ITS eNews R·I·T
Information & Technology Services at the Rochester Institute of Technology

Managing Desktop Computers

By Dave Pecora, Associate Director, ITS, dave.pecora@rit.edu

(Author's note: For purposes of this article, the term personal computer or PC refers to all desktop computers regardless of operating system. While I am a Windows user, I assure everyone that I am Macintosh (and Linux) friendly).

If the personal computer were a person, it would be living a most interesting life. Born in the late 1970's, PCs exploded in usefulness and popularity in the early 80's. Companies that were started in basements and garages eventually became multi-billion dollar enterprises. In 1982 "The Computer" was named Time Magazine's Man of the Year, a testament to the importance of personal computers in daily life. (To date, no other object has been so honored, although the TiVo box in my house may soon be nominated). After settling into what seemed like a comfortable societal role in the early 90's, PCs once again boomed as the Internet finally ushered in the Information Age.

PCs started essentially as personal devices. And despite the remarkable changes personal computers have had on our lives, PCs themselves have changed very little. Yes there have certainly been breathtaking advances in speed, power, and storage, however PCs basically work the same as they did in the early 80's. All of them have a CPU, memory, and storage functions, as well as keyboards, mice, and monitors.

What has dramatically changed, however, is how PCs are *used*. These personal devices eventually grew up, evolved, went into the workplace, and changed organizations forever. PCs grew like weeds throughout businesses and other organizations because they offered the potential for huge productivity increases.

Complexity and the desire for efficiency eventually forced corporations to adopt a managed model towards the support of PCs. These factors and a commitment to information security are forcing many universities to review their support model today.

A New Support Model

Within higher education, computers have certainly changed *us*. But most universities have not changed how we support *them*.

Many universities still use what I call the "CompUSA" model of desktop computer support. Support organizations that use this model relate to their customers much like a computer store

would relate to a customer. Go into any CompUSA store and you'll generally find a friendly and (usually) knowledgeable representative available to help you. A good rep will talk to you about your needs, help you choose a system, and assist with selecting the options that are right for you. They'll give you instructions on how to set it up, and a phone number to call if you need help.

All of which is great, but after the initial system set-up you're basically on your own. Keeping your operating system and anti-virus software working and up to date is completely up to you. The same goes for installing software to protect your computer from spyware, or running system scans to find and clean viruses.

With increased attention and concern on information security, it's clear that universities need a new model when it comes to the support of personal or desktop computers. Universities must take a page from the corporate playbook and move to a *managed* model of workstation support, with some important differences. Universities must implement managed support in a manner that preserves the flexibility so important to institutes of higher education. Managed support must enhance the university's mission – not contradict it.

How the Managed Support Model Works

"Managed" means several things when applied to desktop computer support. First and foremost, it means that critical security updates like operating systems patches or anti-virus updates are managed centrally, and pushed to the workstation. Desktop applications like Microsoft Office can also be updated and patched via a central service.

Most organizations that move to this model do so with the help of software that can manage and report on the configuration of desktop computers. Such software typically works via an agent that runs on the desktop machine and communicates with a central server. Commands at the server level can then be issued to the desktop – to patch an operating system or update a desktop application.

One of the most important advantages of the managed model is that it dramatically reduces the need for many individuals to have administrative rights on their desktop workstations. Currently, most faculty and staff have administrative rights on their desktop computers, as this has historically been the only way they could install and run the software they need. Having many or most employees with administrative rights on their desktop systems has become a liability – not an asset – for security reasons. A managed model – with the proper set of tools in place – will allow systems administrators on campus to deliver desktop services effectively and efficiently without the need for end-user administrative rights.

Getting There

The path to a managed model will not be easy – few things worth doing are. ITS has formed a team to manage the initiative, and has worked with others on campus to set a few high level goals for the project:

1. Any solution implemented must be cross-platform, which means it must be able to manage the three main brands of desktop operating systems: Macintosh, Windows, and Linux. This does not necessarily mean that a single product will accomplish this best – a

best-of breed approach using more than one software package might turn out to be a better option – but a single software solution that meets the needs of the environment is certainly desireable.

2. While the solution will be centrally hosted, it must allow for distributed management, which means it can be used by system administrators across campus to manage the desktops under their charge, not just within ITS. One of the strengths of our campus has been the deployment of consolidated but cooperative technology management – our Active Directory implementation is an example of this. A solution must allow for distributed management to be a good fit for RIT.
3. A good solution must also allow for flexibility and service… along with security. By allowing for the responsive installation of approved software without end-user administrative privileges, a good solution will allow us to improve service and security – not be forced to choose between them.

After completing research on which software products are market leaders, what other universities are doing, and identifying requirements, the team decided to focus on three products: LANDesk, Altiris, and Microsoft SMS (with a plug-in from Vintela to manage Mac workstations). These products are well-established market leaders, and all offer the ability to manage Windows, Macintosh, and Linux systems with a single product. A call to an industry expert with Gartner Inc. strongly confirmed this direction. Product evaluations have begun.

Some areas at RIT have made strides in moving towards a managed model. Their work will make a university-wide managed model easier to achieve. The Finance and Administration Systems Team (FAST) has implemented a locked-down managed model for its desktop computers using Microsoft Active Directory (AD) and Global Policy Objects (GPOs). The College of Business recently purchased and implemented LANDesk to manage the laptop computers given to students in the Executive MBA program. ITS Distributed Support Services (DSS) system administrators use Altiris to manage laboratory computers in several colleges, including the College of Engineering, the College of Science, and the College of Liberal Arts.

More communication will follow as this exciting initiative develops. For more information about the project, feel free to contact me at Dave.Pecora@rit.edu. myMessage Center Coming Soon!

Streamlining RIT Communications through the myRIT Portal Underway

By Brenda Lunham, ITS Sr. Project Manager, brenda.lunham@rit.edu

Have you ever felt overwhelmed by your email? ITS is developing a new portlet for the myRIT Portal called the Message Center. The initial phase of the new Message Center project will be rolled out in the next several months and is part of a larger vision to provide you with control

over what communications you receive and how you receive them. One of the primary objectives of the Message Center is to be a trusted source of communication.

The initial phase will replace the current ALLSTAFF and ALLSTUDENT email distribution lists. The ALLSTAFF and ALLSTUDENT are used for the institute communications to the RIT community (parking and safety, institute closing, etc.). The RITSTAFF is used for individual communications to the RIT community who subscribe to RITSTAFF (e.g. retirement party, lecture series, etc.). The RITSTAFF will remain intact.

The information you currently receive through ALLSTAFF and ALLSTUDENT will be sent through Message Center. Each message will be assigned a category. Some categories will be mandatory for you to receive, such as Institute Emergency Notifications, while other categories will be optional. You will have the ability to opt in or opt out of each of these optional categories. You will also have the choice to receive each message category either by email or via your personal message board in the *my*RIT portal.

At the present time, over half of the students forward their RIT computer account to an outside Internet Service Provider (ISP) such as AOL, Yahoo, etc. As you probably know, any message you receive via an ISP can be flagged as SPAM. After a certain number of ISP subscribers have flagged messages from the same message sender as SPAM, the ISP will block all mail from that sending mail server.

Unfortunately, this has happened to RIT mail servers because students were unable to easily identify the message as an RIT message that they had agreed to receive. The Message Center will attach a 'footer' in each message indicating the source of the message and instructions for how to "opt out" if the communication category is an optional one.

When the Message Center goes live, there will be no action required on your part. You will receive an email telling you how to personalize your preferences. If you decide not to set up your preferences, you will continue to receive all communication categories via email just as you receive them today. You will be able to set your preferences using the myRIT portal. Instructions for setting your preferences will also be posted there.

As you begin to use the new Message Center, we will be looking forward to hearing from you. We'll use your feedback to help us build additional features and functions for future releases.

Secure Wireless Networks: Separating Myth from Reality

By Michelle Cometa, ITS Administrative Services, michelle.cometa@rit.edu

Incorporating emerging technologies on campus is part of the role of ITS. Evaluating the best technologies for campus use, ensuring they are secure applications, or providing adjunct applications to secure the network also is a big part of ITS' role. This article includes one such emerging technology, wi-fi protected access or WPA. It is not necessarily a new technology, having been around for three years, but it is the forerunner for newer wireless security

mechanisms. ITS is exploring the logistics of how this technology could improve wireless access for campus users, as part of the developing RIT wireless network.. – ed.

Anytime, anywhere access to email and the Internet makes wireless devices very appealing. It is all too common to see people chatting into mobile phones, tapping Blackberrys and working on their laptops in Internet cafes. The wireless technology landscape is changing as more individuals and companies look to secure their network traffic. Use of authentication and encryption protocols has evolved in such a way that reliable security over wireless networks can take place.

There are myths however, about some of the newer wireless protocols being implemented for both home and enterprise networks. More is being heard about WEP, WPA, WPA2, - and the acronyms are only the tip of the 'information' iceberg about each of these wireless security protocols. Let's back up for a moment, and define some of the terms being used about these wireless technologies and their ability to provide varying levels of data integrity over wireless networks.

Wired Equivalent Privacy (WEP) was one of the first iterations of wireless encryption. While access via wireless simplified work for telecommuters, for example, the security using WEP was poor. Users need to take care with the information they access and the information they send across unencrypted or WEP encrypted wireless networks, said Greg Gardner, Manager of Communication Services. It's easy for passwords to be detected and other information keyed-in to be acquired by other people on the wireless network.

Weaknesses in WEP prompted improvements and the next iteration of securing wireless systems was Wi-fi Protected Access, or WPA. It is part of the evolution of wireless security that can be used to protect data as it passes from mobile devices to access points and back again. It is a modification and improvement to WEP.

"WPA is a rework of many things that were originally bad about WEP," said Gardner. "Enterprise WPA has not been cracked in the three years it has been out – but who knows how much longer this will be." WPA is enabled by configuration in access points and in client devices such as laptops or handheld devices.

WPA has come under fire of late and some challenge the premise that it qualifies as protected. "Although home configurations of WPA with shared keys have been shown to be vulnerable, WPA has not been cracked at the enterprise level," Gardner said. He noted too, that while WPA has a strong track record of security so far, this might change in the near future as hackers and hacking tools become more sophisticated.

"WPA, when properly installed, provides users of wireless local area networks (WLANs) with a high level of assurance that their data will remain protected and that only authorized users can access their networks. (Wi-fi Protected Access, 2005)

Never too far out of the conversation about WPA is the most current development in protected access, WPA2, which makes use of industry standard Advanced Encryption Standard (AES),

said Gardner. This advanced encryption technology is satisfies government standards for encrypting information and is used by key departments in the US government. “The hardware requirements for AES are high,” said Gardner, “so most current wireless cards, client hardware and access points will not be capable of handling WPA2 .”

Links within this article go to the Wi-fi Alliance, the first organization to detail standards for security over wireless technology. More information about the Alliance, WPA, WPA2 and wi-fi technology standards can be found at: http://www.wi-fi.org

Avoiding Identity Theft: Detecting Online Scams and Phishing

By Ben Woelk, Information Security Office, ben.woelk@rit.edu

Dear Pay Pal User,
We’ve recently noticed one or more attempts to log into your account from a foreign IP address. If you did not initiate the logins, please visit Pay Pal at: http://paypal-secure.com
Thank you,
Pay Pal Security

Have you received an email like this? Did you click on the link and enter login information?

You’ve been phished!

According to a 2003 RIT Computer Use and Ethics survey, nearly 200 of the student respondents have been victims of some sort of computer abuse, including identity theft through phishing scams.

Phishing is a commonly-used technique in identity theft. We’ve all received phishing emails or instant messages that appear to link to a legitimate site. These emails and web sites are designed to capture personal information, such as bank account passwords, social security numbers and credit card numbers.

Email phishing started to become a serious problem in August of 2003. Since that time, it has grown astronomically, with phishing emails peaking in May 2005 at more than 9,000,000 attempts (Message Labs Intelligence, November 2005). Losses to phishing attempts may be as high as $500M (Truste) to $2.4 billion (Gartner, Inc.) every year.

How does phishing work? A typical phishing attack follows the following steps:

- Phishers send out millions of emails disguised as official correspondence from a financial institution, e-tailer, ISP, etc.
- You receive the phish in your email.
- After opening the email, you click on the link to access your financial account.

- Clicking on the link takes you to a web site that looks just like a legitimate site.
- At this point, you enter your account and password information, which is captured by the person who sent out the phish.

Phishers typically attempt to impart a sense of urgency, urging you to act quickly to address the problem referenced in the phishing email. Phishing emails used to be easy to recognize because of their poor spelling and grammar. Now phishing emails are often indistinguishable from official correspondence.

Phishing web sites, linked to from the email, may also be difficult to distinguish from legitimate sites, because of their use of these techniques:

- **URL masking**—phishing emails may display a link that appears to go to one site, but in reality goes to another.
- **Copying of official email**—phishers may simply copy an official email from a bank or retailer, and edit that email for their own purposes before sending it to you.
- **Cybersquatting**—phishing sites may rely on similar URLs, such as googkle.com, ebay-secure.com, upgrade-hsbc.com to fool users.
- **Use of @symbol**—the phishing URL may include the @ symbol somewhere within the address. (When reading an Internet address, browsers ignore everything to the left of the @ symbol, so the address ebay.com@fake-auction.com would actually be "fake-auction.com.)

Phishing techniques are becoming more difficult to detect as phishing attempts become more complex. Some links may actually send you to a legitimate site, and use some other vulnerability to capture your information. Be suspicious of every email!

There are a number of utilities available to help warn you of suspicious web sites. Install and use one or more for your protection.

- The **Netcraft Toolbar** displays information about a web site including whether it is new (typical of phishing) and which country hosts it. The Netcraft Toolbar also works like a neighborhood watch community, blocking access to reported phishing sites.
    - http://www.netcraft.com

- The **Google Safe Browsing Extension** will warn you when a "phishy" site has been detected, and block you from entering information into the site.
    - http://www.google.com/tools/firefox/safebrowsing

- **Earthlink ScamBlocker** provides an easy-to-see security rating for each web site you visit, based on a blacklist of fraudulent sites.
    - http://www.earthlink.net/software/free/toolbar

However, these technical tools are not going to prevent you from being victimized. In the end, you must decide if an email or web site is fraudulent. Keep these tips in mind when reading email and visiting web sites:

- Never click on links directly from an email! Type the address into the address bar or go to the institution's web site and navigate to the correct location.
- Check the properties of web pages before entering information. You can check the properties from the file menu or by right-clicking on the web page and selecting properties.
- Secure web sites use a technique called SSL (Secure Socket Layer) that ensures the connection between you and the web site is private. This is indicated by "https://" instead of "http://" at the beginning of the address AND by a padlock icon which must be found either at the right end of the address bar or in the bottom right-hand corner of your browser window. A padlock appearing anywhere else on the page does not represent a secure site.

For more information, visit the Information Security web site at security.rit.edu to read the security standards, get the schedule for our Digital Self Defense workshops, or find out more ways to protect yourself. If you have any questions, feel free to contact RIT Information Security at infosec@rit.edu.

New CAST Building Breaks Ground

Rosica Family and McGowan Foundation Recognized for Supporting State-of-the-Art Telecommunications Facility

By Michelle Cometa, ITS Administrative Services, michelle.cometa@rit.edu

Another building will be added to the campus family after groundbreaking September 19 for the new CAST Engineering Technology Building. A centerpiece of the new building will be the William G. McGowan Center for Telecommunications and McGowan Student Commons.

Representing the William G. McGowan Foundation, Mrs. Lenore Rosica, addressed the standing room only crowd at Golisano College about the opportunity to set new standards for telecommunications technology at RIT. "This is an outstanding opportunity to honor my brother, Bill, and the future of telecommunications education. The field of telecommunications will be forever changed," she said. "RIT will set a new standard for scholarship. Future practitioners, scholars and entrepreneurs will embark on their careers through the McGowan Center."

Groundbreaking participants, left to right, Klaus Gueldenpfennig, RIT Board of Trustee member and REDCOM Laboratories president & chairman, CAST Dean Wiley McKinzie, Dr. Al Simone, Mr. Michael Morley, RIT Board of Trustees chairman and Mrs. Lenore Rosica, trustee of the William G. McGowan Foundation *Photo by M. Cometa*

More than 38 years ago, William McGowan founded MCI Corporation. The company grew, transforming the telecommunications industry from monopoly to competitive landscape, said Mrs. Rosica about her brother. William McGowan led technology innovation and believed that "tapping the minds and spirits of young people" would help them realize their potential in the ever growing and changing industry, she added.

This marked a special day for ITS as well. Dan Rosica, manager of ITS Distributed Support Services, stood proudly with his family, wife, Keely, daughter, Megan, father, Sebastian, brother Mark, associate professor and member, Counseling and Academic Services (NTID) and children, as his mother, Lenore, participated in the groundbreaking for what will be one of the premier telecommunications technology centers in the U.S.

The Rosica family, representing the William G. McGowan Foundation, left to right, Diana Spencer, executive director of the Foundation, Francesca Brand, Marianne Brand, Lenore Rosica, spokeswoman and trustee for the Foundation, Keely Rosica, Megan Rosica, Mark Rosica, Daniel Rosica and Sebastian Rosica. *Photo by M. Cometa*

The new $8.5 million, 33,600-square-foot building will be constructed adjacent to the B. Thomas Golisano College. It will house the students and faculty, high-tech programs and laboratories from Electrical, Computer and Telecommunications Engineering Technology, Civil Engineering Technology, Environmental Management and Safety, Manufacturing and Mechanical Engineering Technology and Packaging Science. Construction will begin shortly and is scheduled for completion in December 2007. The building will officially open spring quarter of 2008.

Considered a “college of innovation,” CAST has cutting edge, applied technology programs giving students “a competitive advantage for a lifetime,” said Carol Richardson, interim dean of CAST. She was recently named to this position as Wiley McKinzie, dean of the college for the last 19 years stepped down to pursue other opportunities within CAST and RIT. He received a standing ovation from the crowd gathered at the event for his efforts over more than 35 years at RIT and to spearhead the development of this new building project.

The CAST Building’s first benefactor, the McGowan Foundation, contributed $2 million which will be applied to the new telecommunications center as well as a student commons. An artist’s rendering of the facility shows a multi-level, atrium area surrounded by classrooms, open walkways and laboratory areas.

The McGowan Student Commons will be the centerpiece of the School of Engineering Technology Building.

(Graphic retrieved from http://www.rit.edu/~umagwww/fall2004/TeleFac.html part of the online version of the 2004 issue of University Magazine, recognizing the grant launching the new telecommunications facility.)

Each of the presenters at the groundbreaking ceremony expressed gratitude for the generous contribution of the McGowan Foundation. Without their support the building that will house for the first time all the CAST departments could not have been constructed. “The private funding for this facility was pivotal,” said Dr. Al Simone. “We are grateful for your support and confidence in RIT.”

As ground was broken and participants gathered to celebrate another milestone for RIT and CAST, the Rosica family greeted the RIT family. Congratulations on this newest addition to RIT growth. In Lenore Rosica’s words, “There is a very bright future for telecommunications students at RIT.”

More information about William G. McGowan and the charitable fund behind his name can be found at http://www.mcgowanfund.org/ It is a wonderful story of the pursuit of the American dream and the ability of one person to influence an industry as well as education.

http://www.rit.edu/~umagwww/fall2004/TeleFac.html

Additional sponsors for the new CAST Building are: Choice One Communications; Joseph P. Clayton; Eastman Kodak Co.; Fibertech Networks; Melles Griot Optical Co.; Mitel Networks Inc.; REDCOM Laboratories Inc.; Rock-Tenn Co.; LaBella Associates PC; LeChase Construction Services LLC; Parrone Engineering.

Google Jockey: Reining in Student Energy

By Donna Cullen, ITS Computer Policy Analyst, donna.cullen@rit.edu

You are standing in front of a classroom wishing for the days when a baseball cap was the only thing between you and making eye contact with your students. Laptops, ostensibly open so that the students can take notes, are engaging the students in email, reviewing notes for the quiz in the next class, adding to a paper in progress, and Instant Messaging (IM) sessions. A few of the students may be privately engaged in searching for additional material associated with your lecture – a definition, an opposing view, an illustration.

Along comes *Google Jockeying* -an innovative approach to incorporating the private research already going on. During class time, a faculty member appoints a "jockey." The role of the jockey is to use a laptop to look up the contents of a URL you provide or do parallel Google searches to help expand the information related to your presentation. The work of the jockey is displayed on another screen in the room so that all the students benefit from the findings.

Google Jockeying helps to rein in some of the attention and multitasking energy of the students. Other students in the class use IM to provide URL suggestions to the jockey. One of the tasks of the jockey may be to email the class with all the resources found during the class.

Is *Google Jockeying* the answer for your classroom? There are a number of factors to consider.

- **Projection -** Is your classroom outfitted with enough screen space to make the extra projection practical? Are you projecting materials – if so, you will need an additional projector for the display of the jockey's findings.
- **Searching –** Students' search skill sets can vary widely. Be prepared with URL suggestions to get a student started. Class time or remedial time might need to be scheduled to bring a portion of the students up to speed on the concept and on searching. Some faculty have assigned jockeying to a teaching assistant or a student they have identified as having the needed skills.
- **Evaluate –** Not all techniques work for you, for a particular class of students, or for a given topic. In other words, *Google Jockeying* might be just the technique you were looking for to enliven your lectures and stimulate your students. It could also overwhelm your students or slow down your progress in a course.

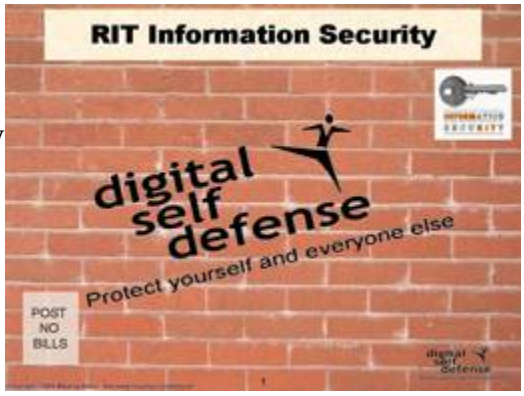
The EDUCAUSE Learning Initiative published an overview of *Google Jockeying* in May 2006. The article includes references to sites that are using or experimenting with the technique. The article can be accessed at http://www.educause.edu/LibraryDetailPage/666?ID=ELI7014

The next time you catch your students "horsing" around in class, consider "reining" them in by appointing a "jockey." Your "bet" on this technique may have you "winning the race."

[home]

Changing the Culture—Digital Self Defense and Freshman Orientation 2006

By Ben Woelk, Information Security Office, ben.woelk@rit.edu



Did you know that more than half* of the RIT student body will be victims of some form of computer abuse?

One way to decrease the likelihood of victimization is by providing incoming students with the tools they need to use the RIT network successfully and safely. We can do this by creating a culture that has a heightened awareness of information security threats.

Digital Self Defense helps create this culture by equipping students with the tools and knowledge they need to protect themselves and everyone else. This year, the RIT Information Security Office Digital Self Defense (DSD) team presented DSD sessions to all incoming freshmen at Orientation, staffing 18 different sessions and reaching more than 2,500 students.

Our goal for the sessions was to introduce students to the requirements of the Desktop and Password Standards, help them balance paranoia and common sense, and urge them to practice ethical computing. topics included Phishing and Identity Theft, Internal and External Threats, Cyberbullying, Safe Blogging, and Legal vs. Illegal File Sharing. (You can view the presentation at security.rit.edu/articles/students.ppt

Our thanks to everyone who volunteered as presenters—an All-Star lineup consisting of Dave Pecora, Dave Ballard, Donna Cullen, Tom Dixon, Nick Francesco, Denise Lake, Bob Parmalee, and Joel Yates joined the RIT Information Security Office in delivering the sessions. We couldn't have done it without you! And a special thank you to Kerry Hughes and the Orientation Office for including us in their program.

* *RIT Computer Use and Ethics Survey*, 2003

ITS Technology Seminar Series Opens October 24

Technology Careers, Security and ID Management to be Featured

By Michelle Cometa, ITS Administrative Services, michelle.cometa@rit.edu

The ITS Technology Seminar Series returns for the 2006-2007 with three featured programs by well known names in the IT field today. The annual seminars are part of an ongoing series of professional programs sponsored by ITS to keep the campus up-to-date about technology issues, solutions, practices and emerging technologies.

The first ITS Technology Seminar features **EDUCAUSE Vice President, Cynthia Golden, editor of the recent E-Book, *Cultivating Careers: Professional Development for Campus IT* .Golden will be on campus for a presentation on Tuesday, October 24, 11 a.m. – 1 p.m. in the Golisano Auditorium.** Her session is about the special demands of continuing education and training for IT professionals within academic settings, how to succeed in cultivating current talent and creative ways to provide training for IT staff.

Cynthia Golden coordinates the content of all EDUCAUSE professional development activities as well as the association's e-content and knowledge management initiatives, and has general oversight of information technology services and strategies within the association. Prior to joining EDUCAUSE in the summer of 2001, she served as Executive Director of Computing and Technology Services at Duquesne University, where she had been the CIO since 1998. Before coming to Duquesne, Golden was manager of business applications in the Information Systems division at MIT, where she also coordinated administrative computing architecture. She was Associate Director of Administrative Systems at Carnegie Mellon University before joining the staff at MIT.

On Monday, November 6, Steve Worona, Director of Policy and Networking Programs, EDUCAUSE, will come to RIT to present, *ID Management: Balancing Security and Privacy in Times of Cyber Terror*. His session takes place from 11 a.m. to 1 p.m. in CIMS 2230-2240.

After more than 30 years at Cornell University, Steve Worona joined EDUCAUSE in 2001 as Director of Policy and Networking Programs. He taught courses in both the Computer Science Department and Graduate School of Management, and co-founded Cornell's Computer Policy and Law Program, which is now the EDUCAUSE/Cornell Institute for Computer Policy and Law. He has lectured internationally on a wide range of topics, focusing most recently on the impact of technology on our social and legal system. With EDUCAUSE, his responsibilities include programs in such areas as leading-edge authentication systems, computer and network security, intellectual property policy, and management of the .EDU top-level Internet domain. He holds degrees in Philosophy and Computer Science from Cornell.

In February, Dr. Keith Hazelton, IT Architect, from the University of Wisconsin-Madison, and member of the Internet2 Middleware Architecture Council for Education (MACE), chair of the MACE-Dir Working Group, and a member of the Net@Edu PKI Working Group sponsored by Internet2 and Net@Edu. He will discuss Understanding Middleware Technology. His program takes place, Tuesday, February 13, 10 a.m. – noon in Golisano Auditorium.

Keith Hazelton is Senior IT Architect at the University of Wisconsin-Madison and works half-time for Internet2 as a charter member of the NSF-funded Middleware Architecture Committee for Education (MACE) and chair of its directory working group, MACE-Dir. He concentrates on middleware infrastructure issues and is a frequent speaker and panel member at Internet2, Common Solutions Group,

Educause and other venues.

All seminars are free and open to faculty, staff and students. To register, email macits@rit.edu. More information about the seminars will be posted on the ITS website. Some background information about the EDUCAUSE e-book, *Cultivating Careers* can be found at http://www.educause.edu/cultivatingcareers
Information about the Internet2 Middleware Initiative can be found at:

http://middleware.internet2.edu/

ITS Organizational News

New Customer Teams Announced; Tobin Promoted to Director of Infrastructure

Dave Pecora, Associate Director of Customer Support Services (CSS) announced the development of a new **Desktop Engineering** team to be led by Dan Swab. Swab, former team lead for Resnet, has been with ITS for more than 5 years, managing the residential computer support group based in Nathanial Rochester Hall.

The mission of the Desktop Engineering team is to research and deploy tools to better manage the workstations of our customers, improving efficiency and security. The Desktop Engineering team will provide an additional avenue of escalation for desktop problems, and will work closely with our customers, Technical Support Services, other areas of Customer Support as well as different departments within ITS. Jeremy Reichman and Shawn Thomas will be on the Desktop Engineering team, and will report to Swab.

Resnet and **Desktop Support** have been consolidated into a single Desktop Support – Operations team, led by Vince Incardona. The mission of the Desktop Support – Operations team is to provide high quality, day-to-day desktop support service for students, faculty, and staff, both on the residential and administrative side of campus. Tom Dixon, Charles Hall, Cheryl Williams, and the CS co-op will report to Vince Incardona.

As part of this overall transition, calls to the Resnet phone line (5-2600) will be taken by ITS HelpDesk staff starting December 4th, the first day of Winter quarter.

Emilio DiLorenzo, Associate CIO announced the promotion of **Dan Tobin to Director of Infrastructure Support Services**. Dan has been with ITS for 5 years, serving as Associate Director of the Technical Support Services group. Tobin will manage all infrastructure projects supported by the TSS group, giving operational direction and supervision.

Tobin was instrumental in the recent integration of the Telecommunications Services and Data Network Support teams into a single organization named Communication Services. He also helped establish a separate Infrastructure Engineering team. The Infrastructure Engineering team is a multi-disciplinary group with four members whose primary function is to support and execute the ITS Infrastructure strategy: analyze emerging technologies that can be of value to RIT and develop an action plan to implement the selected technologies for campus.