Sergey Bratus, Ph.D.

Institute for Security, Technology, and Society
Dartmouth College
ph. 603-646-9224

Employment

- ◇ **Research Assistant Professor**, Computer Science Dept., Dartmouth College (2008–present)
- ◇ **Principal Security Technology Advisor to Kiewit Computing**, Dartmouth College (2008–present)
- ◇ **Senior Research Associate**, Institute for Security Technology, and Society, Dartmouth College (2005–2008)
- ◇ **Consultant**, BAE Systems (2006–2009)
- ◇ **Research Associate**, Institute for Security Technology Studies, Dartmouth College (2002–2005)
- ◇ **Scientist**, BBN Technologies/Verizon (1999–2001)
- ◇ **Instructor**, Northeastern University, College of Computer Science (1997–1999)
- ◇ **UNIX system administrator**, Northeastern University, Dept. of Mathematics (1997–2001)
- ◇ **Teaching Assistant**, Northeastern University, Dept. of Mathematics (1993–1996)

Research and Software Engineering

◇ **Computer security, Intrusion Analysis, Reverse Engineering**

Institute for Security, Technology, and Society, Dartmouth College, 2002–present time

- · Worked on distilling security practitioner methodologies behind the discovery of high-impact vulnerabilities by vulnerability researchers, hackers
- · Studied the security challenges of composition of software modules in terms of Formal Language Theory and Theory of Computation
- · Led a security assessment of a Control Center network of a Fortune 500 utility company.
- · Managed the Dartmouth Internet Security Testbed (DIST) wireless, an 802.11 research infrastructure of over 200 Air Monitors distributed throughout diverse locations of the Dartmouth College campus (`http://www.cs.dartmouth.edu/~dist/`)
- · Proposed new hardware security primitives for Trusted Computing systems and security context separation in virtualized environments (Best Paper Award at the TRUST 2008 conference)
- · Performed fuzz-testing of proprietary SCADA protocols and equipment `http://lzfuzz.cs.dartmouth.edu/`
- · Researched link layer fingerprinting techniques for 802.11 stations and designed an active fingerprinting tool (`http://baffle.cs.dartmouth.edu/`)
- · Designed and developed automated log analysis tools for host and network logs for the Kerf project (`http://kerf.cs.dartmouth.edu/`)
- · Applied statistical machine learning, data organization and information theory techniques to log and network trace analysis tasks

- Extended a research Linux kernel system call logging and policy enforcement framework and developed tools for visualization and analysis of resulting system call traces
- Analyzed rootkit deception techniques, their detection and defensive applications
- Studied UNIX kernel security mechanisms, including LSM and NSA SELinux security policies, Linux Vserver, BSD jails and other virtualization solutions, and researched ways to improve their usability
- Performed security assessment of PlanetLab Central, for the PlanetLab project
- Directed parts of the campus-wide Dartmouth computer security assessment, organized various graduate and undergraduate student efforts
- Performed analysis of compromised systems, data recovery, OS hardening
- Directed student research related to Linux kernel security and Xen virtualization security mechanisms
- Reviewer for ACSAC, SecSE, PST, SiS, ATC and other conferences, subreviewer for CCS, NDSS, USEC.

BAE Systems, National Security Solutions, Inc., 2006—2009

- Windows kernel mode rootkit detection software
- Defensive reverse engineering protection measures
- Participated in developing research proposals

Publications:

- *"Composition Patterns of Hacking"* with Julian Bangert, Alexandar Gabrovsky, Anna Shubina, Daniel Bilar, Michael E. Locasto, in Proceedings of Cyberpatterns 2012
- *"A Patch for Postel's Robustness Principle"* with Len Sassaman, Meredith L. Patterson, IEEE Security and Privacy Journal, Volume 10, Issue 2, March-April 2012
- *"Identifying Vulnerabilities in SCADA Systems via Fuzz-Testing"*, with Rebecca Shapiro, Edmond Rogers, Sean Smith, in IFIP Advances in Information and Communication Technology, 2011, Volume 367, 2011
- *"Packets in Packets: Orson Welles In-Band Signaling Attacks for Modern Radios"* with Travis Goodspeed, Ricky Melgares, Rebecca Shapiro, Ryan Speers, in Proceedings of the 5th USENIX Workshop on Offensive Technologies, August 2011
- *"Exploiting the Hard-working DWARF: Trojan and Exploit Techniques with No Native Executable Code"* with James Oakley, in Proceedings of the 5th USENIX Workshop on Offensive Technologies, August 2011
- *"Exploit Programming: from Buffer Overflows to Weird Machines and Theory of Computation"* with Michael E. Locasto, Meredith L. Patterson, Len Sassaman, Anna Shubina, in USENIX ;login:, December 2011
- *"The Halting Problems of Network Stack Insecurity"* with Len Sassaman, Meredith L. Patterson, Anna Shubina, in USENIX ;login:, December 2011
- *"Intrusion Detection for Resource-constrained Embedded Control Systems in the Power Grid"* with Jason Reeves, Ashwin Ramaswamy, Michael Locasto, Sean Smith, International Journal of Critical Infrastructure Protection, 2011
- *"Beyond SELinux: the Case for Behavior-Based Policy and Trust Languages"* with Michael E. Locasto, Boris Otto, Rebecca Shapiro, Sean W. Smith, Gabriel Weaver, Dartmouth Computer Science Technical Report TR2011-701, August 2011
- *"Security Applications of Formal Language Theory"* with Len Sassaman, Meredith L. Patterson, Michael E. Locasto, Anna Shubina, Dartmouth Computer Science Technical Report TR2011-709, 2011

- *"Api-do: Tools for Exploring the Wireless Attack Surface in Smart Meters"* with Travis Goodspeed, Ricky Melgares, Ryan Speers, Sean W. Smith, Hawaii International Conference on System Sciences, January 2012
- *"On Tuning the Knobs of Distribution-Based Methods for Detecting VoIP Covert Channels"* with Chrisil Arackaparambil, Guanhua Yan, Alper Caglayan, Hawaii International Conference on System Sciences, January 2012
- *"Assessing the Vulnerability of SCADA Devices"*, with Rebecca Shapiro and Sean Smith, Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, 2011, August 2011
- *"Lightweight Intrusion Detection for Resource-Constrained Embedded Control Systems"*, with Jason Reeves, Ashwin Ramaswamy, Michael Locasto, and Sean Smith, Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, 2011, August 2011
- *"Using Hierarchical Change Mining to Manage Network Security Policy Evolution"*, with Gabriel A. Weaver, Nick Foti, Dan Rockmore, and Sean W. Smith, USENIX HotICE, Boston, 2011
- *"Exploiting the hard-working DWARF"* with James Oakley. Shmoocon 2011, Washington, DC
- *"Exploiting the hard-working DWARF"* with James Oakley. Hackito Ergo Sum 2011, Paris, France
- *"Detection of Rogue APs Using Clock Skews: Does It Really Work?"*, with Chrisil Arackaparambil and Anna Shubina, Shmoocon 2010, Washington, DC
- *"Detection of Rogue APs Using Clock Skews: Does It Really Work?"*, with Chrisil Arackaparambil and Anna Shubina, Toorcon 2009, San Diego, CA
- *"SegSlice: Towards a New Class of Secure Programming Primitives for Trustworthy Platforms"*, with Michael E. Locasto, Brian Schulte, TRUST 2010, Berlin, Germany, 2010
- *"Software on the witness stand: what should it take for us to trust it?"*, with Ashlyn Lembree, Anna Shubina, TRUST 2010, Berlin, Germany, 2010
- *"The diversity of TPMs and its effects on development: a case study of integrating the TPM into OpenSolaris"*, with Anna Shubina, Wyllys Ingersol, Sean W. Smith, 5th ACM Workshop on Scalable Trusted Computing (STC '10), New York, NY, USA, 2010.
- *"VM-based security overkill: a lament for applied systems security research"*, with Michael E. Locasto, Ashwin Ramaswamy, Sean W. Smith, 2010 Workshop on New Security Paradigms (NSPW '10). New York, NY, USA, 2010.
- *"Automated Mapping of Large Binary Objects Using Primitive Fragment Type Classification"*, with Gregory Conti et al., 10th Annual DFRWS Conference, `http://www.dfrws.org/2010/`, Portland, OR, 2010
- *"A Visual Study of Primitive Binary Fragment Types"* with Gregory Conti et al., BlackHat USA 2010
- *"On the reliability of wireless fingerprinting using clock skews"*, with Chrisil Arackaparambil, Anna Shubina, David Kotz, 3rd ACM Conference On Wireless Network Security, Hoboken, NJ, 2010
- *"Teaching the principles of the hacker curriculum to undergraduates"*, with Anna Shubina, Michael E. Locasto, 41st ACM technical symposium on Computer science education, Milwaukee, WI, 2010

- *"Distributed Monitoring of Conditional Entropy for Anomaly Detection in Streams"*, with Chrisil Arackaparambil, Joshua Brody, Anna Shubina, 10th Workshop on Communication Architecture for Clusters, International Parallel and Distributed Processing Symposium, Atlanta, GA, 2010
- *"Katana: A Hot Patching Framework for ELF Executables"*, with Ashwin Ramaswamy, Michael E. Locasto, Sean W. Smith, 4th Workshop on Secure Software Engineering (SecSE), part of the ARES conference, Krakow, Poland, April, 2010
- *"Katana: Towards Patching as a Runtime Part of the Compiler-Linker-Loader Toolchain"*, with James Oakley, Ashwin Ramaswamy, Sean W. Smith, Michael E. Locasto, International Journal of Secure Software Engineering (IJSSE), Volume 1, Issue 3, 2010
- *"What Hacker Research Taught Me"*, Keynote at TROOPERS 2010, Germany, `http://www.troopers10.org/`
- *"What Hacker Research Taught Me"*, Defcon 802, May 2010, Burlington, VT, `http://dc802.org/`
- *"Bickering In-Depth: Rethinking the Composition of Competing Security Systems"*, with Michael E. Locasto, Brian Schulte, IEEE Security and Privacy Journal, vol. 7, no. 6, pp. 77–81, 2009
- *"The cake is a lie: privilege rings as a policy resource"*, with Peter C. Johnson, Ashwin Ramaswamy, Sean W. Smith, Michael E. Locasto, 1st ACM workshop on Virtual Machine Security (VMSec), Conference on Computer and Communications Security, Chicago, IL, 2009
- *"Dartmouth Internet Security Testbed (DIST): building a campus-wide wireless testbed"*, with David Kotz, Keren Tan, William Taylor, Anna Shubina, Bennet Vance, Michael E. Locasto, USENIX 2nd Workshop on Cyber Security Experimentation and Test (CSET), Montreal, Quebec, 2009
- *"Using Domain Knowledge for Ontology-Guided Entity Extraction from Noisy, Unstructured Text Data"*, with Anna Rumshisky, Rajendra Magar, Paul Thompson, 3rd Workshop on Analytics for Noisy Unstructured Text Data, Barcelona, Spain, 2009
- *"Traps, Events, Emulation, and Enforcement: Managing the Yin and Yang of Virtualization-based Security"*, with M.E.Locasto, A.Ramaswamy, and S.W.Smith, 1st Workshop on Virtual Machine Security (VMSec), Washington, D.C., 2008
- *"Why Do Street-Smart People Do Stupid Things Online?"*, with Chris Masone, Sean W. Smith, IEEE Security and Privacy Journal, vol. 6, no. 3, pp. 71–74, May 2008
- *"Embedded Systems – "Invisible" Devious Devices"*, TROOPERS 2009, Munich, Germany, `http://www.troopers09.org/`
- *"Backhoe, a packet trace and log browser"*, with Axel Hansen, Fabio Pellacini, and Anna Shubina, 5th International Workshop on Visualization for Computer Security (VizSec '08), Boston, 2008
- *"Streaming Estimation of Information-theoretic Metrics for Anomaly Detection (Extended Abstract)"*, with Joshua Brody, David Kotz and Anna Shubina, 11th International Symposium on Recent Advances in Intrusion Detection (RAID '08), Boston, 2008
- *"New Directions for Hardware-assisted Trusted Computing Policies (Position Paper)"*, with Michael Locasto, Ashwin Ramaswamy and Sean Smith, Future of Trust in Computing, Berlin, 2008
- *"Fuzzing Proprietary SCADA Protocols"*, Black Hat USA 2008, Las Vegas, NV, 2008
- *"LZfuzz: a fast compression-based fuzzer for poorly documented protocols"*, with Axel Hansen and Anna Shubina, Dartmouth Computer Science Technical Report TR2008-634, 2008

- *"TOCTOU, Traps and Trusted Computing"*, with Nihal D'Cunha, Evan Sparks and Sean Smith, **Best Paper Award** at TRUST 2008, Villach, Austria
- *"Active behavioral fingerprinting of wireless devices"*, with Cory Cornelius, David Kotz, and Daniel Peebles, 1st ACM Conference on Wireless Network Security (WiSec '08), Alexandria, VA, March 2008
- *"Active 802.11 Fingerprinting: Gibberish and "Secret Handshakes" to Know Your AP"*, with C.Cornelius and D.Peebles, Shmoocon 4, February 2008
- *"Attacking and Defending Networked Embedded Devices"*, with J.Baek, S. Sinclair and S.Smith, 2nd Workshop on Embedded Systems Security, Salzburg, Austria, October 2007
- *"Dumbots: Unexpected Botnets through Networked Embedded Devices"*, with J.Baek, S.Sinclair and S.Smith, Dartmouth technical report TR2007-591, May 2007,
- *"Hacker Curriculum: How Hackers Learn Networking"*, IEEE Distributed Systems Online, vol. 8, no. 10, 2007
- *"What Hackers Learn that the Rest of Us Don't: Notes on Hacker Curriculum"*, IEEE Security and Privacy, vol. 5, no. 4, pp. 72–75, July/August 2007
- *"Entropy-based data organization tricks for browsing logs and packet captures"*, Defcon 15, August 2007
- *"Simple entropy-based heuristics for log and traffic analysis"*, Shmoocon 3, March 2007
- *"Pastures: Towards Usable Security Policy Engineering"*, with A.Ferguson, D. McIlroy and S. Smith, 1st Workshop on Secure Software Engineering (SecSE), part of the ARES conference, April, 2007
- *"Semi-supervised Data Organization for Interactive Anomaly Analysis"*, with J.Aslam and V.Pavlu (Northeastern University), International Conference on Machine Learning and Applications (ICMLA) , December, 2006
- *"The Kerf Toolkit for Intrusion Analysis"*, with J. Aslam, D. Kotz, D. Rus, R. Peterson, B. Tofel (Dartmouth College), IEEE Security and Privacy, 2(6):42-52, November/December, 2004.
- *"The Kerf Toolkit for Intrusion Analysis"*, with J. Aslam, D. Kotz, D. Rus, R. Peterson (Dartmouth College), IAnewsletter, 8(2):12-16, Summer, 2005.
- *"Ubiquitous Redirection as Access Control Response"*, with G. Bakos, Privacy, Security and Trust Conference, 2005
- *"Kerf: Machine Learning To Aid Intrusion Analysis"*, Work-in-progress report at USENIX Security Conference 2004

◇ **Information Extraction, Natural Language Processing**

BBN Technologies, Speech and Language Dept., 1999–2001

- Worked on statistical Text Understanding systems, in particular on name and fact extraction from natural English text.
- Designed and/or implemented:
  - Statistical and rule-based algorithms for NLP tasks such as parsing, name and descriptor finding and classification, coreference, pronoun resolution, summarization of natural English text.
  - XML-based architecture for processing and storing natural language documents.
  - XML and HTML-based visualization tools for annotated and processed documents and training data.
  - Web front-ends and relational database back-ends for the above.

Publications:

- *"Experiments in Multi-Modal Content Extraction"*, with L. Ramshaw, E. Boschee, S. Miller, R. Stone, R. Weischedel, A. Zamanian (BBN Technologies), Human Language Technology (HLT) Conference 2001,
- *"FactBrowser Demonstration"*, with S. Miller, L. Ramshaw, R. Weischedel, A. Zamanian (BBN Technologies), HLT 2001,

◇ **Computer Algebra and Symbolic Computation**

Developed new efficient algorithms for recognition of and computation in finite groups of various types.

Software projects:

- GAP share package for two new black box recognition algorithms (GAP/Unix,Win32)
- Package for search and computation in finite permutation groups (LISP)
- Custom package for computation with polynomials in commuting and anti-commuting variables (LISP)

Publications:

- *"Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's Conjecture"*, with I. Pak, Journal of Symbolic Computation, vol. 29, 2000
- *"On sampling generating sets of finite groups and product replacement algorithm"*, with I. Pak, ISSAC-99 Conference Proceedings
- *"Constructive recognition of black box groups isomorphic to central extensions of $PSL(n, q)$"*, with G. Cooperman, L. Finkelstein, S. Linton, preprint
- *"Recognition of finite black box groups (Algorithms for constructive recognition of finite black box groups isomorphic to symmetric and special linear groups)"* Ph.D. thesis, Northeastern University, 1999

Teaching

◇ **Instructor**, Dartmouth College (2005–2012)

- Secure Information Systems Mentoring and Training (SISMAT)
  Developed and taught computer security hands-on "immersion" classes to students and interns of the SISMAT program (`http://www.cs.dartmouth.edu/~sismat/`).
- Advanced Operating Systems (CS108)
  Used OpenSolaris kernel code and DTrace to demonstrate and explore aspects of modern OS design.
- Computer Security (CS38) course and labs.
  Designed and implemented a virtual host and network environment for the students to practice network reconnaissance and attacks, shellcode development, live analysis of compromised hosts (described in *"Hacker Curriculum: How we can use it in teaching"*, IEEE Distributed Systems Online, vol. 8, no. 11, 2007

◇ **Instructor**, College of Computer Science, Northeastern University (1997–1999)

- Classes in C++/STL, Software Design, Data Structures.
- Wrote and ported courseware to Win32 (Visual C++ 5,6 and Cygwin)
- Teaching Assistant/Instructor, Dept. of Mathematics, Northeastern University
- Calculus and Discrete Mathematics Courses

Other Professional Activities

Expert witness for the defence in UMG Recordings, et al. v. Mavis Roy.

Education

◇ **Northeastern University**, Boston (1993–1999)

Ph.D. in Mathematics, M.S. in Computer Science, 1999

◇ **Moscow Institute of Physics and Technology** (aka MIPT, "Phystech") (1988–1993)

References

Available upon request.