

Dr. James D. Cannady, Jr.
Assistant Professor
School of Computer and Information Sciences
Nova Southeastern University
Fort Lauderdale, FL 33314

EDUCATIONAL BACKGROUND

Ph.D. in Computer Information Systems, 2000, Nova Southeastern University

M.S. in Management Information Systems, 1995, Nova Southeastern University

B.S. in Criminal Justice, 1987, Georgia State University

EMPLOYMENT HISTORY

Assistant Professor, Nova Southeastern University, 2000 - present

Research Scientist II, Georgia Institute of Technology, 1995 – 2000

Associate Director for Applied Research, Georgia Tech Information Security Center, 1998 - pres

Senior Special Agent, U.S. Naval Investigative Service, 1987 – 1995

CURRENT FIELDS OF INTEREST

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 software agents that are designed to actively protect the computer network from attack. Through my involvement with the Georgia Tech Information Security Center I have been involved in a variety of security-related research projects, including public-key infrastructure interoperability, malicious code detection, and system vulnerability assessments.

I. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

An Adaptive Neural Network Approach to Intrusion Detection and Response. Ph.D Thesis, 2000, Dr. Sumitra Mukherjee (Advisor), Nova Southeastern University.

A New Approach to Security in Object-Oriented Database Systems, M.S. Thesis, September, 1995, Dr. Rollins Guild (Advisor), Nova Southeastern University.

B. Published Journal Papers (refereed)

- 1) Cannady, J. (1997, February). Security in Object-Oriented Databases. Database Management, 8, (2), 45-52.
- 2) Cannady, J. (1997, October). Security Models for Object-Oriented Database Management Systems. Journal of Data Security Management, 11, (10), 38-44.

C. Published Books and Parts of Books

- 1) 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).

D. Published Papers (non-refereed)

- 1) Cannady, J. (1996, December). Security and SQL Programming. Databased Advisor, 14, (12), 34-37.
- 2) Cannady, J. (1997, February). Software Development with Cryptography. Databased Advisor, 15, (2), 78-82.

E. Technical Papers

- 1) Cannady, J., & Sills, L. (1996). Survey of State of Georgia Juvenile Court Automation Program - Phase I, (Final Technical Report, Project A-5230, Georgia Courts Automation Commission). Atlanta, GA: Georgia Institute of Technology, Georgia Tech Research Institute.
- 2) Cannady, J., & Sills, L. (1997, June). Survey of State of Georgia Juvenile Court Automation Program - Phase II, (Final Technical Report, Project A-5230, Georgia Courts Automation Commission). Atlanta, GA: Georgia Institute of Technology, Georgia Tech Research Institute.
- 3) Cannady, J. (1997, December). Greater Atlanta Data Center Wide Area Network MIS Plan, (Project B-0875, Burruss Institute of Public Service). Atlanta, GA: Georgia Institute of Technology, Georgia Tech Research Institute.
- 4) Cannady, J., & Bell, E. (1998, June) Survey of State of Georgia Juvenile Court Automation Program - Phase III, (Final Technical Report, Project A-5230, Georgia Courts Automation Commission). Atlanta, GA: Georgia Institute of Technology, Georgia Tech Research Institute.
- 5) Cannady, J. (1998, August). A Neural Network-Based Approach to Intrusion Detection - GTRI Internal Research and Development Project Final Report, (Final Technical Report, Project E-8604-302, GTRI Fellow Council). Atlanta, GA: Georgia Institute of Technology, Georgia Tech Research Institute.

F. Conference Presentations

F1. Conference Presentations with Proceedings (refereed)

- 1) 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.
- 2) 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.
- 3) Cannady, J., Harrell, J., & Huggins, D. (1996). A Model of an Attack Database System. Proceedings of DOD Database Colloquium '96, 78-90.

- 4) Cannady, J. (1998). Neural Networks for Misuse Detection: Initial Results. Proceedings of the Recent Advances in Intrusion Detection '98 Conference, 31-47.
- 5) Cannady, J. (1998) Applying Neural Networks to Misuse Detection. Proceedings of the 21st National Information Systems Security Conference, 368-381.
- 6) Cannady, J. Applying CMAC-based On-line Learning to Intrusion Detection. Proceedings of the 2000 IEEE/INNS Joint International Conference on Neural Networks.
- 7) Cannady, J. Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks. Proceedings of the 23rd National Information Systems Security Conference.
- 8) Rhodes, B., Mahaffey, J., & Cannady, J. Multiple Self-Organizing Maps for Intrusion Detection. Proceedings of the 23rd National Information Systems Security Conference.

F2. Conference Tutorials

- 1) Cannady, J. Foundations of Information Security. Tutorial presentation for ITEA '99, Atlanta, GA, September, 1999.

G. Research Proposals and Grants

H1. Awarded (PI)

Title: Georgia Juvenile Court Automation Program – Phase I
Sponsor: Georgia Courts Automation Commission
Funding Level: \$65,000
Period of Performance: June, 1996-December, 1996

Title: Georgia Juvenile Court Automation Program – Phase II
Sponsor: Georgia Courts Automation Commission
Funding Level: \$225,000
Period of Performance: December, 1996-June, 1997

Title: Georgia Juvenile Court Automation Program – Phase III
Sponsor: Georgia Courts Automation Commission
Funding Level: \$398,000
Period of Performance: July, 1997 – June, 1998

Title: Design of the Metropolitan Atlanta Wide-Area Law Enforcement Network
Sponsor: Burruss Institute of Public Service
Funding Level: \$20,000
Period of Performance: October, 1997 – May, 1998

Title: Design and Development of Neural Network-based Intrusion Detection System
Sponsor: GTRI Fellows Council
Funding Level: \$105,000
Period of Performance: October, 1997 - June, 1998

Title: Intelligent System Approach to Data Mining
Sponsor: GTRI Fellows Council
Funding Level: \$100,000
Period of Performance: October, 1997 - June, 1998

Title: Inclusion of Security in Linux Operating System
Sponsor: National Security Agency
Funding Level: \$47,500
Period of Performance: March, 1999 - November, 1999

Title: Interoperable Large-Scale Public Key Infrastructures
Sponsor: State of Georgia (Department of Administrative Services)
Funding Level: \$250,000
Period of Performance: July, 1999 – June, 2000

Title: Development of an Advanced Neural Network in a High-Performance Computing Environment
Sponsor: Army Research Laboratory
Funding Level: \$400,000
Period of Performance: May, 1999 - June, 2000

Title: An Intelligent System Approach to Data Mining
Sponsor: GTRI Fellows Council
Funding Level: \$106,000
Period of Performance: September, 1999 - June, 2000

H2. Awarded (Contributor)

Title: Superior and State Court Automation Project
Sponsor: Georgia Courts Automation Council
Amount Funded: \$400,000
Period of Performance: Jul 1997 – Jun 1998
Contributions: Proposal co-author, information security architecture.

Title: Georgia Tech Online Accounting System (OLAF)
Sponsor: Georgia Institute of Technology
Amount Funded: \$100,000
Period of Performance: Jul 1997 – Jun 1998
Contributions: Proposal co-author.

H. Curriculum Development

I am developing a course in Information Assurance that will be presented in the graduate program in the College of Computing at the Georgia Institute of Technology in Fall 2000. This course is one of several in a series of which I am contributing that will lead to a complete graduate-level curriculum in Information Security. The final program will provide students in the College of Computing with the opportunity to receive a Masters degree in Computer Science with a specialization in Information Security.

I. Media Coverage

J1. Information Security Research

- December 1999. Information Security Magazine. “Security in the 21st Century”.
- Fall 1999. Research Horizons. Featured intrusion detection research.
- July 12, 1999. CNN. “Researchers Tackle Cyber Security”.
- July 7, 1999. Associated Press International (national distribution). “Hackers Beware”
- May 1999. Signal Magazine. “Scientists Advance Security”.
- November 1998. CNN Future Watch. Segment on information warfare.
- November, 1997. New Scientist Magazine. “Tracking Computer Crime”.

II. SERVICE

A. Membership in Professional Societies

- 1) Member, American Association for the Advancement of Science, 1992 – present
- 2) Member, Association for Computing Machinery, 1994- present
- 3) Member, IEEE Computer Society, 1997 – present
- 4) Member, Armed Forces Communications and Electronics Association, 1996 – present

B. On-Campus Committees

- 1) Member, Georgia Institute of Technology General Faculty Assembly, 1999-present.
- 2) Member, Georgia Institute of Technology Security and Welfare Committee, 1999-present.
- 3) Member, Georgia Institute of Technology Campus Working Group on Secure Network Infrastructures, 1997-present

C. Consulting

- 1) Tridata Corporation. Analysis of Computer Crime in the Southeastern United States. August 18-25, 1999.

D. Civic Activities

- 1) Volunteer, State Botanical Garden of Georgia, 1996-present

E. Special Activities

- 1) Senior Judge, Georgia Science and Engineering Fair, 1995-present
- 2) Judge, Georgia Junior Science and Humanities Symposium, 1997- present