

Yonghwi Kwon

ASSISTANT PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF VIRGINIA

85 Engineer's Way, Charlottesville, VA, 22903

EMAIL : yongkwon@virginia.edu

WEB : <http://yongkwon.info>

RESEARCH INTERESTS	Systems Security with focuses on <i>Program Analysis (Static/Dynamic and Binary Analysis)</i> , <i>Causality Inference</i> , and <i>Reverse-Engineering</i>
APPOINTMENTS	University of Virginia , Dept. of Computer Science, Charlottesville, VA, USA <i>John Knight Career Enhancement Assistant Professor</i> Aug 2018 - Current
EDUCATION	Purdue University , Dept. of Computer Science, West Lafayette, IN, USA <i>Ph.D. in Computer Science</i> May 2012 - Aug 2018 – Advisors: Professor Xiangyu Zhang and Professor Dongyan Xu Konkuk University , Dept. of Computer Science and Engineering, Seoul, South Korea <i>B.E. in Computer Science and Engineering (Summa Cum Laude)</i> March 2004 - Aug 2011
PUBLICATIONS	CONFERENCES [C18] “CUBISMO: Decloaking Server-side Malware via Cubist Program Analysis,” A. Naderi, Y. Kwon , A. Nguyen, J. Davidson, and M. Bagheri, In Proc. of the <i>35th Annual Conference on Computer Security Applications (ACSAC’19)</i> , December 9-13, 2019 [C17] “BDA: Practical Dependence Analysis for Binary Executables by Unbiased Whole-program Path Sampling and Per-path Abstract Interpretation,” Z. Zhang, W. You, G. Tao, G. Wei, Y. Kwon , and X. Zhang, In Proc. of the <i>2019 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA’19)</i> , October 20-25, 2019 [C16] “Probabilistic Disassembly,” K. Miller, Y. Kwon , X. Zhang, and Z. Lin, In Proc. of the <i>41st International Conference on Software Engineering (ICSE’19)</i> , May 25-31, 2019 [C15] “LPROV: Practical Library-aware Provenance Tracing,” F. Wang, Y. Kwon , S. Ma, X. Zhang, and D. Xu, In Proc. of the <i>34th Annual Conference on Computer Security Applications (ACSAC’18)</i> , December 9-13, 2018 [C14] “Kernel-Supported Cost-Effective Audit Logging for Causality Tracking,” S. Ma, J. Zhai, Y. Kwon , K. H. Lee, X. Zhang, G. Ciocarlie, A. Gehani, V. Yegneswaran, D. Xu, and S. Jha, In Proc. of the <i>2018 USENIX Annual Technical Conference (ATC’18)</i> , July 11-13, 2018 [C13] “AdBudgetKiller: Online Advertising Budget Draining Attack,” I. L. Kim, W. Wang, Y. Kwon , Y. Zheng, Y. Aafer, W. Meng, and X. Zhang, In Proc. of the <i>27th International World Wide Web Conference (WWW’18)</i> , April 23-27, 2018 [C12] “MCI: Modeling-based Causality Inference in Audit Logging for Attack Investigation,” Y. Kwon , F. Wang, W. Wang, K. H. Lee, W. C. Lee, S. Ma, X. Zhang, D. Xu, S. Jha, G. Ciocarlie, A. Gehani, and V. Yegneswaran, In Proc. of the <i>25th Network and Distributed System Security Symposium (NDSS’18)</i> , February 18-21, 2018 [C11] “RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications,” T. Kim, C. H. Kim, H. Choi, Y. Kwon , B. Saltaformaggio, X. Zhang, and D. Xu, In Proc. of the <i>33rd Annual Conference on Computer Security Applications (ACSAC’17)</i> , Dec 4-8, 2017 [C10] “PAD: Programming Third-party Web Advertisement Censorship,” W. Wang, Y. Kwon , Y. Zheng, Y. Aafer, I. L. Kim, W. C. Lee, Y. Liu, W. Meng, X. Zhang, and P. Eugster, In Proc. of the <i>32nd IEEE/ACM International Conference on Automated Software Engineering (ASE’17)</i> , October 31-November 3, 2017 [C9] “CPR: Cross Platform Binary Code Reuse via Platform Independent Trace Program,” Y. Kwon , W. Wang, Y. Zheng, X. Zhang, and D. Xu, In Proc. of the <i>26th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA’17)</i> , July 10-14, 2017 [C8] “J-Force: Forced Execution on JavaScript,” K. Kim, I. L. Kim, C. H. Kim, Y. Kwon , Y. Zheng, X. Zhang, and D. Xu, In Proc. of the <i>26th International World Wide Web Conference (WWW’17)</i> , April 3-7, 2017 [C7] “A2C: Self Destructing Exploit Executions via Input Perturbation,” Y. Kwon , B. Saltaformaggio, I. L. Kim, K. H. Lee, X. Zhang, and D. Xu, In Proc. of the <i>24th Network and Distributed System Security Symposium (NDSS’17)</i> , February 26-March 1, 2017

[C6] “Apex: Automatic Programming Assignment Error Explanation,” D. Kim, Y. Kwon, P. Liu, I. L. Kim, D. M. Perry, X. Zhang, and G. Rodriguez-Rivera, In Proc. of the 2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA’16), October 30–November 4, 2016

[C5] “WebRanz: Web Page Randomization For Better Advertisement Delivery and Web-Bot Prevention,” W. Wang, Y. Zheng, X. Xing, Y. Kwon, X. Zhang, and P. Eugster, In Proc. of the 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE’16), November 13–18, 2016

[C4] “LDX: Causality Inference by Lightweight Dual Execution,” Y. Kwon, D. Kim, W. N. Sumner, K. Kim, B. Saltaformaggio, X. Zhang, and D. Xu, In Proc. of the 21st International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS’16), April 2–6, 2016

[C3] “Dual Execution for On the Fly Fine Grained Execution Comparison,” D. Kim, Y. Kwon, W. N. Sumner, X. Zhang, and D. Xu, In Proc. of the 20th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS’15), March 14–18, 2015

[C2] “P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions,” Y. Kwon, F. Peng, D. Kim, K. Kim, X. Zhang, D. Xu, V. Yegneswaran, and J. Qian, In Proc. of the 22nd Network and Distributed System Security Symposium (NDSS’15), February 8–11, 2015

[C1] “PIEtrace: Platform Independent Executable Trace,” Y. Kwon, X. Zhang, and D. Xu, In Proc. of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE’13), November 11–15, 2013

Best Paper Award (1/317) and ACM SIGSOFT Distinguished Paper Award (3/317)

WORKSHOPS

[W2] “Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic,” B. Saltaformaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, J. Qian, In Proc. of the 10th USENIX Workshop on Offensive Technologies (WOOT’16)

[W1] “Virtual Machine-based Stack Overflow Detector,” Y. Kwon and N. Park, In Proc. of the 12th International Workshop on Information Security Applications (WISA’11)

BOOK

[B1] “Effective Windows Programming,” Y. Kwon, Y. Kim, and Y. Shin, Wellbook (In Korean), June 2010, ISBN 8901109107.

AWARDS AND GRANTS

GRANTS

I have contributed to secure more than **\$2.7M (My share: \$937K)** to support my research projects.

[G4] *SaTC: CORE: Medium: Collaborative: Doctor WHO: Investigation and Prevention of Online Content Management System Abuse*, with Georgia Tech and the University of Georgia, National Science Foundation (NSF), Total \$1.2M (My share: \$387,700.0) 10/01/2019–09/30/2023

[G3] *OAC Core: Small: Collaborative Research: Data Provenance Infrastructure towards Robust and Reliable Data Sharing and Analytics* (Recommended), with the University of Georgia, National Science Foundation (NSF), Total \$500K (My share: \$250,000.0) 7/01/2019–06/30/2022

[G2] *Athena: System Auditing by Learning Causality from Application and System Logs*, with Intelligent Automation, Inc. (IAI) and Purdue University, Office of Naval Research (ONR), Total \$900,000.0 (My share: \$125,000.0) 02/01/2019–01/31/2021

[G1] *CRII: SaTC: Secure and Comprehensive Forensic Audit Infrastructure for Transparent Heterogeneous Computing*, Sole-PI, National Science Foundation (NSF), Total \$174,379.0 03/01/2019–02/28/2021

AWARDS

NSF CISE CRII (RESEARCH INITIATION INITIATIVE) AWARD	2019
MAURICE H. HALSTEAD MEMORIAL AWARD for Outstanding Research in Software Engineering	2017
ACM SIGSOFT DISTINGUISHED PAPER AWARD	2013
BEST PAPER AWARD, IEEE/ACM International Conference on Automated Software Engineering	2013

MICROSOFT MVP (MOST VALUABLE PROFESSIONAL) (5 Time Awardee) 2008 – 2013

TEAM AWARDS

Winner (Faculty Advisor), the National Collegiate Cyber Defense Competition 2019

Winner (Faculty Advisor), the Mid-Atlantic Collegiate Cyber Defense Competition 2019

WORK EXPERIENCE

Purdue University, Graduate Research Assistant *May 2012 – Present*

- Perform research in the area of system security, programming language, and reverse-engineering.
- Highlights include publications in top-tier conferences (3 NDSS, 2 ASPLOS, 2 ASE, ISSTA, OOPSLA, FSE, WWW), ACM SIGSOFT Distinguished Paper and Best Paper Award (PIEtrace in ASE'13), and Maurice H. Halstead Memorial Award for outstanding research in software engineering.

Settec, Researcher *July 2006 – July 2009*

- Developed various security solutions such as DRM (Digital Rights Management).
- Implemented several security solutions leveraging API hooking techniques.

Korea Telecom, Part-time Developer *July 2004 – Aug 2004*

- Developed a system utility that analyzes and optimizes Windows systems.

INVITED TALKS

POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY (POSTECH), SOUTH KOREA 2019

- Combatting APTs via Input Perturbation

KONKUK UNIVERSITY, SOUTH KOREA 2019

- Software Security via Program Analysis

SUNGKYUNKWAN UNIVERSITY, SOUTH KOREA 2019

- Combatting APTs via Input Perturbation

KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY (KAIST), SOUTH KOREA 2019

- Combatting APTs via Input Perturbation

KOCSEA TECHNICAL SYMPOSIUM (19TH), KOCSEA 2018

- Combatting APTs via Program Analysis

CERIAS SECURITY SEMINAR, PURDUE UNIVERSITY 2017

- A2C: Self Destructing Exploit Executions via Input Perturbation

CERIAS SECURITY SEMINAR, PURDUE UNIVERSITY 2015

- P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions

MICROSOFT TECHNICAL SEMINAR, MICROSOFT KOREA 2011

- Migration to the Visual Studio 2010

MICROSOFT TECHNICAL SEMINAR, MICROSOFT KOREA 2010

- Effective Windows Programming

MICROSOFT TECHNICAL SEMINAR, MICROSOFT KOREA 2009

- Advanced topics in Windows Programming

SAMSUNG ELECTRONICS TECHNICAL SEMINAR (PRIVATE), SAMSUNG ELECTRONICS 2009

- Debugging Applications in Windows

OTHER ACTIVITIES

Online Community Moderator, Korean Visual Studio User Group *2008 – 2012*

Student Researcher, Samsung Software Membership, Samsung Electronics *July 2004 – July 2006*

SERVICES

PROGRAM COMMITTEE:

Network and Distributed System Security Symposium (NDSS'20/19)

Annual Conference on Computer Security Applications (ACSAC'19/18)

International Workshop on Theory and Practice of Provenance (TaPP'17)

IEEE Security & Privacy 2017 Student PC (SP'17)

EXTERNAL REVIEWER:

ACM Conference on Computer and Communications Security (CCS'18/16/15/13)

The Network and Distributed System Security Symposium (NDSS'17/14)

The International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'17)

The ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'17)

IEEE Conference on Communications and Network Security (CNS'16)

The International Conference on Software Engineering (ICSE'17)

The ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE'18/16)
The International Symposium on Software Testing and Analysis (ISSTA'17/16/14)
The IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'16)
The International Symposium on Research in Attacks, Intrusions and Defenses (RAID'16)

REFERENCES

Available upon a request.