Weidong Cui **Curriculum Vitae**

CONTACT INFORMATION

Voice: +1 (425) 421-7749
E-mail: wdcui@microsoft.com
Web: http://research.microsoft.com/~wdcui/

EDUCATION

1. **University of California, Berkeley** Berkeley, CA, USA
   Ph.D., Electrical Engineering and Computer Sciences December 2006
   Thesis: "Automating Malware Detection by Inferring Intent"

2. **University of California, Berkeley** Berkeley, CA, USA
   M.S., Computer Science May 2003
   Thesis: "Backup Path Allocation based on a Correlated Link Failure Probability Model in Overlay Networks"

3. **Tsinghua University** Beijing, CHINA
   M.Eng., Electronic Engineering June 2000
   Thesis: "Design and Implementation of a Support Vector Machine-based Automatic Text Categorization System"

4. **Tsinghua University** Beijing, CHINA
   B.Eng., Electronic Engineering June 1998
   Thesis: "Design and Implementation of a Category-based Search Engine System"

EMPLOYMENT

1. **Microsoft Research** Redmond, WA, USA
   Senior Researcher March 2014 - Present
   Researcher September 2006 - March 2014

   - *Crash Dump Triaging*: Developed a new crash dump triaging system that improves the bug bucketing accuracy from 50% to 90% and is being deployed it on Windows Error Reporting to analyze all crashes sent back to Microsoft.
   - *Windows Kernel Rootkit*: Developed a new Windows kernel rootkit detection system based on precise pointer analysis that improves the memory analysis coverage from 30% to 90%; deployed it in multiple production systems.
   - Other projects on binary/source code analysis, virtualization, security analytics, reverse engineering.

2. **International Computer Science Institute** Berkeley, CA, USA
   Research Assistant May 2005 - May 2006

   - *Honeyfarm*: designed and implemented a large-scale honeyfarm system from scratch to monitor a quarter-million IP addresses and detect Internet worms.

3. **Hewlett-Packard Laboratories** Palo Alto, CA, USA
   Summer Intern May 2002 - August 2002

   - *Congestion Control for Media Streaming*: designed and implemented a new congestion control scheme for media streaming that can significantly reduce playback disruptions.

4. **University of California, Berkeley** Berkeley, CA, USA
   Graduate Student Researcher August 2000 - September 2006

- *Extrusion-based Break-In Detector*: designed and implemented a system that can detect malware break-ins by correlating user inputs with outbound network connections.
- *Backup Path Allocation*: designed a new algorithm for backup path allocation in overlay networks that takes into account the correlations of overlay links.

5. **Tsinghua University** Beijing, CHINA
   Graduate Student Researcher September 1998 - July 2000

   - *Text Classification*: designed a new Support Vector Machine-based text classification algorithm that leverages boosting for better feature selection.

HONORS AND AWARDS

1. **Gold Star Award**, Microsoft Corporation, 2011.
2. **Regents Fellowship** of the University of California, Berkeley, 2000.
3. **Motorola Scholarship** for Academic Excellence, 1999.
4. **Tsinghua Student Scholarship** for Academic Excellence, 1995-1998.
5. **Tsinghua Freshman Scholarship** for Academic Excellence, 1994.
6. **Henan Zhong-Yuan Scholarship** for Academic Excellence in High School, 1994.
7. **Second Place** in Henan Province in Chinese National Mathematical Olympiad, 1993.

PUBLICATIONS

Refereed Publications

1. Adam Doupe, **Weidong Cui**, Mariusz Jakubowski, Marcus Peinado, Christopher Kruegel, Giovanni Vigna, "deDacota: Toward Preventing Server-Side XSS via Automatic Code and Data Separation", in *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS)*, ACM, November 2013.
2. **Weidong Cui**, Marcus Peinado, Zhilei Xu, Ellick Chan, "Tracking Rootkit Footprints with a Practical Memory Analysis System", in *Proceedings of the 21st USENIX Security Symposium*, USENIX, August 2012.
3. Christian Kreibich, Nicholas Weaver, Chris Kanich, **Weidong Cui**, Vern Paxson, "Practical Containment for Measuring Modern Malware Systems", In *Proceedings of the 2011 International Measurement Conference*, Berlin, Germany, November 2 - 4, 2011.
4. Martim Carbone, **Weidong Cui**, Long Lu, Wenke Lee, Marcus Peinado, Xuxian Jiang, "Mapping Kernel Objects to Enable Systematic Integrity Checking", In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, November 9 - 13, 2009.
5. Zhi Wang, Xuxian Jiang, **Weidong Cui**, Peng Ning, "Countering Kernel Rootkits with Lightweight Hook Protection", In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, November 9 - 13, 2009.
6. Monirul Sharif, Wenke Lee, **Weidong Cui**, Andrea Lanzi, "Secure In-Vm Monitoring Using Hardware Virtualization", In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, November 9 - 13, 2009.
7. Zhi Wang, Xuxian Jiang, **Weidong Cui**, Xinyuan Wang, Mike Grace, "ReFormat: Automatic Reverse Engineering of Encrypted Messages", In *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS)*, Saint Malo, France, September 2009.
8. **Weidong Cui**, Marcus Peinado, Karl Chen, Helen J. Wang, Luis Irun-Briz, "Tupni: Automatic Reverse Engineering of Input Formats", In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, USA, October 27 - 31, 2008.
9. Zhi Wang, Xuxian Jiang, **Weidong Cui**, Xinyuan Wang, "Countering Persistent Kernel Rootkits Through Systematic Hook Discovery", In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Boston, MA, USA, September 15 - 17, 2008.

10. Benjamin Livshits, **Weidong Cui**, "Spectator: Detection and Containment of JavaScript Worms", In *Proceedings of the 2008 USENIX Annual Technical Conference*, Boston, MA, USA, June 22 - 27, 2008.
11. **Weidong Cui**, Jayanthkumar Kannan, Helen J. Wang, "Discoverer: Automatic Protocol Reverse Engineering from Network Traces", In *Proceedings of the 16th USENIX Security Symposium*, Boston, MA, August 6 - 10, 2007.
12. **Weidong Cui**, Marcus Peinado, Helen J. Wang, Michael Locasto, "ShieldGen: Automated Data Patch Generation for Unknown Vulnerabilities with Informed Probing", In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Oakland, CA, May 20 - 23, 2007.
13. **Weidong Cui**, "Automating Malware Detection by Inferring Intent", Ph.D. Dissertation, University of California, Berkeley, September 2006.
14. **Weidong Cui**, Vern Paxson, Nicholas Weaver, Randy H. Katz, "Protocol-Independent Adaptive Replay of Application Dialog", In *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2 - 3, 2006.
15. **Weidong Cui**, Randy H. Katz, Wai-tian Tan, "Design and Implementation of an Extrusion-based Break-In Detector for Personal Computers", In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC)*, Tuscon, AZ, December 5 - 9, 2005. 22.8%)
16. Martin Casado, Tal Garfinkel, **Weidong Cui**, Vern Paxson, Stefan Savage, "Opportunistic Measurement: Extracting Insight from Spurious Traffic", In *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, College Park, MD, November 14 - 15, 2005.
17. **Weidong Cui**, Randy H. Katz, Wai-tian Tan, "BINDER: An Extrusion-based Break-In Detector for Personal Computers", In *Proceedings of the 2005 USENIX Annual Technical Conference*, Anaheim, CA, USA, April 10 - 15, 2005.
18. Wai-tian Tan, **Weidong Cui**, John Apostolopoulos, "Playback-Buffer Equalization for Streaming Media using Stateless Transport Prioritization", In *Proceedings of the 13th International Packet Video Workshop*, Nantes, France, April 28 - 29, 2003.
19. **Weidong Cui**, Ion Stoica, Randy H. Katz, "Backup Path Allocation based on a Correlated Link Failure Probability Model in Overlay Networks", In *Proceedings of the Tenth International Conference on Network Protocols (ICNP)*, Paris, France, November 12 - 15, 2002.
20. B. Raman, S. Agarwal, Y. Chen, M. Caesar, **W. Cui**, P. Johansson, K. Lai, T. Lavian, S. Machiraju, Z. M. Mao, G. Porter, T. Roscoe, M. Seshadri, J. Shih, K. Sklower, L. Subramanian, T. Suzuki, S. Zhuang, A. D. Joseph, R. H. Katz, I. Stoica, "The SAHARA Model for Service Composition Across Multiple Providers", In *Proceedings of the First International Conference on Pervasive Computing*, Zürich, Switzerland, August 26 - 28, 2002. (invited paper)
21. **Weidong Cui**, Zhihua Zhou, Xing Li, "Research on the VC-Dimension Computation for Neural Networks", *Computer Science*, n6, 2000. (in Chinese)
22. **Weidong Cui**, Zhihua Zhou, Xing Li, "Research of Support Vector Machines", *Computer Engineering and Applications*, 2000. (in Chinese)
23. **Weidong Cui**, Xing Li, "ATM-based Wireless Broadband Networks", *Telecommunications Technology*, n5, 1999. (in Chinese)
24. **Weidong Cui**, Xing Li, "Design and Implementation of a Category-based Search System for Chinese Homepages", *Computer Engineering and Applications*, 1999. (in Chinese)

Non-Refereed Publications

1. Chengyu Song, **Weidong Cui**, Marcus Peinado, Wenke Lee, "CloudShot: Fast Capturing of Virtual Machine Memory for Security Monitoring", Microsoft Research Technical Report MSR-TR-2014-138, October, 2014.

2. Brendan Dolan-Gavitt, **Weidong Cui**, David Molnar, Wenke Lee, "CAR2: Continuous Application Record and Replay", Microsoft Research Technical Report MSR-TR-2014-137, October, 2014.
3. **Weidong Cui**, Zhilei Xu, Marcus Peinado, Ellick Chan, "Typing Dynamic Data for Memory Analysis and Debugging", Microsoft Research Technical Rerpot MSR-TR-2011-79, June, 2011.
4. Benjamin Livshits, **Weidong Cui**, "Spectator: Detection and Containment of JavaScript Worms", Microsoft Research Technical Report MSR-TR-2007-55, May, 2007. (26 pages)
5. **Weidong Cui**, Vern Paxson, Nicholas Weaver, "GQ: Realizing a System to Catch Worms in a Quarter Million Places", ICSI Technical Report TR-06-004, September 2006. (19 pages)
6. **Weidong Cui**, Randy H. Katz, Wai-tian Tan, "BINDER: An Extrusion-based Break-In Detector for Personal Computers", Technical Report UCB-CSD-04-1352, October 2004. (13 pages)
7. **Weidong Cui**, Sridhar Machiraju, Randy H. Katz, Ion Stoica, "SCONE: A Tool to Estimate Shared Congestion Among Internet Paths", *Technical Report UCB-CSD-04-1320*, Berkeley, CA, USA, May 2004. (18 pages)

PATENTS

1. "Application Monitoring through Collective Record and Replay", U.S. Patent Granted.
2. "Automatic Reverse Engineering of Input Formats", U.S. Patent Granted.
3. "Automatic Data Patch Generation for Unknown Vulnerabilities", U.S. Patent Number 8,613,096.
4. "Demand-Driven Analysis of Pointers for Software Program Memory Analysis and Debugging", U.S. Patent Number 8,589,888.
5. "Data Access Reporting Platform for Secure Active Monitoring", U.S. Patent Number 8,584,254.
6. "Malware Investigation by Analyzing Computer Memory", U.S. Patent Number 8,566,944.
7. "Detecting Data Propagation in a Distributed System", U.S. Patent Number 7,933,946.
8. "Automatic Reverse Engineering of Message Formats from Network Traces", U.S. Patent Number 7,802,009.
9. "Automatic Code and Data Separation of Web Applications", Pending, June, 2013.
10. "Fast and Secure Virtual Machine Memory Checkpointing", Pending, June, 2013.
11. "Personal Identification Combining Proximity Sensing with Biometrics", Pending, March, 2012.
12. "Computer Memory Access Monitoring and Error Checking", Pending, November, 2011.
13. "Determining Target Types for Generic Pointers in Source Code", Pending, June, 2009.

PROFESSIONAL ACTIVITIES

1. **Technical Program Committee Member**, the 21st ACM Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3 - 7, 2014.
2. **Technical Program Committee Member**, the 35th IEEE Security and Privacy Symposium, San Jose, CA, USA, May 19 - 21, 2014.
3. **Technical Program Committee Member**, the 20th ACM Conference on Computer and Communications Security, Berlin, Germany, November 4 - 8, 2013.
4. **Technical Program Committee Member**, the 34th IEEE Security and Privacy Symposium, San Francisco, CA, USA, May 19 - 21, 2013.
5. **Technical Program Committee Member**, the 33rd IEEE Security and Privacy Symposium, San Francisco, CA, USA, May 20 - 23, 2012.
6. **Technical Program Committee Member**, the 32nd IEEE Security and Privacy Symposium, Oakland, CA, USA, May 22 - 25, 2011.

7. **Technical Program Committee Member**, the 18th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, February 6 - 9, 2011.
8. **Technical Program Committee Member**, the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, October 4 - 8, 2010.
9. **Technical Program Committee Member**, the 17th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, February 28 - March 3, 2010.
10. **Technical Program Committee Member**, the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, November 9 - 13, 2009.
11. **Technical Program Committee Member**, the Fifth ICST Interantional Conference on Security and Privacy in Communication Networks, Athens, Greece, September 14 - 17, 2009.
12. **Technical Program Committee Member**, the 30th IEEE Security and Privacy Symposium, Oakland, CA, USA, May 17 - 20, 2009.
13. **Technical Program Committee Member**, the 16th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, February 8 - 11, 2009.
14. **Technical Program Committee Member**, the Fourth ICST Interantional Conference on Security and Privacy in Communication Networks, Istanbul, Turkey, September 22 - 25, 2008.
15. **Technical Program Committee Member**, the Fifth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment, Paris, France, July 2008.
16. **Technical Program Committee Member**, the Second International Workshop on Critical Information Infrastructures Security, Benalmadena-Costa (Malaga), Spain, October 3-5, 2007.
17. **Technical Program Committee Member**, the Fourth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment, Lucerne, Switzerland, July 12 - 13, 2007.
18. **Technical Program Committee Member**, the 16th International World Wide Web Conference, Banff, Alberta, Canada, May 8 - 12, 2007.

PROFESSIONAL SOCIETY MEMBERSHIPS

1. **Member** of the Association of Computing Machinery (ACM)
2. **Member** of the Institute of Electrical and Electronics Engineers (IEEE)