SECUREPURDUE NEWS
www.purdue.edu/securepurdue

August 2007
Volume 2, Issue 1

All the news that's secure to print.

Draft IT policies available for review and comment

Purdue community asked to contribute

The SecurePurdue initiative has begun posting working drafts of new information security policies, standards, guidelines, and procedures for public review and comment. The move includes drafts that originate from IT Networks and Security (ITNS) and the University Security Officers' Working Group, which will be posted on the SecurePurdue Web site.

According to Joanna Grama, project manager for ITNS, all members of the Purdue community are invited to submit comments on draft documents posted on the site, which policy developers will then read and consider.

"ITNS and the policy subcommittee of the Security Officers' Working Group will review and discuss all comments received by the due date indicated in the draft document," says Grama. "Documents may undergo further revisions based upon comments received."

ITNS works with the University Security Officers' Working Group and other pertinent stakeholders to develop University-wide IT policies, standards, guidelines, and procedures. IT policies are reviewed, at a minimum, by the University Security Officers' Working Group, the IT Executive Steering Committee, the Vice President for Information Technology, the Executive Vice President and Treasurer, the Provost, the University President, and University Legal Counsel.

To view draft versions of information security policy documents, and to provide comments, visit the "Best Practices" tab of the SecurePurdue Web site, and click on the "Draft IT Policies."

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

In the IT world, changing technology is a constant. Current technologies mature at an alarming rate and new technologies sprout every day. This constant change also produces new technologies that can be used to protect the security of Purdue's information and data, Yet, these new technologies cannot be effectively applied without proper training.

One of the critical components of the University's SecurePurdue initiative is to provide training and awareness opportunities for members of the Purdue community. To that end, the SecurePurdue Web site serves as a clearinghouse for information and resources on computer security specific to the University. In addition, we offer training on security issues in the form of documentation, videos, and courses on both technical and non-technical subjects.

While training that addresses awareness of security topics is important for members of the general University community, training in technical security subjects for our IT staff is of equal importance.

As part of SecurePurdue, we at ITNS are exploring additional ways to bring high-quality, timely, and relevant training to Purdue's IT staff. We had the opportunity to host a SANS course on-site at Purdue at the beginning of this year. That course was well-received, and we are looking to host another course at the University later this year.

Hosting training sessions from proven vendors at the University not only brings us quality training

See CISO, Page 2

STEAM-CIRT NEWS

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

In January, STEAM-CIRT deployed the campus intrusion detection and prevention service to monitor network traffic on the primary Internet connection on Purdue's West Lafayette campus. This monitoring alerts STEAM-CIRT staff to the presence of attacks on or by Purdue computers.

On July 19, STEAM-CIRT began blocking some of these attacks as well. Blocking prevents attacks from reaching their intended target and stops infected machines from leaking data out to the Internet. STEAM-CIRT is monitoring this service enhancement closely to ensure it does not adversely impact Purdue users, and no negative effects have been discovered.

"This new service further enhances STEAM-CIRT's ability to respond to incidents before real damage occurs," says Addam Schroll, security and privacy analyst for ITaP.

For more information about incident response or the campus intrusion detection and prevention service, contact your IT department's designated Security Officer or visit www.purdue.edu/securepurdue/steam/.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page: http://www.purdue.edu/securepurdue/steam/

MILESTONES

Training gets advanced

Staffers attend web-based conference

Thirty Purdue staff attended an interactive video conference training on July 11, hosted by the University of South Carolina and Virginia Tech and coordinated by the SANS Institute. The training covered implementation of the new Windows Vista operating system. Sixteen other sites participated in the all-day training, including more than 240 staff from West Point, University of Nebraska, Indiana University, and other institutions.

The remote training was a pilot session in using an interactive video-conference format. This type of training requires significant IT preparations to make sure all connections work effectively and all attendees are able to interact.

Doug Couch, IT Security and Privacy analyst, attended the training and says the format was very effective.

"I was pleasantly surprised at the effectiveness of the technology solution that enabled us to take this course remotely. I didn't feel like I missed anything at all by taking the course in this fashion, and the session was what I expected from a SANS course," Couch says.

As technology continues to advance, ITNS hopes to continue to provide innovative and varied training opportunities for campus IT staff. For more information on information security training opportunities available at Purdue, please visit the Training section of the SecurePurdue Web site at http://www.purdue.edu/securepurdue/training/.

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 July 31

Viruses	Max. Occurrences
W32/Mytob-GH	6731
W32/MyDoom-O	1090
W32/Sality-AA	638
W32/Virut-A	240
W32/Dolebot-A	235
W32/Mytob-D	128
W32/Nyxem-D	127
W32/Netsky-P	126
W32/Mytob-JF	102
W32/Dolebot-A	99

CISO, from Page 1

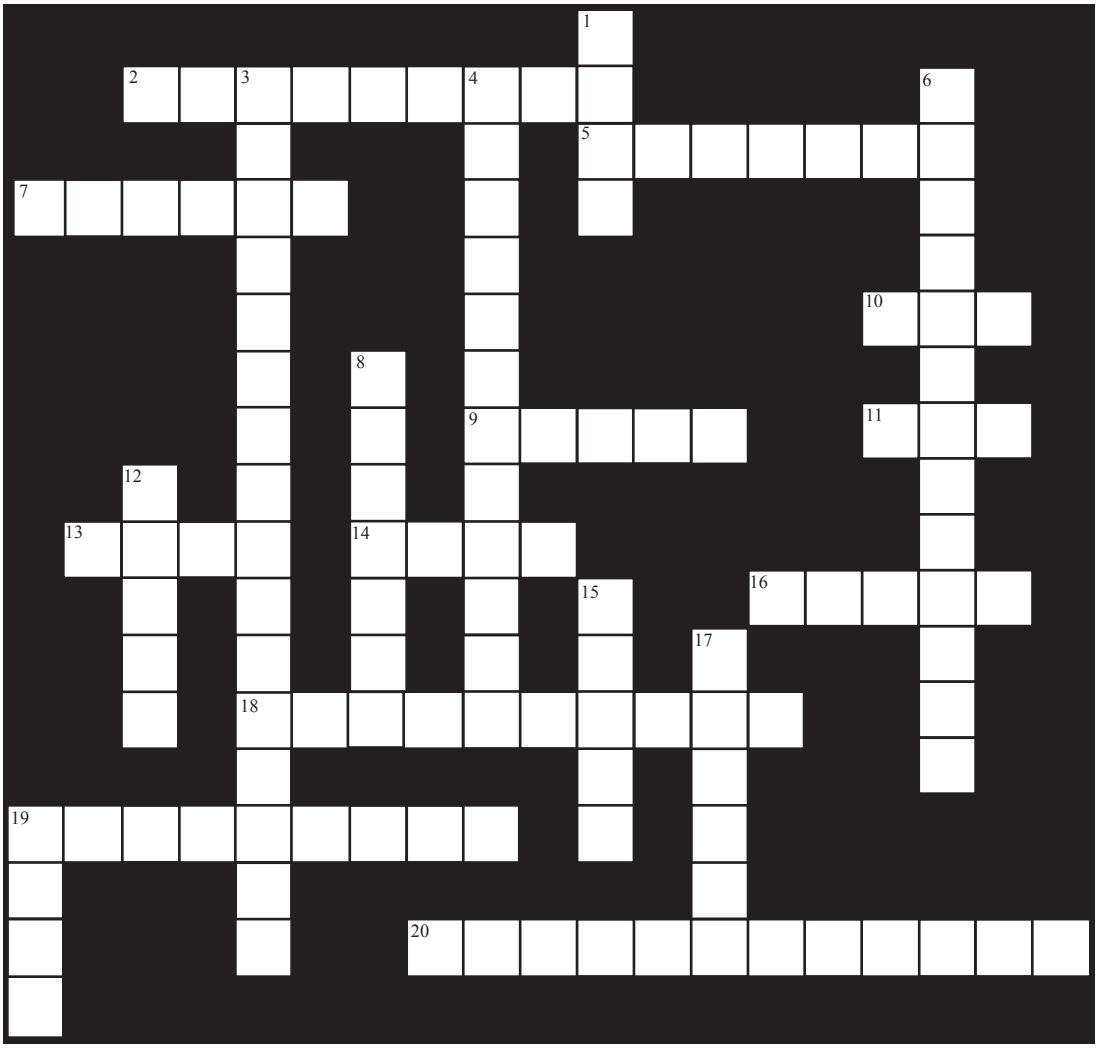
opportunities, but also saves us money.

We have also been exploring external training opportunities, such as web-based training and video conference training. Additionally, we are striving to improve the quality of our internal training opportunities, both on the Web and through live presentations given by members of the Purdue community who are experts in their fields. We must take advantage of the fact that we have an exceptionally large number of talented IT professionals here at Purdue, both as part of our staff and within the University faculty.

Continuous improvement through training opportunities helps Purdue flourish and succeed in its missions. It allows us to remain flexible and responsive to change. It allows us to protect the University's information assets and keep one step ahead of the security threats that are ever-present. I urge you to continue to support these opportunities. To learn more about the information security training available at Purdue, visit the "Training" section of the SecurePurdue Web site.

As always, thank you for reading, and, be careful out there.

SECUREPURDUE CROSSWORD



ACROSS

2. Tool developed at Purdue that automatically delivers vulnerability notifications
5. Software designed to infiltrate or damage a computer system without the owner's informed consent.
7. An overall general statement of principle that provides scope and direction
9. According to current standards, passwords must be at least ___ characters long
10. A network that uses the public network to transfer information using secure methods (abbrev.)
11. Purdue's secure wireless network (abbrev.)
13. Activities of the Security Officers' Group are coordinated by (abbrev.)
14. The electronic equivalent to "junk mail"
16. The usual medium for 14 Across
18. A computing asset provided by the University to further its mission of discovery, learning, and engagement
19. Detailed step-by-step tasks that should be performed to achieve a certain goal
20. A major initiative focused on improving the security of data and campus IT resources at Purdue

DOWN

1. Acronym for the office at Purdue that maintains centralized authentication credentials
3. The body that serves in an advisory capacity for SecurePurdue
4. At Purdue, these people are responsible for defining the classification and handling procedures of University data
6. A collection of Purdue IT security policies, procedures, and guidelines
8. The Vulnerability Scanning _____ developed at Purdue is a self-serve mechanism for network vulnerability scanning available to system and network administrators
12. This legislation, passed in 1996, is designed to improve the efficiency and effectiveness of the health care system
15. Reports of misuse of Purdue's IT resources should be sent to _____ @purdue.edu
17. Brand of antivirus software currently licensed by the University for use by faculty, staff, and students
19. Ten digit number used for identification in electronic systems at Purdue

For an answer key to this month's crossword puzzle, browse to: http://www.purdue.edu/securepurdue/news/newsletter.cfm

SECURITY RESOURCES

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

- **IT Incident Response Report Form**
  http://www.purdue.edu/SecurePurdue/incidentReportForm.cfm
- **Purdue data handling requirements**
  http://www.itap.purdue.edu/security/procedures/dataHandling.cfm
- **Purdue data stewards**
  http://www.itap.purdue.edu/ea/stewards/
- **Purdue data handling roles**
  http://www.itap.purdue.edu/security/policies/roles.cfm