

October, 2003
Vol. 13, No. 4

TeraWord

The Newsletter of High-Performance Computing and Communications in Nevada

**Special
Security
Issue**

Contents

Security, Security Security!	1
NSCEE and HIPAA	1
Research Activities at NSCEE	2
Help Desk	
SSH - Secure Shell	3
Firewalls and Intrusion Detection	3
Do's and Don'ts of Securing your Desktop System	3
Upcoming Network and System Security Related Seminars	4
Accessing Mail Securely Using pop3 Over ssl	4
NSCEE Hires	
Network Security Administrator	4
Articles Invited	4

Security, Security, Security!

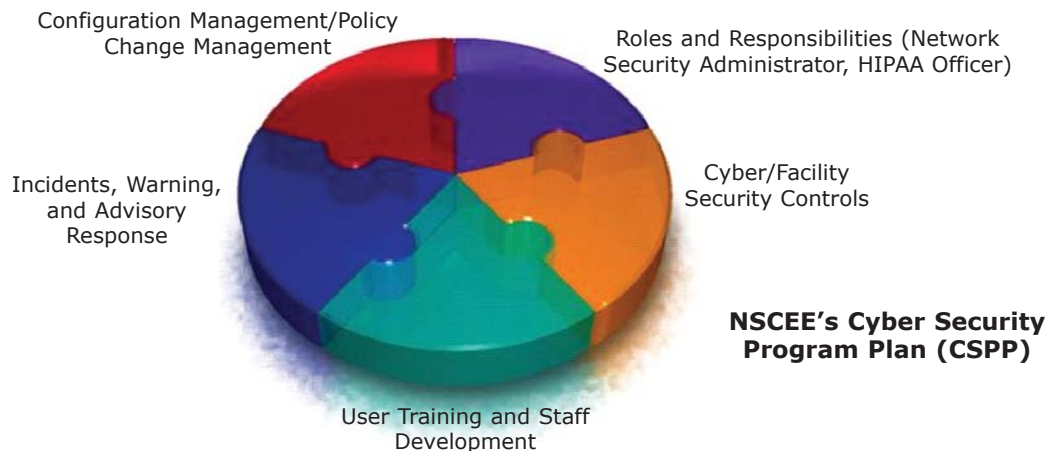
The number and potential severity of cyber security attacks is increasing. In the first quarter of 2003, the Computer Emergency Response Team (CERT) at Carnegie Mellon University received more than 42,000 reports of network attacks and intrusions. That's more than half of the attacks reported in all of 2002, indicating the number of incidents could well be on its way to quadrupling in 2003.

These numbers underscore the need to ensure that the NSCEE works quickly, aggressively and cooperatively to upgrade facility security features. A blueprint for this daunting task is already in place and described within the NSCEE's Cyber Security Program Plan (CSPP). The CSPP represents a two-year collaborative effort between the NSCEE and DOE's National Nuclear Security Administration (NNSA). The CSPP became operational in June 2002 after it was reviewed and approved by NNSA.

The CSPP outlines a number of activities and steps to secure the cyber environments.

Accomplishments to date include:

- a new Network Security Administrator has been hired (see page 4),
- a CSPP has been created and approved by NNSA (June, 2002),
- firewalls and intrusion detection systems have been installed and configured,
- a 24-hour facility access and monitoring system has been installed and configured,
- a Health Insurance Portability and Accountability Act (HIPAA) officer has been identified,
- a new Uninterruptible Power Supply (UPS) will be installed in fall 2003,
- regular user and staff training sessions have been scheduled, and
- a Disaster Recovery (DR) Site has been identified and will soon be operational.



NSCEE and HIPAA

NSCEE is involved in a number of projects that require HIPAA compliancy, among them the Nevada E-Health Initiative and Medical Records Knowledge and Information Management for Radiation Workers.

What is HIPAA?

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA), which went into effect on April 14, 2003, is intended to improve the efficiency and effectiveness of the health care system by standardizing electronic data interchange.

HIPAA has three main parts: (1) Insurance Portability, (2) Fraud Enforcement (accountability), and (3) Administrative Simplification.

Portability ensures that individuals moving from one health-plan to another will have continuity of coverage and will not be denied coverage under preexisting condition clauses. **Accountability** increases the federal government's fraud enforcement authority in several areas. The third component, **administrative simplification**, was developed to provide privacy protec-

Research Activities at NSCEE

UNLV Cybermedia Research Center (CRC) Update

In its August meeting, the University of Nevada Board of Regents approved a new research center in Cybermedia. The Cybermedia Research Center's new Director is Hal Berghel, also the Director of UNLV's School of Computer Science. Berghel brings to the Center over fifteen years of research experience in Internet and World Wide Web technologies.

According to Berghel, the concept of a "Cybermedia" dates back to the Fall of 1999 when Berghel first came to UNLV. "I wanted to add a new strategic research direction to UNLV's capabilities - one that included both experimental networking (the "cyber" part) and advanced media applications (the "media" component). I coined the term to reflect the dual emphasis," Berghel reports.

CRC is organized into several relatively autonomous labs. Both the Graphics Lab and Visual and Sound Processing Lab, located on campus, are under the Direction of Professor Angelo Yfantis. Professor Laxmi Gewali also has a campus-based research program in computational geometry. The two remaining labs are located off-campus within UNLV's National Institute for Advanced Technology (NIAT). These labs are the Cybermedia Research Lab and the Internet Security Lab, both directed by Berghel, and including several other UNLV faculty. Taken together, the CRC labs will produce close to \$1.5 million in external funding in it's first year of operation.

CRC is actively involved in several Federally funded research projects in the security arena. One project developed a new digital watermarking technique that includes the "environmental fingerprint" of the watermarking event into the watermark itself. According to Berghel, "Ten years ago my watermarking work was pretty traditional in that it dealt with the techniques of burying digital data into other digital data. In those days, you could count the number of people working in the area on your hands. Nowadays, every major research lab does work in this area, so traditional watermarking is less interesting than it used to be. What sets our work apart from the others is the degree of personalization that we add to the watermarking process. Our focus is exclusively on the issue of non-repudiable denial.

NSCEE and HIPAA

continued from page 1

tion for health information, and is known as the **Privacy Rule**.

The **Privacy Rule** establishes new requirements for access to health-related records by researchers and the use and further disclosure of Protected Health Information (PHI), identifiable health information that providers have acquired in the course of serving patients. PHI data elements that make information individually identifiable include, but are not limited to: names, addresses, employers' names or addresses, relatives' names or addresses, dates, telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, certificate numbers (including device serial numbers for implants), fingerprints, full face photos and comparable images, or any other characteristics that may be used, individually or in combination, to identify an individual.

Releasing this information for reasons other than treatment, payment, or operations, without obtaining an authorization or a waiver is a violation of the privacy regulations.

Improper use or disclosure can result in criminal and civil penalties including:

That's what sets our work apart."

Another cluster of security projects has to do with the development of network utilities that facilitate network hardening. For example, one project produced a software wizard that enables users to harden Windows XP workstation clusters without requiring Group Policy and Active Directory support on local domain controllers. "Until a "gold standard" for XP appears, over 90% of the XP workstation community will be rudderless when it comes to hardening their computers. Our tools enable them to pick and choose from NSA, SANS, FBI, Microsoft and any other third-party security templates for the configuration that best suits their environment. The convenience of being able to cut-and-paste between security templates and local security policy registry entries is an innovation that will have enormous practical benefit to Windows end-users," Berghel said. Other projects include the development of tools for determining the limits of wireless perimeter security and the creation of a suite of security auditing tools. On both of these latter projects, CRC is in partnership with NSCEE.

Berghel has been a prolific expositor of security issues, vulnerabilities and innovative technologies. Reprints of many of his articles are available online. Here are a few that may be of interest:

- "Digital Watermarking" (1996): http://www.acm.org/~hbl/publications/dig_wtr/dig_watr.html
- "Cyberspace 2000: Dealing with Information Overload" (1997): http://www.acm.org/~hbl/col-edit/digital_village/feb-97/dv_2-97.html
- "Social Security Numbers, Identity Theft and the Web" (1999): http://www.acm.org/~hbl/col-edit/digital_village/feb-00/dv_2-00.html
- "The Code Red Worm" (2001): http://www.acm.org/~hbl/col-edit/digital_village/nov-01/dv_11-01.html
- "Hijacking the Web" (2002): http://www.acm.org/~hbl/col-edit/digital_village/apr-02/dv_4-02.html

- \$25,000 for multiple violations in the same year,
- \$250,000 and/or up to 10 years imprisonment for knowingly misusing a person's protected health information.



NSCEE's HIPAA Projects

NSCEE's Nevada E-Health Initiative uses the StorageTek PowderHorn® 9310 mass storage resource for archival storage and retrieval of digital medical images from Picture Archiving and Communications Systems (PACS) located throughout the state. Additionally, a digital library is planned that will make available over 1000 hours of endoscopic procedures performed at the Endoscopy Pulmonary Disease Clinic, Heidelberg, Germany.

NSCEE's Medical Records Knowledge and Information Management for Radiation Workers project provides the US Department of Energy (DOE) with an integrated electronic management system for medical records. The new records system is designed with non-proprietary software to provide the DOE with survivable documentation in areas such as occupational medicine, industrial hygiene and radiation exposure.

Help Desk

SSH - Secure Shell

Many users of the Internet assume that their communications between systems is secure or at least difficult to intercept. In fact, most networking protocols transmit data and commands in clear text; anyone with access to the network between the two communicating machines (referred to as "man-in-the-middle") can eavesdrop on the conversation, reading passwords and other sensitive information.

NSCEE encourages the use of SSH as a replacement for telnet/login sessions and file transfer (ftp). The rcommands (rsh, rlogin, etc.), telnet and ftp all transmit data and commands in the open. SSH protocol sets up an encrypted channel between two systems, similar to what happens when accessing a secure website. Once the two systems connect, authentication information is exchanged to ensure the machine being connected to is who it claims. After this, the user is authenticated and either a shell is opened for the user or file transfer operations are performed.

Another benefit of session encryption is that it makes hijacking, or man-in-the-middle attacks more difficult or impossible. A man in the middle attack is performed by listening to the conversation between hosts and, at some time after the user has authenticated, taking over the session and hanging up on the real client's connection.

Many SSH clients also support the tunneling of other protocols over their connection. Most notably many clients allow for tunneling of Xwindows connections between the client and server, protecting the Xwindows communications from eavesdropping and hijacking.

**Hey You!!
If you know
what's good for
you, you'll use
ssh!!**



SSH clients exist for all major operating systems. OpenSSH includes both client and server and runs on most Unix and unix-like operating systems. Their website at www.openssh.org has a list of OpenSSH and SSH alternatives.

For Macintosh users, OpenSSH has been included in Mac OS X. Other programs providing support for Mac OS 9 are listed on the OpenSSH website.

A number of SSH clients are available for windows users. PuTTY/WinSCP is a free implementation of ssh and scp (the ssh server's file transfer client). A link to it can be found on the OpenSSH web site above.

There are other commercial versions of SSH clients and servers available, and some provide additional features. Most commercial clients are freely available for evaluation. SSH Communications Security (www.ssh.com) offers free use of their SSH for workstations for non-commercial use.

Firewalls and Intrusion Detection

NSCEE is installing new firewalling and intrusion detection equipment on all of our external network connections. This includes NSCEE's connections to the Internet, Internet2 and the UNLV campus network.

NSCEE is currently configuring the firewalls and monitoring communications to minimize impact on connectivity. Any concerns relating to NSCEE's firewalling and monitoring should be sent to:

help@nscee.edu

A detailed explanation of the firewall configuration would be too complex for this forum and more importantly, access to firewall configuration information itself needs to be monitored and controlled.

Do's and Don'ts of Securing your Desktop System

In addition to all of the information regarding the network and system security, it is important to remember that the desktop systems used to connect to NSCEE resources also need to be secure. Here is a general list of Do's and Don'ts on securing your desktop system. Note, this list is meant to provide only general information; please contact your local network security organization for specific tips.

- Do:** make sure you are aware of the network and system security policies of your local organization.
- Do:** make sure that you are running a recent version of the operating system used by your desktop computer.
- Do:** make sure that you have all relevant security related patches installed. Consider carefully if you want to enable your system to automatically apply security updates. Manually reviewing the patches' descriptions and then applying them may be a better approach.
- Do:** consider running anti-virus software (i.e., Symantec's Norton AntiVirus™) as well as using a spyware removal utility (i.e., Lavasoft's Ad-aware™, www.lavasoftusa.com/software/adaware).
- Don't:** use the root or administrator account routinely. Use a low privilege account for normal computing.
- Do:** use secure methods to connect to the NSCEE

network, for Unix: ssh/openssh, for Microsoft Windows: Ttssh or putty. Use scp (Unix) or pscp/winscp (Windows) for file transfers instead of FTP.

- Don't:** run unneeded services on your desktop system.
- Do:** use secure passwords: minimum of 8 characters, with at least three different occurrences of uppercase letters, lowercase letters, numeric digits, or special characters within the first 6 characters of the password.
- Do:** change your password regularly, and don't reuse old passwords.
- Don't:** configure your desktop system to allow usage without having to specify a password.
- Do:** consider using a web browser and email client on Microsoft Windows other than Internet Explorer and Outlook Express. If you do use them, then consider disabling ActiveX, Java, and Javascript scripting. Also, don't open attachments.
- Do:** consider installing either a hardware or software firewall utility, even if there are already firewalls deployed around your network perimeter. Take a look at BlackICE™ (blackice.iss.net), PassGo's Defender (www.passgo.com), and ZoneLabs' ZoneAlarm (www.zonelabs.com). Doing this along with using anti-viral software will help protect you if you pick up a virus or worm from somewhere other than the internet.

Upcoming Network and System Security Related Seminars

NSCEE announces the following two short seminars to be held in our Internet2 Visualization Lab located on the 3rd floor of the Thomas Beam Engineering Complex.

- **Internet Security: the 10,000 Foot View**

This non-technical presentation describes the components that make up the hardware and software of the Internet, how malware (viruses and worms) target

these components, and how to protect against them.

- **Introduction to Network Monitoring Tools**

This presentation is targeted towards network and system administrators. Topics include: packet capture tools (tcpdump and snort), and general management tools, net-snmp and MRTG (Multi-Router Traffic Grapher).

Watch our web site for details regarding dates, times and how to sign-up for these upcoming seminars.

Accessing Mail Securely Using pop3 Over ssl

Concerned about the security of your E-mail?

One simple measure you can take to improve security is to use ssl (secure sockets layer) to encrypt your connections to the pop server for your incoming mail. In most cases this can be done using your existing email client (i.e., Eudora, Mozilla, Netscape, etc.).

certificate used by our pop3 server (clark.nscee.edu) is self signed. This means that a third party is not vouching for the identity of the server. Since we are mainly concerned with encrypting our connection, the lack of third party verification just adds some additional actions to the setup.

Instructions for making Eudora, Mozilla, or Netscape email clients receive incoming mail via an SSL encrypted connection can be found on NSCEE's web site at:

<http://www.nscee.edu/Publications/QuickRef/secure-mail.html>

First, a word about SSL certificates. The

NSCEE Hires Network Security Administrator

Ron Young recently joined the staff of NSCEE as Network Security Administrator. Ron has over 20 years of software design, network and systems administration experience within UCCSN, most recently specializing in Optical Character Recognition and Information Retrieval systems.

The Network Security Administrator's major responsibilities include:

- Manage and evaluate all daily security operations and practices to ensure compliance with established policies, procedures, and security standards
- Monitor networks to ensure confidentiality, integrity of data, the availability of all network services, and investigate and report system problems and security breaches
- Provide technical support for the DOE and UNLV user community, including maintaining technical documentation and operational procedures for locally developed security systems
- Design, deploy and test secure and reliable network architecture and disaster recovery procedures

Articles Invited

The National Supercomputing Center for Energy and the Environment invites you to contribute articles on your work on high-performance computers and especially our resources. Please submit your articles to:

TeraWord	email
UNLV/NSCEE	teraword@nscee.edu
4505 Maryland Parkway	
Box 454028	Phone
Las Vegas, NV 89154-4028	(702) 895-4153

Fax
(702) 895-4156

TeraWord is published by the National Supercomputing Center for Energy and the Environment. Materials of interest in the newsletter may be reprinted, provided acknowledgement of the source is included. Hardware and software products mentioned in this publication are trademarks of their respective companies. The use of their names does not constitute an endorsement or approval by the NSCEE or the University of Nevada Las Vegas.

NSCEE

National Supercomputing Center for Energy and the Environment

High-Performance Computing and Communications in Nevada

National Supercomputing Center for Energy and the Environment
4505 Maryland Parkway, Box 454028
Las Vegas, NV 89154-4028

Visit us at www.nscee.edu



UNLV
UNIVERSITY OF NEVADA LAS VEGAS