Stuart Staniford, PhD

812 Irish Settlement Rd,
Freeville, NY 13068
stuart@earlywarn.org
(607) 844-3052 (office/fax)
(415) 613-4497 (cell/voicemail)

Summary

I am a scientist, inventor, and start-up executive with two decades of experience in statistical analysis, computer security threat detection, and software architecture. I specialize in the design and implementation of fast, practical algorithms to solve hard problems. In the last decade, I have mainly worked on multi-threaded, multi-core statistical reasoning systems, but prior to that have I done GUI design and Internet standards work. Recent interests have included understanding and detecting Chinese APT attacks, web drive-by attacks, wire-speed parsing and detection of client-side code-based attacks (including in PDF, Java, and Flash files), network worm propagation, computer intrusion detection and prevention. My research papers have been cited over 5500 times in the scientific literature, as well as being covered in major national magazines and newspapers. I have two decades of experience as a designer and executive developing computer security products. I was a key inventor and an executive at FireEye, recently crowned the *"Hottest Security Startup in Silicon Valley"* by Forbes Magazine. I have extensive and recent hands-on development experience in C and Perl with secondary languages including Java, C++, and SQL. I am intimately familiar with web technologies such as HTML/JS and HTTP.

Work Experience

Cornell University. Adjunct Professor of Computer Science, Jul 2013-present.

Researched novel statistical algorithms for network detection of advanced malware.
Taught graduate course on Defending Computer Networks.

FireEye. Chief Scientist, Jan 2008 – Feb 2013.

Developed novel statistical algorithms and module for network detection of malicious websites installing illegal malicious software on client computers. This allowed FireEye to repurpose its existing product line, which was previously failing in the marketplace, as a solution to the web-bot problem. Company successfully raised two rounds of venture capital based on this new value proposition, sold into numerous Fortune 500 accounts, and began doubling and tripling in size annually, eventually reaching well over $2b in valuation and being named the "Hottest Security Startup in Silicon Valley" by Forbes magazine. I also invented and developed a PDF parser and zero-day detection module to address shift of web attacks to primarily PDF vector, and then did the same for Java and SWF. Performed analysis of our global data for marketing and scientific purposes. Discovered significant deployment issues at a large minority of our customers and led resolution effort. FireEye's success obligated top analysts Gartner to create an entire new market category, Advanced Threat Protection Appliances, which recognized FireEye as the "first company to bring to market automation of attack detection and prevention using virtual execution of objects and analysis." FireEye has recently registered for its IPO, and the share price has gone from 7c when I joined to $23 now.

Invicta Consulting. President, 2005 - Present

Solo consultant. Clients include:

- ***Internet Security Systems (ISS)/King and Spalding***. 2005 - 2009. I was an expert witness in patent litigation (SRI sued ISS for infringement). Analyzed patents and prior art, wrote expert report, defended analysis at deposition, testified at trial.
- ***Nevis Networks***. 2005 - 2006. Consulted on maintenance issues in systems that I designed as an employee, helped with patent filings, reviewed security algorithms, helped with product testing, and wrote white papers.
- ***FireEye***. 2006 – 2007. Reviewed algorithms, provided third party validation of effectiveness of system for this startup with an innovative security product involving virtual execution of network attacks in transit. Also performed technical analysis of competitor systems.
- ***Sleepy Hollow Capital***. Aug 2011-present. Advisor on oil supply/price issues for this energy-focussed hedge fund.

Nevis Networks. Principal Scientist, April 2004 – July 2005

Architected a very high-speed event correlation system and the traffic anomaly subsystem for this startup developing 10Gbps network security solutions for the ethernet edge of internal enterprise networks. These systems resulted in four patent applications including a novel multi-dimensional external memory algorithm for storing log-records on disk at very high speeds. Designed portions of the product's graphical user interface. Worked extensively with engineering teams in Pune, India and Santa Clara, California implementing my designs.

Silicon Defense. Founder and President, 1998 - 2004

Managed 23 staff performing a mixture of government contract research and commercial product development. Obtained ten research contracts for the company up to $2.3m in size, working for four different DARPA program managers. Published research into intrusion detection, intrusion correlation, and worms. Work was covered in Business Week, Federal Computer Week, PC World, Network World, American Banker, *etc*. Coauthored patent application on invention of worm containment.

Wrote business plan for the company and raised $300k in angel capital. Sold commercial products into Fortune 500 accounts (company gained over 50 commercial customers during my tenure, including Disney, AT&T, Hartford Insurance, and Invesco). Had profit and loss responsibility for a $2.3m operation, and extensive experience interacting with press, analyst, and investment communities. Also led two standards groups, and served on a number of program committees.

After five years of 100%+ annual growth out of cashflow, company was obliged to file bankruptcy due to DARPA's decision to classify further information security research. I was also obliged to file personal bankruptcy due to guarantees of corporate obligations.

UC Davis. Researcher, 1994 – 1997, and Assistant Adjunct Professor, 1997 - 1999

Founded and cochaired the working group that developed the Common Intrusion Detection Framework at the request of DARPA. This involved working with a team of over a hundred researchers and developers from a wide variety of companies and organizations. Led a team of ten researchers and students building a large, distributed, intrusion-detection system (GrIDS). Performed research in new statistical techniques to help in tracing intruders across the Internet. Presented work at conferences and to funding agencies. Wrote successful funding proposals and published papers on work.

Education

M.S. (Computer Science). March 1995. University of California at Davis. Advisor: Prof. Karl Levitt

Ph.D. (Physics) June 1993. University of California at Davis. Awarded fellowships for three years consecutively.

M.S. (Physics) June 1990. University of California, Davis.

B.Sc. (Mathematical Physics) June 1988. University of Sussex, UK. First Class Honors.

Refereed Publications

S. Staniford, D. Moore, N. Weaver, and V. Paxson, *The Top Speed of Flash Worms.* Proceeding of the ACM Workshop on Rapid Malcode (WORM), 2004

N. Weaver, D. Ellis, S. Staniford, and V. Paxson, *Worms vs Perimeters – The Case for Hard-LANS.* Proceedings of Hot Interconnects, 2004

N. Weaver, V. Paxson, and S. Staniford, *Very Fast Scanning Worm Containment.* Proceedings of USENIX Security, 2004

S. Staniford. *Containment of Scanning Worms in Enterprise Networks.* To appear in the Journal of Computer Security.

N. Weaver, V. Paxson, S. Staniford, and R. Cunningham *A Taxonomy of Computer Worms.* Proceedings of the ACM Workshop on Rapid Malcode (WORM). Washington D.C. October, 2003.

D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, *Inside the Slammer Worm*, IEEE Security and Privacy, July/August 2003.

S. Staniford, J. Hoagland and J. McAlerney. *Practical Automated Detection of Stealthy Portscans.* Journal of Computer Security. Vol 10, Issue 1/2, 2002.

S. Staniford, V. Paxson, and N. Weaver *How to 0wn the Internet in Your Spare Time,* Proceedings of the 11th USENIX Security Symposium 2002.

D. Donoho, A. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford, *Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay*, Proc. RAID 2002.

J. Hoagland, and S. Staniford, *Viewing IDS alerts: Lessons from SnortSnarf.* Proceedings of DISCEX II, Anaheim, June 2001.

J. Coit, S. Staniford, and J. McAlerney. *Towards Faster Pattern Matching for Intrusion Detection: Exceeding the Speed of Snort*. Proceedings of DISCEX II, Anaheim, June 2001.

R. Feiertag, S. Rho, L. Benzinger, S. Wu, T. Redmond, C. Zhang, K. Levitt, D. Peticolas, M. Heckman, S. Staniford-Chen, and J. McAlerney, *Intrusion Detection Inter-component Adaptive Negotiation*. Computer Networks. 2000.

S. Staniford, J. Hoagland and J. McAlerney. *Practical Automated Detection of Stealthy Portscans.* Proceedings of the ACM CCS IDS Workshop,November 1, 2000. Athens, Greece.

R. Feiertag, S. Rho, L. Benzinger, S. Wu, T. Redmond, C. Zhang, K. Levitt, D. Peticolas, M. Heckman, S. Staniford-Chen, and J. McAlerney,. *et al*. *Intrusion Detection Inter-Component Adaptive Negotiation.* Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID 99), Lafayette, Indiana; September, 1999.

S. Staniford-Chen, B. Tung, and D. Schnackenberg,. *The Common Intrusion Detection Framework (CIDF).* Proceedings of 1998 Information Survivability Workshop – ISW'98, Orland, Florida; October, 1998.

S. Staniford-Chen, S. *et al* *GrIDS: A Graph-Based Intrusion Detection System for Large Networks*. Proceedings of the 19th NISSC, Baltimore, 1996.

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. 1995.

J. Kiskis and S. Staniford-Chen, *Universal Amplitude Ratios and Functions for the SU(2), Finite-Temperature Phase Transition*. In Axen, D., Bryman, D., and Comyn, N. (eds) Vancouver Meeting. Particles and Fields '91. p 821. World Scientific. 1992.

Published Reports and Theses

N. Weaver, V. Paxson, and S. Staniford, *The Worst Case Worm.* Silicon Defense Technical Report. August 2003.

S. Staniford and C. Kahn, *Worm Containment on the Internal Network.* Silicon Defense Technical White Paper. March 2003

N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, *Large Scale Malicious Code: A Research Agenda*. Silicon Defense Technical Report, Dec 2002.

B. Tung, et al. The Common Intrusion Detection Framework Specification. Nov 2001.

S. Staniford, O.S. Saydjari, and K. Williams *The US is Not Safe in a Cyberwar*. Paper presented to Department of Defense and National Security Council executives. May 2001. 2nd Edition.

S. Staniford, O.S. Saydjari, and K. Williams *The US is Not Safe in a Cyberwar*. Paper presented to DARPA. Sep 2000.

S. Cheung, S. *et al* *The Design of GrIDS: A Graph-Based Intrusion Detection System*. UCD Technical Report CSE-99-2, January, 1999.

S. Staniford-Chen, *Distributed Tracing of Intruders*. Master's Thesis, University of California at Davis. 1995.

S. Staniford-Chen, Finite Size Scaling and the Universality Class of SU(2) Lattice Gauge Theory. PhD Thesis, University of California at Davis. 1993**.**

S. Staniford-Chen, Finite Size Scaling of Probability Distributions in SU(2) Lattice Gauge Theory and Phi^4 Field Theory . Preprint UCD-92-17, University of California at Davis. 1992.

Patent Filings

S. Staniford and M. Bakshi, *A System and Method for Selecting Memory Locations for Overwrite.* Filed January 23rd, 2006

S. Staniford *et al*, *A System and Method for Aggregating and Consolidating Security Event Data.* Filed November 26th, 2005

S. Staniford and T. Mustafa, *A System and Method for Deprioritizing and Presenting Data.* Filed November 4th, 2005

S. Staniford and P. Sobel. *System and method for storing multi-dimensional network and security event data*. Filed October 14th, 2005

S. Staniford, C. Kahn, N. Weaver, C. Coit, and R. Jonkman , *Method and system for reducing the rate of infection of a communications network by a software worm.* Filed December 6th, 2002. Filing serial number: 313623.

S. Staniford et al. *Systems and Methods for Detecting Malicious Network Content.* Application #20100115621.

S. Staniford et al. *Systems and Methods for Detecting Malicious PDF Network Content.* Application #20110247072.

A. Aziz et al. *Electronic Message Analysis for Malware Detection.* Application #20110314546.

Software Systems

FireEye Multiflow Virtual Execution Engine. I designed and personally implemented a high-speed multithreaded multicore Bayesian prioritization/detection engine for web traffic which allowed selection of about 1 in 5000 objects from an HTTP stream to be replayed in virtual machines for detection of web drive-by attacks. The system has so far scaled to 4Gbps with only minor modifications to the original architecture, and has been extended to cover PDF and SWF in addition to the original HTTP/HTML/JS. Currently about 100kloc of C.

Nevis Event Correlation System. I architected this high-speed multithreaded event correlation system intended to handle very large event volumes and flow rates from a global deployment of high speed security switches. The system was designed to scale naturally across multiple processors and involved a novel external memory algorithm capable of storing and retrieving event data orders of magnitude faster than SQL databases.

CounterMalice was the first automated worm containment system in the world capable of containing zero-day worms, and became a commercial product. It operates by dividing a network into cells, recognizing wormlike behavior, and suppressing spread of a worm from one cell to another. CounterMalice was developed with Cliff Kahn, Nick Weaver, Jason Coit, Roel Jonkman, Joe McAlerney, and Dan Watson. My role was providing the initial vision, developing quantitative methods for tuning the system such that its performance against worms could be engineered in advance, and coding portions of the user interface.

Spice was the first system capable of detecting stealthy portscans from multiple sources using simulated annealing to correlate disparate events. It became part of a commercial product (CounterStealth). Spice was developed with James Hoagland and Dan Watson. My role was initial vision, much of the design, and techniques for validating its performance.

Spade was a network anomaly detection system (used as an input to Spice). It became well known and gained widespread operational use when it was incorporated as a plug-in into the open-source GPL intrusion detection system Snort. Spade was developed with James Hoagland. My role was the basic idea and much of the design.

Snortsnarf was an open-source alert viewer for Snort, that was innovative in systematically taking account of the possibility of attackers deliberately targeting the user interface screen real-estate. Snortsnarf gained widespread operational use at sites generating large volumes of Snort alerts, and was the main user interface for intrusion detection at the 2002 Winter Olympics. Snortsnarf was developed with James Hoagland. My role was to build the first version of the system, and provide design input during ongoing maintenance and extension.

GrIDS was the first intrusion detection/correlation system capable of correlating alerts hierarchically to infer the presence of large scale automated attacks throughout a network (including scans and worms). The system could handle a wide variety of inference tasks through a set of rules that assembled activity into distributed graphs which the system reasoned about. The inference hierarchy could by dynamically rearranged via a drag-and-drop UI. GrIDS was developed with Mark Dillinger, James Hoagland, Chris Wee, Dan

Zerkle, Rich Crawford, Steven Templeton, Stephen Cheung, and Karl Levitt. My role was that of team leader/group facilitator, contributor to the design of the inference mechanism and hierarchy, and implementer of the components that supported the rearrangable hierarchy. GriDS was tested in a medium-sized deployment at UC Davis.

External Funding Obtained

Northrop Grumman (subcontract under DARPA contract). International Coalition Exercises. $203k (2002-2003)

BBN Technologies (subcontract under DARPA contract). Information Assurance Operational Experimentation. $500k (2002-2003)

DARPA Internet Trap-and-Trace. $2.3m (2000-2003). With Felix Wu (UC Davis) and Vern Paxson, ICIR.

US Air Force, Rome Labs. IA-INTER-OP IETF IDWG. $145k (2001-2003). Co-PI with Joseph Betser

WetStone Technologies (subcontract under DARPA contract). NetFlare IDWG subcontract. 2000-2001

US Air Force, Rome Labs. IDS Correlation Using IDWG. $50k (2000-2001)

University of California, Davis (subcontract under DARPA contract). Global Guard: A Protection Architecture for Survivability of Large Scale, High-Confidence Information Networks. $90k (1999-2000)

The Boeing Company (subcontract under DARPA contract). Multi-Community Cyber Defense. $480k (1999-2002)

EMC Corp. Explorations of Randomness in Hard Disk Rotation Times. $32k (1999-2000)

Network Associates (subcontract under DARPA contract). *Intrusion Detection InterComponent Adaptive Negotiation.* $100k (1998-1999)

Service

Blogging at earlywarn.blogspot.com, November 2009-Present. Pro-bono research on global risks.

Editor of **The Oil Drum**, September 2005 – February 2008. Wrote hundreds of posts for this popular blog on the scientific issues of peak oil and energy economics. Conducted major forensic investigation into condition of Saudi oilfields.

Program committee member of the **ACM Workshop on Rapid Malcode (WORM).** 2005

Advisory board member for the **Collaborative Center for Internet Epidemiology and Defenses**. 2004-present

General chair/program committee member of the **ACM WORM Workshop**. 2003

Co-organizer of the DIMACS Workshop on Large Scale Attacks, 2003.

Program committee member of the Symposium on **Recent Advances in Intrusion Detection (RAID)** from 1999-2003.

Member of the **Mitre CVE Editorial Board**. This group developed a standard naming system for computer vulnerabilities. (1999-2002, now emeritus member)

Founder/cochair of **IETF working group IDWG** (1999-2004). This group developed a set of documents to allow common reporting by disparate intrusion detection systems.

Founded and chaired the **Common Intrusion Detection Framework** working group, at the request of DARPA (1998-2000). This group was responsible for developing a standard for all DARPA-funded intrusion detection researchers to build their systems to in order to allow inter-operation.

Invited Presentations

Association for the Study of Peak Oil. *Status of North Ghawar.* Houston Annual Conference, October 2007.

ABN-Amro. *Status of North Ghawar.* Presentation for analysts and clients. Aug 2007.

Association for the Study of Peak Oil. *Is Peak Oil Here?* Boston Annual Conference, October 2006.

Usenix Security, 2004. *Military Strategy in Cyberspace.* San Diego, August 2004.

University of California, Davis. *Worms and Worm Containment.* Seminar at Computer Science Department, Feb 2003.

John Moores University Computer Science Department. *Worms and Worm Containment.* Seminar at Computer Science Department, Dec 2003.

DIMACS Workshop on Large Scale Attacks. *Introduction to Worms and Worm Containment.* Oct 2003.

The Forum on Information Warfare. Future *Technologies of Cyberwar Operations*. November 2003

Microsoft Corporation. Worms and CounterMalice – presentation to the Security Business Unit. Sep 2003.

Government Communications Conference. *Cyber-Weapons of Mass Destruction*. Invited Keynote Presentation. July 2003.

Annual Computer Security Applications Conference. *Defeating Worms.* Invited panel presentation. Dec 2002.

AT&T. *Worms and Anti-worm devices*. Invited presentation to security group. Sep 2002.

National Security Agency. *Worms and Traceback.* Invited presentation to technical groups. Aug 2002.

UC Berkeley. *Military Strategy in CyberSpace*. Invited lecture as part of a special series of lectures on critical infrastructure protection. Mar 2002.

Ground Systems Architectures Workshop. *CyberSpace risks to Ground Systems*. Invited presentation on risks to satellite ground systems due to dependence on the Internet. Mar 2002.

Annual Computer Security Applications Conference. *IDWG Progress Report* – invited panel presentation. Dec 2001.

ACM Conference on Computer Security. *Detecting Distributed Portscans*. Tutorial as part of joint tutorial with Vern Paxson on Intrusion Correlation. Nov 2001.

RAID Symposium. *State of Intrusion Detection*. Invited Panel Presentation. Oct 2001.

National Security Telecommunications Advisory Council. *The US is not safe in a cyberwar*. Joint work with O. Sami Saydjari (presenting) and Ken Williams. June 2001.

SRI Workshop on Adversary Characterization. *Cyberwar and Strategy – some lessons from history.* Aug 2001.

SANS National Conference. *Viewing Snort Alerts with Snortsnarf.* May 2001.

CanSecWest. *Spade and Spice*. Mar 2001.

RAID Symposium. IDWG: Progress towards an open IDS alert standard. October 2000.

National Security Council. Presentation to members of the NSC staff on future risks from cyber attacks on US. Sep 2000.

RAID Symposium. IDS Standards – Lessons Learned to Date. September 1999.

CIO Council, Monterey Meeting. *Standardizing IDS Alerts*. March 1999.

White House Workshop on Cybersecurity Research. *Standardizing IDS Alarms*. February 1999.

Selected Press Coverage of Work

My work has been featured in several dozen stories in major media and technical publications. A small sample include:

New York Times Thieves Winning Online War, Maybe Even in Your Computer
http://www.nytimes.com/2008/12/06/technology/internet/06security.html
A research report last month by Stuart Staniford, chief scientist of FireEye, a Silicon Valley computer security firm, indicated that in tests of 36 commercial antivirus products, fewer than half of the newest malicious software programs were identified.

ComputerWorld Antivirus no defense against botnets, says vendor
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9121901

A new analysis of botnets has come up with a possible reason for their prodigious ability to infect PCs: Many antivirus programs are near to useless in blocking the binaries used to spread them.

Atlantic Magazine Running Dry
http://www.theatlantic.com/doc/200710/oil-field-decline
The world's most essential oil field may be in decline.

Business Week To Trap a Superworm
http://www.businessweek.com/technology/content/feb2003/tc20030225_4104_tc047.htm
The Slammer worm's ability to spread so rapidly adds a frightfully new dimension to the species. Does Stuart Staniford have the cure?

PC World Dawn of the Superworm,
http://www.pcworld.com/news/article/0,aid,110014,00.asp

ComputerWorld Study: Slammer was fastest spreading worm yet,
http://www.idg.com.hk/cw/readstory.asp?aid=20030205005

The Independent Internet worm took 10 minutes to create global chaos,
http://news.independent.co.uk/digital/news/story.jsp?story=375374