Rust Transparent Proxy

Daniel Karzel

saasyan

Why? - Web Filtering for schools!

- Filtering web content in schools → saasyan.com.au
- “Filtering” requires:
  - Traffic capture
  - Traffic analysis
    - SSL Decryption (using own trusted cert)
  - Decision to allow / block
  - Action to allow / block
- After installation users are unable to “turn off” the filter

How? - Proxy!

- Explicit proxy
  - Browser (e.g. Firefox)
  - System Proxy
  - Packet redirection handled by the operating system and applications
  - → Can easily be bypassed
- Transparent Proxy
  - Packet redirection on the network level
  - Applications are unaware of the proxy
  - → Hard to bypass

Let’s not reinvent the wheel, but …

squid-cache / **squid**

- Existing solutions
  - Squid Proxy (C++)
    - Transparent redirection: IPTables
    - OK for setup as cloud or on-premise proxy
    - Not designed for “on-device”
      - Hard to deploy on Windows, no transparent support for Windows
  - Mitmproxy (Python)
    - Functionality beyond what we need, but performance/stability not good enough

Let’s build it in Rust…

Let’s plug some libs/projects together…

Proxy?

hyperium / **hyper**

- Hyper!
- The hyper **http_proxy example** is a great start.
- It’s all about streams and bidirectional copy.
- Hyper helps with keeping the focus on the application layer
  - TCP, upgrades (...) all done by hyper
  - If you need to configure some TCP flags e.g. **socket2** can be a great crate to add…

Decryption?

hatoo / **http-mitm-proxy**

- Sooo many Rust MITM proxies out there…

hatoo / **http-mitm-proxy**	Good balance of maintenance, code quality and functionality
omjadas / **hudsucker**	Similarly good as ⬆️ - but not as easy to read (subjectively)
emanuele-em / **proxelar**	Python mitmproxy maintainer's project, code quality soso
campbellC / **third-wheel**	Not maintained (code decent)

Transparent?

- Transparent filters are hard because TCP packet redirection is hard…
- Platform specific code needed
  - OS level network filters require elevated rights (service)
  - OS level network filters are quite different on Windows and MacOS
    - Windows: WFP, Filter Drivers, …
    - MacOS: Network Extensions

Python mitmproxy(_rs)

mitmproxy / **mitmproxy_rs**

- Python cross-platform proxy (Linux, MacOS, Windows)
- Packet redirection in Rust - the proxy all in Python
- Packet “redirection” using smoltcp stack (including virtual device)
- Lots of functionality. Hard to understand. Feels complicated.
  - Redirector in separate process. IPC communication on top of 100x indirection.
  - Can do way more than what we need (at least initially)

MacOS still WIP, let’s focus on Windows

WinDivert

basil00 / **WinDivert**

- Open Source
- Built on top of the WFP
- Comes with it’s own filter language to define packet capture
- Exactly what we need.
- But… It’s in C++
- Has anybody written a Rust wrapper for that…?

WinDivert Rust

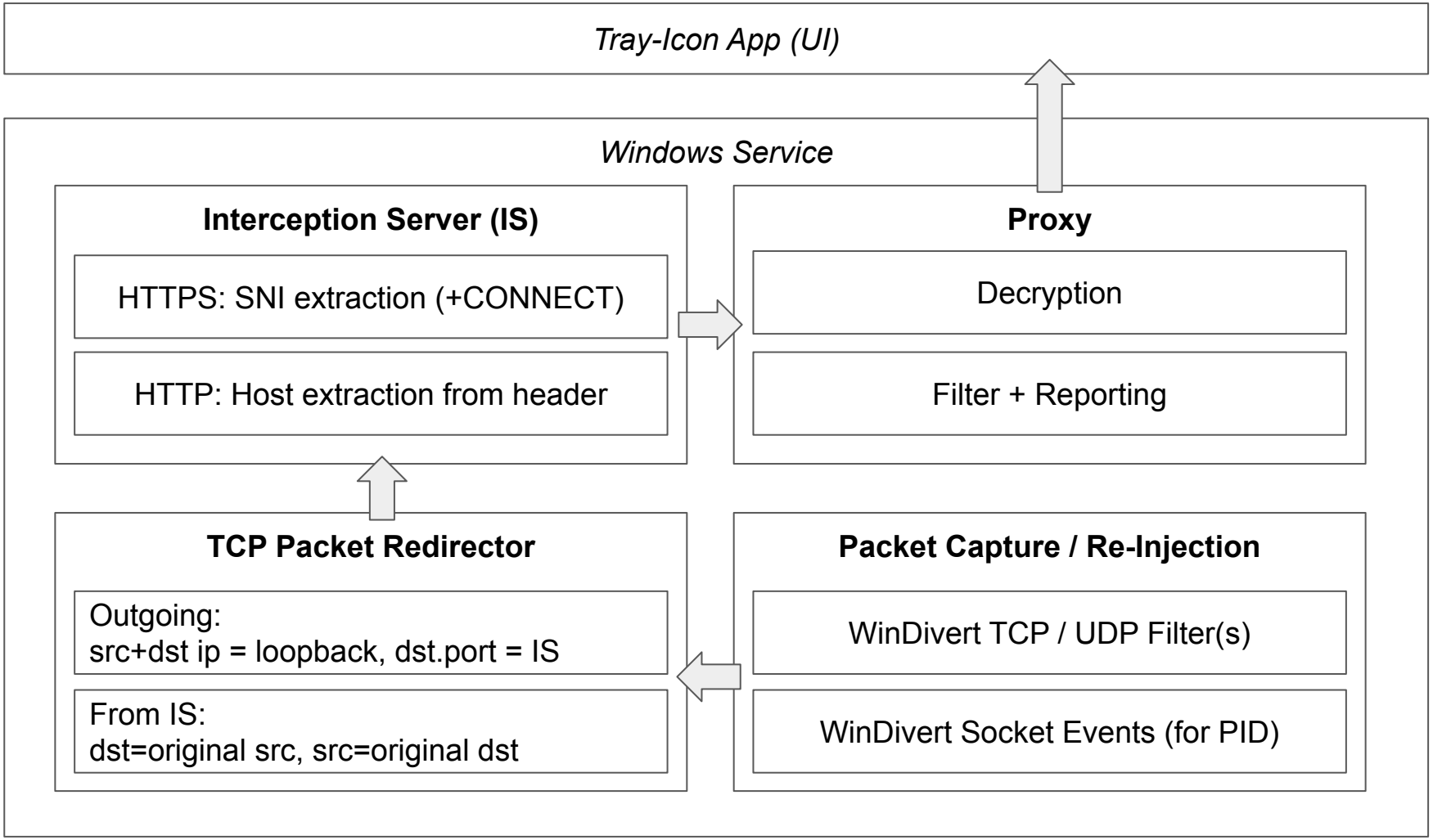
Rubensei / **windivert-rust**

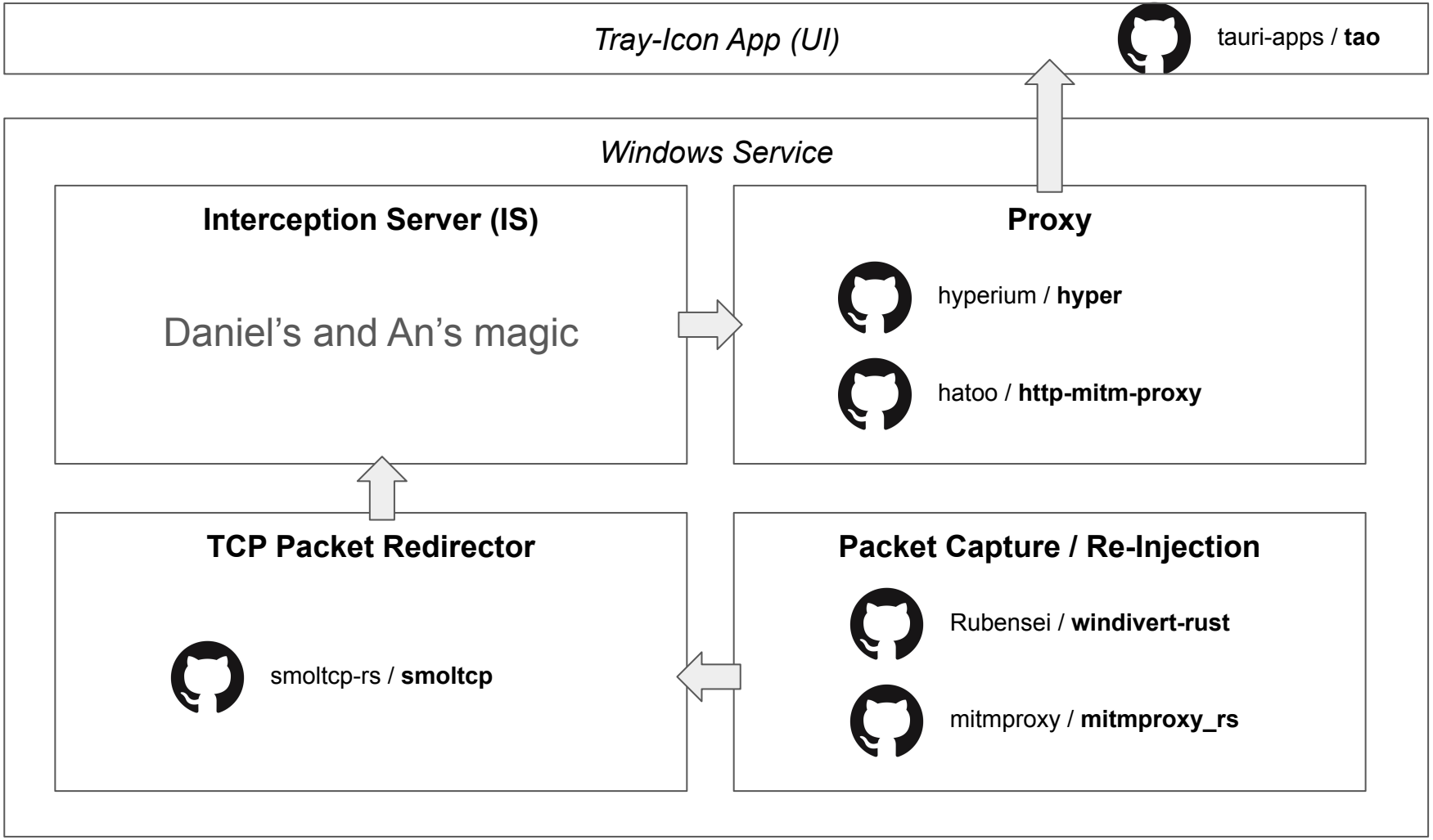
- **windivert** and **windivert-sys** crates
- Windivert crate nice abstraction on top of the low-level interface
- Quite easy to use
- Maintenance could be better, but hey, it works!

smoltcp for packet redirection

smoltcp-rs / **smoltcp**

- It’s actually a complete TCP stack
- Yes, that’s an overkill…
- But it’s one of the better maintained libraries out there 🙅‍♂️


Tray-Icon App (UI)
Windows Service
Interception Server (IS)
HTTPS: SNI extraction (+CONNECT)
HTTP: Host extraction from header
Proxy
Decryption
Filter + Reporting
TCP Packet Redirector
Outgoing:
src+dst ip = loopback, dst.port = IS
From IS:
dst=original src, src=original dst
Packet Capture / Re-Injection
WinDivert TCP / UDP Filter(s)
WinDivert Socket Events (for PID)


Tray-Icon App (UI)
tauri-apps / tao
Windows Service
Interception Server (IS)
Daniel's and An's magic
Proxy
hyperium / hyper
hatoo / http-mitm-proxy
TCP Packet Redirector
smoltcp-rs / smoltcp
Packet Capture / Re-Injection
Rubensei / windivert-rust
mitmproxy / mitmproxy_rs

10.12.128.3 - daniel (admin)

Assure Web Filter Block Page

127.0.0.1:18181/block?message=Sorry, you are not allowed to access https://www.pornhub.com

The page you are trying to access is restricted.

Sorry, you are not allowed to access https://www.pornhub.com

assure Web Filter

User-ID: daniel

Assure Cloud Status: OK

About

Blocked requests (click on the url to copy it)

21:30:43 - https://www.pornhub.com

Type here to search

Result ENG 9:32 PM 28/10/2024