# Stephen Harris - Curriculum Vitae

## PERSONAL DETAILS


Name: STEPHEN William Edward Harris
Nationality: British
Employment Status: Legal Permanent Resident (Green Card)
Home Address: 1-40 26th Street, Fair Lawn, NJ 07410
Cellphone: (917) 715 4143
Email: sweh@sweharris.org
Web/Blog: https://www.sweharris.org/
https://github.com/sweharris


## PROFESSIONAL PROFILE

Key Details:
- Unix Systems Engineer with a security focus
- 25+ years commercial experience in Unix Systems Administration, designing/architecting, engineering and implementing technology solutions.
- Very competent in Perl and ksh scripting, competent in C, basic SQL, some experience in other languages (Java, Python, Go etc)
- Deep knowledge of "how Unix works", including libraries (e.g. PAM, NSS), services (e.g. sendmail, apache) and protocols (e.g. HTTP, SMTP, NNTP).
- Able to explain technology in a manner people understand
- Takes an overall view of processes and solutions to determine process/technology gaps, and how to remediate them.
- Interviewed by Linux Journal, Aug 1995 *"Linux Goes to Sea"*
- Participated in and listed contributor to the Linux Filesystem Hierarchy Standard
- Participant in a number of cross-industry working groups, include FS-ISAC, Enterprise Cloud Customer Council (e3c) and RFG100, helping shape industry and regulatory direction.
- Presented at Cloud Expo NY on container security and the challenges involved.

Education: MA Oxford University, Mathematics and Computation (1987-1990)

## EMPLOYMENT HISTORY

**2016-present: Enterprise IT Architect in Cyber Security, Fiserv (First Data Corporation)**

Role involves assisting teams develop new products that meet the security requirements of the organisation, both to the letter of the security standards but also for the underlying information data security risks. This involved becoming a SME in a number of areas (e.g. Docker) to be able to provide useful direction and guide rails. Solutions need to be pragmatic, allowing for "minimum viable product" day-1 delivery and a tracked path to day-2 improvements.

**Major tasks/roles**

- Created framework and requirements for Pivotal CloudFoundry deployment to support PCI-scoped applications
- Drove remediation of Apigee API gateway deployments to close multiple gaps
- Defined interim solution for Docker container management
  - Created process to install Docker on corporate builds to allow central ops teams to support the engine.
  - Created scripts for CLAIR scanning of containers to allow DevOps teams to scan their containers
  - Worked with Tenable to improve their Nessus scanner container capabilities
  - On Customer Advisory Board for ShiftLeft.io container security while they were in stealth mode
- Creation of processes and procedures for on-prem and cloud deployments
  - Scripts for allow for CLI use of MFA protected users (e.g. https://github.com/sweharris/aws-cli-mfa)
  - Created interim tools to use AWS API to determine misconfigurations (e.g. open port 22 to the internet)
  - Interim use of "Prowler" to perform CIS Benchmark tests on AWS accounts
- Evaluation of multiple vendor products (e.g. DivvyCloud, Redlock, Dome9) to ensure cloud deployments are compliant. Worked with CloudOps to deploy the chosen solution and to define what rules/controls need to be validated.
- Defined control requirements around AWS accounts connected to Transit Gateway to avoid backdoor paths into the core datacenters, bypassing firewalls.
- Created usage guidelines around cloud KMS and encryption at rest requirements for data in S3, RDS, etc. Controls include the ability to perform data destruction as well as data protection.
- Hands on security evaluation of proposed solutions (e.g. Office 365, BYOD, DLP) to discover gaps. This involved attempting to break into the solution and bypass controls. Was able to determine the Mobile Email solution needed a complete redesign.

**2006-2016: Vice President, JPMorgan Chase**
**1999-2006: Senior Computer Scientist, Computer Sciences Corporation (CSC)**

*These two have been linked together because they are effectively one continuous employment. When I joined, JP Morgan had outsourced their IT to CSC; in 2006 I was insourced as a VP.*

Held various roles including: Cloud Security Engineer, Unix Authentication Architect, Process Automation, Configuration Management, Systems Administration

**Major tasks/roles**

- Designed and implemented an encryption tool to allow applications on Cloud Foundry to receive credentials in a secure manner ("miniVault")
- Designed and implemented reporting portal for Unix authentication infrastructure (vendor product was a "black box" to end users).
- Voting member of "Global Authentication Committee" (defining and promoting corporate standards).
- Architected and implemented multiple automation tools
- Participated in multiple external audits, representing central technology.
- Participant in 'Expert Engineer' (E2) programme; a JPMC internal course for top performing technologists (less than 40 participants at the time) introducing them to techniques such as how to create effective proposals for presentation to senior management, helping them expand their scope of effectiveness.
- Designed, implemented, deployed, documented tool to track remediation status of machines, which involved tracking 10,000 machines, 4 million accounts, ownership, trending etc. This was part of a 3 year programme to convert the existing environment into the corporate central account provisioning/administration tool (Keon aka BoKS). Passed audit with no comments.
- Evaluated then-current (2008) market options for centralised account provisioning and controls. This involved requirements definitions (controls and end-user), interaction with other parts of the company, vendor interaction, product evaluation, proof of concept build out, recommendations to management
- "Unix Collection and Reporting Facility" (UCRF) deployed globally. This was a centralised data collection from all servers (approx 2,000), web front end reporting, integration with asset management systems, CA Unicenter TNG, etc, with daily reports to risk management and SA teams
- Designed and implemented early automation tools; Y2K health checks - validated all managed servers for core functionality on Y2K, which became "BAU" tests running for 8+ years; mass password changes; code deployments; etc

**1995-1999: Senior Infrastructure Administrator, VNU Business Publications Ltd**

*VNU BPL was the London division of a Dutch based global publishing company. I started in the "MatriX Publishing Network" department as Unix & Network Administrator and developer, but as the company evolved my role expanded to cover "VNU Online Europe" and then I moved into the core IT department as Senior Infrastructure Administrator*

My primary role was as Systems and Network administrator, initially focused on managing the web content delivery services and then later the core infrastructure for BPL, including Unix (Solaris, HP-UX, Linux), Oracle (7.*,8i), NT4, routers (Cisco), switches (DEC, 3Com) and firewalls (Firewall 1, Linux iptables).

**1990-1995: Computer & Communications Manager, Papachristidis Ltd (Hellespont Group)**

*Hellespont consisted of four offices worldwide (London, Aberdeen, Greece, Philippines) as well as various companies owning different ships. Papachristidis Ltd provided most of the administration and technical support for the group based in London. This was my first full time job after leaving University.*

My role was to manage the group computing and communications, with an assistant based in the Greek office, and an assistant in the London office. Based in London but traveled frequently to Greece and once to the Philippines. Systems used include Sun Sparc (SunOS 4.x), various SVR2 and SVR3 machines, and Linux machines, with primary access being from DEC VT and Wyse terminals using terminal servers.