

David E. Thiel

San Francisco, CA

lx-jobs2023@grumplicio.us

<https://github.com/lxcode>

<https://orcid.org/0000-0002-0947-5921>

Experience

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 submitted articles.
- Design of journal publication framework, templating, layout and proofing.

Chief Technologist, Stanford Internet Observatory

March 2020–Present

- Designing and building tooling and architecture for large-scale ingest, archival, cleaning, enrichment and analysis of social networking platforms.
- Original research into online trust and safety issues, including NCII, child safety, privacy, extremism and alt-tech platforms.
- OSINT investigations to support SIO research projects; training for researchers and RAs.
- Management of the student technical research assistant team.
- Design and production of research publications and data visualization.

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.
- 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.

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.
- 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 internal tools.

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 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, 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.
- Development work in Python, Objective-C and Java on public and internal tools.
- Debugging and exploit development for software in C/C++.
- Training of developers and security professionals on penetration testing and secure coding practices.

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.
- Application penetration testing and remediation of in-house applications.

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, RAID arrays, and corporate development/QA labs.

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, server configuration, and application reliability testing.

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, firewalls, 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.

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, authentication, penetration testing, and DoS resistance.

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.

Publications and Software

- Designer and contributor, [Memes, Magnets, and Microchips](#)
- Designer and Co-Author, [The Long Fuse: Misinformation and the 2020 Election](#)
- 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](#)
- 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)
- Ports committer, [FreeBSD](#), 2006–2022

Skills

<u>Security:</u>	Application and network penetration testing, source code review, red team, Incident Response, protocol analysis, fuzzing, OSINT, architecture review, reverse engineering, anti-DDoS, IDS, SDR
<u>Languages:</u>	Python, Objective-C, La TeX, C, PHP, Bourne, Lua, Go, R and Java. Rudimentary ARM assembly. Conversational and literate in Japanese, basic Portuguese.
<u>Tools</u>	Vim, UNIX and visidata . Also Burp Pro, mitmproxy, Maltego, Frida, Wireshark, BigQuery, Data Studio
<u>Platforms</u>	GCP, AWS, Digital Ocean, FreeBSD 2.x–13.x, macOS, iOS, Linux (Ubuntu / Debian / Fedora)