Kulesh Shanmugasundaram
kulesh@gmail.com
http://isis.poly.edu/kulesh/

SYNOPSIS

A recognized academic researcher in network security and digital forensics. Co-founder of a successful startup who built and led a team to bring research innovations to market through product development. Experienced in designing and implementing portable software libraries of complex data structures and algorithms in C++ (STL & Boost). Currently seeking a challenging software engineering position in a team solving interesting problems.

EDUCATION

Ph.D. Computer Science, Polytechnic Institute of NYU (NYU-Poly), January 2006
Graduate Advisor: Nasir Memon
– Recipient of Pearl Brownstein Doctoral Research Award (NYU-Poly)
– Runner-up in the international ACM Student Research Competition

B.S. Computer Science, Polytechnic Institute of NYU (NYU-Poly), June 1999

RELEVANT SKILLS

– High-level Programming: C, C++ (STL & Boost), Java (basic knowledge)
– System Programming: BSD sockets, raw traffic capture (pcap), POSIX threads, POSIX APIs
– Libraries: BerkeleyDB (C/C++), PostgreSQL, pcap
– Operating Systems: OS X, FreeBSD, Linux

WORK EXPERIENCE

Co-Founder/Software Architect — Summer 2006 – Present
Digital Assembly, Inc. — New York, New York
http://digital-assembly.com/

- Abstracted complex data carving algorithms and data structures developed while at NYU-Poly into generic STL-like constructs (containers, iterators, and algorithms). Designed and implemented a generic, portable, STL-like library in C++ for data carving.
- Successfully developed and commercialized two products using the libraries developed: Adroit Photo Forensics for enterprise and government markets and Adroit Photo Recovery for consumer market.
- Successfully integrated the software libraries into a Department of Defense forensic tool (DC3's DCCI_StegCarver).
- Developed many rapid prototypes in C++ (and some Java), wrote proposals, and successfully raised funding for product development and commercialization.
- Worked with customers on product vision, feature development and refinement.
- Recruited, trained, and managed a team of talented engineers.
- Filed for and obtained the necessary intellectual property rights for the technologies developed (US Patent #7756899 and others pending)

Partner/Software Architect — Summer 2006 – 2010
Vivic Networks, LLC — New York, New York

- Conceived original ideas behind an infection detection system that uses symptoms, roles, and reputations of hosts to identify infected hosts.
- Developed novel algorithms and data structures for analyzing network flows and characterizing various symptoms and roles, such as peer-to-peer node, frequent-reboots, bruteforcers, etc.
- Implemented the algorithms and data structures using C++ and tested their accuracy.
- Designed and implemented an infection detection system with multiple network sensors (C), analyzers (C++), payload search, and a user interface (HTML/CSS/JavaScript/PHP).
- Integrated select algorithms and data structures into a network monitoring system operated by the U.S. Army Research Lab, called Interrogator.
- Developed a situational awareness tool that facilitates the visualization and analysis of a network of hosts, automatically determines the roles of the hosts, and helps identify and isolate interesting hosts in real-time. The system was implemented in C++/Java.
- Filed for and obtained the necessary intellectual property rights for the technologies developed (US Patent #7756997 and others pending)

Research Assistant Fall 2001 – 2005
ISIS Laboratory, NYU-Poly Brooklyn, New York

- Developed and deployed a campus-wide distributed system for gathering evidence for network forensics. (See Research Projects: ForNet)
- Developed and deployed a campus-wide distributed system for monitoring network content and enforcing content-based policies. (See Research Projects: Nabs)
- Developed methods and tools for reassembling fragmented documents and images for digital forensics. (See Research Projects: DeShredder)
- Published research results in leading conferences and journals in computer science.

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

- Designed and implemented a system that tightly integrated Exp's Q&A website with user cell phones. The system allowed customers to phone in questions/answers and alerted the customers of new questions/answers on their cell phones.
- Developed applications for cell phones using WAP/WML and Vox/VoiceXML.
- Integrated the WAP application seamlessly with the website and PSTN systems.
- Performed user acceptance tests and delivered the product on schedule.

Network Administrator Summer 1998
Wall Street Reporter New York

- Designed and implemented a network of 20-25 hosts.
- Automated the workflow of publishing audio/video interviews to the website directly from the recording studio.
- Administered the network, a web server, and a live streaming server.

RESEARCH PROJECTS

ForNet: Distributed Forensics Network
[`http://isis.poly.edu/projects/fornet/`]
ForNet is a scalable, distributed network logging system to aid forensics over wide area networks. It uses a *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 original ideas behind ForNet, such as synopses, cascading collections etc.
- Designed a scalable and extensible network forensics system.
- Implemented the system using the C language on Linux/FreeBSD platforms; the system consists of a network sniffer, dynamically loadable synopsis modules, and an XML-based query processor.
- Developed and analyzed the usefulness of novel synopsis techniques for network forensics.
- Deployed the system on the campus network to monitor live traffic ($\approx$3500 hosts and $\approx$ 1.5TB of traffic daily); identified and analyzed many security incidents on campus using ForNet.
- ForNet is still operational (at two NYU schools) and a catalyst for network security research at NYU-Poly.

Nabs: Network Abuse Detector
[`http://isis.poly.edu/projects/nabs/`]
Nabs allows a network administrator 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, monitor for policy violations, and generate alerts in real-time.

- Developed techniques based on support vector machines for identifying flow content types.
- Designed and implemented a sniffer in the C language that collects packets and uses the support vector machine techniques we developed to identify flow content types.
- Designed and implemented a management console that can receive and archive flow records from multiple sensors, create use-policies via a UI, alert administrators of violations, and allow drill-down of traffic to/from offending hosts in real-time. Management console was implemented in Java.

DeShredder: Automated Reassembly of Highly Fragmented Files
[`http://isis.poly.edu/projects/evidence/`]
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.

- Pioneered research in reassembling fragmented files by first showing the problem is intractable and proposing many efficient heuristics to solve the problem.
- Designed and implemented prototypes in C/C++ and Java.
- Tested and validated the efficacy of the proposed methods on various storage media and file types.

SELECTED PUBLICATIONS

- ForNet: A Distributed Forensics Network, K. Shanmugasundaram *Ph.D. Thesis, Polytechnic Institute of NYU, January 2006*
- String Matching on the Internet, K. Shanmugasundaram, H. Brönnimann, and N. Memon. *Combinatorial and Algorithmic Aspects of Networking, Lecture Notes in Computer Science, 2005*
- Payload Attribution via Hierarchical Bloom Filters, K. Shanmugasundaram, H. Brönnimann, and N. Memon. *11^{th} 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*
- 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

- Effective policies and policy enforcement using characterization of flow contents (US #7756997)
- Reassembling fragmented files or documents in an order-independent manner (US # 7756899)
- Facilitating storage and querying of payload attribution information (Pending)
- Using host symptoms, host roles, and/or host reputation for detection of infection (Pending)
- Passive detection of rebooting hosts in a network (Pending)
- Network-based infection detection using host slowdown (Pending)

TEACHING EXPERIENCE

Instructor — Fall 2001 – 2005
ISIS Laboratory — Polytechnic University

- Developed materials (labs, homework, and source code) and co-taught 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, lab sessions, and delivered guest lectures in network and computer security courses (`http://isis.poly.edu/courses/`)
- Instrumental in the creation of ISIS laboratory as well as the certification of ISIS as an NSA Center of Excellence in Information Education.

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

AWARDS & HONORS

- Pearl Brownstein Doctoral Research Award for Best Ph.D. Thesis, 2005
- Ranked Second in the international 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.