

Jim Yuill
Durham, NC
919-271-6883
jimyuill@pobox.com
August 2011

Dear prospective employer,

I'm seeking a computer-security R&D position that is compatible with my skills and experience. I have over 20 years of computer-systems R&D experience, including 9 years in computer-security research, 7 years in mainframe operating-systems development at IBM, and 5 years of university teaching. I have a PhD in computer security from North Carolina State University (2006), and I've been a professor there for the last three years.

My computer-security research is practical and applied, and most of it has been for the Department of Defense (DoD), where it has been very well received and used. I've conceived of and led almost all of these projects, recruited top people in the field to collaborate, obtained research funding, and reported directly to senior management (e.g., at the Office of the Secretary of Defense).

Computer-security R&D requires several different skill sets, in which I have strong experience and abilities, including: security engineering, systems and networking internals, systems design, large-scale systems development, and standardized-process development. From university teaching, I have skill in conveying complex technologies to technical and non-technical audiences.

I've spent nine years designing and analyzing computer-security systems, and also, standardized processes for security development, risk analysis, and incident-response. I've been fortunate to collaborate with and be trained by top people in the field, including the retired head of the FBI's computer-crime group, a retired CIA senior security-analyst, and Cisco's manager for global incident-response. As a designer, I'm creative, and I have the ability to see systems in my mind, create orderly and simplified structures, and balance requirements. I have strong abilities in vulnerability detection and "thinking like a hacker".

Having worked in operating-systems development at IBM, I'm experienced in developing systems that are secure, large-scale and mission-critical. Also, I have substantial experience with using and teaching software-engineering techniques, including Agile. I have a solid technical background in systems and networking internals, and I've worked with mainframes, Unix and Windows, as well as a variety of programming languages (e.g., assembler, C-like languages, shell scripting, SQL, Java, VB, etc.)

As my most recent manager will attest, I take a strong and sincere interest in my work, and I consistently do more than is required. As a researcher, I've had to learn new technologies and new fields quickly (e.g., economics and military operations), and I've had to regularly invent and develop new approaches and solutions. My attached resume further describes my skills and experience.

I'm seeking a computer-security R&D position where I'll have opportunity for doing good and useful work. If I can be of help, I'd be delighted to speak with you.

Sincerely,
Jim Yuill

James J. Yuill

Durham, NC

919-271-6883; jimyuill@pobox.com

August 2011

Summary: Seeking a computer-security R&D position. Over 20 years of experience, including 9 years in computer-security research, 7 years in operating-systems development at IBM, and 5 years of university teaching. Most recently a professor at North Carolina State University (NCSU). PhD in computer security from NCSU (2006).

Computer Security Research

1998 – June 2011: North Carolina State University. Lead researcher for university and Department of Defense (DoD) research projects, as summarized below. A list of my research publications is attached.

12/00 – 2006: Research in designing deception-based systems for computer security:

- Developed a manual for designing deception-operations for computer-security. It was well received in the DoD: used in designing a large DoD network-security system, used in a NATO computer-security course, and used by Air Force CERT.
- Invented and designed two deception-based computer-security devices; developed a prototype and a network simulation; also, designed and implemented a honeynet for system testing.
- Several papers are published and presented; Presentations include IEEE, ACM, and DoD conferences, and to senior officials at the Office of the Secretary of Defense (OSD) and at the DoD's Joint Task Force for Global Network Operations (JTF-GNO).
- I initiated these projects and was the lead researcher; formed the research team with three well-known university and CIA (ret.) researchers; we obtained funding from OSD (\$100K) and the JTF-GNO (\$20K).

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

- My Ph.D. thesis is a subset of my research in deception for computer security.

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

- Applied the DoD's battlefield-intelligence process to incident-response; made novel discoveries in data management for investigation, and developed a prototype system.
- The research received very favorable reviews from the DoD, academia, and law enforcement.
- Published a journal paper; gave presentations at conferences for academia (RAID, at Purdue University), industry (FIRST, in France), and black-hat hackers (Rubicon, in Detroit); DoD presentations to: OSD, a committee of generals (JTF-GNO), and the DoD Computer Forensics Lab (DCFL)
- I conceived of and lead this research project, and formed collaborations with experts from the FBI (ret.), US Marine Corps, and industry. Funding was from the DoD (DARPA).

11/07 – present: Research in creating standardized processes for computer-security, for use in: system-development, design, operations, and incident-response

- Developed principles and guidelines for creating standardized computer-security processes, and for evaluating and choosing such processes. Several papers are written. Presentations include a major DoD computer-security conference, the upcoming ACM computer-security conference, and an IBM/NCSU cloud-computing conference.
- I'm the lead researcher, and I'm currently collaborating with a Cisco incident-response manager, with whom I've co-authored a paper.
- Performed an extensive survey of the published computer-security processes, e.g., Microsoft's Security Development Lifecycle, NIST's IT security standards, the DoD's Common Criteria, etc.

8/10 – 1/11: Digital forensics consulting for a high-profile murder case

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

- Lead 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:

- I 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 an IMAP server.

Systems Development

12/84 - 4/93: IBM; Poughkeepsie, NY; operating-system development; designed and coded new versions of IBM's MVS operating system (now called z/OS):

- *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.

6/94 – 10/07: Various consulting projects: systems administration, analysis, and conversion.

Teaching

2008 - July 2011: North Carolina State University; teaching assistant-professor in the College of Management's IT program, full-time

- Received a \$35K grant from IBM to develop an on-line graduate course in Agile software engineering. I co-taught this course with one of IBM's corporate Agile leaders.

1995 - 2004: North Carolina State University; part-time instructor in Computer Science and the College of Management

Summary of courses taught (29):

- Graduate courses (8): Agile software engineering (1), networking (7)
- Undergraduate courses (21): databases (3), systems analysis and design (4), Agile project (1), networking (2), assembly language (4), advanced data structures (1), intro. to programming (2), intro. to IT (4)
- Independent-research courses: recruited and supervised 6 students, for projects related to my research

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

- Agape Corner Boarding School; Durham, NC; a privately-funded charity
- 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.

Education

Ph.D. Computer Science: NCSU; 2006; thesis on computer security, entitled “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”; Dorothy Denning (Distinguished Professor at Naval Postgraduate School) was a committee member and an advisor for much of my thesis; 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

Research Publications and Presentations

Some publications are on-line, and accessible via 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 tutorials

- Yuill, J., M. Nystrom. “Developing Standardized Processes for Incident Response: Challenges and Opportunities”, tutorial and research presentation, accepted for the upcoming *18th ACM Conference on Computer and Communications Security (CCS 2011)*, Chicago, IL, October 2011.
- 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 and research 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. Invited speaker for conference panel-discussion, “Cyber Intersection with Deception”. Upcoming *InfowarCon 2011: Maneuvering in Cyberspace and IO*, Linthicum Heights, MD, September 2011.
- 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. “Intrusion-Detection During Incident-Response, Using a Military Battlefield-Intelligence Process”, *13th Annual FIRST Conference on Computer Security Incident Handling*, Toulouse, France, June 2001.
- Yuill, J. “Understanding Hacker Behavior, Using Principles from Economics”, *Austrian Scholars Conference 2000* (an economics conference), Ludwig von Mises Institute, Auburn, AL, March 2000.

Dissertation and research reports

- Yuill, J. “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”, Ph.D. Thesis, North Carolina State University, 2006.
- 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.

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

References

David Baumer – Department Head

Department of Business Management
 North Carolina State University
 David_Baumer@ncsu.edu; (919) 515-6950
relationship: my recent department head

Mladen Vouk – Department Head

Computer Science Department
 North Carolina State University
 vouk@csc.ncsu.edu; (919) 515-2858
relationship: my Ph.D. co-advisor

Dorothy Denning – Distinguished Professor

Naval Postgraduate School
 (contact information available on request)
*relationship: research advisor and collaborator;
 member of my Ph.D. committee*

William Alvin Wallace

Director, Plans, Programs & Policy
 DoD Cyber Crime Center
 (contact information available on request)
*relationship: DoD computer-security director who
 has been very supportive of my research*