Byoungyoung Lee

Assistant Professor
Department of Computer Science
Purdue University
West Lafayette, IN 47907

Phone: (404) 903-6742
Email: byoungyoung@purdue.edu
Homepage: https://lifeasageek.github.io

Education

Georgia Institute of Technology, Atlanta, GA ..... Aug 2016

Ph.D. in Computer Science.

Thesis: Protecting Computer Systems through Eliminating or Analyzing Vulnerabilities

Advisors: Prof. Wenke Lee and Prof. Taesoo Kim

POSTECH, Pohang, South Korea ..... May 2011

B.S. and M.S. in Computer Science and Engineering

Advisor: Prof. Jong Kim

Research Interests

Interested in **all computer security and privacy related problems** in general. In particular, my research focus is in **system security**, e.g., designing and implementing secure systems through eliminating vulnerabilities and mitigating attacks.

Honors & Awards

Internet Defense Prize by Facebook and USENIX ($100,000 award), 2015 [13]

Qualified for **DARPA Cyber Grand Challenge** (Team Disekt, $750,000 award), 2015

The third place award by **CSAW Best Applied Research Paper Award**, 2015 [15]

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

DEFCON 19 CTF[1], 8th place (Team PLUS@POSTECH). Las Vegas, USA, 2011

DEFCON 17 CTF, 3rd place (Team PLUS@POSTECH). Las Vegas, USA, 2009

KAIST-POSTECH Science War - Hacking Competition. Winner. 2008

DEFCON 14 CTF, 6th place (Team The East Sea). Las Vegas, USA, 2006

Wowhacker Hacking Festival. Supreme Award, 2006

KISA Hacking Defense Competition, Special Prize, 2006

KAIST-POSTECH Science War - Hacking Competition, Winner 2005

POSTECH Undergraduate Research Program Scholarship, 2005

Full undergraduate study scholarship, Korea Science and Engineering Foundation, 2003 – 2009

[1]DEFCON CTF (Capture The Flag) is the most prestigious hacking competition in the world among more than 200 teams

Professional Experience

Purdue University. West Lafayette, IN ..... Aug 2016 – Current
Assistant Professor, Department of Computer Science

Chrome Security Team, Google. Mountain View, CA ..... May 2014 – Aug 2014
Software Engineering Intern: worked on detecting runtime bad-casting
Mentor: Abhishek Arya

Microsoft Research Redmond, Microsoft. 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

Open Source Contribution

SGX-Shield. Enabling ASLR for SGX Programs [6]. Contributor.
https://github.com/jaebaek/SGX-Shield

LLVM/Clang. Contributed to Undefined Behavior Sanitizer
http://llvm.org

Chromium Browser. Contributed to Security Enhancement Tool
http://www.chromium.org

CaVer. Runtime Bad-casting Detection Tool [13]. Lead author.
https://github.com/sslab-gatech/caver

Morula. Enhancing weakened Android ASLR [18]. Lead author.
https://github.com/lifeasageek/morula

TrackMeOrNot. A web browser enabling selective privacy-sensitive browsing [9]. Developer.
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 [19]. Lead author.
https://github.com/lifeasageek/locpriv

Reported Security Vulnerabilities (selected list)

CVE-2016-7219: Windows Crypto Driver Information Disclosure Vulnerability (MS16-149)

CVE-2016-0040: Windows Kernel Elevation of Privilege Vulnerability (MS16-014)

CVE-2014-1594: Mozilla Firefox Bad casting from BasicThebesLayer to BasicContainerLayer

WebKit Bug #120633: Partial Information Leakage in Hash Table Implementations (PrivateName)

CVE-2013-2910: Mozilla Firefox Use-after-free when updating offline cache

CVE-2013-2910: Google Chrome Use-after-free in Web Audio

CVE-2013-2917: Google Chrome Out of bounds read in Web Audio

CVE-2013-2918: Google Chrome Use-after-free in DOM

CVE-2013-2921: Google Chrome Use-after-free in resource loader

CVE-2012-1139: BDF font overflow on Freetype2

Publication

Conference Papers

[1] **Obliviate: A Data Oblivious Filesystem for Intel SGX**.
Adil Ahmad, Kyungtae Kim, Muhammad Sarfaraz, and Byoungyoung Lee.
In *Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2018.

[2] **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.
In *Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2018.

[3] **Enhancing Memory Error Detection for Large-Scale Applications and Fuzz Testing**.
Wookhyun Han, Byunggill Joe, Byoungyoung Lee, Chengyu Song, and Insik Shin.
In *Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2018.

[4] **HexType: Efficient Detection of Type Confusion Errors for C++**.
Yuseok Jeon, Priyam Biswas, Scott Carr, Byoungyoung Lee, and Mathias Payer.
In *Proceedings of the 24nd ACM Conference on Computer and Communications Security (CCS)*, Dallas, Texas, October 2017.
Acceptance rate: 18.1% (151 of 836).

[5] **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.
In *Proceedings of the 2017 USENIX Annual Technical Conference (ATC)*, Santa Clara, CA, July 2017.
Acceptance rate: 21.2% (60 of 283).

[6] **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.
In *Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2017.
Acceptance rate: 16.1% (68 of 423).

[7] **Instant OS Updates via Userspace Checkpoint-and-Restart**.
Sanidhya Kashyap, Changwoo Min, Byoungyoung Lee, Taesoo Kim, and Pavel Emelyanov.
In *Proceedings of the 2016 USENIX Annual Technical Conference (ATC)*, Denver, CO, June 2016.
Acceptance rate: 17.7% (47 of 266).

[8] **HDFI: Hardware-assisted Data-Flow Isolation**.
Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek.
In *Proceedings of the 37th IEEE Symposium on Security and Privacy (Oakland)*, San Jose, CA, May 2016.
Acceptance rate: 13.8% (55 of 400).

[9] **TrackMeOrNot: Enabling Flexible Control on Web Tracking**.
Wei Meng, Byoungyoung Lee, Xinyu Xing, and Wenke Lee.
In *Proceedings of the 25th International Conference on World Wide Web (WWW)*, Montreal, Canada, April 2016.
Acceptance rate: 15.8% (115 of 727).

[10] **Enforcing Kernel Security Invariants with Data Flow Integrity**.
Chengyu Song, Byoungyoung Lee, Kangjie Lu, William R. Harris, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2016.
Acceptance rate: 15.4% (60 of 389).

[11] **ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks**.
Kangjie Lu, Chengyu Song, Byoungyoung Lee, Simon P. Chung, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, Colorado, October 2015.
Acceptance rate: 19.9% (128 of 646).

[12] **Cross-checking Semantic Correctness: The Case of Finding File System Bugs**.
Changwoo Min, Sanidhya Kashyap, Byoungyoung Lee, Chengyu Song, and Taesoo Kim.
In *Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP)*, Monterey, CA, October 2015.
Acceptance rate: 16.1% (30 of 186).

[13] **Type Casting Verification: Stopping an Emerging Attack Vector**.
Byoungyoung Lee, Chengyu Song, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 24th Usenix Security Symposium (Security)*, Washington, DC, August 2015.
Acceptance rate: 15.7% (67 of 426).
∗ **Internet Defense Prize** by Facebook and USENIX,
∗ Top 10 Finalists by **CSAW Best Applied Research Paper Award**.

[14] **Understanding Malvertising Through Ad-Injecting Browser Extensions**.
Xinyu Xing, Wei Meng, Byoungyoung Lee, Udi Weinsberg, Anmol Sheth, Roberto Perdisci, and Wenke Lee.
In *Proceedings of the 24th International Conference on World Wide Web (WWW)*, Florence, Italy, May 2015.
Acceptance rate: 14.1% (131 of 929).

[15] **Preventing Use-after-free with Dangling Pointers Nullification**.
Byoungyoung Lee, Chengyu Song, Yeongjin Jang, Tielei Wang, Taesoo Kim, Long Lu, and Wenke Lee.
In *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2015.
Acceptance rate: 16.9% (51 of 302).
∗ Third place award by **CSAW Best Applied Research Paper Award**.

[16] **Abusing Performance Optimization Weaknesses to Bypass ASLR**.
Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee.
In *2014 BlackHat USA*, Las Vegas, NV, August 2014.

[17] **Exploiting Unpatched iOS Vulnerabilities for Fun and Profit**.
Yeongjin Jang, Tielei Wang, Byoungyoung Lee, and Billy Lau.
In *2014 BlackHat USA*, Las Vegas, NV, August 2014.

[18] **From Zygote to Morula: Fortifying weakened ASLR on Android**.
Byoungyoung Lee, Long Lu, Tielei Wang, Taesoo Kim, and Wenke Lee.
In *Proceedings of the 35th IEEE Symposium on Security and Privacy (Oakland)*, San Jose, CA, May 2014.
Acceptance rate: 13.1% (44 of 334).

[19] **Protecting Location Privacy Using Location Semantics**.

Byoungyoung Lee, Jinoh Oh, Hwanjo Yu, and Jong Kim.
In *Proceedings of the 17th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)*, San Diego, CA, August 2011.
Acceptance rate: 17.6% (126 of 714).

[20] **binOb+: A Framework for Potent and Stealthy Binary Obfuscation**.
Byoungyoung Lee, Yuna Kim, and Jong Kim.
In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Beijing, China, April 2010.
Acceptance rate: 15.1% (25 of 166).

Journal Papers

[21] **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.
In *ACM Computing Surveys (CSUR)*, 49(2), August 2016.

Invited Talks

Toward Secure Trusted Computing

Seoul National University. Seoul, South Korea. Jan 2017

KAIST. Daejeon, South Korea. Dec 2016

Protecting Computer Systems through Eliminating or Analyzing Vulnerabilities

Rice University. Houston, TX. 2016

University of Georgia, Athens, GA. 2016

Arizona State University. Tempe, AZ. 2016

University of Massachusetts, Amherst. Amherst, MA. 2016

Purdue University. West Lafayette, IN. 2016

University of California, Riverside. Riverside, CA. 2016

Georgia Institute of Technology. Atlanta, GA. 2016

Abusing Performance Optimization Weaknesses to Bypass ASLR

KAIST. Daejeon, South Korea. 2014

Seoul National University. Seoul, South Korea. 2014

POSTECH. Pohang, South Korea. 2014

Detect Bad-Casting at Runtime with Undefined Behavior Sanitizer

Google. Mountain View, CA. 2014

Identifying Memory Corruption Bugs with Compiler Instrumentation

National Intelligence Service. Daejeon, South Korea. 2014

National Security Research Institute. Seoul, South Korea. 2014

Power of Community (POC). Seoul, South Korea. 2014

Samsung Electronics. Suwon, South Korea. 2014

Mapping Dynamic Data for User-mode Crash Dump Analysis

Microsoft Research. Redmond, WA. 2011

Teaching

Operating Systems (CS 50300), Purdue University, Spring 2018

Operating Systems (CS 50300), Purdue University, Fall 2017

Secure and Trusted Systems (CS 59000), Purdue University, Spring 2017

Software Security (CS 52700), Purdue University, Fall 2016

Professional Activities

Program committee

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

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

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

WCTF Belluminar Beijing, Judges, 2016

Last updated: April 9, 2018