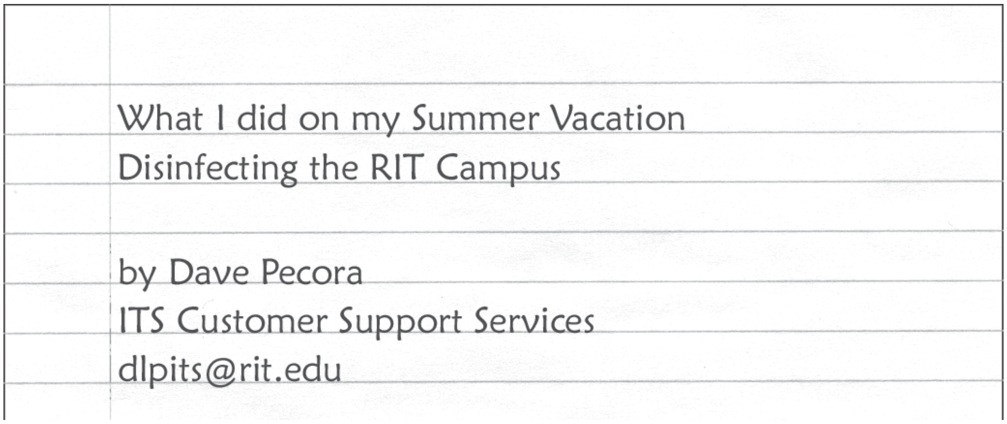
ITS Information & Technology Services
ITS news

The official source of news from ITS Information & Technology Services

December 2003



What I did on my Summer Vacation
Disinfecting the RIT Campus

by Dave Pecora
ITS Customer Support Services
dlpits@rit.edu

Universities are great places to work in general, but especially during summertime. This past summer started out as no exception. As the campus slows down, projects for fall heat up. For most of the weeks of June and July, ITS worked on projects like email and directory services, and we began to intensify our focus on student move-in.

Move-in week is a critical time for ITS, as it is for many organizations on campus. Prior to 2002, move-in weeks were far and away the busiest time for the ITS HelpDesk. Lines of students would typically start at the HelpDesk in building 7B and wind through the hallway as students stood patiently with the paperwork necessary to obtain an RIT computer account. Thanks to an automated account generation process, students arriving on campus during move-in week of September, 2002 already had accounts; they just needed to activate them. Postcards were sent over the summer and many students had active accounts before arriving on campus. Those that needed activation were easily handled. Move-in 2002 went without a hitch. As Fall 2003 approached, we were confident that this years move-in would also go well.

On Tuesday, August 12, summer officially got interesting. I received a call that day from one of our network administrators. He was monitoring the traffic on some of the servers hosted within the ITS data center. He began to see something disturbing; increased "port scans" were coming from other computers on the network. Ports are like windows or doors on a computer – an open port is like an open door on a house; it can allow an intruder access to a computer. Scanning for open ports is a common technique used by hackers looking for vulnerable computers. Firewall software on ITS servers was picking up an increasing level of port scans.

The most disturbing aspect of these port scans was not the impact they would have on ITS servers. ITS servers are protected by firewall software, as are most other servers on campus. Much more disturbing was the source of the probes: computers on the RIT campus network were doing the scanning. After some quick research, we quickly discovered that these computers had been hacked themselves; many had what would be later called the Blaster virus.

continued on page 5

Focusing on Network and Individual Security

By Diane Barbour, Chief Information Officer, dhbcio@rit.edu

There is good news and bad news.

The good news is that RIT has a robust, state-of-the-art, both wired and wireless campus network. The bad news is that this robust network infrastructure makes RIT especially vulnerable to attacks and network abuse.

Our recent experience with the battles against the various viruses and worms as well as bandwidth abuse such as peer to peer file sharing of copyrighted materials, has prompted the need for more formal and permanent security strategies. ITS is implementing a variety of security tools and strategies such as firewalls, bandwidth management, intrusion detection and prevention.

Like every institution of higher learning, we need to provide an open, collaborative working and learning environment for students, faculty, and staff. At the same time we need to protect ourselves from attacks that permeate the network.

This issue of ITS News is focused on Security. The issue includes ways that you can help to keep our working and learning environment safe and secure. During the month of December (Dec 8- 12), ITS hosts a SECURITY WEEK. I urge you to participate in the events of that week.

Worldwide, IT security spending was 20 billion in 2002. Security spending is projected to hit 30 billion in 2004. The cost to ITS alone for the most recent security incident was over $130,000 in staff and general resources. We all need to pay attention to security. Security threats will continue as the Internet continues to mature.

Be Safe and Secure.

In This Issue

“Microsoft Exchange” is trademark of Microsoft Corporation

Using Technology to Improve Learning

By Joeann Humbert, Director of Online Learning, jmhetc@rit.edu

This fall quarter, the Online Learning department started a Blended Online Learning Pilot Project designed to develop and promote the use of instructor-led online teaching and learning activities to replace some classroom activities. As mentioned last month in the ITS newsletter, one of Online Learning's goals is to enhance the teaching and learning experience with new educational technologies that meet the learning needs of today's students.

Four Unique Courses Adopt Blended Learning

Four professors, teaching what were five traditional classes, are participating in the project this Fall quarter. They have successfully adopted a variety of online educational strategies ranging from online team projects to whole class discussion forums to in-class and out-of-class chat. All these strategies are supported in the RIT myCourses course management system (CMS).

It's interesting to note that these four courses are quite different from each other. They include: two undergraduate-level courses: "The History of Modern America" taught by James Revell and "Ethics of Information Technology" taught by Catherine Irving, and two graduate-level courses: "Operating Systems for Telecommunications" taught by Tony Trippe and "Psychology/Sociology of Adolescence," with two sections taught by NTID professors Sara Schley and Michael Stinson.

Survey and Usage Reveal Positive Outcomes

Between weeks three and four of the fall quarter, we surveyed all the students (nearly 100% responded) in these courses about their experiences using educational technology. Here are some of the results of that survey:

- The vast majority of students said they possessed the computer skills necessary to use myCourses effectively.
- Sixty-two percent agreed that they received adequate information about the technology, 18% were undecided, and 18% said they did not get enough support. (We have since developed steps to improve learner support services.)
- Seventy percent said they did not experience any technical problems, 6% were undecided, and 22% said they did experience problems. (Online Learning and ITS are continually looking for ways to improve performance of myCourses.)

The asynchronous discussion board is the primary instructional tool used in the online portion of the blended courses. The same is true with our distance learning courses. Overall, the student and faculty comments from these courses reveal that the myCourses system works well, is easy to use, helps students organize their thoughts and class impressions more accurately, helps faculty to accurately assess both small-group and entire class discussion, and ultimately facilitates an improved level of learning. These results are consistent with the recent research findings.

Research in the Field Helps Guide RIT

Much of the research being conducted by the State University of New York Learning Network (SLN) reveals that online distance students learn more if three factors are in place for any given online course: consistency in course design, contact with course instructors, and real communication through discussion. The RIT Blended Learning Pilot Project emulates these three design factors. The SLN has been surveying students for over three years and the purpose of the research examines levels of distance learning student satisfaction at 53 SUNY campuses that currently offer online courses to more than 53,000 students.

Call for Participants

The Online Learning Department is seeking additional faculty participants in the Blended pilot for the upcoming spring and fall quarters. If you would like to participate in the pilot, please contact Michael Starenko at 5-5035 or e-mail at mssetc@rit.edu.

You're Invited to Our Upcoming Workshops

Peter Shea, director of the SUNY Learning Network, is coming to RIT to share his insights regarding student perceptions of online learning. On January 9, 2004 Shea will be the keynote presenter at an Online Learning Department luncheon workshop to be held in A-400 on the lower level of the Wallace Library beginning at noon. To register for the workshop, go to online.rit.edu/faculty.

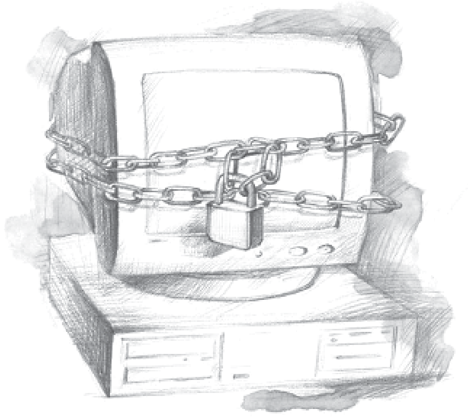
Also to come during the Spring 2004 quarter, Chuck Dzubian, director of the Research Institute of Teaching Effectiveness (RITE) at the University of Central Florida (UCF), will visit with us to discuss RITE's ongoing research that is documenting the success of blended learning at UCF, where both faculty and students have seen increased levels of satisfaction in learn-

continued on page 5

Desktop Defense Project

Are your Windows closed and locked?

by Jack Mangione, ITS Project Management Office, jamits@rit.edu



RIT's infrastructure depends on its networked information systems. Keeping these systems operationally sound, protected and trustworthy is a consistently challenging endeavor. The economics of today's environment dictates using commercial off the shelf (COTS) components whenever possible. The issue here is the increasing use of these COTS components, whose functionality can be unknowingly, extended means users cannot know what software has entered their system or what actions those components might take.

To help improve RIT's information systems and to make sure each system is safe, additional precautionary measures are now required. Viruses, Trojan horses, worms and now blended threats (combination of virus and worm propagation techniques with automated hacking capabilities in separate deadly programs) are becoming even more widespread then before and can be extremely destructive.

While you browse the latest headlines or purchase a cashmere sweater on the Web, some hacker could be lurking in the background, stealing credit card numbers or rifling through the data stored on your system. Simply put, your Internet connection has become a wide-open path to your PC. Anyone connected to the web with malicious intent and technology skills can creep in without your knowledge.

Up until now, anti-virus software was all that was needed to fend off unwanted intrusions. That is no longer the case. Virus checkers can protect only against *"known"* viruses. Even if you regularly update your virus software, there is always a lag between when a virus (or a worm or a Trojan horse) appears and when protection against the virus is available. In the mean time, your computer is vulnerable and can become infected unless further steps are taken.

To protect yourself against these threats, the industry now suggests you do the following:

· make sure your anti-virus software is always up to date
· set up "automatic update" for your operating system - you will need to check the bulletins for additional updates
· implement a firewall technology on each desktop
· implement a scalable tool for anti-virus and security policy management

The desktop defense project was setup to address some of these steps. This project will provide a desktop firewall component and integrate existing McAfee anti-virus software into an overall management ability to ensure consistent and complete protection of your system.

The purpose is to limit exposure and prevent unauthorized executable files from running. If an attacker tries to break into your system, you can elect to ban the malicious address indefinitely. Likewise, you can also place an address in a trusted list so that the firewall will automatically allow access without querying you.

continued on page 12

"With dozens of Windows vulnerabilities that require patching of all enterprise computers disclosed in the last six months," said Gartner's John Pescatore. "It's crucial that companies deploy personal firewalls on as many machines as possible."

Disinfecting the RIT Campus

continued from page 1

ITS was soon faced with the first in a series of difficult decisions. If we took no action, these infected computers would soon find other vulnerable on-campus computers, and the Blaster worm would quickly spread. Or ITS could block these computers from accessing the network, which would slow the spread of the virus but would clearly be disruptive to many people on campus.

By this time, Microsoft had acknowledged the Blaster virus and had issued a patch to its Windows operating system. Antivirus software vendors such as McAfee had also discovered the virus and issued a data file which would detect and clean an infected computer. While these operating system patches and data files were welcome, they also presented a logistical nightmare; how could we deploy these as quickly as possible to over 5,000 institute computers?

With the scanning increasing every hour, ITS decided to act. Our first decision was to block all computers that were the source of the scans from having any access to the Internet. As news of Blaster hit the national level, we also decided to scan and block Windows computers that were not yet infected but vulnerable to infection. This dramatically slowed the progress of the virus on campus. RIT later learned that some campuses that did not act as quickly decided to disconnect from the Internet entirely. The Maryland Department of Motor vehicles was so crippled by the virus one day that they decided to close and send their employees home.

Slowing Blaster to a crawl was certainly a good thing, but it left us with the daunting task of patching hundreds of computers not connected to the network. This meant we needed to assemble a technical team quickly, give them information as to the whereabouts of blocked computers, and equip them with media and instructions required for patching and cleaning these computers manually. And we needed to deal with the biggest issue of all; thousands of computers that were about to return to campus with students as fall quarter quickly approached.

At this point, the technical community across RIT came together to meet every challenge. The ITS systems team quickly developed a system to allow infected and vulnerable desktop computers to be found and fixed. Soon after, ITS developed a system of “quarantining” computers that allowed users to fix their own vulnerable systems but protected other computers from these systems. The HelpDesk took three times the normal volume of calls and somehow lowered their abandoned call rate during the virus crisis. The Golisano College supplied CDs, volunteers, and a high tech lab of over 100 computers. This allowed us to burn over 4,000 CDs for returning students to use to patch their computers before connecting to the network. Residence Life posted notices in residence halls and delivered a CD and notice to each student. System administrators, student employees, co-ops, and staff from all over campus dropped other projects to pitch in to help. In addition, all of these professionals were challenged by the power outage in late August that shut most of the county down for a day.

Plans and strategies are one thing. Difficult situations require great professionals to rise to meet them. The summer of 2003 will be remembered for many things, but my lasting memory will be of how a group of professionals pulled together to avert a crisis.

Using Technology to Improve Learning

continued from page 3

ing and teaching when participating in blended learning courses.

All RIT faculty and staff are invited to attend these workshops.

Don’t forget that we offer our own workshops too. Our online learning specialists will be offering the following workshops this winter: “Assessment—Using Testing to Build Student Confidence,” “Extend you Classrooms Using Online Discussion,” and “Student Groups in myCourses.”

For more information about all of the services provided to faculty by RIT’s Online Learning Department, please come visit us in the lower level of Wallace Memorial Library, phone 585-475-5089 (voice), 585-475-5896 (TTY), e-mail online@rit.edu.

Top Twenty Things to do for Protecting Your Personal Information

By Jim Moore, RIT Security Officer jhmfa@rit.edu and
Jonathan Lane, Security/Risk Management Co-op Student
Warren Carithers, Computer Science Dept.
Maisy Chong, Security/Risk Management Co-op Student

Don't put this article aside. It is estimated that 99% of all network attacks are readily preventable. Don't wait for it to be your turn. You don't have to read this document the whole way through just now, but you do need to read it. Take it in whatever bite (byte) sized chunks that you can.

We are in the middle of a cultural change. This document should help you become a leader in this change. Leading will actually be easier than following in some significant ways. If you don't believe us, then reflect upon what it was (or would have been) like to be a follower in the anti-virus area.

This Top 20 list has items that are not technical in nature. Many people wonder why today's technology cannot solve all technical problems. The short answer is that technology exists for the benefit of people; therefore people, the attitudes they possess, and the ways that they use technology, all have to be addressed. It is the proverbial 3-legged stool. [*We took this idea from a generalization of some technology models called CMMs. This is both an acknowledgement of their good inspiration, and an apology for generalizing it so much.*]

The Top Twenty

1. Assessment

This is a term that security professionals use all the time. It means, "Do you know where you are?" in terms of network security and individual safeguards.

2. Respect Privacy

Respect the privacy and confidentiality concerns of others***, and expect it in return***. This means turning away when someone is typing his or her password. It means asking others to turn away when you are typing your password (you will be doing them a favor by making them aware of privacy.) It means communicating needs for confidentiality. It means reading privacy statements on web sites that you visit, where you enter personal information.

3. Handle Online or Remote Purchases with Care

My current understanding is that whereas credit cards have limits on liability of around $50, debit/check cards even VISA debit cards have no such liability limits. So do not use debit cards for on-line purchases. Also, to make credit cards more secure, some banks, such as MBNA and Discover, are offering "single use" charge card numbers. You go to their site, securely log on, and then get a single use VISA or MasterCard number that you use for a single online or telephone transaction. The transaction goes against your real credit card number, and if anyone intercepts it, or steals it in any way after the transaction, it is no good. This makes online and remote purchases much more reasonable.

4. Use Anti-Virus

Install and use Anti-Virus products (if you use Windows or a Macintosh). **Do you keep it up to date? And if so, how often?** It begins to get really risky if it isn't at least weekly. Viruses spread at incredible rates. Lots of people go to the virus site the first time they sit down at their computer for the day. This isn't extreme; it's merely being careful. Some viruses are programmed to mutate to avoid detection.

5. Use Personal Firewalls

Personal firewalls are a great awareness tool. When you first set one up, allow it to alert you when it detects any attempts to connect to your machine from the Internet. You will be amazed, even if you are on a modem. The next step involves the process of setting up and using a firewall. How do you use a firewall? Usually, the system will ask if you want to add a rule allowing network traffic to or from an application (note: software firewalls ask about applications; hardware "appliance" firewalls ask about ports or services).

6. Locate Valuable Information

Where is your valuable information? If your first response is "What valuable information?" then think of it this way: Information probably has value to you in one of four ways:

a. It is something that you use every day / frequently (e.g. email).

b. It is something important that you are using your computer to track for you (e.g. finances/investments in a spreadsheet or financial program).

continue on page 7

Top Twenty Things to do for Protecting Your Personal Information

continued from page 6

c. It is something that you are working on, such as a paper, project, drawing, etc.).
d. It is information that may not have much value in itself, but its confidentiality has value.

7. Protect Valuable Information

How do you protect your valuable information? This is a process piece. It is part of the wise choices mentioned earlier. You probably realize that for each location you will probably need to know how to protect the information there. You should also realize that something which needs high confidentiality and high availability needs at least two things – one that protects the confidentiality and one that protects the availability. You don't need to do it *all* now. All data needing integrity or availability at the medium or high levels needs to be backed up regularly.

8. Applications Security

Now that you know where you store your valuable and sensitive data, you need to ask the simple question "How do I get at it and use it?" This leads us into the area of application security. The Web is a common interface for so many systems. It may be that your web browser is your most used application to access your most valuable data. Maybe it is your email client. Maybe your copy of an office applications suite is your most used application. Maybe it is your instant messenger (and its address book or buddy list). It is hard to say how people work most frequently.

9. Create Checklist

Create a checklist from your detailed table and your big bucket table. When you get a new piece of information that is valuable, ask the questions about it that are in the details. See if it fits within one of the big bucket categories and see which of the protections apply. Do the protections fit the value of the data?

When determining the category, if you have the ability and the policy to mark it then do so. Label confidential documents as confidential, sensitive, or secret. Label public documents as public.

10. Passwords

This is a special case of the above. Some day, smart cards, biometrics, and other technologies may reduce or eliminate our dependence on passwords, but for now they are a necessity. Software exists that save passwords for you, such as Internet Explorer, Password Officer, and Web Confidential. The best thing to do is to look at how well each product does their job. Go to a search engine and look for comments concerning each. In essence, these programs are a lockbox for your keys used to access protected valuable data. So the password keeper ends up with the total value of all data protected or accessed through passwords.

11. Now Look at Your Vulnerabilities

There are a number of ways to do this. The best are with commercial scanners. Some companies offer a 15-day trial for scanner software for a very limited range of addresses. Download it, or have a very good friend that you trust a lot download it, and run it against your system. See all the "high risk" categories; often they are labeled as "high risk" because an exploit is known. Microsoft Update and BigFix offer services that tell you what to fix and may fix it for you.

12. Update Your System

Keep your system up to date. First, probably most of the vulnerabilities that you discovered in step 10 already have patches out for them. If you think that patching is all straight forward, then look at the vulnerabilities that most often get corporations into trouble (and remember, they have professional systems administrators) at http://www.sans.org/top20.htm. Some of the issues are the same as what we have discussed, like backups, but notice that most of them can be prevented.

What updates won't do. They won't upgrade your operating system. If you have an insecure version of Windows, like 95 or 98, they will not make it more secure by moving to Windows 2000. Which is probably good, since performance/memory/hard disk requirements are different. Applications are treated in a similar manner. If you have Photoshop 4.0, don't expect the update expert to give you Photoshop 7.0. They won't in general make configuration decisions based on security.

What updates will do. They will install newer versions of software. First, newer versions are assumed to fix all holes previously discovered. Second, maintenance and patches are not always available for old versions of software; generally the newer versions get fixed first, and only recent versions get patches.

13. Work from User Account

Don't work in the Administrator or Root account. If

continued on page 11

ITS Technology Seminar Series:

Security Week

December 8-12, 2003

Join ITS for a series of technology workshops to showcase network security issues and how individuals can safe-guard their personal desktop systems as well as contribute to the safety of the enterprise network.

Participants will work with on and off campus "experts in the field" to learn specific techniques and strategies for prevention. The entire week of workshops are a means to encourage participants in the effort to protect their machines and their respective departments and businesses.

All workshops are free and open to faculty, staff and students. Register for as many of the events as you'd like by emailing cioits@rit.edu or go online at: http://www.rit.edu/its/news/news_items/sec_week.html

ITS Technology Seminar: Opening Session, Monday, December 8, 2003

Security Assessment Results: Policies, Practices and Prevention

Opening Remarks: CIO Diane Barbour
Presenter: James Moore, RIT Security Officer
1 – 3 pm
Xerox Auditorium, Kate Gleason College of Engineering

Re-capping this summers' security assessment, Moore will discuss the results, those involved and policies recommended for safeguarding the RIT network.

About the presenters…
Diane Barbour is RIT's first chief information officer leading Information and Technology Services (ITS), the computer and telecommunications network teams for the university.

James Moore came to RIT several years ago from Xerox Corporation and Kodak Research Labs where he held positions in the area of network security architecture. As part of Finance and Administration, Moore's role at RIT is to help establish policies and procedures related to enterprise security.

Tuesday, December 9

Identity Theft

Presenters: Special Agent Steven Petro (ret.), United States Secret Service
Rodney Lezette, RIT Campus Safety Officer
9 – 10: 30 am
Golisano College Auditorium

What is identity theft, how does it occur and what can be done to prevent it? Additionally, what can be done should one's identity be compromised?

About the presenters:
Steven Petro was commissioned by the US Secret Service in 1970 and served in several capacities before retiring from his most recent duty as Resident Agent in Charge, Social Security Administration, Office of the Inspector General, Office of Investigations. Prior to this he was Corporate Security Director at Bausch & Lomb, Rochester, NY. **Rodney Lezette** is the RIT Campus Safety officer heads the team investigating identity theft and will discuss his department's protocol if the team were to investigate a case.

The Top 10 Things to Do to Prevent Hacking – Student Only Presentation

Swab

Bradstreet

Presenters: Dave Bradstreet and Dan Swab, ITS Resnet Staff
11:30 am – 1 pm
RIT SAU, Alumni Room

Presenters will discuss what hacking is, how its done, individual and network vulnerabilities as well as "The Top 10 Things to do to Prevent Hacking"

About the presenters:
Both **Dave Bradstreet** and **Dan Swab** work with residence hall students in the Resnet of-

Security Week Schedule

continued from page 8

fice located in Nathanial Rochester Hall. From helping students connect to the RIT network at Move-In and Orientation in the fall to providing network support, information and equipment repair, they are instrumental in keeping the resident student well connected.

Physical Security

Presenter: Lt. Michael Kozak, Chief Information Officer Rochester Police Department
1:30 – 3 pm
CIMS, Room 2220

This topic is about the emerging technologies in physical security from building and office entry to an awareness of an individual's workspace security.

Using the RIT Virtual Private Network (VPN)

Petro

Presenters: John Petro, ITS Technical Support Services and Tom Dixon. ITS Customer Support Services
1 – 3 pm
VIA Lab on the second floor of the Wallace Library

Dixon

Access to the RIT network from off campus is safeguarded using VPN – but what is this, how is it used and how do customers access VPN? Presenters will be able to answers these questions and discuss this system: a private connection between RIT systems and a remote location so that the information is safe from third party interception.

About the presenters…
Both **John Petro** and **Tom Dixon** provide customer support when on campus faculty and staff use the virtual private network. They work to maintain and safeguard this important connection as well as work with those unfamiliar with this system.

Wednesday, December 10

The Importance of Patching Operating Systems and Anti-Virus Software Usage

Presenters: Sid Pendelberry, ITS Technical Support Services and Dave Bradstreet, ITS Resnet
9:30 – 11 am
VIA Lab, on the second floor of the Wallace Library

This discussion will be about the importance of system patches, what they are and why they should be installed. Presenters will include information about both PC and Macintosh applications.

About the presenters…
In August, RIT was presented a major challenge when the SoBig virus was launched across the Internet. Installation of patches and anti-virus software alleviated some of what could have been an imposing effect on the network. Behind the scenes support for customers, for individual computers as well as network servers were provided **by Sid Pendelberry** and **Dave Bradstreet** and members of their respective departments in ITS.

Combating SPAM

Young

Presenters: Mike Young, ITS Technical Support Services and Jason Polito, ITS Customer Support Services
12-1 pm
VIA Lab, on the second floor of the Wallace Library

Polito

Discussion will be about the behind-the-scenes work ITS staff do to filter spam messages, what they are, how spammers work and research about spam-prevention software.

About the presenters…
According to a recent ITS News article, RIT rejects more than 63,000 spam messages daily. Behind the scenes, **Mike Young**, TSS systems administrator, uses several innovative and interesting methods to prevent the spam from infiltrating network mailboxes. As Desktop Support Specialist for the ITS-Customer Support Services department, **Jason Polito** works directly with customers to install spam filters and to use them effectively.

continued on page 10

Security Week Schedule

continued from page 9

Desktop and Enterprise Firewalls

Mangione

Presenter: Jack Mangione, ITS Technical Support Services
1:30 – 3
Student Alumni Union, Clark A

Information about enterprise and personal firewalls will be discussed along with the concepts of “trustworthy systems”, explanations of firewall software messages and how individuals make decisions about using the software effectively.

About the presenter…

Jack Mangione is new to ITS, but has a strong background in network security and project management. He will discuss how desktop firewall software can be used effectively and will give a brief status on two important projects, the Desktop Defense and Data Center Firewall Projects.

Thursday, December 11

Ethics in the Age of Technology

Presenters: Vince Incardona and Dave Pecora, both of ITS Customer Support Services
10:30 am – 12 pm
Student Alumni Union, Clark A

Pecora

Incardona

This discussion will be about ethics in the information age and how the technology and users have impacted what is considered open and available to the public.

About the presenters…
Dave Pecora is the operations manager of ITS and oversees the ITS HelpDesk and Desktop Suppport team located in the Gannett Building. He has a strong background in customer support. **Vince Incardona** oversees the ITS desktop support group, providing computer support to faculty, staff and students in their respective departments and labs. Additionally, he is an adjunct faculty member in the Criminal Justice Department, presenting coursework in Technology in Criminal Justice.

Campus Dialogue: Peer-to-Peer File Sharing – Issues and Information

7 – 9 pm
Panara Theater, NTID

Presenters:
Dr. Stanley McKenzie, Provost, RIT
Dr. Charles Phelps, Provost, University of Rochester and member Joint Committee of the Higher Education and Entertainment Communities
Professor Evelyn Brister, RIT, College of Liberal Arts,
Professor Sam McQuade, RIT, College of Liberal Arts
Travis Crawford, RIT Student and president, Information Technology Student Organization (ITSO)

Moderators:
Diane Barbour, RIT Chief Information Officer
Dr. Stan McKenzie, RIT Provost

The topic of Peer-to-Peer file sharing is timely and discussion about the stand of the Recording Industry Association of America, Motion Picture Association of America and higher education communities will be presented by **Dr. Charles Phelps**. He will be joined by **Dr. Evelyn Brister**, who will discuss “Ethics versus Self-Interest in Peer-to-Peer File Sharing. She will examine “whether the major parties involved in disputes about P2P file sharing (of music files) act ethically. The dispute concerns possible violation of copyright, and copyright is established by the Constitution for the purpose of promoting creative art. Thus, whether, why and how file sharing is or is not ethical hinges on whether it has the potential to play a role over the long term in promoting the most diverse and most creative musical production.”

Dr. Sam McQuade will also participate on the panel to discuss this issue and P2P file sharing as a crime. He teaches courses in the College of Liberal Arts, Criminal Justice department about computer crime and criminal justice technology. A former police officer, McQuade has done extensive research on the development and adoption of technology by criminal justice agencies and criminals. Professor McQuade will share the stage with **Travis Crawford**, the president of the Information Technology Student Organization, a student advocate group that has taken an interest in this situation and will present student “voices” for this issue. All will give short presentations on their respective topics, then address participant questions.

continued on page 12

Top Twenty Things to do for Protecting Your Personal Information

continued from page 7

you create a regular user account for yourself, with limited privileges and all your data in a particular area, and then happen to click on a mail bomb, then at worst you have probably messed up your data, which can be restored from backup. But if you are Administrator (Windows) or Root (*nix) and tell an unknown and malicious program to execute, you may have just lost your whole system.

14. Disaster Planning

The next thing to think about is disaster planning. It isn't just for big corporations – individuals need it, too. What is a disaster to you? Think about the data you value and the security attributes of confidentiality, integrity, availability, and authenticity, and any others that you need. Consider what could happen if some or all of your valuable data lost these attributes.

15. Consider the Opportunist

This is really the start of looking at your vulnerabilities. Many people insist that "I don't have anything that someone else would want." You do, though, if you have a PC connected to a network. It is the opportunistic threat. If you have a system with a network connection, even if it isn't always on, you are a target.

16. Avoid Offering Unnecessary Services

Don't share disks, printers, or offer services, unless absolutely necessary. This is the first of the cautions concerning Attitude and Awareness. Some things, like file sharing or printer sharing, are less likely to have nice interfaces, except possibly during installs. Some people consider them "essential". For homes with more than 1 system, they may be essential for sharing resources. If you want to share a service with other computers, put the whole network behind a firewall.

17. Don't Have Guests

Any guest has the potential to be dangerous. Guest accounts with a "guest" password, or no password, are invitations that unwanted people will gladly accept. For example, Linux users often have requests for "shell accounts". Giving others network access accounts via your system can open you up to people accusing you of things, in addition to having concerns that your data is unmodified.

18. Practice Download Safety / Practice Simplicity

These two issues are put together because they relate. It is easy to download more and more applications. It is fun to play with them. Unfortunately, it is usually more difficult to clean them up. So, a good process is to have a queue when you download something and set a date to review how useful it has been. Alternatively, ask yourself the question "Do I really need this?" And "Will I really have the time to learn this?" This applies to commercial software as well as shareware / freeware.

19. Turn Off / Disconnect Your Computer When Not in Use

This is another easy one. If your computer isn't on, or your network connection isn't on, then it is really tough for anyone to get at your information. Turning off your computer means that even if someone gains physical access, they will face a screen requesting a password. [There are ways around this, like booting from a floppy or CD-ROM, but unless your computer is very exposed, you may not have to worry about that extreme.] If you do backups or complete system scans and your system is connected to a network, then you can temporarily unplug the network cable from the back of the computer [This may not be feasible in business situations.]

20. Productivity Wasters

Things like browser pop-ups and spam are time wasters. Commercial products exist in the Windows area, like McAfee Spamkiller and Panicware's Pop-up Stopper (Pro). Anti-spam products can reduce the likelihood of spyware or virus-laden emails from unknown sources. They can also save you time by automatically filtering your email.

Security Week Schedule

continued from page 10

Friday, December 12

Security Panel Discussion: RIT Alumni in the Security Business
11:30 am – 1:30 pm
Golisano College Auditorium

We'll close the week with presentations and a Q & A session with a panel of RIT Alumni making a name for themselves in the security industry. They will discuss the security industry, its challenges and opportunities as well as the role they play in safeguarding their respective company systems.

Presenters:
Linda Stutzman, Xerox Corporation
Jennifer Love, Eastman Central Credit Union
Wes Shields, Central Intelligence Agency
Robin Tremblay, GGCIS

The Holidays are approaching...

Many departments will be closed during the holiday break. Please remember to change your RIT Messenger System mailbox greeting to reflect your availability. Messages are retained in your mailbox for 10 days. You may want to consider call answer disable if you are going to be away from your office and will be unable to check your messages. Please call the Telecommunications Services Help Desk at 5-5800 with any questions.

Desktop Defense Project

continued from page 4

The security industry recommends not relying on users to install updates: even if you have policies to control the use of computers, they tend to be forgotten over time. The media concentrates on the most commonly exploited Windows vulnerabilities, but there are many more areas a hacker could exploit. For instance, even a relatively minor gap in your firewall could quickly be turned into a serious flaw.

> *"A report by IT analyst firm the Aberdeen Group said that there are more than 7,000 "spyware" programs in existence, running on millions of corporate and personal computers."*

The Desktop Defense project will begin by deploying a desktop management agent onto your system. The agent's purpose is to retrieve incremental changes to policies and tasks from the management server, execute policies to protect against known problems, install products and perform scheduled maintenance tasks. It does this all the while running invisibly in the background on client computers. It provides your system administrator with a comprehensive and efficient means of proactively managing the environment.

Shortly after the agent and management tool are in place, the desktop firewall software will be deployed. The firewall software will proactively defend and control clients to prevent new threats that anti-virus alone cannot. The Desktop Firewall will also prevent clients from sending or receiving hostile threats from unauthorized network traffic or applications. It also prevents authorized applications from being manipulated in order to send or receive threats across the network

This is the first in a series of articles explaining the objectives of the Desktop Defense Project. Look for more project information in upcoming issues and don't forget to attend the ITS Security Seminar scheduled for December 8th through the 12th.

Vini, Vidi, Viri (I Came, I Saw, I Infected)

By Dave Bradstreet, Residential Computing Administrator dmbdss@rit.edu, and Jeremy Beyette, Residential Computing Consultant

Many of the computer viruses today fall under the category of **Worms**. A worm attempts to replicate itself through open network shares or by e-mailing itself to e-mail addresses found in the address book of a computer. Some of the subtle things worms do is open up your computer ports and allow access by the worm's sender to access and sometimes remove files from your computer or, in some instances, delete information and data saved on your various drives.

There were two large-scale viruses released toward the end of September, *Bugbear* and *Opaserv*. Bugbear is a mass-mailing worm that:

- Stops anti-virus and firewall processes.
- E-mails itself to everyone in an address book with its own messaging engine.
- Creates a backdoor for intercepting keystrokes and allows remote administration.
- Replicates itself to other computers through open network shares.

Opaserv is a worm that attempts to replicate itself to other computers through open network shares. If it finds an open network share, it copies itself to that computer in a file named **Scrsvr.exe** and then attempts to download updates from www.opasoft.com.

There are steps that you can take to help protect yourself from existing and new viruses

Other viruses that remain on the list of top threats and that are often discovered on the RIT network include *Klez* and *Nimda*. Klez is a mass-mailing worm that attempts to copy itself to open network shares, e-mail itself to entries in a Microsoft Outlook address book, and cause files to become zero bytes in size on several days during the year. Nimda is another mass-mailing worm that sends itself out by e-mail, replicates through open network shares, copies itself to vulnerable Microsoft IIS web servers, and infects files on local and remote computers.

There are steps that you can take to help protect yourself from existing and new viruses.

- **Use anti-virus software**. McAfee VirusScan is available for free to all RIT students, staff, and faculty. The file can be found at http://www.rit.edu/~wwwits/services/security/.
- **Update your anti-virus product on a regular basis**. Most antivirus products feature automatic or scheduled update capabilities to keep you protected from the latest threats.
- **Practice e-mail safety**. Microsoft Outlook is a feature rich e-mail client, but is also the target of many attacks. To prevent these attacks, follow several steps to prevent infection:

  1. Delete e-mail from unrecognized senders
  2. Turn off the preview pane
  3. Do not open suspicious or unrecognized attachments
  4. Last, install updates regularly

Installing Windows and Office updates on a regular basis help close security holes and prevent infection from a virus. Windows Updates can be found at http://windowsupdate.microsoft.com/ and Office Updates can be found at http://office.microsoft.com/.

Need Help With Viruses?
Contact the ITS Help Desk to answer any questions about computer viruses and installing virus programs for your computer. Call the HelpDesk at 5-HELP (4357) or 5-2810 TTY.

ITS News

By Tom Dixon, ITS HelpDesk, trdhelp@rit.edu

As you have probably noticed, this month's issue is related to Network Security. Most of us take security for granted. We assume that what was installed on our computers is good enough to protect our machines. In the past, this may have been true but in the 21st century, we have come to realize this is not the case. We have all been rudely awakened to new viruses, worms, and Trojans with the ability to takeover machines at a fevered pace.

The fact that the use of home broadband (Road Runner, Lightning Link, etc) connections have skyrocketed has allowed these "nasties" to take out big business as well as home systems. This is because your computer is ALWAYS vulnerable because it is always on line. Unlike dial up connections, your computer sits out on the Internet ready to go all the time. If you chose not to protect your computer, it is the equivalent of swimming in shark-infested waters with a raw steak bathing suit…it's just asking for trouble!

So how do you protect your computer? Well, first you need to be sure you do two BIG things. First, keep your operating system (OS) up-to-date. All OSs have patches or updates to keep them safe when a vulnerability is found. Second, keep your virus protection software up to date. Both of these tasks should be performed at home and at work at LEAST once a week. These two basic tasks can protect your machine from days of rebuilding should one of the "nasties" hit. If you have spent more than two months at RIT, you should be well aware of the importance of completing these tasks. I am still trying to recover from August and September!

Okay, so how about some advanced protection for your machine. Lets focus today on your home network or system. First let's put security in perspective. The basic protection, the updates you complete on your computer, are like the locks on your door. Occasionally you need to change the locks, but for the most part locks serve a basic purpose of keeping those who we don't want in, out. Everyone knows to lock your door when you leave the house. Advanced protection would be to buy a guard dog, or install an alarm system; this makes it more difficult for intruders to get in. They may still get in but they will have to pay a price. Advanced computer protection works the same way. The links that I provide in this article will help you understand more about advanced protection like firewalls, network topography, and general security plans.

ZoneAlarm
www.zonealarm.com

ZoneAlarm is a free firewall program that works best with a broadband or LAN connection like we have at RIT. ZoneAlarm comes completely configured to block all network traffic. As you use it, you are able to teach it what is good and what is bad traffic. Occasionally, windows will pop-up asking if you want to block a certain application from reaching the Internet. In this case, you have the choice to allow it once or have the firewall remember each time the application tries. In the case where you don't know what the application is, it's always good to reject the connection. That way you protect your computer. The great part is, if you accidentally block something that you find later you need, you can go into the properties of the firewall and reconfigure it. ZoneAlarm takes a little getting used to but it works great. There are a few shortcomings in ZoneAlarm. Some applications cannot talk to your computer through a firewall such as VPN. However, for everyday use, ZoneAlarm gives you another step up in security on your PC.

Practically Networked
http://www.practicallynetworked.com

This website is invaluable to users who wish to set up a home network. Several sections that discuss many home network related issues. The review of network hardware assists you in purchasing just the right router for your needs. They step you through an entire home network setup from start to finish. This section is the main reason I recommend this site.

continued on page 15

Tom’s Tidbits

continued from page 14

They are very thorough in their details regarding proper setup of a home network. Although the setup can still be somewhat complicated, this site makes it much easier. Plus, you don’t have to go to the bookstore and buy a “Networking for Dummies” book and spend $25. It’s all here in a nice concise format. The website also touches on wireless setups and security. Although it is not as in depth as I would like, it does lay the groundwork for a good start. They also have a new discussion forum which allows you to ask the experts if you have questions. This is a new feature and I guarantee the people who hang out in this group will be able to answer any of your networking questions!

CERT Coordination Center/ Home Network Security
http://www.cert.org/tech_tips/home_networks.html

This website, run by CERT, is a conglomerate of everything you wanted to know about home network security but were afraid to ask. I can’t even begin to tell you everything this page covers, but it does a fine job of explaining difficult network issues in a clear and somewhat less technical language. If you have ever wondered what protocol is, why IP addresses exist, etc, this site is for you. Not to mention the fact that it answers pretty much any question you have about network security. This is a top-notch site!

Newest and Coolest:

Vectron Flying Saucer
http://www.techtv.com/products/games/story/0,23008,3369679,00.html

This is not a gadget for your computer but it definitely classifies as a cool tech item. Although this was posted last January, I would venture a guess that no one has actually seen one of these yet so it can still be considered “new.” This is a remote controlled helicopter that allows for 30 characters to be displayed on its LED device. I am adding this one to my list of cool things as a suggestion for the kid (or husband) that has everything. It’s pretty cool check it out!

Telecommunications Services News

Training Process for RIT Messenger System Improved
We Asked, You Answered, We Listened

Telecommunications is pleased to announce a change in the training process for new RIT Messenger System subscribers. Starting November 1, 2003, training will be recommended, not required for new subscribers. Telecommunications will continue to offer 1-2 training classes monthly.

The procedure will change slightly for the Telecommunications Coordinators. Coordinators will continue to request new mailboxes as they have in the past. The ITS-Telecommunications department will email the coordinator notification of the mailbox activation and the default password. The coordinator will be responsible for passing on the information to the new subscriber.

Training information is available on line at http://www.rit.edu/~wwwits/services/tele/voice.html

ITS Update

Check Closings with Campus Cancellations Hotline

With winter here, campus closings are a strong possibility. To ensure that our students, faculty and staff know of closings, an automated call line provides information about cancelled day, evening and weekend classes or special events due to weather conditions or other emergencies. To access this line, dial:

475-7075 (voice)
475-7076 (TTY)

Please share this information with your co-workers and student workers. It may save them a trip to campus when we are in the throes of one of our infamous Rochester snow storms!

ITS Contact Information

DSS Computing Labs

Hours, locations, hardware, software, and reservations information available at:
http://www.rit.edu/its/services/computer_labs

Telecommunications Services

Located in the Facilities Mgmt. bldg. (99)
To contact the Telecommunications Services call 475-5800.

ITS HelpDesk

Located in the Gannett building, rm. 7B-1113

To contact the ITS HelpDesk

- Call 475-HELP or 475-2810 (TTY)
- Send e-mail to helpdesk@rit.edu

Regular hours

Sunday	12 p.m.–6 p.m.
Monday–Thursday	8 a.m.–8 p.m.
Friday	8 a.m.–5 p.m.

ITS News is published monthly, September–May, for RIT students, faculty, and staff. It is available in electronic form at http://www.rit.edu/its

ITS News is created with AdobePageMaker 6.5 on a Dell OptiPlex GX260 and is printed at a service bureau through RIT's HUB. Photographs taken with Nikon COOLPIX 900 digital camera.

Managing Editor: Dave Pecora, dlpits@rit.edu

Editor: Michelle Cometa, macits@rit.edu

Design/Layout: Omar Phillips, odphelp@rit.edu

Use of registered trademarks does not constitute endorsement by RIT or ITS. Rather than put a trademark symbol in every occurrence of a trademark name, we state that we are using the names only in an editorial fashion, with no intention of infringement of the trademark.

ITS News is printed on Graphica Smooth Cool PC White recycled paper and is itself recyclable.

Rochester Institute of Technology
Information & Technology Services
135 Lomb Memorial Drive
Rochester, NY 14623-5608