3725 Turtle Creek Blvd Apt D
Dallas, TX 75219

STACEY D. SON

M 1-214-490-7698
W stacey.son.org
E stacey@son.org

WORK EXPERIENCE

VOLUNTEER – FREEBSD/TRUSTEDBSD OS AND SECURITY DEVELOPMENT
FreeBSD.org and TrustedBSD.org

SENIOR SECURITY ENGINEER – SECURITY ENGINEERING AND ARCHITECTURE (SEAR) GROUP
Apple, Inc *2015-2020*
Worked on both hardware and software relating to iPhone and Macintosh security. Highlights include:
- Added system and Mach IPC filtering in the kernel for application sandboxing (aka., 'Seatbelt')
- Created CHERI-Qemu to support CHERI research and development on the ARMv8 architecture (AARCH64)
- Created an CHERI ARMv8 ISA test suit.
- Modified QEMU to support iOS development.
- Modified internal instruction level emulator to support CHERI.
- Evaluation of ARM pointer authentication (PAC).
- Evaluation of Memory Taggging Extension (MTE) and other ARM hardware proposed extensions.

CONSULTANT – CLEAN–SLATE DESIGN OF RESILIENT, ADAPTIVE, SECURE, HOSTS
SRI International Menlo Park, CA & Cambridge University UK *2011-2015*
- Created CHERI-QEMU, an adaptation of the popular QEMU ISA emulator to implement CHERI-MIPS instruction set.
- General FreeBSD/mips64 OS bring-up and kernel feature support on CHERI prototype targets (CHERI-QEMU and FPGA based tablet implemented using Bluespec SystemVerilog).
- New PMAP implementation for FreeBSD/mips64 including reference bit emulation, large pages for kernel thread stack, and Superpages.
- Added FreeBSD user-mode support to Qemu for cross building and cross development code with machine dependent support for ARM, ARM64, Mips and Mips64. Partial CHERI ISA support. Created miscellaneous binaries image activator kernel module for FreeBSD for transparent execution of target binaries on x86 host.
- Sandbox demo application development including web browser and example exploit creation for target CHERI prototype system.
- Performance counters support and general feature evaluation.
- Thread Local Storage (TLS) register support for FreeBSD/mips.

CONSULTANT – CORE OS SECURITY DEVELOPMENT
Apple, Inc. Cupertino, CA (Working remotely in Dallas, TX) *2008-2012*
- Created VM subsystem unit tests. Code signing code testing and evaluation.
- Added common criteria auditing to Apple's *Gatekeeper* policy updates.
- Developed an OpenSSL compatible API shim for Apple's *CommonCrypto*.
- Worked on application sandboxing for Mac OS X, added debugger support for sandbox exceptions, and sandboxed *iChat/Messages* app.
- Created sandbox and privilege separation example apps for WWDC.
- Created the *CommonCrypto* kernel extension ("KEXT") for Mac OS X.
- Created validation suites for FIPS 140-2 certification for the *CommonCrypto* KEXT.
- Updated Core OS security auditing subsystem to meet the Common Criteria for Information Technology Security Evaluation version 3.1 (CC v3.1), evaluation assurance level 3 (EAL3).
- Added performance enhancements so minimal security auditing can be enabled by default without any measurable overhead.
- Incorporated *OpenBSM* v1.1 into Mac OS X 10.6 (*Snow Leopard*).
- Added *Launchd* integration for user level security auditing support.
- Developed Core OS security audit session tracking for *securityd* and *launchd* including *kevent*(2) notifications and capability-based security.
- Developed Abstract Machine Testing (AMT) software.

• Added flexible storage and management features for audit record storage including aggregation of records from multiple systems, log rotation, and record expiration and deletion.
• Developed a *Python* extension and framework for unit testing the audit subsystem.
• Identified fixes and developed resolutions for Radars (Apple's bug reports) associated with the project. Communicated with Apple engineering contacts as necessary. Worked and communicated with ADC developers.

VOLUNTEER – FREEBSD/TRUSTEDBSD OS AND SECURITY DEVELOPMENT
FreeBSD.org and TrustedBSD.org *2004-Present*
• Added user-mode support to Qemu for FreeBSD and kernel module for transparent binary execution to support cross building of packages for tier 2 architectures include ARM, ARM64, MIPS and MIPS64. Now being used in production on package build cluster.
• Grand Central Dispatch (GCD) port: *kevent(2)* EVFILT_USER filter and thread workqueues.
• *Dtrace*: lockstat kernel provider and *lockstat* command-line tools.
• */dev/ksyms*: pseudo device for attaining kernel and module symbol table snapshot.
• OpenBSM: Open implementation of Sun's Basic Security Module (BSM) security audit API.
• OpenAMT: Abstract Machine Testing (AMT) for Common Criteria compliance.
• Mandatory Access Control (MAC).
• AoE (ATA over Ethernet) driver.

CHIEF ARCHITECT
NTT/Verio Dallas, TX *2000-2008*
• Managed R&D group that prototyped new server software architectures.
• Developed Linux VPS/Cloud prototype based on OpenVZ containers:
    • Created Linux *virtlink* implementation in kernel and user level utils.
    • Modified *libproc* library to include VPS information.
    • Developed kernel module to add a *vkern table* so BSD user level utilities could be easily ported.
    • Ported X.509 certificate management kernel module from BSD.
• Help design and implement system call, disk I/O, and network rate limiting in FreeBSD.
• Architected SAN storage system for hosting server clusters.
• Help implement simplified iSCSI initiator for FreeBSD.
• Created TCP/IP stack state "hand-off" for network load balancing between servers for FreeBSD.

VP, HOSTING TECHNOLOGY
Verio, Inc. Englewood, CO *1998-2000*
• Managed the hosting technology software development group.
• Added intrusion detection to the hosting systems by adding a *setuid* registration FreeBSD extension.
• Modified the GCC compiler to detect and prevent stack buffer overruns.
• Helped architected and implement *virtlinks* to increase code segment sharing between VPS's.
• Helped port VPS software to Solaris 2.6.

CTO AND CO–FOUNDER
iServer and Secure.net Orem, UT *1995-1998*
• Technical founder, innovator of core technology, manager of R&D group.
• Created OS-level virtualization (VPS) using BSD/OS for web hosting (including process containers, network isolation, and resource limits).
• Implemented a "super" *inetd* that started network services for each VPS on demand and allowed code segment sharing to save memory resources.
• Helped develop X.509 management kernel module so wild card certificates can be securely shared between VPS's.
• Helped design and develop server power and console management hardware; help port embedded FreeBSD to embedded controller.
• Added multi-layer quotas so quotas can be used within VPS.
• Successfully merged iServer, Inc. with Verio, Inc. in a stock swap deal.

PROGRAMMER/TECHNICAL CONSULTANT
AccessData Orem, UT *1990-1994*

- Developed core products.
- Created password recovery software for WordPerfect, Norton's Discreet, and other popular desktop/server applications with encryption features.
- Built hardware DES encryption/decryption engine for FBI using FPGAs.

SYSTEMS PROGRAMMER/RESEARCHER/MANAGER
BYU - College of Engineering Provo, UT *1989-1994*

- Managed college's network, computers systems & supercomputers.
- Supervised full-time and part-time IT staff for all computer systems in college.
- Implemented disk cache prefetching algorithm on BSD Unix System.
- Measured overhead of Mach 3.0 syscall redirection on cache performance.
- Developed distributed batch queuing and process checkpointing software.

RECENT PUBLICATIONS

CONFERENCE PAPERS

CHERI: A Hybrid Capability-System Architecture for Scalable Software Compartmentalization, Proceedings of the 36th IEEE Symposium on Security and Privacy ("Oakland"), San Jose, California, USA, May 18 2015.

CONFERENCE PRESENTATIONS

Embedded FreeBSD Development and Package Building via QEMU, BSDCan 2015, Ottawa, Ontario, Canada, June 12 2015.

(See https://stacey.son.org/publications/ for more.)

EDUCATION

BYU – COLLEGE OF ENGINEERING

Provo, UT – PhD Engineering (Incomplete - left to pursue business startup)
Provo, UT – MS Computer Engineering 1994
Provo, UT – BS Electrical and Computer Engineering/Science 1992

SKILLS

TEAMWORK

Experience in

- Team software development.
- Group management and leadership.
- Communication (including directly with customers).

COMPUTER

Proficient

- System virtualization, especially OS-level virtualization. User-mode and Full System-mode Emulation (Qemu).
- 4.2BSD-4.4BSD(BSD/OS), FreeBSD 4.0-Current(11.0), Xnu (Mac OS X) and Linux 2.6 kernel architecture, programming and driver development.
- C, C++, Perl and various assembly programming languages.
- Unix system security architecture, security-enhanced unix, various encryption algorithms and security protocols.
- IPv4, IPv6, TCP/IP stack and packet processing, and many IP-based protocols.
- CPU and system level architecture: x86, ARM/ARM64, and MIPS/MIPS64.

Familiar

- Mach 2.5/3.0, Solaris 2.6 kernel architecture and programming
- Forth, Objective C, Python, and Java; dtrace, ddb, gdb, kgdb.
- VLSI, digital logic design, computer system architecture and design.
- DEC (Alpha/MIPS/VAX), HP 300 (68030), HP 700/800 (PA/RISC), IBM PC/RT, IBM RS/6000, SGI, SUN (Sparc), etc.
- Xen Hypervisor (hardware-assisted virtualization, paravirtualization), L4 Microkernel.

AWARDS BUSINESS AND UNIVERSITY

- 5 Year Service Award - Apple, Inc.
- 10 Year Service Award - Verio/NTT.
- Selected member of BYU Advisory Council for Engineering School.
- Former selected member of Utah Technology Board for Gov. Leavitt.
- 5 Year Service Award - BYU College of Engineering.
- Student Teacher of the Year - BYU College of Engineering.
- Dean's Academic List and Scholarship.

ASSOCIATIONS ACM, IEEE, USENIX, Advisory board for BYU College of Engineering

REFERENCES **(UPON REQUEST)**