Research Statement

Debin Gao
School of Information Systems, Singapore Management University
Email: dbgao@smu.edu.sg; Tel: (65) 6828-0969
Last updated on Dec 25, 2023

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 an attacker to inject attack code and cause the vulnerable machine to run the attacker's program. Automatically detecting the intrusions and analyzing the vulnerabilities and malware are critical in securing a computer system.

My research centers on mobile security and malware analysis. The following points show an overview of my research areas while Figure 1 provides a graphical view with the main publications in each (and intersection of) research area(s).

- Malware analysis
  - 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
  - Binary difference analysis: a novel idea by focusing on (control-flow) graph similarity to detect polymorphism and metamorphism in malware
- Mobile security: tracing the latest mobile platform architectures and the corresponding security and privacy they provide, with focus on attacking and defense techniques
- 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
- Host-based intrusion detection
  - Gray-box systematic framework: a systematic framework that captures most existing technologies and allows exploring of new techniques
  - Using software diversity: a novel idea of using software diversity for security by making it next-to-impossible for attackers to compromise diverse systems at the same time

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.

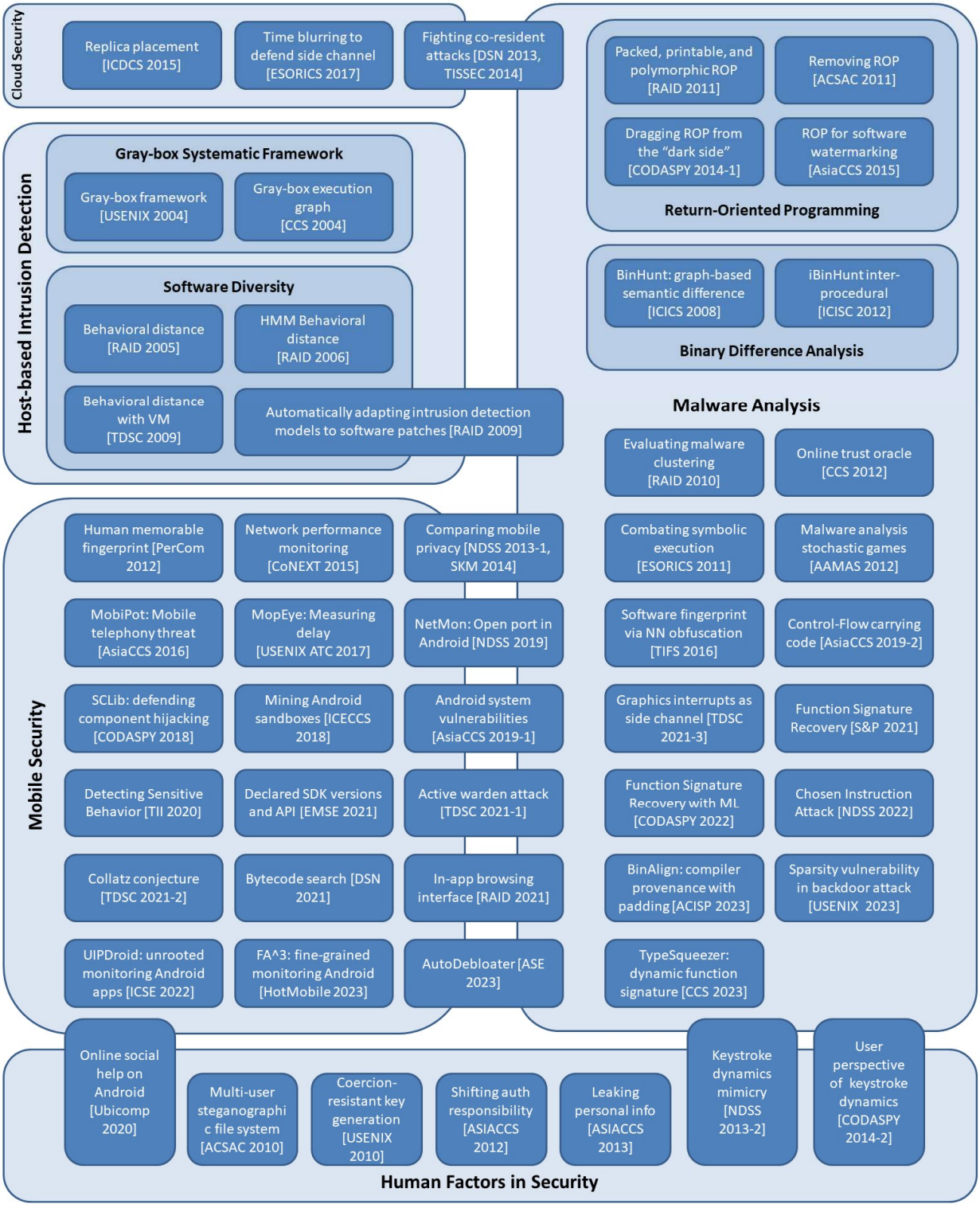

Figure 1: My research areas and selected publications

Intrusion detection: My contributions in the research of intrusion detection are mainly two-fold. First, 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.

Second, 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].

The idea of using software diversity for improving security does not stop in the area of intrusion detection. We apply a similar idea to perform binary difference analysis for analyzing polymorphic malware [ICICS 2008, ICISC 2012]. We further extend the idea of software diversity to mobile platform to perform a comparison of privacy protection mechanisms on Android and iOS [NDSS 2013-1, SKM 2014].

Malware analysis and defense: Malware research is a big topic, and my research covers many sub-areas including unpackers, symbolic execution, distributed denial of service attacks, randomization, etc. Among them, two notable contributions are on return-oriented programming (ROP) and binary difference analysis.

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]. BinHunt is further improved by analyzing inter-procedural control flow to combat function obfuscations [ICISC 2012].

Return-oriented Programming 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 2014-1]. Following along the same direction, we also propose using ROP for software watermarking [AsiaCCS 2015].

Besides the two themes of binary difference analysis and Return-Oriented Programming, we work on a variety of topics related to malware analysis and defense. Representative work include those for Control-Flow Integrity [AsiaCCS 2019-2, S&P 2021, CODASPYA 2022, CCS 2023], software obfuscations [TIFS 2016], graphics interrupts serving as side channels [TDSC 2021-3], and code virtualization obfuscations [NDSS 2022].

Mobile security: 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 2013-1, SKM 2014], and analyze a number of malicious behaviors in Android applications, including general bytecode search [DSN 2021], open ports [NDSS 2019], re-packaging mechanisms [TDSC 2021-1, TDSC 2021-2], and in-app browsing interfaces [RAID 2021].

Besides these topics that are highly related to my malware analysis research on desktop environment, we 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 application 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 2019-1].

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 general 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 as well as identifying unknown open port vulnerabilities in many Android applications.

Research Strategies

Cross-area solution to research problems: With appropriate customization and modification, some technique initially proposed in one area might be useful in another, sometimes even providing surprisingly significant benefits. My first success of doing this was when designing host-based intrusion detection systems, in which we apply the concept of human immune system of which the main mechanism is to distinguish self cells (cells of the human body) from non-self cells (dangerous foreign cells). Inspired by the human immune system, we design host-based intrusion detection systems as an anomaly detector to distinguish system calls generated normally (not under attack) and system calls generated abnormally (under intrusion) [USENIX 2004, CCS 2004].

My next successful applications of this concept were in proposing a solution to behavioral distance [RAID 2005, RAID 2006], where the two solutions we propose were originating from evolutionary distance, a technique initially proposed in biology to process DNA sequences, and Hidden Markov Model, a mathematical model widely used in speech recognition. Again, these (modified and customized) techniques work surprisingly well in a difficult problem in computer security in comparing system call sequences generated from different operating systems.

A successful application of this strategy typically requires one to think "out-of-the-box" and careful customization and modification to existing techniques. Having benefited from this research strategy, I continue applying it in other difficult problems. For example,

- DDoS attacks: we use a customized randomness check test suite initially designed to test random and pseudorandom number generators to distinguish flash events and distributed denial of service attacks [ISC 2008];
- Binary analysis: we use a modified version of the Collatz conjecture (an unsolved mathematical conjecture) to combat symbolic execution [ESORICS 2011] and Android application re-packaging [TDSC 2021-2];
- Malware analysis: we use stochastic gaming theories to actively analyze malware [AAMAS 2012];
- Control-Flow Integrity: we investigate the usage of a relatively old idea of dynamic code optimization to improve the efficiency of the recently proposed security mechanism of enforcing Control Flow Integrity, and obtain some encouraging results [ISC 2016];
- Telephony scamming: we apply the idea of HoneyPot to automatic gathering of telephony scamming activities [AsiaCCS 2016].

Human factors: Human is usually the weakest link in evaluating the security of a system. In view of this, there have been significantly more and more exploits in recent years targeting this weakest link, e.g., phishing attacks. I believe that research involving human factors will receive more attention in the near future.

One important and interesting topic I work on is keystroke dynamics as an authentication method. Through a large-scale user study, we show that a person could imitate another by incremental adjustment of typing patterns [NDSS 2013-2]. We demonstrate that keystroke dynamics is not a good authentication method for many people. The paper was praised for a well-designed user study and careful analysis of results, and received the best paper award of NDSS 2013. We subsequently show that personal keystroke dynamic information could leak in everyday browsing activities [ACNS 2013-2], and some practical limitations in using keystroke dynamics [CODASPY 2014-2].

Another interesting project about human factors is on coercion attacks and coercion resistant techniques. Most existing key generation and authentication mechanisms are vulnerable to coercion attacks in which a person is forcefully asked to reveal or generate the key to gain access to a system or to decrypt a file. It is a very hard problem by itself, and one can imagine it is even harder to conduct user studies involving coercions without “crossing the line”. We are the first to propose and evaluate (through a user study) a coercion resistant key generation algorithm [USENIX 2010] using skin conductance. We further extend our technique in more general settings of authentication responsibility shifting by using coercion resistant techniques [ASIACCS 2012].

“Crazy” ideas: Calling these ideas crazy might be an exaggerated claim, but I make myself ready in working on very hard problems, in trying out ideas that are controversy, and am willing to make multiple attempts in promoting the idea before acceptance.

The project on coercion attacks is one example of hard problems. It is a hard problem because a coercion resistant system needs to remove the capability of generating the correct key from the legitimate user when he/she is coerced. We also had relatively low confidence in the successfulness of using skin conductance to detect coercion before carrying out the user study. Nevertheless, as a researcher, I think one should accept such uncertainty and be ready to try new and “crazy” things out. Results turned out to be good and our paper is accepted by one of the best security conferences [USENIX 2010].

We also work on a controversy idea of dragging return-oriented programming (ROP) from the "dark side" and use it for legitimate purposes or even to improve security of a system. ROP has always been regarded as an attacking technique since its introduction. It interprets machine instructions at an unintended offset to obtain unintended instructions to be executed. We argue that a software developer could intentionally transform the execution of part of the program to ROP execution for obfuscation purposes or even to make the program more difficult to exploit. Although we demonstrate our idea with an automatic tool to embed ROP into an executable and the applications of the tool on a number of programs, responses from reviewers were quite controversy in that some find it innovative and novel while others consider it impractical. It took three major revisions and resubmissions before it was finally accepted [CODASPY 2014-1]. Again, I find the risk worth taking and the process fun and enjoyable. The good news is that this idea is receiving more positive feedback after our first publication. For example, our follow-up work on using ROP for software watermarking was recently accepted by AsiaCCS 2015 [AsiaCCS 2015].

Selected publications

[USENIX 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.

[ISC 2008] 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.

[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.

[DIMVA 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.

[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.

[ICICS 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.

[USENIX 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.

[ICISC 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.

[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.

[SecureComm 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.

[NSS 2011] 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.

[TrustCom 2011] Limin Liu, Jin Han, Debin Gao, Jiwu Jing, and Daren Zha, “Launching Return-Oriented Programming Attacks against Randomized Relocatable Executables”, In *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011)*, Changsha, China, November 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.

[ISC 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.

[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 2013-1] 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.

[ACNS 2013-2] 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.

[ICICS 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.

[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.

[SecureComm 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.

[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.

[ICISC 2015] Yu Liang, Xinjie Ma, Daoyuan Wu, Xiaoxiao Tang, Debin Gao, Guojun Peng, Chunfu Jia and Huanguo Zhang. “Stack Layout Randomization with Minimal Rewriting of Android

Binaries". In *Proceedings of the 18th annual International Conference on Information Security and Cryptology (ICISC 2015)*, Seoul, Korea, November 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.

[ISC 2016] Yan Lin, Xiaoxiao Tang, Debin Gao and Jianming Fu. "Control Flow Integrity Enforcement with Dynamic Code Optimization". In *Proceedings of the 19th Information Security Conference (ISC 2016)*, Honolulu, USA, September 2016.

[SCN 2016] Lina Wang, Weijie Liu, Neeraj Kumar, Debiao He, Cheng Tan, and Debin Gao. "A novel covert channel detection method in cloud based on XSRM and improved event association algorithm". In *Security and Communication Networks*, October 2016.

[ICISC 2016] Xiaoxiao Tang, Yu Liang, Xinjie Ma, Yan Lin, and Debin Gao. "On the effectiveness of code-reuse-based Android application obfuscation". In *Proceedings of the 19th Annual International Conference on Information Security and Cryptology (ICISC 2016)*, Seoul, Korea, December 2016.

[WASA 2017] Daoyuan Wu, Ximing Liu, Jiayun Xu, David Lo, and Debin Gao. "Measuring the Declared SDK Versions and Their Consistency with API Calls in Android Apps". In *Proceedings of the 12th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2017)*, Guilin, China, June 2017.

[ACISP 2017] Yan Lin, Xiaoxiao Tang, and Debin Gao. "SafeStack+: Enhanced Dual Stack to Combat Data-Flow Hijacking". In *Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP 2017)*, Auckland, New Zealand, July 2017.

[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.

[PST 2017] Akshaya Venkateswara Raja, Jehyun Lee and Debin Gao. "On Return Oriented Programming Threats in Android Runtime". In *Proceedings of Privacy, Security, and Trust 2017 (PST 2017)*, Calgary, Canada, August 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.

[WiSec 2018] Xiaoxiao Tang, Yan Lin, Daoyuan Wu, and Debin Gao. “Towards Dynamically Monitoring Android Applications on Non-rooted Devices in the Wild”. In *Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2018)*, Stockholm, Sweden, June 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.

[ACNS 2019] Xiaoyang Cheng, Yan Lin, Debin Gao, and Chunfu Jia. “DynOpVm: VM-based Software Obfuscation with Dynamic Opcode Mapping”. In Proceedings of the *17th International Conference on Applied Cryptography and Network Security (ACNS 2019)*, Bogota, Colombia, June 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.

[PST 2019] Jehyun Lee, Akshaya Venkateswara Raja, and Debin Gao. “SplitSecond: Flexible Privilege Separation of Android Apps”. In *Proceedings of the 17th International Conference on Privacy, Security and Trust (PST 2019)*, Fredericton, NB, Canada, August 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.

[ISC 2020] Haoyu Ma, Jianwen Tian, Debin Gao, and Chunfu Jia. “Walls Have Ears: Eavesdropping User Behaviors via Graphics-Interrupt-Based Side Channel”. In *Proceedings of the 23rd International Conference on Information Security (ISC 2020)*, November 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.

[Mobile HCI 2021] Tamir Mendel, Debin Gao, David Lo, and Eran Toch. “An Exploratory Study of Social Support Systems to Help Older Adults in Managing Mobile Safety”. In *Proceedings of the ACM International Conference on Mobile Human-Computer Interaction (Mobile HCI 2021)*, September 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 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.