Yonghwi Kwon

Assistant Professor, University of Virginia

yongkwon@virginia.edu
http://yongkwon.info

Appointments

University of Virginia, Department of Computer Science, Charlottesville, USA
John Knight Career Enhancement Assistant Professor — Aug 2018 - Current

Education

Purdue University, Department of Computer Science, West Lafayette, USA
Ph.D. in Computer Science — May 2012 - Aug 2018

Konkuk University, Department of Computer Science and Engineering, Seoul, South Korea
B.E. in Computer Science and Engineering (Summa Cum Laude) — March 2004 - Aug 2011

Awards

NSF CAREER Award — 2022
Research Communication Fellow, University of Virginia — 2022
ACM SIGPLAN Distinguished Paper Award — 2019
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 (Faculty Advisor)

National Collegiate Cyber Defense Competition (NCCDC) — 2019/2020 (1st place)
Mid-Atlantic Collegiate Cyber Defense Competition (MACCDC) — 2019 (1st place), 2020/2022 (2nd place)

Honors

Finalist, Meta Silent Data Corruptions at Scale Research Award — 2022

Publications

Conferences

– Top-venues (25): S&P (4), NDSS (4), CCS (3), ICSE/FSE/ASE (7), ASPLOS (2), OOPSLA (2), WWW (3).

	2012∼2018 (Ph.D.)	2019	2020	2021	2022
Security/ System (13)	NDSS (3) [2, 7, 12], ASPLOS (2) [3, 4]	CCS [19]	S&P (2) [20, 21]	NDSS [22], S&P [23], CCS [26]	S&P [31], CCS [34]
PL/SE (9)	ASE (2) [🏆 1, 10], FSE [5], OOPSLA [6]	ICSE [16], OOPSLA [🏆 17]		FSE [27], ASE [28]	ICSE [32]
Web (3)	WWW (2) [13, 8]			WWW [24]	

[34] **CCS'22** – **DriveFuzz: Discovering Autonomous Driving Bugs through Driving Quality-Guided Fuzzing**, *29th ACM Conference on Computer and Communications Security*

> S. Kim, M. Liu, J. Rhee, Y. Jeon, **Y. Kwon**, and C. H. Kim

[33] **Dazzle-attack: Anti-Forensic Server-side Attack via Fail-free Dynamic State Machine**, *23rd World Conference on Information Security Applications* (WISA'22)

> B. Lee*, K. Lim* (*: co-first authors), J. Lee, C. Jung, D. Kim, K. H. Lee, H. Cho, and **Y. Kwon**

[32] **ICSE'22** – **Hiding Critical Program Components via Ambiguous Translation**, *44th International Conference on Software Engineering*

> C. Jung, D. Kim, A. Chen, W. Wang, Y. Zheng, K. H. Lee, and **Y. Kwon**

[31] **S&P'22** – **SwarmFlawFinder: Discovering and Exploiting Logic Flaws of Swarm Algorithms**, *43rd IEEE Symposium on Security and Privacy*

> C. Jung, A. Ahad, Y. Jeon, and **Y. Kwon**

[30] **Software Watermarking via a Binary Function Relocation**, *37th Annual Conference on Computer Security Applications* (ACSAC'21)

> H. Kang, **Y. Kwon**, S. Lee, and H. Koo

[29] **Defeating Program Analysis Techniques via Ambiguous Translation**, *36th IEEE/ACM International Conference on Automated Software Engineering (New Ideas and Emerging Results)* (ASE'21 NIER)

> C. Jung, D. Kim, W. Wang, Y. Zheng, K. H. Lee, and **Y. Kwon**

[28] **ASE'21** – **An Empirical Study of Bugs in WebAssembly Compilers**, *36th IEEE/ACM International Conference on Automated Software Engineering*

A. Romano, X. Liu, **Y. Kwon**, and W. Wang

[27] **FSE'21** – **Swarmbug: Debugging Configuration Bugs in Swarm Robotics**, *29th ACM SIGSOFT International Symposium on the Foundations of Software Engineering*

C. Jung, A. Ahad, J. Jung, S. Elbaum, and **Y. Kwon**

[26] **CCS'21** – **Spinner: Automated Dynamic Command Subsystem Perturbation**, *28th ACM Conference on Computer and Communications Security*

M. Wang, C. Jung, A. Ahad, and **Y. Kwon**

[25] **Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem**, *16th ACM ASIA Conference on Computer and Communications Security* (ASIACCS'21)

D. Kim, H. Cho, **Y. Kwon**, A. Doupe, S. Son, G. Ahn, and T. Dumitras

[24] **WWW'21** – **TLS 1.3 in Practice: How TLS 1.3 Contributes to Internet**, *30th The Web Conference*

H. Lee, D. Kim, and **Y. Kwon**

[23] **S&P'21** – **OSPREY: Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary**, *42nd IEEE Symposium on Security and Privacy*

Z. Zhang, Y. Ye, W. You, G. Tao, W. Lee, **Y. Kwon**, Y. Aafer, and X. Zhang

[22] **NDSS'21** – **C^{2}SR: Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis**, *28th Network and Distributed System Security Symposium*

Y. Kwon, W. Wang, J. Jung, K. H. Lee, and R. Perdisci

[21] **S&P'20** – **TARDIS: Rolling Back The Clock On CMS-Targeting Cyber Attacks**, *41st IEEE Symposium on Security and Privacy*

R. Kasturi, Y. Sun, R. Duian, O. Alrawi, E. Asdar, V. Zhu, **Y. Kwon**, and B. Saltaformaggio

[20] **S&P'20** – **PMP: Cost-effective Forced Execution with Probabilistic Memory Pre-planning**, *41st IEEE Symposium on Security and Privacy*

W. You, Z. Zhang, **Y. Kwon**, Y. Aafer, F. Peng, Y. Shi, C. Makena Harmon, and X. Zhang

[19] **CCS'19** – **MalMax: Multi-Aspect Execution for Automated Dynamic Web Server Malware Analysis**, *26th ACM Conference on Computer and Communications Security*

A. Naderi, **Y. Kwon**, A. Nguyen, A. Razmjoo, M. Zamiri, and J. W. Davidson

[18] **CUBISMO: Decloaking Server-side Malware via Cubist Program Analysis**, *35th Annual Conference on Computer Security Applications* (ACSAC'19)

A. Naderi, **Y. Kwon**, A. Nguyen, M. Bagheri, and J. W. Davidson

[17] **OOPSLA'19** – **BDA: Practical Dependence Analysis for Binary Executables by Unbiased Whole-program Path Sampling and Per-path Abstract Interpretation**, *2019 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications*
ACM SIGPLAN Distinguished Paper Award

Z. Zhang, W. You, G. Tao, G. Wei, **Y. Kwon**, and X. Zhang

[16] **ICSE'19** – **Probabilistic Disassembly**, *41st International Conference on Software Engineering*

K. Miller, **Y. Kwon**, Y. Sun, Z. Zhang, X. Zhang, and Z. Lin

[15] **LPROV: Practical Library-aware Provenance Tracing**, *34th Annual Conference on Computer Security Applications* (ACSAC'18)

F. Wang, **Y. Kwon**, S. Ma, X. Zhang, and D. Xu

[14] **Kernel-Supported Cost-Effective Audit Logging for Causality Tracking**, *2018 USENIX Annual Technical Conference* (ATC'18)

S. Ma, J. Zhai, **Y. Kwon**, K. H. Lee, X. Zhang, G. Ciocarlie, A. Gehani, V. Yegneswaran, D. Xu, and S. Jha

[13] **WWW'18** – **AdBudgetKiller: Online Advertising Budget Draining Attack**, *27th International World Wide Web Conference*

> I. L. Kim, W. Wang, **Y. Kwon**, Y. Zheng, Y. Aafer, W. Meng, and X. Zhang

[12] **NDSS'18** – **MCI: Modeling-based Causality Inference in Audit Logging for Attack Investigation**, *25th Network and Distributed System Security Symposium*

> **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

[11] **RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications**, *33rd Annual Conference on Computer Security Applications* (ACSAC'17)

> T. Kim, C. H. Kim, H. Choi, **Y. Kwon**, B. Saltaformaggio, X. Zhang, and D. Xu

[10] **ASE'17** – **PAD: Programming Third-party Web Advertisement Censorship**, *32nd IEEE/ACM International Conference on Automated Software Engineering*

> W. Wang, **Y. Kwon**, Y. Zheng, Y. Aafer, I. L. Kim, W. C. Lee, Y. Liu, W. Meng, X. Zhang, and P. Eugster

[9] **CPR: Cross Platform Binary Code Reuse via Platform Independent Trace Program**, *26th ACM SIGSOFT International Symposium on Software Testing and Analysis* (ISSTA'17)

> **Y. Kwon**, W. Wang, Y. Zheng, X. Zhang, and D. Xu

[8] **WWW'17** – **J-Force: Forced Execution on JavaScript**, *26th International World Wide Web Conference*

> K. Kim, I. L. Kim, C. H. Kim, **Y. Kwon**, Y. Zheng, X. Zhang, and D. Xu

[7] **NDSS'17** – **A2C: Self Destructing Exploit Executions via Input Perturbation**, *24th Network and Distributed System Security Symposium*

> **Y. Kwon**, B. Saltaformaggio, I. L. Kim, K. H. Lee, X. Zhang, and D. Xu

[6] **OOPSLA'16** – **Apex: Automatic Programming Assignment Error Explanation**, *2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications*

> D. Kim, **Y. Kwon**, P. Liu, I. L. Kim, D. M. Perry, X. Zhang, and G. Rodriguez-Rivera

[5] **FSE'16** – **WebRanz: Web Page Randomization For Better Advertisement Delivery and Web-Bot Prevention**, *24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering*

> W. Wang, Y. Zheng, X. Xing, **Y. Kwon**, X. Zhang, and P. Eugster

[4] **ASPLOS'16** – **LDX: Causality Inference by Lightweight Dual Execution**, *21st International Conference on Architectural Support for Programming Languages and Operating Systems*

> **Y. Kwon**, D. Kim, W. N. Sumner, K. Kim, B. Saltaformaggio, X. Zhang, and D. Xu

[3] **ASPLOS'15** – **Dual Execution for On the Fly Fine Grained Execution Comparison**, *20th International Conference on Architectural Support for Programming Languages and Operating Systems*

> D. Kim, **Y. Kwon**, W. N. Sumner, X. Zhang, and D. Xu

[2] **NDSS'15** – **P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions**, *22nd Network and Distributed System Security Symposium*

> **Y. Kwon**, F. Peng, D. Kim, K. Kim, X. Zhang, D. Xu, V. Yegneswaran, and J. Qian

[1] **ASE'13** – **PIEtrace: Platform Independent Executable Trace**, *28th IEEE/ACM International Conference on Automated Software Engineering*
Best Paper Award (1/317) and **ACM SIGSOFT Distinguished Paper Award** (3/317)

> **Y. Kwon**, X. Zhang, and D. Xu

Journals

[1] **TRACE: Enterprise-Wide Provenance Tracking for Real-Time APT Detection**, H. Irshad, G. Ciocarlie, A. Gehani, V. Yegneswaran, K. H. Lee, J. Patel, S. Jha, **Y. Kwon**, D. Xu, and X. Zhang, *IEEE Transactions on Information Forensics and Security* (IEEE TIFS'21, Impact Factor: 6.211)

Workshops

[2] **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, and J. Qian, *10th USENIX Workshop on Offensive Technologies* (WOOT'16)

[1] **Virtual Machine-based Stack Overflow Detector**, **Y. Kwon** and N. Park, *12th International Workshop on Information Security Applications* (WISA'11)

Book

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

Grants

I have contributed to secure more than **$3.4M** (**My share: $1.6M**) to support my research projects.

[G6] *CAREER: Automated Forensic-in-the-Loop Cyber Defense Infrastructure*, Sole PI, National Science Foundation (NSF), Total $547,574. 9/1/2022–8/31/2027

[G5] *Securing the IoT Infrastructure via Execution Diversification and Active Deception*, Sole PI, Cisco Systems, Total $107,963. 12/31/2021–12/31/2022

[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). 10/01/2019–09/30/2023

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

[G2] *Athena: System Auditing by Learning Causality from Application and System Logs*, with IAI and Purdue University, Office of Naval Research (ONR), Total $900K. (My share: $125K). 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. 03/01/2019–02/28/2021

Teaching

University of Virginia, Assistant Professor *2018 – Current*

- **CS6501**: Cyber Forensics: Covering how to develop next level cyber forensic analysis/reverse engineering techniques.
- **CS6501**: Software Security via Program Analysis: Covering how to understand and secure vulnerable programs via various program analysis/reverse-engineering tools including Pin, Valgrind, LLVM, and disassemblers.
- **CS4401**: Operating Systems: Teaching core concepts and algorithms in modern operating systems including virtual memory, schedulers, threading, etc.

Purdue University, Guest Lecturer *2017*

- **CS503**: Operating Systems: Presented "Program analysis for security applications."
- **CS590**: System Security Research Seminar: Presented "Preventing malicious payloads via input randomization."

Invited talks

Pohang University of Science and Technology (POSTECH), South Korea 2021
- Program Analysis for Security Applications

The World Conference on Information Security Applications (WISA), Jeju Island, South Korea 2021
- Invited Talk: Program Analysis for Security Applications

Soongsil University, Seoul, South Korea 2021
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

Seoul National University, Seoul, South Korea 2021
- Software Security via Data-centric Analysis

Saint Louis University, St. Louis, MO, USA 2021
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

Ulsan National Institute of Science and Technology (UNIST), South Korea 2021
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

Hanyang University, South Korea 2021
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

Korean-American Scientists and Engineering Association (KSEA) 2021
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

Sungkyunkwan University, South Korea 2020
- Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis

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 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

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 Eletronics Technical Seminar (PRIVATE), Samsung Electronics 2009
- Debugging Applications in Windows

SERVICES

REVIEW PANEL:
NSF (National Science Foundation) Proposal Review Panelist (2019, 2022)

PROGRAM CHAIR/CO-CHAIR:
– **Workshop Program Chair**: CheckMATE'21, co-located with the ACM CCS'21
– **Poster Co-chair**: ACSAC'22/21 (Annual Conference on Computer Security Applications)
– **Financial/Communication Co-chair**: KOCSEA'21/20 (Korean Computer Scientists and Engineers Association in America)

PROGRAM COMMITTEE:
Network and Distributed System Security Symposium (NDSS'20/19)
Annual Conference on Computer Security Applications (ACSAC'22/21/20/19/18)
European Symposium on Research in Computer Security (ESORICS'20/21)
Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA'20/21)
ACM ASIA Conference on Computer and Communications Security (ASIACCS'21)
ACM Conference on Data and Application Security and Privacy (CODASPY'21)
International Workshop on Theory and Practice of Provenance (TaPP'17)
IEEE Security & Privacy 2017 Student PC (S&P'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)