David E. Thiel
San Francisco, CA
lx-jobs2018@redundancy.redundancy.org
https://github.com/lxcode

Experience

Dedicated Security Partner, Facebook Connectivity Lab September 2015 – Present

- Helping secure technologies that provide Internet connectivity to the unconnected or poorly connected. Evaluating new connectivity projects to determine potential security and human safety threats, developing threat models, designing product security architecture, and coordinating security review and penetration testing of projects.
- Responsible for security architecture, coordinating code and feature review, and continuous threat modeling of Facebook's Express Wi-Fi ecosystem, as well as the Terragraph 60GHz urban mesh networking solution.
- Developed threat model and mitigations for attacks on the Aquila UAV, including defenses for GPS spoofing, communications jamming, radio interception, physical attacks and attacks on the FSO/mmwave payloads and ground stations.
- Co-founded a cross-functional team analyze and promote human safety issues in areas connected by the Connectivity Lab. Helped develop safety documentation for new internet users, ensuring translation into local languages. Analyzed incidence of abusive or exploitative behavior in these regions to ensure Connectivity projects were not being used to enable malicious behavior.
- Helped design and architect ground facilities and communications security for a satellite that Elon Musk subsequently blew up.
- As interim DSP for WhatsApp, conducted risk assessment and designed remediations for the WhatsApp production environment, developed security operations policy and SOC 2, ported osquery to FreeBSD, developed FreeBSD-specific osquery modules, and coordinated deployment to the production environment.

Distinguished Security Engineer, NCC Group (née iSEC Partners) June 2015 – September 2015

- Black box and source assisted penetration tests of web, mobile and desktop applications as part of the DSE team, primarily deployed for more technically challenging engagements.
- "Red Team" covert network and system penetration testing of both internal and external environments, compromising large portions of infrastructure and documenting fixes to help prevent compromise in the future.
- iOS application security research, documentation and training.
- Technical mentorship of North American NCC consultants, helping consultants learn new technologies and manage research projects.
- Development work in Python and Objective-C on public and private internal tools.

VP, iSEC Partners, Inc. July 2006 – June 2015

- Management of the North American iSEC security consultant team. Direct manager of principal consultants, technical mentor to consulting staff.

- Management and coordination of research projects, public GitHub, as well as responsible vulnerability disclosure.
- Original research in the areas of mobile devices, media technologies, & rich web content. Results presented publicly at numerous security conferences.
- White box and black box penetration testing of a wide variety of high-profile web applications, mobile applications, desktop software, server software, embedded devices and network environments. Specializations in iOS and UNIX.
- Source review of applications in C, C++, Objective-C, C#, PHP, Ruby and Java.
- Security architecture review of production infrastructure and software, as well as embedded device architecture, communication and encryption schemes.
- "Red Team" covert network and system penetration testing of both internal and external environments.
- Development work in Python, Objective-C and Java on public and private internal tools.
- Debugging and exploit development for software in C/C++.
- Training of developers and security professionals on penetration testing and secure coding practices.
- Extensive writing of professional technical documentation.

Security Architect, Shopping.com→eBay December 2004 – July 2006

- Designed, implemented, and wrote tools to support a Kerberos/LDAP-based centralized authentication and authorization system, for both UNIX systems and in-house applications.
- Implemented host-based intrusion detection and centralized logging for 2000+ UNIX and Windows machines, creating custom tools for HIDS event reporting and host management.
- Deployed and performed daily maintenance and monitoring of a Sourcefire-based Network Intrusion Detection System for corporate offices and multiple production hosting facilities.
- Conducted application penetration testing against in-house applications, reporting security weaknesses and risk analyses to engineering groups for correction. Used both automated and manual means for vulnerability detection.
- Defined access control policies for role-based authorization and privilege escalation in production and development environments, using sudo, cfengine, and LDAP-based access control.
- Instrumental in Sarbanes-Oxley compliance efforts, owner of the majority of systems, network and information security controls. Wrote internal security policies and standards, worked to identify potential areas of deficiency, and led efforts to correct them.
- Managed vendor selection, security product evaluation, and dedicated security budget.

IT Manager (Part-time Contract), Jigsaw Data Corporation October 2004 – June 2005

- Conducted penetration testing on in-house developed applications, production networks, and production systems and devices. Assisted in resolution of exposed security weaknesses.
- Responsible for purchase, configuration, testing and administration of production x86 Linux systems, Cisco PIX clusters, switches, Cisco LocalDirectors, RAID arrays, and corporate development/QA labs.
- Managed equipment selection and purchasing to expand datacenter environment, adding in full network and system redundancy, load balancing, and network segmentation.

Systems/Security Architect, NetEnrich, Inc. November 2004 – May 2005

- Designed and built prototype KVM/datacenter management appliance in an early-stage startup environment.

- Designed secure architecture and for encrypted communications between client, management appliance, and KVM controllers.
- Performed OS customization/hardening/minimization, web server configuration, and application reliability testing.
- Worked with hardware vendors to design x86-based appliance prototypes meeting cost and performance requirements.
- Wrote user interface and back-end for OS and application configuration.

Security Administrator, WagerWorks, Inc. August 2002 – July 2004

- Designed and applied security policies to production OSes and applications, including the hardening of Solaris, Linux, Apache, WebLogic, remote access, DMZ design, proxy architecture, firewall security, and DNS and mail services in an online gaming environment serving several high-profile casinos.
- Designed mechanisms and network devices to mitigate DDoS attacks on customer sites, worked with backbone providers and law enforcement to combat organized attacks.
- Conducted comprehensive penetration testing program, exposing and correcting weak points in both public and corporate network security.
- Implemented centralized intrusion detection with Snort, MySQL and Samhain, collecting data over secure channels from local and remote locations to a central database and display system for analysis.

Sr. Hosting Operations Engineer, NexPrise, Inc. June 2000 – June 2002

- Design, administration and maintenance of Solaris, FreeBSD, and Linux server environment in a 3-tier app architecture, with a focus on redundancy, reliability, and security.
- Security auditing and enhancement of the product and hosting offerings, including active and passive intrusion detection, cryptographic authentication, penetration testing, and DoS resistance. Developed and implemented policies to improve production site security.
- Configuration, hardening, and maintenance of Oracle, Apache-SSL/Jserv/Tomcat, IPF-based firewalls, qmail, POP3, IMAP/SSL, and sendmail.

Computer Specialist, US Department of the Interior, USGS July 1999 – May 2000

- Administered Solaris, FreeBSD, Linux, DG/UX, Windows NT, and WinNT TSE servers in a datacenter environment.
- Implemented server and network security best practices, including extensive use of encryption, BSD login classes, chrooted server applications, host and router-based packet filtering, TCP wrappers, intrusion detection, and proactive security auditing.
- Assisted and instructed other districts nationwide implement similar security procedures as part of the national WRD Security Team.

Systems Administrator/HW Technician, DCWI, Inc. June 1995 – May 1999

- Assisted in configuration and maintenance of FreeBSD servers, Cisco routers, and modem banks for a local ISP of approximately 1000 customers.
- Performed troubleshooting, repair, and upgrading of third-party manufactured systems, peripherals, and software. Installation and maintenance of corporate LANs.

Publications and Software

- Author, iOS Application Security, 2016 No Starch Press
- Author/Presenter, Secure Development on iOS
  (Mobicase 2010, SOURCE Boston 2011, PacSec 2011)
- Co-author/Presenter, Living in the RIA World
  (Black Hat Vegas 2008, DEFCON 16, PacSec 2008, SyScan HK 2009)
- Author/Presenter, Exposing Vulnerabilities in Media Software (whitepaper)
  (Black Hat Vegas 2007, Black Hat EU 2008)
- Author, Mobile Application Security, 2010 McGraw Hill
- Contributor and FreeBSD wrangler, osquery
- Ports committer, FreeBSD

Skills

Security:	Application and network penetration testing, source code review, red team, Incident Response, protocol analysis, fuzzing, architecture review, reverse engineering, anti-DDoS, IDS, SDR
Languages:	Objective-C, Python, LaTeX, C, PHP, Ruby, Bourne, Lua, Go, R and Java. Rudimentary ARM assembly. Mildly conversational and moderately literate in Japanese.
Tools/Frameworks:	Vim, mostly. Also Rails, Docker, Vagrant, Git, osquery, HackRF, Kerberos, MySQL, Postgres, Apache, Nginx.
Operating Systems:	FreeBSD 2.x-12.x, macOS, Linux (Ubuntu/Debian/CentOS/Fedora), Solaris 2.6-10, Cisco IOS, DG/UX

Tangential pursuits

- Avid motorcyclist, former Motorcycle Safety Foundation instructor
- Instructor, volunteer and training coordinator, SFSI
- Foster parront, Mickaboo Bird Rescue
- Enthusiast, analogue modular synthesizer construction

PGP: https://redundancy.redundancy.org:4/lx25519.gpg
Fingerprint: 66F7 D26A D90F 308D 20A5 3697 2E07 53DF B9CB B1C3

https://redundancy.redundancy.org:4/resume.pdf
https://redundancy.redundancy.org:4/resume.txt