George R. Louthan IV

20 E Archer #604
Tulsa, OK 74103

918.289.2458
georgerlouth@nthefourth.com
http://georgerloutha.nthefourth.com

Education

- **University of Tulsa** — Tulsa, OK
  M.S., Computer Science (expected) — *May, 2011*
  - Federal Information Assurance Certifications CNSS 4013-4016 (expected)
- **University of Tulsa** — Tulsa, OK
  B.S., Computer Science; B.S. Mathematics — *May, 2009*
  - Federal Information Assurance Certifications CNSS 4011-4012

Employment History

- **Institute for Information Security, TU** — Tulsa, OK
  Research Assistant — *May 2009 - Present*
  - Student lead for a formal methods research project
  - Overseeing the deployment and upkeep of the Institute's computer systems
- **Vidoop** — Tulsa, OK
  Research and Technical Writing Intern — *May 2007 - Mar 2009*
  - Developed technical documentation for an authentication security product, conducted a NIST 800-63 compliance study
  - Traveled to provide technical expertise at trade shows
  - Performed vulnerability assessments and delivered recommendations for mitigation

Courses Taught

- **Fundamentals of Algorithm and Computer Applications Lab** — Tulsa, OK
  University of Tulsa — *Spring 2010*
  - Weekly sophomore-level lab section for assisting students with weekly assignments
  - Topics include basic data structures, sorting, searching, and basic analysis of algorithms

Projects

- **Cyber-physical Systems** — Tulsa, OK
  Institute for Information Security, TU — *Jan 2010 - Present*
  - Leading a formal methods research group for networked hybrid systems (i.e. systems with discrete and continuous components)
  - Building a formal framework for modeling and analyzing networked process control systems
- **Deployment Plan** — Tulsa, OK
  University of Tulsa — *Spring 2010*
  - Writing a comprehensive deployment plan for a generic enterprise computing system.
  - Included hardware and software deployment procedures and checklists, maintenance, as well as business IT policies (e.g. backup/restore, acceptable use, remote access, password, etc.)
- **Intrusion Detection System** — Tulsa, OK
  University of Tulsa — *Spring 2010*
  - Developing a Snort rule compatible network intrusion detection system in Java

- **SAND/DVNE** Tulsa, OK
  Enterprise Security Group, TU *Summer 2007 - Present*
  - Led a network monitoring research group
  - Led the project's deployment at FAA Computer Security Incident Response Center
  - Developing large-screen multi-touch network visualization system
  - Presented with Cody Pollet at DEFCON 17 and as a poster at USENIX Security 2009

Selected Coursework

- **Network Security** Tulsa, OK
  University of Tulsa *Spring 2010*
  - Topics included host-based and network-based intrusion detection, anomaly and misuse detection, and appliances including firewalls
  - Semester-long project to build a Snort-compatible network intrusion detection system
- **Secure System Administration** Tulsa, OK
  University of Tulsa *Spring 2010*
  - Topics included provisioning, procurement and installation of network, hardware and software systems, as well as incident handling.
  - Emphasis on specific policy and procedure development (acceptable use, password, backup and restore, data redundancy, patch management, etc)
  - Semester-long project to develop a complete deployment plan for an enterprise computing system
- **Risk Management for Information Systems** Tulsa, OK
  University of Tulsa *Spring 2010*
  - Risk analysis and threat profiling for mission critical information systems. Adversarial analysis and countermeasure synthesis. Policy development and implementation. Incident handling and response.
- **Information Systems Assurance** Tulsa, OK
  University of Tulsa *Fall 2009*
  - Included design and analysis methods for high assurance information systems, formal models such as Biba and Bell-LaPadula.
  - Emphasis on security controls documents, specifically DIACAP (DoD Instruction 8510.01) and NIST SP 800-53
  - Built from scratch a set theoretic formal model for contingency planning
- **Enterprise Security Management** Tulsa, OK
  University of Tulsa *Spring 2007*
  - Studied the managerial aspects of computer security; included development and maintenance of policies and procedures, regulatory compliance, risk management, and disaster planning and recovery
  - Participated in tabletop exercises in risk management and development of specific policies and procedures
  - Significant work with NIST SP 800-63 and ISO-17799 documents
- **Computer Forensics** Tulsa, OK
  University of Tulsa *Spring 2006*
  - Topics included incident response and recovery, identification and extraction of electronic evidence, and forensic tools

Awards and Honors

General Co-Chair, TU Student Research Colloquium	2010
Chair, Computer Security Special Topic Symposium, TU Student Research Colloquium	2010
Honorable Mention, Best Presentation, AAAS-SWARM 2009	2009
Runner-Up, Donald W. Reynolds Governor's Cup Business Plan Competition	2007

Publications and Presentations

- ***Towards Formal Analysis of Cyber-Physical Systems*** — TU Colloquium, *March 2010*
  G Louthan, N Singleton, M Papa, and J Hale
- ***Large-scale Multitouch Interactive Network Visualization*** **(Poster)** — USENIX Security, *August 2009*
  C Pollet, G Louthan and J Hale
- ***SAND: An Architecture for Signature-based Automatic Network Protocol Detection*** **(Poster)** — USENIX Security, *August 2009*
  G Louthan and J Hale
- ***Hack Like the Movie Stars: A Big-Screen Multitouch Network Monitor*** — DEFCON 17, *August 2009*
  G Louthan, C Pollet, and J Hale
- ***Content-based Alternatives to Conventional Network Monitoring***[1] — CSIIRW '09, *April 2009*
  G Louthan, B Deetz, M Walker, and J Hale
- ***Toward Robust and Extensible Network Protocol Identification***[1] — ICOMP '09, *July 2009*
  G Louthan, C McMillan, C Johnson, and J Hale
- ***Communication without Boundaries: Breaching the Great Firewall of China*** — AAAS-SWARM '09, *March 2009*
  G Louthan and J Hale

Skill set

Programming Languages Java; Python; Clojure; Common Lisp; Basic; some Ruby, Perl and PHP

Technologies TCP/IP; Computer networking; Shorewall/IPTables and general firewalling; Mathematica; LaTeX; Network monitoring; Virtualization; some .NET

Processes Risk management for information systems (NIST SP 800-30), including some familiarity with IT aspects of Sarbanes-Oxley risk assessment (PCAOB Auditing Standard 5); Information Security Management (ISO/IEC 17799:2005); Information Assurance Controls and Accreditation (NIST SP 800-53 and DoDI 8510.01); Incident response and computer forensics; General policy development; General familiarity with NIST 800 series

Platforms Linux (especially Debian/Ubuntu); Windows 2000/XP/Vista/7 (Personal and Server versions); VMWare ESXi; OpenWrt/FreeWrt; Mac OS X

Mathematics Numerical analysis; Finite difference methods; Finite element analysis; Real analysis; Discrete mathematics; Modern algebra; Finite state automata; Hybrid automata; Process calculi; Analysis of algorithms

[1] Denotes a peer-reviewed publication