



Engineering **ENTERPRISE**

THE ALUMNI MAGAZINE FOR ISyE AT GEORGIA INSTITUTE OF TECHNOLOGY

Fall 2003

**Enterprise Security and IT Security:
Asymmetric Warfare**

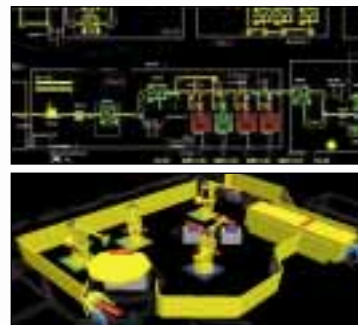
**Perspectives on Security:
An Interview with John Gilligan,
Chief Information Officer of the U.S. Air Force**

How ISyE is Addressing U.S. Security Challenges

SIMULATION SOFTWARE AND SERVICES

- ARENA
- AUTOMOD
- Enterprise Dynamics (Taylor II/ED)
- KanbanSIM/PDSim
- PROMODEL
- QUEST
- SIMUL8
- WITNESS

More than 3000 Simulation projects since 1979 in Manufacturing, Logistics, and Service Industries.



ADVANCED PLANNING & SCHEDULING SOFTWARE AND SERVICES

- Finite Capacity Planning and Scheduling for improved customer service, reduced inventory, and better utilization of resources
- High-speed creation of multi-product, multi-process production schedules
- Interface to other software (SAP, Baan, etc.) and shop-floor control systems
- Cost effective and web-enabled finite capacity scheduling solutions

More than 600 installations worldwide including Automotive, Chemical, Consumer Products, Food Processing, Manufacturing, Electronics, and Pharmaceutical Industries.

LEAN MANUFACTURING SOLUTIONS

- Value Stream Mapping
- Standardized Work
- Load Leveling
- Kaizen Events
- Visual Workplace
- Hands-on Shop-Floor Implementation
- Setup Time Reduction
- Build-in Quality
- Overall Equipment Effectiveness
- Process Simulation
- Total Production Measurements
- Lean Methods Training



TECHNICAL STAFFING SERVICES

Engineers on Demand! Productivity on Demand! Experience on Demand!

- Industrial and Simulation Engineers (Arena, AutoMod, IGRIP, Simul8, etc.)
- Mechanical and Manufacturing Engineers
- Supply Chain Analysts and Software Implementers
- Electrical and Computer Engineers
- Designers (ALIAS, AutoCAD, CATIA, Pro-E, SDRC, UG, etc.)
- IT Staffing (C/C++, Java, XML, SQL, Oracle, .NET, etc.)

Production Modeling Corporation
Three Parklane Blvd, Suite 1006 West
Dearborn, MI 48126

Phone: 313.441.4460 x 1131
Email: sales@pmcorp.com
Web: www.pmcorp.com



Security

by William B. Rouse

PUBLISHED BY

ISyE Georgia Institute of Technology
Lionheart Publishing Inc. John Llewellyn, President

EDITORIAL

Managing Editor Ruth Gregory
ISyE / Georgia Tech
Atlanta, GA 30332-0205
Tel: (404) 385-2627
Fax: (404) 894-2301
ruth.gregory@isye.gatech.edu

Contributing Editor Sarah Banick
sbanick@mindspring.com

ART DIRECTION & PRODUCTION

Art Director Alan Brubaker, ext. 218
albrubaker@lionhrtpub.com

Publication Designer Donna Mazal, ext. 226
donnam@lionhrtpub.com

SALES & MARKETING

Advertising Sales John Llewellyn, ext. 209
llewellyn@lionhrtpub.com

CIRCULATION

Circulation Manager Maria Bennett, ext. 219
bennett@lionhrtpub.com

ADVERTISING OFFICE

LIONHEART PUBLISHING INC.
506 Roswell Street, Ste. 220
Atlanta, GA 30060, USA
phone: +1 (770) 431-0867
fax: +1 (770) 432-6969
e-mail: llewellyn@lionhrtpub.com

Engineering Enterprise is published quarterly by Lionheart Publishing Inc. and ISyE, Georgia Institute of Technology. Editorial contributions including manuscripts, news items, and letters to the editor are welcome. Unless stated otherwise, articles and announcements reflect the opinions of the author or firm and do not necessarily reflect the opinions of *Engineering Enterprise*, Lionheart Publishing Inc., ISyE, its advertisers, or sponsors. Yearly subscriptions (four issues) are available for \$18 (U.S.), \$22 (Canada & Mexico). Payable in U.S. funds.

Copyright © 2003 by Lionheart Publishing Inc., and ISyE. All rights reserved. No portion of this publication may be reproduced in any form without the written permission of the publisher. Printed in the USA.

Security has demanded our attention for the past two years. Challenges to our physical security became painfully compelling with September 11th. Our financial security has been challenged by the weak economy and corporate financial scandals. SARS has threatened our health security. Viruses, worms, and other creations have continually assaulted our information security.

Security is the theme of this issue of *Engineering Enterprise*. Industrial and Systems Engineering is concerned with security at several levels. First, of course, many of us are personally apprehensive. Second, we are concerned with the ability of our enterprises to function efficiently in light of heightened measures to address security. Finally, we are very interested in applying our competencies in optimization, stochastics, statistics, and so on to enhance security.

This issue includes an interview with Rich DeMillo, Dean of Georgia Tech's College of Computing and former CTO of Hewlett-Packard. This interview is based on his recent keynote presentation at the Georgia Tech Business Network, where the spring program focused on security. He provides an overview of "asymmetric warfare" in enterprise security and IT security, and argues for some new ways of thinking about these issues.

Also in this issue is an interview with John Gilligan, CIO of the U.S. Air Force. His remarks focus on the changing nature of security issues for the Department of Defense in general and the Air Force in particular. He considers the R&D issues where Air Force investments are most focused, as well as those issues where investments are coming from the broader IT community. He points out the challenges of electronic collaboration and interoperability vs. security and information assurance.

Chip White, a Chaired Professor in Industrial and Systems Engineering, considers the role of the School in addressing security challenges. He articulates the ways in which security concerns are affecting private and public enterprises and where these issues fit in the School's portfolio of research initiatives. Chip also outlines the types of problems most amenable to solution using our core competencies, and briefly summarizes a few initiatives in these areas.

We are all concerned with security, whether it is physical, health, financial, or information security. Our families, communities, and enterprises are threatened, and we feel compelled to do something. Of course, these problems also represent opportunities for Georgia Tech faculty, staff, and students to both discover fundamental knowledge and create innovative solutions. We are committed to doing our part. 

William B. Rouse is the H. Milton and Carolyn J. Stewart Chair and Professor of the School of Industrial and Systems Engineering at the Georgia Institute of Technology.



Mike Lanham (2nd from left) and his students at Sprayberry High School use equipment donated by EPICS in their Electric Vehicle class.

EPICS NEWS

Engineering Projects in Community Service (EPICS) is a national program that places teams of undergraduate engineering students in partnerships with local community service agencies and institutions. These interdisciplinary teams design, build, and deploy systems to solve engineering-based problems for the non-profit community and educational organizations. This partnership provides many benefits to the students and to the agencies. The students receive academic credit for experiential learning and the community organizations benefit from custom technical expertise that they may not otherwise be able to afford. Students also gain an understanding of the role that engineering and technology can provide in efforts to solve social problems.

EPICS was founded at Purdue University in fall 1995. By 1998, similar EPICS initiatives began at Notre Dame and Iowa State. In 1999, a National Science Foundation (NSF) grant provided for programs to start at the University of Wisconsin and Georgia Tech. Since then, several other universities have started EPICS programs at their campuses.

A national EPICS program was initiated in 2002 to involve a number of EPICS sites on projects of national impact. The first national EPICS project is a partnership with Habitat for Humanity for EPICS affiliates to develop and implement tools to increase the efficiency and quality of home construction and ownership.

The EPICS program at Georgia Tech was established in fall 2000 in the School of Industrial and Systems Engineering. Through spring 2003, the pro-

gram has worked with 27 project teams, 27 community partners, 159 students and 11 faculty advisors. The EPICS teams include a diverse mixture of students – males, females, African-Americans, Hispanics, and Asians.

Georgia Tech EPICS Accomplishments

- In February 2003, ISyE and EPICS hosted a Regional Workshop on Engineering and Service Learning that was facilitated by Purdue University and sponsored by Campus Compact and American Association for Higher Education. Twenty-four participants attended the all-day workshop and came from Purdue University, University of Tennessee, Tuskegee University, Atlanta University Center, Southern Polytechnic State University, Mercer University, Georgia Southwestern State University, George Mason University, and Georgia Tech.
- In May 2003, five faculty and staff representatives attended the National EPICS conference at Purdue University in West Lafayette, Indiana.
- Microsoft Corporation, a national EPICS partner, donated software to three Georgia Tech EPICS clients and the EPICS lab, totaling more than \$80,000 in retail value.
- Hewlett-Packard became a national EPICS partner this year and donated tablet computers to EPICS sites.
- Through a NSF grant, Georgia Tech EPICS sponsored three local high school teachers via the Georgia Tech CEISMC Georgia Industrial Fellowships for Teachers (GIFT) program. Teachers from Sprayberry High School, Lithonia High School, and Chamblee High School all worked with EPICS during the summers of 2001, 2002, and 2003. GIFT teachers were given equipment for their respective school labs valued at approximately \$5,000. Among these was Mike Lanham of Sprayberry High School, who received equipment to be used in his Electric Vehicle class.

EMIL'S "FUTURE STATE OF SUPPLY CHAIN CHALLENGE" SPARKS VISION AND IMAGINATION

On June 5, 2003, ISyE's Executive Master's in International Logistics (EMIL) program marked the end of its most recent 18-month degree program with the EMIL Capstone Event and "real-time" business case competition. This competition required EMIL participants to envision the leading edge of supply chain management in the year 2015 and how companies could use this knowledge to gain a competitive advantage. EMIL is a master's degree program that helps the world's leading companies develop creative, global logistics solutions by grooming their supply chain executives.



Tracy Flagg of Ford Motor Company presents her team's view of logistics in the 21st century

The "Future State of Supply Chain Challenge" gave five teams of EMIL participants two hours to predict the changes that will shape the supply chain more than a decade from now. The case competition served as a "final exam" for the EMIL program, requiring EMIL participants to apply key program learning to real-world business problems. Participants drew on their understanding of significant business drivers, world conditions, cultural concerns, economic conditions, and trends to identify likely future supply chain "pain points" and discern possible solutions. Each team had ten minutes to present their projections to a panel of judges made up of EMIL Advisory Board members including: Daryl Mickley, Bax Global; Jim Kellso, Intel; John Vande

Vate, Georgia Tech; Maria Rey, Latin America Logistics Center; Rodger Mullen, Schneider Logistics; Scott Gardner, FEDEX; and Terri Herod, Georgia Tech.

After all the presentations, the judges awarded the EMIL Supply Chain Leadership Award to the team of Jim McCabe, Milliken & Co.; Jonathan Hartman, Ford Motor Co.; John Kehoe, Baxter Healthcare; and Cheryl Martin, U.S. Postal Service.

All the teams addressed the extended supply chain, including procurement, manufacturing, transportation, warehousing, consumer management, and reverse logistics, within an international context. The scenarios they developed ranged from extrapolations of current trends to an almost "sci-fi" image of the tomorrow's business world.

The Winning Response

The winning team postulated a future driven by market-savvy consumers, an increased environmental awareness and a focus on quality of life and global wealth. To compete, companies will respond with "real-time" integration marked by instant information transfer throughout the supply chain. This will facilitate increased speed-to-market and product adaptability, resulting in "global transparency on a scale we can only imagine today." Key predictions included:

- Macro-collaboration among corporations and governments, ensuring more efficient and cost-effective supply chains.
- Emergence of four geographic trading blocks: the Americas, Europe, Asia-Pacific, and the Africas.
- Global data exchange based on globally established data definitions, creating the data transparency needed for macro-collaboration and increased supply chain speed.
- A global security plan implemented by the geographic trading blocks to secure the safety of supply chain channels.
- Automated transportation networks featuring vehicles driven by GPS3, the next generation of GPS.
- Universal currency to facilitate the

ease of information exchange and reduce supply chain complexity.

The other teams presented a range of equally intriguing forecasts about virtually every area of the supply chain. Among the highlights were:

Regionalization & Speed

- Inventory-in-motion as a means to reduce "idle" warehouse inventory.
- Equalized global labor costs, reducing companies' need to chase lower labor costs.
- Regionalized logistics providers fed by a small number of inter-continental mega-providers.

IT & Security

- Commoditized IT.
- Intelligent data mining capabilities to combat data overload.
- A move to more off-the-shelf software products, achieving balance between customized supply chain

software applications and affordable, off-the-shelf applications.

- Contingency planning & security.

Adaptive/Flexible Supply Chains

- Refocusing of supply chain on "demand" as the key driver.
- Product individualization expanded to capture customer preferences through customized, personalized solutions.
- Micro-manufacturing & mass customization.
- Collaborative planning & execution.
- Reliance on reverse supply chains with an emphasis on recycling and reuse as resources continue to become scarce.
- Global-friendly trade policies.

"The team competition was a great opportunity to develop an idea in a short time and present it," said Mark Michaels, an EMIL participant from

(continued on page 18)

Tired of Resume Blasting and No Results?



In a recent study, candidates using **High Impact Job Search™** received more than **5 Times as Many Job Offers** as those using traditional resume and networking techniques.

Get High Impact Job Search™, an Innovative, State-of-the-Art, Job Search Software System.

Order High Impact Job Search™ Now for \$199

Must use Marketing Code: EE63

<http://hij.s.group56.com> to order and view our streaming video.

Money Back Guarantee



<http://hij.s.group56.com>

Enterprise Security and IT Security:

Asymmetric WARFARE

An Interview with Richard A. DeMillo



This interview is based on an address by Richard A. DeMillo (left) to members of the Georgia Tech Business Network on May 14, 2003.

DeMillo is the Imlay Dean of the Georgia Tech College of Computing.

Regarded as one of the pioneers of the Internet, DeMillo's distinguished

technology career spans business, government, and academia, including major positions at

Hewlett-Packard, the National Science Foundation, Telcordia Technologies (formerly Bellcore),

Purdue University, and Georgia Tech.

Engineering Enterprise: What is your perspective on the information security disruptions we seem to be increasingly experiencing in private and public enterprises?

DeMillo: To address this question, we need to consider the contemporary nature of enterprises. The depth of the enterprise as we are used to thinking about it — as we learned about it in textbooks, as we became acquainted with it when we first entered the Web age — is a consequence of what is going on both within enterprises and with the infrastructure that is used to support enterprises. This has profound consequences for IT security.

Think about how things have transitioned in large businesses and small businesses during the last 10 to 15 years. One way of looking at the growth of the enterprise is as a set of premises where activities are taking place, assets are being held, and where there are definite boundaries. Vertical integration of enterprises refers to enterprise activities now located across a metropolitan area, across a state, or across a geographic region to the emergence of globally integrated companies. However, it remains a recognizable enterprise in that the connecting components of the enterprise are owned by the enterprise itself. For example, a closed network, a free relay network, a local area network, an internet, an intranet, or something like a railroad that connects two cities — something that is owned, recognizable, and tangible.

During the Internet boom, these things really started to change. Manufacturing and distribution partners became less tightly coupled to their enterprises, so the notion in particular of an intranet became problematic. We also saw extranets opening up the corporate resources to manufacturing and distribution partners. Then, in the 1990s, change continued very quickly, including exchanges and outsourcing. Not only did we open things up, but we also created marketplaces, so that we do not have complete control over who enters our borders and boundaries. Finally, there was the climactic emergence of the Web and portal technology, and B2B, B2E exchanges.

The first time this hit me in a dramatic way was in the employee portal at Hewlett-Packard (HP), when I realized that with one push of a button, I was changing an address that spawned transactions to my 401K, my cell phone service provider, and to many people who were not within any business sphere of HP, but were connected by relationships that were either constructed in real time or on the fly.

John Leggate of British Petroleum (BP) refers to the “commoditized enterprise.” As John tells us, this notion came about when he was talking to someone in the new Department of Homeland Security (DHS) in the federal government. John couldn’t get across the idea that BP does not really own the channels that it takes to connect its wells, suppliers, dealers, or even its customers. Instead, it uses commodity hardware, open-

source infrastructure, open protocols, and the Internet. If a planner or strategist in DHS thinks that the energy infrastructure is going to be contained within borders and within a set of business processes that you have control over, forget it. It just does not happen. BP has always been ahead of the curve on this, but you can find many examples where the commoditized enterprise is a reality today, and more and more companies are moving towards this view.

**The interesting thing about this
for an IT dogmatist is the obvious
parallel in the evolution of
information processing technology.**

The interesting thing about this for an IT dogmatist is the obvious parallel in the evolution of information processing technology. Joel Birnbaum, who was chief scientist at HP for many years, gave me the multidimensional view shown in Figure 1. The evolution of information technology is a series of Moore’s Laws: a series of exponential curves followed by inflexion points, followed by discontinuities that again lead to exponential growth. Once you think about it, you can understand how and why that has happened and what is going on. It began with the early mainframe days. Then came many computers, distributed computers, computers on desktops. We have all heard about the famous memo from IBM that says, “Forget about any sustained business use for personal computers; only 50,000 of them will ever be sold worldwide.” By the time the memo was received at the Management Committee at IBM, there were 50 million in use.

As far as open systems, client/server is disappearing and clients, the end points of networks, are the intelligent nodes. Smart handheld devices are not necessarily cell phones anymore, but are remote control devices that we can use to access an array of resources including open global services, from Microsoft, for example. We have access to services that are assembled when needed; we negotiate identities, negotiate authorizations, and then they are torn apart, torn down, and disappear. They literally do not exist when they are not needed anymore, so each of these waves, each of these exponential mini-Moore’s Laws, has given rise to a set of capabilities that has enabled the commoditized enterprise.

**What we are trying to defend has now evolved from a border
or theater of operations, which we can array forces around,
into a much more ambiguous world of asymmetric warfare.**

EE: What does the emergence of the commoditized enterprise mean for information security?

RD: At the most basic level, it means that this picture is grossly wrong because it is based on the left hand side of Figure 1 and on a glassed-in data center that has a perimeter, or at least is connected by railroad tracks that we own. Imagine all of the defenses that it takes to guard this perimeter: IT resources, security alarms, chemical means for controlling fires, intrusion detectors, and all the things it takes to keep people out of our space. The ways in which we defend this type of perimeter is very much in line with the classical view of war fighting that the United States has built into its military planning since the inception of the Republic. That is, we have an estimation of what the attacking force is going to be, and we overwhelm the attacking force with counterforce. When the counterforce mounts, we overwhelm

those forces. This actually works reasonably well in a traditional environment.

The difficulty is that in the real world, we have people that do not play by the rules. What we are trying to defend has now evolved from a border or theater of operations, which we can array forces around, into a much more ambiguous world of asymmetric warfare. There are people and groups pursuing complex ends inside your perimeter that you do not fully understand and cannot attack with overwhelming force without destroying yourself. The whole idea of asymmetric warfare is that this countervailing balance of attacker and defender simply does not make sense anymore. And we saw what that means in real life in the most recent Gulf War. The insistence on agile military forces reflected the fact we are not defending a perimeter. We do not have a theater of battle; rather we have

people moving all over our sphere of influence.

Returning to our earlier example, what does it mean for BP to defend its perimeter? BP does not have a perimeter. BP is in every gas station that pumps BP gas. It is in every well, every supplier of parts to those wells, and it is in Bechtel, which is a subcontractor to BP. We can go through all of the ways in which BP interacts with the world, and that is the enterprise. So any threat that BP is going to see to its infrastructure is very much an asymmetric threat.

EE: What changes for information security when threats are asymmetric?

RD: Asymmetric threats in the IT world mean some very special things. They obviously mean there are no perimeters to defend, which is a very big change. You do not have a guard sitting at the door because there is no door. Indirect attacks are the common mode of

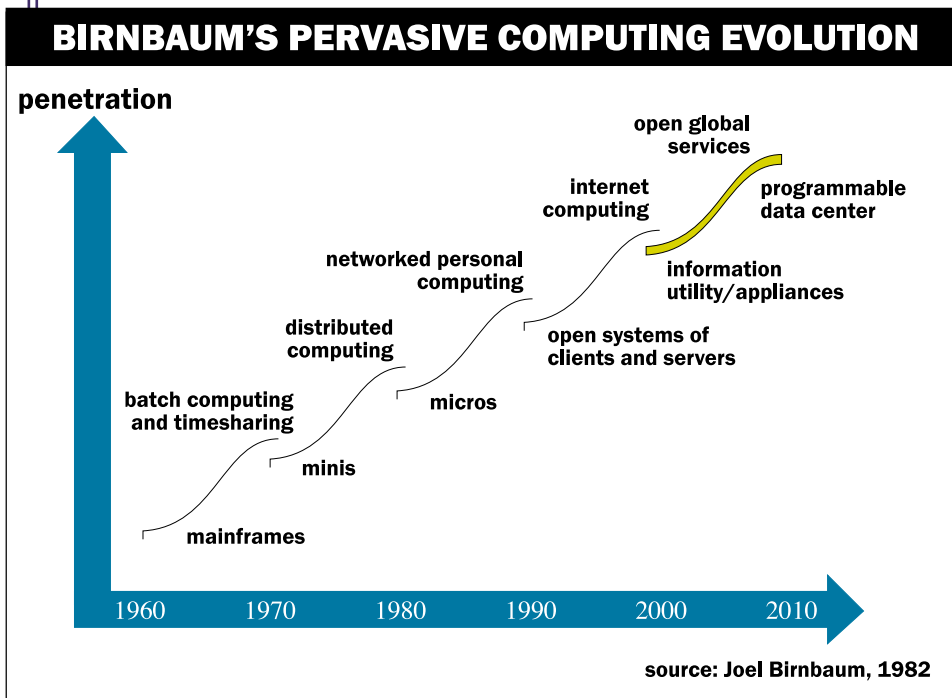


Figure 1

attack. People are not going to approach you head on; they are going to approach you in ways that are not anticipated by your defense. Things like insider threats become the dominant risk in the enterprise, which means that when we look at the newspaper or see what is happening in the world of IT security, asymmetric threats abound.

We have to recognize that our own security depends on the security of everyone else we are connected to; if we are connected over an open network, that means everyone else in the world. It is a growing set of people that we are depending on. Think about it. Why does Microsoft get beat up for Internet security violations? Because that is where the money is. Why do people rob banks? That is where the money is. Why are there relatively few muggings on deserted islands? People do not live there. Everybody lives on Microsoft infrastructure, which is why we see the incidents rising. It is an interdependent war.

Those little mini-Moore's laws in Figure 1 are also attack scenarios, or threat scenarios. People are using automation to mount sophisticated attacks against infrastructure, and we can see this in things like distributed denial of service attacks. It is not that we are accessing resources that we are not supposed to access; it is that we are flooding resources with so much traffic that they cannot respond, and they cannot do what they are supposed to do, which is what a "denial of service" is.

This may be a sophisticated concept, but it is not the infrastructure that we are attacking. We are attacking the value of the network. Metcalf's Law says the value of a network grows in proportion to the square of the number of nodes in the network. The only way the network has value is if we can talk to someone; so those connections between people attached to the network are where all the value is. So, it is enough to get access to the transactions; it is enough to find out what is going on; it is enough to spoof a resource; and it is enough to convince someone that you are person A and not person B. It is an attack against things that do not really exist in the sense that a glassed in data center exists.

EE: What can we do to win, or at least hold our own, in this asymmetric information warfare?

RD: At some point you go to the executive suite and you whisper in the right ear that there are these people out there trying to get us. What are we going to do about it, boss? That's a great question.

One of the reasons I am delighted to be back in academia is that I do not have to answer that question anymore. I can just raise the question.

At some point you go to the executive suite and you whisper in the right ear that there are these people out there trying to get us.

It is not an easy concept to align responding to those kinds of threats with business value. What you would like to say is that investing in security is like putting a padlock on your garage or locking your car. You would like a straightforward return on investment analysis for IT security. As you increase the level of security, you take down the cost or at least the expected cost of a security breach, because you are taking down the probability that a breach is going to occur. What does it cost you to do that? You have to invest in the cost of security countermeasures. You want to be sure that your bike is not going to be stolen? Put a bigger lock on it. The bigger lock costs more

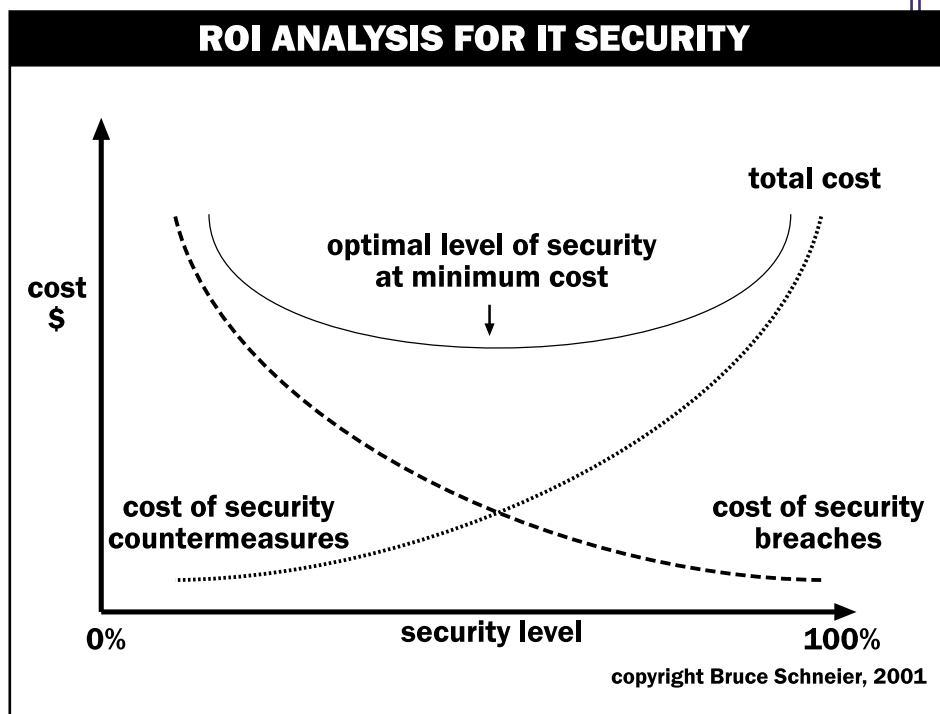


Figure 2

money, but it means that the guy walking down the street is going to have to get a bigger pair of wire bolt cutters in order to get at the lock. So those two ends of the spectrum are in balance with each other at some point where the investment makes sense. This is an analysis by Bruce Schneier (see Figure 2). The optimal level of security at minimal cost is going to be somewhere on this curve.

The difficulty with the analysis is this idea of indirect attack. This assumes that you know what the right countermeasure is going to be. It assumes that you know that people are going to try to cut the lock on the bike rack, as opposed to driving a pickup truck and lifting the bike rack onto the back of the pickup truck and driving away with it. You can see that in a variety of scenarios.

The difficulty with the analysis is

this idea of indirect attack.

This assumes that you know what the

right countermeasure is going to be.

Encryption is one of those security technologies that is unassailable. It is mathematical, it is beautiful, and you can sell it. Companies distribute public keys over the Internet. Those of you who use the Internet regularly have a bazillion keys sitting on your desktop or laptop now. It is part of the fabric of commerce these days, and one of the compelling things about encryption is this: you know that the cost of breaking 128-bit RSA encryption is going to be about \$20 million. Why? That is the cost of the machine that can break RSA encryption. If you do not have this machine or have not made the investment, the probability of compromising the crypto system is way down near zero. There may be some instances where you can find some things out by accident, but it is not until you get enough resources or invest enough in your attack infrastructure that you raise the probability to "one." The behavior is quite striking, and it gets to one right away.

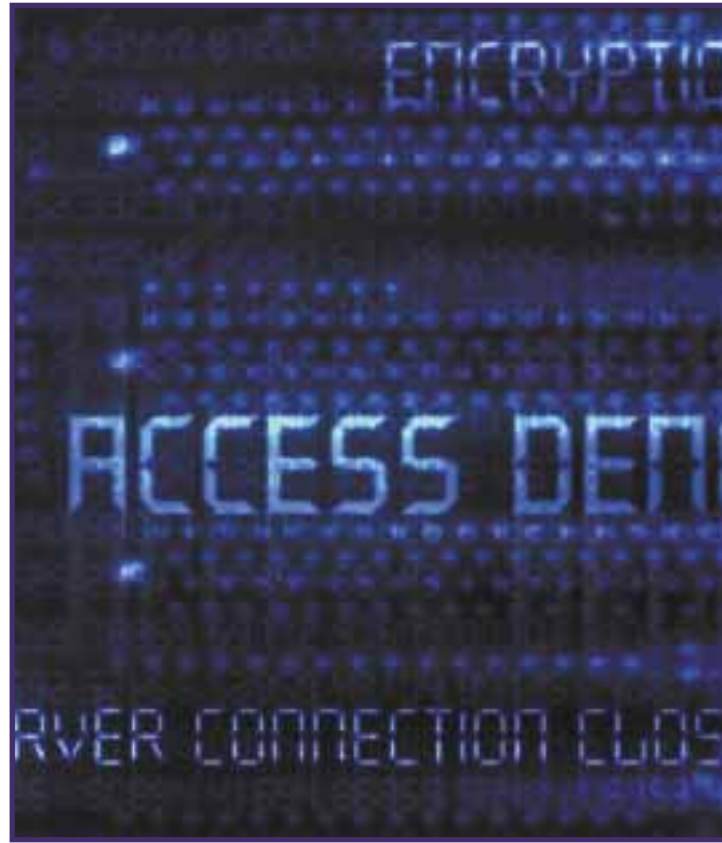
Once you have the machine, you may think you have things knocked. What's the problem with that? The problem is that people are much more cost effective than \$20 million cryptanalysis machines. It cost \$2.5 million to buy Aldrich Ames; \$1.4 million for Robert Hannsen; Robert Walker was had for \$1 million, and poor old Mr. Pollard down here was bought for \$50,000. What does that do to the analysis? As you start to buy off people who know things, I can no longer make any guaran-

tees that my investment dollar is buying me more security? The asymmetric threat makes it difficult for the return-on-investment analysis.

What are you willing to pay for security? Sprint figured out 20 years ago that you were willing to pay for hearing a pin drop; you are willing to pay for a quality of service guarantee. Perhaps you will also pay for IT security. I will pay for a closed network; I will pay for the modern equivalent of a closed network, provided that you can instrument your open network and make quality of service guarantees about who is on it and what they are doing. There is a business model behind this because service providers make money every day. Actually, these days they do not make money, but in normal times they could make money by providing quality of security guarantees.

EE: How has September 11th affected the ways we think about and address these issues?

RD: One of the discussions that has taken place nationally and internationally is that the homeland security problem is really an enterprise security problem. It is an enterprise that has blown up quite literally, but also figuratively. We live in a country without borders; we live in an economy without borders. We connect and disconnect and provide services in ways that are difficult to understand and model precisely as a business enterprise. Homeland security is really an enterprise security problem. As a country, we are on the verge of investing billions of dollars in homeland security. Are we doing it wisely?





Probably not. If you look at the DHS budget, you find billions of dollars for very traditional defenses, such as handheld devices for first responders and chemical foam for mounting defenses against a chemical attack. We are making investments in bioterrorism, when in fact the lesson from the 1960s about how we built our arsenal to confront the Russians is that information technology is almost certainly going to drive the problem.


What did we see in the last two Gulf Wars? We saw flying computers and flying computer programs. We take it for granted now, but as we look at the laser-guided weapons hitting their targets, we forget the many articles that said, "There is a software crisis; none of our weapons work." We built weapons without thinking that they were going to be flying computers, and we found out, later, that it was very costly to fix problems. It took a lot of investment that we did not have to make and could have gone into other things, like accelerating the development of the Internet by many years.

We are at an inflection point today in deciding how to invest in homeland security as an enterprise problem. You have to look at it as an information technology problem. We already know, to a large extent, the technologies that need to be invested in and the kinds of technologies that we need to invent over the next generation. We have known it for some time, but we simply have not invested in them.

EE: Are there any especially important success factors in addressing this enterprise problem?

RD: One in particular — this stuff is just too complicated. The whole world of IT is not human-centric. It is boxcentric, it is protocol-centric, and it really is a conglomeration of processes and knowledge and legends that have grown up with this technology for the last 20 years. Widespread deployment of technology, widespread use of the technology, and widespread extraction of value from the investment are going to be difficult unless it becomes much more human-centric.

We think of information security as a technology problem — a business problem. However, it is also a mindset problem, and somehow this stuff has to become much more "human-centric." People have to drive what is going on. The technology should not drive what people do. I expect this insight to form the basis for what happens nationally on the R&D side. We are excited about this at Georgia Tech, but it remains to be seen how widely the message is received and understood.

EE: Thank you, Dean DeMillo, for your ideas and insights into an enterprise-oriented view of information security. 

GAMS

OPTIMIZATION

The General Algebraic Modeling System (GAMS) is a high-level modeling system for mathematical programming problems. It consists of a language compiler and a stable of integrated high-performance solvers. GAMS is tailored for complex, large scale modeling applications, and allows you to build large maintainable models that can be adapted quickly to new situations.

GAMS Development Corporation

1217 Potomac Street, N.W.

Washington, D.C. 20007, USA

Tel.: +1-202-342-0180 • Fax: +1-202-342-0181

sales@gams.com • <http://www.gams.com>

PERSPECTIVES ON SECURITY

Engineering Enterprise: From the perspective of the Air Force and Department of Defense, what do you think are the most prominent security issues now, and how have they changed in the last year or two, if at all?

John Gilligan: I don't think the situation has changed much in the last couple of years, although there is greater visibility now on the set of issues that I view as most important. The most pressing security challenge is to get a better handle on the consequences of commercial software delivered to us in the Air Force – the same software that is delivered across the world, that has insufficient quality. As a result, inherent logic flaws can be exploited and used as the basis of attacks against our systems – viruses, worms, as well as more sophisticated attacks.

EE: Is this just for the business side of the Air Force, or does this include Command and Control as well?

JG: This is an issue across the spectrum of our mission areas and systems.

EE: So it's not just Microsoft Windows and Office?

JG: No, but Microsoft provides the primary operating system and desktop software that we use across the Air Force. We also have Unix-based systems and other commercial software that is being exploited in a similar manner. These include Cisco routers, Oracle databases, and Internet utilities. Microsoft tends to get the most visibility because it is the biggest software supplier in the world. Because it is the biggest, it is the focus of the largest number of exploits. But we see the problem across the board.

And why is this the most significant security problem? Because when you look at the successful penetrations of our systems and disruptions of Air Force operations, roughly 90 percent are based on the exploitation of previously discovered logic

flaws in commercial software products. The remedy has been to patch the software flaws. However, the rate of discovery of these logic flaws is increasing to almost one per day. In an environment like the Air Force, where we have 500,000 Microsoft desktops, patching 500,000 computers is a non-trivial exercise.

EE: Everyone can't just go to the Microsoft website and download the update?

JG: Oh they can, but just think of the logistics of getting 500,000 people to have enough knowledge to go to the Microsoft site, download the patch, and install it properly. We don't do that. What we do is push the patch to our major commands and our bases, and our bases generally have their IT folks install the patches for the users on the base. Increasingly we're using automated tools to install the patches, but the automated tools are not fully fielded, nor do automated tools let us cover the full gamut of different configuration and vendors of software systems.

Two years ago I told the president of Microsoft that "we are now spending more money patching and fixing your software than we are spending to buy it." Since then, the rate of discovery of flaws in Microsoft and other commercial software products has been a growing problem. Because 90 percent of the successful exploitations of our systems are exploiting this path to disrupt Air Force operations, whether it is root access to our systems or just denial of service, this becomes the most pressing security problem. I've got to dampen this security problem – why? Because it's consuming an awful lot of resources and, to be honest, most of these attacks are coming from relatively unsophisticated people. These attacks can mask what could be a much more serious attack from a more sophisticated adversary, who might be using methods that are less "noisy," less visible, and could have potentially greater consequences.

An Interview with John Gilligan



John M. Gilligan (left) is the U.S. Air Force Chief Information Officer in Washington, D.C. He is the principal advisor to the Air Force leadership on information management, business processes, and information technology standards. He previously held the same position at the U.S. Department of Energy. He earned his B.A. in mathematics from Duquesne University and master's degrees in computer engineering from Case Western Reserve University and in business administration from Virginia Polytechnic Institute and State University. In this interview, Gilligan speaks with *Engineering Enterprise* about security issues affecting the Air Force and homeland security in the United States.

Unfortunately, dampening the impact of exploitation of logic flaws in commercial software will take years because it will take that long for the software industry to dramatically improve the quality of its software. Moreover, modern software products consist of many millions of lines of code. I do not expect software will be delivered without any exploitable logic flaws in the foreseeable future. However, we hope within five years we'll see a significant improvement in overall software quality.

I believe that the engineering practices used to ensure reliability and correct operations in other disciplines will become increasingly important for software. I also predict we will see a rebalancing of the business equation for commercially provided software. In the past, those who got to market with new features were the ones that captured market share. I predict that, in the future, software quality will be increasingly important in the purchase decision. Improved quality will reduce lifecycle support and, therefore, total cost of the software product. I envision the maturing process for software as analogous to maturing the automobile industry. In the early days of the automobile, quality wasn't important; it was features. Now, many consumers look at *Consumer Reports* for quality and operating cost assessments before purchasing an automobile.

EE: It seems like the trends you are talking about so far have just been the disruptive ones, as opposed to manipulative ones.

JG: Let me attempt to put what I have described in context. In our unclassified computing systems, we manage our aircraft maintenance operations, our supply activities, and our personnel training qualifications. Each of these capabilities is absolutely essential in order to operate our aircraft and conduct combat operations. The same systems and networks that support these functions also support our back office finance and personnel support functions. The architecture of our network

enterprise is based on the philosophy captured in the phrase: One Air Force, One Network. Our computer systems are architected with trust relationships such that one computer can talk to another. Moreover, leveraging networking protocol conventions, these systems interact with a higher degree of trust than a system that is not part of our Air Force network. As a result, if you break into one computer, depending on how sophisticated you are, you may be able to get into any computer that we have on our Air Force network. One can postulate a scenario that on the first night of a military conflict, such as in Iraq, an adversary triggers an exploit against a software flaw that denies the ability of the Air Force to get at maintenance, supply, and critical pilot information. If not detected and countered in a fairly short period of time, you could ground our Air Force. This is my nightmare scenario.

EE: Why do you think that hasn't happened? Are people not up to the task yet?

JG: I think there are a couple of reasons. One, it is not trivial to pull off the type of scenario I just described. It's pretty complex. Second, we work very hard in the Air Force to defend against such scenarios.

Within the Air Force, we have installed patches for each of the previous worms and viruses (I LOVE YOU, Code Red, Blaster, SoBig, Slammer, etc.), but let's face it; the patches we're putting in are somewhat like band-aids. We still have exposure because an adversary only needs to find another logic flaw in a software product that exhibits similar attributes.

I should note that some computer security aficionados have hypothesized that the series of viruses and worms that we have seen over the past couple of years have been the test bed for a well-planned effort to launch a very potent attack at some point in the future. They have reasoned that sophisticated attackers

have been trying out their techniques, seeing how quickly they propagate, assessing the impact, and monitoring the defenses and response actions. The theory is that the source of many of these attacks is more sophisticated than misguided teenagers. They suggest a well-coordinated effort that is gathering intelligence and refining the tool set and doing it fairly publicly in order to use the media to gauge impact and reactions.

On balance, I think it is important to say that we are, in fact, dramatically improving our defenses in the Air Force. In the military, we have robust command and control of our network of computers, and we have made dramatic improvements in the methods used to detect an attack and to counter cyber attacks. Even when we see major attacks, we are able to rapidly isolate the source and the target. We use filtering at the Internet Protocol level to quickly block types of traffic and certain types of activity. We then use more fine-grained methods to mitigate the effects of the attacks.

**The theory is that the source of
many of these attacks is more
sophisticated than misguided teenagers.**

EE: This is at the Internet Protocol level?

JG: In many cases, yes. At the main gateways to our networks, for example at the routers and firewalls into our bases, we block selected IP addresses and certain protocols. When we see an attack, we extend the Internet Protocol blocks. Other large organizations are also using similar techniques. Within the military, we have a Command and Control structure that orchestrates our cyber defenses. The structure starts with the four-star commander of Strategic Command, Admiral Ellis, at Offutt Air Force Base in Omaha, Nebraska. Strategic Command has command links to the military services, and then to each of our major commands and bases in a highly parallel fashion. Within minutes of detection of an event, we are able to execute cyber protection actions that may not patch all the targeted computers, but at least mitigate the potential damage. We're continually working to increase the effectiveness of our detection and response actions.

EE: You mentioned different vendors and the problems of the quality of the software. What is going to bring about the change? Is the Air Force waiting for the commercial world to deliver what you want, or are you more proactive in trying to get that world to provide the quality?

JG: I mentioned that two years ago I met with Microsoft to ask it to focus on this problem. My message to the president of Microsoft was that the Air Force could no longer stand the cost

and risk of the poor quality of software that Microsoft was providing to us. I was basically informing them that that "I'm going to start going public. It is not because Microsoft is the worst offender, but you are the biggest." Since the Air Force is Microsoft's largest customer, and a highly visible one, the message got to Bill Gates. Immediately after September 11, 2001, my message and similar messages from other customers started to get a lot of attention. Recently, there has been a chorus challenging Microsoft and other software vendors for the poor quality of their products.

Unfortunately, it is going to take a long time to improve the quality of the many millions of lines of code that have been fielded. To its credit, Microsoft initiated its Trustworthy Computing effort right before September 11, 2001. It has addressed all aspects of its software efforts, including culture, training, tools, and testing processes. Likewise, Oracle, Cisco, and the other vendors have initiated similar efforts. This is non-trivial change from an engineering perspective because, in the case of Microsoft, you're changing a business culture that very successfully followed the model that "you write code as quickly as you can, get an adequate level of quality, and push it out the door." Features are what you're after. And we're now saying, "no, we want well-engineered, high quality code." This is a major change for the software industry.

As a relatively immature field, software doesn't have the same definition of quality attributes and methodologies and process that are in other engineering disciplines. I'm not an expert in the details, but the Sustainable Computing Consortium at Carnegie Mellon University is focusing on the root problem, which is "what are the measurable characteristics of quality." It then hopes to begin to establish these characteristics as recognized standards. Long term, this is going to be the type of effort that is going to pay off. I'm seeing more emphasis on this type of effort now, because the lack of quality is hitting everybody in the pocketbook.

EE: Are there any investments that the Air Force has to make because the commercial world just won't do it?

JG: The investments that we're making are not unique because the commercial world won't do them, but I will say we incur a lot of expenses because we have to do workarounds to compensate for the fact that the quality is not good. We spend an awful lot of money for patch distribution and verification. In the future, we plan that these capabilities become part of the standard architecture and toolset. My goal is that if we are going to have to patch systems, we want to be able to do it instantaneously and then verify patches on a continuing basis. We spend a lot of money on firewalls, filters, and intrusion detection systems, when in many cases, if the software quality was better, we wouldn't have to place so much reliance on these defense mechanisms. We do spend a lot of money on our hardware and software cyber defenses. However, the biggest cost of our cyber defenses is manpower. When we get one of these virus or worm attacks, it takes a lot of manpower to deal with the immediate actions and then clean up the consequences.

EE: *So there really aren't threats that are unique to the Air Force. If you can deal with the threats that are the primary concern of the commercial world, those are the primary ones you're concerned with, too.*

JG: Yes and no. I can say that most of the threats are going to be common between the Air Force and the commercial world. But I think there is a source of threats that are of more concern for us than they would be for many in the commercial world. Obviously, our job in the military is very specific and we're the first line defenders, especially in homeland security. So if someone wanted to attack the United States or potentially prevent us from being able to take military action in other parts of the world, one of their focus areas could be Air Force networks and computers. So, we think we have a higher priority on some adversaries' radar than some parts of the commercial sector. Although I'll add that when you look at the effect of the recent blackout in the Northeast, if someone were going to attack the United States, they might not worry about the military networks if they could successfully take out the power grid. Or they might disrupt the water supply. Critical infrastructures can also become key cyber targets, communications and electricity being the two that are most fundamental.

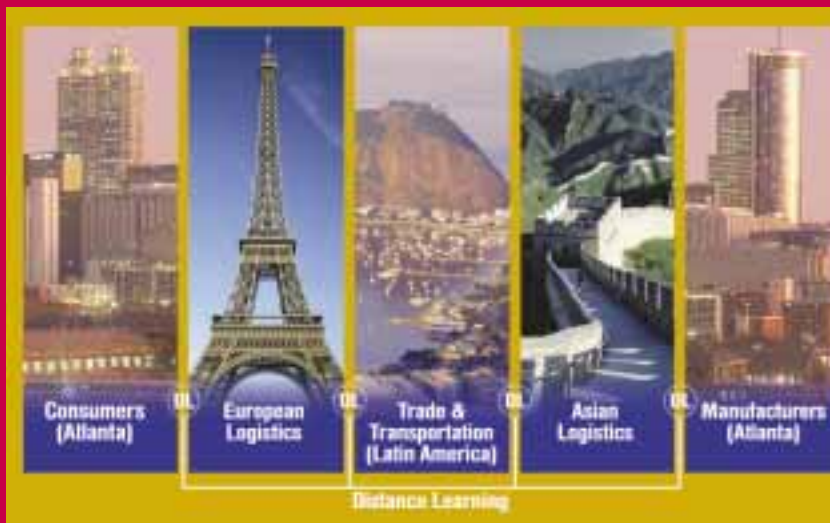
EE: *That sounds like the military and civil blend together from an infrastructure point of view.*

JG: When you're talking about homeland defense, yes. In the United States, the military relies heavily on the civilian infrastructure. Once we go outside the confines of the United States, then the military is much more self-contained from an infrastructure standpoint.

EE: *How have the homeland security issues affected your priorities and initiatives?*

JG: Candidly, not a lot to this point in time. However, increasingly, the military focus is changing. Until fairly recently the military believed we were always going to fight overseas, so we didn't have to worry about the interaction with state and local governments and other Federal agencies. We're now realizing that for any conflict that has its focus in the U.S., it is absolutely essential that we are able to coordinate with and leverage state and local activities, industry, utility providers, etc. There is now a robust dialogue that is coordinated by the new Department of Homeland Security and by the Northern Command, the military organization that supports homeland defense, with the many Federal, state, and local organizations. They are spending an awful lot of their time working with state and local governments to set up communications, to establish protocols for cooperative agreements, and it is still early. It is a massive task.

REAL WORLD EDUCATION FOR WORLD-CLASS EXECUTIVES



TODAY'S COMPANIES NEED TO:

- Increase supply chain efficiencies.
- Move to a global supply chain strategy.
- Groom their rising stars.
- Expand collaborative relationships.

LEARN to improve supply chain efficiencies by grooming your executives in Georgia Tech's Executive Master's in International Logistics (EMIL) Program.

EXPERIENCE real-world results by learning best practices from the world's leading experts in EMIL's five 2-week residences at key locations around the globe.

BUILD a team that can deliver measurable results by linking finance with global supply chain management.

For more information, visit <http://www.emil.gatech.edu> or call 404.385.2538



EE: *You talked before about the situation where someone could breach one weak link within the Department of Defense, and then communicate with other computers as more trusted than they are justified. How about when you deal across organizations in homeland security? If they could reasonably penetrate the fire department, for example, could they then communicate with the Air Force, Marines, and police in a trusted way?*

JG: Today it is less likely. The good news is, since we don't have better electronic sharing relationships with the civil organizations such as fire and police, that's less of an avenue of attack. However, as we move forward to better link our military and civil systems and databases, an attack that exploited these trust relationships could become more likely. Within the Air Force, as we are achieving our goal of a seamless enterprise-wide network, the threat actually becomes more significant. As we better link military systems to federal agencies, and then state and local civil agencies, we also expand our collective vulnerabilities. This is why improving our defenses becomes extremely important. As we move forward to achieve the goals for the defense of our nation, we're actually opening up a greater potential to be exploited.

EE: *So there is some downside to interoperability?*

JG: Right. In fact, there is a parallel issue that some have argued. For example, the former presidential advisor on cyber security, Dick Clark, used to advocate that we should have heterogeneous computer software for our systems, because that minimized the extent that somebody could attack us and exploit a common flaw that would be resident on the vast majority of our systems. He argued that we ought to move away from everything being on Microsoft, and move to Linux, and have heterogeneous software product architecture. The problem is that a more diverse set of software products complicates the task of seamless integration and efficient management. I don't believe that is the right way to go. You'll find people who will have different philosophies on how to approach this.

EE: *It also seems like it goes back to Alexander Hamilton in the Federalist Papers about centralization vs. decentralization.*

JG: Yes, you can get into those arguments quite easily.

EE: *What is your overall sense of things right now? Do you feel like we're getting better at coping with the challenges? Are we just keeping our head above water, or what?*

JG: My experience in tracking this area goes back now 30 years. I started working in computer security in graduate school, where I got involved in a multilevel security research effort that was funded by the Air Force. I also focused on computer security when I was in private industry. My conclusion is the following: the threat and the sophistication of the threat continue to increase, and it is roughly parallel to our improvements in defense measures. This is a race, and it is not one that we will ever

say that we've won, because as the defense protection approaches get more capable, the inherent systems become more powerful. When we finally figured out how we could secure a single computer, we connected them all. All of the sudden, we had networks that brought a whole new dimension and complexity to security. As we made additional progress on networks, then we expanded the scope to an enterprise of interconnected networks. It used to be that you would have small enclaves that were closely interconnected, and now we've embraced the concept that we want seamless connectivity across the globe. And the body of code that must perform correctly grows larger and larger. Back in graduate school, I was doing mathematical proofs of code. We were going to mathematically prove that the software correctly implemented the design. We eventually gave up on that approach to security because, as you get millions and millions of lines of code, it became impractical.

EE: *It almost sounds like the way our bodies fight bacteria and viruses. We keep adapting, they keep adapting, and life happens.*

JG: Right. Our intent is that we run as fast as we can in improving our security defenses; we continue to get better, realizing that there will be new attacks for which our defenses are not effective and so we adapt. I do not foresee a time when the security folks are going to be out of business.

EE: *Does the immune situation analogy hold very well?*

JG: It does. In fact, increasingly, those who are doing research in this area are looking to biological analogies in trying to develop the protection measures. They're looking for software that will recognize a threat, be able to adapt itself to the nature of the threat, learn, counter the threat, and then be able to better recognize the next threat. Building on the human analogy, this area of research might be the most promising for the future.

EE: *Is that research being done by the Air Force and Department of Defense, or is it all over the place?*

JG: I think it's all over the place. I don't know that it is limited to defense applications, but I'm sure the Department of Defense is sponsoring some of the research. You're probably doing some of it down there at Georgia Tech.

EE: *Any other observations?*

JG: What I highlighted was the biggest vulnerability, the quality of software. Let me quickly mention two other areas of security concern, and they both deal with our humans who operate and use our systems. The first observation is that statistically the most significant and severe security threat is an insider—an employee of the organization who has authorized access to systems. In many cases the insider is not somebody malicious, but they are poorly trained or poorly motivated individuals who make a mistake and bring down your network. One may not consider it a security problem, but from our


standpoint it is. When you don't have availability of your networks and systems that is a security problem.

You also often find that people don't use the mechanisms that are enabled within the systems, like passwords. One of the things you can do to help assess the strength of the security in an organization is to take an automated tool and run it against the password file. Even if the password file is encrypted, you will find that you can break a fairly high percentage of the passwords, because they are generated based on common words. There are a lot of things that individuals can and should be doing to ensure security. This is a constant training challenge. In some cases, your well-intended end user becomes a vulnerability. In reality, most of them say that "it won't happen to me."

What we are doing with our enterprise Air Force Portal and the surrounding infrastructure is implementing a single sign-on capability that will initially use passwords but eventually will be public key encryption-based, where we will pass the security credentials from your ID card into the computer and then to all the applications so that you don't have to remember all the separate passwords used for different appli-

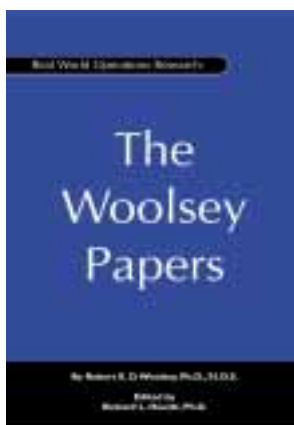
cations and write them all down, which becomes another vulnerability. Password security can work well, except when you have to remember 50 of them.

There is also a long-standing recognition that an insider who has administrator-type privileges can do an awful lot of damage from a security standpoint and also be fairly effective in covering their tracks. We expect that the individuals we hire to do systems and network administration be highly trained, but we also want to have a high degree of assurance of their personal integrity. It is likely that in the future we will certify these people and put them under what we in the government call the "Personal Assurance Program," which in some cases means polygraph administration. We say, "you are so critical to the operations of this system that not only will we do extensive background investigations, we might also do periodic polygraphs."

EE: Thank you for sharing your rich experiences and insights. Our readers will certainly gain a much deeper appreciation of the nature of the security threats you have outlined. 

Real World Operations Research:

The Woolsey Papers



Real World Operations Research: The Woolsey Papers is a collection of the diverse writings of one of OR's most outspoken and controversial figures, Gene Woolsey. Woolsey's humorous and practical writings leave little wonder as to his venerable status in the field.

This collection contains 33 articles published from 1972 and 2003, covering a broad spectrum of subject matter relevant not only to OR/MS professionals, but also educators, managers and corporate administration. To accompany his writings on operations research, chapters also cover topics from communication in the corporate world to handling labor disputes, getting promoted and getting fired. Through creative storytelling and down-to-earth advice, Woolsey provides readers with the knowledge and philosophical mindset to conquer operations and management situations in all settings.

Real World Operations Research: The Woolsey Papers

By Robert E. D. Woolsey, Ph.D., F.I.D.S. Edited by Richard L. Hewitt, Ph.D.

\$19.95 (+S&H) • 164 pages • 6 x 9 • paperback ISBN: 1-931634-25-4 **Order online at:** www.lionhrtpub.com/books

Published by **Lionheart Publishing, Inc.:** 506 Roswell Street, Suite 220, Marietta, Georgia 30060
(888) 303-5639, ext. 214, fax: (770) 432-6969 e-mail: lpi@lionhrtpub.com



How ISyE is Addressing U.S. SECURITY CHALLENGES

By Chelsea C. White III, ISyE Chair of Transportation and Logistics

There are a variety of ways that ISyE, through its research and teaching, can help the nation address the security challenges that emerged on September 11, 2001. A key challenge that this article will focus on is ensuring that the national and international transportation systems are secure, for both passengers and freight, and that the U.S. economy, which is inextricably linked to these transportation systems, remains strong.

Exploiting the U.S. transportation system, the terrorist events of September 11, 2001, caused the deaths of more than 3,000 individuals and roughly \$100 billion in direct and indirect economic losses, and pushed the nation into a war. It is well recognized that the attacks of September 11, 2001, were in large part attacks on symbols of U.S. economic strength and hence on the U.S. economy. Indeed, economic disruption as a result of terrorism is a major concern for many of those who have addressed these horrific events, their impacts, and how they can be avoided in the future.

According to *Fortune* (2002), the impact on U.S. supply chains due to higher shipping costs, increased inventories, border closures, increased travel times, and other changes as a direct result of the September 11, 2001, terrorist attacks is estimated to be \$150 billion per year. In terms of potential future terrorist attacks, O'Hanlon, et al. (2002; p.7, Table 1-2) provide a table that lists the nature of economic disruption and the potential cost of each of several different types of possible terrorist attacks. At the

top of this list is "weapons of mass destruction shipped via containers (or the mail)" with a potential cost of up to \$1 trillion.

In response to September 11, 2001, a variety of different U.S. policies and regulations has been put in place to help secure the vehicles, cargo, individuals (e.g., truck drivers), and physical infrastructure of global supply chains, e.g., Container Security Initiative (CSI), Customs-Trade Partnership Against Terrorism (C-TPAT), Secured Trade in the APEC Region (STAR), and Trade Act 2002: Rules on Inbound Air Cargo to the U.S.A (descriptions of these terms can be found at www.isye.gatech.edu/setra). In particular, the CSI places U.S. Customs officials at the 20 largest non-U.S. "mega ports" (e.g., Singapore, Hong Kong, Rotterdam) to inspect sea cargo containers bound for U.S. ports.

Where do security-related issues fit in the ISyE research portfolio? What are the types of problems most amenable to solution, using ISyE core R&D competences? There are many possibilities. One particularly natural fit, which we will discuss below, involves modeling and analyzing the impact of the new U.S. security initiatives on the productivity of the users and providers of freight transportation. This research, funded through Georgia Tech's The Logistics Institute (TLI, www.tli.gatech.edu) and the Trucking Industry Program (TIP, a member of the Sloan Industry Centers Network, www.isye.gatech.edu/tip), involves the use of mathematical modeling,

logistics and supply chain management analyses, simulation, and optimization, all of which are part of the ISyE curriculum.

CSI essentially “pushes back the borders” for container inspections. It can also increase the complexity of various processes and, as a result, decrease productivity. For example, moving containers from in-bound ships to out-bound ships at a CSI-compliant trans-shipment seaport now also involves taking a percentage of U.S.-bound containers to inspection stations for (at least initially, non-invasive) security inspections. Although the inspections themselves tend to be completed quickly (within two or three minutes), they currently require draying each container to another part of the port, putting the container into a queue, x-raying (or gamma-raying) the container, and then draying the container back to its proper position for loading onto the out-bound vessel. Thus, security inspections require extra container moves, extra time, and extra infrastructure and manpower (e.g., dock space for the inspection equipment, extra drayage vehicles), which add up to more cost. Our studies show (again, see www.isye.gatech.edu/setra for further explanation and quantitative analyses) that, as the percentage of containers inspected increases:

- The average number of container moves will increase modestly, and the variability of this increase will be modest.
- The length of time needed to unload an in-bound ship and load an out-bound ship may increase substantially, and the variability of this time will increase, possibly substantially as well.
- The optimal safety inventory of a supply chain will increase rather dramatically for high velocity supply chains if the customer service level is held constant.


The percentage of containers inspected does not have to get particularly high (5 percent to 10 percent) in order for these measures of productivity to be noticeably affected. These results indicate that the providers of transportation services (e.g., a seaport) may not be as affected as the users (e.g., a supply chain using the port) by these new security initiatives. Much effort in the private sector is now being placed on determining whether or not applications of new security-focused processes, combined with information technologies, will have an ancillary productivity benefit with the hope that the efficiency gains due to these new processes and information technologies will counterbalance the productivity degradations due to the added complexity inherent in the new regulations.

An example of on-going research involves understanding the productivity impact of performing freight security inspections at foreign, rather than domestic, seaports and airports. We instinctively feel that “pushing back the borders” is a security enhancing policy. Containers are checked before reaching U.S. borders, reducing the likelihood that a terrorist attack involving a weapon in a sea cargo container will occur at a U.S. port. Initial research results indicate that inspecting a container closer to the point of origin of the supply chain, and thus resolving uncertainty early, rather than inspecting the contain-

er closer to its destination can enhance productivity. Hence, non-U.S. port security inspections may benefit both the security and productivity of supply chains that originate in a foreign country and terminate in the U.S.

CSI essentially “pushes back the borders” for container inspections.

It can also increase the complexity of various processes and, as a result, decrease productivity.

In summary, the list is long of interesting and highly relevant research topics associated with security that can be analyzed by the collection of problem solving disciplines taught and studied in ISyE. We have briefly discussed only a few of the many possibilities and look forward in the future to further addressing this critical national challenge. Further discussion of these and related issues can be found in the references. With the intent of leading a national discussion on supply chain security and productivity research and education, we are pleased to report that TLI and TIP will be hosting an NSF-sponsored workshop early next year on supply chain security and productivity, which will have as its deliverable a list of key research and education issues involving the impact of security on supply chain productivity. We anticipate a future article in this publication providing an overview of this workshop. 

References

- Committee on Science and Technology for Countering Terrorism, National Research Council of the National Academies. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. The National Academy Press, Washington, D.C., 2002.
- Daalder, I. H., et al., “Protecting the American Homeland: One Year On,” Brookings Institution, Washington, D. C., January 2003.
- Flynn, S., “America – Still Unprepared, Still in Danger,” Council on Foreign Relations, Washington, D. C., 2002.
- Fortune*, “The Friction Economy,” 18 February 2002.
- Korb, L. J., “A New National Security Strategy in an Age of Terrorists, Tyrants, and Weapons of Mass Destruction,” Council on Foreign Relations, Washington, D. C., 2003.
- Kunreuther, H., G. Heal, and P. R. Orszag, “Interdependent Security: Implications for Homeland Security Policy and Other Areas,” Brookings Institution, Washington, D. C., October 2002.
- O’Hanlon, M. E., et al., “Protecting the American Homeland: A Preliminary Analysis,” Brookings Institution, Washington, D.C., 2002.

(continued from page 3)

Kuehne & Nagel. “It gave us the chance to move from knowledge gathering to creative strategic thinking – working quickly and cooperatively.”

“This was an excellent program,” commented Tracy Flaggs of Ford Motor Company, “causing us to get outside of the month-to-month, quarter-to-quarter environment we live and work in every day.”

While some of the forecasts for the supply chain in 2015 may appear extreme, the teams urged us to “look at the speed of events in the last 20 or 30 years.” In light of that perspective and the acceleration of change, these ideas may not seem so radical.

ISyE UNDERGRADUATE PROGRAM TOPS RANKINGS AGAIN

The School of Industrial and Systems Engineering continues to lead as the nation’s best undergraduate program in Industrial/Manufacturing Engineering, according to rankings issued this summer by *U.S. News & World Report*. ISyE also leads in the same graduate rankings, released earlier this year.

In the undergraduate rankings, Georgia Tech ranks as the 9th best public university in the nation and 37th among all of the nation’s universities, up one slot from last year. The College of Engineering is the 5th Best Undergraduate Engineering Program, with three of its engineering programs in the top five (civil, aerospace, and ISyE).

The rankings also noted outstanding programs that lead to student success. Georgia Tech was one of 10 schools cited for an outstanding program in Internships/Co-Ops.

For more complete information on Georgia Tech’s *U.S. News & World Report* rankings, please see www.gatech.edu/news-room/.

TLI MAKING CHANGES

The Logistics Institute’s Expanding Focus with New Director

The Logistics Institute (TLI) has a new executive director and an expanded



Chelsea C. “Chip” White III, ISyE Chair of Transportation and Logistics

vision. Chelsea C. “Chip” White III, ISyE Chair of Transportation and Logistics, became executive director of TLI in July. TLI, a center within ISyE, coordinates all logistics-related activities on the Georgia Tech campus. TLI is in partnership with the National Science Foundation and a broad spectrum of corporations and government agencies known as *Leaders in Logistics*.

TLI’s mission is to create the next generation of logistics and supply chain systems knowledge through basic and applied research, disseminating this new knowledge through the Institute’s logistics curriculum and professional courses, and applying it to the real world through joint industry/academic practice. “The primary aim for TLI’s future is to grow these core activities while at the same time expand the TLI capabilities footprint to include related enterprise- and industry-level strategic analyses,” says Dr. White.

Dr. White and his colleagues anticipate that this expansion will take TLI to a higher level of visibility and impact. “This expanded vision involves a more global, multidisciplinary perspective. Georgia Tech is a multinational university,” says Dr. White. “Our students need to understand logistics and supply chain systems at the global level, which is greatly benefited by our current partnership with TLI-Asia Pacific in Singapore, our Executive Master’s in International Logistics (EMIL), and TLI’s growing number of other international contacts and relationships.”

The implications of this expanded vision include a more diverse funding

base. TLI is looking forward to increased engagement with federal agencies, foundations, state governments, and international funding sources, as well as an expanded involvement with the private sector. The vision also will include a broader disciplinary span, involving to a greater extent operations management, economics, and corporate strategy, while continuing to be the dominant institute nationally for optimization, logistics, and supply chain research and applications.

Don Ratliff, former TLI executive director, is remaining with TLI, but has scaled back his involvement in order to focus more attention on his own projects. TLI Director Harvey Donaldson remains in his post, where White says he will take a more central role in the organization.

In addition, Diane Kollar, ISyE director of development, will increase her responsibilities to include development activities for TLI. “With Diane, we’re looking forward to a higher level of coordination between TLI and ISyE development activities,” says White.

TLI also has a new home and new space, moving upstairs into what has been the office suite for the School chair. This is possible because the DuPree College of Management has moved to its new home across campus, freeing up space next door to ISyE. The ISyE faculty and staff now have the opportunity to spread out from what have been cramped quarters.

Dr. White came to Georgia Tech in 2002 from the University of Michigan, where he served as professor of Industrial and Operations Engineering and Electrical Engineering and Computer Science, as well as director of the Intelligent Transportation Systems Research Center and co-director of the University of Michigan Trucking Industry Program. He earned his Ph.D. from the University of Michigan in Computer, Information, and Control Engineering, and has served on the faculties of Southern Methodist University and the University of Virginia.

JEFFREY TEW IS 2003-04 EDENFIELD EXECUTIVE-IN-RESIDENCE

Dr. Jeffrey D. Tew will serve as ISyE's Edenfield Executive-in-Residence for the 2003-4 academic year. Tew is group manager of the e-Manufacturing and Alliances Group in the Manufacturing Systems Research Lab at General Motor's Research and Development Center in Warren, Michigan.

Tew's contributions to General Motors (GM) are many. He has served as a member of strategy teams that established GM's Order-to-Delivery Division and the GM India Research Lab; is a current member of the GM-Allison Transmission Channel Strategy Team; and he helped design GM's supply chain.

Tew received a B.S. in Mathematics, an M.S. in Statistics, and a Ph.D. in Industrial Engineering from Purdue University. His current research interests include the application of operations research and information technology tools to large-scale logistics systems and e-commerce.

While at Georgia Tech, Tew is expected to work with Dr. Rouse and ISyE faculty to develop a vision and strategy that enhances ISyE interactions across Tech's six colleges and the Georgia Tech Research Institute. The overall goal is to formulate a faculty recruiting and resource development plan that will enable substantial growth of ISyE's programs in research and education in enterprise aspects of the automobile industry. This includes attracting one or more endowed chairs, as well as a diversified base of funding for interdisciplinary research across engineering, management, computing, and behavior and social sciences.

Prior to joining GM, Tew was the director of Logistics Engineering at Schneider Logistics, Inc.; a senior systems engineer at Consolidated Freightways, Inc.; and an Adjunct associate professor of Computer Simulation at the Oregon Graduate Institute. He was also on the faculty in the ISyE Department at the Virginia Polytechnic Institute and State University. He is a visiting professor at Tsinghua University in Beijing. He is

widely published and well known for his work in supply chain management, Six Sigma implementations, quality control, and operations research.

James C. Edenfield, BIE 1957, president of American Software, founded the Executive-in-Residence program to bring experienced and proven executives to campus each year, sharing research and education knowledge from industry. The endowment supports office space, computer equipment, software, secretarial and student support.

ALUMNI NEWS

Evan Fleisher, BIE 1990, has opened his own business, Tri-State Logistics, Inc., in Dubuque, Iowa. Tri-State is a full-service truck/freight brokerage operation, specializing in the movement of temperature-controlled freight.

Steven J. Halmos, BIE 1970, is the retired chief executive officer of SafeCard Services, Inc., a credit card services company he founded as a student at Harvard Business School. Now a private investor, Halmos and his wife Madelaine have two children and live in Ft. Lauderdale, Florida.

Don King, BIE 1960, is the retired Standards and Manufacturing Productivity Manager for MeadWestvaco in Atlanta. He and his son Steven recently completed a 53-mile backcountry hike with full backpack in Yosemite, reaching 11,000 feet at Red Peak Pass.

J. Thomas Rocker, BIE 1964, has retired in Haines City, Alabama, after operating his own specialty construction business for 34 years. He is now volunteering as business administrator for his church and serving on the boards of the Haines City Citrus Growers Association and Center State Banks of Florida, Inc. He enjoys seeing his five grandchildren as often as possible.

Bill Swint, BIE 1969, has moved to Seattle as the head of order fulfillment for Cutter & Buck. He most recently spent two years in France as project manager for Columbia Sportswear's distribution center.

Randy Thayer, MSIE 1980, was recently appointed plant manager of General Motor's new Lansing Delta Township Assembly Plant in Michigan.

Travis A. Turberville, BIE 1948, is retired from Reynolds Metals Company. He tells *EE* he has slowed some, but he is still hunting, fishing, and trying to keep up with his six grandchildren.

GEORGIA TECH PIONEER SHIRLEY MEWBORN DIES

Georgia Tech has lost one of its first women graduates, and one of the Institute's most honored and respected alumni. Shirley Clements Mewborn, EE 1956, died last July of colon cancer at her home in Marietta, Georgia.

Mewborn had a long career with Southern Engineering Company of Atlanta, eventually becoming vice president and treasurer before retiring in



Subscribe to ORMS Today,
your source for
**Operations Research and the
Management Sciences.**

Visit us on the web:
www.orms-today.com

or call Maria Bennett:
770.431.0867, ext. 219
for more information



Shirley Mewborn, EE 1956

1998. She remained active at Tech throughout her life, serving as the first female president of the Alumni Association and a member of the Georgia Tech Foundation. She received the Alumni Association's prestigious

Joseph Mayo Pettit Alumni Distinguished Service Award and the College of Engineering Distinguished Alumnus Award. She is a member of the Georgia Tech Engineering Hall of Fame and the Georgia Technology Hall of Fame.

"Shirley Mewborn was a pioneer at Georgia Tech," said President Wayne Clough. "We will miss her fine leadership, her excellent judgment, her tireless energy, and her warm smile. She was the embodiment of a Georgia Tech education."

Mewborn, 68, was married to Francis "Duke" Mewborn, also a member of the class of 1956.

BIRTHS

Mark Lane, BIE 1986, and his wife Christine announce the birth of their first child, in Brevard, North Carolina. After teaching high school math for seven years, Lane has joined Smith Systems, Inc., as a project manager.

DEATHS

Ronald L. Bacon, MSIE 1950, of Hingham, Massachusetts, in January 2003. Bacon was a retired tennis teaching professional.

Ray Thomas Ervin, BIE 1949, in November 2000.

Paul L. Strong, BIE 1966, in September 2002 after a long illness. Strong founded Allbright Systems, a building and maintenance company in Chesterfield, Missouri.

FACULTY NEWS

Jiangang "Jim" Dai and **Richard Serfozo** have been elected as fellows of the Institute of Mathematical Statistics, the most prestigious society in math statistics. Professor Dai received the award for fundamental contributions to applied probability through his work on fluid and diffusion approximations to multiclass queuing networks, and in particular for key contributions relating to the stability of such networks. Professor Serfozo received the award for contributions to the fields of point processes and stochastic networks and his editorial service to the profession.

Judith Norback received the Best Paper Award at the June meeting of the American Society of Engineering Education, Industrial Engineering Division. Her paper was titled, *Teaching Workplace Communication in Senior Design*.

New Faculty

Ronald L. Billings has joined the ISyE faculty as an assistant professor in the manufacturing systems area.

Billings has been an instructor at the University of Texas, as well as Concordia University in Austin. His experience includes service in the U.S. Air Force as a civilian radiographic file technician. From 1991 to 2002, he worked at SEMATECH (a consortium of semiconductor manufacturing companies) in Austin, as an engineering editor/team leader, automation engineer, faculty architecture group manager, and material logistics standards project manager. Since that time, he has served as partner and chief executive officer for Fluid Analysis for Balancing Queues, an Austin company that develops software for factory scheduling and dispatching using fluid models.

Billings holds a bachelor's in Electrical Engineering (with honors); a master's in Business Administration; a master's in Mechanical Engineering; a master's in Computational and Applied Mathematics; and a doctorate in Operations Research and

Industrial Engineering – all from the University of Texas at Austin.

STUDENT NEWS

Doctoral student **Matt Drake** was selected to attend the 12th Annual Council of Logistics Management Doctoral Symposium in Chicago in September. Held each year before the annual conference, the Symposium invites approximately 20 students from around the world.

Six doctoral students have received \$5,000 fellowships from the Atlanta Chapter of ARCS (Achievement Rewards for College Scientists) Foundation. They include: **Paul Brook**, **James Luedtke**, **Brian Lewis**, **Jerome O'Neal**, **Josh Reed**, and **Ray Popovic**. ARCS was founded to encourage students to pursue challenges in science and engineering. The Atlanta Chapter provides scholarships to students from Tech, Emory University, and Morehouse College.

Doctoral student **Milind Sohoni** received an Honorable Mention in the 2003 George B. Dantzig Dissertation Prize, awarded each year by INFORMS. The prize includes a certificate and \$100.

NSF Fellow Helps Determine Health Care Treatment Options

The National Science Foundation (NSF) recently honored ISyE Ph.D. student **Paula Edwards, BIE 1995**, with a 2003 Graduate Research Fellowship. Each year NSF very selectively awards these prestigious fellowships to recognize and support outstanding research in science and engineering. Edwards' received this award for her proposed research, "Patient Decision Support Systems in Healthcare." Over the next three years, she will be exploring human-computer interaction, cognitive engineering, and decision theoretic aspects of developing web-based patient decision support systems.

The goal of Edwards' research is to design systems to help health care providers and patients work together to decide which treatment options are

right for the patient. For example, with diseases like cancer, the treatment options frequently have serious side effects, so it is important that the patient and doctor work together, considering not just the patient's physical health, but also their values and preferences in the treatment decision. Edwards' research will contribute toward developing systems that educate patients about their disease and treatment options and help them work with their doctor to determine which treatment is right for them. "It is an honor to have my research recognized by the NSF," said Edwards, "It shows that there is a real need in the market for systems designed to consider the human, in addition to technical and information, requirements, especially in healthcare."


Edwards performs her research in ISyE's Laboratory for Human-Computer Interaction and Health Care Informatics, co-directed by Dr. Julie

Jacko, associate professor of ISyE, and Dr. François Sainfort, William W. George Professor of Health Systems and associate dean for Interdisciplinary Programs in the College of Engineering. Dr. Jacko's expertise is focused on human-computer interaction, human aspects of computing, and universal access to electronic information technologies. Dr. Sainfort's expertise focuses on consumer and medical decision making, healthcare informatics, quality assessment and management in healthcare, and evaluation of medical technologies.

Drs. Jacko and Sainfort are co-advising Edwards in her multidisciplinary dissertation research. "Paula's dissertation research crosses traditional boundaries and links two very compelling areas of research: human-computer interaction and medical decision making. Her contributions to these fields will yield unprecedented advances that will translate into new solutions and

innovative systems for healthcare delivery," stated Dr. Jacko.

Edwards is currently a second year Ph.D. student concentrating on Human-Integrated Systems. This is not her first experience with Georgia Tech – she earned her undergraduate degree from ISyE in 1995. She worked as an IT consultant designing business intelligence and Internet systems for six years before returning to Georgia Tech to pursue her Ph.D. "My industrial engineering background and my industry experience have given me a unique foundation on which to build my research," she says.

Through her practical experience developing systems in industry and the theoretical and research experience acquired in the School of Industrial and Systems Engineering, she hopes to begin designing the next generation of decision support systems – systems that put the user first. 

 <p>Georgia Tech Business Network</p> <p>WWW.GTBN.ORG</p> <p>SPONSORED BY THE SCHOOL OF INDUSTRIAL AND SYSTEMS ENGINEERING</p>	<p>K N O W L E D G E</p> 
<p>C O N N E C T I O N</p> 	<p>C O M M U N I T Y</p> 

ALUMNI NEWS

Please take a minute to complete this form,
and mail or fax it to the school.

Please send to:

Engineering Enterprise
School of Industrial and Systems Engineering
Georgia Institute of Technology
765 Ferst Drive, Atlanta, GA 30332-0205
or fax to 404.894.2301



**What has been
happening with you?
Job change?
Any recognition you
wish to share with
your classmates?**

Name _____

Degree/Year _____

Home Address _____

City _____ State _____ Zip _____

Home Phone (____) _____

Title/Company Name _____

Business Address _____

City _____ State _____ Zip _____

Business Phone (____) _____

E-mail Address _____

Your News _____

Other IE topics you would like to read about in Engineering Enterprise _____

