Report z ročníkového projektu

Samuel Čavoj – gloryctl

Web: https://www.cavoj.net/gloryctl/
Autor: Samuel Čavoj <samuel@cavoj.net>
Vedúci projektu: RNDr. Richard Ostertág, PhD. <ostertag@dcs.fmph.uniba.sk>
Repozitár s projektom: https://git.sammserver.com/sammko/gloryctl

Zimný semester:

- Pomocou nástroja usblyzer som reverse-engineeroval časť komunikačného protokolu myši s oficiálnou aplikáciou pre Windows od výrobcu. Rovnaký protokol používa variant myši Model O– , zrejme obsahuje rovnaký hardware. Model D nemám k dispozícii, ale software od výrobcu je podobný, no využíva iné USB identifikátory. Komunikačný protokol som tým pádom nevidel, ale predpokladám, že sa líšiť veľmi nebude.
- Do istej miery som sa zoznámil s protokolom USB a niektorými jeho detailmi.
- Naprogramoval som v jazyku Rust knižnicu na komunikáciou s myšou. Implementuje časť protokolu, vrátane jeho prekladanie z a do natívnych dátových štruktúr jazyka. Používa na nízkoúrovňovú komunikáciu s myšou knižnicu hidapi, ktorá funguje cross-platform.
- Zdokumentoval som komunikačný protokol v súbore README.md v git repozitári.

Letný semester:

- Namiesto programu USBLyzer som na analýzu komunikácie originálneho softwaru začal používať API monitor. Stačilo nastaviť filter na HID volania a mohol som pohodlne skúmať (prípadne ukladať do súboru) prenášané reporty.
- Pokračoval som v reverznom engineeringu protokolu a implementoval jeho kódovanie a dekódovanie z a do natívnych Rust dátových štruktúr.
    - V rámci tohto som implementoval prototypný dekóder makier v jazyku Python, nachádza sa v súbore dump_macro.py.
    - Na dekódovanie som používal parser-combinator knižnicu `nom`, ktorá sa ukázala ako možno zbytočne silná a komplikovaná. Ako možno lepší nástroj mi príde niečo ako Kaitai, ale jeho podpora pre Rust je zatiaľ v počiatočných štádiách. Iné alternatívy sú napríklad knižnica `binread`, alebo manuálna implemetácia pomocou napríklad `byteorder`, ktorá by možno vzhľadom na relatívnu jednoduchosť protokolu postačovala.
- Rozšíril som dokumentáciu protokolu v README.md.
- Implementoval som command line rozhranie na konfigurovanie myši (RGB osvetlenia, mapovania tlačítok, programovanie makier, DPI profilov). Dokumentácia je integrovaná aj v aplikácii pod bežným flagom `--help`.
- Pri zisťovaní koľko macro bankov myš podporuje som ju brickol, zrejme vo firmwari chýba bounds check a myš si pri zápise prepísala nejakú dôležitú oblasť pamäti. Po tomto sa pri zapojení vôbec nerozsvietila ani neobjavila na USB zbernici.