Debin Gao

Assistant Professor
School of Information Systems
Singapore Management University
80 Stamford Road, Singapore 178902

Tel: +65 6828 0969
Email: dbgao@smu.edu.sg
Web: http://flyer.sis.smu.edu.sg

Education

Carnegie Mellon University, Pittsburgh, PA, USA.

- Ph.D., Electrical and Computer Engineering, Dec 2006.
  Advisors: Michael K. Reiter, Dawn Song
  Thesis Topic: Gray-Box Anomaly Detection using System Call Monitoring

- M.S., Electrical and Computer Engineering, May 2004.
  Advisors: Michael K. Reiter, Dawn Song
  Thesis Topic: Gray-Box Program Tracking for Anomaly Detection

Nanyang Technological University, Singapore.

- B.Eng., Electrical and Electronic Engineering, May 2001.
  First Class Honor

Professional Experience

Assistant Professor (July 2007 – present)
School of Information Systems
Singapore Management University

Software Engineer (January 2007 – May 2007)
CyLab
Carnegie Mellon University

Intern in Systems & Networking Research Group (May 2005 – August 2005)
Microsoft Research
Microsoft Corp., Redmond, WA, USA.

Publications

Debin Gao, Michael K. Reiter and Dawn Song. On Gray-Box Program Tracking for Anomaly Detection. In *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, USA, August 2004.

Debin Gao, Michael K. Reiter and Dawn Song. Gray-Box Extraction of Execution Graphs for Anomaly Detection. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, Washington, DC, USA, October 2004.

Debin Gao, Michael K. Reiter and Dawn Song. Behavioral Distance for Intrusion Detection. In *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID 2005)*, Seattle, WA, USA, September 2005.

Debin Gao, Michael K. Reiter and Dawn Song. Behavioral Distance Measurement using Hidden Markov Models. In *Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection (RAID 2006)*, Hamburg, Germany, September 2006.

Hyundo Park, Peng Li, Debin Gao, Heejo Lee and Robert H. Deng. Distinguishing between FE and DDoS using Randomness Check. In *Proceedings of the 11th Information Security Conference (ISC 2008)*, Taipei, September 2008.

Debin Gao, Michael K. Reiter and Dawn Song. BinHunt: Automatically Finding Semantic Differences in Binary Programs. In *Proceedings of the 10th International Conference on Information and Communications Security (ICICS 2008)*, Birmingham, UK, October 2008.

Peng Li, Hyundo Park, Debin Gao and Jianming Fu. Bridging the Gap between Data-flow and Control-flow Analysis for Anomaly Detection. In *Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC 2008)*, Anaheim, California, USA, December 2008.

Debin Gao, Michael K. Reiter and Dawn Song. Beyond Output Voting: Detecting Compromised Replicas using HMM-based Behavioral Distance. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, April 2009.

Jin Han, Debin Gao and Robert H. Deng. On the Effectiveness of Software Diversity: A Systematic Study on Real-World Vulnerabilities. In *Proceedings of the 6th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2009)*, Milan, Italy, July 2009.

Peng Li, Debin Gao and Michael K. Reiter. Automatically Adapting a Trained Anomaly Detector to Software Patches. In *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID 2009)*, Saint-Malo, Brittany, France, September 2009.

Limin Liu, Jiang Ming, Zhi Wang, Debin Gao and Chunfu Jia. Denial-of-Service Attacks on Host-Based Generic Unpackers. In *Proceedings of the 11th International Conference on Information and Communications Security (ICICS 2009)*, Beijing, China, December 2009.

Payas Gupta and Debin Gao. Fighting Coercion Attacks in Key Generation using Skin Conductance. In *Proceedings of the 19th USENIX Security Symposium*, Washington, DC, USA, August 2010.

Peng Li, Limin Liu, Debin Gao and Michael K. Reiter. On Challenges in Evaluating Malware Clustering. In *Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID 2010)*, Ottawa, Ontario, Canada, September 2010.

Jin Han, Meng Pan, Debin Gao and HweeHwa Pang. A Multi-User Steganographic File System on Untrusted Shared Storage. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, Texas, USA, December 2010.

Zhi Wang, Renquan Cheng and Debin Gao. Revisiting Address Space Randomization. In *Proceedings of the 13th Annual International Conference on Information Security and Cryptology (ICISC 2010)*, Seoul, Korea, December 2010.

Jiang Ming, Haibin Zhang and Debin Gao. Towards Ground Truthing Observations in Gray-Box Anomaly Detection. In *Proceedings of the 5th International Conference on Network and System Security (NSS 2011)*, Milan, Italy, September 2011.

Jin Han, Qiang Yan, Robert H. Deng and Debin Gao. On Detection of Erratic Arguments. In *Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2011)*, London, United Kingdom, September 2011.

Zhi Wang, Jiang Ming, Chunfu Jia and Debin Gao. Linear Obfuscation to Combat Symbolic Execution. In *Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS 2011)*, Leuven, Belgium, September 2011.

Kangjie Lu, Dabi Zou, Weiping Wen and Debin Gao. Packed, Printable, and Polymorphic Return-Oriented Programming. In *Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID 2011)*, Menlo Park, California, USA, September 2011.

Kangjie Lu, Dabi Zou and Debin Gao. deRop: Removing Return-Oriented Programming from Malware. In *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC 2011)*, Orlando, Florida, USA, December 2011.

Payas Gupta, Tan Kiat Wee, Narayan Ramasubbu, David Lo, Debin Gao, and Krishna Balan. Human: Creating Memorable Fingerprints of Mobile Users. In *Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications (PerCom 2012)*, Lugano, Switzerland, March 2012.

Payas Gupta, Xuhua Ding, and Debin Gao. Coercion Resistance in Authentication Responsibility Shifting. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2012)*, Seoul, South Korea, May 2012.

Simon Williamson, Pradeep Varakantham, Debin Gao and Chen Hui Ong. Active Malware Analysis using Stochastic Games. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012)*, Valencia, Spain, June 2012.

Lei Zhao, Debin Gao and Lina Wang. Learning Fine-Grained Structured Input for Memory Corruption Detection. In *Proceedings of the 15th Information Security Conference (ISC 2012)*, Passau, Germany, September 2012.

Tiffany Hyun-Jin Kim, Payas Gupta, Jun Han, Emmanuel Owusu, Jason Hong, Adrian Perrig and Debin Gao. OTO: Online Trust Oracle for User-Centric Trust Establishment. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS 2012)*, Raleigh, NC, USA, October 2012.

Jiang Ming, Meng Pan and Debin Gao. iBinHunt: Binary Hunting with Inter-Procedural Control Flow. In *Proceedings of the 15th Annual International Conference on Information Security and Cryptology (ICISC 2012)*, Seoul, Korea, December 2012.

Jin Han, Qiang Yan, Debin Gao, Jianying Zhou and Robert Deng. Comparing Mobile Privacy Protection through Cross-Platform Applications. In *Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS 2013)*, San Diego, CA, USA, February 2013.

Chee Meng Tey, Payas Gupta and Debin Gao. I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics. In *Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS 2013)*, San Diego, CA, USA, February 2013, distinguished paper award.

Payas Gupta, Swapna Gottipati, Jing Jiang and Debin Gao. Your Love is Public Now: Questioning the use of Personal Information in Authentication. In *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013)*, Hangzhou, China, May 2013.

Peng Li, Debin Gao and Michael K. Reiter. Mitigating Access-Driven Timing Channels in Clouds using StopWatch. In *Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)*, Budapest, Hungary, June 2013.

Jin Han, Mon Kywe Su, Qiang Yan, Feng Bao, Huijie Robert Deng, Debin Gao, Yingjiu Li, and Jianying Zhou. Launching generic attacks on iOS with approved third-party applications. In *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)*, Banff, Alberta, Canada, June 2013.

Chee Meng Tey, Payas Gupta, Debin Gao and Yan Zhang. Keystroke Timing Analysis of on-the-fly Web Apps. In *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)*, Banff, Alberta, Canada, June 2013.

Chee Meng Tey and Debin Gao. Defending against heap overflow by using randomization in nested virtual clusters. In *Proceedings of the 15th International Conference on Information and*

Communications Security (ICICS 2013), Beijing, China, November 2013.

Kangjie Lu, Siyang Xiong and Debin Gao. RopSteg: Program Steganography with Return Oriented Programming. In *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY 2014)*, San Antonio, TX, USA, Mar 2014.

Chee Meng Tey, Payas Gupta, Karthik Muralidharan and Debin Gao. Keystroke Biometrics: the user perspective. In *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY 2014)*, San Antonio, TX, USA, Mar 2014.

Haoyu Ma, Xinjie Ma, Weijie Liu, Zhipeng Huang, Debin Gao and Chunfu Jia. Control Flow Obfuscation using Neural Network to Fight Concolic Testing. In *Proceedings of the 10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014)*, Bejing, China, September 2014.

Peng Li, Debin Gao and Michael K. Reiter. StopWatch: A Cloud Architecture for Timing Channel Mitigation. In *ACM Transactions on Information and System Security (TISSEC)*, November 2014.

Jin Han, Qiang Yan, Debin Gao, Jiangying Zhou and Robert Deng. Android or iOS for Better Privacy Protection? In *Proceedings of the International Conference on Secure Knowledge Mangagement in Big-data era (SKM 2014)*, Dubai, United Arab Emirates, December 2014, invited paper.

Haoyu Ma, Kangjie Lu, Xinjie Ma, Haining Zhang, Chunfu Jia and Debin Gao. Software Watermarking using Return-Oriented Programming. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)*, Singapore, April 2015, to appear.

Conference Program Committee and Advisory Services

- Program committee member, the 6th Applied Cryptography and Network Security (ACNS 2008).
- Program committee member, the 11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008).
- Program committee member and session chair, the 11th Information Security Conference (ISC 2008).
- Program committee member, the 2009 IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2009).
- Program committee member, the 31st IEEE Symposium on Security and Privacy (Oakland 2010).
- Program committee member, the 4th IEEE International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2010).

- Program committee member, the 6th International Conference on Information Systems Security (ICISS 2010).
- Program committee member, the 32nd IEEE Symposium on Security and Privacy (Oakland 2011).
- Program committee member, the 7th Information Security Practice and Experience Conference (ISPEC 2011).
- Program committee member, the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2011).
- Program committee member, the 14th International Symposium on Recent Advances in Intrusion Detection (RAID 2011).
- Editorial board member, International Journal of Security and Networks (IJSN), 2011-2012.
- IT steering committee member, Singapore Management University, 2011-2012.
- Program committee member, the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2012).
- Program committee member, the 33nd IEEE Symposium on Security and Privacy (Oakland 2012).
- Program committee member, the 15th International Symposium on Recent Advances in Intrusion Detection (RAID 2012).
- Program committee member, the 3rd ACM Conference on Data and Application Security and Privacy (CODASPY 2013).
- Program committee member, the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013).
- Program committee member, the 9th Information Security Practice and Experience Conference (ISPEC 2013).
- Program committee member, the 34nd IEEE Symposium on Security and Privacy (Oakland 2013).
- Program committee member, the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2013).
- Program committee member, the 15th International Conference on Information and Communications Security (ICICS 2013).
- Program committee member, the 1st Learning from Authoritative Security Experiment Results workshop (LASER 2013).
- Program committee member, the 4th ACM Conference on Data and Application Security and Privacy (CODASPY 2014).

- Program committee member, the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014).
- Workshops chair, the 10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014).
- Program committee member, the 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2014).
- Program committee member, the 1st International Conference on Information Systems Security and Privacy (ICISSP 2015).
- Program committee member, the 5th ACM Conference on Data and Application Security and Privacy (CODASPY 2015).
- Program committee member, the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015).

Grants

- PI. Malware analyais, January 2009 – September 2011, SGD 720,000.
- PI. Return-Oriented Programming on mobile platforms, Dec 2013 – Dec 2014, SGD 200,000.
- PI. Advanced ROP execution and defenses on Android, Jan 2015 – Jan 2016, SGD 200,000.
- PI. Secure Mobile Center, Jan 2015 – Jan 2019, SGD 4,000,000.

Graduate Students

Jin Han	2007 – 2012	SMU PhD scholarship, $(ISC)^2$ information security scholarship
Payas Gupta	2008 – 2013	SMU PhD scholarship
Peng Li	2008 – 2014	PhD student at UNC at Chapel Hill, co-advise
Chee Meng Tey	2008 – 2013	DSO scholarship
Xiaoxiao Tang	2013 – now	SMU PhD scholarship

Grudate Student Attachments

Hyundo Park	2007 – 2008	PhD student from Korea University
Peng Li	2007 – 2008	Masters student from Wuhan University
Jie Lin	2008 – 2009	PhD student from Wuhan University
Limin Liu	2008 – 2009	PhD student from Chinese Academy of Science
Jiang Ming	2009 – 2011	PhD student from Peking University
Zhi Wang	2009 – 2010	PhD student from Nankai University
Kangjie Lu	2010 – 2011	PhD student from Peking University
Weijie Liu	2011 – 2012	Masters student from Nankai University
Lei Zhao	2011 – 2012	PhD student from Wuhan University
Nan Zong	2012 – 2013	Masters student from Nankai University
Haoyu Ma	2013 – 2014	PhD student from Nankai University
Xinjie Ma	2014 – 2015	Masters student from Nankai University
Yu Liang	2014 – 2015	PhD student from Wuhan University
Yan Lin	2014 – 2015	Masters student from Wuhan University