

# David Plonka

Computer Sciences Department  
University of Wisconsin - Madison  
1210 West Dayton Street  
Madison, WI 53706  
email: plonka@cs.wisc.edu  
<http://www.cs.wisc.edu/~plonka/>

## Research Interests

Internet traffic measurement and anomaly detection, Internet protocols, network management, security vulnerabilities, and software design.

## Education

Pre-dissertator pursuing Ph.D. Computer Science, in progress  
University of Wisconsin - Madison, Madison, WI  
Advisor: Paul Barford

**M.S. Computer Science** December, 2008  
University of Wisconsin - Madison

**B.S. Computer Science and Artificial Intelligence majors, *magna cum laude*** May, 1991  
Carroll College (now Carroll University), Waukesha, WI

## Professional Experience

**Computer Sciences Department, University of Wisconsin**, Madison, WI 2006 - present  
Fellow (2009 - present), Research Assistant

**Division of Information Technology, University of Wisconsin** 2006 - present  
Student Programmer (Network Services)

**Computer Sciences Department, University of Wisconsin** 2001 - 2006  
Co-manager of the Wisconsin Advanced Internet Laboratory

**Division of Information Technology, University of Wisconsin** 1997 - 2006  
Senior Systems Programmer / Network Engineer, Systems Programmer

**McHugh Freeman (now RedPraire Corporation)**, Waukesha, WI 1991 - 1997  
Lead Systems Programmer, Systems Programmer

## Consulting Experience

Independent Consultant, Madison, WI 1997 - 1999, 2009 - present

## Awards and Honors

Lawrence H. Landweber NCR Fellowship in Distributed Systems 2009

Student Travel Grants: USENIX LISA and ACM IMC Conferences 2007, 2008, 2009

USENIX 21st Large Installation System Administration Conference (LISA '07), **Best Paper Award** 2007

Carroll College Computer Science Department, **Outstanding Computer Science Student** 1991

## Professional Activities

### Chair

Internet Protocol Flow Information eXport (IPFIX) Working Group co-chair, 2001 - 2006  
Internet Engineering Task Force (IETF)

### Program Committees

USENIX Large Installation System Administration Conference (LISA) 2008, 2009  
ACM Workshop on Network Data Anonymization (NDA) 2008  
IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON) 2006

### Panelist

National Science Foundation 2009

### Other Service

Internet2 Network Research Review Committee (NRRC) 2009 - present

### Memberships

Association for Computing Machinery (ACM) 2002 - , 2008 - present  
IEEE 2008 - present

## Refereed Conference and Workshop Publications

1. David Plonka and Andres Jaan Tack. "An Analysis of Network Configuration Artifacts", In *Proceedings of the USENIX 23rd Large Installation System Administration Conference (LISA '09)*, Baltimore, November, 2009. 35% accept rate.
2. David Plonka, Paul Barford. "Context-aware Clustering of DNS Query Traffic", In *Proceedings of the ACM SIGCOMM / USENIX Eighth Internet Measurement Conference (IMC 2008)*, Vouliagmeni, Greece, October, 2008. 17% accept rate.
3. Jeff Kline, Sangnam Nam, Paul Barford, David Plonka, Amos Ron. "Traffic Anomaly Detection at Fine Time Scales with Bayes Nets", In *Proceedings of the IEEE Third International Conference on Internet Monitoring and Protection (ICIMP 2008)*, Bucharest, Romania, June/July, 2008. 23% accept rate.
4. David Plonka, Archit Gupta, Dale Carder. "Application Buffer-Cache Management for Performance: Running the World's Largest MRTG", In *Proceedings of the USENIX 21st Large Installation System Administration Conference (LISA '07)*, Dallas, November, 2007. **Best Paper Award winner.**
5. David Mills, Judah Levine, Richard Schmidt, David Plonka. "Coping with Overload on the Network Time Protocol Public Servers", In *Proceedings of the 36th Annual Precise Time and Time Interval Systems and Applications Meeting (PTTI 2004)*, Washington, D.C., December, 2004.
6. Vinod Yegneswaran, Paul Barford and David Plonka. "On the Design and Use of Internet Sinks for Network Abuse Monitoring", In *Proceedings of the Symposium on Recent Advances in Intrusion Detection (RAID '04)*, pp. 146-165, Sophia Antipolis, France, September, 2004. 20% accept rate.
7. Paul Barford, Jeff Kline, David Plonka, Amos Ron. "A Signal Analysis of Network Traffic Anomalies", In *Proceedings of ACM SIGCOMM Internet Measurement Workshop '02*, pp. 71-82, Marseilles, France, November, 2002. 42% accept rate.
8. Paul Barford and David Plonka. "Characteristics of Network Traffic Flow Anomalies", In *Proceedings of ACM SIGCOMM Internet Measurement Workshop '01*, pp. 69-73, San Francisco, November, 2001. 26% accept rate.
9. Dave Plonka. "FlowScan: A Network Traffic Flow Reporting and Visualization Tool", In *Proceedings of the USENIX 14th Systems Administration Conference (LISA 2000)*, New Orleans, December, 2000.

## Other Publications

### Internet RFC Documents

1. David Plonka. Best Current Practice 105, RFC 4085: “Embedding Globally-Routable Internet Addresses Considered Harmful”, Internet Engineering Task Force, June, 2005.

### Invited Papers

1. David Plonka and Paul Barford. “Network Anomaly Confirmation, Diagnosis and Remediation”, In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton Conference 2009)*, Monticello, Illinois, September/October, 2009.

### Journals and Periodicals

1. Dave Plonka. “An Analysis of Napster and Other IP Flow Sizes”, *Network Analysis Times*, April, 2001.
2. Dave Plonka. “How I Recovered Data I Thought I’d Lost”, *Sys Admin - the Journal for UNIX Systems Administrators*, August, 2000.
3. Dave Plonka. “Sys Admin File Revision Control with RCS”, *Sys Admin - the Journal for UNIX Systems Administrators*, December, 1998.
4. Dave Plonka. “Managing System Administration Tasks Using GNATS”, *Sys Admin - the Journal for Unix Systems Administrators*, February, 1997.

### Online Technical Reports

1. Aaron Bergstrahl, Erik Paulson, and David Plonka. “Bill-Pay Control: An Interactive User Interface to Select IP Service Quality”, December, 2006.
2. Dave Plonka. “Flawed Routers Flood University of Wisconsin Internet Time Server”, August, 2003.
3. Dave Plonka. “UW-Madison Napster Traffic Measurement”, March, 2000.

## Invited Talks and Workshops

1. Invited talk, “Rendezvous-based Network Traffic Analysis”, Lockdown 2009 Conference, UW-Madison, Madison, Wisconsin, July, 2009.
2. Invited talk, “Rendezvous-based Network Traffic Analysis”, Massachusetts Institute of Technology, Cambridge, Massachusetts, February, 2009.
3. Invited talk, “Rendezvous-based Network Traffic Analysis”, Boston University, Boston, February, 2009.
4. Invited talk, WiP: “Network Admins are Programmers: An Analysis of Network Management Artifacts”, LISA 2008, San Diego, November, 2008.
5. Invited talk, BoF: “DNS and Network Traffic Analysis with TreeTop”, LISA 2008, San Diego, November, 2008.
6. Invited participant and session moderator, “NSF NeTS Future Internet Design (FIND) Student Meeting”, Seattle, August, 2008.
7. Invited talk, “Application Buffer-Cache Management for Performance: Running the World’s Largest MRTG”, Madison Chapter of The League of Professional System Administrators (LOPSA-Madison) Meeting, Madison, Wisconsin, January, 2008.
8. Invited participant, “Wisconsin Entrepreneurial Bootcamp”, UW-Madison, Madison, Wisconsin, July/August, 2007.

9. Invited talk, "Anomalous Traffic from Internet Consumer Products", ESCC/Internet2 Joint Techs Workshop, Madison, Wisconsin, July, 2006.
10. Invited talk, "Get Your FIX: Flow Information eXport Analysis and Visualization", ESCC/Internet2 Joint Techs Workshop, Madison, Wisconsin, July, 2006.
11. Invited panelist, "12 Hot Research Topics in Monitoring and Measurements", Fourth IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON'06), Vancouver, Canada, April, 2006.
12. Invited talk, "AANTS: Web-Based Tools for Cooperative Campus Network Administration", Fall 2005 Internet2 Member Meeting, Philadelphia, September, 2005.
13. Invited participant, Sampling 2005 Workshop, Paris, July, 2005.
14. Invited talk, "Exposing Abuse in Internet Traffic Measurements", Lockdown 2005 Conference, UW-Madison, Madison, Wisconsin, July, 2005.
15. Invited talk, "Flow-based Measurements and Other Means to Expose Internet Pathology", Institut Eurecom, Sophia Antipolis, France, December, 2004.
16. Invited talk, "Bare-Bones Measurement Data Archiving", ISMA Data Catalog 2004 Workshop, CAIDA/SDSC, La Jolla, California, June, 2004.
17. Invited talk, "Embedding Globally-Routable Internet Addresses Considered Harmful", Global Routing Operations (GROW) Working Group, 58th IETF meeting, Minneapolis, November, 2003.
18. Invited talk, "A Case Study in Internet Pathology: Flawed Routers Flood University's Network", LISA 2003, San Diego, October, 2003.
19. Invited talk, "Flawed Routers Flood University of Wisconsin Internet Time Server", NANOG 29, Chicago, October, 2003.
20. Invited talk, "IP Flow Measurement and Analysis with FlowScan", Duke University, Durham, North Carolina, September, 2003.
21. Invited talk, "A Case Study in Internet Pathology: Flawed Routers Flood University's Network", Duke University, Durham, North Carolina, September, 2003.
22. Invited talk, "Flawed Routers Flood University of Wisconsin Internet Time Server", MAD-SAGE meeting, Madison, Wisconsin, August, 2003.
23. Invited talk, "Internet Sink Deployments", IEPG meeting, Vienna, Austria, July, 2003.
24. Invited talk, "IP Flow Measurement and Analysis with FlowScan", IPAM Mini-Workshop on "Internet-wide Measurements", Los Angeles, March, 2002.
25. Invited talk, "FlowScan at the University of Wisconsin-Madison", EDUCAUSE 2001, Indianapolis, October, 2001.
26. Invited talk, "Practical Flow-based Passive Measurements and FlowScan", Computer Sciences Department Network Seminar, UW-Madison, Madison, Wisconsin, June, 2001.
27. Invited talk, "Better Campus Network Health Through Instrumentation", UW System Network Operators Meeting, Madison, Wisconsin, March, 2001.
28. Invited talk, "FlowScan - LIVE!", NANOG 21, Atlanta, February, 2001.
29. Invited talk, "FlowScan - a Network Traffic Reporting and Visualization Tool", MAD-SAGE meeting, Madison, Wisconsin, November 2000.

30. Invited talk, BoF: “Flow-based Passive Measurements”, CANARIE/NLANR/Internet2 Techs Workshop, Toronto, August, 2000.
31. Invited talk, “Unix Security”, UW-Madison Unix Fair, Madison, Wisconsin, August, 1999.
32. Invited participant, CAIDA ISMA Workshop on “Passive Measurement Data and Analysis”, La Jolla, California, January, 1999.
33. Invited talk, “Unix Security Basics and Tools - an Introduction”, UW-Unix meeting, Madison, Wisconsin, April, 1998.

## Patents

1. Paul Barford and David Plonka. “Apparatus and Method for Classifying Network Packet Data”, U.S. Patent pending, 2009.
2. Paul Barford, Jeff Kline, Sangnam Nam, David Plonka and Amos Ron. “Multi-resolution Methods for Network Anomaly Detection”, U.S. Patent pending, 2007.
3. Vinod Yegneswaran, Paul Barford and David Plonka. “Scalable Monitor for Malicious Network Traffic”, U.S. Patent pending, 2005.

## Teaching Experience

**Computer Sciences Department, University of Wisconsin**, Madison, WI

CS 640 - Introduction to Computer Networks

Fall 2008, Fall 2009

Guest lectures on Ethernet, Wireless Ethernet, IP Multicast, TCP

## Available Software

The following software packages are available at: <http://net.doit.wisc.edu/~plonka/packages.html>

### **fincore**

fincore (“File IN CORE”) is a command that shows which pages (blocks) of a file are in core memory. It is particularly useful for determining the contents of the buffer-cache.

### **FlowScan**

FlowScan is a system to analyze and report on flows exported by IP routers and collected using flow-tools, argus, cflowd, etc. It could also be considered a “front-end” for RRDTOOL.

### **RRGrapher**

RRGrapher is a CGI graphing tool for RRDTOOL. It’s basically an interactive web graph construction set.

### **Net::Patricia**

This is a perl API to a Patricia Trie data structure to perform fast lookups by IP address. Patricia Trie is the data structure used by the BSD kernel routing code where it is named “radix.”

### **junipoll**

junipoll is a JUNIper router snmp POLLer. It is an mrtg-like utility that polls the counter values from the firewall filters configured on Juniper routers.

### **Spectrum::CLI**

This is a perl module/class that provides a way to invoke the functionality of Spectrum Enterprise Manager’s Command Line Interface.

**headers**

This is a utility to identify C header files that should be included in C source files. You run it on your C source files, and it looks for your use of ANSI or POSIX identifiers and generates include directives for those source files.

**Altoids**

This is a distribution of my perl module that provides SNMP get/walk functionality with built-in name to OID translation alternatively by using .oid files.

**Cflow**

Cflow is a perl module for analyzing flow files written by flow-tools, argus, cflowd, etc.

**IOSchat / getcnf**

This is a distribution of my perl module that provides the ability to “chat” (ala expect(1), chat2.pl, or Comm.pl) with Cisco Internet Operating System routers. The getcnf utility, probably the useful component of this package, uses IOSchat to get the flash and/or running configuration. This output is suitable for storing in an RCS revision file, or to diff(1) to discover configurations changes.

**NetCMS**

NetCMS is a Network Configuration Management System for network devices. It supports various hardware including Cisco routers and switches.

**NetTree**

NetTree is a perl package to encapsulate the subnet allocations within a network. If you’re a hostmaster that manages a large number of subnets it may be useful to you to be sure that you don’t define overlapping subnets and such.

**find\_revisions**

find\_revisions is a reporting utility for use with RCS. This is the accompanying code for my article “Sys Admin File Revision Control with RCS” from the December 1998 issue of Sys Admin magazine.

**ipwatch**

ipwatch is a perl script that maintains a simple database of IP addresses that it has “seen.” It was written to help discover which IP addresses can be recovered by observing that they were not in use over some specified period of time - e.g. 1 month. (Once this tool is adopted, its data file serves as a rudimentary database to track assignment of IP addresses.)

ipwatch uses two methods to determine if a given IP address is in use: (1) by sending ICMP echoes (pings) and waiting for responses, and (2) by examining the ARP cache of specified routers or switches, via SNMP.

**physaddrwatch**

physaddrwatch is a perl script that maintains a simple database of physical media addresses (MAC or ATM) that it has “seen” and the IP or AppleTalk address to which they belong. It does this by walking various tables via SNMP on gateways (routers) that you specify.

**iftop**

iftop shows router top interfaces in real time, similarly to the way the Unix top command displays top CPU processes. This script is supplied with Simon Leinen’s “SNMP in Perl” distribution.

**ip2anonip**

ip2anonip is a perl script that can be used to anonymize or obfuscate IP addresses or translates IP addresses to hostnames, like ip2hostname. The anonymization employs the prefix-preserving technique implemented in tcpdpriv.

**stpgraph**

stpgraph is a grapher for ethernet networks utilizing the spanning tree protocol.

## **Personal Information**

Amateur radio station N9HZF operator.

Bicyclist and recreational inline skater.

Amateur artist, visual media.