Daehee Jang (장 대 희)

010.9165.4116
daehee87@khu.ac.kr
https://pwnlab.kr

Education

KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY (KAIST) **……………………………**Daejeon, South Korea

- *Ph. D.* in Graduate School of Information Security (Advisor: Prof. Brent Byunghoon Kang) 8/2014 - 2/2019
- *M.S.* in Graduate School of Information Security (Advisor: Prof. Brent Byunghoon Kang) 3/2012 - 2/2014

HANYANG UNIVERSITY……………………………………………………………………… Seoul, South Korea

- *B.S.* in Department of Computer Engineering (Cum laude) 3/2005 - 2/2012 (w/ army service)

Work Experience

KYUNGHEE UNIVERSITY………………………………………………………………... Yongin, South Korea

- *Assistant Professor (Computer Engineering Department)* 3/2023 - Current

SUNGSHIN W. UNIVERSITY……………………………………………………………... Seoul, South Korea

- *Assistant Professor (Convergence Security Engineering Department)* 3/2021 - 2/2023

GEORGIA TECH ……………………………………………………………………………… Atlanta, USA

- *Post Doctoral Researcher (Advisor: Prof. Taesoo Kim)* 5/2019 - 12/2020

Publications (1st Author, Corresponding)

- "Fuzzability Testing Framework for Incomplete Firmware Binary", Jiwon Jang, Gyeongjin Son, Hyeonsu Lee, Deokjin Kim, Sangwook Lee, Seongmin Kim, **Daehee Jang.** (IEEE Access 2023 Vol 11. IF:3.47)

- "Fuzzing@Home: Distributed Fuzzing on Untrusted Heterogeneous Clients", **Daehee Jang**, Ammar Askar, Insu Yun, Stephen Tong, Yiqin Cai, Taesoo Kim**.** (RAID 2022. Acceptance Rate: 25.0%)

- "Efficient Generation of Program Execution Hash", Eunyeong Ahn, Sunjin Kim, Saerom Park, Jong-Uk Hou, **Daehee Jang (corresponding author).** (IEEE Access 2022 Vol 10. IF: 3.47)

- "Badaslr: Exceptional cases of ASLR aiding exploitation", **Daehee Jang (sole author).** (ELSEVIER Computers and Security Journal. Accepted 2021.10.14 IF: 5.10)

- "On the Analysis of Byte-Granularity Heap Randomization", **Daehee Jang**, Jonghwan Kim, Hojoon Lee, Minjoon Park, Yunjong Jeong, Minsu Kim, Brent Byunghoon Kang. (IEEE Transactions on Dependable and Secure Computing. Accepted 2019.10.01 IF: 6.99)

- "Rethinking Anti-Emulation Techniques for Large-Scale Software Deployment", **Daehee Jang**, Yunjong Jung, Sungman Lee, Minjoon Park, Donguk Kim, Kuenhwan Kwak, Brent Byunghoon Kang. (ELSEVIER Computers and Security Journal. Accepted 2019.02.10. IF: 3.75)

- "SGX-LEGO: Fine-Grained SGX Controlled-Channel Attack and its Countermeasure", Deokjin Kim, **Daehee Jang (co-first author)**, Minjoon Park, Yunjong Jung, Jonghwan Kim, Seokjin Choi, Brent Byunghoon Kang. (ELSEVIER Computers and Security Journal. Accepted 2018.12.04. IF:3.47)

- "ATRA: Address Translation Redirection Attack against Hardware-based External Monitors", **D.Jang**, H Lee, M. Kim, D. H. Kim, D. G. Kim and B. Kang. (ACM CCS 2014. Acceptance Rate: 19.4%), **Google Scholar Citation #: 49**

- "DNS Spoofing Protection System for Wi-Fi Networks", **Daehee Jang**, Yongsu Park. (정보과학회. KCI Journal. 2012.)

Publications (Full)

- "Fuzzability Testing Framework for Incomplete Firmware Binary", Jiwon Jang, Gyeongjin Son, Hyeonsu Lee, Heesun Yun, Deokjin Kim, Sangwook Lee, Seongmin Kim, **Daehee Jang.** (IEEE Access Journal. 2023)

- "Effective Memory Diversification in Legacy Systems ", Heesun Yun, **Daehee Jang.** (IJECES Journal. 2023)

- "Detection Enhancement for Various Deepfake Types Based on Residual Noise and Manipulation Traces", Jihyeong Kang, Sangkeun Ji, Sangyeong Lee, **Daehee Jang**, Jong-Uk Hou**.** (IEEE Access Journal. 2022)

- "Fuzzing@Home: Distributed Fuzzing on Untrusted Heterogeneous Clients", **Daehee Jang**, Ammar Askar, Insu Yun, Stephen Tong, Yiqin Cai, Taesoo Kim**.** (RAID 2022)

- "Efficient Generation of Program Execution Hash", Eunyeong Ahn, Sunjin Kim, Saerom Park, Jong-Uk Hou, **Daehee Jang (corresponding author).** (IEEE Access Journal. 2022)

- "EmuID: Detecting presence of emulation through microarchitectural characteristic on ARM", Yeseul Choi, Yunjong Jeong, **Daehee Jang,** Brent Byunghoon Kang, Hojoon Lee**.** (ELSEVIER Computers and Security Journal. 2022)

- "Badaslr: Exceptional cases of ASLR aiding exploitation", **Daehee Jang (sole author).** (ELSEVIER Computers and Security Journal. 2022)

- "On the Analysis of Byte-Granularity Heap Randomization", **Daehee Jang**, Jonghwan Kim, Hojoon Lee, Minjoon Park, Yunjong Jeong, Minsu Kim, Brent Byunghoon Kang. (IEEE Transactions on Dependable and Secure Computing. 2021)

- " Preventing Use-After-Free Attacks with Fast Forward Allocation ", Brian Wickman, Hong Hu, Insu Yun, **Daehee Jang**, JungWon Lim, Sanidhya Kashyap, and Taesoo Kim. (USENIX Security 2021)

- "Fuzzing JavaScript Engines with Aspect-preserving Mutation", Soyeon Park, Wen Xu, Insu Yun, **Daehee Jang** and Taesoo Kim. (IEEE Symposium on Security and Privacy 2020)

- "POLaR: Per-allocation Object Layout Randomization", Jonghwan Kim, **Daehee Jang**, Yunjong Jeong, Brent Byunghoon Kang. (IEEE/IFIP International Conference on Dependable Systems and Networks 2019)

- "Rethinking Anti-Emulation Techniques for Large-Scale Software Deployment", **Daehee Jang**, Yunjong Jung, Sungman Lee, Minjoon Park, Donguk Kim, Kuenhwan Kwak, Brent Byunghoon Kang. (ELSEVIER Computers and Security Journal. 2019)

- "KI-Mon ARM: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object", H. Lee, H. Moon, I. Heo, **D. Jang**, J. Jang, K. Kim, Y. Paek, and B. Kang. (IEEE TDSC. 2019)

- "SGX-LEGO: Fine-Grained SGX Controlled-Channel Attack and its Countermeasure", Deokjin Kim, **Daehee Jang (co-first author)**, Minjoon Park, Yunjong Jung, Jonghwan Kim, Seokjin Choi, Brent Byunghoon Kang. (ELSEVIER Computers and Security Journal. 2018)

- "Domain Isolated Kernel: A lightweight sandbox for untrusted kernel extensions", Valentin J.M. Manes, **Daehee Jang**, Brent Byunghoon Kang, Chanho Ryu. (ELSEVIER Computers and Security Journal. 2017)

- "S-OpenSGX: A System-level Platform for Exploring SGX Enclave-Based Computing", Changho Choi, Nohyun Kwak, Jinsoo Jang, **Daehee Jang**, Kuenwhee Oh, Kyungsoo Kwag, Brent Byunghoon Kang (ELSEVIER Computers and Security Journal. 2016)

- "Efficient Kernel Integrity Monitor Design for Commodity Mobile Application Processors", Ingoo Heo, **Daehee Jang**, Hyungon Moon, Hansu Cho, Seungwook Lee, Brent Byunghoon Kang, and Yunheung Paek. (Journal of Semiconductor Technology and Science. 2015)

- "ATRA: Address Translation Redirection Attack against Hardware-based External Monitors", **D.Jang**, H Lee, M. Kim, D. H. Kim, D. G. Kim and B. Kang. (ACM Conference on Computer and Communications Security 2014)

- "KI-Mon: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object", H. Lee, H. Moon, **D. Jang**, K. Kim, J. Lee, Y. Paek and B. Kang. (USENIX Security 2013), **Google Scholar Citation #: 88**

- "DNS Spoofing Protection System for Wi-Fi Networks", **Daehee Jang**, Yongsu Park. (Conference of Korean Institute of Information Scientists and Engineers 2012)

International Hacking Competition (CTF) Awards

- 8th place in 2019 DEFCON Hacking Competition Finals (R00timentary, 12 person team)
- 9th place in 2018 SECCON Hacking Competition Finals (BlueBananaKing, four person team)
- 8th place in 2017 TrendMicro Hacking Competition Finals (BrentKawaii, four person team)
- 2nd place in 2016 SECCON Hacking Competition Finals (PwnPineappelApplePwn, four person team)
  http://www.boannews.com/media/view.asp?idx=53251
- 5th place in 2016 DEFCON Hacking Competition Finals (KaisHackGoN, 16 person team)
  http://www.etnews.com/20160802000228
- 9th place in 2016 CODEGATE Hacking Competition Finals (KaSec, four person team)
  http://news.mk.co.kr/newsRead.php?no=318253&year=2016
- 9th place in 2015 CODEGATE Hacking Competition Finals (Alternatives, four person team)
  http://www.boannews.com/media/view.asp?idx=45889
- 13th place in 2015 SECCON Hacking Competition Finals (KaSec, four person team)
  http://www.ddaily.co.kr/news/article.html?no=139921
- 8th place in 2013 DEFCON Hacking Competition Finals (Alternatives, eight person team)
  http://www.boannews.com/media/view.asp?idx=37199

Domestic Hacking Competition (CTF) Awards

- 3rd place in 2018 Korea CCE Hacking Competition Finals (BraveBluKat. four person team)
  5,000,000 KRW prize, https://www.boannews.com/media/view.asp?idx=74271
- 2nd place in 2017 CCE Hacking Competition Finals (에베베베, five person team)
  6,000,000 KRW prize, http://www.boannews.com/media/view.asp?idx=58207
- Winner of 2015 WHITEHAT Hacking Competition Finals (아몰랑, four person team)
  20,000,000 KRW prize, http://www.boannews.com/media/view.asp?idx=48326
- 4th place in 2015 KISA Hacking Competition Finals (KaSec, four person team)
  2,000,000 KRW prize, https://www.yna.co.kr/view/AKR20151130140100017
- 3rd place in 2014 WHITEHAT Hacking Competition Finals (Alternatives, four person team)
  8,000,000 KRW prize, http://www.boannews.com/media/view.asp?idx=44060
- 7th place in 2013 KISA Hacking Competition Finals (Alternatives, four person team)
  http://www.boannews.com/media/view.asp?idx=36730

Academic Awards

- Excellence Award in 2018 Korea Information Security Paper Competition. 1st author. 1,000,000 KRW prize.
- Grand Prize Winner of 2017 Information Security Paper Competition. 1st author. 5,000,000 KRW prize.
  https://news.kaist.ac.kr/news/html/news/?mode=V&mng_no=2285
- Excellence Award in 2017 Korea Information Security Paper Competition. 2nd author. 1,000,000 KRW prize.
- Excellence Award in 2017 Korea Information Security Paper Competition. 1st author. 1,000,000 KRW prize.
- 2016 NAVER Ph.D. Fellowship Award. 5,000,000 KRW prize.

Bug Bounty Awards (Sole activity)

- KISA 2018 Software 0-day Bug Bounty Award
  Arbitrary Code Execution via Heap Overflow in KMPlayer FLV Parser (CVE-2018-5200)
  4,300,000 KRW prize, https://nvd.nist.gov/vuln/detail/CVE-2018-5200
  https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=30113
- Information Security Elite Nomination in KISA 2016 Ceremony. Special Prize for Hancom Office Bug Bounty
  http://www.zdnet.co.kr/news/news_view.asp?artice_id=20161223171127
- KISA 2016 Software 0-day Bug Bounty Award
  Arbitrary Code Execution via Heap Overflow in Hangul (Report number 16-251). 3,200,000 KRW prize
- KISA 2015 Software 0-day Bug Bounty Award.
  Arbitrary Code Execution via Heap Use-After-Free in Hangul (Report number 15-621). 2,400,000 KRW prize
- KISA 2015 Software 0-day Bug Bounty Award
  Arbitrary Code Execution via Stack Overflow in Hangul (Report number 15-284). 1,500,000 KRW prize
- KISA 2015 Software 0-day Bug Bounty Award
  Arbitrary Code Execution via Stack Overflow in IPTIME router (Report number 15-074). 1,800,000 KRW prize

Remarks

- **Director of Graduate School of Convergence Security in Kyunghee University 2023.7 ~**
- **Defense Acquisition Program Administration Advisory Committee 2023.6**
- **KISTI Advisory Committee 2022.12.6 – 2022.12.7**
- **Department of Defense Advisory Committee 2021.11**
- **Founder/creator of http://pwnable.kr wargame (Since 2014 – Current)**
- **Hacking Competition (CTF) Challenge Author/Organizer**
  - Samsung CTF 2017, 2018 Organizing Team
  - CODEGATE CTF 2017 Challenge Author
  - SECUINSIDE CTF 2017 Challenge Author

Invited Seminars

- Agency of Defense Development (ADD) Invited Speaker, 2023 Fall, "Fuzzing PX4 Drones"
- KIISE WDSC Workshop Invited Speaker, 2023 Fall, "BadASLR: Exceptional cases of ASLR aiding Exploit"
- KIISC Drone Security Workshop Invited Speaker, 2023 Fall, "Applying libfuzzer to PX4 Drones"
- KIISC Cyber Security Education Program Invited Speaker, 2023 Fall, "Drone System and Security"
- TyphoonCon Invited Speaker, 2023 Summer, "BadASLR: Exceptional cases of ASLR aiding Exploit"
- KIISC Cyber Security Education Program Invited Speaker, 2023 Summer, "Drone System and Security"
- CPS Workshop Invited Speaker, 2023 Spring, "Applying Dynamic Analysis to Embedded System"
- KIISC Cyber Security Education Program Invited Speaker, 2023 Spring, "Drone System and Security"
- UNIST Software Department Invited Speaker, 2022 Fall, "Distributed Fuzzing on Untrusted Heterogeneous Clients"
- KISA Invited Speaker, 2022 Fall, "Security Vulnerabilities in Web Application Frameworks"
- Sejong University Invited Speaker, 2022 Fall, "System Security issues in Wargame/CTFs"
- CPS Workshop Invited Speaker, 2022 Fall, "Fuzzing and Security in Embedded Systems"
- WISA Invited Speaker, 2021 Fall, "Introduction to OS Command Injection"
- ETRI System Security Lab Invited Speaker, 2022 Spring, "DBI and Offensive Security Technologies"
- ETRI System Security Lab Invited Speaker, 2021 Spring, "Explaining Address Sanitizer and Fuzzing"
- UNIST Software Department Invited Speaker, 2019 Spring, "0-day attack explained"
- KAIST PLRG Lab Invited Speaker, 2019 Spring, "WASM Sandbox Explained"
- ETRI System Security Lab Invited Speaker, 2019 Spring, "H/W based Fine Grained Memory Access Control"
- KISA Invited Speaker, 2018 Winter, "Explaining Hacking Competition Challenges"
- CODEGATE 2016 Conference Invited Speaker, "Codemap: Visualization tool for software reverse engineering"
- Hong Kong Cyber Security Symposium 2015 Speaker, "Android Mobile Malware Threats"
- Dankook Univ. Security Lab Invited Speaker, 2014 Fall, "Applying CVE-2014-3153 to x86 Ubuntu 13.04 Kernel"

Patents

- (International) Byunghoon Kang, **Daehee Jang**, Minsu Kim, Jonghwan Kim, Daeggyung Kim, Hojoon Lee "Memory Alignment Randomization Method for Mitigation of Heap Exploit", Application Date: 2017-04-12, Application Number: 15485868.
- (Domestic) Donguk Kim, Byonghoon Kang, Sengyon Ha, **Daehee Jang**, Jinsoo Jang, Hong Suk, "Electronic Device and Control Method", 10-2017-0148241.
- (Domestic) Jinsoo Jang, **Daehee Jang**, Brent Byunghoon Kang, Donguk Kim, "An Electronic Device and Method For Protecting The Kernel Space of the Memory", 10-2015-0165474.