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

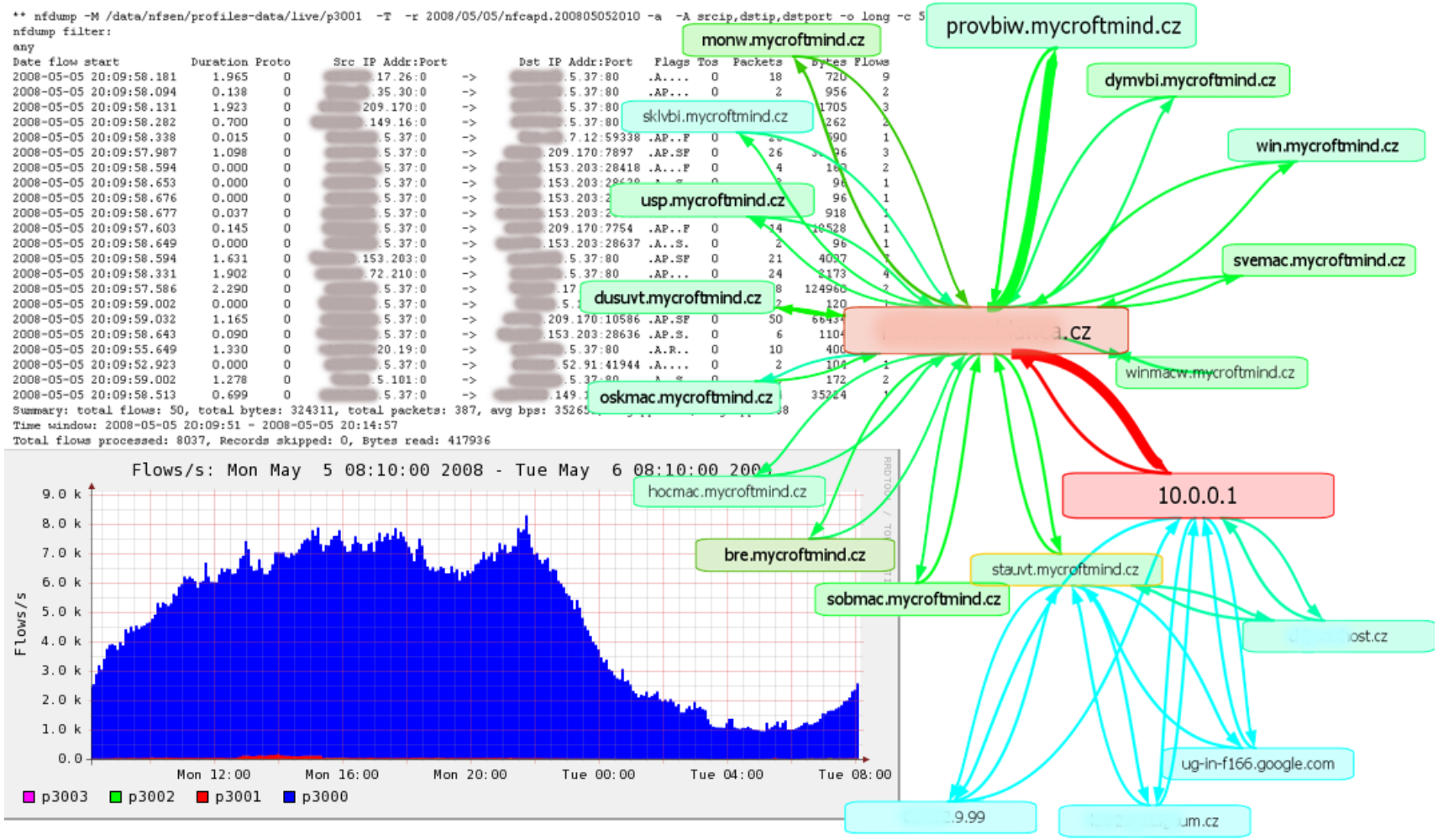
Network security in our point of view

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



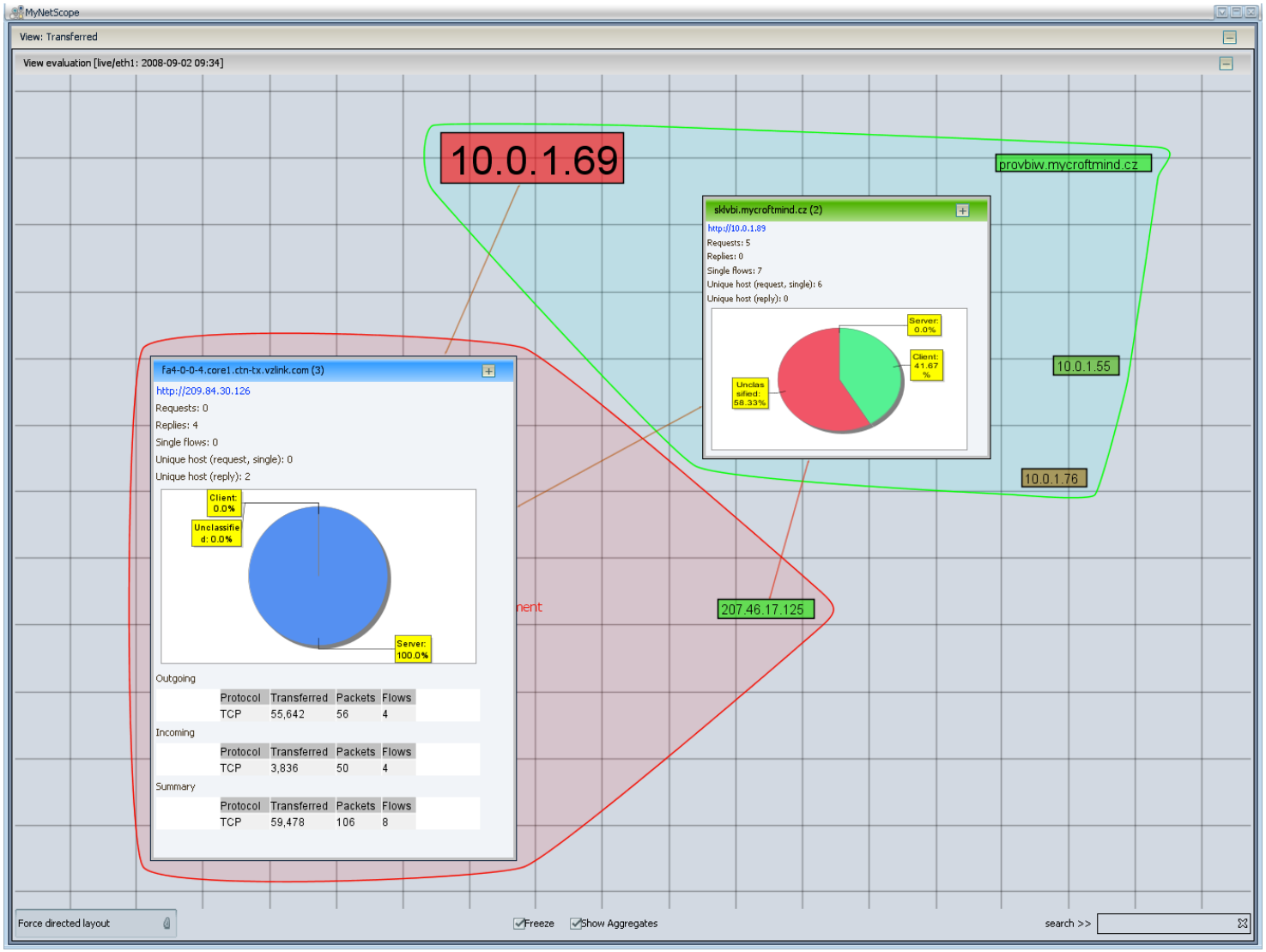
Key principles

- 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?