

NEWSLETTER INFO

Published nine times per year (September – June) by the Minnesota Information Professional Society. We welcome materials for publication. Submit materials on disk or via E-mail to:

Earl C Joseph
365 Summit Avenue
St. Paul, MN 55102
Tel. (651) 290-2846
E-mail: ejoseph@waldenu.edu

NOTE

MEETING INFORMATION

MEETING PLACE:

**Holiday Inn – Bloomington
35W at 94th**

Phone (612) 884-8211

Meeting Times:

5:00 PM Social Hour
6:00 PM Dinner
6:45 PM Meeting & Program
8:00 PM Adjourn

For Reservation Call:

John Belich
by May 11th
and choose:
Steak or Shrimp

Tel: (651) 634-1440
e-E-mail:

john.belich@tech-pro.com

\$20 Members
\$25 for non-members

Dinner Meeting NOTICE Tuesday, May 15, 2001

Joint Meeting of
**Minnesota Information
Professional Society**

And

**Association of Information
Technology Professionals**
Speakers Topic: **“Cool Robots
and What They Do”**
Speaker: **Dr. Richard Voyles**

Topic Information

Robots have been around for decades but they seem to have faded from our consciousness. Except for the occasional spark-throwing robot in a car commercial, the hype of several years ago has all but disappeared. Have robots reached the limits of technology?

This talk will provide a broad tour of robots in research, as opposed to robots in industry. From miniature surveillance robots for the military, to child-like humanoid robots that learn, to medical robots that perform surgery on humans, there are a variety of experiments underway in research labs around the world bringing robots in touch with humans. We will start by examining the challenges of robotics and then examine how these advanced applications provide meaningful solutions.

Speaker Profile

Dr. Richard Voyles received the B.S. in Electrical Engineering from Purdue University in 1983, the M.S. in Manufacturing Systems Engineering from the Department of Mechanical Engineering at Stanford University in 1989, and the Ph.D. in Robotics from the School of Computer Science at Carnegie Mellon University in 1997. He is an Assistant Professor in the Department of Computer Science and Engineering at the University of Minnesota but will be on leave this summer to work at Avanti Optics, a telecommunications manufacturing startup.

Dr. Voyles' research interests are in the areas of miniature, constrained robots; microassembly; mobile manipulation; programming by human demonstration; skill-based approaches to robot programming; and haptic sensors and actuators.

PRESIDENT'S LETTER

April showers bring May flowers...and the end of this year's MnIPS monthly meetings. After our May 15th joint meeting with AITP, our next monthly dinner meeting will be Tues-

day, September 18th, at the Bloomington Holiday Inn (I-35W and 94th Street).

MnIPS is a volunteer organization and we always welcome any help in our regular, ongoing committees or at a specific event, such as registering people at monthly dinner meetings or at the Golf Outing in June. A member that recently stepped forward to help is David Ortega, who agreed to do our annual membership invoicing (for dues) in January. Thanks for your help, David!

At the May 15th meeting, we will accept nominations for MnIPS' 2001-02 officers (namely President, V.P., Secretary and Treasurer) that will be elected by September. We are also looking for a regular attendee at our monthly dinner meetings to register people. The time commitment would be 5:00-6:00pm on the 3rd Tuesday from September to May, except for December. If you want to be an officer or if you can regularly help at the meetings, please call me at 651-707-0523.

We also need volunteers at our annual Golf Outing on June 18th at Greenhaven Golf Course. The time commitment would be 11:30am-1:30pm and/or 6:30-9:00pm. If you can assist us or you are interested in playing at the Golf Outing, please contact Jeff Hemauer at 612-375-7968 or by e-mail at ["jhemauer@valspar.com"](mailto:jhemauer@valspar.com). The cost to play is \$65 for members or \$85 for non-members (includes golf, dinner and prizes) and the dinner only cost is \$25. Company sponsorships of the MnIPS golf tournament are always welcome, please call Jeff if you're interested.

We also welcome ideas from you that can improve our organization. If you can assist us this year in any capacity please let me or any board mem-

bers (that are listed on the back page) know.

I look forward to hearing our May 15th speaker, Richard Voyles, from the University of Minnesota, who will speak on "Nano-Technology Robotics" (or better known as "Cool Robots and What They Do"). Thanks to our April 17th presenter, Steve Kloyda of Telemasters, who talked about "Personal Development". Thanks again to our March 20th guest host, Tom Cocchiarella of Pareo, Inc., who spoke on "What's New in e-Security: IP Architecture & Lessons Learned about Social Engineering". For a summary of Tom's talk, please read the regular meeting review column in this newsletter.

I hope to see all of you at the May 15th meeting!

-- Dennis Cummings, President

**THE ONLY SECURE THINGS ARE
STILL DEATH AND TAXES!**

(March 2001 MnIPS meeting review,
by Dennis Cummings)

Mr. Tom Cocchiarella was the featured presenter at the Minnesota Information Professional Society's monthly dinner meeting held on March 20, 2001. He began his career in the computer industry in 1971 as a Weapons Control Systems Technician on F4 Phantom Fighters (Secret Security Clearance) where he maintained Radar, Air-Air Targeting, and Air-Ground Bombing Computers. Mr. Cocchiarella attended the University of Minnesota, then transferred to St. Paul Technical College, where he received degrees in Industrial Electronics and Electronic Communications. He also earned a FCC Radiotelephony Commercial License with Radar Endorsement. While working for Control Data Corporation as a Customer Engineer, he maintained CYBER 170 & 7600 Super Computers.

In 1978, Mr. Cocchiarella joined Deluxe Corporation as a Computer Technician supporting a variety of systems, including DEC, Data General, and IBM systems. He managed the Deluxe National Hardware Support Depot and Field Support organization, and also managed software development for a variety of applications using mainframe, client/server, minicomputer, and PC systems. As a Telecom-

munications Analyst, Mr. Cocchiarella developed and delivered "Introduction to Data Communications" classes at St. Paul's Technical College. He served as Director of Systems Development for Deluxe Corporation, the VP of IS for Colwell Systems, and as the VP of IT for Deluxe Business Forms & Supplies. As President/CEO of Preferred Consulting Services, he launched a Computer Security consulting practice in 1997, before the company was sold to AccuStaff, Inc.

Mr. Cocchiarella joined [Pareo, Inc.](#) a Minneapolis based IT consulting company, as Practice Leader for the Information Protection Practice in 1998, and oversaw Pareo's IP Team efforts on a project for a large International Financial Services client based in Minneapolis. This major project included several of the client's international sites. He is now Practice Leader of IT Architecture for Pareo, which includes responsibilities for Systems Design, Enterprise Application Integration (EAI), and Information Protection Services including IP Architecture. Tom is a member of the Computer Security Institute ([CSI](#)), and is Treasurer of the Midwest Electronic Criminal Investigation Association ([MECIA](#)).

Mr. Cocchiarella started his presentation by warming up to the crowd, as a concerned sheriff would talk to the local citizenry about a burglary problem in the neighborhood. "There's a new global game now being played in town, folks!" was the warning from the lawman. It's not a physical encounter with criminals, but a technological one that thrives on getting information through the Internet or regular telephone conversations. Just as we lock up our houses to deter burglary, we should also have "information protection". More than just protecting your hardware and software, securing your information means keeping your business productive, your information intact and, most importantly, keeping your customers' trust! Sophisticated hackers and technically savvy employees can infiltrate your systems; misuse resources; and gain access to sensitive financial information, trade secrets, employee records, and confidential customer information!

How do we identify these thieves? Mr. Cocchiarella drew a sketch of what people should look for and Rules for this Global Game now being played:

1. There are no rules - Some of the traditional tricks employed by thieves are also used here such as distraction and deception.
2. Anyone and everyone can play - as long as they have a PC or just a telephone.
3. Players are not allowed to know who the other players are - secrecy is kept via alias Web addresses and pay phones.
4. You don't know when the game starts - any story given by a crook can seem reasonable.
5. You don't know what the other players' goals are - are they teasing or really stealing your personal or company secrets?
6. You must choose to play - unless you decide not to go online or even answer the telephone.

How are we exposed to this information thievery to begin with? There are several technical/IT factors that help fuel the widening security gap:

1. There are a wide variety of network devices, each having their own unique security profiles and capabilities.
2. There could be many access points into and out of a typical network environment, which complicates security.
3. There are constantly changing networks and new technologies.
4. Disgruntled employees can leak information following a layoff or disciplinary action.
5. A company's budget or limited security expertise can lead to untrained staff or substandard security tools and equipment.

"Information thieves" get access to their prized data through:

1. Eavesdropping and Packet Sniffing - overhearing conversations or accidentally seeing information (and copying it for later use) that was not intended for them to read.
2. Snooping and Downloading - looking through company directories or Intranet files for files that look interesting enough to keep and eventually misuse.

3. Tampering or "Data Diddling" – changing a data file's contents to disturb the system, such as rounding off a penny on each payroll check and putting it in another account. Another incident involved moving up a prisoner's release date.
4. Spoofing or Impersonating – calling the "help desk" as an employee asking for immediate access to the system.
5. Denial of Service (jamming or flooding) – filling up e-mail or voice-mail storage so that customers cannot contact the company.
6. Injecting Malicious Code (viruses or worms) – usually involves a vulnerable employee to open an attached "*.exe" file which copies itself to other users in an e-mail address book.
7. Exploiting Flaws in Design, Implementation, or Operation - does the firewall really stop outsiders?
8. Cracking Passwords, Codes, and Keys – employees should not have easy-access passwords (such as their initials) and should regularly change them to avoid detection.
9. Misuse of Resources – using company resources to order or download things from the Internet (such as sports gambling or accessing porn).
10. Physical Interference or Damage – untrained employees could accidentally shut off needed CPU's or peripherals.
11. Social Engineering – Portraying an employee or VIP trying to access company or personal information. In one case, a man called the help desk after being booted out on 3 wrong passwords. He claimed to be a sales rep trying to land a big account and threatened to call the CEO if he was denied a new password. Simple identification questions (or actually calling the CEO in that case) will stop most attacks.

How do "Social Engineers" attack vulnerable people?

1. Many attacks start with social engineering—the use of lies and

deception to con another human being into providing information or performing some operation that facilitates an attack.

2. It is usually performed over the telephone so the true identity of the attacker is concealed, and it can be launched from anywhere in the world.
3. Most common attack is someone pretending to be an employee in desperate need of an account access or password in order to fix a problem, close a deal with a customer, etc.
4. A small amount of public information makes it easy to play this game—phone listings, annual reports, officer names, customer names, etc.

Mr. Cocchiarella said that each company must introduce 5 "layers of information protection". They are the steps which "prepare your company to provide the protection services it needs". The first layer is **Education and Awareness**, which consists of:

1. Executive Awareness Sessions
2. Management and Staff Awareness
3. Project Level Consulting
4. Enterprise Level Awareness
5. IT Staff Training/Awareness
6. End-User Staff Training/Awareness

The second layer is **Policy Development**, which consists of:

1. Evaluation of Existing Information Protection Policies
2. Recommendations for Additional/ Modified Policies
3. Development of Communication Processes
4. Implementation of Information Protection Policies

The third layer is **Assessment and Prevention**, which consists of:

1. Security Assessment and Evaluation
2. Prioritization and Action Plans for Improvements
3. Development of Information Protection Standards
4. Penetration Testing Services
5. Security Product Evaluations and Recommendations
6. Intrusion Detection System (IDS)
7. Organizational Design

The fourth layer is **Recovery Planning**, which consists of:

1. Return Breached Systems to Normal Operation:
2. Hacker Eradication
3. Virus Elimination
4. Eradicate "Denial of Service" Attacks
5. Restoring Firewall Integrity
6. Restoring Operating Systems

The fifth and final layer is **Investigation Services**, which consists of investigating fraud, crime, and espionage. This includes, but is not limited to:

1. Data Tampering, especially when there is/are:
 - a. Records changed
 - b. Impersonation
 - c. Embezzlement
 - d. Fraud
 - e. Computer Forensics
2. Electronic Espionage
3. Licensed & Bonded Criminal Investigations
4. Undercover Investigations

Who should be concerned with information security?

1. Every Officer – since management is responsible for the company's asset protection!
2. Every Employee – because if the company's security is at risk, so are employees' jobs!
3. Every Customer – only deal with organizations that honor the statement "I trust the products I buy are safe and the information collected about me is secure and private."
4. Every Company - The U.S. Economic Espionage Act of 1996 makes it a crime to take, download, receive, or possess trade secret information. (Companies will find it in their best interest to develop new policies and procedures devoted exclusively to avoiding liability under EEA.)

Mr. Cocchiarella ended his presentation by summarizing the main points, namely:

1. Information Protection is a complex topic!
2. The majority of intruders are specialists in specific areas (Operating Systems, Network, Phone Systems, Viruses, Encryption, etc.)!

3. You, your company, and our country is at risk!
4. Malicious and/or Disgruntled Employees may be one of your highest risks!
5. Most hackers are looking for the "easy targets."
6. You can protect your systems - and you are strongly encouraged to do so immediately!

7. Awareness, Education, and Policy are the first steps.
7. Assessment and Evaluation are next.
8. Prioritization, Planning, and Implementation.
9. Have a "Disaster Recovery" Plan/Policy.

10. "Walk the Talk!" – don't just talk about installing secure systems, do it!
 11. Schedule Regular Re-evaluations - Networks are changing rapidly!
- If you wish to learn more about Mr. Cocchiarella's experience or Pareo Inc., please contact him at 612-371-0400 or by visiting their website www.pareoinc.com.

MnIPS Officers 2001

President
 Dennis Cummings (W) 651-205-2632
 Vice President
 Kurt Linberg (W) 612-252-4335
 Past President & Programs
 Joe Perzel (W) 612-340-1110
 Marketing
 Joe Reilly (W) 612-513-5951
 Treasurer
 Gerry Lindner (W) 651-292-9304
 Secretary
 Bob Burkert (W) 952-888-1108
 Arrangements
 John Belich (W) 651-634-1440

Newsletter Editor
 Earl C. Joseph (W) 651-290-2846
 Education
 Haziel Matias (W) 612-627-2171
 Summer Golf Outing
 Jeff Hemauer (W) 651-766-1387
 Audit & Bylaws
 Dave Farmer (W) 651-637-2568
 Special Projects
 Bill McTeer (W) 612-333-4115
 Data Base
 Adair Mariana (W) 612-359-4960

MnIPS Newsletter
 P.O. Box 201243
 Bloomington, MN 55420-1243

Address Service Requested

DINNER MEETING
 Tuesday, May 15, 2001 – 5-8PM
TOPIC
**“Cool Robots
 and What They Do”**

NOTE: Meeting Location
 Holiday Inn Bloomington
 35W & 94th (1201 W. 94th St.)

