L. Todd Heberlein

1008 Dolcini Lane
Davis, CA 95616

Mobile: (916) 600-1074

www.toddheberlein.com
todd_heberlein@mac.com

SUMMARY OF PROFESSIONAL EXPERIENCE

30+ years leading research and development efforts in cyber security.

Led R&D projects for DARPA, IARPA, Air Force, Navy, and Department of Energy.

Pioneered the field of network-based intrusion detection with the development of the Network Security Monitor (NSM).

Developed host-based sensors, including designing and implementing audit log analysis tools for Linux, Mac, Windows, and Solaris.

Developed back-end detection, aggregation, and presentation systems using several different database systems (Elasticsearch, Redshift, MySQL) and front-end solutions (Kibana, AWS QuickSight, PHP+Javascript).

Written code in many different languages including Swift, Obj-C, C++, C, Go, Java, and Python.

Developed for many different operating system including Linux, Mac, iOS, Windows, and Solaris.

Developed and shipped Virtual and Augmented Reality (AR/VR) applications for iOS.

For access to papers, articles, presentations, and videos, please see the web site toddheberlein.com

EMPLOYMENT HISTORY

Principal Engineer	Five Directions, Inc.	2020 – 2021
Senior Scientist	FICO – San Diego, CA	2014 – 2019
Senior Researcher, Founder	Net Squared, Inc. – Davis, CA	1996 – 2014
Postgraduate Researcher 10	UC Davis – Davis, CA	1991 – 1996
Postgraduate Researcher 1	UC Davis – Davis, CA	1988 – 1989

EDUCATION

University of California, Davis — Master of Science
University of California, Davis — Bachelor of Science

PEER-REVIEWED ARTICLES

L.T. Heberlein, M Bishop, "*Attack Class: Address Spoofing*", 19th National Information Systems Security Conference, Baltimore, MD, 22-25 Oct 1996, pp. 371-377. (best paper)

M Bishop, L.T. Heberlein, "*An Isolated Network for Research*", 19th National Information Systems Security Conference, Baltimore, MD, 22-25 Oct 1996, pp. 349-357.

S. Staniford-Chen, and L.T. Heberlein , "*Holding Intruders Accountable on the Internet*", Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA, 8-10 May 1995, pp. 39-49.

B. Mukherjee, L.T. Heberlein, K.N. Levitt., "*Network Intrusion Detection*", IEEE Network, Vol. 8 No. 3, pp. 26-41, May/June 1994.

C. Ko, D. Frincke, T. Goan, L.T. Heberlein, K. Levitt, B. Mukherjee, C. Wee , "*Analysis of an Algorithm for Distributed Recognition and Accountability*", Proc. 1st ACM Conference on Computer and Communication Security. Fairfax, VA, Nov. 1993, pp. 154-164.

L.T. Heberlein, B. Mukherjee, K.N. Levitt., "*Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks*", Proc. 15th National Computer Security Conference, pp. 262-271, Oct. 1992.

Levitt, Mukherjee, Bishop, Heberlein, ed., Proceedings of the Workshop on Future Directions in Computer Misuse and Anomaly Detection. The Office of INFOSEC Computer Science, Department of Defense, Mar. 1992.

S.R. Snapp, G.V. Dias, T.L. Goan, T. Grance, L.T. Heberlein, C. Ho, K.N. Levitt, D. Mansur, B. Mukherjee, S.E. Smaha, J Brentano., "*DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype*", Proc. 14th National Computer Security Conference, pp. 167-176, Oct. 1991. (best paper)

L.T. Heberlein, B. Mukherjee, K.N. Levitt., "*A Method to Detect Intrusive Activity in a Networked Environment*", Proc. 14th National Computer Security Conference, pp. 362-371, Oct. 1991.

L.T. Heberlein, "*Network Security Monitor: a brief description*", Appendix to Master's Thesis, June 1991.

L.T. Heberlein, "*Towards Detecting Intrusions in a Networked Environment*", Division of Computer Science, UC Davis, Report No. CSE-91-23.

L.T. Heberlein, B. Mukherjee, K.N. Levitt, D. Mansur., "*Towards Detecting Intrusions in a Networked Environment*", Proc. 14th Department of Energy Computer Security Group Conference, pp. 17.47-17.65, May 1991.

J. Brentano, S.R. Snapp, G.V. Dias, T.L. Goan, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee., "*An Architecture for a Distributed Intrusion Detection System*", Proc. 14th Department of Energy Computer Security Group Conference, pp. 17.25-17.45, May 1991.

S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, T. Grance, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, D.L. Mansur, K.L. Pon, S.E. Smaha., "*A System for Distributed Intrusion Detection*", digest of papers COMPCON 91, pp. 170-176, Feb. 1991.

L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood., "*Network Attacks and an Ethernet-based Network Security Monitor*", Proc. 13th Department of Energy Computer Security Group Conference, pp. 14.1-14.13, May 1990.

L.T. Heberlein, G.V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, D. Wolber., "*A Network Security Monitor*", Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, May 1990.

TECHNICAL REPORTS

T. Heberlein, "*DIDS: Integrated host and network monitoring, live taps, lateral tracking, oh... and all in 1991*", Net Squared, Inc., 20 Sep 2012.

T. Heberlein, "*The Making of 'The Advanced Persistent Threat You Have: Google Chrome'*", Net Squared, Inc., 28 Apr 2012.

T. Heberlein, "*The Advanced Persistent Threat You Have: Google Chrome*", Net Squared, Inc., 17 Apr 2012.

T. Heberlein, "*Windows 7 Security Event Log Format*", Net Squared, Inc., Technical Report TR-2010-09-23, Sep 2010.

T. Heberlein, "*Windows 7 Auditing: An Introduction*", Net Squared, Technical Report TR-2010-06-14, June 2010.

L.T. Heberlein, "*Statistical Problems with Statistical-based Intrusion Detection*", Net Squared, Technical Report 2007-02-05, Feb 2007.

L.T. Heberlein, T. Stallard, "*Review of the CPP Cyber Security Program*", Net Squared, Technical Report, June 2005.

L.T. Heberlein, "*Beyond the Anomaly: The Quest for the Underlying Cause*", Net Squared, Technical Report 2005-03-01, March 2005.

L.T. Heberlein, "*Why Anomaly Detection Sucks*", Net Squared, Technical Report 2005-02-01, Feb. 2005.

L.T. Heberlein, "*Environment Aware: Future Directions*", Net Squared, Technical Report 2005-01-02, Jan. 2005.

L.T. Heberlein, "*Environment Aware Report: A Minimalist Approach To a Complex Problem*", Net Squared, Technical Report, Aug. 2004.

L.T. Heberlein, "*Automatic Signature Generation Final Report: Addressing Limitation of Approach for Self-Propagating Attacks*", Net Squared, Technical Report, Aug. 2004.

T. Heberlein, M. Bishop, E. Ceesay, M. Danforth, C.G. Senthilkumar, T. Stallard, "*A Taxonomy for Comparing Attack-Graph Approaches*", Net Squared, April 2004.

L.T. Heberlein, "*Automatic Signature Generation: Report On The Initial Implementation*", Net Squared, Technical Report 2004-01-20, Jan. 2004.

L.T. Heberlein, "*On Accurate Measurements of Bytes Transmitted in Network Sessions*", Net Squared, Technical Report 2003-12-22, Dec. 2003.

L.T. Heberlein, "*Trend Center Final Report*", Net Squared, Oct 2003.

L.T. Heberlein, "*TrendCenter Phase I: Final Report*", Net Squared, Technical Report 2002-05.01, Oct 2002.

L.T. Heberlein, "*Tactical Operations and Strategic Intelligence: Sensor Purpose and Placement*", Net Squared, Technical Report 2002-04.02, Sep, 2002.

L.T. Heberlein, "*Understanding Strategic Malicious Code Attacks: Some Initial Thoughts*", Net Squared, Aug 2002.

L.T. Heberlein, "*Before Applying New Technologies*", Net Squared, Technical Report 2001-05, 2001.

L.T. Heberlein, "*Network Radar: Final Report*", Net Squared, Technical Report 2002-01, Aug 2002.

L. T. Heberlein, "*Network Radar: STTR Phase I Final Report*", Net Squared, June 1997.

CONSULTING

Quinn Emanuel Urquhart & Sullivan, LLP (started 2014) Served as a consultant for a patent lawsuit. The subject matter was intrusion detection technology.

Kirkland & Ellis LLP – SRI vs. McAfee. (started 2013) Served as a consultant for a patent lawsuit. The subject matter was network-based intrusion detection technology.

Perkins Coie – Finjan vs. Secure Computing Corp. (started 2007). Served as an expert witness, wrote expert report, was deposed, and testified in court. The subject matter was firewall technology.

Lawrence Livermore National Laboratory (LLNL). (started 2005). Reviewed LLNL's Cooperative Protection Program (CPP), wrote a report for recommended changes. CPP was a DOE-wide network sensor grid.

Day Casebeer Madrid & Batchelder LLP – SRI vs. Symantec (and ISS/IBM). (started 2005) Served as an expert witness, wrote expert report, was deposed, and testified in court. The subject matter was network-based intrusion detection technology.

Akin Grump & Strauss LLP – Veridian vs. Ball Aerospace Technology Corp. (started 2001) Served as a consultant in an intellectual property suit. The subject matter was network-based intrusion detection.

Boeing. (started 2000). Provided technical support as Boeing developed a hardware-based (FPGA) Snort-compatible intrusion detection system.