

Hyunsang Choi



Ph.D.
Div. of Computer & Communication Eng., Korea University
Date of Birth: August 23, 1981
Office: +82-2-3290-3638
Fax: +82-2-3290-3638
Mobile: +82-10-6766-7656
Email: realchs@korea.ac.kr
Citizenship: Republic of Korea

Education

Ph.D. Computer Science, Korea University, 2012.

M.S. Computer Science, Korea University, 2006.

B.S. Computer Science, Korea University, 2004.

Industrial Experiences

Research Intern, Microsoft Research Asia, Beijing (Media Computing Group, Aug. 2009 - Apr. 2010)

Research

WORK IN PROGRESS

Finding software vulnerabilities and developing exploits, with Prof. Heejo Lee (2011~)

3G network specified DDoS and smartphone malware detection, with Prof. Heejo Lee (2010~)

Malicious URL detection and categorization, with Bin B. Zhu at Microsoft Research Asia (2009~)

Botnet visualization using DNS traffic, with Inhwan Kim and Prof. Heejo Lee (2008~)

Botnet detection using the group activity property, with Prof. Hyogon Kim and Prof. Heejo Lee (2006~)

Attack visualization on parallel coordinates, with Prof. Hyogon Kim and Prof. Heejo Lee (2004~)

INTERNATIONAL JOURNAL PAPERS

Hyunsang Choi, Heejo Lee, "Identifying Botnets by Capturing Group Activities in DNS Traffic", *Computers Networks*, Vol. 56, No. 1, pp. 20-33 Jan. 2012.

Hyunsang Choi, Heejo Lee, Hyogon Kim, "Fast Detection and Visualization of Network Attacks on Parallel Coordinates", *Computers & Security*, Vol. 28, No. 5, pp. 276-288, Jul. 2009.

DOMESTIC JOURNAL PAPERS

Jong Hoon 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.

Yuseung Kim, Hyunsang Choi, Hyunchul Jeong, Heejo Lee, "Comparison of Characteristics between IRC Botnet and P2P Botnet by Traffic Analysis", Journal of Korean Institute of Information Technology, Vol. 7, No. 1, pp. 220-226, Feb. 2009.

INTERNATIONAL CONFERENCE PAPERS

Hyunsang Choi, Bin B. Zhu, Heejo Lee, "Detecting Malicious Web Links and Identifying Their Attack Types", USENIX Int'l Conf. on Web Application Development (WebApps), Jun. 15. 2011.

Tae Hwan Oh, Shinyoung Lim, Young B. Choi, Kwang-Roh Park, Heejo Lee, Hyunsang Choi, "State of the Art of Network Security Perspectives in Cloud Computing", Proc. of Int'l Conf. on Security-enriched Urban Computing and Smart Grid (SUComS), Sep. 2010.

Inhwan Kim, Hyunsang Choi, Heejo Lee, "BotXrayer : Exposing Botnets by Visualizing DNS Traffic", Proc. of Int'l Conf. on Internet (ICONI), Dec. 2009.

Hyunsang Choi, Heejo Lee, Hyogon Kim, "BotGAD: Detecting Botnets by Capturing Group Activities in Network Traffic", Proc. of ACM 4th Int'l Conf. on COMMunication System softWARE and middlewaRE (COMSWARE), Jun. 2009.

Inhwan Kim, Hyunsang Choi, Heejo Lee, "Botnet Visualization using DNS Traffic", Proc. of Workshop on Information Security Applications (WISA), Sep. 2008.

Hyunsang Choi, Hanwoo Lee, Heejo Lee, Hyogon Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic", Proc. of IEEE 7th Int'l Conf. on Computer and Information Technology (CIT), Oct. 2007.

Hyunsang Choi, Heejo Lee, "PCAV: Internet Attack Visualization on Parallel Coordinates", Proc. of Int'l Conf. on Information and Communications Security (ICICS), LNCS 3783, pp. 454 466, Dec. 2005.

DOMESTIC CONFERENCE PAPERS

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.

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.

Hanwoo Lee, Hyunsang Choi, Heejo Lee, "DNS-based Botnet Detection System", KIPS, vol 13 no 2, 2006.

Hyunsang Choi, Heejo Lee, "PCAV: Parallel Coordinates Attack Visualizer", KISS, pp. 130-132, 2005.

PATENTS

Hyunsang Choi, Hyun-Cheol Jeong, Heejo Lee, Chaetae Im, Seung-Goo Ji, Sang-gyun No, Joohyung Oh, "Method for Detecting IRC Botnet Based on Network", Domestic, Registration, 10-1045556, Jun. 24. 2011.

Hyunsang Choi, Bin B. Zhu, Heejo Lee, "Detection and Categorization of Malicious URL", Patent Pending U.S., Application, 2010.

Hyunsang Choi, Heejo Lee, "Apparatus and Method of Searching Group Activity Malicious Code", Domestic, Application, 2008-0006826, Jan. 22. 2008.

Hyunsang Choi, Heejo Lee, "Apparatus and Method for Monitoring Network Using the Parallel Coordinate System", Domestic, Registration, 10-0716620, May. 3. 2007.

Hyunsang Choi, Heejo Lee, "Apparatus and Method for Monitoring Network Using the Parallel Coordinate System", Patent Pending U.S., Application, 11/324,698, Mar. 7. 2006.

TECHNICAL REPORTS

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

Hyunsang Choi, Heejo Lee, "Behavior based Botnet Detection Technique", Information Security 21C, Vol. 86, pp. 80-83, Oct. 1. 2007.

RESEARCH PROJECTS

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

Behavior Analysis of Executable Codes without Their Execution supported by Microsoft Research Asia (2009~2010).

Study on Wired/Wireless DDoS Attack Response Method supported by SK Telecom (2010).

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).

Static Analysis for Finding Malwares before Their Execution supported by Microsoft Research Asia (2007~2008).

Study on Hacking and Virus Response Technology supported by the Ministry of Knowledge Economy, Korea, under the ITRC (Information Technology Research Center) support program (2004~2011).

Online Game Security Consulting supported by Electronic Arts Inc. (2005).

SOFTWARES

PCAV application, Parallel Coordinate Attack Visualization, with Kyoochang Jeong and Prof. Heejo Lee, <http://ccs.korea.ac.kr/PCAV/> (2005).

BotGAD, Botnet Group Activity Detector, with Prof. Heejo Lee, <http://ccs.korea.ac.kr/BotGAD/> (2008).

INVITED TALKS

“Detecting Malicious Web Links and Identifying Their Attack Types”, CMU Cylab Seminar, Apr. 23. 2012.

“Recent Botnet Trend and Defense Mechanisms”, SECUI Technical Seminar, Feb. 23. 2012.

“Recent Botnet Trend”, TTA PG503 Technical Seminar, May. 13. 2010.

“Tutorial for The Latest Hacking Techniques and Demos”, The 15 Network Security Workshop Korea (NetSec-KR 2009), Apr. 15. 2009.

References

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

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

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

Last updated: May 9, 2012
<http://ccs.korea.ac.kr/~realchs/cv.pdf>