

BYOUNGYOUNG LEE (이병영)

Associate Professor
Department of Electrical and Computer Engineering (ECE)
Seoul National University (SNU)
Email: byoungyoung@snu.ac.kr
Homepage: <https://lifeasageek.github.io>
Lab: [CompSec at SNU](#)

RESEARCH INTERESTS

Interested in **security and privacy problems** in general. In particular, my research focus is in **systems security**, e.g., building confidential computing systems or mitigating security vulnerabilities in production systems.

EDUCATION

- **Ph.D. in Computer Science, Georgia Institute of Technology**, Atlanta, GA, USA (Aug 2016)
Thesis: Protecting Computer Systems through Eliminating or Analyzing Vulnerabilities
Advisors: Prof. Wenke Lee and Prof. Taesoo Kim
- **M.S. in Computer Science and Engineering, POSTECH**, Pohang, South Korea (May 2011)
Thesis: Protecting Location Privacy Using Location Semantics
Advisor: Prof. Jong Kim
- **B.S. in Computer Science and Engineering, POSTECH**, Pohang, South Korea (May 2009)

PROFESSIONAL EXPERIENCE

- **Seoul National University (SNU)**, Seoul, South Korea (Sep 2018 - Current)
Assistant/Associate Professor, Department of Electrical and Computer Engineering
- **EPFL**, Lausanne, Switzerland (Apr 2022 – May 2022)
Visiting Researcher, collaborated with Prof. Mathis Payer
- **Purdue University**, West Lafayette (Aug 2016 – Aug 2018)
Assistant Professor, Department of Computer Science
- **Google, Chrome Security Team**, Mountain View, CA (May 2014 – Aug 2014)
Software Engineering Intern: worked on detecting runtime bad-casting
Mentor: Abhishek Arya
- **Microsoft Research Redmond (MSR)**, Redmond, WA (May 2012 – Aug 2012)
Research Intern: worked on mapping dynamic data for user-mode crash dump analysis
Mentors: Marcus Peinado and Weidong Cui
- **Georgia Institute of Technology**, Atlanta, GA (Aug 2011 – Aug 2016)
Research Assistant

HONORS AND AWARDS

- Ministerial citation for excellent researcher, Minister of Science and ICT (대한민국 과학기술부 장관 우수연구자 표창), 2020
- Google ASPIRE Award (\$30,000 award), 2019
- **Internet Defense Prize** by Facebook and USENIX (\$100,000 award), 2015
- Qualified for **DARPA Cyber Grand Challenge** (Team Disekt, \$750,000 award), 2015
- Third place award by **CSAW** Best Applied Research Paper Award, 2015
- Vulnerability Bounty Award by Firefox, Mozilla (\$3,000 award), 2014
- Vulnerability Bounty Award by Firefox, Mozilla (\$3,000 award), 2013

- Vulnerability Bounty Award by Chrome, Google (\$3,000 award), 2013
- The 8th place at DEFCON 19 CTF (Team PLUS@POSTECH), Las Vegas, USA, Aug. 2011
- The 3rd place at DEFCON 17 CTF (Team PLUS@POSTECH), Las Vegas, USA, Aug. 2009
- The 6th place at DEFCON 14 CTF (Team TheEastSea), Las Vegas, USA, Aug. 2006
- ‘Supreme Award’ at Wowhacker Hacking Festival, Seoul, Korea, Jun. 2007
- ‘Special Prize’ at KISA Hacking Defense Competition, Seoul, Korea, Mar. 2006
- POSTECH Undergraduate Research Program Scholarship, 2005
- Full undergraduate study scholarship, Korea Science and Engineering Foundation (KOSEF), 2003

PUBLICATION (CONFERENCE PAPERS)

1. **Metamong: Detecting Render-update Bugs in Web Browsers through Fuzzing**
Suhwan Song, and Byoungyoung Lee
ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (FSE) 2023
2. **An Extensible Orchestration and Protection Framework for Confidential Cloud Computing**
Adil Ahmad, Alex Schultz, Byoungyoung Lee, and Pedro Fonseca
USENIX Symposium on Operating Systems Design and Implementation (OSDI) 2023
3. **SEGFUZZ: Segmentizing Thread Interleaving to Discover Kernel Concurrency Bugs through Fuzzing**
Dae R. Jeong, Byoungyoung Lee, Insik Shin, and Youngjin Kwon
IEEE Symposium on Security and Privacy (SP) 2023
4. **GRAMINER: Fuzz Testing Gramine LibOS to Harden the Trusted Computing Base**
Jaewon Hur, and Byoungyoung Lee
Workshop on System Software for Trusted Execution (SysTEX) 2023
5. **Extending a Hand to Attackers: Browser Privilege Escalation Attacks via Extensions**
Young Min Kim, and Byoungyoung Lee
USENIX Security Symposium (Security) 2023
6. **Pspray: Timing Side-Channel based Linux Kernel Heap Exploitation Technique**
Yoochan Lee, Jinhan Kwak, Junesoo Kang, Yuseok Jeon, and Byoungyoung Lee
USENIX Security Symposium (Security) 2023
7. **Diagnosing Kernel Concurrency Failures with AITIA**
Dae R. Jeong, Minkyu Jung, Yoochan Lee, Byoungyoung Lee, Insik Shin, and Youngjin Kwon
ACM EuroSys Conference (EuroSys) 2023
8. **Perfect Spray: A Journey From Finding a New Type of Logical Flaw at Linux Kernel To Developing a New Heap Exploitation Technique**
Yoochan Lee, Byoungyoung Lee, Yuseok Jeon, Jinhan Kwak, and Junesoo Kang
BlackHat Europe 2022
9. **SpecDoctor: Differential Fuzz Testing to Find Transient Execution Vulnerabilities**
Jaewon Hur, Suhwan Song, Sunwoo Kim, and Byoungyoung Lee
ACM Conference on Computer and Communications Security (CCS) 2022
10. **FuzzOrigin: Detecting UXSS vulnerabilities in Browsers through Origin Fuzzing**
Sunwoo Kim, Young Min Kim, Jaewon Hur, Suhwan Song, Gwangmu Lee, and Byoungyoung Lee
USENIX Security Symposium (Security) 2022
11. **SYMSAN: Time and Space Efficient Concolic Execution via Dynamic Data-flow Analysis**
Ju Chen, Wookhyun Han, Mingjun Yin, Haochen Zeng, Yuxuan Chen, Chengyu Song, Byoungyoung Lee, Heng Yin, and Insik Shin
USENIX Security Symposium (Security) 2022

12. **MundoFuzz: Hypervisor Fuzzing with Statistical Coverage Testing and Grammar Inference**
Cheolwoo Myung, Gwangmu Lee, and Byoungyoung Lee
USENIX Security Symposium (Security) 2022
13. **R2Z2: Detecting Rendering Regressions in Web Browsers through Differential Fuzz Testing**
Suhwan Song, Jaewon Hur, Sunwoo Kim, Philip Rogers, and Byoungyoung Lee
IEEE/ACM International Conference on Software Engineering (ICSE) 2022
14. **FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks**
Kyungtae Kim, Taegy Kim, Ertza Warraich, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian
IEEE Symposium on Security and Privacy (SP) 2022
15. **DiFuzzRTL: Differential Fuzz Testing to Find CPU Bugs**
Jaewon Hur, Suhwan Song, Dongup Kwon, Eunjin Baek, Jangwoo Kim, and Byoungyoung Lee
IEEE Symposium on Security and Privacy (SP) 2021
16. **ExpRace: Exploiting Kernel Races through Raising Interrupts**
Yoochan Lee, Changwoo Min, and Byoungyoung Lee
USENIX Security Symposium (Security) 2021
17. **Constraint-guided Directed Greybox Fuzzing**
Gwangmu Lee, Woochul Shim, and Byoungyoung Lee
USENIX Security Symposium (Security) 2021
18. **M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles**
Arslan Khan, Hyungsub Kim, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, and Dave Tian
USENIX Security Symposium (Security) 2021
19. **KARD: Lightweight Data Race Detection with Per-Thread Memory Protection**
Adil Ahmad, Sangho Lee, Pedro Fonseca, and Byoungyoung Lee
International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2021
20. **Chancel: Efficient Multi-client Isolation Under Adversarial Programs**
Adil Ahmad, Juhee Kim, Jaebaek Seo, Insik Shin, Pedro Fonseca, and Byoungyoung Lee
Network and Distributed System Security Symposium (NDSS) 2021
21. **BlackMirror: Preventing Wallhacks in 3D Online FPS Games**
Seonghyun Park, Adil Ahmad, and Byoungyoung Lee
ACM Conference on Computer and Communications Security (CCS) 2020
22. **TRUSTORE: Side-Channel Resistant Storage for SGX using Intel Hybrid CPU-FPGA**
Hyunyoung Oh, Adil Ahmad, Seonghyun Park, Byoungyoung Lee, and Yunheung Paek
ACM Conference on Computer and Communications Security (CCS) 2020
23. **Vessels: Efficient and Scalable Deep Learning Prediction on Trusted Processors**
Kyungtae Kim, Chung Hwan Kim, Junghwan Rhee, Xiao Yu, Haifeng Chen, Dave Tian, and Byoungyoung Lee
ACM Symposium on Cloud Computing (SoCC) 2020
24. **A Tale of Two Trees: One Writes, and Other Reads. Optimized Oblivious Accesses to Large-Scale Blockchains**
Duc V. Le, Lizzy Tengana Hurtado, Adil Ahmad, Mohsen Minaei, Byoungyoung Lee, and Aniket Kate
Privacy Enhancing Technologies Symposium (PETS) 2020
25. **CrFuzz: Fuzzing Multi-purpose Programs through Input Validation**
Suhwan Song, Chengyu Song, Yeongjin Jang, and Byoungyoung Lee
ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (FSE) 2020

26. **Exploiting Kernel Races through Taming Thread Interleaving**
Yoochan Lee, Changwoo Min, and Byoungyoung Lee
BlackHat USA 2020
27. **HFL: Hybrid Fuzzing on the Linux Kernel**
Kyungtae Kim, Dae R. Jeong, Chung Hwan Kim, Yeongjin Jang, Insik Shin, and Byoungyoung Lee
Network and Distributed System Security Symposium (NDSS) 2020
28. **uXOM: Efficient eXecute-Only Memory on ARM Cortex-M**
Donghyun Kwon, Jangseop Shin, Giyeol Kim, Byoungyoung Lee, Yeongpil Cho, and Yunheung Paek
USENIX Security Symposium (Security) 2019
29. **All Your Clicks Belong to Me: Investigating Click Interception on the Web**
Mingxue Zhang, Wei Meng, Sangho Lee, Byoungyoung Lee, and Xinyu Xing
USENIX Security Symposium (Security) 2019
30. **Razzor: Finding Kernel Race Bugs through Fuzzing**
Dae R. Jeong, Kyungtae Kim, Basavesh Ammanaghatta Shivakumar, Byoungyoung Lee, and Insik Shin
IEEE Symposium on Security and Privacy (SP) 2019
31. **PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications**
Yuseok Jeon, Junghwan Rhee, Chung Hwan Kim, Zhichun Li, Mathias Payer, Byoungyoung Lee, and Zhenyu Wu
ACM Conference on Data and Application Security and Privacy (CODASPY) 2019
32. **OBFUSCURO: A Commodity Obfuscation Engine on Intel SGX**
Adil Ahmad*, Byunggil Joe*, Yuan Xiao, Yinqian Zhang, Insik Shin, and Byoungyoung Lee
Network and Distributed System Security Symposium (NDSS) 2019
33. **Obliviate: A Data Oblivious Filesystem for Intel SGX**
Adil Ahmad, Kyungtae Kim, Muhammad Sarfaraz, and Byoungyoung Lee
Network and Distributed System Security Symposium (NDSS) 2018
34. **Securing Real-Time Microcontroller Systems through Customized Memory View Switching**
Chunghwan Kim, Taegyu Kim, Hongjun Choi, Zhongshu Gu, Byoungyoung Lee, Xiangyu Zhang, and Dongyan Xu
Network and Distributed System Security Symposium (NDSS) 2018
35. **Enhancing Memory Error Detection for Large-Scale Applications and Fuzz Testing**
Wookhyun Han, Byunggil Joe, Byoungyoung Lee, Chengyu Song, and Insik Shin
Network and Distributed System Security Symposium (NDSS) 2018
36. **HexType: Efficient Detection of Type Confusion Errors for C++**
Yuseok Jeon, Priyam Biswas, Scott Carr, Byoungyoung Lee, and Mathias Payer
ACM Conference on Computer and Communications Security (CCS) 2017
37. **CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems**
Su Yong Kim, Sangho Lee, Insu Yun, Wen Xu, Byoungyoung Lee, Youngtae Yun, and Taesoo Kim
USENIX Annual Technical Conference (ATC) 2017
38. **SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs**
Jaebaek Seo, Byoungyoung Lee, Sungmin Kim, Ming-Wei Shih, Insik Shin, Dongsu Han, and Taesoo Kim
Network and Distributed System Security Symposium (NDSS) 2017
39. **Instant OS Updates via Userspace Checkpoint-and-Restart**
Sanidhya Kashyap, Changwoo Min, Byoungyoung Lee, Taesoo Kim, and Pavel Emelyanov
USENIX Annual Technical Conference (ATC) 2016
40. **HDFI: Hardware-assisted Data-Flow Isolation**

Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek

IEEE Symposium on Security and Privacy (SP) 2016

41. TrackMeOrNot: Enabling Flexible Control on Web Tracking

Wei Meng, Byoungyoung Lee, Xinyu Xing, and Wenke Lee

International Conference on World Wide Web (WWW) 2016

42. Enforcing Kernel Security Invariants with Data Flow Integrity

Chengyu Song, Byoungyoung Lee, Kangjie Lu, William R. Harris, Taesoo Kim, and Wenke Lee

Network and Distributed System Security Symposium (NDSS) 2016

43. ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks

Kangjie Lu, Chengyu Song, Byoungyoung Lee, Simon P. Chung, Taesoo Kim, and Wenke Lee

ACM Conference on Computer and Communications Security (CCS) 2015

44. Cross-checking Semantic Correctness: The Case of Finding File System Bugs

Changwoo Min, Sanidhya Kashyap, Byoungyoung Lee, Chengyu Song, and Taesoo Kim

ACM Symposium on Operating Systems Principles (SOSP) 2015

45. Type Casting Verification: Stopping an Emerging Attack Vector

Byoungyoung Lee, Chengyu Song, Taesoo Kim, and Wenke Lee

USENIX Security Symposium (Security) 2015

Internet Defense Prize by Facebook and USENIX ([link](#))

Top 10 Finalists by CSAW Best Applied Research Paper Award ([link](#))

46. Understanding Malvertising Through Ad-Injecting Browser Extensions

Xinyu Xing, Wei Meng, Byoungyoung Lee, Udi Weinsberg, Anmol Sheth, Roberto Perdisci, and Wenke Lee

International Conference on World Wide Web (WWW) 2015

47. Preventing Use-after-free with Dangling Pointers Nullification

Byoungyoung Lee, Chengyu Song, Yeongjin Jang, Tielei Wang, Taesoo Kim, Long Lu, and Wenke Lee

Network and Distributed System Security Symposium (NDSS) 2015

Third place award by CSAW Best Applied Research Paper Award ([link](#))

48. Abusing Performance Optimization Weaknesses to Bypass ASLR

Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee

BlackHat USA 2014

49. Exploiting Unpatched iOS Vulnerabilities for Fun and Profit

Yeongjin Jang, Tielei Wang, Byoungyoung Lee, and Billy Lau

BlackHat USA 2014

50. From Zygote to Morula: Fortifying weakened ASLR on Android

Byoungyoung Lee, Long Lu, Tielei Wang, Taesoo Kim, and Wenke Lee

IEEE Symposium on Security and Privacy (SP) 2014

51. Protecting Location Privacy Using Location Semantics

Byoungyoung Lee, Jinoh Oh, Hwanjo Yu, and Jong Kim

ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2011

52. binOb+: A Framework for Potent and Stealthy Binary Obfuscation

Byoungyoung Lee, Yuna Kim, and Jong Kim

ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2010

PUBLICATION (JOURNAL PAPERS)

1. ProS: Light-weight Privatized Secure OSes in ARM TrustZone

Donghyun Kwon, Jiwon Seo, Yeongpil Cho, Byoungyoung Lee, and Yunheung Paek

IEEE Transactions on Mobile Computing 2019

2. **Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques**

Meng Xu, Chengyu Song, Yang ji, Ming-Wei Shih, Kangjie Lu, Cong Zheng, Ruian Duan, Yeongjin Jang, Byoungyoung Lee, Chenxiong Qian, Sangho Lee, and Taesoo Kim

ACM Computing Surveys (CSUR) 2016

ACADEMIC SERVICE

- **Program committee members**

USENIX Security, 2022

ACM Asia Conference on Information, Computer and Communications Security (ASIACCS), 2022

ACM Conference on Computer and Communications Security (CCS), Web Chair, 2021

USENIX Security, 2021

ACM Cloud Computing Security Workshop (CCSW), 2021

ACM Asia Conference on Information, Computer and Communications Security (ASIACCS), 2021

Network and Distributed System Security Symposium (NDSS), 2020

ACM Workshop on Forming an Ecosystem Around Software Transformation (FEAST 2020)

World Conference on Information Security Applications (WISA), 2019

ACM Workshop on Forming an Ecosystem Around Software Transformation (FEAST 2019)

ACM Workshop on the Internet of Safe Things (SafeThings), 2018

World Conference on Information Security Applications (WISA), 2018

ACM Conference on Computer and Communications Security (CCS), 2018

ACM Asia Conference on Information, Computer and Communications Security (ASIACCS), 2018

World Conference on Information Security Applications (WISA), 2017

ACM Conference on Computer and Communications Security (CCS), 2017

Engineering Secure Software and Systems (ESSoS), 2017

ACM Conference on Computer and Communications Security (CCS), Posters and demo, 2016

- **Reviewer**

ACM Transactions on Privacy and Security (TOPS)

IEEE Transactions on Dependable and Secure Computing (TDSC)

IEEE Transactions on Information Forensics and Security (TIFS)

IEEE European Symposium on Security and Privacy (EuroS&P), 2016

Network and Distributed System Security Symposium (NDSS), 2015 2016

USENIX Security Symposium (Security), 2015

ACM Conference on Computer and Communications Security (CCS), 2014-2015

European Symposium on Research in Computer Security (ESORICS), 2014-2015

IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2012

- **Others**

Advisory committee, Central Bank Digital Currency (CBDC), Bank of Korea, 2021

Advisory committee, Digital Forensic Center, Supreme Prosecutors' Office of Republic of Korea, 2020-2021

Cyber Security Awareness Week (CSAW) Applied Research Competition, Preliminary Judges, 2017

Cyber Security Awareness Week (CSAW) Applied Research Competition, Preliminary Judges, 2016

WCTF Belluminar Beijing, Judges, 2016

OPEN SOURCE CONTRIBUTION

- **SGX-Shield:** Enabling ASLR for SGX Programs, Contributor.

<https://github.com/jaebaek/SGX-Shield>

- **LLVM/Clang**: Contributed to Undefined Behavior Sanitizer, Contributor
<http://llvm.org>
- **Chromium Browser**: Contributed to Security Enhancement Tool.
<http://www.chromium.org>
- **CaVer**: Runtime Bad-casting Detection Tool.
<https://github.com/sslabs-gatech/caver>
- **Morula**: Enhancing weakened Android ASLR.
<https://github.com/lifeasageek/morula>
- **TrackMeOrNot**: A web browser enabling selective privacy-sensitive browsing.
<https://github.com/wei-meng/trackmeornot>
- **DarunGrim**: Patch Analysis and Binary Diffing Tool. Contributor.
<https://github.com/ohjeongwook/DarunGrim>
- **ExploitShop**: 1-day vulnerability analysis project. Lead author.
<https://exploitshop.wordpress.com>
- **LocPriv**: Location Privacy with Location Semantics.
<https://github.com/lifeasageek/locpriv>

TEACHING

- Spring 2023 : Software and Systems Security
- Fall 2022 : Systems Programming
- Spring 2021 : Software and Systems Security
- Spring 2021 : Introduction to Data Structures
- Fall 2020 : Introduction to Data Structures
- Spring 2020 : Computer Architecture
- Fall 2019 : Software Security
- Spring 2019 : System Security Seminar
- Fall 2018 : Advance Computer Security Theories and Techniques
- Spring 2018 : Operating Systems (CS 50300, Purdue)
- Fall 2017 : Operating Systems (CS 50300, Purdue)
- Spring 2017 : Secure And Trusted Systems (CS 59000-STS, Purdue)
- Fall 2016: Software security (CS 52700, Purdue)

Byoungyoung Lee
Department of Electrical and Computer Engineering Department
Seoul National University
Last update: May 01, 2024