Ke Wang

604 CEPSR, Computer Science Dept.
Columbia University
New York, NY 10027
Tel: (646) 775-6076 (o) / (646) 270-4513 (c)
E-mail: kewang@cs.columbia.edu
URL: http://www.cs.columbia.edu/~kewang

EDUCATION

- 07/2002-present, PhD candidate
  Computer Science Dept, Columbia University
  GPA 4.1/4.0

- Cornell University, Computer Science Dept.
  Master of Science, Minor: Financial Engineering
  GPA 3.8/4.0, 09/2000 – 05/2002

- Univ. of Science & Technology of China (USTC), Computer Science Dept.
  Bachelor of Science (Graduate with Top Honor)
  GPA 4.0/4.0, Rank 1 out of 98, 09/1995 – 06/2000 (5-year program)

RESEARCH INTERESTS

- Payload-based network anomaly detection
  - Design algorithms to build succinct, accurate models for network traffic payload, which is site-specific and can avoid mimicry attack
  - Develop light-weight, self-calibrated network sensors that can accurately detect truly anomalous events at real-time, with low false positive rate
  - Correlate ingress and egress traffic to detect worm propagation, and generate worm signature automatically

- Collaborative Security
  - Design and implement a secure infrastructure that can distribute, correlate and aggregate alert and statistical information from multiple security sensors in real-time
  - Design privacy-preserving data format to be exchanged between sites while carrying all necessary information.
  - Reliably detect the zero-day attacks by collaborative payload sensors

- Machine learning and data mining algorithm and their application in security

RESEARCH EXPERIENCE

- July 02 – present, Research Assistant
  Intrusion Detection System (IDS) lab, Columbia University
  Advisor: Prof. Salvatore J. Stolfo

Data mining based approach to detect intruders to computer system and other related computer security problems. Large quantities of data are collected from the system and analyzed to build models of normal behavior and intrusion behavior. These models are evaluated on data collected in real time to detect intruders.

The projects that I previously worked on:

- **EMT** (Email Mining Toolkit – a user behavior-based approach to secure email system, including detect virus, spam, and abnormal usage of the emails.)
- **FWRAP** (Host-based anomaly detection by wrapping the file system.)
- **RUU** (Are you you? Build models for user's normal behavior on a system from multiple aspects to detect masqueraders, for example, commands executed, system calls, file system, registry access, etc.)

- 06/2004-08/2004, Summer intern
  Systems and Networking Research Group, Microsoft Research Redmond
  Mentor: Dr. John Dunagan

My project: FDR - Flight Data Recorder. In this project we are trying to use black-box analysis for the persistent state changes to manage changes in a computer. Persistent state means the registry system and file system. The goal of this project is given all the registry and file modification traces of some machine, can we automatically group them into meaningful groups that correspond to the actions that occurred on that machine. During the summer I finished initial algorithm design and implemented a GUI to present results. Ongoing work aims to refine the system and scale it up to larger sets of traces.

- May 01 – May 02, Research Assistant,
  Information Assurance Institute (IAI), CS Dept, Cornell University
  Advisor: Prof. Emin Gun Sirer

Worked on enforcing security policies on web applications using a policy language approach. We created a simple language to specify the security policy of a web server, and then wrote translators to translate the language into proper codes on different platforms. Security can be automatically enforced on a web server once the administrator specifies the rules using the language.

- May.99 – Jun. 00, Research Assistant,
  National High-Performance Computing Center at Hefei, China
  Advisor: Prof. Guoliang Chen
  Research and development of IDE on Dawning-3000 Cluster System

TEACHING EXPERIENCE

- Fall 2004, Instructor for CS3101-3 Programming Language in Java
  Columbia University, Computer Science Dept

- Fall 2003, Teach Assistant for CS4701 Artificial Intelligence
  Columbia University, Computer Science Dept

PUBLICATIONS

1. Ke Wang, Salvatore J. Stolfo. "Anomalous Payload-based Network Intrusion Detection", *Recent Advances in Intrusion Detection (RAID 2004)*

2. Rui Kuang, Eugene Ie, Ke Wang, Kai Wang, Mahira Siddiqi, Yoav Freund and Christina Leslie. "Profile-based String Kernels for Remote Homology Detection and Motif Extraction", *Proc. of the Computational Systems Bioinformatics Conference (IEEE CSB 2004)*

3. Salvatore J. Stolfo, Wei-Jen Li, Shlomo Hershkop, Ke Wang, Chia-Wei Hu, Olivier Nimeskern. "Detecting Viral Propagations Using Email Behavior Profiles". *ACM Transactions on Internet Technology (TOIT), May 2004*.

4. Ke Wang, Salvatore J. Stolfo, "One Class Training for Masquerade Detection", *ICDM Workshop on Data Mining for Computer Security (DMSEC 2003).*

5. Salvatore J. Stolfo, Shlomo Hershkop, Ke Wang, Olivier Nimeskern, Chia-Wei Hu, "A Behavior-Based Approach to Secure Email Systems". *Int. Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (ACNS-2003)*

6. Salvatore J. Stolfo, Shlomo Hershkop, Ke Wang, Olivier Nimeskern, Chia-Wei Hu, "Behavior Profiling of Email". *1st NSF/NIJ Symposium on Intelligence & Security Informatics (ISI 2003).*

7. Emin Gun Sirer, Ke Wang, "An access control language for web services". *7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002)*

AWARDS

- Best Bachelor's Thesis of 2000, USTC 2000
  (Title: Distributed Sorting by Sampling and High-Speed Crossbar Network)
- Guo Moruo Presidential Fellowship (Highest honor in USTC) 1999
- Baogang National Education Fellowship (12 out of 8000 students) 1998
- National Mathematical Contest of Modeling, First Prize of Region 1998
- Zhong Zhongzhi Sci&Tech Fellowship 1997
- Outstanding Student Scholarship, First Prize, USTC 1996
- First Award in National Mathematics Contest of Middle School 1993

ACTIVITIES

- Invited as university representative to the Microsoft Professional Developers' Conference (PDC) 2001 by Microsoft Corporation.

- Presented poster "EMT- detect virus by email behavior profiling" in Recent Advances in Intrusion Detection (RAID), Sept 2003, Pittsburg.

- Reviewed papers submitted to several security, network, data mining conferences including DNS, ICDM, CCS etc.