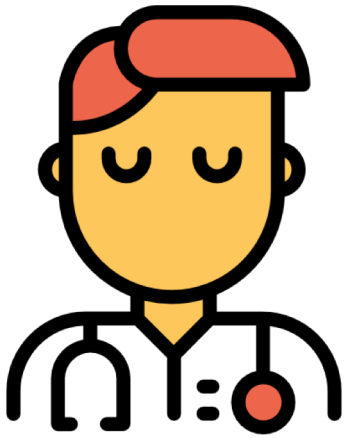
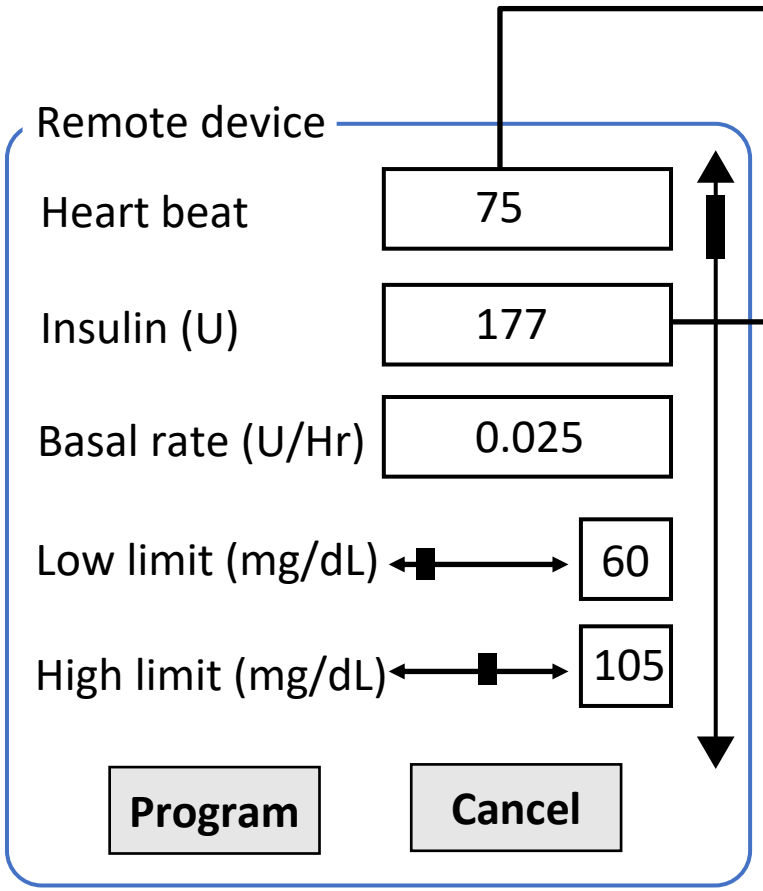
ETH zürich

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

Aritra Dhar, Enis Ulqinaku, Kari Kostiainen, Srdjan Capkun
ETH Zurich

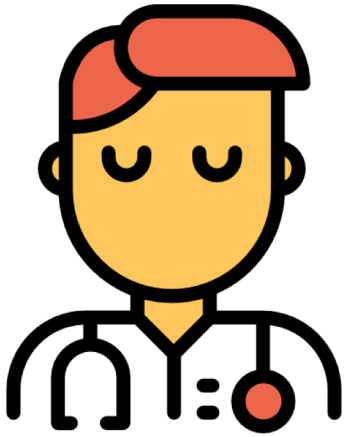
Motivation

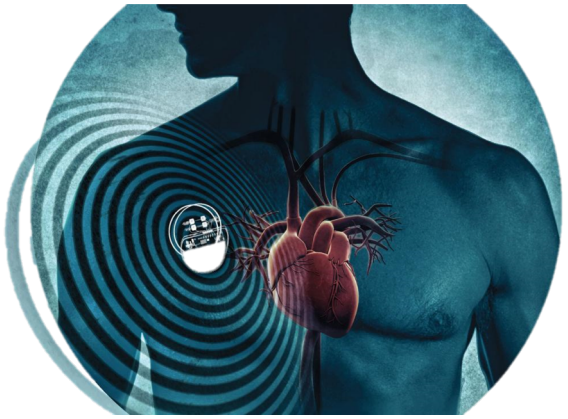



Remote device
Heart beat
75
Insulin (U)
177
Basal rate (U/Hr)
0.025
Low limit (mg/dL)
60
High limit (mg/dL)
105
Program
Cancel


HAUPT MENÜ
BOLUS
OK

Motivation





Remote device

Heart beat 75

Insulin (U) 177

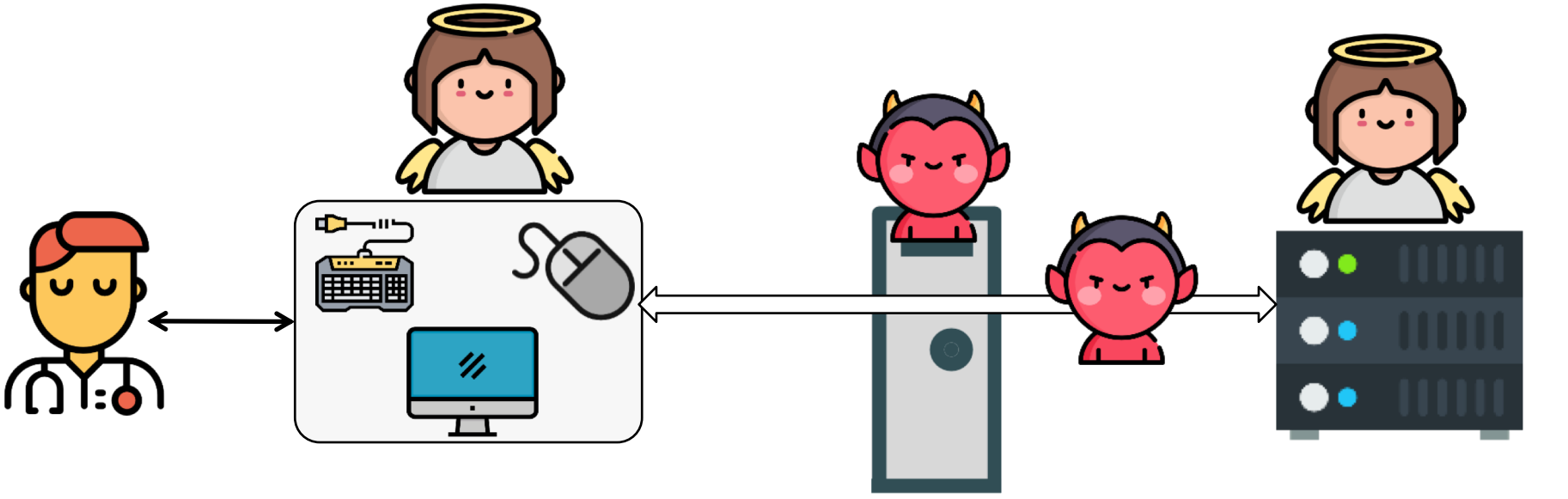
Basal rate (U/Hr) 0.025

Low limit (mg/dL) 60

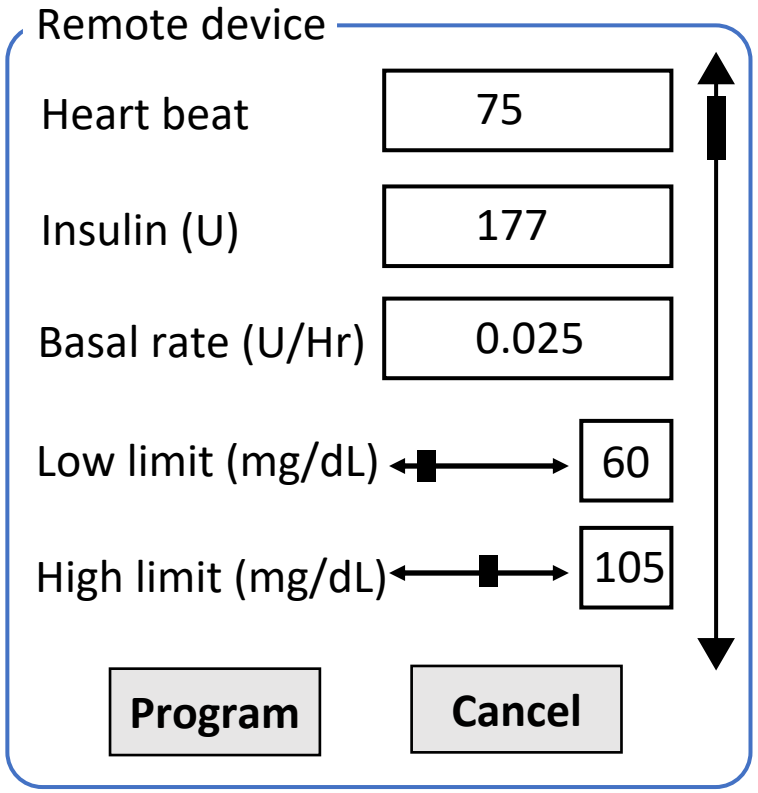
High limit (mg/dL) 105

Program **Cancel**

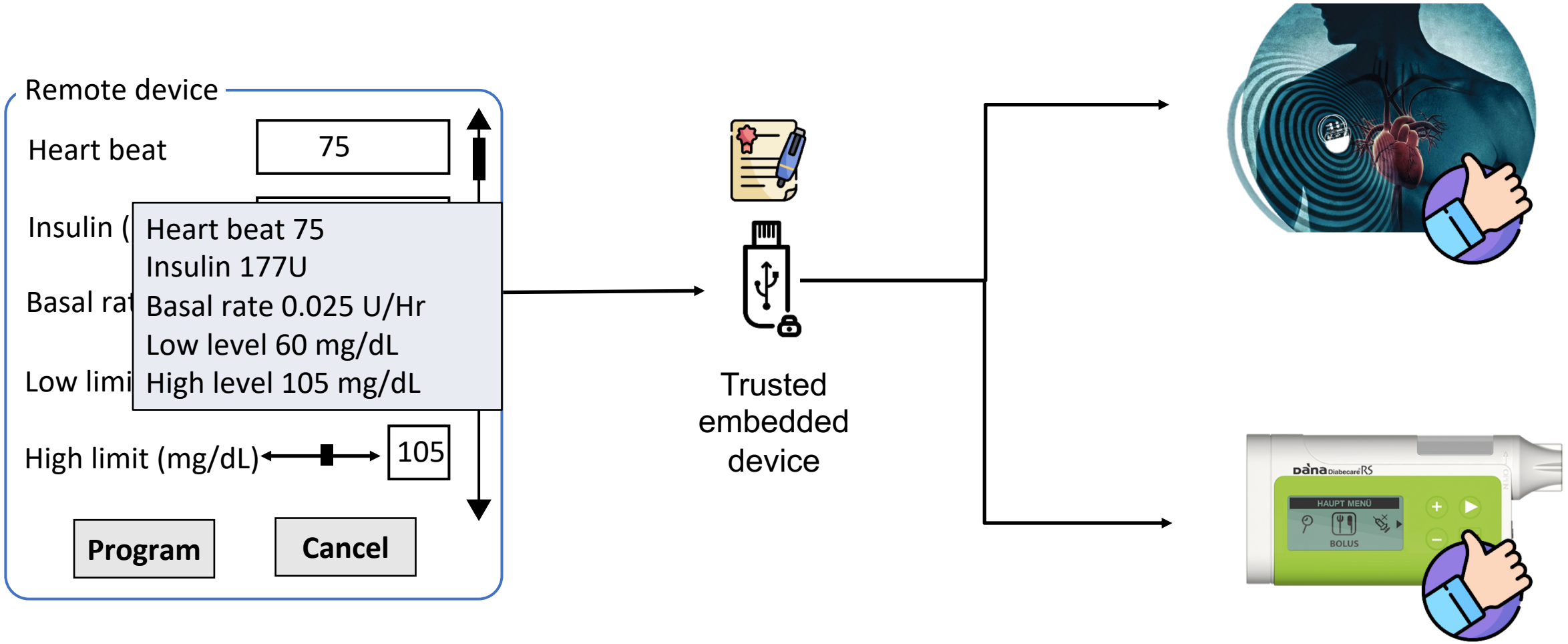
Remote Trusted path



Solution 1: Transaction Confirmation Device



Solution 2: Input Signing



Display manipulation attack

177

177

Insulin | 17

7

1777

Insulin | 177

User sees 177

Device records 1777

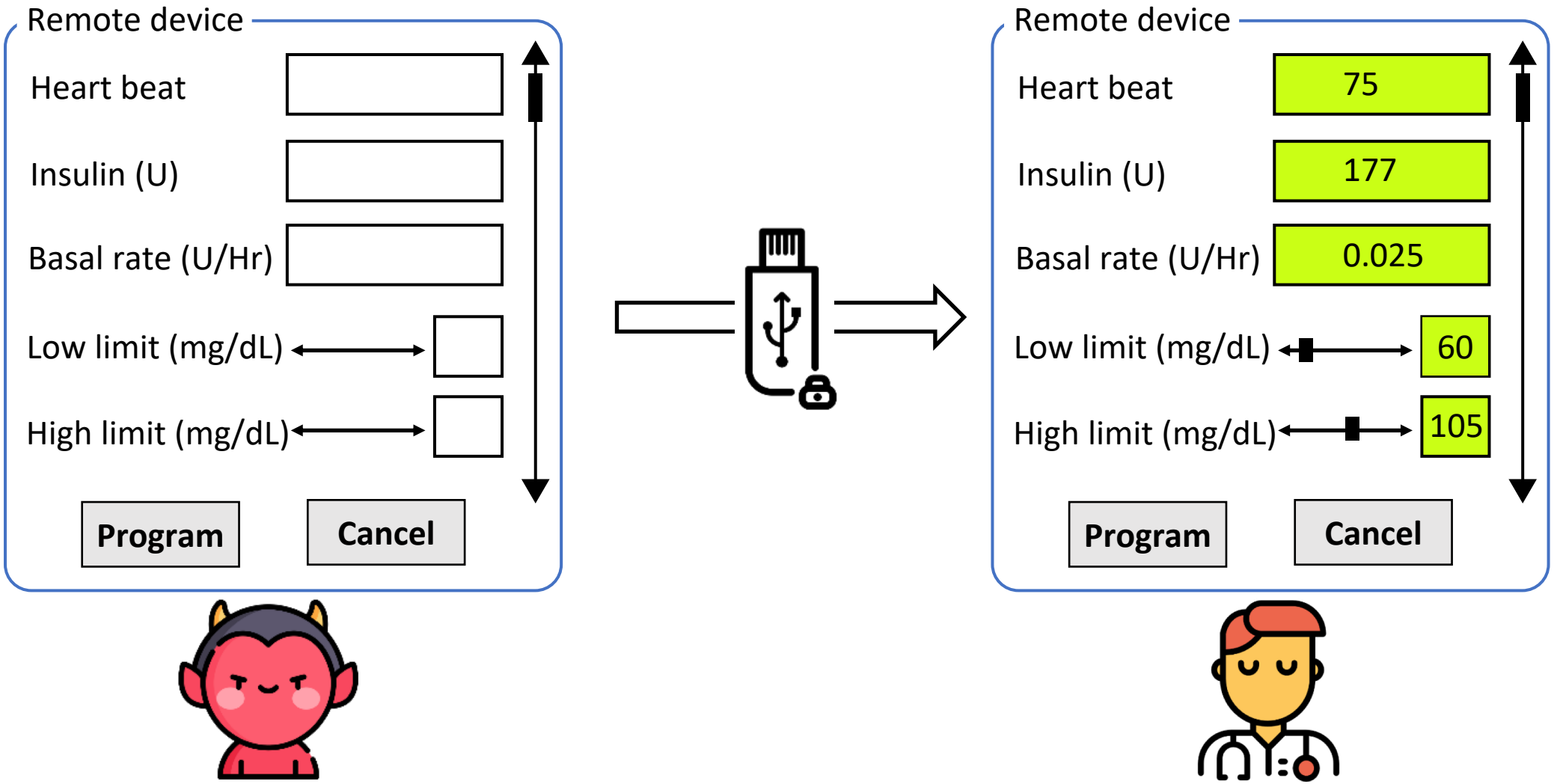
Host sends 1777

- IntegriKey

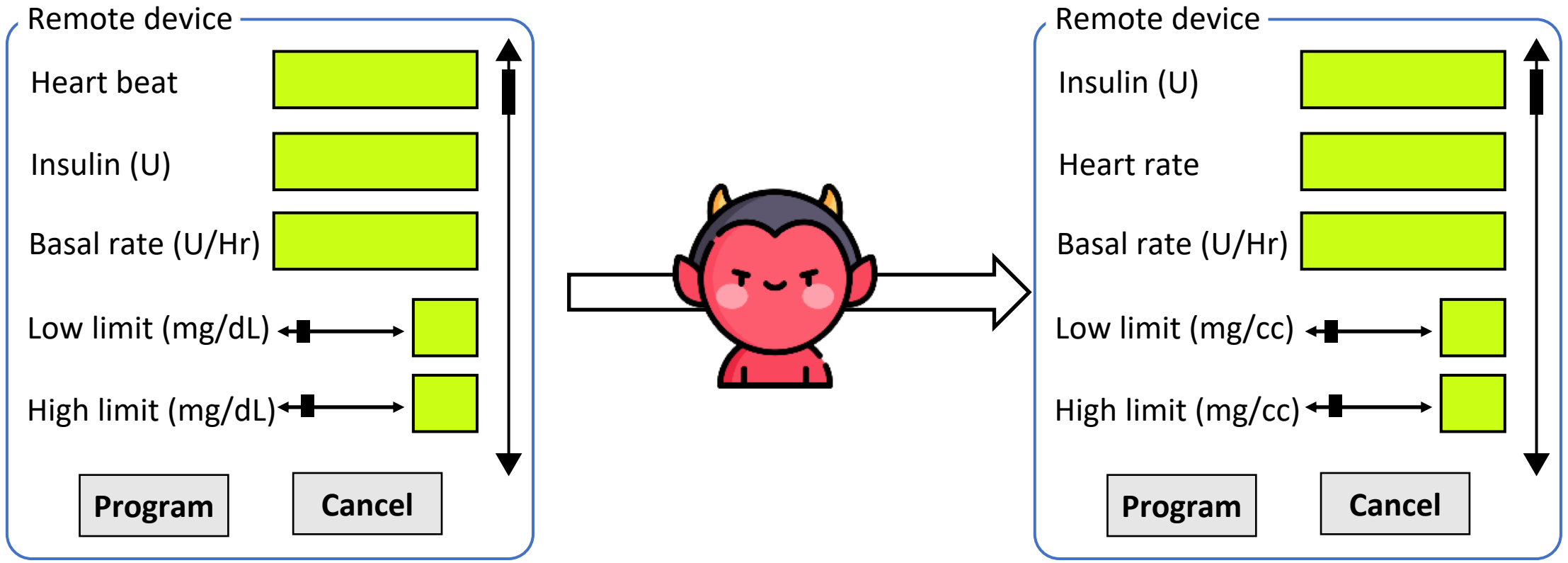
Observation 1

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

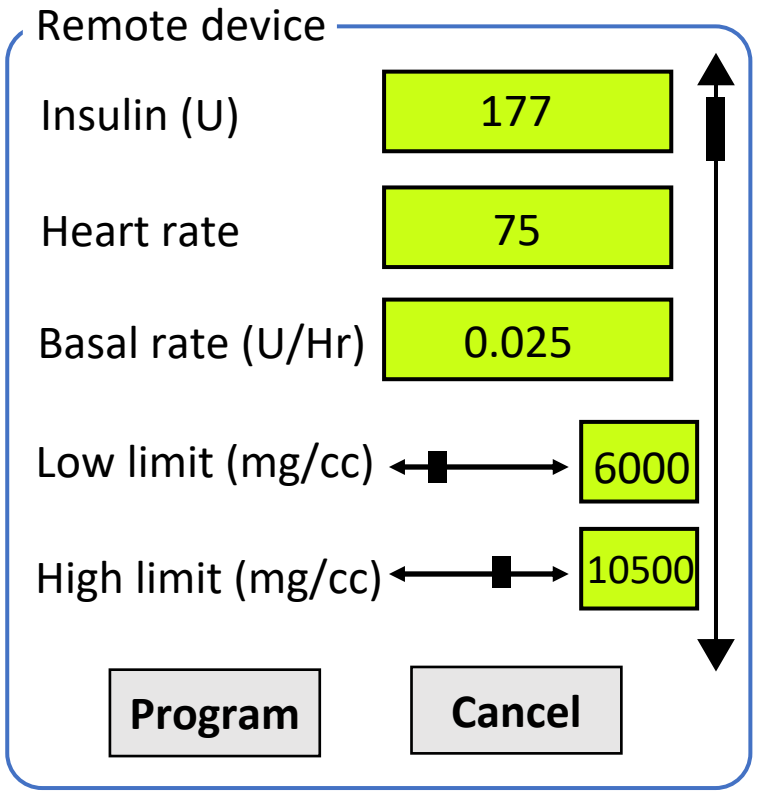
Solution 3: Overlay



Overlay: Output Manipulation



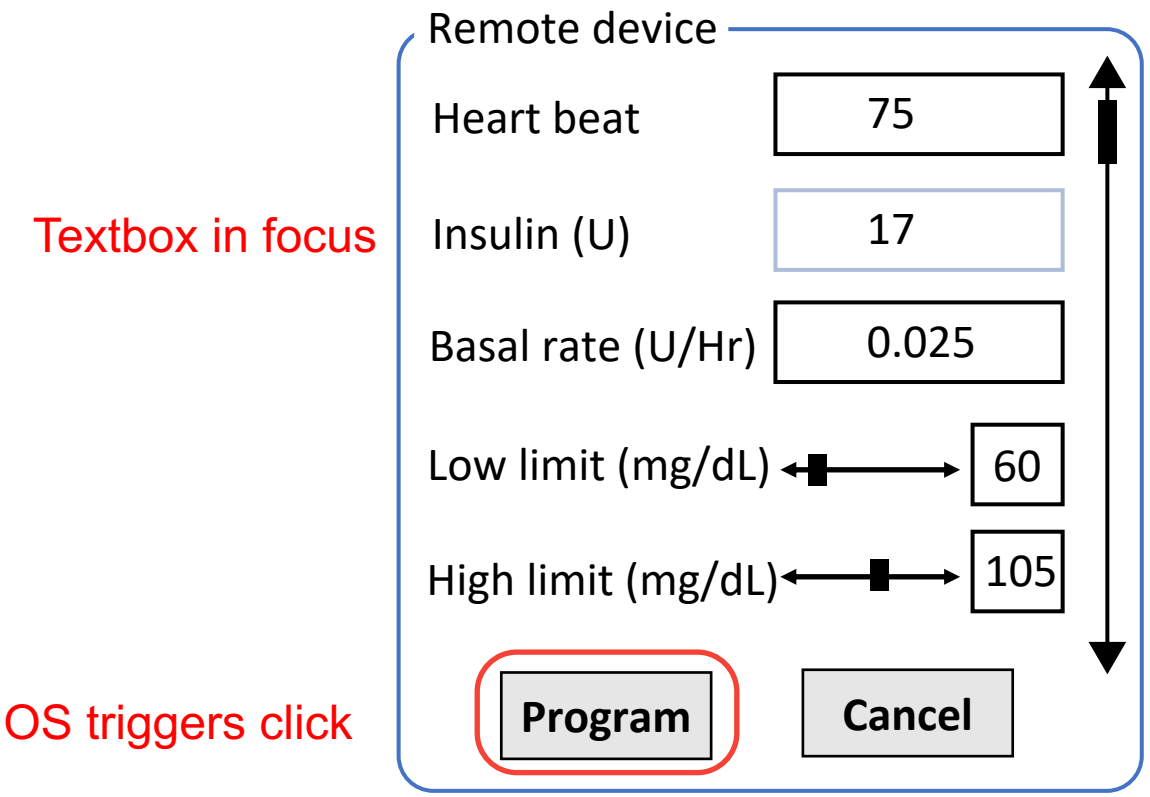
Overlay: Output Manipulation



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.

Overlay: Early Form Submission Attack



- Fidelius
- Trusted overlay from FPGA

Observation 3

If *not all the modalities of inputs* are secured simultaneously, none of them can be fully secured.

Requirements

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

Inter-dependency between Input and output

Requirements

If *not all the modalities of inputs* are secured simultaneously, none of them can be fully secured.

All modalities of input

Requirements

If the *protected output* is provided *out-of-context*, users are more likely not to verify it.
Therefore input integrity can be violated.

Low cognitive load

Requirements

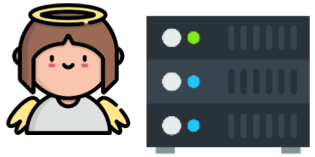
Low TCB and easy deploy

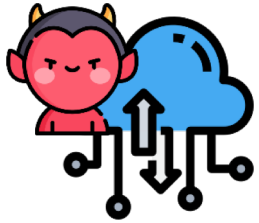
Requirements

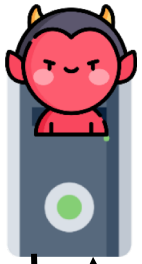
ProtectIOn

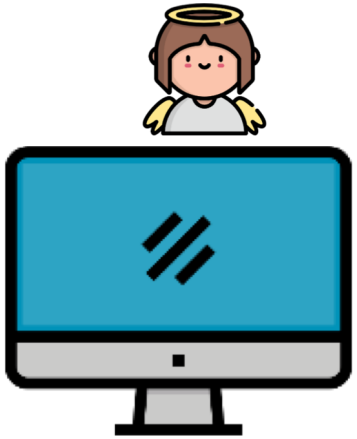
Low TCB + fast deployment

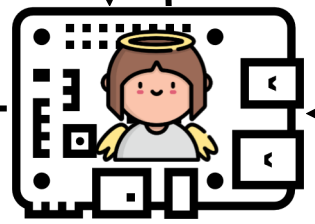
Input modalities



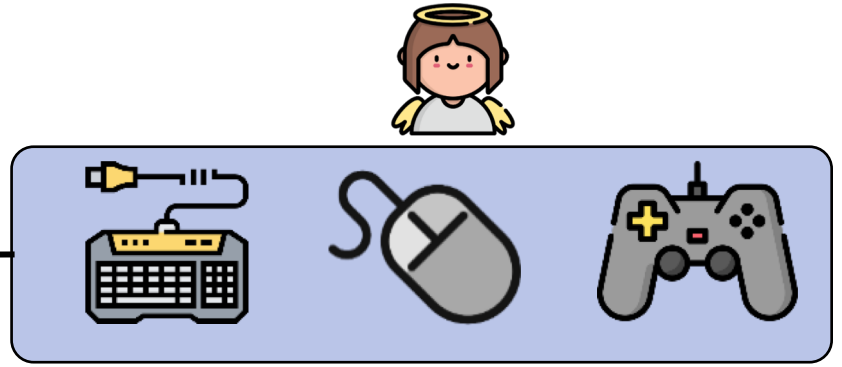






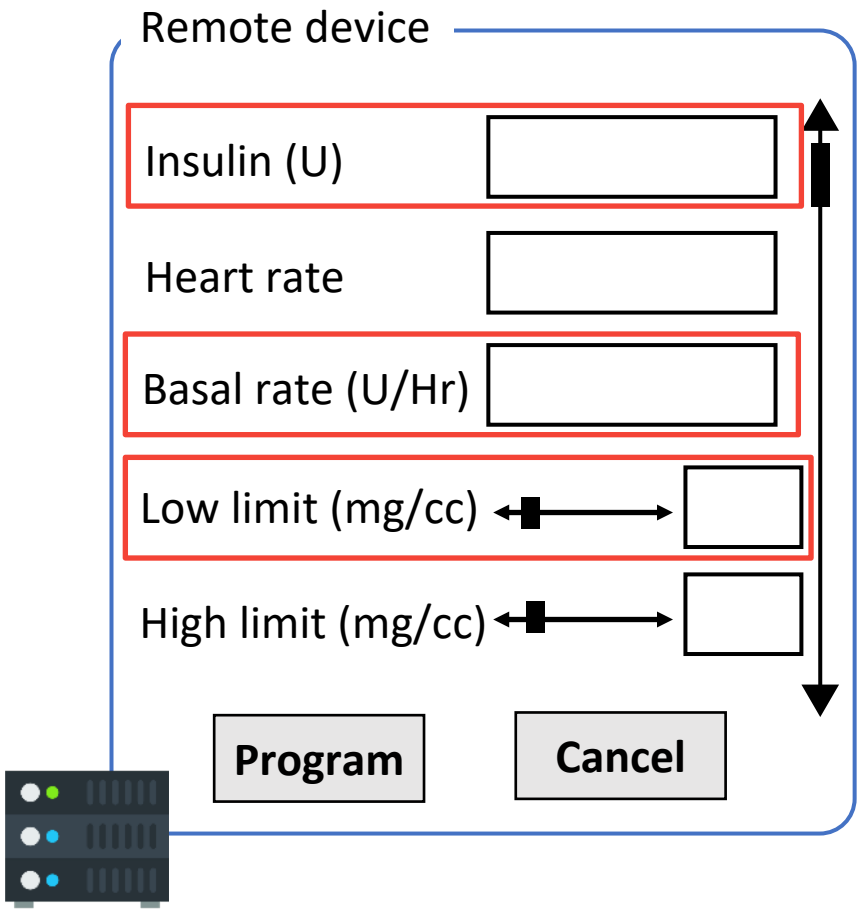


IOHub



IO Integrity – Overlay Generation

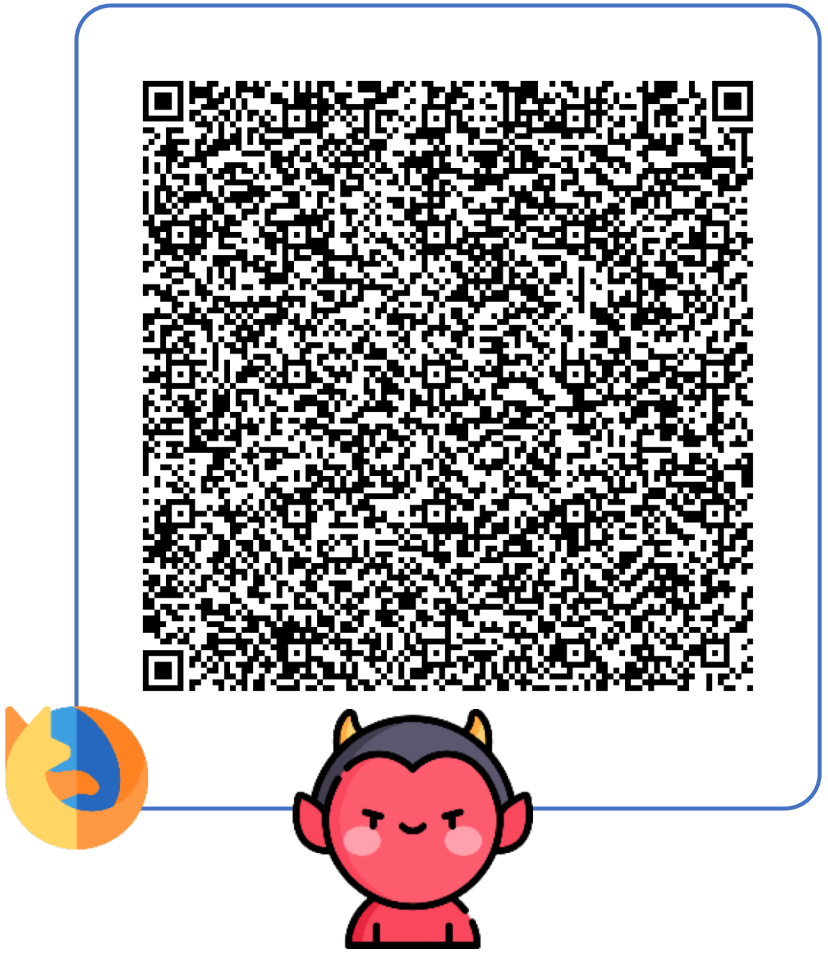
Simultaneous IO




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

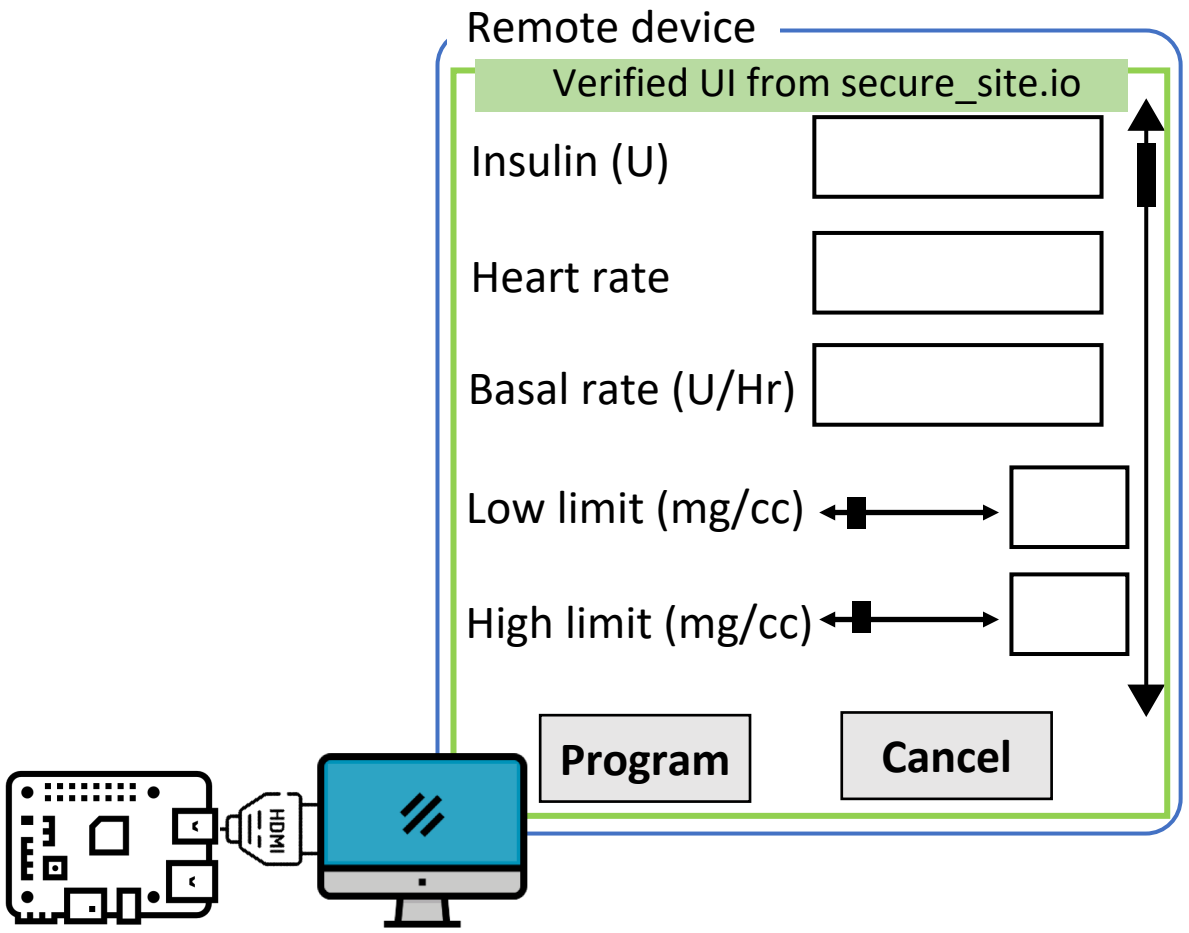
IO Integrity – Overlay Generation

Simultaneous IO



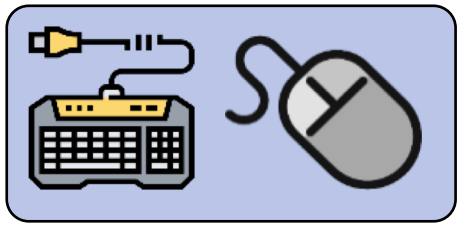
IO Integrity – Overlay Generation

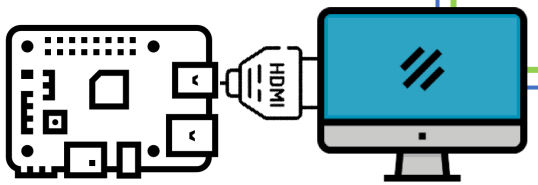
Simultaneous IO

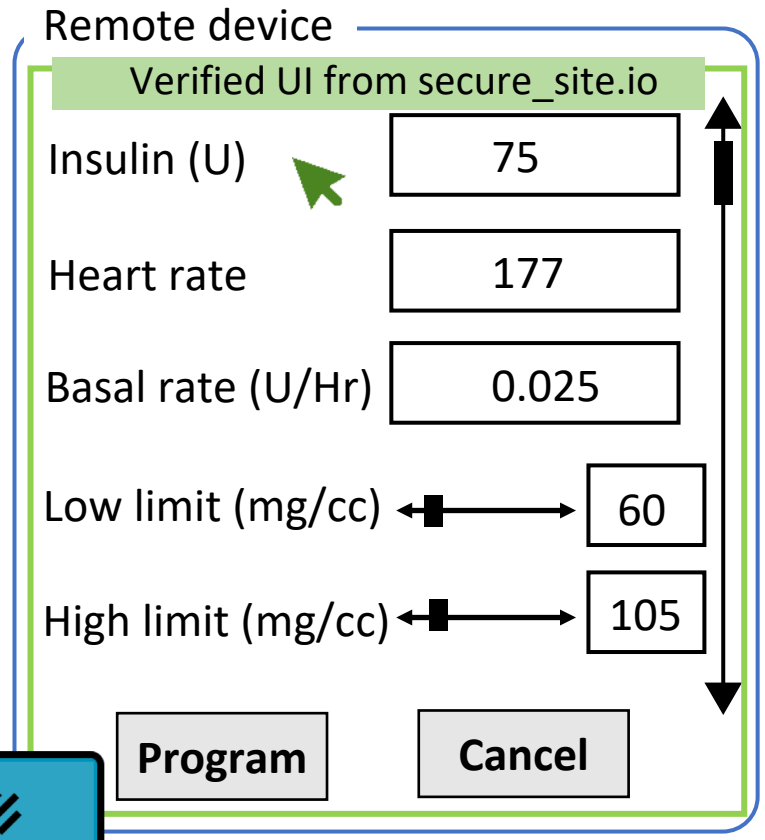


IO Integrity – Input

Simultaneous IO







Grabbing 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

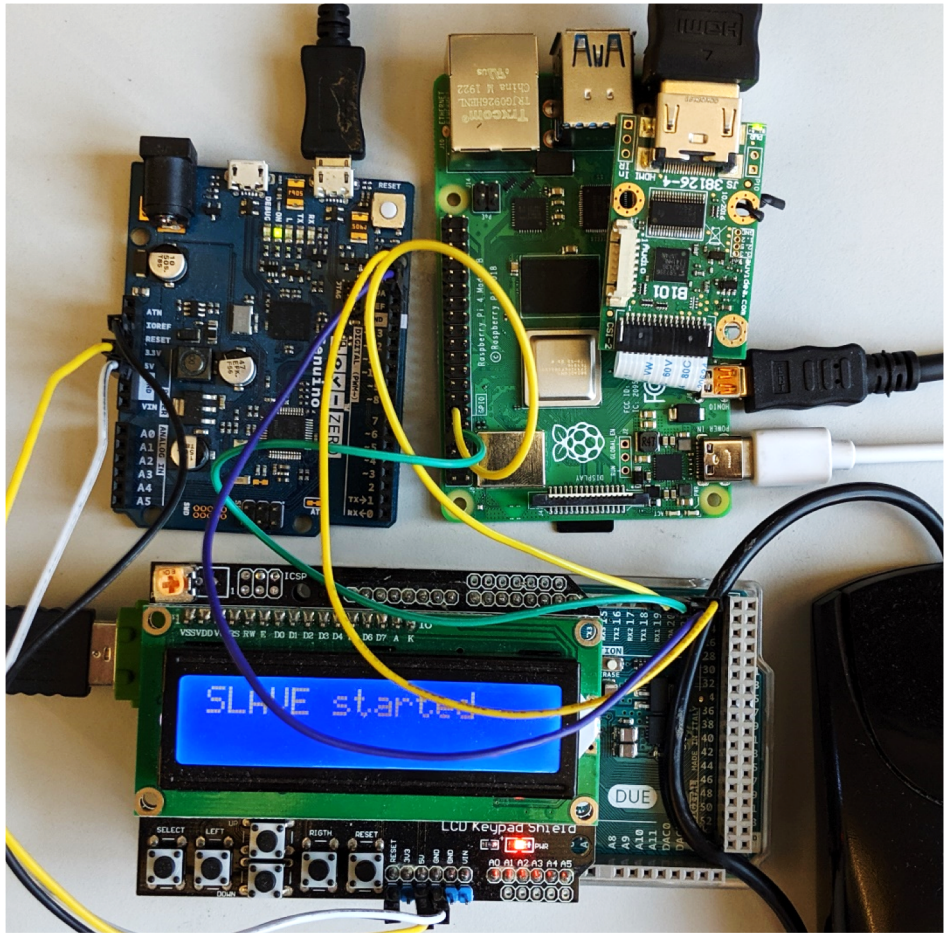
Put 1 in front of all inputs

Grabbing User Attention

Low cognitive load

- Output Integrity: Low cognitive load
- Several existing mechanisms
  - Lightbox
  - Highlight
  - Freezing
  - Combination
- How to determine when to engage?
  - Track pointer
  - Mouse movement on the overlay

Prototype and TCB



Low TCB

Fast deployment

25.16M

20.92M

2M

71K

600K

36.68M

HDMI

1.9K

256

3.5K

893

121K

Performance

- Display latency: 21.67 ms
  - ~46 fps
- Mouse latency: 250 μs
- Keyboard latency: 170 μs
- Pointer detection accuracy: 0.997

Summary

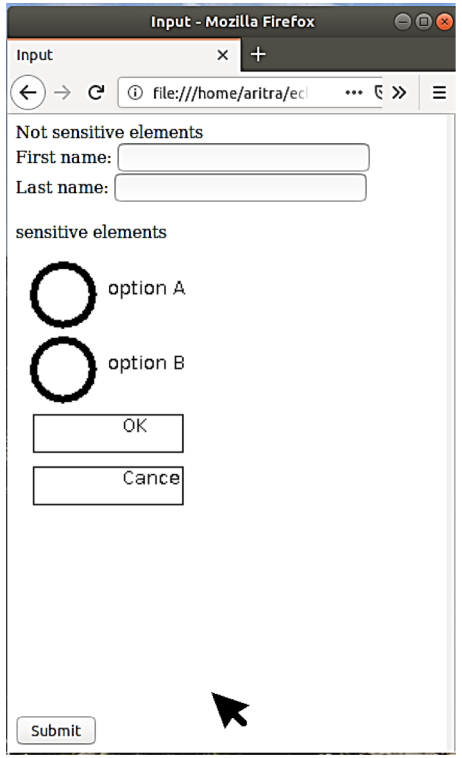
- Existing research
  - Drawbacks
  - Observations
- Requirements for Trusted Path
- ProtectIOn design
- Prototype

Thank you! Questions?

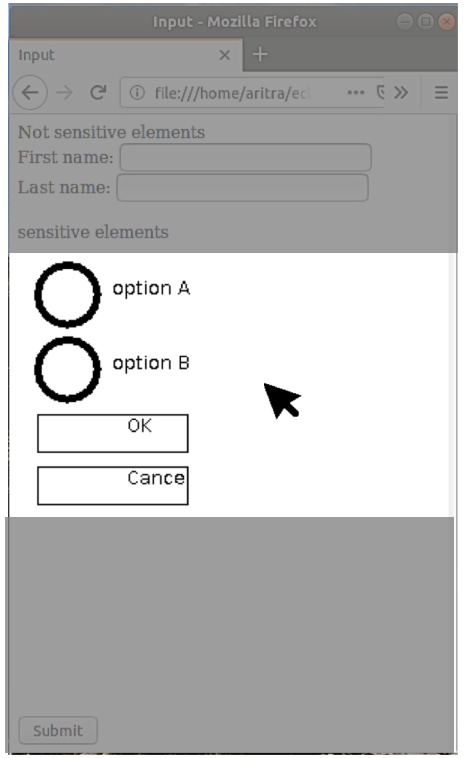
Backup slides

Prototype View

Attacker's view



User's view on the monitor



Focusing user's attention

Other Trusted Path Solutions

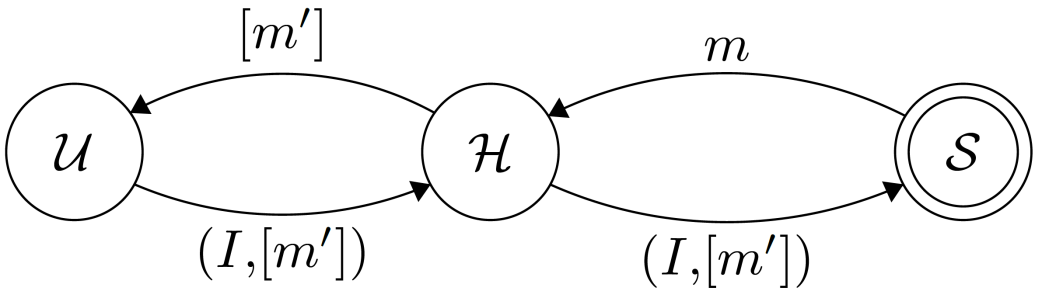
Security Requirements		R4				R1 R2				R3a/b
		Trust Assumption				IO Security Features				Usability
		Hardware		Software		Input			Output	
Category	Solutions	Requires TEE	External trusted HW	Isolated API/Drivers	Hypervisor/ OS	Keyboard	Pointer	Touch	Display	No SI / PnP
Hypervisor/OS-based	Shadowcrypt [29]			✔	✔		✔			✔
	Browser-based [30]			✔	✔				❑	✔
	InContext [16]				✔		✔			✔
	Overshadow [16]				✔					
	Virtual ghost [31]				✔					
	TrustVisor [32]				✔					
	Inktag [33]				✔					
	Splitting interfaces [34]				✔	✔			✔	
	SP^3 [35]				✔	✔				
TEE-based	SGX IO [4]	✔		✔	✔	✔				
	SchrodinText [36]	✔			✔				✔	
	BASTION-SGX [37]	✔				✔				✔
	Slice [38]	❑								
	TrustOTP [39]	✔				✔			❑	✔
	VeriUI [40]	✔		✔		❑			❑	
	AdAttester [41]	✔		✔				❑	❑	
	TruZ-Droid [15]	✔		✔		✔			❑	✔
	TrustUI [42]	✔		❑				❑	❑	✔
	VButton [14]	✔		✔		❑		✔	✔	
External HW	CARMA [43]	✔	✔							✔
	PROXIMITEE [11]	✔	✔	❑		✔				✔ ✔
	Fidelius [9]	✔	✔	✔		✔			❑	
	FPGA-based [44]		✔			✔			✔	
	IntegriKey [8]		✔	❑		❑				✔ ✔
	Terra [45]		✔	❑						

How to Build a Trusted Path

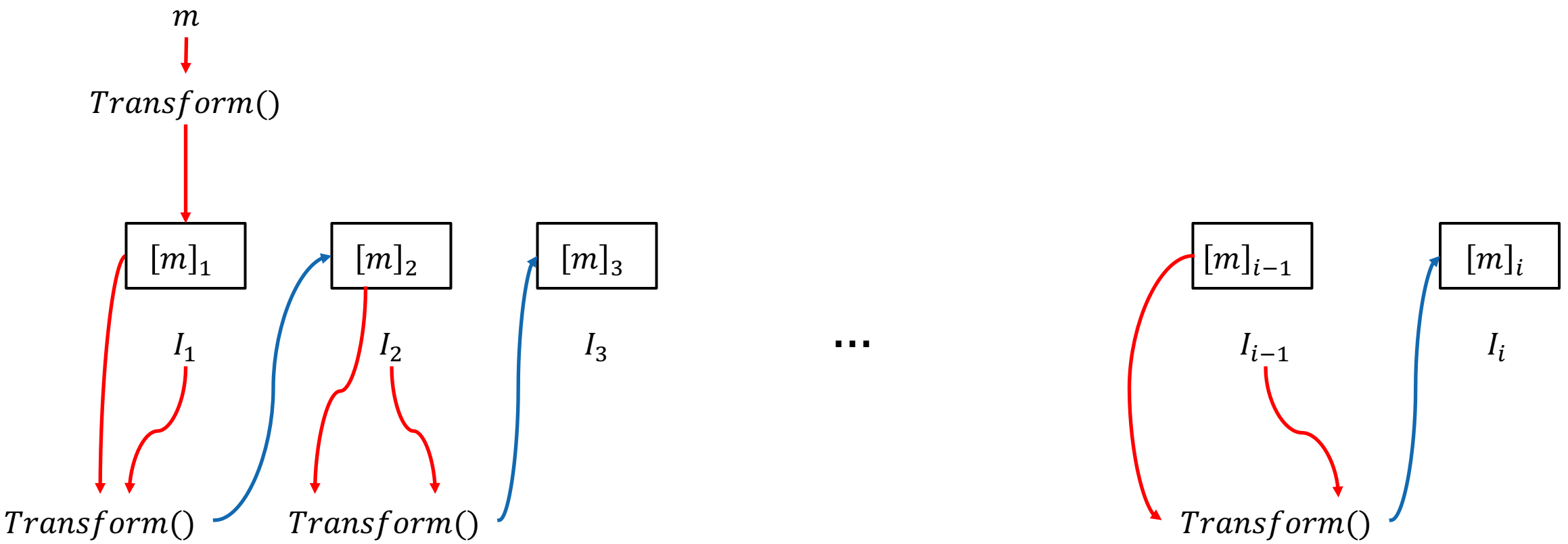
- Server sends messages : HTML, JS … → m
- All modalities of inputs → I
  - $Input(\quad) \rightarrow [m] \rightarrow I$
- Host transforms them : Browser, GPU … + I → $[m]$
  - $Transform(\quad): m, I \rightarrow [m]$
- Host is a bad guy → $[m]$ or $[m']$
- Output integrity → Users need to report back $[m]$ / $[m']$

Definition: Violation of Input/output Integrity

- Sever sends m
- Server knows $[m]$
- Given $[m]$, correct input is I
- Host sends $[m'] \neq [m]$ Output integrity
- User sends $I' \neq I$ Input integrity



Verification



Anything missing in the chain → IO integrity violation

Overlay: Output Manipulation