Abstract:

I will describe a new binary-tree based paradigm of constructing Oblivious RAM, leading to extremely simple constructions. Within this framework, I will describe Path ORAM. Under reasonable assumptions about the block size, Path ORAM achieves $O(\log n)$ bandwidth overhead with just a little more than $O(\log n)$ trusted cache --- this is nearly optimal in light of Goldreich and Ostrovsky's lower bound.

Based on Path ORAM, we implement the first real-life ORAM-capable secure processor prototype called Phantom. We run real-world programs such as sqlite on top of Phantom, and demonstrate reasonable practical performance.

Then, I will describe programming language techniques that can compile a program into its memory-trace oblivious equivalent, while achieving order-of-magnitude speedup in comparison with the naive approach of placing all variables in a single, large ORAM.

Finally, I will describe a vision of building a cloud computing platform secure against physical attacks.

Biodata:

Elaine Shi is an Assistant Professor at the University of Maryland, College Park. She completed her Ph.D. at Carnegie Mellon University in 2008, and prior to joining Maryland, she also worked at Palo Alto Research Center (PARC) and UC Berkeley as a research scientist.

In her research, Elaine takes a theory-meets-practice approach towards the design of secure and privacy-preserving systems. He has a broad range of expertise covering secure software
systems, cryptography, network security, and language-base security. Elaine's work on practical Oblivious RAM won a Best Student Paper award in ACM CCS (2013). She is also winner of the IJCNN/Kaggle Social Network Challenge (2011), the UMD Invention of the Year Award (2014), and a Sloan Research Fellow (2014).