Shengzhi Zhang

Rm.328, IST Building,
The Penn State University, University Park, PA, 16802

Email: suz116@cse.psu.edu
Phone: 1-814-206-4609

Education Background

* **Department of Computer Science & Engineering,** The Penn State University, University Park
Ph.D candidate 08/2007 – present Supervised by Dr. Peng Liu GPA: 3.79

* **School of Information Technology, Inha University,** Inchon, Korea
Research Assistant 08/2006 – 07/2007 Supervised by Dr. Sang-Jo Yoo

* **Department of Electrical Engineering and Automation, Tongji University**, Shanghai, China
Bachelor's degree 09/2002 – 06/2006 Class Ranking: 1st/154 GPA: 4.66

Summary

* Four years experiences of using virtual machines (Xen, Qemu, KVM and UML) to enhance system security, e.g., intrusion analysis for production workload servers, driver bug oriented intrusion detection.
* Profound understanding of Linux kernels and proficient Linux kernel debugging
* Proficient C programming in Linux environment, including signal, socket, multi-threaded and etc., comfortable with perl programming.
* Hands-on experiences of Apache http/Tomcat server and proxy deployment, logging, and analysis in the cloud.
* Traffic control and resource management for tiered web server farm in cloud environment (IBM websphere).
* Deep understanding of MAC layer protocol of wireless networking, especially IEEE 802.15.4 networks.
* Key data flow tracking on Flight Management System

Research and Industry Experiences

* **Honeywell Aerospace, Golden Valley, MN** 05/2011 – present

✓ Correspond with DoD project entitled Non-interference Verification of Military Systems.
✓ Investigated the zeroization functionality in Flight Management System of military airplane.
✓ Designed and developed a generic verification approach for zeroization.

* **The Penn State university, University Park** 08/2007 – present

✓ Correspond with AFOSR MURI project entitled Autonomic Recovery of Enterprise-wide Systems after Attack or Failure with Forward Correction.
✓ Designed and implemented PEDA system to comprehensively analyze intrusion/anomaly throughout production workload server systems with lightweight runtime overhead.
✓ Implemented Heter-device system to detect kernel compromise launched from driver code vulnerabilities, and proposed device driver diversity based replication approach.
✓ Developed backtracking intrusions, OS semantics reconstruction, and heterogeneous virtual machine migration from Xen to Qemu.

* **IBM Research Lab in China** 05/2010 – 07/2010

✓ Investigate the issues when applying traditional centralized traffic control and resource management in cloud.
✓ Designed and developed SCOPS system to do QoS differentiation and bottleneck resource overload protection for typical tiered web server farm in cloud environment.

* **Inha University, South Korea** 08/2006 – 06/2007

✓ Investigate IEEE 802.15.4, IEEE 802.15.2, and IEEE 802.11 specifications and analyzed the performance of the MAC layer protocol.

- ✓ Discovered Continuous Hidden Node Collision (CHNC) problem specialized in IEEE 802.15.4 networks.
- ✓ Designed a group-based lightweight protocol to help swiftly recover from CHNC problem

Honors and Awards

* **ACSAC Conferenceship/Student Travel Award**, 2010
* **CCS Workshop Student Travel Grant**, 2010
* **AT&T Graduate Fellowship**, 2010
* **IT Scholarship,** Korea Government, 08/2006 - 06/2007
* **Outstanding Graduates in Shanghai,** Shanghai Municipal People's Government, 05/2006
* **Guo/Xie Birong Scholarship**, 12/2004
* **Excellent Student Scholarship,** Tongji University, 2003, 2004, 2005

Selected Publication

* **S. Zhang**, P. Liu. *Heter-Device: Towards Swift Detecting of Compromised Drivers* (Submitted to DSN '12).

***** J. Jiang, X. Jia, D. Feng, **S. Zhang**, P. Liu. *HyperCrop: A Hypervisor-based Countermeasure for Return Oriented Programming*. ICICS '11.

* **S. Zhang**, W. Wang, H. Wu, B. Yang, P. Liu. *SCOPS: Towards Transparent and Distributed Workload Management for Large Scale Web Servers t* (To appear in IEEE Transactions on Network and Service management).

* **S. Zhang**, W. Wang, H. Wu, B. Yang, P. Liu. *Distributed Workload and Response Time Management for Web Applications*. CNSM '11 (accept rate = 15%).

* J. Yu, **S. Zhang**, P. Liu, Li Zhitang. *LeakProber: A Framework for Profiling Sensitive Data Leakage Path.* ACM CODASPY '11 (accept rate = 30%).

* **S. Zhang**, X. Jia, J. Jing, P. Liu. PEDA: Comprehensive Damage Assessment for Production Environment Server Systems. IEEE Transactions on Information Forensics and Security.

* **S. Zhang**, X. Jia, J. Jing, P. Liu. *Cross-Layer Comprehensive Intrusion Harm Analysis for Availability-Critical Server Systems*. ACSAC '10 (accept rate = 17%).

* **S. Zhang**, X, Xiong, P. Liu. *Challenges in Improving the Survivability of Data Centers*. Workshop on Survivability in Cyberspace sponsored by Air Force '10 (invited paper).

* **S. Zhang**, X. Xiong, X. Jia, P. Liu. *Availability-Sensitive Intrusion Recovery.* ACM VMSec '09 (position paper).

* **S. Zhang**, S. Yong. *Fast Recovery from Hidden Node Collision for IEEE 802.15.4 LR-WPANs.* IEEE CIT 2007.

Technical Presentations

* *Cross-Layer Comprehensive Intrusion Harm Analysis for Availability-Critical Server Systems*. ACSAC '10
* *Challenges in Improving the Survivability of Data Centers*. Survivability in Cyberspace by Air Force, 2009
* *Availability-Sensitive Intrusion Recovery.* VMSec '09
* *Using Virtual Machines to Do Cross-Layer Damage Assessment*. VMSec '08
* *Cross-Layer Comprehensive Infection Diagnosis for Availability-Critical Server Systems*. Eurosys '10 poster

Patent

Adaptive Hidden Node Collision Recovery Protocol for IEEE 802.15.4 LR-WPANs. Patent NO. 10-0896986. Korean Intellectual Property Office

Profesional Activities (Peer Reviewers)

* ACM CCS '08, IEEE INFONCOM '09, '10, '11, ESORICS '08, ACSAC '08, '09, SecureComm '08, '09, ACNS '10