



Spring 2010 CIS Colloquium

Towards High Performance Network Defense

Zhichun Li

(Northwestern University)

11:00 PM – 12:00 PM, Friday, March 12
Wachman Hall 447
(4th Floor Conference Room)

ABSTRACT:

Security has become one of the major concerns for today's networks. Network level defense mechanisms are of critical importance. They protect the network as a whole, including the users who do not apply host-based schemes for various reasons (reliability, overhead, conflicts, etc.). Three challenges need to be addressed for network level defense mechanisms. First, the mechanisms have to be high accurate. Second, the mechanisms have to be scalable to the high speed networks with a large number of users. Third, the mechanisms have to be able to respond fast to the emerging threats. My research is to solve these challenges through building a high performance network defense and forensic system.

Particularly, in this talk, I will present the design of NetShield, a new vulnerability signature based NIDS/NIPS which achieves high throughput comparable to that of the state-of-the-art regular expression based systems while offering much better accuracy. This is accomplished because of the following contributions: (i) we propose a candidate selection algorithm which efficiently matches thousands of vulnerability signatures simultaneously using a small amount of memory; (ii) we propose a parsing transition state machine that achieves fast protocol parsing. We intend to implement the software prototype of NetShield as a better alternative to the popular NIDS Snort in terms of both accuracy and speed.