Younghee Park, Ph.D

Assistant Professor in Computer Engineering at San Jose State University

Contact Information

Email: younghee.park@sjsu.edu
Mobile Phone: (919) 368-9351
Information: http://cmpe.sjsu.edu

Research Interests

My primary research interest lies in network, software and system security, with emphasis on malicious code (worm) detection, botnet analysis, insider threat, and traceback to find an attack origin. The current research focuses on addressing security issues in Smart Grid.

Education

Ph.D., Computer Science, North Carolina State University, Raleigh, NC USA. Dec. 2010

- Thesis Topic: Network and Host Based Countermeasures against Large-scale Networked Compromised Systems or Malicious Software

M.S., Computer Science, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea. Feb. 2003

- Thesis Topic: Hierarchical Node-based Group Key Agreement Protocol using Diffie-Hellman Key Exchange

B.S., Computer Engineering, Kyungsung University, Busan, South Korea. Feb. 2000

- ***Summa Cum Laude, with Honors in the Engineering of College***

Awards & Honors

Travel Grant for Grace Hopper Celebration of Women in Computing 2010, Altalant, Workshop Student Travel Grant for 7th ACM Conference on Computer Communications Security(CCS), 2010, Chicago, USA

Excellent Teaching Assistant Award at NCSU, April 2008

Research Assistantship at NCSU, Summer 2005 - Dec. 2010

Teaching Assistantship at NCSU, Fall, 2006 - Spring 2009

Korean National Scholarship at KAIST, 2001 - 2002

President Award at Kyungsung University, Feb. 2000

Excellent Academy Record Full Scholarship at Kyungsung University, 1996 – 2000

Work Experience

Universtiy of Illinois at Urbana-Champaign, IL USA

Post-doctoral Research Associate, Information Trust Institute By June

- Development of Trustworthy Smart Grid Networks against DDoS Attack

  Developing a new defense method against malware propagation in Smart Grid.

  Implementing the propose system based on Smart Grid Protocols.

Columbia University, New York, USA

Post-doctoral research scientist, Computer Science Department 2011

- Anomaly Detection At Multiple Scales via Forensic Analysis, Models of Isolation, and Learning of Internetworked Anomalies (ADAMS FAMILIA supported by DARPA)
  Developing a new software-based decoy system for insider threat. Implementing software decoys based on Java.

National Security Research Institute at Electronics and Telecommunications Research Institute(ETRI), Daejeon, South Korea

Researcher, Information Assurance Research Department 2003

- Cyber Attack Correspondence Management System
  Developing real-time collection and management system about attack information on Internet.
  Designing and implementing attack detection sensor, a snort-log extractor by using Snort.
- Vulnerability Analysis Tool Development
  Designing and implementing attack detection sensor, a snort-log extractor by using Snort.

Academic Experience

North Carolina State University, Raleigh, NC USA

Research Assistant May 2005 - Dec. 2010

- The Modus Operandi Project (Fall 2008 - Dec. 2010)
  Developed and designed a new system to identify polymorphism and metamorphism based on static analysis or dynamic analysis. Implemented and experimented real malware based on Windows XP or Linux.
- The Footfall Project (May 2005 - December 2007)
  Designed a new correlation technique for identifying and tracing the attack traffic through compromised intermediate hosts in the presence of complex interferences.
  Developed an adaptive watermarking scheme to find a robust watermark against attacker‘s random delay for the success of network flow correlation.

Teaching Assistant Fall 2007

- CSC/ECE 574 Computer and Network Security
  Graded assignments and projects, held office hours regularly, assisted lab sections, assisted grading exams and supervising exams, answered students questions.
  Technical assistant with Java programming for programming assignments.

Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea

Research Assistant March 2001 - Feb. 2003

- Cyber Attack Correspondence Management System (Aug. 2002 - Sep. 2003)
  Designed and implemented Cyber Attack Correspondence Management System.
  Designed and developed prototypes such as parsing modules utilizing a rule-based log filtering mechanism and incident response modules.
- Cyber Attacker Observation and Control Technology (March 2002 - October 2002)
  Developed an intelligent correspondence system based on attack by classifying ways of attack.
  Developed a packet diversion mechanism, which is a virtual router with interoperability between intrusion detection system (IDS) and Honeypot by using IpFilter on Linux to develop cyber-network to deceive attacker.
- Development of Embedded Lightweight Cryptography Processing Modules based on Elliptic Curve Cryptography (ECC) (March 2001 - Feb. 2002)
  Implemented ECC library on Java card by utilizing Java 2 Micro Edition (J2ME) and emulated it with a Palm OS device.

Working Journal

Younghee Park, Douglas Reeves, "Deriving Common Malware Behavior through Graph Clustering", submitted to the International Journal of Computer and Security, Elsevier. (Wait for a final decision)

Younghee Park, Qinghua Zhang, Douglas Reeves, Vikram Mulukutla, "The Origin of the Code: Automated Generation of Common Behavior in Malware Classes", ready for submission.

Younghee Park, Salvatore J. Stolfo, "FOG2: The Detection of Insider Threat by Using Software Decoys", submitted to the IEEE Transaction.(Under Review)

Sayali Deshpande, Younghee Par, Mark Stamp, "Eigenvalue Analysis for Metamorphic Detection" submitted for Journal of Virology (revision)

Journal Publications

Young June Pyun, Younghee Park*, Douglas S. Reeves, et al., "Interval-based flow watermarking for tracing interactive traffic", in the International Journal of Computer Networks, Vol. 56, Pages 1646-1665, Elsevier. Feb. 2012. (*This author is a corresponding author.) (SCIE. Impactor Factor:1.589)

Young Hee Park, Byungchun Chung, et al., "Scalable Hierarchical Group Key Establishment using Diffie-Hellman Key Exchange", in Korea Institute of Information Security and Cryptology (KIISC) Journal , December, 2003.

Conference Publications

Younghee Park, David M. Nicol, "Design of Policy Engine to Prevent Malware Propagation in AMI", submitted to IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, Canada, October 2013.

Younghee Park, Salvatore J. Stolfo, "Software Decoys for Insider Threat", in the 7th ACM Symposium on Information, Computer and Communications Security(ASIACCS), Seoul, South Korea, May 2012.

Younghee Park, Douglas Reeves, "Deriving common malware behavior through graph clustering", Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security(ASIACCS), Hong Kong, China, March 2011.

Younghee Park, Qinghua Zhang, Douglas Reeves, Vikram Mulukutla, "AntiBot: Clustering Common Semantic Patterns for Bot Detection", Proceedings of 34th Annual IEEE Computer Software and Applications Conference (COMPSAC), Seoul, South Korea, July 2010. (Acceptance ratio: 20%(25/193 for Full Papers))

Younghee Park, Douglas S. Reeves, "Fast Malware Classification by Automated Behavioral Graph Matching", Proceedings of 6th ACM Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW), Oak Ridge National Lab., TN, USA, April, 2010.

Younghee Park, Douglas R. Reeves, "Identification of Bot Commands By Run-time Execution Monitoring", Proceedings of 25th Annual Computer Security Applications Conference (ACSAC 2009), Hawaii, USA, December 2009. (Acceptance Ratio: 19.6% (44/224))

Young Hee Park and D. S. Reeves, "Adaptive Watermarking Against Deliberate Random Delay for Attack Attribution Through Stepping Stones", Proceedings of 9th International Conference on Information and Communications Security (ICICS 2007) December 2007.

Y. J. Pyun, Young Hee Park, X. Y. Wang, D. S. Reeves, and P. Ning, "Tracing Traffic Through Intermediate Hosts that Repacketize Flows", Proceedings of 26th Annual IEEE Conference on Computer Communications (INFOCOM 2007), May 2007. (Acceptance Ratio: 18%)

Young Hee Park, B. Chung, and H. Yoon, "Efficient Group Key Agreement Protocol using a Tree", Proceedings of Korea Institute of Information Security and Cryptology Conference, November, 2002.

Others

Young Hee Park and Reeves, Douglas S., "Adaptive Timing-Based Active Watermarking for Attack Attribution Through Stepping Stones", Technical Report in North Carolina State University, TR-2007-17, June 26, 2007.

Young June Pyun and Young Hee Park, "Tracing Attack Traffic Across Uncooperative Networks", Proceedings of Eighth International Conference on Information and Communications Security (ICICS), November 2006 (Poster).

Young Hee Park, "Hierarchical Node-based Group Key Agreement Protocol using Diffie-Hellman Key Exchange", M.S. thesis, KAIST.

Technical Skills

Programming: C/C++, Java, Python, Shell Script, and others

Operating Systems: Microsoft Windows, Linux, and other UNIX variants

Applications: LaTeX, Virtual Machines, OPNET, Matlab, IDA Pro, Microsoft Office, and other common productivity packages for Windows, OS/X, and Linux platforms