Joe Loughry

Software development for cross domain systems, CDS C&A, project lead, and information security.

Email: Joe.Loughry@gmail.com
Mobile (720) 277-7800
Centennial, Colorado

Business Experience

Specialist in understanding computer security standards. Programmer in C and UNIX—including multi-level (CMW) software development under Trusted Solaris and FreeBSD—with experience in Common Criteria, DIACAP, NIST SP 800-53 security controls, DCID 6/3, and the new Risk Management Framework (RMF) for government C&A of cross domain systems (CDS).

- call-with-current-continuation dot com, Inc: founder, 2015–present.

  Computer security compliance startup: proposals and documentation assessment for Common Criteria security evaluations, cross domain C&A consulting, and software R&D.

- University of Oxford, England: Ph.D. student, 2007–2015.

  Discovered methods to control the schedule and predict the outcome of security Certification and Accreditation (C&A) testing of cross domain solutions and cross domain systems for Intelligence Community (IC), collateral, and international environments, with application to privacy protection of Electronic Health Record (EHR) systems.

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

  Proposed and won a $968,000 Air Force Research Laboratory contract for a probabilistic redaction system; the R&D project was completed on time and under budget. Wrote the Security Target for the Common Criteria (CC) evaluation of Radiant Mercury(TM). Took on analysis of international security accreditation standards for the F-35 Joint Strike Fighter. Primary interface with UK's GCHQ.

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

  Invented nested digital signatures for satellite imagery files—U.S. patent no. 8,793,499 issued. Discovered the optical TEMPEST effect and its countermeasures—U.S. patent no. 6,987,461. Software developer and security engineer with responsibility for the real-time performance of Radiant Mercury(TM) on the B-2 stealth bomber.

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

  Practical networking design from a business perspective, layers 1 through 4 and TCP/IP. NICs, topology, routers, and firewalls. IP numbering, DHCP and DNS, file and print servers. Network backbone design trade-offs, structured cabling, security and data encryption.

Leadership, Proposal Wins, and Funding

Principal Investigator, awarded $968,412 for 'Probabilistic Redaction", USAF Rome Laboratory contract no. FA8750-09-C-0006, period of performance 2009–2012; completed on time and budget.

Security Vulnerabilities Discovered

- Silent reversion to insecure defaults in Mac OS X 'Yosemite' `/etc/sshd_config` file, 2014.
- 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.
- Time-of-check/time-of-use gap is exploitable in EEPROM boot password across Sun Microsystems UltraSPARC hardware, 1999.
- Full control of Trusted Path indicator from unprivileged process, Trusted Solaris 2.5, 1998.

Open Source Software

- Terence Eden, Joe Loughry, and Bruce Nordman. *Unicode Technical Committee* (San Jose, CA: February 3–6, 2014) `https://github.com/jloughry/Unicode/#readme` *added the IEC 60417-5007, -8, -9, and -10 (ISO 7000:2012) and IEEE-Std-1621:2004 symbols to Unicode 9.0.*
- 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 and accepted.*
- The FreeBSD Project: `http://www.freebsd.org` (1999) *contributed a new console screen saver based on Wu's fast anti-aliased line drawing algorithm to FreeBSD 3.2.*
- Fetchmail: `http://www.fetchmail.info/` (1998) *patch to handle multi-homed machines.*

Refereed Journal Articles

- "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 Conference Presentations

- "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, *et al.* (in preparation).
- "Probabilistic Redaction" final technical report. US Air Force, 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, 27.19, and 28.02.

Security Clearance

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

Education

- Doctoral student, University of Oxford, Department of Computer Science. Thesis topic: *Security Test and Evaluation of Cross Domain Systems*, accepted July 2015.
- Master of Software Engineering (M.S.E.) degree, Seattle University.
- Bachelor of Arts (B.A.) in mathematics, University of Colorado at Boulder.

PGP key fingerprint: `2C3B 11A1 CE7C 5B1F 87BC F5D0 299D 7116 EDC2 ABE5`