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
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

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
Solution 2: Input Signing

Remote device

Heart beat 75

Insulin 177U

Basal rate 0.025 U/Hr

Low limit 60 mg/dL

High limit 105 mg/dL

High limit (mg/dL) 105

Program

Cancel

Trusted embedded device

Heart beat 75

Insulin 177U

Basal rate 0.025 U/Hr

Low level 60 mg/dL

High level 105 mg/dL
Display manipulation attack

User sees 177

Device records 1777

Host sends 1777

• IntegriKey

Insulin

17

177

1777

177

7
Observation 1

The lack of output integrity – the render of user inputs on the screen – compromises input integrity.
Solution 3: Overlay

Remote device
Heart beat
Insulin (U)
Basal rate (U/Hr)
Low limit (mg/dL)
High limit (mg/dL)

Program Cancel

Remote device
Heart beat
Insulin (U)
Basal rate (U/Hr)
Low limit (mg/dL)
High limit (mg/dL)

Program Cancel

Heart beat: 75
Insulin (U): 177
Basal rate (U/Hr): 0.025
Low limit (mg/dL): 60
High limit (mg/dL): 105
Overlay: Output Manipulation

Remote device
Heart beat
Insulin (U)
Basal rate (U/Hr)
Low limit (mg/dL)
High limit (mg/dL)
Program
Cancel

Remote device
Insulin (U)
Heart rate
Basal rate (U/Hr)
Low limit (mg/cc)
High limit (mg/cc)
Program
Cancel
Overlay: Output Manipulation

Remote device

- Insulin (U): 177
- Heart rate: 75
- Basal rate (U/Hr): 0.025
- Low limit (mg/cc): 6000
- High limit (mg/cc): 10500

Program  Cancel
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

Remote device

- Heart beat: 75
- Insulin (U): 17
- Basal rate (U/Hr): 0.025
- Low limit (mg/dL): 60
- High limit (mg/dL): 105

• 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

Remote device

- Insulin (U)
- Heart rate
- Basal rate (U/Hr)
- Low limit (mg/cc)
- High limit (mg/cc)

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

Program
Cancel

Simultaneous IO
IO Integrity – Overlay Generation

Simultaneous IO
IO Integrity – Overlay Generation

Remote device
Verified UI from secure_site.io

Insulin (U)
Heart rate
Basal rate (U/Hr)
Low limit (mg/cc)
High limit (mg/cc)

Simultaneous IO
IO Integrity – Input

Remote device

Verified UI from secure_site.io

- Insulin (U): 75
- Heart rate: 177
- Basal rate (U/Hr): 0.025
- Low limit (mg/cc): 60
- High limit (mg/cc): 105

Simultaneous IO
Grabbing User Attention

- Output Integrity: Low cognitive load
- Several existing mechanisms

Put 1 in front of all inputs
Grabbing User Attention

- Output Integrity: Low cognitive load

- Several existing mechanisms
  - Lightbox

Put 1 in front of all inputs
Grabbing User Attention

- Output Integrity: Low cognitive load

- Several existing mechanisms
  - Lightbox
  - Highlight

Put 1 in front of all inputs
Grabbing User Attention

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

Put 1 in front of all inputs
Grabbing User Attention

- Output Integrity: Low cognitive load

- Several existing mechanisms
  - Lightbox
  - Highlight
  - Freezing
  - Combination

Put 1 in front of all inputs
Grabbing User Attention

- 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

1.9K
3.5K
893
121K
Performance

- Display latency: 21.67 ms
  - ~46 fps
- Mouse latency: 250 $\mu$s
- Keyboard latency: 170 $\mu$s
- 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](image1)

![User's view on the monitor](image2)

![Focusing user's attention](image3)
## Other Trusted Path Solutions

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>R1 (Input)</th>
<th>R2 (Output)</th>
<th>R3a/b (Usability)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
<td>Hardware</td>
<td>Software</td>
<td>Hypervisor/OS</td>
</tr>
<tr>
<td></td>
<td>Requires TEE</td>
<td>Isolated API/Drivers</td>
<td></td>
</tr>
<tr>
<td><strong>Solutions</strong></td>
<td>External trusted HW</td>
<td>Hypervisor/OS</td>
<td></td>
</tr>
<tr>
<td>Shadowcrypt [29]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Browser-based [30]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>InContext [16]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Overshadow [16]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Virtual ghost [31]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>TrustVisor [32]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Inhtag [33]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Splitting interfaces [34]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Strö [35]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>SGX IO [4]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>SchrodinText [36]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>BASTION-SGX [37]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Slice [38]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>TrustOTP [39]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>VeriUI [40]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>AdAttester [41]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>TrustZ-Droid [15]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>TrustUI [42]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>VButton [43]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>CARMA [43]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>PROXIMITEE [111]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Fidelius [9]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>FPGA-based [44]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>IntegriKey [8]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Terra [45]</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
How to Build a Trusted Path

- Server sends messages: HTML, JS … → $m$
- All modalities of inputs → $I$
  - $Input(\cdot) \rightarrow [m] \rightarrow I$
- Host transforms them: Browser, GPU … + $I \rightarrow [m]$
  - $Transform(\cdot): m, I \rightarrow [m]$
- 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 $\rightarrow$ IO integrity violation
Overlay: Output Manipulation

Remote device

- Insulin (U): 177
- Heart rate: 75
- Basal rate (U/Hr): 0.025
- Low limit (mg/cc): 6000
- High limit (mg/cc): 10500

Program  Cancel