DOUG TYGAR

Address:

University of California.
739 Soda Hall #1776
Berkeley, CA 94720-1776
(510) 643-7855
tygar@berkeley.edu

Personal Information:

Full name: Justin Douglas Tygar
US Citizen

Education:

A.B., 1982 **University of California, Berkeley**, *Math/Computer Science*
Bell Labs University Relations Student (1981)

Ph.D., 1986 **Harvard University**, *Computer Science*
Thesis: *An Integrated Toolkit for Operating System Security*
Advisor: Michael Rabin
NSF Graduate Fellow (1982 – 1985), IBM Graduate Fellow (1985 – 1986)

Academic Appointments:

University of California, Berkeley
Department of Electrical Engineering and Computer Science
& School of Information
1998 – Present *Professor* (tenured, joint appointment)

Carnegie Mellon University
Computer Science Department
2000 – 2005 *Adjunct Professor*
1992 – 2000 *Associate Professor* (tenured 1995, on leave 1998 – 2000)
1986 – 1992 *Assistant Professor*

Major Awards:

NSF Presidential Young Investigator, 1988
Outstanding Professor Award, *Carnegie Magazine*, 1989
Chair, Defense Information Science and Technology Study Group on Security with Privacy
Member, National Research Council Committee on Information Trustworthiness
Member, INFOSEC Science and Technology Study Group
Okawa Foundation Fellow, 2003-4
Test of Time Award, USENIX Security, 2015
Wide consulting for both industry and government

Major speeches:

Keynote addresses:

PODC (1995), ASIAN-96 (1996), NGITS (1997), VLDB (1998), CRYPTEC (1999),
CAV (2000), Human Authentication (2001), PDSN (2002), ISM (2005), ISC (2005), ASIACCS (2006),
Croucher ASI (2004, 2006), ISC (2008), AISEC (2010), ISRCS (2013), SERE (2014), IWSPA (2016)

Invited addresses:

Harvard Graduate School of Arts and Science 100th Anniversary,
CMU Computer Science Department 25th Anniversary
More than 260 talks & 20 professional seminars since 1985

External review activities:

Electronic Commerce Program, City University of Hong Kong
Information Systems Management Program, Singapore Management University
Information Technology Program, United Arab Emirates University
Computer Science Program, University of California, Davis

Publications

Books

1. **Adversarial Machine Learning: Computer Security and Statistical Machine Learning.** A. Joseph, B. Nelson, B. Rubinstein, J. D. Tygar. Cambridge University Press, 2017. (To appear).

2. **Computer Security in the 21st Century.** Eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, March 2005. (This book includes item 12 below as well as a technical introduction by me and the other editors.)

3. **Waiyādo/Waiyaresu Nettowōku ni Okeru Burōdokyasuto Tsūshin no Sekyuriti**
ワイヤード/ワイヤレスネットワークにおけるブロードキャスト通信のセキュリテ.
A. Perrig and J. D. Tygar; translated by Fumio Mizoguchi and the the Science University of Tokyo Information Media Science Research Group with the assistance of J. D. Tygar. Kyoritsu Shuppan, October 2004. (This is a Japanese translation of item 4 which also contains new and additional material written by me in Japanese.)

4. **Secure Broadcast Communication in Wired and Wireless Networks.** A. Perrig and J. D. Tygar. Springer, October 2002. (See also item 3.)

5. **Trust in Cyberspace.** National Research Council Committee on Information Systems Trustworthiness (S. Bellovin, W. E. Boebert, M. Branstad, J. R. Catoe, S. Crocker, C. Kaufman, S. Kent, J. Knight, S. McGeady, R. Nelson, A. Schiffman, F. Schneider [ed.], G. Spix, and J. D. Tygar). National Academy Press, January 1999.

Book Chapters (does not incude items listed above)

6. "Classifier evasion: Models and open problems." B. Nelson, B. Rubinstein, L. Huang, A. Joseph, and J. D. Tygar. In **Privacy and Security Issues in Data Mining and Machine Learning**, eds. C. Dimitrakakis, et al. Springer, July 2011, pp. 92-98.

7. "Misleading learners: Co-opting your spam filter." B. Nelson, M. Barreno, F. Chi, A. Joseph, B. Rubinstein, U. Saini, C. Sutton, J. D. Tygar, and K. Xia. In **Machine Learning in Cyber Trust: Security, Privacy, Reliability**, eds. J. Tsai and P.Yu. Springer, April 2009, pp. 17-51.

8. "Preface." J. D. Tygar. In **從DIGIart@eTaiwan談互動創意 (Interaction and Creation in DIGIart@eTaiwan)**,ed. S. Hsu. Ylib Publisher, July 2007.

9. "Case study: Acoustic keyboard emanations." L. Zhuang, F. Zhou, and J. D. Tygar. In **Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft**, eds. M. Jakobsson and S. Myers. Wiley-Interscience, December 2006, pp. 221-240. (This is a popularized version of item 31.)

10. "Dynamic security skins." R. Dhamija and J. D. Tygar. In **Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft**, eds. M. Jakobsson and S. Myers. Wiley-Interscience, December 2006, pp. 339-351. (This is a popularized version of item 84.)

11. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." A. Whitten and J. D. Tygar. In **Security and Usability: Designing Secure Systems that People Can Use**, eds. L. Cranor and G. Simson. O'Reilly, September 2005, pp. 679-702. (An earlier version of this paper was published in **Proceedings of the 8th USENIX Security Symposium**, August 1999, pp. 169-183. See also item 134.)

12. "Private matching." Y. Li, J. D. Tygar, J. Hellerstein. In **Computer Security in the 21st Century**, eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, March 2005, pp. 25-50. (See item 2.) (An early version of this paper appeared as Intel Research Laboratory Berkeley technical report IRB-TR-04-005, February 2004.)

13. "Digital cash." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction,** ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 167-170.

14. "Spamming." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction**, ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 673-675.

15. "Viruses." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction**, ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 788-791.

16. "Privacy in sensor webs and distributed information systems." J. D. Tygar. In **Software Security: Theories and Systems,** eds. M. Okada, B. Pierce, A. Scedrov, H. Tokuda, and A. Yonezawa. Springer, 2003, pp. 84-95.

17. "Atomicity in electronic commerce." J. D. Tygar. In **Internet Besieged**, eds. D. Denning and P. Denning. ACM Press and Addison-Wesley, October 1997, pp. 389-405. (An expanded earlier version of this paper was published in **Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing**, *Keynote paper*, May 1996, pp. 8-26; and as Carnegie Mellon University Computer Science technical report CMU-CS-96-112, January 1996. See also item 41.)

18. "Cryptographic postage indicia." J. D. Tygar, B. Yee, and N. Heintze. In **Concurrency and Parallelism, Programming, Networking, and Security**, eds. J. Jaffar and R. Yap. Springer, 1996, pp. 378-391. (Preprint also available. Early versions appeared as Carnegie Mellon University Computer Science technical reports CMU-CS-96-113, January 1996, UC San Diego Computer Science technical report UCSD-TR-CS96-485, and in the 1996 **Securicom Proceedings,** Paris, June 1996. See also item 136.)

19. "Dyad: A system for using physically secure coprocessors." J. D. Tygar and B. Yee. In **Technological Strategies for the Protection of Intellectual Property in the Networked Multimedia Environment**. Interactive Multimedia Association, 1994, pp. 121-152. (An early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-91-140R, May 1991.)

20. "A system for self-securing programs." J. D. Tygar and B. Yee. In **Carnegie Mellon Computer Science: A 25-Year Commemorative**, ed. R. Rashid. ACM Press and Addison-

Wesley, 1991, pp. 163-197. (Note: The first printing of this volume had incorrect text due to a production error.)

21. "Implementing capabilities without a trusted kernel." M. Herlihy and J. D. Tygar. In **Dependable Computing for Critical Applications**, eds. A. Avizienis and J. Laprie. Springer, January 1991, pp. 283-300. (Note: An early version appeared in the **(IFIP) Proceedings of the International Working Conference on Dependable Computing for Critical Applications**, August 1989.)

22. "Strongbox." J. D. Tygar and B. Yee. In **Camelot and Avalon: A Distributed Transaction Facility**, eds. J. Eppinger, L. Mummert, and A. Spector. Morgan-Kaufmann, February 1991, pp. 381-400.

23. "ITOSS: An Integrated Toolkit for Operating System Security." M. Rabin and J. D. Tygar. In **Foundations of Data Organization**, eds. W. Litwin and H.-J. Shek. Springer, June 1989, pp. 2-15. (Preprint also available.) (Note: Earlier, longer versions appeared as Harvard University Aiken Computation Laboratory technical report TR-05-87R and my Ph.D. dissertation.)

24. "Formal semantics for visual specification of security." M. Maimone, J. D. Tygar, and J. Wing. In **Visual Languages and Visual Programming**, ed. S. K. Chang. Plenum, 1990, pp. 97-116. (An early version was published in **Proceedings of the 1988 IEEE Workshop on Visual Programming**, pp. 45-51, and as Carnegie Mellon University Computer Science technical report CMU-CS-88-173r, December 1988.)

Journal Articles (does not include items listed above)

25. "Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study. L. Connolly, M. Lang, J. Gathegi, J. D. Tygar. *Information & Computer Security*. 25:2, April 2017, pp. 118-136.

26. "Machine Learning Methods for Computer Security." A. Joseph, P. Laskov, F. Roli, J. D. Tygar, B. Nelson. *Dagstuhl Manifestos* 3:1, December 2013, pp. 1-30.

27. "A low-bandwidth camera sensor platform with applications in smart camera networks." P. Chen, K. Hong, N. Naikal, S. Sastry, J. D. Tygar, P. Yan, A. Yan, L. Chang, L. Lin, Leon S. Wang, E. Lobaton, S. Oh, and P. Ahammad. *ACM Transactions on Sensor Networks*, 9:2, March 2013, pp. 21:1-21:23.

28. "Query strategies for evading convex-inducing classifiers." B. Nelson, B. Rubinstein, L. Huang, A. Joseph, S. Lee, S. Rao, and J. D. Tygar. *Journal of Machine Learning Research*, May 2012 (volume 13) pp. 1293-1332. (Also available as arXiv report 1007.0484v1, July 2010.)

29. "The security of machine learning." M. Barreno, B. Nelson, A. Joseph, and J. D. Tygar. *Machine Learning*, 81:2, November 2010, pp. 121-148. (An earlier version appeared as UC Berkeley EECS technical report UCB/EECS-2008-43, April 2008.)

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.