Hermes: Developing Novel Attacks Against Cold Wallets

Trezor Wallets have been cracked, are Ledger Wallets next?

Summer 2021

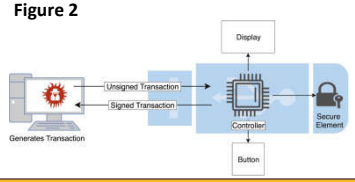
Team Members

Second year PhD Student in Computer Science funded by Kraken. Primary research interests include cold wallet security assessment, cryptography, and side-channel attacks.

Problem Statement

To understand how to better secure recovery phrases, this project takes an adversarial approach. By understanding currently known exploits and developing novel attacks the design space can then be expanded or restricted as needed. A variety of devices will be attacked to give a broad sense of design decisions and vulnerabilities.

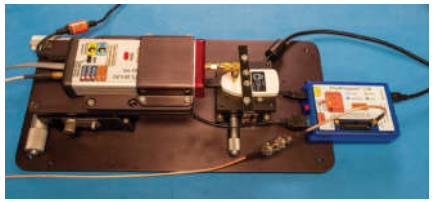
Figure 2



Motivating Prior Work

A Trezor One wallet can be glitch attacked using a ChipSHOUTER EMFI tool to deliver an electromagnetic pulse to a specific region of the device. Triggering and target power control is done via a PhyWhisperer-USB device.

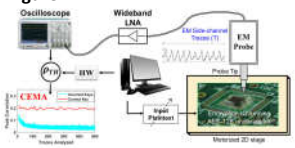
Figure 4



Background

Hardware wallets, also know as cold wallets, that are based on the STM32F2 FPGA have previously been attacked via electromagnetic fault injection. With cryptographic recovery phrases being dumped directly from flash memory, it begs the questions of how to properly secure recovery phrases. With the rise in cryptocurrencies and NFTs, securing them is critical to a fiscally safe future.

Figure 1



Methods

The core requirement of each attack will be accessing the physical device. Without out direct access, these devices offer unparalleled security for private keys. Utilizing glitch, electromagnetic fault injection, and other physical attack strategies will be paramount to exposing weaknesses in current cold wallets.

Figure 3

```
[b'WINUSB',
 b'TRZR',
 b'stor',
 b'exercise muscle tone skate lizard trigger hospital weapon volcano rigid
veteran elite speak outer place logic old abandon aspect ski spare victory
blast language',
 b'My Trezor',
 b'FjFS',
 b'XhYF',
 b'JFAF',
 b'FHDMD',
```

Challenges & Future Work

Some challenges include:

- Attacks are replicated using a theoretical framework. Applying such attacks are difficult in practice
- If we can attack this, what does security mean?

Future work:

- Complete an identical attack
- Explore similar attacks on different devices
- Can this type of attack be anticipated from a software design perspective?

Advisor: Dr. Mike Borowczak
Contact information:

- Email: ccarper2@uwyo.edu
- Discord: Clay!#4368

REFERENCES:

- Figure 1: https://tinyurl.com/y46knm7k
- Figure 2: https://tinyurl.com/3npfwbpd
- Figure 3: “Hardware Hacking Handbook”, Woudenberg and O’Flynn, EARLY ACCESS pg. 152
- Figure 4: “Hardware Hacking Handbook”, Woudenberg and O’Flynn, EARLY ACCESS pg. 147

UNIVERSITY OF WYOMING

CEDAR