

# Blayne Dreier

---

*Network and Software Security Engineer*

---

Phone: **980-254-6961**  
Website: <http://www.blaynedreier.com>  
Email: [blayne@blaynedreier.com](mailto:blayne@blaynedreier.com)

## Summary

- 2+ years of DevOps experience
- 2+ years of product and software security evaluation
- 8+ years of Cisco TAC experience with knowledge of how to handle cases correctly and efficiently
- BS in Computer Science with concentrations in math and business
- Quick and enthusiastic about learning absolutely anything
- Well-traveled with interests spanning across and beyond the tech world

## Profile

- Experience recreating and troubleshooting Cisco networks.
- Experience evaluating Cisco products for security vulnerabilities.
- On-site experience working with teams to plan installations and solve problems.
- 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.
- Able to maintain high energy. Worked 45-50 hours per week while attending school full-time.
- Effectively manage many different responsibilities simultaneously.

**CISSP #442524**

ISC2

IOS, Cisco Routers/Switches/Firewalls, ASA, Zone-Based Firewall, IOS-FW, DDoS, IDS/IPS, IOS-IPS, IDSM-2, NAC, ACS, CSM, CSA, Python, Java, C, C++, PHP, HTML, Javascript, XML, Windows, Linux, OSX, SQL, TCP/IP, Wireshark, OWASP, VMware VSphere ESX/ESXi

**SKILLS****PUBLICATIONS****Patents**

**Method and apparatus for identifying a physical link interconnecting network devices**

*Issued*

<https://www.google.com/patents/US8675496>

**Visualization of Question and Related Informational Item Data**

*Pending*

<https://www.google.com/patents/US20140146051>

**Automatic correlation of dynamic system events within computing devices**

*Pending*

<https://www.google.com/patents/US20140172919>

**Method and system for delegating administrative control across domains**

*Pending*

**Kinetic event detection in microphones**

*Pending*

<https://www.google.com/patents/US20140270275>

**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>

**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.

**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>

## Tools

### Zone-based Firewall Configuration Parser

<https://www.blaynedreier.com/zbf/>

## EXPERIENCE

## Cisco Systems (Austin, TX)

*March 2012 to January*

### Security Researcher

*2014*

- Perform security evaluations for Cisco products
- Review source code for security vulnerabilities
- Create defect reports to communicate security vulnerabilities to development
- Consolidate supporting security collateral to drive security vulnerabilities to resolution
- Work directly with development to resolve discovered vulnerabilities
- Test and verify fixes for resolved vulnerabilities
- Report to executive management about evaluation progress and outcome
- Lead and coordinate a team of security researchers to evaluate a product
- Write proof-of-concept code to validate vulnerabilities
- Create videos of vulnerability exploitation to drive security vulnerabilities to resolution

## Cisco Systems (Richardson, TX)

*August 2010 to March*

### TAC Security Escalation

*2012*

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

## **Cisco Systems (Richardson, TX)**

*March 2009 to August*

### **TAC Security Technical Lead**

*2010*

- Speaker at Cisco Live
- Assist TAC security team with significantly complex and difficult cases
- Assist high-profile customers in resolving network down scenarios
- Review and refine defects filed against Cisco security products
- Mentor new employees on practices and technology training.
- Provide technology training to other teams within Cisco.
- Review and publish technical documentation for internal and external use.

## **Cisco Systems (RTP, NC)**

*May 2005 to March*

### **TAC Security Engineer**

*2009*

- Troubleshoot customer networks in the area of system security.
- Resolve cases dealing with Firewall, IDS, VPN, and AAA.
- Work in groups with other engineers to solve customer network complications.
- Use recreation of a customer network to resolve issues hands-on.
- Give presentations on common attack tools and methods.
- Investigate software defects and file reports for resolution.

## **Cisco Systems (RTP, NC)**

*August 2004 to January*

### **Co-op/Pseudo-Engineer**

*2005*

- Troubleshoot customer networks in the area of system architecture.
- Resolve system crashes, memory leaks, and high CPU utilization.
- Attend engineering trainings to better develop knowledge in Cisco system architecture.
- Surf IOS C code to find and repair software related bugs.
- Communicate problem and resolution to customer via various channels.
- Communicate with software development engineers to resolve code instabilities.

## **Cisco Systems (RTP, NC)**

*January 2004 to May*

### **Co-op/Network Recreation and Engineering**

*2004*

- Recreate customer networks for engineering and troubleshooting.
- Build an understanding of the hardware architecture of nearly every Cisco platform.
- Become familiar with Cisco IOS commands, configuration and environment.
- Obtain Cisco CCNA certification.
- Conduct weekly lab audits to assure cleanliness and order.
- Help to maintain inventory of more than ten thousand Cisco machines and modules.
- Monitor a case queue of engineer-submitted recreate cases.
- Attend weekly training sessions to further conceptual and practical networking knowledge.
- Mentor incoming co-ops and transfer knowledge learned from previous rotations.

## **Appalachian State University (Boone, NC)**

*June 2001 to June 2002*

### **Network Analyst/Software Administrator**

- Install software packages for both faculty and student use.
- Obtain an understanding of schools network system and analyze traffic and usage.
- Assume liability of computer system security.
- Design software configurations for use by students and library staff.
- Troubleshoot and diagnose computer system malfunction.
- Provide assistance to others with personal computer problems.
- Repair malfunctioned computer and printer hardware.

## **Best Buy Corp. 175 (Gastonia, NC)**

*June 2000 to March*

### **Mobile Audio/Video Installation Technician**

*2001*

- Install mobile amplifiers, speakers, decks, television monitors, and alarms.
- Obtain an understanding of every car make and model's interior construction and wiring schematics.
- Assume liability while driving customers' cars into bay and throughout installation.
- Design and build component mobile audio and video systems.
- Troubleshoot and diagnose automobile electronic system malfunction.
- Track daily and weekly progress, competing with previous personal

numbers and other stores.

## **Best Buy Corp. 175 (Gastonia, NC)**

*July 1999 to May 2000*

### **In-Store & On-Site Audio/Video/Computer Repair Technician**

- Perform preventative maintenance, bench repair, diagnosis and parts ordering.
- Conduct in-house and on-site customer equipment orientation, training, and repair.
- Diagnose silicon boards to component level, soldering and replacing parts as needed.
- Maintain and repair test facilities and grounds.
- Complete electrical wiring and component installation from the ground up for industrial and personal computer networks.
- Support Internet providers by providing technical assistance with routers and other equipment.
- Utilize signal generators, AC/DC volt, ohm and amp meters (fluke), oscilloscope, and other precision measuring instruments.
- Attend technical conferences and seminars to stay informed about product developments.
- Prepare detailed documentation recording the repairs needed and test log information.
- Establish workload schedules, repairs priorities and assigned specific duties to personnel.
- Report weekly and monthly to regional manager, providing written and oral reports.

## **Best Buy Corp. 235 (Corpus Christi, TX)**

*September 1998 to April  
1999*

### **In-Store & On-Site Audio/Video/Computer Repair Technician**

- Perform preventative maintenance, bench repair, diagnosis and parts ordering.
- Conduct in-house and on-site customer equipment orientation, training, and repair.
- Diagnose silicon boards to component level, soldering and replacing parts as needed.
- Maintain and repair test facilities and grounds.
- Complete electrical wiring and component installation from the ground up for industrial and personal computer networks.
- Support Internet providers by providing technical assistance with routers and other equipment.





## EDUCATION

- Utilize signal generators, AC/DC volt, ohm and amp meters (fluke), oscilloscope, and other precision measuring instruments.
- Attend technical conferences and seminars to stay informed about product developments.
- Prepare detailed documentation recording the repairs needed and test log information.
- Establish workload schedules, repairs priorities and assigned specific duties to personnel.
- Report weekly and monthly to regional manager, providing written and oral reports.

### **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