Brian Sturk

bsturk@comcast.net ❖ (603) 809-6825 ❖ Hudson, NH ❖ www.briansturk.com

Seasoned professional bringing over two decades of specialized experience in cybersecurity, threat research, and advanced software development, with a strong focus on cyber threat mitigation and innovative technology solutions.

CERTIFICATIONS & PATENTS

- **Offensive Security Certified Professional** (**OSCP**) [Ethical Hacker] - License OS-15502
- **Patent 11042633** - “Methods for Protecting Software Hooks, and Related Computer Security Systems and Apparatus”

PROFESSIONAL DIGITAL ENGAGEMENT

- Presentation at BSides CT - Providing Robustness in Endpoint Security Controls (won CTF as 3rr0rsmith)
- Blog Linux - CVE-2016-5195 "Dirty Cow" kernel vulnerability
- Blogs Windows - “Atombombing", “Macro-less Hacks - Retefe Malware”
- Webinar - Crypto Crime : Hunting for Cryptocurrency Mining in Your Enterprise
- Ransomware emulation - software written in Python
- Extracting Windows PE binaries from png images - software written in C++.

WORK EXPERIENCE

VMWare Carbon Black — **Aug. 2016 – Present**

Staff Threat Researcher - Team Lead — *Threat Research / Blue Teaming* — *Remote*

- Detection and prevention rules writer for app control, cloud, container, XDR/EDR, and NGAV products.
- Reversing/detonating malware, threat hunting and emulation for writing and testing product rules.
- Maintained and added new features to Powershell deobfuscation product using Rust.
- Advanced threat research and cross team collaboration for new product functionality/patents.
- Architect and developer on their next generation rules platform team for EDR and endpoint products.
- Managed VMWare’s Microsoft Active Protections Program participation, vulnerability analysis, and Yara rules.
- Various digital engagement activities including blogs, threat bulletins, webinars, and presentations.

Verdasys/Digital Guardian — **Jul. 2014 – Aug. 2016**

Consulting Engineer - Cyber R&D — *C++ Kernel Driver Development / Threat Research* — *Remote*

- Enhanced DLP product’s advanced threat detections - Process Hollowing, Reflective/App_Init injection.
- New features and support for product’s hooking and injection subsystems. Also support for packed binaries.
- Coded demos for BlackHat 2014 (iPhone hijacking via malicious image) and 2015 (fileless ransomware).

Avid Technologies — **Jan. 2010 – Jul. 2014**

Senior Principal Engineer — *C/C++ Kernel Driver Development* — *Burlington, MA*

- Development using C/C++ on their ISIS kernel file system driver and related software on OS X and Windows.
- Designed and implemented the embedded Linux platform for the ISIS 2000 product including distribution, installation/upgrade/recovery system, root file system, bootloader, and file system redundancy strategy.
- Designed and implemented a Linux version of the ISIS file system driver using FUSE on RHEL 6.
- Implemented a system for creating, installing, and deploying system recovery images using Qt.

Facilis Technologies — **Aug. 2008 – Nov. 2008, Sep. 2009 – Jan. 2010**

Consultant — *C/C++ Kernel Driver Development* — *Remote*

- Designed and created a new product to allow access to their Terrablock storage product over iSCSI. Heavily

modified the OSS iSCSI Enterprise Target Linux software package both at the user and kernel level.
- Re-designed and re-implemented their existing file migration application used for movement of files/projects.
- Ported client application to Linux using wxWidgets and consolidated all supported platforms into one codebase.
- Wrote applications to remount and resize Apple Partition Map partitions for OS X.

L3 Security — **Jan. 2009 – Jul. 2009**

Consultant *Embedded Linux Development* *Woburn, MA*

- Wrote diagnostic code for MODBUS based Galil controller over Ethernet doing analog/digital I/O in C.
- Wrote diagnostic code for serial RS-232 based Mforce motion controller in C.
- Implemented Qt based diagnostics interface. Also implemented all QtScript based diagnostic code.
- In house Linux expert for a team of DOS/Windows programmers transitioning into the project.

Tour Andover Controls — **Mar. 2006 – Sep. 2006, Dec. 2007 – Aug. 2008**

Consultant *Embedded Linux Development* *Andover, MA*

- Ported 2.6.16 Linux kernel and u-boot to custom ARM AT91 board used for security and automation systems.
- Wrote a Linux kernel driver to handle RS-485 communications utilizing on chip DMA for on board USARTs.
- Implemented use of Debian and Scratchbox/qemu for cross compilation and debugging for ARM9, x86 hosts.
- In house Linux expert to large group of RTOS developers in US and Sweden.

Cylant/Reflex Security — **Sep. 2006 – Dec. 2007**

Consultant *C/C++ Kernel Driver Development* *Lexington, MA*

- Ported driver portion of existing Cylant Secure HIDS product to Windows XP from Windows 2000. Driver hooked kernel calls and monitored for rootkits/malware in real time.
- Added features and bug fixes to Reflex Security's Snort based intrusion prevention product on Debian Linux.

JK Enterprises/Kobe Steel — **Apr. 2006 – Sep. 2006**

Consultant *C/C++ Development* *Remote*

- Wrote an application using wxWindows to interface with a custom data acquisition system over RS-232.
- Removed need for dongle in abandoned application by reverse engineering and binary patching DLL.

Media Matters — **Dec. 2005 – Apr. 2006**

Consultant *Python Development* *Remote*

- Wrote an application to monitor and interface with a robotic tape archive machine using wxPython.

Siemens SNC LLC — **Jul. 2004 – Mar. 2006**

Consultant *Embedded Linux Kernel Development* *Billerica, MA*

- Brought up kernel on custom PowerPC 400GX based board on Montavista Linux.
- Ported u-boot bootloader to Siemens' next generation ATCA hardware platform.
- Wrote a Linux kernel driver and API for an MRC FPGA for monitoring board status.
- Wrote a Linux I2C kernel driver to interface with GPIO circuitry, also wrote related diagnostics.
- Wrote a Linux kernel driver and API for Siemens' ARC chip which handled card redundancy/failover.
- Debugged and fixed many kernel bugs in User Mode Linux bundled with the Montavista PRO Linux kernel.

EqualLogic Inc. — **Mar. 2004 – Jun. 2004**

Consultant *Embedded NetBSD Kernel Development* *Nashua, NH*

- Coded new features for their iSCSI peer-storage array kernel device drivers on MIPS NetBSD.
- Designed solution and wrote kernel code to detect and fix specific hard drive issues dynamically (*NDA).
- Wrote an application that could induce specific hard drive errors under very high load (*NDA).
- Wrote many applications related to disk drives to monitor, search, diagnose, qualify, and repair them.

Axiam Inc. — **Nov. 2002 – Mar. 2004**

Consultant *RTOS / Embedded Linux Development* *Remote*

- Worked on metrology software interfacing with hardware (LVDT, encoders, motors) which ran on QNX.
- Re-designed and implemented their entire system to work with custom ISA data acquisition boards.
- Wrote software (ncurses application and Linux kernel module) to test their proprietary data acquisition boards.

Pinnacle Systems

Apr. 2003 – Mar. 2004

Consultant *C/C++ Windows Development* *Lowell, MA*

- Added many new features and maintained their VMG broadcast archiving/storage product.
- Implemented an FTP server and client with high performance, multiple threads, 64 bit REST, encryption, and site specific commands for control.
- Designed and wrote an application to query a system's configuration and verify state over a network using Qt.
- Wrote an application to interface with Adrienne time code boards using C# and .NET..

Avid Technologies

Apr. 2000 – Mar. 2003

Consultant *C Kernel File System Development* *Tewksbury, MA*

- Designed, wrote, and maintained Linux kernel file system driver (VFS) and associated device drivers.
- Wrote a kernel file system driver and associated device drivers for Solaris 8.0 (SPARC and x86).
- Wrote kernel device drivers, a file system driver (VFS), and related user-mode tools for Macintosh OS X.
- Wrote an application to interface with Adrienne time code boards using C# and .NET.
- Designed and implemented a reliable protocol over UDP running on multiple platforms and in varying environments, including soft real-time, low memory, and kernel/user mode.
- Designed and wrote a generic, extensible, and distributed testing framework in Python used for smoke testing multiple machines over a network using pyro.
- Implemented redundant server support for products using sockets, INET Helper API, and MFC.
- Reverse engineered the 3Ware IDE RAID/SAN JBOD user mode/kernel mode protocol for integration.

Speedline Technologies/CAMalot

Nov. 1998 – Apr. 2000

Consultant *C/C++ Windows Embedded Development* *Haverhill, MA*

- Wrote a Win2K kernel driver to access IO boards on parallel ports. Also install and config utilities.
- Implemented many major subsystems for semiconductor dispensing machines including temperature controllers, weight scales, conveyor, digital I/O, motion control.
- Wrote an NT Virtual Device Driver to run DOS based GFX product on Windows NT.

Northern Research and Engineering

Oct. 1997 – Nov. 1998

Consultant *C/C++ Windows GUI Development* *Woburn, MA*

- Provided new features, bug fixes, and an installer for their RITAP product
- Redesigned and rewrote COMIG, their mechanical design software. Also added many new features.

Henschel, Inc.

Jan. 1996 – Oct. 1997

Consultant *C/C++ Windows Kernel Development* *Newburyport, MA*

- Wrote NT kernel driver and apps for interfacing/data acquisition with synchro cards and other hardware.
- Wrote many programs interfacing with various military computers/systems using RS-422, NTDS, and Ethernet.

SKILLS & INTERESTS

- **Skills:** C/C++; Python; Assembly language; cyber security; white hat/ethical hacking; reverse engineering; OS/kernel internals and device drivers; embedded systems; Linux; MacOS; NAS/SAN/Filesystems; RTOS;
- **Interests:** Capture the Flag/Boot2Roots; Music/Drums; Electronics; Vintage Computers; Boardgames

EDUCATION & MILITARY SERVICE

- **University of Mass Lowell** *Electrical Engineering* **May. 92 - Jun. 1996**
- **US Army National Guard** *Rank E4* 12C Combat Engineer / 96B Intel Analyst