

James J. Yuill, Ph.D.

Durham, NC

919-271-6883; jimyuill<AT>pobox<DOT>com

March 2008

Summary: Seeking a senior-level computer-security position, in R&D. Experience includes computer systems R&D for over 18 years, with 8 years in computer-security research, 7 years in operating-systems development, and several years of university teaching. Ph.D. in computer security.

Computer Security Research

1998 – present: Primary researcher for university and Department of Defense (DoD) research projects, as summarized below. Also, a list of my publications and presentations is attached.

12/00 – present: Research in deception for computer security:

- Initiated project, and served as principal investigator (PI) and co-PI; formed research team with three distinguished university and CIA researchers; we obtained funding from the Office of the Secretary of Defense (OSD) and the DoD's Joint Task Force for Global Network Operations (JTF-GNO).
- Several papers and a book are published or pending publication; gave presentations at IEEE, ACM, and DoD conferences, and to senior officials at OSD and the JTF-GNO; the publications have been well-received in the DoD and used in a NATO computer-security course.
- Invented two deception-based computer-security devices; built a prototype, simulation and performance model.

11/07 – present: Survey and analysis of computer-security software development methods; funded by NCSU IT department.

12/06: Completed Ph.D. in computer science, at North Carolina State University (NCSU)

- My Ph.D. thesis is a subset of my deception research. My co-advisors were Drs. Mladen Vouk and Annie Anton.

2/99 – 12/02: Research in incident-response investigation processes:

- Primary researcher for DARPA-funded project; applied DoD's battlefield-intelligence process to incident-response; made novel discoveries in data management for investigation, and developed a prototype system.
- Initiated collaboration with experts from the FBI, US Marine Corps, and industry; primary author of journal paper; gave presentations at conferences for academia (RAID, at Purdue University), industry (FIRST, in France), and black-hat hackers (Rubicon, in Detroit); also presented at OSD, a JTF-GNO committee of generals, and the DoD Computer Forensics Lab (DCFL); the research received very favorable reviews from the DoD, academia, and law enforcement.

2/98 – 10/98: Research in network risk-assessment:

- Primary researcher on a project for the National Security Agency. Investigated the use of engineering reliability-theory for network risk-assessment. The research results were very well received by the sponsor.

8/98 – 2/99: Network penetration-testing:

- Initiated the project, obtained the client (an electronics corporation), and recruited a co-worker.
- We extensively penetrated the client's network and presented the results to senior management; we wrote a buffer-overflow exploit for IMAP.

INDUSTRY EXPERIENCE

12/84 - 4/93: IBM; Poughkeepsie, NY; operating system development; designed and coded new versions of IBM's MVS operating system.

- *MVS:* IBM's principal mainframe operating system. Developed programs which embody: parallelism, security, error recovery, reentrancy, performance constraints, downward compatibility, high-level and assembly-level languages, documentation in IBM manuals.
- *Design and code:* Evaluated and approved interdivision requests for Job Control Language (JCL) enhancements. Developed JCL-related enhancements. Each enhancement was up to 5,000 LOC (lines of code), and was incorporated within a system consisting of millions of LOC.
- *Development process:* Used IBM's formally-defined software development process. Wrote specifications, designs and code. Performed unit test. Provided technical oversight for maintenance programmers, testers and technical writers. Reviewed other programmers' work.
- *Programming methods:* Through self-study initiative, championed a department project introducing JSP, a software engineering design method. Researched programming methods, CASE and technology transfer. Hired software engineering consultants. Also, introduced quality assurance methods to my department.
- *Administration:* Implemented department-wide compliance with legally-imposed documentation requirements. Helped implement ISO 9000.
- *Awards:* Two \$1,500 awards, two \$100 awards.

TEACHING

1995-2005: instructor at North Carolina State University (NCSU), part-time:

Courses taught:

- Computer Networking, for MBA students: designed curriculum and networking lab; 5 semesters.
- Assembly Language: 4 semesters; Advanced Data Structures: 1 semester; Databases: 1 semester.
- Independent Research: recruited and supervised students for projects related to my research; 6 semesters.

Guest lectures:

- Network Security (M.S. level); lectured and developed a class project; 5 semesters.
- Cluster Computing (Ph.D. level); lectured and developed a class project; 2 semesters.
- Software Engineering (B.S. and M.S. level): 3 semesters.

Other:

- Graduate teaching-assistant: 4 semesters.
- Interviewed on local TV news, regarding a high-profile computer-security attack; March 2000.

1998-present: volunteer instructor at an inner-city children's home:

- Vocational-education instructor at Agape Corner Boarding School (ACBS), an inner-city children's home; part-time volunteer; started the home's vocational-education program; recruited other volunteer teachers; we built and equipped several workshops.

EDUCATION

Ph.D. Computer Science: NCSU; 2006; thesis on computer security, entitled "Defensive Computer-Security Deception Operations: Processes, Principles and Techniques"; passed written Ph.D. qualifying exam; 18 graduate classes completed; GPA 3.7.

Masters of Computer Science: NCSU; 1996; GPA 3.8

B.S. Computer Science: North Dakota State University; 1984; GPA: overall 3.4, major 3.7

PUBLICATIONS and PRESENTATIONS

Some of these publications are on-line, and they can be accessed through the links underlined in black, below. The other publications are available on request.

Journal papers

- Yuill, J., D. Denning, F. Feer. “Using Deception to Hide Things from Hackers : Processes, Principles, and Techniques”, *Journal of Information Warfare*, 5(3):26-40, November, 2006.
- Yuill, J., F. Wu, J. Settle, F. Gong, R. Forno, M. Huang and J. Asbery. “Intrusion-Detection for Incident-Response : using a military battlefield-intelligence process”, *Computer Networks*, Elsevier, 34(4): 671-697, October 2000.

Conference papers and tutorial

- Yuill, J., D. Denning, F. Feer. “Psychological Vulnerabilities to Deception, for Use in Computer Security”, *DoD Cyber Crime Conference 2007*, St. Louis, MO, January 2007.
- Yuill, J., F. Feer. “Designing Deception Operations for Computer Security: Processes, Principles, and Techniques”, tutorial presentation, *12th ACM Conference on Computer and Communications Security (CCS 2005)*, Alexandria, VA, November 2005.
- Yuill, J., F. Feer, D. Denning. “Designing Deception Operations for Computer Network Defense”, *DoD Cyber Crime Conference 2005*, Palm Harbor, FL, January 2005.
- Yuill, J., M. Zappe, D. Denning, and F. Feer. “Honeyfiles: Deceptive Files for Intrusion Detection”, *Proceedings of the 2004 IEEE Workshop on Information Assurance*, West Point, NY, June 2004.
- Yuill, J., S. Wu, F. Gong, M. Huang. “Intrusion Detection for an On-Going Attack”, *Proceedings of the 1999 International Symposium on Recent Advances in Intrusion Detection (RAID '99)*, Purdue, IN, September 1999.

Conference and workshop presentations

- Yuill, J., F. Feer. “Deception: Attacking Hackers’ Decision-Making Processes”, *Workshop on the Active Response Continuum to Computer Network Attacks*, George Mason University, Fairfax, VA, March 2005. (invited speaker)
- Yuill, J. “Applying Military-Intelligence Techniques to Incident-Response”, *Rubi-Con 2002* (hacker conference), Detroit, MI, April 2002.
- Yuill, J. “Understanding Hacker Behavior, Using Principles from Economics”, *Austrian Scholars Conference 2000* (an economics conference), Ludwig von Mises Institute, Auburn, AL, March 2000.
- Yuill, J. “Intrusion-Detection During Incident-Response, Using a Military Battlefield-Intelligence Process”, *13th Annual FIRST Conference on Computer Security Incident Handling*, Toulouse, France, June 2001.

Dissertation and DoD research report

- Yuill, J. “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”, Ph.D. Thesis, North Carolina State University, Raleigh, NC, USA, December 2006.
Thesis Committee: Mladen Vouk (co-chair, dept. head), Annie Anton (co-chair), Dorothy Denning (Naval Postgraduate School), Donald Bitzer (Distinguished University Research Professor)
- Yuill, J., F. Feer, D. Denning, B. Bell. “Deception for Computer Security Defense”, research project final-report for the Office of the Secretary of Defense, January 2004.

Publications near completion

- paper: Yuill, J., M. Vouk, D. Bitzer. “Using Deception to Stop Scanning within Protected Intranets”, largely an abridgement of my Ph.D. thesis
- book: Yuill, J., D. Denning, F. Feer. *Designing Deception Operations for Computer Security Defense*, a compilation of our deception papers and reports

DoD research-presentations

- 9/07: *Navy and FBI counter-intelligence analysts*, Washington, D.C.; presentation on designing deception operations for computer security
- 2004 – 2006: *Joint Task Force for Global Network Operations (JTF-GNO)*; presented to research director and team; numerous presentations on deception for computer security
- 2004: *Office of the Secretary of Defense*; presented to Andrew Marshall, Director, Office of Net Assessment; two presentations on our team’s deception research
- 2001 – 2003: *Office of the Secretary of Defense*; presented to Dr. Linton Wells, Principal Deputy Assistant Secretary of Defense; one presentation on our team’s deception research, and another on my incident response research
- 2001 – 2003: *DoD Computer Forensics Lab*; presented to senior management and team; two presentations on my incident response research
- 2000: *Joint Task Force for Computer Network Defense (JTF-CND)*; presented to a committee of generals; one presentation on my incident response research