Hong, Sanghyun *C.V.*

CONTACT INFORMATION

Maryland Cybersecurity Center (MC2)
3400, A.V. Williams Bldg.
College Park, MD 20732

Work: +1 (301) 771-1475
E-mail: shhong@cs.umd.edu
Web: www.sanghyun-hong.com

EDUCATION

University of Maryland, College Park — College Park, MD
Ph.D. student in Computer Science — **Sep. 2015 - Present**
- Academic advisor: Dr. Tudor Dumitraș

M.S. in Computer Science — **Sep. 2015 - Dec.2017**
- Academic advisor: Dr. Tudor Dumitraș
- Scholarly paper: *Peek-a-Boo: Inferring Program Behaviors in a Virtualized Infrastructure without Introspection* [J.1].

Seoul National University — Seoul, South Korea
B.S. in Electrical and Computer Engineering (magna cum laude) — **Mar. 2007 - Feb. 2015**
- Academic adviser: Dr. Seongsoo Hong
- Thesis: *A Power Saving Mechanism for the Smartphone Modem via Application-based Packet Piggybacking*

SUMMARY

Publications:
- In Security: USENIX'19 (1), HotCloud'18 (1), COSE'18 (1),
- In Machine Learning: ICML'19 (1), BigData'17 (1), ACM HT'17 (1), NeurIPS'16 Workshop (1)

CONFERENCE PUBLICATIONS

C.1 **S. Hong**, P. Frigo, Y. Kaya, C. Giuffrida and T. Dumitraș, "Terminal Brain Damage: Exposing the Graceless Degradation in Deep Neural Networks Under Hardware Fault Attacks", *USENIX Security*, 2019. [Paper]

C.2 Y. Kaya, **S. Hong**, and T. Dumitraș, "Shallow-Deep Networks: Understanding and Mitigating Network Overthinking", *36th International Conference on Machine Learning (ICML)*, 2019. [Paper] [Website]

C.3 **S. Hong**, S. Kwon, H. Kang, and N. Park, "PAGE: Pattern-Query Answering via Knowledge Graph Embedding". *International Conference on Big Data*, 2018. [Paper]

C.4 H. Kang, **S. Hong**, K. Lee, N. Park, and S. Kwon, "On Integrating Knowledge Graph Embeddings into SPARQL Query Answering", *International Conference on Web Services*, 2018. [Work in Progress Paper]

C.5 **S. Hong**, T. Chakraborty, S. Ahn, G. Husari, and N. Park, "SENA: Preserving Social Structure for Network Embedding", *In Proceedings of the ACM Conference on Hypertext and Social Media (Hypertext)*, 2017. [Paper]

JOURNAL PUBLICATIONS

J.1 **S. Hong**, A. Nicolae, A. Srivastava, and T. Dumitraș, "Peek-a-Boo: Inferring Program Behaviors in a Virtualized Infrastructure without Introspection", *Computer & Security (COSE)*, 2018. [Paper]

PRE-PRINTS

P.1 **S. Hong**, *M. Davinroy, Y. Kaya, S. Locke, I Rackow, K. Kulda, D. Dachman-Soled and T. Dumitraș, "Security Analysis of Deep Neural Networks Operating in the Presence of Cache Side-Channel Attacks", 2018. [Paper] [Code]

WORKSHOP PAPERS

W.1 **S. Hong**, A. Srivastava, W. Shambrook, and T. Dumitraș. "Go Serverless: Securing Cloud via Serverless Design Patterns", *2018 USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 18)*, 2018. [Paper]

W.2 R. Stevens, O. Suciu, A. Ruef, **S. Hong**, M. Hicks, and T. Dumitraș, "Summoning Demons: The Pursuit of Exploitable Bugs in Machine Learning", *Neural Information Processing Systems (NeurIPS) Workshop on Crowdsourcing and Machine Learning*, 2016. [Paper]

*Equal contribution

Poster Presentations

P.1 **S. Hong**, T.H. Kim, T. Dumitraș, and J. Choi. "Poster: On the Feasibility of Training Neural Networks with Visibly Watermarked Dataset." *NDSS Symposium*, 2019. (Poster) [Paper]

Professional Experience

Frame.io — New York, NY, USA
Security Research Intern — **Nov. 2017 - May. 2018**

- Implemented a threat-intelligence system that monitors threat indicators and detects attacks or unauthorized accesses to our application infrastructures running on the cloud.
  - Identified suspicious actions against our infrastructure such as port scanning, brute force attacks (ssh/login), NTP DDoS attacks, IPv4 address scanning, and anonymous accesses via Tor.
  - Identified and fixed deviations from the best security practices in the cloud, e.g., misconfiguration of access policies, privilege escalation actions by an account, etc.
- Mentor: Abhinav Srivastava [Google Scholar][LinkedIn]

Openwise Inc. (Mobile Solution Start-up) — Seoul, South Korea
Co-founder and Chief Technology Officer — **Dec. 2011 - Aug. 2014**

- Developed a light-weight real-time operating system (RTOS) for Samsung's new mobile healthcare devices that provide various wireless connectivity to other Samsung's electronics and appliances. It was highly commended at the Mobile World Congress (MWC) 2014.
- Found a lagging issue in word searching at our English-dictionary Android application and resolved the issue by improving the searching time from 1 second to 0.3 seconds by creating a novel lookup table in the SQLite database of over thousand words.
- Shortened the development time of organizing the graphical interface for Android applications by introducing a new way of Android UI composition that supports all sizes of Android device screens with only 1-specific-sized design architecture.

MBridge Systems Inc. (Middleware and Mobile Software Developer) — Seoul, South Korea
Lead Researcher, R&D Department — **Dec. 2010 - Dec. 2013**

- Finished the Android OS upgrade project (GingerBread to IceCreamSandwitch) by resolving all the audio/video architecture issues with a team comprised of 3 software developers.
- Implemented the MHL and HDMI close caption (CC) feature in Android OS with expertise in the video framework architecture of the OS. The project term dramatically shortened by implementing the feature in 3.5 months, which had been expected 5 months.
- Developed software solution for Infrared Ray (IR) touchscreen for Linux which consists of new device drivers and X-window drivers supporting multi-touch for the 1st time in Korea.

Services

2019: External reviewer at the USENIX, CCS, IEEE S&P, and RAID.
2018: External reviewer at the NDSS and IEEE S&P.
2018: External reviewer at the USENIX, CCS, and RAID.
2017: Chair, National Math and Science Competition (NMSC), Washington Metro Chapter.
2017: External reviewer at the USENIX, CCS, NDSS, and IEEE S&P.
2016: External reviewer at the USENIX.

Awards

2018: 1st/3rd Place at the Research Competition for Korean Graduate Students
2017: KSEA-KUSCO Scholarships for Korean Graduate Students in the United States
2016: Summer Research Fellowship from the Department of Computer Science at UMD
2015: 2-year Dean's Fellowship from UMD for outstanding academic achievement
2015: 3-year scholarship from Seoul National University Alumni Association (SNUAA)
2015: Full 2-year Graduate Teaching Assistantship from UMD for academic excellence

Invited Talks

T.1 **S. Hong**, "Can Machine Learning be Secure and Trustworthy in the Presence of Micro-architectural vulnerabilities?", *Yonsei University, South Korea*, Jan., 2019.

T.2 **S. Hong**, "The Matrix: Toward More Safe & Secure Environment for Cloud-Infrastructures", *UMD KGSA-KESA Biannual Symposium*, Nov., 2015. **(Best Presentation Award)**

References

References available upon requests