Joe Loughry

(At Lockheed, our code was pen-tested by NSA's tame hackers; it was my job to frustrate those people.)

Email: Joe.Loughry@gmail.com Phone: +1 (720) 277-7800 Blog: https://cnadocs.com

Researcher *C&Adocs, Inc.* 2017–present

Currently working on a route to low cost high assurance cross-domain systems inherently immune to malware. FPGA or VLSI implementation from a security-approval–forward basis. The intended application is between multiple international partners and the intelligence community.

Visiting Assistant Professor *University of Denver* 2016–2017

Taught computer security, beginning C programming, and ethical hacking classes. Lecture and laboratory demonstration in cyberweapons, counterintelligence, TEMPEST countermeasures. Presented a special public lecture on current topics in cybersecurity, Snowden, and the U.S. government.

Consultant *C&Adocs, Inc.* 2015–2016

Secret-and-Below Interoperability (SABI) certification testing of two new cross domain solutions (CDS) for a developer in the D.C. area. Lots of experience with NIST 800-53 security controls: selection and arguing them with the certifier. Advising on likely certifier directions and anticipating certifier moves. Writing documentation to continually evolving requirements. Vulnerability analysis.

Postgraduate Researcher *University of Oxford* 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 applications in the area of privacy protection of Electronic Health Record (EHR) systems.

Information Assurance Engineer *Lockheed Martin IS&GS* 2006–2012

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

Senior Software Engineer *Lockheed Martin Missiles & Space Company* 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: embedded UNIX, built-in test, and bare metal programming.

Security Vulnerabilities Discovered

- Silent reversion to insecure defaults in Mac OS X 10.10 '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 (a side channel) from data comms: CVE-2002-2447.
- 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 of Sun Microsystems hardware, 1999.
- Full control of Trusted Path indicator from an unprivileged process, Trusted Solaris 2.5, 1998.

Leadership, Proposal Wins, and Funding

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

Joe.Loughry@gmail.com

Refereed Journal Articles

- "Information Leakage from Optical Emanations" by J. Loughry and D.A. Umphress. *ACM Trans. Info. Sys. 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.

Open Source Software Contributions

- Bitcoin Core: `https://github.com/bitcoin/bitcoin` (2016) *pull request accepted and merged.*
- 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) *new console screen saver based on Wu's fast anti-aliased line drawing algorithm in FreeBSD 3.2.*
- Fetchmail: `http://www.fetchmail.info/` (1998) *patch to handle multi-homed machines.*

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.

Education

- Doctor of Philosophy (D.Phil.) computer science, Oxford. Co-supervisors: Professor Andrew Martin and Dr Ivan Fléchais. Thesis: *Security Test and Evaluation of Cross Domain Systems.*
- Master of Software Engineering (M.S.E.), Seattle University.
- Bachelor of Arts (B.A.) mathematics, University of Colorado at Boulder.

Side Projects

- A bare metal RTOS kernel for the Raspberry Pi: a bootable kernel in 160 bytes of object code.

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