SECUREPURDUE NEWS
www.purdue.edu/securepurdue

May 2008
Volume 1, Issue 16

All the news that's secure to print.

## FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Last month I was asked about my view of major themes of "The Future" for information security for the coming years. This seemed like an interesting question to consider, even though my ability to see the future is no better than anyone else's. So I thought I would share my thoughts. I believe the future themes will break down into the following areas:

1. Successfully help the growing population of technology users (young and old) to understand the risks undertaken when "devices" containing valuable information are connected to "the network."

2. Provide simple-to-use tools and techniques that non-technical users can effectively apply to enable them to help themselves once they understand the risks in the "Cyber World".

3. Change the culture within the development, business, and higher education community so that information security is integrated into system and process design, and is not just an afterthought, bolt-on, or "somebody else's problem."

4. Implement creative technologies that, where possible, can embed security into all other technologies.

The common theme of all of these areas is that information security concepts need to become embedded in our culture. One of our SecurePurdue goals is to help enable that change. I do not believe that these areas are unique to higher education, however. Technology users are growing in all age groups. Students are now going to "computer lab" in kindergarten and pre-school. Those students will be Purdue students before we know it. Just as all ages learn the risks of walking down a dark alley, we must create that same cultural awareness for what "dark alleys" look like in the Cyber world.

## In this issue



Additionally, I believe that the future for technology usage at the University in the next few years will focus on "mobility." Mobility without security will not be effective, however. One of our strategic goals in ITNS is to establish a Secure Mobility infrastructure on and around campus. This infrastructure would include, providing access to secure applications "on the go;" converging technologies (data, voice, video); facilitating learning available anytime, anywhere; securing all sensitive data in motion; enabling secure social networking with the University community; and providing personal physical security information and options. In order to achieve secure mobility for campus users, creative and strategic partnerships will be required. These relationships will create new opportunities for integration, research, and collaboration. While there are very significant technology challenges in this strategy, I believe that the more difficult factors will not be technology based. In order to motivate understanding and create cultural change, we will need more than just technology. A complete and understandable set of policies, procedures, and best practices is a necessary foundation for this work.

**CISO continued, Page 3**

# End User License Agreements: A User's Guide

We all have done it, clicking "I agree" without reading the pages of terms that we are presented with before we can use a new program or service downloaded from the web. Often end users simply want to download an application or sign up for the service, and this information is merely a simple obstacle to get the product that the user wants. Reading this information is tough work. Often the font is small and the terms are written in legalese that would give any lawyer a test of an expensive law school education.

***Before accepting an end-user license agreement, make sure you understand and are comfortable with the terms of the agreement.***

Short for End User License Agreement, a EULA (pronounced "You-la") is a contract between the manufacturer or distributor of a piece of software or an application, and the end user of the application. The EULA dictates how the software or service can and cannot be used, and typically limits the ability of the end user to share the software with others.

Often these agreements are presented right before an application download screen or a service registration screen. The user has to click "I agree" before continuing to the download or registration page.

Not all EULAs are created equal, however. While many EULA detail the intellectual property rights held by the owner of the application, some EULAs actually contain terms that would allow the application owner to install additional software onto a computer system to ascertain the user's internet habits (agreed-to spyware). A EULA might also contain hidden licensing fees or deeply buried upgrade, support, or maintenance fees.

Look for some of the following issues before agreeing to your next EULA:

-Product Use: Does the EULA reserve the right to change the service and/or product supplied and end certain supplied features?

-Representations and Warranties: Does acceptance of the EULA mean that the end user bears all economic and other risk related to downloading and using the software (i.e., risk with respect to viruses, errors, data loss, hardware/software costs, installation charges, etc.)?

Does the EULA specifically state that use of the software and service is at the user's own risk?

-Termination and Breach: Does the EULA allow an end user to terminate the EULA at any time by uninstalling and destroying software and documentation?

-Advertising: Does acceptance of the EULA state that the end user specifically authorizes embedded software or other advertising that "comes with" the download of the intended product (i.e., Does the EULA allow adware/spyware)?

Does user acceptance of the EULA also consent to advertising content, either from the vendor or other third party vendors? Does acceptance of the EULA allow the vendor to collect usage data and other statistics related to use of the service from the end user? (And how will this data be used?)

-Product Criticism: Does the EULA specifically prohibit the end user from publicly criticizing the product?

-Software Updates: Does the EULA state that software updates are covered by the original EULA or by a subsequent EULA that end user must specifically agree to?

**End User Agreement continued, Page 3**

# SPOTLIGHT

## End User Agreement continued

-EULA Boilerplate Terms: Does the EULA state that it is subject to change without notice, and that the end user specifically consents to any modifications of the EULA without notice?

If the End User License Agreement that you are reviewing includes some of these terms, it may be time to take a step back and think about the application or service that you are attempting to download or access. You will need to balance your need for the use of the service or application with the amount of additional information that you might be supplying to the vendor, and the other contracts that you might be subjecting yourself to.

## CISO from Page 1

This can't just be "documentation", however. It must be something that "lives" in the University community. The continued expansion of the SecurePurdue outreach programs is fundamental to achieving a "living concept." All members of the information security teams at Purdue are going to need to be visible members of the Purdue community, giving information security a "presence" and helping to change the culture. The Security Officers group has made significant advances in this area, but there is much more work to do. When these visions are realized, students, faculty, and staff of Purdue University will have a unique, mobile and secure environment to achieve the University vision of discovery, engagement, and learning.

While I have the future in sharp focus, there is one more thing. The Cubs will win the World Series, too.

As always, thanks for reading and be careful out there.

# 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 e-mail viruses

The following list is a 30-day snapshot of the most active e-mail 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 April 25th, 2008)

| Viruses | Max. Occurrences | Last Occurrence |
|---|---|---|
| W32/MyDoom-O | 168 | 71 |
| W32/Netsky-P | 56 | 20 |
| Troj/Pushdo-Gen | 573 | 0 |
| Mal/Iframe-E | 52 | 16 |
| Mal/Behav-004 | 563 | 0 |

# MILESTONES

ITNS is a great group of people!!

Scott Ksander, Executive Director of IT Networks and Security and Chief Information Security Officer, was named a finalist for the the 2008 Information Security Executive of the Year Central award for the central region on April 17, 2008, in Dallas, Texas.

Ksander was nominated for the award by his colleagues in ITNS for his efforts in the Secure-Purdue initiative and was one of 21 nominees for the award. Nominees were information security executives from a number of different industries and U.S. government departments. Scott was the only representative of a higher education institution. Ksander was excited to be a higher education representative for the region.

"Being named a finalist for this award is a great acknowledgement of the success of the entire SecurePurdue team," Ksander said.

"Being the only Higher Education finalist in the company of major corporations such as Texas Instruments, Dow Chemical, and EDS is a great honor."

The Executive Forum and Information Security Executive of the Year Central Awards 2008 (ISE Central Awards 2008) is spearheaded by Executive Alliance in partnership with some of the leading technology and media companies in the industry.

The award recognizes the individual who has demonstrated outstanding leadership in the field of information security in the central region, which includes Arkansas, Illinois, Indiana, Iowa, Kansas, Louisiana, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, Oklahoma, South Dakota, Texas and Wisconsin. The winner of this year's award was Brian Wrozek, an IT Security and Disaster Recovery Manager from Texas Instruments, Inc.

# SECURITY RESOURCES

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

• *Purdue University IT Resource Acceptable Use Policy*
http://www.purdue.edu/policies/pages/information_technology/v_4_1.html