

NetFlow Data Visualization Based on Graphs

Pavel Minarik, Tomas Dymacek

ICS MUNI, Mycroft Mind

September 8, 2008

Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute



- Mycroft Mind, Brno, Czech Republic

Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute
 - Research and development of information and communication technologies

- Mycroft Mind, Brno, Czech Republic



Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute
 - Research and development of information and communication technologies
 - Focus on network security

- Mycroft Mind, Brno, Czech Republic



Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute
 - Research and development of information and communication technologies
 - Focus on network security
- Mycroft Mind, Brno, Czech Republic
 - University spin-off company



Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute
 - Research and development of information and communication technologies
 - Focus on network security
- Mycroft Mind, Brno, Czech Republic
 - University spin-off company
 - Addressing the problems of Visual Analytics



Who we are. What we do.



- Institute of Computer Science, Masaryk University, Brno, Czech Republic
 - University Institute
 - Research and development of information and communication technologies
 - Focus on network security



- Mycroft Mind, Brno, Czech Republic
 - University spin-off company
 - Addressing the problems of Visual Analytics
 - Development of a platform for the processing, integration, analysis and visualization of information

Network security in our point of view

1 Visualize

- To be able to understand network behavior
- To be able to discover and describe behavior patterns

2 Recognize

- Based on NetFlow (Layer 3) data because deep packet inspection is useless in the case of encrypted traffic.
- Using knowledge from the visualization step

Motivation

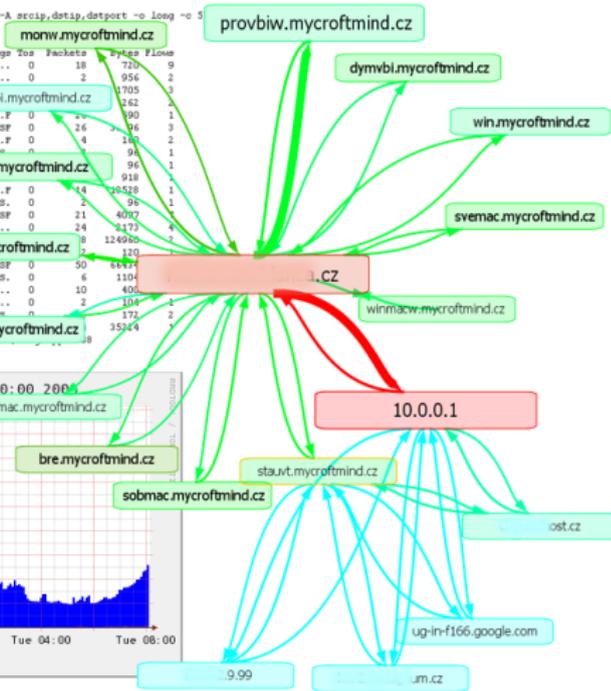
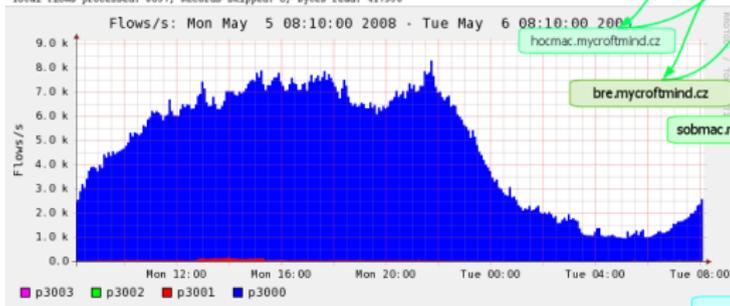
- NetFlow data
 - Layer 3 communication statistics
 - NetFlow record: Source IP, Source port, Destination IP, Destination port, Protocol, Bytes, Packets, Flags, ...
 - Cisco standard
- Integration of data sources and tools from the network domain
 - DNS, WHO IS, port information records
 - Ping, Trace route, NMAP integration
- Graph-based visualization
 - Suitable level of detail between plain text log file and statistical graphs
 - Efficient method for the inspection and analysis of security incidents

Methods example

```

** nfdump -M /data/nfsen/profiles-data/live/p3001 -T -r 2008/05/05/nfsenpd.200805052010 -a -A scip,dstip,dstport -o long -o 5
nfdump filter:
easy
Date flow_start      Duration Proto      Src IP Addr:Port      Dest IP Addr:Port      Flags Win  Packets      Bytes  Flows
2008-05-05 20:09:58.181 1.965  0          17.26.0      -> 5.37.80      .A...  0  18  720  9
2008-05-05 20:09:58.094 0.138  0          16.30.0      -> 5.37.80      .AP... 0  2  956  2
2008-05-05 20:09:58.131 1.923  0          209.170.0    -> 5.37.80      .A...  0  2  956  2
2008-05-05 20:09:58.282 0.700  0          149.16.0     -> 5.37.80      .A...  0  2  956  2
2008-05-05 20:09:58.338 0.015  0          5.37.0       -> 7.12.59336   .AP..F 0  2  990  1
2008-05-05 20:09:57.987 1.098  0          5.37.0       -> 209.170.7897 .AP.SF 0  26  996  3
2008-05-05 20:09:58.594 0.000  0          5.37.0       -> 153.203.28418 .A...F 0  8  240  2
2008-05-05 20:09:58.653 0.000  0          5.37.0       -> 153.203.28418 .A...F 0  8  96  1
2008-05-05 20:09:58.676 0.000  0          5.37.0       -> 153.203.28418 .A...F 0  8  96  1
2008-05-05 20:09:58.677 0.027  0          5.37.0       -> 153.203.28418 .A...F 0  14  918  1
2008-05-05 20:09:57.603 0.145  0          5.37.0       -> 209.170.7754  .AP..F 0  14  4528  1
2008-05-05 20:09:58.649 0.000  0          5.37.0       -> 153.203.28637 .AP.S.  0  2  96  1
2008-05-05 20:09:58.594 1.631  0          153.203.0    -> 5.37.80      .AP.SF 0  21  4077  1
2008-05-05 20:09:58.331 1.902  0          72.210.0     -> 5.37.80      .AP... 0  24  2473  4
2008-05-05 20:09:57.586 2.290  0          5.37.0       -> 17.26.0      .A...F 0  7  12408  1
2008-05-05 20:09:59.002 0.900  0          5.37.0       -> 5.37.0       .A...F 0  5  120  1
2008-05-05 20:09:59.032 1.165  0          5.37.0       -> 209.170.10596 .AP.SF 0  50  16471  1
2008-05-05 20:09:58.643 0.090  0          5.37.0       -> 153.203.28636 .AP.S.  0  6  1104  1
2008-05-05 20:09:55.649 1.130  0          20.19.0      -> 5.37.80      .A.P..  0  10  400  1
2008-05-05 20:09:52.923 0.000  0          5.37.0       -> 5.37.80      .A...  0  2  104  1
2008-05-05 20:09:59.002 1.278  0          5.101.0      -> 5.37.80      .A...  0  2  172  2
2008-05-05 20:09:58.513 0.699  0          149.9.0       -> 5.37.0       .A...  0  18  3524  1
Summary: total flows: 50, total bytes: 324311, total packets: 387, avg hps: 35245
Time window: 2008-05-05 20:09:31 - 2008-05-05 20:14:57
Total flows processed: 8037, Records skipped: 0, Bytes read: 417934

```



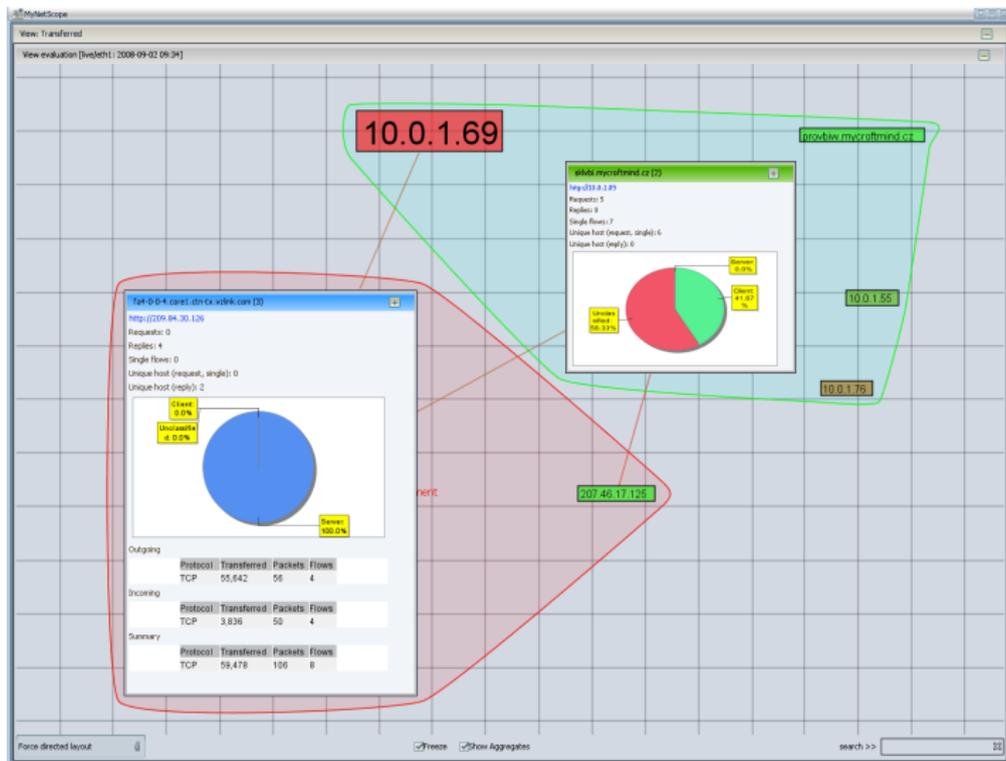
Key principles

- Nodes represent IP addresses
- Edges represent communication between two IP addresses
- Dynamic visualization adjustment
 - Node size, shape and color
 - Edge size and color
 - Decorators

Graph-based visualization in practice

- This method is used by Mycroft Mind in its network visualization tool NFVis (NetFlow Visualizer)
- NFVis is available as a plug-in for Layer 3 network probe
- Short preview ...

Nested visualization



Institute of Computer Science MUNI (www.ics.muni.cz)
Pavel Minarik (pavel.minarik@mail.muni.cz)

Mycroft Mind (www.mycroftmind.com)
Tomas Dymacek (dym@mycroftmind.com)

Thank you for listening.

Any questions?