Jonghoon Kwon

Ph.D.
Div. of Computer & Communication Eng., Korea University
Date of Birth: Sep. 1, 1981
Office: +82-2-3290-3638
Fax: +82-2-3290-3638
Mobile: +82-10-2576-4993
Email: jonghoonkwon@gmail.com
Citizenship: Republic of Korea

Education

Ph.D. Computer Science, Korea University, 2016.

DISSERTATION: A Scalable Botnet Countermeasures for Large-scale DNS Traffic
Committee: Heejo Lee, Saewoong Bahk, Hyogon Kim, Hoh Peter In, Junbeom Hur,

M.S. Computer Science, Korea University, 2010.

B.S. Computer Science, Korea University, 2007.

Research Fields

Network attack detection and prevention

Malware detection in network

Software Defined Networking for network security

Privacy issues on social network services

Other topics on network security

Industrial Experiences

Research Intern, Microsoft Research Asia, Beijing (Media Computing Group, Sep. 2012 ∼ Mar. 2013)

Research

WORK IN PROGRESS

Malicious document detection, with Jongmin Kim, Seokmyung Hong and Prof. Heejo Lee (2014∼)

Finding software vulnerabilities, with Hongzhe Li and Prof. Heejo Lee (2011∼)

Malware detection by analyzing semantic behavior graph, with Prof. Heejo Lee (2010∼)

Botnet detection by analyzing DNS query pattern, with Jehyun Lee Lee and Prof. Heejo Lee (2009∼)

Botnet detection using the user interaction property in the host machine, with Prof. Heejo Lee (2008∼2009)

Spyware detection using the bogus event generation in the host machine, with Prof. Heejo Lee (2007∼2008)

International Journal Papers

Jonghoon Kwon, Jehyun Lee, Heejo Lee, Adrian Perrig, "PsyBoG: A scalable botnet detection method for large-scale DNS traffic", Computer Networks, Vol. 97, pp. 48-73, Mar. 14. 2016.

Hongzhe Li, Hyuckmin Kwon, Jonghoon Kwon, Heejo Lee, "CLORIFI: Software Vulnerability Discovery using Code Clone Verification", Concurrency and Computation: Practice and Experience, Vol. 28, No. 6, pp. 1900-1917, Apr. 14. 2015.

Jonghoon Kwon, Dongwon Seo, Minjin Kwon, Heejo Lee, Adrian Perrig, Hyogon Kim, "An incrementally deployable anti-spoofing mechanism for software-defined networks", Computer Communications, Vol. 64, pp. 1-20, Jun. 15. 2015.

International Conference Papers

Hongzhe Li, Hyuckmin Kwon, Jonghoon Kwon, Heejo Lee, "A Scalable Approach for Vulnerability Discovery Based on Security Patches", Applications and Techniques in Information Security (ATIS 2014), pp. 109-122, Nov. 28. 2014. (Best Paper Award)

Jonghoon Kwon, Jihwan Jeong, Jehyun Lee, Heejo Lee, "DroidGraph: Discovering Android Malware by Analyzing Semantic Behavior", IEEE Conf. on Communications and Network Security (CNS), pp. 345-346, Oct. 30. 2014.

Jonghoon Kwon, Jeongsik Kim, Jehyun Lee, Heejo Lee, Adrian Perrig, "PsyBoG: Power Spectral Density Analysis for Detecting Botnet Groups", The 9th IEEE Conference on Malicious and Unwanted Software (IEEE MALWARE 2014), pp. 85-92, Oct. 29. 2014.

Jihwan Jeong, Dongwon Seo, Chanyoung Lee, Jonghoon Kwon, Heejo Lee, John Milburn, "MysteryChecker: Unpredictable Attestation to Detect Repackaged Malicious Applications in Android", The 9th IEEE Conference on Malicious and Unwanted Software (IEEE MALWARE 2014), pp. 50-57, Oct. 29. 2014.Oct. 29. 2014.

Jonghoon Kwon, Heejo Lee, "BinGraph: Discovering Mutant Malware using Hierarchical Semantic Signature", The 7th IEEE Conference on Malicious and Unwanted Software (IEEE MALWARE 2012), Oct. 19. 2012.

Jonghoon Kwon, Jehyun Lee, Heejo Lee, "Hidden Bot Detection by Tracing Non-human Generated Traffic at the Zombie Host", The 7th Information Security Practice and Experience Conference (ISPEC), May. 30. 2011.

Jehyun Lee, Jonghoon Kwon, Hyo-Jeong Shin, Heejo Lee, "Tracking Multiple C&C Botnets by Analyzing DNS Traffic", Workshop on Secure Network Protocols(NPSEC), pp. 67-72, Oct. 5. 2010.

Jeheon Han, Jonghoon Kwon, Heejo Lee, "HoneyID : Unveiling Hidden Spywares by Generating Bogus Events", IFIP Int'l Information Security Conference (IFIP SEC), Vol. 278, pp. 669-673, Sep. 9. 2008.

Domestic Journal Papers

Jonghoon Kwon, Jehyun Lee, Hyunchul Jeong, Heejo Lee, "Metamorphic Malware Detection using Subgraph Matching", Journal of Korean Institute of Information Security & Cryptology, Vol. 21, No. 2, pp. 37-47, Apr. 2011.

Jonghoon Kwon, Chaetae Im, Hyunsang Choi, SeungGoo Ji, JooHyung Oh, HyunCheol Jeong, Heejo Lee, "Cooperative Architecture for Botnet Detection and Management", Journal of Korea Institute of Information Security & Cryptology, Vol. 19, No. 3, Jun. 2009.

Domestic Conference Papers

Jonghoon Kwon, Chatae Im, Hyunsang Choi, Hyunchul Jeong, Heejo Lee, "Cooperative Architecture for Botnet Detection and Management", KIPS, Vol. 15, No. 2, pp. 1517-1520, Nov. 14. 2008.

Yuseung Kim, Hyunsang Choi, Inhwan Kim, Jonghoon Kwon, Heejo Lee, "An Analysis on Botnet Traffic", KIPS, Vol. 15, No. 2, pp. 1429-1432, Nov. 14. 2008.

Patents

Heejo Lee, Jonghoon Kwon, Jongmin Kim, "SYSTEM AND METHOD FOR DETECTING MALICIOUS CODE IN DOCUMENT FILES", Domestic, Registration, 10-1641295, Jul. 14. 2016.

Heejo Lee, Hongzhe Li, Jonghoon Kwon, Hyuckmin Kwon, "SOFTWARE VULNERABILITY ANALYSIS METHOD AND DEVICE", International, Application, 14/978,300, Dec. 22. 2015.

Heejo Lee, Hongzhe Li, Hyukmin Kwon, Jonghoon Kwon, "ANALYSIS DEVICE AND METHOD FOR SOFTWARE SECURITY", Domestic, Registration, 10-1568224, Nov. 5. 2015.

Heejo Lee, Jonghoon Kwon, Jusuk Lee, Jehyun Lee, Taebum Kim, Hyun-Cheol Jeong, Chaetae Im, Seung-Goo Ji, Joohyung Oh, Dongwan Kang, "SYSTEM AND METHOD FOR DETECTING MALICIOUS CODE", Domestic, Registration, 10-1230271, Jan. 31. 2013.

Heejo Lee, Jonghoon Kwon, Jehyun Lee, "METHOD AND APPARATUS FOR DETECTING BOT PROCESS", Domestic, Registration, 10-1158464, Jun. 14. 2012.

Heejo Lee, Jehyun Lee, Jonghoon Kwon, "Method and System for Detecting Botnets using Domain Name Service Queries", Domestic, Registration, 10-1182793, Sep. 13. 2012.

Technical Reports

Hyunsang Choi, Jonghoon Kwon, Inhwan Kim, Heejo Lee, "Botnet Attacks using Malicious Codes", Business and Computer (KyungCom), pp. 144-147, Jul. 2008.

Research Projects

Research on Exploit Code Detection for Hangul Word Processor supported by Softforum Inc.(2013∼).

A Study of a Scalable Vulnerability Discovery Approach in Real World Source Code supported by Microsoft Research Asia (2013∼2014).

Research on DDoS Attack Type Analysis and Maximum Capacity Measurement Method supported by Electronics and Telecommunications Research Institute (2012).

Automated Vulnerability Analysis using Machine Learning supported by Microsoft Research Asia (2011∼2012).

Developing A Method for DDoS Defense Evaluation supported by SK InforSec Inc. (2011).

Large-scale Botnet Detection using Email Log Mining and DNS Traffic Analysis supported by National Research Foundation (2009∼2012).

Developing A Method for Discovering DDoS Attack Origins supported by Korea Information Security Agency (2009).

The Development of Active Detection and Response Technology against Botnet supported by the IT R&D program of MKE/IITA (2008∼2011).

Study on Hacking and Virus Response Technology supported by the Ministry of Knowledge Economy, Korea, under the ITRC (Information Technology Research Center) support program (2007∼2011).

Miscellaneous

Computer Skills

Operating system: Windows, and Ubuntu Linux

Programming Language: C, C++, C#

Skills on Tools: Machine learning tool (Weka), Software-defined networking simulator (Mininet), Network simulator (Qualnet), Reversing tool (OllyDbg), Graph processing (Pajek), LaTeX, GNU plot, Virtual machines, Wireshark

Language Skills

English (Intermediate), Korean (Native)

References

Heejo Lee, Ph.D.
Professor
Div. of Computer & Communication Eng., Korea University, Seoul, Korea
heejo@korea.ac.kr

Hyogon Kim, Ph.D.
Professor
Div. of Computer & Communication Eng., Korea University, Seoul, Korea
hyogon@korea.ac.kr

Bin Zhu, Ph.D.
Researcher
Microsoft Research Asia, Beijing, China
binzhu@microsoft.com

Jehyun Lee, Ph.D.
Senior Researcher
Cyber Security Research Center, Korea Advanced Institute of Science and Technology, Deajeon, Korea
jehyunlee@kaist.ac.kr