UNWIND

CARSTEN STROTMANN

Created: 2019-05-21 Tue 15:14

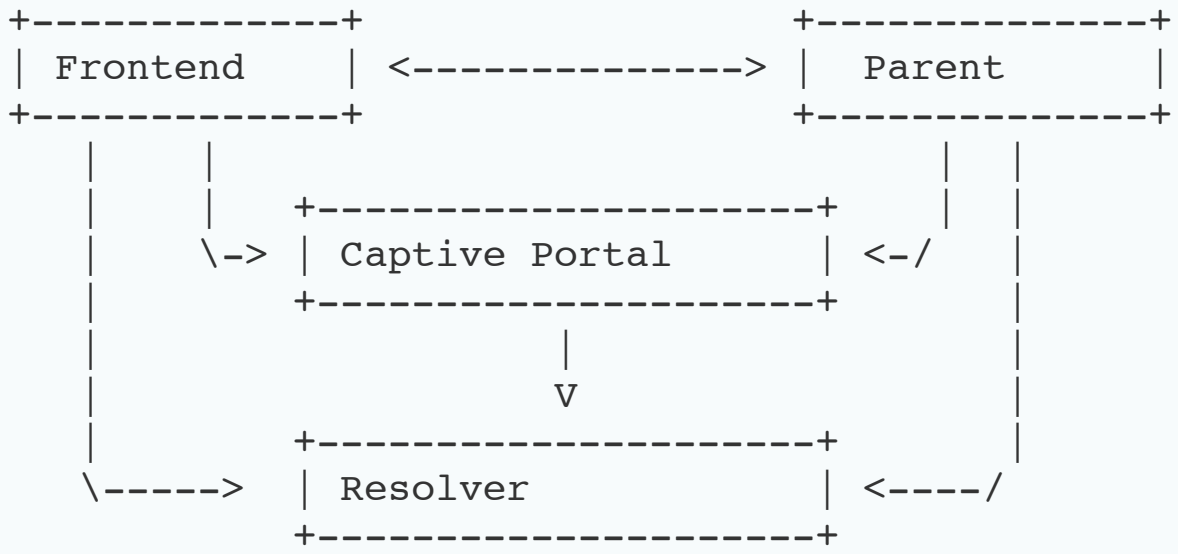
ABOUT UNWIND(8)

- unwind is a local DNS resolver aimed at mobile devices (laptops)
- does (opportunistic) DNSSEC validation and transport encryption (DoT)
- captive portal detection
- defensive design (pledge, unveil)
- first release as part of OpenBSD 6.5 (April 2019)

WHO

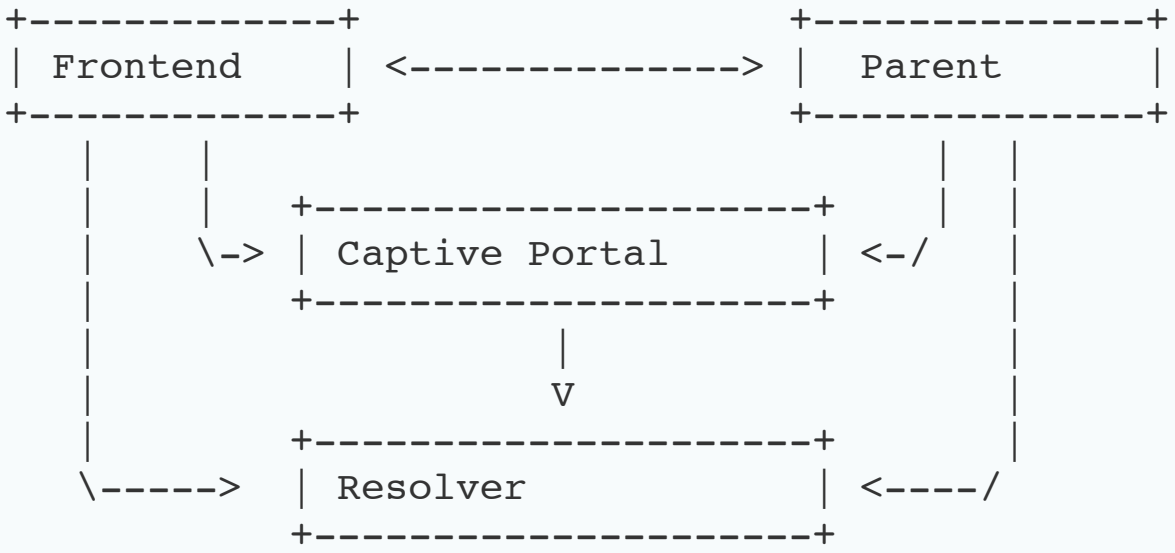
- unwind is beeing developed by Florian Obser (forian@openbsd.org)
  - OpenBSD developer since 2012
  - author of many good tools (slowcgi(8), slaacd(8), sysupgrade(8) ...)

UNWIND ARCHITECTURE



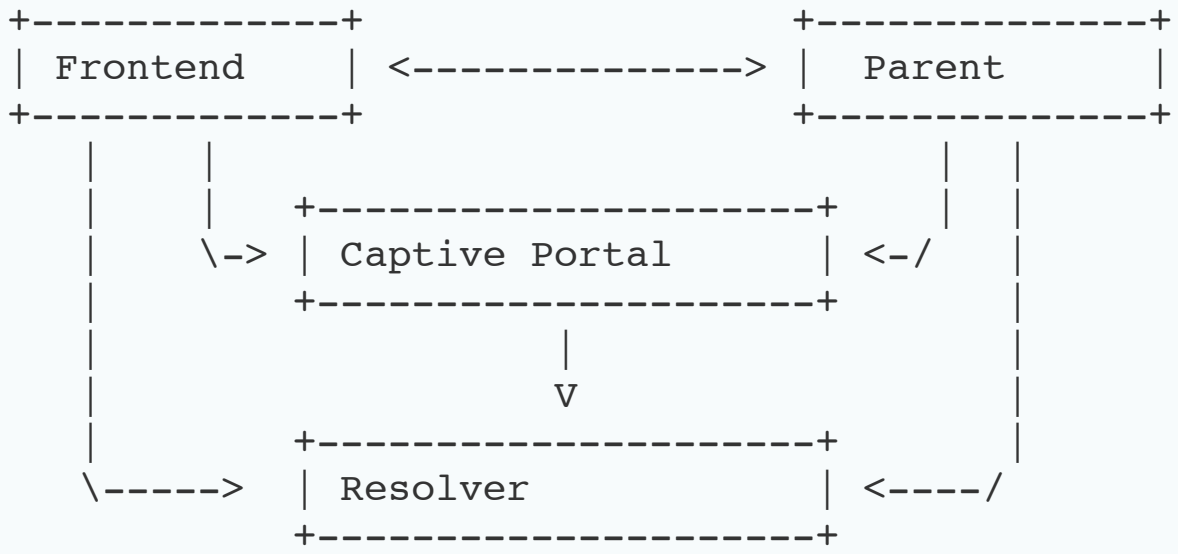
- Privilege separation - each process has it's little duties and is separated from the other parts
- a security bug in one component does not lead to full compromise

UNWIND ARCHITECTURE



- DNS resolver work is done via `libunbound`

UNWIND ARCHITECTURE



- captive portal checks webserver acces (HTTP Port 80) towards the Internet
  - if checks fail, the DHCP supplied DNS-resovler are used

NETWORK QUALITY

- unwind monitors the DNS resolution and dynamically switched between resolving strategies
  - direct recursion
  - use of the DHCP supplied DNS resolver
  - use of configured DNS-over-UDP forwarder
  - use of configured DNS-over-TLS forwards
- preferred resolving strategy order configurable

GETTING STARTED

- `unwind` can work without configuration
- short example configuration file in `/etc/unwind.conf`

```
captive portal {
        url "http://detectportal.firefox.com/"
        expected response "success\n"
}

forwarder 5.45.107.88 authentication name doh.defaultroutes.de DoT
preference DoT
```

INTERFACE TO UNWIND

- user can control `unwind` via `unwindctl`

```
# unwindctl
valid commands/args:
  reload
  status
  log
  recheck

# unwindctl status
captive portal is unchecked

selected             type status
       *              DoT validating
                recursor validating
                    dhcp validating
```

WORKS GREAT, BUT IS NOT FINISHED

- future work:
  - get DNS resolver from IPv6 router advertisements in addition to DHCPv4
  - support for "Split-Horizon" DNS
  - "strict" DNSSEC validation
  - build-in captive-portal detection

MORE INFO

- on OpenBSD: `man unwind` / `man unwind.conf`
- Presentation by Florian Obser from BSDCan May 2019
- HTML Version of this presentation: doh.defaultroutes.de/unwind/unwind.html

YOUR QUESTIONS