DIMITRIOS SIGANOS

11 Kirkby Close, Friern barnet, London N11 3FE
Company: Packet Storm Ltd, http://pstorm.co.uk

(14 Jan 1974, Greek / Japanese, dimitrios@siganos.org, 07931 931 942)
Linkedin: http://uk.linkedin.com/in/dsiganos

Profile

I am a software engineer specialising in cryptography/security, networking, embedded systems and multi-threaded applications. I operate at driver, kernel, protocol and application level of the software stack. I have experience in cryptography and in particular IPsec, RSA, PKI/X.509, WPA and smartcards. I have a good understanding of hardware, expert knowledge of C and good knowledge of C++, Java, Python, Tcl and shell scripting. I am experienced in Linux and RTOS (VxWorks, Velosity).

Work Experience - Contracts

- **Crypta Labs, London** (remote work): Nov 2019 – Dec 2019
  - Generating random numbers for quantum safe cryptography (openmv, movidius).
- **Pigzbe, London** (remote work): Sep 2019 – Nov 2019
  - ESP32 device-side software for a blockchain based digital piggy bank.
- **Toshiba Research, Cambridge** (remote work): Dec 2018 – June 2019
  - Writing linux C/C++ software for a high performance Quantum Key Distribution system (managing quantum cryptography and post quantum algorithms).
- **Hamillroad, Cambridge** (remote work): May 2018 – Dec 2018
  - Developing a pay-per-use software system for the printing industry using Gemalto USB dongles. Qt, Visual Studio, GUI development on Windows.
- **IoT Cashless Vision**, Malaysia (remote work): Q4 2017
  - RS485 to Cloud gateway SW/HW (Flask Python REST API)
- **Miura Systems**, High Wycombe (2 contracts, remote work): 2017, 2018, 2019
  - WiFi and Bluetooth connectivity to a payment device. Integrated WiFi and bluetooth (classic/BLE) on a Linux system using ltib build system. Implemented the system on Realtek RTL8723. Proof of concept on Espressif ESP32.
    https://github.com/dsiganos/vhcibridge
  - VISA VCAS qualification software
    Python Flask SOAP server implementing the VISA VCAS WSDL interface and controlling a contactless credit card payment device via bluetooth.
- **Timespace Technology**, Huntingdon (3 contracts, remote work)
  - Jan 2017 – Apr 2017, Oct 2015 – May 2016, Oct 2014 – Jan 2015
    Wifi connectivity of a bus security system using a linux based WiFi module.
- **Abaco Systems**, Towcester
  - May 2016 – Oct 2016: RedHawk Linux BSP, linux drivers
- **BSkyB**, Osterley
  - Nov 2014 – Sep 2015: Security/cryptography developer, C++11, xmldsig
    Infrastructure for signing and protecting third-party applications.
    Implemented internal test and development PKI hierarchies using openssl.

- **Abbott Point of Care**, Princeton, USA (remote work, multiple contracts, medical)
  - 2010 - 2016: Adhoc Wifi consultancy (medical device, Abbott Wireless iStat)
    https://www.pointofcare.abbott/us/en/offerings/istat/istat-wireless
  - Nov-Dec 2015: Backported SHA-2 (sha224, sha256, sha384, sha512) support to an old openssl library that only supported SHA-1.
  - Jan 2013 - Apr 2013: .Net app debugging and Windows 7 64-bit compatibility.
  - Apr 2012 – Jun 2012:
    Wifi, network protocol (TCP/IP), and, network application troubleshooting.
    Visited hospitals in USA for field debugging - all issues were solved.
  - Feb 2011 – May 2011 and Sep 2010 – Nov 2010:
    WiFi cryptography troubleshooting EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-MsCHAPv2. Fixed bugs in wpa supplicant, fixed issues with incompatible sets of ciphers in older windows, resolved issues regarding incompatible TLS key exchange methods (RSA vs Diffie-Hellman key exchange).
- **Laird Technologies** (previously called Ezurio), High Wycombe (6 contracts)

  Skills developed: Linux, buildroot,Velosity (Greenhills's Integrity kernel), WiFi 802.11, WPA, Interpeak, BSP, Atmel AT91M58000A, ARM, Python, Serial RS-232
  - Aug 2012 – Dec 2013: Wifi, buildroot, linux, wpa_supplicant development.
    I lead the development of a new product establishing the build framework, change and release processes, spearheading development and coaching the team.
  - Jan 2010 – Feb 2010:
    Implemented WiFi WPA Enterprise security (EAP, RADIUS, X.509 certificates) for a WiFi product that only supported WPA Personal.
  - Dec 2008 – Jul 2009:
    Ported TCP/IP stack to a new platform (uVelocity/ARM Cortex-M3) and introduced SSL security and GPRS connectivity (PPP, EAP, AT commands).
  - June 2006 – Oct 2007:
    Integrated the Interpeak TCP/IP stack with Velosity RTOS and in-house scripting language. Marvell Wifi 802.11 Linux driver. RS232 and power saving drivers.
- **Alertme**, Cambridge (remote work)
  - May 2014 – Dec 2014: Linux, python, xml-rpc, Zigbee, home automation
    Worked on Alertme's home automation hub fixing issues with zigbee devices.
- **YouView TV**, **BBC** media centre, London
  - Sep 2011 – Mar 2012:
    Openssl, hashing, X.509, linux, testing of Intertrust's Wasabi/Sockeye SDK, C++.
    Supported Huawei and Humax's engineers implement Youview security features.
    Devised a way to off-load the primitive RSA private key signing to an external organisation without having to change the way the high level signing worked.
    Implemented and maintained the X.509 test and development hierarchies.
- **Green Energy Options**, Hardwick, Cambridge (2 contracts)
  - Dec 2010 – Jan 2011: Embedded Linux development. Qt, webkit, C++.
  - Aug 2010: Embedded Linux. Buildroot, bifferboard, networking, multicast.
- **Airvana**, Cambridge (4 contracts)
  - Mar 2010 – Jun 2010:
    Integrated Strongswan with a smartcard chip (Atmel AT98SC) which acted as an HSM. Developed an openssl engine to integrate strongswan (IPsec daemon) with the smartcard/HSM drivers.

- Aug 2009 – Dec 2009:
  IPsec hardware acceleration using iMX51 Sahara. Implemented a Linux kernel crypto layer transform that made the Sahara crypto hardware available to the linux kernel through the standard linux crypto APIs and thus making it available to the IPsec module for offloading the encryption and hashing of IPsec packets.
- Nov 2008 – Dec 2008: Smartcard development. PKI, RSA, X.509.
  Developed drivers for the Atmel smartcard chip and provisioning tools to provision the smartcard with X.509 credentials and secret keys
- Oct 2008 – Nov 2008: PPPoE integration: uClinux, Blackfin, Interpeak.**Speakerbus**, Hoddesdon and Maidenhead
- Oct 2007 – Aug 2008:
  Designed, developed and tested a telephony gateway integrating RTP and T1/E1 based on a custom PowerPC board with a DSP daughtercard and running Montavista Linux. Worked on an telephony turret device that supported SIP and RTP calls. Wrote a CDR collection and dispatch module for the turret. Wrote a CDR forwarding application that run on both Windows and Linux servers. Developed multiple network python scripts for automatic testing of the devices. Wrote scripts for manufacturing processes and testing.

Work Experience – Permanent

- **Solarflare Communications**, Cambridge (Mar 2004 – Jun 2006)

  Skills developed: OpenOnload, TCP/IP, Ethernet, Linux kernel/drivers, Advanced C, C++, O/S bash shell scripting, CVS, multi-threaded, multi-core, super-scalar

  Developed the IP layer of TCP/IP stack and interfacing to the layers above (TCP, UDP, Sockets) and below (Ethernet driver). Developed the ARP and route tables, IP interfaces management, interfacing to Sockets interface of extreme low latency stack.

  The work involved both driver/kernel level and application level work because the stack operated both as a library and as a driver (to avoid unnecessary context switching). Due to the duality of operation, the IP layer tables had to be directly accessible from both user and kernel context and had to be implemented using lock-less techniques. The code was initially written for Linux but was later ported to Windows and Solaris.

- **Newport Networks**, High Wycombe: (Sep 2001 – Mar 2004)

  Skills developed: Team leading, RTOS(VxWorks), C/C++, Tcl, UML, OOD, TCP/IP, Ethernet, SCSI, NFS, fault-tolerance, Perforce, multi-threaded, PowerPC

  Fault tolerant (2-way redundant) disk host module (FTP, NFS, TFTP).
  SCSI and network related drivers (Ethernet) and other low-level software.
  UDP streaming with guaranteed delivery, high throughput and fault tolerance.
  Technical team leading of platform group.

- **Altera**, High Wycombe (5 Jun 2000 – 2 Sep 2001)

  Skills developed: **Java**, Swing, AWT, GUI design, Tcl, FPGA, PVCS

  Developed wizard GUIs in Java and a system for formally specifying and automating their creation process. Developed an automatic test environment in Tcl for testing and characterising the wizards and other products. Developed an automatic build system.

Education

‘A’ levels: Maths **(Grade A),** Physics **(Grade A),** Computing **(Grade A)**
Barnet College (92-94)

BEng. Hons: **Information Systems Engineering**
Imperial College (94 – 97)

PhD: Automatic Qualification of FPGA Designs
Imperial College (97 – 99, Not Completed)

Computer languages & Other Skills

C I have expert knowledge of C. I have been using C professionally for over 15 years (see Work Experience). My first C steps started at age 16 with the Greek edition of “The C programming language” by K&R, which I bought with money that I was saving for some time. Prior to that, I was working with BASIC.

C++ I have good knowledge of C++ and C++11. I have written user interfaces, controlled hardware, and represented logical entities such as hardware circuits.

Java I used it professionally for over a year during my employment with Altera.

Python I use Python to write test cases/frameworks and for general scripting tasks.

Tcl/Tk I have used Tcl to implement a language designed to control the test process of an FPGA design. I have also written a fairly complicated graphical user interface.

Shell scripts I have written numerous bash scripts for automating configuration steps.

HDL I have used VHDL and Verilog at the beginning of my career.

Languages I have used Javascript, Perl, Pascal, OCaml and Assembly in the past for small to medium projects.

O/S I have used both Linux and Windows as development hosts. I am familiar with both the GNU tools and Visual Studio and CYGWIN. I have developed applications for all of them. I have written drivers for Linux, VxWorks and Velosity/Integrity.

Open Source I am an open source proponent and comfortable with open source methodologies.

GNU tools I use GNU tools heavily for my everyday tasks. Vim, ctags, grep are my staples.

Multi-thread I have extensive experience in multi threading and deeply understand the issues. I have written lock-less synchronisation schemes, have build my own synchronisation primitives and worked on architectures that make use of re-ordering. I understand how critical sections, memory model and lock primitives interact to create a multi-thread safe environment.

Cross Compile Lots of cross compiling experience using the gnu toolchain and the usual open source packages (gcc, busybox, glibc, etc).

Linux Distros Familiar with Ubuntu, Redhat, Fedora, Debian, Mint distros.

Crypto I have hands-on cryptography experience and can operate at all levels of the crypto stack, all the way down to the primitive operations.
Created and debugged applications that use TLS/SSL and understand TLS/SSL down to the network packet level.
I have maintained a number X.509 deployments at Sky, Youview and Laird.
Developed openssl engines to offload the crypto number crunching.
Worked with XML signatures at Youview and Sky.
Created drivers for a smartcard (HSM) chip at Airvana.
Added new hashing algorithms to an old openssl library at Abbott/Laird.
I am familiar with FIPS. I worked on a FIPS compatible module at Laird.