

Zak Blacher

Software Engineer, Security Features

I'm a software engineer with a formal background in applied cryptography & digital privacy enhancing technologies. I'm passionate about bridging the gap between security & usability.

✉ resume@chalkzebra.com

📍 San Francisco

🌐 [linkedin.com/in/zakblacher](https://www.linkedin.com/in/zakblacher)

📞 206-###-####

🌐 gitlab.com/zblach

🌐 github.com/zblach

WORK EXPERIENCE

Staff Software Eng., Security Engineering coinbase

06/2017 - 10/2020

San Francisco, CA

- cold storage tech lead (2017-2019) (patents pending)
- initial architect for custody and staking products
- designed & built multi-hop message integrity systems
- product lead - top-of-funnel tokenization
- bootcamp and intern mentor
- internal security & software architecture consultant
- provided employee security onboarding & education

Sr. Software Engineer, Security Features fitbit

10/2016 - 06/2017

San Francisco, CA

- built upgradeable user authentication systems
- performed SSO integration with internal services

Trust Engineer, Security Infrastructure LinkedIn

01/2015 - 10/2016

Mountain View, CA

- developer of the internal service-to-service auth systems
- partner for developer security education
- third-party software vendor assessment

Software Engineer, Payments Integration amazon

08/2013 - 10/2014

Seattle, WA

- banking partner integration owner
- developer on large-scale payments batch-processing systems

ENGAGEMENTS & PUBLICATIONS

"Offline Storage System and Method of Use"

[USPTO: 20190318356](https://www.uspto.gov/patent/publications/20190318356) @ coinbase

"Transcending Cloud Limitations by Obtaining Inner Piece"

novel limit-bypass exploits against cloud storage APIs @ DEFCON 21

Filesystems & Volume Encryption (Guest Lecture)

CSC Talks @ UWaterloo

"A Study of NTFS Cluster-Slack Retention Characteristics"

Masters Thesis: Filesystem forensics research for FIVES working group

"An Ontological Approach to SIP DoS Attack Detection"

Junior Masters Thesis: Classifying DoS attacks by traffic differentials

October 17, 2020

SKILLS & COMPETENCIES

security engineering

privacy engineering

applied cryptography

secdevops

developer education

mentorship

OPEN SOURCE CONTRIBUTIONS

argon2-jvm – API compatibility fixes & testing

openssl – x509 validation bug fixes

sudo – excision of flawed crypto library dependency

EDUCATION

Masters of Mathematics (Comp. Sci.)

University of Waterloo

09/2011 - 08/2013

Waterloo, Ontario

- Differential Privacy

- Machine Learning

Magister Nätverkssäkerhet (Security)

Karlstads Universitet

08/2009 - 09/2010

Karlstad, Värmland

- Filesystem Forensics

- Cryptography & Privacy

B.Sc. H (CS: w/ Networks & Security spec.)

University of Windsor

09/2006 - 08/2011

Windsor, Ontario

LANGUAGES

Python

Expert

Golang

Upper-intermediate

Java

Intermediate

Ruby on Rails

Intermediate

INTERESTS

cooking

cryptography

defcon culture

privacy enhancing technologies

blockchain

jazz music

architecture

puns