

DEREK A. CHAMORRO – CISSP

13417 Tossa Lane

Austin, TX 78729

Phone (512) 593-3368 Email derek.chamorro@gmail.com

Website: <https://therandomsecurityguy.com> Twitter: [@theredinthesky](https://twitter.com/theredinthesky)

SUMMARY OF QUALIFICATIONS

- Expertise in building secure cloud framework architectures (Openstack, AWS, GCE)
- Expertise in building secure container platforms (Docker, Kubernetes)
- Expertise with routers (Cisco, Juniper, ALU), Layer 2 and 3 switches, firewalls (ASA/PIX, Netscreen, Juniper SRX)
- Extensive experience in abstracted networking (Calico, Flannel, VXLAN)
- Elements and applications: SIM, firewalls, IPS/IDS, AAA (RSA SecurID, RADIUS, TACACS+), PKI, IPsec, OS and app hardening.
- Extensive experience in Solaris/Linux administration including bash/Python scripting, code compiling and cron.
- Extensive experience in DDOS mitigation techniques (BGP blackholing/sinkholing, flow detection, TCP sanitization)
- Ground-up build out of security and network architecture, SOC, Operations Support Systems (OSS).
- Process creation: Audit, Incident Response, Credential Management, Vulnerability Assessment, AV/Patch Management.
- Extensive experience in designing multi-tiered security architectures.
- Possess superior communication, interpersonal, and organizational skills.
- Ability to work in a team environment, as well as, assume leadership roles.
- Execute high-level technical customer service.
- Fluent Spanish speaker.

EDUCATION & CREDENTIALS

Ashworth College Norcross, GA
Business Administration program

John Adams High School Miami, FL
Received diploma

Technical Certifications

CISSP #114423

EMPLOYMENT

*Atlassian
Austin, TX
Senior Security Architect
Present*

I am responsible for product security for Atlassian's cloud product services. My charter is to develop and execute programs to improve security across our global footprint as well as architect/engineer/support new system deployments.

Technologies:

*Secrets and key management
Secure Docker builds
Policy API for tenant segmentation
PKI
SAML/OAUTH2 integration*

*Ebay
Austin, TX
Senior Cloud Security Architect
2016*

- Chartered cloud security strategies, architecture, and roadmap.*
- Recommend, implement, and integrate new security tools and technologies.*
- Develop cloud and container-based security frameworks.*

*Cisco
Austin, TX
Technical Leader
2015-2016*

Responsible for building the low level architecture within Cisco Cloud Services. My responsibilities involve both network and security architecture, covering both physical and virtual networks.

Technologies:

- Openstack build automation*
- Firewall architecture*
- VXLAN and eVPN*
- SDN integration*

- *DDOS mitigation*
- *Automation (Ansible/Python)*

HPCloud

Austin, TX

Senior Network Security Engineer

2013 - 2015

- Designed and re-architected DDOS mitigation program for HPCS. Technologies included are: Large scale Arbor Peakflow and TMS deployments, destination-based BGP blackholing, and source-based BGP sinkholing.
- Built flow-based detection framework for stateless ACL building.
- Managed routing protocol security
- Designed high-bandwidth production-grade open-source firewall solution
- Researched and tested different SDN applications for network management and overlay implementation.
- Audited existing systems and network infrastructure.

eBay

Austin, TX

Senior Security Engineer

2013

- Designed and managed DDOS mitigation program for X.commerce domains. Technologies included are: Behavioral DDOS detection/mitigation, SYN cookies, flow-based detection, and BGP sinkholing.
- Managed security architecture of Openstack Folsom network.
- Researched, evaluated, tested, recommended, and implemented new security solutions.
- Audited existing systems and network infrastructure.

HomeAway

Austin, TX

Senior Security Engineer

2012 - 2013

- Responsible for designing and implementing dynamic security controls.
- Architected network access control solution for L2/L3VPN environments.
- Designed MS Server 2012 PKI infrastructure.
- Managed ISS IPS deployments including custom signature development.
- Managed firewall, ACL and VPN policies (ASA 8.4, Nexus7k, DMVPN)
- Audited network security controls for PCI compliance.

*Bioware
Austin, TX
Network Security Engineer
2012*

- Responsible for designing and implementing Arbor Threat Management System for DDOS traffic scrubbing.
- Architected Tippingpoint IDS deployment for passive, signature-based threat detection. Tuned and created custom signatures.
- Managed distributed Nessus deployment, scheduling and tuning scans for various environments.
- Managed firewall and ACL policies.
- Audited network security controls.

*Time Warner Cable
Buffalo, NY
Senior Network Security Engineer
2008 - 2012*

- Responsible for analyzing and administering security controls for regional engineering and transport network.
- Designed safeguards for public networks against unauthorized infiltration, modification, destruction and disclosure.
- Researched, evaluated, tested, recommended, implemented new security software and devices.
- Created and developed security policies and procedures.
- Worked closely with systems engineers to design and implement security controls.

*Creative Breakthroughs Inc.
Troy, MI
Senior Security Engineer
2007 - 2012*

Senior security engineer and consultant for Symantec and Juniper partner.

Provided security consulting services for US Army and many Fortune 500 companies.

Services included:

- Vulnerability Assessments
- Penetration Testing (Internal/External) using commercial and open source tools
- Technology Audits (Wireless, IDS/IPS, BlueTooth)
- Social Engineering (Remote, Onsite)
- Physical Security Audits
- Compliance Framework Implementation (CobiT, ITIL) and auditing (PCI, HIPAA, SOX)
- Business Impact Analysis
- Security Awareness Training

*Synacor
Buffalo, NY
Network Engineer
2007*

Responsibilities included:

- Designed and tested a Cisco NAC appliance framework, building redundant clean access servers, traffic shaping and anti-virus policies.
- Developed a disaster recovery plan in conjunction with Synacor's plans for building a redundancy NOC.
- Responsible for design, administration, and troubleshoot of Synacor's multi-cluster networks.
- Assisted in designing and implementing new secure Cisco wireless deployment, utilizing WPA2 encryption.
- Member of Synacor's Security Team

*Inergex
Buffalo, NY
Senior Security Consultant
2006 – 2007*

Provided part-time security consulting services to the following:

Healthnow/BCBS:

- Designed a centralized access control system through Cisco ACS for TACACS authentication, authorization, and auditing of all layer 2 and layer 3 network devices. Created 3 administration groups through Active Directory to allow for more granular control.
- Performed firewall auditing. Cleaned up configurations, removed stagnant access lists, and consolidated multiple firewalls onto one firewall appliance.
- Installed and configured a Juniper Netscreen SA4000 SSL VPN appliance for clientless remote access.
- Drafted multiple security policies to create baseline standards for encryption,

router security, wired and wireless LAN communication, and remote access. This was to help comply with HIPAA and SAS70 requirements.

- VPN administration through existing Cisco series VPN Concentrator. Responsible for OS upgrades, session administration, and group creation.
- Responsible for troubleshooting connectivity problems through deep packet inspection using TCP analysis tools.
- Designed a virtualized PKI in a test lab, developing a proof of concept for portable device encryption.

The Travel Team:

- Performed a vulnerability assessment. Scans uncovered open ports, unsecured web and DNS servers.

First Niagara Financial Group:

- Built a statement of work, detailing the vulnerability assessment that was to be used as a pre-audit assessment on FNFG's AD infrastructure.

*Comcast Communications
Philadelphia, PA
Network Security Engineer
2006*

Member of Comcast's Network Security Assurance team
Responsibilities included:

- Designed and administered Radius RSA SecurID servers for two factor authentication for all network devices and servers for Comcast's national IP network. Applied configurations on all networks devices and UNIX/Linux servers.
- VPN administration through Cisco series VPN Concentrators. Designed current VPN cluster solution, load balancing all remote access sessions. Policy management through rules, filters, and Radius authentication.
- Designed PGP PKI infrastructure for securing interdepartmental mail. Managed PGP servers and public key distribution.
- Administered and deployed IDS appliances from Enterasys Systems. Managed IDS sensors through Enterasys Dragon console, identifying attacks and vulnerabilities through deep packet inspection on signature-based IDS.
- Administered and deployed Netscreen firewalls. Managed appliances through the Netscreen Security Manager, collecting logs and pushing configurations.
- Audited all changes on production assets under existing operating model to ensure the security policy was not compromised or negatively affected.

*Adelphia Communications
West Seneca, NY*

*Network Security Engineer
2003 – 2006*

Member of Adelphia's Network Security Operations at their West Seneca Data Center. Responsibilities included:

- Maintaining multi-area OSPF areas connecting Adelphia local systems across the country.
- VPN administration through Cisco series VPN Concentrator. Responsible for designing, administering, and troubleshooting LAN to LAN VPN tunnels and remote access sessions. Policy management through filters, rules, NAT and IPSec Security Associations.
- Assisted in writing and developing security policies in accordance with Sarbanes Oxley, SAS 70, and HIPAA regulations.
- Maintained edge network security through Cisco PIX firewalls. Designed access lists, static NAT and PAT, IP routing, and LAN to LAN tunnels.
- Designed, implemented, and administered IPS solution through Internet Security Systems (ISS) Site Protector and Proventia G appliances.
- Designed, implemented, and administered web proxy cluster solution using Microsoft ISA 2004 in conjunction with ISS Web Filter.
- Designed and administered an HP Openview Network Node Manager solution for monitoring on corporate network nodes. Created traps and alarms for RMON events and data collection and reporting through SQL.
- Incorporated Cisco ACS to use TACACS for centralized authentication on all network devices.
- Performed day-to-day routine administration and support tasks associated with Windows 2000/2003 network systems infrastructure including policy implementation through Active Directory and DNS, NAT, subnetting, and IP routing.

*Adelphia Communications
Buffalo, NY
Network Support Engineer
2000 – 2003*

- Extensive troubleshooting through Cisco 2600, 3600 and 7000 series routers, Catalyst switches and UNIX backend servers.
- Secure provisioning of DOCSIS compliant cable modems through Nortel Networks NetID/CPS2000, Arris, Cisco CNR, and ALOPA Metaserv DHCP servers.
- Maintained IP and serial database connectivity through local LAN and WAN connections.
- Troubleshot network, hubs, broadband modems, and asynchronous connections.

References available upon request