Application-interception in 100G networks

ISS Dubai, March 3rd, 2014

Petr Kastovsky
kastovsky@invea.com

Company Introduction

- HQ: Brno, Czech Republic
- Established in 2007
- 40 employees, $ 3M revenue
- Key focus
  - **Lawful Interception and Data Retention**
  - **Hardware acceleration and FPGA Solutions**
  - **Flow Monitoring and Network Behavior Analysis**
- Products deployed at 500+ customers worldwide

Reference

INVEATECH

Modern threats

INVEATECH

eurostat newsrelease

21/2011 - 7 February 2

8 February 2011: Safer Internet Day

Nearly one third of internet users in the EU27 caught a computer virus

84% of internet users use IT security software for protection

ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage

BY RIGHARD ZWIENENBERG POSTED 21 JUN 2012 AT 04:58AM

"VIRUSES REVEALED" 1 TAGS AUTOCAD

The malware news today is all about new targeted, high-tech, military grade malicious code such as Stuxnet, Duqu and Flamer that have grabbed headlines. So imagine our surprise when an AutoCAD worm, written in AutoLISP, the scripting language that AutoCAD uses, suddenly showed a big spike in one country on ESET's LiveGrid® two months ago, and this country is Peru.

TIME Techland

News and reviews about gadgets, gear, apps and the web

Home | Gadgets | Apps & Web | News | Reviews & Features | Compa

SECURITY

DNSChanger: FBI Warns Infected Computers Will Lose Web, Email Access in July

By MATT PECKHAM @mattpeckham April 23, 2012 8

29 August 2011, 13:27

IT Security & Network Security News

Japan's Largest Defense Contractor Hit by Cyber-Attackers

LinkedIn Twitter 5 Facebook 3 +1 0 Share 8

By: Fahmida Y. Rashid
2011-09-19
Article Rating: ☆☆☆☆☆ / 0

Worm spreads via Windows Remote Desktop

Anti-virus software vendor F-Secure is warning of a piece of malware by the name of Morto, which spreads using Windows' Remote Desktop Server (RDP server). It does not exploit a Windows security vulnerability; instead, it scans IP address ranges for RDP port 3389 and then tries to log in as an administrator to any computers which respond using a list of common passwords.

'It's a complete attack tool kit designed for general cyber-espionage purposes.'

— Alexander Gostev, analyst, Kaspersky Lab

Challenges

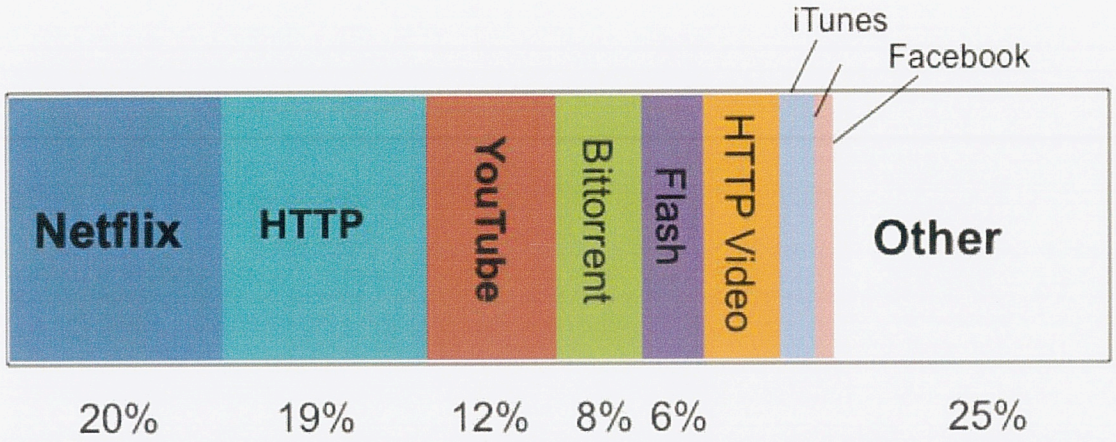
- Typical deployment in core network
  - **high bandwidth** and line utilization
- New **link layer technologies** (10G, 40G, 100G)
- Growing **number of end users and devices**
- Growing **number of services**
- A lot of different network protocols
- Predicted growth of network traffic variability
- Limited computational resources

40/100G network

- **40G Ethernet**
  - Shortest packet 64B, IPG 20B, max rate 59,5 Mpps
  - New packet in every 16,8ns
  - 5GB/s (DVD), 300GB/min, 18TB/h, 432TB/day
  - ~ 100 000 DVDs a day
- **100G Ethernet**
  - Shortest packet 64B, IPG 20B, max rate 148,8 Mpps
  - New packet in every 6,7ns
  - 12,5GB/s (~3 DVDs), 750GB/min, 45TB/h, 1080TB/day
  - ~ 250 000 DVDs a day → 300m tall column

Traffic mix

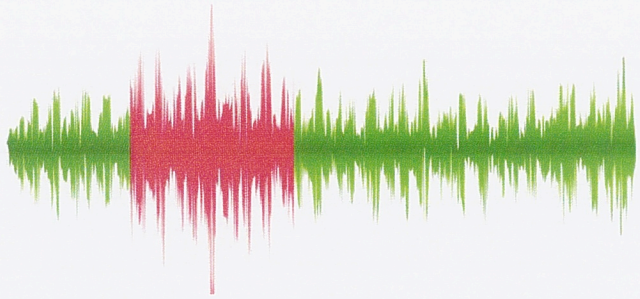
- Thousands of applications and services



- Heavy-tail traffic distribution
  - Well-known apps and services representing up to 80%
  - Typical interest in the last 20% (or less)
  - Specifically e-mail and VoIP interception

VoIP interception

- SIP, H323, etc. signalling protocols
  - Decode L2, L3, L4
  - Decode application protocol
  - Extract necessary fields (URI)
  - Lookup identifier match
  - Set up interception of call content stream



- Requires many steps, impossible when new packet arrives every 6,7ns

E-mail interception

- Various protocols (SMTP, POP3, IMAP)
  - Inspection of L2,L3, L4
  - Decode application protocol
  - Extract e-mail addresses
  - Lookup matching addresses
- Requires many steps, impossible when new packet arrives every 6,7ns

Next generation monitoring

INVEATECH

- Novel approach of software defined monitoring
  - Analogy to software defined networking
  - Abstraction of monitoring functions
  - Flexible application protocol analysis
  - Intelligent, configurable level of detail

Software defined monitoring

INVEATECH

- *Hardware* provides various methods of packet preprocessing
  - *The Muscles*

- *Software* controls the usage of preprocessing on flow basis
  - *The Controller*

- *User applications* request the HW acceleration and perform advanced monitoring tasks
  - *The Intelligence*

Applications can adjust acceleration of traffic processing according to their actual needs

Hardware Part

INVEATECH

- Driven by instructions from „intelligent“ software
  - Hardware as fast as possible
- Well-defined set of operations:
  - Forward (cut) packet to a receive queue
  - Send unified headers to a receive queue
  - Update flow cache entry
    - create, remove, reset, export
  - Drop packet
- Configurable, flow aware distribution of traffic into receive queues

Software Part

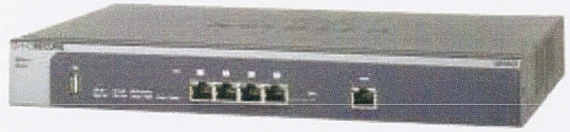
INVEATECH

- *Monitoring applications* in SW
  - process traffic from receive queues
  - determine the traffic of interest
  - instruct SW controller
- *SW controller* configures HW so that monitoring applications
  - *always* get what they asked for
  - get *the least* undesired traffic
- Application parsers for selected protocols
  - VoIP, SMTP, DNS etc.

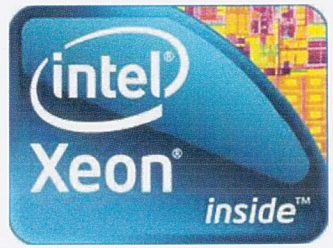
Platforms

INVEATECH

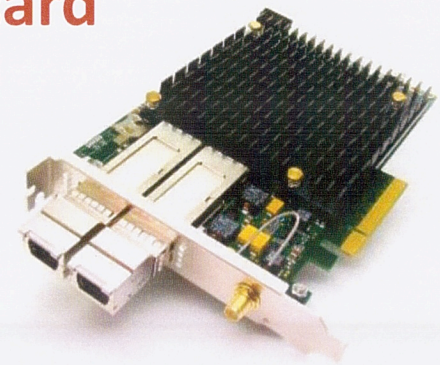
- **Dedicated hardware**
  - High I/O performance
  - Expensive, limited flexibility



- **Commodity hardware**
  - Cheap and flexible
  - Limited I/O performance

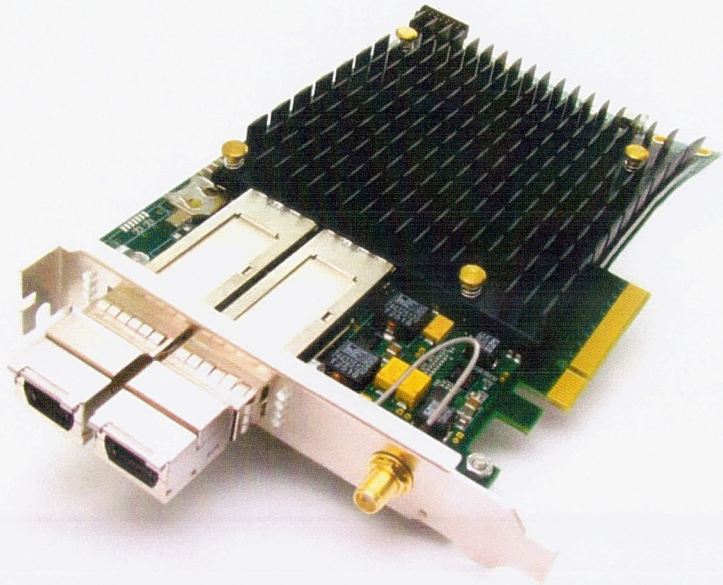


- **Commodity hardware + Hardware acceleration**
  - **Multi-core CPUs + FPGA network interface card**
  - **High I/O performance**
  - **Reasonable price**
  - **Flexible**



COMBO 80G

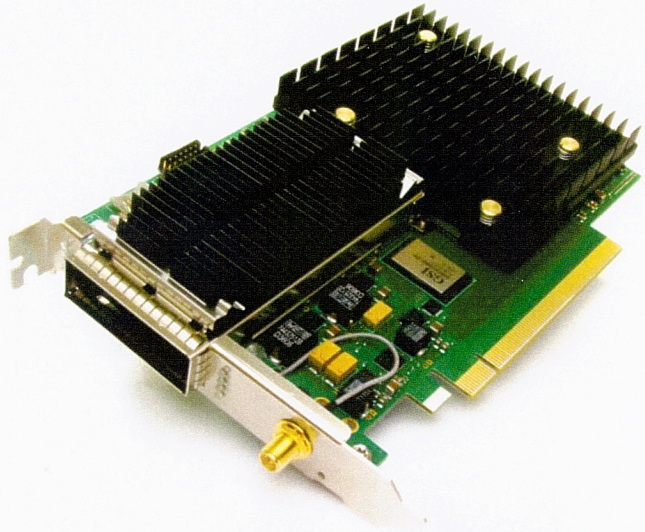
- Xilinx Virtex 7 – XC7VX690T
- Dual port 40G card, 2× QSFP+ cage
- PCI Express Gen 3 x8 host interface
- 4× 10G to 40G fanout modules for 8× 10G setup
- QDRII+ SRAM, RLDRAM III, DDR3 memory
- Embedded management CPU
- PPS sync connector



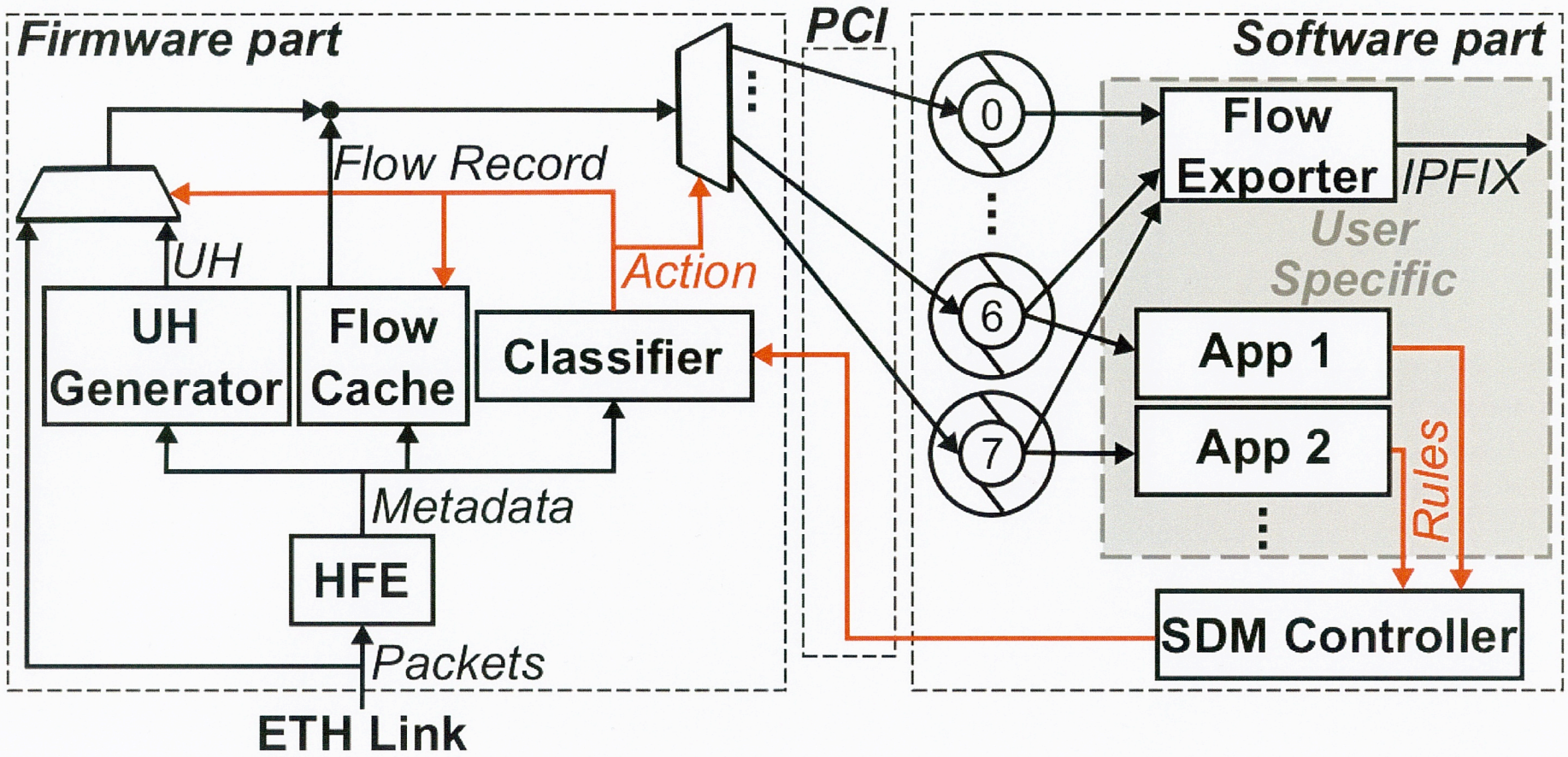
COMBO 100G

INVEATECH

- Xilinx Virtex 7 – XC7VH580T
- Single CFP2 port for 100G Ethernet
  - 100GBASE-LR4 / ER4 / SR4
- PCI Express Gen 3 x16 host interface
- QDR-IIIe SRAM memory, DDR3 DRAM memory
- parallel NOR flash for configuration
- Embedded management CPU
- PPS sync connector



Architecture



HANIC for SDM

- Fully software controlled hardware accelerator
- Network IP traffic monitoring at 100+ Gbps
- Easy deployment of new tasks without HW modifications
- Accelerated application level processing
- Special focus on interceptions
- Easy integration into existing solutions
- Delivered as an adapter and software packages

Visit us in exhibition room

INVEATECH

INVEATECH High-Speed Networking Technology Partner

Petr Kastovsky

kastovsky@invea.com

+420 774 799 726

INVEA-TECH a.s.

U Vodárny 2965/2

616 00 Brno, Czech Republic

www.invea.com