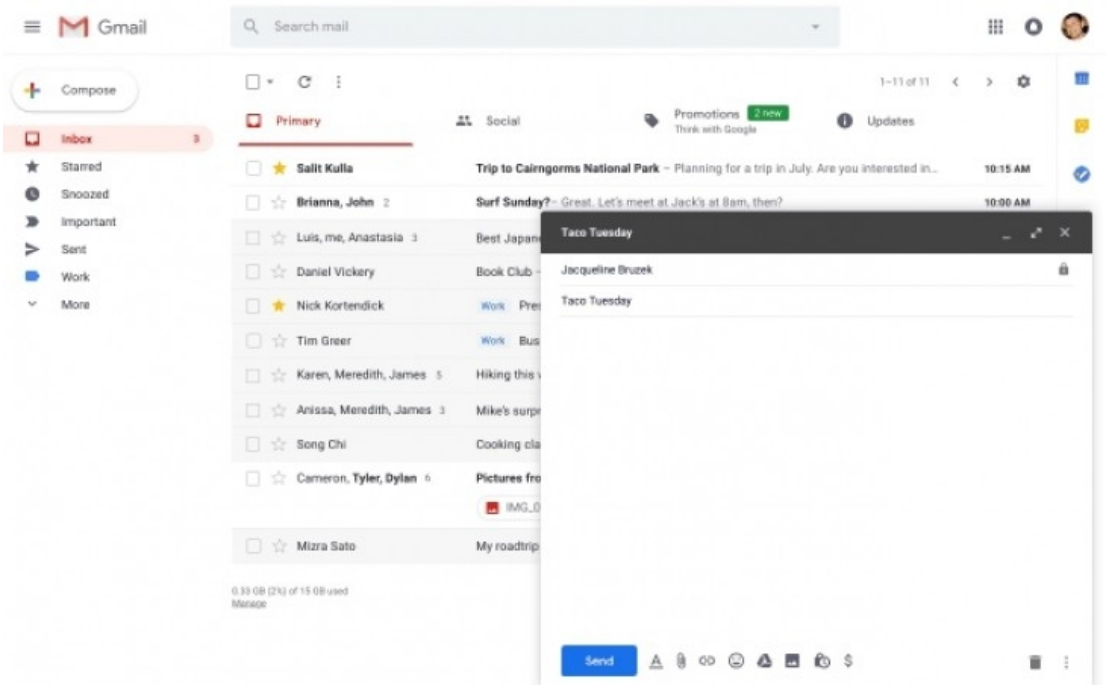
ProtectIOn: Root-of-Trust for IO in Compromised Platforms

A. Dhar, E. Ulqinaku, K. Kostiainen, S. Capkun
ETH Zürich

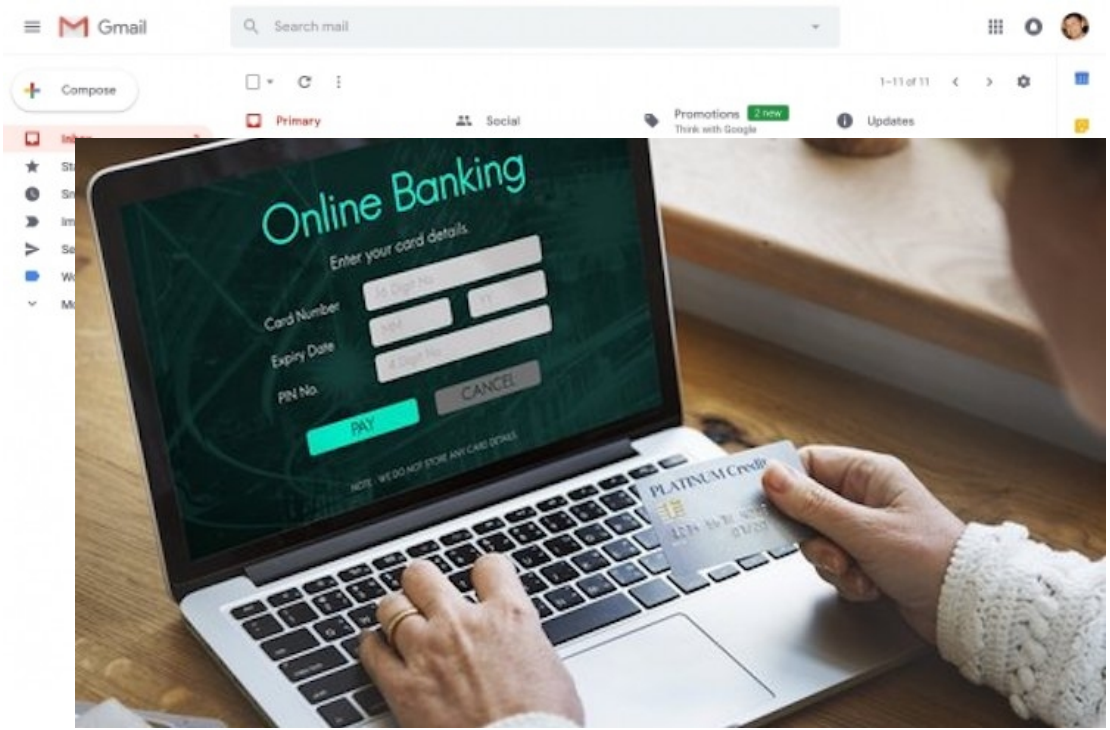
Motivation

- Communication



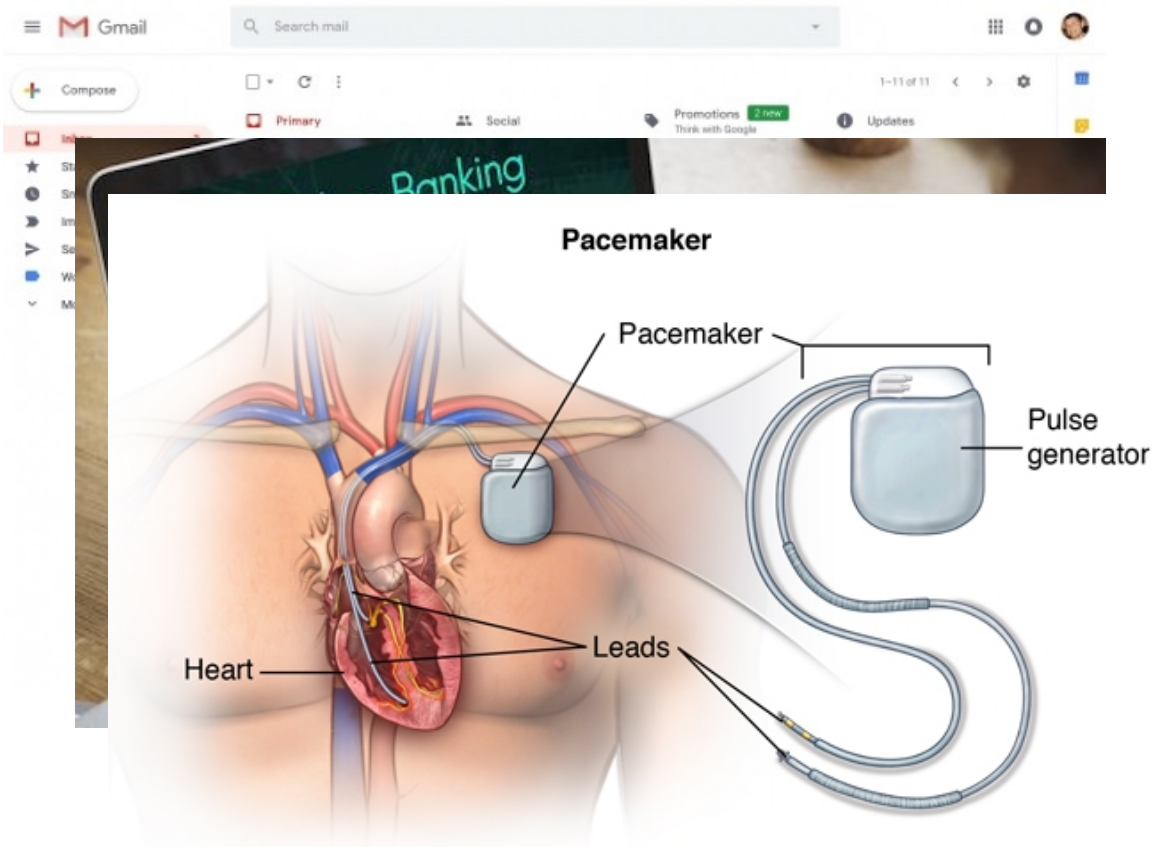
Motivation

- Communication
- Financial Transaction



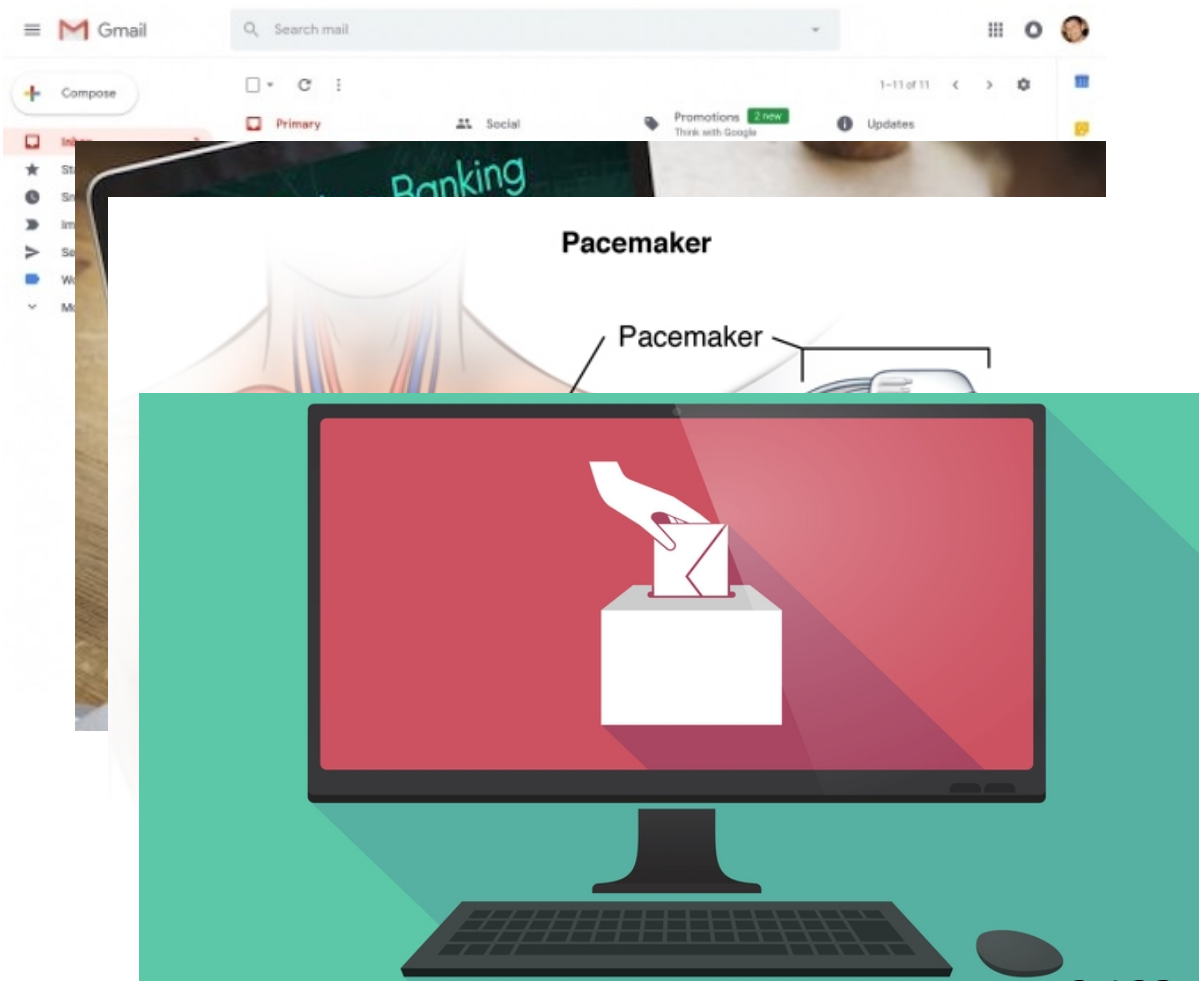
Motivation

- Communication
- Financial Transaction
- Configurations



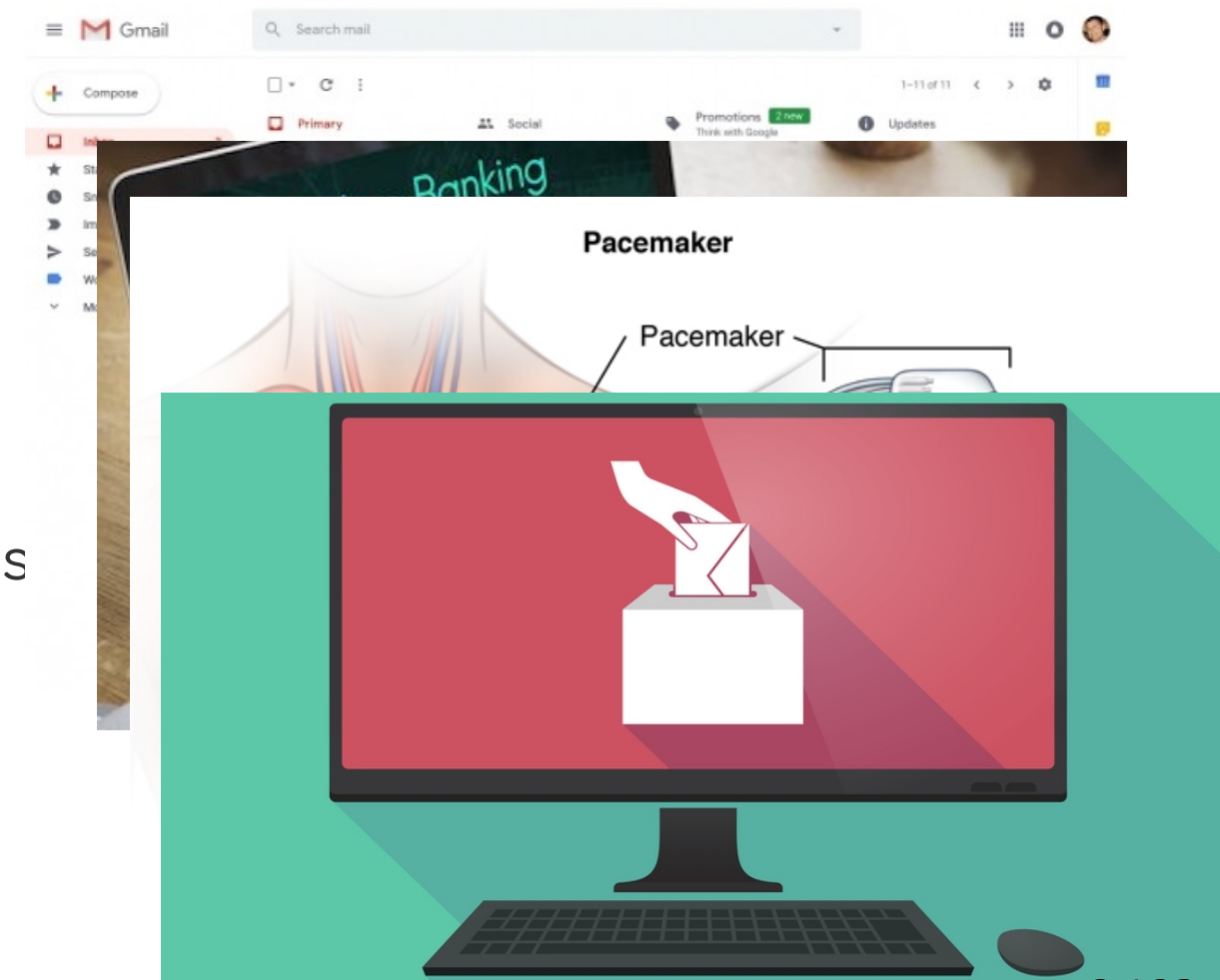
Motivation

- Communication
- Financial Transaction
- Configurations
- Voting

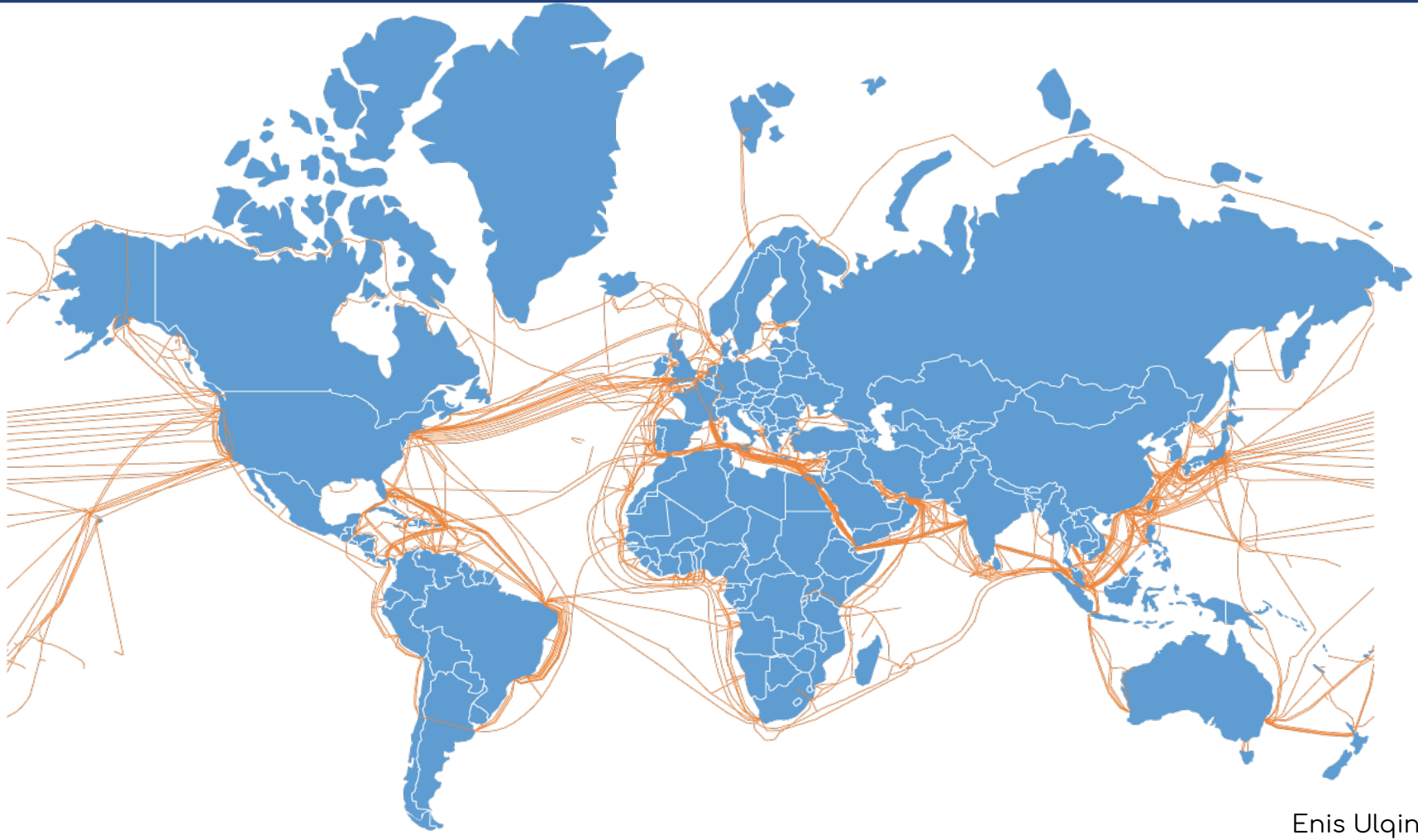


Motivation

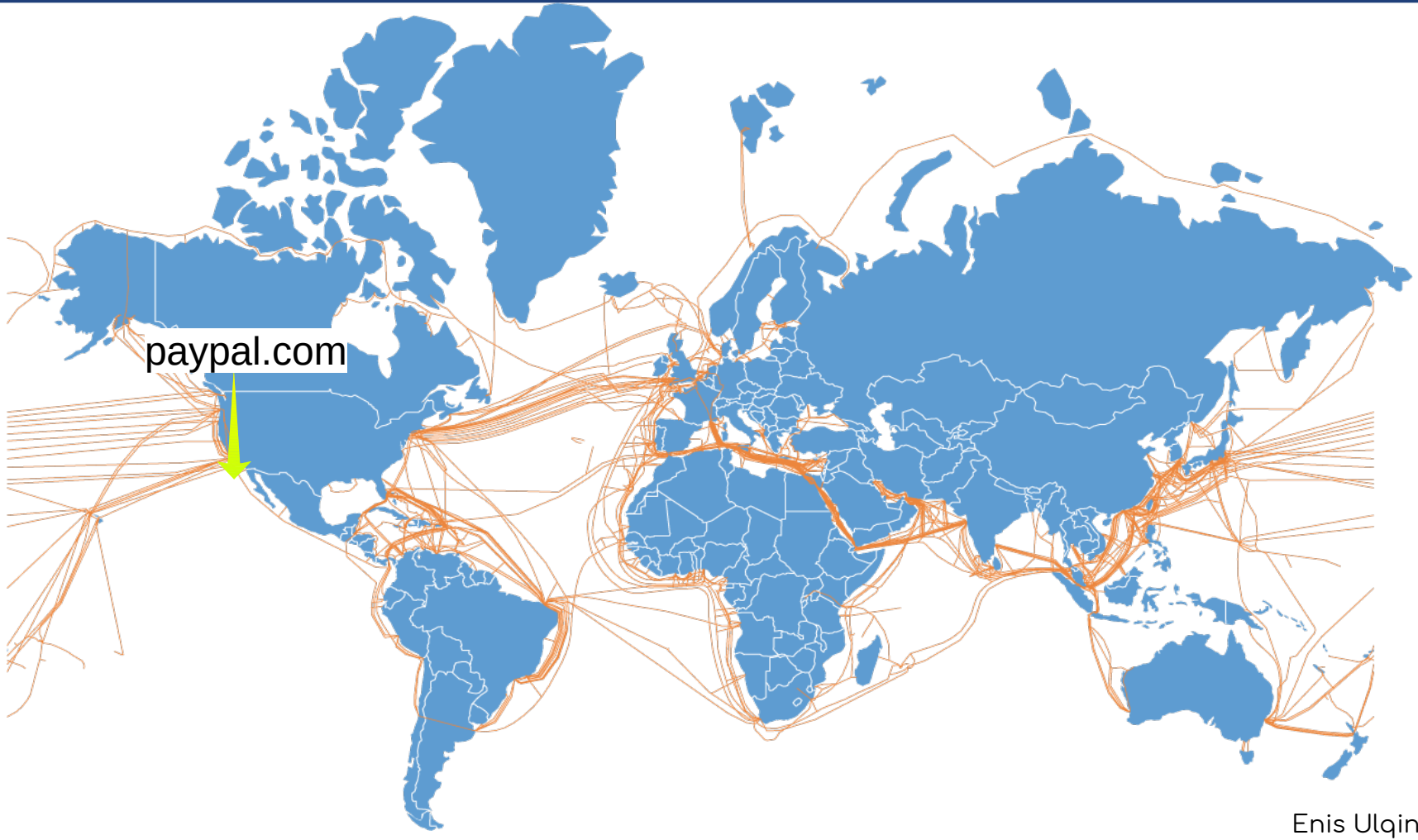
- Communication
- Financial Transaction
- Configurations
- Voting
- Cyber-Physical Systems
- ...



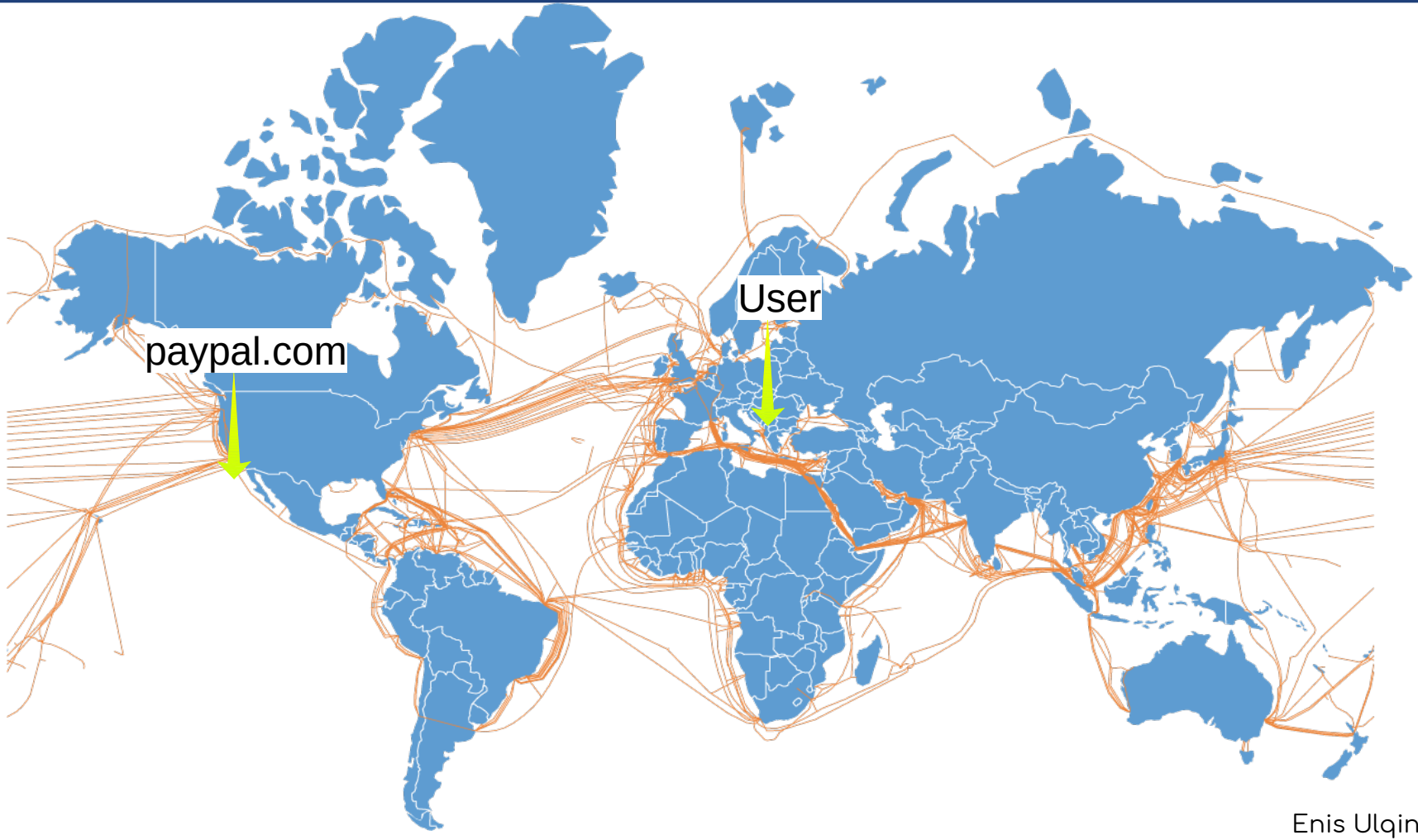
Connection Overview



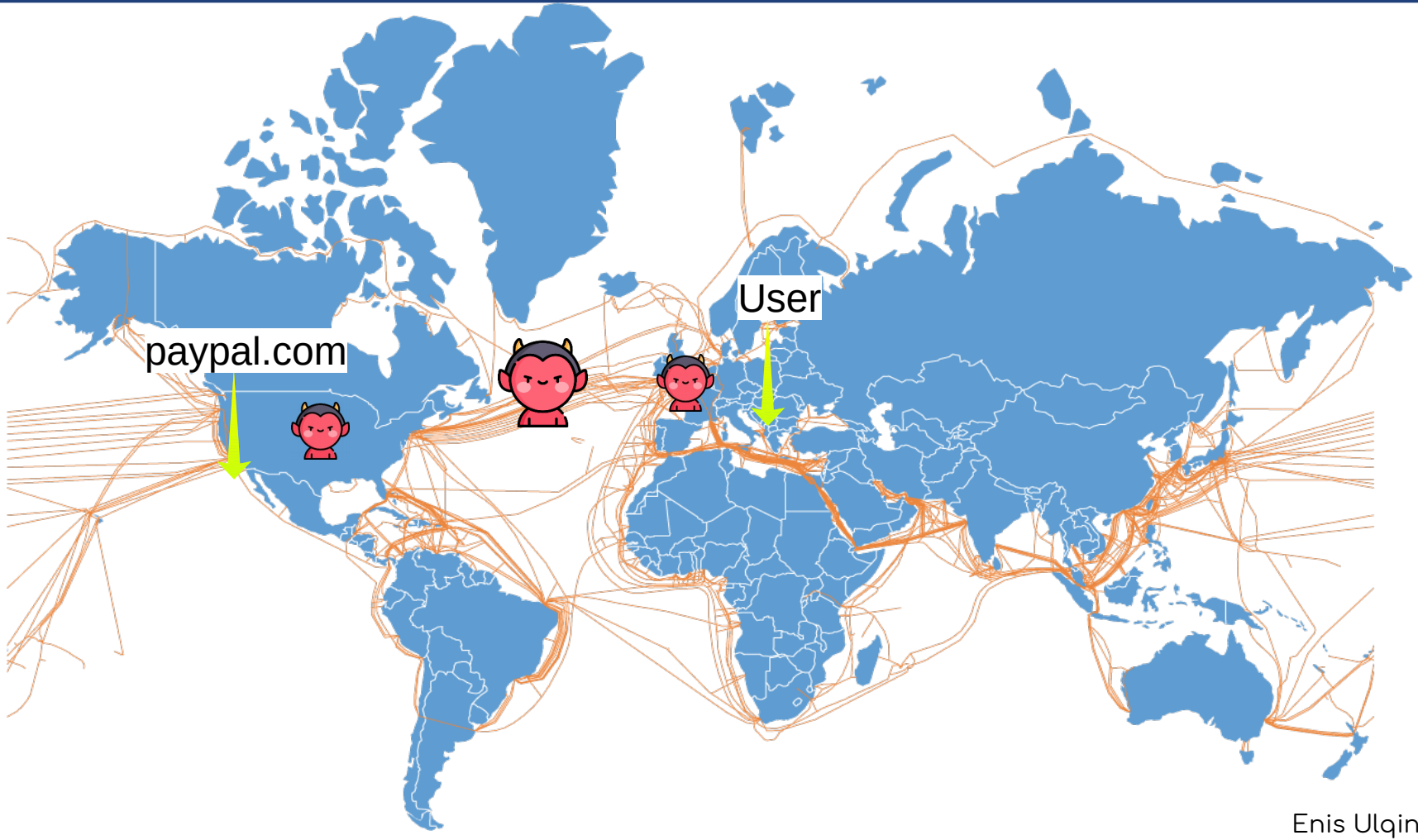
Connection Overview



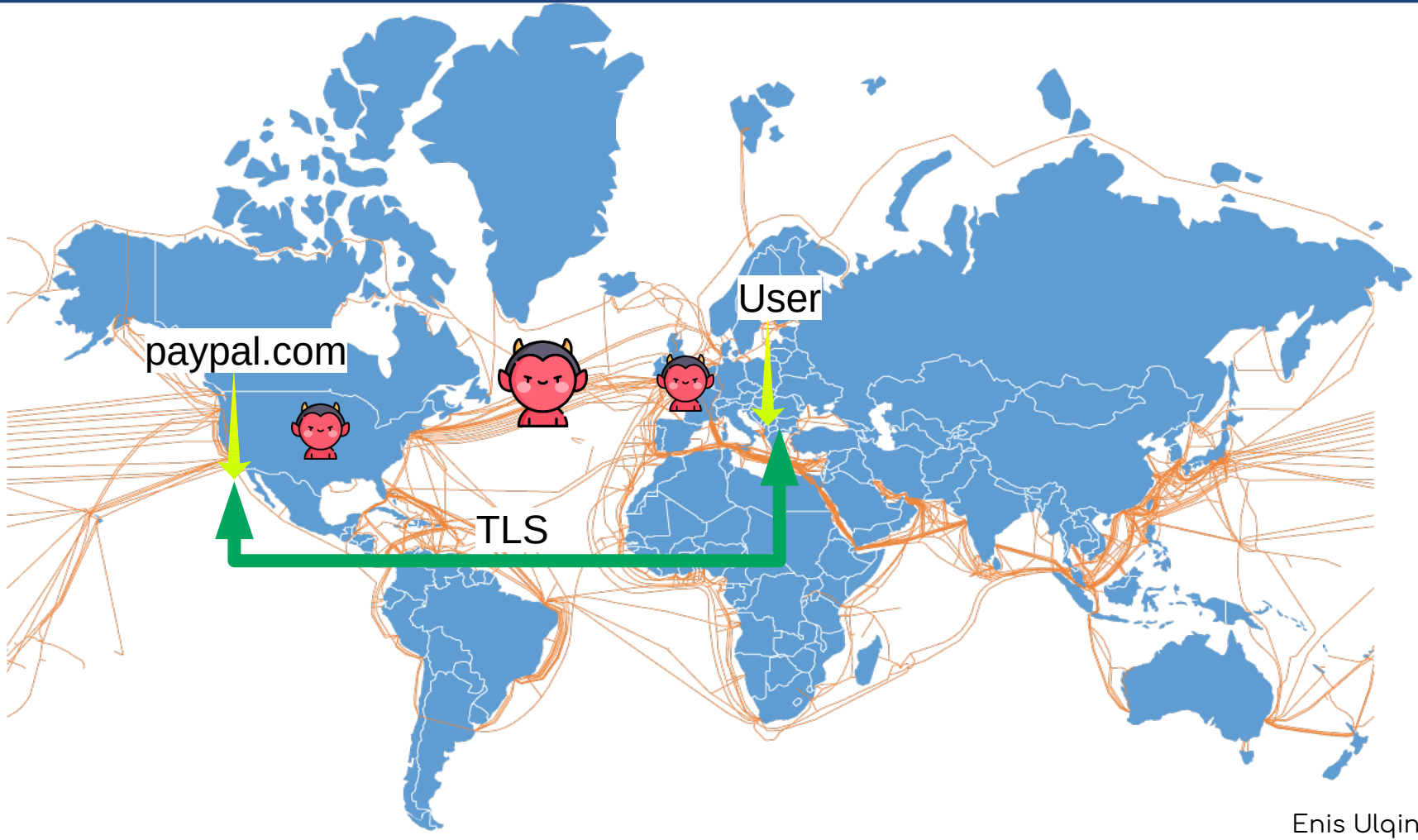
Connection Overview



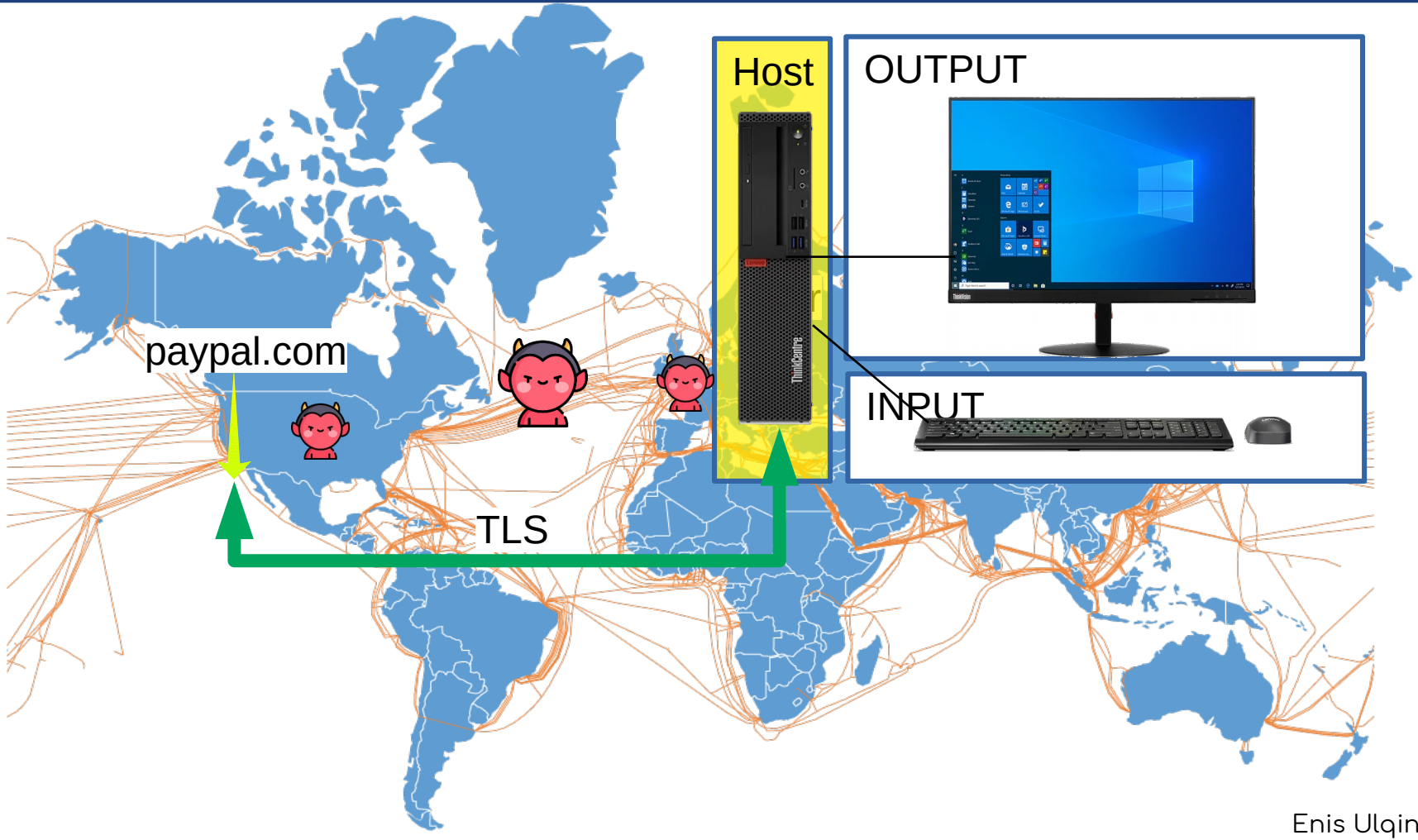
Connection Overview



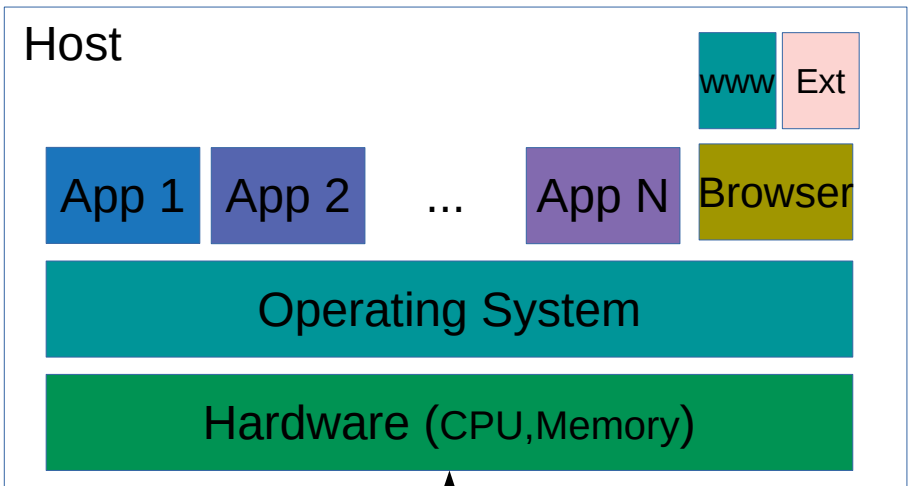
Connection Overview



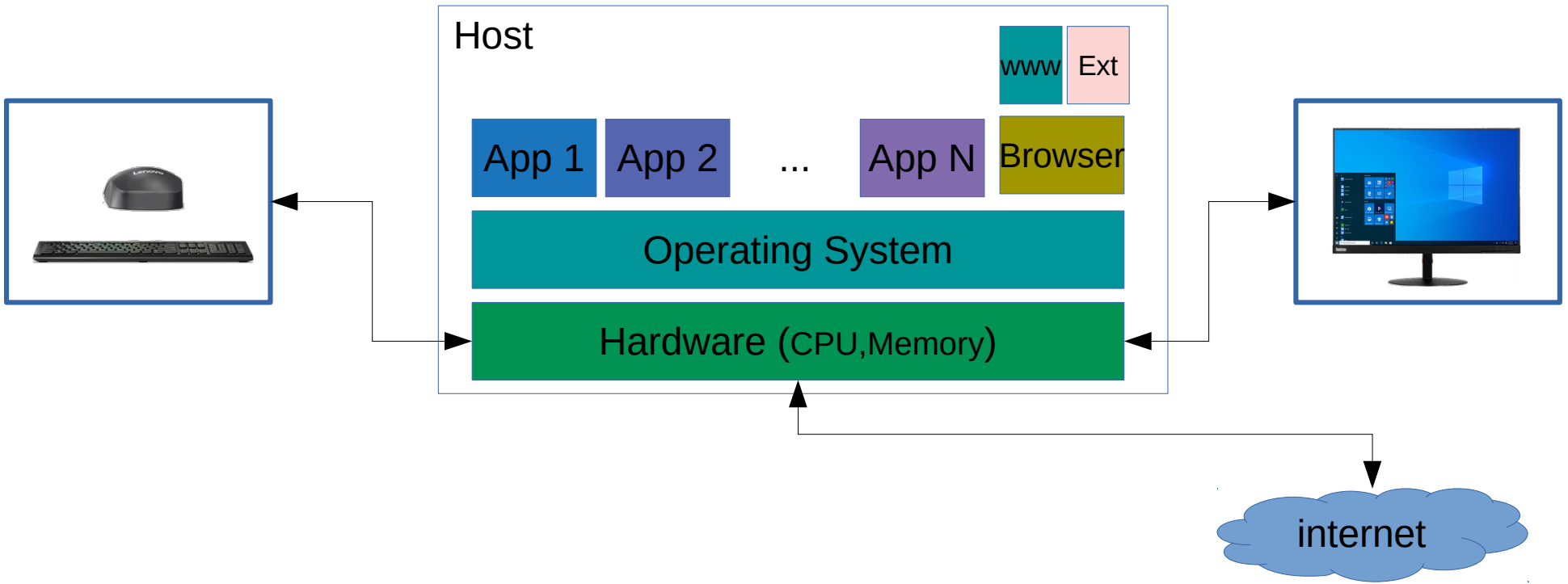
Connection Overview



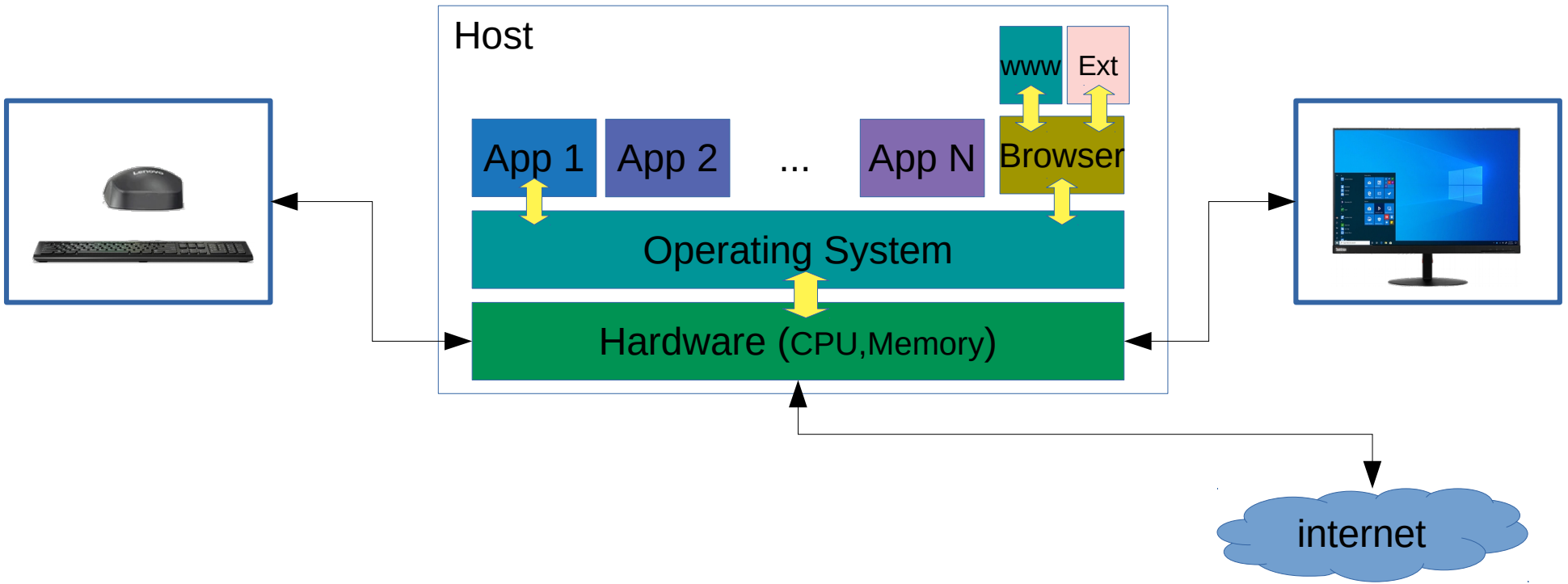
How secure are computers?



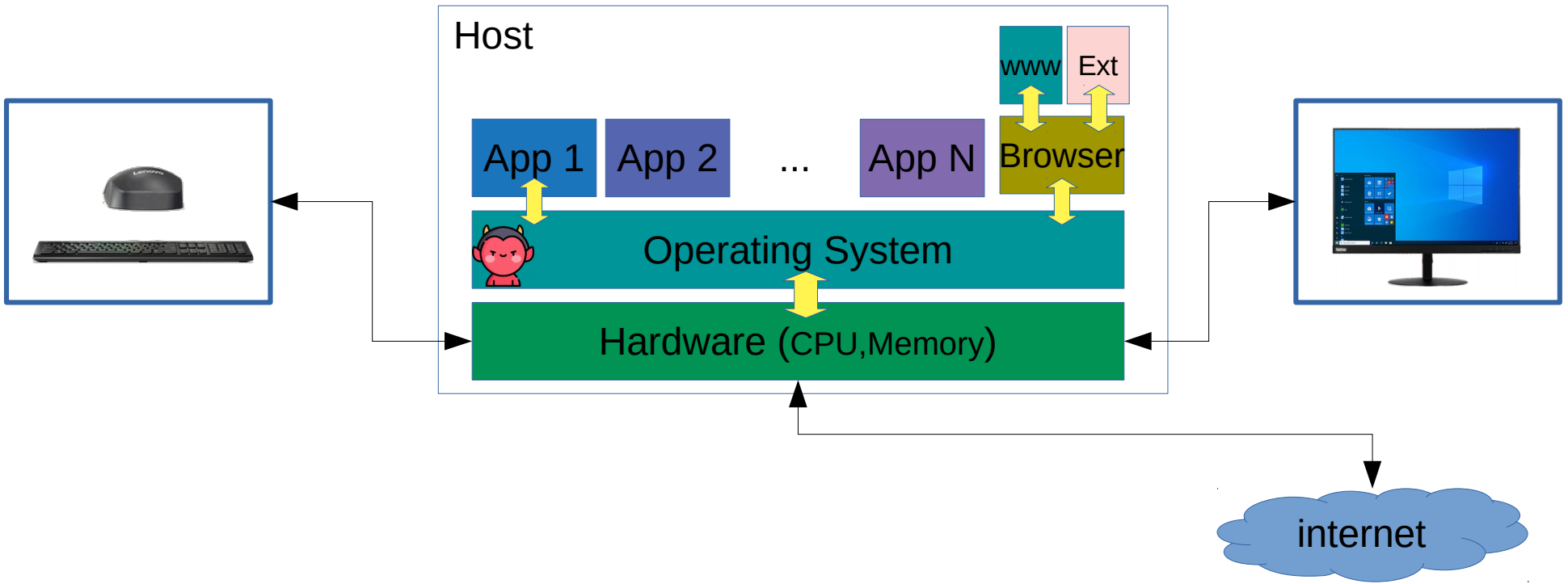
How secure are computers?



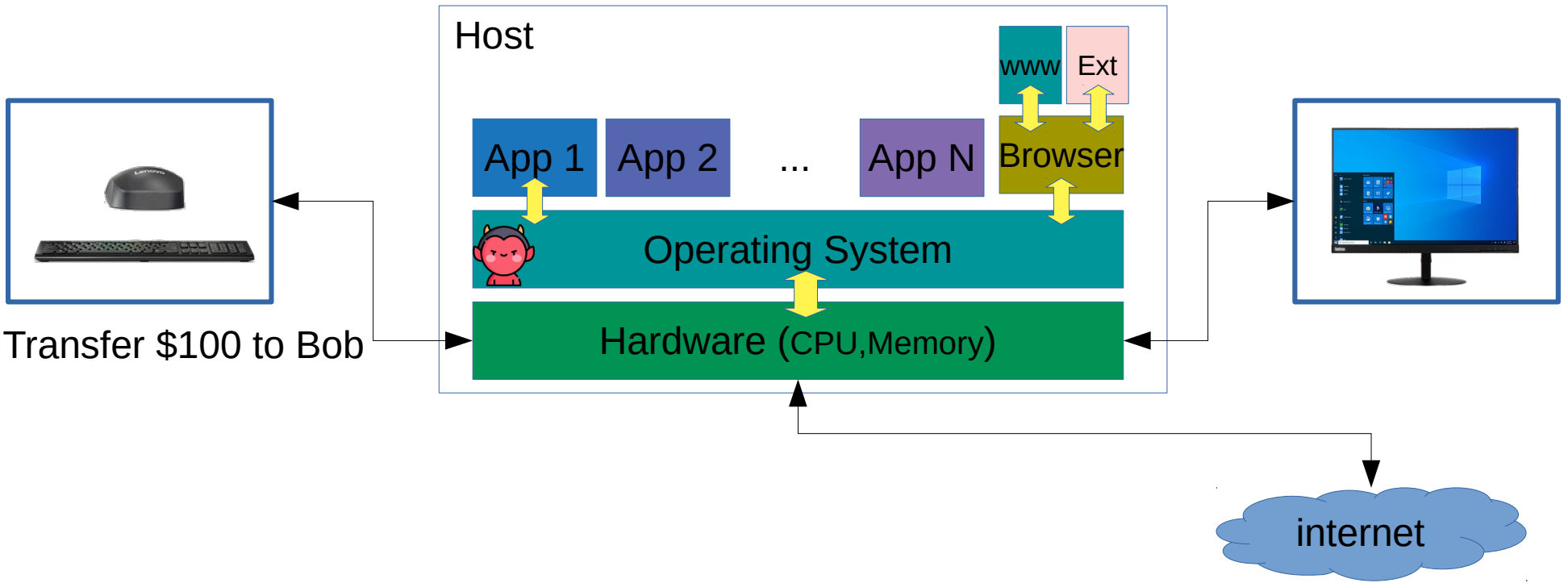
How secure are computers?



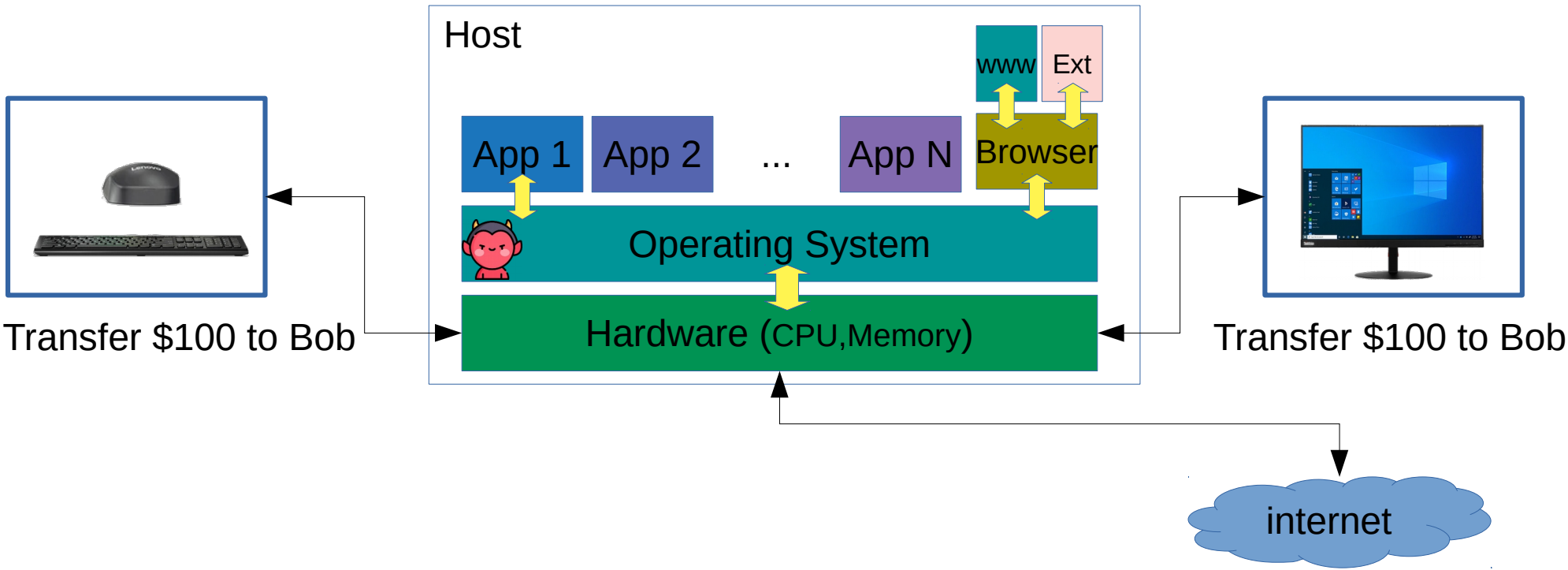
How secure are computers?



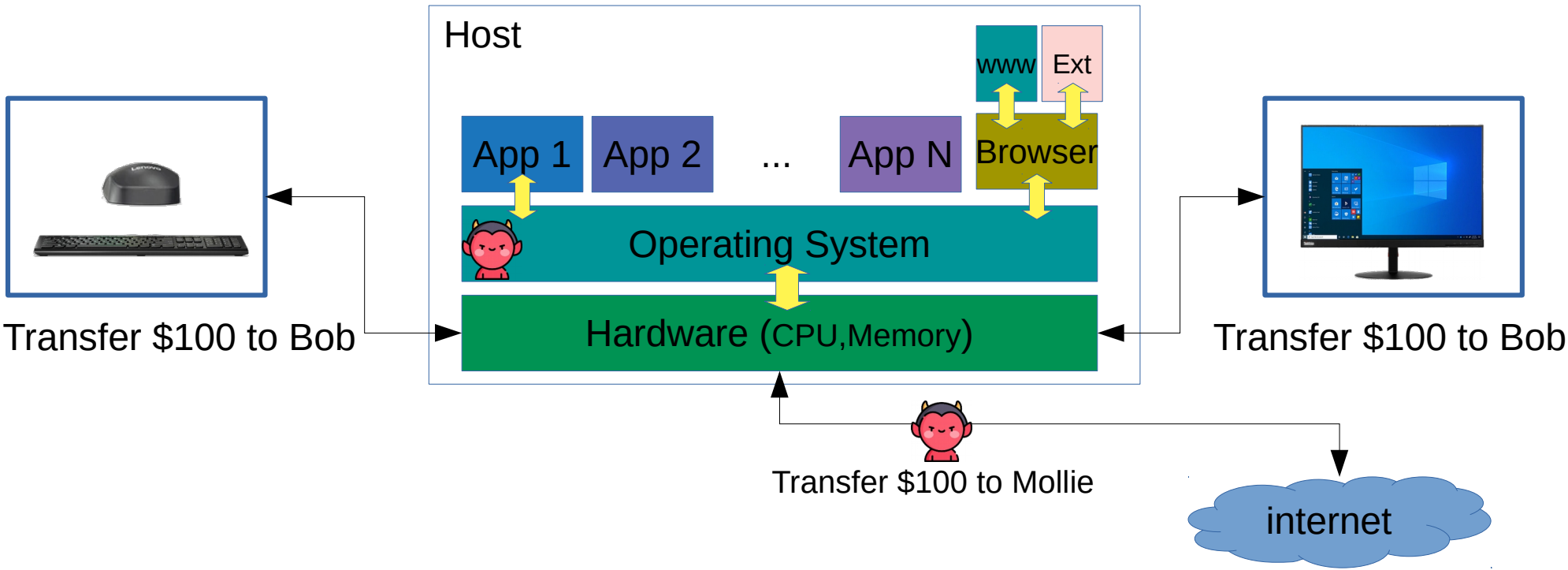
How secure are computers?



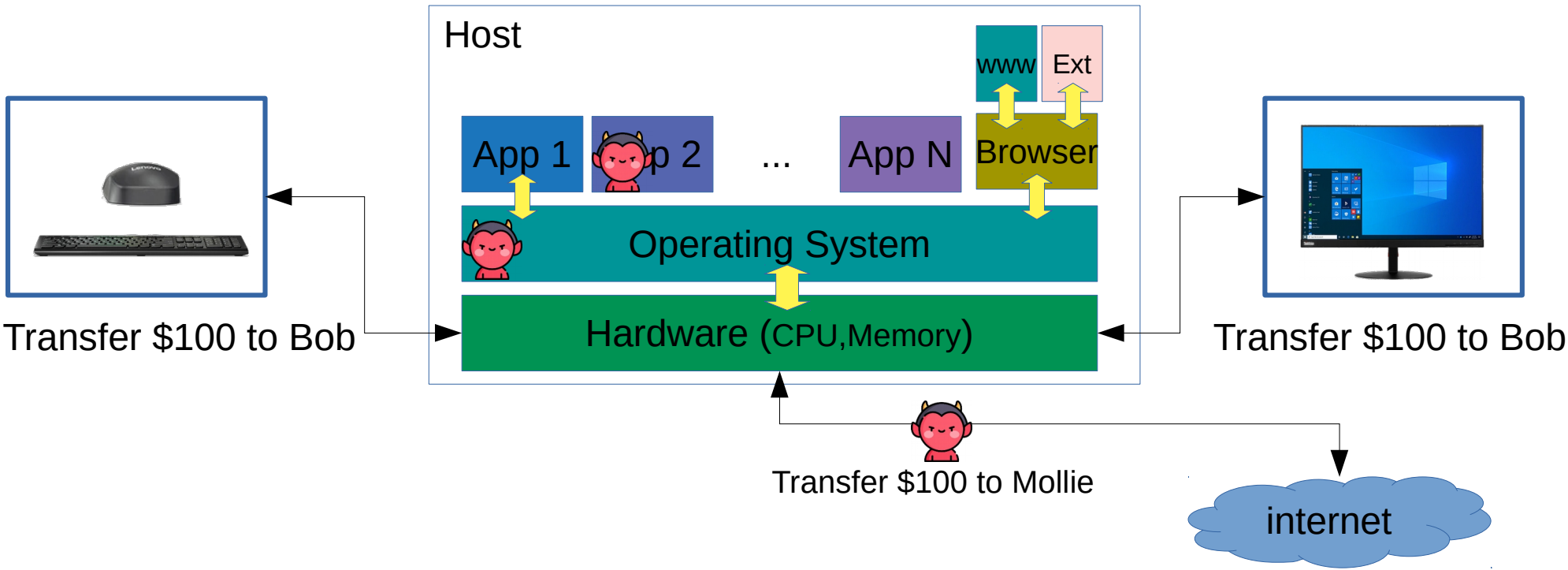
How secure are computers?



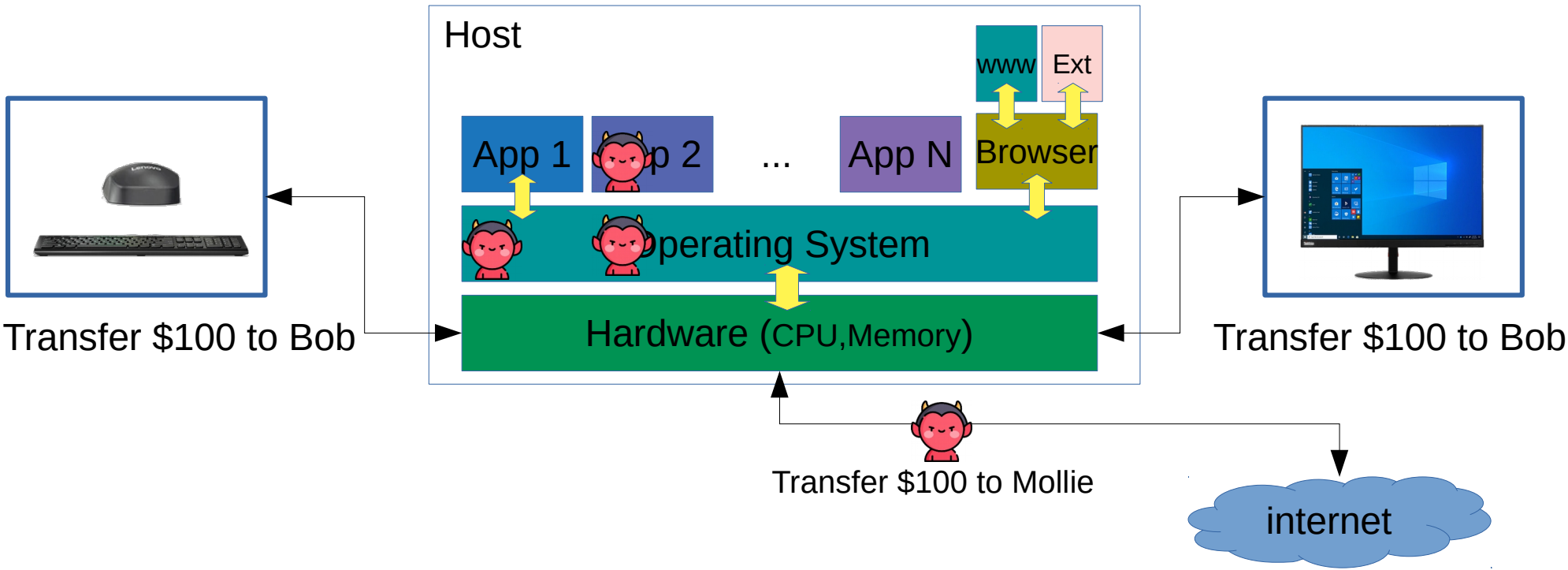
How secure are computers?



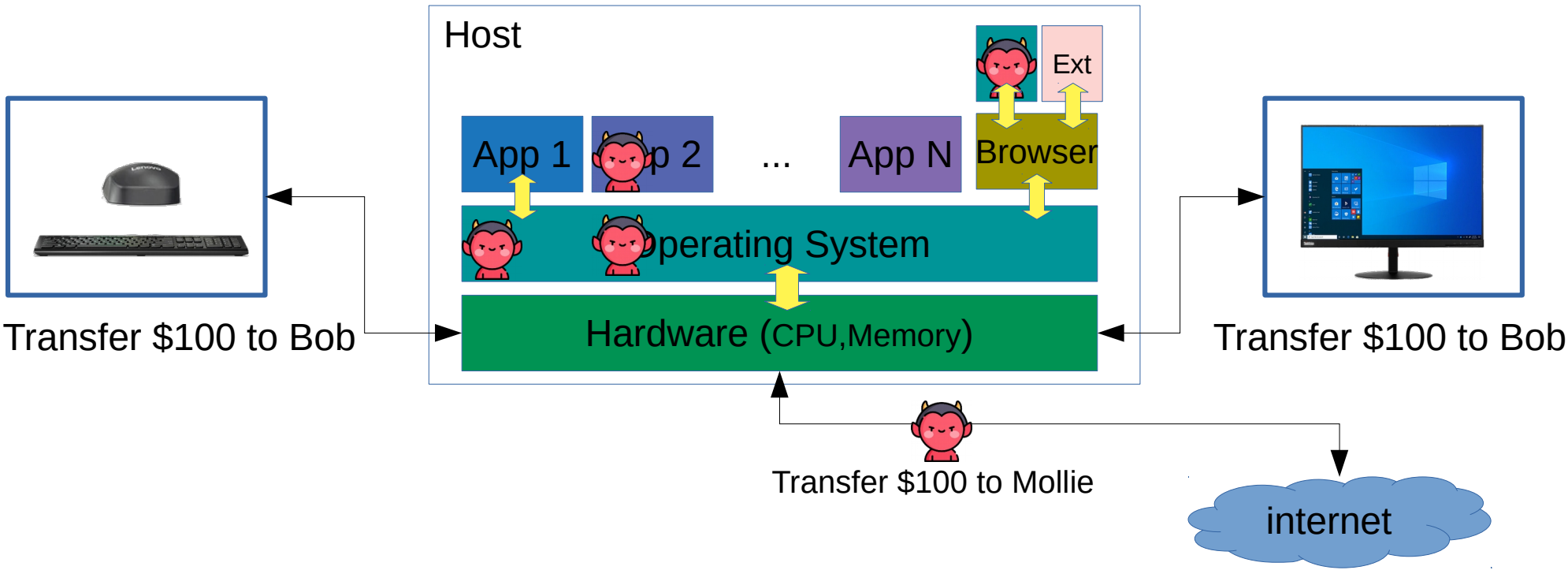
How secure are computers?



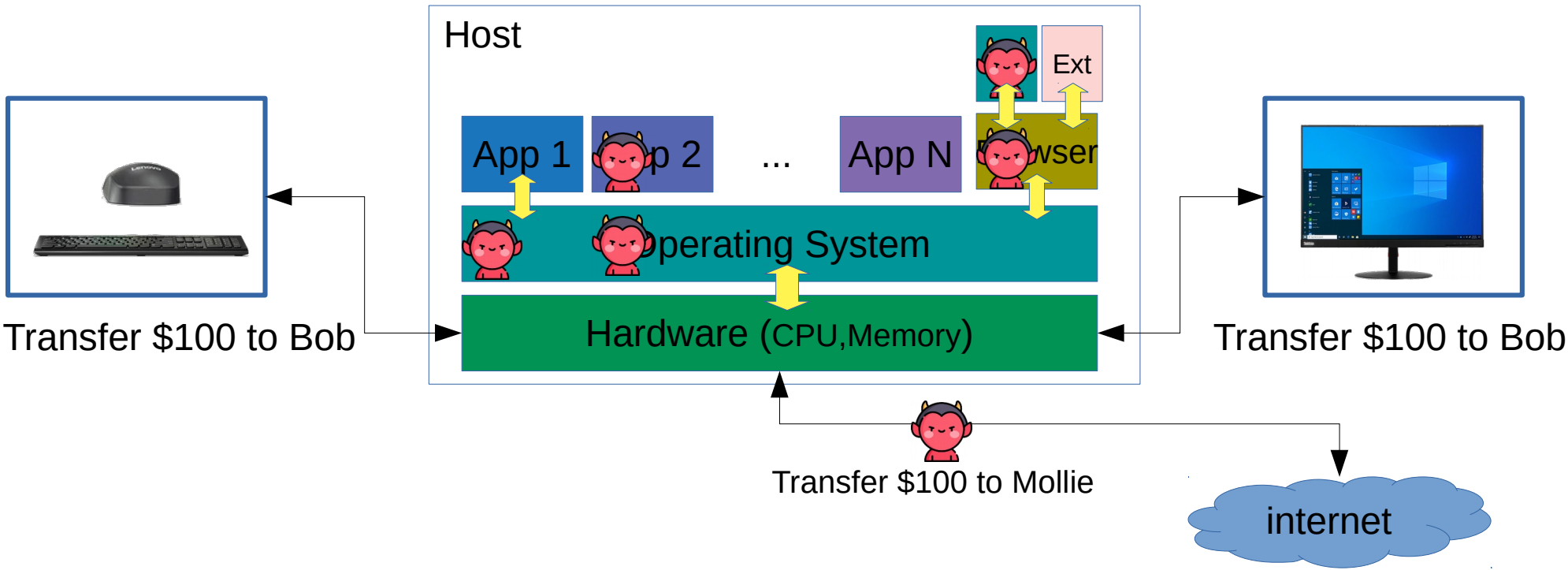
How secure are computers?



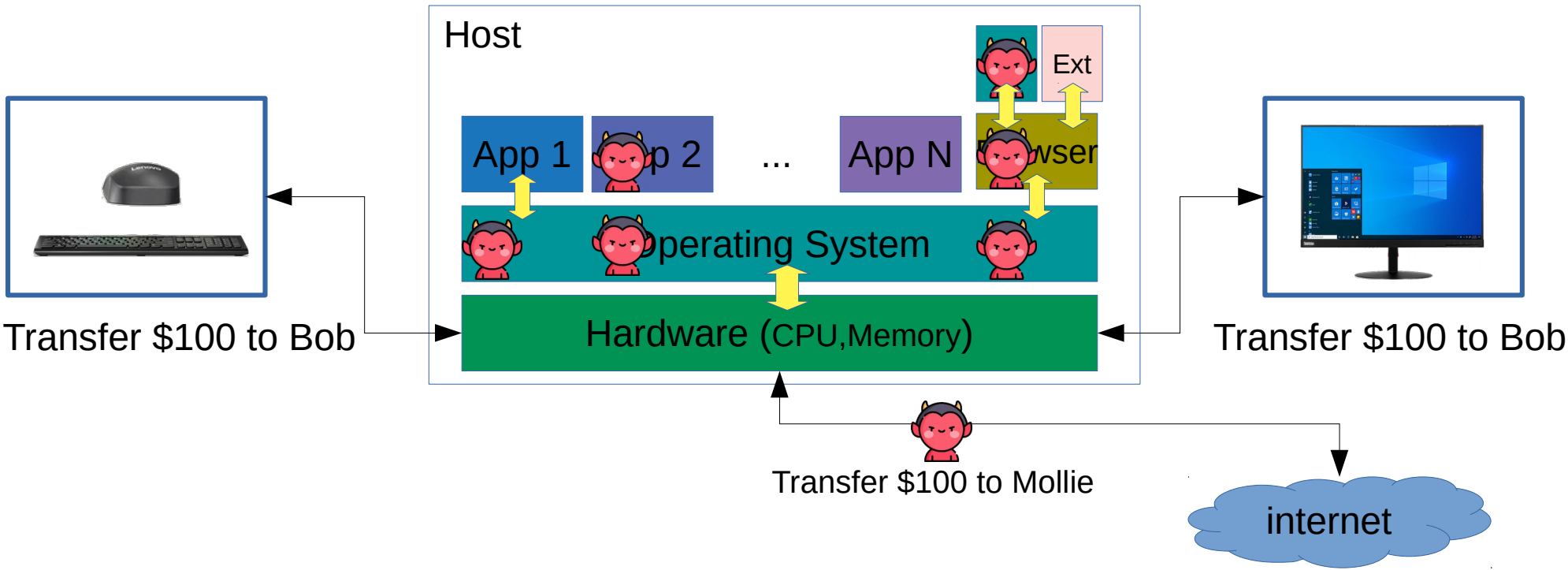
How secure are computers?



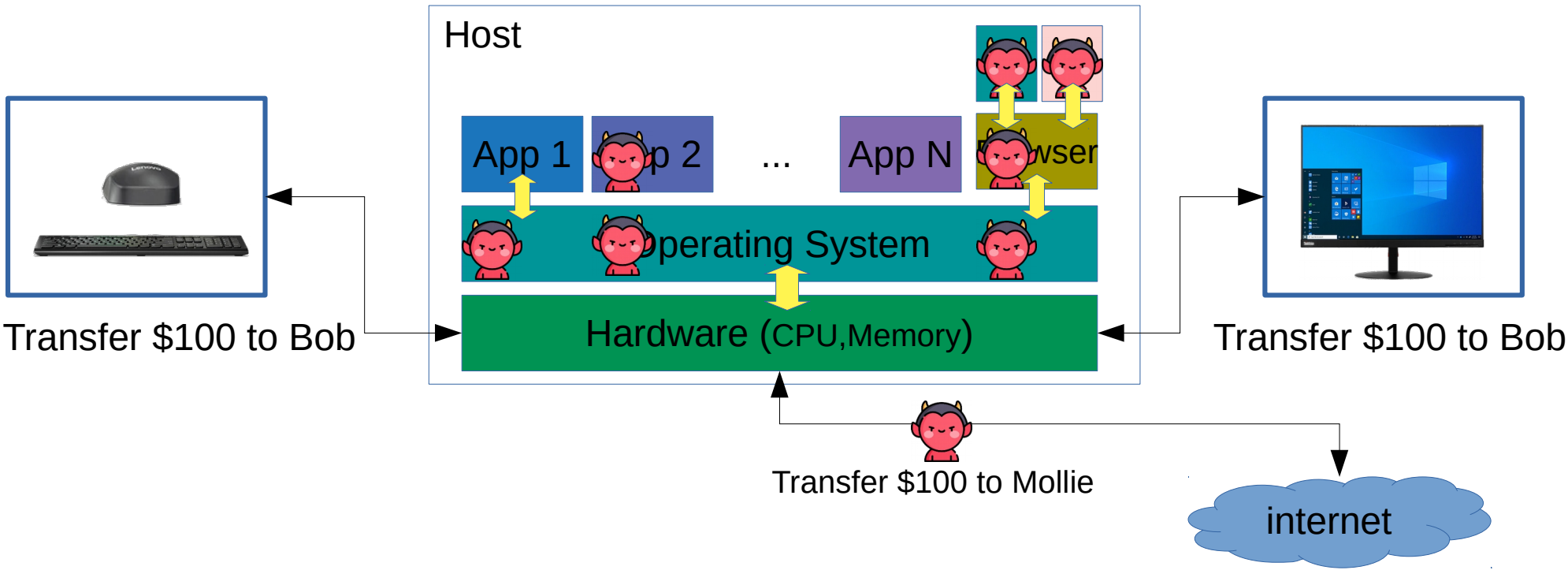
How secure are computers?



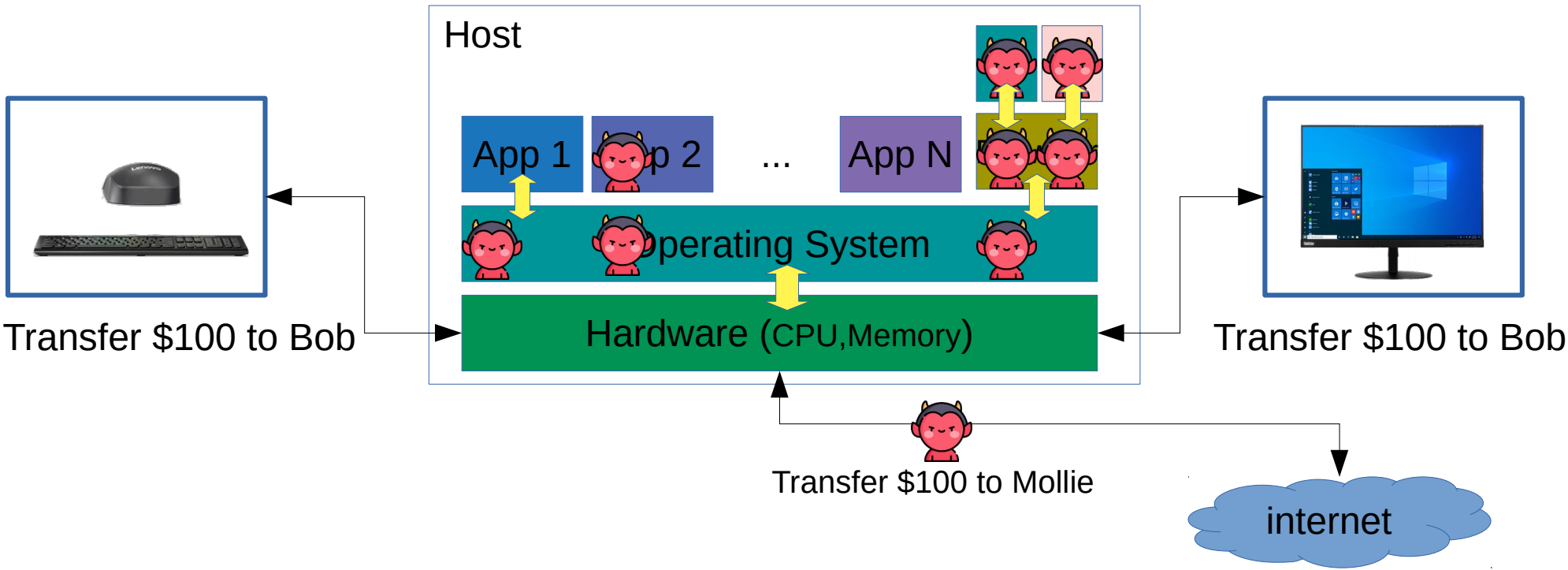
How secure are computers?



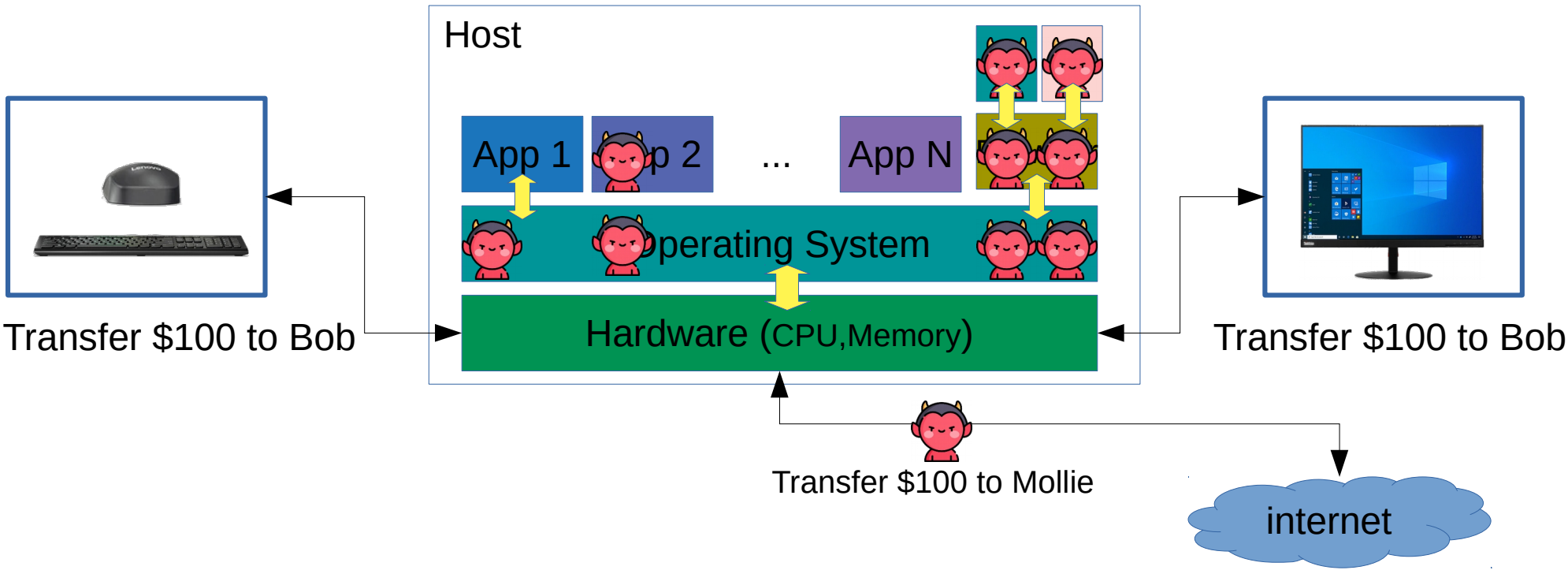
How secure are computers?



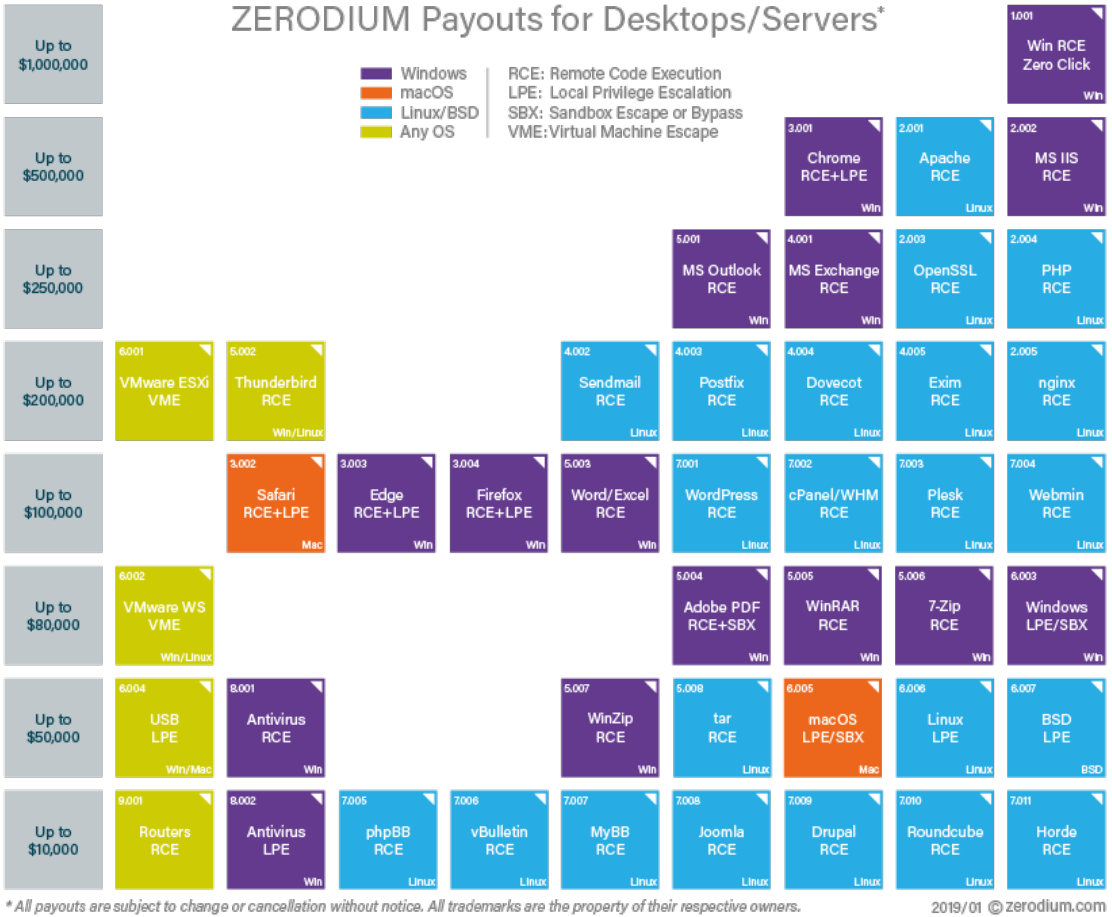
How secure are computers?



How secure are computers?



Vulnerabilities Price



Trusted Paths Requirements

Trusted Paths Requirements

- Observation 1: The lack of output integrity – *the render of user inputs on the screen* – compromises input integrity.

Trusted Paths Requirements

- Observation 1: The lack of output integrity – *the render of user inputs on the screen* – compromises input integrity.
- Observation 2: If the protected output is provided out-of-context, users are more likely not to verify it. Therefore input integrity can be violated.

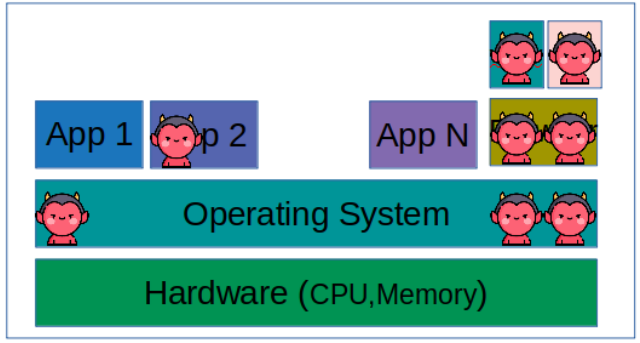
Trusted Paths Requirements

- Observation 1: The lack of output integrity – *the render of user inputs on the screen* – compromises input integrity.
- Observation 2: If the protected output is provided out-of-context, users are more likely not to verify it. Therefore input integrity can be violated.
- Observation 3: If not all the modalities of inputs are secured simultaneously, none of them can be fully secured.

Trusted Paths approaches

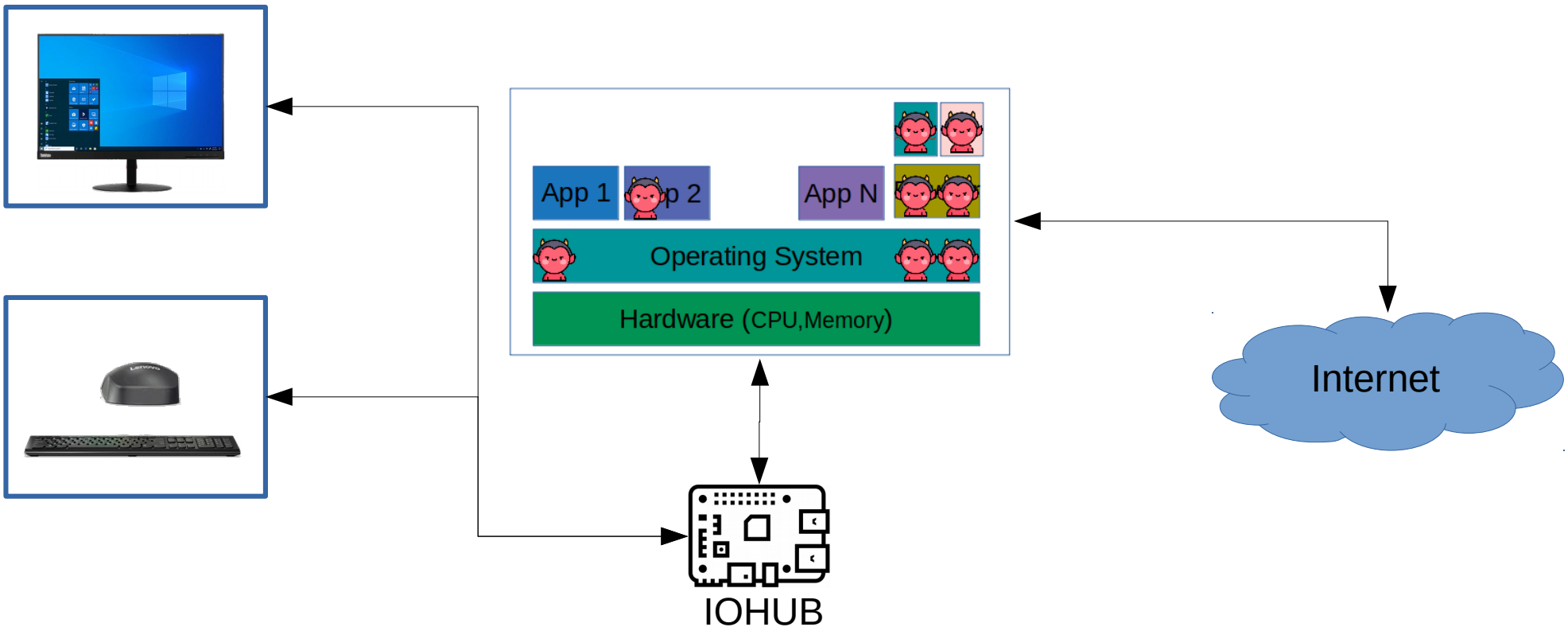
- Trusted path
  - **A.** Transaction confirmation Device
    - Uni-dir [5]
  - **B.** Trusted intermediary
    - **B1.** Hypervisor-based
      - Overshadow [18]
      - SGXIO [4]
    - **B2.** External HW
      - PROTECTION
      - Fidelius [9]
    - **B3.** System TEE
      - VButton [16]
      - TruZ-Droid [17]

ProtectIOn Architecture

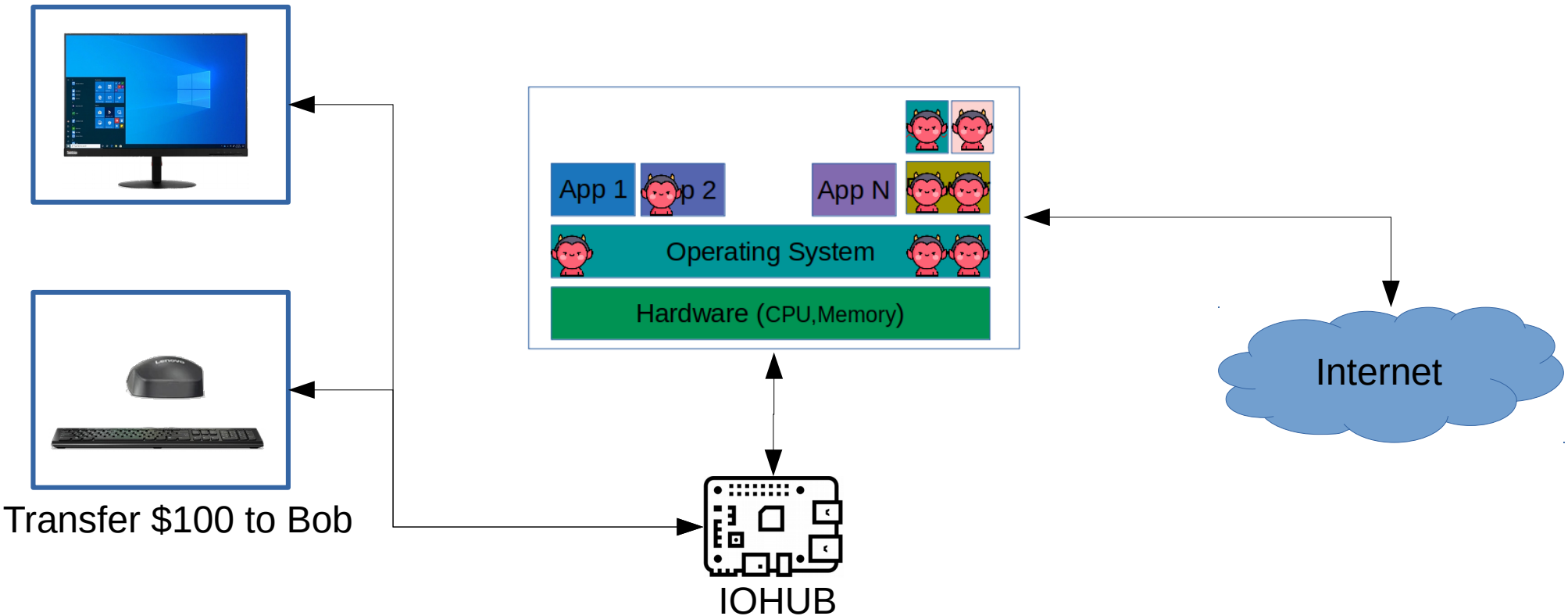


Internet

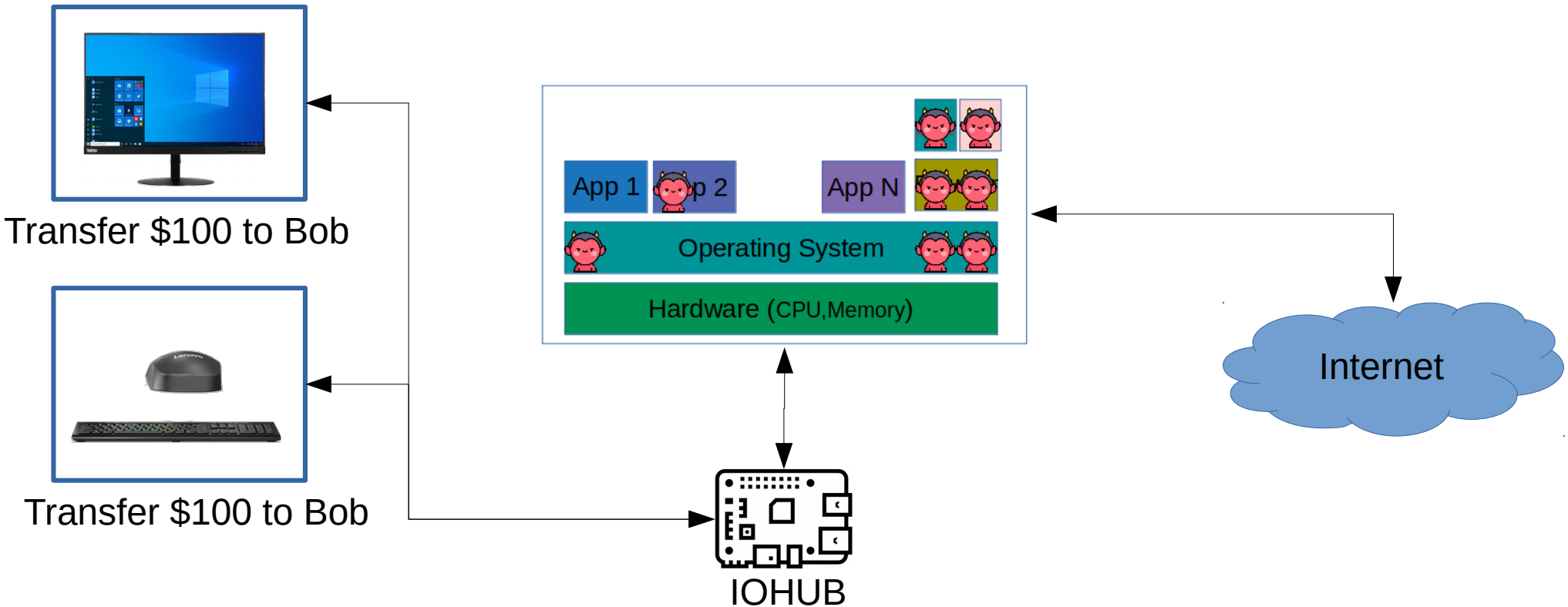
ProtectIOn Architecture



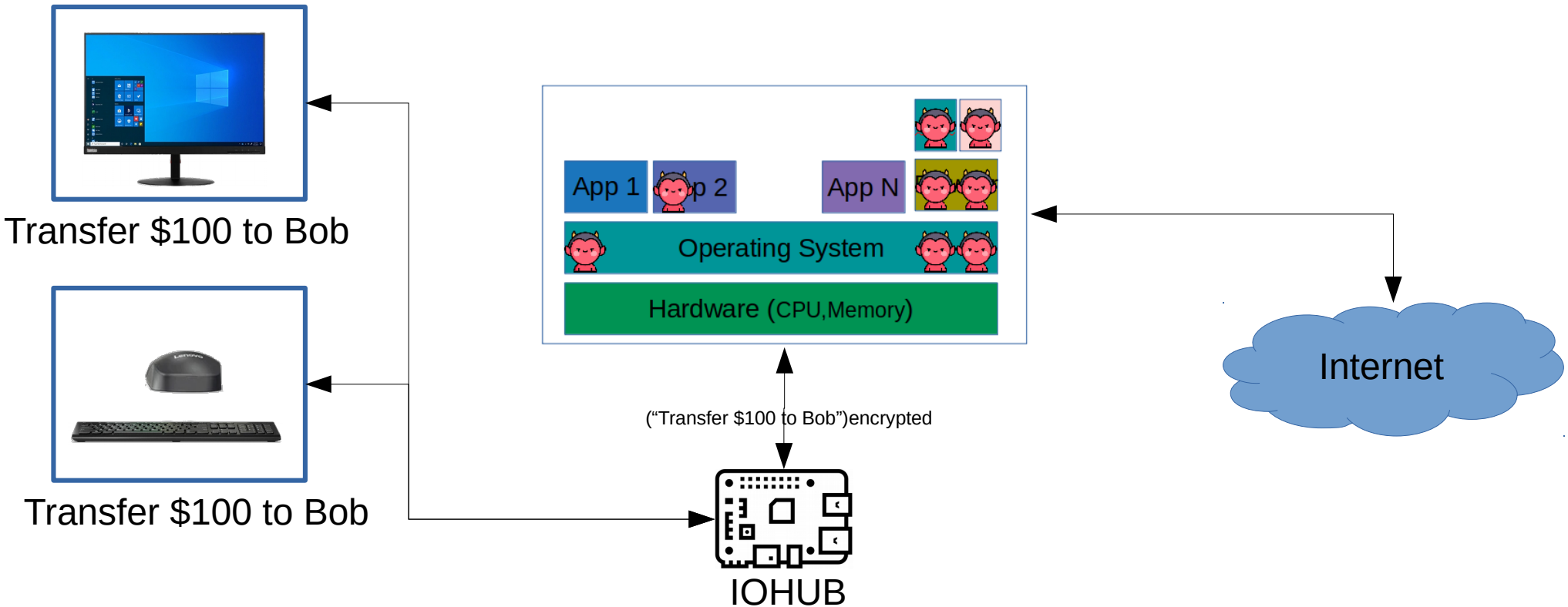
ProtectIOn Architecture



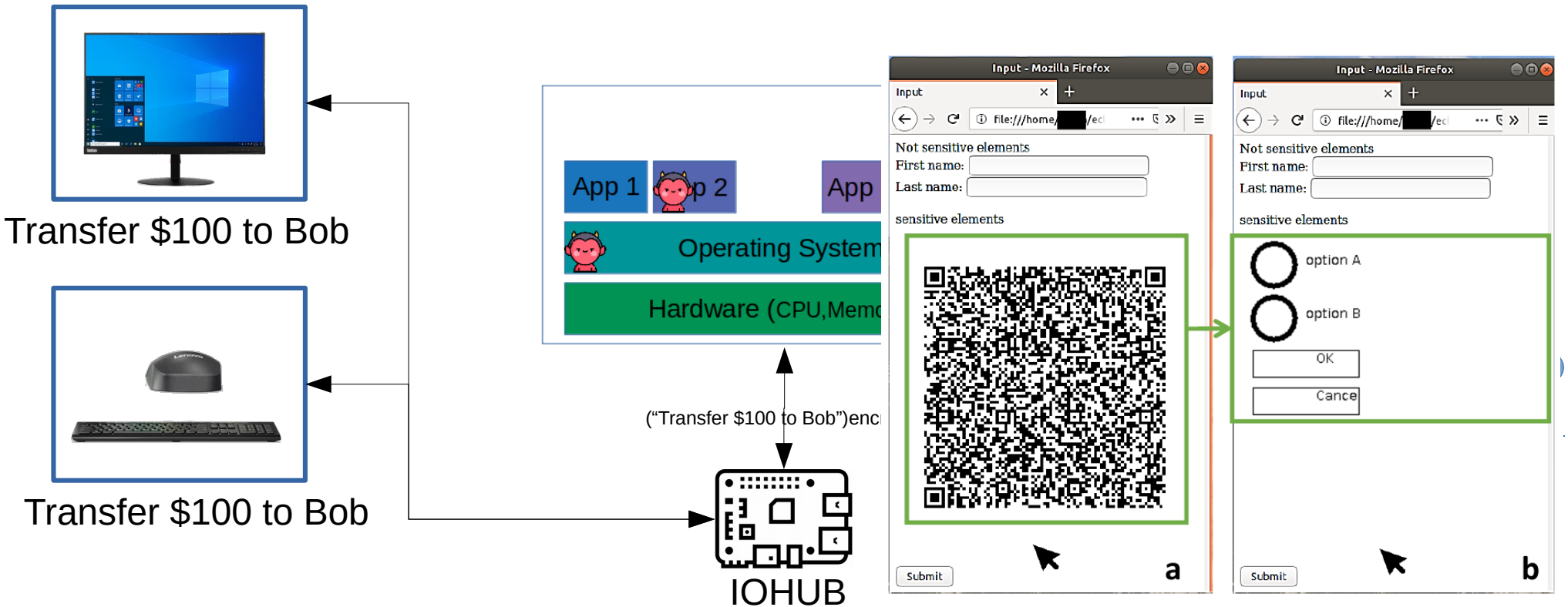
ProtectIOn Architecture



ProtectIOn Architecture

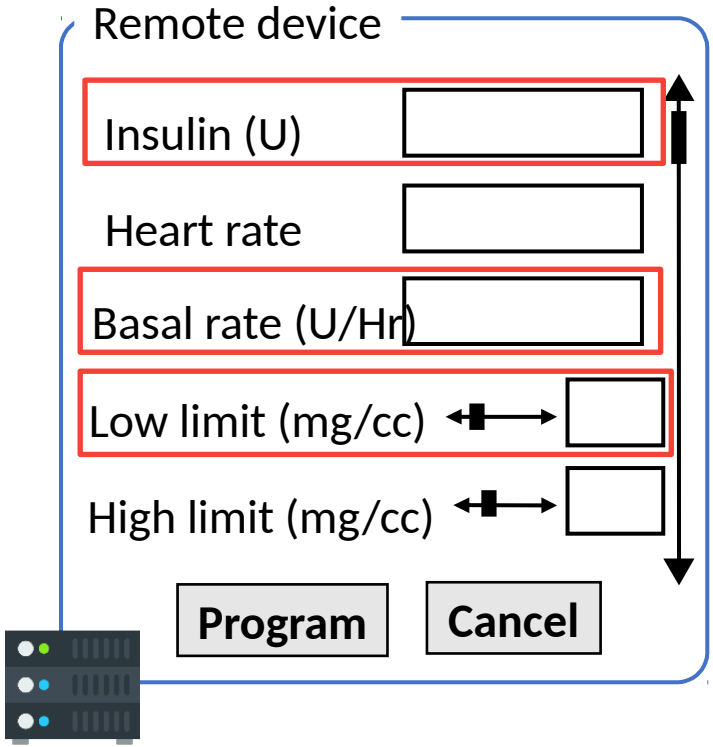


ProtectIOn Architecture



IO Integrity – Configuration

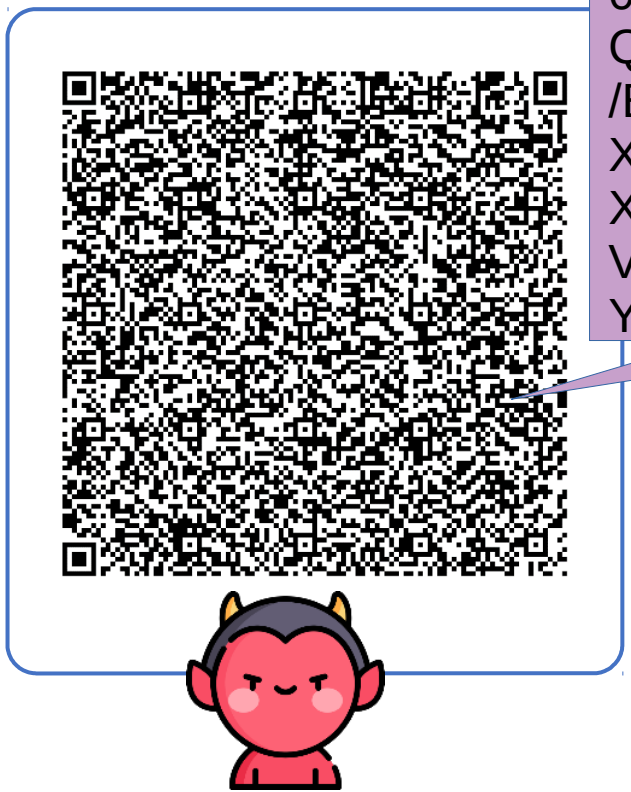
Simultaneous IO



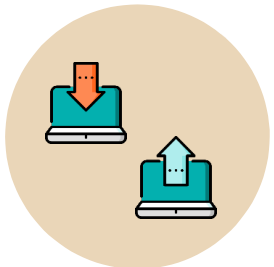

```
<form action="/some_action", signature = "0x45AB…", id
= "0x0ab">
```

IO Integrity – Host's view

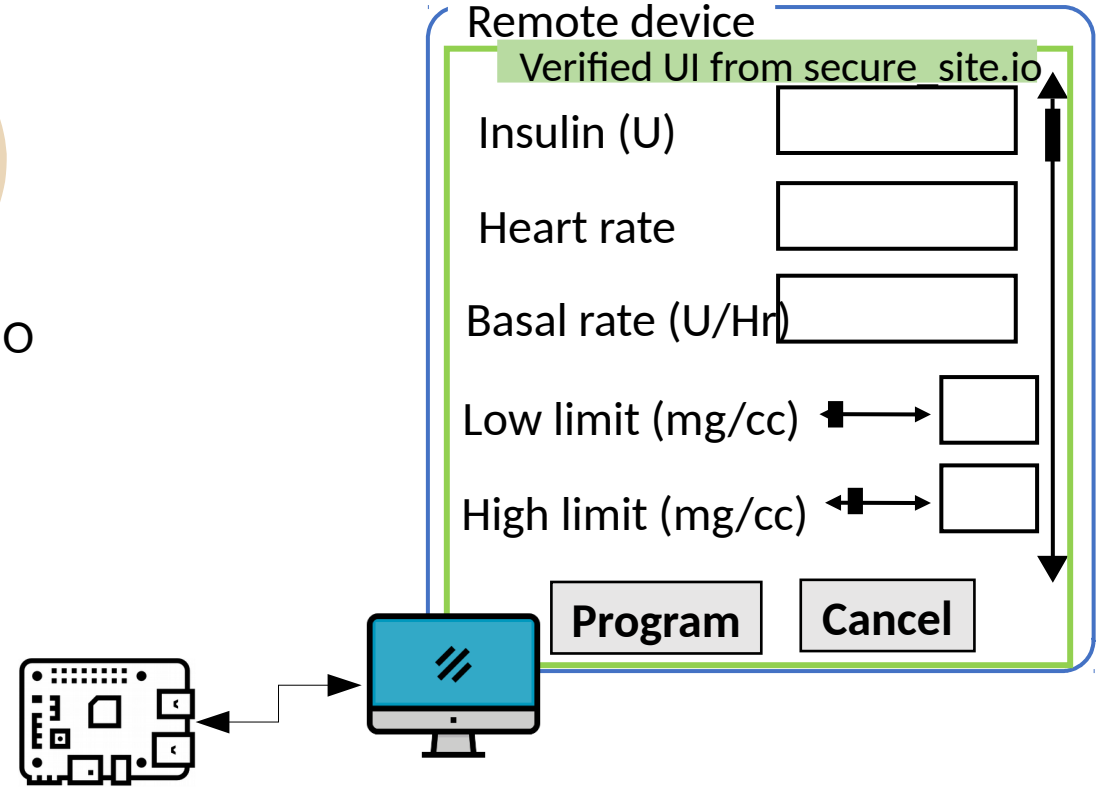
Simultaneous IO



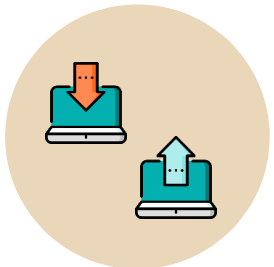
IO Integrity – User's view



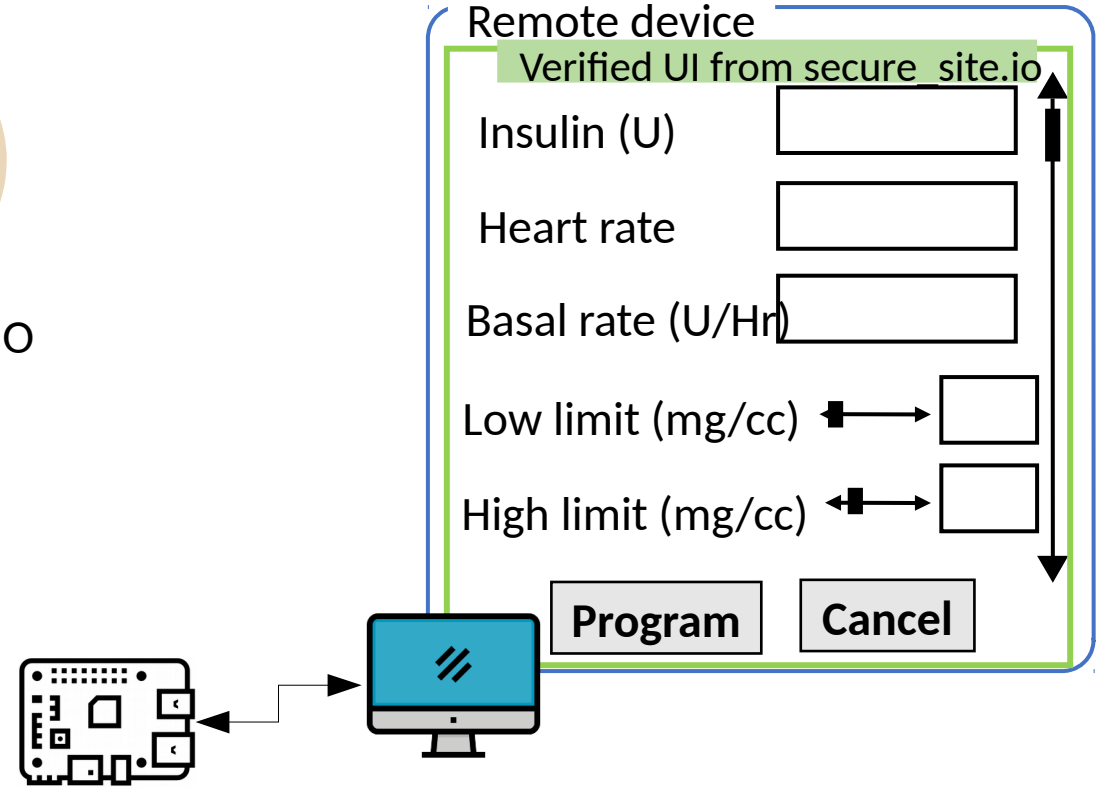
Simultaneous IO



IO Integrity – User's view



Simultaneous IO



Put 1 in front of all inputs

User Attention

Low cognitive load

User Attention

Low cognitive load

- Output Integrity: Low cognitive load

Put 1 in front of all inputs

User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms

Put 1 in front of all inputs

Grabbing User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms
  - Lightbox

Put 1 in front of all inputs

Grabbing User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms
  - Lightbox
  - Highlight

Put 1 in front of all inputs

Grabbing User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms
  - Lightbox
  - Highlight
  - Freezing

Put 1 in front of all inputs

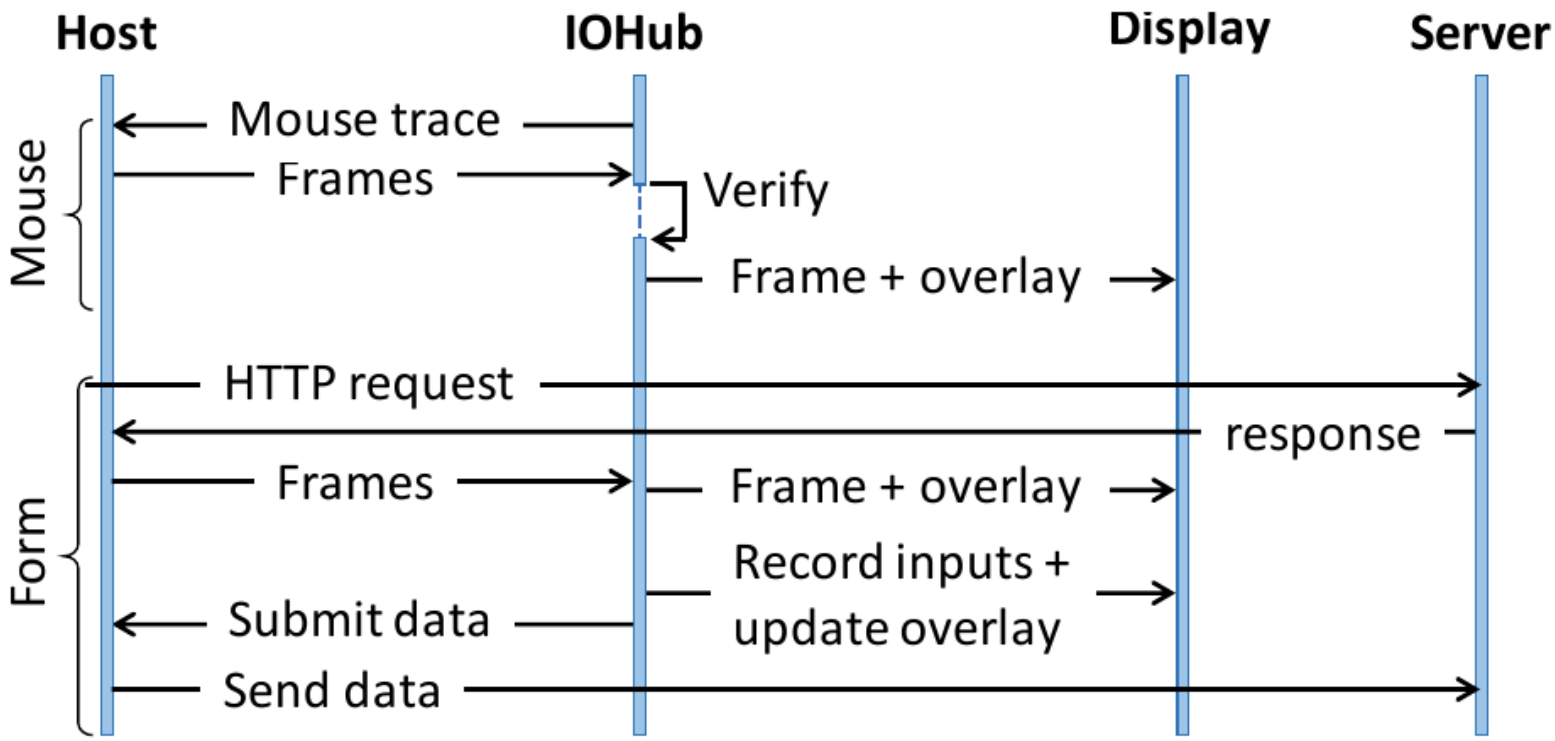
Grabbing User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms
  - Lightbox
  - Highlight
  - Freezing
  - Combination

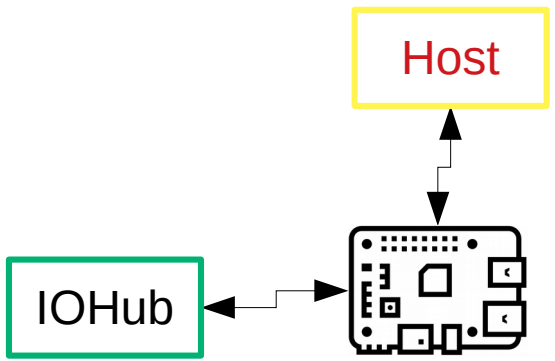
Put 1 in front of all inputs

Protocol flow

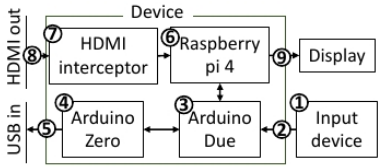


IOHub benefits

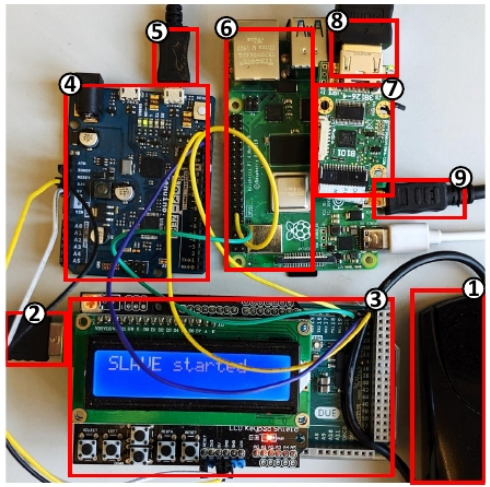
- Low TCB (possible to formally verify)
- Limited interfaces
- Generalization
  - Security guarantees
  - Easy to deploy
  - Scalability
- Low cost



Prototype Implementation



(a) The figure shows the basic components and connections between them in our PROTECTION prototype.



(b) PROTECTION prototype uses Arduino Due and Zero microcontroller board and a Raspberry Pi 4 SBC. The highlighted numbers correspond to the labels in Figure 9a

Takeaways

Takeaways

- Root-of-trust for user Input/Output is critical for many applications.

Takeaways

- Root-of-trust for user Input/Output is critical for many applications.
- Solutions should put low cognitive load to the user while preserving usability.

Takeaways

- Root-of-trust for user Input/Output is critical for many applications.
- Solutions should put low cognitive load to the user while preserving usability.
- ProtectIOn's security guarantees:
  - Integrity (both input and output)
  - Confidentiality (both input and output)

Takeaways

- Root-of-trust for user Input/Output is critical for many applications.
- Solutions should put low cognitive load to the user while preserving usability.
- ProtectIOn's security guarantees:
  - Integrity (both input and output)
  - Confidentiality (both input and output)
- Scalability.

Thank You