SECUREPURDUE NEWS
www.purdue.edu/securepurdue

September 2007
Volume 1, Issue 10

All the news that's secure to print.

Text Messaging to be Tested as Alert Method

Purdue is going to put text messaging to the test.

Researchers will send a text message to a broad cross section of the campus in September to analyze the message speed and dependability. It is believed to be the first test designed to generate independent data.

"There are about 50 companies right now that offer this service, but no independent research we know of has been done to validate their promises," said Scott Ksander, executive director of information technology networks and security. "Besides having the technical expertise, Purdue has the size--50,000 students and employees on the West Lafayette campus--to really learn how well these systems perform."

Within a few days of the Virginia Tech shootings, Purdue was deluged with offers from dozens of vendors offering services that would allow the University to send emergency text messages to students and the campus community. Some promised to deliver 18,000 messages per minute, but the only proven record was 200 to 300 per minute, Ksander says.

Testing is complex, he says, because of a variety of variables, such as the various phone services users choose, cell tower availability, cell signal coverage, and traffic volume

"We will harvest the complex data on performance and share the research findings with others," Ksander says. "The information will help everyone know what to ask when they request bids."

Purdue students, faculty, and staff who want to take part in the test, tentatively scheduled for September, should register their cell phone number.

Go to www.purdue.edu/securepurdue, click on "Change My Password," enter your career account name and password, and then select the "Emergency contact Information" link.

Registrants also will be able to receive emergency text messages should the need arise while the University analyzes the test data.

In addition to text messages on the testing day, Purdue also is exploring other notification techniques that can be tested at the same time. These notification systems are part of the University's multi-layered emergency communications plan, says Ronnie Wright, Purdue director of emergency preparedness and planning.

"Our first line of communication is our sirens," Wright says. "Next, information will be available on the University's home page and on Facebook. We also will send an e-mail campus wide.... Clearly, text messaging, if it works in a timely fashion, would be a significant addition to our communication toolbox."

So far, 6400 of the Purdue community have registered their cell phone number. At least three times that number is needed to really test the system.
To learn more about Purdue's emergency response procedures, please visit www.purdue.edu/emergency_preparedness/.

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

The term "IT Professional" conjures up many different images in today's society. Despite some stereotypes that might suggest an overabundance of seriousness, IT professionals like to have fun within their jobs. From geeky behavior and Hawaiian-shirt Friday to science fiction references and "Talk Like a Pirate Day" (September 19), the group of networking and security professionals at Purdue celebrate that which makes work fun while managing and moving Purdue University's data in a secure manner.

After all, who wouldn't want to talk like a pirate? (Actually, see one of this month's articles on a type of piracy to avoid.)

The fall semester brings a renewed focus on cybersecurity at Purdue with a series of non-technical presentations for the Purdue

See CISO, Page 4

Pirates on the Seas of Open Computers

Pirates are pretty cool right now. There are a host of popular pirate-themed movies, and a newly refurbished pirate ride at "The Happiest Place on Earth." In fact, pirates are so popular that September 19 is recognized (by Dave Barry, no less) as International Talk Like a Pirate Day.

Despite pirate popularity, there is at least one type of piracy that is not so cool: intellectual property piracy. In fact, intellectual property thievery is quite a serious matter, both for Purdue University and for the larger, non-academic community. Artists, singers, authors, inventors, and companies transform ideas into tangible property (movies, music, works of art, books, etc.). This type of property is often referred to as intellectual property and can qualify for protection under the law. Intellectual property covers copyrights, patents, trademarks, and trade secrets. Federal laws covering these areas set forth the rights that owners have with respect to their creations as well as the ramifications of violating those intellectual property rights.

Avoid untrustworthy downloads!

Holders of intellectual property rights are diligent in protecting those rights. For instance, music copyright holders and their representatives have been particularly vocal about protecting the copyright holder's right, particularly with respect to illegally sharing copyrighted materials over the Internet through peer-to-peer (P2P) file sharing applications. Activities on college campuses that have been closely examined include both downloading copyrighted materials without the appropriate consent from the copyright holder; but also sharing or offering copyrighted materials for download without the appropriate consent.

People who are caught illegally downloading or offering copyrighted materials for download can face stiff fines and costly legal actions. The use of P2P networks and applications for sharing copyrighted materials has figured prominently in discussions about copyright enforcement.

Keeping in mind that the use of P2P networks and file sharing applications is not in itself illegal, there are other dangers to indiscriminately downloading materials, even if not copyrighted materials, from the Internet. Since P2P networks can be large, are hard to manage, and tend to be less secure, using such networks can open up your computer to a number of security threats that include viruses, worms, and Trojans. Spyware and other forms of malware can also be distributed via P2P activity, and can be a serious privacy threat to the computer user. These types of programs can allow other users to monitor your computing activities, gain user names and passwords to accounts, and use your computer without your knowledge.

In addition, if a user is not careful while using some P2P programs, they can also inadvertently share other information on their computers, such as files containing bank account information, medical information, and other personal and confidential information. Using P2P applications to share large files can also slow network performance and decrease computing resources available to other users. Finally, P2P applications can be hard to remove from a computer system when they are no longer needed.

Before sailing on the high seas of the Internet, consider the following tips:

- Always adhere to the law: Make sure that you have a copyright holder's permission to download and share copyrighted materials.

Even if you have legally obtained copies of copyrighted materials and stored them on your computer, you must take care to protect those copies from being copied by others.

- Obtain your P2P software from a known and legitimate source: This helps to ensure that you do not unintentionally affect your computer system with malware or other undesirable software.

- Restrict access: Restrict other's access to your computer by only allowing P2P access to specific files. Change the default settings in P2P applications so that others on the P2P network cannot see other files and folders on your computer.

- Avoid untrustworthy downloads: If a file, URL, or other type of clickable link looks suspicious, do not click on it or download the file. In addition, be sure to run up-to-date anti-virus and anti-spyware programs on your computer and scan every file that you download before you open it.

- Install and use a firewall: Firewalls may be able to prevent some types of malware by blocking it before it can even enter your computer. Many operating systems include a firewall, which you should enable. You can also consider the purchase of a hardware firewall.

When using P2P networks at the University, keep in mind that Purdue University takes the intellectual property rights of others seriously and expects students, faculty, and staff to respect the intellectual property rights of others. Improperly sharing copyrighted works like music and movie files can subject a user to discipline under the Purdue IT Resource Acceptable Use Policy and could constitute a violation of federal copyright law.

There are many resources available to members of the Purdue community to learn more about intellectual property issues.

Copyrighted materials information is available on SecurePurdue at: http://www.purdue.edu/securepurdue/copyright.cfm

SPOTLIGHT

Don't Just Click It

Click It or Ticket is the most successful seat belt enforcement campaign ever. We want to create an equally successful campaign to caution people from clicking on URL links in emails or Instant Messages (IM) or e-greeting messages sent to you from a friend. Clicking on links in an email or IM can take you to a fraudulent website in an attempt to steal your personal information.

Here are a few ways to to tell if an email is fraudulent. A suspicious message may contain certain key phrases:
• "Click the link below to gain access to your account."
HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony site. To view the real web address, rest your mouse pointer on the link. The string of cryptic numbers may look nothing like the company's Web address, which is a suspicious sign.

• "If you don't respond within 48 hours, your account will be closed."
These messages convey a sense of urgency to entice you into responding immediately without thinking. E-mails might even claim that your response is required because your account has been compromised.

• "Dear Valued Customer."
Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

Another sure clue that the email is fraudulent is if you have no account with the company that is attempting to contact you.

Install up-to-date antivirus and antispyware software.
Some phishing e-mail contain malicious or unwanted software that can track your activities or simply slow your computer.
Purdue provides free anti-virus software for students, staff, and faculty. For use on non-Purdue owned equipment (Windows machines), students, faculty and staff can download VirusScan Home Edition Software which includes a built-in firewall and anti-spyware options.
Virex, an anti-virus product for Mac operating systems, is also available.

To download the above software, visit the SecurePurdue Web site at www.purdue.edu/SecurePurdue and click "software downloads."

Unfortunately, not all malicious or unwanted software can be prevented with antivirus or antispyware software. So take precautions to not infect your computer or your network.

Don't Just Click It! Just like you put your seat belt on before you start your car, think before clicking on a URL link in an email or IM. Do you know the person who sent it? Is the URL really taking you where you believe you are going?

You can learn more about the dangers of indiscriminate clicking by viewing the 2nd place video, titled "Whoa, That's Awkward," in the 2007 Educause Computer Security Awareness Video Contest. The video is available at: http://www.researchchannel.org/securityvideo2007/

STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at:

http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue email viruses

The following list is a 30-day snapshot of the most active email viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

(30-day snapshot as of August 24)

Viruses	Max. Occurrences
W32/MyDoom-0	1090
W32/Mytob-GH	2959
W32/Virut-A	297
W32/Sality-AA	374
W32/Mytob-FN	780
W32/Mytob-D	128
W32/Netsky-P	90
W32/Nyxem-D	127
W32/Dolebot-A	235
W32/Mytob-JF	96

MILESTONES

ITNS staff Certified

GIAC Certified Incident Handlers

Addam Schroll and Bill Harshbarger, Security and Privacy Analysts in the Security Services area of ITNS, passed the GIAC Certified Incident Handler Exams. This helped fulfill their criteria to receive the GCIH Silver certification. Prior to this they attended the SANS 504 training at the University of Kansas in April.

ITaP Networks and Security (ITNS) and the Center for Education and Research in Information Assurance and Security (CERIAS) presented a 12-week information security lecture series to assist Purdue staff to become more knowledgeable about IT security. These presentations targeted Purdue staff who wanted to expand their knowledge and gain the most sought-after security accreditation—(ISC)2's Certified Information Systems Security Professional (CISSP) designation.

The goal of these presentations was to provide a high-level overview of the (ISC)2 common bodies of knowledge that are represented on the CISSP exam and to provide participants with an opportunity to study information security concepts with other Purdue professionals.

The presentations were given by ITNS and CERIAS professionals who have themselves received the CISSP designation, as well as other Purdue professionals with subject matter expertise. To view the presentations or archived streaming video files, visit http://www.purdue.edu/securepurdue/training/cissp.cfm

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

- **Purdue's emergency response procedures**
http:// www.purdue.edu/emergency_preparedness/

- **Copyrighted Materials FAQ**
http://www.purdue.edu/securepurdue/bestPractices/draftITPolicies.cfm

- **Purdue Printing Services Copyright Information**
http://www.purdue.edu/printingservices/services/*copyright.htm*

- **Purdue Fair Use of Copyrighted Materials**
http://centaur.pmc.purdue.edu/pages/communications/copyright_fair_use.html

- **Copyright and Legal Issues**
http://centaur.pmc.purdue.edu/pages/communications/copyright.html

- **Purdue Draft IT Policies for Review**
http://www.purdue.edu/securepurdue/bestPractices/draftITPolicies.cfm

CISO, from Page 1

community designed to be both serious and fun. In October, ITaP and IT Networks and Security will mark the University's second annual observance of National Cybersecurity Awareness Month. The theme for this year's series of presentations will be "The Internet: Your Ticket to Ride" and will focus on using the Internet safely and emerging trends in information technology The target audience for this year's presentation will be expanded outside of staff members and will include students, faculty, and the general public.

Sessions for the month-long cybersecurity awareness event include:
October 10: Internet Riding Safety. Scott Ksander and Pablo Malevenda will discuss ways to safely use the Internet, including appropriate information to share on social networking sites like Facebook.

October 17: Cybercrime and Copyright Infringement. Mr. Chris Burgess, CISCO Senior Security Advisor and Chief Scientist, will speak on intellectual property strategies, and Purdue Professor Marcus Rogers will speak on the law and Cyber Forensics.

October 24: Future Destinations: Trends in Technology. Featured speakers will discuss new technology trends and how these might impact cybersecurity. Come listen to Professor Ed Delp, The Silicon Valley Professor of Electrical and Computer Engineering and professor of biomedical engineering. George Heron, VP and Chief Scientist for McAfee will share security and technology trends.

To be sure that a little fun is included in presentations that focus on the serious issue of cybersecurity, on October 31, we will feature a presentation called "Destination Unknown." This session will include our second annual Halloween security-costume contest (last year's winner was a costume depicting "security on the web") and will discuss the role of information technology and security with respect to the changing face of higher education.

More information about Cybersecurity Awareness Month events at Purdue can be found in this issue and next month's issue of the SecurePurdue news, as well as on the "Training" tab of the SecurePurdue website. I hope each of you will plan on attending at least one of the October events.

As always, thanks for reading and "Arrr, ye be careful out thar."