Hyang-Ah Kim

Computer Science Department
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Mobile: (412) 818-7633
Office: (412) 268-3069
Fax: (412) 268-5576

hakim@cs.cmu.edu
http://www.cs.cmu.edu/~hakim

Research Interest

- Internet security and privacy including worm and spam detection/prevention techniques
- Distributed systems design, monitoring, and analysis

Education

- Carnegie Mellon University (CMU), Pittsburgh, PA, USA
  Ph.D. candidate in Computer Science (Advisors: David O'Hallaron and Dawn Song)
- Korea Advanced Institute of Science and Technology (KAIST), Taejon, Korea.
  M.S., in Computer Science, 1999. (Advisor: Kilnam Chon)
  B.S., in Computer Science, *Magna Cum Laude*, 1997. (Advisor: Jin Hyong Kim)

Research Experience

· **Autograph: Automatic Worm Signature Detection System, Intel Research Pittsburgh/CMU (May 2003 –):** Autograph is a distributed system that automatically generates sensitive and specific signatures for novel Internet worms by analyzing the prevalence of portions of flow payloads. Our goal is to detect signatures before 1-2% of total vulnerable hosts are compromised. Joint work with Brad Karp and Dawn Song.

· **Seurat: A Pointillist Approach to Anomaly Detection, CMU (Sep 2003 – Sep 2004):** We proposed a new approach to detect anomaly, and developed a prototype that consists of a multi-platform file system monitoring tool and a correlation engine using various machine-learning and data-clustering techniques. Joint work with Yinglian Xie, Dave O'Hallaron, Mike Reiter, and Hui Zhang.

· **Flow Count Estimation in Real Time, CMU (Nov 2002 – March 2003):** I proposed a timestamp-vector algorithm, a variation of bitmap algorithms, which improves the correctness of real time monitoring.

· **IPMon Project, Sprint ATL (June 2002 – August 2002):** I worked for the development of the metadata management system that automates the database population and the trace analysis when new data sets arrive. Worked with Christophe Diot, Sue Moon, Richard Gass.

· **Trace Publishing System, CMU (May 2001 – May 2002):** Trace publishing system aims to help both trace providers and users to share the trace easily with automated anonymization and filtering. Assuming the semi-trusting relationship, this system provides the requestors with a flexible way to specify their demand with plug-in filters.

· **Quake Project, CMU (January 2001 – May 2001):** The goal of Quake is to develop the capability for predicting, by computer simulation, the ground motion of large basins during strong earthquakes. We developed an efficient caching scheme for accessing remote geospatial data. The experiment with our prototype showed this caching helps reducing the network bandwidth consumption and the response time. Worked with Tiankai Tu and David O'Hallaron.

· **Matrix Project, Thrunet Co., Ltd. (April 1999 – August 2000):** The main goal of Matrix project was to build the broadband backbone network using DWDM and Gigabit Ethernet, and provide innovative Internet applications and service. My role in Matrix was to build the network traffic/performance monitoring system for traffic engineering, develop the multicast monitoring system, and coordinate Matrix project.
· **Internet Multicast Infrastructure, APAN (March 1998 – February 1999):** I worked on the analysis of the Mbone scalability issues and proposed an inter-domain multicast routing protocol with BGP4+.
· **High Performance Mbone Project, KAIST (July 1997 –February 1999):** We demonstrated the prototype of high performance Mbone. I inspected Mbone management tools and designed a debugging tool to detect multiple tunnels over one link.
· **Online Character Recognition Project, KAIST (Fall 1996):** I designed the user interface for the client application with Java and implemented the communication module between a recognition server and clients with Java and C. The client application can recognize some gestures of users, accept user's online/offline handwriting data, and display the results from the recognition server.
· **Intelligent Tutoring System Project, KAIST (Summer 1995):** I implemented the user interface of the Intelligent Tutoring System using Motif. This program allows students to edit their own C codes, and displays the result of the program execution and AI module's diagnosis.

Work Experience

· Intel Research Pittsburgh, Pittsburgh, PA, USA: May 2003 – August 2003. Summer intern.
· Sprint ATL, Burlingame, CA, USA: May 2002 – August 2002. Summer intern.
· Thrunet Co. Ltd, Seoul, Korea :April 1999 – August 2000. Technical staff of Matrix project.

Teaching Experience

· Teaching Assistant for Advanced Systems Programming (lecturer: David O'Hallaron), Advanced Institute of Information Technology, Seoul, Korea, Summer 2006.
· Teaching Assistant for 15-712 Advanced Operating Systems and Distributed Systems (lecturer: Garth Gibson), CMU, Spring 2005.
· Teaching Assistant for 15-441 Computer Networks (lecturer: Hui Zhang and Randy Bryant), CMU, Fall 2003.
· Teaching Assistant for CS206 Data Structure (lecturer: Kyu-young Hwang), KAIST, Spring 1997.
· Teaching Assistant for CS441 Introduction to Computer Networking (lecturer: Kilnam Chon), KAIST, Fall,1997 & Spring 1998.

Publication

· Hyang-Ah Kim and Dawn Song, "Challenges for Pattern-Extraction-Based Automatic Worm Signature Generation," CMU Computer Science Department Technical Report, CMU-CS-06-165, 2006.

· Lea Kissner, Hyang-Ah Kim, Dawn Song, Oren Dobzinski, and Anat Talmy, "Efficient, Secure, and Privacy-preserving Distributed Hot-Item Identification," CMU Computer Science Department Technical Report, CMU-CS-05-159, 2005.

· Hyang-Ah Kim and Brad Karp, "Autograph: Toward Automated, Distributed Worm Signature Detection," In Proceedings of the 13th Usenix Security Symposium (Security 2004), San Diego, CA,

August 2004. A previous version of this work: Intel Research Pittsburgh Technical Report IRP-TR-04-03, February, 2004.

· Yinglian Xie, Hyang-Ah Kim, David R. O'Hallaron, Mike Reiter, and Hui Zhang, "Seurat: A Pointillist Approach to Anomaly Detection," To appear in Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), Sophia Antipolis, French Riviera, France, September 2004.
An extended version of this paper is available as Technical Report CMU-CS-06-118

· Hyang-Ah Kim and David R. O'Hallaron, "Counting Network Flows in Real Time," In Proceedings of IEEE Globecom 2003, San Francisco, CA, December, 2003.

· Hyang-Ah Kim, "Inter-domain Multicast Routing Protocol for Forwarding State Reduction," MS Thesis, Department of Computer Science, KAIST, 1999.

· Hyang-Ah Kim, Multiple Multicast Tunnels Detection, SAL-TM-74, SALab., Department of Computer Science, KAIST 1997.

· Hyang-Ah Kim, Jongmin Hahm, and Hyunje Park, "Internet Service Technology," Magazine of the IEEK, vol.26, no.8, 1999.(Korean)

· Hyang-Ah Kim, Youngmo Kim, and Hyunje Park, "Thrunet High Speed Network," Magazine of the KICS, 1999. (Korean)

Service

· President of Korean Student Association of Pittsburgh (2004-2005)
· Student Representative of CS Department, KAIST (1997)

Reference

David O'Hallaron
Associate Professor,
Carnegie Mellon University,
5000 Forbes Avenue,
Pittsburgh, PA 15213.
Phone: (412)268-8199,
Email: droh@cs.cmu.edu

Brad Karp
Senior Lecturer
Department of Computer Science
University College London,
Gower Street, London, WC1E 6BT
United Kingdom
Phone: +44 20 7679 0406
Email: bkarp@cs.ucl.ac.uk

Dawn Song
Assistant Professor
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213.
Phone: (412) 268-4268,
Email: dawnsong@cmu.edu