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*
- **University of Tulsa** — Tulsa, OK
  B.S., Computer Science; B.S. Mathematics — *May, 2009*

Certifications

- **CNSS 4011-4016** — Tulsa, OK
  National Information Assurance Training Standards — *May, 2011*
  - Issued by the University of Tulsa

Employment History

- **Institute for Information Security at the University of Tulsa** — 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

- **Information Security – Assurance and Risk Assessment** — Tulsa, OK
  TU Continuing Engineering & Science Education — *May 11-12, 2010*
  - Instructed applied portions of a short course in information security for the Information Systems Audit and Control Association (ISACA)
  - Developed and led interactive demonstrations of SQL injection, cross-site scripting, ARP poisoning, SSL spoofing, wireless sniffing, and browser securty
  - Lectured and led discussion on the above topics, as well as public key cryptography and infrastructure, SSL, DNS, and ARP

- **Fundamentals of Algorithms 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

- **GSM Scale**
  Tulsa, OK
  June 2010 - Present
  - Developing a system for wirelessly collecting, recording, and analyzing patients' weights
  - Working with Alexander Barclay (Laureate Institute for Brain Research), and Kevin Hall (National Institute of Diabetes and Digestive and Kidney Diseases)

- **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

- **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

Conferences

International Conference for High Performance Computing, Networking, Storage and Analysis 2008 (SC08)	Participant
IT Security World Conference and Expo 2008	Exhibitor
12th TU Student Research Colloquium and 84th AAAS-SWARM Regional Meeting	Speaker, Session Chair
DEFCON 16	Participant (Human)
Computer Security and Information Intelligence Research Workshop (CSI-IRW) 2009	Speaker
The 2009 International Conference on Internet Computing (ICOMP '09) at WORLDCOMP '09	Speaker
DEFCON 17	Speaker
18th USENIX Security Symposium	Poster Presenter
13th TU Student Research Colloquium	General Co-chair, Speaker
Blackhat USA 2010	Participant
DEFCON 18	Participant (Human)
19th USENIX Security Symposium	Workshop Speaker

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

- ***The Blunderdome: An Offensive Exercise for Building Network, Systems, and Web Security Awareness***[1]   CSET 2010 at 19th USENIX Security Symposium
  P Gehres, N Singleton, G Louthan, and J Hale   *July 2010*

- ***Toward Sensitive Information Redaction in a Collaborative, Multilevel Security Environment***[1]
  P Gehres, N Singleton, G Louthan, and J Hale
  WikiSym 2010
  July 2010

- ***Towards Formal Analysis of Cyber-Physical Systems***
  G Louthan, N Singleton, M Papa, and J Hale
  TU Colloquium
  March 2010

- ***Large-scale Multitouch Interactive Network Visualization* (Poster)**
  C Pollet, G Louthan and J Hale
  USENIX Security 18
  August 2009

- ***SAND: An Architecture for Signature-based Automatic Network Protocol Detection* (Poster)**
  G Louthan and J Hale
  USENIX Security 18
  August 2009

- ***Hack Like the Movie Stars: A Big-Screen Multitouch Network Monitor***
  G Louthan, C Pollet, and J Hale
  DEFCON 17
  August 2009

- ***Content-based Alternatives to Conventional Network Monitoring***[1]
  G Louthan, B Deetz, M Walker, and J Hale
  CSIIRW '09
  April 2009

- ***Toward Robust and Extensible Network Protocol Identification***[1]
  G Louthan, C McMillan, C Johnson, and J Hale
  ICOMP '09
  July 2009

- ***Communication without Boundaries: Breaching the Great Firewall of China***
  G Louthan and J Hale
  AAAS-SWARM '09
  March 2009

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