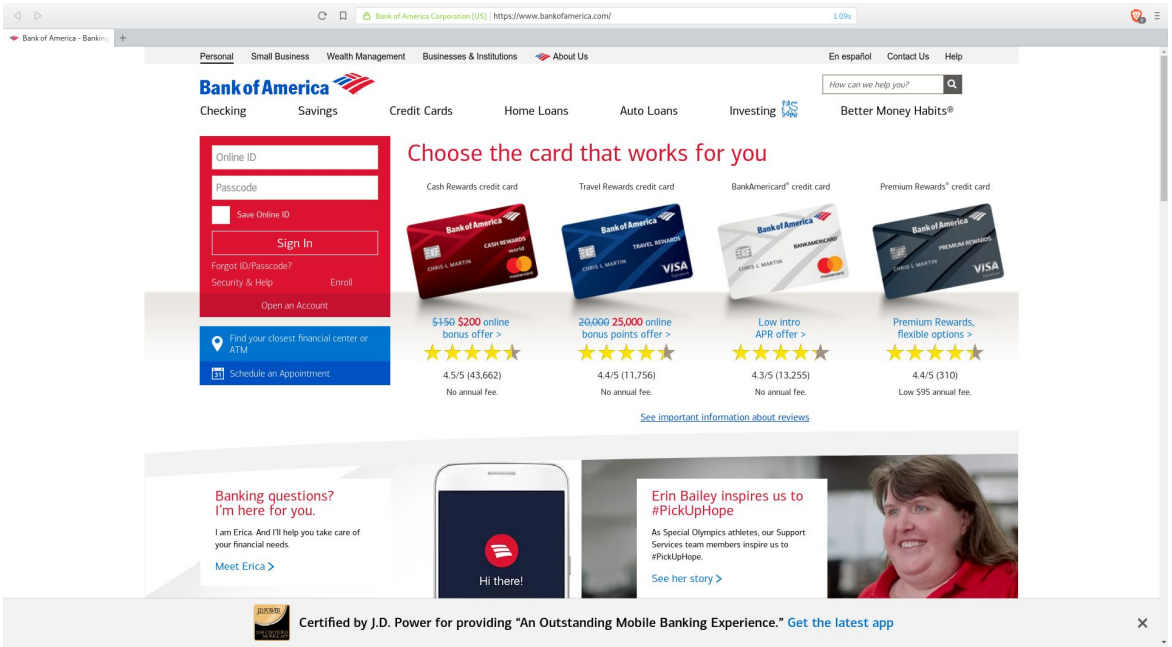
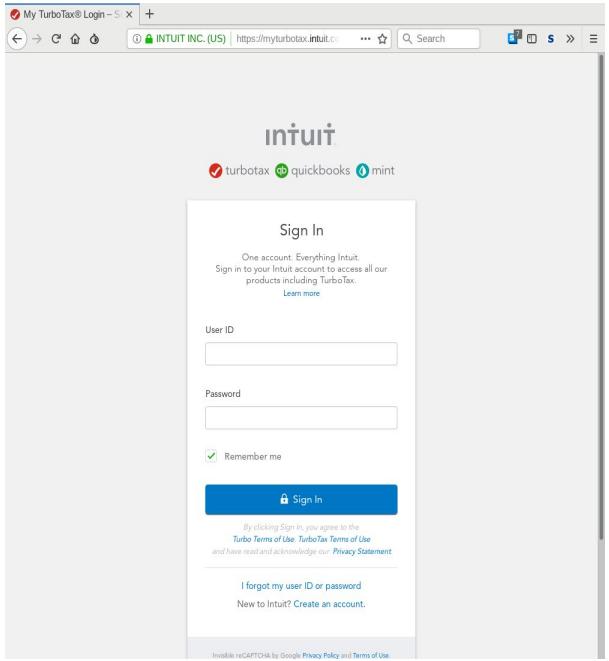
Fidelius: Protecting User Secrets from Compromised Browsers

Saba Eskandarian, Jonathan Cogan, Sawyer Birnbaum, Peh Chang Wei Brandon, Dillon Franke, Forest Fraser, Gaspar Garcia, Eric Gong, Hung T. Nguyen, Taresh K. Sethi, Vishal Subbiah, Michael Backes, Giancarlo Pellegrino, Dan Boneh

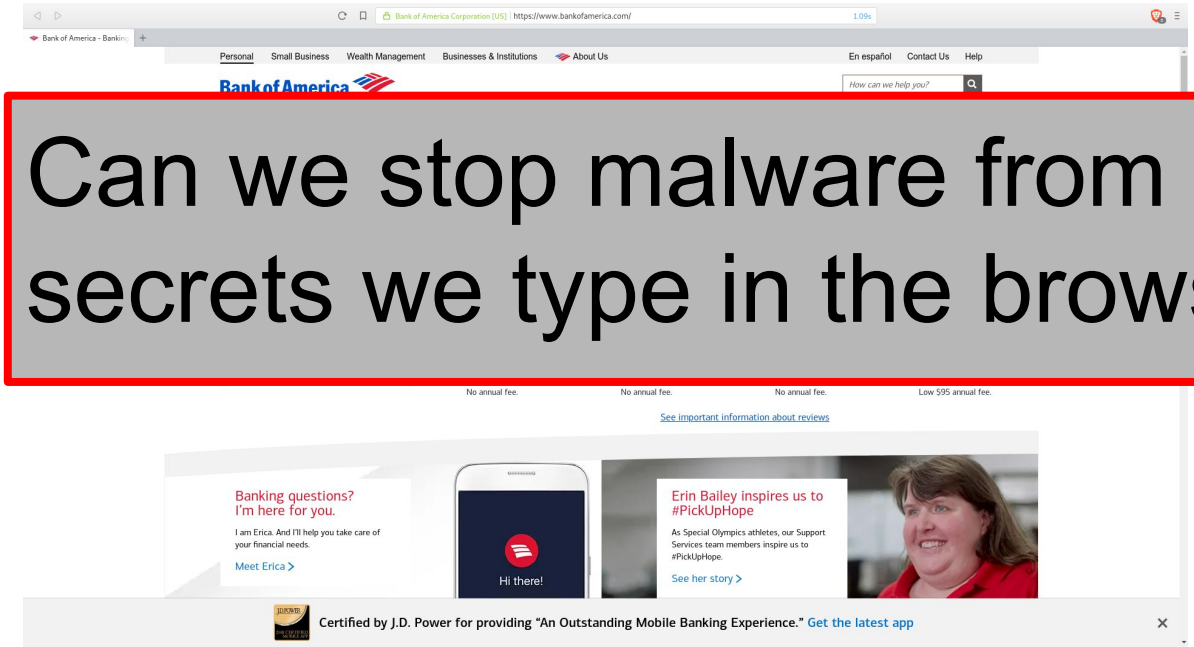
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

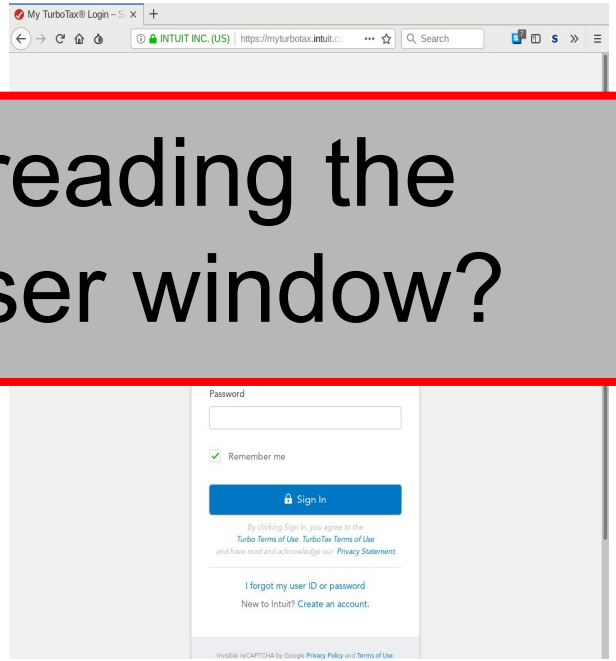
In Browsers we Trust





In Browsers we Trust



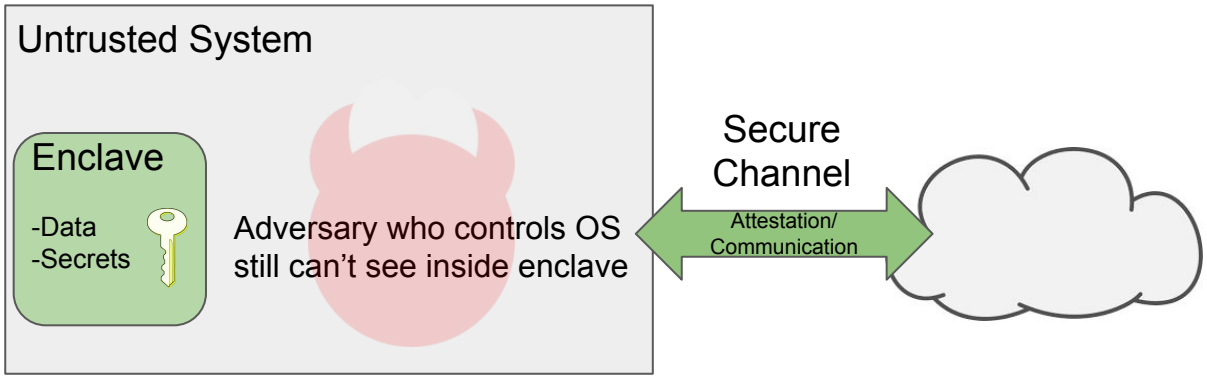


Can we stop malware from reading the secrets we type in the browser window?

Hardware Enclaves

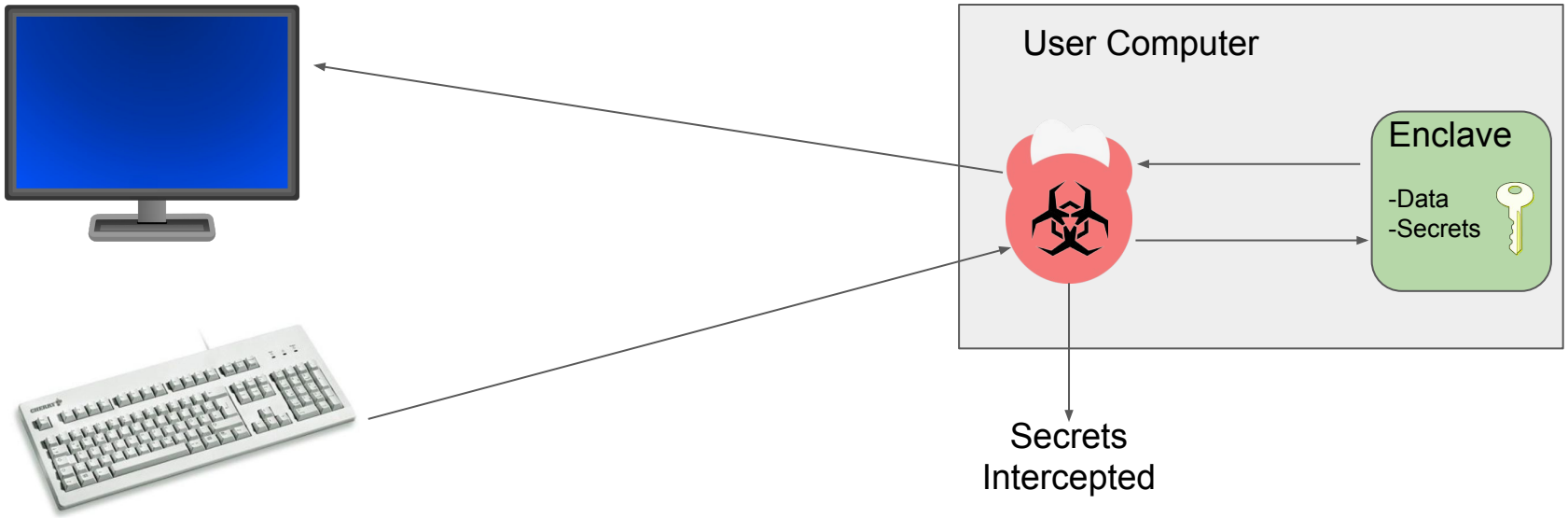
A trusted component in an untrusted system

- Protected memory isolates enclave from compromised OS
- Proves authenticity via *attestation*
- Enclaves in our implementation use Intel SGX



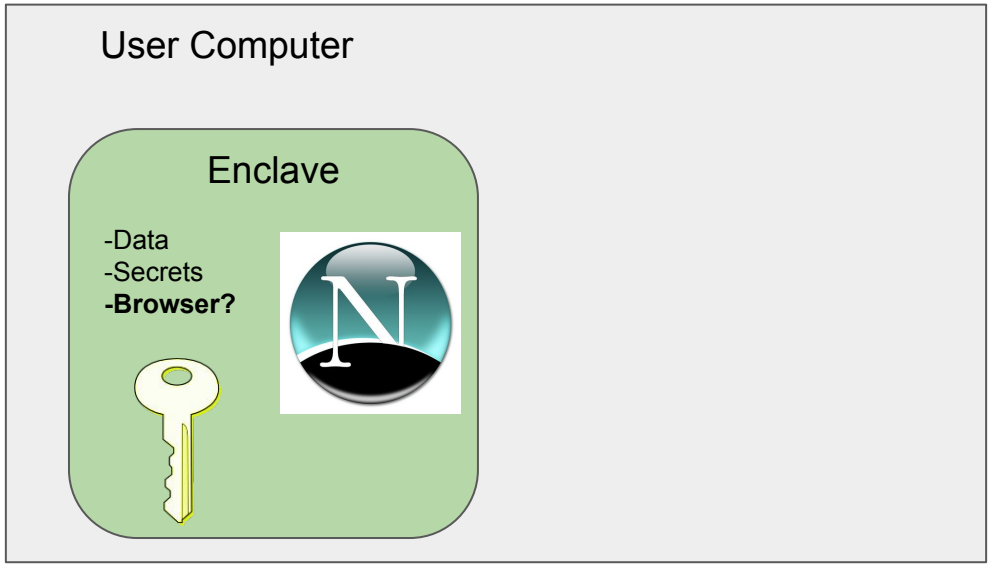
Challenges

1. Enclave only interacts with outside world through OS



Challenges

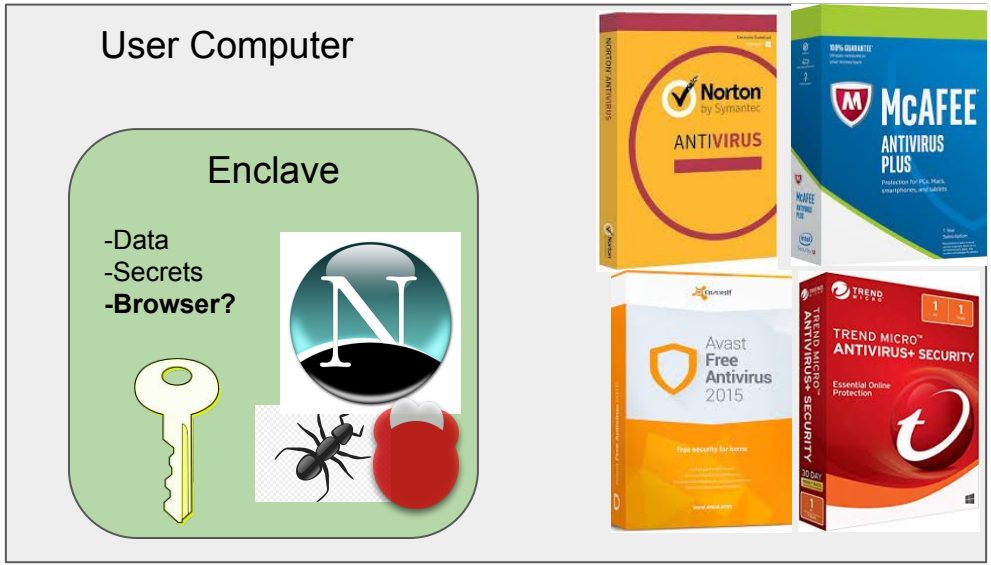
2. Browsers have a LOT of code and many bugs/vulnerabilities.



Challenges

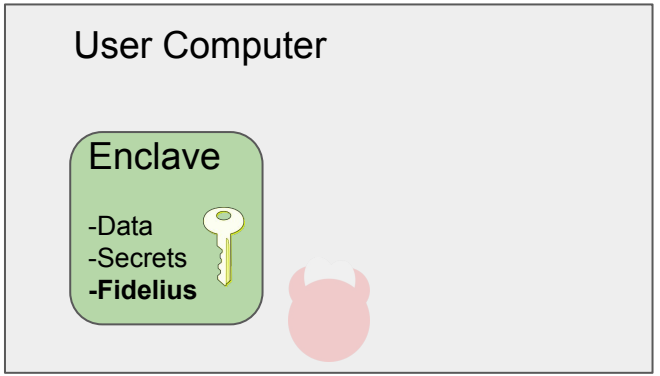
2. Browsers have a LOT of code and many bugs/vulnerabilities.

   Vulnerable code in enclave → super-malware!



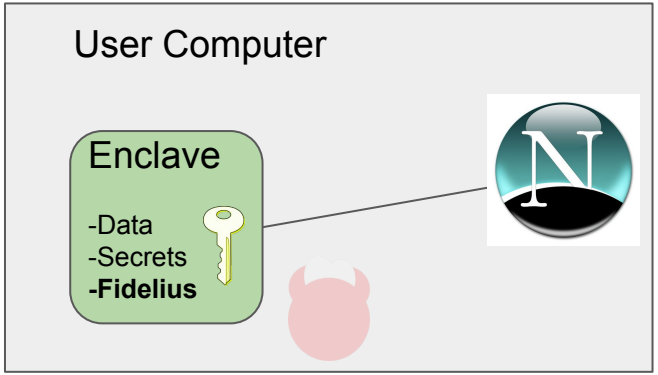
The Fidelius System

Goal: protect user keyboard inputs to browser from fully compromised OS



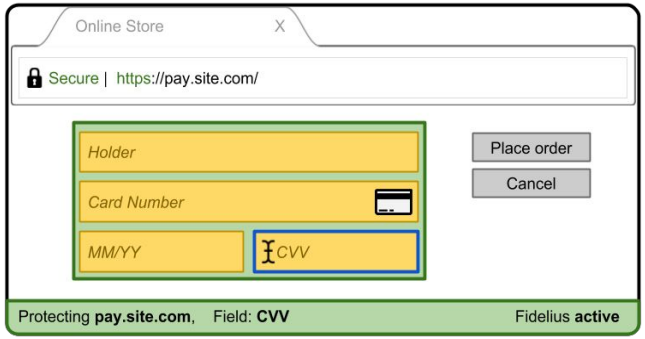
The Fidelius System

Keeps browser outside of hardware enclave

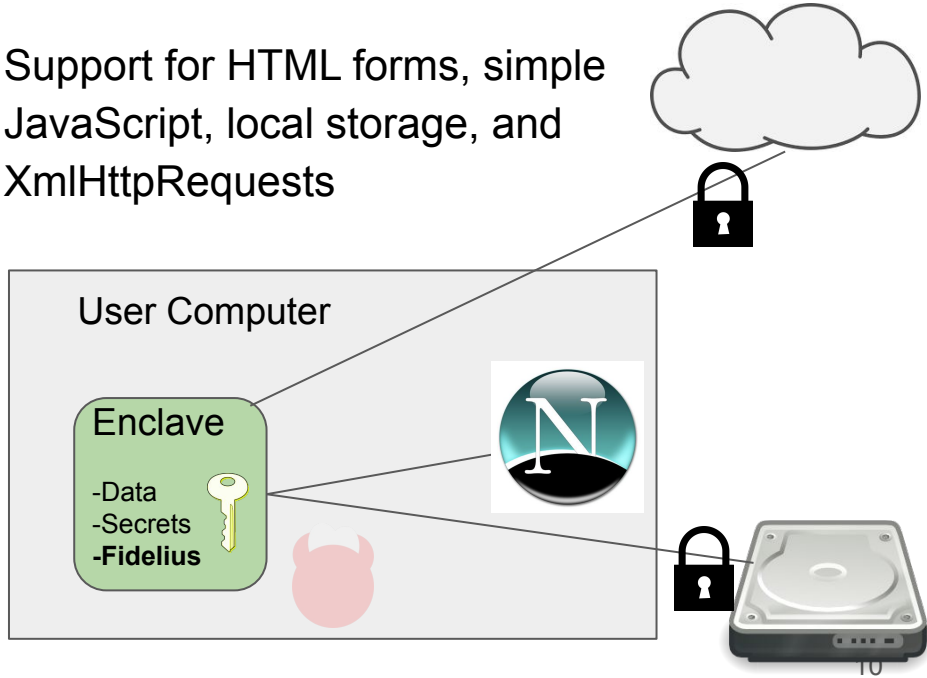


Related earlier approach: Microsoft Palladium...

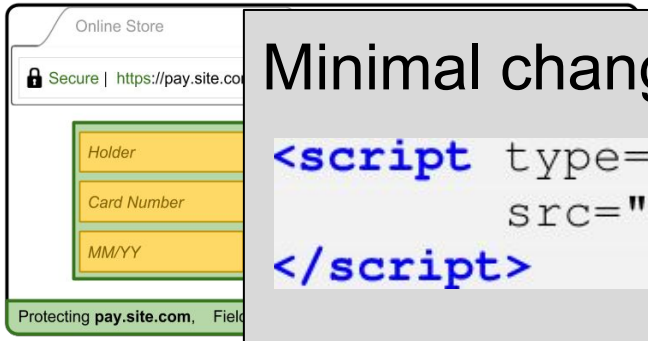
The Fidelius System



Support for HTML forms, simple JavaScript, local storage, and XmlHttpRequests



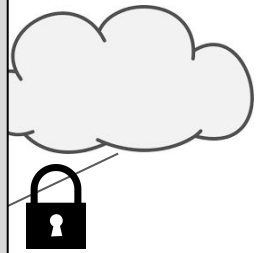
The Fidelius System



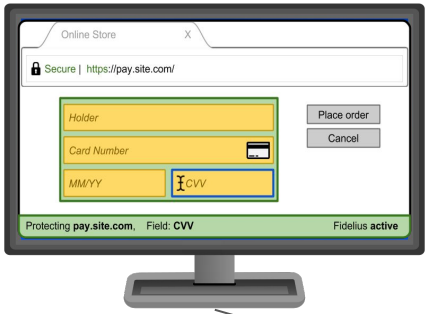
Minimal changes for developers

```
<script type="text/JavaScript"
        src="validator.js"
</script>
```

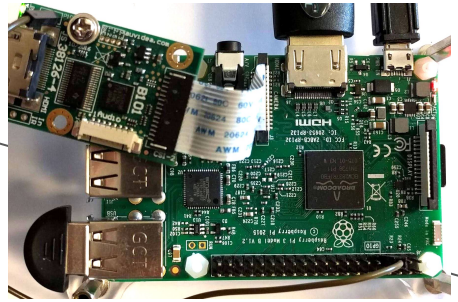
```
<script type="text/JavaScript"
        src="validator.js"
        secure="True" sign="Fi3Rt9mq2ff0">
</script>
```

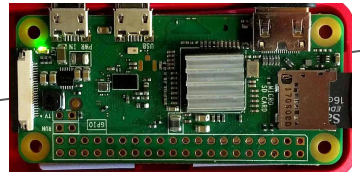


The Fidelius System



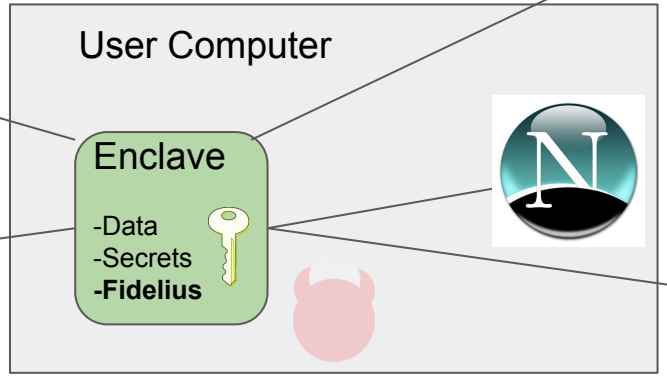
Trusted path from enclave to secure I/O devices





Minimal changes for developers

```
<script type="text/JavaScript"
        src="validator.js"
        secure="True" sign="Fi3Rt9mq2ff0">
</script>
```



Trusted Path to/from Enclave

Keyboard/display dongles built from Raspberry PIs

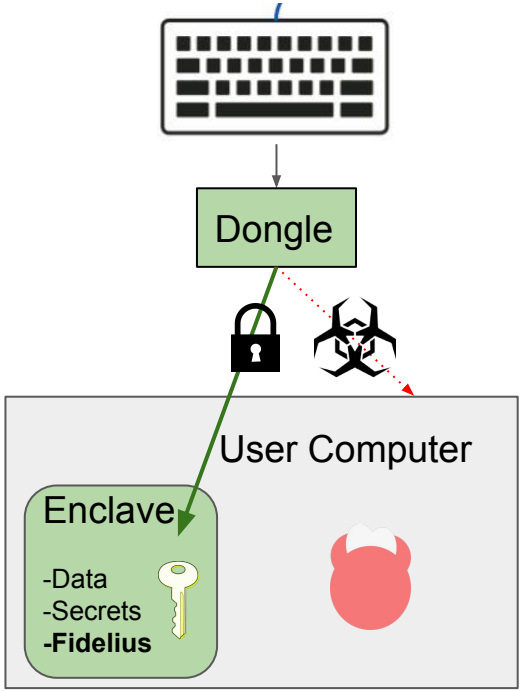
Dongles switch between trusted/untrusted modes

Trusted Path to/from Enclave

Keyboard/display dongles built from Raspberry PIs

Dongles switch between trusted/untrusted modes

Keyboard: encrypt keystrokes at constant rate



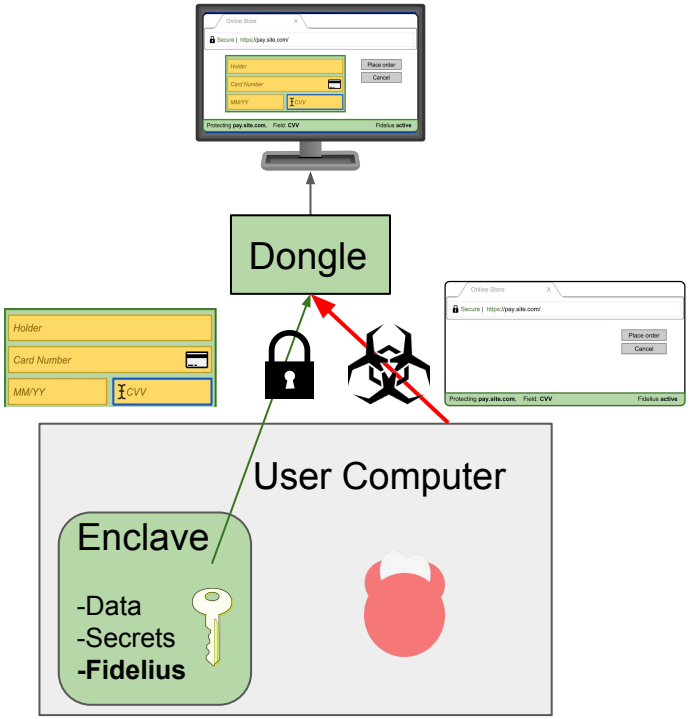
Trusted Path to/from Enclave

Keyboard/display dongles built from Raspberry PIs

Dongles switch between trusted/untrusted modes

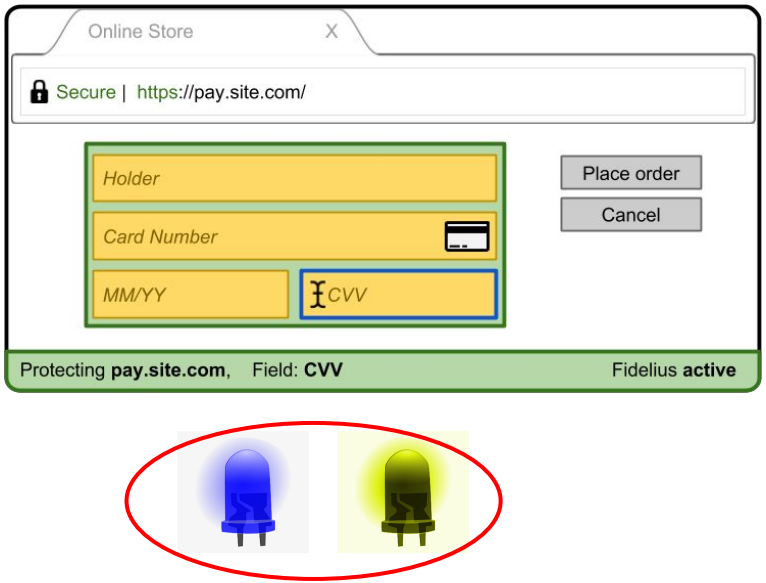
Keyboard: encrypt keystrokes at constant rate

Display: decrypt overlays sent by enclave



Fidelius for Users

Security indicator lights for keyboard and display



Schechter and Dhamija, The Emperor's New Security Indicators. S&P 2007.

Whalen and Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers. GI 2005.

Fidelius for Users

Security indicator lights for keyboard and display

Green overlay verifies who gets data and what data you are giving

Schechter and Dhamija, The Emperor's New Security Indicators. S&P 2007.
Whalen and Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers. GI 2005.

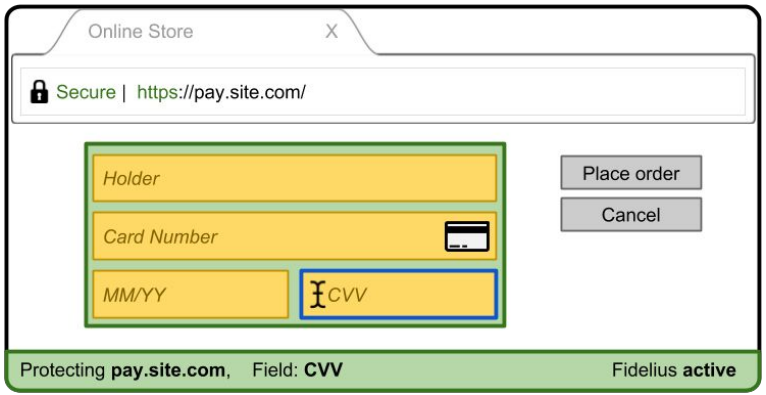
Fidelius for Users

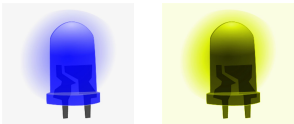
Security indicator lights for keyboard and display

Green overlay verifies who gets data and what data you are giving

Security relies on users watching

indicators (in our prototype)

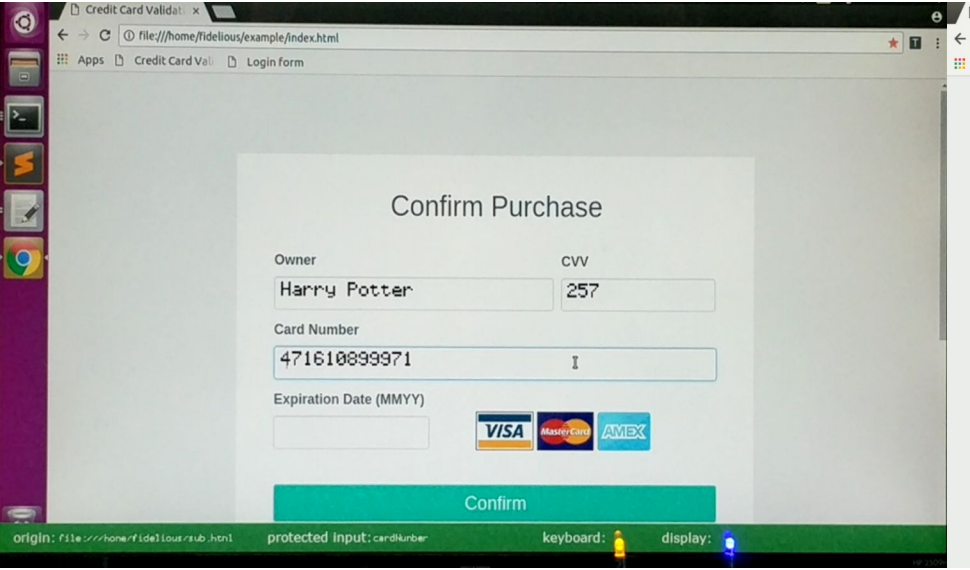




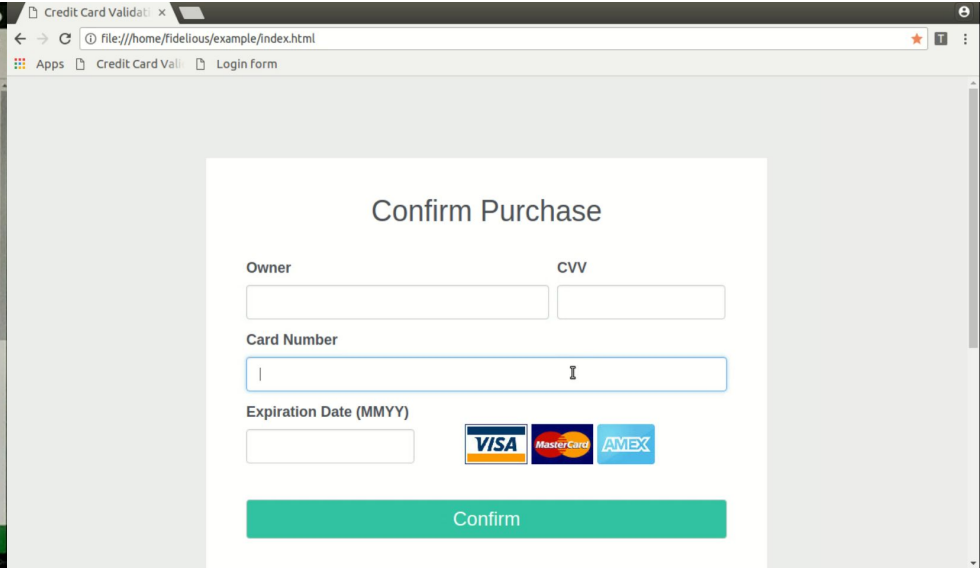
Schechter and Dhamija, The Emperor's New Security Indicators. S&P 2007.
Whalen and Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers. GI 2005.

Example

User view (photograph)



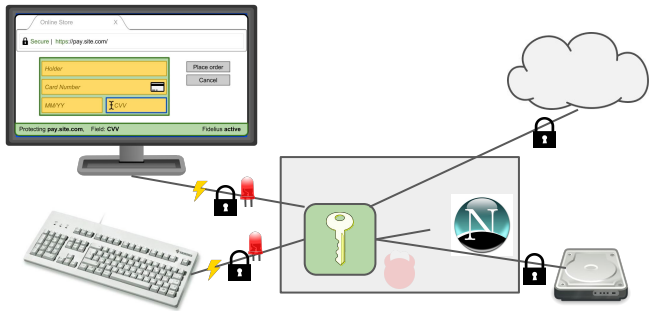
Malware view (screen capture)



See video demo at https://crypto.stanford.edu/fidelius

What Fidelius Does

- Secure user I/O against tampering, eavesdropping, replay, etc.
- Give trusted Javascript local access to sensitive data
- Only allow data to be sent to designated destination

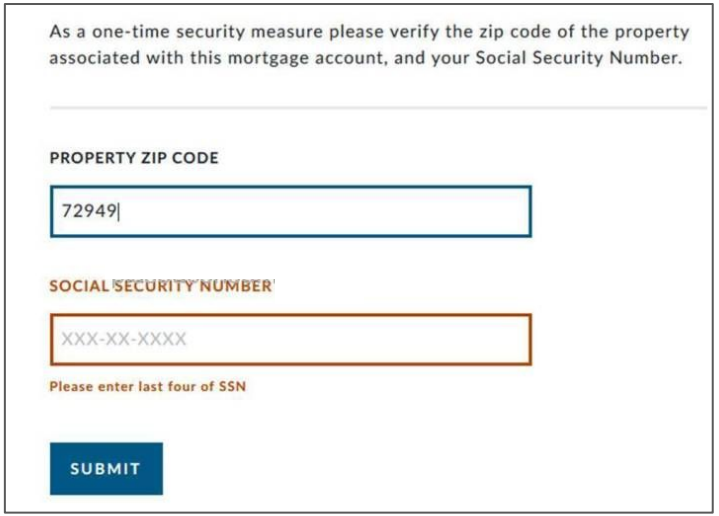


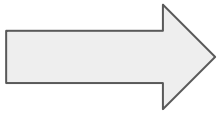
What Fidelius Does Not Do

- Secure hardware enclave against side-channel attacks
  [XCP’15,GESM’17,BMD+’17,WKPK’17,LSG+’17,CCX+’18,BMW+’18]

What Fidelius Does Not Do

- Secure hardware enclave against side-channel attacks
  [XCP'15,GESM'17,BMD+'17,WKPK'17,LSG+'17,CCX+'18,BMW+'18]
- Protect against dumb web sites





Performance

TCB: ~8,500 lines of C++

Performance

TCB: ~8,500 lines of C++

Field size(s)	W	H	W×H px	Time (ms)	Incr. (ms)
1 Small	171	50	8,550	195.83	-
1 Medium	342	50	17,100	199.20	3.38
1 Large	683	50	34,150	209.65	10.45
1 Extra large	911	50	45,550	214.74	-
2 Extra large	911	100	91,100	227.02	12.28

Display Latency Scaling

Doubling trusted display size only slightly increases display latency

Performance

TCB: ~8,500 lines of C++

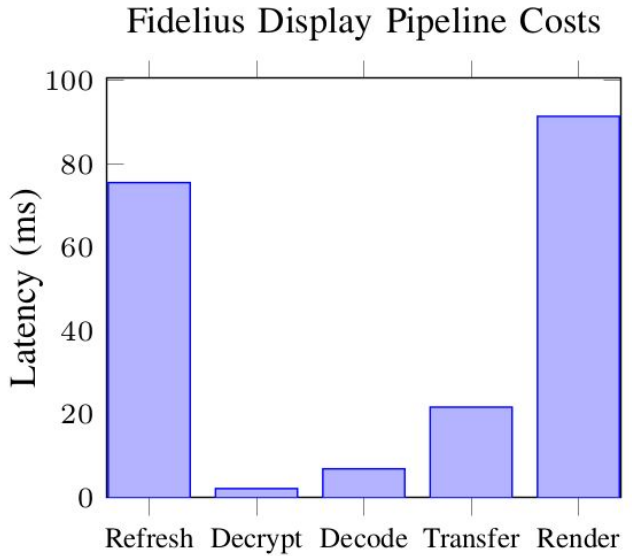
Field size(s)	W	H	W×H px	Time (ms)	Incr. (ms)
1 Small	171	50	8,550	195.83	-
1 Medium	342	50	17,100	199.20	3.38
1 Large	683	50	34,150	209.65	10.45
1 Extra large	911	50	45,550	214.74	-
2 Extra large	911	100	91,100	227.02	12.28

Display Latency Scaling

Doubling trusted display size only slightly increases display latency

Display Bottlenecks

Expensive Render/Refresh due to implementation hacks, easily improvable



Performance

TCB: ~8,500 lines of C++

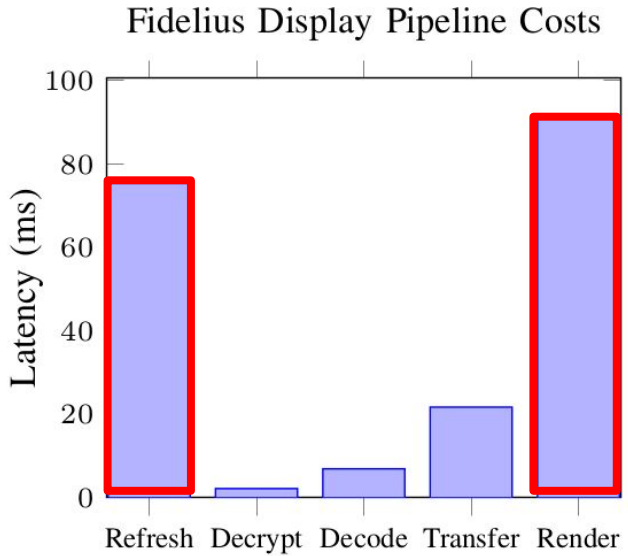
Field size(s)	W	H	W×H px	Time (ms)	Incr. (ms)
1 Small	171	50	8,550	195.83	-
1 Medium	342	50	17,100	199.20	3.38
1 Large	683	50	34,150	209.65	10.45
1 Extra large	911	50	45,550	214.74	-
2 Extra large	911	100	91,100	227.02	12.28

Display Latency Scaling

Doubling trusted display size only slightly increases display latency

Display Bottlenecks

Expensive Render/Refresh due to implementation hacks, easily improvable



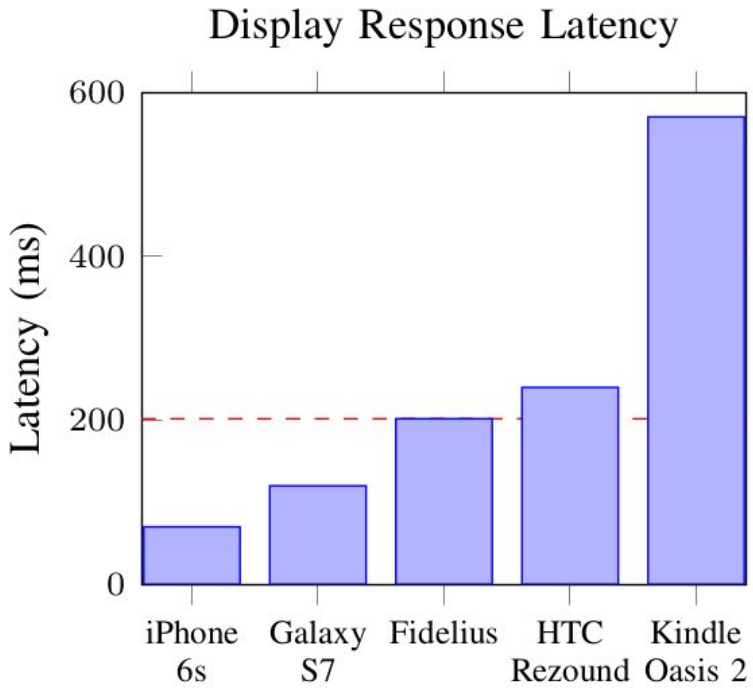
Performance

Display Latency

(Unoptimized) refresh rate 2.8x faster than latest Kindle

Speed due to only sending small overlay rather than encrypting full display

Graph shows latency for Fidelius rendering a username/password login form



Summary

Fidelius uses enclave to protect user secrets even if entire OS compromised

Support for forms, JS, persistent local storage, and XmlHttpRequests

Trusted path to enclave for user I/O (other projects welcome to use)

https://crypto.stanford.edu/fidelius
https://github.com/SabaEskandarian/Fidelius