L. Todd Heberlein

7285 Charmant Dr. #211
San Diego, CA 92122

Mobile: (916) 600-1074
Home: (530) 758-1359

www.toddheberlein.com
todd_heberlein@mac.com

SUMMARY OF PROFESSIONAL EXPERIENCE

I have led research and development efforts in cyber security for over 25 years. As a graduate student and postgraduate researcher I designed and developed the first network-based intrusion detection system, the Network Security Monitor (NSM), and was one of the primary developers of the first multi-platform intrusion detection system, the Distributed Intrusion Detection System (DIDS). I founded Net Squared in 1996 and led many government-sponsored cyber security research projects as well as internally developed commercial software systems. Projects and systems include network security systems, attack aggregation platforms, and endpoint detection and analysis tools.

I have been an active leader in all levels R&D, including the development of novel concepts, writing research proposals for funding the work, leading teams, writing academic and technical reports, giving presentations, developing videos, shipping products, and supporting customers. I have also testified as an expert witness in cyber security patent cases. Currently I am a Senior Scientist and subject matter expert (SME) in FICO's analytics division helping develop FICO's first cyber security products.

I have developed for many different platforms (Solaris, Linux, Windows, Mac, iOS), using many different development tools (GNU tools, SparcWorks, Visual Studio, Xcode, NetBeans), and in many different programming and scripting languages (Java, Python, Swift, C, C++, Obj-C, Bourne shell, PHP, and others).

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

EMPLOYMENT HISTORY

Senior Scientist	FICO – San Diego, CA	2014 – present
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, 1991
University of California, Davis — Bachelor of Science, 1988

SOFTWARE SYSTEMS DEVELOPED

Data Fence – *Lead developer.* Data Fence is a security tool that uses Apple's BSM audit data to monitor access to a user's data, alerting the user when hackers, government spies, or overly curious co-workers access the user's personal files. Data Fence puts a virtual fence around data and generates alerts when that fence is crossed in a suspicious manner. It doesn't care what the malicious software looks like. It doesn't care if an attacker has logged in with stolen credentials. It doesn't care if the user

lets others mount the file system to access just *some* of the files. It doesn't care about any of the ways the threat might manifest itself, but it does care when the threat accesses protected data. By focusing on the data files instead of malware, Data Fence avoids the trap of continuously chasing ever-changing malware. (Version 1.0 released April 2014; available through the Mac App Store)

Audit Viewer – *Lead developer.* Audit Viewer is a forensics tool for Mac OS X computers. It analyzes BSM audit data, identifies individual processes, shows the programs the processes were running, and lets you drill down to the individual audit records. (Version 1.1 released April 2014; available through the Mac App Store)

Audit Explorer – *Lead developer.* Audit Explorer is a security tool for Mac OS X computers. Audit Explorer analyzes BSM audit files generated by the OS, highlights security relevant events, lets you drill down to the actions of individual processes, and lets you explore the relationships between processes. Most recent release: (Version 1.1 released 2011; available through the Mac App Store)

Log Browser – *Lead developer.* Log Browser is a front-end GUI to connect to the Free Audit Aggregation System (FAAS) web service to visually browse the logs on the server and quickly find log files of interest. You can then download the files to your computer for in-depth analysis using other tools such as Audit Explorer, Audit Viewer, and Data Fence. (Most recent release 2013 for Mountain Lion)

Free Audit Aggregation System (FAAS) – *Lead developer.* The Free Audit Aggregation System (FAAS) is a web service to aggregate, large, high fidelity security relevant logs, browse the logs in the archive, and download logs of interest to explore with security tools such as Audit Explorer, Audit Viewer, and Data Fence. (Most recent release: 2013 for Mountain Lion)

Audit Control Manager – *Lead developer.* Audit Control Manager (also known as ACManager) manages configurations for the BSM audit system for the Apple's Snow Leopard operating system. Audit Control Manager lets users generate, store, and share configurations. The purpose was to create a collection of audit configurations that were effective for various security scenarios and that could be shared within the security community. (Most recent release: 2011)

Cube Dreams – *Lead developer.* Cube Dreams is a 3D game for iOS devices where the player runs and jumps through various maps trying to grab all the jewels in the fastest time possible. The program leverages many of the core iOS capabilities including its 3D engine, gesture detection, and gyroscopes and compass for motion and position detection. This was a exercise to determine what was needed to develop and ship for iOS. (Version 1.0 released July 2014; available through the Apple App Store)

RESEARCH PROJECTS

Environment-Aware Security System (2003-2005) – *Principal Investigator.* The Environment-Aware Security project consumed detailed information about a network (e.g., vulnerabilities and topology) and a (potentially hypothetical) adversary's capabilities and produced (1) a set of your computer systems that could be penetrated by the adversary and (2) a prioritized list of changes to the network (e.g., patches to specific systems) that would maximally disrupt the adversary's ability to move through the network. The prioritized list of changes, referred to as Network Tasking Orders (NTOs), would be the primary way network and system administrators would interact with the system. Customers: Navy, ARDA.

Automatic Signature Generation (2003-2004) – *Principal Investigator.* Automatic Signature Generation was designed to address self-propagating attacks (e.g., worms), especially so-called zero-day worms targeting previously unknown vulnerabilities, by automatically generating a signature as

soon as the attack is first observed. The system used suffix-trees to nearly instantaneously determine expected false positive rates of automatically generated candidate signatures. The best candidates would be pushed into intrusion prevention systems (IPS) to quickly stop the worm. Customer: Air Force.

Intrusion Detection for FAA's Next-Generation ATC (2002-2004) – *Principal Investigator.* This work examined the possibility of bringing network-based intrusion detection to the FAA's next generation air traffic control network. The NextGen ATC network was not based on TCP/IP but what had been considered the future networking standard – the International Standards Organization's Open System Interconnection protocols, ISO/OSI. Customers: FAA, Northrop Grumman.

TrendCenter (2000-2001) – *Principal Investigator.* TrendCenter aggregated alerts from many organizations, spotted trends, and predicted the attacks a site was most likely to encounter in the near future (what we called "over-the-horizon intrusion detection"). We prototyped the first version on SANS intrusion detection data. Based on a site's attack prediction, TrendCenter generated a custom Nessus vulnerability scanner configuration file to find the vulnerabilities most likely to be exploited at your site. Customer: Air Force.

Audit Work Bench (1999-2000) – *Principal Investigator.* Audit Workbench extended the Network Radar approach to audit trail analysis. It consisted of a flexible object oriented library (Audit Monitoring Framework, AMF) that could be extended and assembled into a range of audit trail monitors. Many of our current tools such as Audit Explorer, Audit Viewer, and Data Fence were built using this design. Customer: Air Force.

Network Radar (1996-2000) – *Principal Investigator.* Network Radar took the lessons learned from the NSM to build a next-generating network monitoring capability. The core of Network Radar was an object oriented library (called the Network Monitoring Framework, NMF) that could be extended and assembled into a wide range of network monitors to meet custom monitoring needs. The technology was designed to be purpose-agnostic so that it could be deployed against a wide range of threats. Many years later the NSA's XKeyScore systems looked very much like Network Radar. Customers: Air Force, DARPA.

Attack Classification (1995-1996) – *Researcher.* The Attack Classification effort moved beyond describing specific instances of attacks to developing a taxonomy for describing attacks. The taxonomical approach would let us understand threats at a more fundamental level, giving us insights into potential variations of the attack, and suggesting solutions and detection strategies that would be more robust than dealing with each specific attack. Customer: Air Force.

Intrusion Detection for Large Networks (1993-1995) – *Researcher.* The Intrusion Detection for Large Networks project was designed to extend the DIDS concepts to arbitrarily large networks. The project included a basket of other security technologies, including specification-based detection and tracking users across networks by fingerprinting connection content over specified chunks of time. Eventually this worked morphed into the Graph-based Intrusion Detection System (GrIDS). Customer: DARPA.

Distributed Intrusion Detection System (DIDS) (1990-1993) – *Researcher.* DIDS was a distributed, heterogeneous intrusion detection system. It included host monitors (for SunOS and VMS), network monitors (based on the Network Security Monitor), and a Director that could aggregate low-level suspicious behavior into a stronger signal. The Director also tracked lateral movement in a network and could identify suspicious movement patterns that could not be detected by any one sensor. The Air Force eventually took the network monitor and Director, renamed the system ASIM, and by 1997 rolled it out across all Air Force sites. Customer: Air Force.

Network Security Monitor (NSM) (1988-1995) – *Researcher.* The Network Security Monitor (NSM) was the first network-based intrusion detection system and the first widely deployed intrusion detection system (deployed by the Air Force under the name ASIM and DISA under the name JIDS). By 1991 the NSM included statistical profiling, content pattern matching, and rules to combine these analyses into an aggregated warning value. The NSM also included transcript and playback tools to observe an attacker's actual activity down to the keystroke level. Customer: DOE.

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.