『清华信息大讲堂』第 72 讲

报告题目：	**NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks**	
报告人：	**Prof. Yan Chen (陈焰)**	
	Northwestern University， USA	
报告时间：	2011年3月21日　19:00-21:00	
报告地点：	FIT 1-312	

Abstract:

Accuracy and speed are the two most important metrics for Network Intrusion Detection/Prevention Systems (NIDS/NIPSes). Due to emerging polymorphic attacks and the fact that in many cases regular expressions (regexes) cannot capture the vulnerability conditions accurately, the accuracy of existing regex-based NIDS/NIPS systems has become a serious problem. In contrast, the recently-proposed vulnerability signatures can exactly describe the vulnerability conditions and achieve better accuracy. However, how to efficiently apply vulnerability signatures to high speed NIDS/NIPS with a large ruleset remains an untouched but challenging issue.

We present the first systematic design of vulnerability signature based parsing and matching engine, NetShield, which achieves multi-gigabit throughput while offering much better accuracy. Particularly, we made the following contributions: (i) we proposed a candidate selection algorithm which efficiently matches thousands of vulnerability signatures simultaneously requiring a small amount of memory; (ii) we proposed an automatic lightweight parsing state machine achieving fast protocol parsing. Experimental results show that the core engine of NetShield achieves at least 1.9+Gbps signature matching throughput on a 3.8GHz single-core PC, and can scale-up to at least 11+Gbps under a 8-core machine for 794 HTTP vulnerability signatures. We release our prototype and sample signatures at www.nshield.org.

Biography:

陈焰，2003年获加州大学伯克利分校计算机科学博士学位，现为西北大学电子工程与计算机科学系副教授，计算机科学教学委员会主席, 互联网安全技术实验室主任，主要研究方向为Internet网络管理/测量和网络安全。2005年获得美国能源部青年成就奖（Early CAREER Award），2007年获得美国国防部（Air Force of Scientific Research）青年学者奖（Young Investigator Award），2004和2005年分别获得Microsoft可信计算奖（Trustworthy Computing Awards）。Google Scholar显示，论文总引用超过3600次，H-index指数为21。申请了4项专利。论文Generic and Automatic Address Configuration for Data Center Networks 入选SIGCOMM 2010 最佳论文候选，应邀直接在ACM/IEEE Transaction on Networking上出版. 受邀加入ACM CCS 2009，2011 和SIGCOMM IMC 2009的组织委员会, 并担任ACM CCS 2011的总主席。自2004年起多次受邀在美国自然科学基金委信息科学与工程处担任评委, 并多次受邀担任美国能源部(DOE)和美国空军科研部(DOD) SBIR计划及STTR计划的评委。 Email: ychen@northwestern.edu Web page: www.cs.northwestern.edu/~ychen.

主办单位：信息科学技术学院　　　　联 系 人：李军（62796400）