Emil Stefanov: Bridging the Theory and Practice of Cloud Computing Security

Elaine Shi
University of Maryland
elaine@cs.umd.edu

Emil Stefanov, aged 26, passed away on March 27, 2014. Emil was a Ph.D. student at the University of California, Berkeley. During his short but splendid academic career, Emil designed novel algorithms and built new systems that bridged the theory and practice of cloud computing security.

Emil was well-known for his innovative work on obfuscating access patterns to sensitive data. Among his numerous novel inventions, he proposed the Path Oblivious RAM algorithm, which is by far one of the most simple, elegant, and efficient solutions known to date. Path ORAM has enabled ORAM-capable secure processors to be prototyped -- the first of its kind. Emil's Path ORAM algorithm earned him the 2013 ACM CCS Best Student Paper Award.

Emil was the recipient of numerous other prestigious award, including the 2011 National Defense Science and Engineering Graduate Fellowship (NDSEG), the 2012 AT&T Best Applied Security Paper Award, the 2009 NSF Graduate Research Fellowship, and 2009 the U.C. Berkeley EECS Department Chair's Excellence Award.

Emil earned his bachelor's in three majors -- honors computer science, mathematics and computer science mathematics -- from Purdue University. During this time, he was the recipient of the Cisco Systems Scholarship, the Lockheed Martin Scholarship, the CERIAS Symposium research poster award, the first place award (out of 1,125) in the Robotics National Website Design Contest, the Raytheon Systems Scholarship, and the 7th place (out of 113 teams) in the ACM East Central North America Programming Contest. Emil also developed a course scheduling website that is now widely used by students at Purdue University. Emil was born in 1987 in Bulgaria, and went to schools in Canada, Bulgaria, Brazil, France, and the US. He graduated from the West Lafayette High School in Indiana. His parents are Plamen and Paola Stefanov, Professors of Mathematics at Purdue University.

In his lifetime, Emil's passion and dedication to research were infectious to many around him. To honor Emil and to celebrate his life, we held a memorial symposium for Emil in Berkeley, CA on April 26, 2014. Emil's memorial website is available at http://www.rememberingemil.org/.

We thank the organizers for letting us host the Emil Stefanov Memorial Lecture at CCSW-- a top venue for cloud computing security. The memorial lecture will feature talks from Professor Srini Devadas (MIT), Professor Ari Juels (Cornell-Tech), and Professor Zygmunt Pizlo (Purdue):

Memory Access Pattern Protection in the world of Malicious Operating Systems and Commercial Hardware

Srini Devadas, MIT

Memory access patterns are a big privacy problem for a multitude of systems. From cloud file servers to stand-alone cryptographic routines, all programs need memory and access it in ways that leak information about the program and the data it computes upon. The resulting memory access trace is easy to measure, typically requiring just sniffer software as opposed to sophisticated equipment such as probes. Further, it continuously leaks privacy: the longer the program runs, the more information can be leaked. In this talk, we first outline different trusted computing bases (TCBs) that apply to the malicious OS setting. We will then describe the 'diff' is needed in existing hardware and

CCSW'14, November 7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-3239-2/14/11.
http://dx.doi.org/10.1145/2664168.2673751

software infrastructure to support protocols such as Oblivious RAM that obfuscate memory access patterns.

A Visitor's Guide to a Post-Privacy World

Ari Juels, Cornell Tech

Privacy, in today's usual sense of confidentiality of sensitive personal information, is historically anomalous. Until recently, even the upper classes commonly lived, died, and engaged in the most intimate activities always under the eyes of those around them.

With the massive sweep and scale of cloud computing, however, there is a considerable chance of drifting again toward such a world. All manner of personal data—location, health status, social contacts, perhaps even thoughts—may in coming decades be widely and continuously accessible by corporations, governments, friends, and acquaintances.

Today, the risk of abuse of sensitive personal information is typically addressed by enforcing confidentiality. In a post-privacy world, it may be necessary to aim instead at accountability. If personal information spreads inexorably, it may be possible, at least, to ensure that it is used fairly. I'll talk about what a post-privacy world might look like and how we might prepare to navigate it.

A new look at human problem solving: near-optimal solutions to NP-hard problems

Zygmunt Pizlo, Purdue

The modern study of human problem solving started with the seminal work of Newell and Simon. Newell and Simon relegated mental representation to the back burner of Artificial Intelligence when they emphasized the role of search in problem solving. Now we know that search cannot form the basis of intelligent problem solving because the search spaces of most interesting problems are too big and human working memory is too small. I will present results on and a model of how humans solve the Traveling Salesman Problem (TSP), which is NP hard. Our model is based on the known anatomy and physiology of the human visual system. It also incorporates the known limitations of human working memory, as well as what we know about visual attention. The two main operations of the model are: (i) hierarchical clustering, and (ii) a coarse-to-fine sequence of approximations of the TSP tour. The key element of this model is starting with the correct representation of the problem; this allows the search of the problem space to be kept to a minimum. This approach is completely opposite to the way in which human problem solving has been studied and modeled during the last half a century. The abstract nature of the new model, along with its key operations of clustering (chunking) and top-down reasoning, should make this model a good starting point for formulating a general theory of human problem solving.