Resume of
Paul W. Nelson
4810 Arabian Ct.
Arlington TX 76017
817.480.7125
nelsonlogic@me.com

Self Employed
March 2021 to Present

I am building a SwiftUI vision recognition-based application for iOS that makes use of the iOS text recognizer. This application is fully internationalized and makes use of the user's location to record text properly. My github project CompactLocation is a Swift package to make location reverse lookups provide caching and improved localization for pricing and numbers. You may review the CompactLocation code at https://github.com/paulnelsontx

Consultant, Self Employed
November 2020 to Present

I perform consulting and software development services to a company in the user identity/authentication business. Skills include iOS development, cryptography, public key infrastructure and encryption. I developed a CryptoTokenKit implementation for a customer for use in an iOS application where hardware tokens were required.

From November 2020 through March 2021, I worked with the worldwide OpenSSL team **www.openssl.org** to help them adopt agile methods to provide better visibility into the status of the project for FIPS sponsors. The team needs to get OpenSSL 3.0.0 into the FIPS validation queue by September 2021. To better understand the OpenSSL team's workflow, I took on one of the issues and wrote some sample code showing how to use the new APIs. I set up the team to use ZenHub for a Kanban board and to help them plan sprints. The Kanban board for OpenSSL can be viewed here. I wrote some code to use GraphQL to collect data from GitHub that helped identify trends for the project. In addition to working with the team, I was responsible for handling OpenSSL premium support contracts. Customers with a premium support contract can get security updates for OpenSSL 1.0.2 among other support offerings.

CTO and VP of Engineering, Thursby Software Systems, Inc.
Arlington Texas
www.thursby.com
1988-November 2020

Sub Rosa Mobile applications – 2010 to 2020

In 2010 I began a new product offering for Thursby using smart card readers with mobile devices. The project was originally named PKard and was renamed and marketed as Sub Rosa a few years later. The solution provides a web browser with TLS two-factor authentication that could be used by military and federal government personnel to access unclassified web sites. Since FIPS 140-2 was a requirement, I worked with OpenSSL and Steve Marquess and Tim Hudson. OpenSSL was working on the FIPS 140 validation for iOS and I was able to provide

some software to handle fingerprinting for macho binaries. I integrated our CAC and PIV middleware with the OpenSSL code because iOS had no way of integrating with their own TLS. They also lacked FIPS 140 for iOS at the time. We had to implement an HTTP layer for TLS to integrate with Apple's UIWebView.
As our mobile technology advanced, we added support for Microsoft Exchange and included S/MIME leveraging smart cards for signing and decrypting mail. We use the OpenSSL PKCS7 code in our solution. We now support Exchange 2010, 2013 and O365. We settled on using agile methods and use JIRA and Bitbucket.

While I was attending a conference for the Department of Defense Information Systems Agency (DISA) I talked with a Navy captain about our technology. Thursby worked with the Navy to develop the Ready 2 Serve (R2S) mobile application that allows Navy reservists to do all their computer work from their own mobile device. Our solution won a Navy award for innovation. We were able to obtain an authorization to operate (ATO) from the Navy Cyber Command. R2S is currently used by 40K reservists. This is the largest and one of the first bring your own device (BYOD) projects in the US military.

During these years I managed development of our corresponding Android product as well. We use OpenSSL on the Android platform for the same purposes.

I have worked with military and government agencies promoting our solution and developing custom derivations. I am very comfortable pitching technology and I excel at explaining complex systems.

DAVE and ADmitMac – 1995-2015

In 1995, I thought integrating the Macintosh platform with Microsoft Windows 95 would make a useful product. My team built the code and I build the networking parts. Around that time, Microsoft decided they would push their SMB file protocols as an open standard named CIFS for common internet file system. They held the first CIFS conference in Redmond, and we participated and demonstrated our Mac client next to a Windows 95 computer connecting to a Samba server in Australia. I think we were the most surprised as anyone when the demo worked. As this product was developed further, we added a file server for the Mac and supported printing. When Mac OS X came out, we built our file system as a kernel extension. I have extensive experience with kernel programming both on the Mac and previously on a number of UNIX platforms, including symmetric multiprocessor kernels.

While developing DAVE, I told Bill Thursby (our president) that we needed a code name for the project. He suggested naming it after my family's new dog, Dave, that I was less than thrilled about. I figured we would have to change the name later, but we never did. DAVE was one of my most successful products.

Later, we added Active Directory integration. In 2013, we worked with the US Army NETCOM to integrate Common Access Card support on the Macintosh platform building our PKINIT and integrating it with LDAP with the help of Sam Hartman (MIT) and Love Hörnquist (Heimdal)

Network protocols 1988-1994

Bill Thursby and I were friends at Michigan State University. When he started Thursby Software Systems, he wrote a DECnet stack for the early Macintosh computers. I was the fourth employee at Thursby and spent the early years developing DECnet stacks for Sun and ATT UNIX computers, integrating with the kernel for both BSD and Streams environments. This product sold under the name TSSnet.

Software Developer, RDA
Tacoma Washington
1986 to 1988

I worked on a contract developing a computerized management system for Army maneuvers for the Army Development and Employment Agency (ADEA)

System Engineer, Boeing Aerospace
Kent Washington
1979 to 1986

I worked for the Boeing research and development team developing some of the first digital autopilots for missiles. I developed all sorts of computer tools, simulations and test beds for a prototype autopilot. Later, I was part of a team of engineers working on one of the first multi-level secure network solutions with the NSA

Software Developer, Michigan State University
East Lansing Michigan
1976 to 1979

1977-1979 I worked on a management information system for agricultural extension agents that was written in COBOL and used a relational database.

1976 to 1978 I worked with my Physics professor integrating an Eclipse minicomputer with our experiment at Fermilab in Batavia Illinois.

Education: BS Physics, Michigan State University

Skills:

Excellent communicator able to explain complex topics both verbally and in writing.
Project leadership.
Managing technical teams by seeking input from everyone and building consensus.
Software development: C, C++, Objective C, Swift, SwiftUI, Java, Kotlin, JavaScript/AJAX, HTML, ASN1.
TLS, Cryptography, X509 and PKI/PKE, PKCS1, PKCS7, digest and signature algorithms and suites used in TLS. Kerberos with PKINIT. Microsoft Active Directory.
Extensive experience with Apple platforms including iOS. Experience with Android development including JNI. Xcode and Android Studio.
I have experience with agile development, but with a pragmatic approach.
Implemented my own PDF viewer in Swift based on the Adobe specifications.