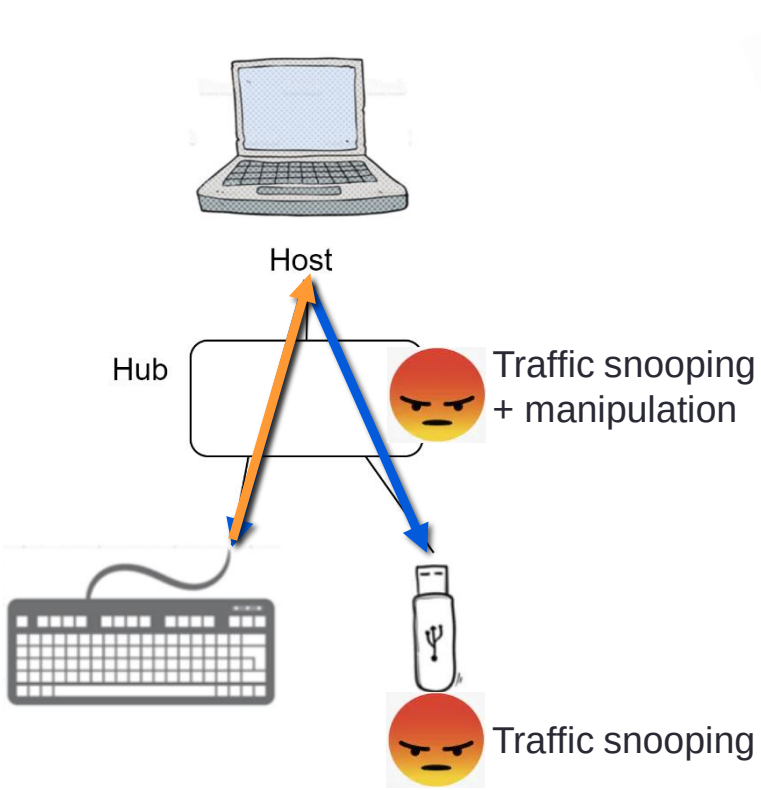
USB Built-in Security Measures

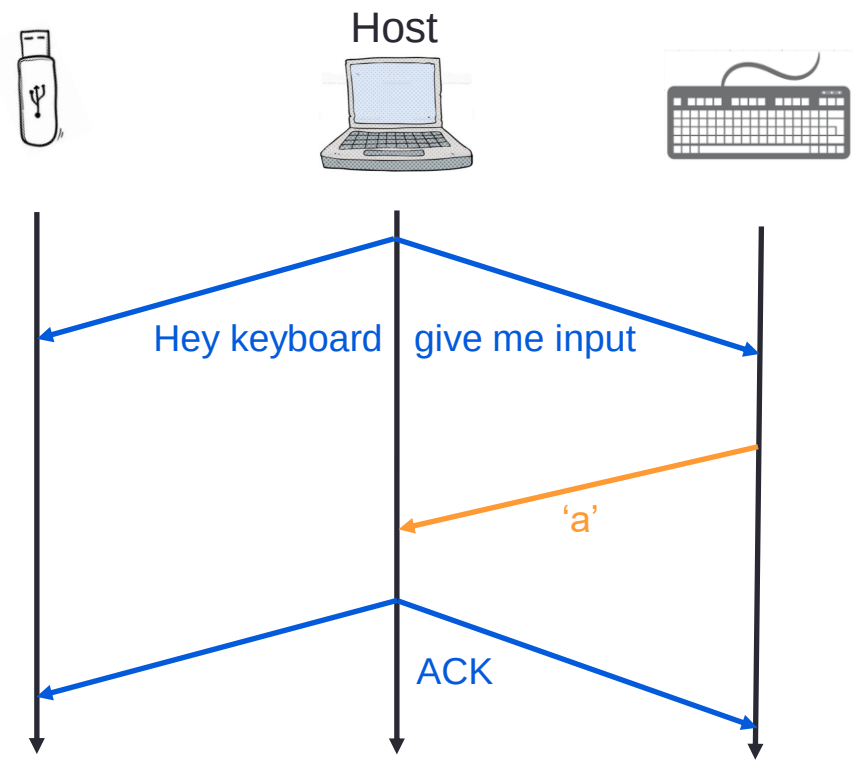
Masquerading Attacks

- Innocuous devices with unexpected function
- Typically emulating keyboards
- Leverages:
  - Default trust
  - User-understanding gap
- Firewall approach in software is the go-to defence

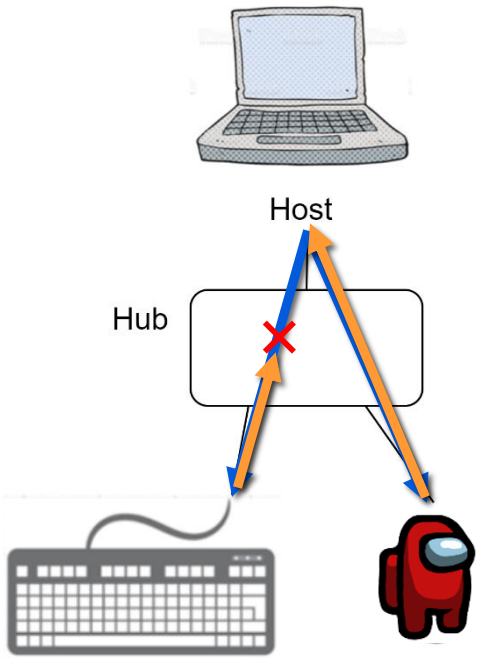


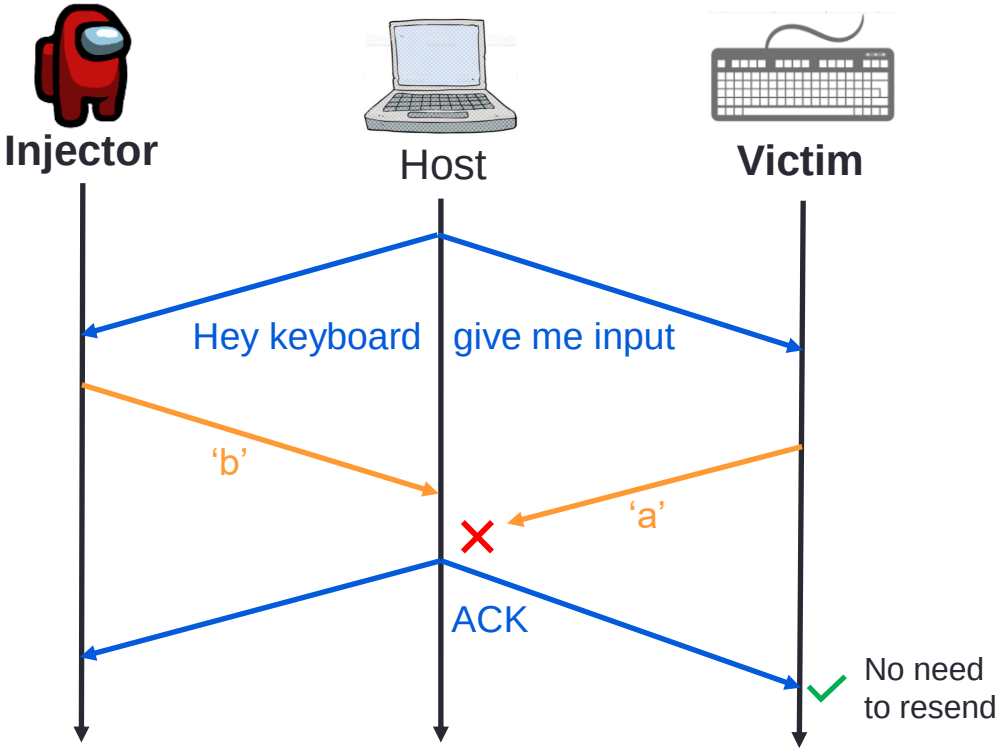
USB 1.1 & 2.0 Prior Attacks



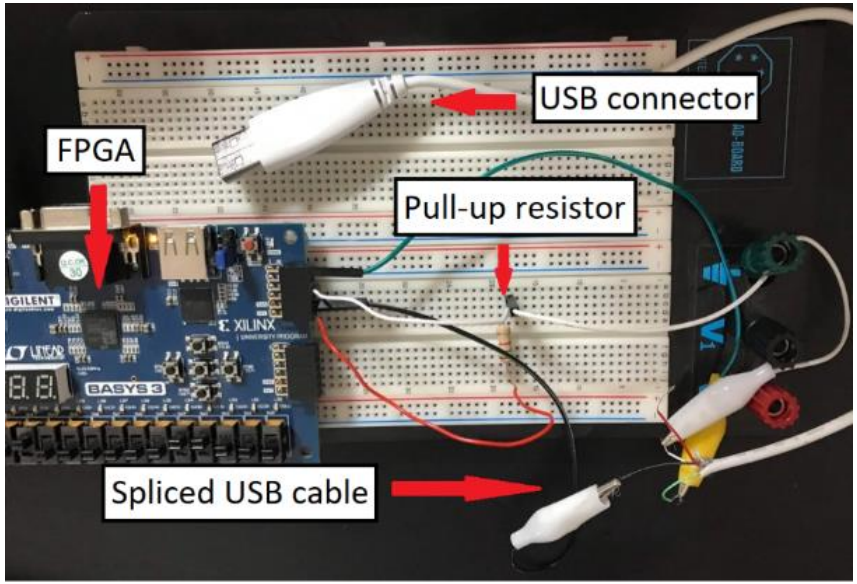


Our Work – Off-Path Injection





Keystroke Injection Demo !

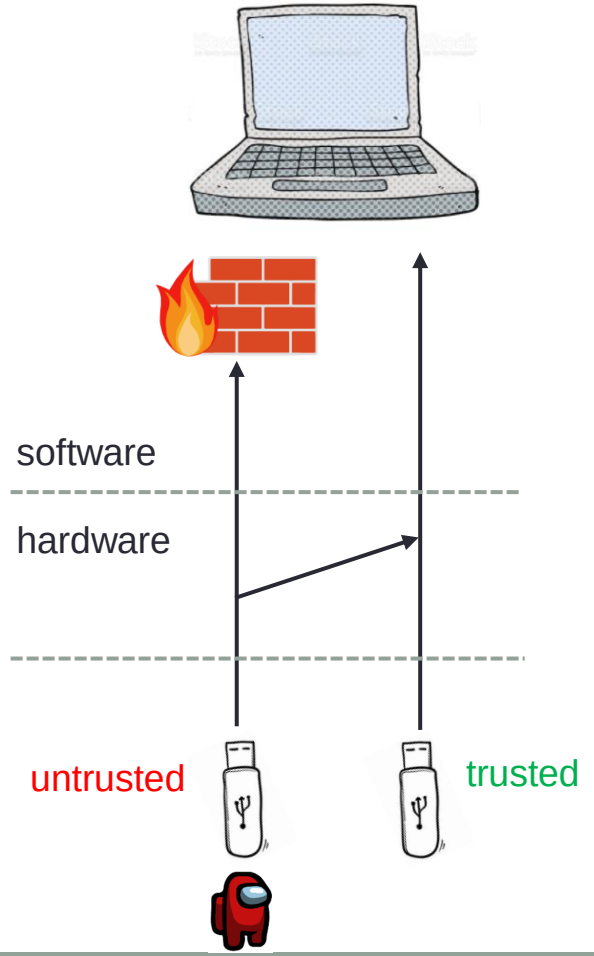


Impact

- Can exploit **any** USB interface trusted in software
- 48% of hubs found vulnerable
- Some motherboards also found vulnerable
- Keystroke injection
- OS install hijack

Policies bypassed:

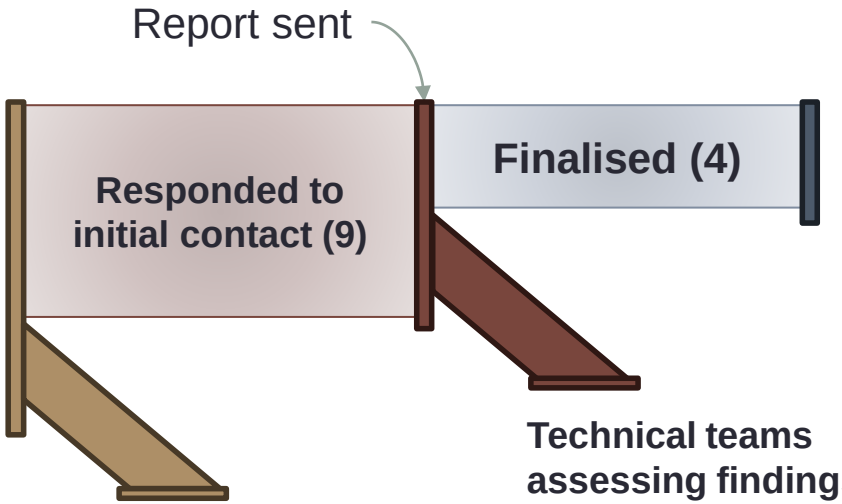
- `USBFilter` (*Sec. '16*)
- `GoodUSB` (*ACSAC '15*)
- USB-LOCK-RP By Advanced Systems International
- USBGuard
- Oracle VirtualBox



Responsible Disclosure

Contacted affected parties (14):

- USB-IF
- Hub vendors
- Software vendors



“Not relevant with our hubs”,
“Not a network device”,
“Product discontinued”,
“Taken into account”

Summary

Hardware-level signal injection bypassing software-based protections

- Keystroke injection using adjacent mouse
- OS installation hijack using adjacent serial device
- **Open Source** – Keystroke injector source RTL available at:
  https://github.com/0xADE1A1DE/USB-Injection

Paper

Code