

James J. Yuill, Ph.D.

4222 American Dr., Durham, NC 27705

919-271-6883; jimyuill@pobox.com

February 2010

Education

Ph.D. in Computer Science, December 2006

North Carolina State University (NCSU)

Thesis: “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”

Course work: 18 computer-related graduate classes; GPA 3.7; passed a written Ph.D. 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

Experience

Summary: 18 years of computer-science experience including 8 years in computer-security research, 7 years in operating-systems development (at IBM), and several years of university teaching.

North Carolina State University

Computer Science Department, Department of Business Management

2008 – present Visiting Assistant Professor; Department of Business Management – IT concentration

1998 – present Primary researcher for several computer-security research projects; this includes: Ph.D. research from 1998 to 2006; post-doctoral research from 2007 to 2008

**1994 – 1997,
2001 – 2005** Instructor in Computer Science and Business Management departments, part-time

U.S. Department of Defense (DoD)

2003 – 2004 PI for two computer-security research projects; independent contractor

IBM Corporation

1985 – 1993 Operating systems development

Agape Corner Boarding School

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

Teaching

2008–present: Visiting Assistant Professor in NCSU’s Department of Business Management—IT Concentration; full-time; courses taught:

- MBA course (on-line): Software Development and Project Management—Using Agile and Lean; obtained \$35K grant from IBM to develop this course
- Undergraduate: Networking; Systems Analysis and Design; Intro. to Info. Systems; Intro. to Programming

1994–1997, 2001–2005: Instructor, in NCSU’s Computer Science and Business Departments; part-time:

- **Instructor—graduate courses (7 total):**
 - Computer Networking; in the MBA e-commerce program; seven sections, over five semesters
- **Instructor—undergraduate courses (6 total):**
 - Assembly Language; four semesters
 - Advanced Data Structures; one semester
 - Databases; one semester
- **Supervised teaching assistants for my courses (10 courses)**
- **Supervised independent-research courses (6 semesters):**
 - graduate and undergraduate; recruited and supervised students, for projects related to my research
- **Guest lectures in Computer Science Department (10 semesters):**
 - Network Security (M.S. level); lectured and developed a class project; five semesters
 - Parallel Computing (Ph.D. level); lectured and developed a class project; two semesters
 - Software Engineering (B.S. and M.S. level); three semesters
- **Graduate teaching-assistant (4 semesters)**

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.

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: security; parallelism, 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 instructors. Also, introduced quality assurance methods to my department. Helped implement ISO 9000 compliance.

Various dates: five computer-related summer-jobs, including: systems analysis, database development, mainframe system-administration, and system conversion (mainframe to PCs)

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, 2008.

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

Funding Obtained

- 2009: \$35K for developing an on-line software-engineering course, from IBM's Faculty Awards program; in collaboration with one of IBM's corporate leaders for its software engineering practices.
- 2004-2005: \$20K, for research on deception for computer security, from the DoD's Joint Task Force for Global Network Operations; I was a co-PI.
- 2002-2004: \$100K, for research on deception for computer security, from the Office of the Secretary of Defense; I was the PI.
- 1999: \$3K, for computer-security penetration testing, from an electronics corporation; I was the PI.

References

Prof. Mladen Vouk – Department Head

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

William Alvin Wallace – Special Agent, US Air Force

DoD Cyber Crime Center (DC3)
Linthicum, MD
relationship: Alvin is a director at DC3, and he has been very supportive of my research.

Prof. David Baumer – Department Head

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

Prof. Dorothy Denning

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

Prof. S. Felix Wu

Computer Science Department
University of California at Davis (UC Davis)
Davis, CA
relationship: my first Ph.D. advisor, before he left for UC Davis

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

Statement of Teaching Plan

Teaching Interests

The primary areas I can teach include computer security, networking, software engineering, programming, operating systems, systems architecture, databases, and core computer science courses. Also, I've taken 18 computer-related graduate classes, for which I earned a 3.7 GPA. This provides a strong background for teaching a wide variety of courses.

I find teaching very rewarding, and from experience, I believe I am skilled at it. My principal teaching goal is to best prepare students for their career objectives. Having experience in both academia and industry provides a background for teaching both theory and practice. I have experience teaching at the graduate and undergraduate level, and I have received very positive feedback from students, faculty and the department administration. Also, I take a sincere interest in, and have concern for, my students.

Experience, skills, and approach

I've taught 19 courses, including both graduate and undergraduate courses, and I'm currently teaching three courses. Five courses were in the Computer Science Department, and the others in the College of Management's IT program. I taught part-time while a graduate student, and I stayed as a visiting faculty member here at NCSU after finishing my PhD. The courses I've primarily taught are:

Software Engineering and Project Management, using Agile and Lean: I obtained a \$35K IBM Faculty Award grant to develop this online course, which I'm currently teaching. It is offered as an MBA class, but most students are from the College of Engineering. I developed this course in collaboration with one of IBM's corporate leaders for its software engineering capabilities. Agile and Lean are relatively new, so I've had to create much of the course material myself, which has been similar to textbook writing.

Computer networking: This graduate course was part of the MBA e-commerce program at NCSU. I taught seven sections of the course, over five semesters. I redesigned the course, and the new course was very well received by students and faculty. The course covered networking principles and protocols. On my own initiative, I set-up a computer lab for the course, equipped it with PCs, switches and routers, and I wrote a collection of lab assignments. There is an undergraduate version of the course, and the instructor for that course also used my lab and assignments.

Assembly language: I taught this undergraduate Computer-Science course four times. I wrote a tutorial for using the course's assembler and debugger. My main objective was to help students understand how computers work. The course included extensive programming projects. The projects enhanced the students' software development skills, and helped the students understand the internals of computers and high-level programming languages. I taught unit testing, to both manage assembly-language details, and to instill a career-long programming habit.

In addition to my university teaching experience, I've been a volunteer teacher at an inner-city children's home for the last eleven years. I started the home's vocational education program, and recruited other teachers. This experience has provided valuable teaching skills, and it has helped me better understand students' needs.

A principal goal in all my courses is to not only teach the material in the course syllabus, but to also best prepare students for their career objectives. This includes providing students with knowledge and skills that are of enduring use, e.g., foundational computer-science principles, foundational engineering principles, and software development skills. I also provide students with structure and accountability, to help them keep-up with, and complete, the course. This includes a regular schedule of lectures, homework assignments and tests. I earnestly work to provide just and fair grading, and to prevent cheating. I find that problem-solving is essential for learning. Problem solving compels students to apply what they are learning, and it provides deeper understanding and better retention. I try to make the students' work load challenging, though not excessive. My aim is to deliver courses that are rigorous and substantial, within the students' abilities. The feedback for my courses indicates I have been succeeding in this.

Based on my teaching experience and interest, it appears I have the gift of teaching—an ability to explain things in a way that is clear and organized, and that caters to students' learning styles and needs. Also, I have a strong interest in, and concern for, my students. This encourages the students, and it motivates me to serve them—to effectively provide useful knowledge and skills.

Statement of Research Plan

Research Interests

My primary research area is computer security. My research and industry experience also includes networking, operating systems, system architecture, software engineering, quality, the philosophy of science, military theory, and economics (Austrian).

The next section summarizes my recent and current research. A subsequent section describes my future research plans.

Research Projects

Two of my primary research projects are: 1) the use of deception for computer-security defense, and 2) the investigation process for computer-security incident response. Much of this research applies military theory and established military processes to computer security. This cross-discipline approach is a fruitful source of novel solutions, and also, it frames my research in a context that is appealing to military research sponsors.

Deception for computer-security: This research is concerned with the processes, principles and techniques that are involved in deception-operations for computer-security defense. *Computer security deception-operations* are defined as the planned actions taken to mislead hackers and thereby cause them to take (or not take) specific actions that aid computer-security defenses. Researchers have investigated hackers' use of deception to attack networks and the deceptive honeypot systems used to defend networks. However, relatively little had been done to systematically model and examine computer security deception-operations [Yui06]. There are two parts to my deception research: process models and experimental systems.

We developed extensive process models for deception operations [YFD04, YFD05, YDF06, YDF07]. They provide deception planners with a framework for designing and conducting deception operations. Much of this work is based on military deception theory and practice. The work also includes a novel model for deceptive hiding, which aids in developing new hiding techniques and in evaluating existing techniques [YDF06]. In developing these models, I collaborated with Dr. Dorothy Denning, a well-known computer-security researcher at the Naval Postgraduate School, and with Fred Feer, a retired CIA deception expert. I was the PI, and they were senior advisors.

Deception-based computer-security systems: In addition, I developed two novel deception-based computer-security systems. The deception process-models informed the design and evaluation of these intrusion detection systems. The Net-Chaff system employs computer-impersonations to detect and contain hackers' network scans within a protected intranet [Yui06]. The Net-Chaff architecture was simulated and modeled analytically. This performance analysis indicates that the Net-Chaff system can reliably detect and contain intranet scans before they access vulnerable computers. Also, Net-Chaff's use of deception makes it much simpler, and cheaper, than many similar types of systems. This makes Net-Chaff a promising solution for stopping worms from spreading within protected intranets. The other system is called Honeyfiles, and it extends the network file system to provide bait files for hackers [YZD04]. These files trigger an alarm when opened. A prototype Honeyfile system was implemented, and it involved modifying the Linux kernel to enhance NFS.

Incident-response investigation: This part of my research focuses on the process of investigation during computer-security incident response (IR). There are two parts to this research: IR investigation process-models, and IR data-management. The process-models provide a framework for understanding and conducting IR investigations. For a compromised network (i.e., hacked network), investigating the network for all compromised devices is a very difficult task. I developed codified principles and techniques to help solve this problem [YWS00]. This work is based largely on the U.S. military's battlefield-intelligence process. Models from the economics of crime were also used. Also, in this work I was privileged to be tutored by, and collaborate with, Jim Settle, who was the chief of the FBI's computer-crime group (retired).

In addition, I am developing a more general process-model for IR investigation. The general process of investigation is abstract and complex. This model explains the environment, nature and process of investigation, within the context of IR. The model is based largely on published research in jurisprudence. My research on this is largely completed. Portions of the model were used in our research on deceptive hiding [YDF06].

Incident-response data management: I am also developing a data-management system for IR investigation. Data-management for IR poses uncommon challenges--challenges not present in traditional data-management systems. During IR investigation, large amounts of data are collected, processed and analyzed. The data is often incomplete and uncertain, and the relationships among the data are also uncertain. Also, the variation among IR investigations makes it difficult to know, in advance, what data models must be supported. Often, data models must be constructed during the investigation. Further, most investigators have limited skill in data modeling. I have found that such requirements make relational databases ill-suited for IR data management.

The management of investigation-data serves two purposes: 1) efficient access to the data and 2) organization of the data in a manner that aids in the discovery of new hypotheses. The consideration of elements of evidence, in combination, is a useful means for discovering new hypotheses [Sch99]. I devised a prototype data-management system, and it meets all of these requirements. The system borrows from existing work in two similar fields: military intelligence and sociology research. I recruited a graduate student to spend a semester working with the prototype, using data we obtained from military-intelligence analysts. These experiments were very positive. Also, I made a number of presentations of the system within the Department of Defense (DoD), including the Office of Secretary of Defense. The presentations were very well received, but at the time, I had to set this project aside due to a change in research funding.

Research Plans

This section describes my plans for completing my on-going research projects, and also, my plans for pursuing funding.

Short-term projects: I have several well-developed research projects that can be completed in the short-term (e.g., one or two semesters). The only funding needed is for my own research time. The Net-Chaff device was described earlier. It is a deception-based intrusion detection system, and it is very promising for stopping worms from spreading within a protected intranet. This research is extensively documented in my Ph.D. thesis [Yui06]. A paper on net-chaff,

including analytical performance models, is almost complete, and it is largely an abridgement of my thesis. Another project that is near completion is a book on designing computer-security deception operations. The book is a compilation of our deception papers [YFD05, YDF06, YDF07], and DoD report [YFD04]. This is novel research. It has been well received within the DoD, and most of it has yet not been published outside of the DoD. Another well-developed project is my research on a general process for incident-response investigations. This research is adapted from jurisprudence. The research is largely completed, and the paper is partially written.

Longer-term projects: My most promising long-term project is the data-management system I developed for incident response. I plan to seek funding to further develop this system and experiment with it. Another promising long-term project is Net-Chaff. Thus far, I've designed its architecture and developed performance models. The device is very promising for stopping worms from spreading within a protected intranet. I'm hopeful that I can get funding to develop a prototype and to perform empirical performance tests. Also, I built a prototype of the Honeyfile system, and I'd like to develop an improved version of it, as an open-source system. All of these systems projects are well-suited for involving students, for their design projects or research, at graduate or undergraduate levels.

Another long-term project extends my prior work on deception process-models. The models we developed are for computer security defense. Deception process-models are also needed for computer security offense. For this research, I plan to model hackers' use of deception in computer-security attacks. The purpose of these models is to help with counter-deception for defending against such attacks. I'm not aware of any extensive research on hackers' use of deception, nor on counter-deception. These are fertile research areas, and the only funding required is for my time. This project is also well-suited for incorporating student research.

Funding: My research experience provides some unique advantages in seeking DoD research funding. Much of my research applies military theory and established military processes to computer security. This approach not only provides a fruitful source of ideas, but it also frames my research in a context that is appealing to DoD research sponsors. Further, my collaborations with DoD experts, and my industry experience, provide research skill-sets that are useful for military applications, and that are credible to DoD research sponsors. My published research has been well received within the DoD, and this provides further credibility. Overall, this funding plan has enabled me to get DoD funding twice, as a Ph.D. student.

Overall, my research plan is to generate research results in the short-term, while seeking funding for longer-term projects. I have several projects that are near completion, and that can be finished in one or two semesters. The longer-term projects are well-developed and are promising extensions of my prior research. In addition, they are well-suited for student design and research projects.

References

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

[Sch99] Schum, D. "Marshaling Thoughts and Evidence During Fact Investigation", *South Texas Law Review*, 40(2): 401-454, Summer 1999.

- [YDF06] 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.
- [YDF07] 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.
- [YFD04] 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.
- [YFD05] Yuill, J., F. Feer, D. Denning. “Designing Deception Operations for Computer Network Defense”, *DoD Cyber Crime Conference 2005*, Palm Harbor, FL, January 2005.
- [Yui06] Yuill, J. “Defensive Computer-Security Deception Operations: Processes, Principles and Techniques”, Ph.D. Thesis, North Carolina State University, Raleigh, NC, USA, December 2006.
- [YWS00] 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.
- [YZD04] 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.