Funkční vzorek

1) HW podpora detekce NAT (HW aided NAT detection)

2) Ing. Jiří Dostál – KPS FIT ČVUT
Ivan Rusnačko – KČN FIT ČVUT

3) Identifikátor VVVS: 204283

4) Popis:

Abstrakt:

Jedná se o zařízení monitorující provoz na síti Ethernet, které na základě analýzy TCP/IP detekuje NAT. HW podpora detekce NAT je IP jádro napsané v jazyce VHDL a implementované na deskách s obvodem FPGA Spartan6/Virtex 5. Detektor je schopen pracovat na rychlosti 1Gbps. Implementovány jsou detekční metody: OS fingreprint, TCP timestamps, TTL, IPID, source port, MSS.

Abstract:

HW aided NAT detection module is an IP core, which monitors Ethernet traffic and detects NAT. The detection is based on TCP/IP analysis. IP core is written in VHDL language and implemented in boards with Spartan6/Virtex5 FPGA. The detector can operate at 1Gbps. Implemented detection methods: OS fingreprint, TCP timestamps, TTL, IPID, source port, MSS.

Účel:

Účelem vytvořeného zařízení je detekce zařízení skrytých za NAT serverem v lokální síti využívající TCP/IP. Vytvořené zařízení obsahuje FPGA čip, který zajišťuje jak vlastní detekci, tak obsahuje uživatelský SW, který slouží k nastavování detekčních parametrů zařízení. Zařízení zasílá výsledky detekce přes sériovou linku – ty jdou pak zpracovat či jinak využít v nadřazené aplikaci. Přes sériovou linku lze zařízení též konfigurovat.

Hlavní charakteristiky:

- HW detekceNAT
- používá všechny běžné metody detekce

- využívá uživatelské metody detekce
- IP core implementovaný v FPGA
- nízká spotřeba (0,35 W)
- konfigurovatelný filter IP adres za běhu
- změna použitých detekčních metod za běhu
- využívá soft-core CPU pro zpracování vstupu a výstupu sériové linky
- obsahuje API, kterým je možné posílat výstup na další zpracování

5) Popis originality:

Existuje řada softwarových aplikací, které implementují část detekčních metod, případně všechny implementované metody. V České republice byl v této oblasti vytvořen plugin NATdet do programu Nfsen, který byl vytvořen na Masarykově univerzitě. Jde však o softwarovou aplikaci a využívá méně detekčních metod a zvláště v oblasti OS fingerprintu, který je pro NAT detekci zásadní, jeví výrazně nižší pravděbodobnost správné detekce. Používá mnohem méně signatur. Je založen na NetFlow architektuře, narozdíl od této práce, která díky FPGA může analyzovat každý paket na fyzickém médiu. Celosvětově je v této oblasti nejdále program p0f, který obsahuje nejlépe implementovanou metodu OS fingerprint a obsahuje i ostatní metody, jde ale jedná se o čistě SW aplikaci, z čehož plyne vyšší spotřeba elektrické energie (nutnost zapnutého PC) a omezení možnosti rychlosti zkoumaných dat (dáno počtem a rychlostí síťových karet). Vytvořené IP jádro je přenositelné i na jiné architektury, takže je možné přes SFP konektor bez problémů přijímat desítky GB dat za minimální spotřeby elektrické energie.

Schéma:

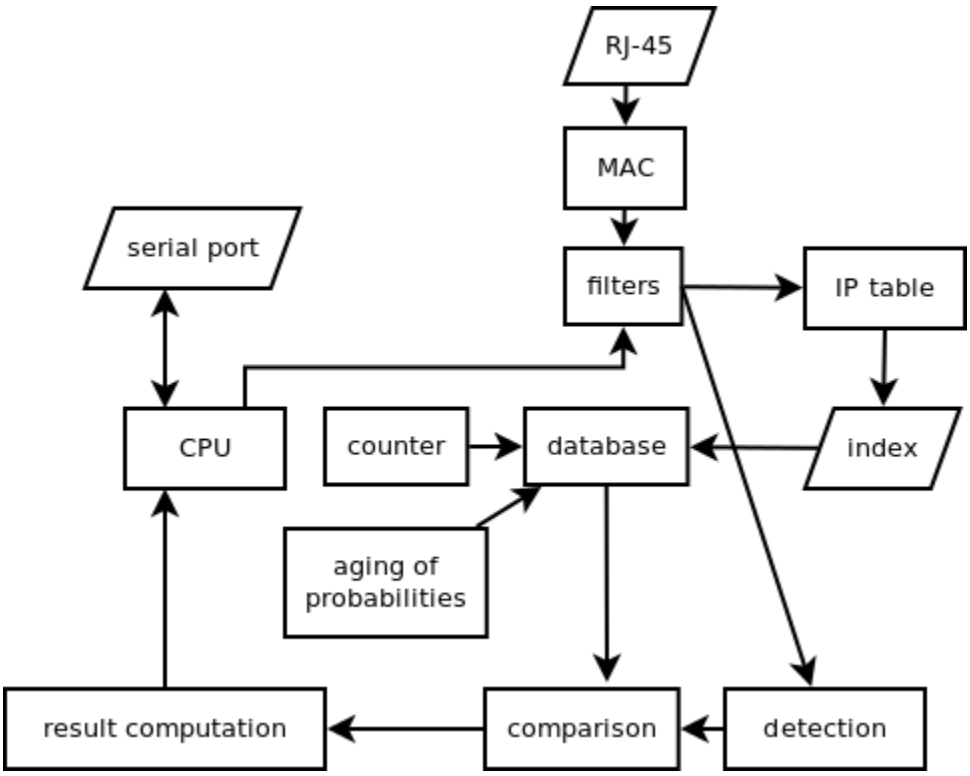
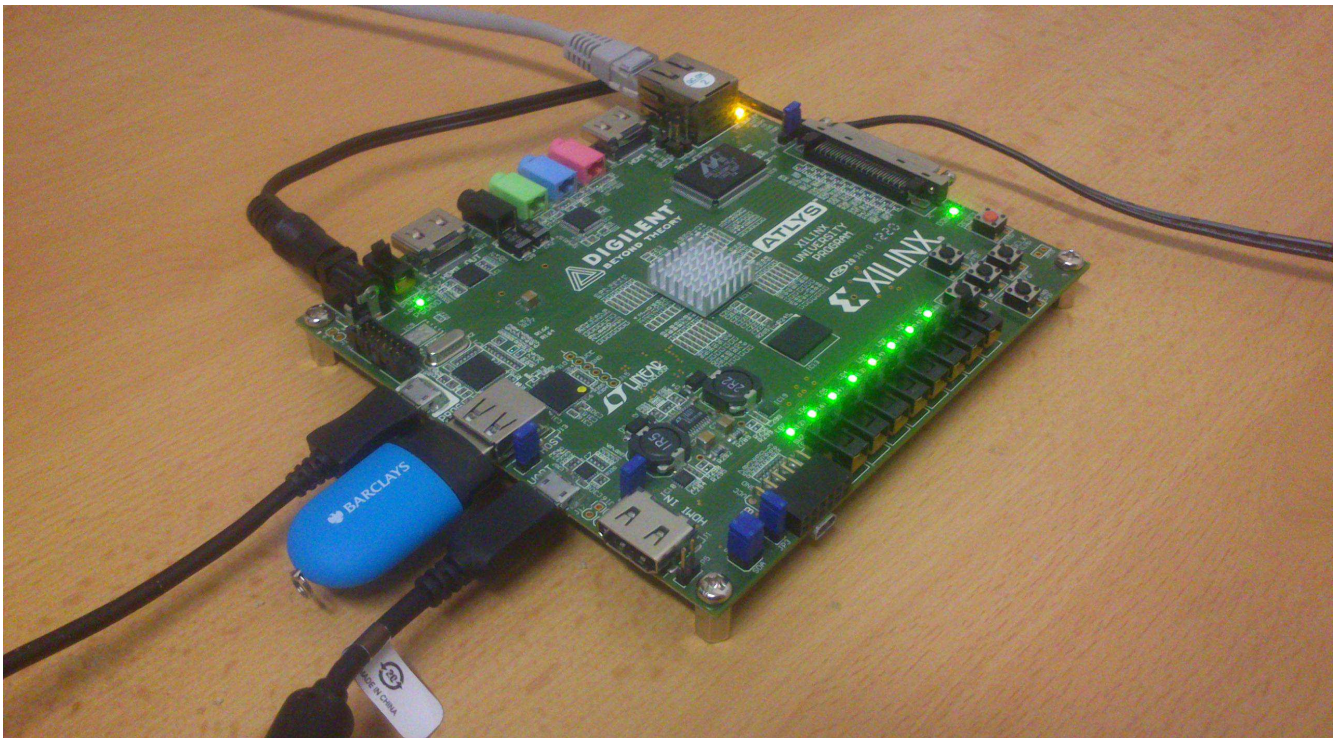

RJ-45
MAC
serial port
filters
IP table
CPU
counter
database
index
aging of probabilities
result computation
comparison
detection

Foto:


DIGILENT
BEYOND THEORY
ATLYS
XILINX
BARCLAYS

6) Odkaz na publikace
bez odkazu

7) Specifikace výzkumného grantu,
RVO|18000|ext:|Institucionální podpora na rozvoj výzkumné org.

8) Adresa fyzického umístění FVZ
Fakulta informačních technologií
České vysoké učení technické v Praze
Thákurova 9
160 00 Praha 6

Místo a datum vyhotovení protokolu:

Podpis autora: