Philip B. Tricca

San Bruno CA, 94066

flihp@twobit.org

https://twobit.org

Qualification Summary

Software engineer with combined 15 years experience (7 in government research and 8 in the private sector) analyzing, designing, and building security-focused products and tools. Deep understanding of software / firmware integrity measurement and reporting concepts and technologies. Long-time OSS contributor and creator of the OSS TPM2 software stack. Strong technical, organizational and planning skills. Professional, trustworthy and a natural communicator.

Key Qualifications

- Transformed Intel's TPM2 Software Stack (TSS2) from one-person prototype to healthy Open Source Software (OSS) project by embracing OSS community best practices (ex. rigorous unit and integration testing, continuous integration & automation tools, metrics collection and community role modeling).
- Deep understanding of firmware / software integrity measurement architectures, secure boot, roots of trust (TCG) and supply chain security considerations.
- Successfully transitioned platform security prototype from research project developed in government research lab to Citrix product.

Professional Experience

Intel — Santa Clara, CA

Platform Architect, Platform Security Division — 10/2014 - present

Performed design and development tasks to create and promote the adoption of platform security technologies.

- Designed and implemented TSS2 libraries / APIs, resource management daemon and tools based on TCG specifications published and maintained as OSS: `https://github.com/tpm2-software/`
- Analysis of UEFI measured boot architecture and prototype of reference integrity measurement architecture to promote firmware transparency throughout the supply chain.
- Design and prototype of high value usage models for Intel® SGX including analysis and documentation of threat models, prototype planning and implementation.

Citrix Systems — Bedford, MA

Architect, Client Virtualization Group — 10/2011 - 07/2014

Performed implementation and design tasks on the security oriented XenClient XT client hypervisor product. Primary customers included government defense agencies particularly concerned with strong separation guarantees between mutually distrusting workloads.

- Designed and implementated platform measured launch using the TPM, Intel® TXT and the OpenEmbedded / Yocto build framework.
- Designed and implementated virtual disk encryption component using the Xen blktap2 interface and AES XTS from OpenSSL.
- Defined and documented threat models and the software architectures mitigating identified threads.
- Developed platform mandatory access control policy (SELinux / XSM).
- Lead customer requirements collection and design reviews.

Air Force Research Lab — Rome, NY

Computer Engineer, Information Directorate — 07/2004 - 08/2011

Performed a mix of work on research efforts relevant to military needs in the area of information systems security. Defined and managed research contracts with private sector and academic partners.

- Acted as lead engineer on SecureView project. Responsible for security architecture, technical design and customer / certifier reviews.
- Designed improvements to "Guard" systems through the application of mandatory access control mechanisms and information flow principles.
- Performed contract management tasks including technical guidance and review of cooperative research agreements with academic institutions including Cornell and PSU totaling over $2M.

Education

Syracuse University — New York

M.S. in Computer Engineering — 2012
Software Security and Systems Assurance
Advisor: Dr. Wenliang (Kevin) Du

B.S. in Computer Engineering — 2004
Software Engineering with a specific focus on system programming.
Graduated Magna Cum Laude

Awards

- Division Recognition Award for contributions to the advancement of trusted computing. Intel Open Source Technology Center. 2018-12-01
- Key Contributor Award. Trusted Computing Group. 2017-11-01
- Special recognition of service from the Commander for service rendered while leading Commander Directed Investigation, 2009.

Public Speaking & Publications

- Contributing author to Trusted Computing Group TPM2 Software Stack Specifications `https://trustedcomputinggroup.org/work-groups/software-stack/`
- Reference Integrity Measurements for TPM2 Security Policy. Linux Plumbers Conference, Lisbon Portugal. 2019 URL: `https://linuxplumbersconf.org/event/4/contributions/514/`
- Getting started with the TPM2 Software Stack (TSS2). Linux Security Summit, Vancouver BC. 2018 URL: `https://events.linuxfoundation.org/wp-content/uploads/2017/11/Getting-Started-with-the-TPM2-Software-Stack-TSS2-Philip-Tricca-Intel-1.pdf`
- *In-Guest Mechanisms to Strengthen Guest Separation.* Xen Summit co-located with LinuxCon. Edinburgh, Scotland, 2013. URL: `https://www.youtube.com/watch?v=6Q8mlTBn-ZI`
- TCG TSS2 async APIs and event driven programming: `https://twobit.org/2017/10/15/tcg-tss2-async-api-event-driven/`

Relevant Technical Proficiencies

- TPM2 & TCG TSS2 API and infrastructure concepts and implementation on Linux and Windows.
- GNU / LLVM tool chain, Autotools build and parallel test harness.
- Test strategies and test driven development methodologies.
- Continuous integration and test automation: travis-ci, coveralls, cmocka etc.
- Proficiency with the OpenEmbedded / Yocto build system and the construction of meta layers.
- Flask policy development and system configuration (SELinux / XSM).
- Threat modeling software systems using the STRIDE methodology.
- Applied use of cryptographic APIs & systems (OpenSSL, TPM2).
- Programming in popular languages (shell,C,Python), quickly learns new languages as needed.
- Professional / technical writing and documentation suitable for submission as project deliverables.