SECUREPURDUE NEWS
www.purdue.edu/securepurdue

December 2010
Volume 5, Issue 4

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

It is that time of year when many people will be traveling for holiday gatherings. If flying is required, you may notice some changes to the now routine security procedures. Hopefully, a TSA pat down won't be part of that experience! Over the years since 2001, those security procedures have increased in response to new and evolving threats. A process of risk assessment targets the threats and then a decision is made how to search for that threat and implement a procedure to mitigate that threat. This is much the same process that those of us in computer security go through. The problem is that it is difficult to imagine what terrorists will think up next. I don't think like a criminal, you probably don't either. So it is hard to stay ahead of them and protect ourselves.

Computer security has a history a lot like the airport security scenario. People have been flying since the 1950's but is has just been over the past 10 years that security has escalated. Similarly when the internet was born in 1969 it was relatively "safe" until the 1980's when various attacks began to emerge. Who can forget the "I Love You" worm in 2000? The variety of attacks created a variety of security responses.

With the emergence of Phishing or social engineering, hackers tried to get you to infect your own computer instead of them gaining access the hard way.

Users flocked to social networking sites, like Facebook and Myspace, and in 2008, the Koobface computer worm targeted this group. New variants appear constantly as hackers follow where the majority of people move on usage of the internet.

Cell phones, iPads, Kindles, all these indispensable tools for today's highly mobile society come equipped with built-in hardware, GPS receivers, wireless interfaces and vulnerabilities. As more people flock to using a new device, more hackers find vulnerabilities and ways to break through your security. Unfortunately, features often trump security until it gets bad enough and security products are built into stabilize the devices.

As a user of various online sites for shopping, professional organizations, health insurance sites and investment sites, I have a total of 96 different passwords. I have to use a password vault to keep track of all of them. It is a nuisance but necessary for protecting my identity and my data access.

All these procedures are meant to keep us more secure but it is not without a cost of convenience and time. It is a trade off for the technology we enjoy and the risks we incur using them.

The security procedures imposed on travelers change as new threats arise. The same is true for computer security protection. Layers of security work at the airport and on your network and computer. With a few simple routine procedures in place, like updating your anti-virus, and software packages, and just stopping to think before you click either to check out a link from an email that your wife's third cousin sent you or to purchase gifts online, you can stay safe and calm over the holidays with the extended family.

Enjoy your holidays, be careful with new technology "toys" you may receive and as always, be careful out there.

In this issue

Happy Holidays from ITNS!

As the holiday season quickly approaches, many of us look forward to exchanging gifts with friends and family. To increase the chances that your online shopping experience this year is a safe one, we offer the following reminders:

- Keep your operating system's firewall turned on.
- Ensure that your system software and all applications are up to date.
- Use antivirus and antispyware software.

See www.purdue.edu/securepurdue/download for current versions of security software that you can install on one personal computer at home.

- When using your computer, use a standard user account, and not an "administrator" account.

Whether you are reading e-mail, browsing the web, or chatting in an instant messaging client, you may

Remember, caveat emptor! Offers that seem too good to be true online often are.

see offers for free shipping, bargain basement prices or expedited shipping flash across your screen. Remember, caveat emptor! Offers that seem too good to be true online often are. Instead of clicking on a dubious link and putting your finances or identity at risk, open your web browser and visit the web presence of well-known retailers to comparison shop for yourself. Always check to make sure that the website is secure before entering credit card information or personal identification.

If you are traveling this year, and plan to take a Purdue owned laptop with you, keep in mind that you must have a current Property Accounting Form 12 on file with your business office. See your supervisor for details. Also, make sure you have a complete backup of your data to come home to in case equipment is lost, stolen, or damaged.

If you will be conducting business while you're off site, use the appropriate Purdue Virtual Private Network (VPN) client software, and beware of unsecured wireless networks, where it is easier to have your user ID, password, and data harvested. Remember - you are also responsible for complying with Purdue's security requirements whenever you view, update, or delete University data. See http://www.purdue.edu/securepurdue/procedures/dataHandling1.cfm for details.

Finally, before you leave home, consider shutting down your computers to save energy and turning off or unplugging your router(s) and wireless access point(s) to safeguard your home network while you are away.

It is our hope that by reviewing these tips and being mindful of security awareness that we can all have a safer, and happy holiday season this year.

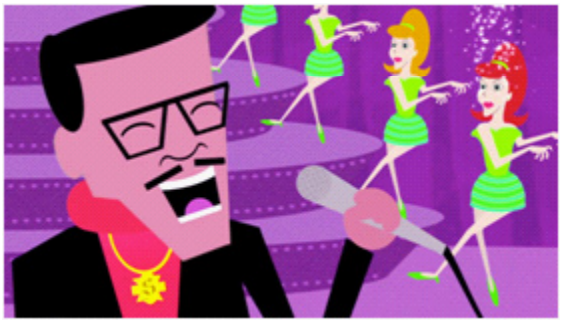
New Data Handling Educational Resources Available

How the University handles the vast amounts of data entrusted to it continues to be something that every Purdue employee is interested in. The Purdue University Data Stewards Organization has recently created an Educational Resources webpage . The new webpage features new and revised data handling training resources. The newest resources include a data handling power point presentation and an updated version of the "Keys to Securing Purdue's Data" pamphlet.

http://www.purdue.edu/securePurdue/policies/dataStewards.cfm

http://www.purdue.edu/securePurdue/procedures/dataClassif/Resources.cfm

New Purdue Cybersecurity Training Video



View the latest SecurePurdue Cybersecurity Training Series Video on Social Networking. The video was created by the Video and Multimedia Production Services (VMPS) group within Information Technology at Purdue (ITAP).

You can view the video at: http://www.purdue.edu/securepurdue/videos/socialNetworkPrivacy.wmv

You can view other videos at: http://www.purdue.edu/securepurdue/training/

SPOTLIGHT

ITNS Facts

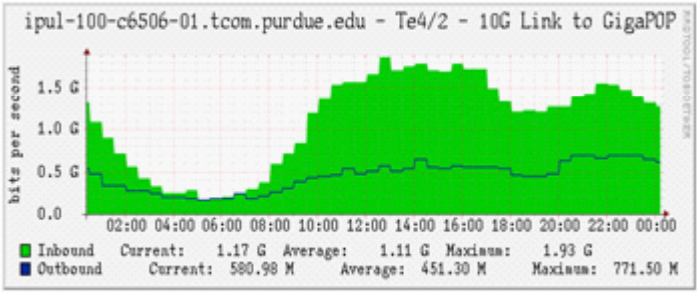
Telephone Office Facts
- Number of active telephone lines - 20,700
- Biggest telephone office in Tippecanoe county
- 614 miles of fiber optic cable installed
- 485 miles of copper cable installed
- Voice service orders - 8,134/yr
- Voice Trouble tickets – 1,339/yr
- Data service orders – 11,589/yr
- Telephone switch calls processed - 22,672,736/yr
- 2,000 wireless Access Points installed covering 3.7 million sq. ft.
- 40,500 active wired data ports
- 138 UPS units in service protecting network equipment
- Networking active in 255 "buildings"
- 568 network equipment "sites"

	2006	2007	2008
Number of Telephone Lines	20,483	20,639	20,722
Total Number of Calls	26,258,794	24,658,106	22,672,736
Voice Mail Answered Calls	5,985,604	5,442,601	4,786,699
Voice Mail Users	18,816	18,965	8,514

A Typical Day in the Networks

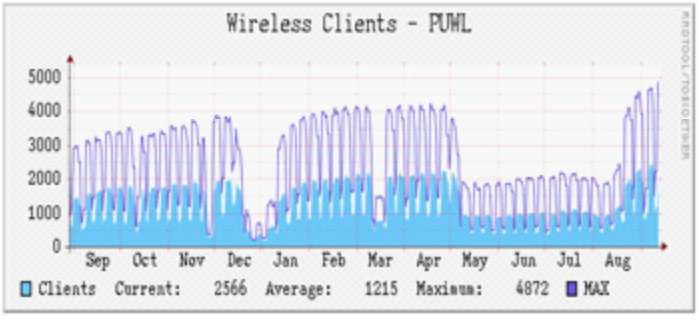
Ports
- 23,800 in academic/business areas
- 13,000 in student rooms
- 2,600 in Math for RCAC Research clusters
- 1,700 in Freh/Haas/Math for Data Center

Equipment
- 255 buildings
- 568 network equipment sites
- 3,030 network devices



Wireless Growth

- Now have 2,000 Access Points
- Covers approximately 3.7 million SqFt.
- Routinely over 4,000 simultaneous active users



Identity Access Management Operation Trends
Increased use of IAMO authentication services
- New services supported by ITAP (incl. regionals)
  - Several new web applications
- New services provided at the department level
  - HR, SATS, CFS, and a number of others

Increasing use of CAS authentication
- Single sign-on experience for web applications and services

Interest in Federated Authentication services

Network Initiatives
- 802.11n project
- SIP Enable switch to project voice services to wider network
- Green initiatives for cabling design (researching latest trend in LEED credits for technology products and processes) i.e. re-use of existing cable plant in Mackey proper rather than re-cable the entire building to match the Mackey addition
- Green projects for paperless billing and paperless records system
- Web billing information for customer access
- Voice Mail Replacement in 2009 (Unified Messaging opportunities)
- WAN capacity upgrade (10Gb/s to Internet2)
- Campus core upgrade for redundant "Virtual Switching System"
- Building strategic partnership with Cisco
- Considering other strategic partnerships (HP, McAfee)