FEELING GOOD ABOUT SORTING THINGS OUT

In continuing what is becoming a tradition, Ph.D. student Michael Conley once again won world records for data sorting in multiple categories. He was competing in the annual Sort Benchmark competition with CNS associate director George Porter and former CNS director Amin Vahdat (now at Google). Conley employed an updated version of their sorting system, Tritonsort, which was designed not only to achieve record-breaking speeds but also to maximize system resource utilization. Tritonsort tied for the "Daytona Graysort" category and won outright in both the "Daytona" and "Indy" categories of the new "Cloudsort" competition.

The established metric to win the GraySort competition is to achieve the highest sort rate (terabytes of data per minute) while sorting a minimum of 100 TB of data. The new CloudSort competition measures the minimum cost of sorting at least 100 TB of data on a public cloud. Conley’s group achieved their victory with Tritonsort on Amazon’s Elastic Compute (EC2) cloud computing platform.

Several factors underscore the effectiveness of Tritonsort’s system resource utilization scheme as compared to the far more resource-intensive methods followed by their competitors. The team that tied with CNS for first place in the Daytona Graysort category, Databricks, used 10 percent more processors to achieve a slightly (though for the purpose of the contest, equivocal) slower sorting speed.

Tritonsort also continues to hold the world record for energy efficiency in data sorting. The 2011 iteration of Tritonsort still holds the record for the least amount of energy required to sort 100 TB of data in the "Joulesort" competition. The 2011 record set by Tritonsort still holds at 132 MJoules.

To see all the details about the competition: http://sortbenchmark.org

And to read more about the technical aspects of Tritonsort: http://sortbenchmark.org/TritonSort2014.pdf
The past year has seen recognition for the excellence and importance of CSE professor Yuanzhen (YY) Zhou's research by two of the premier professional associations in computer science and engineering.

In December 2013, the Association for Computing Machinery (ACM) announced its annual recognition of members from academic institutions, companies, and research labs all over the world who “have achieved advances in computing research and development that are accelerating the digital revolution and impacting every dimension of how we live, work, and play.” Zhou is one of 50 ACM members elevated to be Fellows of the ACM in 2014. She was cited for her “contributions to software reliability and quality.” Professor Zhou joins other CNS members Keith Marzullo and Stefan Savage as ACM Fellows.

More recently, in November 2014, professor Zhou was named an IEEE Fellow for “contributions to scalable algorithms and tools for computer reliability.” For more than a century, IEEE has honored the distinction of Fellow upon those of its members with extraordinary accomplishments in any of the fields of endeavor that are of interest to IEEE.

RESEARCHER RECEIVES 2014 IEEE INTERNET AWARD

The head of the Center for Applied Internet Data Analysis (CAIDA) research group at the San Diego Supercomputer Center, kc claffy, was named one of the two recipients of this year’s IEEE Internet Award. She was cited (along with UC Berkeley’s Vern Paxson) for their “seminal contributions to the field of Internet measurement, infrastructure, and network data analysis, and for distinguished leadership in and service to the Internet community by providing open access data and tools.”

“kc was a Ph.D. student here and, unable to escape the gravity of San Diego, created a completely independent research group, CAIDA, that single-handedly established UC San Diego as a worldwide leader in network measurement,” said CNS director Stefan Savage, a professor in the Department of Computer Science and Engineering (CSE). “We’re lucky to have her as a colleague, an adjunct in CSE, and as a member of the Center for Networked Systems.”

Begun in 1999, the IEEE Internet Award is given to an individual or small number of collaborators who have provided exceptional contributions to the advancement of Internet technology for network architecture, mobility, and/or end-use applications.

RANJIT JHALA RECEIVES “TEST OF TIME” AWARD

Sometimes the best way to judge the importance of work is to view it in hindsight. An idea that might have seemed important or groundbreaking at the time of its publication can prove to be a dead end, while a seemingly modest proposal that was overlooked when it first came out eventually becomes the standard for how things are done in a particular field. With this phenomenon in mind, many subfields in computer science have taken to presenting annual “test of time” awards for work that has proven to be most influential.

Every year at the ACM Symposium on Principles of Programming Languages (POPL), the program committee announces the recipient of the POPPL Most Influential Paper Award. The committee goes back to the papers presented at the symposium a decade earlier and determines which of those papers proved most influential in retrospect.

In January 2014, the POPL committee recognized the 2004 paper, “Abstractions from Proofs,” co-authored by CNS member and CSE professor Ranjit Jhala while he was finishing up his doctoral work at UC Berkeley with colleagues Tom Henzinger, Rupak Majumdar, and Ken McMillan. The committee explained that, in this paper, Jhala and his team “demonstrated a fundamental generalization of Craig interpolation to program analysis by predicate abstraction, opening the door for interpolation to be applied to abstraction refinement for "infix-express" systems.” Prior to the publication of Jhala’s paper, interpolation had only been used by those researching programming languages in the model checking of “finite-state” systems. The award committee further praised how the 2004 paper “showed how interpolation offers a fundamental way to explain abstraction refinement in a logical framework, and has led to many extensions to increase the power of abstraction in program analysis.”

WHO WATCHES THE WATCHMEN?

If you have traveled by air in the United States in the last few years, chances are that you have passed through a security checkpoint that was monitored by some kind of advanced imaging technology (AIT). But how effective is this technology at scanning for weapons and explosives? Government agencies have assured the public and policy makers that the technology has been thoroughly tested for efficacy, but those details about those tests have not been forthcoming, and existing studies were only conducted by manufacturers, significant doubts about the machines have persisted.

In a groundbreaking paper presented at the 2014 USENIX Security Symposium, a group of CNS students and faculty at UC San Diego, partnering with researchers at Johns Hopkins University and the University of Michigan, conducted the first independent security evaluation of an AIT. Specifically, they tested whether individuals could smuggle weapons or explosives through security checkpoints by exploiting flaws in the design of an X-ray backscatter scanner, the scanner’s software and hardware, and scanning protocols.

The U.S. Transportation Security Administration (TSA) adopted AITs in 2009 to screen for both metallic and non-metallic objects such as knives, personal firearms, and explosive devices or materials that passengers might smuggle onto airplanes. The primary deployment of AITs from 2009 to 2013 took the form of an X-ray backscatter scanner called the Rapiscan Secure 1000. Though the Rapiscan was removed from service by TSA and replaced with a different kind of AIT in 2015, it has also been widely distributed to other secured venues throughout the U.S. (such as courthouses and prisons), so it remains widely though less visibly in use.

With the Rapiscan, travelers are asked to enter the machine and face it with their feet spread and their hands raised while they are illuminated with constant-spectrum X rays. Because different atomic compositions of materials reflect the radiation at different intensities, the pattern of radiation reflected back to the sensor creates an image. In this image, thin and more diffuse materials (such as clothing) become invisible, while less dense materials (e.g., flesh) can be discerned in contrast to very dense materials (such as steel or aluminum).

When first introduced in 2009, the scanners were presented as having been tested, effective, safe, and necessary components of the TSA’s physical security system. However, the systems were almost immediately criticized by a number of periodic or try to find concealed objects. The technology, as well as the search protocols used to implement it, was considered by some to be ineffective and even potentially hazardous. What made the discussion difficult to resolve, however, was that while independent observers were not allowed to conduct their own evaluations of the technology, the existing studies by the manufacturer, if released at all, were presented in a highly redacted form that made informed criticism impossible. Perhaps more troubling to some observers, it was questionable how thorough the previous studies had tested the technology by trying to mimic motivated, malicious actors who might adapt their behaviors to circumvent the device.

(Story continued on page 8)
Mr. Jang Goes to Mountain View

When Computer Science and Engineering Ph.D. student Dongseok (Don) Jang was given the opportunity to complete a CNS internship at Google with Software Engineer Charlie Reis, he jumped at the chance. Jang knew Reis by reputation as a leader in the creation of innovative browser architectures that improve security. For a doctoral student passionate about security issues, the prospect of working under Reis on a project to improve the security of Google’s web browser Chrome was impossible to pass up.

Web browser security is a constantly evolving problem of longstanding and great importance. Creators of browsers have to develop products that provide an excellent user interface while ensuring that their users are protected from the less savory elements on the Web. The company whose browser is best able to deliver to Internet users a fast and safe experience on the Web becomes the preferred provider of a window on the Internet. That company can then charge the most from advertisers who wish to place themselves into that window frame. However, creating a browser that is safe for users to operate while also rating high in ease of usability is a daunting task.

Problems with Web Browser Security

In order to understand the work upon which his internship was based, Jang provided some background into how Reis had already changed Chrome to make it more secure. Historically, browsers have been vulnerable to low-level security attacks. To prevent this from happening, Reis proposed separating the browser into smaller, self-contained pieces, each of which runs a different process. Because of this innovative measure, called site isolation, even if one window frame is compromised, site isolation prevents the insecure data from being affected.

The company whose browser is best able to deliver to Internet users a fast and safe experience on the Web becomes the preferred provider of a window on the Internet. That company can then charge the most from advertisers who wish to place themselves into that window frame. However, creating a browser that is safe for users to operate while also rating high in ease of usability is a daunting task.

To make <img>, <script>, etc. work, we block the insecure data without breaking the existing website?

As time passed and Web sites evolved, a couple of factors made it clear that site isolation needed to be extended beyond just separating the operation of tabs. Web sites became more complex, and this increasing complexity opened more doors to hackers.

It is the nature of modern Web sites that a number of documents are embedded within the Web page. For example, Web pages often include several inline frames (called iframes), which are HTML documents embedded within another HTML document on a Web site. Iframes allow documents from other sources to be part of a site's presentation to the viewer and are familiar to anyone who has ever seen an embedded media file. Further, an iframe allows a Web site to provide a window to other places on the Internet. However, the insecurity of iframes allows malicious parties to use low-level memory attacks to access browsers through the embedded objects. A compromised tab in a browser can then steal data from any subsequent site the user chooses to visit.

Don Jang’s summer project focused on how to expand site isolation so that the browser can restrict the access of documents embedded within a website to the other sites or the other tabs on the user’s browser. The immediate solution to this conundrum would be to set up a document filter within the browser. But right at the beginning, there was a significant technical obstacle that needed to be addressed. Jang and his colleagues could not simply tell their document blocker to filter out specific categories of problematic documents. This is because Web sites often mislabel content headers that provide the identifying data about the documents being transmitted. For example, something may claim that something is HTML, when it is not, or vice versa. Therefore, building a simple filter based on content header information would block or compromise, or be acceptable, any number of innocent documents that the page is actually insecurable documents, making for a disrupted and yet still unprotected user experience.

The question posed to Jang when he undertook the project was: How do we block the insecure data without breaking the existing website?

At Google, Jang and his research colleagues at Google, Ph.D. student Don Jang recalls that working on the project was “overwhelming at first. It was hard to figure out what I could contribute because Chrome is a really gigantic project.”

The Solution

One of the most straightforward solutions to this issue would be to use a Cross-site Document Blocking (CSD) policy, which would prevent the insecure data from being accessed by the browser.

Don Jang’s summer project focused on how to expand site isolation so that the browser can restrict the access of documents embedded within a website to the other sites or the other tabs on the user’s browser.

Don Jang’s summer project focused on how to expand site isolation so that the browser can restrict the access of documents embedded within a website to the other sites or the other tabs on the user’s browser.

The solution conceived by Jang and his research colleagues at Google was to create a cross-site document blocking policy. They designed a framework that routes navigations to pages only within its own site and which will not read documents that are vulnerable to attack from other sites. For example, if we request a JavaScript file from its own site while blocking cross-site HTML files, this prevents cross-site data theft.

Implementation and Evaluation

CNS’s Jang and colleagues produced their modified version of Chrome and tested it while viewing Alexa Top 50K Web pages. During the testing process, they fine-tuned their policy by incrementally excluding more and more document types, thereby increasing browser security while also increasing the number of disruptive blocks. They then measured the likely number of definite and possible disruptive and non-disruptive blockings and used this information to estimate the probable effect the use of their implementation would have on the user experience.

After tinkering with some of the parameters of the process, Jang and colleagues lowered the disruptive blocking rate to 0.075%, a level deemed to be acceptable, especially considering the parallel increase in security that it conferred. The modification is now an active setting in Chrome.

For more information about this project, visit the Wikipedia page for “Blocking Cross-Site Documents for Site Isolation” at http://www.chromium.org/developers/design-documents/blocking-cross-site-documents.

CNS SUMMER INTERNSHIP EXPERIENCE: A WIN–WIN–WIN PROPOSITION

While reflecting on his internship experience at Google, Ph.D. student Don Jang recalls that working on the project was “overwhelming at first. It was hard to figure out what I could contribute because Chrome is a really gigantic project.”

When the site of Jang’s ideas would have resulted in substantially slower response times for Web browsing in Chrome. In a business environment where one of the main priorities is speed, this would be unacceptable — “an example of the cure being worse than the disease,” he adds. Other proposals would have resulted in a high percentage of blocking of JavaScript resources that are insecurable but useful for the user experience, which would have caused an unacceptable degradation in the user experience, which would be unacceptable.

I had to talk to more than 50 or 60 engineers scattered throughout the world. Someone was working in Germany, someone was in Zurich, another was in Asia.” Collaborating with such a large number and more diverse group of people stood in stark contrast to Jang’s prior programming experience in academia, in which he generally only teamed up with a handful of other students or faculty on a local basis.

I had to talk to new people every day, and I became able to see different aspects of a problem,” says Jang. “Beforehand, when I looked at a problem, I only looked at really small, academically-oriented ideas, things that people could see as academically relevant. The solution I wasn’t able to think about industry-level impacts or how it would be to implement an idea in some corporate environments. Now I can measure how to do that.

Based on his internship, Jang might have come up with a solution to a different kind of problem to himself. “The solution is so easy! Why don’t they just implement this solution?” he asked. His colleagues agreed and set up a meeting with the people responsible for the team working on that.”

Before his internship, Jang might have come up with a solution to a real-world problem and thought to himself, “The solution is so easy! Why don’t they just implement this solution?”

The value of the internship to Jang was not merely the experience of working on a novel solution to a serious problem. Indeed, it changed his white approach to formulating research questions and solutions.

“I went to Google with a really academically-oriented mindset that I could do whatever I wanted to do,” explains Jang. “So I proposed really aggressive ideas to secure Chrome.” However, he soon learned that the most obvious solutions to problems are often incompatible or unworkable when seen in the context of a system’s bigger picture. For example, one of Jang’s ideas would have resulted in substantially slower response times for Web browsing in Chrome. In a business environment where one of the main priorities is speed, this would be unacceptable — “an example of the cure being worse than the disease,” he adds. Other proposals would have resulted in a high percentage of blocking of JavaScript resources that are insecurable but useful for the user experience.

“The solution [we came up with] consisted of millions of lines of code with thousands of people who work on it. To make even a small change in Chrome was really hard — just to make a patch of the lines of code takes about two or three days because there are many people working on that.”

However, in the end, Jang derived from his internship experience a satisfaction that everyone involved — himself, his fellow team members at Google, and users of the Chrome Web browser — walked away with something positive.

In the first place, notes Jang, the team’s implementation increased the security of the browser without degrading the user’s experience of ease and rapidity, thus bolstering Chrome’s reputation as a premier Web browser and supporting Google’s constant efforts to build the strongest, safest browser available. Moreover, it reduced overall blocking, thereby minimizing its effects on their viewing of content. And for Jang personally, the lessons he learned from his summer experience are likely to prove invaluable in his career.

The solution conceived by Jang and his research colleagues at Google was to create a cross-site document blocking policy. They designed a framework that routes navigations to pages only within its own site and which will not read documents that are vulnerable to attack from other sites. For example, if we request a JavaScript file from its own site while blocking cross-site HTML files, this prevents cross-site data theft.

The solution conceived by Jang and his research colleagues at Google was to create a cross-site document blocking policy. They designed a framework that routes navigations to pages only within its own site and which will not read documents that are vulnerable to attack from other sites. For example, if we request a JavaScript file from its own site while blocking cross-site HTML files, this prevents cross-site data theft.

The solution conceived by Jang and his research colleagues at Google was to create a cross-site document blocking policy. They designed a framework that routes navigations to pages only within its own site and which will not read documents that are vulnerable to attack from other sites. For example, if we request a JavaScript file from its own site while blocking cross-site HTML files, this prevents cross-site data theft.
In an ongoing effort to support diversity in computer science and engineering, CNS selected two Ph.D. students to represent the center at the Grace Hopper Celebration of Women in Computing, organized by the Anita Borg Institute.

CNS awarded CNS 2014 Grace Hopper Travel Grants to two CSE Ph.D. students: Malveeka Tewari and Soohyun Nam. The students were chosen to attend the Phoenix, AZ, conference in November 2014. The Grace Hopper Celebration is the premier conference bringing together women in computing and technology to focus on research and careers. Tewari and Nam attended special sessions focusing on this year’s theme of “the global prevalence of computer technology and the participation of one and all in its design, development, and deployment.” The students were among approximately 40 young women from UC San Diego attending the 2014 conference, in a delegation led by CSE professor Christine Alvarado.

FENG LU
Fong Lu earned his Ph.D. in ECE in August 2014 after defending his dissertation, “Downclocking WiFi to Improve Energy Efficiency in Mobile Devices.” Dr. Lu’s advisors were Tara Javidi, Alex C Snoeren and Geoffrey M Voelker. He now works as a Software Engineer at Google.

DO-KYUM KIM
CSE Ph.D. student Do-kyum Kim became a Software Engineer at Google after presenting “Topic Modeling of Hierarchical Corpora” in September 2014. He was co-advised by Lawrence Saul and Geoffrey M Voelker.

QING ZHANG
Qing Zhang, a CSE Ph.D. student advised by Geoffrey M. Voelker, did her dissertation on “Utilizing Source Information to Detect and Prevent Online Fraud.” After graduating in October 2014, Dr. Zhang became a Software Engineer at Google.

ARUP DE
In June 2014, CSE Ph.D. student Arup De, advised by Steven Swanson, became a member of the research staff at HGST, a Western Digital company, after defending his dissertation, “A Compute Capable SSD Architecture for Next-Generation Non-volatile Memories.”

SARAH MEIKLEJOHN
CSE Ph.D. student Sarah Meiklejohn completed and defended her dissertation on "Flexible Models for Secure Systems" in April 2014. She was co-advised by Stefan Savage and Mihir Bellare. Dr. Meiklejohn is now an Assistant Professor at University College London in the departments of Computer Science as well as Security and Crime Science.

JIAQI ZHANG
CSE professor YY Zhou advised CSE Ph.D. student Jiaqi Zhang, who defended his dissertation on “Software Configuration Learning and Recommendation” in October 2014. Dr. Zhang is a Software Engineer at Wihora (a startup founded by Zhou).

SIVASANKAR RADHAKRISHNAN
In March 2014, CSE Ph.D. student Sivasankar Radhakrishnan presented “Network Performance Improvements for Web Services – An End-to-End View.” He was jointly advised by Amin Vahdat and George Porter. Dr. Radhakrishnan is now a member of the technical staff at Forward Networks.

DEVIN LUNDBERG
CSE M.S. student Devin Lundberg graduated in April 2014 and became the first Application Security Engineer at Pinterest. Lundberg works to protect ‘pinners’ by securing the company’s web and mobile applications in addition to Pinterest’s many internal tools.
CSR solves the challenges and delivers the core innovations that enable their customers to win in the global consumer electronics market. Their technologists create innovative and integrated platforms, helping their customers turn great ideas into market-leading products.

CSR is a highly successful, UK-headquartered fabless semiconductor company employing over 2,000 people across 10 countries, offering a range of "technology platform solutions" and System-on-a-Chip devices for a multitude of consumer electronics applications, from Indoor Location to DSLR cameras and Bluetooth wireless audio. Founded in 1998, the company has ongoing collaborations with world-class centers of excellence established at particular universities. CSR also supports and funds exceptional PhD candidates pursuing leading-edge innovation in fields related to CSR's research interests including Wi-Fi, Bluetooth, audio, NFC and power management technologies.

In October 2014 Qualcomm agreed to acquire the UK-based CSR for an estimated $2.5 billion. The acquisition is expected to be completed in late summer 2015.

CNS WELCOMES NEW MEMBER

The Center for Networked Systems (CNS) welcomes its newest member, CSR.

CSR

Push every boundary.

CSR solves the challenges and delivers the core innovations that enable their customers to win in the global consumer electronics market. Their technologists create innovative and integrated platforms, helping their customers turn great ideas into market-leading products.

CSR is a highly successful, UK-headquartered fabless semiconductor company employing over 2,000 people across 10 countries, offering a range of "technology platform solutions" and System-on-a-Chip devices for a multitude of consumer electronics applications, from Indoor Location to DSLR cameras and Bluetooth wireless audio. Founded in 1998, the company has ongoing collaborations with world-class centers of excellence established at particular universities. CSR also supports and funds exceptional PhD candidates pursuing leading-edge innovation in fields related to CSR's research interests including Wi-Fi, Bluetooth, audio, NFC and power management technologies.

In October 2014 Qualcomm agreed to acquire the UK-based CSR for an estimated $2.5 billion. The acquisition is expected to be completed in late summer 2015.