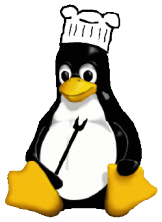
The Open Pitt

What's cooking in Linux and Open Source in Western Pennsylvania



Issue 10 | March 2005 | www.wplug.org

CPLUG Security Conference Notes

About twenty WPLUGers made the trek out to Messiah College near Harrisburg for the Central Pennsylvania Linux Users Group (CPLUG) Security Conference on March 5. Paul Moran of Potential Technologies `<http://www.potentialtech.com/>` *helped contribute to this review of the day's events.*

The CPLUG Security Conference was a fantastic first time event. Even if security is not your primary responsibility, there was plenty to keep any Linux or UNIX user interested.

Ed Reed, Novell's security tzar, gave the keynote address. He offered some great perspective on the role Novell will be playing in bringing SuSE Linux into mainstream business environments. His high-level overview covered the current state of computer security and what the near future holds. In a humorous slip of the tongue while discussing the SuSE product line, he said that it takes about 18 months to "incorporate the newest problems" from SuSE desktop Linux into the Enterprise edition.

State Trooper Jon Nelson spoke on Pennsylvania's computer crime law passed in 2002. The audience was so inquisitive that he was unable to complete his talk, taking up an extra hour without protest from anyone in the room. See the article on page 2 for a detailed review of the law.

Eric Andreychuk of CPLUG, the primary organizer of the event, gave an overview of Security Enhanced Linux (SELinux) using White Castle as a metaphor. User Sean takes on different roles at the burger joint with the *newrole* command and gains access to different domains and objects as his role changes.

Protecting against buffer overflows and other memory-based attacks was the subject of Brandon Hale's talk. The Hardened Gentoo team member discussed protection techniques used by the project such as the no-execute bit available in some processors, randomizing a process' address space with ASLR, stack-smashing protection, and role-based access control.

Russell Coker of Red Hat, who traveled here from Australia for the SELinux Symposium in DC, spoke about his experience running "play machines." Systems using SELinux are put on the Internet, and Russell gives away the root password, challenging all comers to break out of the constraints imposed by SELinux.

Marcus Ranum captured great interest from the audience. His approach to examining and organizing logs using *syslog-ng* was two days of information crammed into a one-hour crash course. His method involves profiling "normal" activity and only attracting the administrator's attention when an anomaly appears.

The lightning talks could have filled another full day of topics but were instead limited to five minutes each under threat of being gonged off the stage. WPLUG's own Bill Moran and Beth Lynn Eicher respectively spoke about the Survivability and Information Assurance program and Kerberos.

Overall, the turnout was great, the room stayed full for most of the day, and there was plenty of food and prizes for the 150 or so in attendance. There was talk of this becoming an annual event and for good reason. Great work by the organizers who got a list of generous sponsors to help make the event fun and affordable.

If you weren't able to attend the conference, copies of each speaker's slide presentation can be downloaded from the conference web site at `<http://cplug.net/conference/>`. The organizers intend to make a DVD of the event available. Keep watching their web site for details.

February Roundup

Feb. 5 General User Meeting: **Ted Rodgers** discussed RPM—the package format originally developed by Red Hat but now used in many Linux distributions. He explained the difference between source and pre-packaged binary RPMs, as well as some of the incompatibilities you can run into when trying to install an RPM built for one distribution onto a different one. He described the many options to the *rpm* command and reviewed some of the front ends available to make life easier for casual users. Another important subject was how to resolve dependencies.

Feb. 19 Tutorial: **Beth Lynn Eicher** covered the basics of Linux system administration including handling disk devices, controlling which system services are run, managing multiple users, and sharing files over networks via NFS.

`Tutorial - <http://www.wplug.org/meetings/one-meeting?wp_meeting_id=3171>`

Coming Events

Mar. 19: General User Meeting, Topic: Kernel Basics. 10AM to 2PM, 1507 Newell-Simon Hall, CMU

Apr. 9: General User Meeting, Topic: Managing a Small Open Source Project. 10AM to 2PM, 1507 Newell-Simon Hall, CMU

Apr. 23: Event TBA. 10AM to 2PM, 1507 Newell-Simon Hall, CMU

May 21: Installfest. 10AM to 5PM, 1507 Newell-Simon Hall, CMU

May 28: General User Meeting, Topic: Version Control with Subversion. 10AM to 2PM, 1507 Newell-Simon Hall, CMU

The public is welcome at all events

Bad Boys, Bad Boys *by Logan Stack*

When Pennsylvania State Trooper Jon Nelson continued talking about Pennsylvania's computer crime law for nearly an hour past the scheduled time, no one objected except one guy who was concerned that he wouldn't be able to both hear what Nelson had to say and get pizza, since his remarks were running through the lunch break.

Nelson's talk was extended, in part, by the usual questions from people trying to make sure that the law didn't criminalize what they do normally on their job such as routine backups. A couple of people asked hypothetical questions that didn't sound too hypothetical, such as: "What if someone were to, say, log all traffic on an open network at a security conference?"

One surprise to me was that war-driving may be illegal. Section 7611 says, "A person commits the offense of unlawful use of a computer if he: intentionally and without authorization accesses or exceeds authorization to access…any computer, computer system, computer network…"

That means if you're sitting at Starbucks and accidentally connect to the network belonging to the geek next door, you're fine. But if you go around the city with a laptop, intentionally trying to find networks which you know you're not authorized to use, that is a crime.

However, the law also says, "It is a defense to an action [if] the actor: reasonably believed that he had the authorization or permission of the owner" (section 7605). This could cover war-driving, as the courts may decide that you can "reasonably believe that you had authorization" when a network is set up to allow anyone to connect to it. That, of course, will depend on how the courts choose to interpret the language.

This law is sweeping. It covers everything from defacing IBM's web site to releasing a virus. It is written in very broad terms and defines a computer as a "high speed data processing device or system which performs logic, arithmetic, or memory functions." Under that definition, if your boss's secretary can file documents quickly, she might qualify.

I was not able to find any case law which would provide some clarification. This isn't surprising, as the bill was only passed in 2002. With a law so young, many provisions have not yet been tested. Eventually, a judge may deem war driving to be legal but not more sinister activities such as crashing computers or altering someone's web site.

So what else is illegal? Well, the law's definition of a "computer virus" could land a programmer in jail if he "knowingly sells, gives or otherwise distributes... computer software or a computer program that is designed or has the capability to:…degrade, disable, damage, or destroy the performance of a computer" (section 7616). There is no word yet on whether Microsoft Windows fits this definition.

Sending e-mail "with the intent to falsify or forge electronic mail transmission information" (section 7661), which could include sending mail from an address which you don't own, is also covered. So the old pranks where you send e-mail to your friend from `billy_g@microsoft.com` or `dubya@whitehouse.gov` could be illegal. The upshot of that is that any spammer who sends you mail from your address or the address of your friend probably has committed a crime too. Unfortunately, he will not spend time in jail for it because under the law this is a misdemeanor with a maximum fine of $2500 and no jail time. Before you start imagining collecting millions, keep in mind that part of this falsification is almost always to conceal the original sender, making it nearly impossible to track down spammers and fine them.

So what happens if you're spammed by someone in Florida, or someone local defaces a web site in Utah? A translation of the legalese in section 7602 says an offense was committed either where they did it, or where the victimized computer was. The person from Florida can be extradited to a Pennsylvania court, and Pennsylvania will indict a local criminal for defacing a web site elsewhere.

Trooper Nelson also reviewed the Computer Security Institute/Federal Bureau of Investigation survey of major companies' security. He didn't have permission to reprint this information in the online version of his notes. The survey may be obtained for free, however, if you register at `<http://gocsi.com/>`.

The law isn't that obtuse or long, and it is available online at `<http://www.legis.state.pa.us/WU01/LI/BI/BT/2001/0/SB1402P2429.HTM>`. However, as the law itself and a member of the audience point out, it's certainly not the only law on the subject; there are additional federal and state laws addressing computer issues, including the infamous Patriot Act.

Logan Stack is a student at Penn State.

The Open Pitt is published by the Western Pennsylvania Linux Users Group
`<http://www.wplug.org/top/>`

Editors: Elwin Green
Vance Kochenderfer

What is Linux?

Linux is a *kernel*, the core of a computer operating system, created by Linus Torvalds. It is typically packaged as a *distribution*, which includes the extra programs necessary to make a computer functional and useful. Since 1991, it has grown from a one-man project which ran on one computer to one with thousands of contributors running on everything from personal organizers to million-dollar supercomputers.

What are Open Source and Free Software?

Open Source and Free Software provide you, the user, with the opportunity to see the source code of the programs you use. You are free to use it, share it with others, and even make changes to it if you wish. While the Free Software and Open Source communities differ in their philosophical approach, in practical terms they share nearly identical goals. Learn more at `<http://www.opensource.org/>` and `<http://www.gnu.org/>`.

This newsletter was produced using Open Source and Free Software.