Yonghwi Kwon

Assistant Professor, University of Maryland

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

Appointments

University of Maryland, College Park, Maryland, USA
Assistant Professor of Electrical and Computer Engineering (MC^2 and UMIACS) — Aug 2023 - Current

University of Virginia, Charlottesville, Virginia, USA
Assistant Professor of Computer Science — Aug 2018 - July 2023

Education

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

Konkuk University, 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
- Best Student Paper Award, WISA — 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) — 2008 – 2013

Team Awards (Faculty Advisor)

- National Collegiate Cyber Defense Competition — 2020/2019 (1st place)
- Mid-Atlantic Collegiate Cyber Defense Competition — 2023/2019 (1st place), 2022/2020 (2nd place)

Publications

Conferences

– Top-venues (**29**): S&P×**5**, NDSS×**5**, CCS×**3**, ICSE/FSE/ASE×**8**, ASPLOS×**3**, OOPSLA×**2**, WWW×**3**.

	2012∼2018 (Ph.D.)	2019-2020	2021-2022	2023-
Security/ System (16)	NDSS [2, 7, 12], ASPLOS [3, 4]	CCS [19], S&P [20, 21]	NDSS [22], CCS [26, 34], S&P [23, 31]	S&P [35], NDSS [37], ASPLOS [38]
PL/SE (10)	ASE [🏆1, 10], FSE [5], OOPSLA [6]	ICSE [16], OOPSLA [🏆17]	FSE [27], ASE [28], ICSE [32]	ICSE [36]
Web (3)	WWW [13, 8]		WWW [24]	

[38] **ASPLOS'24** – **FreePart: Hardening Data Processing Software via Framework-based Partitioning and Isolation**, *29th International Conference on Architectural Support for Programming Languages and Operating Systems*.

> Ali Ahad, Gang Wang, Chung Hwan Kim, Suman Jana, Zhiqiang Lin, and **Yonghwi Kwon**

[37] **NDSS'23** – **SynthDB: Synthesizing Database via Program Analysis for Security Testing of Web Applications**, *30th Network and Distributed System Security Symposium*.

> An Chen, JiHo Lee, Basanta Chaulagain, **Yonghwi Kwon**, and Kyu Hyung Lee

[36] **ICSE'23** – **BFTDetector: Automatic Detection of Business Flow Tampering for Digital Content Service**, *45th International Conference on Software Engineering*.

> I Luk Kim, Weihang Wang, **Yonghwi Kwon**, and Xiangyu Zhang

[35] **S&P'23** – **PyFET: Forensically Equivalent Transformation for Python Binary Decompilation**, *44th IEEE Symposium on Security and Privacy*.

> Ali Ahad, Chijung Jung, Ammar Askar, Doowon Kim, Taesoo Kim, and **Yonghwi Kwon**

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

> Seulbae Kim, Major Liu, Junghwan Rhee, Yuseok Jeon, **Yonghwi Kwon**, and Chung Hwan Kim

[33] WISA'22 – **Dazzle-attack: Anti-Forensic Server-side Attack via Fail-free Dynamic State Machine**, *23rd World Conference on Information Security Applications*.
🏆 **Best Student Paper Award**

> Bora Lee*, Kyungchan Lim*, JiHo Lee, Chijung Jung, Doowon Kim, Kyu Hyung Lee, Haehyun Cho, and **Yonghwi Kwon** (*: co-first authors)

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

Chijung Jung, Doowon Kim, An Chen, Weihang Wang, Yunhui Zheng, Kyu Hyung Lee, and **Yonghwi Kwon**

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

Chijung Jung, Ali Ahad, Yuseok Jeon, and **Yonghwi Kwon**

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

Honggoo Kang, **Yonghwi Kwon**, Sangjin Lee, and Hyungjoon Koo

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

Chijung Jung, Doowon Kim, Weihang Wang, Yunhui Zheng, Kyu Hyung Lee, and **Yonghwi Kwon**

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

Alan Romano, Xinyue Liu, **Yonghwi Kwon**, and Weihang Wang

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

Chijung Jung, Ali Ahad, Jinho Jung, Sebastian Elbaum, and **Yonghwi Kwon**

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

Meng Wang, Chijung Jung, Ali Ahad, and **Yonghwi Kwon**

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

Doowon Kim, Haehyun Cho, **Yonghwi Kwon**, Adam Doupe, Sooel Son, Gail-Joon Ahn, and Tudor Dumitras

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

Hyunwoo Lee, Doowon Kim, and **Yonghwi 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*.

Zhuo Zhang, Yapeng Ye, Wei You, Guanhong Tao, Wen-chuan Lee, **Yonghwi Kwon**, Yousra Aafer, and Xiangyu Zhang

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

Yonghwi Kwon, Weihang Wang, Jinho Jung, Kyu Hyung Lee, and Roberto Perdisci

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

Ranjita Pai Kasturi, Yiting Sun, Ruian Duian, Omar Alrawi, Ehsan Asdar, Victor Zhu, **Yonghwi Kwon**, and Brendan Saltaformaggio

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

Wei You, Zhuo Zhang, **Yonghwi Kwon**, Yousra Aafer, Fei Peng, Yu Shi, Carson Harmon, and Xiangyu Zhang

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

Abbas Naderi-Afooshteh, **Yonghwi Kwon**, Anh Nguyen-Tuong, Ali Razmjoo-Qalaei, Mohammad-Reza Zamiri-Gourabi, and Jack W. Davidson

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

Abbas Naderi-Afooshteh, **Yonghwi Kwon**, Anh Nguyen-Tuong, Mandana Bagheri, and Jack 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

> Zhuo Zhang, Wei You, Guanhong Tao, Guannan Wei, **Yonghwi Kwon**, and Xiangyu Zhang

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

> Kenneth Adam Miller, **Yonghwi Kwon**, Yi Sun, Zhuo Zhang, Xiangyu Zhang, and Zhiqiang Lin

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

> Fei Wang, **Yonghwi Kwon**, Shiqing Ma, Xiangyu Zhang, and Dongyan Xu

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

> Shiqing Ma, Juan Zhai, **Yonghwi Kwon**, Kyu Hyung Lee, Xiangyu Zhang, Gabriela Ciocarlie, Ashish Gehani, Vinod Yegneswaran, Dongyan Xu, and Somesh Jha

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

> I Luk Kim, Weihang Wang, **Yonghwi Kwon**, Yunhui Zheng, Yousra Aafer, Weijie Meng, and Xiangyu Zhang

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

> **Yonghwi Kwon**, Fei Wang, Weihang Wang, Kyu Hyung Lee, Wen-Chuan Lee, Shiqing Ma, Xiangyu Zhang, Dongyan Xu, Somesh Jha, Gabriela Ciocarlie, Ashish Gehani, and Vinod Yegneswaran

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

> Taegyu Kim, Chung Hwan Kim, Hongjun Choi, **Yonghwi Kwon**, Brendan Saltaformaggio, Xiangyu Zhang, and Dongyan Xu

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

> Weihang Wang, **Yonghwi Kwon**, Yunhui Zheng, Yousra Aafer, I Luk Kim, Wen-Chuan Lee, Yingqi Liu, Weijie Meng, Xiangyu Zhang, and Patrick Eugster

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

> **Yonghwi Kwon**, Weihang Wang, Yunhui Zheng, Xiangyu Zhang, and Dongyan Xu

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

> Kyungtae Kim, I Luk Kim, Chung Hwan Kim, **Yonghwi Kwon**, Yunhui Zheng, Xiangyu Zhang, and Dongyan Xu

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

> **Yonghwi Kwon**, Brendan Saltaformaggio, I Luk Kim, Kyu Hyung Lee, Xiangyu Zhang, and Dongyan Xu

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

> Dohyeong Kim, **Yonghwi Kwon**, Peng Liu, I Luk Kim, David Mitchel Perry, Xiangyu Zhang, and Gustavo 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.*

> Weihang Wang, Yunhui Zheng, Xinyu Xing, **Yonghwi Kwon**, Xiangyu Zhang, and Patrick Eugster

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

> **Yonghwi Kwon**, Dohyeong Kim, William Nick Sumner, Kyungtae Kim, Brendan Saltaformaggio, Xiangyu Zhang, and Dongyan 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.*

> Dohyeong Kim, **Yonghwi Kwon**, William Nick Sumner, Xiangyu Zhang, and Dongyan 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*.

> **Yonghwi Kwon**, Fei Peng, Dohyeong Kim, Kyungtae Kim, Xiangyu Zhang, Dongyan Xu, Vinod Yegneswaran, and John 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)

> **Yonghwi Kwon**, Xiangyu Zhang, and Dongyan Xu

Journals

[1] **TRACE: Enterprise-Wide Provenance Tracking for Real-Time APT Detection**, H. Irshad, Gabriela Ciocarlie, Ashish Gehani, Vinod Yegneswaran, Kyu Hyung Lee, Jignesh Patel, Somesh Jha, **Yonghwi Kwon**, Dongyan Xu, and Xiangyu Zhang, *IEEE Transactions on Information Forensics and Security* (IEEE TIFS'21, Impact Factor: 6.211).

Workshops and Posters

[3] **Poster: Automated Discovery of Sensor Spoofing Attacks on Robotic Vehicles**, Kyeongseok Yang*, Sudharssan Mohan* (*: co-first authors), **Yonghwi Kwon**, Heejo Lee, and Chung Hwan Kim, *29th ACM Conference on Computer and Communications Security* (CCS'22).
[2] **Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic**, Brendan Saltaformaggio, Hongjun Choi, Kristen Johnson, **Yonghwi Kwon**, Qi Zhang, Xiangyu Zhang, Dongyan Xu, and John Qian, *10th USENIX Workshop on Offensive Technologies* (WOOT'16).
[1] **Virtual Machine-based Stack Overflow Detector**, **Yonghwi Kwon** and Neungsoo Park, *12th International Workshop on Information Security Applications* (WISA'11).

Book

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

Grants

I have contributed to secure more than **$6.7M** (**My share: $1.9M**) to support my research projects.
[G9] *Attack Investigation via Telemetry Analysis for Cloud Services*, PI, Sandia National Laboratories, My share: $44K. 1/1/2023–9/30/2023
[G8] *Developing Anti-Reverse Engineering Techniques for Weapon Systems*, PI (Sub-contract), LIG, My share: $250K. 10/1/2023–9/30/2027
[G7] *Collaborative: PPoSS: Co-designing Hardware, Software, and Algorithms to Enable Extreme-Scale Machine Learning Systems*, Senior Personnel, National Science Foundation (NSF), Total $3M. 10/1/2022–9/30/2027
[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.

Invited talks

Understanding and Securing Software Systems in Emerging Systems
- Hanyang University, South Korea Aug, 2023

- University of Texas at Dallas (UTD), Dallas, TX, USA — April, 2023
- Korea Advanced Institute of Science and Technology (KAIST), South Korea — Nov, 2022
- Soongsil University, South Korea — Oct, 2022
- Sungkyunkwan University, South Korea — Oct, 2022

Program Analysis for Security Applications
- Pohang University of Science and Technology (POSTECH), South Korea — Aug, 2021
- The World Conference on Information Security Applications (WISA), Jeju Island, South Korea — July, 2021

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

Stitching and Reconstructing Cyber Forensic Evidence via Program Analysis
- Soongsil University, South Korea — April, 2021
- Saint Louis University, St. Louis, MO, USA — March, 2021
- Ulsan National Institute of Science and Technology (UNIST), South Korea — March, 2021
- Korean-American Scientists and Engineering Association (KSEA) — Feb, 2021
- Hanyang University, South Korea — Jan, 2021
- Sungkyunkwan University, South Korea — Sep, 2020

Combatting APTs via Input Perturbation
- Pohang University of Science and Technology (POSTECH), South Korea — June, 2019
- Konkuk University, South Korea — June, 2019
- Sungkyunkwan University, South Korea — June, 2019
- Korea Advanced Institute of Science and Technology (KAIST), South Korea — June, 2019
- KOCSEA Technical Symposium — Nov, 2018

A2C: Self Destructing Exploit Executions via Input Perturbation
- CERIAS Security Seminar, Purdue University — Feb, 2017

P2C: Understanding Output Data Files via On-the-Fly Transformation
- CERIAS Security Seminar, Purdue University — Sep, 2015

Migration to the Visual Studio 2010
- Microsoft Technical Seminar, Microsoft Korea — April, 2011

Effective Windows Programming
- Microsoft Technical Seminar, Microsoft Korea — April, 2010

Advanced topics in Windows Programming
- Microsoft Technical Seminar, Microsoft Korea — March, 2009

Debugging Applications in Windows
- Samsung Eletronics Technical Seminar (INTERNAL), Samsung Electronics — Feb, 2009

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)