Sushant Sinha

Areas of Interest Data exploration, Search Engine, Internet Security and management.

Education

University of Michigan, Ann Arbor, USA — 2003 - 2009
Ph.D. in Computer Science and Engineering
GPA: 7.4/8
Advisor: Farnam Jahanian

Indian Institute of Technology, Madras — 1998 - 2003
B.Tech and M.Tech in Computer Science and Engineering
GPA: 9.12/10
M. Tech Thesis Advisor: C. Siva Ram Murthy

Professional Experience

Indian Kanoon	Founder (indiankanoon.org)	2008 - Present
Yahoo	Technical Yahoo	2009 - Present
University of Michigan	Research Assistant	2004 - 2009
Cisco Inc., Boston	Summer Internship	2007
University of Michigan	Graduate Student Instructor (Operating Systems)	2004
TIFR, Mumbai	Summer Internship	2001

Founder - Indian Kanoon A publicly available search engine for Indian law that enables people to quickly determine the most relevant law clauses and court judgments. It brings out a number of technological innovation to make searching law documents easier and to make law more accessible to common people. It currently searches in central laws, supreme court judgments, high court judgments, tribunals, constituent assembly debates, law commission reports, and law journals. Fortunately, many people have found it useful and it receives hundred thousand unique visitors a day.

Publications

Kaustubh Nyalkalkar, Sushant Sinha, Michael Bailey, and Farnam Jahanian. A Comparative Study of Two Network-based Anomaly Detection Methods. In (mini-conference) The 30th IEEE International Conference on Computer Communications (INFOCOM '11), Shanghai, China, April 2011.

Sushant Sinha, Michael Bailey, and Farnam Jahanian. Improving SPAM Blacklisting through Dynamic Thresholding and Speculative Aggregation. In Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS '10), San Diego, California, USA, February 2010.

Sushant Sinha, Michael Bailey, and Farnam Jahanian. Shades of Grey: On the effectiveness of reputation based "blacklists", International Conference on Malicious and Unwanted Software (Malware 2008), Washington, USA, October 2008.

Sushant Sinha, Michael Bailey, and Farnam Jahanian. Shedding Light on the Configuration of Dark Addresses, Network and Distributed System Security (NDSS) Symposium, San Diego, California, USA, February 2007.

Sushant Sinha, Farnam Jahanian, and Jignesh M. Patel. WIND: Workload-aware INtrusion Detection, Recent Advances In Intrusion Detection (RAID), Hamburg, Germany, September 2006.

Michael Bailey, Evan Cooke, Farnam Jahanian, Andrew Myrick, and Sushant Sinha. Practical darknet measurement, Conference on Information Sciences and Systems, March 2006.

Sushant Sinha and C. Siva Ram Murthy. Information theoretic approach to traffic adaptive WDM networks. IEEE/ACM Transactions on Networking, vol. 13, no. 4, August 2005.

Sushant Sinha, N. Rammohan, and C. Siva Ram Murthy. Dynamic virtual topology reconfiguration algorithms for groomed WDM networks, Photonic Network Communications, vol. 9, no. 2, March 2005.

Thesis

Ph.D. Advisor: Farnam Jahanian

Thesis Title: Exploiting Deployment Context To Improve Performance and Accuracy of Network Based Security Systems

Thesis Description:

Network based security systems have become popular and are deployed in a large number of production networks. These networks exhibit significant diversity in applications, end host characteristics and traffic behavior. However, the current network based security systems have taken a "one size fits approach". As a result, they lag in performance and fail to provide an accurate threat view on a network. Our theses is that automated adaptation to the deployment context will significantly improve the performance and accuracy of network-based security systems.

M. Tech Advisor: C. Siva Ram Murthy

Thesis Title: Virtual Topology Reconfiguration for Traffic Adaptation in WDM Optical Network

Thesis Description Wavelength division multiplexing (WDM) networks provide a virtual topology of lightpaths for routing higher layer traffic such as IP/MPLS. As the higher layer traffic changes, the WDM networks are reconfigured for better throughput. However, reconfiguration of WDM networks disrupts the current traffic. Our theses is that a learning model for traffic together can provide a significantly better trade-off between resource utilization a traffic disruption.

Research Projects

Traffic-Aware Spam Blacklist Generation: Blacklists have become popular among the operational community to alter or block the explosive growth of unwanted traffic on the Internet. We performed a preliminary study on the effectiveness of spam blacklists and found that the blacklists exhibited significant amount of false negatives and non-trivial amount of false positives. We developed two techniques for blacklist generation that leverage the local mail usage in a network and global spamtrap deployment on the Internet. A deployment of context aware blacklists for over a month in a large academic network demonstrated significant improvement in blacklist accuracy.

Network-Aware Honeynet Configuration: Existing approaches to deploying honeynets largely ignore the problem of configuring operating systems and applications on individual hosts, leaving the user to configure them in a manual and often ad hoc fashion. We demonstrate that such ad hoc configurations are inadequate: they misrepresent the security landscape of the networks they are trying to protect and are

relatively easy for attackers to discover. We developed an automated way to generate honeynet configuration representative to the network and demonstrated significantly more visibility and higher resistance to discovery than current methods.

Workload-Aware Intrusion Detection: Intrusion detection and prevention systems have become essential to the protection of critical networks across the Internet. Existing approaches to signature evaluation apply statically-defined optimizations that do not take into account the network in which the IDS or IPS is deployed or the characteristics of the signature database. We developed an adaptive algorithm that systematically profiles attack signatures and network traffic to generate a high performance and memory-efficient packet inspection strategy.

Internet Motion Sensor Project: Internet Motion Sensor (IMS) is a globally-scoped threat monitoring system whose goal is to measure, characterize, and track emerging threats such as worms, denial of service attacks and network scanning activities. Developed data collection software for the distributed sensors and the web front-end for querying and aggregation of results from the sensors.

Video repair strategies for IPTV - (Cisco Inc.): Streaming television over IP networks is fast becoming a reality. However, one problem that may impede the acceptance of IPTV technology is the perceived drop in video quality. We developed and evaluated several strategies for fast and bandwidth efficient repair of the video stream.

Academic Honors

University of Michigan Fellowship, 2003.
Ranked 14th in Graduate Aptitude Test in Engineering (GATE), 2002.
Top 0.1% of students who took IIT Joint Entrance Examination, 1998.
Gold medal for being in top 35 students in Indian National Physics Olympiad 1998.
Bronze medal in Regional Mathematics Olympiad 1997.

Software Use

Languages:	Python, Java, C++, C
Software:	NGinx, Postgres, Apache, Django

Reviewed Papers

IEEE/ACM Transactions on Networking
Distributed Systems and Networks (DSN) (2005 - 2009)
Recent Advances in Intrusion Detection (RAID) (2005 - 2008)
ICCCN 2005, CSICC 2006, Network Management Systems (NMS) 2006
NetDb 2007, IEEE Security and Privacy (S&P) 2008
Computer and Communication Security (CCS) 2008,
Network and Distributed Systems Security (NDSS) 2008
Networked System Design and Implementation (NSDI) 2008