Deian Stefan

Curriculum Vitae

353 Serra Mall, #288
Stanford, CA 94305
☎ *(646) 821 1675*
✉ *deian@cs.stanford.edu*
deian.org

Interests

Systems, programming languages, and security & privacy.

Education

2010–today **Ph.D. student in Computer Science**, *Stanford University*.
Thesis title *Principled and Practical Web Application Security*
Advisors David Mazières and John C. Mitchell

2009–2011 **Master of Engineering in Electrical Engineering**, *The Cooper Union*.
Thesis title *Analysis and Implementation of eSTREAM and SHA-3 Cryptologic Algorithms*

2005–2009 **Bachelor of Engineering in Electrical Engineering**, *The Cooper Union*.
Magna Cum Laude

Positions

07/14–today **Co-founder, President, and CTO**, *GitStar, Inc.*, San Francisco, CA.
05/13–09/13 **Security Research Intern**, *Mozilla, Inc.*, San Francisco, CA.
07/11–06/12 **Web Developer**, *HyaQu, Inc.*, San Francisco, CA.
90/09–01/11 **Graduate Research Fellow**, *Cooper Union*, New York, NY.
06/09–09/09 **Crypto Research Intern**, *LACAL at EPFL*, Laussanne, Siwtzerland.
08/09–02/09 **Security Research Intern**, *DyDAn at Rutgers University*, New Brunswick, NJ.
05/09–08/08 **NSF REU Research Fellow**, *DIMACS*, New Brunswick, NJ.
07/07–07/09 **Undergraduate Research Fellow**, *Cooper Union*, New York, NY.
05/06–07/06 **NSF REU Research Fellow**, *Stevens Institute of Techology*, Hoboken, NJ.
08/05–05/08 **Head Network Administrator**, *Cooper Union EE Deptartment*, New York, NY.
08/02–08/04 **Founder and Web Developer**, *EasyPixel*, New York, NY.

Projects

ESpectro Security architecture for building least privileged Node.js applications. ESpectro provides application-level virtualization for implementing different security mechanisms.

COWL Backwards-compatible browser confinement system. COWL provides a way to build secure client-side applications (e.g., mashups) that involve multiple untrusted parties.

Hails Framework for building secure extensible web applications. Hails allows applications to integrate third-party code in a way that preserves data privacy and integrity.

LIO Programming environment for building applications that preserve privacy and integrity, by construction, using dynamic information flow control.

Publications

Conferences

1. Stefan Heule, Deian Stefan, Edward Z. Yang, John C. Mitchell, and Alejandro Russo IFC Inside: Retrofitting Languages with Dynamic Information Flow Control. In Proceedings of *Conference on Principles of Security and Trust (POST)*. Springer, April, 2015. Accepted.
2. Deian Stefan, Edward Z. Yang, Petr Marchenko, Alejandro Russo, Dave Herman, Brad Karp, and David Mazières. Protecting Users by Confining JavaScript with COWL. In Proceedings of *Symposium on Operating Systems Design and Implementation (OSDI)*. USENIX, October, 2014.
3. Pablo Buiras, Deian Stefan, and Alejandro Russo. On Dynamic Flow-sensitive Floating-Label Systems. In Proceedings of *Computer Security Foundations Symposium (CSF)*. IEEE, July, 2014.
4. Deian Stefan, Pablo Buiras, Edward Z. Yang, Amit Levy, David Terei, Alejandro Russo, and David Mazières. Eliminating Cache-based Timing Attacks with Instruction-based Scheduling. In Proceedings of *European Symposium on Research in Computer Security (ESORICS)*. Springer, September, 2013.
5. Pablo Buiras, Amit Levy, Deian Stefan, Alejandro Russo, and David Mazières. A Library for Removing Cache-Based Attacks in Concurrent Information Flow Systems. In Proceedings of *Trustworthy Global Computing (TGC)*. Springer, August, 2013.
6. Daniel B. Giffin, Amit Levy, Deian Stefan, David Terei, David Mazières, John Mitchell, and Alejandro Russo. Hails: Protecting Data Privacy in Untrusted Web Applications. In Proceedings of *Symposium on Operating Systems Design and Implementation (OSDI)*. USENIX, October, 2012.
7. Deian Stefan, Alejandro Russo, Pablo Buiras, Amit Levy, John C. Mitchell, and David Mazières. Addressing Covert Termination and Timing Channels in Concurrent Information Flow Systems. In Proceedings of *International Conference on Functional Programming (ICFP)*. ACM SIGPLAN, September, 2012.
8. John C. Mitchell, Rahul Sharma, Deian Stefan, and Joe Zimmerman. Information-flow control for programming on encrypted data. In Proceedings of *Computer Security Foundations Symposium (CSF)*. IEEE, June, 2012.
9. Deian Stefan, Alejandro Russo, John C. Mitchell, and David Mazières. Flexible Dynamic Information Flow Control in Haskell. In Proceedings of *Haskell Symposium*. ACM SIGPLAN, September, 2011.
10. Deian Stefan and Danfeng Yao. Keystroke-dynamics authentication against synthetic forgeries. In Proceedings of *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. IEEE, October, 2010.
11. Shahram Khazaei, Simon Knellwolf, Willi Meier, and Deian Stefan. Improved Linear Differential Attacks on CubeHash. In Proceedings of *International Conference on Cryptology (AFRICACRYPT)*. Springer, May, 2010.
12. Deian Stefan. Hardware Framework for the Rabbit Stream Cipher. In Proceedings of *International Conference on Information Security and Cryptology (INSCRYPT)*. Springer, December, 2009.
13. Jared Harwayne-Gidansky, Deian Stefan, and Ishaan L. Dalal. FPGA-based SoC for real-time network intrusion detection using counting bloom filters. In Proceedings of *SoutheastCon*. IEEE, March, 2009.
14. Ishaan L. Dalal, Deian Stefan, and Jared Harwayne-Gidansky. Low discrepancy sequences for Monte Carlo simulations on reconfigurable platforms. In Proceedings of *International Conference on Application-Specific Systems, Architectures and Processors (ASAP)*. IEEE, July, 2008.
15. Deian Stefan, David B. Nummey, Jared Harwayne-Gidansky, and Ishaan L. Dalal. On Parallelizing the CryptMT Stream Cipher. In Proceedings of *Vehicular Technology Conference (VTC Spring)*. IEEE, May, 2008.

16. Ishaan L. Dalal and Deian Stefan. A hardware framework for the fast generation of multiple long-period random number streams. In Proceedings of *International Symposium on Field Programmable Gate Arrays (FPGA)*. ACM, February, 2008.

Journals

17. Deian Stefan, Alejandro Russo, David Mazières and John C. Mitchell. Flexible Dynamic Information Flow Control in the Presence of Exceptions. *Journal of Functional Programming*. Cambridge University Press. 2012. *Accepted/under revision.*
18. Deian Stefan, Xiaokui Shu, and Danfeng (Daphne) Yao. Robustness of keystroke-dynamics based biometrics against synthetic forgeries. *Computers & Security*. Elsevier. 31(1), 2012.
19. Kui Xu, Huijun Xiong, Chehai Wu, Deian Stefan, and Danfeng Yao. Data-Provenance Verification For Secure Hosts. *Transactions on Dependable and Secure Computing*. IEEE. 2012.

Workshops

20. Edward Yang, Deian Stefan, John Mitchell, David Mazières, Petr Marchenko, and Brad Karp. Toward Principled Browser Security. In Proceedings of *Workshop on Hot Topics in Operating Systems (HotOS)*. USENIX, May, 2013.
21. Deian Stefan, Alejandro Russo, David Mazières, and John C. Mitchell. Disjunction Category Labels. In Proceedings of *Nordic Conference on Security IT Systems (NordSec)*. Springer, October, 2011.
22. Joppe W. Bos and Deian Stefan. Performance analysis of the SHA-3 candidates on exotic multi-core architectures. In Proceedings of *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, August, 2010.
23. Dag Arne Osvik, Joppe W. Bos, Deian Stefan, and David Canright. Fast software AES encryption. In Proceedings of *International Workshop on Fast Software Encryption (FSE)*. Springer, February, 2010.
24. Deian Stefan and Christopher Mitchell. On the Parallelization of the MICKEY-128 2.0 Stream Cipher. In Proceedings of *The State of the Art of Stream Ciphers (SASC)*. Springer, February, 2008.

Demos

25. Deian Stefan, Amit Levy, Alejandro Russo, and David Mazières. Building Secure Systems with LIO. In Proceedings of *Haskell Symposium*. ACM SIGPLAN, September, 2014.
26. Amit Levy, David Terei, and David Mazières. Making Web Applications -XSafe. In Proceedings of *Haskell Symposium*. ACM SIGPLAN, September, 2014.
27. Deian Stefan and David Mazières. Building Secure Systems with LIO. In Proceedings of *Workshop on Programming Languages and Analysis for Security (PLAS)*. ACM SIGPLAN, July, 2014.

Non-Refereed Papers

28. Daniel B. Giffin, Stefan Heule, Amit Levy , David Mazières, John Mitchell, Alejandro Russo, Amy Shen, Deian Stefan, David Terei, and Edward Z. Yang. Security and the average programmer. In Proceedings of *Conference on Principles of Security and Trust (POST)*. Springer, April, 2014.
29. Alex Bain, John Mitchell, Rahul Sharma, Deian Stefan, and Joe Zimmerman. A Domain-Specific Language for Computing on Encrypted Data. In Proceedings of *Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*. LIPIcs, December, 2011. *Invited paper.*
30. Deian Stefan and John C. Mitchell. Analysing Object-Capability Patterns With Murφ. *Stanford TR*. April, 2011.

In Preparation

31. Deian Stefan, Anie Liu, and Dan Boneh. Building least privileged applications with ESpectro *In preparation for the* Symposium on Operating Systems Principles (SOSP).
32. Dante Zanarini, Deian Stefan, Pablo Buiras, and Alejandro Russo. Coarse-grained IFC ⇔ Fine-grained IFC. *In preparation for the* Computer Security Foundations Symposium (CSF).
33. Pablo Buiras, Deian Stefan, and Alejandro Russo. On Dynamic Flow-sensitive Floating-Label Systems. *In preparation for the Journal of Computer of Security.*

Software

ESpectro A libary for building building least privileged Node.js apps
COWL A backwards-compatible browser confinement system
Hails Haskell framework for building secure exensible web applications
LIO Library to building secure systems with information flow control

Talks

COWL

Oct 2014 W3C Technical Plenary / Advisory Committee Meeting. Santa Clara, CA.
Oct 2014 OSDI 2014. Broomfield, OR.
Apr 2014 Stanford Security Workshop. Stanford, CA.
Oct 2013 Mozilla Research Seminar. San Francisco, CA.
May 2013 HotOS 2013. Santa Ana Pueblo, NM.

Hails

Jul 2014 PLAS 2014. Uppsala, Sweden.
Jun 2013 MIT CSAIL Security Seminar. Boston, MA.
Dec 2012 UPenn Programming Languages Club. Pennsylvania, PA.
Oct 2012 OSDI 2012. Hollywood, CA.
Apr 2011 Stanford Security Workshop. Stanford, CA.

LIO

Sep 2014 Haskell Symposium 2014. Gothenburg, Sweden.
Sep 2013 ESORICS 2013. Egham, U.K.
Sep 2012 ICFP 2012. Copenhagen, Denmark.
Jul 2012 Symantec Security Seminar. Mountain View, CA.
Apr 2012 Stanford Security Workshop. Stanford, CA.
Sep 2011 Haskell Symposium 2011. Tokyo, Japan.

Teaching Experience

Stanford University

Fall 2014 **Programming Languages (CS242)**, *Co-instructor*.
Fall 2013 **Programming Languages (CS242)**, *Co-instructor*.
Winter 2013 **Advanced Topics in Operating Systems (CS240)**, *Teaching assistant*.
Fall 2013 **Programming Languages (CS242)**, *Teaching assistant*.

The Cooper Union

Summer 2010 **Advanced Programming in Java**, *Retraining-program instructor*.
Spring 2010 **Programming in Java**, *Retraining-program instructor*.
Spring 2009 **Topics in Probability & Stochastic Processes (ECE 403)**, *Teaching assistant*.
Spring 2007 **Digital Logic Design (ECE150)**, *Teaching assistant*.
Fall 2006 **Digital Logic Design (ECE150)**, *Teaching assistant*.

Awards and Honors

2014 Mozilla research grant for COWL-related work.
2011–2014 NDSEG graduate fellowship.
2010 CubeHash cryptanalysis prize for AFRICACRYPT 2010 paper.
2010 Best paper award at CollaborateCom 2010.
2009–2011 Cooper Union full-tuition graduate fellowship.
2009 NSF Research Highlight for botnet-detection work.
2005–2009 Cooper Union full-tuition undergraduate scholarship.

Professional Service

Working Groups

2014-today W3C Web Application Security Working Group

Program Committees

2016 Conference on Principles of Security and Trust (POST)
2015 Workshop on Foundations of Computer Security (FCS)

Reviewing

Conference ICFP 2014, PLAS 2014, Oakland 2013, ESORICS 2012, CSF 2011, NSDI 2011
Journal Int. Journal of Information Security, Computer & Electrical Engineering, Microprocessors and Microsystems, IEEE Potentials

Other

2013–2014 Stanford CS faculty hiring committee
2011–2014 Stanford CS PhD admissions committee

References

David Mazières (advisor)
Associate Professor
Computer Science
Stanford University
deianfaculty@nospam.scs.stanford.edu

John C. Mitchell (advisor)
Professor
Computer Science and Electrical Engineering
Stanford University
jcm@cs.stanford.edu

Alejandro Russo
Associate Professor
Computer Science and Electrical Engineering
Chalmers University of Technology
russo@chalmers.se

Dan Boneh
Professor
Computer Science and Electrical Engineering
Stanford University
dabo@cs.stanford.edu