SECUREPURDUE NEWS
www.purdue.edu/securepurdue

May 2009
Volume 4, Issue 2

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Wikipedia, an often-cited source of all knowledge, defines "Web 2.0" as "a perceived second generation of web development and design, that aims to facilitate communication, secure information sharing, interoperability, and collaboration on the World Wide Web." I was happy that the word "secure" made it into the definition. Sadly, however, much of this type of development has been quickly designed, prototype style, and is highly vulnerable from a security standpoint.

When Willy Sutton, a depression era bank robber, was captured in 1950, a reporter asked him why he robbed banks. Sutton's now-famous reply was, "Because that's where the money is." In today's world we might well ask why bad guys target web applications. The analogous answer would be because that is where the data is accessible and where security is the weakest .

Data from Purdue's own border intrusion detection system shows that 77% of all detected intrusions are aimed at Purdue's web applications. Nearly 42% of those events are attempts to gain administrative or privileged access on those systems.

ITNS has scanned 104 web applications in recent months. Application scanning is a new technology that we have deployed recently as a SecurePurdue initiative. These scans took place on a range of web applications--from highly directed departmental applications to widely used enterprise-level applications. Usage of these applications resulted in the scan of almost 50,000 unique URLs. Over 50% of those URLs showed security issues! Over 10% of the issues were categorized as high risk by current industry standards. Furthermore, 71% of the issues were attributed to application-related problems. The remaining issues were either infrastructure or platform security related.

In this issue

The combined message from the growth of Web 2.0 and our own security scanning is clear: Web applications are going to be an important part of our service delivery model, but we must find better ways to insure the integrity and security of these applications.

Our web application scanning technology will help us catch problems more quickly. However, it is imperative that we also find ways to not insert the problems in the first place. A problem found in the development phase or before we sign a contract with a vendor is always going to be less expensive to correct than one found by scanner or, worse yet, by a malicious individual targeting the production application. If your organization is involved in developing or deploying web applications, please don't forget proper development and programming principles with a focus on testing and security. Properly developed and thoroughly tested web applications will go far in securing Purdue web-based services.

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

802.11n Popping Up on Campus

The new Armstrong building is sporting a new technology: 802.11n wireless connections are now available. Several more buildings on campus will be updated by the end of 2009.

What is 802.lln?

IEEE 802.11n is a proposed amendment to the IEEE 802.11-2007 wireless networking standard. 802.11n proposes to significantly improve network throughput over previous standards, such as 802.11b and 802.11g, with a significant increase in the maximum ray (PHY) data rate from 54 Mbit/s to a maximum of 70-100 Mbit/s.

So, what are the benefits of 802.11n?

Users will notice two things about this new and improved wireless technology: significantly greater speed and range. The faster speed is especially noticed when streaming video or for game enthusiasts.
The increased range of 802.11n will mean fewer "dead spots" in places served by a single Wi-Fi router. It also will open the way to high-bandwidth applications such as streaming video from, say, desktop computers that store video to Wi-Fi-enabled televisions. The new standard will also be more reliable for voice-over-IP and, in general, for multiple users doing multiple things over the network.

Review the Wireless Network Acceptable Use Standard at:
http://www.purdue.edu/securepurdue/bestPractices/wirelessUseStandards.cfm
http://www.purdue.edu/securepurdue/help/view.cfm?KBTopicID=238

POWER DOWN for the PLANET

Information Technology at Purdue (ITaP) and Purdue Sustainability Council officials are encouraging the campus community to make "powering down" personal computers as common a practice as turning off a car and shutting refrigerator doors. ITaP and Purdue Convocations are offering incentives for pledging. Details can be found in the news article. To learn more, visit http://news.uns.purdue.edu/x/2009a/090323McCartneyChallenge.html

Other energy saving tips:

1. Don't use a screen saver. Screen savers are not necessary on modern monitors and studies show they actually consume more energy than allowing the monitor to dim when it's not in use.
2. Turn down the brightness setting on your monitor. The brightest setting on a monitor consumes twice the power used by the dimmest setting.
3. Turn off peripherals such as printers, scanners and speakers when not in use.
4. Fight phantom power; plug all your electronics into one power strip and turn the strip off when you are finished using your computer. When feasible, unplug the power strip from the wall to avoid high-voltage surges which may occur during an electrical storm.
5. Use a laptop instead of a desktop. Laptops typically consume less power than desktops.
6. Close unused applications and turn off your monitor when you're not using it.
7. Use a power meter to find out how much energy your computer actually consumes and to calculate your actual savings.
8. Establish multiple power schemes to address different usage models. For example, you can create a power scheme for playing music CDs that shuts off your hard drive and monitor immediately, but never puts your system into standby mode.

Purdue University is an equal access/equal opportunity/affirmative action university.

SPOTLIGHT

Telephone Office Billing

"Four years ago the telephone portion of ITNS, with the assistance of Informatics, launched a web site for easier viewing of telephone billing information. This site was created to securely and quickly deliver telephone billing data to Purdue employees as well as empower them to store and manage that data without the need for printed records.

Prior to the creation of the website the monthly billing, preliminary review, and annual/quarterly reports were generated as printed copies. This resulted in roughly 15 reams of paper being used monthly. Through the creation of the website, the University has not only realized savings in reams of paper but also in time and money that used to be spent manually sorting papers, stuffing envelopes, and mailing the reports out monthly.

Currently the billing information is posted to the website as soon as the charges are posted to SAP. This in turn saves employees the delay of waiting for a paper copy. The ITNS Telephone Office Billing website has been extremely beneficial to campus. It has provided the campus wide business offices as well as individual users the ability to access, manage, and maintain their telephone billing information in a timely manor; as well as providing additional environmental and monetary benefits."

How do you know who your e-mail is really coming from? When sending e-mails, how can you be sure your data is safe from prying eyes? PGP is one answer.

PGP, or "Pretty Good Privacy," is a technology that utilizes a signature key to allow you to verify your identity to others as well as to verify the identity of people sending you e-mail. These keys act like electronic ID cards, which can then be verified with a trusted source to validate that the person sending the e-mail is who they say they are. PGP can also be used to encrypt or decrypt data in e-mails, files, or even entire computer hard drives, keeping your data secure and ensuring that only those with the proper keys can unlock their contents.

IT Networks & Security recently implemented PGP for the Purdue Telephone Office billing e-mails. The Purdue Telephone Office has selected PGP signatures as a way for you to verify that telephone billing e-mails that come from that office are authentic. For further information describing how to make use of the PGP signature featured on the Purdue Telephone Office billing e-mails, please search for the knowledge base article number 003793 located at help.itap.purdue.edu .

MILESTONES

Educational Security Incidents - Review 2008

The Educational Security Incidents (ESI) serves as a clearinghouse for compiling data on information security incidents that have occurred at higher educational institutions. ESI provides a single point of reference for educational faculty and staff researching the various security threats that colleges and universities face. In February 2009, ESI released its Year in Review-2008, which looks at the reported information security breaches that colleges and universities faced in 2008. The statistics are compiled using information security incidents at colleges and universities that were reported in news media.

In 2008, ESI reports that 173 different information security incidents occurred at 178 different colleges and universities; exposing a total of 4,880,052 records. The number of incidents reflects a 24.5% increase over 2007, and the average number of records exposed per incident is 28,208. ESI categorizes security incidents as follows:

- Employee Fraud: Incidents involving fraudulent activity by employees (6% of 2008 incidents)
- Theft: Incidents involving the theft of physical mediums such as drives, equipment, or printouts (23% of 2008 incidents)
- Impersonation: Incidents involving one individual(s) masquerading as a different individual(s) or organization (2% of 2008 incidents)
- Loss: Incidents involving the loss of physical mediums such as drives, equipment, or printouts (5% of 2008 incidents)
- Penetration: Incidents involving the breach of computer software, a computer system or a computer network (20% of 2008 incidents)
- Unauthorized Disclosure: Incidents involving the release of information to unknown and/or unauthorized individuals (44% of 2008 incidents)

ESI also catalogs the type of information exposed during a security incident. Those classifications are educational information, financial information, medical information, personally identifiable information, Social Security numbers, and usernames and passwords. The 2008 report shows that unauthorized disclosure of records continues to be the number one security incident at colleges and universities and personally identifiable information continues to be the most common information exposed.

Purdue University had no security incidents listed in the 2008 ESI report.

The statistics compiled by ESI illustrate that there are a number of types of confidential information held by colleges and universities that needs to be protected. Purdue University continues to take many steps to protect the personal information entrusted to it under the auspices of the SecurePurdue program. To read more about security awareness, visit www.purdue.edu/securepurdue.

SECURITY RESOURCES

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

- Confidential Document Destruction Service visit *http://www.purdue.edu/securepurdue/files/Shred_Singlepage.pdf*

- To learn more about the University's Data Handling requirements for printed information, visit: *http://www.purdue.edu/securepurdue/procedures/dataHandling/printedInfo.cfm*

Confidential Paper Recycling Program a Valuable Service to Purdue

Since October 1999, Purdue Refuse and Recycling has operated the Confidential Document Destruction Service. Known informally as the "Blue Barrel Program," Purdue currently has over 400 blue secured confidential recycling bins around campus. These bins are used in a number of academic and business areas to properly dispose of University restricted and sensitive information

Scott Ksander, Chief Information Security Officer for Purdue University praises the Confidential Document Destruction Service program. "Having a reliable, auditable and secure mechanism in which to dispose of the University's highly confidential data is very important for the University's many regulatory requirements, as well as for complying with the University's own Data Handling requirements," Ksander said.

Departments that are using the bins are responsible for ensuring that it is kept in a secured and controlled area while the bin is in their possession. When Recycling collects the bin, it is locked and transported to a secure location at the recycling center where it is stored until it is securely shipped to a vendor for shredding. Under the program, Purdue Recycling provides the locked bins free of charge and departments are only charged a modest per-pound rate for the paper that is shredded.

Joel Zarate, Refuse Recycling Coordinator for Purdue University stresses that it is important for departments using the bins to ensure that they remain locked and stored in a secure location until Recycling is called to pick up the bin. "Most departments leave the bins in secured offices, labs, or work areas, which is a requirement of participating in the program. The confidential bins cannot be taken out of a building or moved from its secured location without contacting the departmental contact person. These requirements really help us protect the security of our confidential paper," Zarate said.

According to Zarate, the Confidential Document Destruction Service has been very successful and has grown nearly 600% since its first year of operation. "Almost 91 tons of confidential materials have been recycled in the current operating year," Zarate said.

For Ksander, this is good news. "Proper data destruction is a very important part of the information security lifecycle. Properly using the Confidential Document Destruction Service really goes a long way in keeping paper-based data secure and just is good common sense."

To learn more about the Confidential Document Destruction Service, visit http://www.purdue.edu/securepurdue/files/Shred_Singlepage.pdf

To learn more about the University's Data Handling requirements for printed information, visit http://www.purdue.edu/securepurdue/procedures/dataHandling/printedInfo.cfm