NICHOLAS SULLIVAN

address
1269 South Van Ness Ave Unit C
San Francisco, CA 94110

tel (408) 421-6965
email nicholas.sullivan@gmail.com
web https://crypto.dance

Profile

Engineering leader and security architect with deep expertise in cryptography, computer security, software protection, internet protocols, digital rights management, and distributed systems.

Employment

Head of Cryptography, Cloudflare Inc. San Francisco, CA, USA *2015–present*
Responsible for global cryptographic initiatives.

Head of Security Engineering, Cloudflare Inc. San Francisco, CA, USA *2013–2015*
Software development manager and founding member, security team.

Senior Software Engineer, Apple Inc. Cupertino, CA, USA *2007–2013*
Software engineering lead for digital rights management technologies.

Security Analyst, Symantec Corporation Calgary, AB, Canada *2006–2007*
Security researcher, technical writer, software developer.

Cryptography Researcher, CISaC Calgary, AB, Canada *2004–2006*
Graduate researcher and teaching assistant in mathematics and cryptography.

Skills

Extensive practical and theoretical experience with symmetric cryptography, public key cryptography, protocol design, fraud prevention and detection, threat modeling, cryptanalysis, side-channel attacks, and application security. Proven ability to explain complex technical issues to non-technical audiences.

Education

Master of Science - Mathematics and **Computer Science**
University of Calgary, Calgary, AB, Canada *2004–2006*

Bachelor of Mathematics - Pure Mathematics and **Combinatorics and Optimization**
University of Waterloo, Waterloo, ON, Canada *2000–2004*

Certifications

CISSP - Certified Information Systems Security Professional
(ISC)2 - Licence 484449 *2015–present*

Professional Certificate - Advanced Computer Security
Stanford University, Stanford, CA, *2009*

Selected Publications

The Security Impact of HTTPS Interception, **NDSS 2017**, *2017*
Attacking White-box AES Constructions, **SPRO '16**, *2016*
An Analysis of TLS Handshake Proxying, **IEEE TrustCom**, *2015*
DNSSEC: How far have we come, **Virus Bulletin**, *2014*
A (relatively easy to understand) primer on elliptic curves, **Ars Technica**, *2013*
Strong Cryptography Using Linux's Random Number Generator, **Wired Innovation Insights**, *2013*
Internet Security Threat Report (Volumes XI, XII), **Symantec**, *2007*
Fast Algorithms for Arithmetic on Elliptic Curves over Prime Fields, **Master's Thesis**, *2007*

NICHOLAS SULLIVAN

address
1269 S Van Ness Ave Unit C
San Francisco, CA 94110

tel (408) 421-6965
email nicholas.sullivan@gmail.com
web https://crypto.dance

Patents

Patents: 20+ U.S. patents granted in various computer security topics

Awards

Americas ISLA – Information Security Practitioner 2015 (runner-up)
Program Committee – Real World Crypto, Crypto & Privacy Village, USENIX Security

Media

Speaker at conferences: RSA, Infiltrate, O'Reilly OSCON, Real World Cryptography, Virus Bulletin, NANOG, Crypto & Privacy Village at DEF CON, botconf, CCC, ACSAC, NCC Open Forum, USENIX Enigma, GothamGo, BSides Las Vegas, IGF-USA, O'Reilly Security, EPFL Summer Research Institute, Stanford Security Seminar, DSS ITSEC, IETF Plenary, DEEPSEC, others.

Quoted by: The Wall Street Journal, The New York Times, Forbes, Bloomberg, Wired, Le Monde, TechCrunch, CNET, more.

On-camera appearances: CNBC, CNN, ABC.

Work Experience Details

Head of Cryptography, Cloudflare Inc. San Francisco, CA, USA *2015–present*
Head of Security Engineering, Cloudflare Inc. San Francisco, CA, USA *2013–2015*
At Cloudflare I wear many hats. I was hired as the first security-focused engineer when the company was under fifty employees. As the company grew, I created the Security Engineering group to set the vision for security at the company. I recruited a world-class team of developers, security researchers and security product managers to implement this vision. My responsibilities included managing security product priorities, recruiting talent, providing architectural guidance and leadership, code auditing, and the occasional coding project to stay fresh. I now lead the Cryptography group, a full-lifecycle R&D team that develops novel cryptographic technology (security protocols, encryption hardware, algorithms, etc.) from idea to fully commercialized product.

Cryptography and Security Engineering

- Led the team that built and deployed the first ever production-scale implementation of the TLS 1.3 protocol, improving speed and security for millions of web properties.
- Designed and built a novel key management system for protecting customer TLS keys.
- Led largest commercial deployment of ECDSA certificates on the web with the Universal SSL initiative, nearly doubling the number of HTTPS-enabled sites on the Internet.
- Spearheaded a campaign to build trusted computing elements into Cloudflare's bare metal CDN platform.
- Designed, coded and open sourced several cryptography-related projects including Red October and CFSSL. Became one of the authors of the Go programming language during this work.
- Led the development of Keyless SSL, allowing Cloudflare to provide HTTPS content delivery without having possession of the private key.
- Acted as architect for internal key management infrastructure. This included developing the operational practices for a Certificate Authority for server-to-server communication and customer origin sites.
- Implemented prototype of DNSSEC live signing for an internally developed DNS server in Go, which led to the Universal DNSSEC product.

NICHOLAS SULLIVAN

address
1269 S Van Ness Ave Unit C
San Francisco, CA 94110

tel (408) 421-6965
email nicholas.sullivan@gmail.com
web https://crypto.dance

- Worked with the compliance group to achieve PCI DSS 2.0 and 3.2 certifications.
- Conducted miscellaneous research on Botnet and DDoS trends.

Leadership

- Acted as engineering manager, product manager, security architect, and recruiter for a broad security team and an R&D team focused on cryptographic technology.
- The public face of security at Cloudflare. Spoke at various security and cryptography conferences, often as an invited speaker. Represented Cloudflare in the media, making on-camera appearances and quoted as a security expert in print and online publications of note.
- Participated in several IETF working groups, becoming an official contributor to TLS 1.3 and author of several other Internet drafts. Invited to speak at the IETF 97 Technical Plenary.
- Created the Heartbleed Challenge in response to the Heartbleed vulnerability, resulting in a better understanding of the vulnerability and fostering community discussion.
- Developed the internal application security training program for developers.
- Prolific writer for the widely respected Cloudflare blog, focusing on the topics of security and cryptography. Guest contributions to Ars Technica, Wired Innovation Insights, and the PerfPlanet Calendar.
- Represented the company in sales and strategic meetings with Fortune 100 executives.
- Built relationships with researchers in the academic security community resulting in academic publications.
- Organized a successful cryptography lecture series in the Cloudflare office.
- Participated in working groups for CA-Browser Forum and the Financial TLD working group, helping set cryptographic policy.
- Led the company in developing intellectual property. Awarded “Most Innovative Employee” award in 2014.
- Acted as a mentor for junior employees, and establishing coding style guidelines and code review processes.
- Worked with several universities on Stanford’s Open Academy, mentoring students on how to participate in free and open source software projects.
- Worked with policy team to improve cryptographic policy in the United States through meetings with government representatives.

Senior Software Engineer, Apple Inc. Cupertino, CA, USA *2007–2013*
Lead software engineer responsible for the design and implementation of Apple’s digital rights management (DRM) solutions on desktop clients and servers.

iTunes Store
Responsible for server-side DRM components that handle billions of transactions per day. Implemented optimizations to reduce the total data load by >80% while enabling new fraud detection and mitigation techniques. Developed techniques for key renewability that do not require a client update, allowing rapid iteration to fix DRM vulnerabilities.

FairPlay Desktop Clients
Responsible for Apple’s DRM components on OS X and Windows. Developed new techniques for offline rights enforcement, robustness against reverse engineering, compiler optimization, and media playback protection in C. Invented new client-server protocols, number theoretic algorithms and other

NICHOLAS SULLIVAN

address
1269 S Van Ness Ave Unit C
San Francisco, CA 94110

tel (408) 421-6965
email nicholas.sullivan@gmail.com
web https://crypto.dance

protection techniques that resulted in over a dozen patent applications. Oversaw implementation and design of eBook DRM system for iBooks. Worked with OS X team to develop a new protection scheme for the Mac App Store. Improved performance of existing DRM algorithms and components while increasing security against known and theoretical attacks.

Responsible for coordinating integration of DRM technologies into Apple products shipped to hundreds of millions of customers (iTunes, QuickTime, Game Center, iCloud, iBooks, AirPlay, and others). Development of cross-platform build systems, quality monitoring tools, validity and performance testing in Python, bash, and C.

Other
Member of hiring committee. Mentored junior members of the team. Part of small rapid response team that handled analysis analysis of DRM attacks discovered in the wild.

Security Analyst, Symantec Corporation Calgary, AB, Canada *2006–2007*
Co-authored the *Internet Security Threat Report* (ISTR), Volumes XI and XII, the regionally focused EMEA and APJ ISTR Volume XII, and the Government ISTR Volume XII. Topics covered include trends in malicious code, spam, phishing, geographical distribution of malicious behavior, and political/legal trends in computer security.

Regularly authored research articles about computer security topics for the Symantec Security Response Weblog, some of which were reported by international news organizations.

Cryptography Researcher, CISaC Calgary, AB, Canada *2004–2006*
Worked in the Centre for Information Security and Cryptography (CISaC) on research related to Algebraic Cryptography, Number Theory, Elliptic, Hyperelliptic, and Superelliptic curves. Coded a Superelliptic curve toolkit in C++ using GMP.