

# Daniel Bilar

Wellesley College  
Department of Computer Science  
Wellesley, MA 02481  
(781) 283 3093  
dbilar@wellesley.edu

**EDUCATION**     **Dartmouth College (Thayer School of Engineering)**, Hanover NH  
Ph.D. in Engineering Sciences, 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. 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, 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, June 1995

CS and broad liberal arts curriculum. I completed my degree in three years.

**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. My 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

Wellesley College, Wellesley MA

**Norma Wilentz Hess Fellow**, August 2006 – July 2008

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’.

**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.

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 1<sup>st</sup> prize (poster competition) at the Consortium for Computing Sciences in Colleges (2005).

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.

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.

SELECTED  
REFEREED  
PUBLICATIONS

Tryfonas T. and **Bilar D.** Forensic aspects of modern malware. In preparation: *Digital Evidence Journal* (Bedfordshire, UK). September 2008

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)

Filiol E. and **Bilar D.** (Editors). On self-replicating programs. Submitted: Special Issue of the *Journal In Computer Virology* (Springer, Paris). April 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.** Misleading modern malware. Under revision: *Journal In Computer Virology* (Springer, Paris). October 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 3<sup>rd</sup> 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 37<sup>th</sup> 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

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

Minimizing Error in DNA Computing. Technical Report. Thayer School of Engineering (Dartmouth College). January 1998

SELECTED  
TALKS

Subverting Malware's OODA loop. Oak Ridge National Labs (Oak Ridge, TN). June 2008

HOT processes, power laws and callgraph structure. Sandia National Labs (Albuquerque, NM). 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

Looking ahead: Metamorphic, k-ary malware and modern models. *DIMVA '07 (Lucerne, CH): 4<sup>th</sup> 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

Technical Program Committee, 13<sup>th</sup> *European Symposium on Research in Computer Security* (Malaga, Spain), 2008

Program Committee, 4<sup>th</sup> *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

SELECTED  
NON-  
ACADEMICS

Software Engineer, *Mettler-Toledo AG* (Zurich, Switzerland), Summer 1996-1998

Freelance Software Engineer, *Citibank Card Services* (Frankfurt, Germany), Summer 1995

Assistant Financial Analyst, *Private Bank Julius Bär* (Zurich, Switzerland), Summer 1994

International Payments Clerk, *Union Bank of Switzerland* (Zug, Switzerland), Summer 1993

PERSONAL

US citizen