Blayne Dreier

Software, Hardware, and Corporate Network Security Engineer with SRE/DevOps, DevSecOps, and Engineering Management Experience

Phone: **980-254-6961**
Website: **http://www.blaynedreier.com**
Email: **blayne@blaynedreier.com**

Summary

- 19 years of Network and Software Security experience
- 6 years of focused Software, Hardware, and Corporate Network Security evaluation experience
- 7 years of Corporate Infrastructure Security ownership
- 3 years of Engineering Management experience
- 5 years of Site Reliability/Platform/DevOps experience
- 8 years of Cisco TAC network security experience
- On-site experience working with teams to plan installations and solve problems
- BS in Computer Science with concentrations in math and business

Profile

- Enthusiastic about learning absolutely anything
- Well-traveled with interests spanning across and beyond the tech world
- Attentive to detail, strong-willed, self-correcting, and perceptive
- Ability to stay focused on large projects until completion
- Motivated with a high aptitude for learning skills quickly
- Effective management of many different responsibilities simultaneously

CERTIFICATIONS

OSCP #OS-101-29824

Offensive Security

June 2022

CISSP #442524

ISC2

June 2013

CCIE Security #19346

Cisco Systems

November 2007 - November 2015

SKILLS

Software, Hardware, and Corporate Network Security Assessment, Penetration Testing, Vulnerability Assessment, Threat Modeling, Risk Analysis, Infrastructure Automation, ISO 27k Preparation and Implementation, Burp Suite, TCP/IP, Python, Ansible, HAProxy, nginx, AWS, Mesos, Marathon, HDFS, ZooKeeper, Chronos, IOS, Cisco Routers/Switches/Firewalls (ASA), DDoS, IDS/IPS, Java, C, C++, PHP, HTML, Javascript, XML, Linux, MacOS (OSX), Windows, SQL, Wireshark, OWASP, VirtualBox, VMware VSphere ESX/ESXi

PUBLICATIONS

CVEs

CVE-2014-0667

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0667

The RMI interface in Cisco Secure Access Control System (ACS) does not properly enforce authorization requirements, which allows remote authenticated users to read arbitrary files via a request to this interface, aka Bug ID CSCud75169.

CVE-2014-0656

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0656

Cisco Context Directory Agent (CDA) allows remote authenticated users to trigger the omission of certain user-interface data via crafted field values, aka Bug ID CSCuj45353.

CVE-2014-0655

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0655

The Identity Firewall (IDFW) functionality in Cisco Adaptive Security Appliance (ASA) Software allows remote attackers to change the user-cache contents via a replay attack involving crafted RADIUS Change of Authorization (CoA) messages, aka Bug ID CSCuj45332.

CVE-2014-0654

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0654

Cisco Context Directory Agent (CDA) allows remote attackers to modify the cache via a replay attack involving crafted RADIUS accounting messages, aka Bug ID CSCuj45383.

CVE-2014-0652
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0652
Cross-site scripting (XSS) vulnerability in the Mappings page in Cisco Context Directory Agent (CDA) allows remote attackers to inject arbitrary web script via a crafted URL, aka Bug ID CSCuj45358.

CVE-2014-0651
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0651
The administrative interface in Cisco Context Directory Agent (CDA) does not properly enforce authorization requirements, which allows remote authenticated users to obtain administrative access by hijacking a session, aka Bug ID CSCuj45347.

CVE-2014-0649
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0649
The RMI interface in Cisco Secure Access Control System (ACS) 5.x before 5.5 does not properly enforce authorization requirements, which allows remote authenticated users to obtain superadmin access via a request to this interface, aka Bug ID CSCud75180.

CVE-2013-5541
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5541
Cross-site scripting (XSS) vulnerability in the file-upload interface in Cisco Identity Services Engine (ISE) allows remote authenticated users to inject arbitrary web script or HTML via a crafted filename, aka Bug ID CSCui67495.

CVE-2013-5540
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5540
The file-upload feature in Cisco Identity Services Engine (ISE) allows remote authenticated users to cause a denial of service (disk consumption and administration-interface outage) by uploading many files, aka Bug ID CSCui67519.

CVE-2013-5539
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5539
The upload-dialog implementation in Cisco Identity Services Engine (ISE) allows remote authenticated users to upload files with an arbitrary file type, and consequently conduct attacks against unspecified other systems, via a crafted file, aka Bug ID CSCui67511.

CVE-2013-5538
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5538
The Sponsor Portal in Cisco Identity Services Engine (ISE) uses weak permissions for uploaded files, which allows remote attackers to read arbitrary files via a direct request, aka Bug ID CSCui67506.

CVE-2012-5736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5736
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be

provided.

CVE-2012-5035
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5035
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

Patents

Dynamic second factor authentication for cookie-based authentication

Issued
https://patents.google.com/patent/US10158487B2

Method and system for delegating administrative control across domains

Issued
https://patents.google.com/patent/US20150128264

Method and apparatus for identifying a physical link interconnecting network devices
Issued
https://patents.google.com/patent/US8675496

Automatic correlation of dynamic system events within computing devices
Issued
https://patents.google.com/patent/US20140172919

Kinetic event detection in microphones

Issued
https://www.google.com/patents/US20140270275

Visualization of Question and Related Informational Item Data
https://patents.google.com/patent/US20140146051

Visualizing a network connection's overall health and providing actionable information
Published
http://ip.com/IPCOM/000223070

Method for detection and indication of audio stream degradation in Voice over IP telecommunication sessions
Published
http://ip.com/IPCOM/000239553

EXPERIENCE

Praetorian

June 2022 - Present

Principal Security Engineer

- Perform security assessments of a wide variety of products and environments in many verticals
- Provide consultative and best practice advice to customers
- Author detailed executive and technical findings reports
- Develop internal solutions to increase efficiency of engagement execution
- Mentor multiple engineers at various career stages

Praetorian

September 2019 - June 2022

Staff Security Engineer

Comprehend Systems (Austin, TX)

July 2018 to July 2019

Senior Security Architect

- Developed company security policy
- Represented company during customer audits of application and network security
- Owned and implemented security content for ISO 27001/27002 audits
- Presented to executive staff on security industry best practice, security policy, and solutions for internal infrastructure security
- Developed Standard Operating Procedure (SOP) and work instruction documentation for infrastructure security functions
- Developed secure work, data handling, and monitoring processes and infrastructure for elastic capacity engineering teams
- Assessed and evaluated newly released CVEs (security vulnerabilities) for applicability to infrastructure
- Performed security reviews and threat modeling of open source components, closed source third-party applications, private infrastructure, and internal code
- Developed and deployed S3-backed, encrypted audit trail logging solution for private infrastructure
- Established internal Certificate Authority (CA) and certificate infrastructure to provide traffic encryption and mutual authentication
- Integrated multi-provider Single Sign-On (SSO) for many internal and SaaS applications and components
- Evaluated and deployed hosted LDAP and RADIUS solution (Foxpass) for server and Wi-Fi authentication and authorization
- Developed IAM policies for various AWS services
- Implemented and managed multi-factor authentication (MFA) solution for applications and VPN (Duo)
- Evaluated, tested, and deployed: Vulnerability Management solution (Rapid7 InsightVM), Endpoint Detection and Response (EDR, CrowdStrike), Mobile Device Management (MDM, Jamf), SIEM and Centralized Logging infrastructure (Sumo Logic)

Comprehend Systems (Austin, TX)

January 2015 to June 2018

Senior Platform Engineer

- Launched and managed Platform Engineering team
- Led hiring and interview process for all Platform Engineers
- Developed Standard Operating Procedure (SOP) and work instruction documentation for infrastructure engineering functions
- Established and managed contracted IT services team
- Interviewed and trained Site Reliability Engineers (SRE) to establish new SRE team
- Automated infrastructure across multiple data centers with Ansible
- Developed a change management policy and established defined change windows
- Tuned, deployed, and managed 100+ Postgres clusters
- Dockerized many internal and external applications and components
- Created automated QA solution, which integrated VirtualBox, Selenium, and Docker
- Deployed and managed site-to-Site VPNs between data centers, to customers, and to shared cloud services
- Deployed remote access VPN for employees
- Developed and deployed DNS load-balancing solution for primary application and VPN using AWS Route53
- Developed Slackbot to automate database access requests, generate temporary Wi-Fi credentials, and report service uptime statistics
- Replaced aging ELK stack with fault-tolerant, cross-data center centralized logging solution with Graylog, RSYSLOG, HAProxy, and Elastic Search
- Developed and deployed Secure FTP (SFTP) solution backed by HDFS for customer data uploads
- Developed Python automation scripts and tooling for various services
- Developed Postgres database backup solution with webhook alerting and reporting
- Created and managed internal and SaaS account creation and deletion process
- Managed accounts and equipment for multiple data centers in different geographic regions
- Acquired, deployed, and managed: Cisco ASA, Cisco switches, Servers and network management devices, Cisco wireless Access Points (AP), Cisco Wireless LAN Controller (WLC), Cisco TelePresence, Cisco IP phones
- Deployed and managed server monitoring solution (Ubuntu Landscape)
- Replaced aging Cisco Call Manager infrastructure with cloud-based meeting solutions (Blue Jeans and Zoom) and establishes secure SIP connections for Cisco TelePresence units

Cisco Systems (Austin, TX)

March 2012 to January

Software Security Engineer and Researcher

2015

- Performed security evaluations for Cisco products
- Reviewed source code for security vulnerabilities
- Created defect reports to communicate security vulnerabilities to development
- Consolidated supporting security collateral to drive security vulnerabilities to resolution
- Worked directly with development to resolve discovered vulnerabilities
- Tested and verified fixes for resolved vulnerabilities
- Reported to executive management about evaluation progress and outcome
- Led and coordinated a team of security researchers to evaluate a product
- Wrote proof-of-concept code to validate vulnerabilities
- Created videos of vulnerability exploitation to drive security vulnerabilities to resolution

Cisco Systems (Richardson, TX)

August 2010 to March 2012

TAC Security Escalation

- Presented an 8-hour techtorial covering Cisco security products at Cisco Live
- Acted as the last point of global escalation for customer cases involving Cisco security products
- Acted as the global liaison for TAC-to-developer communication regarding software defects
- Assisted in supplying fixes for software defects described in TAC-generated defect reports
- Led Cisco CCIE Security training for TAC engineers
- Made significant contributions to internal and external technical written and video documentation

Cisco Systems (Richardson, TX)

March 2009 to August 2010

TAC Security Technical Lead

- Presented to customers at Cisco Live
- Assisted TAC security team with significantly complex and difficult cases
- Assisted high-profile customers in resolving network down scenarios
- Reviewed and refine defects filed against Cisco security products
- Mentored new employees on practices and technology training
- Provided technology training to other teams within Cisco
- Reviewed and published technical documentation for internal and external use

Cisco Systems (Research Triangle Park, NC)

May 2005 to March 2009

TAC Security Engineer

- Troubleshot customer networks in the area of system security
- Resolved cases dealing with Firewall, IDS, VPN, and AAA
- Worked in groups with other engineers to solve customer network complications
- Used recreation of a customer network to resolve issues hands-on
- Gave presentations on common attack tools and methods
- Investigated software defects and file reports for resolution

Cisco Systems (Research Triangle Park, NC)

August 2004 to January 2005

Co-op/Pseudo-Engineer

- Troubleshot customer networks in the area of system architecture
- Resolved system crashes, memory leaks, and high CPU utilization
- Attended engineering trainings to better develop knowledge in Cisco system architecture
- Surfed IOS C code to find and repair software related bugs
- Communicated problem and resolution to customer via various channels
- Communicated with software development engineers to resolve code instabilities

Cisco Systems (Research Triangle Park, NC)

January 2004 to May 2004

Co-op/Network Recreation and Engineering

- Recreated customer networks for engineering and troubleshooting
- Built an understanding of the hardware architecture of nearly every Cisco platform
- Became familiar with Cisco IOS commands, configuration and environment
- Obtained Cisco CCNA certification
- Conducted weekly lab audits to assure cleanliness and order
- Helped to maintain inventory of more than ten thousand Cisco machines and modules
- Monitored a case queue of engineer-submitted recreate cases
- Attended weekly training sessions to further conceptual and practical networking knowledge
- Mentored incoming co-ops and transfer knowledge learned from previous rotations

PROJECTS

Customer Engagement

Public documentation

Applying different IPS policies to specific flows with the AIP-SSM
https://supportforums.cisco.com/blog/149951/applying-different-ips-policies-specific-flows-aip-ssm

Cut-Through and Direct ASA Authentication
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113363-asa-cut-through-config-00.html

Forum participation
https://supportforums.cisco.com/users/cdreier

Media

TAC Security Podcast
https://supportforums.cisco.com/document/48396/tac-security-podcast-show-information-and-episode-listing

Cisco IPS Software
https://supportforums.cisco.com/video/11927661/cisco-ips-software

TAC IPS Media Series
https://supportforums.cisco.com/document/48896/tac-ips-media-series-show-information-and-episode-listing

EDUCATION

University of North Carolina at Charlotte

August 2002 to May 2005

Bachelor of Science, Computer Science

- Graduated with honors
- Related concentrations in Math and Business