Effective network security in the golden age of online threats

Lorenzo De Carli
University of Wisconsin-Madison

3/21/2016 at 10:30 am
Core A (Room 301)

Abstract

Intrusion prevention systems (IPSs), which analyze network traffic to detect signs of malicious activity, are a long-standing cornerstone of network security. Nowadays, the combination of advanced, targeted online threats and increasing bandwidth usage is making existing tools increasingly ineffective. In order to cope with the large amounts of data moved by network links, current IPSs limit themselves to simple threat detection strategies which match each network flow against a set of attack signatures. This approach is fragile and limited in expressiveness: signatures can be often evaded by small tweaks in the attack strategy, and fail to capture various classes of attacks altogether.

In my talk I will describe the design of a flexible IPS platform which supports complex threat detection strategies, while satisfying the performance requirement through parallelization. In particular, my work proposes a domain-specific concurrency model, in which a work scheduler partitions network traffic into subsets that can be analyzed independently for threat detection purposes. This scheduler drives a multi-threaded IPS in which concurrent threads always process independent slices of network traffic, making synchronization and inter-thread communication unnecessary. The system uses a novel program analysis technique to automatically generate a suitable work scheduler given any user-defined threat detection algorithm. This makes parallelization general and fully transparent to the operator.

In the second part of my talk I will provide an overview of another relevant contribution of my Ph.D. work: a programmable dataflow-based hardware accelerator for inspection and forwarding of network traffic.

Bio

Lorenzo De Carli is a Ph.D. candidate in Computer Science at the University of Wisconsin-Madison, advised by Somesh Jha. His research interests focus on networking and security, including intrusion prevention and packet
processing. His contributions include parallelization strategies for intrusion prevention, hardware accelerator for packet inspection and forwarding, and analysis of malware communications. He has also worked on optimized signature matching and instruction scheduling for novel processor architectures.


Faculty Host: Thu D. Nguyen