Stuart Staniford

317 N. Aurora St, Box #2,
Ithaca, NY 14850,
stuart@staniford.systems

Summary

I am an inventor and entrepreneur with three decades of experience innovating in network security. I was an executive and a key inventor during the rise of FireEye, which was crowned the *"Hottest Security Startup in Silicon Valley"* by Forbes Magazine, went IPO in September 2013, and subsequently reached a market value of $10b. I have innovated in detecting web application attacks, Chinese APT attacks, web drive-by attacks, and network worm propagation. I have raised millions in funding, spent years on executive management teams, sold into Fortune 500 accounts, closed seven figure deals, and interacted with boards. My security research papers and patents have been cited more than 11,000 times in the scientific literature, as well as being covered in major national magazines and newspapers. I have been an expert witness and testified at trial. I have extensive hands-on development experience in C, C++, Javascript, and Perl, and am intimately familiar with HTML/JS and HTTP.

Experience

Staniford Systems. President, April 2017 – Present

Independent technology consultant for various clients.

Viridius Property. President, April 2014 – Present

Developed this real estate company providing fossil-fuel free rentals for both residential and commercial markets.

Cayuga Networks. CEO/CTO, April 2014 – Feb 2017.

Founded this startup in Ithaca, NY, developing a high-speed network web application attack detection system. Recruited engineering, office, and executive staff, supervised setup of initial systems, instituted continuous integration development methodology and raised $2.3m in outside venture capital. Sold into Fortune 500 accounts. Managed a team of 20. Company failed to establish sufficient traction in time.

FireEye. Chief Scientist, Jan 2008 – Feb 2013.

Developed novel statistical algorithms to detect exploit websites installing malware on client computers. This allowed FireEye to repurpose its existing product line, which was previously failing in the marketplace, as a solution to the drive-by download 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 over $10b 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 successfully went public in September 2013, and the share price went from 7c when I joined to a peak over $95 as of early 2014. I was a member of the management team throughout my tenure at FireEye, reporting directly to the founder and CEO, and participated in all executive planning and operational discussions.

Cornell University. Adjunct Professor of Computer Science, Jul 2013 – Jun 2016.

Taught graduate course on Defending Computer Networks for three years.

Invicta Consulting. President, 2005 - 2007

Solo consultant. Technical consulting for several startups – found security vulnerabilities and false negatives in products, designed algorithms, analyzed competing products for effectiveness. Also worked as litigation consultant and expert witness for several law firms – analyzed patents and prior art, wrote expert report, defended analysis at deposition, testified at trial.

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 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. 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.

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

Founded and co-chaired 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. UC Davis. Advisor: Prof. Karl Levitt

Ph.D. (Physics) June 1993. UC Davis.

M.S. (Physics) June 1990. UC 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.

Patents

A. Aziz, H. Uyeno, J. Manni, A. Sukhera, and S. Staniford, *Malicious network content detection.* Patent #10,757,120. August 25th, 2020.

S. Staniford, *System and method to protect a webserver against application exploits and attacks.* Patent #10,432,650. Oct 10th, 2019.

A. Aziz, S. Staniford, M. Amin, H. Uyeno, and S. Yie, *Method for detecting malware within network content.* Patent #10,282,548. May 7th, 2019.

A. Aziz, H. Uyeno, J. Manni, M. Amin, and S. Staniford, *Electronic message analysis for malware detection.* Patent #10,027,690. July 17th, 2018.

S. Staniford and A. Aziz, *Systems and methods for analyzing PDF documents.* Patent #9,954,890. April 24th, 2018.

A. Aziz, S. Staniford, M. Amin, H. Uyeno, and S. Yie, *Detecting malicious network content.* Patent #9,519,782. December 13th, 2016.

S. Staniford and A. Aziz, *Systems and methods for analyzing malicious PDF network content.* Patent #9,438,622. September 6th, 2016.

S. Staniford and A. Aziz, *Systems and methods for detecting malicious PDF network content.* Patent #9,118,715. August 25th, 2015.

A. Aziz, H. Uyeno, J. Manni, M. Amin, and S. Staniford, *Electronic message analysis for malware detection.* Patent #9,106,694. August 11th, 2015.

S. Staniford and A. Aziz, *Systems and methods for detecting malicious PDF network content.* Patent #8,997,219. March 31st, 2015.

S. Staniford and A. Aziz, *Systems and methods for scheduling analysis of network content for malware.* Patent #8,990,939. March 24th, 2015.

S. Staniford and A. Aziz, *Systems and methods for detecting malicious network content.* Patent #8,850,571. September 30th, 2014

Other Patent Filings

S. Staniford. *Denial of Service and other resource exhaustion defense and mitigation using transition tracking.* US20160182542A1. Filed December 18th, 2015.

S. Staniford and M. Bakshi, *A System and Method for Selecting Memory Locations for Overwrite.* US20070174563A1. Filed January 23rd, 2006

S. Staniford *et al*, *A System and Method for Aggregating and Consolidating Security Event Data.* US20070261061A1. Filed November 26th, 2005

S. Staniford and T. Mustafa, *A System and Method for Deprioritizing and Presenting Data.* US20070118906A1. Filed November 4th, 2005

S. Staniford and P. Sobel. *System and method for storing multi-dimensional network and security event data*. US20070088719A1**.** 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. US20040111531A1.* Filed December 6th, 2002.

Litigation Consultant/Expert Witness Matters

I have been asked to provide expert opinion in the following litigation matters:

Centripetal vs Keysight (E.D. Vir. 1:2022cv00001). 2022-2023. Law Firm Reed Smith for Keysight. Provided declarations in support of IPRs of patents 10,193,917, 10,609,062, and 10,567,343.

Finjan vs Palo Alto Networks (N.D. Cal. 14-cv-04908-PJH). 2022. Law Firm Fish and Richardson for Finjan. Consulted on infringement contentions for US patents 8,225,408 and 8,141,154.

British Telecommunications vs Fortinet (D.Del., 1:18-cv-01018). 2021. Law Firm Keker, Van Nest, & Peters for Fortinet. Consulted on prior art (patent 7,693,971).

Fortinet vs British Telecommunications (IPR2019-01327, IPR2019-01328). 2019. Law Firm Duane Morris for Fortinet. Researched prior art and completed expert declaration (patent 7,370,358).

Nomadix vs Guest-Tek (IPR2018-00376). 2018. Law Firm Knobbe Martens for Nomadix. Consulted on litigation positions.

Cisco vs Centripetal (IPR2018-01436, IPR2018-01437, IPR2018-01559, IPR2018-01760). 2018-2019. Law Firms Merchant Gould and Duane Morris for Cisco. Researched prior art, prepared claim charts, completed expert declarations, (patents: 9,124,552; 9,160,713; 9,686,193; 9,413,722). Was deposed on three patents.

DeepNines vs McAfee (E.D.Tex., 9:06-cv-00174). 2007. Law Firm Williams Morgan for McAfee. Researched prior art, prepared claim charts.

SRI vs ISS (D.Del., 1:04-cv-01199). 2005-2008. Law Firm King and Spalding for ISS. Researched prior art, argued patent invalidity and non-infringement on several of the patents in suit (patents 6,321,338; 6,484,203; 6,708,212). Wrote expert report, was deposed, and testified at trial on one of the patents (due to division of labor between several experts). The client won on the patent I testified on.

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

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

Atlantic Magazine Running Dry
http://www.theatlantic.com/doc/200710/oil-field-decline

Business Week To Trap a Superworm
http://www.businessweek.com/technology/content/feb2003/tc20030225_4104_tc047.htm

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