JOSEPH BONNEAU — C.V.

jcb@cs.nyu.edu

RESEARCH INTERESTS

Computer & web security, applied cryptography, cryptocurrencies, human authentication

CURRENT POSITION

Assistant Professor New York University, 2017–present

- Department of Computer Science, Courant Institute

EDUCATION & ACADEMIC POSITIONS

Postdoctoral Researcher Stanford University, 2015–2016 (half-time appointment)

- Supervisor: Professor Dan Boneh
- Research areas: cryptocurrencies, secure messaging

Technology Fellow Electronic Frontier Foundation, 2015–2016 (half-time appointment)

- Supervisor: Peter Eckersley (EFF Chief Computer Scientist)
- Project areas: policy and regulation for secure messaging, HTTPS, cryptocurrencies

Secure Usability Senior Fellowship, Open Technology Fund. 2015.

Postdoctoral Fellow Center for Information Technology Policy, Princeton University, 2014.

- Supervisors: Professor Arvind Narayanan and Professor Ed Felten
- Research areas: Cryptocurrencies, secure messaging, HTTPS, password security

Ph.D Computer Laboratory, University of Cambridge, 2008–2012.

- Thesis title: Guessing human-chosen secrets (May 2012)
- Supervisor: Professor Ross Anderson
- Gates Cambridge Scholar

M.S. Dept. of Computer Science, Stanford University, 2006–2007.

- Research project: Cache-based timing attacks on AES
- Supervisor: Professor Dan Boneh
- Relevant coursework: cryptography, systems security, finite-state model checking

B.S. Dept. of Computer Science, Stanford University, 2002–2006.

- Terman award winner (top of graduating class)
- Degree conferred with distinction
- Relevant coursework: operating systems, compilers, databases, algorithms, complexity theory, AI, computer architecture, calculus, probability, number theory, group theory, physics.

JOSEPH BONNEAU — C.V.

jcb@cs.nyu.edu

PROFESSIONAL EXPERIENCE

Google Inc., New York, NY. Engineer, 2012-2014.

- Design lead for new project for cross-platform application identification.
- Initiated new project on HTTPS link security across Google properties.

Yahoo! Inc., Sunnyvale, CA. Intern, 2011.

- Researched password choices of Yahoo! users.
- Contributed to development of a dynamic password blacklist.

Cryptography Research, Inc., San Francisco, CA. Cryptographic Scientist, 2007–2008.

- Researched differential power analysis attacks and countermeasures.
- Developed obfuscation techniques and white-box cryptography for Blu-Ray discs.
- Security consultant for a range of consumer electronics products and websites.

Microsoft Corporation, Redmond, WA. Software Development Intern, 2006.

- Developed obfuscation tool for binary executable files.

Federal Bureau of Investigation, Washington, DC. Honors Intern, 2005.

- Designed and developed secure software for document management application.

Integration Appliance, Inc., Palo Alto, CA. Software Development Intern, 2004.

- Developed database management visualization interface.

TEACHING

Co-Instructor w/Andrew Miller. Smart Contracts (MOOC), Coursera. 12 lectures (2019)

Instructor & Course Designer Introduction to Cryptography and Computer Security, New York University. 14 lectures (2018–2019)

Instructor & Course Designer Cryptocurrencies and Decentralized Ledgers, New York University. 14 lectures (2018–2019)

Co-Instructor & Co-Designer w/Professor Dan Boneh. Stanford University CS 251: Cryptocurrencies, 20 lecture course (2015)

Co-Instructor w/Professor Ed Felten and Professor Arvind Narayanan. BTC-Tech Bitcoin and Cryptocurrencies MOOC, 11 lecture massively open online course (MOOC) (2015)

Co-Instructor & Co-Designer w/Professor Arvind Narayanan. Princeton University COS 597E: Bitcoin and Cryptocurrency Technologies, 20 lecture course (2014)

Instructor, East Jersey State Prison. Introduction to Probability and Statistics (2014)

Course Lecturer, University of Cambridge. Big Data, 4 lecture short course (2012)

Course Supervisor, University of Cambridge. Cryptography (2008–2011), Computer Security (2009-2011), Economics and Law for Computer Science (2009–2010), Business Studies (2011), Discrete Mathematics (2010)

Teaching Assistant, Stanford University. Discrete Mathematics A (2006–2007), Discrete Mathematics B (2007), Senior Projects (2006), Introduction to Programming (2004–2006)

ACADEMIC SERVICE

Financial Cryptography Steering commitee, 2016–2023
Dagstuhl Seminar *Security of Decentralized Financial Technologies*. Co-organizer, 2020
Simons Foundation Symposium *Proofs, Consensus and Decentralized Society*. Participant, 2019
Dagstuhl Seminar *Blockchain Security at Scale*. Co-organizer, 2018
Dagstuhl Seminar *Opportunities and Risks of Blockchain Technologies*. Co-organizer, 2017
Financial Cryptography General Chair, 2015

PROGRAM COMMITTEES

USENIX Security Symposium—2020, 2019, 2018, 2017, 2016, 2015
IEEE Symposium on Security & Privacy (Oakland)—2020, 2019, 2017, 2016 (*Student Chair*), 2015
Network and Distributed Systems Security Symposium (NDSS)—2017, 2015
ACM Conference on Computer and Communication Security (CCS)—2016, 2015
Symposium on Usable Privacy and Security (SOUPS)—2018, 2015, 2014
Financial Cryptography—2020 (*Chair*), 2019, 2017, 2016, 2015
Crypto Valley Conference—2019 (*Chair*)
Privacy Enhancing Technologies Symposium (PETS)—2018, 2017, 2016, 2015
European Symposium and Security and Privacy (Euro S&P)—2020, 2019, 2017
Workshop on Bitcoin and Blockchain Research (BITCOIN)—2017 (*Chair*), 2016, 2015
Workshop on the Economics of Information Security (WEIS)—2016, 2014
IEEE Security & Privacy on the Blockchain—2018, 2017
Stanford Blockchain Conference—2019, 2018, 2017 (*Chair*)
International World Wide Web Conference (WWW), Security Track—2017, 2016, 2015, 2012
USENIX Enigma—2017
EuroUSEC: 2nd European Workshop on Usable Security—2018, 2017
Passwords—2016, 2015
USENIX Summit on Hot Topics in Security (HotSec)—2015 (*Chair*)
Learning from Authoritative Experiments in Security Research Workshop (LASER)—2013
Workshop on Social Network Systems (SNS)—2010

LEADERSHIP POSITIONS

2015–2017—Sea Kayaking Guide, Environmental Traveling Companions
2015—Teacher, Prison University Project
2014—Teacher, Princeton Prison Teaching Initiative
2009–2010—President, Gates Scholars' Society
2009–2010—Chairperson, Gates Scholars' Council
2009–2011—MCR Technology Officer, Churchill College

2009–2010—Organiser for Security Seminar Series, Cambridge Computer Laboratory

HONORS & AWARDS

2017—Caspar Bowden Privacy Enhancing Technology Award, PETS

2015—Best Student/Postdoctoral Paper Award, WWW Security

2015—Best Reviewer Award, IEEE Security and Privacy (Oakland)

2013—NSA Award for Best Scientific Cybersecurity Paper

2012—Best Data Control Project, Wall Street Journal Data Transparency Weekend

2008—Gates Cambridge Scholarship

2006—Frederick E. Terman Engineering Scholastic Award (top 5% of School of Engineering)

2006—B.S. conferred with distinction (top of Computer Science Department)

2002—National Merit Scholarship

2002—Robert C. Byrd Scholarship

CERTIFICATIONS

2015—Sea Kayaking Guide

2013—Wilderness Emergency Medical Technician

2013—Emergency Medical Technician

2013—Certified Information Privacy Professional

2012—Open Water Scuba Diver

2002—Private Pilot's Certificate

PERSONAL

Nationality: USA, born 1984 in San Francisco, CA.

Language: English (native). Conversant in French and Spanish.

JOSEPH BONNEAU — C.V.

jcb@cs.nyu.edu

TEXTBOOK

Arvind Narayanan, **Joseph Bonneau**, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016

PUBLICATIONS IN TOP-TIER CONFERENCES & JOURNALS

Dan Boneh, **Joseph Bonneau**, Benedikt Bunz, and Ben Fisch. Verifiable Delay Functions. In *The 2018 IACR International Cryptology Conference*, August 2018

Ruba Abu-Salma, M. Angela Sasse, **Joseph Bonneau**, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy*, May 2017

Joshua Tan, Lujo Bauer, **Joseph Bonneau**, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. Can Unicorns Help Users Compare Crypto Key Fingerprints? In *The 2017 ACM CHI Conference on Human Factors in Computing Systems*, May 2017

Jeremiah Blocki, Anupam Datta, and **Joseph Bonneau**. Differentially Private Password Frequency Lists. In *NDSS '16: The 2016 Network and Distributed System Security Symposium*, February 2016

Gaby G. Dagher, Benedikt Bunz, **Joseph Bonneau**, Jeremy Clark, and Dan Boneh. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. In *CCS '15: Proceedings of the 22nd ACM Conference on Computer and Communications Security*, October 2015

Marcela S. Melara, Aaron Blankstein, **Joseph Bonneau**, Michael J. Freedman, and Edward W. Felten. CONIKS: Bringing Key Transparency to End Users. In *Proceedings of the 24th USENIX Security Symposium*, August 2015 ***2017 PET Award***

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*, July 2015

Nik Unger, Sergej Dechand, **Joseph Bonneau**, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith. SoK: Secure Messaging. In *2015 IEEE Symposium on Security and Privacy*, May 2015

Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *25th International World Wide Web Conference (WWW)*, May 2015 ***Best Student Paper***

Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, May 2015

Rahul Chatterjee, **Joseph Bonneau**, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. In *2015 IEEE Symposium on Security and Privacy*, May 2015

Michael Kranch and **Joseph Bonneau**. Upgrading HTTPS in Mid-Air: An Empirical Study of Strict Transport Security and Key Pinning. In *NDSS '15: The 2015 Network and Distributed System Security Symposium*, February 2015

Joseph Bonneau and Stuart Schechter. Towards reliable storage of 56-bit secrets in human memory. In *Proceedings of the 23rd USENIX Security Symposium*, August 2014

Anupam Das, **Joseph Bonneau**, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *NDSS '14: The 2014 Network and Distributed System Security Symposium*, February 2014

Joseph Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy*, May 2012 ***NSA Award for Best Scientific Cybersecurity Paper of 2012***

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*, May 2012

Joseph Bonneau and Ilya Mironov. Cache Collision Timing Attacks Against AES. In *CHES '06: Proceedings of 2006 Workshop on Cryptographic Hardware and Embedded Systems*, October 2006

OTHER PEER-REVIEWED PUBLICATIONS

Camelia Simoiu, Christopher Gates, **Joseph Bonneau**, and Sharad Goel. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *SOUPS 2019: The 15th Symposium On Usable Privacy and Security*, August 2019

Joseph Bonneau. Hostile blockchain takeovers. In *The 2018 IFCA Workshop on Bitcoin and Blockchain Research*, March 2018

Saba Eskandarian, Eran Messeri, **Joseph Bonneau**, and Dan Boneh. Certificate Transparency with Privacy. In *The 17th Privacy Enhancing Technologies Symposium*, July 2017

Benedikt Bunz, Steven Goldfeder, and **Joseph Bonneau**. Proofs-of-delay and randomness beacons in Ethereum. In *S&B '17: Proceedings of the 1st IEEE Security & Privacy on the Blockchain Workshop*, April 2017

Steven Goldfeder, **Joseph Bonneau**, Rosario Gennaro, and Arvind Narayanan. Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin. In *FC '17: Proceedings of the the 21st International Conference on Financial Cryptography*, April 2017

Joseph Bonneau. Why buy when you can rent? Bribery attacks on Bitcoin consensus. In *BITCOIN '16: Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research*, February 2016

Joseph Bonneau. EthIKS: Using Ethereum to audit a CONIKS key transparency log. In *BITCOIN '16: Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research*, February 2016

Okke Schrijvers, **Joseph Bonneau**, Dan Boneh, and Tim Roughgarden. Incentive Compatibility of Bitcoin Mining Pool Reward Functions. In *FC '16: Proceedings of the the 20th International Conference on Financial Cryptography*, February 2016

Marie Vasek, **Joseph Bonneau**, Ryan Castellucci, Cameron Keith, and Tyler Moore. The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets. In *FC '16: Proceedings of the the 20th International Conference on Financial Cryptography*, February 2016

Stuart Schechter and **Joseph Bonneau**. Learning Assigned Secrets for Unlocking Mobile Devices. *SOUPS '15: Proceedings of the 11th Symposium On Usable Privacy and Security*, July 2015

Harry Kalodner, Miles Carlsten, Paul Ellenbogen, **Joseph Bonneau**, and Arvind Narayanan. An empirical study of Namecoin and lessons for decentralized namespace design. *WEIS '15: Proceedings of the 14th Workshop on the Economics of Information Security*, June 2015

Nicky Robinson and **Joseph Bonneau**. Cognitive Disconnect: Understanding Facebook Connect Login Permissions. In *COSN '14: ACM Conference on Online Social Networks*, October 2014

Joseph Bonneau, Ed Felten, Prateek Mittal, and Arvind Narayanan. Privacy concerns of implicit secondary factors for web authentication. In *WAY 2014: Who are you?! Adventures in Authentication Workshop*, July 2014

Jeremy Clark, **Joseph Bonneau**, Edward W. Felten, Joshua A. Kroll, Andrew Miller, and Arvind Narayanan. On Decentralizing Prediction Markets and Order Books. In *WEIS '14: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2014

Joseph Bonneau and Andrew Miller. Fawkescoin: A cryptocurrency without public-key cryptography. In *22nd International Workshop on Security Protocols*, March 2014

Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In *FC '14: Proceedings of the the 18th International Conference on Financial Cryptography*, March 2014

Joseph Bonneau. S-links: Why distributed security policy requires secure introduction. In *Web 2.0 Security & Privacy*, May 2013

Joseph Bonneau and Rubin Xu. Of contraseñas, sysmawt, and mìmă: Character encoding issues for web passwords. In *Web 2.0 Security & Privacy*, May 2012

Joseph Bonneau. Statistical metrics for individual password strength. In *20th International Workshop on Security Protocols*, April 2012

Joseph Bonneau and Ekaterina Shutova. Linguistic properties of multi-word passphrases. In *USEC '12: Workshop on Usable Security*, March 2012

Joseph Bonneau, Sören Preibusch, and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *FC '12: Proceedings of the the 16th International Conference on Financial Cryptography*, March 2012

Sören Preibusch and **Joseph Bonneau**. The privacy landscape: product differentiation on data collection. In *WEIS '11: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2011

Joseph Bonneau. Getting web authentication right: a best-case protocol for the remaining life of passwords. In *19th International Workshop on Security Protocols*, March 2011

Joseph Bonneau and Rubin Xu. Scrambling for lightweight censorship resistance. In *19th International Workshop on Security Protocols*, March 2011

Sören Preibusch and **Joseph Bonneau**. The Password Game: negative externalities from weak password practices. In *GameSec 2010: Conference on Decision and Game Theory for Security*, November 2010

Joseph Bonneau and Sören Preibusch. The password thicket: technical and market failures in human authentication on the web. In *WEIS '10: Proceedings of the 9th Workshop on the Economics of Information Security*, June 2010

Jonathan Anderson, **Joseph Bonneau**, and Frank Stajano. Inglourious Installers: Security in the Application Marketplace. In *WEIS '10: Proceedings of the 9th Workshop on the Economics of Information Security*, June 2010

Christo Wilson, Alessandra Sala, **Joseph Bonneau**, Robert Zablit, and Ben Zhao. Don't Tread on Me: Moderating Access to OSN Data with SpikeStrip . In *WOSN 2010: The 3rd Workshop on Online Social Networks*, June 2010

Joseph Bonneau. Digital immolation: new directions in online protest. In *18th International Workshop on Security Protocols*, March 2010

Joseph Bonneau, Mike Just, and Greg Matthews. What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions. In *FC '10: Proceedings of the the 14th International Conference on Financial Cryptography*, January 2010

Hyoungshick Kim and **Joseph Bonneau**. Privacy-Enhanced Public View for Social Graphs. In *SWSM '09: The 2nd Workshop on Social Web Search and Mining*, November 2009

Jonathan Anderson, Claudia Diaz, **Joseph Bonneau**, and Frank Stajano. Privacy Preserving Social Networking Over Untrusted Networks. In *WOSN 2009: The 2nd ACM SIGCOMM Workshop on Online Social Networks*, August 2009

Joseph Bonneau, Jonathan Anderson, and George Danezis. Prying Data out of a Social Network. In *ASONAM 09: The 1st International Conference on Advances in Social Networks Analysis and Mining*, July 2009

Joseph Bonneau and Sören Preibusch. The Privacy Jungle: On the Market for Privacy in Social Networks. In *WEIS '09: Proceedings of the 8th Workshop on the Economics of Information Security*, June 2009

Joseph Bonneau. Alice and Bob's life stories: Cryptographic communication using shared experiences. In *17th International Workshop on Security Protocols*, April 2009

Joseph Bonneau, Jonathan Anderson, Frank Stajano, and Ross Anderson. Eight Friends Are Enough: Social Graph Approximation via Public Listings. In *SNS '09: Proceedings of the 2nd ACM Workshop on Social Network Systems*, March 2009

OTHER TECHNICAL PUBLICATIONS & POSTERS

Assimakis Kattis and **Joseph Bonneau**. Proof of Necessary Work: Succinct State Verification with Fairness Guarantees. Technical Report 2020/190, Cryptology ePrint Archive, February 2020

Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On Bitcoin as a public randomness source. Technical Report 2015/1015, Cryptology ePrint Archive, October 2015

Ruba Abu-Salma, M. Angela Sasse, and **Joseph Bonneau**. Secure Chat for the Masses? User-centered Security to the Rescue (poster). In *CCS '15: Proceedings of the 22nd ACM Conference on Computer and Communications Security*, October 2015

Nicky Robinson and **Joseph Bonneau**. Clarity of Facebook Connect login permissions (poster). In *SOUPS 2014: The 10th Symposium On Usable Privacy and Security*, July 2014

Serge Egelman, **Joseph Bonneau**, Sonia Chiasson, David Dittrich, and Stuart Schechter. It's Not Stealing If You Need It: A Panel on The Ethics of Performing Research Using Public Data of Illicit Origin (panel discussion). In *WECSR '12: Workshop on Ethics in Computer Security Research*, March 2012

Luke Church, Jonathan Anderson, **Joseph Bonneau**, and Frank Stajano. Privacy Stories: Confidence in Privacy Behaviors through End User Programming (poster). In *SOUPS 2009: The 5th Symposium On Usable Privacy and Security*, July 2009

Joseph Bonneau, Jonathan Anderson, and Luke Church. Privacy Suites: Shared Privacy for Social Networks (poster). In *SOUPS 2009: The 5th Symposium On Usable Privacy and Security*, July 2009

Jonathan Anderson, **Joseph Bonneau**, and Frank Stajano. Security APIs for Online Applications. In *3rd International Workshop on Analysis of Security APIs*, July 2009

Joseph Bonneau. Robust Final-Round Cache-Trace Attacks Against AES. Technical Report 2006/374, Cryptology ePrint Archive, October 2006

Joseph Bonneau and Andrew Morrison. Finite State Security Analysis of OTR Version 2. 2006

Ben Fisch, **Joseph Bonneau**, Nicola Greco, and Juan Benet. Scaling Proof-of-Replication for Filecoin Mining. Technical report, Stanford University, 2019