ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Jianguo DING
Visited Location : FNR/University of Luxembourg, Luxembourg
Duration of Visit: July 23, 2008 – April 22, 2009 (9 months)

I - Scientific activity

During my first stay of ERCIM fellowship, I was involved in following research topics:

1. Probabilistic fault management in distributed dynamic systems. This work is a continue work of my previous research, which focuses on the fault management in a static distributed system. In complex distributed dynamic systems, fault management has to face the uncertain and incomplete management information and dynamic changes in distributed systems. The research challenges include how to model the dynamic systems, and to provide efficient strategies in indentifying the dependencies between effects and causes for fault management. Dynamic Bayesian networks are applied to model the dependencies among managed objects and to provide efficient methods for locating the root causes of failures arising from inaccurate management information in dynamic distributed systems.
2. Behavior-based detection of malicious codes
   With the rising popularity of the Internet, the resulting increase in the number of available vulnerable machines, and the elevated sophistication of the malicious code itself, the detection and prevention of unknown malicious codes meet great challenges. Traditional antivirus scanner employs static features to detect malicious executable codes and is hard to detect the unknown malicious codes effectively. Behavior-based dynamic heuristic analysis approach is proposed for proactive detection of unknown malicious codes. The behavior of malicious codes is identified by system calling through virtual emulation and the changes in system resources. A statistical detection model and mixture of expert (MoE) model are designed to analyze the behavior of malicious codes. The experiment results demonstrate the behavior-based proactive detection is efficient in detecting unknown malicious executable codes.
3. Probabilistic strategies for distributed intrusion detection
   The level of seriousness and sophistication of recent cyber attacks has risen dramatically over the past decade. This brings great challenges for network protection and the automatic security management. Quick and exact localization of intruder by an efficient intrusion detection system (IDS) will be great helpful to network manager. Probabilistic model is proposed to model the distributed intrusion detection based on the characteristic of intruders' behaviors. Inference strategy are developed, which can be used to track the strongest causes (attack source) and trace the strongest dependency routes among the behavior sequences of intruders. This proposed approach can be the foundation for further intelligent decision in distributed intrusion detection.

I thank Prof. Pascal Bouvry and all the colleagues in our group in University of Luxembourg. They helped me a lot in research work and daily administration issues.

II- Publication(s) during your fellowship

1. ***Jianguo Ding**, Bernd J. Krämer, Pascal Bouvry, Haibing Guan, Alei Liang and Franco Davoli:Probabilistic Fault Management. In: Context-Aware Computing and Self-Managing Systems. Waltenegus Dargie (Ed.), pages 309-347. Chapman & Hall/CRC press, ISBN-10: 1420077716, ISBN-13: 978-1420077711, 2009.*

   Abstract:

   In large-scale uncertain and dynamic network environments, the autonomic fault management paradigm is an alternative strategy in assisting to achieve the self-management of the networks. In dealing with autonomic fault management systems, there are three major aspects to be considered: 1) to design an architecture to support autonomic behavior; 2) to represent the uncertain and dynamic information that is necessary to an autonomic object to achieve an autonomic behavior; 3) to communicate and to organize the autonomic objects among themselves in a possible large context, particularly to execute probabilistic reasoning between the depended objects. In this chapter, application issues of probabilistic models for automatic fault management are investigated in order to resolve the fault detection challenges in uncertain and dynamic network environments.

2. ***Jianguo Ding**, Jian Jin, Pascal Bouvry, Yongtao Hu and Haibing Guan: Behavior-based Proactive Detection of Unknown Malicious Codes. Proceedings of 4th International Conference on Internet Monitoring and Protection, pages 72-77, 2009.*

   Abstract:

   With the rising popularity of the Internet, the resulting increase in the number of available vulnerable machines, and the elevated sophistication of the malicious code itself, the detection and prevention of unknown malicious codes meet great challenges. Traditional antivirus scanner employs static features to detect malicious executable codes and is hard to detect the unknown malicious codes effectively. We propose behavior-based dynamic heuristic analysis approach for proactive detection of unknown malicious codes. The behavior of malicious codes is identified by system calling through virtual emulation and the changes in system resources. A statistical detection model and mixture of expert (MoE) model are designed to analyze the behavior of malicious codes. The experiment results demonstrate the behavior-based proactive detection is efficient in detecting unknown malicious executable codes.

III -Attended Seminars, Workshops, and Conferences

1. The second international conference on Modelling, Computation and Optimization in Information Systems and Management Sciences (MCO'08). September 8-10, 2008, Metz, France – Luxembourg.
2. The International conference on FUTURE TRENDS OF THE INTERNET, official launch of the IPv6 Luxembourg Council. January 28, 2009, Neumünster abbey, Luxembourg.
3. 1st Luxembourg Day on Security and Reliability. February 10, 2009, University Campus Kirchberg, Luxembourg city, Luxembourg.
4. Grid'5000 Spring School 2009.April 7-9, 2009. Nancy, France.
5. The Fourth International Conference on Internet Monitoring and Protection. ICIMP 2009. May 24-28, 2009 - Venice/Mestre, Italy .
6. Workshop on “Making data centres and laboratories more sustainable”.March 5, 2009. Chambre de Commerce of Luxembourg, Luxembourg.