Computer security and privacy are becoming extremely important nowadays. The task of protecting computer systems from malicious attacks and potential subsequent catastrophic losses is, however, challenged by the ever increasing complexity and size of modern hardware and software design.

We propose several methods to improve computer security and privacy from architectural point of view. They provide strong protection as well as cost efficiency. In our first approach, we propose a new dynamic information flow method to protect systems from popular software attacks such as buffer overflow and format string attacks. In our second approach, we propose to deploy encryption schemes to protect the privacy of an emerging non-volatile main memory technology â€” phase change memory (PCM). The negative impact of the encryption schemes on PCM lifetime is evaluated and new methods including a new encryption counter scheme and an efficient error correct code (ECC) management are proposed to improve PCM lifetime. In our third approach, we deconstruct two previously proposed secure cache designs against software data-cache-based side channel attacks and demonstrate their weaknesses. We propose three hardware-software integrated approaches as secure protections against those data cache attacks. Also we propose to apply them to protect instruction caches from similar threats. Furthermore, we propose a simple change to the update policy of Branch Target Buffer (BTB) to defend against BTB attacks. Our experiments show that our proposed schemes are both security effective and cost efficient.

Educational Career:
Bachelor's of Automatic Control, BS, 1999, Southeast University
Master's of Computer Science, MS, 2005, University of Central Florida

Committee in Charge:
Huiyang Zhou, Chair, Computer Science
Mark Heinrich, Computer Science
Cliff Zou, Computer Science
Liqiang Ni, statistics

Approved for distribution by Huiyang Zhou, Committee Chair, on May 28, 2010.

The public is welcome to attend.