

**RESEARCH
INTERESTS**

My interests lie in network security, computer security, and digital forensics. I enjoy discovering solutions to security problems and building systems to secure information systems.

EDUCATION

Ph.D. Computer Science, Polytechnic University, New York, January 2006
Graduate Advisor: Nasir Memon
Concentration: Network Forensics

B.S. Computer Science, Polytechnic University, New York, June 1999

**RESEARCH
PROJECTS**

ForNet: Distributed Forensics Network

[<http://isis.poly.edu/projects/fornet/>]

ForNet is a scalable network logging mechanism to aid forensics over wide area networks. It uses *synopses* based approach to record useful network events in a succinct form for archival. Query APIs and data analysis plug-ins help mine archived synopses for forensic and security needs.

- Conceived the initial ideas for ForNet, such as synopses, cascading collections etc.
- Designed and implemented a prototype currently operational in our campus
- Developed and analyzed novel synopsis techniques for ForNet
- Currently leading the ForNet development team

Nabs: Network Abuse Detector

[<http://isis.poly.edu/projects/nabs/>]

Nabs allows a network to define and enforce a use-policy based on bandwidth *and* content type. It uses statistical properties of packet payloads to robustly identify content types of network flows and monitor the flows for any deviations from the use-policy.

- Research and development of techniques for identifying flow content types
- Designed and implemented a system for monitoring our campus network
- Currently collaborating to further enhance Nabs' feature set

DeShredder: Automated Reassembly of Highly Fragmented Files

DeShredder automates the process of reassembling highly fragmented files when the order of fragments is unknown. DeShredder uses statistical properties of file content, optimization algorithms, and heuristics to determine the most probable order of proper reassembly of files.

- Developed methods to reassemble files when order of fragments is unknown
- Designed and implemented a prototype of DeShredder
- Currently involved in the design and development of a commercial tool that improves on previous techniques

**REFEREED
PUBLICATIONS**

- Integrating Digital Forensics in Network Infrastructures, K. Shanmugasundaram, H. Brönnimann, and N. Memon. *IFIP International Conference on Digital Forensics, 2005*
- Payload Attribution via Hierarchical Bloom Filters, K. Shanmugasundaram, H. Brönnimann, and N. Memon. *11th ACM Conference on Computer and Communications Security, 2004*
- Nabs: A System for Detecting Resource Abuses via Characterization of Flow Content Type, K. Shanmugasundaram, M. Kharrazi, and N. Memon. *Annual Computer Security Applications Conference, 2004*
- Automatic Reassembly of Document Fragments via Context Based Statistical Models, K. Shanmugasundaram and N. Memon. *Annual Computer Security Applications Conference, 2003*
- ForNet: A Distributed Forensic Network, K. Shanmugasundaram, A. Savant, H. Brönnimann, and N. Memon. *The Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, 2003*
- ODISSEA: A Peer-to-Peer Architecture for Scalable Web Search and Information Retrieval, T. Suel, A. Delis, K. Shanmugasundaram, et. al. *Sixth International Workshop on Web and Databases, 2003*
- Automated Reassembly of Fragmented Images, A. Pal, K. Shanmugasundaram, and N. Memon. *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003*

- Data Masking: A Secure-Covert Channel Paradigm, R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. *IEEE Multimedia Signal Processing*, 2002

PATENTS

- Apparatus and Methods for Efficient Payload Attribution, US Patent Applied
- Apparatus and Methods for Identifying and Responding to Resource Abuses in Networks, US Patent Applied
- Apparatus and Methods for Reassembling Highly Fragmented Files, US Patent Applied

TEACHING EXPERIENCE

Instructor Fall 2001 – 2005
 ISIS Laboratory Polytechnic University

- Developed materials (labs, homework, and source code) and co-teaching Digital Forensics, Spring 2004, 2005 (<http://isis.poly.edu/courses/cs996-forensics/>)
- Developed materials and taught Penetration Testing & Vulnerability Analysis, Fall 2003, 2004 (<http://isis.poly.edu/courses/cs996-f2003/>)
- Developed materials for hands-on instruction and delivered guest lectures in network and computer security courses (<http://isis.poly.edu/courses/>)

Teaching Assistant Fall 1998 – Summer 2000
 Department of Computer Science Polytechnic University

- Conducted review sessions and occasionally taught intermediate and advanced C++ to a class of 60-80 graduate and undergraduate students
- Helped students with homework and class projects

WORK EXPERIENCE

Research Assistant Fall 2001 – 2005
 ISIS Laboratory Polytechnic University

- Developed a distributed system for gathering network evidence for forensics
- Developed a method for efficient monitoring of network traffic content
- Developed methods and tools for reassembling fragmented documents and images

Wireless Application Developer Summer 2000
 Exp Systems, Inc. Menlo Park, California

- Designed and implemented a wireless response system to improve customer turn-around time using Wireless Application Protocol (WAP)
- Developed applications for cell phones using WAP
- Integrated the WAP application seamlessly with the Web and PSTN
- Performed user acceptance tests and delivered the product on schedule

Network Administrator Summer 1998
 Wall Street Reporter New York

- Designed and implemented a network for 20-25 hosts
- Maintained and performance tuned the network
- Maintained a web server and a streaming server

AWARDS & HONORS

- Pearl Brownstein Doctoral Research Award for Best Ph.D. Thesis, 2005
- Ranked Second in the ACM Student Research Competition, 2005
- Polytechnic Cyber Security Awareness Week (CSAW 2004) Research Competition Winner
- Polytechnic University Graduate Student Fellowship, 2001-2005
- Ranked First in the Australian Computer Society Examination, 1995

REFERENCES

Available upon request.