CRIMSON VISTA
TECHNICAL CONSULTING & LITIGATION SUPPORT

Seth James Nielson's Vita

410.497.7384
seth@crimsonvista.com
sethjn@cs.jhu.edu
July 2018

Academic Degrees

2010	**Ph.D. Computer Science,** *Rice University*, Houston, TX
2004	**M.S. Computer Science,** *Brigham Young University*, Provo, UT
2000	**B.S. Computer Science,** *Brigham Young University*, Provo, UT

Current Appointments

Founder and Chief Scientist	Crimson Vista, Inc.
Director of Advanced Research Projects	Johns Hopkins University Information Security Institute
Adjunct Associate Research Scientist	Johns Hopkins University Dept. of Computer Science
Senior Professional Staff (Temp/On-Call)	Johns Hopkins University Applied Physics Lab

Subject Matter Expertise and Selected Projects

Applied Cryptography

"Crypto Done Right", Cryptographic Knowledge Base (2017-2018): Co-investigator and co-maintainer of the "Crypto Done Right" project (https://cryptodoneright.org). Cryptographic knowledge based derived from three-year research funded by Cisco. Investigating how to bridge the gap between cryptographers and cryptography users in terms of deployment and lifecycle management. Wrote the grant proposal and am managing day-to-day operations.

Technical Training – *U.S. Dpt. of Justice* (Antitrust Division, Transportation, Energy & Agriculture) (2018): Provided technical guidance and training for cryptographic technologies involved in a potential merger.

Cryptographic Protocol Analysis and Design – *Confidential Client* (2017-2018): Reviewed secure transport protocols for weaknesses and designed improvements. Built rapid prototypes for validation and testing.

Anti-Collision Protocols – *JHUISI/OnBoard Security* (2017): Mentored a student group investigating exploitability of anti-collision protocols used in aircraft. Demonstrated the vulnerability and created a cryptographically secure version using drones.

Lightweight Cryptographic Authentication Algorithms – *Confidential Client* (2016-2017): Analyzed cryptography in patent related to sequences of hash chains. Identified critical prior art and combinations of prior art.

TLS Protocol Analysis – *Confidential Client* (2015): Evaluated the TLS protocol to determine differences between 1.0, 1.1, and 1.2 variants. Also assessed potential patent infringement and prior art relevancy.

Cryptographically Certified Physical Measurements Analysis – *Client Confidential* (2015): Evaluated a patent related to cryptographically signing a physical measurement, such as a temperature, before submission over a network. Evaluated the patent against other patents from the same time period or earlier. Submitted expert declarations for PTAB actions.

Cryptographic Communication Library – *Security First Corp.* (2010-2011): Managed the project from start to finish. Collected the requirements from the client, created the design, implemented the prototype in Python, led the development team for the C++ version, and so forth. The technology used multiple SSL channels with different signing authorities to reduce the possibility of compromise from a rouge CA.

Encryption Library – *Security First Corp.* (2005-2011): Designed and developed a wide range of features and extensions to an encryption library over a long period. Subprojects include:

Prototyped algorithms from cryptographic specification
Developed significant portions of the first release
Designed and implemented a testing framework along with an initial suite of tests
Assisted in creating features and performing testing necessary for FIPS certification
Created a GPU-accelerated variant of the library
Created a ZFS file system providing secure storage using the encryption library

IoT Devices and IoT Security

IoT Management Platform Assessments – *JHUISI/JHUAPL* (2018): Co-investigator on this research in collaboration with industry partner and the Johns Hopkins Applied Physics Lab. Analyzing various threat models for information aggregation in IoT management and developing profiles for IoT behavioral identification. Mentoring related student capstones Summer and Fall 2018.

IoT Physical Forensics – *JHUISI* (2017): Mentored a group of students exploring how IoT devices can be used for physical forensics including tracking a person's movements through a building. Published results in peer-reviewed article.

Network Security

Curriculum Design – *The Johns Hopkins University* (2013-2018): Created a network security curriculum for graduate studies. Developed custom lab work that simulates protocol stack development and application security. Student teams explore attacking autonomous bots, financial institutions and military targets.

Network Security Device Analysis – *Blue Coat* (2017-2018): Reviewed and analyzed the source code for Blue Coat as a technical expert in a patent-related litigation matter. Examined source code, design documentation, and other materials related to SSL visibility, automatic malware sandboxing analysis, automated threat identification, and content categorization. Testified in court.

Telephony-based Security Analysis – *TeleSign* (2016-2018)**:** Reviewed and analyzed the technologies behind various security technologies as a technical expert in multiple patent-related litigation matters. Searched and analyzed prior art, evaluated technical designs, and wrote multiple reports with my findings.

Domain Name Anti-Abuse Technologies Analysis – *Afilias* (2015): Evaluated the design documents, technical specifications, and engineering tickets related to Afilias' Anti-Abuse project.

Evaluated the design, patents, and source code of a competitor accused of misappropriating trade secrets. Submitted expert reports and testified at trial.

Cloud Storage System Security Evaluation – *Confidential Client* (2015): Investigated attacks on the virtual machine appliance, attacks on the local network access, and attacks on the cloud data storage. Approach included analyzing the protocols for the data in motion and the data at rest. Used penetration testing tools including Metasploit.

Secure Gateway Software Security Evaluation – *SecurityFirst Corp* (2015): Evaluated for regulatory compliance issues related to HIPAA, FISMA, SOX, GLBA, NERC, ISO 27002.

High-speed Firewalls Analysis – *Confidential Client* (2012-2014): Evaluated a wide range of firewall designs and source code. Firewall code was written in highly-optimized C for devices meant to handle 10-100 Gbps traffic even while performing layer-7 content evaluation. Assessed code for infringement relevancy.

Software Engineering *Google Inc*. (2005): Summer internship project created a work-around for incorrectly configured Internet web servers. Used heuristics to determine if pages should be removed from the cache even if the server reported that caching was acceptable.

Malware and Viruses

Malware Analysis – *Confidential Client* (2016): Analyzed suspicious executables for malicious behavior. Reverse-engineered binaries using IDA-PRO and also tested them dynamically.

Anti-Key-Logging Software – *Confidential Client* (2015): Evaluated this software, written in C, C++, JavaScript, and other miscellaneous languages to determine changes in the product from 2007 to the present. Also assessed potential patent infringement and prior art relevancy.

Anti-virus, Anti-malware, and Secure Gateways – *Sophos* (2014-2015): Reviewed the technologies between two competitors. Evaluated the code written in C, C++, Perl, Php, and other miscellaneous languages to determine infringement and prior art relevancy. Evaluated custom modification to the Linux kernel for multi-device clustering. Evaluated cloud-based anti-virus technologies. Evaluated patents from both sides. Submitted expert reports and provided a technology tutorial in court.

Anti-virus Analysis – *Confidential Client* (2011-2012): Evaluated source code of two competitors written in C, C++, and other languages. Re-created virus-like signatures from the 1995 era to test against heuristic scanners from that time period. Re-created a gateway-like product for scanning for viruses in FTP transmissions using 1995 era scanners and Java. Assessed source code for infringement and prior art relevancy.

Privacy

Anonymization of Threat Indicators *JHUISI/JHUAPL* (2017): Mentored a student project in conjunction with APL to identify if threat indicators submitted to the AIS project could be de-anonymized. Identified various potential problems and proposed solutions.

Anonymization of Health Records – *Confidential Client* (2014-2015): Evaluated the design documents, specifications, and code of two different competitors. The code, written in PL/SQL, shell scripts, Java, and other languages, remove personally identifying data from medical records. Assessed the code for infringement and prior art relevancy.

An Evaluation of the Mark Monitor Anti-Piracy System – *Center for Copyright Information* (2013-2014): Evaluated the design, implementation, and practices of Mark Monitor's system for identifying online piracy. Our task was to determine to what extent an individual's privacy was adequately protected in their investigation, analysis, and subsequent operations. We produced an internal report of which an executive summary was made publicly available (http://www.copyrightinformation.org/wp-content/uploads/2014/11/Harbor-Labs-Executive-Summary.pdf).

Corporate Spyware Evaluation – *Confidential Client* (2013-2014): Evaluated images, keystrokes, and screenshots captured by corporate-installed spyware related to a class-action lawsuit. Assessed to what extent the data violated wiretapping laws.

Miscellaneous Security Technologies

Cyber-Physical Systems – JHUISI (2018): Mentored student group analyzing attacks on portable chemical systems (Continuous Flow Reactors). Discovered various vulnerabilities and published research findings in peer-reviewed article.

Open-Source Contribution and Sponsorship – *The PyPy Project* (2018): Maintainer of the PyPy Sandbox for sandboxed execution of untrusted Python scripts. Modernized for Python 3 support and deployed to academic projects such as the JHU Network Security course.

Blockchain and Smart Contract Design – *Confidential Client* (2018): Analyzed the suitability for a start-up's technology to use the Blockchain and, in particular, Smart Contracts to provide greater visibility and transparency to customers.

Medical Device System Security Valuation – *Confidential Client* (2015): Led consulting team that analyzed medical devices for potential vulnerabilities. Identified serious buffer-overflow attack. Reported identified issues and provided training to client.

Corporate Patent Portfolio Review – *Confidential Client* (2014): Evaluated approximately 75 patents related to secure enclaves in a client's portfolio. Assessed which patents were the strongest in terms of novelty, technical merit, etc**.**

Network Architecture and Communications

M2M Technologies Analysis - *Telit* (2014-2015): Evaluated the design of a "machine-to-machine" protocol. Submitted expert reports.

Cross-Device Advertisement Tracking – *Confidential Client* (2014-2015): Reviewed the technologies behind cross-device tracking in ESPN and Adobe advertisement systems for a class action lawsuit. Submitted an expert declaration to the court.

Mobile Phone Communications – *Confidential Client* (2014): Evaluated both iOS and Android phones to determine to what extent they can transmit data over cellular and Wi-Fi simultaneously. Conducted experiments by writing and deploying apps to a number of devices.

Software Engineering and Software Analysis

Cyber Insurance Investigation – *Clyde & Co* (2017): Reviewed claims regarding software costs and effort made to cyber-insurance underwriters for reasonableness and validity.

Mid 1990's Screen Sharing Technology Resurrection – *Client Confidential* (2015): Reconstructed a working demonstration of screen sharing technology from the mid 90's. Used 1990's era machines, source code compilers, and utilities. Accessed incomplete CVS repository to extract code and figured out which parts were missing. Created small modifications to fill in gaps and get working C, C++, Java, and C# code.

Financial Trading Software – *Confidential Client* (2016): Reviewed two different automatic financial trading systems, including source code, to assess potential misappropriation.

Configuration Software – *WTS Paradigm* (2016)**:** Reviewed two different software projects, including source code, that provide configuration/customization of products to customers. Evaluated the similarities and differences of the two and set forth my opinions in an expert report.

Distributed Code Coverage Tool – *Confidential Client* (2011): Created a parallelized utility for applying gcov across a large software system. Designed and implemented all of the parallel mechanisms including failure handling, communication, and so forth.

Software Engineering – *Metrowerks Inc.* (2001-2003, formerly Lineo Inc.): Maintained the source code for multiple components of the Embedix Software Development Kit (SDK) including the GUI and the package management system. Also ported the system from Linux to Windows and developed an automatic translation layer for Linux packaging scripts.

Source Code Reviews – *Various Clients* (2016-2018): Reviewed and analyzed source code relating to the following technologies:

Digital Mobile Radios (DMRs)
Firewalls and Security Devices
Commercial CAD software
Robotic Vacuums
Anti-phishing Technology
Anti-keyloggers
Video Content Distribution
Cryptography
Fitness Tracking Devices
Secure Email
Android/iOS code
DRM systems
Cloud-based Multimedia
Document signing
High Frequency Trading Platforms
Mobile Device Network Protocol Stacks
VoIP Systems
Peer-to-Peer Communications
PBX Telecommunications Software

Academic Leadership

Director of Advanced Research Projects at The Johns Hopkins University Information Security Institute (2016-Present)

Tasked with building collaborative bridges to external companies and institutions as well as the Johns Hopkins University Applied Physics Lab. Wrote grant proposals, connected faculty with funding sources, and collaborated on various research initiatives.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.