Invisible Probe: Timing Attacks with PCIe Congestion Side-channel

Mingtian Tan*, **Junpeng Wan***, Zhe Zhou†
Fudan University
{18210240176, 19210240003, zhouzhe}@fudan.edu.cn

Zhou Li
University of California, Irvine
zhou.li@uci.edu

*The first two authors are equally contributed
† Zhe Zhou is the corresponding author

PCIe protocol

PCIe protocol

- De facto protocol to connect CPU and peripheral devices

PCIe protocol

- De facto protocol to connect CPU and peripheral devices
- Increasing numbers of peripheral devices connects to CPU

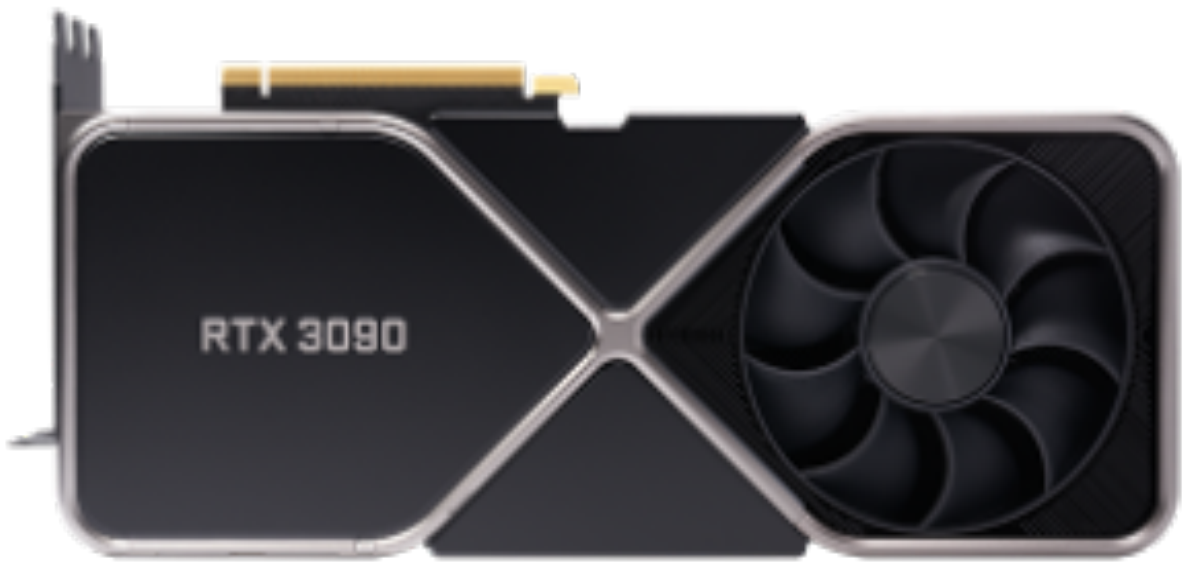

PCIe protocol

- De facto protocol to connect CPU and peripheral devices
- Increasing numbers of peripheral devices connects to CPU
- CPU PCIe interfaces increase slower

PCIe protocol

- De facto protocol to connect CPU and peripheral devices
- Increasing numbers of peripheral devices connects to CPU
- CPU PCIe interfaces increase slower

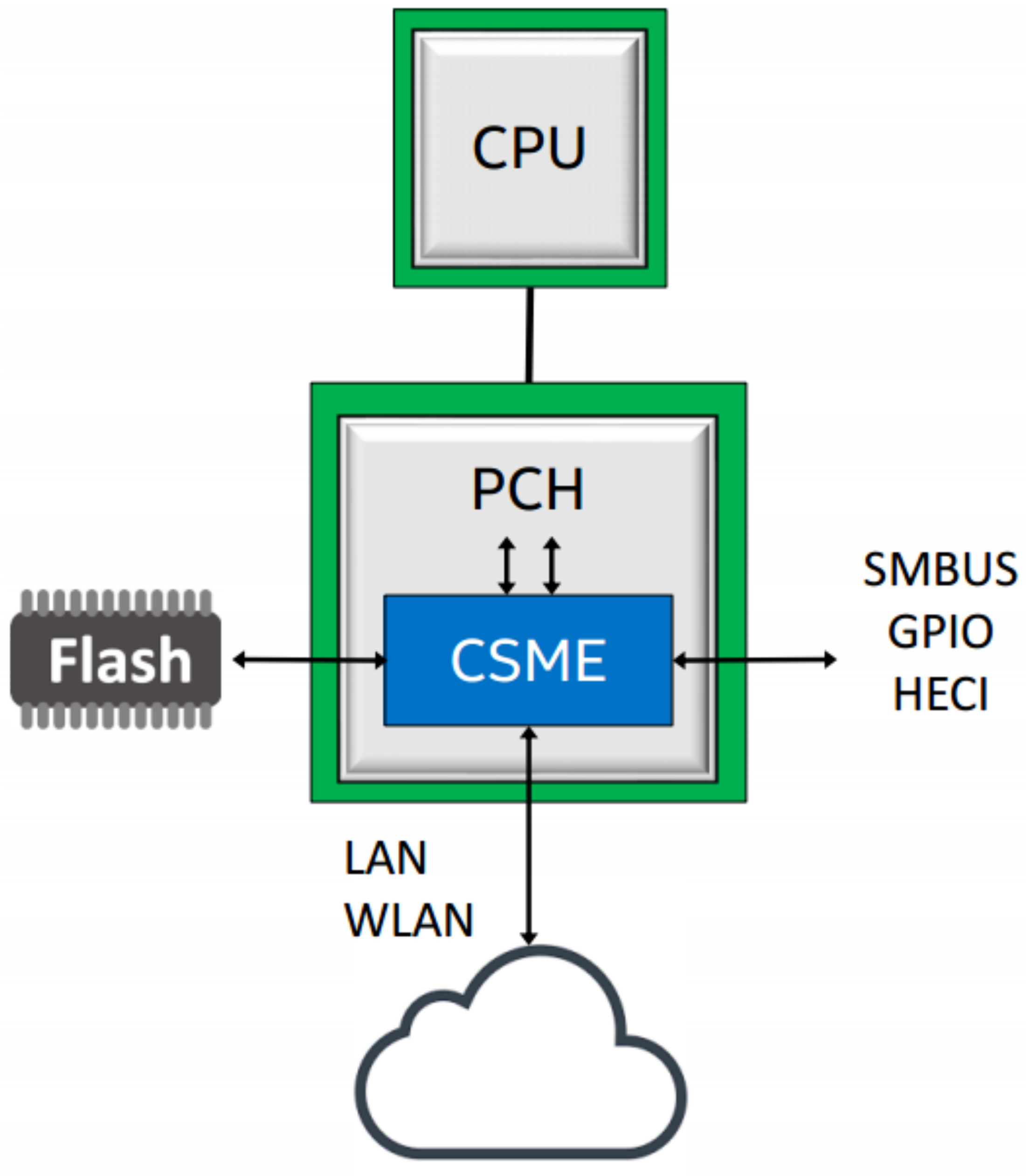
GAP!



IO Switches to support more PCIe interfaces

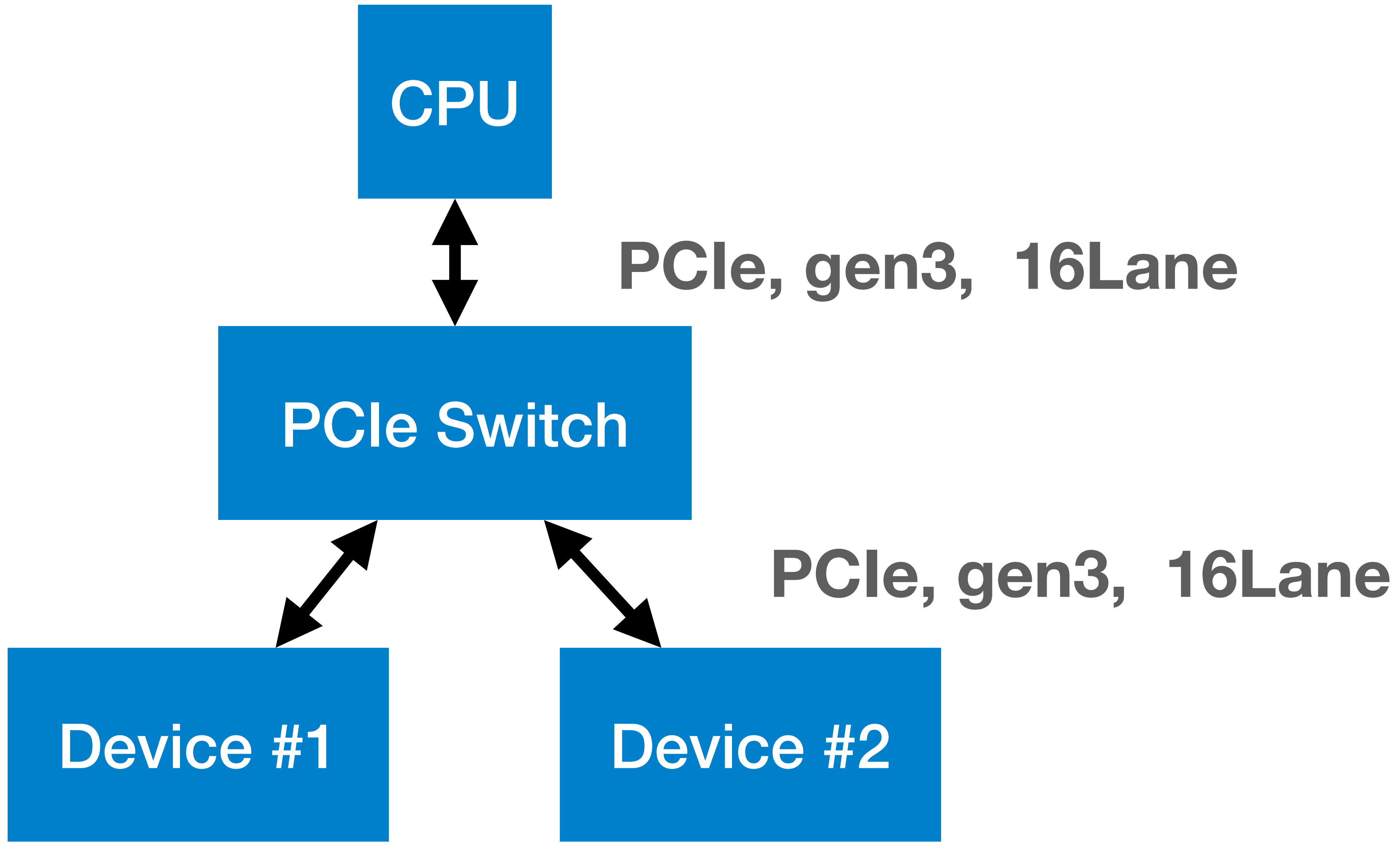
IO Switches to support more PCIe interfaces

Platform Controller Hub (PCH)



[3]

PCIe Switch



Problems of sharing channels

Problems of sharing channels

- Throughput decrease

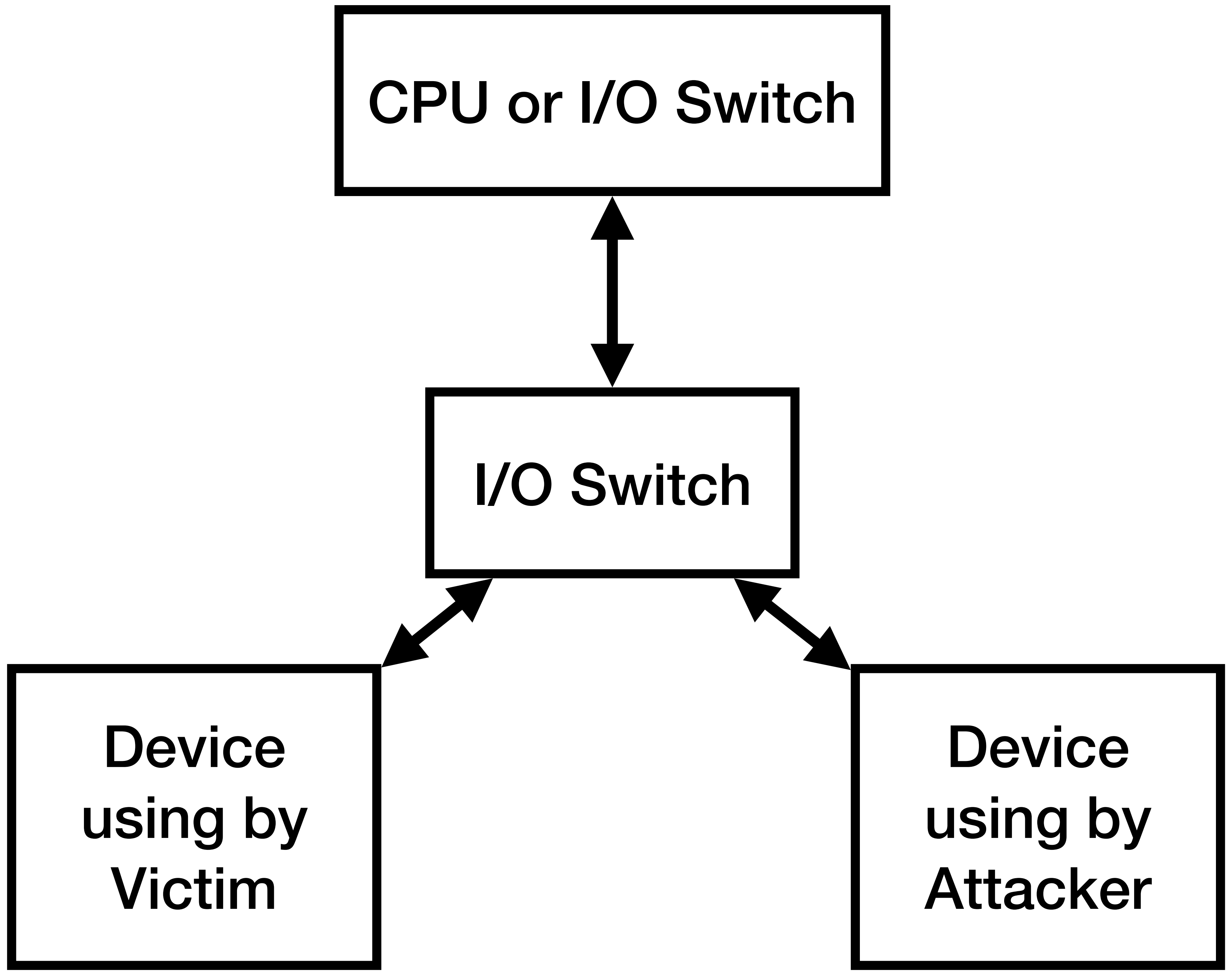
Problems of sharing channels

- Throughput decrease
- Delays introduced

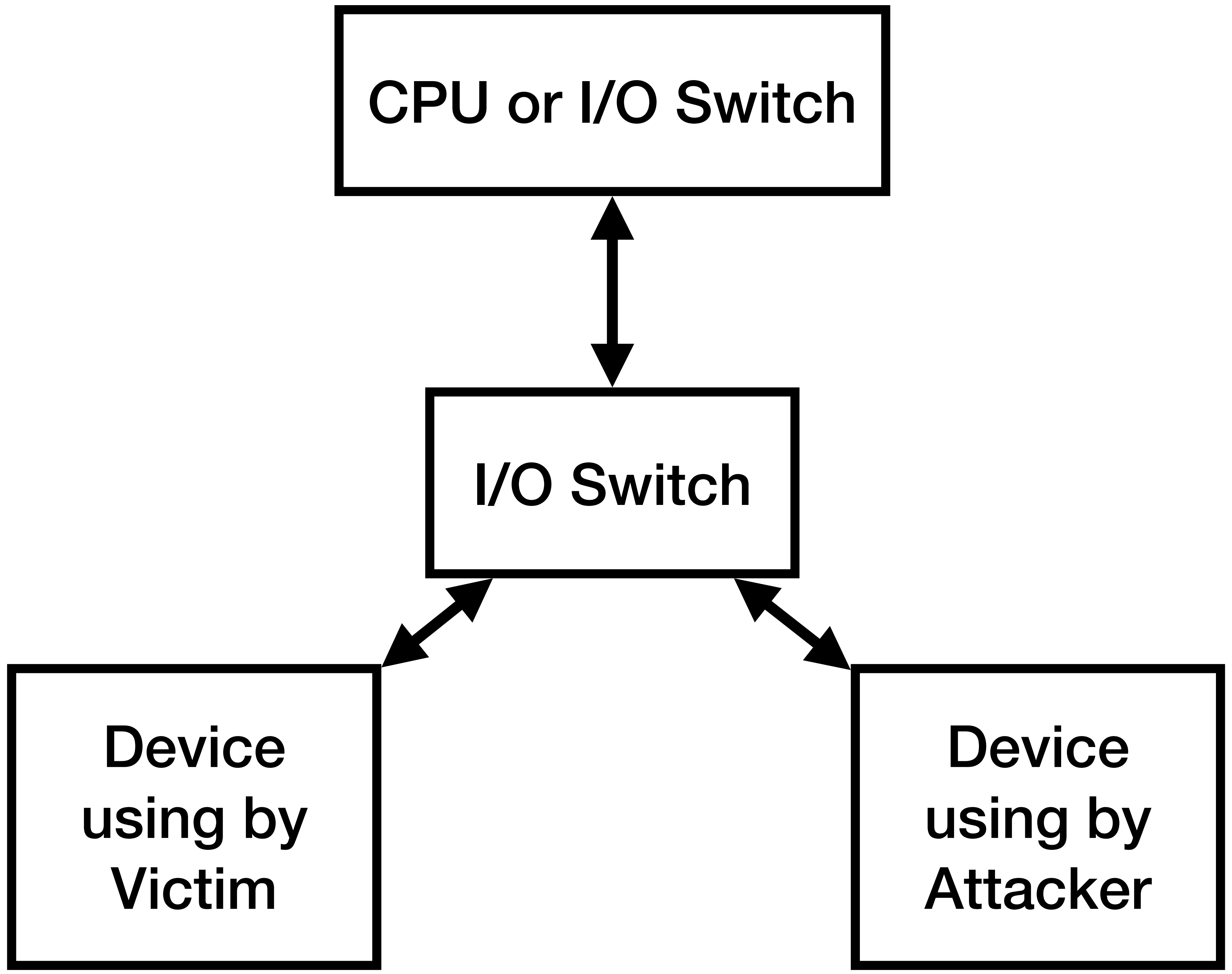
Problems of sharing channels

- Throughput decrease
- Delays introduced
- Secrets leaking! (Side Channel Attack)

Threat Model

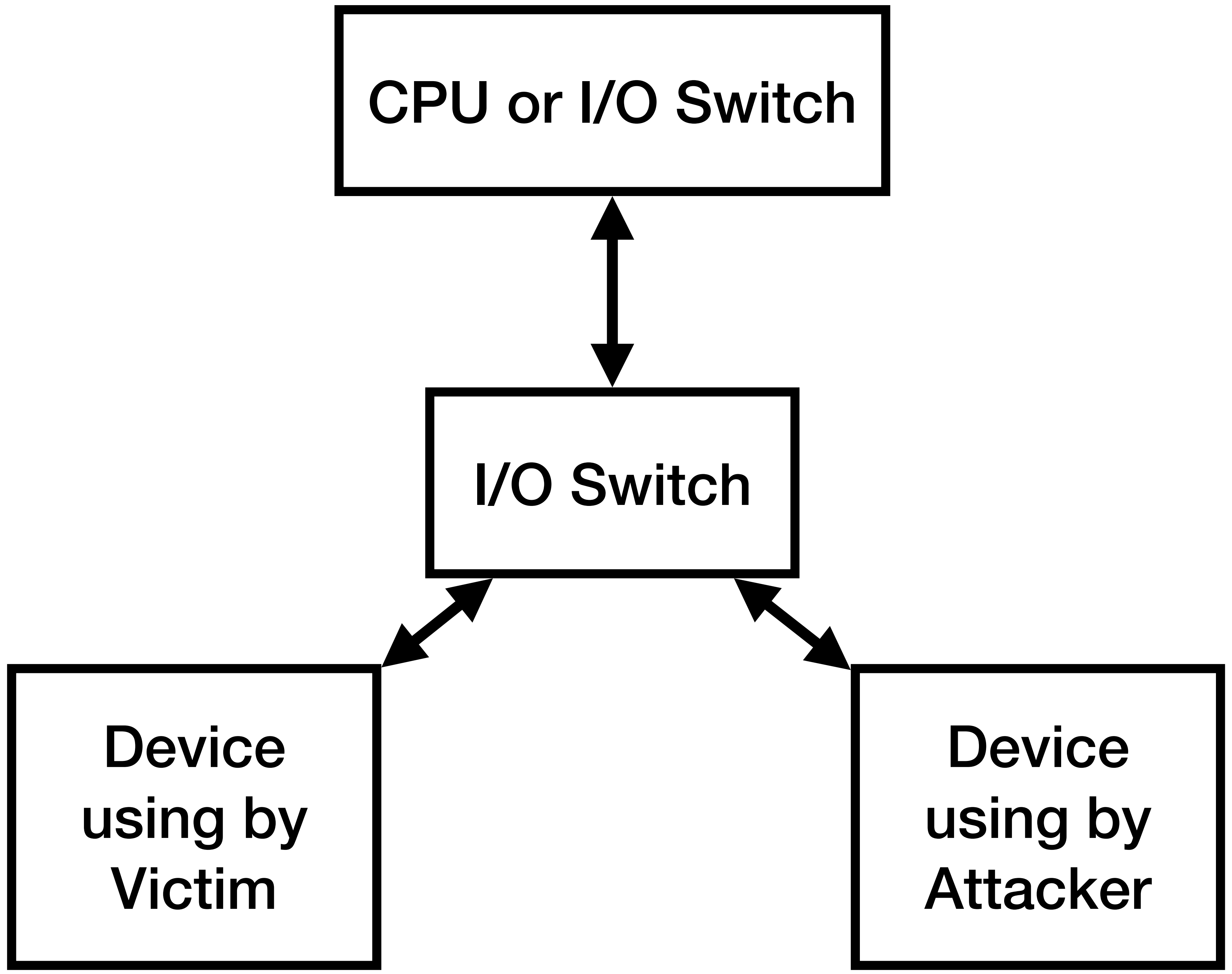


Threat Model



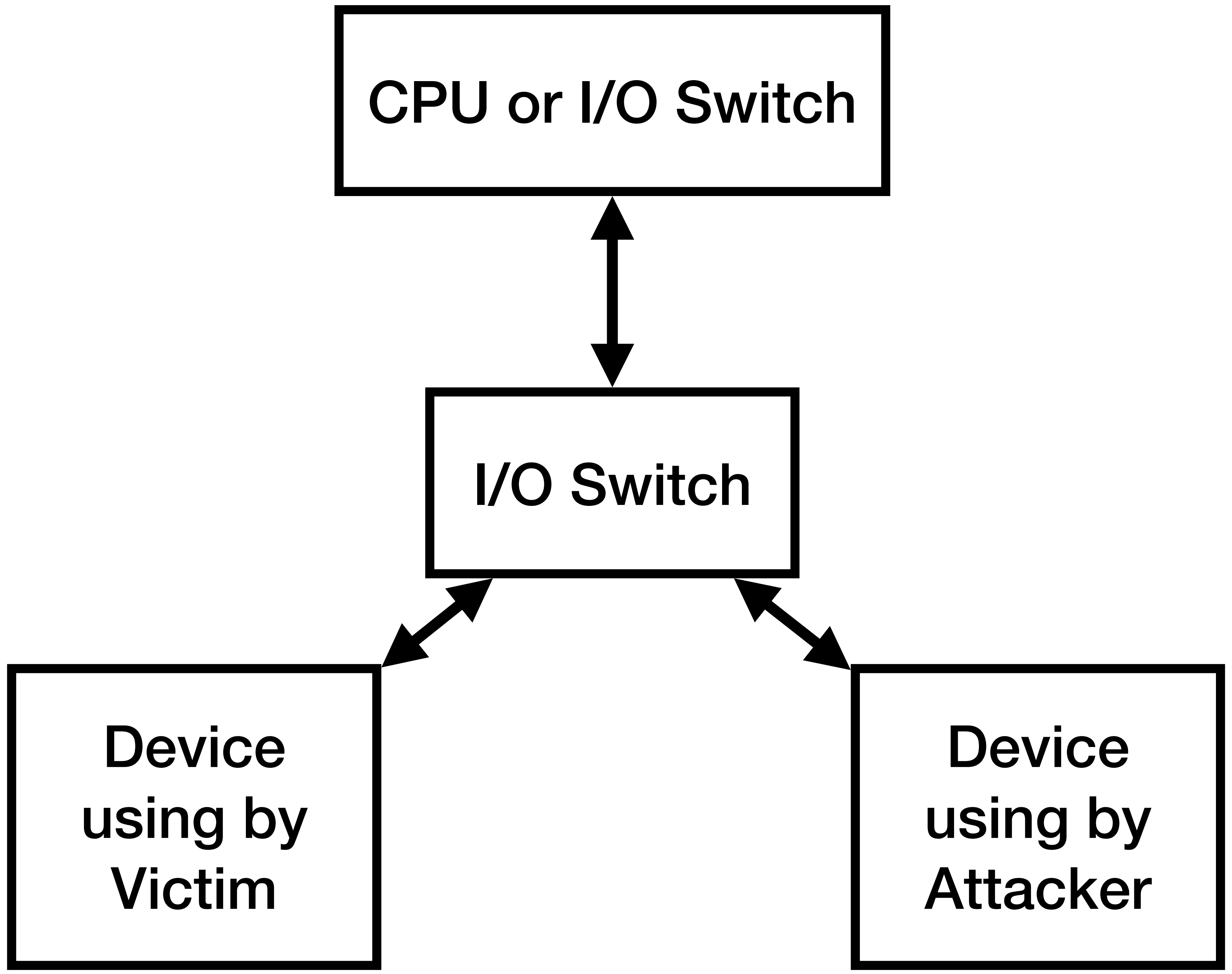
- A pair of I/O devices:
  - one for attacker
  - another for victim

Threat Model



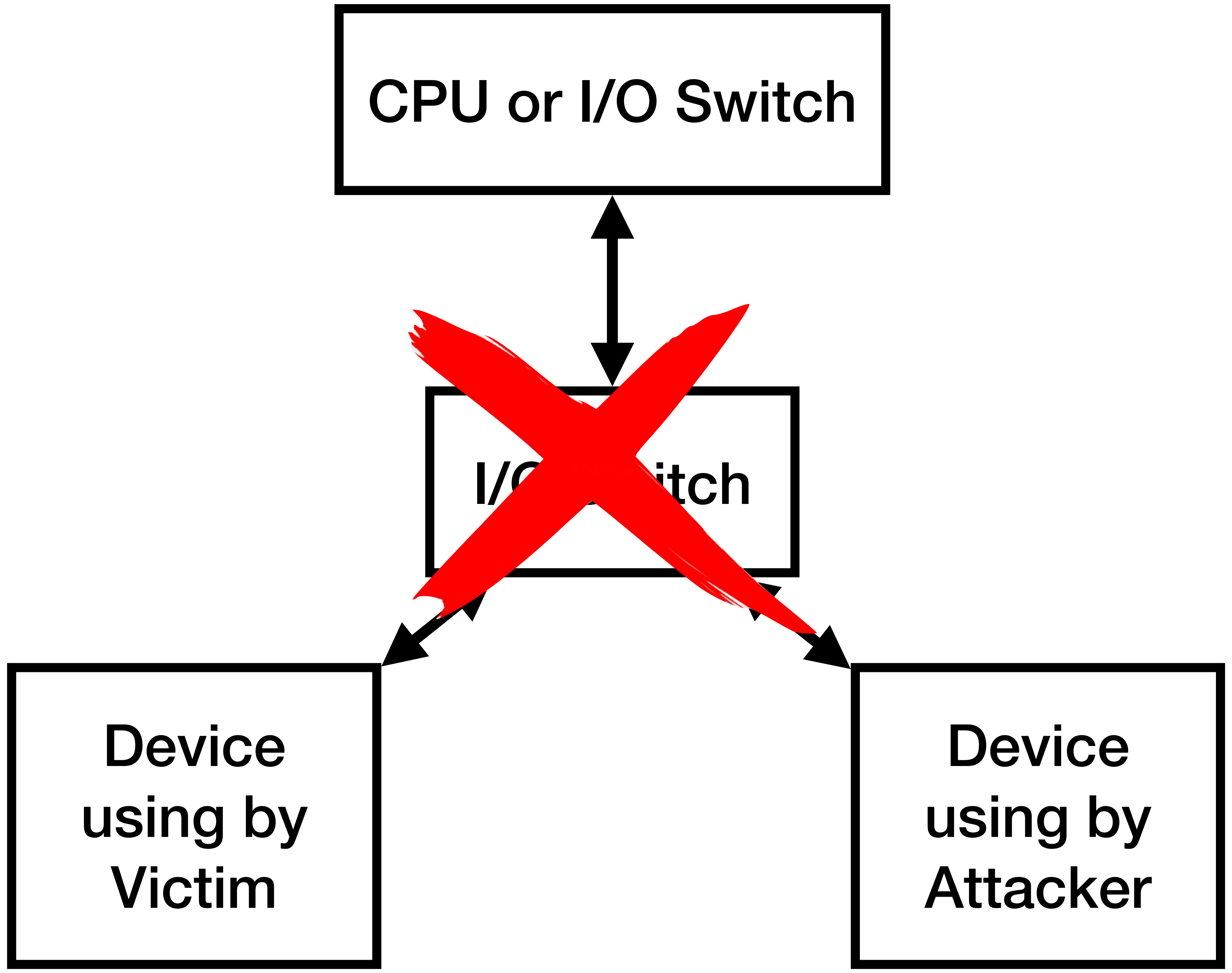
- A pair of I/O devices:
  - one for attacker
  - another for victim
- Devices share **same I/O switch**

Threat Model



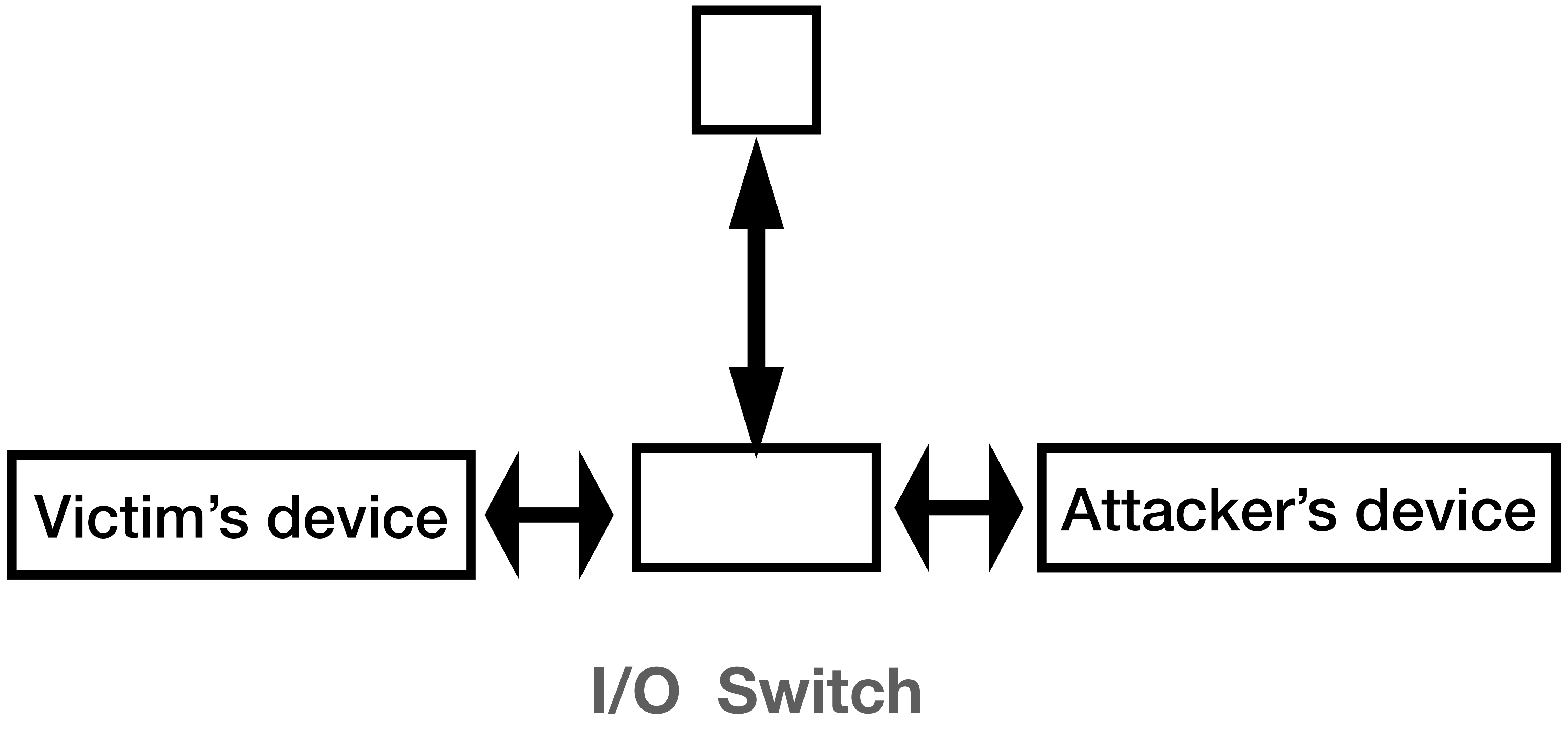
- A pair of I/O devices:
  - one for attacker
  - another for victim
- Devices share **same I/O switch**
- Attacker **cannot access** victim's data or code directly

Threat Model

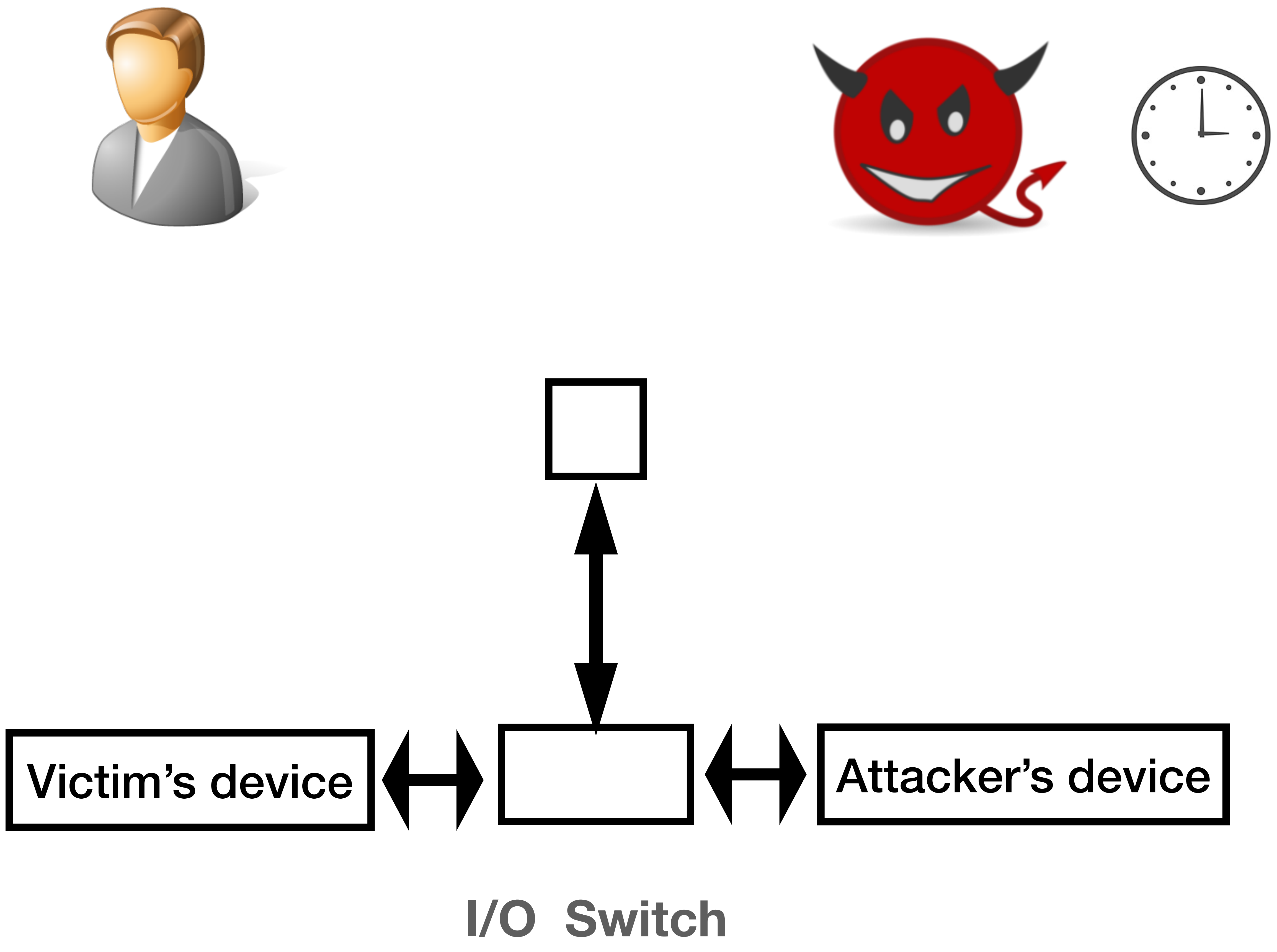


- A pair of I/O devices:
  - one for attacker
  - another for victim
- Devices share **same I/O switch**
- Attacker **cannot access** victim's data or code directly

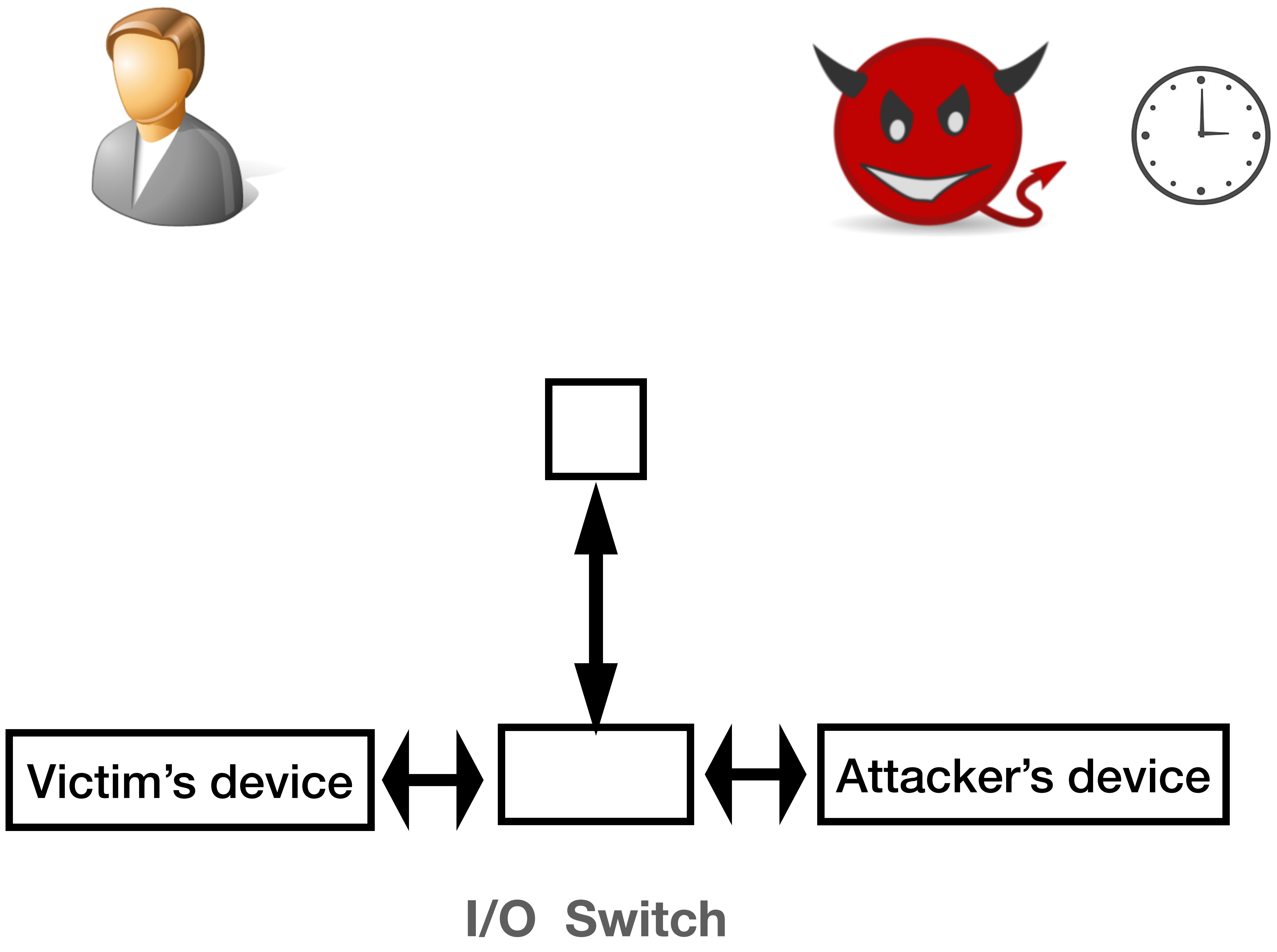
Why are the data leaked?

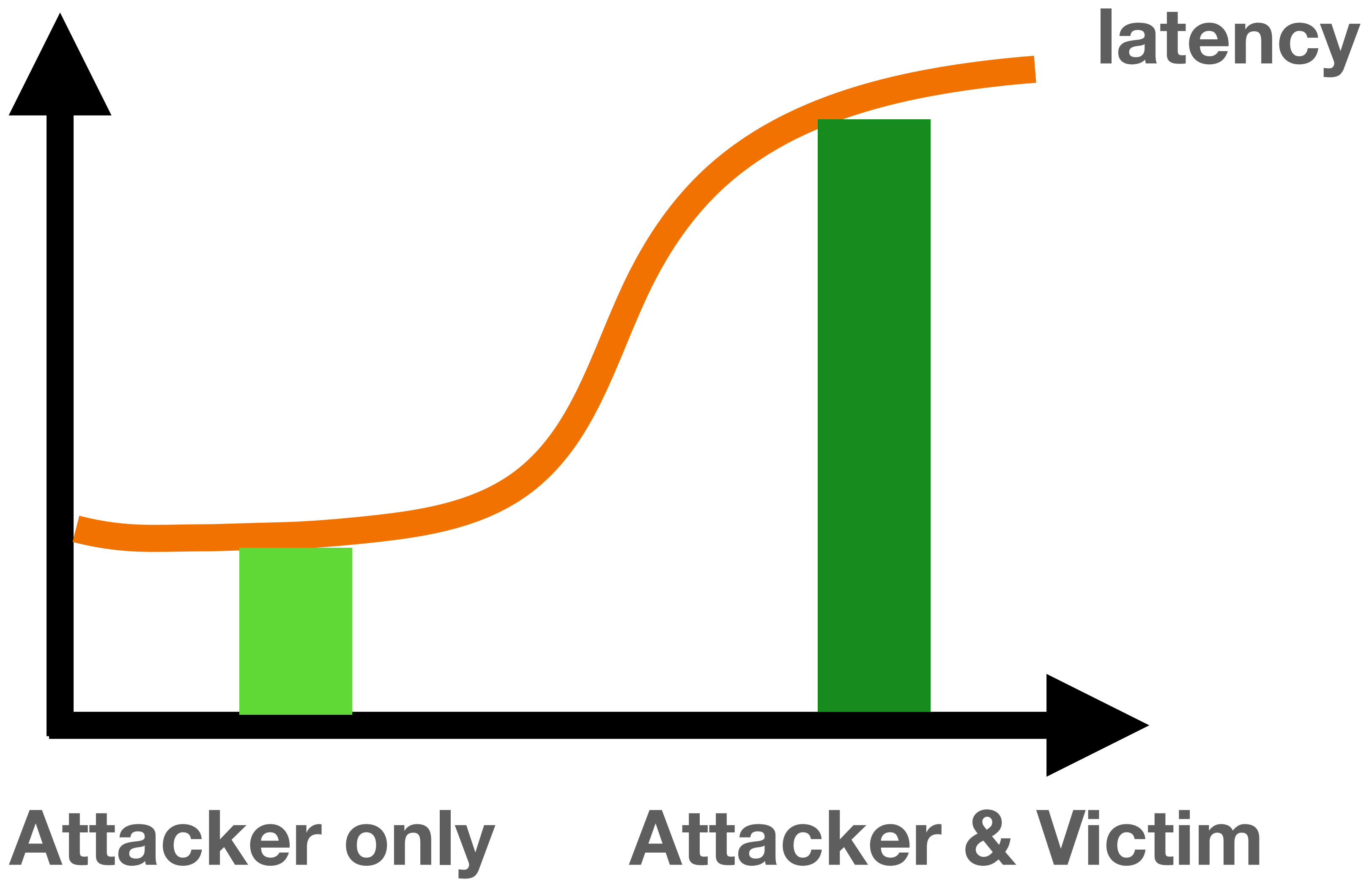


Why are the data leaked?

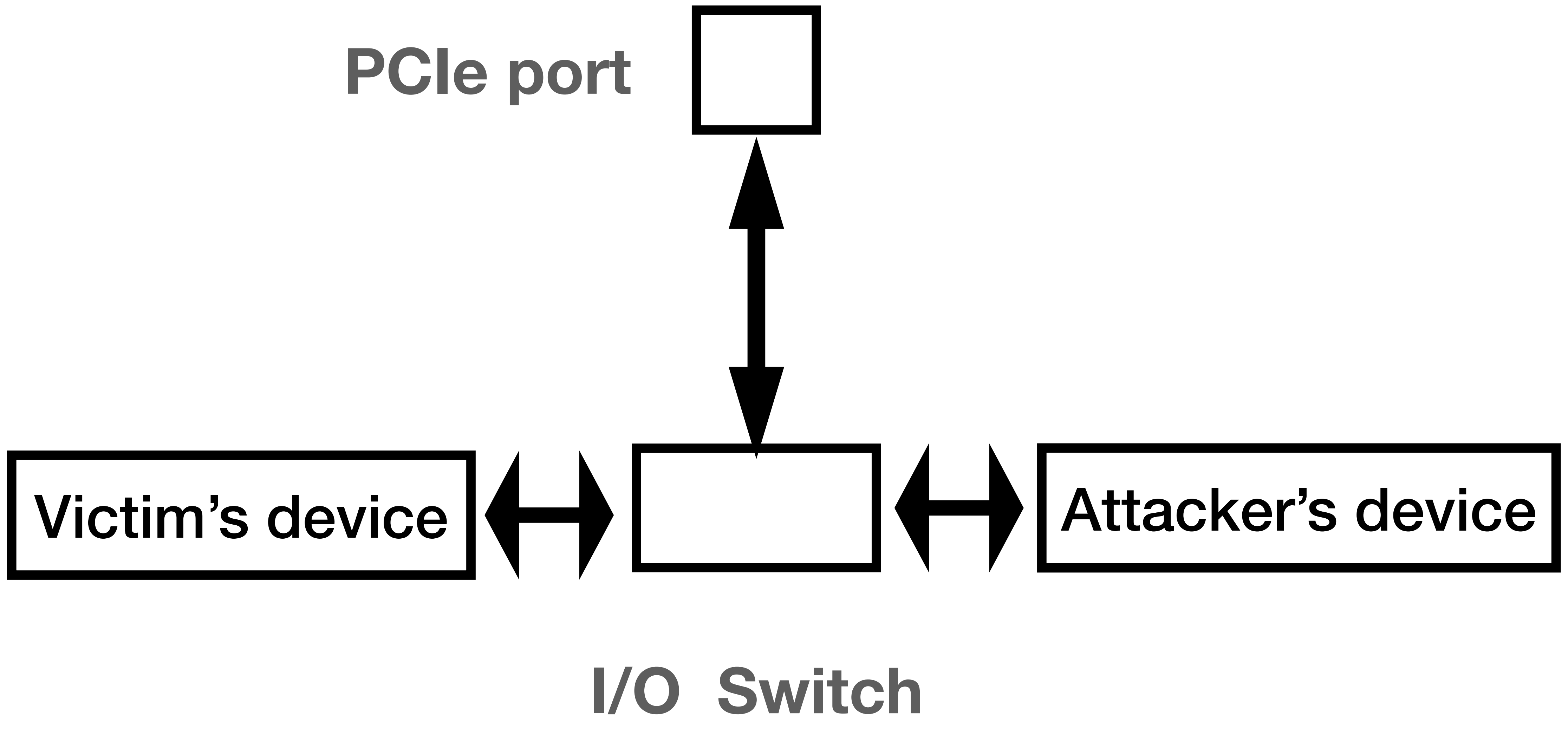


Why are the data leaked?

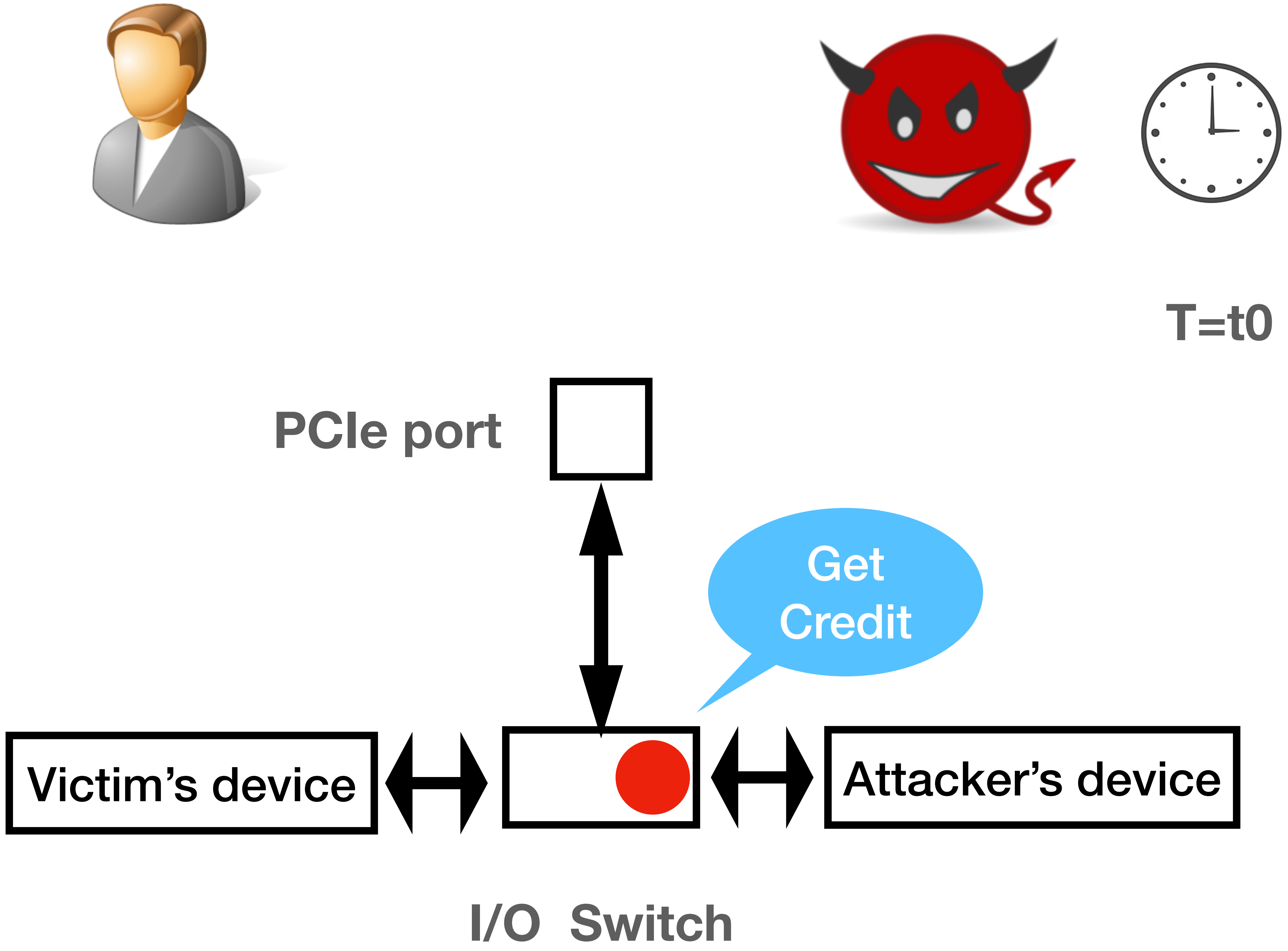




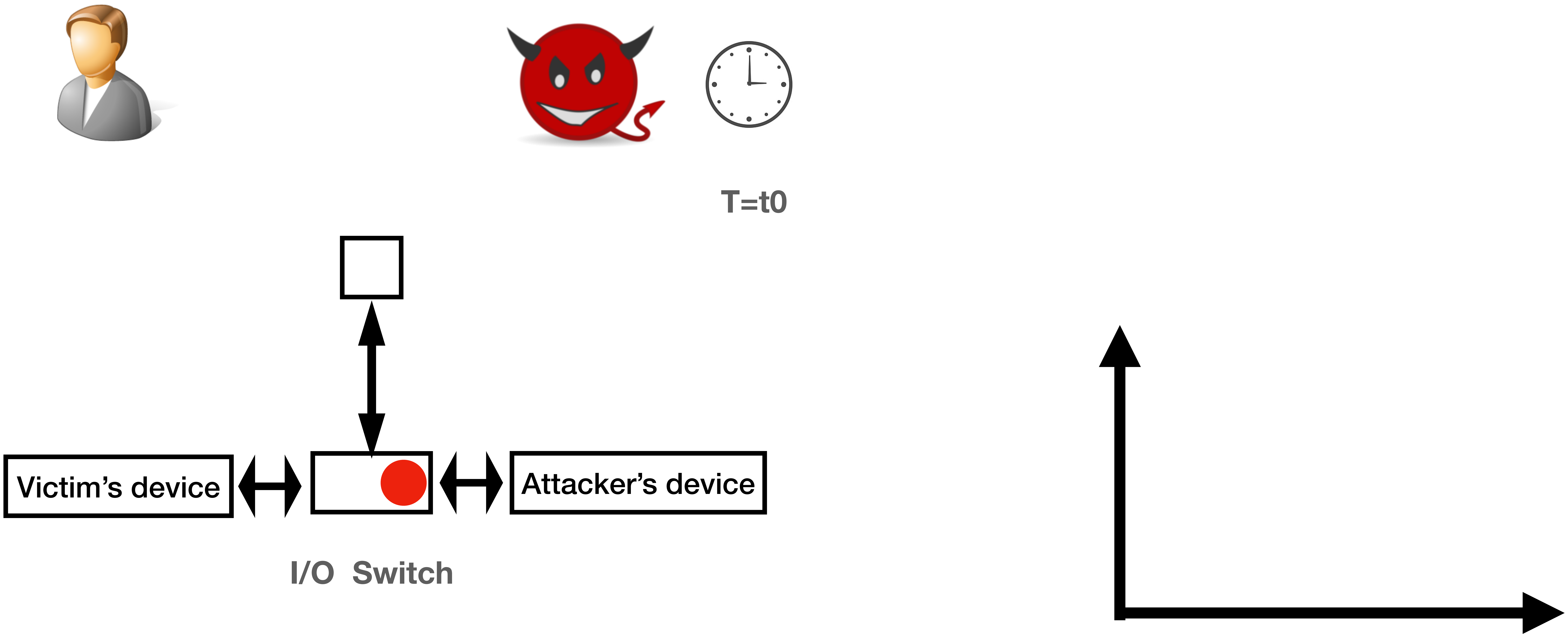
Why are the data leaked?



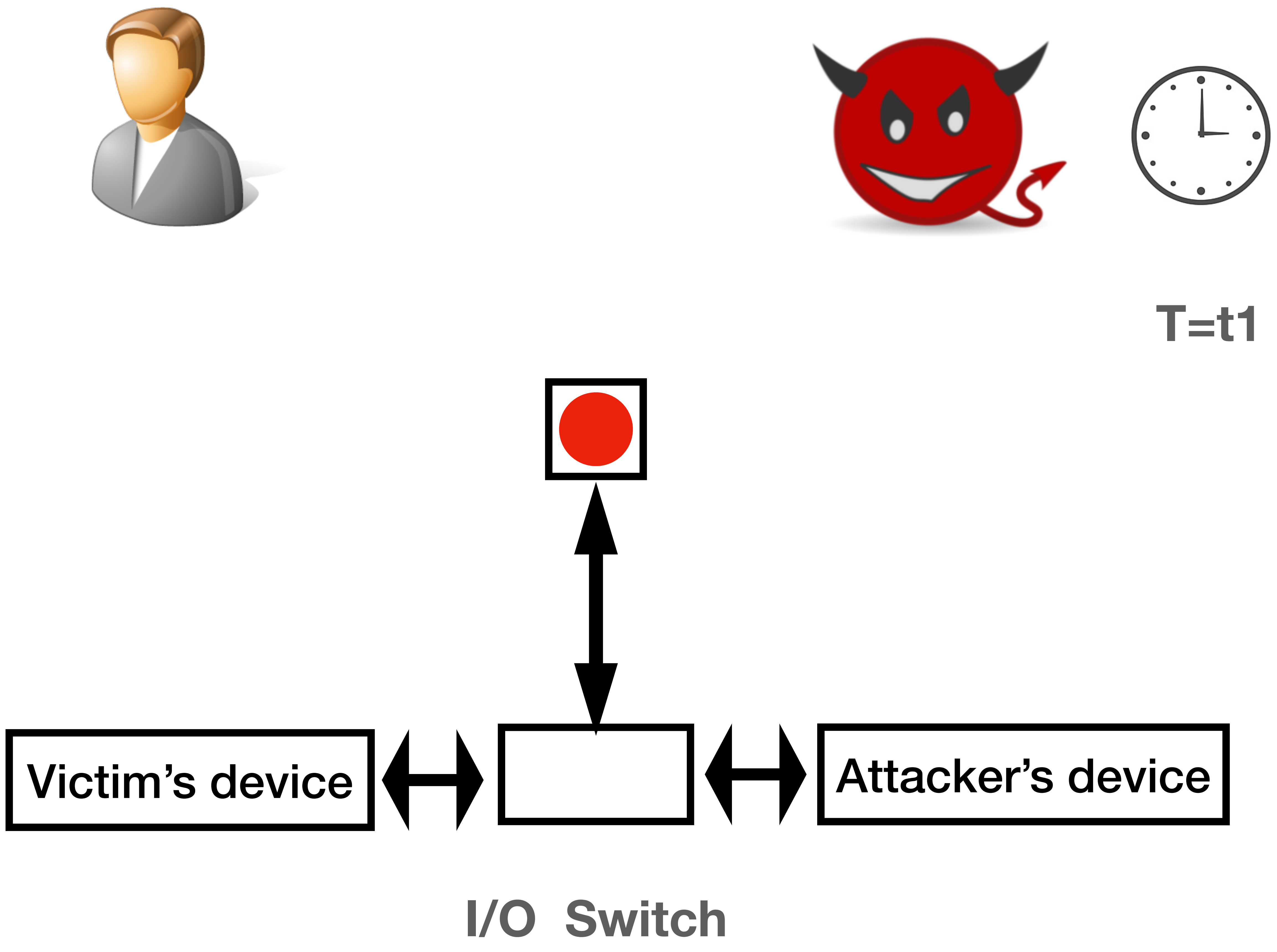
Why are the data leaked?

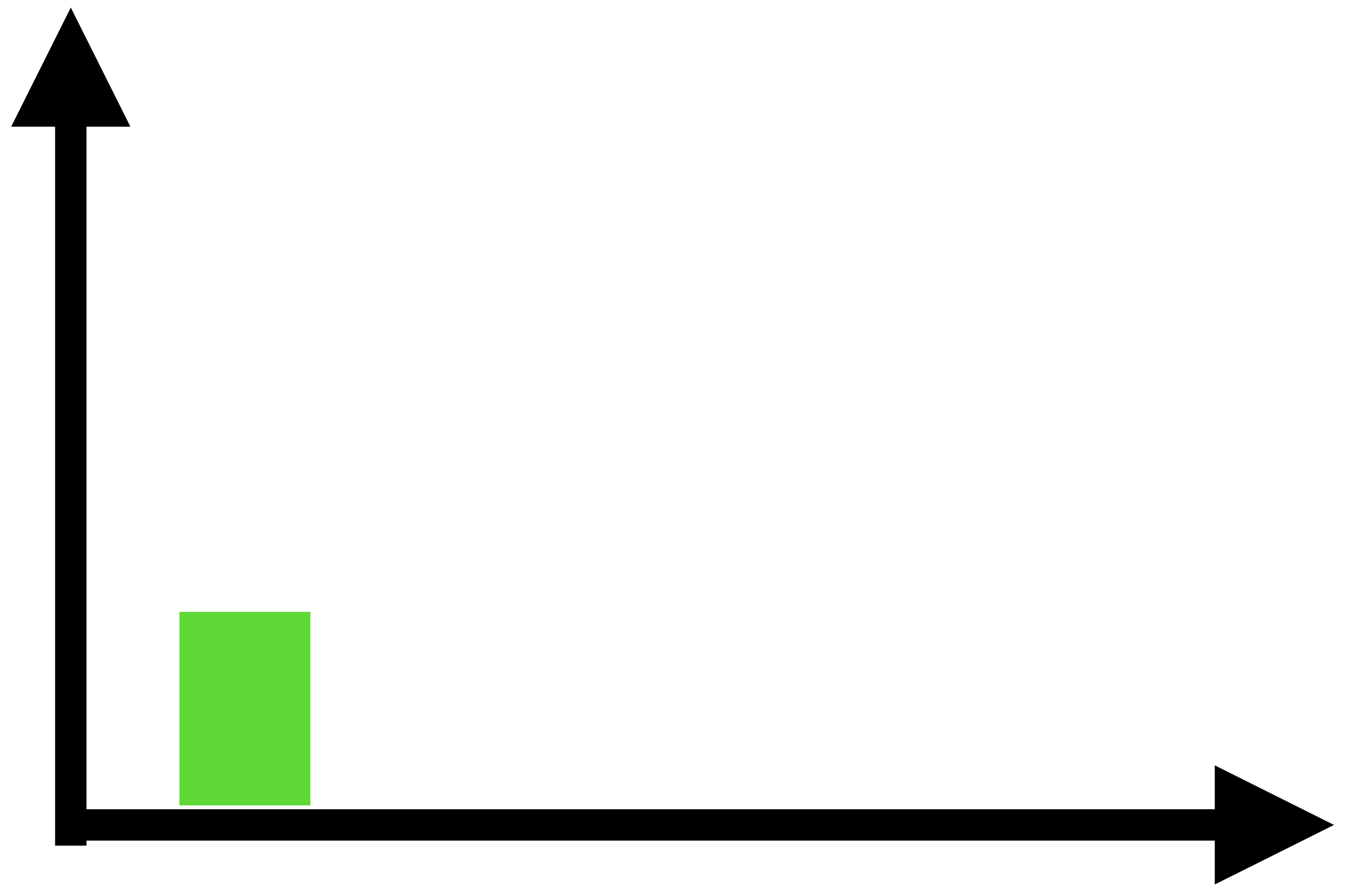


Why are the data leaked?

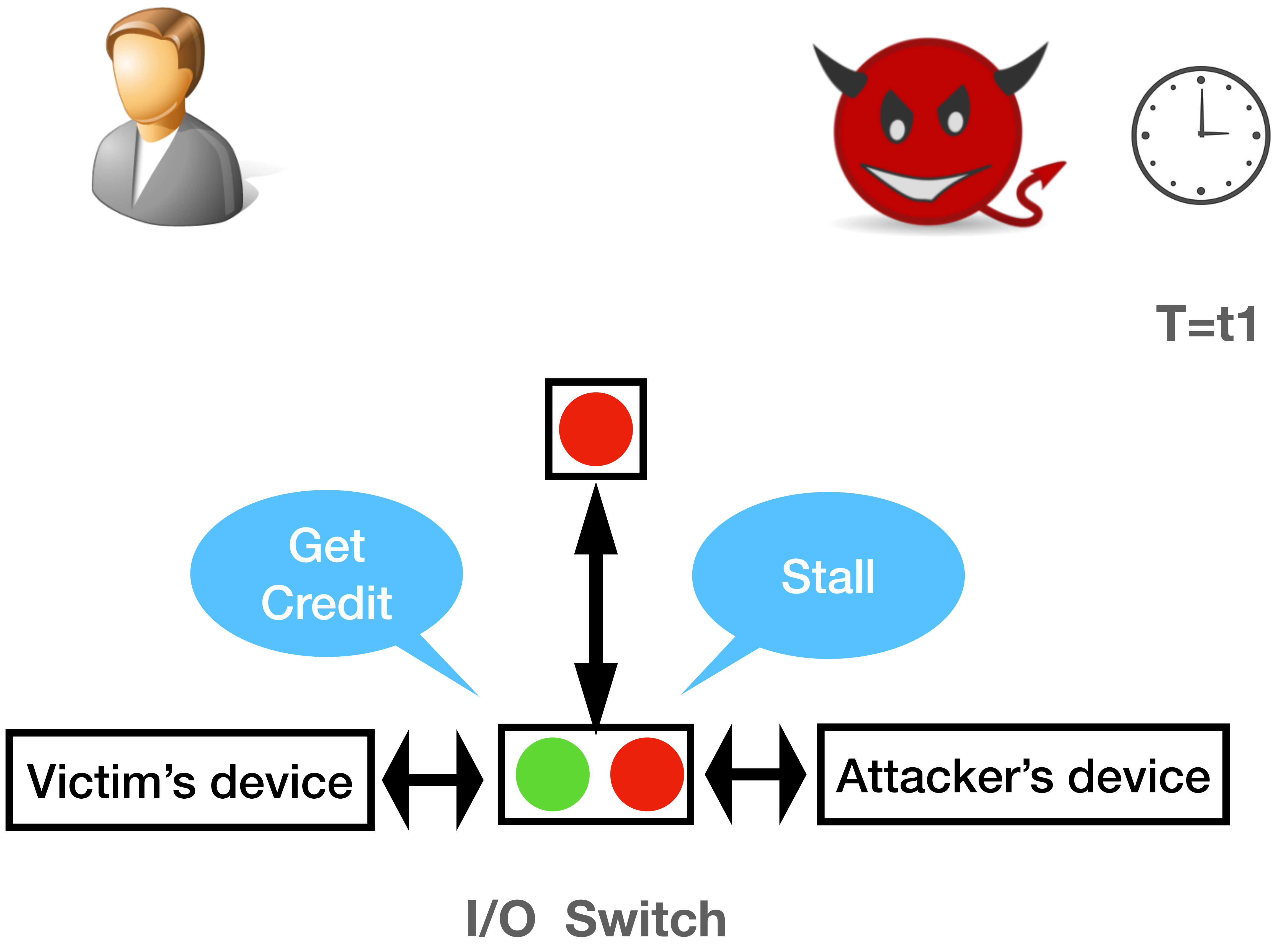


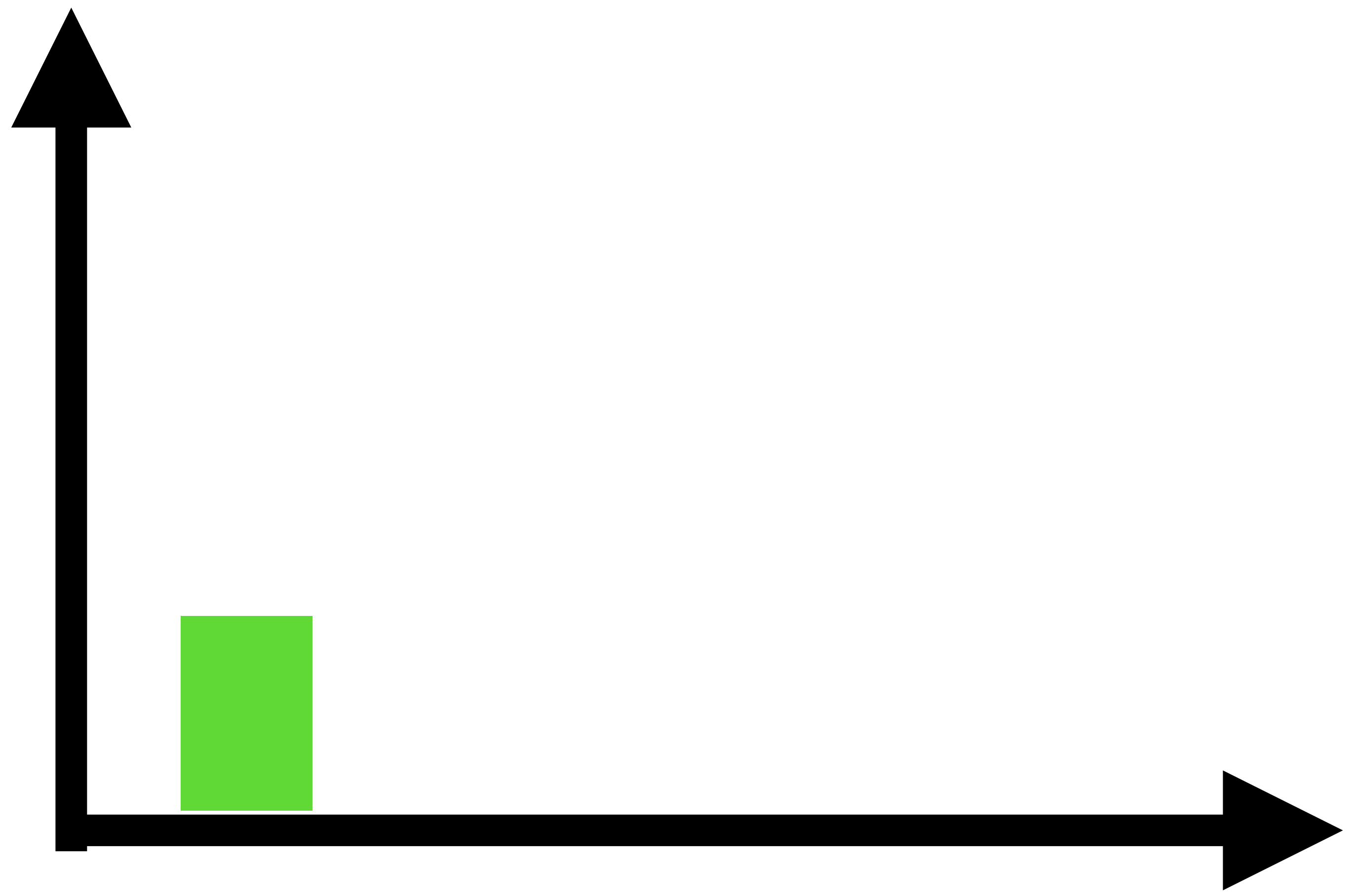
Why are the data leaked?



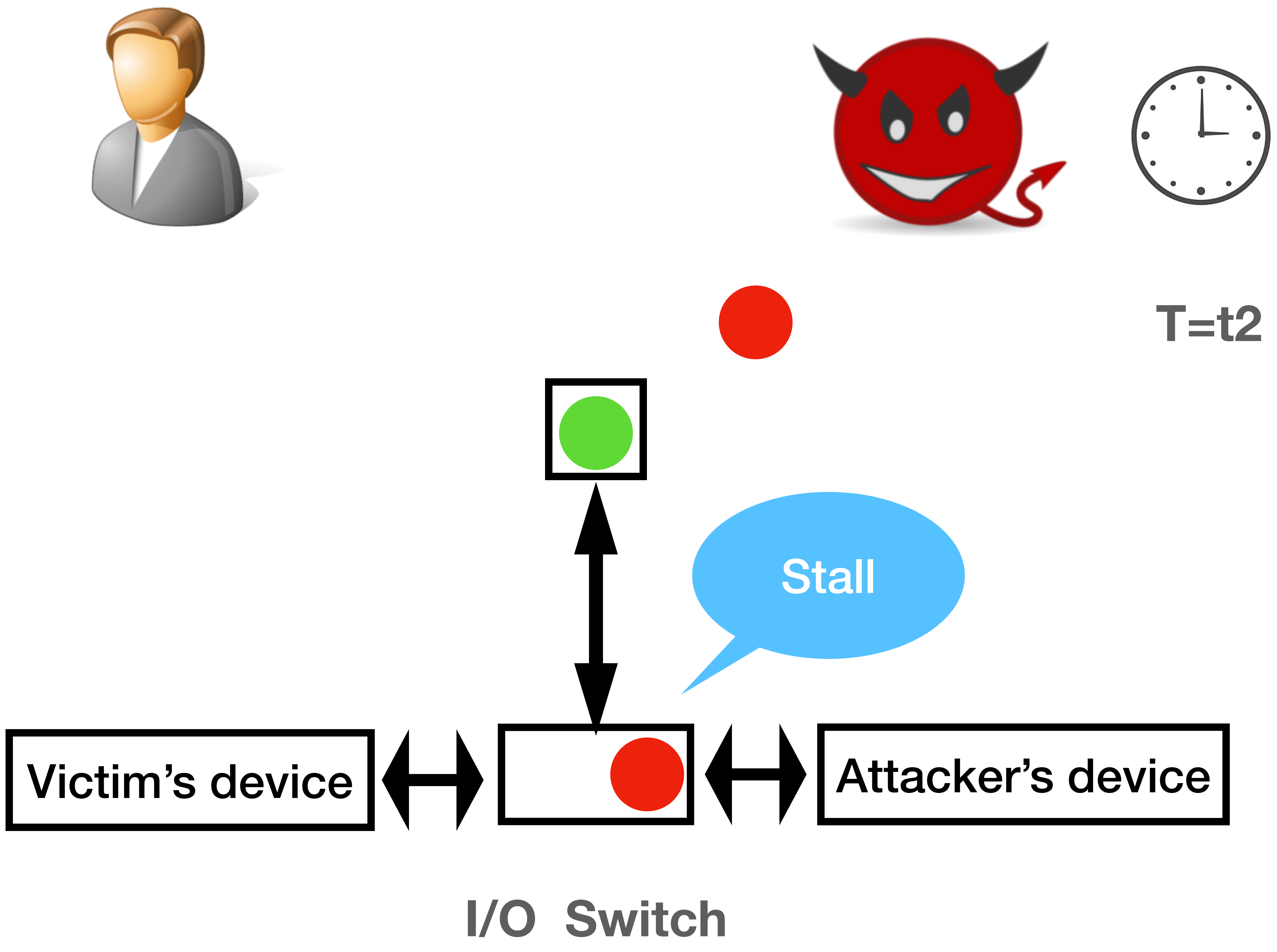


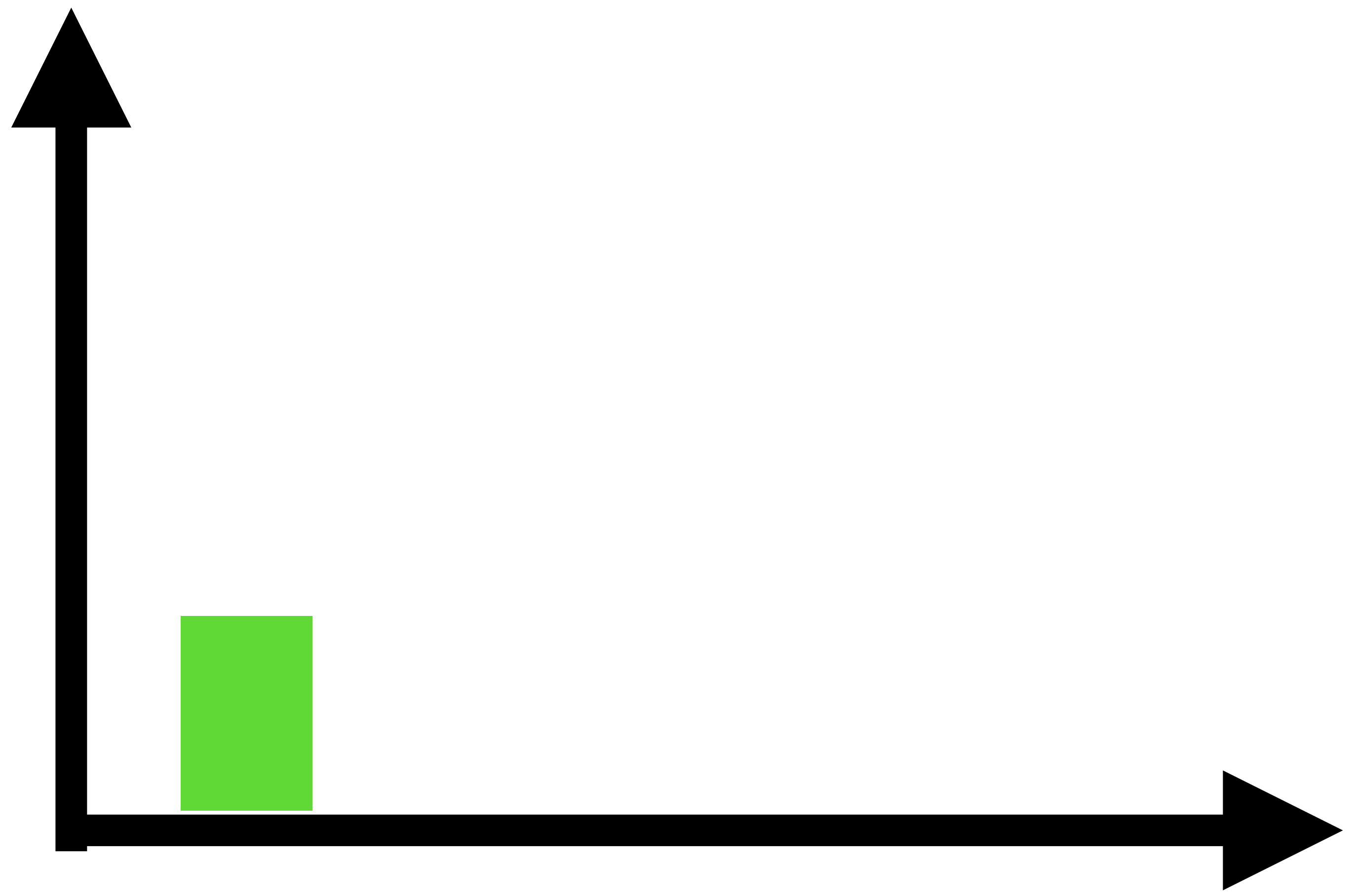
Why are the data leaked?



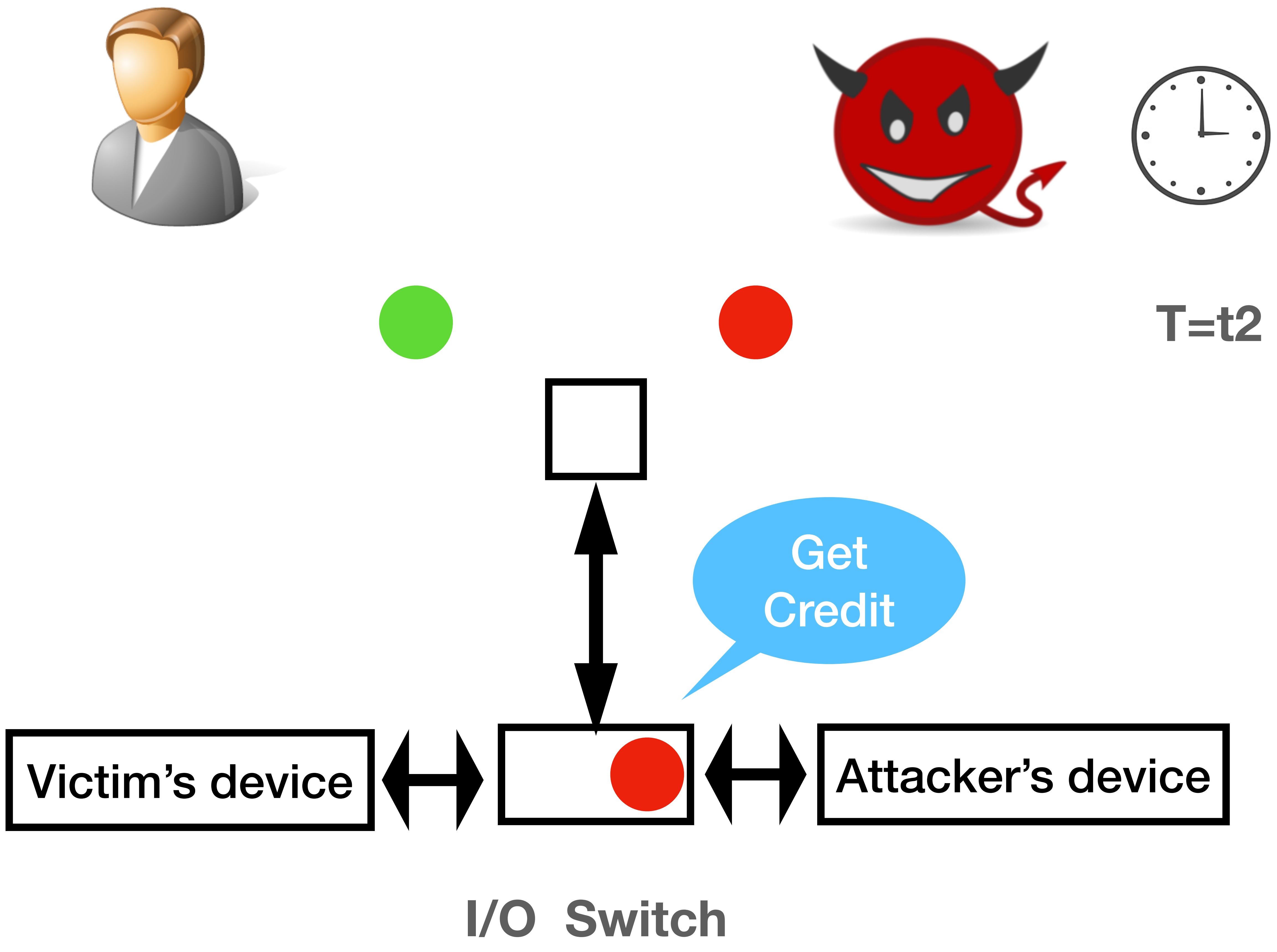


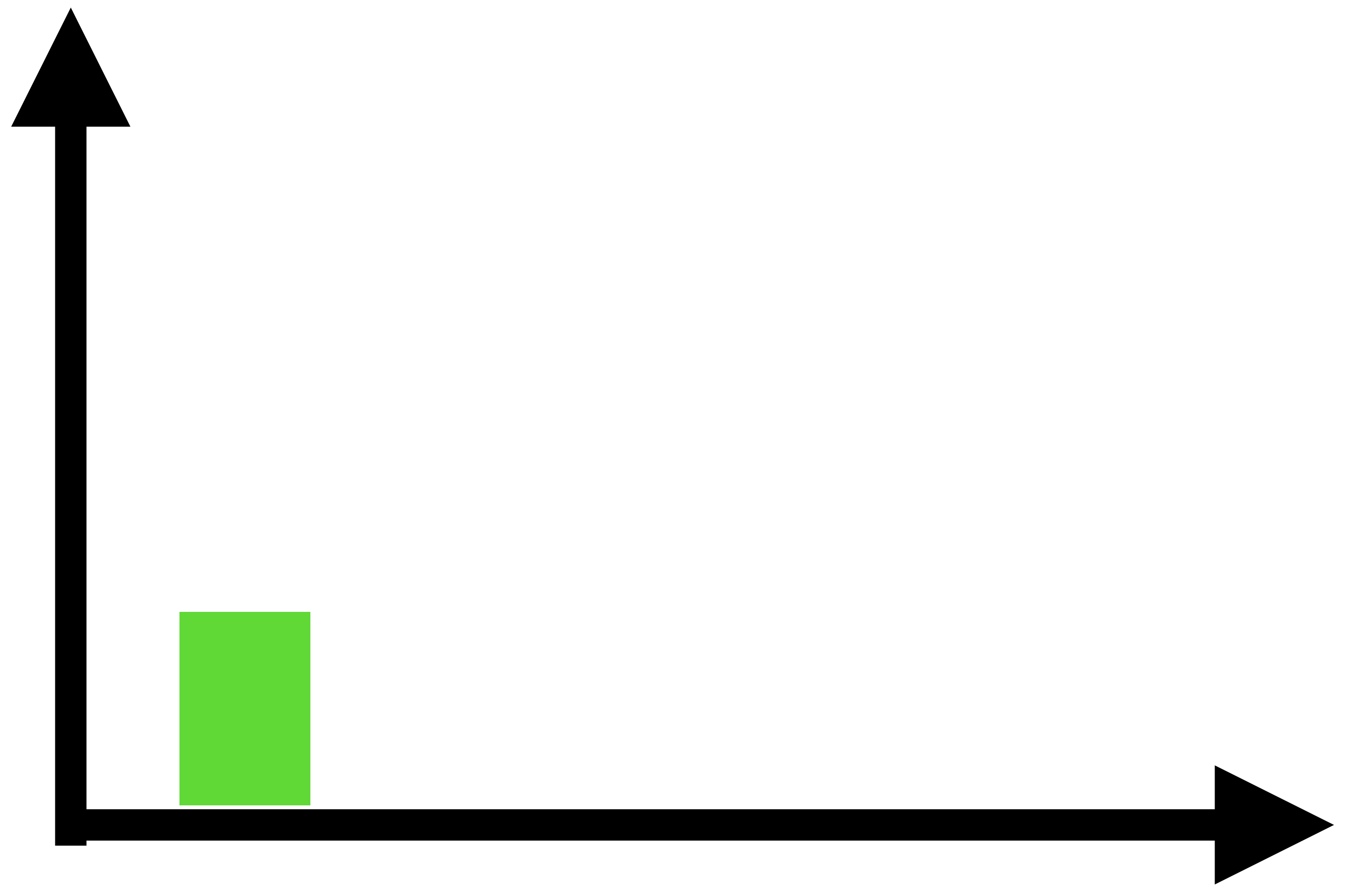
Why are the data leaked?



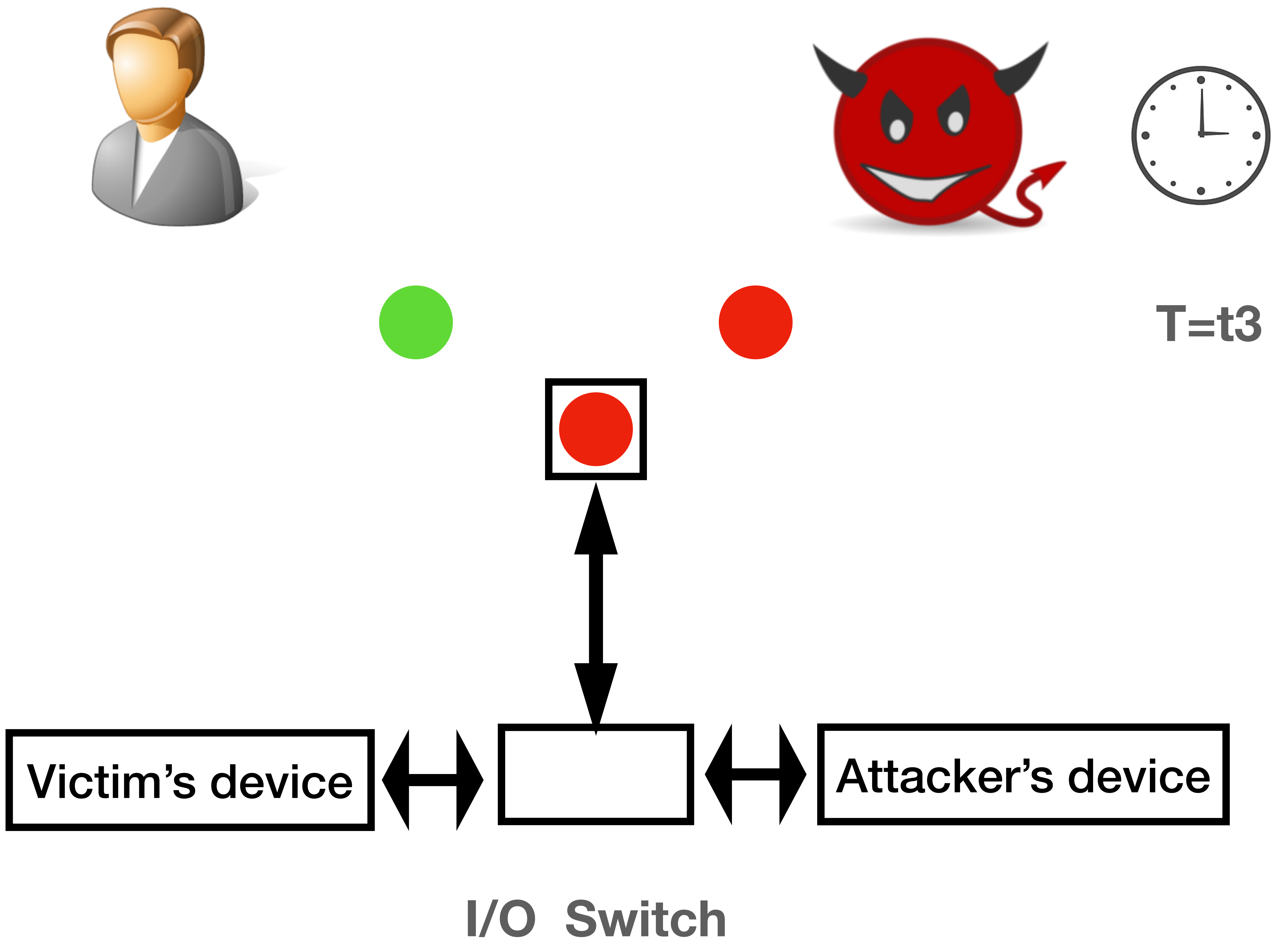


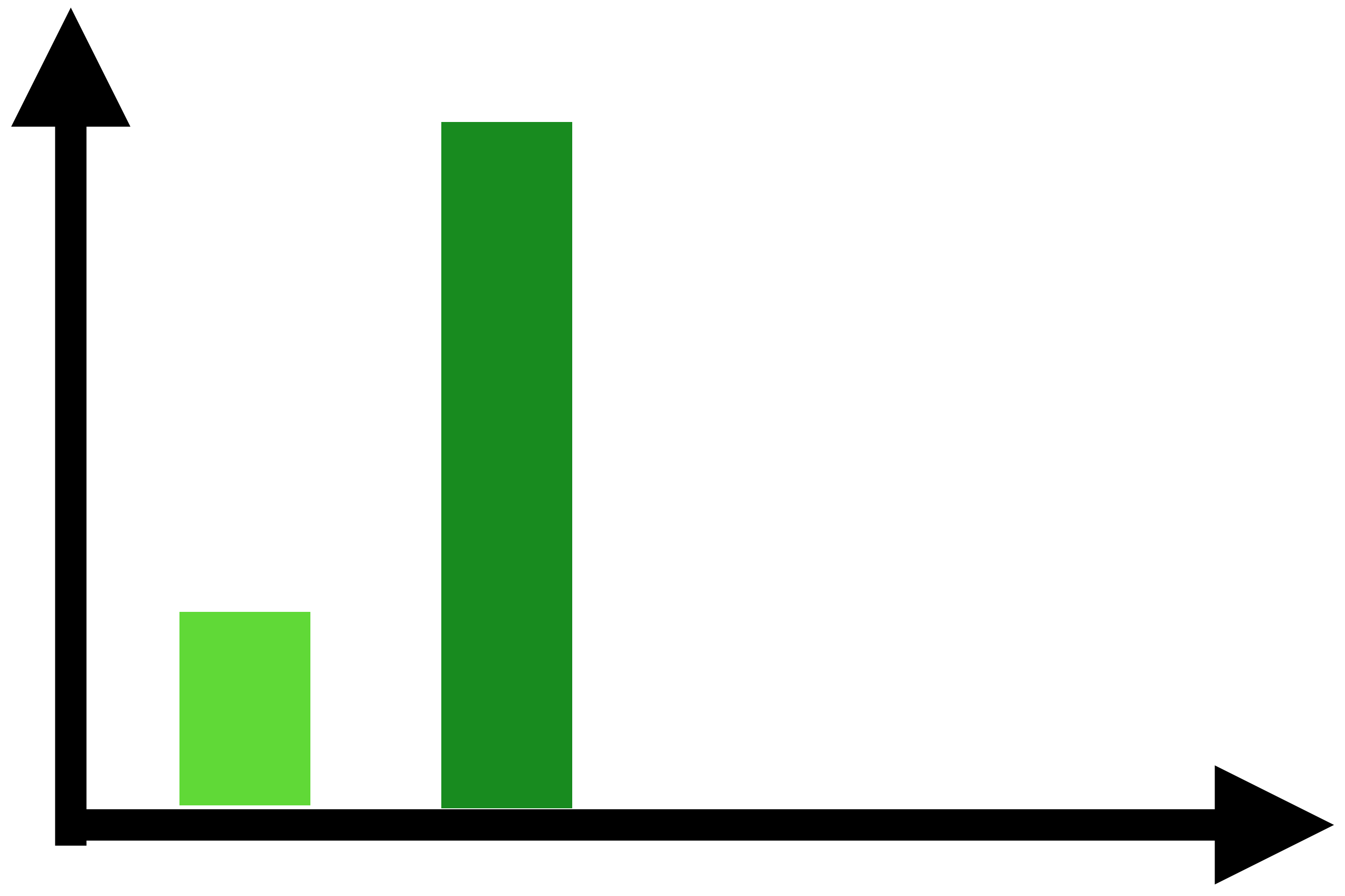
Why are the data leaked?



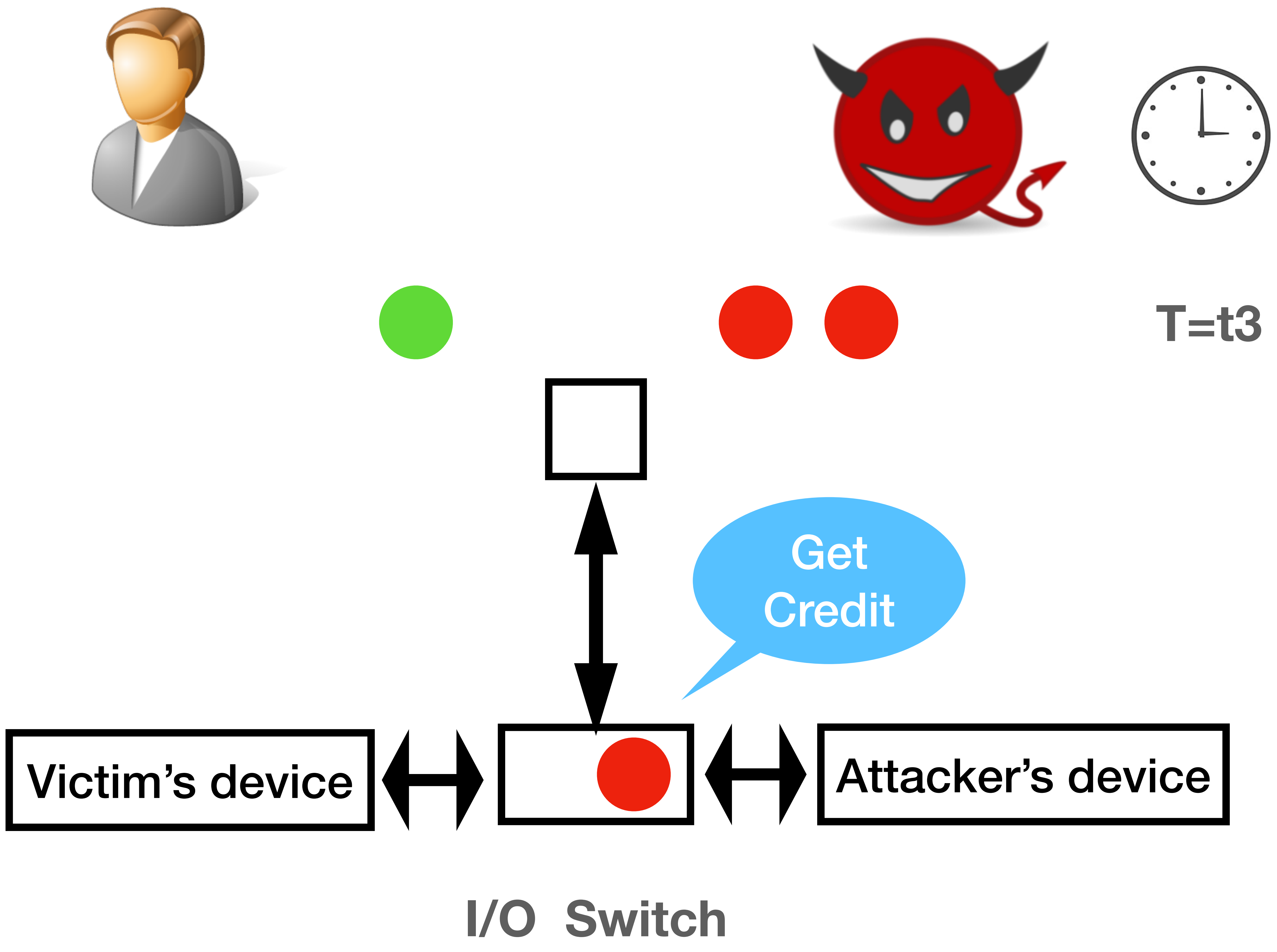


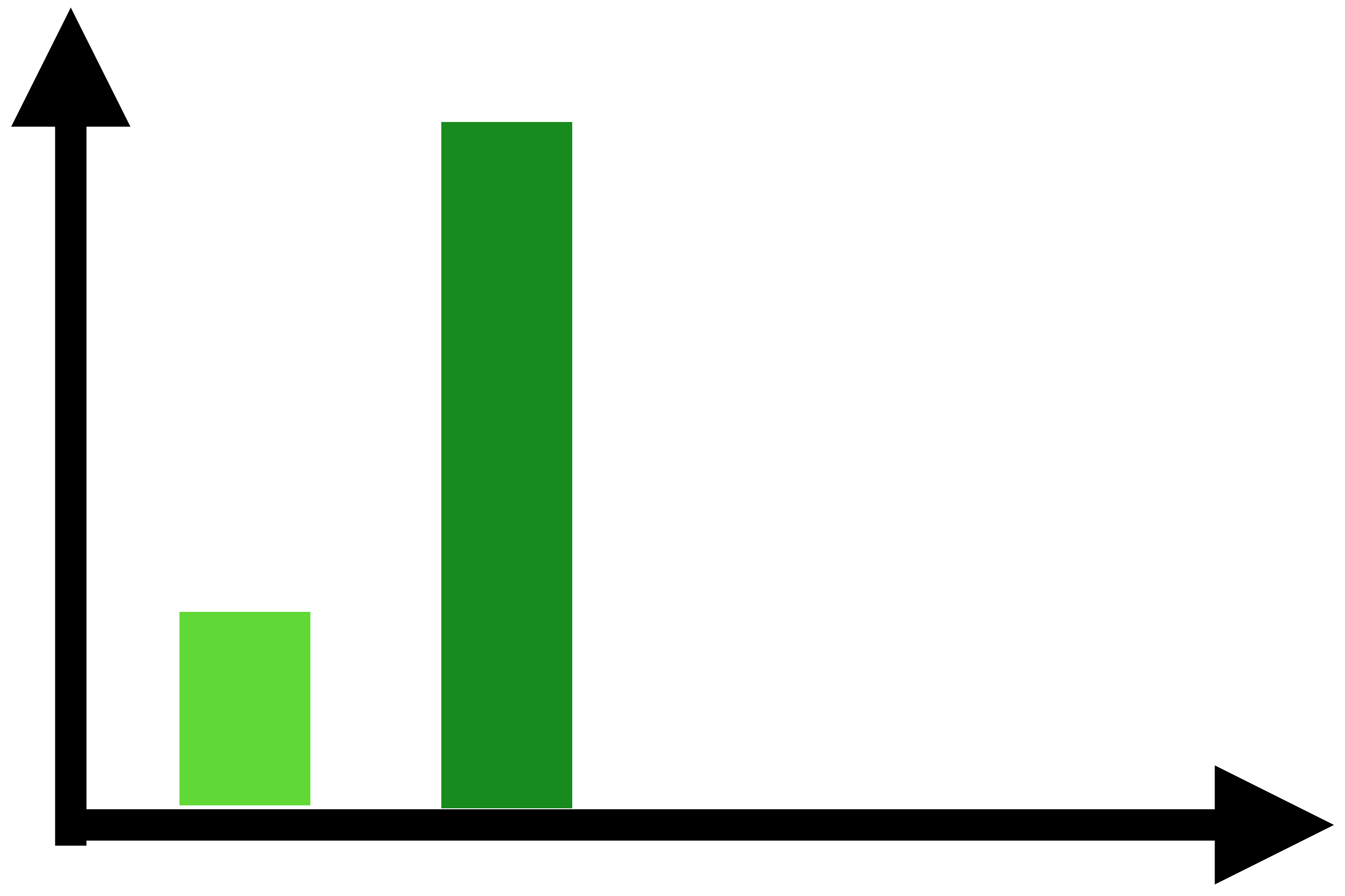
Why are the data leaked?



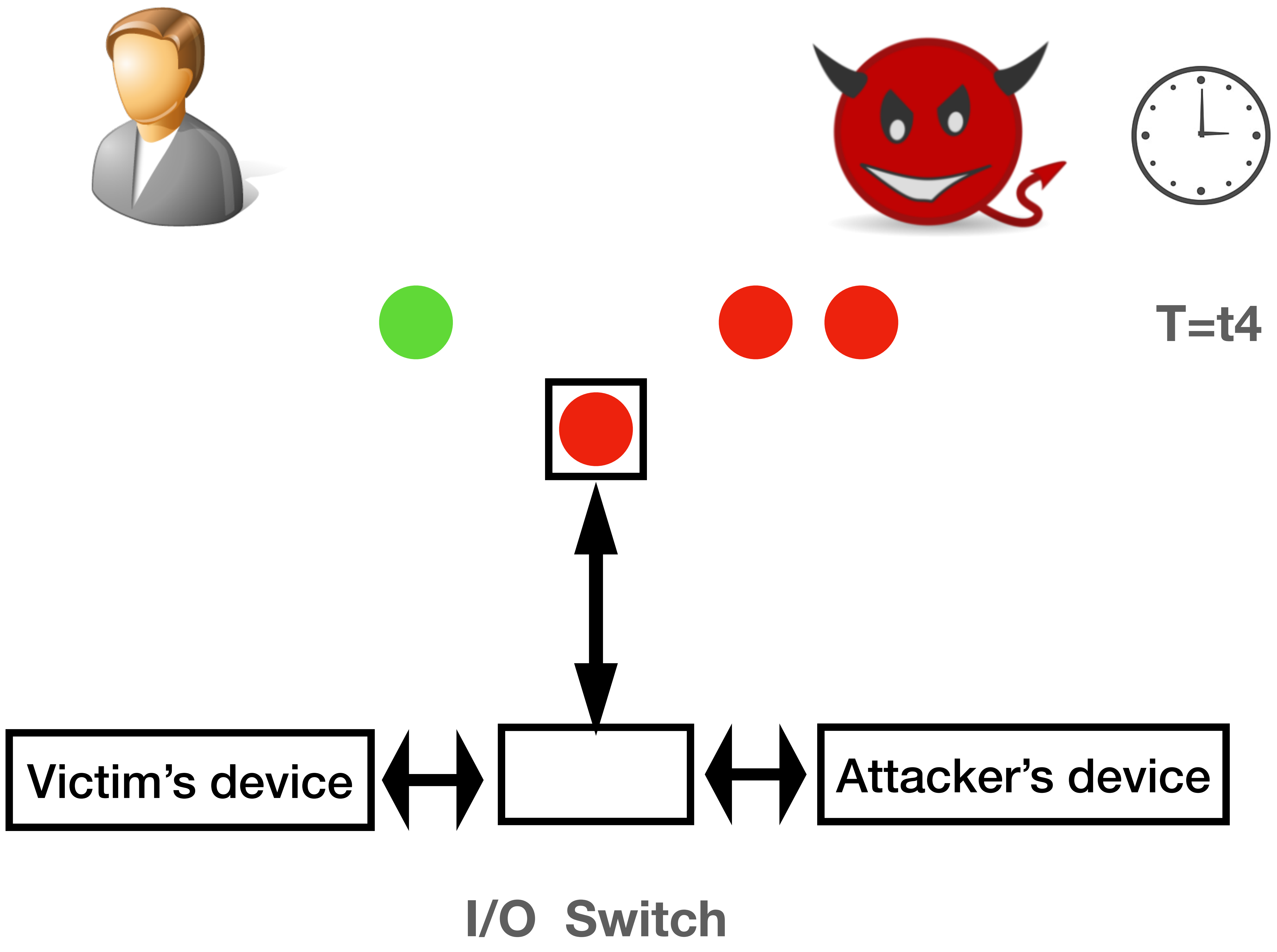


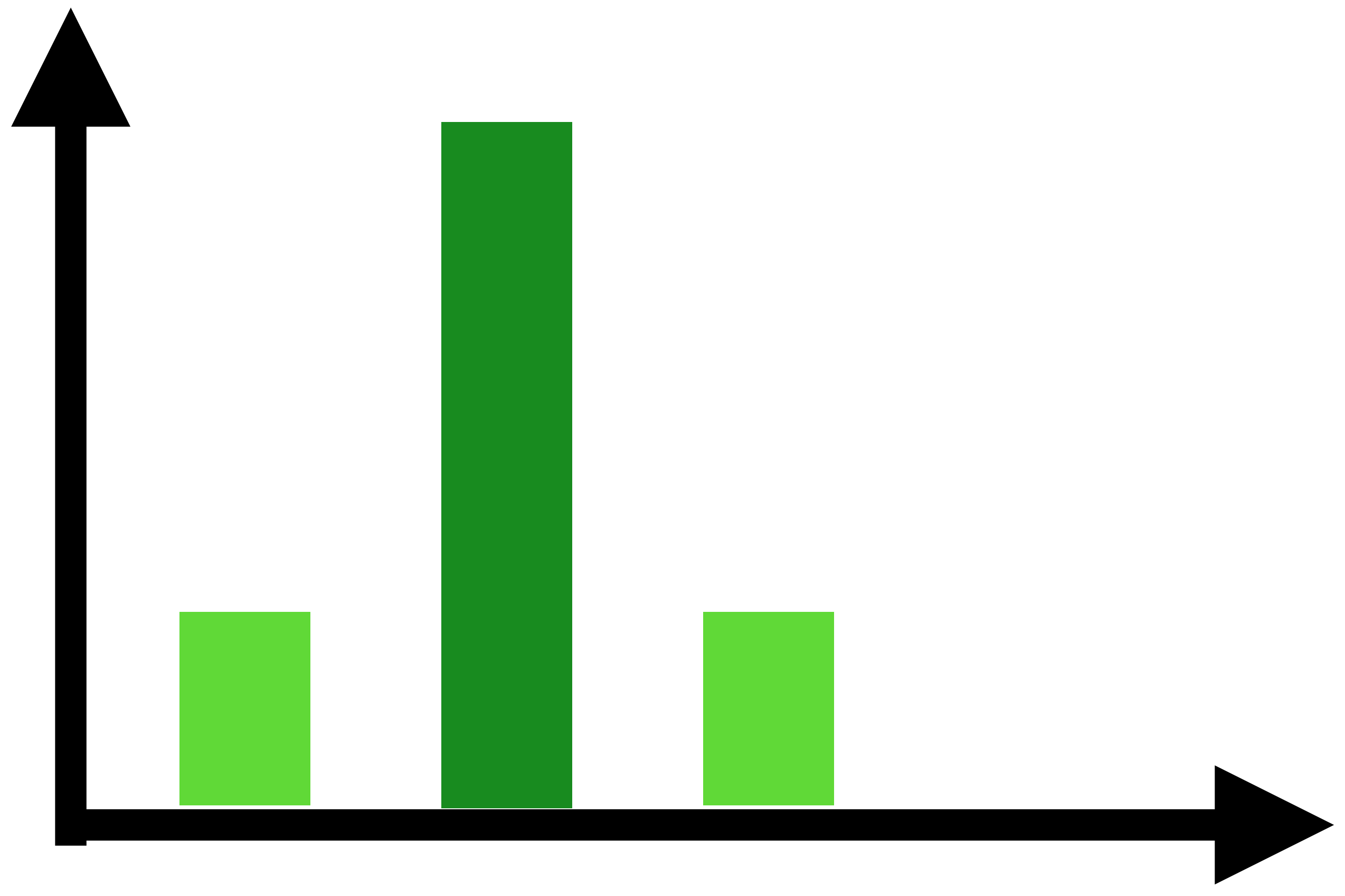
Why are the data leaked?



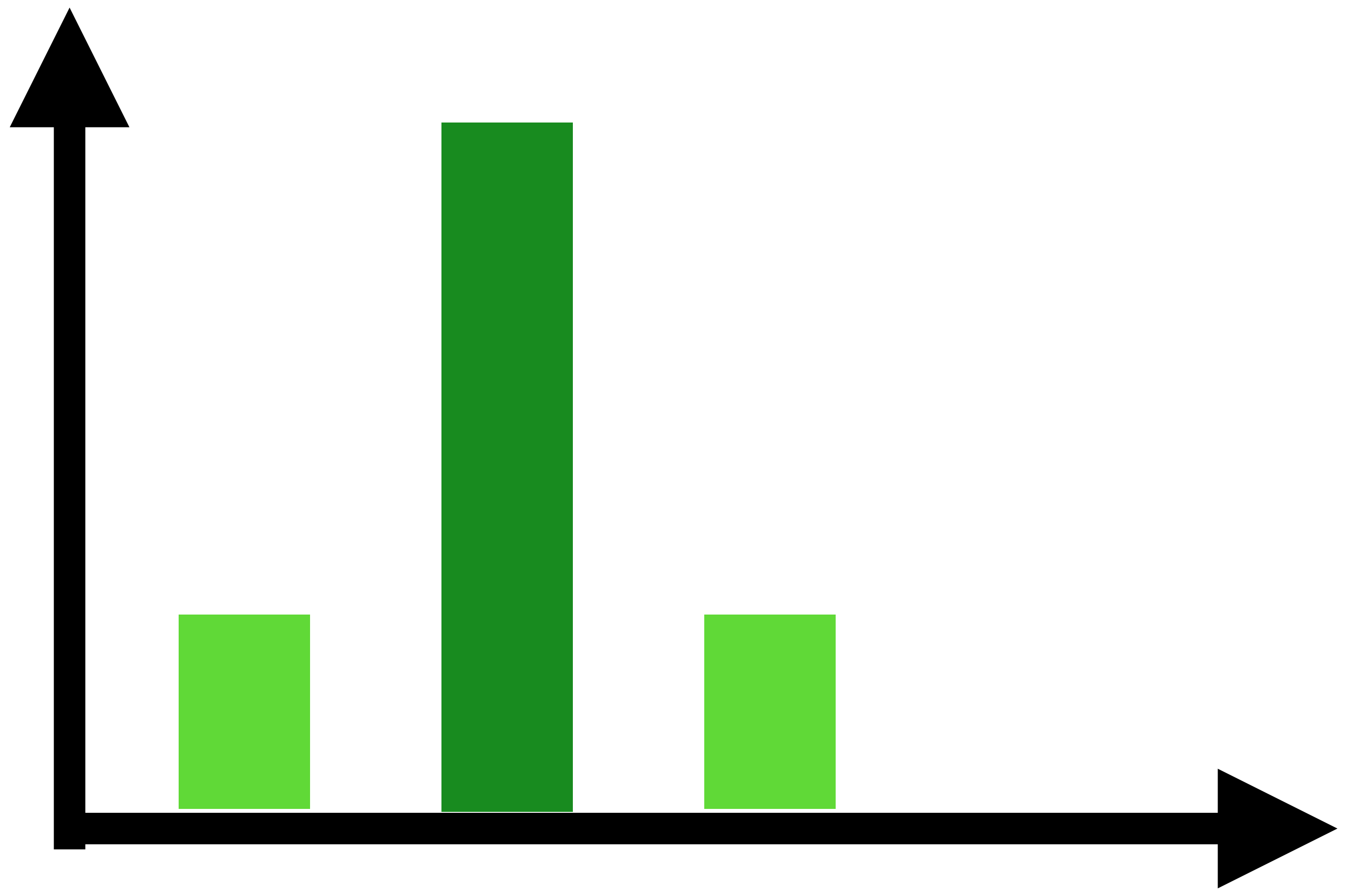


Why are the data leaked?



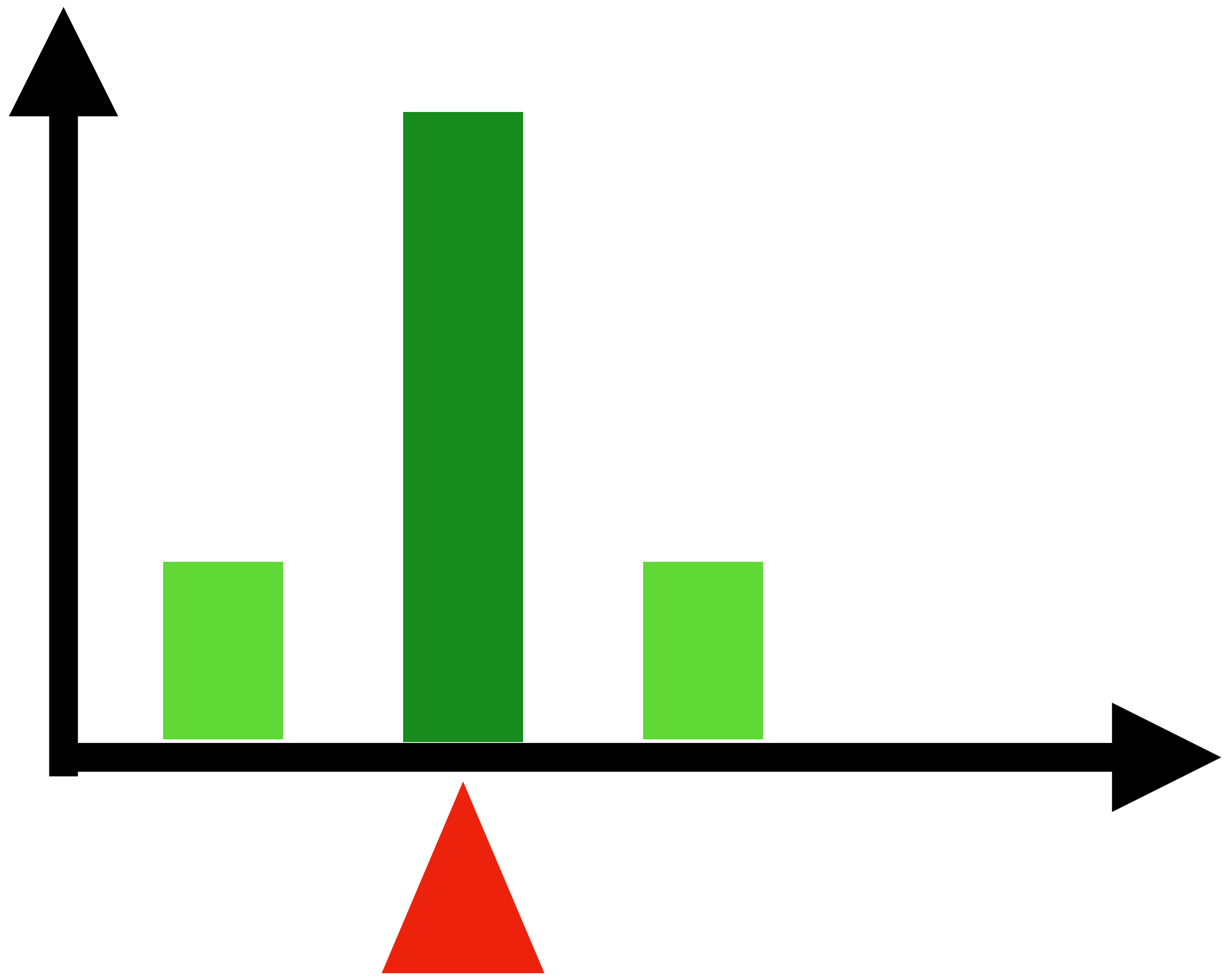


Why are the data leaked?



Why are the data leaked?

- Attacker knows when victim is active!



How to monitor the victim behaviors?

How to monitor the victim behaviors?

- Access data ceaselessly and make congestion

How to monitor the victim behaviors?

- Access data ceaselessly and make congestion
- Record latency between two operations

Probe Pseudocode

```
while True:
    AccessData( )
    T = RDTSCP( )
```

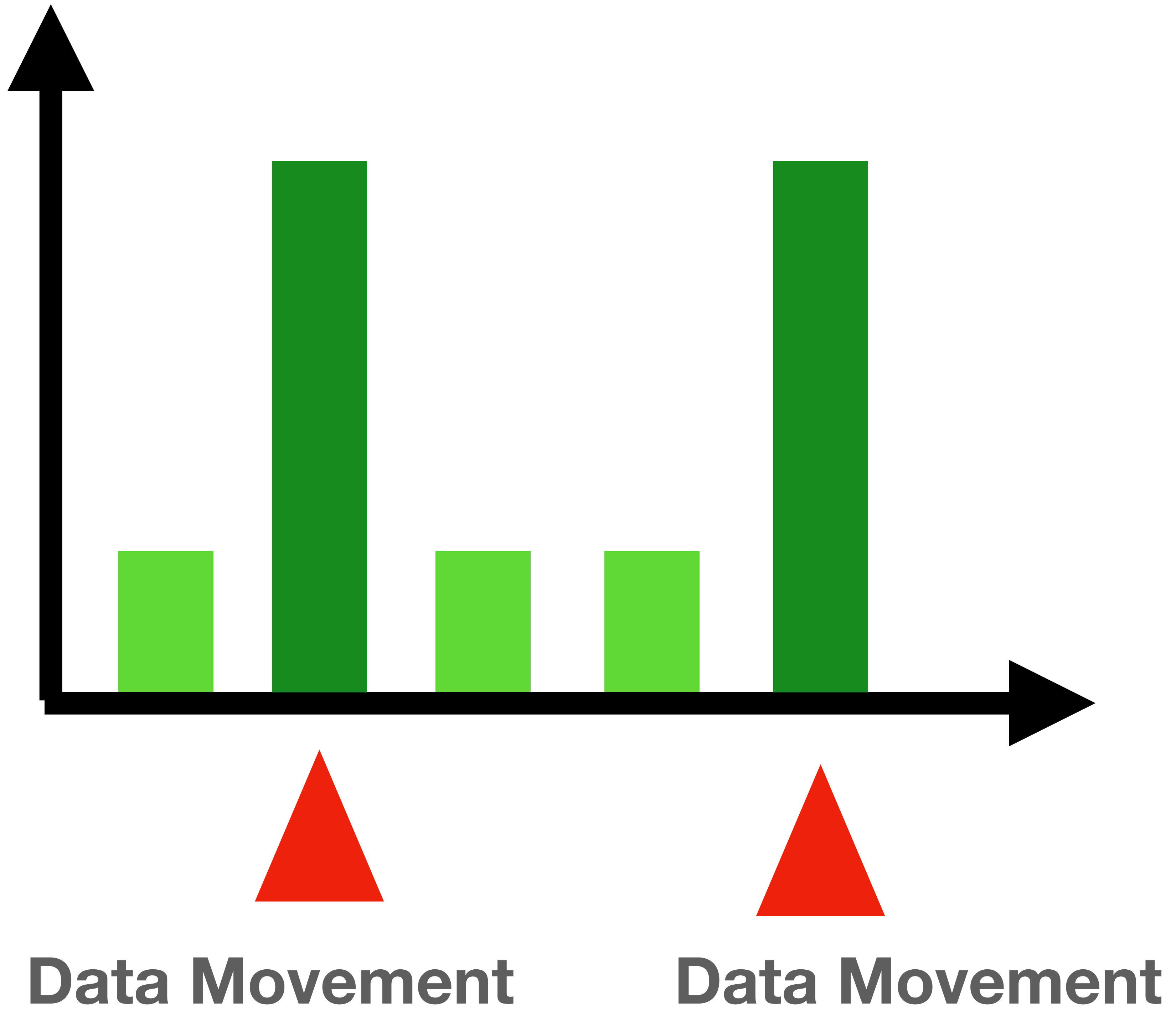
How to monitor the victim behaviors?

- Access data ceaselessly and make congestion
- Record latency between two operations

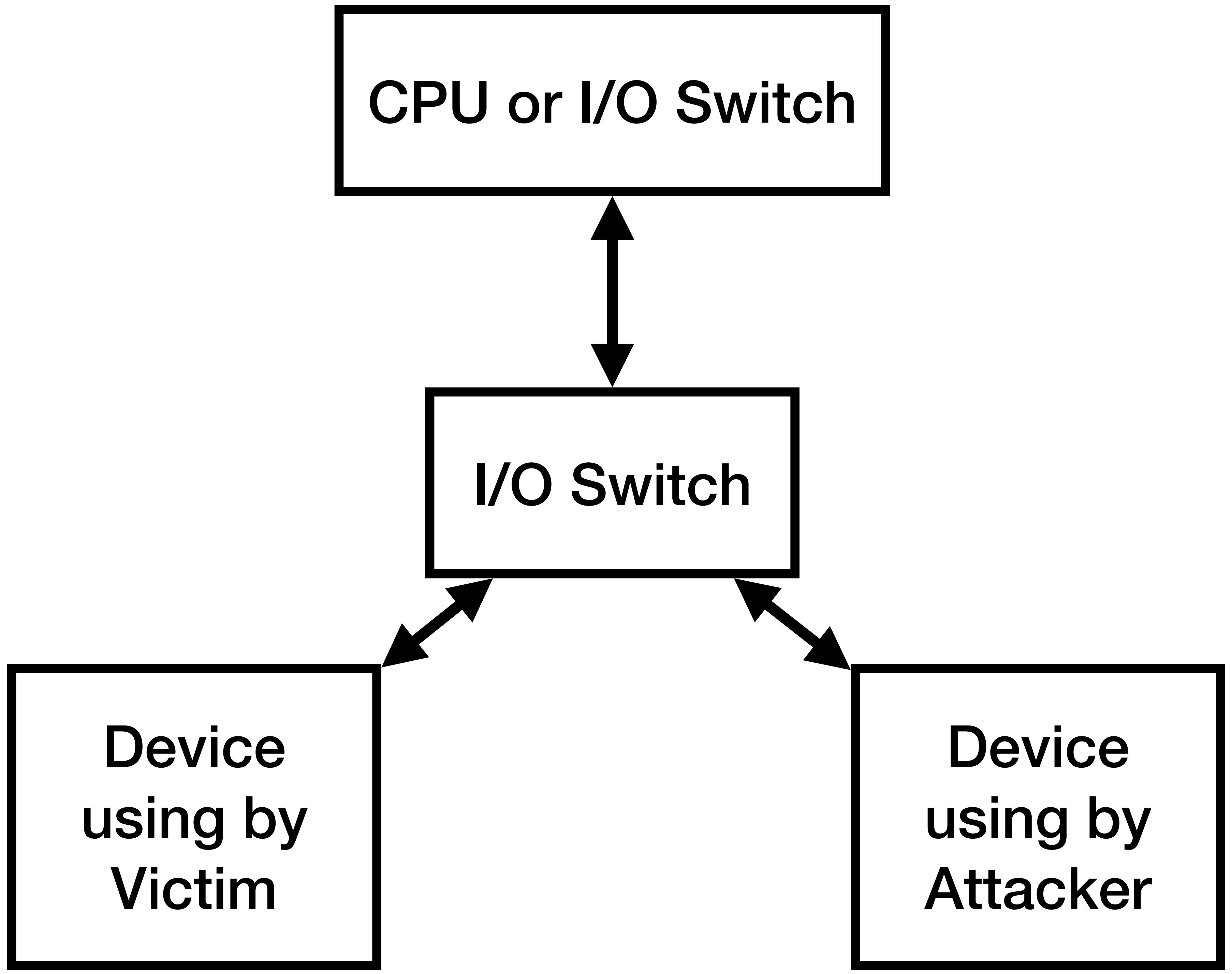
Probe Pseudocode

```
while True:
    AccessData( )
    T = RDTSCP( )
```

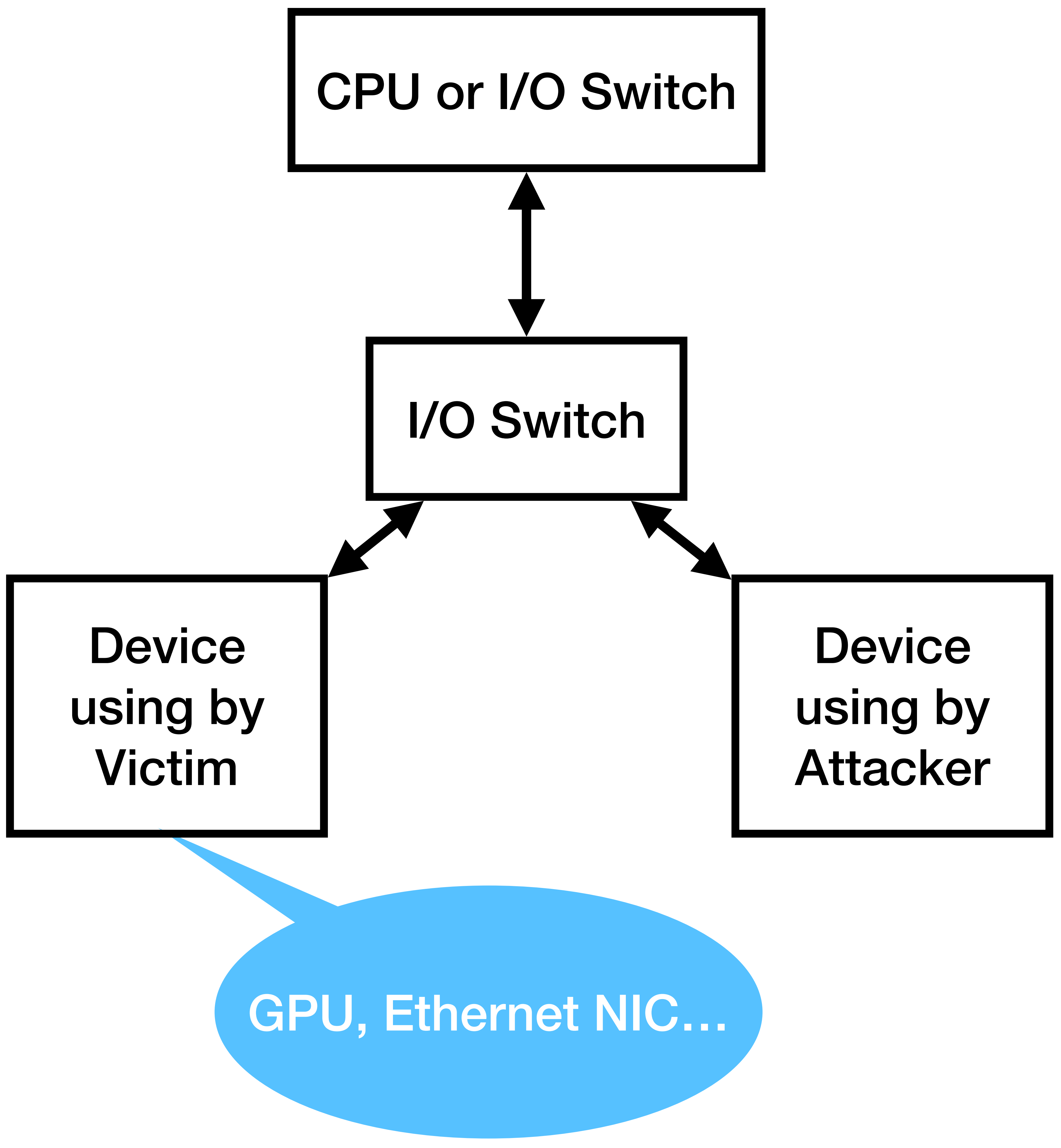
- A higher latency means data is transmitting



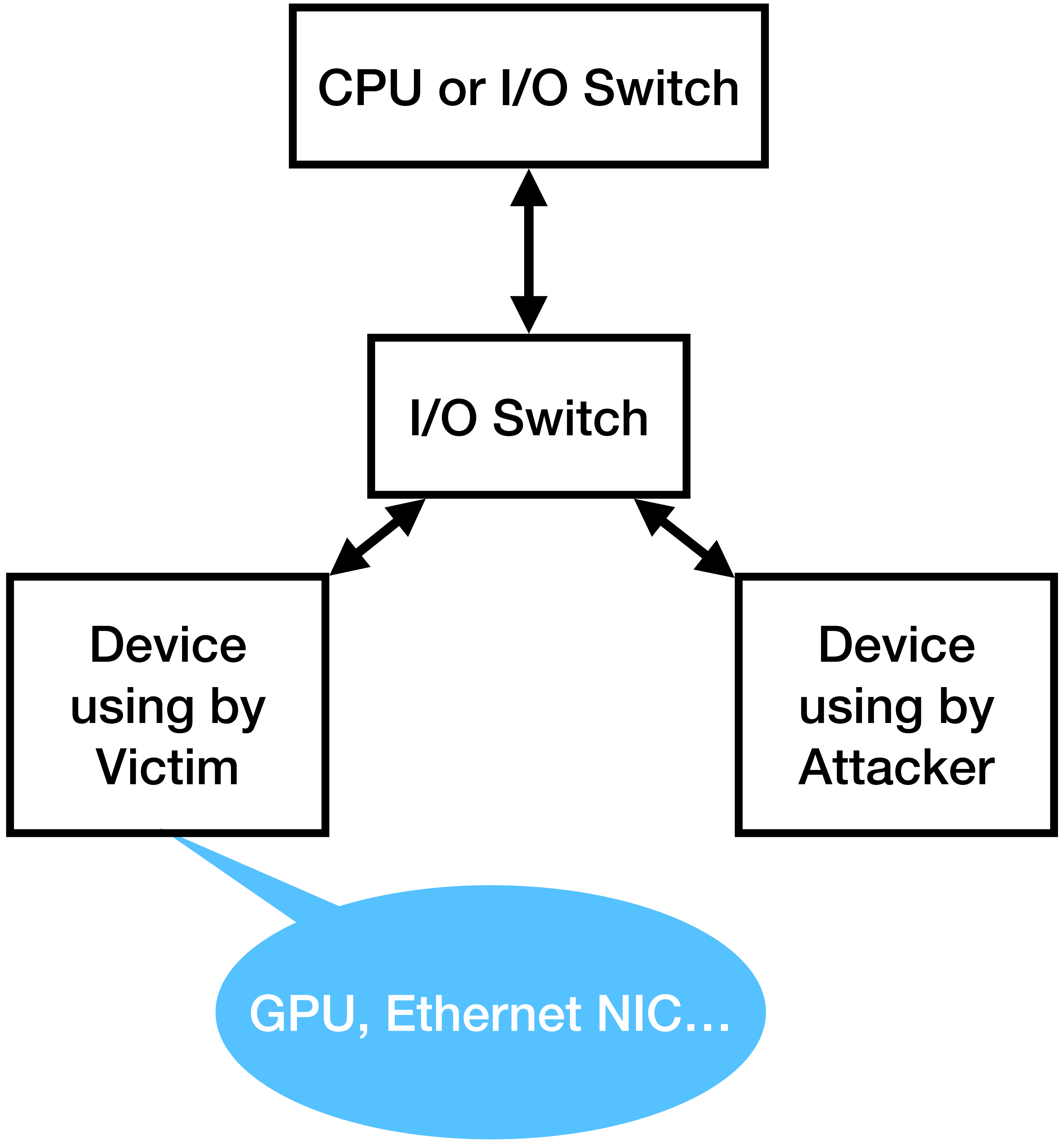
What information can we infer?



What information can we infer?

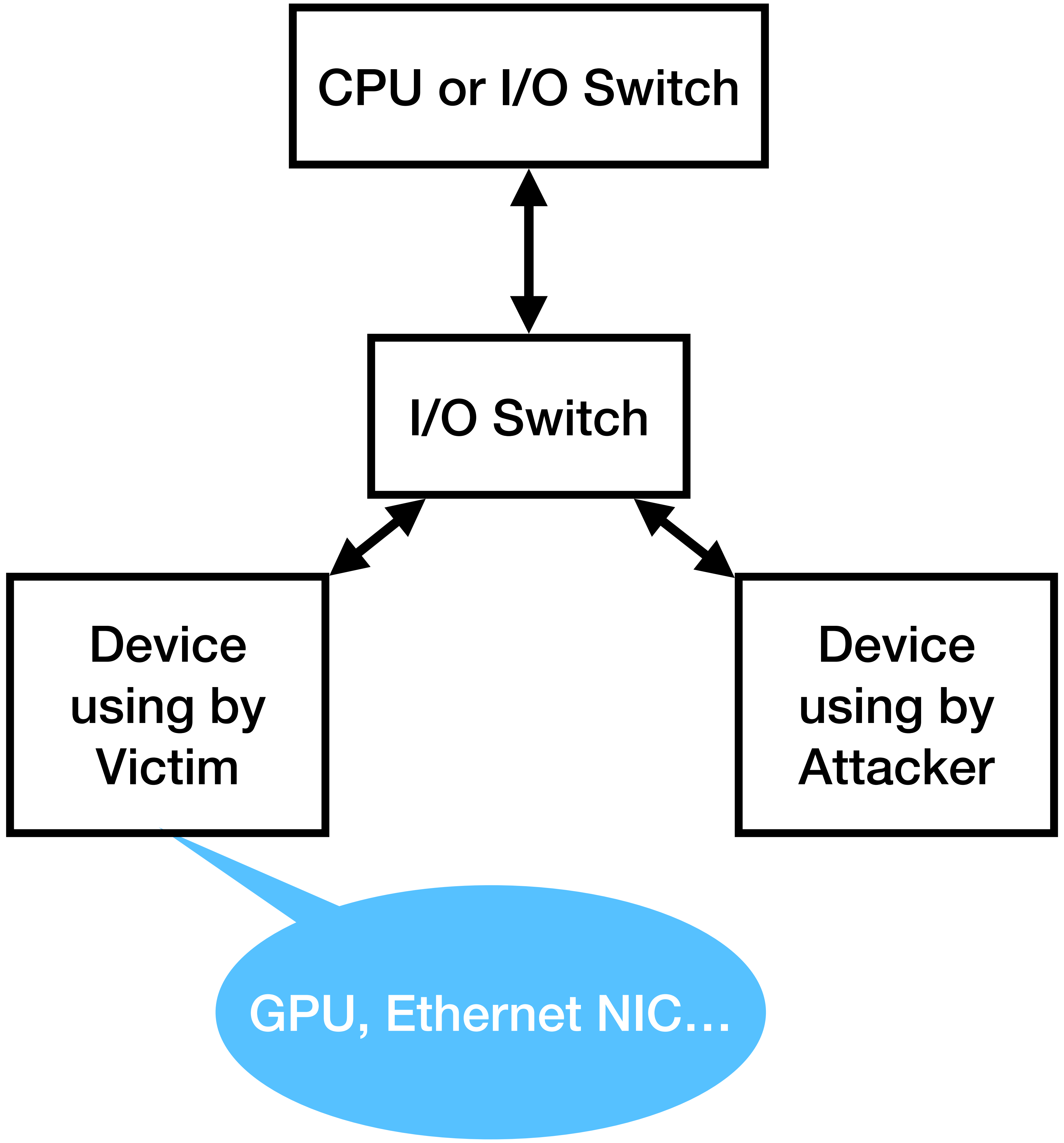


What information can we infer?



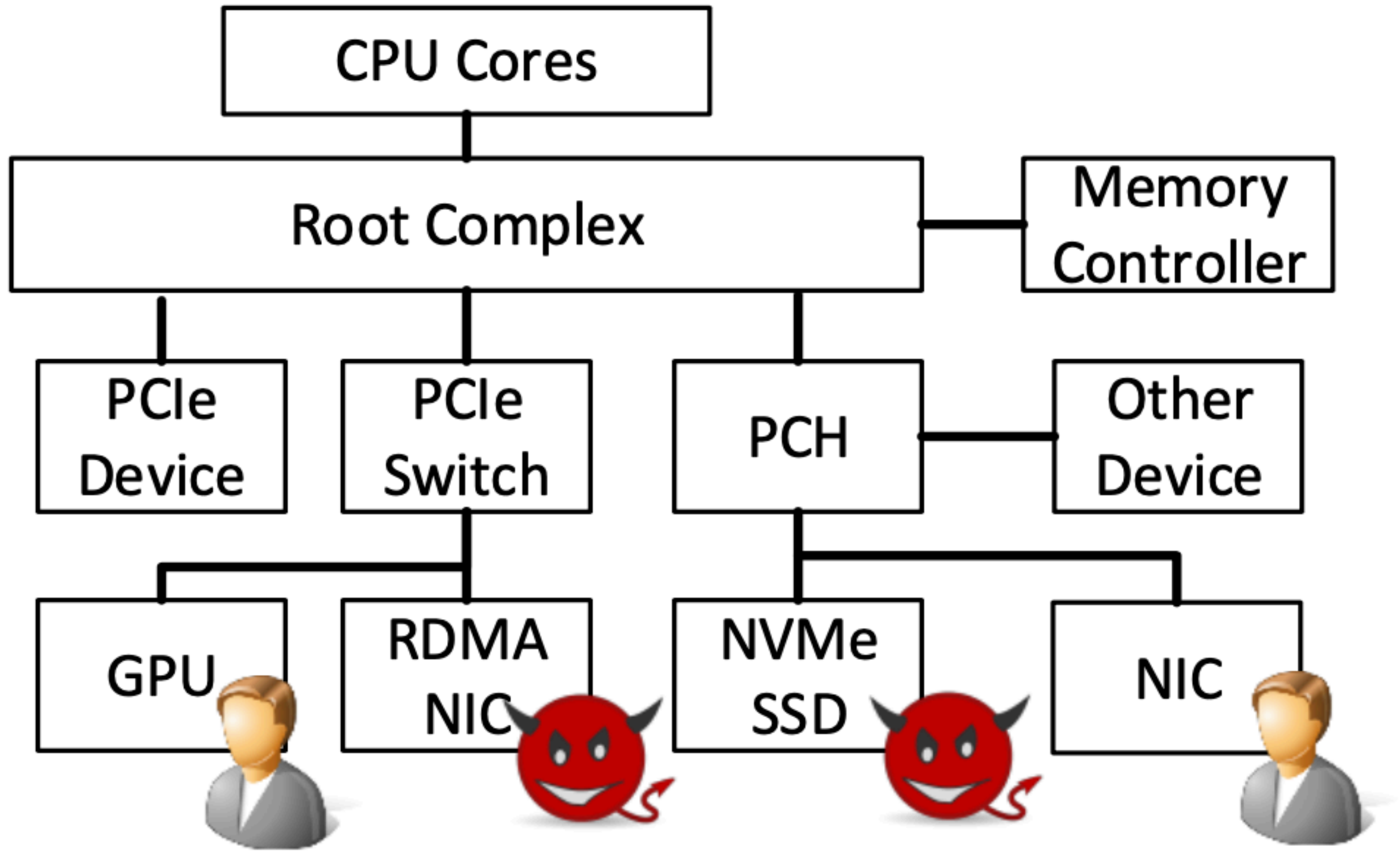
- GPU
  - password input in monitor
  - render webpages
  - machine Learning models trained

What information can we infer?

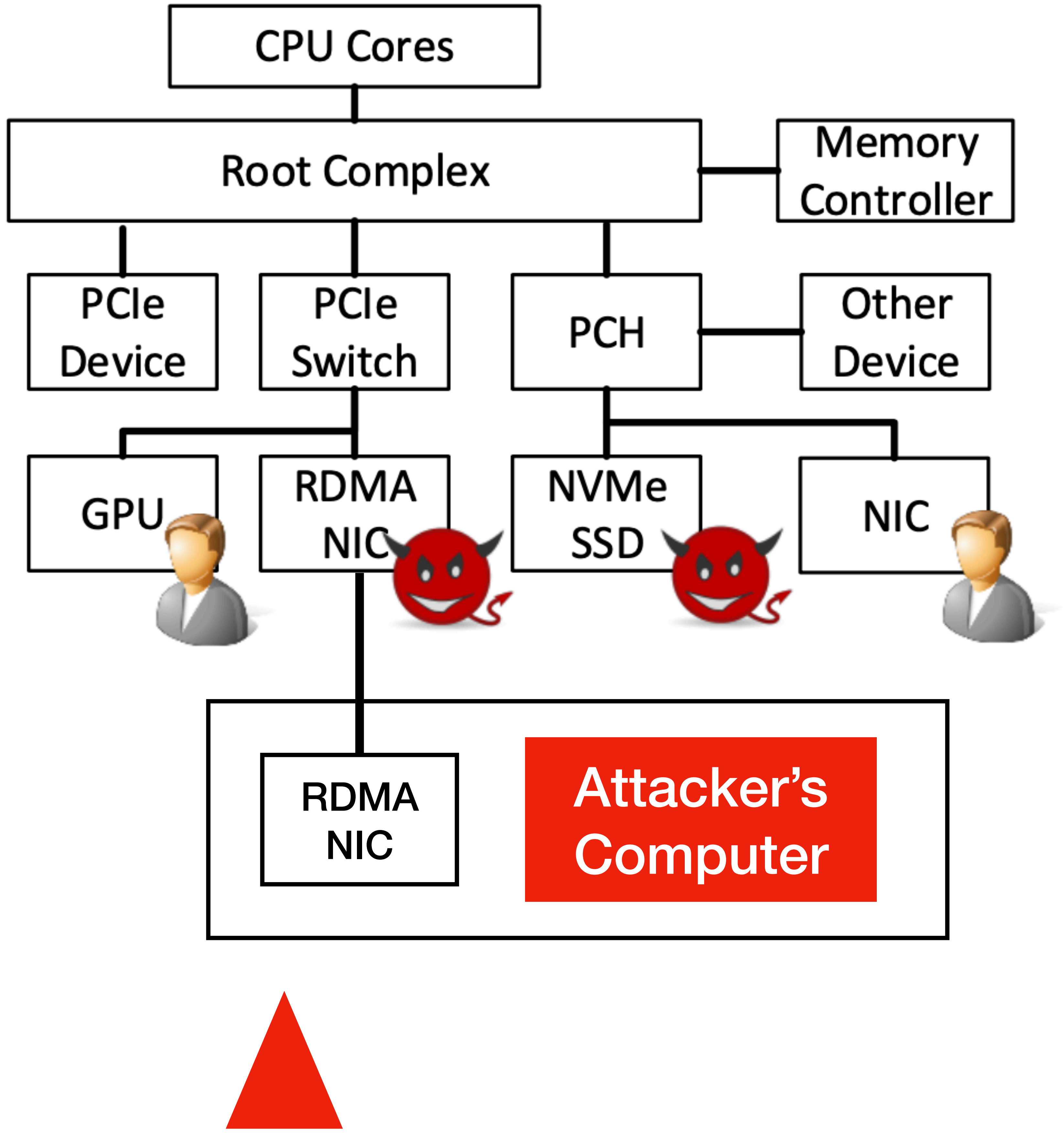


- GPU
  - password input in monitor
  - render webpages
  - machine Learning models trained
- Ethernet NIC
  - transmit webpages packets
  - SSH passwords or texts

Attack scenarios and victim tasks

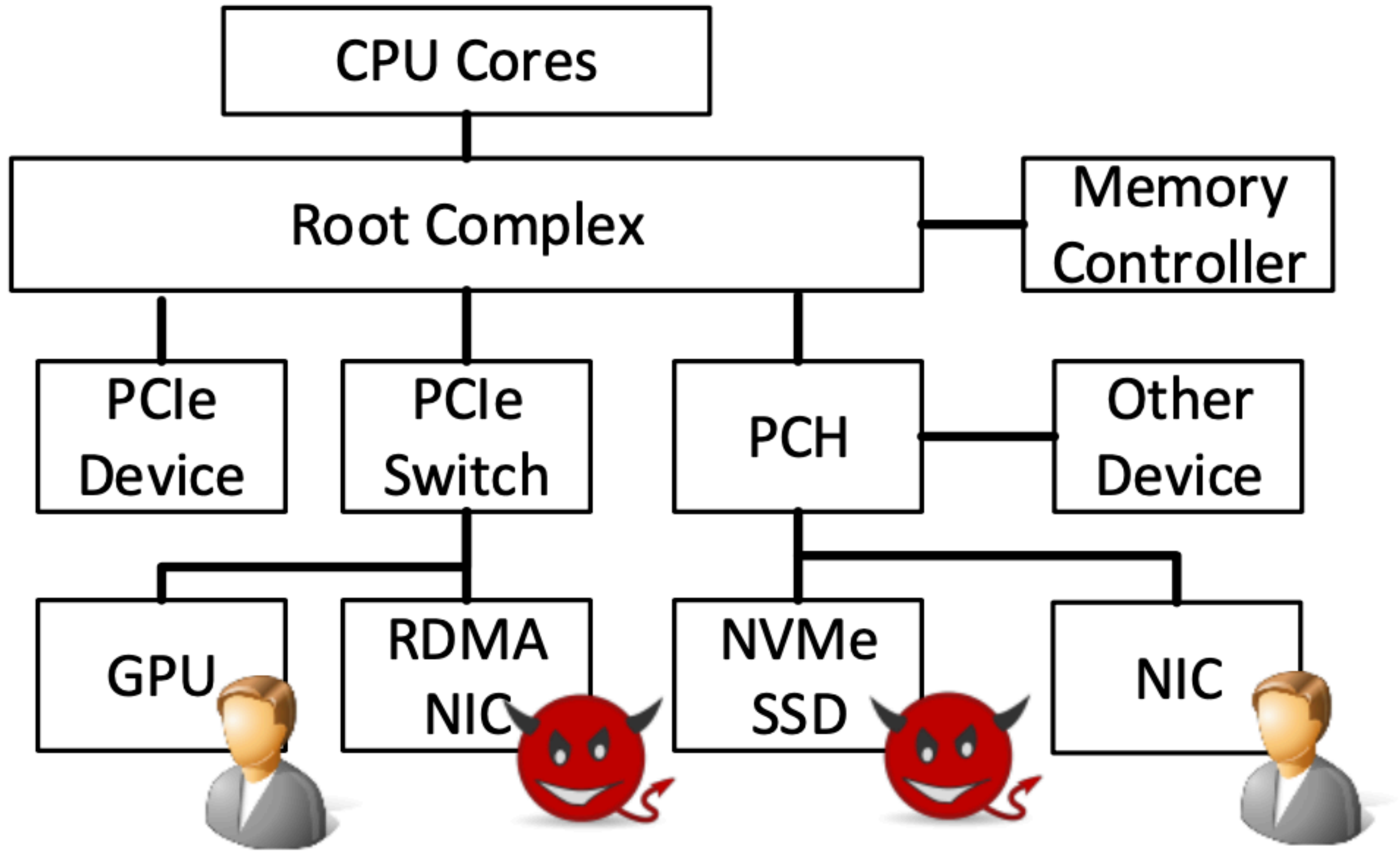


Attack scenarios and victim tasks



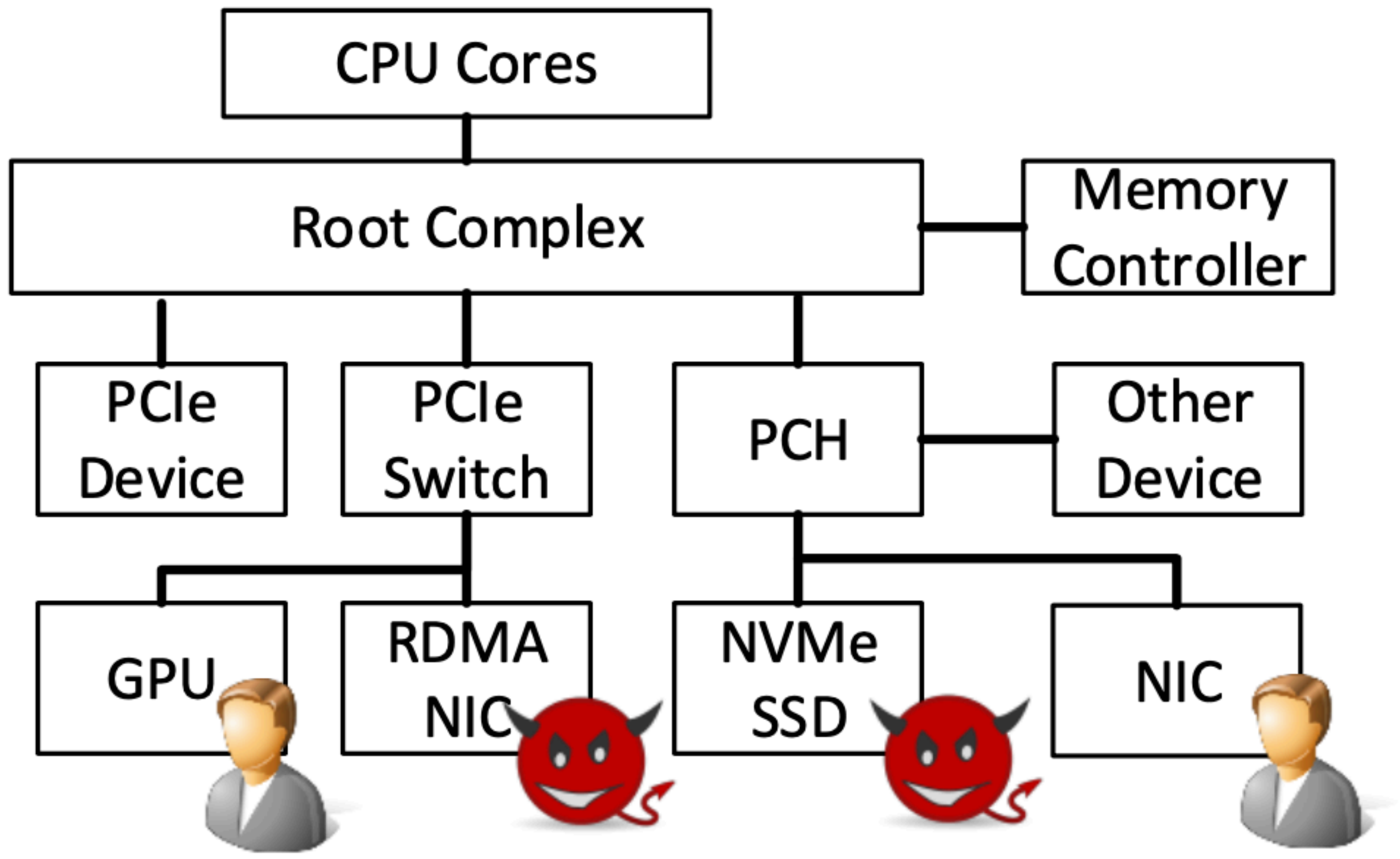
S1 Control RDMA NIC to attack GPU

Attack scenarios and victim tasks



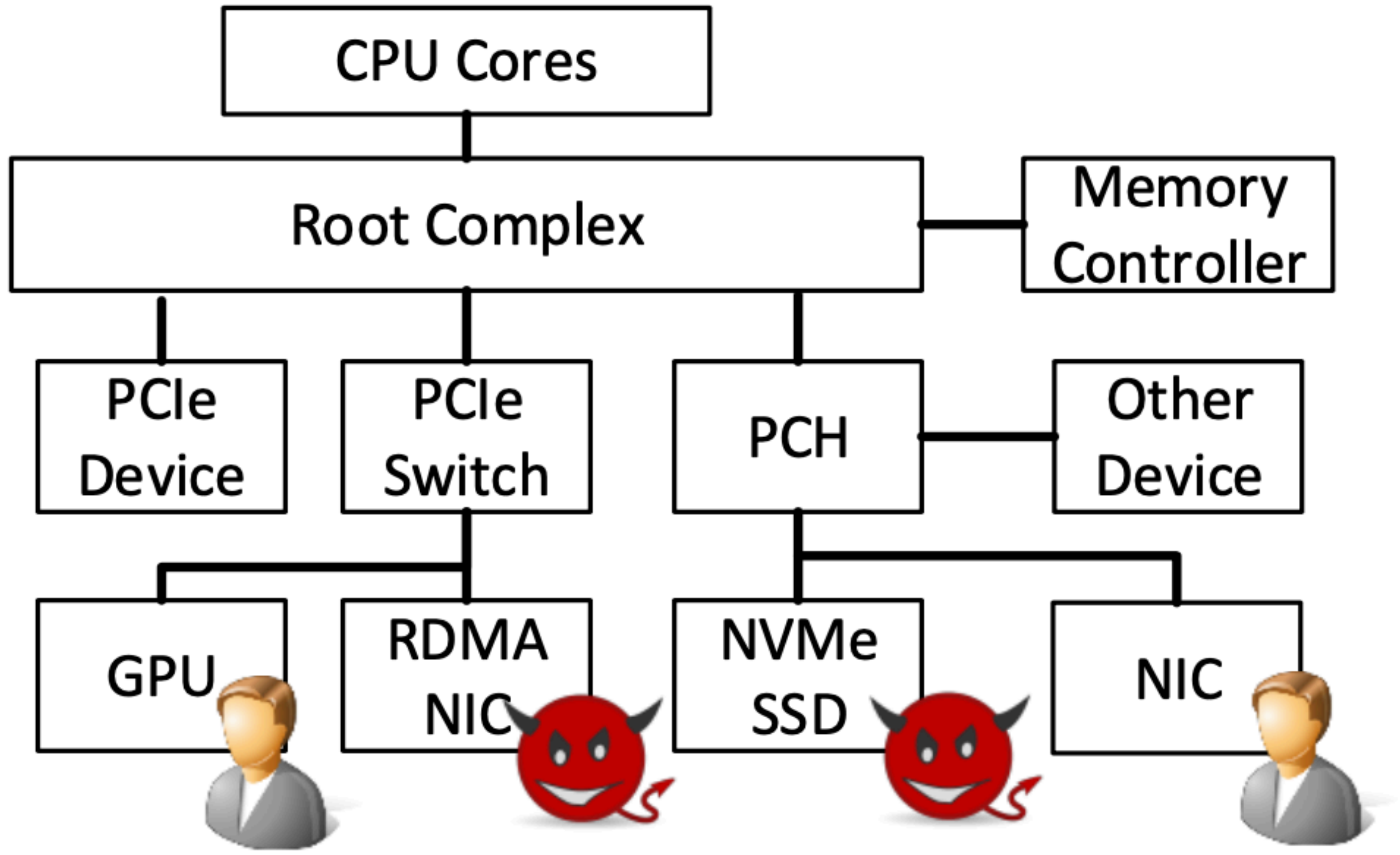
S2 Control NVMe SSD to attack Ethernet NIC

Attack scenarios and victim tasks



- T1 User-input Inference
- T2 Webpage Inference
- T3 Machine-learning Model Inference

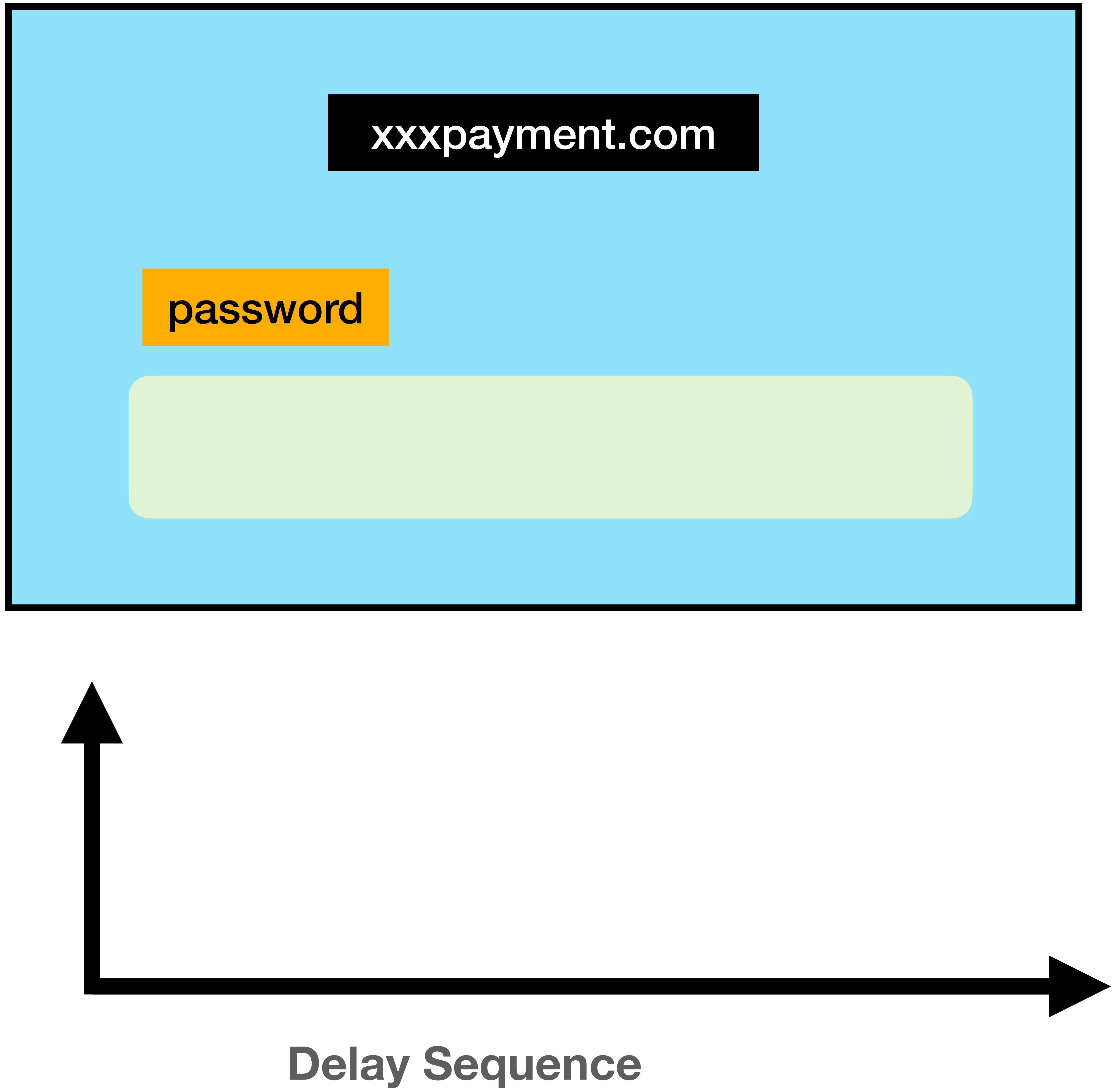
Attack scenarios and victim tasks

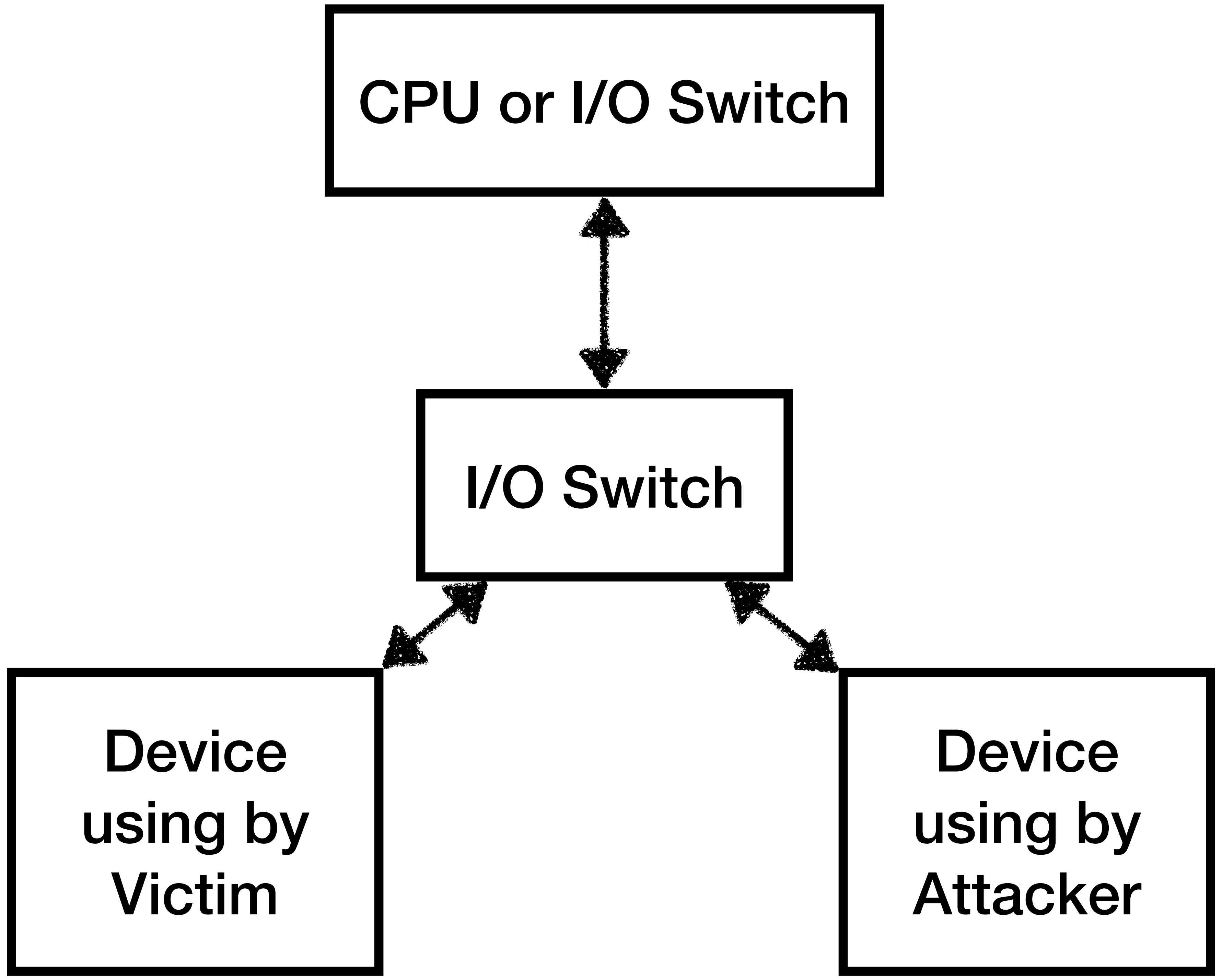


- T1 User-input Inference
- T2 Webpage Inference
- T3 Machine-learning Model Inference

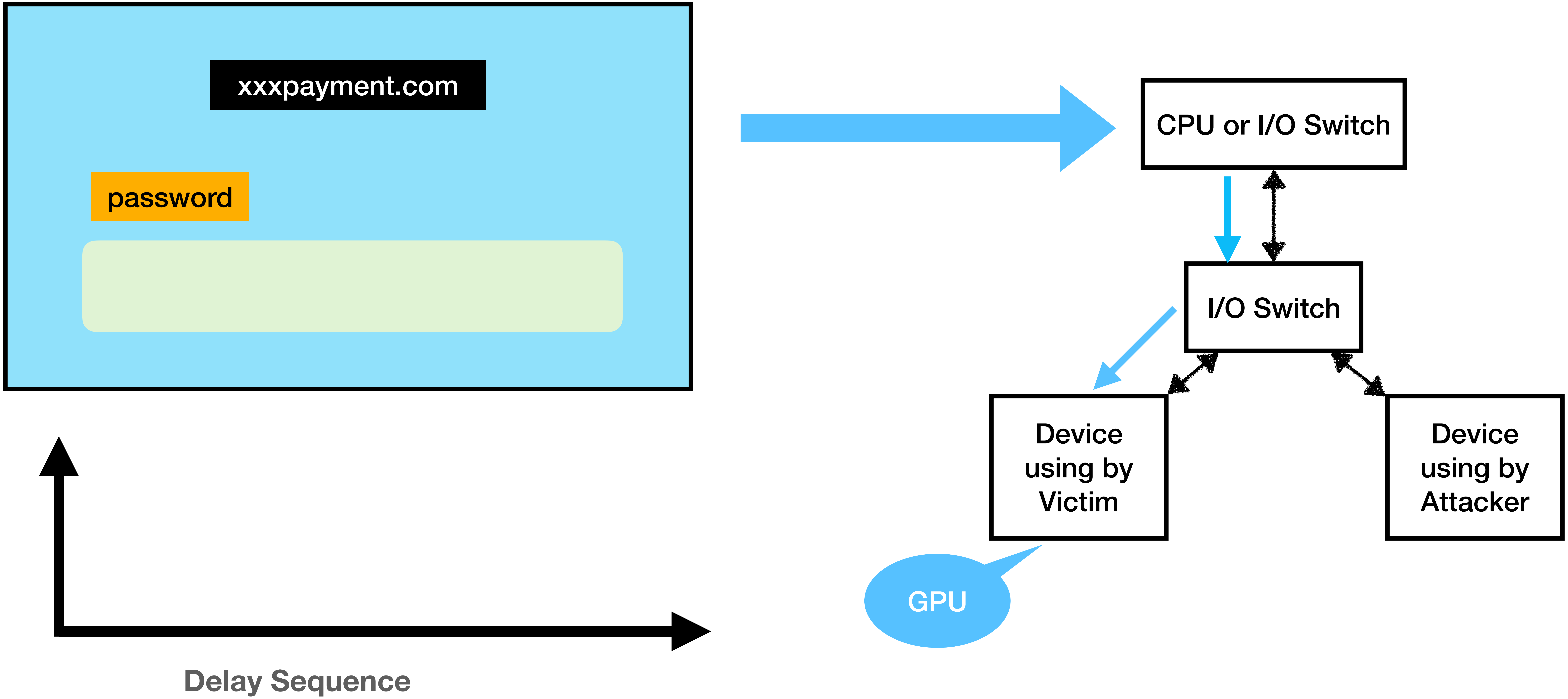
	T1	T2	T3
S1	✓	✓	✓
S2		✓	

User-input Inference

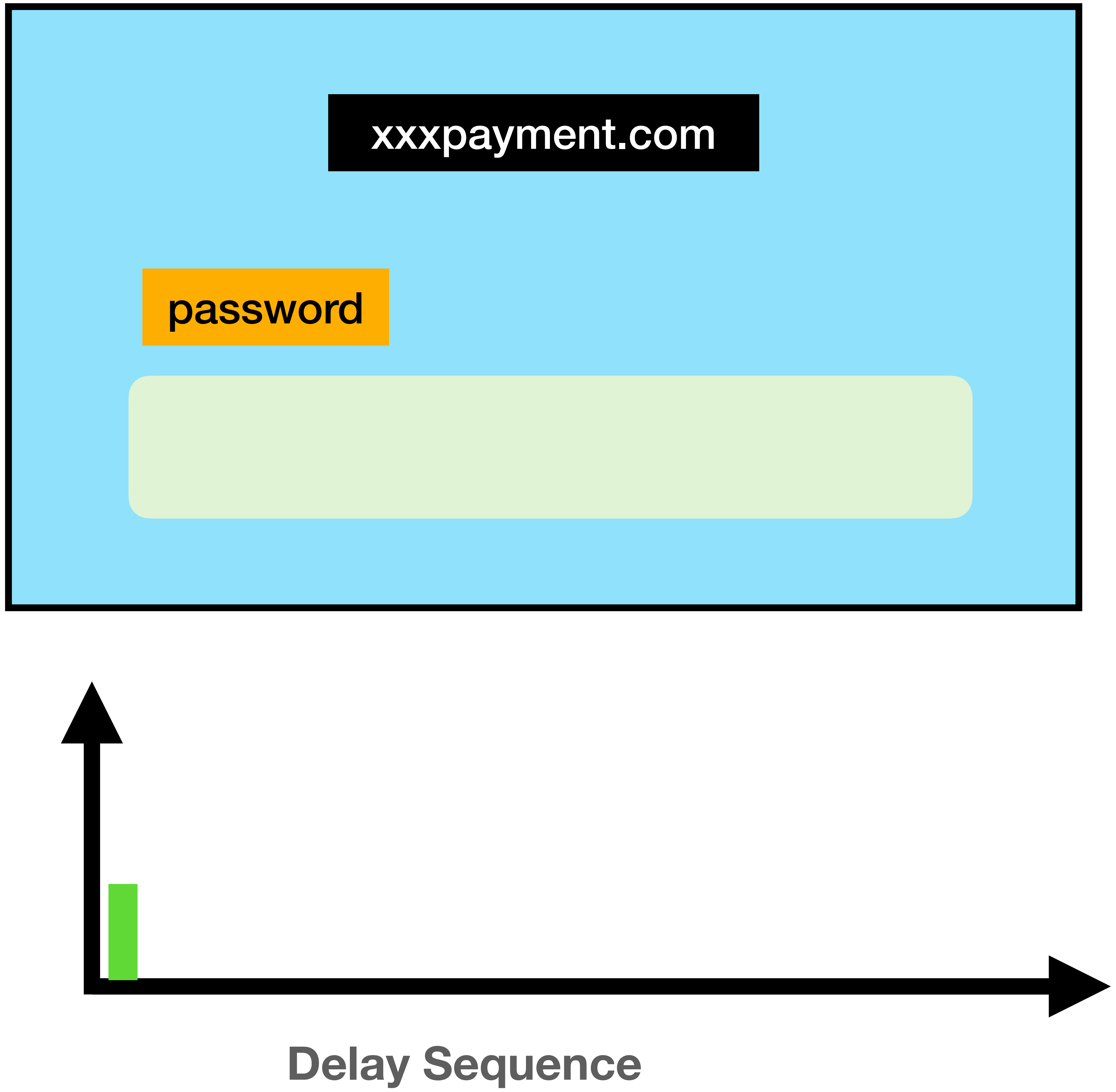


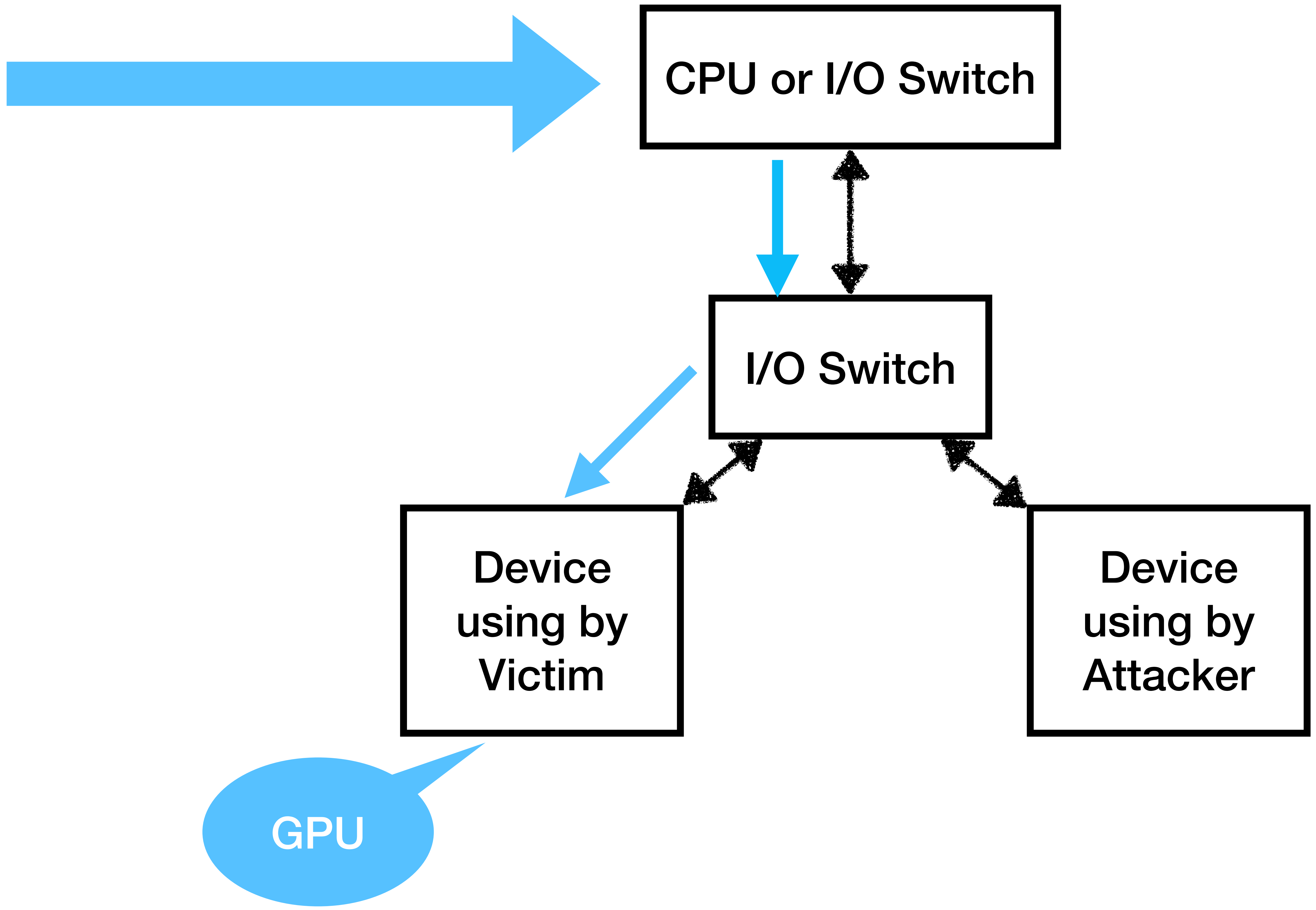


User-input Inference

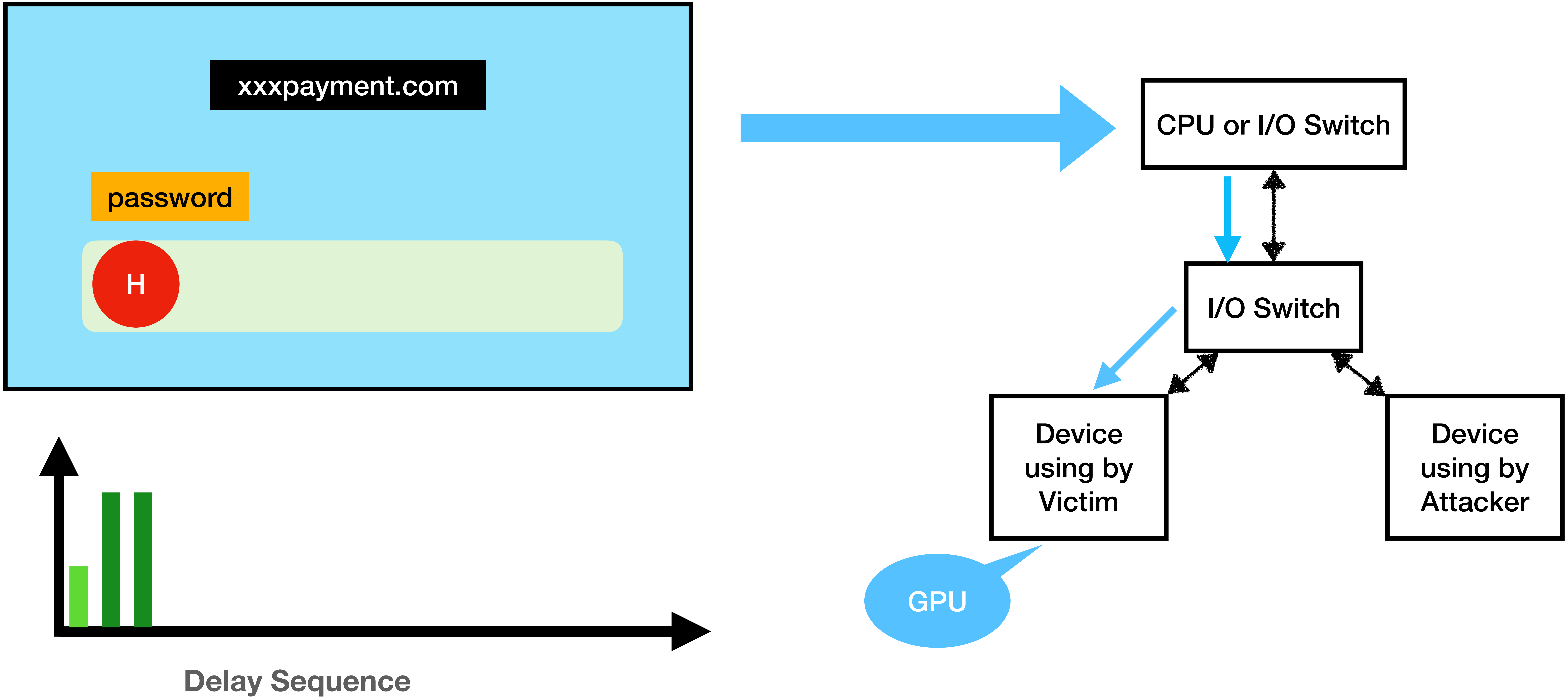


User-input Inference

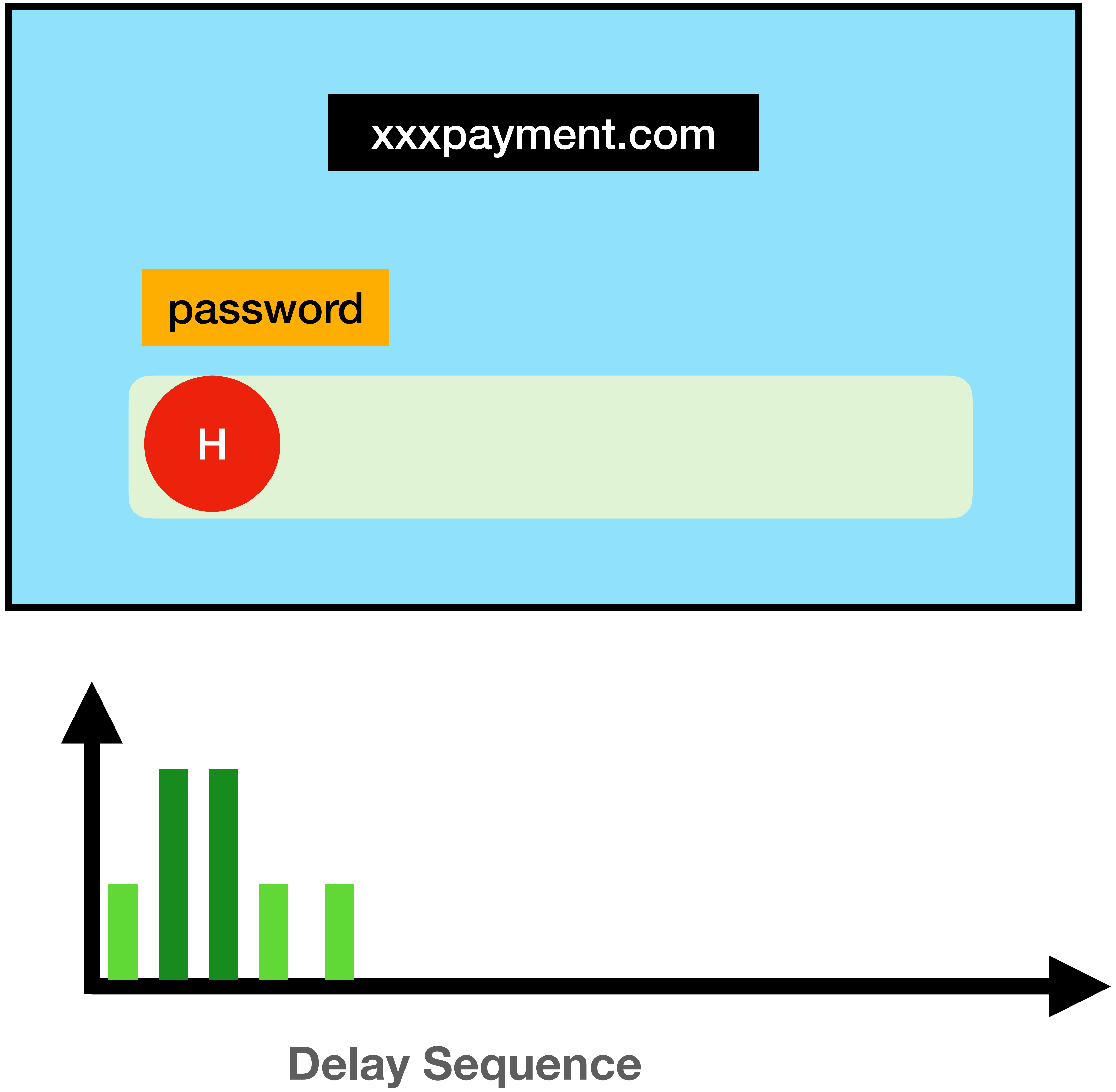


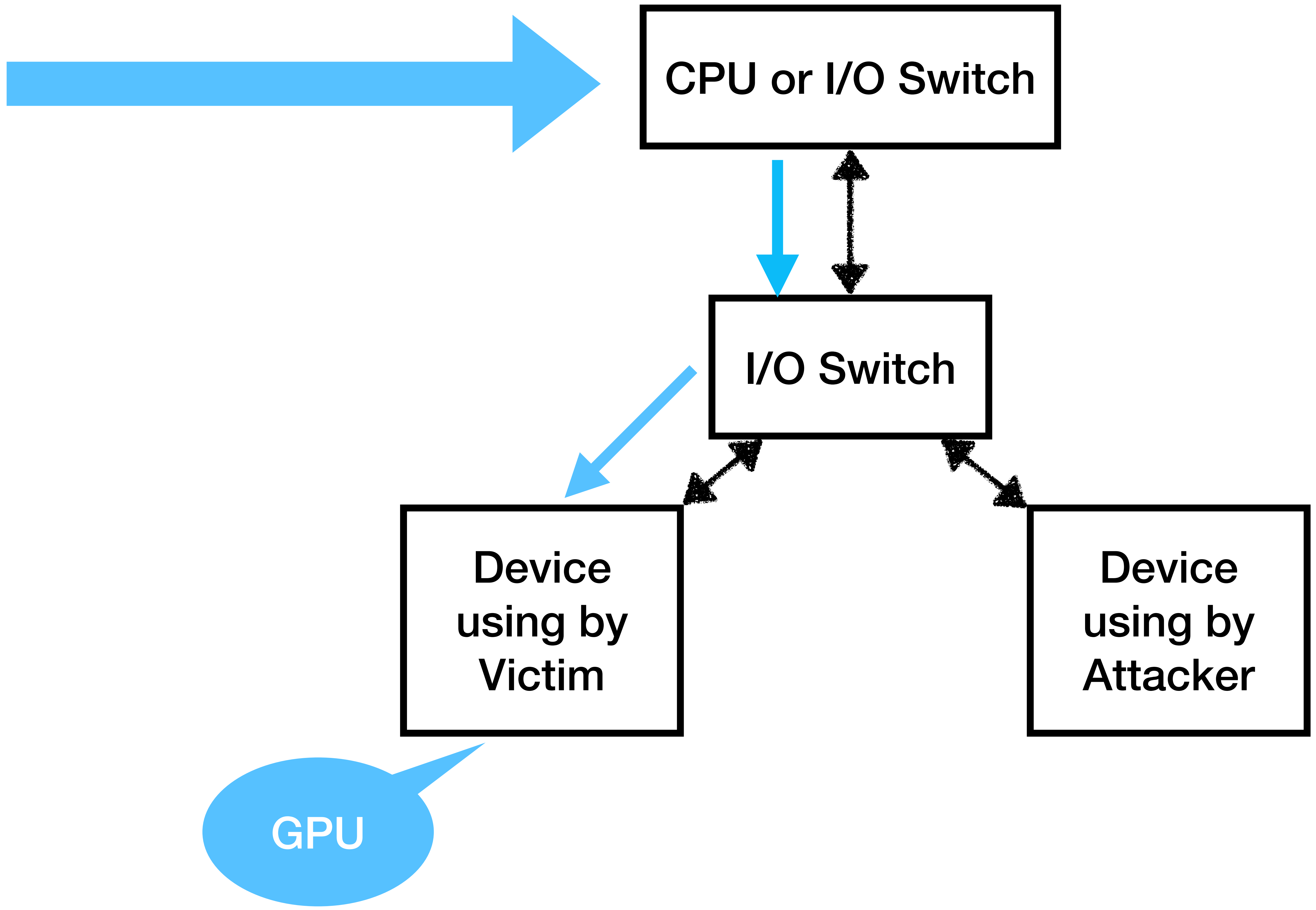


User-input Inference

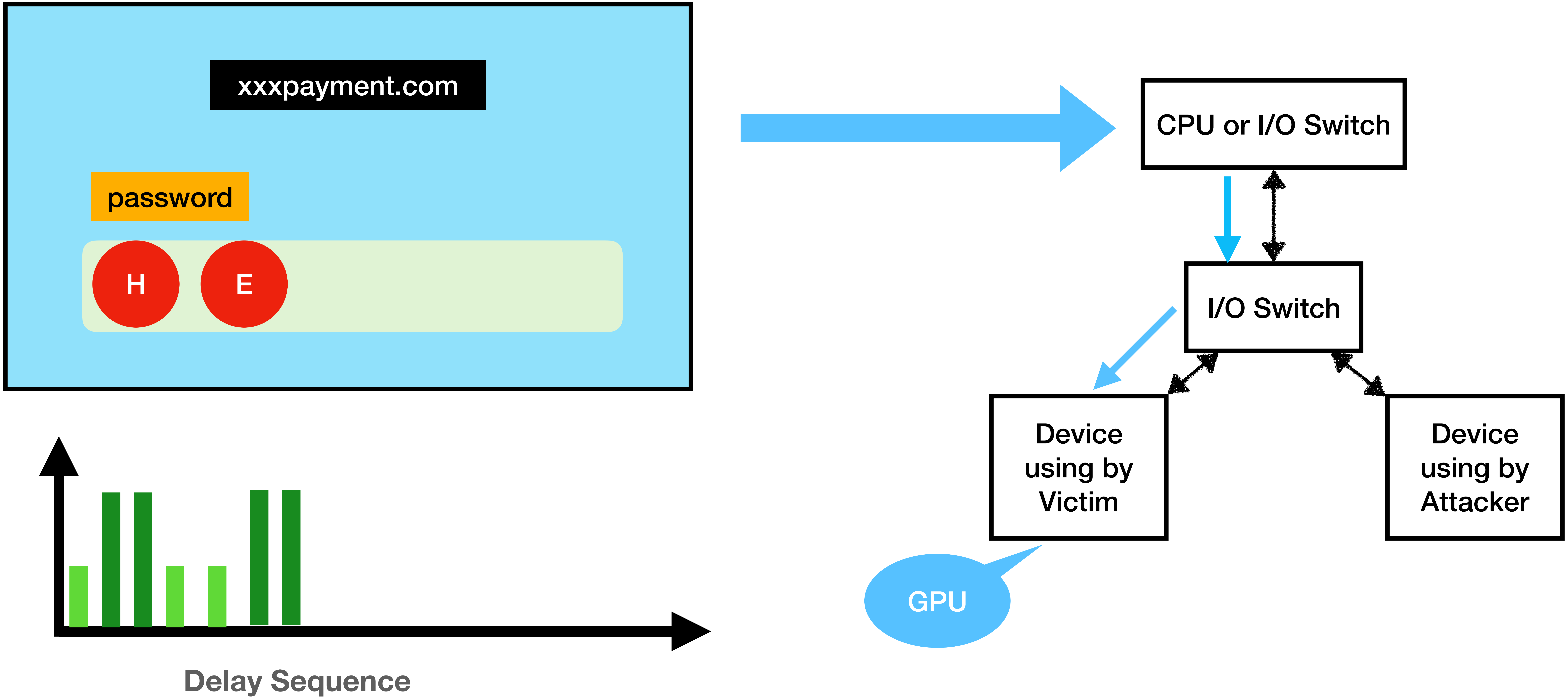


User-input Inference

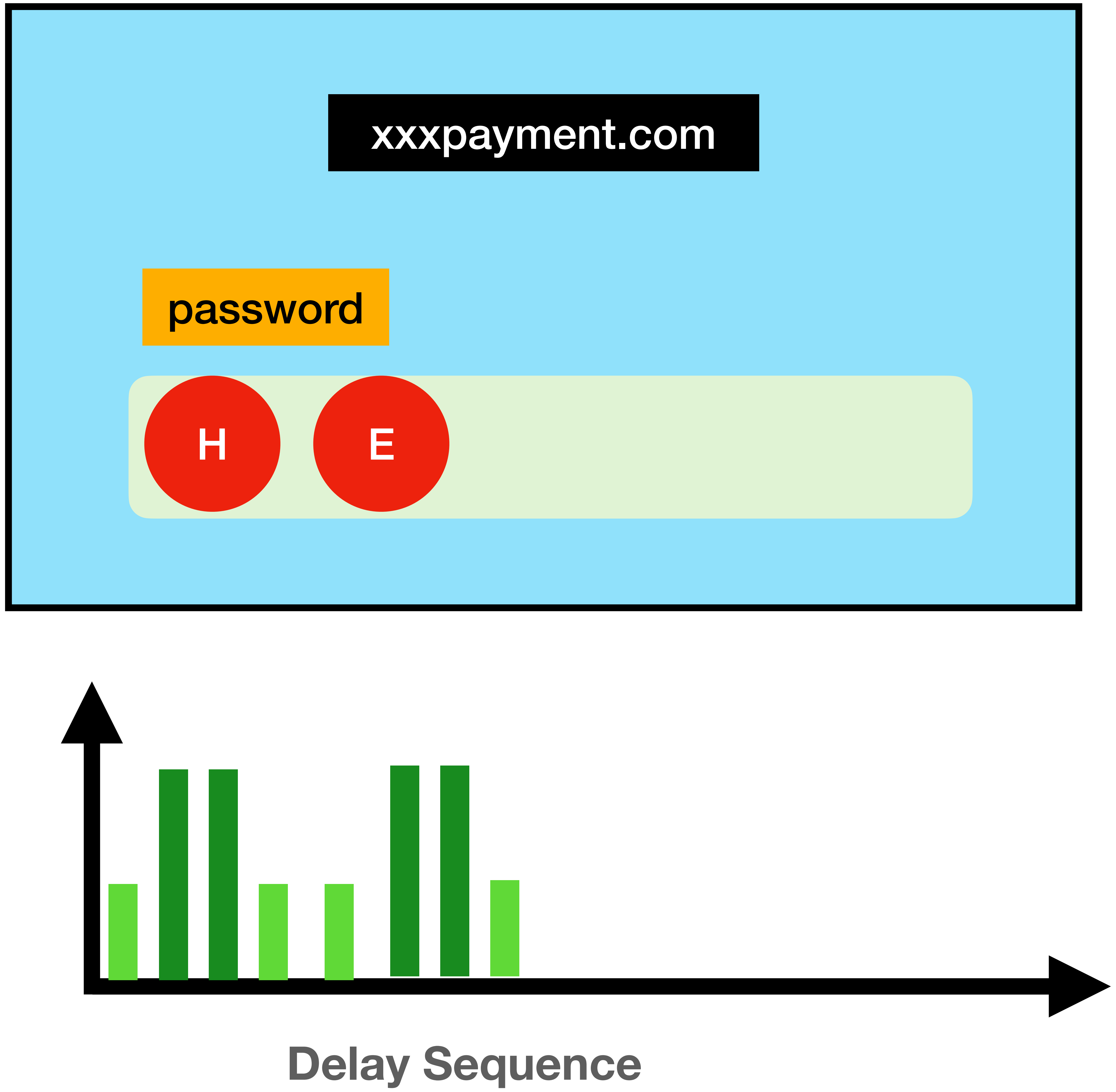


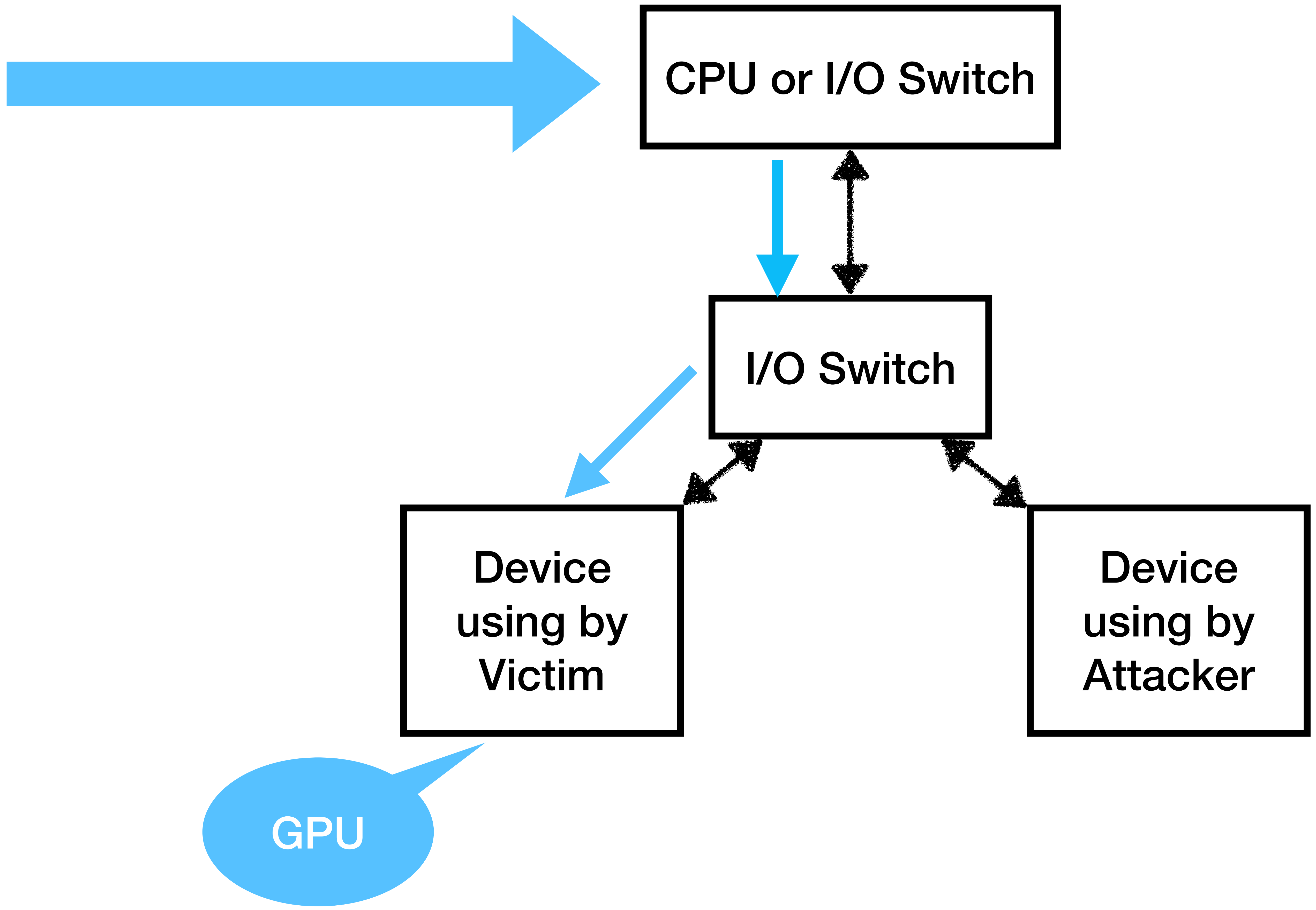


User-input Inference

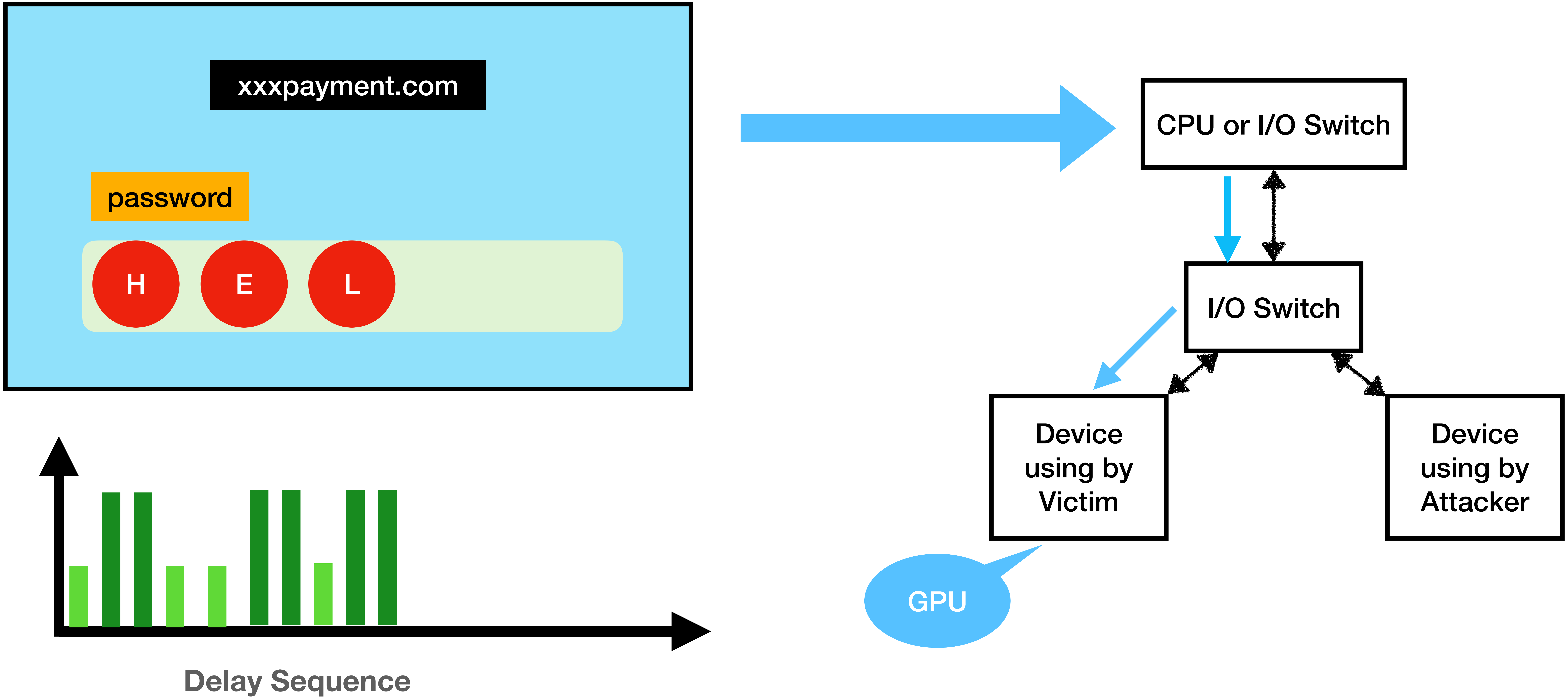


User-input Inference

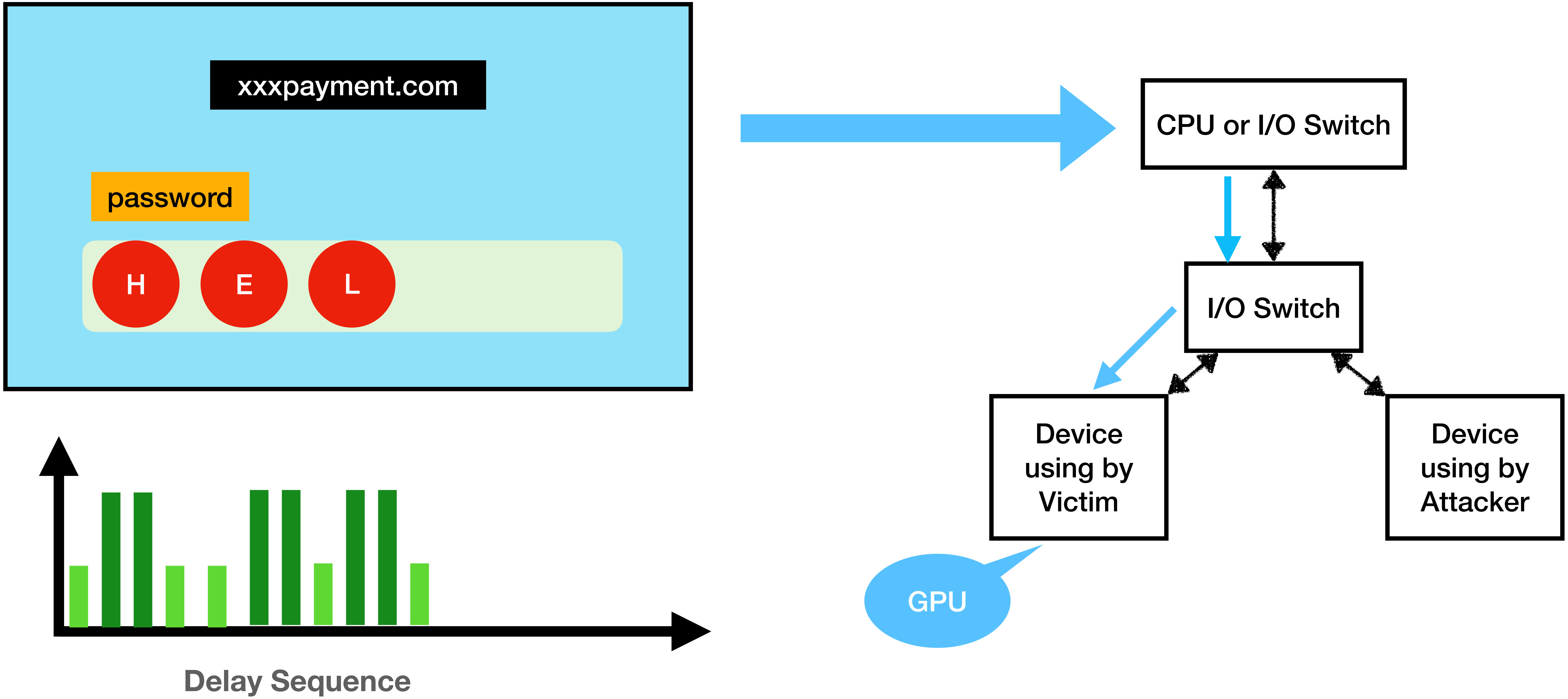




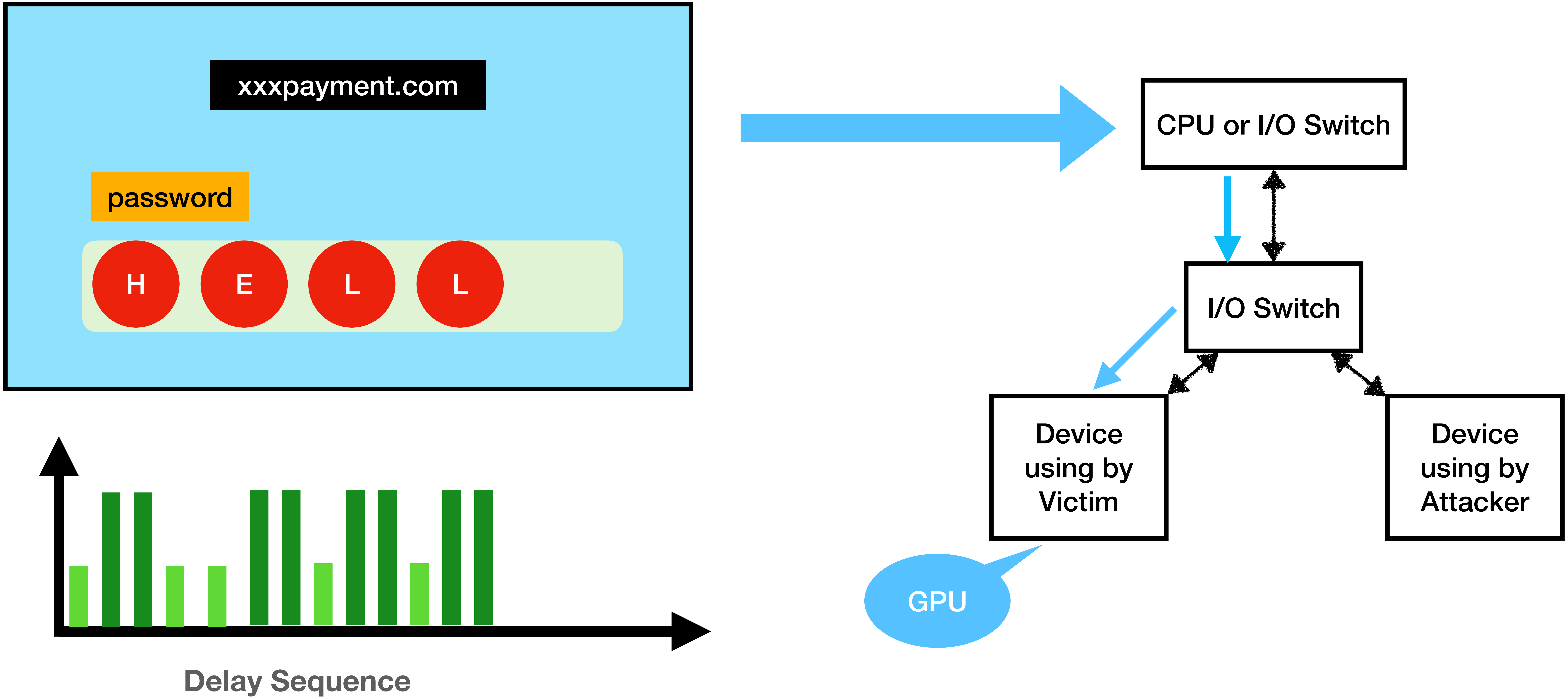
User-input Inference



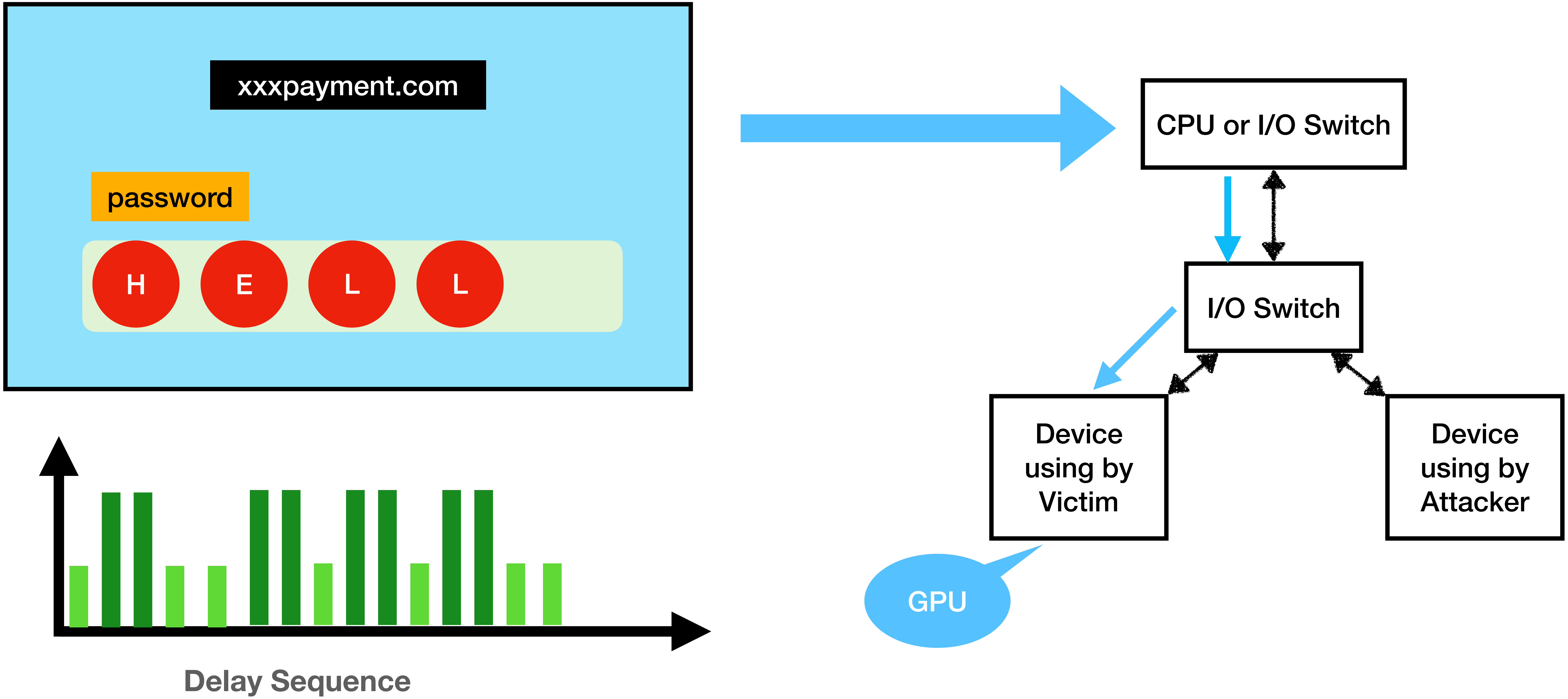
User-input Inference



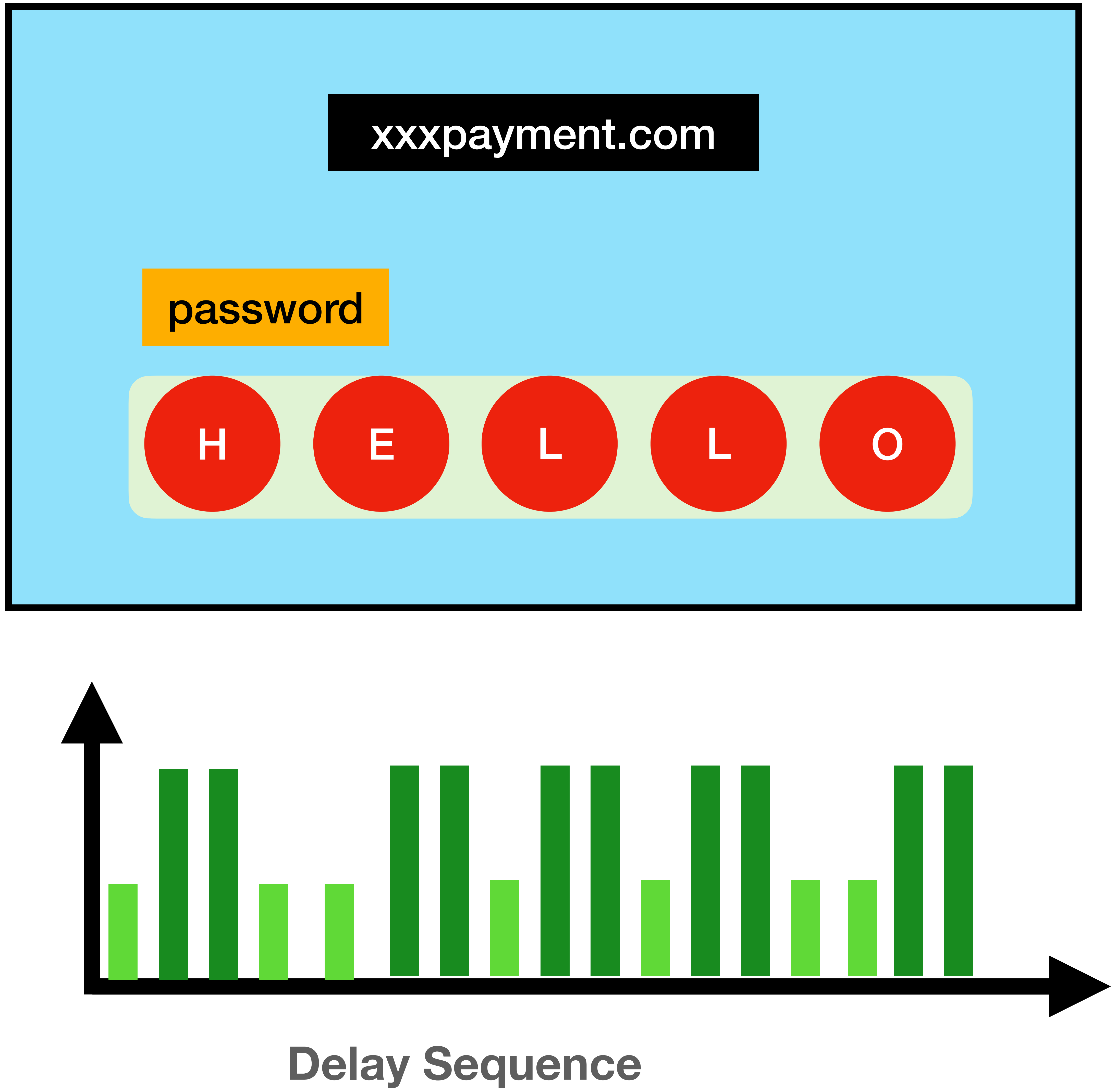
User-input Inference

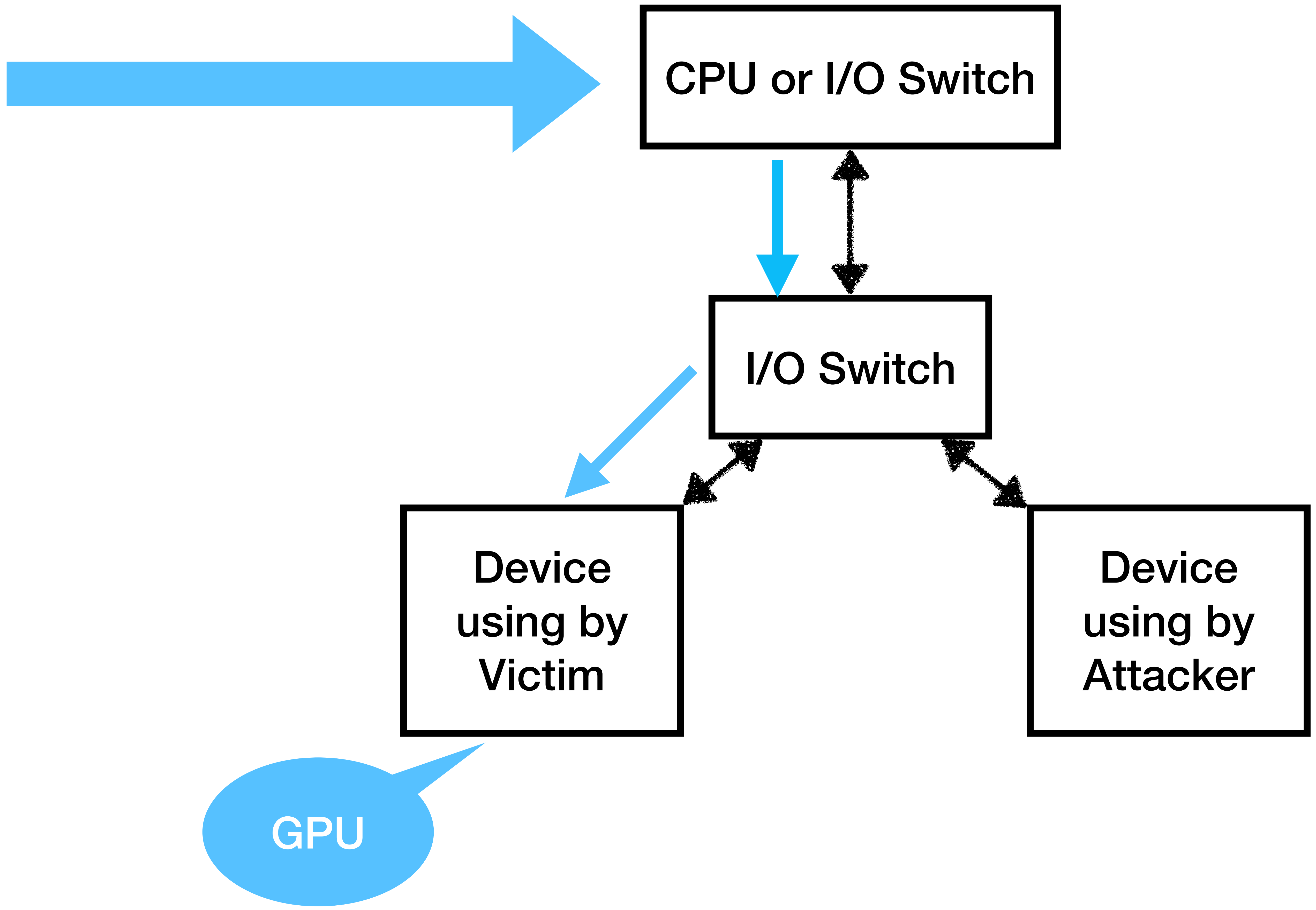


User-input Inference

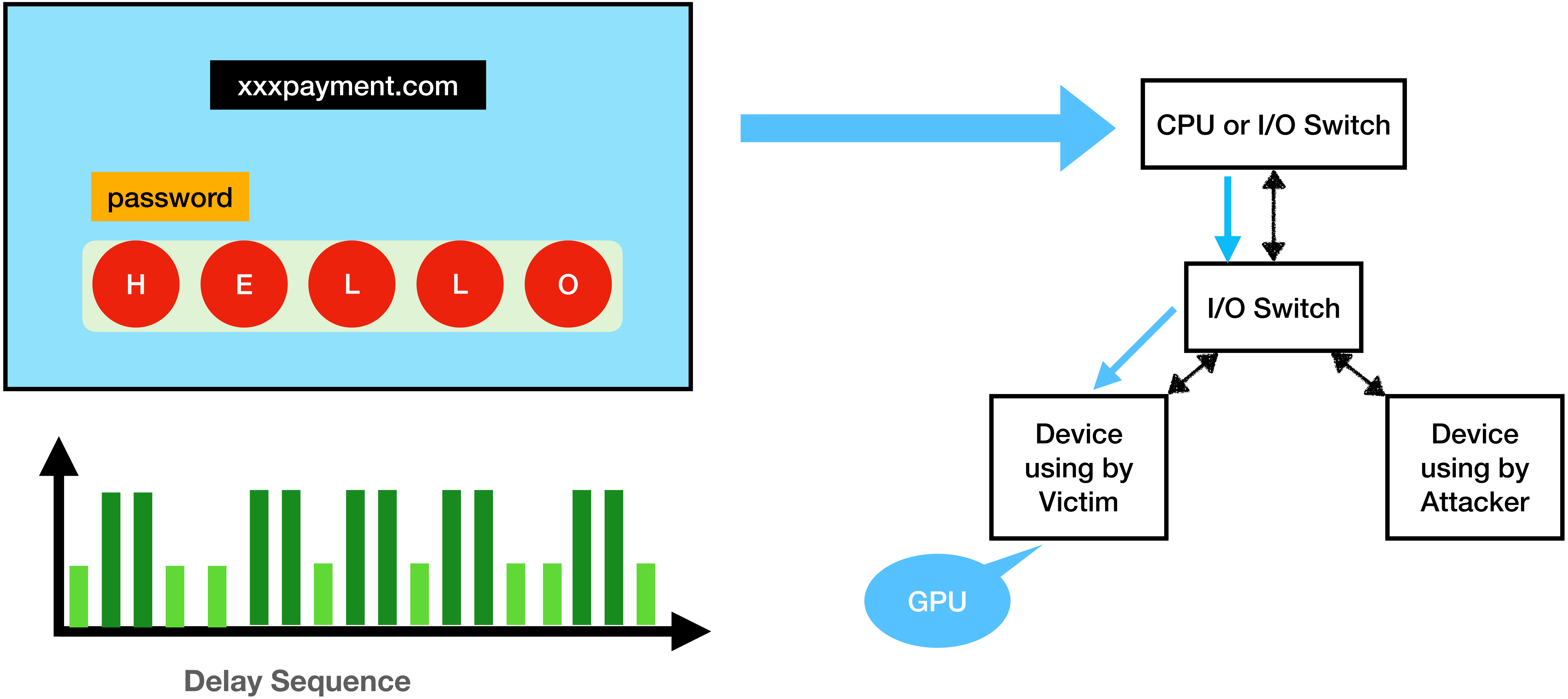


User-input Inference

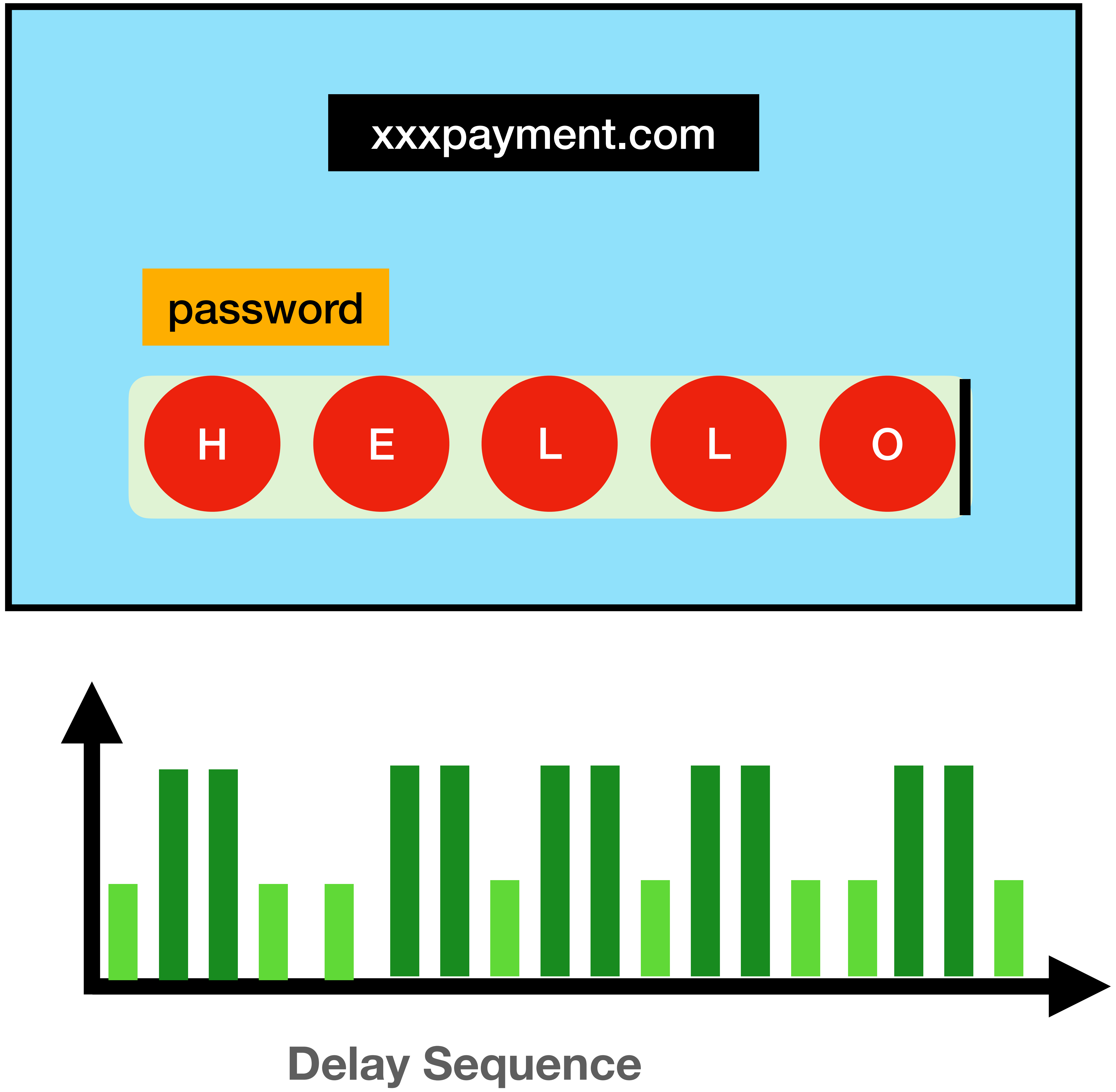


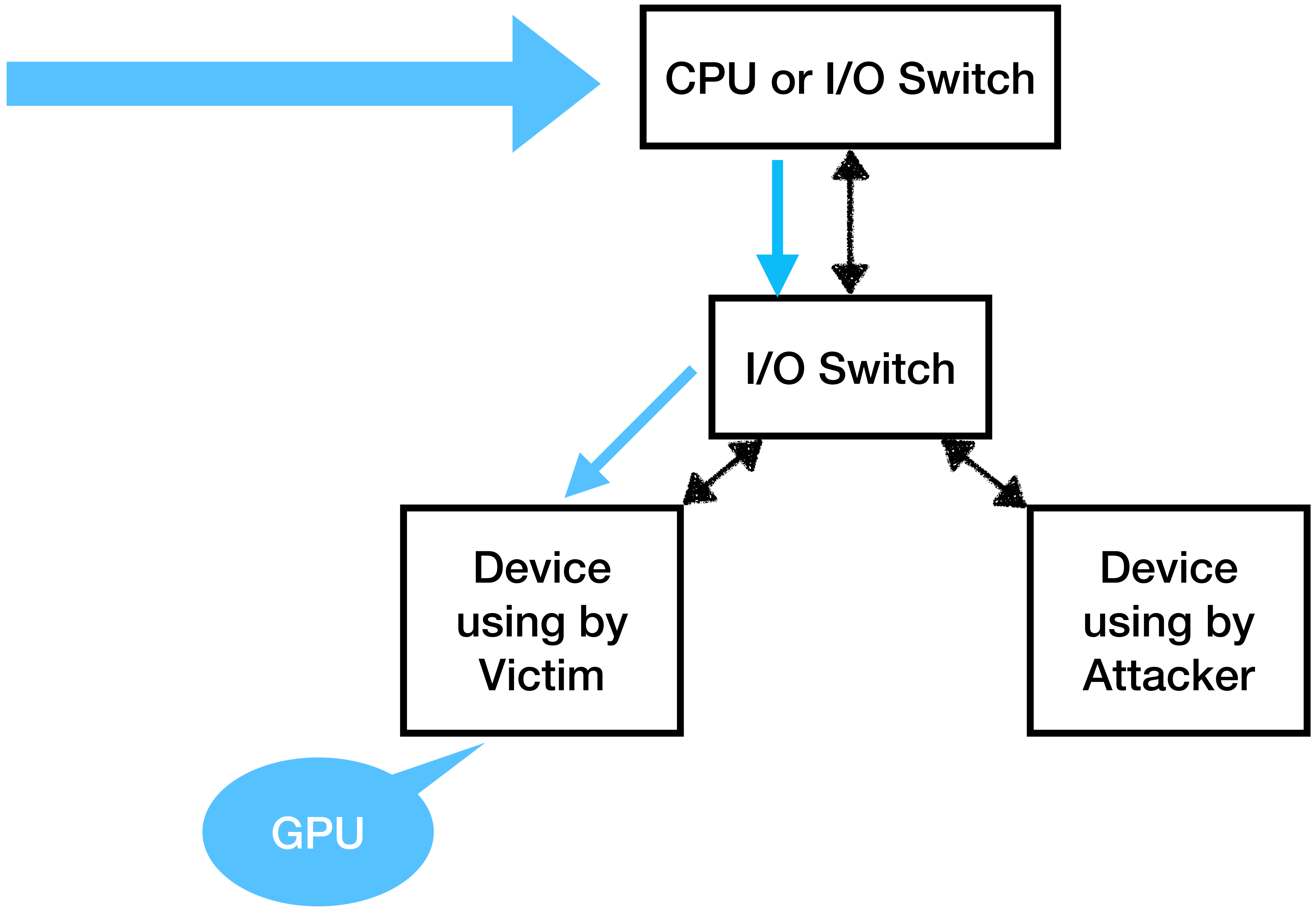


User-input Inference

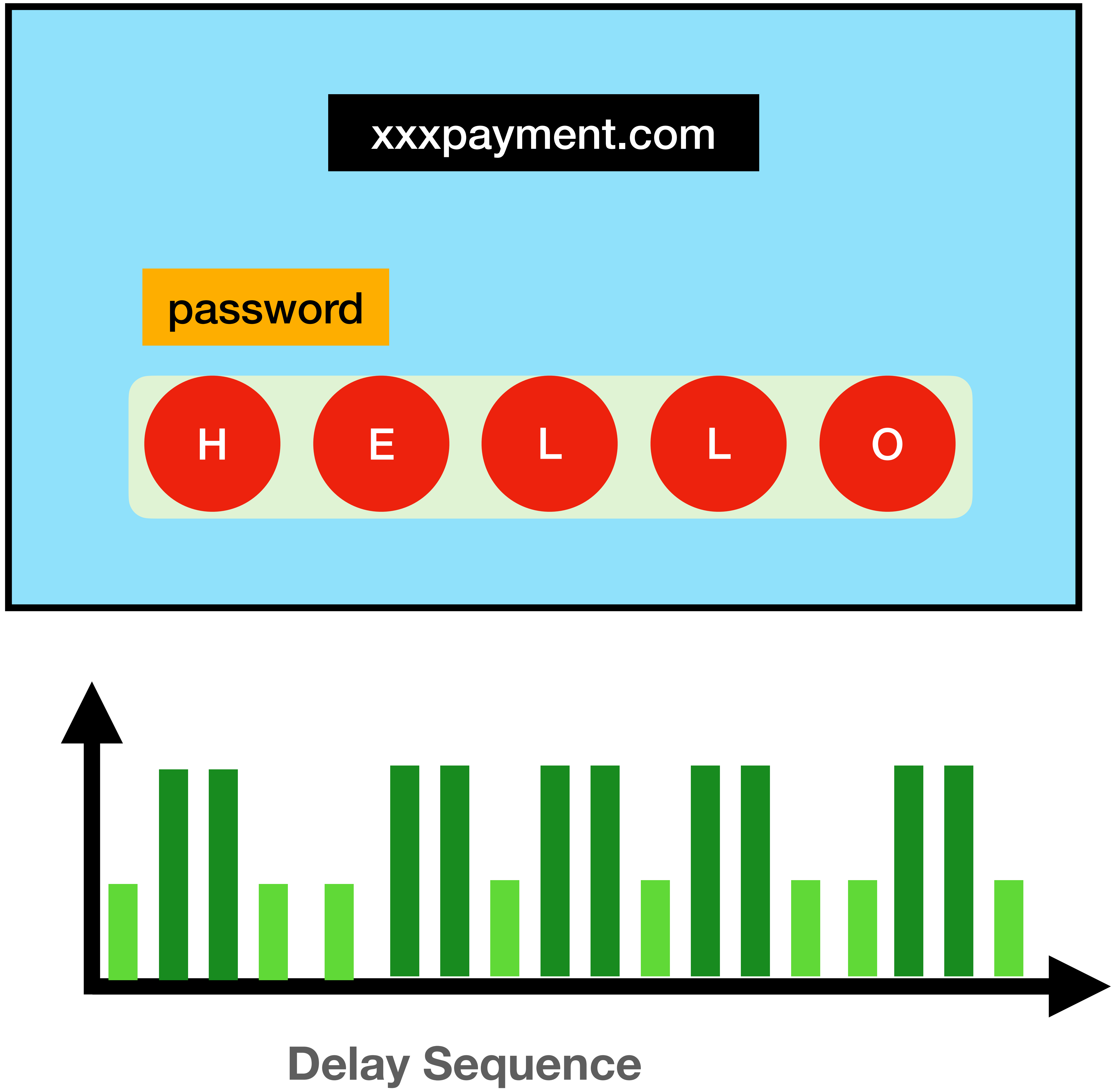


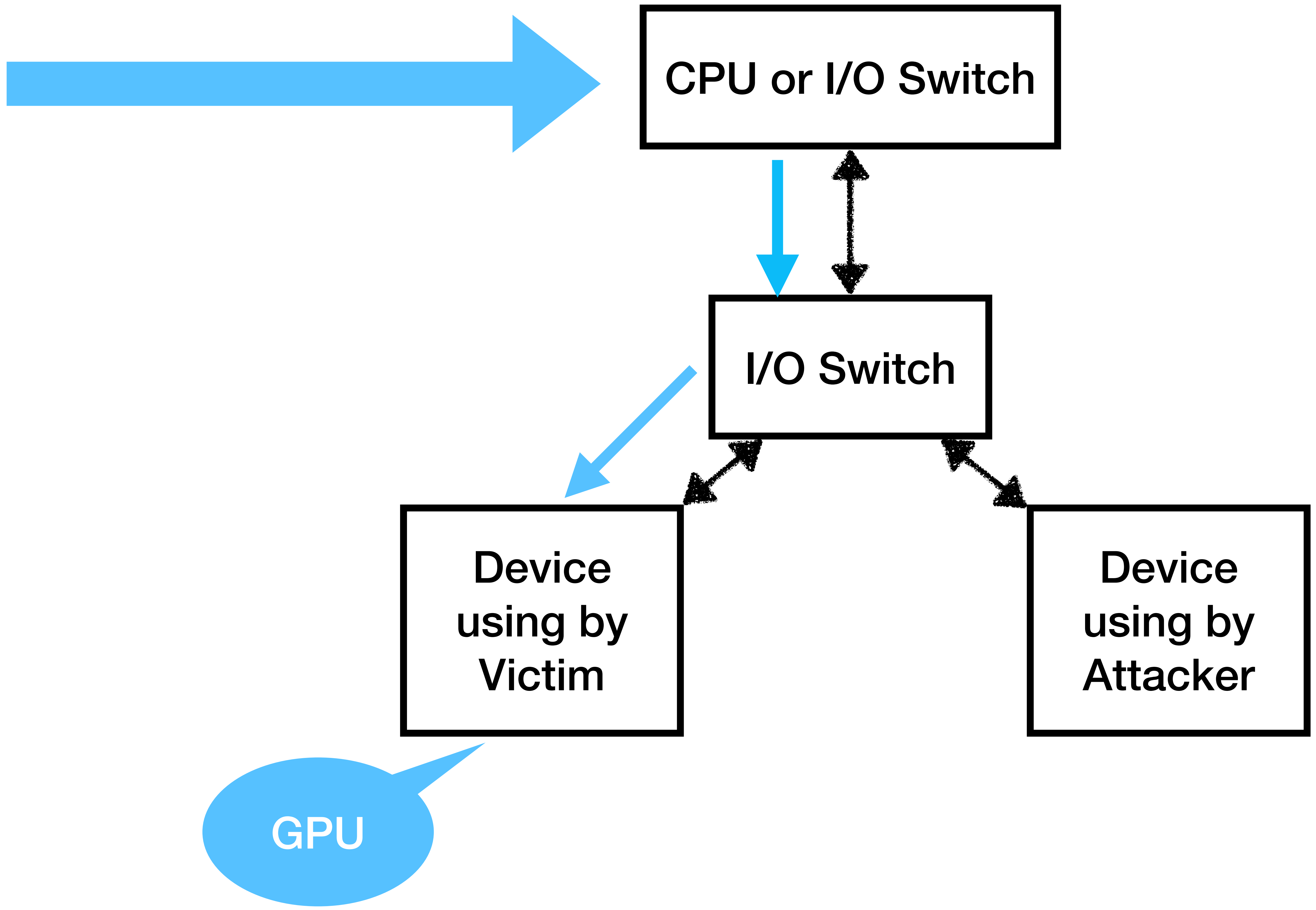
User-input Inference



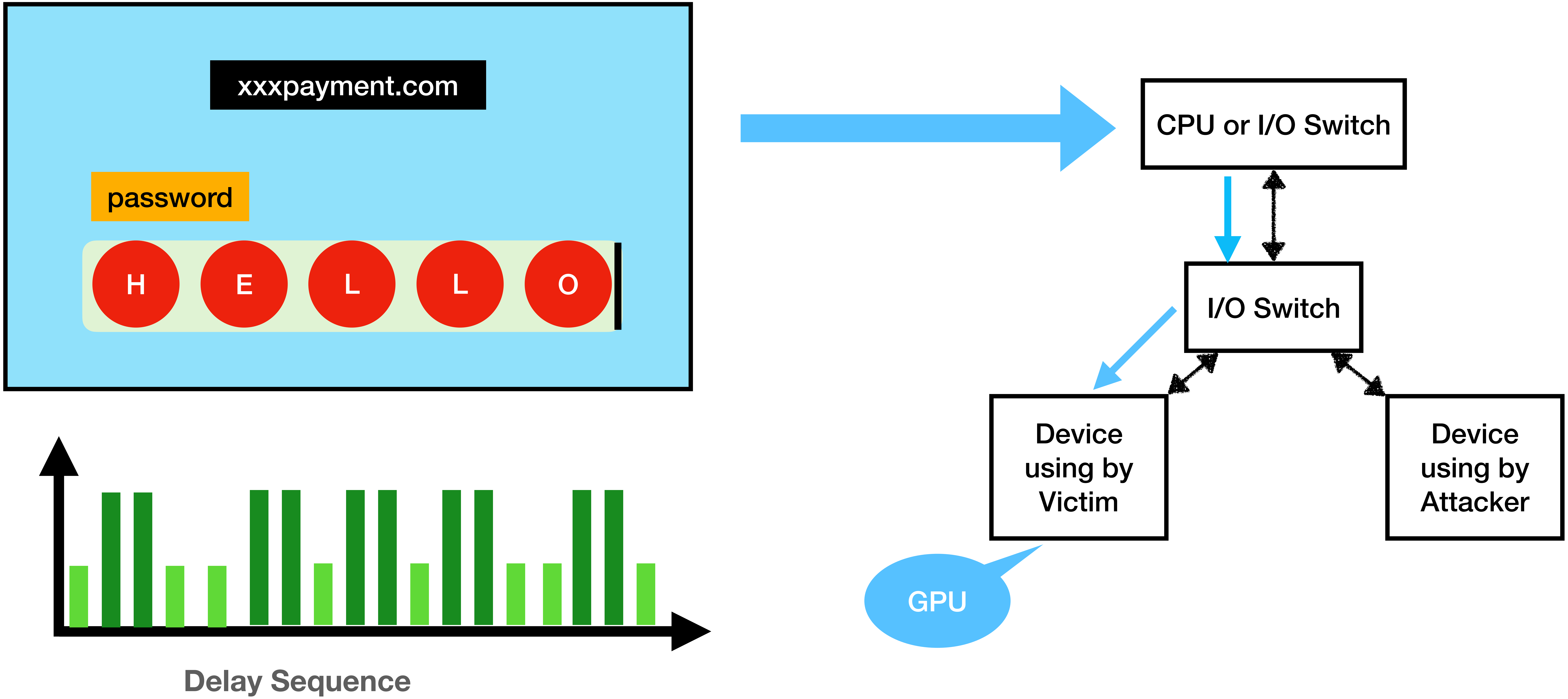


User-input Inference

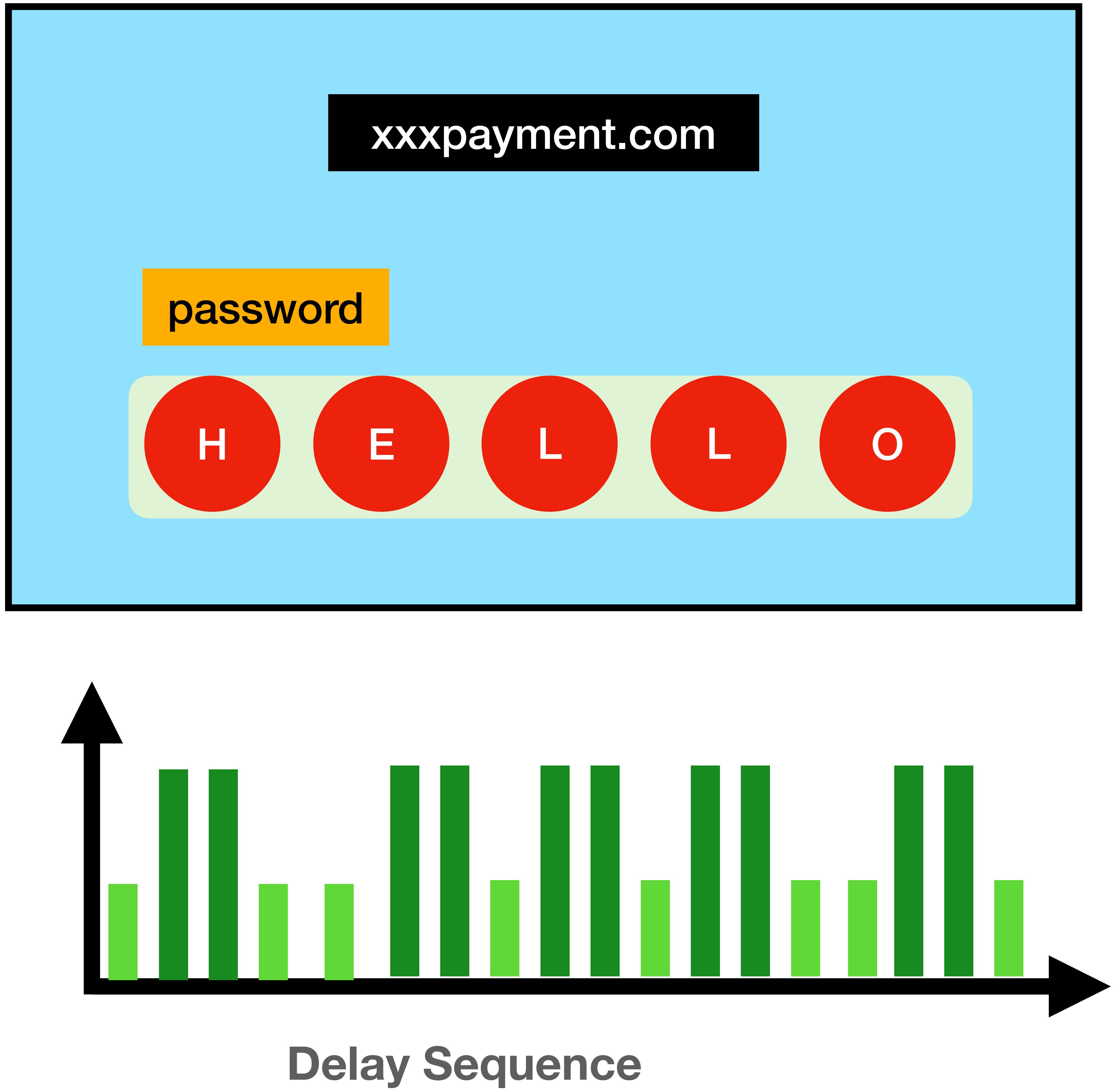


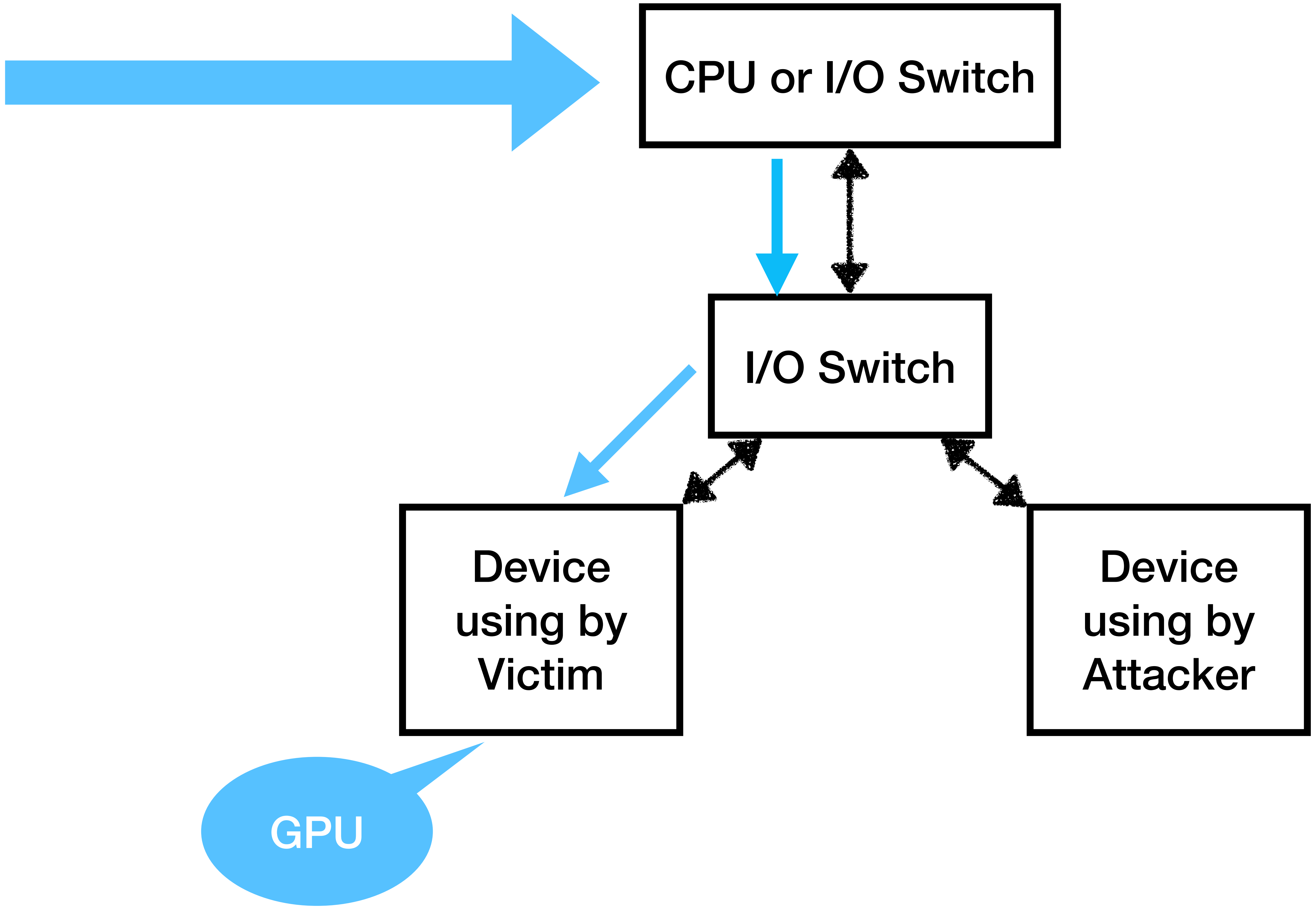


User-input Inference

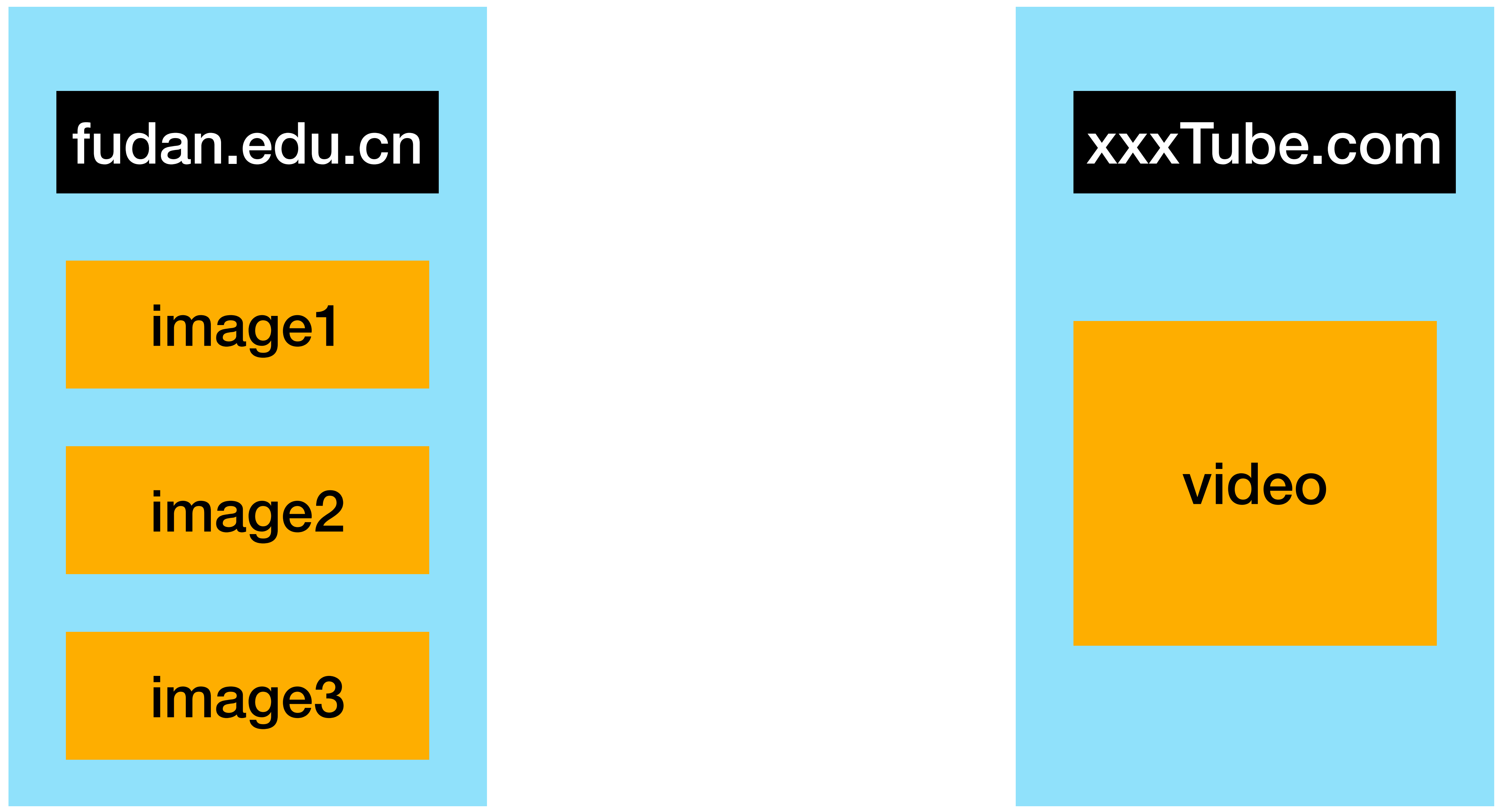


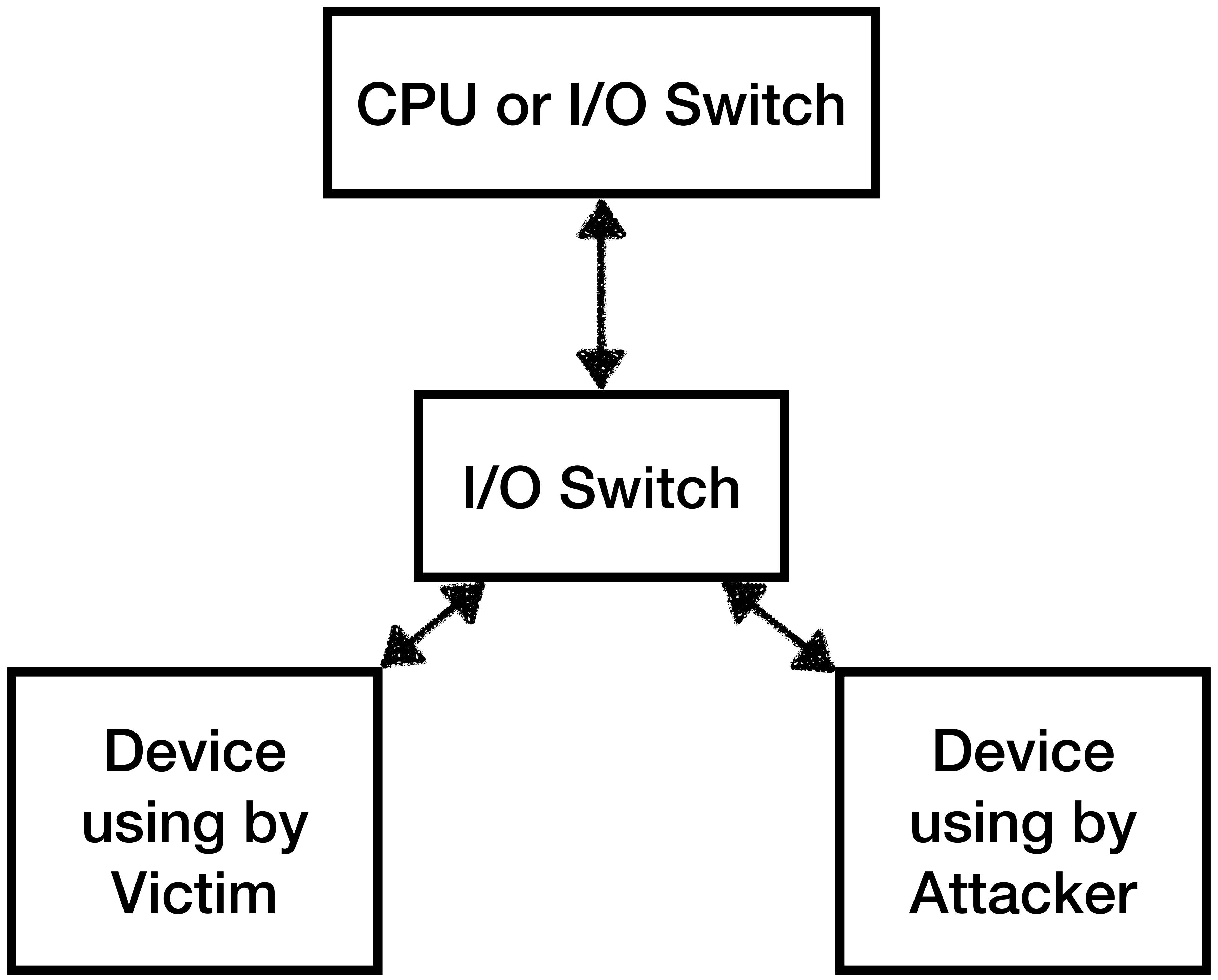
User-input Inference



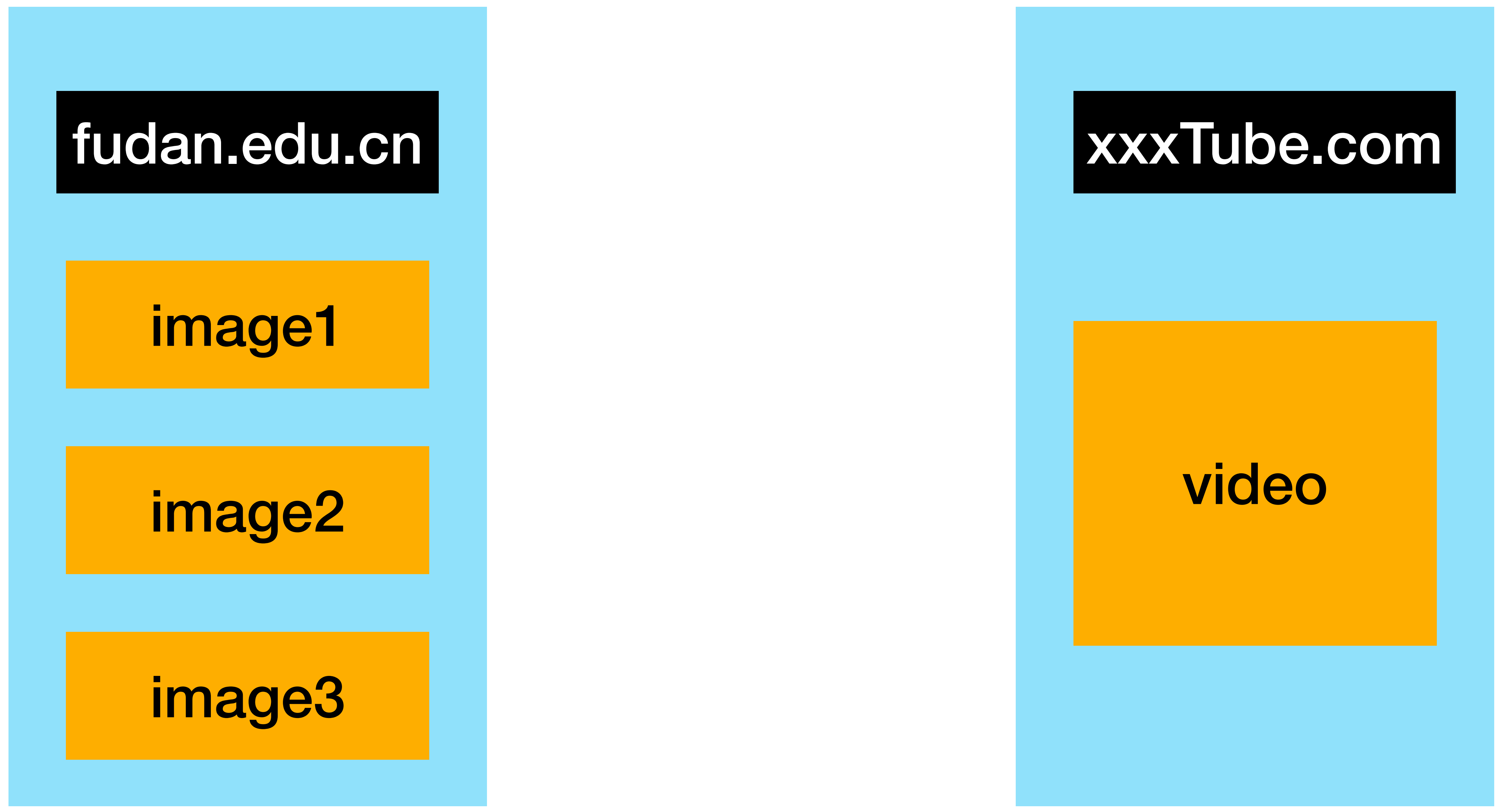


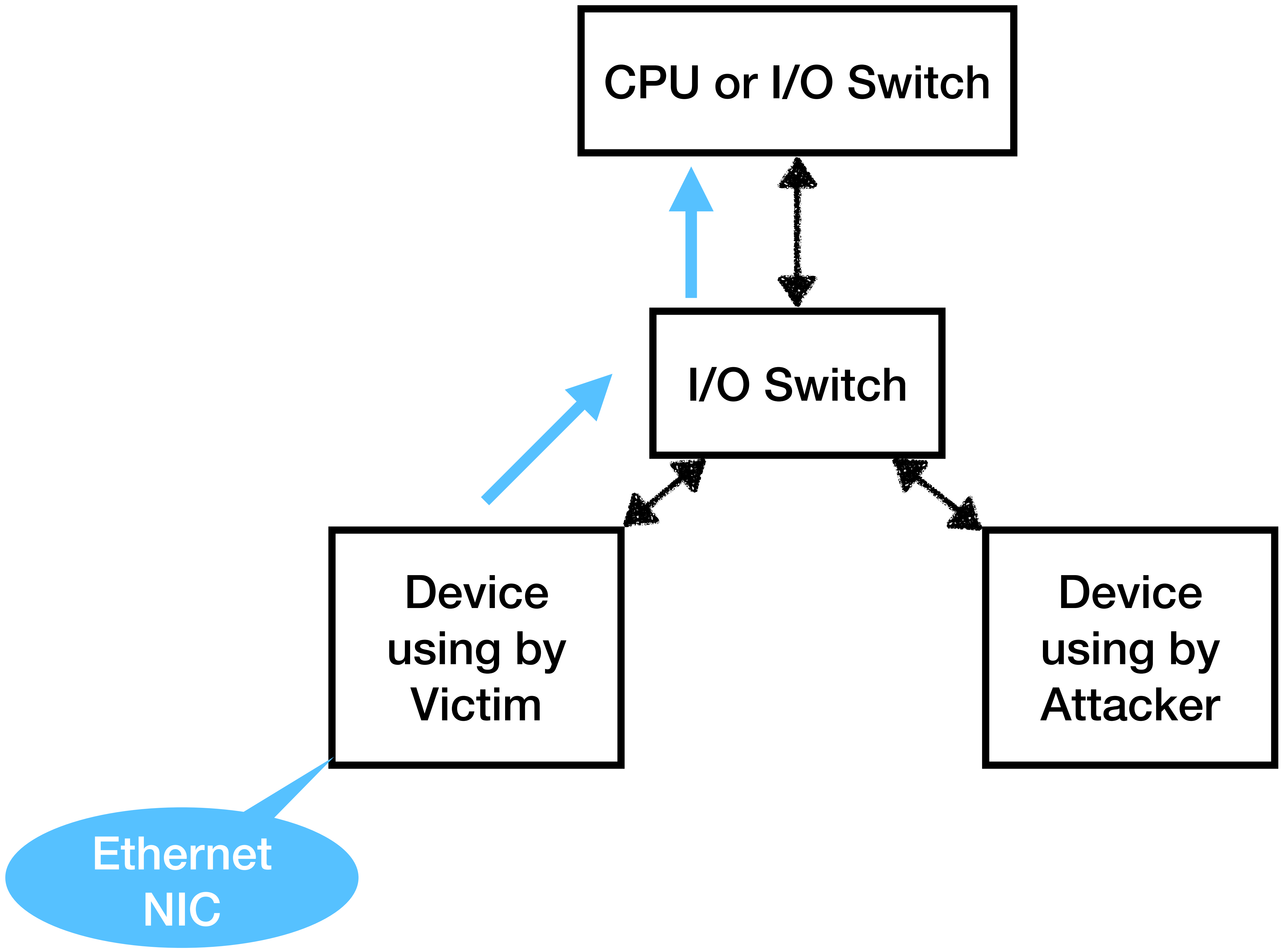
Webpage Inference



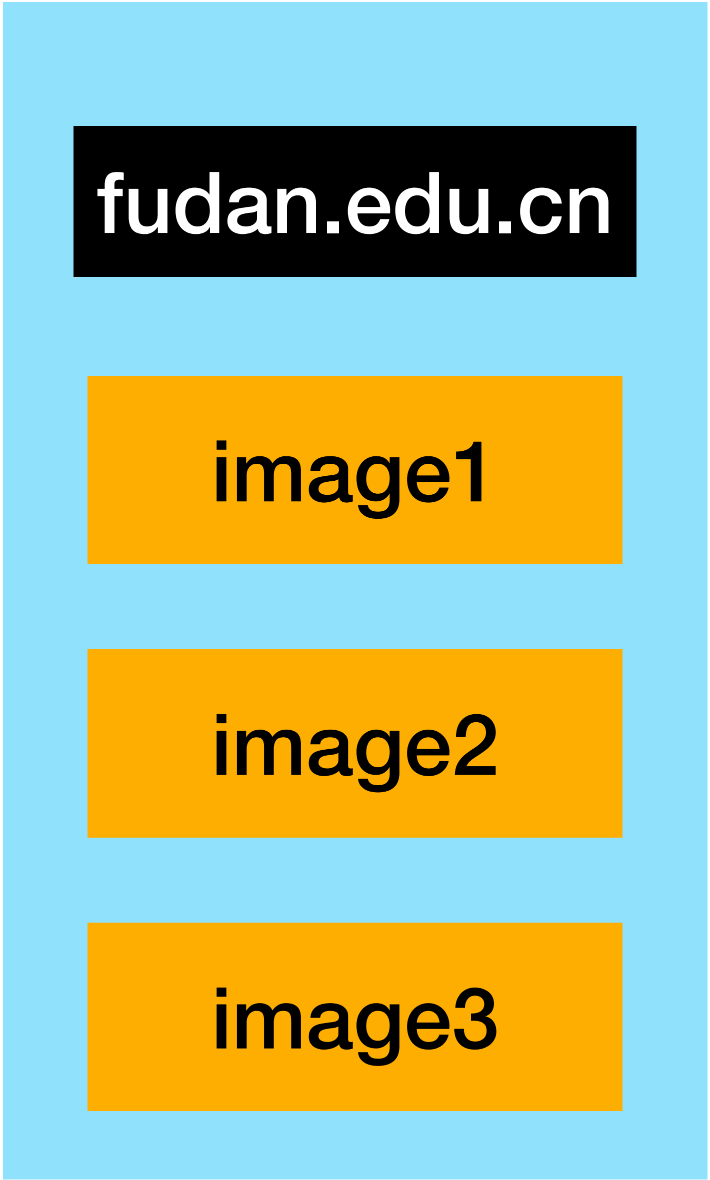


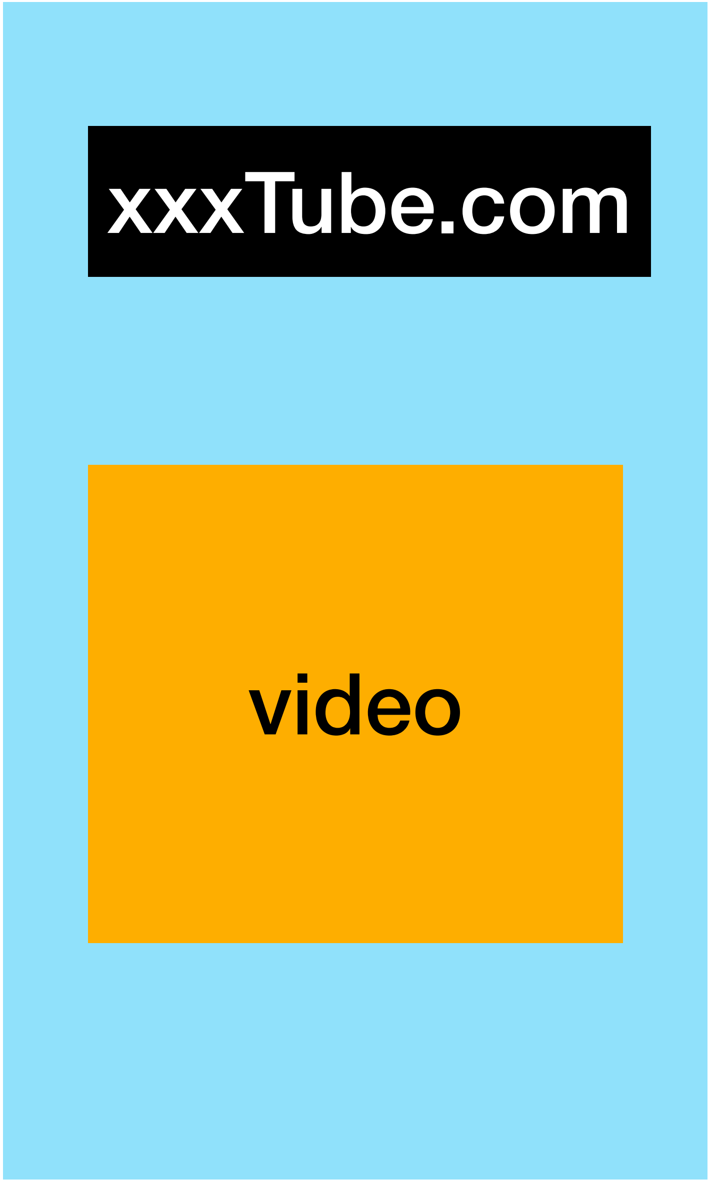
Webpage Inference

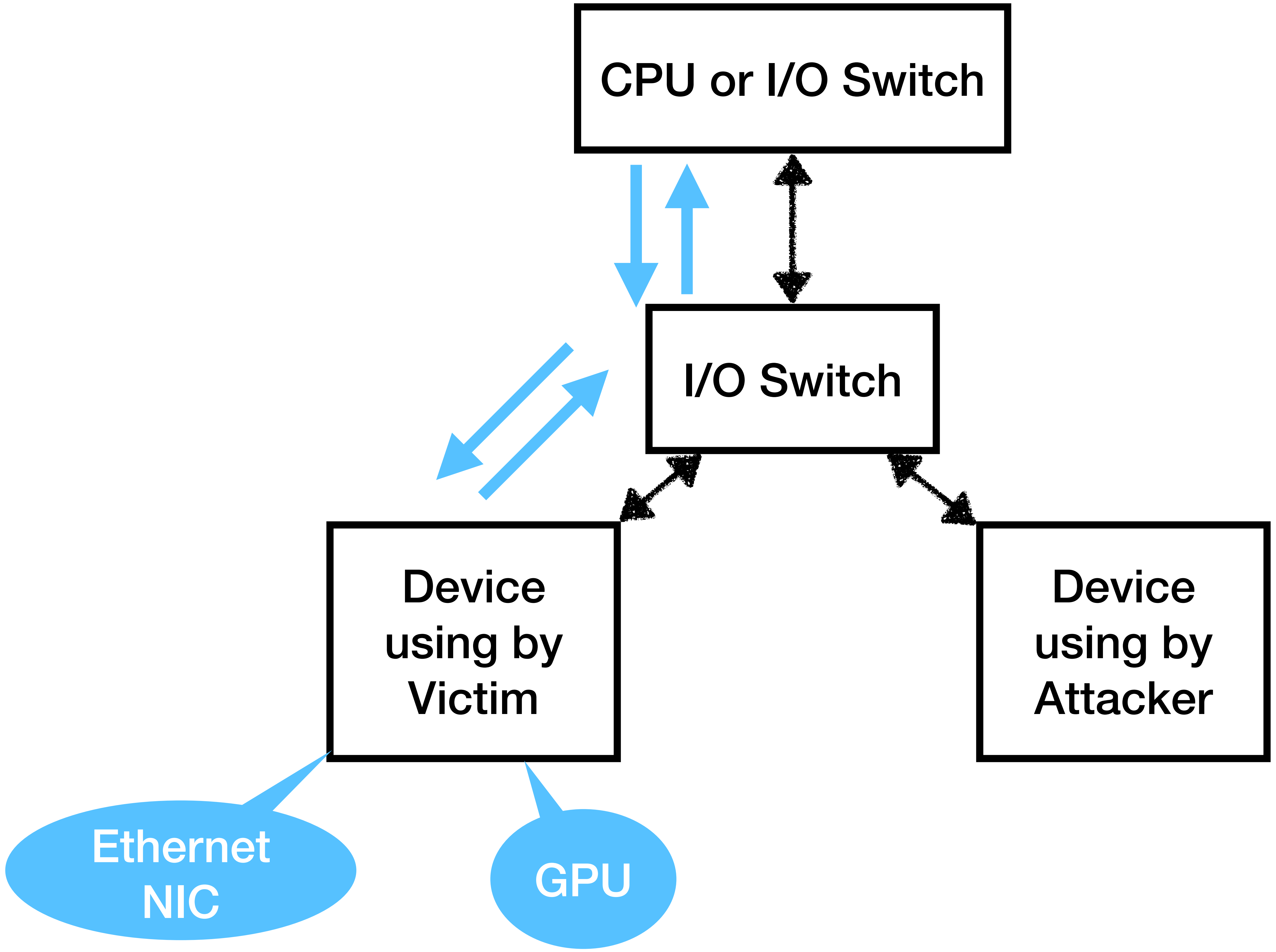




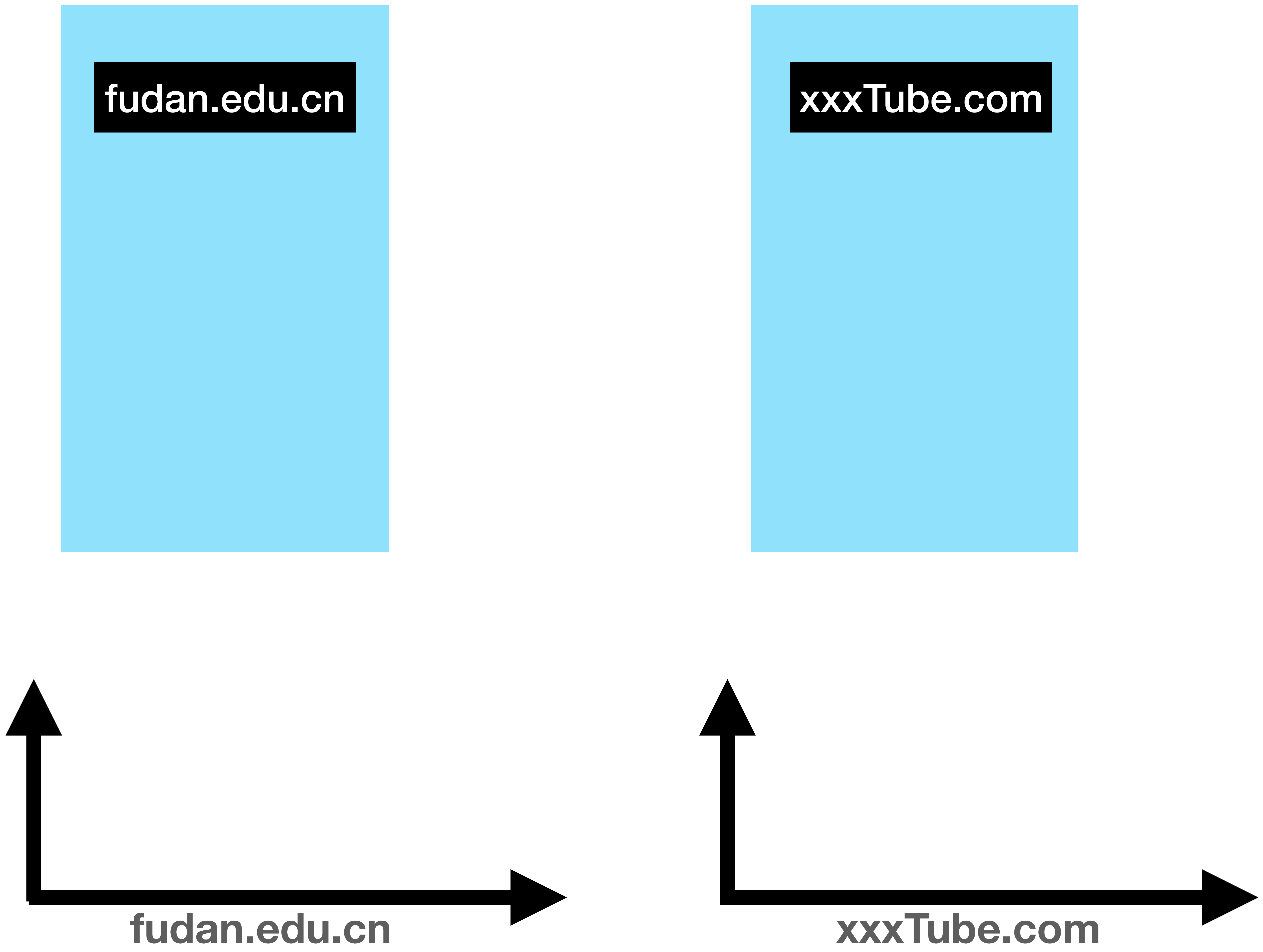
Webpage Inference



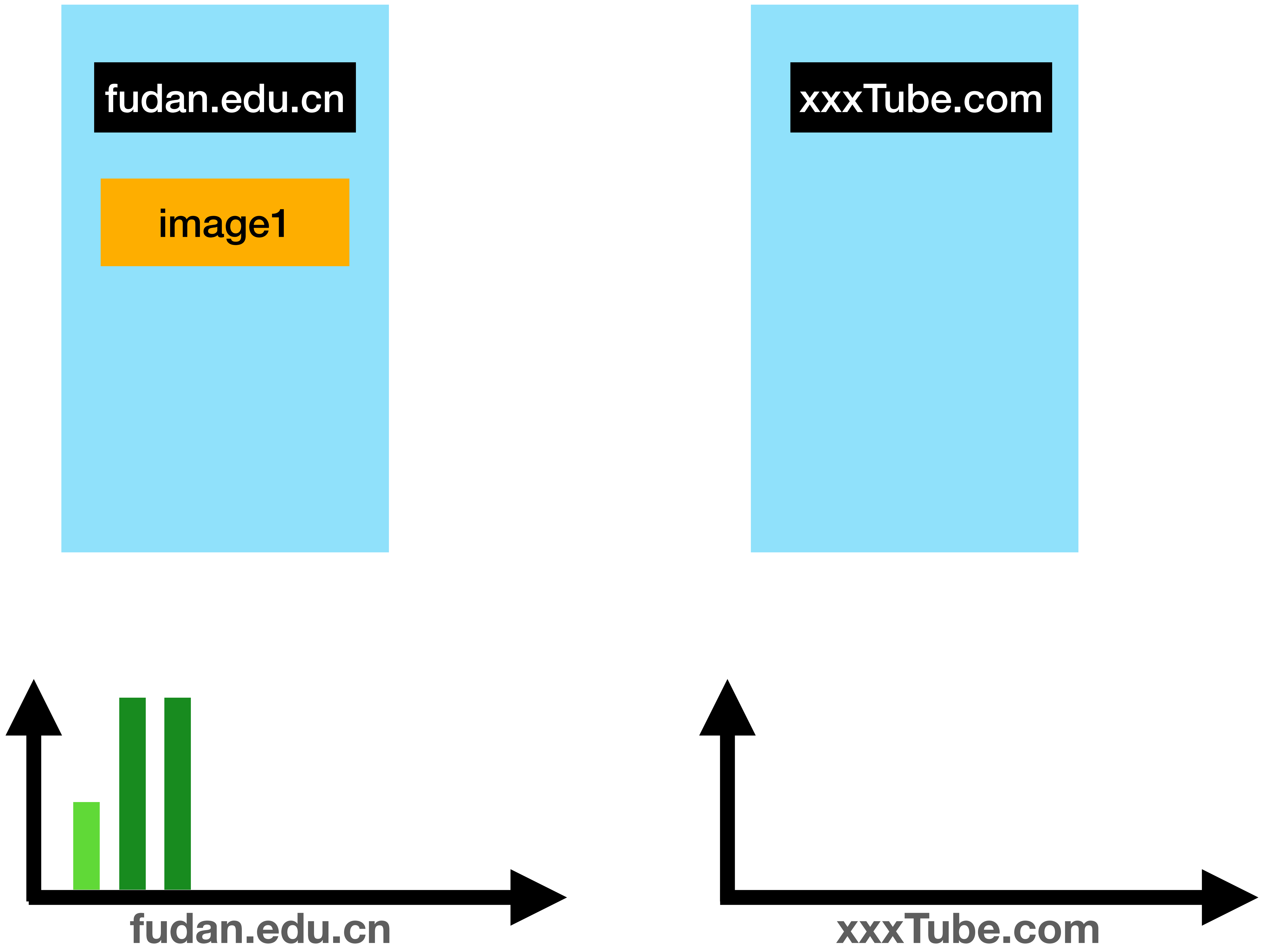




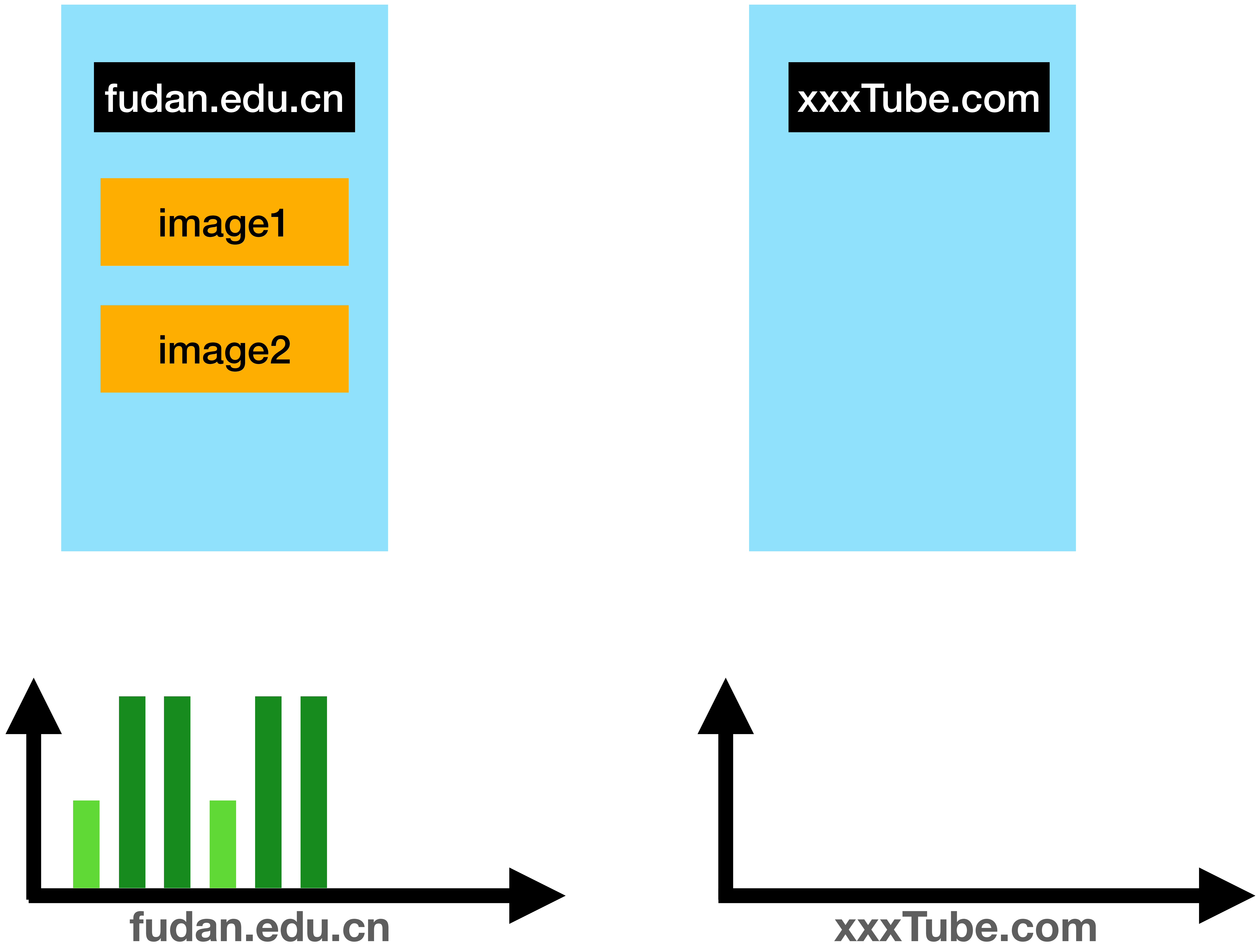
Webpage Inference



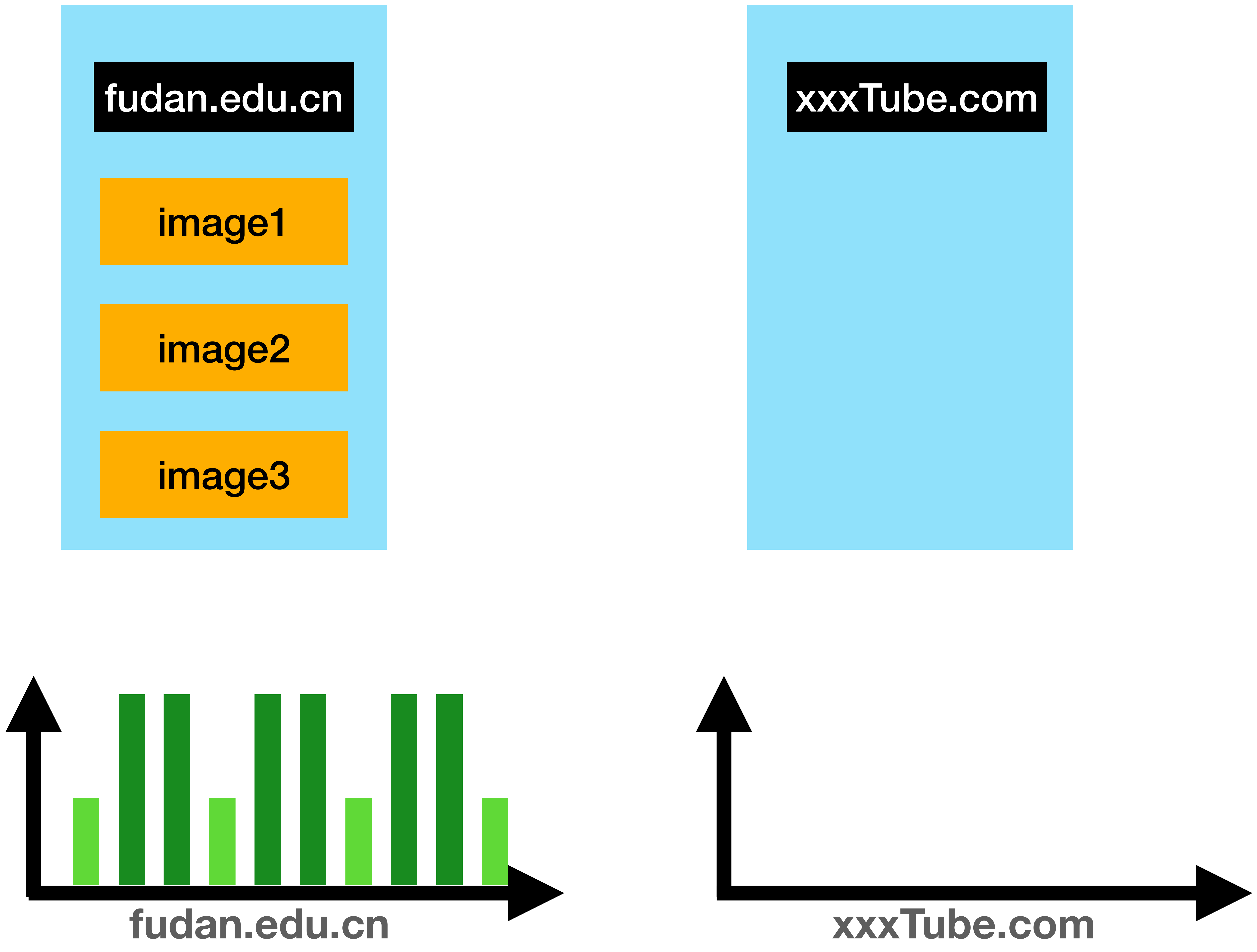
Webpage Inference



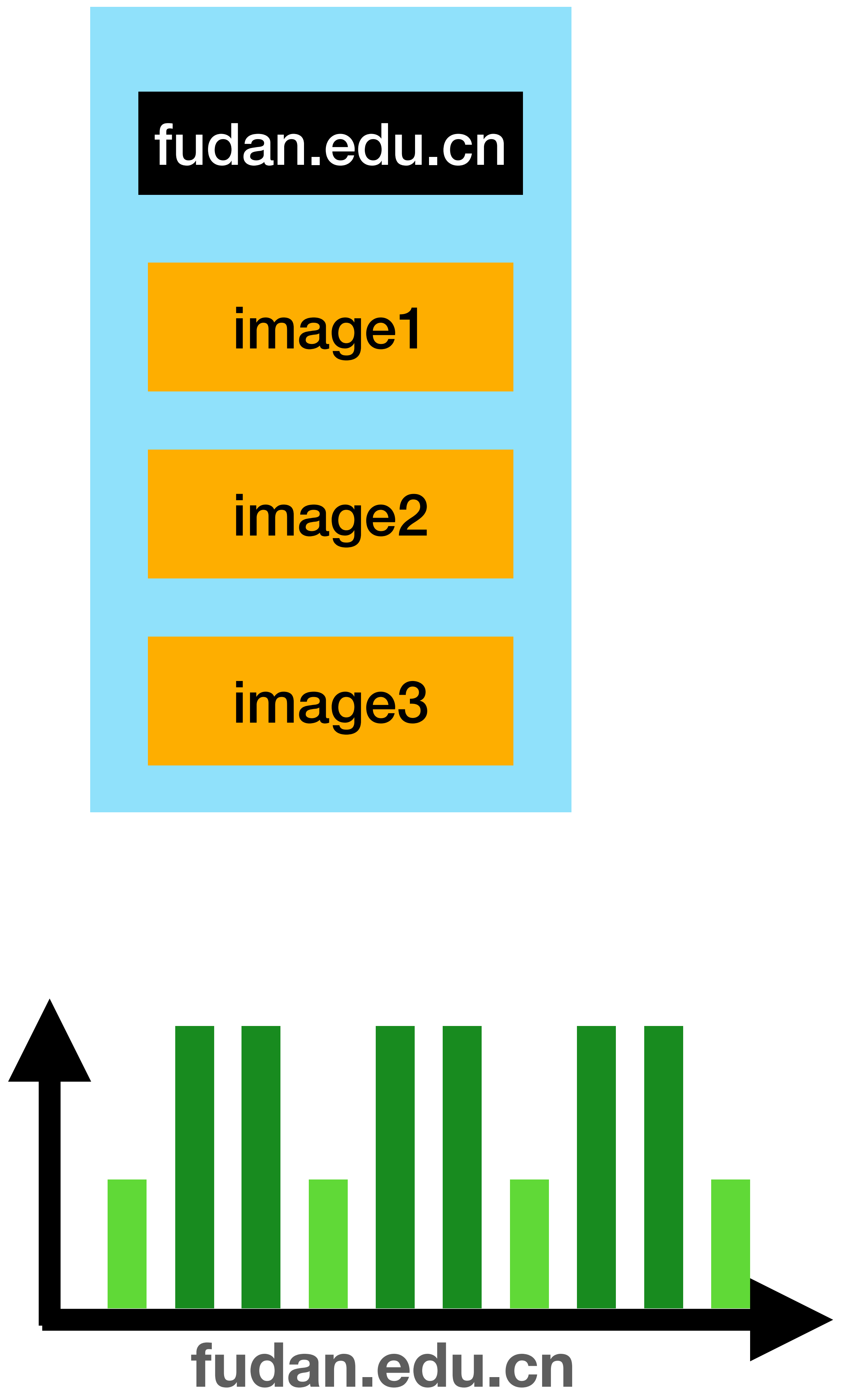
Webpage Inference

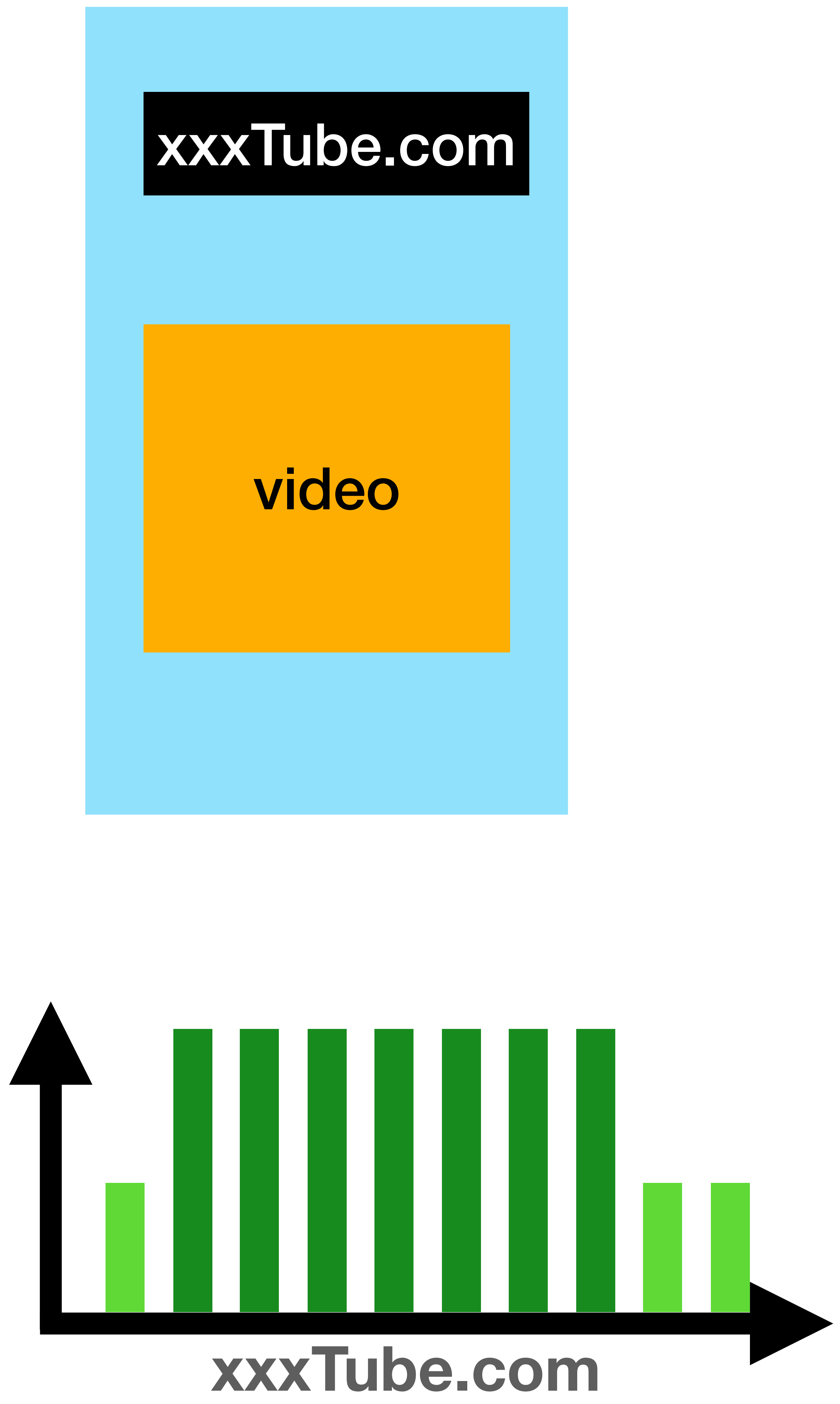


Webpage Inference

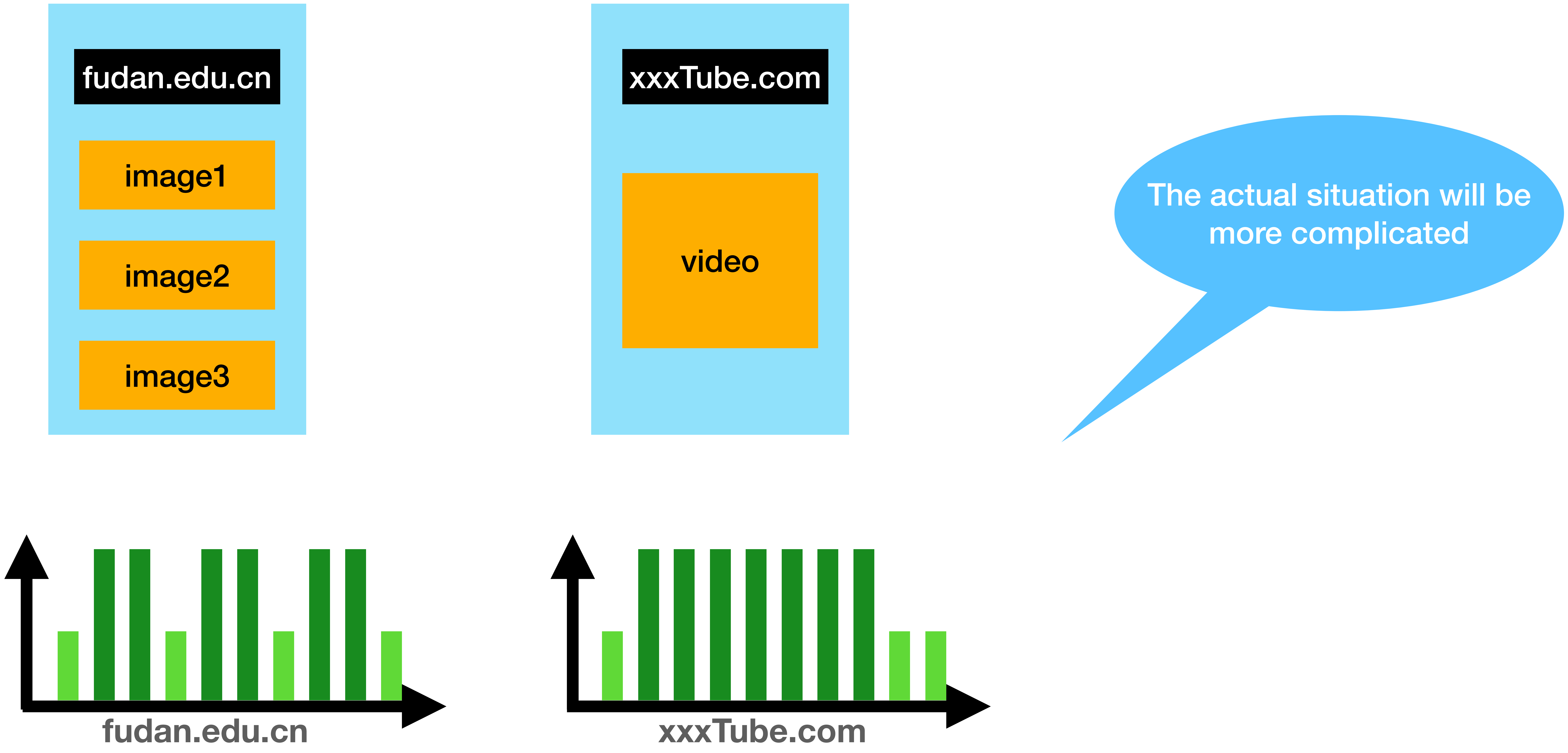


Webpage Inference

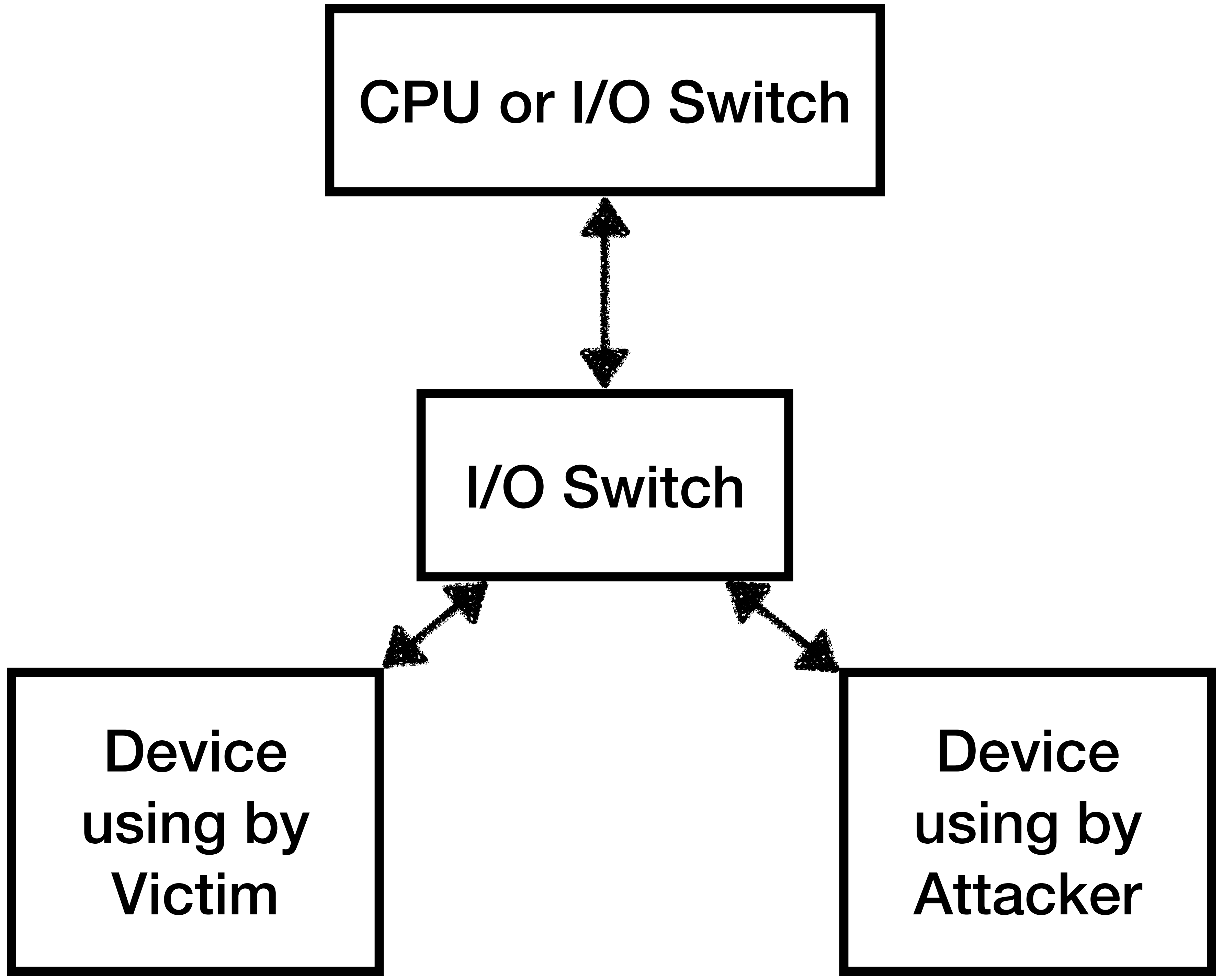




Webpage Inference

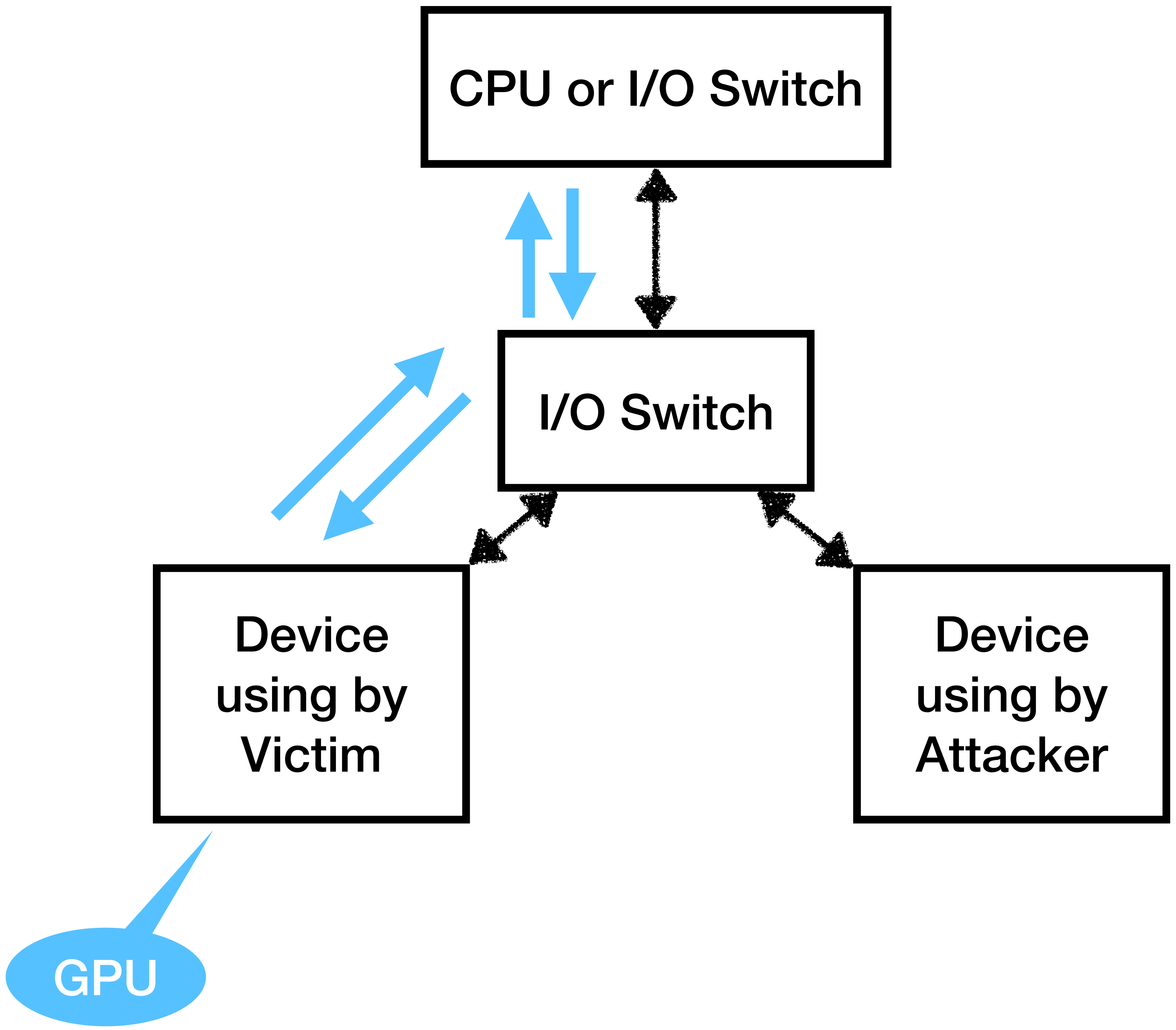


Machine-learning Model Inference



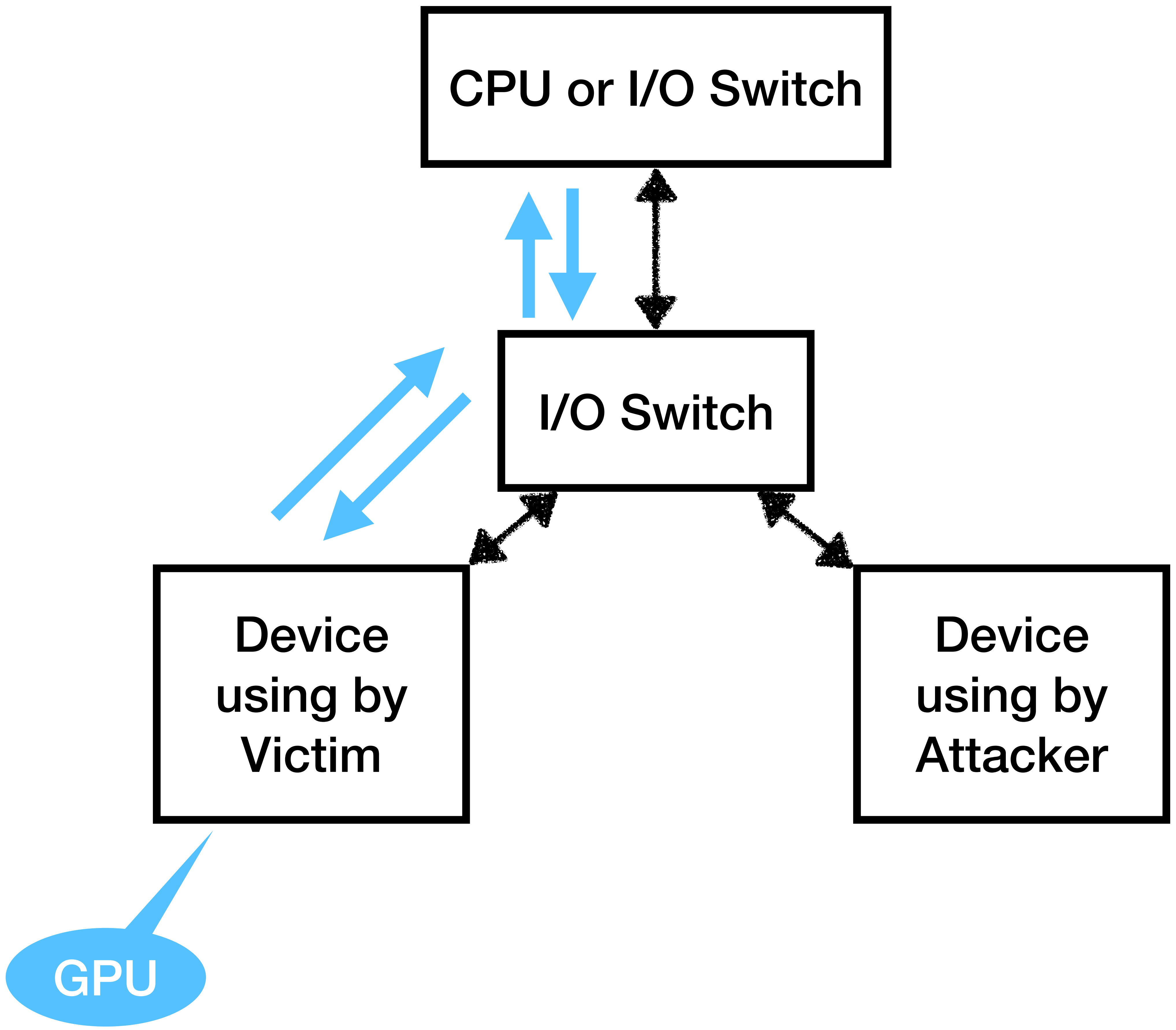
Machine-learning Model Inference

- Data transferred in and out of the GPU



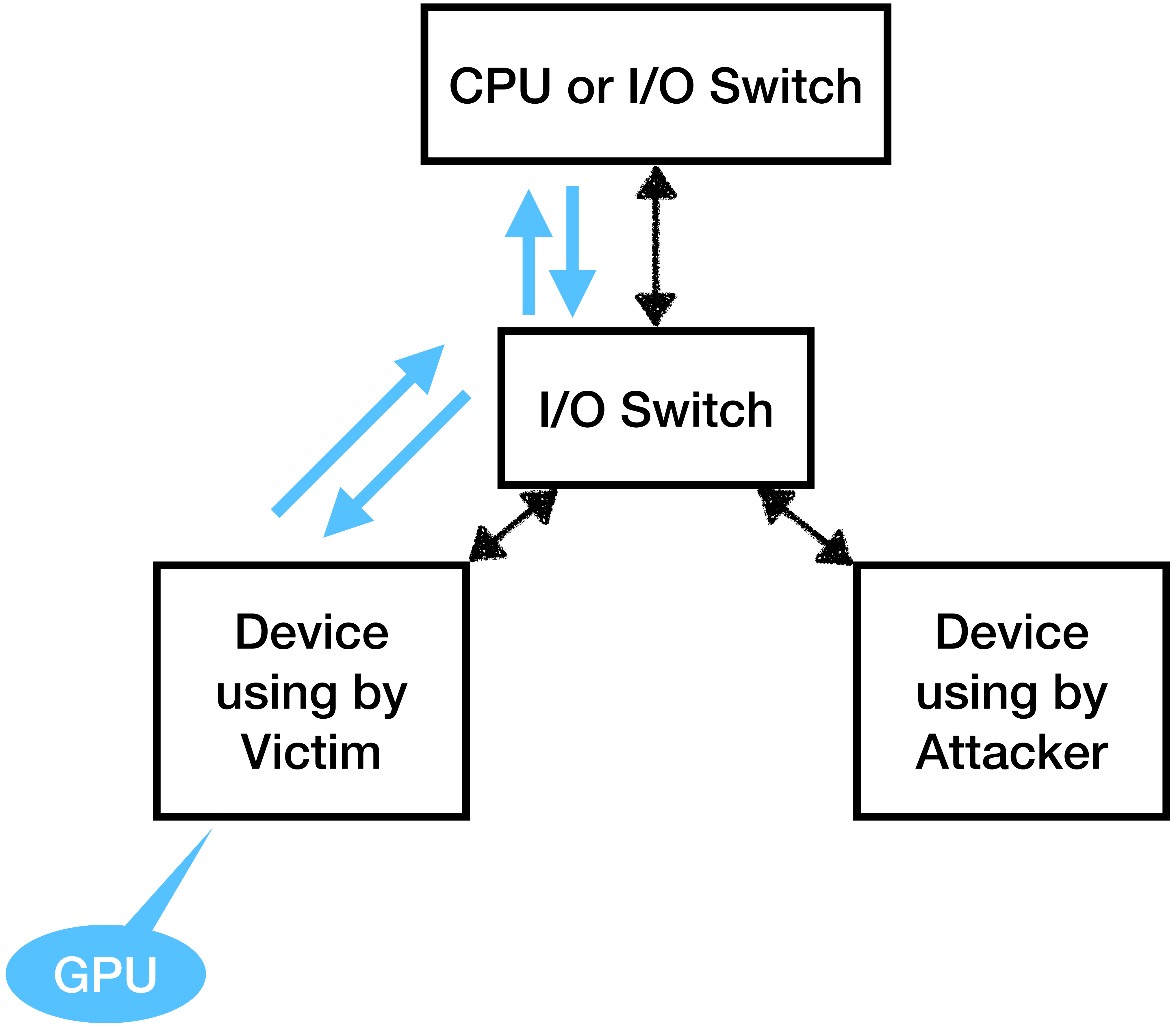
Machine-learning Model Inference

- Data transferred in and out of the GPU
- Different layers transfer different size of data at different frequency



Machine-learning Model Inference

- Data transferred in and out of the GPU
- Different layers transfer different size of data at different frequency
- Delay sequences of models significantly different



Experiments and results

Experiments and results

- User-input Inference
  - Extract keystrokes from delay sequences
  - Accuracy: above 94% without the caret removal
  - Use HMM(Hidden Markov Model) to recover the password [1]

Experiments and results

- User-input Inference
  - Extract keystrokes from delay sequences
  - Accuracy: above 94% without the caret removal
  - Use HMM(Hidden Markov Model) to recover the password [1]
- Webpage Inference
  - Probe 100 webpages, collect delay sequence, and train a classifer (AttBLSTM[2])
  - Accuracy: above 96% in S1, above 93% in S2

Experiments and results

- User-input Inference
  - Extract keystrokes from delay sequences
  - Accuracy: above 94% without the caret removal
  - Use HMM(Hidden Markov Model) to recover the password [1]
- Webpage Inference
  - Probe 100 webpages, collect delay sequence, and train a classifer (AttBLSTM[2])
  - Accuracy: above 96% in S1, above 93% in S2
- Machine-learning Model Inference
  - Probe 10 machine-learning models, collect delay sequence, and train the same classifer
  - All the models are correctly classified

Potential Mitigation

Potential Mitigation

- Blocking high-resolution clock instructions (e.g. RDTSCP)

Potential Mitigation

- Blocking high-resolution clock instructions (e.g. RDTSCP)
- Detecting suspicious probe requests

Potential Mitigation

- Blocking high-resolution clock instructions (e.g. RDTSCP)
- Detecting suspicious probe requests
- I/O bandwidth allocation

Conclusion

Conclusion

- Found a new side-channel attack Based on PCIe congestion

Conclusion

- Found a new side-channel attack Based on PCIe congestion
- Develop two attack strategies:
  - using RDMA NIC to attack GPU
  - using NVMe SSD to attack Ethernet NIC

Conclusion

- Found a new side-channel attack Based on PCIe congestion
- Develop two attack strategies:
  - using RDMA NIC to attack GPU
  - using NVMe SSD to attack Ethernet NIC
- Evaluate them under three tasks:
  - keystroke typing
  - webpage browsing
  - training machine-learning model

Thank you for listening!

Questions?

References

[1] D.X.Song,D.A.Wagner,and X.Tian,“Timing analysis of keystrokes and timing attacks on ssh.” in USENIX Security Symposium, vol. 2001, 2001.

[2] P. Zhou, W. Shi, J. Tian, Z. Qi, B. Li, H. Hao, and B. Xu, “Attention- based bidirectional long short-term memory networks for relation classification,” in Proceedings of the 54th annual meeting of the association for computational linguistics (volume 2: Short papers), 2016, pp. 207–212.

[3] https://hakk.me/windows-secure-boot-process-enumeration-detailed-mechanism-and-overview-a156b57f4f98