Joe Loughry

I do software devel. for cross domain systems, C&A for CDS, project lead & information security.

Email: joe@call-with-current-continuation.com
Centennial, Colorado, USA
Mobile phone (720) 277-7800

Experience

- Postgraduate Research Student, University of Oxford, 2007–present.

  Discovered methods to control schedule and predict the outcome of security certification and accreditation testing for cross domain systems (CDS) in intelligence community (IC), collateral, and international environments, with applications to health care. Dissertation: *Security Test and Evaluation of Cross Domain Systems*; degree expected 2014. 23 years software development experience including Common Criteria, DIACAP, and DCID 6/3.

- Information Assurance Engineer, Lockheed Martin Corporation, 2006–2012.

  Proposed and won a $968,000 Air Force Research Laboratory contract for a probabilistic redaction application; the R&D project was completed on time and in budget. Author of Security Target for Common Criteria (CC) evaluation of Radiant Mercury(™) with NSA.

- Senior Software Engineer, Lockheed Martin Missiles & Space Company, 1998–2006.

  Invented nested digital signatures for imagery files—patent application filed. Discovered the optical TEMPEST effect and its countermeasures—U.S. patent no. 6,987,461 issued. Software developer and security engineer for Radiant Mercury(™). A highly experienced programmer in C and assembly language on UNIX, X11, FreeBSD, and Trusted Solaris.

- University Instructor, CSSE 591 (Computer Networks), Seattle University, 1998.

Patents

- U.S. 6,987,461 *System and Method for Addressing Optical Emanations from an Information Processing Device*.
- 20130191642 A1 *Nested Digital Signatures with Constant File Size*, published 25 July 2013.
- Applications 61/774,539 and 61/879,059 have not been published yet by USPTO; filed 2013.

Leadership, Proposal Wins, and Funding

- Principal Investigator (PI), awarded $968,412.00 for "Probabilistic Redaction," USAF Rome Labs contract number FA8750-09-C-0006, for period of performance 2009–2012.

Security Clearance

- U.S. citizen, cleared to Top Secret/SCI (inactive) with counterintelligence polygraph; last investigation: 5 August 2009 (SSBI PR); last CI poly 26 May 2010. CISSP-ISSEP no. 10411.

Security Vulnerabilities Discovered

- Unlimited password retries permitted in Trusted Solaris 8 HW 2/04 Certified Edition, 2006.
- Light emitting diodes leak information from many types of data communication equipment (a side channel), including plaintext from certain cryptographic hardware modules, 2002.
- Privilege escalation in `crontab` yields root shell on Trusted Solaris 8 version 4/01, 2000.
- Cross-platform EEPROM boot password bypass on Sun workstation hardware, 1999.
- Insecure storage and extraction of plaintext passwords on Sun workstation hardware, 1998.
- Full control of Trusted Path indicator from unprivileged process, Trusted Solaris 2.5, 1998.

Open Source Software

- Unicode Consortium: `https://github.com/jloughry/Unicode/#readme` (2014) *added the IEC 60417-5007, -8, -9, and -10 (ISO 7000:2012) and IEEE STD 1621 symbols to Unicode.*
- OpenSolaris: `http://www.opensolaris.org` (2006) *found a bug in password retry limit of Solaris 8, Solaris 10, and Trusted Solaris; patch provided to Sun Microsystems.*
- The FreeBSD Project: `http://www.freebsd.org` (1999) *contributed a new console screen saver to FreeBSD 3.2.*
- Fetchmail: `http://fetchmail.berlios.de` (1998) *patch to handle multi-homed machines.*

Refereed Journals

- "Information Leakage from Optical Emanations" by J. Loughry and D.A. Umphress. *ACM Transactions on Information and System Security* **5**(3) pp. 262–289, 2002.

Peer-Reviewed Conferences

- "A Model of Certifier and Accreditor Risk Calculation for Multi-Level Systems." *Proc. 13th IEEE International Conference on Technologies for Homeland Security (HST'13).* Boston, Massachusetts, 12–14 November, 2013.
- "Information Asymmetry in Classified Cross Domain System Accreditation." *19th Comp. & Elec. Sec. Appl. Rend. (C&ESAR 2012).* Rennes, France, 20–22 Nov. 2012, pp. 19–28, 2012.
- "Unsteady Ground: Certification to Unstable Criteria." *Second International Conference on Advances in System Testing and Validation Life Cycle.* Nice, France, 2010.
- "Use of XML in the Specification and Development of a New High Assurance Controlled Interface." *Proc. 2nd Network Centric Warfare Conf.*, Washington, D.C., 22nd Jan. 2003.

Other Published Reports

- "Efficiently enumerating the subsets of a set" by J. Loughry, J. von Hemert, and L. Schoofs (in preparation).
- "Probabilistic Redaction" final technical report. Air Force Research Laboratory (AFRL), Rome, New York, 2012. Available from the Defense Technical Information Center (DTIC), Washington, D.C.
- "Subsets of an 8-element set in order by number of elements in each subset." *The On-line Encyclopedia of Integer Sequences*, AT&T Research, 2003.
- RISKS *(ACM Forum on Risks to the Public in Computers and Related Systems)* vols 17.31, 21.94–5, 22.81, 24.07, 24.22–3, 24.55, 24.87, 25.73, 26.46, and 27.19.

Education

- Bachelor of Arts (B.A.) in mathematics, University of Colorado at Boulder, 1986.
- Master of Software Engineering (M.S.E.) degree, Seattle University, 1996.
- Doctoral student, University of Oxford, Department of Computer Science. Thesis: *Security Test and Evaluation of Cross Domain Systems*, degree expected in 2014.