Debin GAO

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: dbgao@smu.edu.sg
Office Phone: (+65) 68280969

Education

PhD, Carnegie Mellon University, United States of America, 2006

Master of Science, Carnegie Mellon University, United States of America, 2004

Bachelor of Engineering, Nanyang Technological University, Singapore, 2001

Academic Appointments

Associate Professor of Computer Science, School of Computing and Information Systems, SMU, Apr 2021 - Present

Associate Professor of Information Systems, School of Computing and Information Systems, SMU, Jul 2015 - Mar 2021

Assistant Professor of Information Systems, School of Computing and Information Systems, SMU, Jul 2007 - Jun 2015

Academic Administrative Positions

Supervisor to SCIS UG Instructors, School of Computing and Information Systems, SMU, Jul 2020 - Present

Faculty Manager, SMU BSc (IS)-CMU Fast-Track Programme, School of Computing and Information Systems, SMU, Jul 2018 - Present

RESEARCH

Research Interests

Systems security, intrusion detection, mobile security, software security, human factors in computer security

Publications

Journal Articles [Refereed]

Active Warden Attack: On the (In)Effectiveness of Android App Repackage-Proofing, by MA, Haoyu; LI, Shijia; GAO, Debin; WU, Daoyuan; JIA, Qiaowen; JIA, Chunfu. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (5), 1-13. https://doi.org/10.1109/TDSC.2021.3100877 (Advance Online)

Secure Repackage-Proofing Framework for Android Apps Using Collatz Conjecture, by MA, Haoyu; LI, Shijia; GAO, Debin; JIA, Chunfu. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (5), 1-15. https://doi.org/10.1109/TDSC.2021.3091654 (Published)

On the Effectiveness of Using Graphics Interrupt as a Side Channel for User Behavior Snooping, by MA, Haoyu; TIAN, Jianwen; GAO, Debin; JIA, Chunfu. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (5), 1-14. https://doi.org/10.1109/TDSC.2021.3091159 (Advance Online)

Scalable online vetting of Android apps for measuring declared SDK versions and their consistency with API calls, by WU, Daoyuan; GAO, Debin; LO, David. (2021). *Empirical Software Engineering, 26* (1), https://doi.org/10.1007/s10664-020-09897-6 (Published)

Deep-Learning-Based App Sensitive Behavior Surveillance for Android Powered Cyber-Physical Systems, by MA, Haoyu; TIAN, Jianwen; QIU, Kefan; LO, David; GAO, Debin; WU, Daoyuan; JIA, Chunfu; BAKER, Thar. (2021). *IEEE Transactions on Industrial Informatics, 17* (8), 1-10. https://doi.org/10.1109/TII.2020.3038745 (Published)

AppMoD: Helping older adults manage mobile security with online social help, by WAN, Zhiyuan; BAO, Lingfeng; GAO, Debin; TOCH, Eran; XIA, Xin; MENDEL, Tamir; LO, David. (2019). *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3* (4), 154:1-22. https://doi.org/10.1145/3369819 (Published)

A novel covert channel detection method in cloud based on XSRM and improved event association algorithm, by WANG, Lina; LIU, Weijie; KUMAR, Neeraj; HE, Debiao; TAN, Cheng; GAO, Debin. (2016). *Security and Communication Networks, 9* (16), 3543-3557. http://doi.org/10.1002/sec.1560 (Published)

Integrated Software Fingerprinting via Neural-Network-Based Control Flow Obfuscation, by MA, Haoyu; LI, Ruiqi; YU, Xiaoxu; JIA, Chunfu; GAO, Debin. (2016). *IEEE Transactions on Information Forensics and Security, 11* (10), 2322-2337. http://doi.org/10.1109/TIFS.2016.2555287 (Published)

StopWatch: A Cloud Architecture for Timing Channel Mitigation, by LI, Peng; GAO, Debin; REITER, Michael K.. (2014). *ACM Transactions on Information and System Security, 17* (2), http://dx.doi.org/10.1145/2670940 (Published)

Beyond Output Voting: Detecting Compromised Replicas Using HMM-Based Behavioral Distance, by GAO, Debin; REITER, Michael K.; SONG, Dawn. (2009). *IEEE Transactions on Dependable and Secure Computing, 6* (2), 96-110. https://doi.org/10.1109/TDSC.2008.39 (Published)

FINDING THE SAME SOURCE PROGRAMS BASED ON THE STRUCTURAL FINGERPRINT DISTANCE OF CALL GRAPH, by YIN, Zhiyi; ZHU, Fuxi; FU, Jianming; GAO, Debin. (2009). *Neural Network World, 19* (6), 681-693. http://www.nnw.cz/obsahy09.html (Published)

Conference Proceedings

TypeSqueezer: When static recovery of function signatures for binary executables meets dynamic analysis, by LIN, Ziyi; LI, Jinku; LI, Bowen; MA, Haoyu; GAO, Debin; MA, Jianfeng. (2023.0). *The 30th ACM Conference on Computer and Communications Security (CCS 2023),* (pp. 2725-2739) Copenhagen, Denmark: (Published)

AutoDebloater: Automated android app debloating, by LIU, Jiakun; HU, Xing; THUNG, Ferdian; MAOZ, Shahar; TOCH, Eran; GAO, Debin; LO, David. (2023.0). *2023 38th IEEE/ACM International Conference on Automated Software Engineering, Kirchberg, Luxembourg, September 11-15: Proceedings,* (pp. 2090-2093) Piscataway, NJ: IEEE. https://doi.org/10.1109/ASE56229.2023.00017 (Published)

Sparsity brings vulnerabilities: Exploring new metrics in backdoor attacks, by TIAN, Jianwen; QIU, Kefan; GAO, Debin; WANG, Zhi; KUANG, Xiaohui; ZHAO, Gang. (2023.0). *Proceedings of the 32nd USENIX Security Symposium, Anaheim, United States, 2023 August 9-11,* (pp. 2689-2706) California: USENIX. (Published)

BinAlign: Alignment Padding Based Compiler Provenance Recovery, by ISMAIL, Maliha; LIN, Yan; HAN, DongGyun; GAO, Debin. (2023.0). *The 28th Australasian Conference on Information Security and Privacy (ACISP 2023),* (pp. 609-629) Brisbane, Australia: https://doi.org/10.1007/978-3-031-35486-1_26 (Published)

FA3: Fine-Grained Android Application Analysis, by LIN, Yan; WONG, Joshua; GAO, Debin. (2023.0). *HotMobile '23: Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications, Newport Beach, 22-23 February,* (pp. 74-80) New York: ACM.

https://doi.org/10.1145/3572864.3580338 (Published)

UIPDroid: Unrooted dynamic monitor of Android app UIs for fine-grained permission control, by DUAN, Mulin; JIANG, Lingxiao; SHAR, Lwin Khin; GAO, Debin. (2022.0). *Proceedings of the 44th International Conference on Software Engineering, Pittsburgh, USA, 2022 May 21-29,* (pp. 227-231) Pittsburgh: IEEE. http://doi.org/10.1109/ICSE-Companion55297.2022.9793833 (Published)

Chosen-instruction attack against commercial code virtualization obfuscators, by LI, Shijia; JIA, Chunfu; QIU, Pengda; CHEN, Qiyuan; MING, Jiang; GAO, Debin. (2022.0). *Proceedings of the 2022 Network and Distributed System Security Symposium, San Diego, California, April 24-28,* (pp. 1-17) San Diego, California: Internet Society. https://www.ndss-symposium.org/ndss-paper/auto-draft-210/ (Published)

ReSIL: Revivifying function signature inference using deep learning with domain-specific knowledge, by LIN, Yan; GAO, Debin; LO, David. (2022.0). *Proceedings of the 12th ACM Conference on Data and Application Security and Privacy, Baltimore, USA, 2022 April 24-27,* (pp. 107-118) Baltimore, USA: ACM. https://doi.org/10.1145/3508398.3511502 (Published)

On the usability (in)security of in-app browsing interfaces in mobile apps, by ZHANG, Zicheng; WU, Daoyuan; LI, Lixiang; GAO, Debin. (2021.0). *The 24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2021), Sebastian, Spain, October 6-8,* (pp. 386-398) San Sebastian, Spain: ACM. (Published)

An exploratory study of social support systems to help older adults in managing mobile safety, by MENDEL, Tamir; GAO, Debin; LO, David; TOCH, Eran. (2021.0). *The ACM International Conference on Mobile Human-Computer Interaction (Mobile HCI 2021),* Virtual: (Published)

When program analysis meets bytecode search: Targeted and efficient inter-procedural analysis of modern Android apps in BackDroid, by WU, Daoyuan; GAO, Debin; DENG, Robert H.; CHANG, Rocky. (2021.0). *Proceedings of the 51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021),* (pp. 543-554) Online: (Published)

When function signature recovery meets compiler optimization, by LIN, Yan; GAO, Devin. (2021.0). *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P 2021), 24-27 May,* (pp. 36-52) New Jersey, United States: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SP40001.2021.00006 (Published)

Walls have ears: Eavesdropping user behaviors via graphics-interrupt-based side channel, by MA, Haoyu; TIAN, Jianwen; GAO, Debin; JIA Chunfu. (2020.0). *the 23rd International Conference on Information Security (ISC 2020),* (pp. 178-195) Germany: Springer. https://doi.org/10.1007/978-3-030-62974-8_11 (Published)

SplitSecond: Flexible privilege separation of Android apps, by LEE, Jehyun; RAJA, Akshaya Venkateswara; GAO, Debin. (2019.0). *2019 17th International Conference on Privacy, Security and Trust (PST): August 26-28, Fredericton, Canada, Proceedings,* (pp. 1-10) Piscataway, NJ: IEEE. https://doi.org/10.1109/PST47121.2019.8949067 (Published)

Control-flow carrying code, by LIN, Yan; CHENG, Xiaoyang; GAO, Debin. (2019.0). *AsiaCCS '19: Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security, Auckland, July 9-12,* (pp. 3-14) New York: ACM. https://doi.org/10.1145/3321705.3329815 (Published)

Towards understanding Android system vulnerabilities: Techniques and insights, by WU, Daoyuan; GAO, Debin; CHENG, Eric K. T.; CAO, Yichen; JIANG, Jintao; DENG, Robert H.. (2019.0). *ASIACCS 2019: Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security, Auckland, July 7-12,* (pp. 295-306) New York: ACM. https://doi.org/10.1145/3321705.3329831 (Published)

DynOpVm: VM-based software obfuscation with dynamic opcode mapping, by CHENG, Xiaoyang; LIN, Yan; GAO, Debin. (2019.0). *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7: Proceedings,* (pp. 155-174) Bogota Colombia: Springer. https://doi.org/10.1007/978-3-030-21568-2_8 (Published)

An empirical study of mobile network behavior and application performance in the wild, by ZHANG, Shiwei; LI, Weichao; WU, Daoyuan; JIN, Bo; CHANG, Rocky K. C.; GAO, Debin; WANG, Yi; MOK, Ricky K. P.. (2019.0). *IWQoS '19: Proceedings of the International Symposium on Quality of Service, Phoenix, June 24-25,* (pp. 1-10) New York: ACM. https://doi.org/10.1145/3326285.3329039 (Published)

Understanding open ports in Android applications: Discovery, diagnosis, and security assessment, by WU,

Daoyuan; GAO, Debin; CHANG, Rocky K. C.; HE, En; CHENG, Eric K. T.; DENG, Robert H.. (2019.0). *Network and Distributed System Security Symposium 26th NDSS 2019: February 24-27, San Diego, CA: Proceedings,* (pp. 1-14) Reston, VA: Internet Society. https://doi.org/10.14722/ndss.2019.23171 (Published)

Towards mining comprehensive Android sandboxes, by LE, Tien-Duy B.; BAO, Lingfeng; LO, David; GAO, Debin; LI, Li. (2018.0). *ICECCS 2018: 23rd International Conference on Engineering of Complex Computer Systems: Proceedings : 12-14 December, Melbourne, Australia,* (pp. 51-60) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICECCS2018.2018.00014 (Published)

Towards dynamically monitoring Android applications on non-rooted devices in the wild, by TANG, Xiaoxiao; WU, Daoyuan; LIN, Yan; GAO, Debin. (2018.0). *WiSec '18: Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Stockholm, Sweden, June 18-20,* (pp. 212-223) New York: ACM. https://doi.org/10.1145/3212480.3212504 (Published)

SCLib: A practical and lightweight defense against component hijacking in Android applications, by WU, Daoyuan; CHENG, Yao; GAO, Debin; LI, Yingjiu; DENG, Robert H.. (2018.0). *CODASPY '18: Proceedings of 8th ACM Conference on Data and Application Security and Privacy, Tempe, AZ, March 19-21,* (pp. 299-306) New York: ACM. https://doi.org/10.1145/3176258.3176336 (Published)

On-demand time blurring to support side-channel defense, by LIU, Weijie; GAO, Debin; REITER, Michael K.. (2017.0). *Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017), Oslo, Norway, September 11-15, Part II,* Germany: Springer. http://doi.org/10.1007/978-3-319-66399-9_12 (Published)

On return oriented programming threats in Android runtime, by RAJA, Akshaya Venkateswara; LEE, Jehyun; GAO, Debin. (2017.0). *Proceedings of Privacy, Security, and Trust 2017 (PST 2017),* Calgary Canada: (Published)

MopEye: Opportunistic monitoring of per-app mobile network performance, by WU, Daoyuan; CHANG, Rocky K. C.; LI, Weichao; CHENG, Eric K. T.; GAO, Debin. (2017.0). *Proceedings of 2017 USENIX Annual Technical Conference, Santa Clara, July 12-14,* (pp. 445-458) Berkeley, CA: USENIX Association. (Published)

Measuring the declared SDK versions and their consistency with API calls in android apps, by WU, Daoyan; LIU, Ximing; XU, Jiayun; LO, David; GAO, Debin. (2017.0). *Wireless Algorithms, Systems, and Applications: Proceedings of the 12th International Conference, WASA 2017, Guilin, China, June 19-21,* (pp. 678-690) Cham: Springer. https://doi.org/10.1007/978-3-319-60033-8_58 (Published)

On the effectiveness of code-reuse-based Android application obfuscation, by TANG, Xiaoxiao; LIANG, Yu; MA, Xinjie; LIN, Yan; GAO, Debin. (2017.0). *Information Security and Cryptology: ICISC 2016: 19th International Conference, Seoul, November 30 - December 2: Revised selected papers,* (pp. 333-349) Cham: Springer. https://doi.org/10.1007/978-3-319-53177-9_18 (Published)

SafeStack+: Enhanced dual stack to combat data-flow hijacking, by LIN, Yan; TANG, Xiaoxiao; GAO, Debin. (2017.0). *Information security and privacy: 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, Proceedings,* (pp. 95-112) Cham: Springer. https://doi.org/10.1007/978-3-319-59870-3_6 (Published)

Control flow integrity enforcement with dynamic code optimization, by LIN, Yan; TANG, Xiaoxiao; GAO, Debin; FU, Jianming. (2016.0). *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, September 3-6, 2016: Proceedings,* (pp. 366-385) Cham: Springer. https://doi.org/10.1007/978-3-319-45871-7_22 (Published)

MobiPot: Understanding Mobile Telephony Threats with Honeycards, by BALDUZZI, Marco; GUPTA, Payas; GU, Lion; GAO, Debin; AHAMAD, Mustaque. (2016.0). *ASIA CCS '16: Proceedings of the 11th ACM Symposium on Information, Computer and Communications Security: Xi'an, China, May 30 - June 3, 2016,* (pp. 723-734) New York: ACM. http://dx.doi.org/10.1145/2897845.2897890 (Published)

MopEye: Monitoring per-app network performance with zero measurement traffic, by WU, Daoyuan; LI, Weichao; CHANG, Rocky K. C.; GAO, Debin. (2015.0). *CoNEXT Student Workshop 2015: Proceedings, Heidelberg, Germany, December 1,* (pp. 1-3) New York: ACM. (Published)

Stack layout randomization with minimal rewriting of Android binaries, by LIANG, Yu; MA, Xinjie; WU, Daoyuan; TANG, Xiaoxiao; GAO, Debin; PENG, Guojun; JIA, Chunfu; ZHANG, Huanguo. (2015.0). *Information Security and Cryptology: 18th International Conference ICISC 2015, Seoul, November 25-27: Proceedings,* (pp. 229-245) Cham: Springer. https://doi.org/10.1007/978-3-319-30840-1_15 (Published)

Replica Placement for Availability in the Worst Case, by LI, Peng; GAO, Debin; REITER, Mike. (2015.0). *2015 IEEE 35th International Conference on Distributed Computing Systems (ICDCS): June 29, 2015 - July 2, 2015, Columbus, OH, USA,* (pp. 599-608) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/ICDCS.2015.67 (Published)

Software Watermarking using Return-Oriented Programming, by MA, Haoyu; LU, Kangjie; MA, Xinjie; ZHANG, Haining; JIA, Chunfu; GAO, Debin. (2015.0). *ASIACCS'15: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security: April 14-17, 2015, Singapore,* (pp. 369-380) New York: ACM. http://dx.doi.org/10.1145/2714576.2714582 (Published)

Android or iOS for better privacy protection?, by HAN, Jin; YAN, Qiang; GAO, Debin; ZHOU, Jianying; DENG, Robert H.. (2014.0). *International Conference on Secure Knowledge Management in Big-data Era SKM 2014, Dubai, UAE, 8-9 December,* Dubai, UAE: BITS Pilani. (Published)

Control Flow Obfuscation using Neural Network to Fight Concolic Testing, by MA, Haoyu; MA, Xinjie; LIU, Weijie; Huang, Zhipeng; GAO, Debin; Jia, Chunfu. (2014.0). *International Conference on Security and Privacy in Communication Networks: 10th International ICST Conference, SecureComm 2014, Beijing, China, September 24-26, 2014, Revised Selected Papers, Part I,* (pp. 287-304) New York: Springer Verlag. http://dx.doi.org/10.1007/978-3-319-23829-6_21 (Published)

RopSteg: Program steganography with return oriented programming, by LU, Kangjie; XIONG, Siyang; GAO, Debin. (2014.0). *CODASPY '14: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy: March 3-5, San Antonio, TX,* (pp. 265-272) New York: ACM. https://doi.org/10.1145/2557547.2557572 (Published)

Keystroke biometrics: The user perspective, by TEY, Chee Meng; PAYAS, Gupta; MURALIDHARAN, Kartik; GAO, Debin. (2014.0). *CODASPY '14: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy: March 3-5, San Antonio, TX,* (pp. 289-296) New York: ACM. https://doi.org/10.1145/2557547.2557573 (Published)

Defending against heap overflow by using randomization in nested virtual clusters, by TEY, Chee Meng; GAO, Debin. (2013.0). *Information and Communications Security: 15th International Conference, ICICS 2013, Beijing, China, November 20-22: Proceedings,* (pp. 1-16) Beijing, China: Springer Verlag. http://dx.doi.org/10.1007/978-3-319-02726-5_1 (Published)

Launching generic attacks on iOS with approved third-party applications, by HAN, Jin; SU, Mon Kywe; YAN, Qiang; BAO, Feng; DENG, Robert H.; GAO, Debin; LI, Yingjiu; ZHOU, Jianying. (2013.0). *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28: Proceedings,* (pp. 272-289) Berlin: Springer. https://doi.org/10.1007/978-3-642-38980-1_17 (Published)

Keystroke Timing Analysis of on-the-fly Web Apps, by Tey, Chee Meng; GUPTA, Payas; GAO, Debin; ZHANG, YAN. (2013.0). *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings,* (pp. 405-413) Banff, Alberta, Canada: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-38980-1_25 (Published)

Mitigating Access-Driven Timing Channels in Clouds using StopWatch, by LI, Peng; GAO, Debin; Reiter, Michael K.. (2013.0). *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),* (pp. 1-12) Budapest, Hungary: IEEE. http://dx.doi.org/10.1109/DSN.2013.6575299 (Published)

Your Love is Public Now: Questioning the Use of Personal Information in Authentication, by GUPTA, Payas; GOTTIPATI, Swapna; JIANG, Jing; GAO, Debin. (2013.0). *ASIA CCS'13: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security: May 8-10, 2013, Hangzhou, China,* (pp. 49-60) New York: ACM. http://dx.doi.org/10.1145/2484313.2484319 (Published)

I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics, by TEY, Chee Meng; GUPTA, Payas; GAO, Debin. (2013.0). *Annual Network and Distributed System Security Symposium 20th NDSS 2013, 24-27 February,* San Diego, CA: http://www.internetsociety.org/doc/i-can-be-you-questioning-use-keystroke-dynamics-biometrics (Published)

Comparing Mobile Privacy Protection through Cross-Platform Applications, by HAN, Jin; YAN, QIANG; GAO, Debin; ZHOU, Jianying; DENG, Robert H.. (2013.0). *Proceedings of NDSS 2013: Network and Distributed System Security Symposium, 24-27 February, San Diego,* Reston, VA: Internet Society.

http://www.internetsociety.org/doc/comparing-mobile-privacy-protection-through-cross-platform-applications (Published)

iBinHunt: Binary Hunting with Inter-Procedural Control Flow, by MING, Jiang; PAN, Meng; GAO, Debin. (2013.0). *Information Security and Cryptology - ICISC 2012: 15th International Conference, Seoul, Korea, November 28-30, 2012: Revised Selected Papers,* (pp. 92-109) Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-37682-5_8 (Published)

OTO: Online Trust Oracle for User-Centric Trust Establishment, by KIM, Tiffany Hyun-Jin; GUPTA, Payas; Han, Jun; Owusu, Emmanuel; Hong, Jason; Perrig, Adrian; GAO, Debin. (2012.0). *CCS'12 : the proceedings of the 2012 ACM Conference on Computer and Communications Security : October 16-18, 2012, Raleigh, North Carolina, USA,* (pp. 391-403) New York: ACM. http://dx.doi.org/10.1145/2382196.2382239 (Published)

Learning Fine-Grained Structured Input for Memory Corruption Detection, by ZHAO, Lei; GAO, Debin; WANG, Lina. (2012.0). *Information security : 15th international conference, ISC 2012, Passau, Germany, September 19 - 21, 2012 ; proceedings,* Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-33383-5_10 (Published)

Active Malware Analysis using Stochastic Games, by WILLIAMSON, Simon; VARAKANTHAM, Pradeep; GAO, Debin; ONG, Chen Hui. (2012.0). *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012): Valencia, Spain, June 4-8,* (pp. 29-36) Richland, SC: IFAAMAS. http://dl.acm.org/citation.cfm?id=2343580 (Published)

Coercion Resistance in Authentication Responsibility Shifting, by GUPTA, Payas; DING, Xuhua; GAO, Debin. (2012.0). *ASIACCS '12: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security,* (pp. 97-98) New York, NY: ACM. http://dx.doi.org/10.1145/2414456.2414512 (Published)

HuMan: Creating memorable fingerprints of mobile users, by PAYAS, Gupta; TAN, Kiat Wee; RAMASUBBU, Narayanasamy; LO, David; GAO, Debin; BALAN, Rajesh Krishna. (2012.0). *2012 IEEE International Conference on Pervasive Computing and Communications Workshops: Lugano, Switzerland, 19-23 March: Proceedings,* (pp. 479-482) Piscataway, NJ: IEEE. https://doi.org/10.1109/PerComW.2012.6197540 (Published)

deRop: Removing Return-Oriented Programming from Malware, by LU, Kangjie; ZOU, Dabi; Weng, Weiping; GAO, Debin. (2011.0). *ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference: Orlando, FL, USA — December 05 - 09, 2011,* (pp. 363-372) New York, NY, USA: ACM. http://dx.doi.org/10.1145/2076732.2076784 (Published)

Launching Return-Oriented Programming Attacks against Randomized Relocatable Executables, by LIU, Limin; Han, JIN; GAO, Debin; Jing, Jiwu; ZHA, Daren. (2011.0). *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 : Changsha, China, 16 - 18 November 2011 ; conferences, symposiums and workshops,* (pp. 37-44) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/TrustCom.2011.9 (Published)

Packed, Printable, and Polymorphic Return-Oriented Programming, by LU, Kangjie; Zou, Dabi; Wen, Weiping; GAO, Debin. (2011.0). *Recent Advances in Intrusion Detection: 14th International Symposium, RAID 2011, Menlo Park, CA, USA, September 20-21, 2011. Proceedings,* (pp. 101-120) Menlo Park, CA: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-23644-0_6 (Published)

Linear Obfuscation to Combat Symbolic Execution, by WANG, Zhi; Ming, Jiang; Jia, Chunfu; GAO, Debin. (2011.0). *Computer Security - ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14: Proceedings,* (pp. 210-226) Berlin: Springer Verlag. http://flyer.sis.smu.edu.sg/esorics11.pdf (Published)

On detection of erratic arguments, by HAN, Jin; YAN, Qiang; DENG, Robert H.; GAO, Debin. (2011.0). *Security and Privacy in Communication Networks: 7th International ICST Conference, SecureComm 2011, London, UK, September 7-9, Revised Selected Papers,* (pp. 172-189) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-31909-9_10 (Published)

Towards ground truthing observations in gray-box anomaly detection, by MING, Jiang; ZHANG, Haibin; GAO, Debin. (2011.0). *2011 5th International Conference on Network and System Security (NSS): Milan, Italy, September 6-8: Proceedings,* (pp. 1-8) Piscataway, NJ: IEEE. https://doi.org/10.1109/ICNSS.2011.6059956 (Published)

Revisiting address space randomization, by WANG, Zhi; CHENG, Renquan; GAO, Debin. (2010.0). *Information Security and Cryptology ICISC 2010: 13th International Conference, Seoul, Korea, December 1-3, Revised Selected Papers,* (pp. 207-221) Berlin: Springer. https://doi.org/10.1007/978-3-642-24209-0_14 (Published)

A multi-user steganographic file system on untrusted shared storage, by HAN, Jin; PAN, Meng; GAO, Debin; PANG, Hwee Hwa. (2010.0). *ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference, Austin, Texas, December 6-10,* (pp. 317-326) New York: ACM. https://doi.org/10.1145/1920261.1920309 (Published)

On Challenges in Evaluating Malware Clustering, by LI, Peng; LIU, Limin; GAO, Debin; Reiter, Michael K. (2010.0). *Recent Advances in Intrusion Detection: 13th International Symposium, RAID 2010, Ottawa, Ontario, Canada, September 15-17, 2010: Proceedings,* (pp. 238-255) Berlin ; Heidelberg: Springer Verlag. http://doi.org/10.1007/978-3-642-15512-3_13 (Published)

Fighting Coercion Attacks in Key Generation using Skin Conductance, by GUPTA, Payas; GAO, Debin. (2010.0). *USENIX Security'10 Proceedings of the 19th USENIX conference on Security,* (pp. 30-30) Washington, DC, USA: USENIX Association Berkeley. (Published)

Denial-of-Service attacks on host-based generic unpackers, by LIU, Limin; MING, Jiang; WANG, Zhi; GAO, Debin; JIA, Chunfu. (2009.0). *Information and Communications Security: 11th International Conference, ICICS 2009, Beijing, China, December 14-17: Proceedings,* (pp. 241-253) Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-11145-7_19 (Published)

Automatically Adapting a Trained Anomaly Detector to Software Patches, by LI, Peng; GAO, Debin; Reiter, Michael K.. (2009.0). *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25: Proceedings,* (pp. 142-160) Saint-Malo, France: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-04342-0_8 (Published)

On the effectiveness of software diversity: A systematic study on real-world vulnerabilities, by HAN, Jin; GAO, Debin; DENG, Robert H.. (2009.0). *Detection of Intrusions and Malware, and Vulnerability Assessment: 6th International Conference, DIMVA 2009, Como, Italy, July 9-10: Proceedings,* (pp. 127-146) Berlin: Springer. https://doi.org/10.1007/978-3-642-02918-9_8 (Published)

Binhunt: Automatically Finding Semantic Differences in Binary Programs, by GAO, Debin; Reiter, Michael K.; SONG, Dawn. (2008.0). *Information and Communications Security: 10th International Conference, ICICS 2008 Birmingham, UK, October 20 - 22, 2008 Proceedings,* (pp. 238-255) Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-540-88625-9_16 (Published)

Bridging the Gap between Data-Flow and Control-Flow Analysis for Anomaly Detection, by LI, Peng; PARK, Hyundo; GAO, Debin; Fu, Jianming. (2008.0). *Twenty-Fourth Annual COMPUTER SECURITY APPLICATIONS Conference,* USA: IEEE. http://dx.doi.org/10.1109/ACSAC.2008.17 (Published)

Distinguishing between FE and DDoS using randomness check, by PARK, Hyundo; LI, Peng; GAO, Debin; LEE, Heejo; DENG, Robert H.. (2008.0). *Information security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, Proceedings,* (pp. 131-145) Berlin: Springer. https://doi.org/10.1007/978-3-540-85886-7_9 (Published)

Behavioral distance measurement using hidden Markov models, by GAO, Debin; Reiter, Michael K.; SONG, Dawn. (2006.0). *Recent Advances in Intrusion Detection: 9th International Symposium, RAID 2006 Hamburg, Germany, September 20-22, 2006 Proceedings,* (pp. 19-40) Hamburg, Germany: Springer Verlag. http://dx.doi.org/10.1007/11856214_2 (Published)

Behavioral distance for intrusion detection, by GAO, Debin; Reiter, Michael K.; SONG, Dawn. (2006.0). *8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005. Revised Papers,* (pp. 63-81) Seattle, WA, USA: Springer Verlag. http://dx.doi.org/10.1007/11663812_4 (Published)

Gray-Box Extraction of Execution Graphs for Anomaly Detection, by GAO, Debin; Reiter, Michael K.; SONG, Dawn. (2004.0). *CCS 2004: Proceedings of the 11th ACM Conference on Computer and Communications Security, October 25-29, 2004, Washington, DC,* (pp. 318-329) Washington, DC, USA: ACM. http://dx.doi.org/10.1145/1030083.1030126 (Published)

On Gray-Box Program Tracking for Anomaly Detection, by GAO, Debin; Reiter, Michael K.; SONG, Dawn. (2004.0). *SSYM'04 Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA,* (pp. 103-118) San Diego, CA, USA: USENIX Association. http://dl.acm.org/citation.cfm?id=1251383 (Published)

Research Grants

Singapore Management University

Less is More: Addressing Mobile Application Security and Privacy through Debloating, NCR-TAU Grant Call, Cyber Security Agency of Singapore (CSA) , PI (Project Level): David LO , Co-PI (Project Level): Debin GAO, 2022, S$599,568

National Satellite of Excellence in Mobile Systems Security and Cloud Security, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, PANG Hwee Hwa, DING XuHua, LI Yingjiu, 2019, S$7,498,320

Enhanced function signature recovery for control-flow integrity enforcement on compiler optimized executables, NSoE TSS Grant Call, National Satellite of Excellence - Trustworthy Software Systems , PI (Project Level): Debin GAO , Co-PI (Project Level): David LO, 2019, S$714,780

A system framework for reliable and dependable incident response on mobile devices, NSoE MSS-CS Research Programme, National Satellite of Excellence - Mobile Systems Security and Cloud Security , PI (Project Level): DING XuHua , Co-PI (Project Level): Debin GAO, 2019, S$1,201,607

Fine-grained Dynamic Analysis and Scalable Static Analysis for Android Applications, NSoE MSS-CS Research Programme, National Satellite of Excellence - Mobile Systems Security and Cloud Security , PI (Project Level): Debin GAO , Co-PI (Project Level): LI Yingjiu, 2019, S$1,070,201

AutoPrivacyModel: Automated Feature Modelling for Identifying Illegitimate Uses of Privacy-Sensitive Data in Mobile Applications, NSoE MSS-CS Research Programme, National Satellite of Excellence - Mobile Systems Security and Cloud Security , PI (Project Level): JIANG Lingxiao , Co-PI (Project Level): David LO, SHAR Lwin Khin, DING XuHua, Debin GAO, 2019, S$700,403

Intelligent and non-instrusive monitoring of Android devices for protection against data-infringing malware, AI Singapore 100 Experiments, AI Singapore , PI (Project Level): Debin GAO , Co-PI (Project Level): David LO, Robert H DENG, 2018, S$479,616

Safety and Privacy of Smart-City Mobile Applications through Model Inference, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): David LO , Co-PI (Project Level): Debin GAO, 2016, S$399,984

Advanced defense techniques for mobile systems and future networks, Huawei Technologies co. Ltd , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, DING XuHua, LI Yingjiu, 2015

Secure Mobile Centre - Technologies and Solutions for Securing Mobile Computing, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Programme Level): Robert H DENG , PI (Project Level): DING XuHua, Debin GAO, JIANG Lingxiao, LI Yingjiu, David LO, PANG Hwee Hwa, 2014, S$6,415,200

Analyzing and defending against ROP-embedded Mobile Applications Techniques, Huawei Technologies co. Ltd , PI (Project Level): Debin GAO, 2013, S$221,000

iBinHunt: Binary Hunting with Inter-Procedural Control Flow, Northeast Asia Grant Program, SafeNet Inc , PI (Project Level): Debin GAO, 2012, S$12,600

Malware Analysis, Ministry of Defence (MINDEF) , PI (Project Level): Debin GAO, S$720,000

A study of the usability of keystroke biometrics in exceptional conditions, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Debin GAO, 2013, S$13,846

User-Centric Mobile Authentication Mechanisms, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Rajesh Krishna BALAN, 2009, S$9,408

Other Institutions

IIE (MDGF) – Fine-Grained Analysis of Android Apps for In-Lab and Crowd-Sourcing Settings, MDGF, MOE Decentralised Gap Funding PI (Project Level): Debin GAO, 2023, SGD250,000

IIE (MDGF) – ANSTEROID, MDGF, MOE Decentralised Gap Funding PI (Project Level): Debin GAO, 2022, SGD50,000

TEACHING

Courses Taught

Singapore Management University

Undergraduate Programmes :

- Information Security and Trust
- Interconnection of Cyber Physical Systems
- Networking
- Software and Systems Security

Postgraduate Professional Programmes :

- Capstone Project - Cybersecurity
- Cybersecurity Technology and Applications

Postgraduate Research Programmes :

- Empirical Research Project 1
- Empirical Research Project 2
- Empirical Research Project 3
- Empirical Research Project 4
- Systems Security

THESES AND DISSERTATIONS

Theses and Dissertations Supervised

Singapore Management University

Supervisor, "A Study of the Imitation, Collection and Usability Issues of Keystroke Biometrics", Dissertation by TEY CHEE MENG, PhD in Information Systems, Singapore Management University, 2013

Supervisor, "Exploiting Human Factors in User Authentication", Dissertation by GUPTA PAYAS, PhD in Information Systems, Singapore Management University, 2013

Supervisor, "Novel Techniques of Using Diversity in Software Security and Information Hiding", Dissertation by HAN JIN, PhD in Information Systems, Singapore Management University, 2012

Theses and Dissertations Assessed

Singapore Management University

Committee Member, "Secure Enforcement Of Isolation Policy On Multicore Platforms With Virtualization Techniques", Dissertation by ZHAO SIQI, PhD in Information Systems, Singapore Management University, 2018

Committee Member, "Advanced Malware Detection for Android Platform", Dissertation by XU, KE, PhD in Information Systems, Singapore Management University, 2018

Committee Member, "Virtualization-Based System Hardening
Against Untrusted Kernels", Dissertation by CHENG YUEQIANG, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "Towards Secure and Usable Leakage-Resilient Password Entry", Dissertation by YAN QIANG, PhD in Information Systems, Singapore Management University, 2013

OTHER ACADEMIC AND PROFESSIONAL ACTIVITIES

Media Contributions and Citations

Remote gambling and technology, Channel 8 Singapore, 05 Jul 2018

Phishing website and emails, Channel 8 Singapore, 11 May 2018

Global ransomware attack, Berita Harian, 15 May 2017

Talking Point: Cybersecurity, Channel News Asia, 15 Feb 2017

Lower risks in digitizing data, Zaobao, 19 Jan 2017

Delinking Singapore government computers from the web, TBS eFM "PrimeTime", 01 Aug 2016

Delinking government computers from the web, Channel 8, 01 Jun 2016

Security research in SMU/SIS, Swiss National TV, 03 Jan 2013

SMU-Symantec MOU, Capital Radio 95.8FM, 01 Jan 2013

"Safer Internet Day", Channel News Asia, 02 Jan 2012

EXTERNAL SERVICE – PROFESSIONAL

Committee Chair, Program Committee, The 19th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2024), 2024 - Present

Committee Member, The 25th International Conference on Information and Communications Security (ICICS 2023), 2023 - Present

Committee Member, The 28th Australasian Conference on Information Security and Privacy (ACISP 2023), 2023 - Present

Committee Member, Program committee, The 17th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2022), 2022 - Present

Committee Member, Program committee, The 27th Australasian Conference on Information Security and Privacy (ACISP 2022), 2022 - Present

Committee Member, Program committee, The 12th ACM Conference on Data and Application Security and Privacy 2020 (CODASPY 2022), 2022 - Present

Committee Member, Program committee, The 20th International Conference on Applied Cryptography and Network Security (ACNS 2022), 2022 - Present

Member, Program committee, 21st International Conference on Applied Cryptography and Network Security (ACNS 2023), 2022 - Present

Member, Program Committee, The 27th European Symposium on Research in Computer Security (ESORICS 2022), 2022 - Present

Program committee, The 18th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2023), 2022 - Present

Committee Member, Program committee, The 24th International Conference on Information and Communications Security (ICICS 2022), 2022 - Present

Member, Program committee, The 13th ACM Conference on Data and Application Security and Privacy (CODASPY 2023), 2022 - Present

Committee Chair, Program Committee, The 23rd International Conference on Information and Communications Security (ICICS 2021), 2021 - Present

Member, Program Committee, The 26th European Symposium on Research in Computer Security (ESORICS 2021), 2021 - Present

Member, Program Committee, The 11th ACM Conference on Data and Application Security and Privacy 2020 (CODASPY 2021), 2021 - Present

Committee Member, Program Comittee, The 25th European Symposium on Research in Computer Security (ESORICS 2020), 2020 - Present

Member, Program Committee, The 16th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2020), 2020 - Present

Member, Program Committee, The 22nd International Conference on Information and Communications Security (ICICS 2020), 2020 - Present

Committee Member, Program Committee, The 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), 2019 - Present

Committee Member, Program Committee, Australasian Computer Science Week 2019 (ACSW 2019), 2019 - Present

Committee Member, Program committee, The 15th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2020), 2019 - Present

Committee Member, Program Committee, The 17th International Conference on Applied Cryptography and Network Security (ACNS 2019), 2019 - Present

Committee Member, Program Committee, Australasian Computer Science Week 2020 (ACSW 2020), 2019 - Present

Committee Member, Program Committee, The 14th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2019), 2019 - Present

Committee Member, Program Committee, The 9th ACM Conference on Data and Application Security and Privacy (CODASPY 2019), 2019 - Present

Committee Member, Program Committee, The 10th ACM Conference on Data and Application Security and Privacy 2020 (CODASPY 2020), 2019 - Present

Committee Member, Program Committee, 18th International Conference on Applied Cryptography and Network Security (ACNS 2020), 2019 - Present

Committee Member, Program Committee, The 21st International Conference on Information and Communications Security (ICICS 2019), 2019 - Present

Committee Member, Program Committee, European Symposium on Research in Computer Security 2019 (ESORICS 2019), 2019 - Present

Committee Member, Program Committee, 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019), 2019 - Present

Committee Member, Program Committee, International workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS 2019), 2019 - Present

Committee Member, Program Committee, 20th International Conference on Information and Communications Security (ICICS 2018), 2018 - Present

Member, Program committee, The International Conference on Information Systems Security and Privacy (ICISSP) 2018, 2018 - Present

Member, Program committee, 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2018), 2018 - Present

Committee Member, Program Committee, The 25th ACM Conference on Computer and Communications Security (CCS 2018), 2018 - Present

Committee Member, Program Committee, 23rd European Symposium on Research in Computer Security (ESORICS 2018), 2018 - Present

Committee Member, Program Committee, Australasian Computer Science Week 2018 (ACSW 2018), 2018 - Present

Committee Member, Program Committee, The 14th China International Conference on Information Security and Cryptology (Inscrypt 2018), 2018 - Present

Member, Program committee, The 8th ACM Conference on Data and Application Security and Privacy (CODASPY 2018), 2018 - Present

Member, Program committee, Australasian Computer Science Week (ASCW) 2018, 2018 - Present

Member, Program committee, The IEEE International Conference on Cloud Computing (CLOUD) 2018, 2018 - Present

Member, Program committee, ACM ASIA CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY (AsiaCCS) 2018, 2018 - Present

Member, Program committee, The 13th China International Conference on Information Security and Cryptology (INSCRYPT 2017), 2017 - Present

Member, Program committee, 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2017), 2017 - Present

Chairperson, Publicity committee, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, 2017 - Present

Member, Program committee, The 19th International Conference on Information and Communications Security (ICICS 2017), 2017 - Present

Member, Program committee, The 20th Information Security Conference (ISC 2017), 2017 - Present

Chairperson, Publicity Committee, The 11th ACM Symposium on Information, Computer and Scommunications Security (AsiaCCS 2016), 2016

Member, Program Committee, The 6th ACM Conference on Data and Application Security and Privacy (CODASPY 2016), 2016

Member, Program Committee, The 1st Singapore Cyber Security R&D Conference (SG-CRC 2016), 2016

EXTERNAL SERVICE – PUBLIC SECTOR AND COMMUNITY SERVICE

Member, Study team, Foundations of Security and Data Privacy FRC, 2021 - Present