Research Statement

Debin Gao
School of Computing and Information Systems, Singapore Management University
Tel: (+65) 6828-0969; Email: dbgao@smu.edu.sg
December 18 2025

Overview

As people rely more on computers (mobile and desktop), building and maintaining a secure computing environment becomes an important research topic. However, many computer programs remain vulnerable, and more advanced techniques for breaking into a computer or a network of computers have been discovered. Vulnerabilities may permit a malicious program (malware) to take full control of the victim machine and run the attacker's code. Automatically analyzing the vulnerabilities and malware as well as detecting such intrusions are critical in securing a computer system.

My research centers on analyzing and detecting malware and intrusions, with a recent focus on mobile platforms. The following points provide an overview of my research areas while Figure 1 shows a graphical view with the main publications in each (and intersection of) research area(s).

- Analyzing and detecting malware and intrusions: binary program analysis is a hard problem especially when we assume that source code is unavailable. Software obfuscation and new attacking techniques like Return-Oriented Programming make this difficult problem more challenging. My research centers on novel techniques to accurately perform such analysis and detection.
  - Binary difference analysis: a novel idea by focusing on (control-flow) graph similarity to detect polymorphism and metamorphism in malware, making the analysis technique resistant to software obfuscations. The idea also leverages software diversity, a well-known phenomenon in software engineering, to fight against evasion attacks.
  - Return-oriented program: analyzing the capability of this latest and most powerful attacking technology, defending against it, and even taking advantage of it for benign applications.
- Mobile security: tracing the latest mobile platform architectures (mostly Android) and the corresponding security and privacy they provide, with a focus on attack and defense techniques. My research uncovers new and zero-day attacks and proposes novel ways of defending against such attacks.
- Human factors in security and cloud security: a couple of focused areas of security closely related to human behavior (keystroke dynamics and coercion attacks) and cloud.

I consider these research areas closely related and interconnected. For example, intrusion detectors focus on mechanisms a defender could use to detect an intrusion to make it more difficult for malware to exploit, while malware analysis tries to understand what malicious programs do to better defend against them.

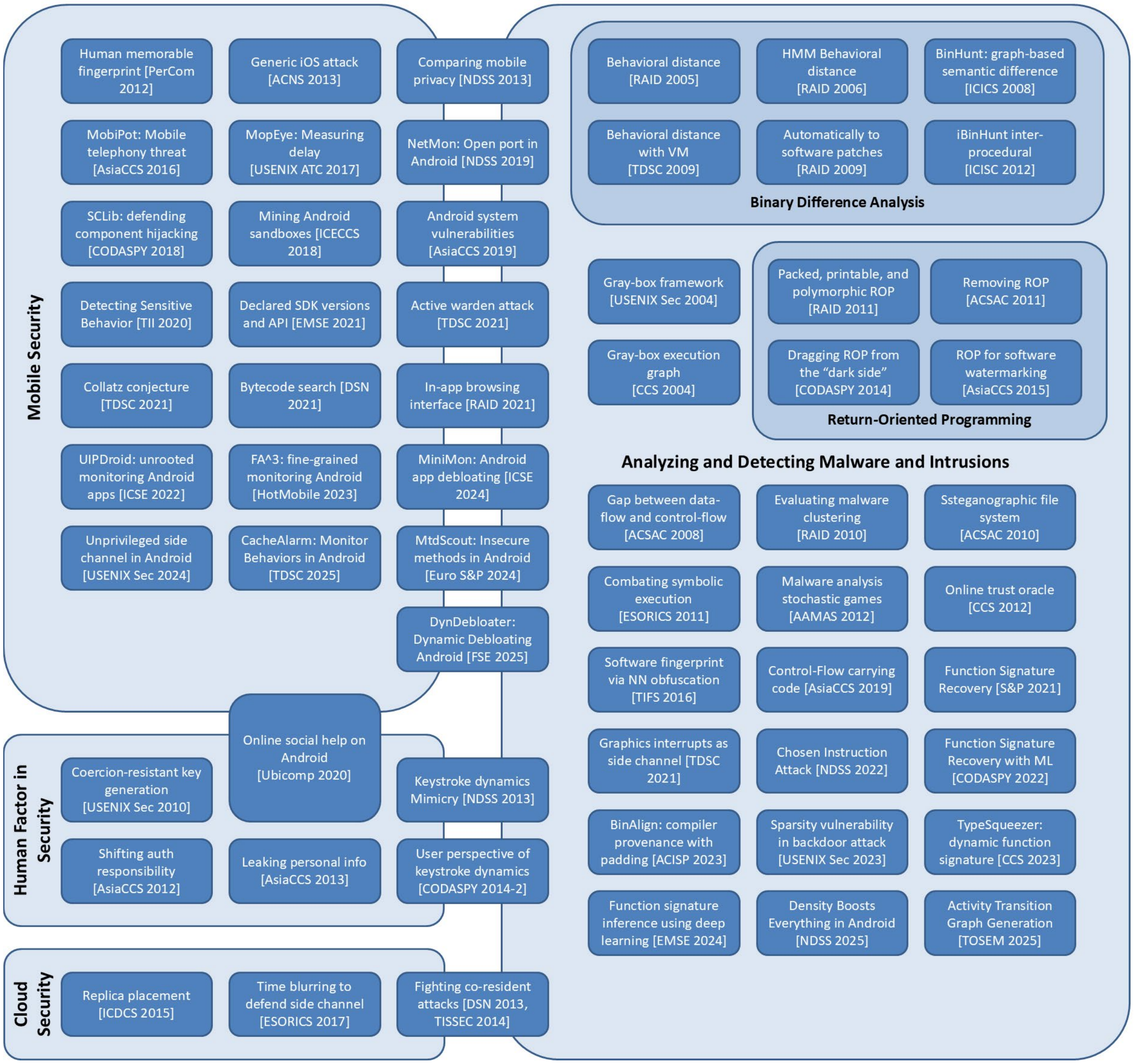

Figure 1: My research areas and selected publications

Specific Research Areas

Malware analysis and defense (my key research theme): Malware research is a big topic, and my research covers many sub-areas including control-flow hijacking, unpackers, symbolic execution, distributed denial of service attacks, randomization, etc. One interesting way of looking at my research in this big area is that I conduct my research from both the defenders’ and attackers’ perspectives.

On the defense side, I make notable contributions to the topic of Control-Flow Integrity, which is widely believed to be one of the most effective approaches to software security. The main idea is to strictly enforce a policy that any piece of software execution has to follow its intended control flow. To this end, we propose a few techniques to accurately extract the control-flow policy [S&P 2021, CODASPY 2022, CCS 2023, EMSE 2024] and to effectively enforce it [AsiaCCS 2019].

On the attack side, besides focusing on some of the latest attacking techniques like Return-Oriented Programming (more on this later), I look into software obfuscation techniques malware writers could employ to make analysis difficult [NDSS 2022], and graphics interrupts serving as side channels that leak sensitive information to potential process eavesdroppers [TDSC 2021].

There are also two specific areas where I contribute significantly to the analysis of malicious programs, namely binary diffing and Return-Oriented Programming.

Polymorphic and metamorphic malware are among the most difficult ones to analyze. We propose a novel binary difference analysis tool, BinHunt, to find semantic differences between binary executables. BinHunt bases its analysis on the control flow of the programs using a novel graph isomorphism technique, symbolic execution, and theorem proving, making it resistant to most obfuscation techniques used in malware polymorphism and metamorphism [ICICS 2008]. We further propose iBinHunt by analyzing inter-procedural control flow to combat obfuscations at the function level (e.g., function inlining) [ICISC 2012]. BinHunt and iBinHunt lay the groundwork for many subsequent binary diffing research and tools and are both highly cited.

Return-oriented Programming (ROP) is one of the latest and most powerful attacking techniques used by malware writers. My research touches on both its attacking capability and its defending mechanisms. On the attacking side, we analyze the capability of ROP, and find that it could be made packed, printable, and polymorphic [RAID 2011]. On the defense side, we propose an automatic system to remove ROP from any malicious program so that the large body of existing software analysis tools can be used to analyze ROP-based malware [ACSAC 2011].

Since its introduction, ROP has always been regarded as an attacking technique. We work on a number of projects to use ROP for security applications other than malicious attacks. For example, we propose a novel idea of using ROP for software obfuscation, which is the first step in dragging ROP away from the “dark side” to perform legitimate tasks [CODASPY 2014]. Following along the same direction, we also propose using ROP for software watermarking [AsiaCCS 2015].

Mobile security (my latest research development): My research into mobile security has substantial overlapping with that in malware analysis and defense. For example, we apply the binary differencing idea in malware analysis to analyze security and privacy models in Android and iOS [NDSS 2013, SKM 2014], and analyze a wide range of malicious behaviors in Android applications, including bytecode search [DSN 2021], open ports [NDSS 2019], re-packaging mechanisms [TDSC 2021-1, TDSC 2021-2], in-app browsing interfaces [RAID 2021], adversarial machine learning for Android malware detection [USENIX Security 2023, NDSS 2025], use of insecure methods [Euro S&P 2024], and activity transition graph [TOSEM 2025].

Besides these topics that are highly related to my research on malware analysis, I also make significant contribution to other mobile platform security research. More specifically, we focus on security implications of the Android OS architecture. For example, we analyze the consistency between declared SDK versions of Android applications and their actual API calling and show potential security flaws that could make Android applications exploitable [EMSE 2021]. We analyze inter-component communications among Android applications and propose a library-based solution to defend against component hijacking [CODASPY 2018]. We also systematically analyze vulnerabilities on the Android OS [AsiaCCS 2019]. Our latest analysis on the Android OS shows that an unprivileged side channel can be used to break the app sandboxing protection [USENIX Security 2024, TDSC 2025].

As one of the latest research efforts in mobile security, we recently investigated the possibility of monitoring Android application's execution on non-rooted devices used by the public. We modify the Android AOSP or utilize side channel information on Android OS while deploying our monitoring apps on Google Play to crowd source usage information from many real-world users [USENIX ATC 2018, NDSS 2019, IWQOS 2019, TII 2020, ICSE 2022, HotMobile 2023, ASE 2023]. Results have enabled us to perform accurate per-app networking measurement, to identify unknown open port vulnerabilities in many Android applications [NDSS 2019], and to debloat Android super apps to trim off unwanted functionalities [ICSE 2024, FSE 2025].

<u>Other areas I'm known for</u>: In my earlier career of security research, I focus on intrusion detection and propose a few novel techniques. We take a systematic view on host-based anomaly detection techniques and propose a unified framework [USENIX 2004]. This framework not only captures most existing host-based intrusion detectors but has become the framework under which new techniques are proposed. Execution graph [CCS 2004] is one of them and has a nice feature of conforming to the control-flow graph of the program (static) while being built from dynamic training. I'm one of the pioneers in proposing the use of software diversity for intrusion detection. We introduce a notion, behavioral distance, for evaluating the extent to which processes — potentially running different programs and executing on different platforms — behave similarly in response to a common input [RAID 2005]. This idea is further extended to improve its accuracy by using a customized Hidden-Markov Model [RAID 2006], and to improve efficiency by using virtual machines running on one physical computer [TDSC 2009].

I also work on a few interesting projects that are closely related to human factors in security. For example, we analyze how individual dynamic keystrokes could potentially be forged [NDSS 2013], altered [CODASPY 2014], and leaked out [ACNS 2014]. We also look into providing resistance to coercion attacks [USENIX 2010, AsiaCCS 2012].

Selected Publications

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

[CCS 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.

[RAID 2005] 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.

[RAID 2006] 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.

[ICICS 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.

[ACSAC 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.

[TDSC 2009] 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.

[RAID 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.

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

[RAID 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.

[ACSAC 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.

[RAID 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.

[ESORICS 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.

[ACSAC 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.

[PERCOM 2012] 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.

[AAMAS 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.

[CCS 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.

[ICISC 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.

[NDSS 2013-1] 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.

[NDSS 2013-2] 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.

[ASIACCS 2013] 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.

[DSN 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.

[ACNS 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), LNCS Vol. 7954, Springer*, Banff, Canada, June 2013.

[CODASPY 2014-1] 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, March 2014.

[CODASPY 2014-2] 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, March 2014.

[TISSEC 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.

[SKM 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.

[AsiaCCS 2015] 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.

[ICDCS 2015] Peng Li, Debin Gao and Mike Reiter. Replica Placement for Availability in the Worst Case. In *Proceedings of the 35th International Conference on Distributed Computing Systems (ICDCS 2015)*, Columbus, Ohio, USA, June 2015.

[CoNEXT 2015] Daoyuan Wu, Weichao Li, Rocky K. C. Chang and Debin Gao. “MopEye: Monitoring Per-app Network Performance with Zero Measurement Traffic”. In *Proceedings of the 11th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2015)*, Heidelberg, Germany, December 2015.

[TIFS 2016] Haoyu Ma, Ruiqi Li, Xiaoxu Yu, Chunfu Jia and Debin Gao. “Integrated Software Fingerprinting via Neural-Network-Based Control Flow Obfuscation”, In *IEEE Transactions on Information Forensics & Security (TIFS)*, Apr 2016.

[AsiaCCS 2016] Marco Balduzzi, Payas Gupta, Lion Gu, Debin Gao and Mustaque Ahamad. “MobiPot: Understanding Mobile Telephony Threats with Honeycards”. In *Proceedings of the 11th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2016)*, Xi'an, China, May 2016.

[USENIX ATC 2017] Daoyuan Wu, Rocky K. C. Chang, Weichao Li, Eric K. T. Cheng, and Debin Gao. “MopEye: Opportunistic Monitoring of Per-app Mobile Network Performance”. In *Proceedings of the 2017 USENIX Annual Technical Conference (USENIX ATC 2017)*, Santa Clara, California, USA, July 2017.

[ESORICS 2017] Weijie Liu, Debin Gao, and Michael K. Reiter. “On-Demand Time Blurring to Support Side-Channel Defense”. In *Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017)*, Oslo, Norway, September 2017.

[CODASPY 2018] Daoyuan Wu, Yao Cheng, Debin Gao, Yingjiu Li, and Robert H. Deng. “SCLib: A Practical and Lightweight Defense against Component Hijacking in Android Applications”. In *Proceedings of the 8th ACM Conference on Data and Application Security (CODASPY 2018)*. Tempe, AZ, USA. March 2018.

[ICECCS 2018] Tien-Duy B. Le, Lingfeng Bao, David Lo, Debin Gao, and Li Li. “Towards Mining Comprehensive Android Sandboxes”. In *Proceedings of the 23rd International Conference on Engineering of Complex Computer Systems (ICECCS 2018)*, Melbourne, Australia, December 2018.

[NDSS 2019] Daoyuan Wu, Debin Gao, Rocky K. C. Chang, En He, Eric K. T. Cheng, and Robert H. Deng. “Understanding Open Ports in Android Applications: Discovery, Diagnosis, and Security Assessment”. In *Proceedings of the 26th Annual Network & Distributed System Security Symposium (NDSS 2019*), San Diego, CA, USA, February 2019.

[IWQOS 2019] Shiwei Zhang, Weichao Li, Daoyuan Wu, Bo Jin, Rocky K. C. Chang, Debin Gao, Yi Wang, and Ricky K. P. Mok. "An Empirical Study of Mobile Network Behavior and Application Performance in the Wild". In *Proceedings of the IEEE/ACM International Symposium on Quality of Service (IWQOS 2019)*, Phoenix, AZ, USA, June 2019.

[AsiaCCS 2019-1] Daoyuan Wu, Debin Gao, Eric K. T. Cheng, Yichen Cao, Jintao Jiang, and Robert H. Deng. "Towards Understanding Android System Vulnerabilities: Techniques and Insights". In *Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2019)*, Auckland, New Zealand, July 2019.

[AsiaCCS 2019-2] Yan Lin, Xianyang Cheng, and Debin Gao. "Control-Flow Carrying Code". In *Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2019)*, Auckland, New Zealand, July 2019.

[UbiComp 2020] Zhiyuan Wan, Lingfeng Bao, Debin Gao, Eran Toch, Xin Xia, Tamir Mendel, and David Lo. "AppMoD: Helping Older Adults Manage Mobile Security with Online Social Help". In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (UbiComp 2020*, September 2020.

[TII 2020] Haoyu Ma, Jianwen Tian, Kefan Qiu, David Lo, Debin Gao, Daoyuan Wu, Chunfu Jia, and Thar Baker. "Deep-Learning-Based App Sensitive Behavior Surveillance for Android Powered Cyber-Physical Systems". In *Proceedings of IEEE Transactions on Industrial Informatics (TII 2020)*, November 2020.

[EMSE 2021] Daoyuan Wu, Debin Gao, and David Lo. "Scalable Online Vetting of Android Apps for Measuring Declared SDK Versions and Their Consistency with API Calls". In *Proceedings of Empirical Software Engineering (EMSE 2021)*, January 2021.

[S&P 2021] Yan Lin and Debin Gao. "When Function Signature Recovery Meets Compiler Optimization". In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P 2021)*, May 2021.

[DSN 2021] Daoyuan Wu, Debin Gao, Robert H. Deng, and Rocky K. C. Chang. "When Program Analysis Meets Bytecode Search: Targeted and Efficient Inter-procedural Analysis of Modern Android Apps in BackDroid". In *Proceedings of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021)*, Jun 2021.

[TDSC 2021-3] Haoyu Ma, Jianwen Tian, Debin Gao, and Chunfu Jia. "On the Effectiveness of Using Graphics Interrupt as a Side Channel for User Behavior Snooping". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, June 2021.

[TDSC 2021-2] Haoyu Ma, Shijia Li, Debin Gao, and Chunfu Jia. "Secure Repackage-Proofing Framework for Android Apps using Collatz Conjecture". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, June 2021.

[TDSC 2021-1] Haoyu Ma, Shijia Li, Debin Gao, Daoyuan Wu, Qiaowen Jia, and Chunfu Jia. "Active Warden Attack: On the (In)Effectiveness of Android App Repackage-Proofing". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, July 2021.

[RAID 2021] Zicheng Zhang, Daoyuan Wu, Lixiang Li, and Debin Gao. "On the Usability (In)Security of In-App Browsing Interfaces in Mobile Apps". In *Proceedings of the 24th*

International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2021), San Sebastian, Spain, October 2021.

[NDSS 2022] Shijia Li, Chunfu Jia, Pengda Qiu, Qiyuan Chen, Jiang Ming, and Debin Gao. “Chosen-Instruction Attack Against Commercial Code Virtualization Obfuscators”. In *Proceedings of the Network and Distributed System Security Symposium 2022 (NDSS 2022)*, San Diego, USA, April 2022.

[CODASPY 2022] Yan Lin, Debin Gao, and David Lo. “ReSIL: Revivifying Function Signature Inference using Deep Learning with Domain-Specific Knowledge”. In *Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (CODASPY 2022)*, Baltimore, USA, Apr 2022.

[ICSE 2022] Mulin Duan, Lingxiao Jiang, Lwin Khin Shar, and Debin Gao. “UIPDroid: Unrooted Dynamic Monitor of Android App UIs for Fine-Grained Permission Control”. In *Proceedings of the 44th International Conference on Software Engineering (ICSE 2022)*, Pittsburgh, USA, May 2022.

[HotMobile 2023] Yan Lin, Joshua Wong, and Debin Gao. “FA^3: Fine-Grained Android Application Analysis”. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications (HotMobile 2023)*, Orange County, USA, Feb 2023.

[ACISP 2023] Maliha Ismail, Yan Lin, DongGyun Han, and Debin Gao. “BinAlign: Alignment Padding Based Compiler Provenance Recovery”. In *Proceedings of the 28th Australasian Conference on Information Security and Privacy (ACISP 2023)*, Brisbane, Australia, Jul 2023.

[USENIX Security 2023] Jianwen Tian, Kefan Qiu, Debin Gao, Zhi Wang, Xiaohui Kuang, and Gang Zhao. “Sparsity Brings Vulnerabilities: Exploring New Metrics in Backdoor Attacks”. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 2023)*, Anaheim, USA, Aug 2023.

[ASE 2023] Jiakun Liu, Xing Hu, Ferdian Thung, Shahar Maoz, Eran Toch, Debin Gao, and David Lo. “AutoDebloater: Automated Android App Debloating”. In *Proceedings of the 38th IEEE/ACM International Conference on Automated Software Engineering (ASE 2023)*, Luxembourg, Sep 2023.

[CCS 2023] Ziyi Lin, Jinku Li, Bowen Li, Haoyu Ma, Debin Gao, and Jianfeng Ma. “TypeSqueezer: When Static Recovery of Function Signatures for Binary Executables Meets Dynamic Analysis”. In *Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS 2023)*, Copenhagen, Denmark, Nov 2023.

[ICSE 2024] Jiakun Liu, Zicheng Zhang, Xing Hu, Ferdian Thung, Shahar Maoz, Debin Gao, Eran Toch, Zhipeng Zhao, and David Lo. “MiniMon: Minimizing Android Applications with Intelligent Monitoring-Based Debloating”. In *Proceedings of the 46th International Conference on Software Engineering (ICSE 2024)*, Lisbon, Portugal, April 2024.

[EMSE 2024] Yan Lin, Trisha Singhal, Debin Gao, and David Lo. “Analyzing and Revivifying Function Signature Inference using Deep Learning”. In *Proceedings of Empirical Software Engineering (EMSE 2024)*, May 2024.

[Euro S&P 2024] Zicheng Zhang, Haoyu Ma, Daoyuan Wu, Debin Gao, Xiao Yi, Yufan Chen, Yan Wu, and Lingxiao Jiang. “MtdScout: Complementing the Identification of Insecure Methods in

Android Apps via Source-to-Bytecode Signature Generation and Tree-based Layered Search". In *Proceedings of the 9th IEEE European Symposium on Security and Privacy (Euro S&P 2024)*, Vienna, Austria, July 2024.

[USENIX Security 2024] Yan Lin, Joshua Wong, Xiang Li, Haoyu Ma, and Debin Gao. "Peep With A Mirror: Breaking The Integrity of Android App Sandboxing via Unprivileged Cache Side Channel". In *Proceedings of the 33rd USENIX Security Symposium (USENIX Security 2024)*, Philadelphia, USA, Aug 2024.

[NDSS 2025] Jianwen Tian, Wei Kong, Debin Gao, Tong Wang, Taotao Gu, Kefan Qiu, Zhi Wang, Xiaohui Kuang. "Density Boosts Everything: A One-stop Strategy for Improving Performance, Robustness, and Sustainability of Malware Detectors". In *Proceedings of the Network and Distributed System Security Symposium 2025 (NDSS 2025)*, San Diego, USA, Feb 2025.

[TDSC 2025] Jianwen Tian, Haoyu Ma, Debin Gao, Xiaohui Kuang. "CacheAlarm: Monitoring Sensitive Behaviors of Android Apps Using Cache Side Channel". In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Mar 2025.

[FSE 2025] Zicheng Zhang, Jiakun Liu, Ferdian Thung, Xing Hu, Wei Minn, Yan Naing Tun, Lwin Khin Shar, David Lo and Debin Gao. "DynDebloater: Dynamically Debloating Unwanted Features of Android Apps without APK Modification". In *Proceedings of the 33rd ACM International Conference on the Foundations of Software Engineering (FSE 2025)*, Trondheim, Norway, June 2025.

[TOSEM 2025] Jiakun Liu, Peixin Zhang, Han Hu, Yonghui Liu, Wei Minn, Ferdian Thung, Shahar Maoz, Eran Toch, Debin Gao, David Lo. "Activity Transition Graph Generation: How Far Are We?". In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, Dec 2025.