# Fast and Flexible Intrusion Detection and Traffic Analysis

Lorenzo De Carli
*Prospective Faculty Candidate*
University of Wisconsin-Madison
Monday, February 8, 2016 at 3:00 p.m.
Bullen Room ECE 226

## Abstract

Intrusion detection systems (IDSs), which analyze network traffic to discover signs of malicious activity, are a long-standing cornerstone of network security. Nowadays, the combination of increasing bandwidth usage and complex, tailored attacks calls for tools that offer both flexibility and high throughput, introducing a fundamental tension in IDS design. Parallel, high-throughput IDSs are easier to architect if they perform a set of simple, standardized analyses, matching each packet or each flow against a set of attack signatures. However, this approach is fragile and limited in expressiveness; signatures can oftentimes be 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 IDS platform, which supports the deployment of complex threat detection algorithms while enabling automatic parallelization across multiple processing nodes. My work tackles the issue of IDS parallelization by developing a domain-specific concurrency model based on the notion of detection scope: a unit for partitioning network events such that the events contained in each resulting subset are independent for detection purposes. A novel program analysis technique is used to automatically infer the appropriate scope given a threat detection algorithm. This information then guides an event scheduler that ensures that concurrent threads always process independent events, making synchronization and inter-thread communication unnecessary.

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 packet forwarding and inspection. I will also outline my future research plans in two important areas of network security: policy generation and enforcement, and usability of enterprise security tools.

## Biography

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 detection and packet processing. His contributions include parallelization strategies for intrusion detection, 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. Lorenzo received a B.Sc. (2004) and a M.Sc. (2007) in Computer Engineering from Politecnico di Torino, Italy, and a M.Sc. in Computer Science (2010) from the University of Wisconsin-Madison.