

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



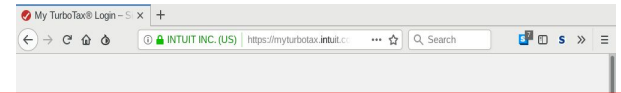
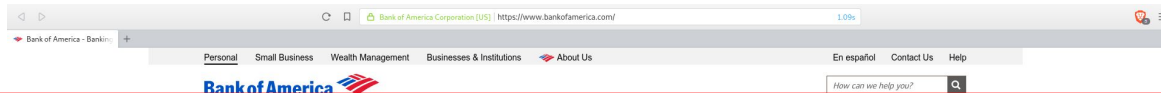
CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

In Browsers we Trust

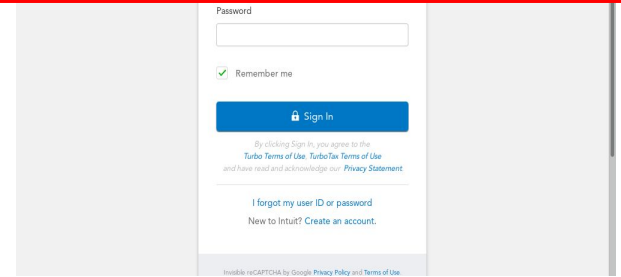
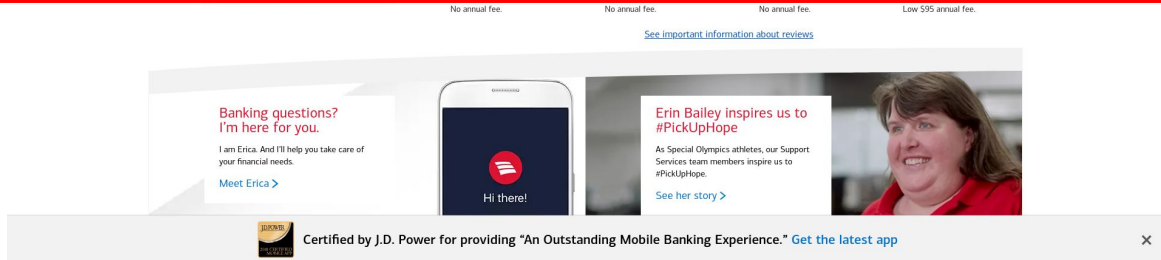
The screenshot shows the Bank of America website. At the top, there is a navigation bar with links for Personal, Small Business, Wealth Management, Businesses & Institutions, and About Us. Below this is the Bank of America logo and a search bar. The main content area features a login form on the left with fields for Online ID and Passcode, and a 'Sign In' button. To the right of the login form is a section titled 'Choose the card that works for you' which displays four credit card options: Cash Rewards, Travel Rewards, BankAmericard, and Premium Rewards. Each card is accompanied by an image, a star rating, and a brief description of its benefits. Below the cards is a link to 'See important information about reviews'. At the bottom of the page, there is a promotional banner for Erin Bailey, a Special Olympics athlete, with the text 'Erin Bailey inspires us to #PickUpHope' and a link to 'See her story'. A J.D. Power award logo is visible in the bottom left corner, certifying the bank for providing an outstanding mobile banking experience.

The screenshot shows the Intuit TurboTax login page. At the top, there is a navigation bar with the Intuit logo and links for TurboTax, QuickBooks, and Mint. Below this is a 'Sign In' section with a sub-header 'One account. Everything Intuit. Sign in to your Intuit account to access all our products including TurboTax.' and a link to 'Learn more'. The login form includes fields for User ID and Password, a 'Remember me' checkbox, and a 'Sign In' button. Below the button, there is a link to 'TurboTax Terms of Use' and 'Privacy Statement'. At the bottom of the page, there is a link to 'Forgot my user ID or password' and a link to 'New to Intuit? Create an account.'.

In Browsers we Trust



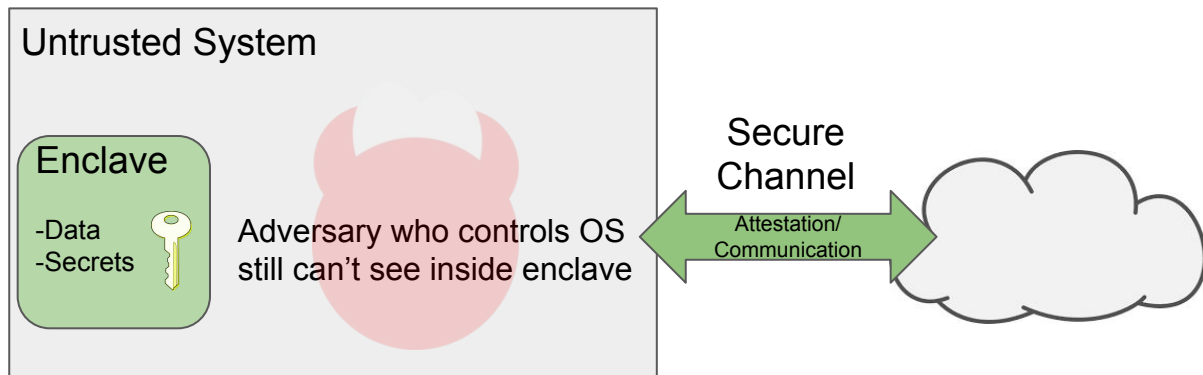
Can we stop malware from reading the secrets we type in the browser window?



Hardware Enclaves

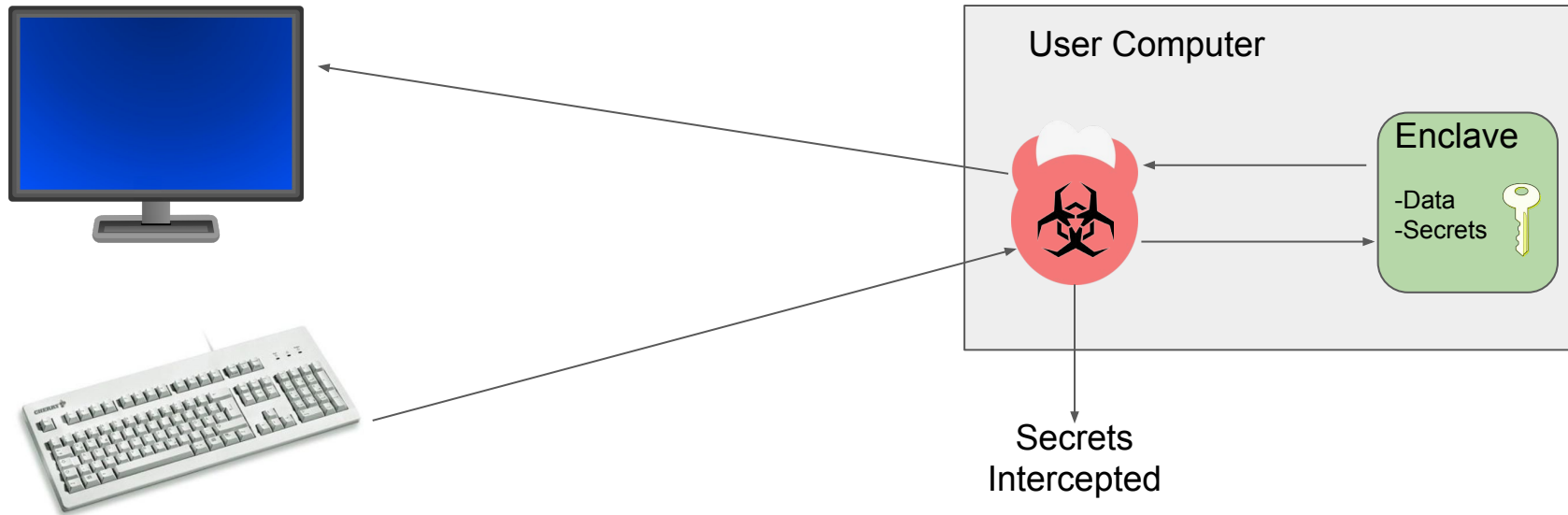
A trusted component in an untrusted system

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



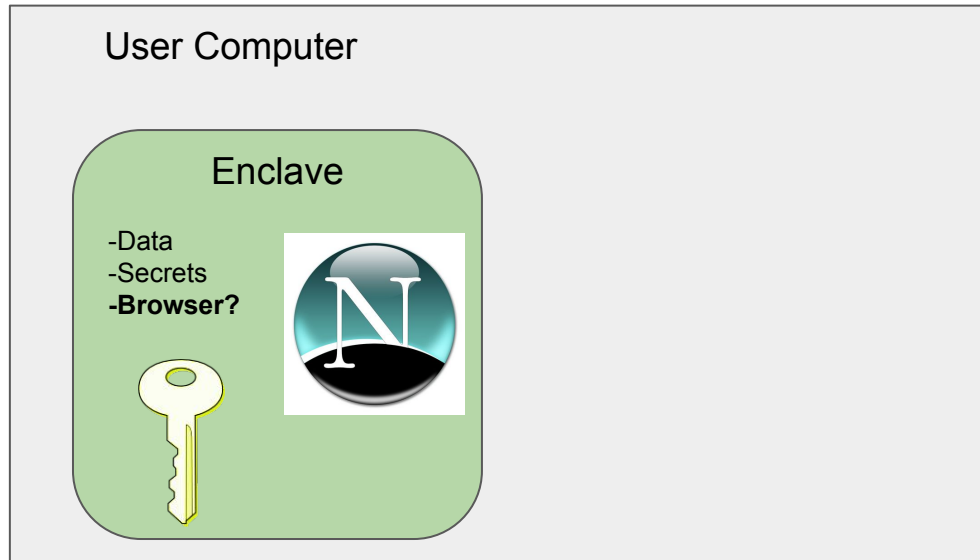
Challenges

1. Enclave only interacts with outside world through OS



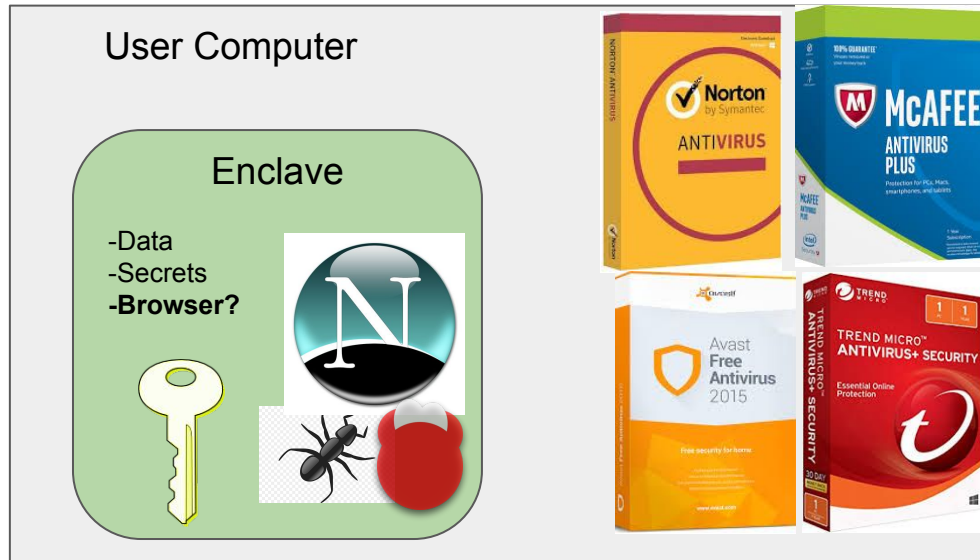
Challenges

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



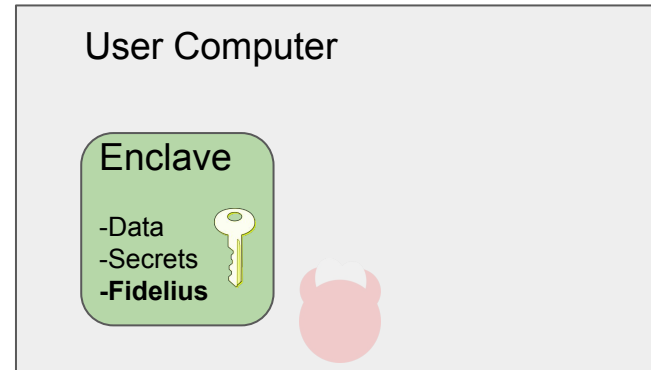
Challenges

2. Browsers have a LOT of code and many bugs/vulnerabilities.
Vulnerable code in enclave → super-malware!



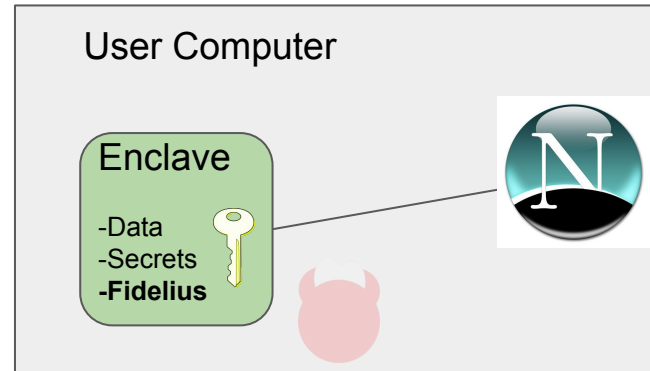
The Fidelius System

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



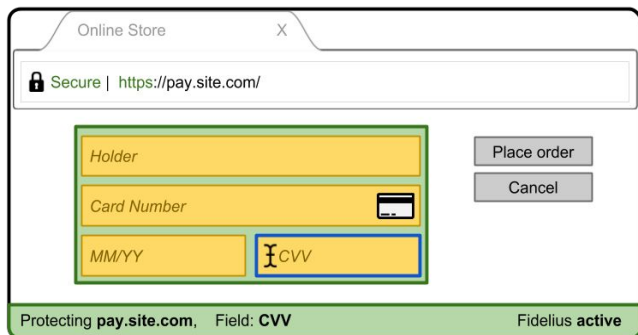
The Fidelius System

Keeps browser outside of hardware enclave

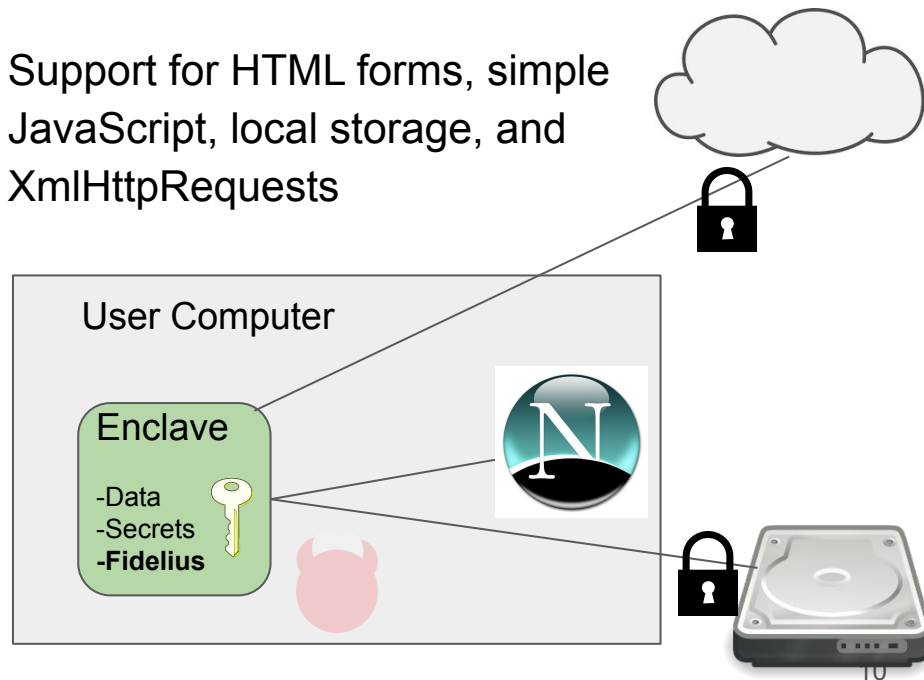


Related earlier approach: Microsoft Palladium...

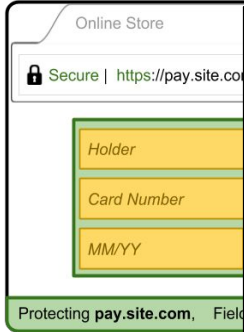
The Fidelius System



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>
```



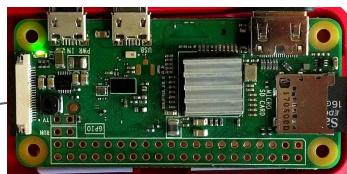
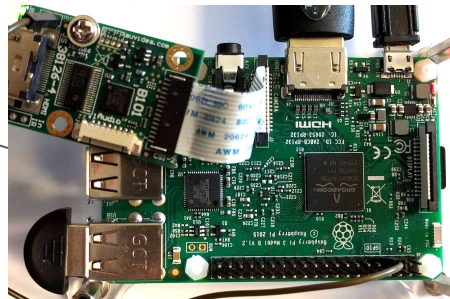
```
<script type="text/JavaScript"  
    src="validator.js"  
    secure="True" sign="Fi3Rt9mq2ff0">  
</script>
```



The Fidelius System



Trusted path from
enclave to secure
I/O devices



Minimal changes for developers

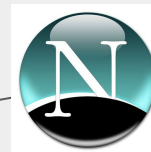
```
<script type="text/JavaScript"  
  src="validator.js"  
  secure="True" sign="Fi3Rt9mq2ff0">  
</script>
```



User Computer

Enclave

-Data
-Secrets
-Fidelius

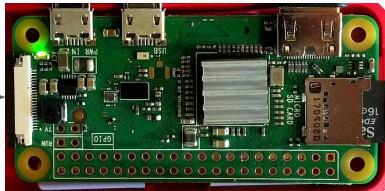
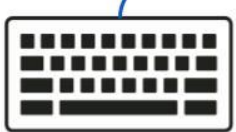


Trusted Path to/from Enclave

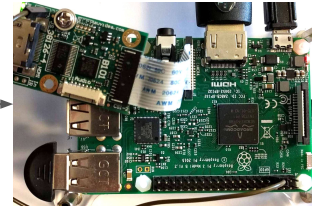
Keyboard/display dongles built from Raspberry Pis

Dongles switch between trusted/untrusted modes

Keyboard Dongle



Display Dongle

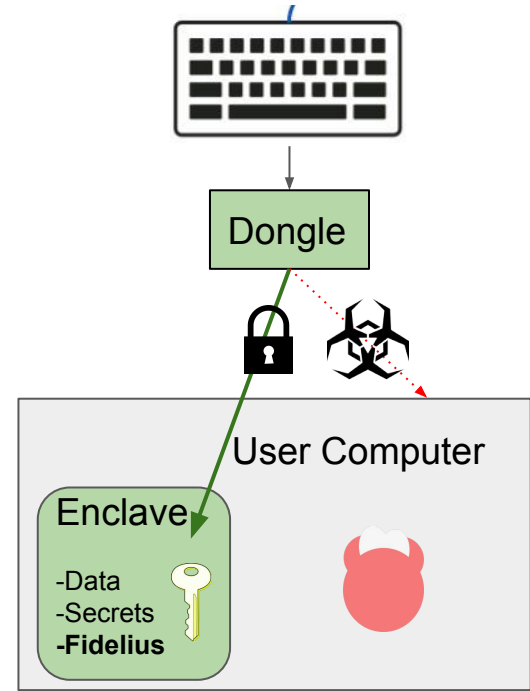


Trusted Path to/from Enclave

Keyboard/display dongles built from Raspberry Pis

Dongles switch between trusted/untrusted modes

Keyboard: encrypt keystrokes at constant rate



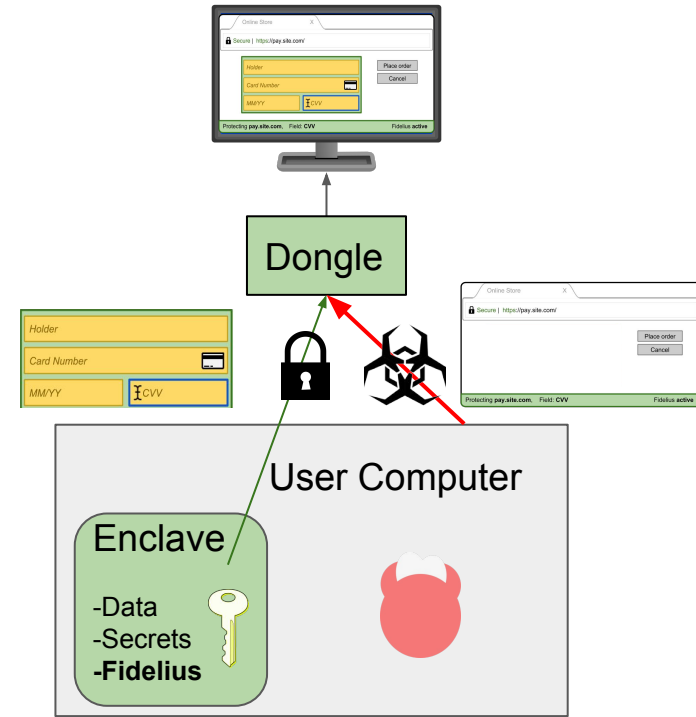
Trusted Path to/from Enclave

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



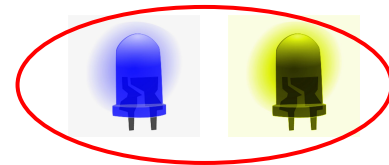
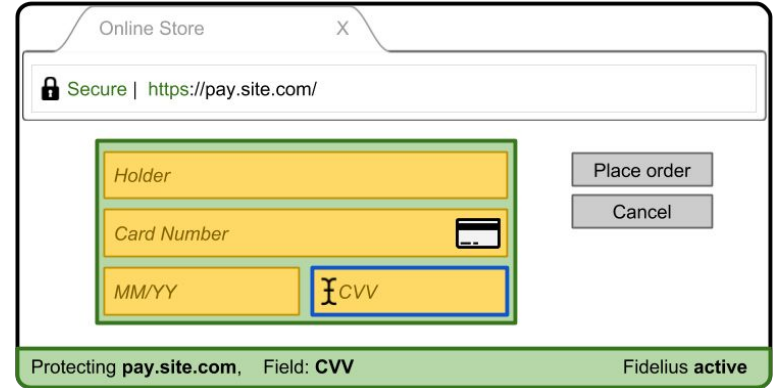
Keyboard Dongle

Display Dongle



Fidelius for Users

Security indicator lights for keyboard and display



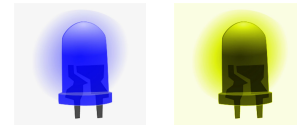
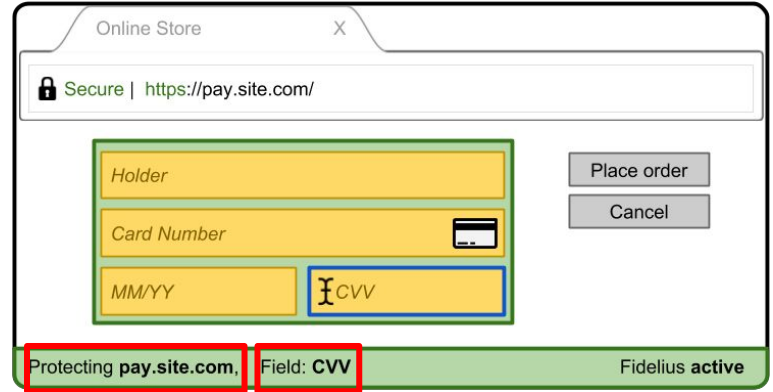
Schechter and Dhamija, The Emperor's New Security Indicators. S&P 2007.

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.

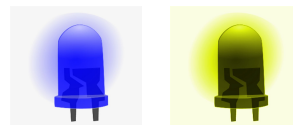
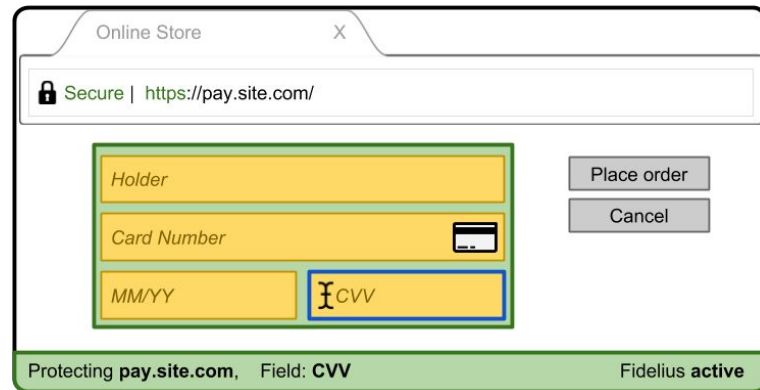
Whalen and Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers. GI 2005.

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)

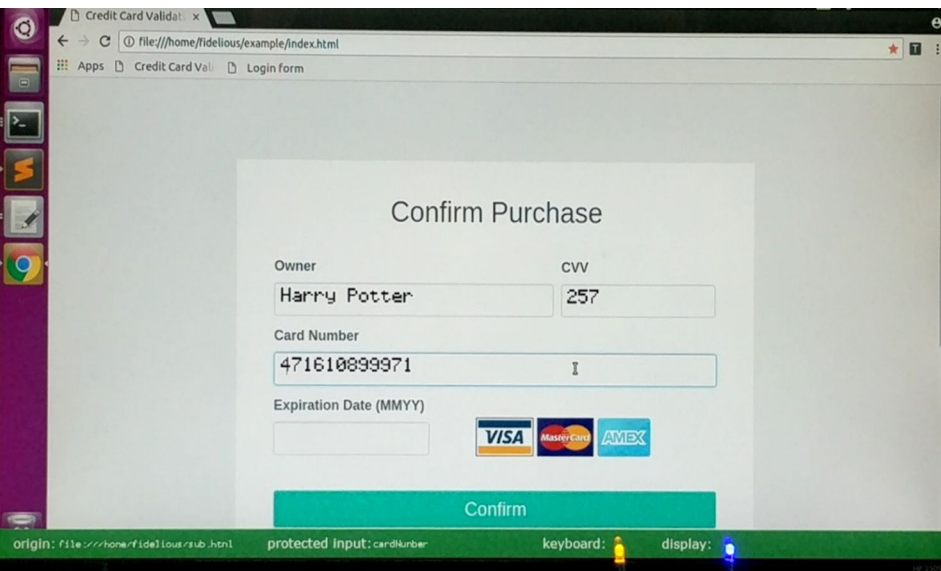


Schechter and Dhamija, The Emperor's New Security Indicators. S&P 2007.

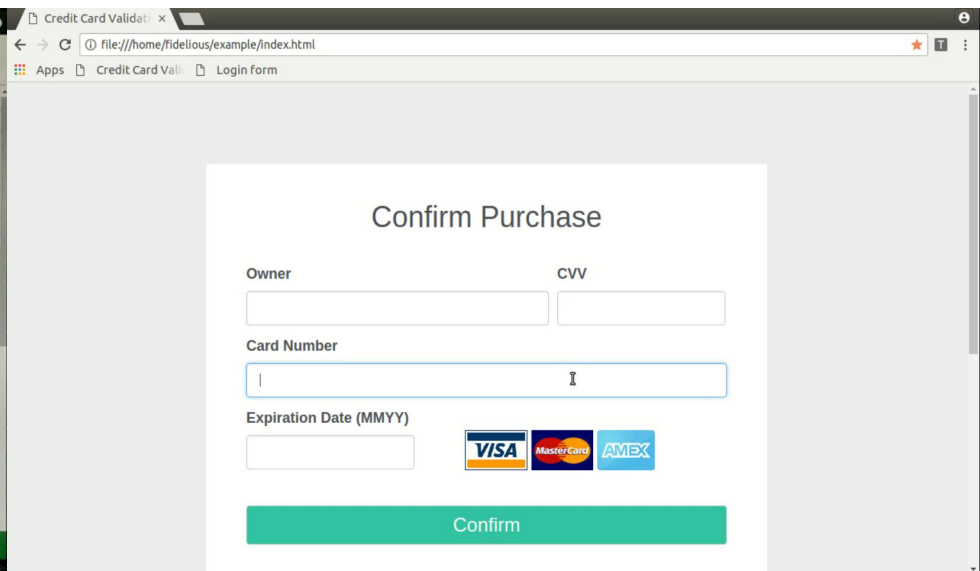
Whalen and Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers. GI 2005.

Example

User view (photograph)



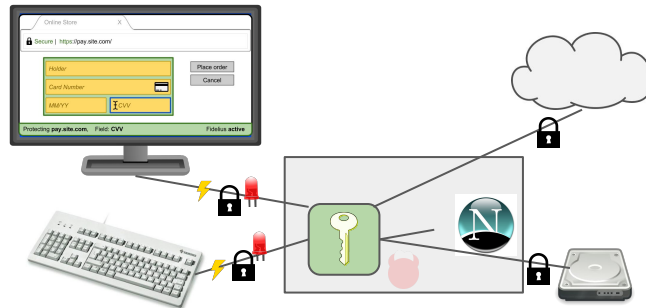
Malware view (screen capture)



See video demo at <https://crypto.stanford.edu/fidelious>

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

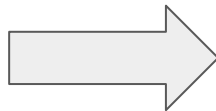
As a one-time security measure please verify the zip code of the property associated with this mortgage account, and your Social Security Number.

PROPERTY ZIP CODE

SOCIAL SECURITY NUMBER

Please enter last four of SSN

SUBMIT



Performance

TCB: ~8,500 lines of C++

Performance

TCB: ~8,500 lines of C++

Display Latency Scaling

Doubling trusted display size only slightly increases display latency

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

Performance

TCB: ~8,500 lines of C++

Display Latency Scaling

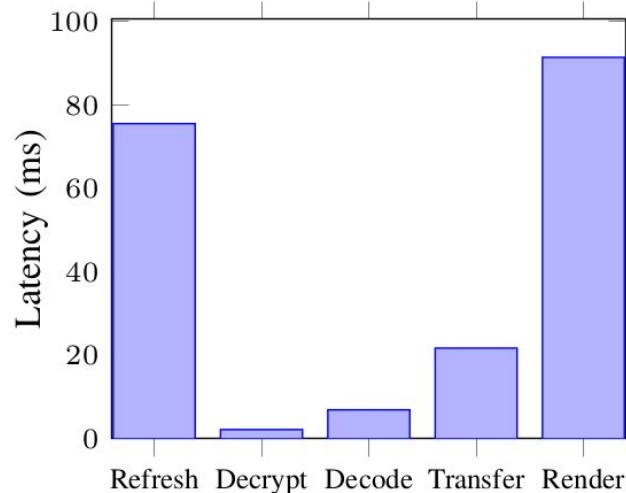
Doubling trusted display size only slightly increases display latency

Display Bottlenecks

Expensive Render/Refresh due to implementation hacks, easily improvable

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

Fidelius Display Pipeline Costs



Performance

TCB: ~8,500 lines of C++

Display Latency Scaling

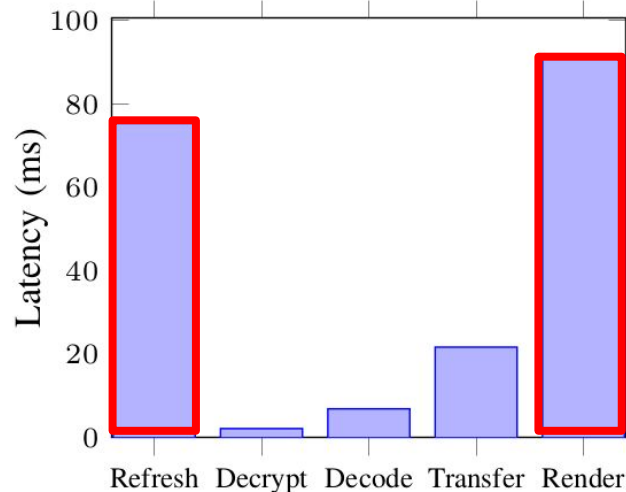
Doubling trusted display size only slightly increases display latency

Display Bottlenecks

Expensive Render/Refresh due to implementation hacks, easily improvable

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

Fidelius Display Pipeline Costs



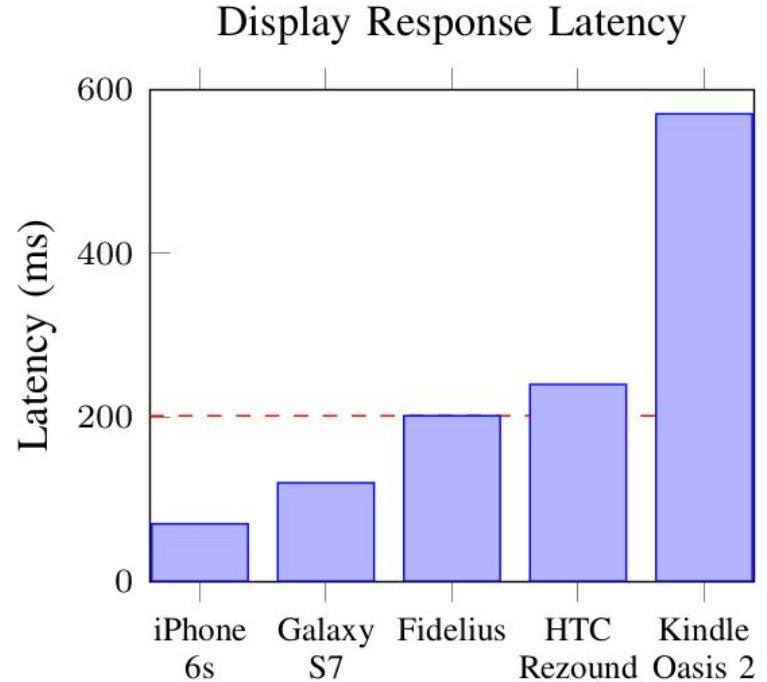
Performance

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>

