David E. Thiel

San Francisco, CA
det-jobs2024@grumplicio.us
https://github.com/lxcode
https://orcid.org/0000-0002-0947-5921

Experience

Chief Technologist, Stanford Internet Observatory March 2020–Present

- Designing and building tooling and cloud architecture for large-scale ingest, archival, cleaning, enrichment and analysis of social networking data.
- Original research into trust and safety topics including NCII, child safety, privacy and disinformation campaigns, as well as decentralized and alt-tech platforms.
- OSINT investigations supporting SIO research projects; OSINT training for researchers and RAs.
- Management of the technical research assistant team.
- Design and production of research publications, curricula and data visualizations.

Managing Editor, Journal of Online Trust & Safety September 2021–Present

- Review of LOIs for inclusion in the journal.
- Peer review, literature review and revision suggestions of accepted articles.
- Design of journal publication framework, templating, layout and proofing.

Dedicated Security Partner, Facebook September 2015–March 2020

- Securing of technologies providing Internet connectivity to the unconnected or poorly connected. Evaluating new projects to identify 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, the Terragraph 60GHz urban mesh networking solution, and the Magma network platform.
- 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. Analyzed incidence of abusive or exploitative behavior in these regions to ensure Connectivity projects were not being used to enable malicious behavior.
- Led efforts to improve the security posture of Facebook's trust and safety infrastructure, including threat modeling, penetration testing, and improving abuse detection and prevention, as well as assisting with red team efforts.

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. Conducted complex Red Team engagements.
- iOS application security research, documentation and training.
- Technical mentorship of North American NCC consultants, helping consultants learn new technologies and manage research projects.

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

- Management of the North American iSEC security consultant team.
- Management and coordination of research projects, public GitHub, as well as responsible vulnerability disclosure.
- Original research in the areas of mobile devices, media technologies, & emerging web technologies. Results presented 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, and Java.
- Security architecture review of production infrastructure and software, as well as embedded device architecture, communication and encryption schemes.
- Red Team covert network, system and physical penetration testing.
- Debugging and exploit development for software in C/C++.
- Development work in Python, Objective-C and Java on public and internal tools.

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.

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

- Responsible for security review, purchase, configuration, testing and administration of production Linux systems, Cisco PIX, LDIR, and RAID arrays.

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

- Designed secure architecture and for encrypted communications between client, management appliance, and KVM controllers. OS customization/hardening/minimization.

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

- Designed and applied security policies to production OSes and applications, including system hardening, remote access, proxy architecture and firewalls 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 and extortion.

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

- Design, administration and maintenance of Solaris, FreeBSD, and Linux server environment, with a focus on redundancy, reliability, and security. Security auditing, intrusion detection and penetration testing.

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

- Administered Solaris, FreeBSD, Linux, DG/UX, Windows NT, and WinNT TSE systems. Intrusion detection and proactive security auditing for local and national WRD networks.

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

- Configuration and maintenance of FreeBSD servers, Cisco routers, and modem banks for a local ISP of approximately 1000 customers.

Selected Publications

- Author, The Strengths and Weaknesses of the Online Child Safety Ecosystem
- Author, Child Safety on Federated Social Media
- Author, Generative ML and CSAM: Implications and Mitigations
- Author, Cross-Platform Dynamics of Self-Generated CSAM
- Author, Gabufacturing Dissent
- Author, Topologies and Tribulations of Gettr
- Author, Contours and Controversies of Parler
- Author, iOS Application Security, 2016 No Starch Press
- Inventor, Secure Registration and Ignition of Network Nodes on a Multi-Hop Wireless Network
- Designer and co-author, The Long Fuse: Misinformation and the 2020 Election
- Designer and contributor, Memes, Magnets, and Microchips

Skills

Security	Application and network penetration testing, source code review, red team, Incident Response, protocol analysis, fuzzing, OSINT, architecture review, reverse engineering, anti-DDoS, IDS
Languages	Python, Objective-C, LaTeX, C, Go, PHP, and Java. Conversational and literate in Japanese, basic Portuguese.
Tools	Vim, UNIX and visidata. Burp Pro, mitmproxy, Maltego, Frida, Wireshark, BigQuery, Data Studio
Platforms	GCP, AWS, Vultr, FreeBSD, macOS, iOS, Linux (Ubuntu / Debian / Fedora)