Technologies and Foundations for Robust and Secure Networked Systems

Spring 2010 Newsletter

Center for Networked Systems

When Private Keys Become Public: A Study of the 2008 Debian OpenSSL Vulnerability

The discovery of security vulnerabilities in systems and software, as well as the subsequent distribution of security patches for those 'bugs,' is a commonplace of contemporary technology lifecycles. How users and administrators respond to the discovery of software vulnerabilities has been well documented, but the rate and efficacy of such security fixes for cryptographic compromises is not so well studied.

CNS professors **Hovav Shacham** (pictured above) and **Stefan Savage** took advantage of the discovery and repair of just such a severe vulnerability in the Debian Linux version of OpenSSL in order to observe and analyze the pattern of recovery from a cryptographic breach. As reported in the Proceedings of ICM 2009, their findings focused on the continued vulnerabilities in systems after the application of the fix and on the unusually extended fixing phase of this particular bug.

OpenSSL is a widely utilized, open-source, general-purpose cryptographic library. In September 2006 the package for OpenSSL, including the Debian distribution of Linux, was changed to include a fix to eliminate uninitialized memory reads flagged by the memory-checking tool Valgrind. While it succeeded in achieving its intention, the fix also nullified OpenSSL's entropy gathering. Until the problem was reported, the accidentally introduced vulnerability severely affected the security of SSL/TLS and SSH servers. "Each server possesses a public/private keypair, but any keypairs generated on an affected machine are easily predictable to

Continues on page 3

DIY Forms-Driven Workflow Web Apps

The Do-It-Yourself revolution is invading the world of web application programming. Professor **Yannis Papakonstantinou** (at left) as principal investigator and co-PI **Alin Deutsch** were awarded an NSF grant to develop their "Do-It-Yourself Forms-Driven Workflow Web Applications." They will be developing a new pattern of interaction between application owners and programmers that will benefit organizations that require long-term web applications and data management systems and yet lack the time or financial wherewithal to develop their own proprietary applications using the conventional code development process.

The goal is to give non-programmers the tools to build rapidly their own custom data management and workflow applications with a low impact on organizational resources. The DIY project could also benefit students across campus. The proposed models of database-driven web applications will impact the education of both computer science (CS) and non-CS students who need to comprehend web applications at a high conceptual level.

CNS Members

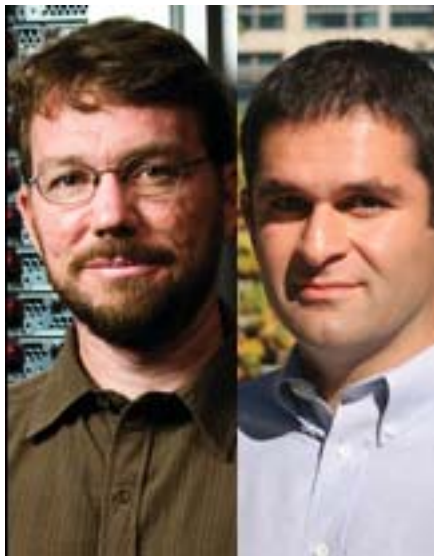
ERICSSON hp invent Google MOTOROLA QUALCOMM NetApp ORACLE CISCO

In This Issue

Gifts to CNS Faculty

Professor **Geoffrey M. Voelker** and CNS Director **Amin Vahdat** (below l-r) will be the recipients of research gifts awarded through Calit2 and made possible by the generous contributions of funds and equipment from Ericsson. The gifts, which will be awarded on an annual basis over a period of three years, will support a project of Voelker's on network security and of Vahdat's on data center networking.

Stefan Savage received gifts from both Google and Microsoft in support of his research in the area of cyber security, while continuing as principal investigator on the Collaborative Center for Internet Epidemiology and Defenses funded by NSF (see article on page 7).



2010 Google Focused Research Award for Energy Efficient Computing

Professors **Tajana Rosing** (pictured at right), **Steven Swanson** and **Amin Vahdat** lead one of only 12 research groups selected to receive a 2010 Google Focused Research Award. The award was given in support of their project "Energy Proportional Warehouse Computer," which will study energy efficiency in computing. The awards were handed out "in areas of study that are of key interest to Google as well as the research community."

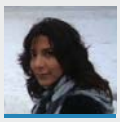
The unrestricted grants are for two to three years, and the recipients have the advantage of access to Google tools, technologies and expertise. The inaugural round of Google Focused Research Awards went to 12 projects led by 31 professors at 10 universities. In addition to energy efficient computing, the program led off with awards in three other categories: machine learning, privacy, and the use of mobile phones as data collection devices for public health and environmental monitoring. A full list of Google Focused Research Award recipients: http://research.google.com/university/relations/focused_research_awards.html.

Recent CNS Graduates

Alvin AuYoung, a Ph.D. student under professor Alex C. Snoeren, defended his dissertation, "Practical Market-Based Resource Allocation," in March 2010. Dr. AuYoung joins the CSE department of UC San Diego as a post-doctoral researcher.

Fallon Chen, M.S. student, is graduating in April 2010. She has already secured a position with Teradata-NCR. Her advisor was CSE professor Joseph Pasquale.

Yanhua Mao, a Ph.D. student of CSE professor Keith Marzullo, graduated in March 2010 after filing his dissertation, "State Machine Replication for Wide Area Networks." Dr. Mao is now a Software Engineer at Facebook.



Pardis Miri, M.S. student, graduated in March 2010. Her thesis dealt with "Miswirings Diagnosis, Detection and Recovery in Data Centers." Miri, whose co-advisors were Marzullo and CNS Director Amin Vahdat, accepted a position as a Program Manager with Microsoft.

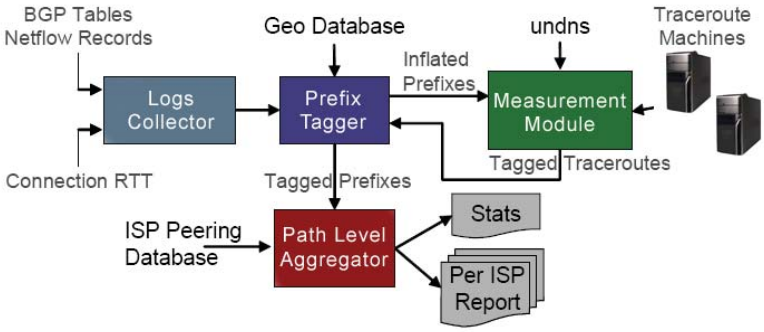
Eric Rubow joins CNS member company Ericsson after graduating in March 2010 with an M.S. in Computer Science.

Patrick Verkaik, Ph.D. student, will be graduating in April 2010 after defending his dissertation, ""Externally Controlling Decentralized Protocols in Network Devices."

Way High with WhyHigh

CNS Post-doctoral Researcher **Harsha Madhyastha** (below) won the best-paper award at Internet Measures Conference 2009 (IMC 2009), a prominent annual meeting focused on the latest and most challenging research being conducted in Internet measurement and analysis.

The paper presents measurement information from CNS member company Google's production content distribution network (CDN).



System architecture for WhyHigh

The prize-winning paper, "Moving Beyond End-to-End Path Information to Optimize CDN Performance," notes that the most common solution for improving client performance when replicating content across geographically distributed servers is to redirect clients to the nearest server with the lowest latency. Madhyastha's research team showed "that redirecting every client to the server with least latency does not suffice to optimize client latencies."

Because the standard procedure for solving this common problem proved inadequate, Madhyastha and his colleagues built a tool called WhyHigh that uses a series of active measurements to diagnose the cause of inflated latency to the relatively large number of clients that experience poor latency to individual CDN nodes. WhyHigh, which is now in production use at Google, has significantly improved the performance of Google's CDN.

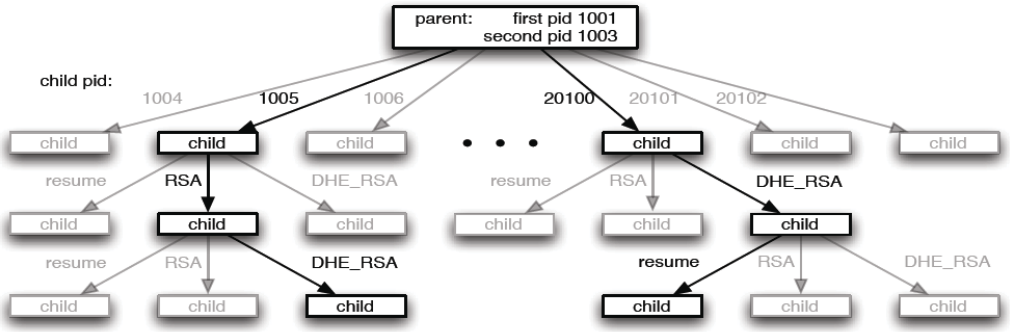
When Private Keys Become Public

Continues from page 1...

an attacker," noted Shacham. "Knowledge of the private key allows an attacker to impersonate that server even when SSL/TLS or SSH is used, and in many cases, to undetectably decrypt traffic to and from the server."

The goal of this work was to measure recovery from this type of vulnerability and to compare it to what is known about recovery from other vulnerabilities. To study user response to this vulnerability, the researchers collected a dataset of daily remote scans of over 50,000 SSL/TLS-enabled web servers. Of those, 751 displayed vulnerable certificates.

The researchers found an extremely slow rate of fixing that, unlike with conventional vulnerabilities with their typically short fixing phases, displayed a much flatter curve, with fixing extending six months after the announcement. On the positive side, these results allowed the researchers to identify some predictive factors for the rate of upgrading for this sort of vulnerability. Less positively, the group also found that certificate authorities continued to issue certificates to servers with weak keys long after the vulnerability was disclosed.



Ericsson Moves Forward by Moving Back to California

Telecommunications equipment and services giant Ericsson inaugurated its new partnership with CNS on March 4 with a signing ceremony and a talk by Ericsson Senior Vice President and General Manager, Group Function Technology, **Håkan Eriksson** (pictured above). Eriksson was appointed head of the company's fledgling Silicon Valley operations in 2008.

In his talk about merging mobile broadband and the Internet, Eriksson reminded the packed audience that Ericsson was previously the major worldwide player in mobile communications (including a research and development unit in San Diego). However, the new dominance of the iPhone and the Android, emerging developments from Google, and the integration of laptops into mobile networks all shifted the center of the world of mobile networking from Sweden to California. Ericsson embraced this shift by choosing to concentrate over 1,200 R&D personnel in San Jose, Calif. According to Eriksson, the Silicon Valley research hub has been charged with working on problems associated with the next generation of technologies in mobile broadband and networking.

Though many of the resources utilized in ongoing initiatives may be spread throughout the world, all have been integrated in Ericsson's Internet Protocol (IP) and broadband headquarters in San Jose. Eriksson explained the company's excitement at this new phase of its business practices as a desire "to combine the Ericsson leadership in mobile communication with Silicon Valley leadership in the Internet and IP." The move also reflects Ericsson's desire to stop designing and making all components of its products, which in the past included such diverse elements as the programming language and the CPUs. Instead the company is forging partnerships with companies that have demonstrated expertise in those components and applications that Ericsson no longer wishes to develop in-house.

Ericsson's collaboration with UC San Diego began in 2001 with projects in radio network testbeds, IP networking and network security. Even as the company was phasing out its business presence in San Diego in the last decade, it continued to support research in Calit2, and that commitment to collaboration with UCSD researchers has been both renewed and strengthened. With CNS, Ericsson has become a supporting member company and is pursuing high priority projects with CNS researchers in such areas as cloud networking and security and malware detection.

Håkan Eriksson told the audience that the company is working to cement strong relationships with competent partners in order to meet its goal of creating a network that can support 50 billion connections by 2020. Currently, there are over 400 million households on fixed connections and over four billion mobile broadband users, but in the hyper-connected world of the future, those numbers will be a drop in the bucket. "Everything that can benefit from being connected will be connected," predicted Eriksson. "It is only the imagination that stops you with what you can do with

that. What will people think about to make applications – to make a business?"

Eriksson explained that the next great leap in traffic growth on mobile networks will be in data, which he said Ericsson can increase by a factor of 1,000 in five years. The prediction was based upon a number of factors. First, it is an extrapolation from data traffic that has grown by a factor of 15 in the last two years – and has already exceeded voice traffic over the mobile broadband network.

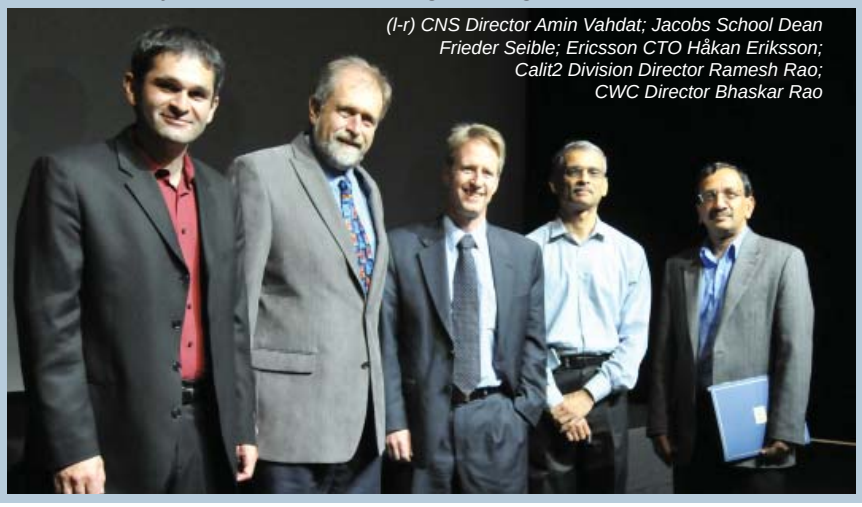
Secondly, Eriksson argued, the move from the use of WCDMA to HSPA and LTE technology, more spectrum allocation, and smaller cell radius can combine to make this explosion in data traffic possible. "You have to handle the signaling, you have to handle the throughput and… keep the latency down, and all of this has to be happening in a very cost-effective way," he concluded.

Wireless base station equipment manufactured by Ericsson

With Ericsson's new investment in resources in Silicon Valley and its committed partnerships in industry and academe, including CNS, CWC and Calit2, Eriksson was firm in his conviction that all of these challenges can be solved.

CNS Welcomes Newest Member: Ericsson

On March 4, at a signing ceremony co-sponsored by the California Institute for Telecommunications and Information Technology (Calit2), the Center for Networked Systems (CNS), and the Center for Wireless Communications (CWC), Ericsson became the newest member of CNS. The ceremony was attended by Ericsson representatives, CNS faculty and students, Calit2 and CWC researchers, and was presided over by Jacobs School of Engineering Dean Frieder Seible.


(l-r) CNS Director Amin Vahdat; Jacobs School Dean Frieder Seible; Ericsson CTO Håkan Eriksson; Calit2 Division Director Ramesh Rao; CWC Director Bhaskar Rao

The signing ceremony was followed by a talk by Håkan Eriksson, entitled "Ericsson in Silicon Valley: Merging Mobile Broadband and the Internet." (above and at left; visit the online CNS Lecture Archives to view a webcast of Eriksson's talk). Ericsson is a leading provider of telecommunications equipment and related services to mobile and fixed network operators globally. Their dedication to research and development as well as their ongoing commitment to technology leadership in the area of systems and networking make them an exciting new partner for CNS.

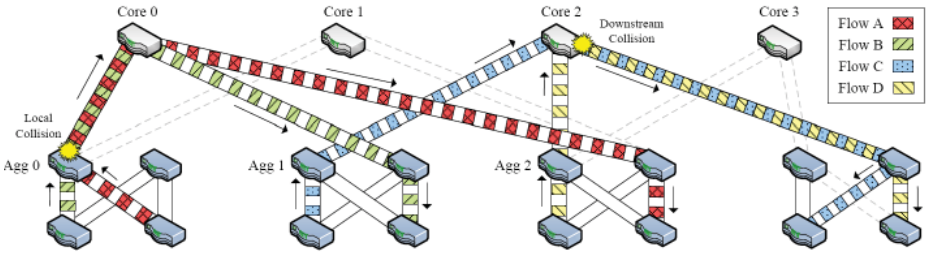
Hedera: Making Data Center Flow Scheduling Dynamic

In a technological development that could not have been predicted even a few years ago, more and more organizations are building large-scale data centers – or they have begun to use data center resources accessed through cloud-computing host providers. These data centers often aggregate bandwidth to thousands or tens of thousands of machines to create complicated services, such as those found in social networking or e-commerce websites, or in powerful distributed computing frameworks like Hadoop, MapReduce, or Dryad. While the scale and pattern of utilization for data centers has changed, however, data center routing and forwarding protocols have yet to adapt to the growing demands of this new paradigm.

In a bid to meet the challenge of this emerging issue, **Mohammad Al-Fares** (pictured), a CNS graduate student researcher in a team with other CNS students and faculty, will be presenting a paper at the prestigious USENIX Symposium on Networked Design and Implementation (NSDI '10) in April 2010.

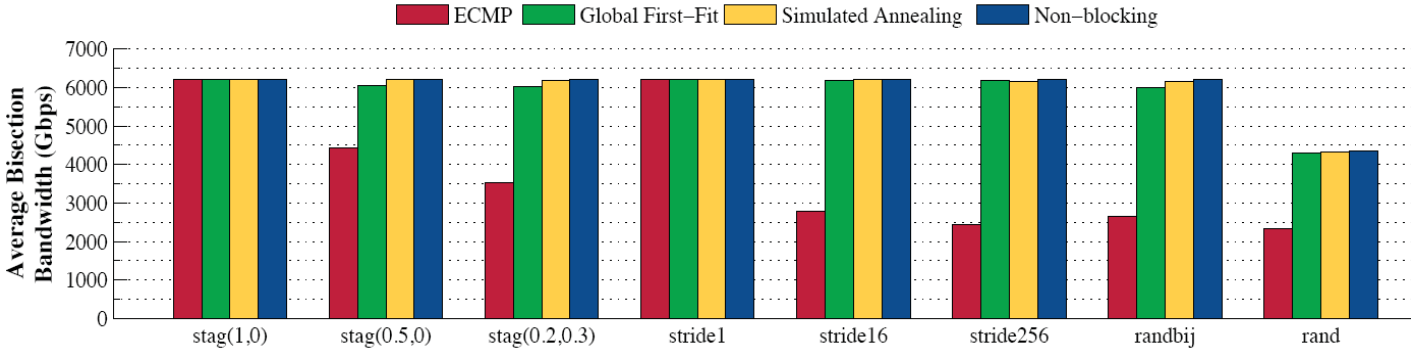
In their paper, "Hedera: Dynamic Flow Scheduling for Data Center Networks," Al-Fares and his fellow researchers introduce Hedera as a "scalable, dynamic flow scheduling system that adaptively schedules a multi-stage switching fabric to efficiently utilize aggregate network resources." Hedera is designed to address some of the major problems – as defined by the CNS researchers – facing network designers of modern data centers.

First, there are several inherent properties of cloud-based applications that complicate the issue of overall data center network design. These include a completely unknown network workload, customer demand to use commodity operating systems, and the network bottlenecks that can arise when using virtualization technology.



The second challenge is the need for routing and forwarding protocols that can adapt to dynamic deployment settings. The designer of a traditional enterprise-level data center could rely upon a predictable pattern of communication with a small number of primary and secondary paths, and so could use routing and forwarding protocols targeted for specific deployment settings. In a break from this, the latest designs for data center topologies now rely upon path multiplicity and utilizes such methods as Equal-Cost Multi-Path (ECMP) forwarding or Valiant Load Balancing (VLB). However, any time more than one long-lived flow is forwarded, these multi-path methods create bottlenecks that consume significant shares of bandwidth.

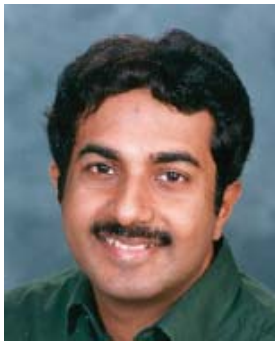
A full implementation of Hedera has been completed on the Portland testbed. Using commodity switches and unmodified hosts, Al-Fares and his colleagues demonstrated that Hedera produces bisection bandwidth for a simulated host data center that is 96 percent optimal and 113 percent better than current, static load-balancing methods. While Hedera's gains in performance depend on network flow and are more apparent when the network is stressed by several large data transfers, the improvements significantly outperform current routing and forwarding protocol solutions. Moreover, noted Al-Fares, given "the large investment in network infrastructure associated with data centers (many millions of dollars), and the incremental cost of Hedera's deployment (e.g., one or two servers), we show that dynamic flow scheduling has the potential to deliver substantial bandwidth gains with moderate additional cost."



(Top of page) Examples of equal cost multi-path collisions resulting in reduced bisection bandwidth [unused links omitted for clarity]; (Bottom) Comparison of scheduling algorithms for different traffic patterns on a fat-tree topology of 8,192-hosts

Scaling the Data Center

In March 2010, CNS Director and PI **Amin Vahdat** and co-PI **George Varghese** (pictured below) were awarded a three-year grant from the National Science Foundation to fund their work on "Scale, Isolation, and Performance in Data Center Networks." The project aims to design a data center architecture with scalable bandwidth, virtualization, modularity, instrumentation and backward compatibility.



Modern data centers host operations as varied as flight planning, drug discovery, and Internet search running on thousands of machines. These services are often limited by the speed of the underlying network to coordinate parallel data access. In current data centers, network input/output remains a primary bottleneck and a significant fraction of capital expenditure (an estimated $10 billion annually). Compounding the problem are operational issues caused by interference between services, down times due to failures, and violations of performance requirements.

This project will develop a hardware/software architecture capable of: non-blocking bandwidth to hundreds of thousands of hosts; "slicing" across services with minimum bandwidth guarantees; detecting fine-grained performance violations; tolerating a range of failure scenarios; as well as supporting end-host virtualization and migration. Our goal is to enable modular deployment and management of networking infrastructure to keep pace with the burgeoning computation and storage explosion in data centers. This work will result in a prototype fully functional virtualizable data center network fabric to support higher-level services. Vahdat and Varghese will work with industry partners to address key performance and reliability issues in a critical portion of the national computation infrastructure. The project will train students in data center networking and cloud computing, and all of the data center communication workloads, protocols, and algorithms developed by the team will be released to the public.

NSF Renews Cyber Trust Center

One of the nation's first Cyber Trust research centers, funded under an NSF initiative in 2004, has been extended beyond its original 5-year mission in order to continue developing tools to counter the threat of worms and viruses that are becoming increasingly virulent, sophisticated and fast to propagate across the Internet.

The Collaborative Center for Internet Epidemiology and Defenses (CCIED) is led by CSE professor **Stefan Savage** (right) and based at UC San Diego, in partnership with Berkeley's International Computer Science Institute.

Together with UCSD co-PIs **George Varghese** and **Geoffrey M. Voelker**, Savage is leading the effort to address critical challenges posed by large-scale Internet-based pathogens, such as worms and viruses. The center aims to understand better the behavior and limitations of Internet epidemics, and to develop systems that can automatically defend against new outbreaks in real time. CCIED is developing early-warning and forensic capabilities, and it also receives industry support from a number of corporations, including CNS member companies HP, Google, Ericsson and Cisco Systems.

The center's focus on the new science of "Internet epidemiology" requires gaining visibility into pathogens propagating across the global Internet. To do so, CCIED is building a distributed "network telescope" of unprecedented scale. The telescope in turn feeds a "honeyfarm" collection of vulnerable "honeypot" servers whose infection serves to indicate the presence of an Internet-scale worm. To then fight worms once detected, the center works on developing mechanisms for deriving "signatures" of a worm's activity and disseminating these to worm suppression devices deployed throughout the global network.

CNS On-Demand

The following talks from the CNS Lecture Series were added to the archive over the winter quarter. They are now available for on-demand viewing (Windows Media player and broadband connection required) at http://cns.ucsd.edu/lecturearchive.shtml [N.B. Talks may not be available behind corporate firewalls that prevent viewing of video streams].

Towards Systematic Enterprise Network Management (March 16)
Sanjay Rao, Assistant Professor,
Electrical and Computer Engineering, Purdue University

Ericsson in Silicon Valley: Merging Mobile Broadband and the Internet (March 4)
Håkan Eriksson, Senior Vice President and General Manager, Group Function Technology, and Chief Technology Officer at Telefonaktiebolaget LM Ericsson (see article on page one)

Resource Aware Programming for Sensor Networks (January 8)
Matt Welsh, Associate Professor
Computer Science, Harvard University

PNUTS: Building and Running a Cloud Database System (December 11, 2009)
Brian Cooper, Research Scientist
Yahoo! Research

Get Connected

Stay up-to-date about upcoming CNS events, including lectures and Research Reviews, by signing up for the CNS Events RSS feed. To do so, visit the CNS website at

http://cns.ucsd.edu

and click on the link "CNS Events RSS Feed."

Upcoming Events

CNS Summer 2010 Research Review

Wednesday, August 4 and Thursday, August 5, 2010
UC San Diego Faculty Club

The CNS Summer 2010 Research Review will be held August 4 and 5 at the Faculty Club on the UC San Diego campus. The agenda includes talks by representatives of CNS industry members; project proposals for the center's 2010-'12 grant cycle; Year One progress and two-year summary reports from researchers conducting CNS-sponsored projects; a graduate student research poster session; and numerous opportunities for informal interactions among industry members and CNS faculty, researchers and graduate students. Attendance is limited to invited guests. If you are interested in attending, please contact Kathryn Krane at cns@ucsd.edu.

CNS Lecture Series: Michael Walfish

May 21, 2010 1:00-2:00 p.m., Room 1202, CSE Building
Michael Walfish, Assistant Professor
Department of Computer Science, University of Texas, Austin

Mission and Objectives of CNS

The mission of CNS is to develop key technologies and frameworks for networked systems. By combining our research talents and strengths in partnership with industrial leaders, CNS achieves critical mass and relevant focus, accelerating research progress and creating key technologies, frameworks and systems understanding for robust, secure networked systems and innovative new applications. CNS also works to educate the next generation of top students with a perspective on industry-relevant research and to train students on how to continue their leadership throughout their careers. This is accomplished by bringing together leading faculty, students, and companies to investigate the most challenging, interesting and important problems in computer networks.

If you are interested in joining the Center, please contact Director Amin Vahdat at vahdat@cs.ucsd.edu.