

**Chad A. Williams**  
**425 Claremont Drive, Downers Grove, IL, 60516**  
**Phone: 630-963-3902**  
**Cell: 630-881-4565**  
**cwilliam@cs.uic.edu**

## **CURRICULUM VITAE**

### **Education:**

Ph.D. Candidate, Computer Science, University of Illinois at Chicago, 2006-present  
Concentrations: Computational Transportation Science  
Dissertation: Transfer Learning of Individual Travel Patterns  
Advisors: Peter C. Nelson (computer science), Abolfazl (Kouros) Mohammadian (civil engineering)

M.S., Computer Science, DePaul University, 2006  
Thesis: Profile Injection Attack Detection for Securing Collaborative Recommender Systems  
Advisor: Bamshad Mobasher

B.S, Computer Science, Cornell University, 1998

### **Experience:**

Teaching Associate, 2006  
University of Illinois at Chicago  
Course: Introduction to Software Engineering

Research Assistant, 2004-2005  
DePaul University  
Secure Personalization Project

Manager, 2001-2004  
Accenture, Chicago, IL

Technical Architect, 2000-2001  
BlueMeteor, Chicago, IL

Consultant, 1998-2000  
Accenture, Chicago, IL

### **Research Interests:**

My primary research interest is in applying machine learning and data mining techniques to practical problems, particularly those with applications to personalization that preserve privacy and trust. My dissertation research focuses on combining individual preference with transportation network and spatial-temporal knowledge to learn individual travel behavior for traveler personalization. A major component of this work is developing algorithms and techniques for transfer learning of individual travel behavior across different geographies. The focus of this research is leveraging transferrable aspects of travel behavior and patterns to reduce learning time, while also creating a richer model of the individual traveler. A major component of this effort is to provide this insight without compromising user privacy. Earlier work focused on ways personalization techniques such as recommender systems could be made more secure to malicious bias and thus more trustworthy while still remaining open systems.

### **Thesis:**

**“Profile Injection Attack Detection for Securing Collaborative Recommender Systems”**

by Chad Williams.

Masters Thesis, Department of Computer Science, DePaul University, June 2006. Technical Report No. 06-014.

**Publications:**

**“An Automated GPS-Based Prompted Recall Survey With Learning Algorithms”**

by Joshua Auld, Chad A. Williams, Abolfazl Mohammadian, and Peter C. Nelson.

*Transportation Letters: The International Journal of Transportation Research*, vol. 1, no. 1, Jan. 2009, pp. 59-79.

**“Mining Sequential Association Rules for Traveler Context Prediction”**

by Chad A. Williams, Abolfazl Mohammadian, Peter C. Nelson, and Sean T. Doherty.

In *Proceedings of the First International Workshop on Computational Transportation Science*, (Held at The International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS 2008), Dublin, Ireland), July 2008.

**“Defending recommender systems: detection of profile injection attacks”**

by Chad Williams, Bamshad Mobasher, and Robin Burke.

*Service Oriented Computing and Applications*, vol. 1, no. 3, Nov. 2007, pp. 157-170.

**“Toward trustworthy recommender systems: An analysis of attack models and algorithm robustness”**

by Bamshad Mobasher, Robin Burke, Runa Bhaumik, and Chad Williams.

*ACM Transactions on Internet Technology*, vol. 7, no. 4, Oct. 2007, ACM.

**“Classification features for attack detection in collaborative recommender systems”**

by Robin Burke, Bamshad Mobasher, Chad Williams, and Runa Bhaumik.

In *KDD '06: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, (New York, NY, USA), 2006, pp. 542-547.

**“Analysis and Detection of Segment-Focused Attacks Against Collaborative Recommendation”**

by B. Mobasher, R. Burke, C. Williams, and R. Bhaumik.

In *Advances in Web Mining and Web Usage Analysis*, vol. 4198 of Lecture Notes in Artificial Intelligence, (O. R. Zaiane O. Nasraoui and P. S. Yu, eds.), 2006, pp. 96-118.

**“The Impact of Attack Profile Classification on the Robustness of Collaborative Recommendation”**

by Chad Williams, Runa Bhaumik, Robin Burke, and Bamshad Mobasher.

In *Proceedings of the 2006 WebKDD Workshop*, (Held at KDD 2006, Philadelphia), Aug. 2006.

**“Detection of Obfuscated Attacks in Collaborative Recommender Systems”**

by Chad Williams, Bamshad Mobasher, Robin Burke, Jeff Sandvig, and Runa Bhaumik.

In *Proceedings of the ECAI'06 Workshop on Recommender Systems*, (Held at the 17th European Conference on Artificial Intelligence (ECAI'06), Riva del Garda, Italy), Aug. 2006.

**“Securing Collaborative Filtering Against Malicious Attacks Through Anomaly Detection”**

by Runa Bhaumik, Chad Williams, Bamshad Mobasher, and Robin Burke.

In *Proceedings of the 4th Workshop on Intelligent Techniques for Web Personalization (ITWP'06)*, (Held at AAAI 2006, Boston, Massachusetts), July 2006.

**“Detecting Profile Injection Attacks in Collaborative Recommender Systems”**

by Robin Burke, Bamshad Mobasher, Chad Williams, and Runa Bhaumik.

In *Proceedings of the 8th IEEE Conference on E-Commerce Technology (CEC'06)*, (San Francisco, California), June 2006.

**“Evaluation of Profile Injection Attacks In Collaborative Recommender Systems”**

by Chad Williams, Runa Bhaumik, Jeff Sandvig, Bamshad Mobasher, and Robin Burke.

In *DePaul CTI Research Symposium / Midwest Software Engineering Conference (CTIRS/MSEC 2006)*, (Chicago, Illinois), Apr. 2006.

**“Segment-Based Injection Attacks against Collaborative Filtering Recommender Systems”**

by R. Burke, B. Mobasher, R. Bhaumik, and C. Williams.

In *Proceedings of the 2005 International Conference on Data Mining (ICDM'05)*, (Houston, Texas), Nov. 2005.

**“Collaborative Recommendation Vulnerability to Focused Bias Injection Attacks”**

by R. Burke, B. Mobasher, R. Bhaumik, and C. Williams.

In *Proceedings of the Workshop on Privacy and Security Aspects of Data Mining*, (Held at ICDM'05, Houston, Texas), Nov. 2005.

**“Effective Attack Models for Shilling Item-Based Collaborative Filtering Systems”**

by B. Mobasher, R. Burke, R. Bhaumik, and C. Williams.

In *Proceedings of the 2005 WebKDD Workshop*, (Held at KDD 2005, Chicago, Illinois), Aug. 2005.

**“Genetically Evolving Optimal Neural Networks”**

by Chad Williams.

In *Neural Networks and Expert Systems*, The Institute of Chartered Financial Analysts of India (ICFAI), Jan. 2007.

**Fellowships and Awards:**

- IGERT Fellowship, Fall 2006 – Summer 2009, \$30,000 / year
- Best Paper Award, The 8th IEEE Conference on E-Commerce Technology 2006
- Best Paper Award, DePaul CTI Research Symposium / Midwest Software Engineering Conference 2006

**References:**

Peter C. Nelson, Dean of Engineering, University of Illinois at Chicago

Abolfazl (Kouros) Mohammadian, University of Illinois at Chicago

Bamshad Mobasher, DePaul University

Robin Burke, DePaul University

**Academic Progress:**

Coursework Requirements - complete

Ph.D. Competency Exam – complete

Ph.D. Preliminary Examination – complete

Ph.D. Dissertation and Defense – anticipated fall 2009a