SECUREPURDUE
www.purdue.edu/securepurdue

May 2007
Volume 1, Issue 6

All the news that's secure to print.

# CIS benchmarks, resources available to Purdue

## Members-only tools available to employees

Creating security configuration guidelines for the many different ages and types of systems used on campus is a daunting and time-consuming task. ITaP Networks and Security (ITNS) is often asked to recommend a set of systems security configuration guidelines for Purdue system administrators in the absence of specific, Purdue University guidelines.

While there are a number of commercial or external benchmark tools and guidelines available to system administrators to provide best practice information for security configuration, ITNS recommends using the benchmarks created by the Center for Internet Security (CIS).

The CIS is a national organization that helps system administrators reduce security risks by using adequate technical security controls. This help comes in the form of best-practice benchmarks for security configuration.

These benchmarks are unique because they are created by consensus of hundreds of security professionals worldwide, and are widely accepted by U.S. government agencies to meet regulatory requirements for FISMA compliance, and by auditors for compliance with the ISO standard as well as the Gramm-Leach Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), HIPAA, FERPA, and other information security regulatory requirements.

Purdue University is a member of the CIS, and as such has the right to distribute the benchmarks and tools for use within Purdue University. ITNS recommends the CIS benchmarks for consultation and use by Purdue University system administrators when no other specific Purdue University policy, standard, guideline, or procedure applies to the underlying system.

Any Purdue University employee can obtain a user account on the CIS members site. To register, browse to http://members.cisecurity.org/ and click "register." Fill out the registration form and submit the registration information. Within 24 hours, an email should arrive indicating active registration.

All CIS benchmarks, and several software scoring tools that can be used to compare the configuration of Purdue systems to the benchmarks, are distributed from the CIS public Web site at www.cisecurity.org. There is no need to register for access to that site. On the members Web site, Purdue employees have access to CIS scoring tools with specialized features, including:

- A command-line version that eases deployment of the tools and scoring of networked systems,

- A version that reads customized input files, enabling users to compare the configuration of their systems with both the CIS benchmarks and their organization's local configuration policies.

The CIS members Web site also contains various discussion forums and development versions of new benchmarks and scoring tools. Please note that ITNS does not provide technical support for the tools and benchmarks available from CIS.

**See BENCH, Page 2**

## In this issue



## FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

In a currently popular TV show, the host asks the question: "Is that your identity?" Contestants on the show "guess" the identity of various people and can win $500,000 if they are able to get it right. In Purdue's IT-security reality, identity is a very key question, and the cost of an incorrect answer is far more than $500,000.

Last month we discussed the Identity and Access Management Office (IAMO). Establishing a unique, formal Purdue identity for all objects may well be the single-most important enabling concept for moving forward with IT technologies at Purdue. Without an accurate and unique identity, there is no way to assign roles, grant privileges, or establish relationships between the various Purdue IT systems. Local system identities are obsolete as our customers don't use just one or two systems. Our

**See CISO, Page 2**

**BENCH, from Page 1**

Greg Hedrick, manager of security services for ITNS, said these benchmarks are unique in the depth and breadth of their coverage. "While they may not be tailored specifically to Purdue, they can serve as guidelines for system administrators and as a way to compare the system security configuration against a benchmark developed by technical folks from a number of industries and computing environments from other higher education institutions to private corporations."

Addam Schroll, a security analyst in ITaP Networks and Security, said that he is frequently asked to recommend best practices for system security settings and that these guidelines are geared toward system administrators and anyone who administers a machine. "Purdue policies and procedures override the benchmarks, which only serve as guidelines for administrators and system owners. These guidelines can be used any time a system owner brings up a new system or changes the existing system configuration and needs a best practices guideline for a security configuration."

For more information about CIS benchmarks, please visit http://www.cisecurity.org/bench.html. To register for a CIS benchmark account, visit http://members.cisecurity.org/.

**CISO, from Page 1**

customers expect significant interconnectedness, and this issue will grow ever more complex as we move forward.

As we put more emphasis on the value of identity, we require improved technologies for validating claims of identity. The password or pass phrase that has served as reasonable validation in the past is no longer sufficient to move forward. Multiple-factor validation, including physical or biometric elements, must be part of the Purdue solution for future security. The costs of local technology to meet these requirements are also likely to be prohibitive. Again, the message is clear that we need to continue to build the concept of a "Purdue identity" where these new technologies can be centrally developed, deployed, and effectively funded. That is the current mission for the IAMO.

As you discuss new projects and find yourself realizing that the application will have to ask the question "Is that your identity?", I ask you to contact the IAMO (iamo@purdue.edu) and discuss options and opportunities. We look forward to working with you and, please, continue to be careful out there.

# Purdue hosting CISSP classes

## Offered by ITNS and CERIAS

Beginning June 4, ITaP Networks and Security (ITNS) and the Center for Education and Research in Information Assurance and Security (CERIAS) will present a series of 12 information-security lectures to assist Purdue staff to become more knowledgeable about IT security.

These presentations are targeted toward Purdue staff who want to expand their knowledge and gain the most sought-after security accreditation—(ISC)2's Certified Information Systems Security Professional (CISSP) designation.

Any Purdue staff member may attend this series. Previous hands-on information security experience is not mandatory, but a working knowledge of information security concepts would be helpful.

The goal of these presentations is 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. It is not necessary to commit to taking the CISSP exam to attend the sessions.

The presentations are given by ITNS and CERIAS professionals who have themselves received the CISSP designation, as well as other Purdue professionals with subject matter expertise.

Topics to be covered include:

June 4: Reasons To Become a CISSP
June 21: Information Security & Risk Management
June 27: Access Control
July 5: Security Architecture & Design
July 10: Physical (Environmental) Security
July 23: Telecommunications & Networking Security
July 31: Cryptography
Aug. 7: Business Continuity & Disaster Recovery Planning
Aug. 14: Legal, Regulations, Compliance & Investigations
Aug. 21: Application Security
Aug. 28: Operations Security
Sept. 4: Exam Strategy: Pretest questions, etc.

**Any Purdue staff member may attend this series of presentations.**

Visit the SecurePurdue training site at www.purdue.edu/securepurdue/training/ for the list of dates, times, and locations.

Visit www.isc2.org for more information about the CISSP designation.

# ITNS streams Purdue president announcement

ITNS, in partnership with the the Purdue Hall of Music and the president's office, used Purdue's networks to stream the May 8 announcement of the new Purdue University president, France A. Córdova, across the Internet.

ITNS took additional steps to handle the expected high traffic, which was also driven by an announcement to 200,000 alumni inviting them to watch the streamed video of the announcement Monday evening.

Numbers were not available as of press time for the number of actual streaming video viewers, but ITNS reports no problems serving the Internet viewers.

## SPOTLIGHT

# Maintaining a secure, wireless Purdue

Purdue Air Link (PAL), an ITaP wireless initiative, first provided wireless access to students, staff, and faculty in the fall of 2002 with 100 access points. Availability is much greater today, with 1,300 access points located in 150 buildings across campus. The ITaP Networks and Security group (ITNS) manages the wireless environment to keep it running smoothly 24/7.

Brandon Case, an ITaP network engineer, doesn't think wireless will replace cable for all users. Brandon said, "We want the speed and reliability that the wired network provides. Cordless phones, blue tooth connections, cell phones, and other rapidly developing wireless technologies can degrade the wireless performance." PAL 1.0 first was implemented in 2001 with about 900 to 1,000 users. There are around 1,900 users of PAL 1.0 and PAL 2.0 with 90 percent using PAL 2.0. PAL 1.0 is maintained for those staff using older computers.

*Rogue wireless PAL 2.0 popping up:* Staff members working in Purdue buildings that are in close proximity to the many apartment buildings and non-Purdue buildings near them have noticed wireless networks that masquerade as Purdue's PAL 2.0 wireless network. Because anyone can set up a wireless network and call it PAL 2.0, it is very important to be sure you are connecting to Purdue's wireless network. Purdue does not broadcast PAL 2.,0 so if you are very far from a known access point and see a wireless network access point named PAL 2.0 it is probably not Purdue's PAL 2.0. When connecting to what you believe to be Purdue's PAL 2.0 wireless network, make sure there is a padlock icon by the PAL 2.0 entry in your connection window. This indicates you have a secure connection to the network which prevents other users of the network from viewing your activities. An unsecured connection allows information to be sent over the network unencrypted.

> "Be careful outside the wireless borders of Purdue."
>
> —Brandon Case, Network Engineer

If you have previously set up your PAL 2.0 connection, then the correct wireless connection should appear in your network connection window while you're on campus. The main concern here is that someone might not be aware they are connected to a non-Purdue PAL 2.0 network. If a user stays associated to a rogue PAL 2.0 network, all their traffic, including usernames and passwords, could be viewed unencrypted and result in the compromising of their computer or allow access to University information. Check the PAL 2.0 network connection in your network connections list, and if it does not have a padlock icon next to it, you may have connected to a rogue wireless network masquerading as PAL 2.0. If you find yourself in this situation, disconnect from the rogue network and immediately change your career account password and any other passwords you may have entered while using this unsecured connection.

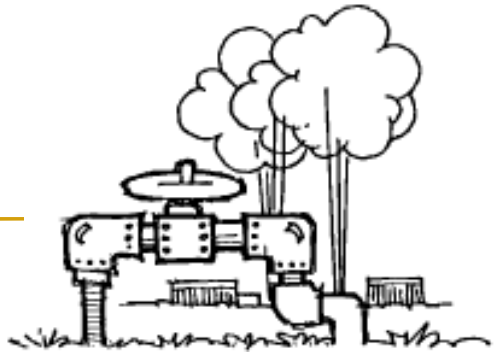
Another important security feature to enable is the option to validate the server certificate. The directions for setting this securely are on the Web site: http://www.itap.purdue.edu/airlink/setup/winxp.cfm, step number 7.

## STEAM-CIRT NEWS

### January 2007 summary and trends

Overall the number of events reported to the STEAM-CIRT increased by 59 percent from December 2006, while the total number of actual IT incidents more than doubled, outpacing STEAM-CIRT expectations. The increase is due to the return of students and faculty to campus after the semester break as well as new IRC Bot detection capabilities provided by the now active campus intrusion detection system.

At the beginning of January, a new campus intrusion detection system was installed to monitor traffic between the Purdue West Lafayette campus and the Internet. At this time, the IDS is a passive monitor that does not intercept or modify traffic in any way. The STEAM-CIRT handlers analyze alerts generated by the IDS and notify appropriate Purdue Security contacts if an IT incident is expected.



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 May 3)

| Viruses | Max. Occurrences |
|---|---|
| W32/Dref-AF | 25,448 |
| W32/Dref-AG | 26,902 |
| W32/Dolebot-A | 5,392 |
| W32/MyDoom-O | 1,382 |
| W32/Mytob-GH | 5,915 |
| Troj/Dorf-Zip | 12,821 |
| W32/Sality-AA | 526 |
| W32/Mytob-FO | 464 |
| W32/Mytob-BV | 191 |
| W32/Netsky-P | 161 |

## MILESTONES

# IT Networks aids robotics

## Makes competition possible with services

ITaP's Networks and Security group recently finished successful support work for the 2007 FIRST Robotics Competition (FRC) Boilermaker Regional March 15 through 17.

The Networks group provided a variety of services and support to make the event possible, including special data access points, printer support, servers for streaming video, telephone service, and network connectivity for officials, event coordinators, participants, and competition attendees.

This spring marked the third year the FIRST organization has brought its robotics competition to the Purdue campus. The 2007 event had about 40 teams of robots designed by high-school students from across the country and was attended by about 2,000 people.

Doug Magers, network engineer for ITaP's Networks and Security group (ITNS), said that the competition is an opportunity for he and his co-workers to showcase technology to people outside the Purdue environment. "It's exciting to have all these kids come in and build robots."

According to Magers, the 2007 event went very smoothly, and the ITNS group received much positive feedback.

"We provide the road your data rides on," Magers said. "That makes what we do much like a utility that you simply expect to work. Even so, we try to make the process so effortless for customers that they notice the great service and results."

The event coordinator, Krista Sturbois, had some very kind words for Purdue: "We love coming to Purdue because the people and the committee are so involved and make it so much easier on us. Many places we go to it's just I and one other person, but [at Purdue] everything is so organized, ready to go, and [the support staff] are so involved and do such a great job."

Another bit of positive feedback came to a network data liaison, Greg McCoy, from a woman in Germany who thanked Purdue for her ability to stream the competition video live across the Internet.

"She had a relative competing in the competition and was able to watch her, even though she had to be thousands of miles away," Magers said. "It was so important to her that she thought to write us a note about it. It was fantastic to hear such good feedback. It makes it all worthwhile. There are a lot of other groups and people involved in making an event come off, but we're proud of our role and it feels good that people use our services."

The FIRST (For Inspiration and Recognition of Science and Technology) organization was founded in 1989 by Dean Kamen, inventor of the Segway HT.

**SECURITY TIPS**

Make sure your anti-virus software is installed, up-to-date, and ACTIVE. Most anti-virus software packages show their activity using an icon in the system tray. Find out which icon means you're protected, and look for it every time you start your computer!

## 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*
- CISSP information and certification process
  *http://www.isc2.org*
- CIS benchmarks
  http://www.cisecurity.org/bench.html
- CIS benchmarks registration
  *http://members.cisecurity.org/*
- Purdue Air Link setup instructions
  *http://www.itap.purdue.edu/airlink/setup/winxp.cfm*