Network Traffic Monitoring & Security

*from academic project to commercial product*

Petr Špringl
springl@invea.com

Campus network monitoring and security workshop, 24.4.2014
Agenda

• INVEA-TECH Introduction
  ▪ from academic project to commercial company

• FlowMon Solution Introduction

• Typical Use Cases from Corporate Environments

• FlowMon for R&D purposes
Company Introduction

- Czech university spin-off company
- Established in 2007
- 40+ employees, $ 3M revenue
- Key focus
  - Flow Monitoring and Network Behavior Analysis
  - Hardware acceleration and FPGA Solutions
- Products deployed at 500+ customers worldwide
• CESNET started activities with programmable hardware in 2002 - project Liberouter
• Cooperation with Masaryk University and Brno University of Technology
• Targets:
  ▪ acceleration of high-speed network application (IPv6 router)
  ▪ usage of programmable hardware
  ▪ development of hardware accelerators COMBO based on FPGA technology for acceleration of critical tasks in data processing
• Participation on EU project 6NET (IST-2001-32063)
• Continuous growth and formation of strong R&D team in area of programmable hardware and high-speed network application
• Successful end of 6NET project
• Cooperation on next EU projects
• SCAMPI (IST-2001-32404)
  ▪ 2002 – 2005, network monitoring of 10Gbps lines
  ▪ joining to project in 2003 instead of commercial partners
  ▪ functional prototype developed, successful review
  ▪ recommendation – commercialize outputs in practice
• GEÁNT2 (contract No. 511082)
  ▪ cooperation of 26 NRENs from 34 countries
  ▪ activity JRA2 – focus on network security
  ▪ functional prototype of HW accelerated NetFlow probe - FlowMon
  ▪ final recommendation – monitor network by the NetFlow probe
  ▪ GEÁNT2 Security Toolset – FlowMon Probes & NfSen collector
June 2007 – INVEA-TECH was established

Technology transfer from CESNET to INVEA-TECH
- hard to find right model
- first technology transfer from CESNET

INVEA-TECH
- long way from prototype to product
- close cooperation with academic area (CESNET, Czech and abroad universities, EU projects)
Products Portfolio

• FPGA products
  ▪ COMBO cards
  ▪ NetCOPE platform
  ▪ High-speed appliances

• FlowMon solution
  ▪ Network traffic monitoring and security solution
  ▪ Flagship product
• Network Traffic Monitoring and Security solution

• DETAILED NETWORK TRAFFIC VISIBILITY
  - Do you know what's really happening in your network – not only to Internet but also in LAN and WAN? Real-time and historically?
  - Are you paying too much for Internet or WAN connection?
  - Is your network slow?

• ANOMALY DETECTION (based on Network Behavior Analysis - NBA)
  - Do you easily detect DOS/DDOS, and attacks against services?
  - What about APTs, zero-day attacks and polymorphic malware?
  - Are you able to reveal viruses/malware not detected by antivirus?
• Based on **IP flows monitoring (NetFlow v5/v9 and IPFIX technology)**

• Provides information about **who** communicates with **whom**, **how long**, **what protocol**, **traffic volume** and more

• **Network Behavior Analysis (NBA)** detects network anomalies, suspicious behavior, changes in behavior and any suspicious communication
FlowMon Architecture

- FlowMon Probes
  - source of network statistics (NetFlow, IPFIX)
- FlowMon Collectors
  - visualization and evaluation of network statistics
- FlowMon ADS
  - detection of attacks, anomalies and undesirable behavior
FlowMon Probe

• High-performance standalone probe - source of IP flow records in NetFlow v5,9 and IPFIX format
• 1U rack appliance / VMware appliance
• Leadership in performance
  ▪ wire-speed models
• Up to 6x 1G, 8x 10G, 2x 40G, 1x 100G monitoring interfaces
• 10MbE to 100GbE, IPv4/IPv6, MPLS, VLAN, GRE ...
• Application detection (NBAR2), VoIP (SIP/RTP), URLs, network performance monitoring (ART, SRT, Delay)…
FlowMon Collector

• Appliance for flow data storage & analysis
  ▪ 1U/2U/VMware appliance
• NetFlow v5/v9, IPFIX, sFlow, Netstream... support
• Based on nfdump/NfSen, but completely redesigned and you wouldn’t recognize it
• Tuned & optimized to be suitable for the largest networks (>200k fps)
FlowMon Collector

- More user friendly, automation, optimizations
- Automatic flow data source detections
- User defined dashboard
- Improved Top N statistics
- Enhanced alerting
- Intelligent reporting - online/email, PDF/CSV
- IPFIX support, extended about lot of fields
- Fast & easy configuration
FlowMon ADS

- **System for automatic network traffic analysis**
  - Detection of security & operational incidents and suspicious behavior

- **Undesirable patterns in communications**
  - Internal and external attacks
  - Undesirable services & applications
  - Operational & configuration problems

- **Behavior Analysis**
  - Behavior profiles
  - Anomalies detection
Detection of undesirable patterns in communication

- **Attacks** (port scanning, dictionary attacks, denial of service, telnet protocol)
- **Data traffic anomalies** (DNS, multicast, non-standard communications)
- **Device behavior anomalies** (changes in long-term device behavior profile)
- **Undesirable applications** (P2P networks, instant messenger, anonymizer)
- **Internal security problems** (viruses, spyware, botnets)
- **Mail traffic** (outgoing spam)
- **Operational problem** (delays, high traffic, reverse DNS records)
• Behavior analysis
  - Behavior profile (client/server, data traffic, partners, traffic structure)
  - Anomaly detection (actual behavior against long-term profile)
  - Statistics information (continues indicators about network behavior)
Use Cases

Typical real use cases from our customers
DDoS from Spoofed IPs

- Finance institutions
- Several workstations infected by botnet
- Spoofed China IPs attack to Vietnam
Authentication Attack

- Healthcare
- Attacker IP somewhere from Indonesia
- Attacks against phpMyAdmin web application
- Exposed to public Internet but not necessary

Event details:
- Type: Web form attack (HTTPDICT)
- Event source: 202.61.105.246
- Probability: 100%
- False positive: No
- Event source host name: NV
- NetFlow source: CORE

Detail: The server (target) has sent the 1.65 KB file 591 times.
Policy violations

- Manufacturing
- TOR (Onion router) client on laptop
- Use is bypassing security measures
  - To access resources blocked by company policy
DNS Changer

- Information technology
- Change of DNS server that is being used
- Attacker can manipulate with DNS records and redirect the user to malicious or phishing sites
Data Leakage

- Retail
- Employee leaving the company
- Internal documents were stored on public data share service hosted by Yahoo
- Detected as data upload from LAN to the Internet
- Inspected and evaluated as serious issue
Sniffing of Network Traffic

• Services
• Malware use DHCP spoofing to introduce itself as gateway and to sniff the traffic
R&D Cooperation

FlowMon Community program
Target
- Enable users to make program changes to FlowMon solution
- Don't provide closed NetFlow based solution, but rather provide possibilities to use it for further R&D in area of traffic monitoring, customize according to needs

Open to any applicant
- Just ask for joining and get update package to FlowMon appliance (open the API)

Main benefits
- Join to community around FlowMon solution
- Access to all plugins developed in the Community program
- Knowledge base, share experience, discussions...
• Customization of FlowMon Probe
  ▪ FlowMon exporter provide API for users plugins which can directly influence process of monitoring, generation and export of flow data
    □ packets parsing, processing and storing to internal structures
    □ computations over the flow data
    □ data storing and export to collector

• Customization of FlowMon Collector
  ▪ realized through plugins to NfSen application
  ▪ usage of NfSen API
• University of Twente
  - SURFmap plugin  
    (http://sourceforge.net/p/surfmap/home/Home/)
  - Collector plugin
  - Adds a geographical dimension to network traffic
  - Based on the Google Maps API
• **University of Twente for SURFnet**
  - Monitoring Ethernet Networks Using IPFIX
  - Probe plugin
  - Probes monitor traffic at Ethernet-layer and use a modified process of flow creation
    - key-fields - SRC and DST MAC, VLAN ID and Ethernet type
  - Provide an overview of all traffic protocols operating on top of Ethernet (ARP, LLDP, STP, Novell IPX, ...)

<table>
<thead>
<tr>
<th>Start time - first seen</th>
<th>End time - last seen</th>
<th>src MAC address</th>
<th>dst MAC address</th>
<th>TYPE</th>
<th>VLAN</th>
<th>EHL</th>
<th>EPL</th>
<th>IN</th>
<th>CVLAN</th>
<th>CP</th>
<th>P</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-12-12 12:21:34.584</td>
<td>2010-12-12 12:24:52.785</td>
<td>00:0e:20:61:08:00</td>
<td>01:00:5f:fa:df:e7</td>
<td>0x0000</td>
<td>14</td>
<td>1356</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1132</td>
<td>155840</td>
</tr>
<tr>
<td>2010-12-12 12:21:37.398</td>
<td>2010-12-12 12:25:21.079</td>
<td>00:1e:40:1a:8f:ce</td>
<td>01:00:5f:fe:de:e4</td>
<td>0x0000</td>
<td>14</td>
<td>1356</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>58</td>
<td>79460</td>
</tr>
<tr>
<td>2010-12-12 12:21:38.232</td>
<td>2010-12-12 12:25:18.888</td>
<td>00:1e:40:1a:8f:ce</td>
<td>01:00:5f:fe:de:bc</td>
<td>0x0000</td>
<td>14</td>
<td>1356</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>64</td>
<td>87600</td>
</tr>
<tr>
<td>2010-12-12 12:21:47.047</td>
<td>2010-12-12 12:24:38.847</td>
<td>00:23:df:8a:10:88</td>
<td>01:00:5f:fe:7f:fd:00</td>
<td>0x0000</td>
<td>14</td>
<td>54</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>188</td>
</tr>
<tr>
<td>2010-12-12 12:21:49.931</td>
<td>2010-12-12 12:25:10.067</td>
<td>00:1e:40:1a:8f:ce</td>
<td>01:00:5f:fe:00:fe</td>
<td>0x0000</td>
<td>14</td>
<td>203</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1299</td>
</tr>
<tr>
<td>2010-12-12 12:22:31.976</td>
<td>2010-12-12 12:24:47.107</td>
<td>00:1e:40:1a:8f:ce</td>
<td>01:00:5f:cb:57:57</td>
<td>0x0000</td>
<td>14</td>
<td>46</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>2010-12-12 12:23:11.976</td>
<td>2010-12-12 12:24:47.107</td>
<td>00:0e:20:61:08:00</td>
<td>01:00:5f:cb:57:57</td>
<td>0x0000</td>
<td>14</td>
<td>46</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>240</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EHL</th>
<th>... ethernetHeaderLength</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPL</td>
<td>... ethernetPayloadLength</td>
</tr>
</tbody>
</table>
FlowMon solution provides data flow monitoring
- Network operational monitoring
- Network security monitoring

Suitable even for the largest networks
Can be used for further R&D in area of flow monitoring and security
Petr Špringl
springl@invea.com
+420 724 899 760

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com

High-Speed Networking Technology Partner