『Tsinghua Information Forum』72

Title:	**NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks**
Speaker:	**Prof. Yan Chen**
	Northwestern University, USA
Time:	2011-3-21 日 19:00-21:00
Venue:	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:

Dr. Yan Chen is an Associate Professor and the Director of the Lab for Internet and Security Technology (LIST) in the Department of Electrical Engineering and Computer Science at Northwestern University. He got his Ph.D. in Computer Science at University of California at Berkeley in 2003. His research interests include network security, network measurement and diagnosis, for both wired and wireless networks. Prof. Chen won the Department of Energy (DOE) Early CAREER award in 2005, the Department of Defense (DoD) Young Investigator Award in 2007, and the Microsoft Trustworthy Computing Awards in 2004 and 2005 with his colleagues.Based on Google Scholar, his papers have been cited for over 3,600 times, and the h-index of his publications is 21. His paper entitled "Generic and Automatic Address Configuration for Data Center Networks" was selected as one of the three best paper candidates and was awarded fast-track publication in ACM/IEEE Transaction on Networking (ToN). He has more than 60 publications in top conferences and journals such as ACM SIGCOMM, ACM/IEEE ToN, IEEE Symposium on Security and Privacy, ACM/USENIX NSDI, NDSS, SIGCOMM IMC, etc. Prof. Chen is the TPC co-chair for the 15th IEEE International Workshop on Quality of Service (IWQoS) 2007, the 5th International Conference on Security and Privacy on Communication Networks (SecureComm) 2009, and the Next Generation Network (NGN) Symposium of Globecom 2010. He was also invited as the General Chair of ACM CCS 2011.