

James J. Yuill, Ph.D.

4222 American Dr., Durham, NC 27705

919-271-6883; jimyuill@pobox.com

February 2010

Summary: Computer-science research, teaching, and product development for over 18 years, including: 8 years in computer-security research, 7 years in operating-systems development, and several years of university teaching. Ph.D. in computer security from North Carolina State University (NCSU), in 2006, where I'm currently a professor.

Computer Security Research

1998 – present: North Carolina State University (NCSU); primary researcher for NCSU and Department of Defense (DoD) research projects, as summarized below. (All of my DoD work is unclassified, i.e., public.)

12/00 – present: Designing deception-operations for computer security:

- Developed a manual for designing computer-security deception operations. It has been well received by, and used in, the DoD, and also in a NATO computer-security course.
- Published a journal paper, and gave presentations at major ACM and DoD conferences, and to senior officials at the Pentagon's Office of the Secretary of Defense (OSD) and the DoD's Joint Task Force for Global Network Operations (JTF-GNO), as well as Navy and FBI counter-intelligence groups.
- Initiated the project, and served as principal investigator (PI) and co-PI; I formed the research team with two well-known security authors (Dr. J. Bowyer Bell, and Dr. Dorothy Denning), and a retired CIA deception expert. We obtained \$120K in research funding from OSD and JTF-GNO.

12/00 – present: Deception-based intrusion detection systems (IDS's):

- Invented and designed a file-system based IDS, and hired a Linux kernel developer to build a prototype. Tested the prototype via a honeynet that we built. Presented a paper at an IEEE security conference.
- Invented and designed a network IDS. Tested it by developing a network simulation and mathematical performance models. It's a major part of my PhD thesis.

11/07 – present: Security-development practices and standards:

- Developed an extensive survey of the published security-development practices used in industry (e.g., Microsoft's SDL) and government. Developed guidelines for evaluating and choosing security-development practices. A lengthy report is written, which I presented at a conference and plan to publish.
- Wrote a paper on the extensive public criticism of Common Criteria (an international security standard). I presented the paper at a major DoD computer security conference.

2/99 – 6/03: Incident-response investigation processes:

- Primary researcher for this DoD-funded project which I conceived of; applied the DoD's battlefield-intelligence process to incident-response; also, made novel discoveries in data management for investigation, and developed a prototype data-management system. Published a journal paper.
- Formed collaborations with experts from the FBI, US Marine Corps, and industry, who were co-authors. Gave presentations at conferences for: academia (RAID, at Purdue University), industry (Forum for Incident Response and Security Teams (FIRST), in France), and black-hat hackers (Rubicon, in Detroit); also gave presentations at OSD, a DoD committee of generals, and the DoD Computer Forensics Lab.

8/98 – present: Penetration testing, and selected examples of low-level technical projects

- Initiated a penetration-testing project: obtained a corporate client and funding, and recruited a co-worker. We extensively penetrated the client's network, and we were flown out to present to senior management.
- To penetrate the network, we developed a buffer-overflow attack for an IMAP server.

- Obtained corporate donations of a network firewall and a vulnerability scanner. Scanned a college's network and worked with them to fix vulnerabilities. Installed and configured the firewall.
- Performed in-depth source-code analysis of the NMAP port scanner and of FreeBSD's SYN-flood defense.
- Rebuilt a corrupted hard drive's partition table, by hand, and recovered the lost partitions.
- Twice competed in the Honey Net Project's "Forensics Challenge". Solved the forensics problems and placed well.
- Assembly language systems-programming, for a mainframe conversion project

2/98 – 10/98: Risk-assessment:

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

Teaching

1995 - present: North Carolina State University; part and full-time teaching positions in the Computer Science Department and the Business Department's IT program; currently a full-time Visiting Assistant Professor in the Business Department; I've taught 19 courses and I'm currently teaching 3 courses.

2009 - present: Received a \$35K Faculty Award Grant from IBM to develop an on-line graduate course in Agile software engineering. I've developed this course in collaboration with one of IBM's corporate leaders for its software engineering capabilities.

- **Graduate courses taught (8):** networking (7), and Agile software engineering (1)
- **Undergraduate courses taught (14):** networking (2), assembly language (4), advanced data structures (1), systems analysis and design (3), databases (1), intro. to info. systems (2); intro. to programming (1)
- **Other graduate teaching:** developed and taught course modules for: computer security (5 courses), and distributed parallel programming (2 courses)

1998 – present: Teacher and mentor at an inner-city children's home; part-time volunteer and paid positions

- Agape Corner Boarding School; Durham, NC; a privately-funded Christian ministry
- Started the home's vocational-education program; recruited other volunteer teachers; we built and equipped several workshops; my wife and I lived on the campus for a year.

Industry Experience

12/84 - 4/93: IBM; Poughkeepsie, NY; operating system development; design and programming for 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.
- **Development:** Used IBM's well-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. Hired software engineering consultants. Also, introduced quality assurance methods to my department. Helped implement ISO 9000 compliance.
- **Awards:** Two \$1,500 awards, two \$100 awards.

Education

Ph.D. in Computer Science: North Carolina State University (NCSU); 2006

Thesis: “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”
18 graduate classes; GPA 3.7; passed a six-hour written qualifying exam

Master 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.

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., M. Vouk. “Choosing System Security-Engineering (SSE) Practices for Cloud Computing”, *3rd International Conference of the Virtual Computing Initiative (ICVCI 3)*, Research Triangle Park, NC, October 2009.
- Yuill, J., M. Vouk. “Common Criteria: A Survey of its Problems and Criticisms”, *DoD Cyber Crime Conference 2009*, St. Louis, MO, January 2009.
- 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 research reports

- 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.
- Yuill, J. “Choosing System Security-Engineering Practices : evaluation criteria and a selected survey”, NCSU Technical Report (polished draft), 2008.

References

Prof. Mladen Vouk – Department Head

Computer Science Department
North Carolina State University
relationship: my Ph.D. co-advisor

Prof. Dorothy Denning

Dept. of Defense Analysis
Naval Postgraduate School
relationship: member of my Ph.D. committee; advisor and collaborator for much of my research

William Alvin Wallace – Special Agent, US Air Force

Director, Plans, Programs & Policy
DoD Cyber Crime Center (DC3)
relationship: Alvin has been very supportive of my research, e.g., facilitated funding and presentations

Prof. David Baumer – Department Head

Department of Business Management
North Carolina State University
relationship: my current department head

Prof. Steven Allen – Associate Dean

Associate Dean for Grad. Programs and Research
Jenkins Graduate School of Management
North Carolina State University
relationship: my supervisor, when I teach in the MBA program