Computer Science and Engineering Department
University of California, San Diego
9500 Gilman Drive
La Jolla, California 92093-0114
858-822-2594
cestan@cs.ucsd.edu

Cristian Estan

Research interests

Computer networking with emphasis on **traffic measurement and analysis**; using measurement and analysis to detect malicious activities such as worms; applying algorithmic, statistical and data mining methods to detect informative traffic patterns.

Education

Ph.D., Computer Science and Engineering — October 2003
University of California, San Diego

M. Sc., Computer Science — June 1996
Technical University of Cluj-Napoca, Romania

Engineer (5 year program), Computer Science — June 1995
Technical University of Cluj-Napoca, Romania

Awards and Honors

SIGCOMM 2002 paper forwarded to IEEE Transactions on Networking (5 out of 25 SIGCOMM papers selected)

Internet Measurement Conference 2003 paper forwarded to IEEE Transactions on Networking (4 out of 19 full IMC papers selected)

SOSP 2003 poster selected for oral presentation (4 out of 36 SOSP posters selected)

Scholarship for completing diploma project at Politecnico di Torino, Italy, Spring 1995 (3 awards out of 80 students)

University programming team for ACM Eastern European Programming Contest (Fall 1994) and National Programming Contest (Spring 1994)

Publications

Journal papers

C. Estan, G. Varghese, "New Directions in Traffic Measurement and Accounting: Focusing on the Elephants, Ignoring the Mice", *ACM Transactions on Computer Systems, August 2003*

Conference and workshop papers

C. Estan, K. Keys, D. Moore and G. Varghese, "Building a better NetFlow", *SIGCOMM, August 2004 (acceptance ratio 31/340)*

C. Estan, S. Savage and G. Varghese, "Automatically Inferring Patterns of Resource Consumption in Network Traffic", *SIGCOMM, August 2003 (acceptance ratio 33/319)*

C. Estan and G. Varghese, "New Directions in Traffic Measurement and Accounting", *SIGCOMM, August 2002 (acceptance ratio 30/300)*

C. Estan, G. Varghese, M. Fisk, "Bitmap Algorithms for Counting Active Flows on High Speed Links", *Internet Measurement Conference, October 2003 (acceptance ratio 33/109)*

G. Varghese and C. Estan, "The Measurement Manifesto", *HotNets-II Workshop on Hot Topics in Networks, November 2003 (acceptance ratio 23/119)*

C. Estan and G. Varghese, "Data Streaming in Computer Networking", *Workshop on Management and Processing of Data Streams, June 2003 (acceptance ratio17/36),* short paper

Other notable work

S. Singh, C. Estan, G. Varghese, S. Savage, "Automated Worm Fingerprinting", *SOSP, October 2003,* student poster

C. Estan, "AutoFocus: A Tool for Automatic Traffic Analysis", talk at the *29th meeting of the North American Network Operators' Group, October 2003*

C. Estan, "Computer Network Design", text used for laboratory sections at Technical University of Cluj-Napoca since 1997

Patents

X. W. Huang, C. Estan and S. Keshav, "Method and System to Provide Multiple Virtual Superusers in an Operating System", patent pending – filed by Ensim Corporation in August 2000

Professional Experience

UCSD CSE Department, San Diego, CA September 2000 – present
Post-doc October 2003 – present
Invented novel **traffic synopses**, that can be computed at high speeds and yet offer good tradeoffs between accuracy and memory consumption. Helped design, implement and evaluate EarlyBird, a system that quickly **detects unknown worms** based on their behavior, allowing fast automatic countermeasures.

Research assistant (Prof. George Varghese) September 2000 – October 2003
Designed and implemented AutoFocus, a traffic analysis application that can mine network traffic for **traffic clusters** – patterns of conspicuous resource consumption such as dominant pairs of networks, denial of service attacks, worms, etc. Despite the combinatorial explosion the underlying algorithms identify clusters across several header fields at the right granularity. *SIGCOMM* paper; invited for presentation at North American Network Operators' Group; adopted in many production networks.

Invented, analyzed and implemented **algorithmic building blocks** for systems that rely on **traffic measurement**. These algorithms operate in streaming fashion, using low amounts of memory and performing at most a fixed small number of memory

accesses per packet, so that they can be implemented in hardware at line speeds. The work on **identifying heavy hitters** resulted in an award *SIGCOMM* paper that was subsequently published in *Transactions on Computer Systems*. The work on **algorithms for counting flows** resulted in an award paper at *Internet Measurement Conference*. A library implementing them is publicly available.

Ensim Corporation, Sunnyvale, CA July 1999 – August 2000
Software developer .
One of first 15 employees, worked on Ensim's first product which implemented **virtual servers** sharing one computer (with performance superior to VMware) by intercepting system calls. Co-invented a patent pending mechanism to ensure isolation between root users of the virtual servers. Ported memory allocation functions; wrote scripts to ensure seamless interoperability with popular applications. Also worked on a second product implementing management and configuration for applications such as web, email and DNS for multiple users sharing a single server; designed most of the system and application configuration solutions; wrote backend scripts in perl.

Cornell University, CS Department August 1998 – June 1999
Research assistant (Professor S. Keshav) .
Developed the publicly available Argus **toolkit for discovering topology and delays** in the Internet by correlating the results of active probing, DNS and SNMP data.

Internet Node – Technical U. of Cluj-Napoca, Romania Dec. 1995 – June 1998
Technical director April 1997 – June 1998
Ran a major hub (connecting tens of universities and schools) of the Romanian Educational Network; kept network and services running, planned network growth, selected equipment to buy, etc.

Network engineer December 1995 – April 1997
Administered network equipment such as Cisco and Linux routers, VLAN capable Ethernet switches, and modems; administered Linux, AIX and Solaris servers running web, email, DNS, ftp, etc.

Teaching Experience

UCSD CSE123A Computer Networks (upper division undergr.) Summer 2003
Instructor
Taught all lectures, handled office hours and grading, designed all exams, coordinated TAs and wrote material presented in class for this networking course focusing on the lower layers of the network protocol stack.

UCSD CSE123B Communications Software (upper div. undergr.) Spring 2003
Teaching assistant (instructor Professor Stefan Savage) .
Graded exams, held office hours and ran discussion sessions for this class on computer networks focusing on protocols, applications and security.

UCSD CSE123A Computer Networks (upper division undergr.) Spring 2001
Teaching assistant (instructor Professor George Varghese) .
Graded exams, held office hours and ran discussion sessions.

Cornell CS542 Internet Internals (master's level) Spring 1999
Teaching assistant (instructor Professor Rosen Sharma) .

Besides regular TA duties I also taught lectures when the instructor was out of town for this class on technical and non-technical aspects of the operation of the Internet.

Cornell CS519 Engineering Computer Networks (master's level) Fall 1998
Teaching assistant (instructor Professor S. Keshav) .
Graded exams, held office hours for this comprehensive class on computer networks.

Technical University of Cluj-Napoca, Romania 1995 – 1998
Instructor for extracurricular summer class introducing the Internet
Teaching assistant for Computer Network Design (Prof. *Kálmán Pusztai*)
Teaching assistant for Data Structures and Algorithms (Prof. *Iosif Ignat*)
Advised undergraduate diploma projects for 2 students
Supervised summer internships at the Internet node for 25 students

Software

Wrote **AutoFocus,** a network traffic analysis application (C++ backend and perl scripts), and developed with Stefan Savage and George Varghese the underlying multidimensional traffic cluster analysis. Multidimensional traffic clusters in the reports generated by AutoFocus can describe the dominant applications, applications used predominantly by certain networks, denial of service attacks, worms, network scans, etc. After public announcement, AutoFocus was downloaded by 207 distinct destinations in first two months; initial feedback extremely positive. Its web based graphical intterface allows quick drill-down in arbitrary directions using filters. Publicly available from http//ial.ucsd.edu/AutoFocus/.

Wrote **bmpcount,** a C++ library implementing a family of bitmap counting algorithms that can give estimates for the number of active flows or equivalently the number of unique items in a data stream. Developed the counting algorithms implemented by the library together with George Varghese and Mike Fisk. Publicly available from http://ial.ucsd.edu/bitmaps/.

Wrote **Argus,** a topology discovery toolkit, together with Haye Chan and Walter Chang, under the supervision of S. Keshav, based on prior work by Rachit Siamwalla, Rosen Sharma and S. Keshav. Argus discovers the IP level topology of a network together with delay information by correlating results from active probing with enhanced variants of ping and traceroute, DNS and SNMP data where available. Publicly available from http://www.cs.cornell.edu/cnrg/argusbeta.tar.gz.

Professional Activities

Reviewer for Internet Measurement Conference 2003
Reviewer for Internet Measurement Workshop 2002
Reviewer for INFOCOM 2002
Reviewer for IEEE Network
Member of Association for Computing Machinery

U.S. visa status

Non-resident, F1

References

Professor **George Varghese**
Department of Computer Science and Engineering
University of California, San Diego
9500 Gilman Drive
La Jolla, CA, 92093-0114
(858) 822-0424
varghese@cs.ucsd.edu

Professor **Stefan Savage**
Department of Computer Science and Engineering
University of California, San Diego
9500 Gilman Drive
La Jolla, CA, 92093-0114
(858) 822-4895
savage@cs.ucsd.edu

Dr. **Vern Paxson**
International Computer Science Institute
1947 Center Street, Suite 600
Berkeley, CA 94704-1198
(510) 666-2882
vern@icir.org

Professor **S. Keshav**
School of Computer Science
University of Waterloo
200 University Ave West, Waterloo
Ontario Canada N2L 3G1
(519) 888-4567 x4456
keshav@uwaterloo.ca

Dr. **Jennifer Rexford**
AT&T Labs - Research
A139 180 Park Avenue
Florham Park, NJ 07932-0971
(973) 360-8728
jrex@research.att.com