Miao Yu

Contact Information

School of Software
Shanghai Jiao Tong University
No.800, Dongchuan Rd.
Minhang District, Shanghai

Mobile: +86-13917246678
E-mail: miao.yu.2012@gmail.com
WWW: http://202.120.40.124/index.php/User:Superymk

Research Interests

Security and privacy on computer and mobile devices.
Virtualization.
High performance computing in virtual machine.

Education

CyLab, Carnegie Mellon University (CMU), Pennsylvania, United States

Ph.D. in Computer Security (Expected) 05/2016

- Area of Study: Virtualization Based Trusted Computing

Shanghai Jiao Tong University (SJTU), Shanghai, China

M.S. in Computer Software and Theory 03/2012

- Area of Study: Virtualization Based Trusted Computing
- Overall Rank: 3/116

B.S. in Software Engineering 07/2009

- Major GPA: 89.0/100.0
- Rank: 15/110

Honors and Awards

- **Ann and Martin McGuinn Graduate Fellowship**, 01/2013
- **Carnegie Institute of Technology Dean's Tuition Fellowship**, 09/2012
- **The 7th China National Post-Graduate Mathematical Contest in Modeling, Third Class Prize**, *Rate:445/1995.* 12/2010
- **SJTU First Class Graduate Scholarship**, *Rate:5/116.* 09/2010
- **SJTU Second Class Graduate Scholarship**, *Rate:27/116.* 09/2009
- **IBM Excellent Students in China Scholarship**, *Rate:1/450 (1st among all undergraduate students in the school).* 06/2009
- **SJTU Excellent Undergraduate Thesis**, *Rate:10/110.* 06/2009
- **SJTU Outstanding Student Scholarship**, *Rate:10/110.* 01/2008
- **Microsoft Student Innovation Contest Third Class and Excellence Awards.** 01/2008
- **Yahoo! Widget Design Contest, Second Class Awards.** 12/2006

Research Experience

Research Assistant, Current Project (Participant) 03/2013 — present

- Improve XMHF system since v0.2.2.
- Develop a secure kernel on ARM Cortex-A15. Modularize TrustVisor/XMHF on all platforms. The root motivation is to point out that micro-hypervisor is one of the future security directions.

Research Assistant, ROP Project (Participant) 03/2013 — 11/2013

- Develop a new tool to detect ROP attack in application level.

Research Assistant, GLaDOS Project (Leader) 07/2011 — 01/2012

- Lead the research on improving the QoS of I/O resources in virtual machine environment. Implement prototype and investigate the related work currently. Conduct several experiments to estimate the effectiveness and performance of the proposed approach.

Research Assistant, *Vis Project (Leader)* 12/2010 — 07/2011

- Vis provides accurate live acquisition on native system. It accurately dumps physical memory content while the target system is running.
- Solved low-accuracy and high impact to running environment problem found in previous approaches. This was achieved by using drop-in Virtual Machine Manager (VMM) as well as hardware assisted nested paging technology. After optimized, Vis achieved 100% result accuracy while only incurring 10% performance overhead.
- Published 1 paper on APSys'11, which is the Asia-Pacific counterpart of EuroSys.

Research Assistant, *Joan Project (Participant)* 03/2010 — 12/2010

- Joan is used to protect the sensitive part of application at runtime.
- Implemented prototypes for required fundamental techniques, such as hypercall interception and Extended Page Table based machine physical page access checking. This enabled Joan to make use of hardware memory virtualization technology and hence improved overall performance.
- Implemented 5 case studies and conducted a series of evaluations.
- Published 1 poster on OSDI'10 and 1 paper on ICPADS'10.

Research Assistant, *SPAD Project (Participant)* 07/2009 — 07/2010

- SPAD is an anti-debugging tool based on hardware virtualization technology. This project is funded by National Natural Science Foundation of China (Trusted Computing on Virtualization Environment Project, 2008).
- Designed and implemented SPAD's core.
- Added anti-debugging logic in the previous drop-in VMM by sampling real world debug mechanism on Windows XP. As a result, it was able to identify all 9 popular debuggers, while incurring less than 3% performance overhead.

Research Assistant, *HBSP Project (Leader)* 01/2009 — 07/2009

- HBSP provides a driver framework of hardware virtualization. This project is part of The 863 Key Program of China (Virtualized Execution in Network Computing Environment, 2006). It is also funded by Intel (Multi-thread Virtualization on Multi-core platform, 2008).
- Designed and implemented the following features: drop-in VMM; compatibility with x86 platform; memory hiding by constructing private page table; fast virtual machine event handling; support for third-party development.

Research Assistant, *SmartHome Project (Participant)* 09/2007 — 09/2008

- SmartHome provides a software framework of home automation. This project is part of The 863 Key Program of China (Reconfigurable RFID middleware research and development, 2006).
- Designed and implemented the gateway-appliance communication protocol as well as the software stack on gateway. These were the most important parts of the whole project. Achieved the properties of high flexibility and modularity.

Internship Experience

MSRA Researcher Intern *10/2011 — 05/2012*
Microsoft Research Asia

- Analyze the workload's essence for China Meteorological Administration.
- Abstract the case to a general problem and solve it on Hadoop implementation.
- Establish a baseline performance curve on top of distributed clusters.

Software Test Engineer Intern *11/2008 — 05/2009*
Microsoft STB in Shanghai

- Tested the Workflow Designer in Visual Studio 2010 Beta 1.
- Found about 40 bugs. Contributed more than 9000 LOC of test cases.

Summer Associate *07/2008 — 09/2008*
Morgan Stanley IT in Shanghai

- Designed and implemented an in-house stock exchange simulator prototype.
- Finished the project in limited 50 days, including writing documents. Learned financial knowledge and studied in-house middleware.

Publications

* Conferences

[conf1] Miao Yu, Chao Zhang, Zhengwei Qi, Jianguo Yao, Yin Wang, and Haibing Guan. VGRIS: virtualized gpu resource isolation and scheduling in cloud gaming. In Manish Parashar, Jon B. Weissman, Dick H. J. Epema, and Renato J. O. Figueiredo, editors, *HPDC*, pages 203–214. ACM, 2013.

[conf2] C. Zhang, Z. Qi, J. Yao, M. Yu, and H. Guan. vGASA: Adaptive scheduling algorithm of virtualized gpu resource in cloud gaming. volume PP, pages 1–1, 2013.

[conf3] Miao Yu, Zhengwei Qi, Qian Lin, Xianming Zhong, Bingyu Li, and Haibing Guan. Vis: Virtualization enhanced live forensics acquisition for native system. *Digital Investigation*, 9(1):22–33, 2012.

[conf4] Miao Yu, Qian Lin, Bingyu Li, Zhengwei Qi, and Haibing Guan. Vis: Virtualization enhanced live acquisition for native system. In *The 2nd ACM SIGOPS Asia-Pacific Workshop on Systems*, APSYS 2011.

[conf5] Miao Yu, Peijie Yu, Shang Gao, Qian Lin, and Zhengwei Qi. HBSP: A lightweight hardware virtualization based framework for transparent software protection in commodity operating systems. FCST 2009.

[conf6] Junqing Wang, Miao Yu, Bingyu Li, Zhengwei Qi, and Haibing Guan. Hypervisor-based protection of sensitive files in a compromised system. In *ACM Symposium on Applied Computing*, SAC 2012.

[conf7] Min Zhu, Miao Yu, Peijie Yu, Shang Gao, and Zhengwei Qi. VASP: Virtualization assisted security monitor for cross-platform protection. In *ACM Symposium on Applied Computing*, SAC 2011.

[conf8] Mingyuan Xia, Miao Yu, Qian Lin, Zhengwei Qi, and Haibing Guan. Enhanced privilege separation for commodity software on virtualized platform. In *International Conference on Parallel and Distributed Systems*, ICPADS 2010.

[conf9] Qian Lin, Mingyuan Xia, Miao Yu, Peijie Yu, Min Zhu, Shang Gao, Zhengwei Qi, and Haibing Guan. SPAD: Software protection through anti-debugging using hardware virtualization. In *ACM Symposium on Applied Computing*, SAC 2011.

[conf10] Tengfei Yi, Aijun Zong, Miao Yu, Shang Gao, Qian Lin, Peijie Yu, Zhong Ren, and Zhengwei Qi. Anti-debugging framework based on hardware virtualization technology. ICRCCS 2009.

[conf11] Shang Gao, Qian Lin, Mingyuan Xia, Miao Yu, Zhengwei Qi, and Haibing Guan. Debugging classification and anti-debugging strategies. In *Proceedings of the 2010 International Conference on Software and Computing Technology*, ICSCT 2010.

* Books

[book1] Miao Yu and Zhengwei Qi. *NewBluePill: Hardware Virtual Machine Under the Hood (In Chinese)*. Tsinghua Press, 1st edition, 2011.

* Technical Reports

[tech1] Miao Yu, Qian Lin, Mingyuan Xia, Peijie Yu, Min Zhu, Shang Gao, Zhengwei Qi, Xue Liu, and Haibing Guan. SPAD: Software protection through anti-debugging based on hardware-assisted virtualization. XCON 2010.

[tech2] Mingyuan Xia, Miao Yu, Zhengwei Qi, and Haibing Guan. Joan: Shepherd application privacy with virtualized special purpose memory. In *9th USENIX Symposium on Operating Systems Design and Implementation*, OSDI 2010 (Poster).

[tech3] Miao Yu, Peijie Yu, Shang Gao, Qian Lin, Zhengwei Qi, and Haibing Guan. HBSP: A lightweight hardware virtualization based framework for transparent software protection in commodity operating systems (In Chinese). CNCC 2009.

PATENTS

Patentee of "Accurate Obtaining Memory Content on Running System" Patent No. 201110190086.5

Patentee of "Feedback Based Virtualized GPU Resource Scheduling Framework and Algorithms" [1] Apply No. 201210261862.0

[1] This patent is accepted by the State Intellectual Property Office of the P.R.C.