Yonghwi Kwon (권용휘), John Knight
Career Enhancement Assistant Professor,
Department of Computer Science, University of Virginia
Email: yongkwon@virginia.edu Site: http://yongkwon.info

Computer Science at the University of Virginia 에서 박사 (석박 통합) 과정 (2019 가을학기)을 하고자 하는 학생들을 모집합니다.

Computer Science at the University of Virginia (UVa). The University of Virginia 는 미국 초대 대통령 Thomas Jefferson 이 설립하였으며, Computer Science Department 는 US News Computer Science Ranking 30 위에 랭크 되어 있는 (2018 년 기준) 세계 최고 수준의 연구를 진행하고 있습니다.

Brief Bio. 저는 2018 년 가을에 Tenure-track Assistant Professor 로 University of Virginia 에 부임하였습니다. 시스템 및 소프트웨어 보안을 연구하고 있으며, 특히 나날이 지능적이고 복잡해져가는 사이버 공격/익스플로잇 (Cyber-attacks and exploits)을 다양한 프로그램 자동 분석 기술을 통하여 (Automated Program Analysis) 분석, 탐지, 방지 (Analysis/Detection/Prevention) 하는 연구를 하고 있습니다.

Financial Support. The University of Virginia 의 Computer Science Department 에서는 입학하는 모든 학생들에게 1 년 동안의 재정 지원 (등록금, 생활비, 학술 활동 지원 (e.g., 학술대회 참석, 장비 구입)) 을 해주고 있습니다. 2 년 이후로는 지도 교수가 Research Assistant (RA) 로 고용하여 재정 지원을 해주거나 학과에서 Teaching Assistant (TA) 로 고용하여 재정지원 (등록금 및 생활비) 을 해주도록 되어 있습니다. 저와 함께 일하게 되면 2 년 이후부터는 연구 성과에 따라 졸업시까지 RA/TA assistantship 을 지원받을 수 있습니다.

Requirements. 관심있는 학생들은 영어 점수 (TOEFL and GRE), 이력서 (CV/Resume), 성적표 (Transcript), 연구 실적 (발표한 논문 또는 포스터) 를 제게 보내주세요.

How to Apply? 2019 가을 학기 입학을 위해서 학과 웹페이지에서 지원 할 수 있습니다. 지원시에 꼭 제 이름을 지원서에 명시하여 주세요. 그리고 지원 후에 메일을 하나 주시면 제가 어플리케이션을 확인해 보도록 하겠습니다. 지원을 해야할지 말아야 할지 잘 모르겠다면, 저에게 개인적으로 메일을 주시면 하고자 하는 연구와 지원 적절성을 상담 해 줄 수 있습니다.

Research Topics. 저희 연구실의 연구 방향은, 프로그램 분석을 통한 사이버 공격 방어와, 공격에 취약한 프로그램들 자동으로 고쳐주는 시스템을 만드는데 집중하고 있습니다. 특히, 최근 큰 화제거리가 되고 있는 취약한 IoT (Internet of Things) 기기들을 분석하고 보완하는 부분과, 나날이 복잡해지고 지능적으로 진화하고 있는 APT (Advanced Persistent Threat (e.g., Stuxnet)) 을 분석하고 방어하는 연구를 진행하고 있습니다.

예제 연구 프로젝트:

1. Analysis of Advanced Persistent Threat
   최근 사이버 공격(특히 Advanced Persisten Threat)들의 특징 중 하나는, 오랜 시간에 걸쳐 발생하고 (e.g., Stuxnet), 여러 프로그램과 취약점을 통하여 퍼지기 때문에, 분석이 복잡하고 어렵습니다. 이 프로젝트의 목적은 여러 복잡한 프로그램 간의 Information Flow 를 추적하여 Advanced Cyber attack 경로를 추척하는데에 있습니다. (참고자료: MCI in NDSS'18 [1], LDX in ASPLOS'16 [2])
2. Malicious Payload Injection Prevention
   원격으로 프로그램을 공격하는 과정에서 가장 중요한 부분 중 하나는 Malicious Payload (e.g., Exploit)를 프로그램에 주입하고 프로그램의 취약점을 공격하여 해당 Payload 를 실행하는 것입니다. 이 프로젝트의 목적은 그러한 원격 프로그램 공격을 원천적으로 차단하는데에 있습니다. Malicious Payload 가 프로그램에 주입될 때, Randomization 기법을 사용하여 이를 무력화 시키거나, Malicious Payload 가 실행될 때를 탐지하여 이를 저지하거나 실행을 방지하는것이 이 프로젝트의 목적입니다. (참고자료 A2C in NDSS'17 [3])
3. Cross-Platform Binary Analysis
   프로그램을 분석할 때 가장 어려운 점은 프로그램 분석 도구 (e.g., Debuggers)의 부재입니다. 특히 이러한 문제는 새로운 플랫폼이나 (e.g. IoT Platforms) 새로운 하드웨어에 동작하는 프로그램을 작성할때 더 두드러집니다. 이를 해결하기 위해 프로그램 바이너리 (Binary)를 각 플랫폼에 구애받지 않는 형태로(e.g., Intermediate Representation) 변형시키거나, 플랫폼 독립적인 (Platform Independent) 프로그램 분석 도구를 만드는것이 이 프로젝트의 목적입니다. (참고 자료: PIEtrace in ASE'13 [4], CPR in ISSTA'17 [5])

[1] "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 NDSS'18 (25th Network and Distributed System Security Symposium)
[2] "LDX: Causality Inference by Lightweight Dual Execution," Y. Kwon, D. Kim, W. N. Sumner, K. Kim, B. Saltaformaggio, X. Zhang, and D. Xu, In ASPLOS'16 (21st International Conference on Architectural Support for Programming Languages and Operating Systems)
[3] "A2C: Self Destructing Exploit Executions via Input Perturbation," Y. Kwon, B. Saltaformaggio, I. L. Kim, K. H. Lee, X. Zhang, and D. Xu, In NDSS'17 (24th Network and Distributed System Security Symposium)
[4] "PIEtrace: Platform Independent Executable Trace," Y. Kwon, X. Zhang, and D. Xu, In ASE'13 (28th IEEE/ACM International Conference on Automated Software Engineering)
[5] "CPR: Cross Platform Binary Code Reuse via Platform Independent Trace Program," Y. Kwon, W. Wang, Y. Zheng, X. Zhang, and D. Xu, In ISSTA'17 (26th ACM SIGSOFT International Symposium on Software Testing and Analysis)