Bryan D. Payne

Information Security Executive

bryanpayne.org bdpayne@gmail.com 650-282-0311 bdpayne

With security experience ranging from Netflix to the National Security Agency, I help organizations understand and manage their cyber risk. I specialize in tuning security investment based on an organziation's risk appetite. And I prioritize investing in the people I work with to create a healthy, trusting, inclusive, and diverse team.

Professional Experience

Netflix Los Gatos, CA

Director, Product & Application Security 4/2017 - present

Manager, Product & Application Security 4/2016 - 4/2017

Manager, Platform Security 4/2015 - 4/2016

Lead broad scope organization responsible for product security, trust and safety, infrastructure security, security software services, and security program management.

- Built an industry leading security team from 3 to 70 people
- Partner with senior leadership and business stakeholders to guide strategic security direction
- Built security culture based on a "context not control" partnership model
- Led team through creation and launch of award winning bug bounty program
- Created fraud and abuse team that saved Netflix tens of millions of dollars in their first 18 months
- Led transformation of central engineering services to secure by default model using both network and scale economies as strategies for adoption and long term efficiency
- Responsible for teams that create and operate production software services for cryptographic key management, public key infrastructure, identity management, authentication, authorization, rate limiting, fraud detection, asset inventory, vulnerability management, and security event detection
- Hire and coach top security, software engineering, and management talent

OpenStack Security Group (OSSG)

Co-Founder 10/2012 - 3/2015

Created and led the global security team for OpenStack, an open source cloud computing infrastructure software project.

- Grew the team to over 200 contributors from around the world in 2 years
- Co-authored the OpenStack Security Guide that is now the official security documentation for OpenStack
- Created the OpenStack Vulnerability Management Team (VMT), and successfully integrated them into dozens of global open source software projects
- Created and integrated a security review process for code changes to core OpenStack projects
- Led a threat analysis function to help prioritize security investments across the OpenStack ecosystem
- Contributed to architecture and development of volume encryption and public key infrastructure (PKI) subsystems

Nebula Mountain View, CA

Director, Security Research 4/2012 - 3/2015

Led security at startup; responsible for product security vision and technical sales for security focused enterprise customers.

- Led security of an enterprise software product including vulnerability management, detection and response, compliance, product security, and creation of security features
- Turned security into a competitive differentiator by mitigating cloud-specific threats
- Architected and wrote software for many security features: self-bootstrapping public key infrastructure (PKI), release signing, logging subsystem, trusted platform module (TPM)-assisted boot attestation, orchestration for operating system hardening, and runtime security monitoring
- Hired and led a team of security software engineers

Sandia National Labs Albuquerque, NM

Principal Member of Technical Staff 6/2010 - 4/2012

- Led four research teams focused on classified projects in virtualization and cloud security
- Co-authored research proposals that secured internal and external funding for new projects
- Created LibVMI, an open source library that simplifies memory access and event-driven monitoring of virtual machines. This work was funded by an Early Career Laboratory Directed Research and Development (EC-LDRD) grant from Sandia, and was recognized in Sandia's *Lab Accomplishments*

Georgia Institute of Technology Atlanta, GA

Research Scientist & Graduate Research Assistant 8/2005 - 6/2010

- Researched the use of virtualization-based architectures to improve system security with an emphasis on techniques such as virtual machine introspection and memory analysis
- Published and presented research concepts at top security conferences and invited talks
- Co-authored and contributed to multiple winning proposals for foundational security research
- Taught *Introduction to Information Security*, a senior-level undergraduate computer security class

BAE Systems Arlington, VA

Senior Software Engineer 3/2003 - 8/2005

- Technical lead on a DARPA project; responsible for developing research ideas, designing system architecture, managing staff and delivering presentations to the customer
- Senior programmer on a large, agent-based distributed system designed using C, C++, and Java

National Security Agency Fort Meade, MD

Security Engineer & Researcher 5/1998 - 3/2003

- Researched network traceback techniques for determining the source of a network attack
- Led "blue team" field evaluations of networks and systems; recommended security improvements
- System administrator for a TS/SCI network; designed, configured, deployed, and maintained systems

Education

CISO Certificate Program Carnegie Mellon University, Pittsburgh, PA

- Executive education from Heinz College and the CERT Division of SEI

Ph.D. in Computer Science Georgia Institute of Technology, Atlanta, GA

- Focus: Systems Security, Minor: Business Entrepreneurship

M.Sc. in Computer Science University of Maryland, College Park, MD

- Focus: Wireless Network Security

B.Sc. in Applied Science Washington University in St. Louis, St. Louis, MO

- Majors: Computer Science and Mathematics

Professional Service

USENIX Enigma Conference

Steering Committee 4/2018 - present

Program Co-Chair 2018

Program Committee Member 2017

QCon New York

Track Host, Real World Security Track 2018

Malware Memory Forensics Workshop (MMF)

Program Committee Member 2014

Annual Computer Security Applications Conference (ACSAC)

Program Committee Member 2013

Program Committee Member 2012

Digital Forensics Research Workshop (DFRWS)

Program Committee Member 2012

IEEE Symposium on Security and Privacy (Oakland)
Program Committee Member 2012

Invited Talks & Presentations

BD Payne. "Fail, Learn, Fix: Improving Security The Old Fashioned Way". In: *OWASP AppSec California*. Jan. 2019.

BD Payne. "BLESS: Better Security and Ops for SSH Access". In: *QConNY*. June 2017.

BD Payne. "Securing Containers the Netflix Way". In: *Container Security Summit*. Jan. 2017.

BD Payne, C Greene, and H Raju. "Afternoon Panel". In: *Stanford Workshop on Web Application Security*. Sept. 2016.

BD Payne. "Security at Different Layers of Abstractions: Application, Operating Systems, and Hardware". In: *Design Automation Conference*. June 2016.

BD Payne. "Improving Cloud Security with Attacker Profiling". In: *QConSF*. Nov. 2015.

BD Payne. "Security at Different Layers of Abstractions: Application, Operating Systems, and Hardware". In: *US Frontiers of Engineering Symposium, National Academy of Engineering*. Sept. 2015.

BD Payne. "Platform Security at Netflix: Securing Microservices from the Ground Up". In: *AWS Loft SF*. July 2015.

BD Payne. "An Introduction to Virtual Machine Introspection Using LibVMI". In: *Malware Memory Forensics Workshop*. Dec. 2014.

BD Payne. "Reducing the Cost of Security in the Cloud". In: *ACM Cloud Computing Security Workshop (CCSW)*. Nov. 2014.

BD Payne. "Contributing to the OpenStack Security Group". In: *Cloud Security: Deep Dive into OSSG and Threat Modeling*. Aug. 2014.

BD Payne. "Forensic Enablement for IaaS Clouds". In: *LBNL DoD Workshop*. June 2014.

BD Payne, R Clark, and N Kinder. "OpenStack Security Guide (OSSG): An Update On Our Progress and Plans". In: *OpenStack Summit*. May 2014.

BD Payne. "Security for Private OpenStack Clouds". In: *OpenStack Summit*. May 2014.

BD Payne. "State of OpenStack Security". In: *OpenStack Security Conclave*. May 2014.

BD Payne. "Good Fences Make Good Neighbors: Rethinking Your Cloud Selection Strategy". In: *RSA Conference*. Feb. 2014.

BD Payne, S Wells, and N Burton. "Panel Discussion: Mission Ready OpenStack". In: *NSA OpenSource Industry Day*. Sept. 2013.

BD Payne and R Clark. "OpenStack Security Group: Status Update and Plans". In: *OpenStack Summit*. Apr. 2013.

BD Payne. "Beyond the Hype: Understanding Cloud Security for Your Application". In: *International Cloud Computing Expo*. Nov. 2012.

BD Payne and R Clark. "Building an OpenStack Security Group". In: *OpenStack Summit*. Oct. 2012.

BD Payne. "Virtual Machine Introspection: From Lab to Reality". In: *UNC Systems Tea*. Sept. 2009.

BD Payne. "Security Through Virtualization". In: *Emerging EW Technologies Conference*. June 2009.

BD Payne. "Kernel Control Flow Attacks and Defenses". In: *Trusted Infrastructure Workshop (TIW)*. June 2009.

BD Payne. "Lares: An Architecture for Secure Active Monitoring Using Virtualization". In: *IEEE Symposium on Security and Privacy*. May 2008.

BD Payne. "Lares: An Architecture for Secure Active Monitoring Using Virtualization". In: *IBM T. J. Watson Research Center*. Apr. 2008.

BD Payne. "Secure and Flexible Monitoring of Virtual Machines". In: *Annual Computer Security Applications Conference (ACSAC)*. Dec. 2007.

BD Payne. "Monitoring Under Fire: Implementing Tamper-Proof Host-Based Monitors". In: *BAE Systems Advanced Information Technologies*. Feb. 2007.

Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. "Gaps and Opportunities in Situational Awareness for Cybersecurity". In: *Digital Threats: Research and Practice* 1.3 (Sept. 2020). issn: 2692-1626. doi: 10.1145/3384471. url: https://doi.org/10.1145/3384471.

P. Klemperer et al. "High-Performance Memory Snapshotting for Real-Time, Consistent, Hypervisor-Based Monitors". In: *IEEE Transactions on Dependable and Secure Computing* 17.3 (May 2020), pp. 518–535. issn: 1545-5971. doi: 10.1109/TDSC.2018.2805904.

A Milenkoski et al. "Evaluation of Intrusion Detection Systems in Virtualized Environments Using Attack Injection". In: *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*. Nov. 2015.

A Milenkoski et al. "Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices". In: *ACM Computing Surveys (CSUR)* 48.1 (Sept. 2015).

TK Lengyel et al. "Scalability, Fidelity and Stealth in the DRAKVUF Dynamic Malware Analysis System". In: *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. Dec. 2014.

BD Payne. "Reducing the Cost of Security in the Cloud (Keynote Abstract)". In: *Proceedings of the 6th Annual ACM Workshop on Cloud Computing Security (CCSW)*. Nov. 2014.

A Milenkoski et al. "An Analysis of Hypercall Handler Vulnerabilities". In: *Proceedings of the 25th IEEE International Symposium on Software Reliability Engineering (ISSRE)*. Nov. 2014.

A Milenkoski et al. *Technical Information on Vulnerabilities of Hypercall Handlers*. SPEC Research Group SPEC-RG-2014-001. Standard Performance Evaluation Corporation (SPEC), Aug. 2014.

Y Jang et al. "Gyrus: A Framework for User-Intent Monitoring of Text-Based Network Applications". In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Feb. 2014.

K Basil et al. *OpenStack Security Guide*. OpenStack Foundation, July 2013.

TK Lengyel et al. "Virtual Machine Introspection in a Hybrid Honeypot Architecture". In: *Proceedings of the 5th Workshop on Cyber Security Experimentation and Test (CSET)*. Aug. 2012.

B Dolan-Gavitt, BD Payne, and W Lee. *Leveraging Forensic Tools for Virtual Machine Introspection*. Tech. rep. GT-CS-11-05. Georgia Institute of Technology, 2011.

BD Payne. "Virtual Machine Introspection". In: *Encyclopedia of Cryptography and Security (2nd edition)*. Ed. by Henk C.A. van Tilborg and Sushil Jajodia. Springer-Verlag Berlin Heidelberg, 2011.

BD Payne. "Improving Host-Based Computer Security Using Secure Active Monitoring and Memory Analysis". PhD thesis. Georgia Institute of Technology, May 2010.

J Wei et al. "Soft-Timer Driven Transient Kernel Control Flow Attacks and Defense". In: *Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC)*. Dec. 2008.

BD Payne et al. "Lares: An Architecture for Secure Active Monitoring Using Virtualization". In: *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*. May 2008.

BD Payne and WK Edwards. "A Brief Introduction to Usable Security". In: *IEEE Internet Computing, Special Issue on Usable Security & Privacy* 12.3 (May 2008), pp. 13–21.

BD Payne, M Carbone, and W Lee. "Secure and Flexible Monitoring of Virtual Machines". In: *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC)*. Dec. 2007.

BD Payne et al. "A Layered Approach to Simplified Access Control in Virtualized Systems". In: *ACM SIGOPS Operating Systems Review* 41.4 (July 2007), pp. 12–19.