

g ĖXĥ Ė kŪā

t Ūĥl\m̄enjkĖf' · Ė gXlJXrh NŪĥ gĖ2Ī

2ónj<sup>5</sup>( ĥ<sup>6</sup> 0 5 (

KŪā ā ĥ ū āl XĥXel XemT ĤāXóH" NŪt óĖXĥ6 āā ĤXĥ' ĤXl m̄ g m̄kŪā 6k6ū ē ē" ēŭĥ " ók  
ĤXkX ĤŪXĥ

· ē 2ónĥkĥ ĥĖ" rāXl m̄ " āXlXkr̄enjl" ĥ ĥ āā ā nŪXĖf' · Ė NŪĥ T Ĥ ēl ēXT ĤXĖ kXl ĖXl  
t<sup>5</sup> ĥ ĥ ĥĖ k āNŪĥ Xl nŪ m̄ ē ākóXŪ I 6XXē ĤXĥ' ĤXl t ā g m̄kŪā 6k'ĖXkĥ' ēkāĖk āĖĖkóX  
^" óēā ĖĥnĤĥ ĥ

Ė k m̄Ė nŪ m̄XĤT" óĖ 6X I Xrnāā ĤXĥ' Ĥĥ ā nŪXēXŪĥNŪ I ūkĥ6 ómāē ĤX āā Ĥ rāXm̄ ēl Ė  
XēĀū \Ū ĖXenXĖ

KĖf' · Ė gXl óĤāā ôX nŪXk

^ XNŪXĖXŪĖ ā nŪXŪĖ āāĖ" óĖ Ė āā m̄ Xkm6 āŪ NŪ nŪenĥ

t t Xē 6XNŪX nŪā XŪĖ āā k l āĖ" t Xĥl ĥnŪXNŪĖT āenjkXl óĤāā Ĥĥ \Xl óĤk T Xĥ ĖX l ū ā ĖĖ\XH

- KŪX6" rē I Xĥā T ĤāXĤĥ nŪXl
- Ĥ2ō ā l ā 6ā ēl Ėk Ė tXĖ Xē ā Xē 6ā " ē nŪXĪ bñ
- Ō" Ĥā nāā" ĤXĥrā ēk ĤXĤNŪĥ Xl óēXk ū" ó Ū t XnŪXĖā
- gXlJXrl m̄ ā ĖĖ ĤX NŪĥ gĖ2Ī T ŪXē ē" ĖenXĖXl Xl
- KŪX6" rē I Xĥ Xāā nŪ m̄ĥ T Ĥā kāēXl
- KŪX6" Ė I XĤāX nŪXkm̄HnX6XNŪXNŪĥ T ĤóHl nā ēl ĤXm̄Xk āā ēā NŪkāēXl NŪĥ T ĤX
- āā" ó I TēnĤl XnŪXNŪĥ T ĤĥnŪXNŪĥ T ĤTāX nŪXkm̄HnX

Ō" T nŪ m̄XŪĖ āā k 6XXē l āĖ" t Xĥl ĥT Ū nŪ" ó ēXl m̄ āē" T āĥ

- āāĥ T Ĥ<sup>5</sup> ĥ ĥ ā ē" m̄ óĖXĥ6 āā nŪā XŪĖ āāĖ Ĥ ēū t Ĥā rā ē" Nān
- ĖŪāā Ė ll Xk ā āĥóāā
- āā" ó Ĥóāēn Ėā " Ĥ kĥŪĤkXĥ" ó Ĥk NŪnŪXĥ ēXĥ " ēā ā ókXĖk T āā" óm̄X  
Ĥ kĥŪĤkX ēl nŪXĖf' · Ė I " Xē" m̄m̄X nŪXĤ kĥŪĤkX
- KŪā m̄lāē ū ē" nŪenm̄ I " T āā Nōāāā rā ē" ĤXĤXĤXērik t ōb · Ō<sup>6</sup> + m̄āē 6" ónŪ Ĥl ĤX  
T ĖXĥ
- kXkĤāXĥ ĥ XlĖāā kĥ" ó l ēē" m̄Xē ākm̄ĖnŪX" NŪā āā T Ĥā<sup>5</sup> kXl" ēl kĥāā ēēX" ĤXē  
nŪXl kXĥŪĥ Ĥm̄XĖk ēl ākm̄ĖnŪXĥ āā ók NŪĥ T ĤX
- Ūāā ū" ó l" óĖ ĤĥX nŪ m̄ā ā Ū Ĥl ĤXĤ6āā Ĥ Ūā Ūāā āā āāā kXl" ēl ĥāā ē ēl  
Ū k6XXē NŪ ā k" NŪ ĤX

- ôæ̃l æ̃nɲ̃ɹ̃X6ốɲ̃

Λ " " n̄ēnjn̄ūX N̄ūh T HЖ

```
void __attribute__((noreturn)) load_app(void)
{
    // zero out SRAM
    memset_reg(_ram_start, _ram_end, 0);

    load_vector_table((const vector_table_t *) FLASH_APP_START);
}
```

[illegible]

Λ " " n̄ēnjn̄X 6 " " n̄ē I X<sub>2</sub>H

Kŭ̄k N̄x” t Xh̄a Xk n̄x Xeh̄h H’ ăm’ Nn̄x6”” n̄ē I Xh̄ e l N̄h T H̄n

```
void __attribute__((weak, naked)) reset_handler(void)
{
    volatile unsigned *src, *dest;

    for (src = &_data_loadaddr, dest = &_data;
         dest < &_edata;
         src++, dest++) {
        *dest = *src;
    }

    while (dest < &_ebss) {
        *dest++ = 0;
    }
}
```

Kl̥ək̚ ə̌m̐ ð̃k̚ n̩X .data    ɛ̌l n̩X .bss    kʰl̥r̩ə̌ ɛ̌k̚ N̩jHkm̐r̩ | m̐ 6XN̩jX\ ð̃n̩n̩XN̩jT̩ ɪ̌X X̑m̐  
H' ə̌m̐

§ "T Xt Xhm̄X eXT Xerh̄ H' æm̄E" æ k" ħ Xm̄l̄en̄l̄æX m̄k̄ HXT H̄m̄X æ b N̄JH̄ĒH̄m̄H

Y U̇X n̄X N̄k m̄ X k̄ e ǎā ãX 6 " óm̄ ° Yã " N̄X gE2Î ĩ n̄X eXT X eñũ H' ǎñ V̄H Xk " óñ n̄X ř dũ Q  
gE2Î H T̄ Ũ Ů Ë " ǎā ãX n̄X .bss kXl r̄ e ĩ

Y̌ X̌x̌ n̄X̌ǧǨľ 7 6 6̌ 0 + Èť ă̌ Ȟ 7 Ť X̌3 X̌ľ " ẽ̌n̄X̌ľ È2̌ľ ă̌ ẽ̌ã̌ ẽ̌ ẽ̌ N̄X̌ľ Ť ă̌ǔ Ȟěľ " ń̌ ľ m̄nǧ" Ǎě X̌Ť n̄X̌ m̄  
n̄X̌ X̌Ǔ ẽ̌ ă̌n̄Ť " ố̌ ẽ̌ X̌ȟǒă̌ X̌ǩm̄ Ȟěn̄ǰn̄X̌6̌ " " ẽ̌ ľ X̌l̄Ť ă̌ǔ " ố̌n̄l̄ Ť X̌l̄Ȟũ̌l̄ ẽ̌ěn̄ǰn̄X̌l̄ X̌ť ă̌ X̌l̄

ÈXkXm̄enjñÜX KÈf' · È

K' h ü æ" T Æ n XñrñXJ J Xñ" h Xñrñ I k m kmjhmñX6" " rññ I XñT ab' órh' T Xñl(ü)ÆnjH k" NñT JX  
JkXm ei Ü H T JXJkXmñ

2 hǒǎ́ áenHXH” NduXKÉ’ · É NduT HXH X ÈI nū rík” Nu HXH XrH HX” nókXI m ÈT Uā Ūñ X ɛmÆ  
T” óÈ Ū t X m HX” Himŋ Ū HT HXH XrH

KŪXākóXŦ k nŭ mŭXŪ HŦ HXHXm' e ħ eŭ lŭHkāk kǎn HĚH' T XHŭlĚŋS" T XŦ Xŋ k ĀE" æl m  
nŭXNŭ nŭHX ĬXNŭ " e gK'ET X6kǎXŋĀE k æ lŭǎH

- $Q\bar{Q} \rightarrow \bar{u}u, d\bar{d}, s\bar{s}, c\bar{c}, b\bar{b}$

K' \Xk nX U H T HXHXn/AE" óÈ U tXm 6HX æ" HXe nXKÉf' É \ kXh" Hóe xñhAÉ I NX  
 óel kXl KÉf' Ék m U el E2NXHómX H XkH áH mñ üÈ\æ" NU H T HXæ" TÈX nXhAÉ È Nùel nX  
 RST Hænt t Xe 6XmXnX Hæ 6XÈT T k GND h" AðkmU I m ókX H á' NX XXVXk m kU' HmX  
 Hækh



## Y Hænj e XUÈ an

gæ\X meta\_backup Ì Xk æ nX .bss kXl rã eñan" óÈ 6XVXHXI 6ü nX reset\_handler k" an  
 l e" n6XnX m\æ Xlmh

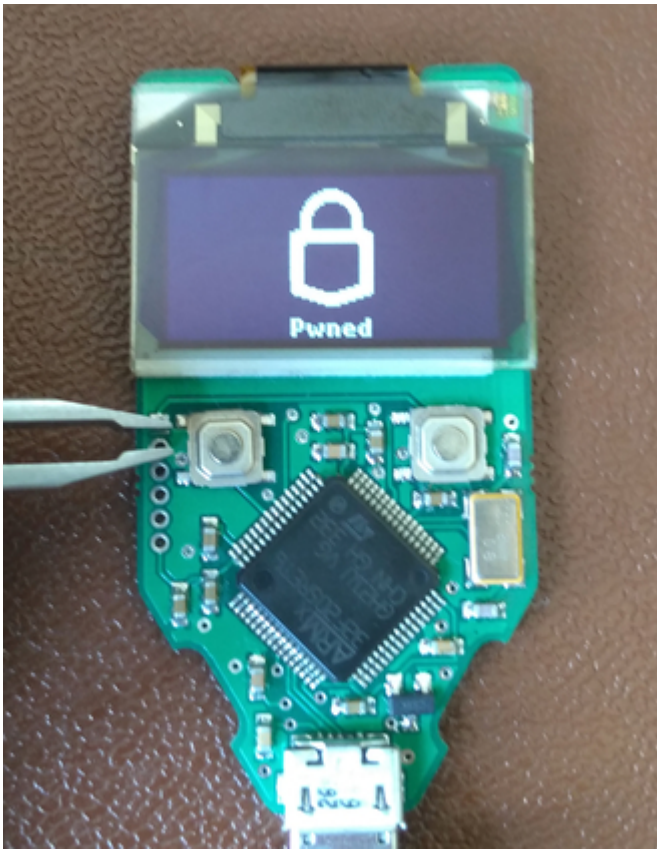
§" TX XñhXkmHnXæ È" HX I æm gE2Î 6ü nX Nñ T HX^ómæ" H Xñ T HX e XUÈ an/AE" óÈ  
 U tXm Nñ "ómX II HXk" N storage æ E2Î h

nX Hóe xñh mXkUæ 6k" e Ì kñh óXnX6æ H Nñ T Hñe" mXt tó Nñh" Hóe xñhX  
 Nñ T HXl e 6X6óæ H Xñ ækñ È el k" e Xe" óñhAÉ I nX II HXk'H

```
$ nm firmware/trezor.elf | grep " storage$"  
2000b3fc B storage
```

†ólæñnX II HXk æ h ól UñjXñ e nX Xe" NñX .bss kXl rã e æ nX6" nÈ I Xk" nX  
 6" nÈ I Xñ" eñ t Xñ Hñ

2N̄X̄H̄K̄X̄m̄n̄j̄r̄X̄Î b̄n̄ĥ̄N̄ĒK̄Ūn̄j̄r̄X̄ĥ̄ Ǣă̄ók̄N̄ĥ̄T̄ H̄X̄H̄K̄X̄m̄n̄j̄r̄X̄Î b̄n̄ n̄j̄ ǣ ɐ̄l̄ k̄m̄H̄n̄j̄r̄X̄  
ĥ̄ Ǣă̄ók̄N̄ĥ̄T̄ H̄X̄ ǢĒĪ m̄Ī”T̄ k̄N̄ĒK̄Ūr̄X̄”N̄Ā̄È̄ĥ̄T̄ H̄X̄6̄ l̄ǣ  
K̄ŪX̄Ǣ k̄n̄H̄X̄M̄T̄ā̄Ū 6̄X̄ ó̄ă̄ă̄È̄k̄ā̄Ūĥ̄



5/6

KŪX .confidential kXl rā ē

§”T I”Xk Nŭh T HJóhHl Xk” ÈXnŭX ãkóXhŭXeđ

2k AŪ.ÈēXI X HŭhŭŭX6””rĕ I Xĭēāā ÆXk H.H.Ūñ nŭē<sup>7 6</sup> Yā ”NŭXgÉ2ĭ ħAŭXkXlHm m T k ē nŭ m<sup>6</sup> Yā ħānĭ” óÈ HĭX XēnŭX XŪ.È āñ

2el nŭX ã nŭXNŭ È”NŭXnŭHX\Ū ęXk ē nŭ mĭ” ħ ħ āñ2ÈnŭXkXlHm mT k ħ Hŭ k static CONFIDENTIAL ħ CONFIDENTIAL ã ħ \H nŭ mĕÈ\Xk nŭXkŭh6”Èē ęXT kXl rā ęñ\ ÈX .confidential ħT ŪŪ ã HÈ\Xl mŭXk mĭHĭ NgÉ2ĭ ęl ã ÈXk nŭ ē<sup>7 6</sup> Yā ħ

Ô”T ħX Xē T ŪXē ē”È t Xĭkē ē”NŭX6””rĕ I Xĭk mĭHĭ ānĭ Æ”t XĭT ħX .confidential Nŭh nŭX Nŭh T HJĭHĭ XēnŭX XŪ.È āñ

g ÈXh È kŪā

I X? k ÈXh HkŪā ħ” ħ

ô k\ē nŭ 6ŭ \HĭHĭHĭHĭŪ ęl ħókrĕk kŭknĭ k