

Daniel Bilar

University Of New Orleans
2000 Lakeshore Drive
Department of Computer Science
Math 311, Lakefront Campus
New Orleans, LA 70148
Office: (504) 280 7191
dbilar at uno dot edu

CAREER OBJECTIVES I am an able synthesizer, unconventional and highly innovative in my approaches. I am willing to apply my expertise and eclectic talents to interesting problems and challenges pertaining to strategic assessment, national security, operations research, network security, threat modeling and policy analysis.

EDUCATION **Dartmouth College (Thayer School of Engineering)**, Hanover NH
Ph.D. in Engineering Sciences, August 1997 – June 2003
Thesis: *Quantitative Risk Analysis of Computer Networks*
My PhD thesis addressed the technical risk opacity of software running on computer networks. This approach focused on the risk induced by vulnerabilities present in non-malicious software. It allowed risk managers to get a detailed and comprehensive snapshot of the constitutive software on the network, assess its risk with assistance of a vulnerability database via multi-factor risk metrics, and manage that risk by rank ordering reduction measures; subject to cost, functionality and risk tolerance constraints. I received the Dean William P Kimball fellowship in 1997. Dartmouth filed a provisional patent for my PhD work in 2003.

Cornell University (School of Engineering), Ithaca NY
M. Eng. in Operations Research and Industrial Engineering, August 1996 – July 1997
Coursework in manufacturing analysis, linear optimization, stochastic processes, with an emphasis on simulation modeling and system analysis. My team and I designed and implemented a discrete-event simulation of customer bank traffic to optimally geographically place ATM machines.

Brown University, Providence RI
B.A in Computer Science, August 1992 – June 1995
CS and broad liberal arts curriculum. I completed my degree in three years and started working the day after graduation.

Kantonsschule Zug, Zug (Switzerland)
Matura Type E (business and law), September 1986 – July 1992
Swiss Maturité with honors in highly selective Swiss public high school. I was class valedictorian.

RESEARCH AREAS AND INTERESTS **Information-gain adversarial malware**
The question is how to detect and classify highly evolved malware.
I research structural and dynamic approaches as alternatives to strict byte sequence pattern matching. The structural classifiers I analyzed included opcode distribution, Win32 system call sequences and structural callgraph properties. In light of recent empirical and theoretical findings, I propose moving beyond techniques premised on Turing Machine models towards iterative games and black-box process modeling within an interactive computational framework. My suggested dynamic approach uses techniques from Interactive Computations, Bayesian statistics, iterative 2-player (possibly n-player) imperfect non zero-sum games, and process query analysis.

Quantitative Risk Analysis of Networks
The question is how to assess, quantify and manage the risk profile of computer networks.

My PhD thesis focused on the inherent risk of vulnerabilities present in non-malicious software. I would like to refine certain aspects: First, hapless or malicious insiders - who account for a majority of attacks, losses and can leverage trust relationships - are not explicitly modeled. Secondly, it should be possible to semi-automatically map the network infrastructure to the business mission/process workflow which it supports (business-process-to-IT-asset mappings) and infer neuralgic points and concomitant loss functions. Thirdly, there is the fundamental of risk of untrusted hardware: How to assess the functionality risk of ASICs and FPGAs produced by a supply chain which cannot fully be trusted. I would like to tackle these questions with like-minded people.

PROFESSIONAL
EXPERIENCE

University of New Orleans, New Orleans LA
Assistant Professor of Computer Science, August 2008 –

Tenure-track faculty position. One of recent “forward-looking” hires drawn specifically to do world-class research on Infrastructure Assurance, draw highly qualified students and revamp IA curriculum.

Wellesley College, Wellesley MA
Norma Wilentz Hess Fellow, August 2006 – July 2008

Endowed Norma Wilentz Hess faculty fellow hired to explore new directions in Computer Science: Interdisciplinary research and learning, innovative course development and teaching methods. Developed and taught advanced courses in computer security, intermediate ones on computer networks, and one on the ‘Science of Networks’. Honed my expertise in malicious software analysis, and interpersonal skills by interacting with experts of all stripes (genius teenie hackers, gov’t officials, professionals, academics, corporate snake oil salesmen).

UCLA (Institute for Pure and Applied Mathematics), Los Angeles CA
Participant in GSS 2005, Summer 2005

Attended lecture series on *Intelligent Extraction of Information from Graphs and High Dimensional Data* at IPAM. Talks emphasized state-of-the-art techniques and connections to current challenges drawn from: data fusion, automated feature extraction, face and shape recognition, spectral and hyper-spectral image analysis, relational data mining, link analysis and discovery, graph mining, social and transactional networks, robust network design, and hidden state inference. Appreciated the domain transfer possibility of data mining, representation and analytical techniques to other fields.

Colby College, Waterville ME
Visiting Assistant Professor of Computer Science, September 2004 – August 2006

Developed and taught computer science undergraduate courses on object-oriented programming and data structures, network and computer security, algorithm design and analysis, as well as complex networks (models, properties, power laws). Supervised honors student thesis *Automated Classification of Malicious Code Variants*, which won 1st prize (poster competition) at the Consortium for Computing Sciences in Colleges (2005). Methodically applied pedagogical best practices to teaching computer science, reaped rave student reviews and gained a deep appreciation for case studies.

Purdue University, West Lafayette IN
Participant in NSA-sponsored faculty development program, Summer 2004

Aimed to provide computer science and technology faculty a strong foundation in information assurance in order to increase the number of IAS professionals graduating from our nation’s colleges and universities. Designed and developed some NSTISSI 4011, CNSSI 4012, and NSTISSI 4013 compliant course material and lectures, which serve as application prerequisites for joining NSA’s and DHS’s National Center of Academic Excellence in Information Assurance Education Program. Learned to artfully follow the letter of the law and to keep an eye on insider people, processes and implementations.

Oberlin College, Oberlin OH
Visiting Assistant Professor of Computer Science, August 2003 – June 2004

Developed and taught computer science undergraduate courses at all levels on object-oriented programming, data structures, network security, as well as general courses on information technology for non-specialist majors. Acquired techniques to effectively convey knowledge, which piqued my interest in pedagogical methodology.

Institute for Security Technology Studies at Dartmouth College, Hanover NH
Research Engineer, January 2000 – June 2000

ISTS is a leading national center for counter-terrorism technology research, development and education. Developed an online vulnerability scanner/database that can be used externally assess the vulnerabilities of remotely accessible hosts. I also designed a methodology/toolset to quantitatively identify, assess and manage software risk, which I developed into my PhD thesis.

Mettler-Toledo AG, Schwerzenbach (ZH), Switzerland
Software Engineer, March-July 1996, Summer 1997, Summer 1998

Mettler Toledo is a global manufacturer of precision instruments for use in laboratory, industrial and food retailing applications (Q1/2008 revenue: USD 435m). I was hired as a C++ developer in the thermal-analytical department. Designed, implemented, debugged and integrated class libraries in C++ and Motif to add scalable and seamlessly integrated viewing logarithmic capabilities to the existing modules without changing existing software dependencies. These modules consisted of 250,000 lines of virtually undocumented C code wrapped in C++ helper functions. In the summer of 1997, I added new features and debugged and streamlined old code. In the summer of 1998, I developed the printing routines and interpolation rendering in the viewing modules. Lessons learned included keeping work/code logs, and an appreciation of real world issues of integrating features into legacy code and processes.

Kantonsschule Zug, Zug, Switzerland
High School Teacher, August 1995 – February 1996

Developed curriculum and taught constitutional/business law, macro-economics, finance and computer science to 9th – 12th students at my former high school. Led and supervised twenty-two 10th graders on a one week art and culture excursion to Rome (Italy). Honed my organizational and group leadership abilities by deftly negotiating youngsters out of trouble (illicit substances, destruction of hotel property).

Citibank Card Services, Frankfurt a. M., Germany
Freelance Software Engineer, Summer 1995

Largest German issuer of credit cards. Designed and implemented a graphical Visual Basic module to present and statistically analyze client data. I was told that my work was also well received in New York. Learned that often, presentation is neglected and as important as content and to listen to users first, second and third.

Private Bank Julius Bär, Zurich, Switzerland
Intern/Assistant Financial Analyst, Summer 1994

Julius Bär is the leading dedicated wealth manager in Switzerland (FY 2008: USD 280b in managed assets). Hired as intern, then given duties as Assistant Financial Analyst at Head Office. I dealt with stock and financial markets recommendations. Researched and wrote a comparative analysis of Swiss Real Estate funds for the bank's investment advisors. Highlighted for me the pitfalls of blindly relying on publicly available financial data in an environment that does not follow US GAAP.

Manor AG, Zug, Switzerland
Sales Assistant, January 1991 – July 1992

EDP and consumer electronics section at largest Swiss department store chain (FY 2008: USD 3b revenue). Hired as sales assistant, specializing in computer hardware and software. Part-time work, averaging 10-12 hours a week after school, with very good sales results (averaged two to three times per capita revenue of full time employees). Learned how to subtly manipulate people into buying things, but used my powers only for pushing quality products.

Zuger Nachrichten, Zug, Switzerland
Layouter, Summer 1992

The “Zuger Nachrichten” (now “Neue Zuger Presse”) is the largest local newspaper in the Kanton of Zug (2007: 20,000 copies). Hired as a layouter preparing text and photographs directly with the help of a computerized layout equipment and Quark Express. I fully substituted for an experienced older layouter. I gained a taste of working under strict deadlines and an aversion to bad design of user-oriented software.

SELECTED
REFEREED
PUBLICA-
TIONS

Endicott-Popovsky B. and **Bilar D.** and Taylor C. Practical gender-aware pedagogy for introductory CS classes. In preparation: *ACM Journal on Educational Resources in Computing* (ACM Press, NYC)

Bilar D. Known Knowns, Known Unknowns and Unknown Unknowns: Anti-virus issues, malicious software and Internet attacks for non-technical audiences. *Digital Evidence and Electronic Signature Law Review* Vol. 6 (Pario, London). October 2009

Bilar D. Sensitivity Analysis on Bio-op Errors in DNA Computing. *Proceedings of the 10th ACIS on Software Engineering, Artificial Intelligence, Networking, Parallel and Distributed Computing*. May 2009

Bilar D. and Filiol E. (Editors). On Self-Replicating Computer Programs. *Journal In Computer Virology* 5:1 (Springer, Paris). February 2009

Bilar D. Noisy Defenses: Subverting Malware’s OODA loop. *Proceedings of 2008 Cyber Security and Information Infrastructure Workshop* (ACM Press, NY). October 2008

Bilar D. Callgraph structure of executables. *AI Communications Special Issue on “Network Analysis in Natural Sciences and Engineering”* 20:4 (IOS, Amsterdam). December 2007

Bilar D. Opcodes as predictor for malware. *International Journal of Electronic Security and Digital Forensics* 1:2 (Geneva, Switzerland). December 2007

Bilar D. On callgraphs and generative mechanisms. *Journal In Computer Virology* 3:4 (Springer, Paris). November 2007

Bilar D. Fingerprinting malicious code through statistical opcode analysis. *Proceedings of the 3rd International Conference on Global E-Security*, (London, UK). April 2007

Cybenko G and Jiang G. and **Bilar D.** Machine Learning Applications in Grid Computing. *Proceedings of the 37th Allerton Conference on Communication, Control, and Computing*. September 1999

SELECTED
NON-
REFEREED
PUBLICA-
TIONS

Review of *Handbook of Logic and Technical Proof Techniques for Computer Science* by Steven Krantz. The Mathematical Association of America (Mathematical Science Digital Library). February 2006

Review of *Brute Force: Cracking the Data Encryption Standard* by Matt Curtin. The Mathematical Association of America (Mathematical Science Digital Library). May 2005

Tabula rasa: Auditing Robin Hood under BeOS. www.sans.org/giac (March 2001)

Introduction to State of the Art in Intrusion Detection Systems. In: *Proceedings SPIE International Symposium on Law Enforcement Technologies (Vol. 4232)*. December 2000

To See the World in a Grain of Sand. In: *IEEE Computing in Science and Engineering (Vol. 2, No. 2)*. March/April 2000

SELECTED
TALKS

HOT processes, power laws and callgraph structure. Sandia National Labs (Albuquerque, NM). TBD
 n^{th} Order Attacks. NATO CCD COE (Tallin, Estonia). June 2009

Subverting Malware’s OODA loop. Oak Ridge National Labs (Oak Ridge, TN). May 2008

Approaching Information-Gain Adversarial Malware. BBN Technologies (Cambridge, MA). November 2007

Flying below the radar: What modern malware tells us. Ruhr-Universität Bochum, Horst Görtz Institut für Sicherheit in der Informationstechnik (Bochum, Germany). October 2007

Back to the Future: From Dortmund to present and future malware challenges. *DAT '07 (Dortmund, Germany): 3rd Dortmunder Alumni Tag* (October 2007)

Looking ahead: Metamorphic, k-ary malware and modern models. *DIMVA '07 (Lucerne, CH): 4th GI International Conference on Detection of Intrusions and Malware and Vulnerability Assessment*. July 2007

Malware Analysis as Science: A Primer. *IPICS '07 (Wales, UK): Intensive Programme on Information and Communication Security*. July 2007

Fingerprinting malicious code through statistical opcode analysis. *ICGeS '07 (London, UK): University of East London*. April 2007

Statistical Structures: Tolerant Fingerprinting for Classification and Analysis. *BH '06 (Las Vegas, NV): Blackhat Briefings USA*. August 2006

Quantitative Risk Analysis of Computer Networks. MIT Lincoln Labs (Lexington, MA). October 2004

Quantitative Risk Analysis of Computer Networks. Alphatech (Washington, DC). February 2002

SELECTED SERVICE

Co-Chair, 6th *Workshop on Digital Forensics and Incident Analysis* (New Orleans, LA), 2010

Advisory Board, *Journal in Computer Virology* (Springer, Paris), 2008-

Technical Program Committee, 6th *Symposium on Research in Computer Security* (Malaga, Spain), 2008

Program Committee, 4th *International Conference on Global E-Security* (London, UK), 2008

External PhD examiner, *University of Glamorgan* (Wales, UK), 2008

Invited Editor, Special Edition of *Journal in Computer Virology* (Springer, Paris), 2008

Professional Advisory Board, *SANS GIAC Systems and Network Auditor*, 2002-2005

PERSONAL

Citizenship US

Languages Fluent in English, German, French and various Swiss dialects

Sports Cross-country skiing, rope jumping, fencing (ranked 8th in junior league in Switzerland in 1985)

Interests Politics (world), history (world), foreign affairs (US), constitutional law (US), current events (world), counter-terrorism techniques and strategies, environmental and quality-of-life issues, general-interest hard science (ecology, physics, computer science, mathematics) and soft sciences (sociology, psychology, anthropology), literature (classical)

Personality Outstanding presentation and communication skills. Upbeat, warm, affable, quick-witted and charming in all social settings. No pushover, though: *Le gant de velours cache une main de fer*.