

James Cannady, Ph.D.

Graduate School of Computer and Information Sciences
Nova Southeastern University, Fort Lauderdale, FL 33314

Phone / Fax : (954)262-2085/3915

E-Mail: cannady@nova.edu

URL: <http://www.scis.nova.edu/~cannady>

Home Address

91 Mountain View Lane, Danielsville, GA 30633

Phone: (706) 335-4116

Education

Ph.D. (Computer Information Systems) 2000, Nova Southeastern University.

Thesis Title: *An Adaptive Neural Network Approach to Intrusion Detection and Response.*

Advisor: Professor Sumitra Mukherjee.

M.S. (Management Information Systems) 1995, Nova Southeastern University.

B.S. (Criminal Justice) 1987, Georgia State University, Atlanta.

Professional Experience

June 2000 to Present, Nova Southeastern University

Associate Professor, School of Computer and Information Sciences (July 2004 – Present)

Served as the GSCIS Center of Academic Excellence representative to NSA

Developed and taught courses at the doctoral and masters level in Artificial Intelligence and Expert Systems, Information Security, Legal and Ethical Aspects of Computing, and Client-Server Computing Systems.

Supervised doctoral students in their dissertation work as primary advisor. Served on doctoral dissertation committees for students in GSCIS.

IRB representative (Feb 2001 – Apr 2008).

Led effort to establish NSU as a National Center of Academic Excellence in Information Assurance.

Led proposal for new Doctorate in Information Assurance degree.
Primary research has focused on information security issues and artificial intelligence.

Assistant Professor, School of Computer and Information Sciences (June 2000– July 2004)

Developed and taught courses at the doctoral and masters level in Artificial Intelligence and Expert Systems, Information Security, Legal and Ethical Aspects of Computing, and Client-Server Computing Systems.

Supervised doctoral students in their dissertation work as primary advisor. Served on doctoral dissertation committees for students in GSCIS.

IRB representative.

Primary research has focused on information security issues and artificial intelligence.

June 2000 to July 2008, University of Georgia.

Faculty Fellow/Adjunct Research Scientist

Provide program guidance and serve as committee member for master's theses in Artificial Intelligence.

April 1999 to December 1999, James Madison University.

Adjunct Assistant Professor

Developed and taught courses at the master's level in Information Security.

November 1995 to July 2008, Georgia Institute of Technology.

Adjunct Senior Research Scientist (June 2000 – July 2008)

Research Scientist II (June 1999 - June 2000)

Research Scientist I (November 1995 – June 1999)

Conducted basic and applied research in information security and artificial intelligence.

Serve as Co-Director of Information Security Center

Supervised graduate students in projects and thesis research.

Served on the Georgia Tech Faculty Senate.

Research Interests

My research concerns the intersection between artificial intelligence and information security. In particular I am working to develop new adaptive intelligent systems that can be applied to protect computer systems and networks. These techniques include the use of advanced neural networks in the detection of network-based attacks. I have developed a modified reinforcement-learning algorithm that enhances the effectiveness of the neural networks. My work has also included the use of adaptive self-organizing software agents that are designed to actively protect the computer network from attack. I have been involved in a variety of security-related research projects, including public-key infrastructure interoperability, malicious code detection, and system vulnerability assessments.

Teaching Interests

Information Security, Artificial Intelligence, and Complex Adaptive Systems.

Professional Affiliations

Senior Member, Institute of Electrical and Electronics Engineers (IEEE)

Member, American Association for the Advancement of Science (AAAS)

Member, American Association for Artificial Intelligence (AAAI)

Member, Association for Computing Machinery (ACM)

Member, ACM SIGART -- ACM's special interest group on Artificial Intelligence

Member, IEEE Computer Society

Member, IEEE Systems, Man, and Cybernetics Society

Associate Editor, International Journal of Information Technology and Decision Making (IT&DM)

Referee, IEEE Transactions on Neural Networks

Research Grants/Contracts

- 2003-2005, Department of Defense (DoDT&E), Operational Test and Evaluation of Information Assurance, \$800,000
- 2001-2003, Department of Defense (ARL), Tactical Intrusion Detection, \$1.2 million
- 2000-2002, Statewide Backbone Network Analysis and Design, State of Georgia, \$1.25 million
- 1999-2000, Cybersecurity Initiative, In-Q-It/GTRI, \$900,000
- 1998-1999, Design of the Metropolitan Atlanta Wide-Area Network, DOJ, \$200,000
- 1997-1998, Design And Development Of Neural Network-Based Intrusion Detection System, Georgia Institute of Technology, \$105,000
- 1997-1998, Georgia Superior and State Court Automation Project, Georgia Courts Automation Commission, \$400,000
- 1997-1998, Georgia Juvenile Court Automation Program – Phase III, Georgia Courts Automation Commission, \$400,000
- 1996-1997, Georgia Juvenile Court Automation Program – Phase II, Georgia Courts Automation Commission, \$398,000
- 1996, Georgia Juvenile Court Automation Program – Phase I, Georgia Courts Automation Commission, \$65,000
- 1996, Network Rating Model, National Security Agency/Georgia Institute of Technology, \$50,000

Service

- 2009-present, Vice-Chair, Georgia Emergency Preparedness Foundation, Macon, GA
- 2006-present, Paramedic/First Responder, Athens-Clarke County Georgia
- 2005-2008, Donation Coordinator, Foodbank of Northeast Georgia, Athens, GA

Refereed Publications in Journals and Proceedings

Cannady, J. (1997, February). Security in Object-Oriented Databases. Database Management, 8, (2), 45-52.

Cannady, J. (1997, October). Security Models for Object-Oriented Database Management Systems. Journal of Data Security Management, 11, (10), 38-44.

Cannady, J., "Security Models for Object-Oriented Databases", in Handbook of Information Security Management. pp. 595-606, (Krause, M. Ed.), New York: CRC Press (1999).

Cannady, J. (1997, February). Software Development with Cryptography. Databased Advisor, 15, (2), 78-82.

Cannady, J., & Harrell, J.R. (1996). A Comparative Analysis of Current Intrusion Detection Technologies. Proceedings of Technology in Information Security Conference (TISC) '96, 212-218.

Cramer, M.L., Cannady, J., & Harrell, J. (1996). New Methods of Intrusion Detection using Control-Loop Measurement. Proceedings of Technology in Information Security Conference (TISC) '96, 229-245.

Cannady, J., Harrell, J., & Huggins, D. (1996). A Model of an Attack Database System. Proceedings of DOD Database Colloquium '96, 78-90.

Cannady, J. (1998). Neural Networks for Misuse Detection: Initial Results. Proceedings of the Recent Advances in Intrusion Detection '98 Conference, 31-47.

Cannady, J. (1998) Applying Neural Networks to Misuse Detection. Proceedings of the 21st National Information Systems Security Conference, 368-381.

Cannady, J. (2000, July). Applying CMAC-based On-line Learning to Intrusion Detection. Proceedings of the 2000 IEEE/INNS Joint International Conference on Neural Networks.

Cannady, J. (2000, October). Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks. Proceedings of the 23rd National Information Systems Security Conference.

Rhodes, B., Mahaffey, J., & Cannady, J. (2000, October). Multiple Self-Organizing Maps for Intrusion Detection. Proceedings of the 23rd National Information Systems Security Conference.

Garcia, R., & Cannady, J. (2001, April). Boundary Expansion of Expert Systems:

Incorporating Evolutionary Computation with Intrusion Detection Solutions. Proceedings of the 2001 IEEE SOUTHEASTCON Conference.

Bauer, D, Cannady, J., & Garcia, R (2001, April). Detecting Anomalous Behavior: Optimization Of Network Traffic Parameters Via An Evolution Strategy. Proceedings of the 2001 IEEE SOUTHEASTCON Conference.

Cannady, J. (2001, August). The Application of Fuzzy ARTMAP in the Detection of Computer Network Attacks. Proceedings of the 2001 International Conference on Artificial Neural Networks.

Cannady, J. (2002). Intrusion Detection – Capabilities and Considerations. Global Infosecurity 2000, World Markets Research Centre. London.

Cannady, J. & Little, M. (2003). Representing Battlefield Network Attacks with Conceptual Structures. In Proceedings of the 2003 Army Science Conference.

Cannady, J. (2003). Identifying Complex Multi-Stage Network Attacks With Dynamic Petri Nets. In Proceedings of the 2003 Army Science Conference.

Dass, M., Cannady, J., & Potter, D. (2003). LIDS: Learning Intrusion Detection System. In Proceedings of the 2003 Florida Artificial Intelligence Symposium.

Dass, M., Cannady, J., & Potter, D. (2003). A Genetic Algorithm-based Intrusion Subclassifier Filter. In Proceedings of the 2003 ACM Southeast Conference.

Lu, J., & Cannady, J. (2003). Application Of Fuzzy Logic Controllers For High Accuracy Laser Tracking With Autonomous Robot System. Proceedings of the 2003 International Conference on Control, Automation, and Systems.

Gonzalez, L., & Cannady, J. (2004). A Self-Adaptive Negative Selection Approach for Anomaly Detection. Proceedings of the 2004 Congress of Evolutionary Computation.

Fuhs, J., & Cannady, J. (2004). An Automated Approach in Reverse Engineering Java Applications Using Petri Nets. Proceedings of the 2004 IEEE SOUTHEASTCON Conference.

Palnitkar, R., & Cannady, J. (2004). A Review of Adaptive Neural Networks. Proceedings of the 2004 IEEE SOUTHEASTCON Conference.

Cannady, J. (2005). Self-Organizing Distributed Intrusion Detection in Mobile Ad Hoc Networks. Proceedings of the 2005 IEEE Workshop on Soft Computing as Transdisciplinary Science and Technology

Wang, Y., Cannady, J., & Rosenbluth, J. (2005). Foundations of Computer Forensics: A

Technology for the Fight Against Computer Crime. Computer Law and Security Report. Volume 21, Issue 2, pp 119-127.

Cannady, J. (2009). Distributed Detection of Attacks in Mobile Ad-hoc Networks Using Learning Vector Quantization. In Proceedings of the Network and System Security Conference (NSS 2009).

Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment using hidden markov models. In Proceedings of the ACM SIGITE Conference.

Rodriquez, R. & Cannady, J. (2009). Byzantine Generals' Problem Driven Dynamic Trust Replication Method for Cognitive Mobile Ad hoc Networks(MANETs). In Proceedings of the 8th WSEAS international conference on Data networks, communications, computers.

Cannady, J. (2010). Detection Of Distributed Attacks In Mobile Ad-Hoc Networks Using Self-Organizing Temporal Neural Networks. In Proceedings of the Second International Conference on Agents and Artificial Intelligence.

Cannady, J. (2010). Real-time Detection of Distributed Zero-day Attacks in Ad Hoc Networks. In Proceedings of the 5th International Conference on Information Warfare and Security.

Fuhs, J. & Cannady, J. (2010). A Model for Detecting Source Code Anomalies by Extending Petri Nets. . In Proceedings of the 5th International Conference on Information Warfare and Security.

Cannady, J. (2010). An adaptive self-organizing approach to detecting complex distributed attacks in ad hoc networks Proceedings of SPIE, Volume 7709A

Cerkez, P. & Cannady, J. (2010). Automated detection of semagram-laden images using adaptive neural networks. Proceedings of SPIE, Volume 7708.

Cannady, J. (2010). Dynamic Neural Networks in the Detection of Distributed Attacks in Mobile Ad-Hoc Networks. International Journal Of Network Security And Its Applications.