FPGA-based DNS Anomaly Detector and Threat Mitigator

Deployment

Hardware

Prerequisites

- Board: `Digilent Arty A7-35T Development Board`
- FPGA Core: `Xilinx Artix-7 (XC7A35TICSG324-1L)`
- Hardware IDE: `Xilinx Vivado Design Suite 2020.2`

Previously...

- Board: `Xilinx Spartan-3E FPGA Starter Kit Board`
- FPGA Core: `Xilinx Spartan-3E FPGA`
- Hardware IDE: `Xilinx ISE Design Suite 14.7`

Instructions

Import `fpga-dns-adtm/hw/dns-anomaly-arty-a7/dns-anomaly-arty-a7.xpr` to `Xilinx Vivado Design Suite 2020.2` (minimum WEBPACK edition).

HDL design sources are availabe in `xil_defaultlib`, with `main.vhd` as the top-level module. Select constraints file `arty-a7.xdc` for production mode, or `arty-a7-debug.xdc` for Chipscope ILA debug mode.

Set hard-coded configurations in the HDL as follows: * Set `i.vhd`, GENERIC `g_admin_key` to the SIPhash key, make sure it is the same key used in software. * Set `i.vhd`, GENERIC `g_dns_rcode` to the RCODE reply in DNS spoof replies, default to `NXDOMAIN`. * Set `o.vhd`, GENERIC `g_reply_mac` to the interface MAC FPGA is responding to.

Follow the workflow to synthesize, implement and generate the design bitstream.

Software

Prerequisites

- GCC `10.0+`
- Editline Library `libedit-devel`
- Linux Kernel `5.0+`

Instructions

Run `git submodule update --init --recursive` to fetch `siphash-ref-impl`.

Make sure the key in `sw/admin-cli/fpga-filter.hh` `admin_buf_key` is the same key used in hardware.

Run `make` to build useful toolkits for this project.

Read `./main.out -h` before proceeding with launching the CLI.

Usually, root privilege is required to access raw sockets, which is a must for the FPGA CLI interface, `sudo ./main.out -f enp8s0 -p`.

Type `> ?`, or `> <command> ?` for more information on CLI utilities. For instance:

```
> ?
admin       FPGA filter administrator utilities
stats       FPGA filter stats utilities
test        FPGA test utilities
history     list history
clear       clear the screen
quit        quit FPGA administrator cli
help        display this text
?           synonym for `help'
> stats ?
show        show filter stats from FPGA (in-cache)
probe       probe FPGA for latest filter stats
help        display this text
?           synonym for `help'
> stats show
valid packets received            = 68290
...
```

Other tools are also built with `make`, under the `tools/` folder. Namely a prototype packet sender and receiver, an administration packet builder and an Ethernet CRC32 checker.

Note, to enable promiscuous mode on NIC for FPGA testing, run `sudo ip link set [interface] promisc on`.

Validation

Simulation in `Vivado Design Suite`

Testbench / Simulation sources are availabe in "Simulation-Only Sources" section in Vivado,/

Integration Simulation `sim_1` set

`test_main.vhd` is the top-level module. Enable / Disable test suites by commenting (out) VHDL procedure calls in `test_main.vhd`.

For instance,

```
 dns_empty_test_suite(E_RX_CLK_period, E_RX_DV, E_RXD);
dns_admin_black_test_suite(E_RX_CLK_period, E_RX_DV, E_RXD);
dns_admin_white_test_suite(E_RX_CLK_period, E_RX_DV, E_RXD);
--reply_dns_test_suite(E_RX_CLK_period, E_RX_DV, E_RXD);
--siphash_test_suite(E_RX_CLK_period, E_RX_DV, E_RXD);
```

SipHash 2-4 module simulation `sim_2` set

`sim_siphash_main.vhd` is the top-level module. Modify the 128-bit SipHash key before simulation, and compare its results with the reference software implementation.

Hardware Validation via Software System

Run `> test all` in the provided CLI interface, and avoid using the FPGA-connected interface while testing.