The Security Blanket

Issue 10, August 2002

Here to help you keep I.T. secure.

In This Issue:

From the CISO

Security and Instant Messaging

Instant messaging use is growing by leaps and bounds, fueled by the benefits it has to offer. Unfortunately, these little apps also contain a potent dose of insecurity, a result of various architectural and development flaws. While many people write about and point to rampant instant messaging misuse (spending hours talking to friends or family while at work, for example), its use is becoming more mainstream as additional work-related applications are put in place.

Two things are certain - instant messaging is not going to go away and its use is only going to increase. It is imperative that the security community gets a handle on instant messaging quickly before it's too late. Some companies are already building more secure instant messaging applications. For instance, AOL and VeriSign, a security company, have announced an effort to develop a security-minded instant messaging solution embodying the security of VeriSign's PKI (public key infrastructure) technology. One of the advantages of instant messaging today is that it is easily obtainable and in most cases, the price is right - it's free. It remains to be seen if the hardened instant messaging applications are made available at no cost as well.

In security, we always try to be an enabler - obtain an appropriate level of assurance while allowing the user to function. That mentality is put to a severe test with instant messaging. Users and technology leaders are seeing the benefits and want to use it and/or make it available, but we have to make it more secure. There are ways to do that, as outlined further in this issue. We need to see the issues as a community and work in concert with one another to ensure the protection of all. All the security in the world can't protect against something that is specifically allowed in the environment that has numerous security flaws. It's time to get a handle on this.

Kip Peters

Return to Table of Contents

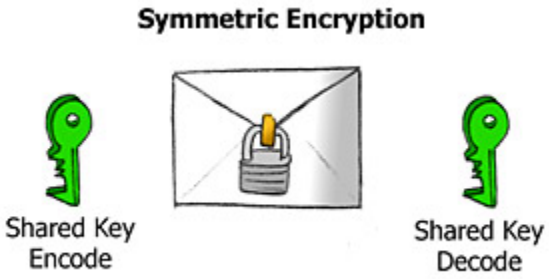
Feature Articles

Privacy in the Open

Have you ever stopped to think about how many places across the world your email travels through when it leaves your computer? If you're sending an email across the country, it can hop through multiple networks before it even leaves the state! The same thing goes for most instant messaging programs. MSN Messenger and AOL Instant Messenger both bounce your messages through multiple networks before they reach their destination. Basic email and Instant Messaging both have an important characteristic in common; they both send messages in clear text. This means that anyone snooping around at any of those networks that your data passes through may be able to read your

email or check your instant message conversation. Always remember that unencrypted emails and instant messaging are like postcards; the message gets to its intended recipient, but anyone along the way could have read its contents. This is where privacy tools can come in handy. Encryption and Steganography are two ways to help you protect your personal information from prying eyes.

First of all, I'll give a quick description of two basic types of encryption: symmetric and public key.



Symmetric encryption is a shared key system. This means that the same key that locked your file or text is also the same key that opens the file or text. The key must be shared between the sender and the receiver of a message (and hope that it stays private). The dangerous part of symmetric encryption is that the key must be traded, and if anyone steals the key, they could decrypt your messages and its "game over" for privacy. Symmetric key encryption is very fast and easy, but it lacks the security of public key encryption.

Public key encryption, unlike symmetric encryption, is based on a two key system. Each user has a public key and a private key that have a mathematical relationship to each other. Your private key doesn't ever have the need to be shared with anyone, but the public key is made available to everyone. The mathematics behind public key encryption is pretty awesome. Here's a quick example of how one would use public key encryption: If I am sending a message to my friend Joe, I encrypt the message with Joe's public key that is available online to everyone. Once my message is encrypted with Joe's public key, the message can then only be decrypted by using Joe's private key. Joe never has to give away his private key, so he keeps it protected on his own PC. This method requires no need for key exchange since I can send a message to Joe without having to know his private key. This makes public key a much more secure method since no one snooping around can intercept your keys and defeat your encryption. Just hold your private keys in a safe place and have a backup!

For quick and easy use of public key encryption for communication privacy, there is a free program available called Pretty Good Privacy (PGP). PGP is probably the most popular client encryption software on the Internet. It uses an extremely powerful public key algorithm that has stood the test of time for durability. PGP is a very powerful tool for protecting sensitive email information that must be transmitted across public networks. It can be a very effective method in our governmental work environment to safely transmit sensitive information about citizens. Consider the use of PGP when email is used for this purpose. Email client plugins have already been created for popular programs like Microsoft Outlook and Eudora. This makes email encryption practically a

push-button operation. For personal use on instant messaging applications like MSN, people have also created encryption plugins. This can help ensure data security on these popular chat networks. Whether the encryption is done on an email or an instant message conversation, anyone intercepting the data would have no idea how to read your encrypted message.

http://www.pgpi.org/products/pgp/versions/freeware/
http://www.commandcode.com/download.html

Along with encryption, there is another popular method of personal privacy called Steganography. For State use it isn't as appropriate as PGP, but it may be good for home privacy use. Steganography (stego) is defined as hiding a secret message within a larger one in a way that others may not detect its presence. The way people use stego online is through image files. Text messages, both encrypted and plain text, can be embedded within an image without any noticeable change to the picture itself. This makes it a very powerful tool to hide messages literally in plain sight. For example, one may use stego to hide a message in an image on a web page. This way, anyone who visits the web page will just see a normal picture and think nothing of it. But, people who know the image contains something more can extract the information from the image file and read your message.

A new stego program named CameraShy was just released recently that is quite easy to use. This program allows you to easily add encrypted messages to images and also find images with hidden messages. Now if you have a message that you want to keep private, you can embed the text within an image and send it to your friends over email. Anyone who may be snooping in on your email would just see a picture and would likely have no idea that there was a secret message embedded within.

http://www.hacktivismo.com/projects/camerashy/
http://sourceforge.net/project/showfiles.php?group_id=57940

I hope the introduction of these tools (PGP and CameraShy) has given you some ideas on how to secure your data in transit. When used individually or in combination, these programs can help bring a great deal of privacy and confidentiality back to insecure email and instant messaging services. Enjoy!

Jared McLaren

Note: The startup company PGP now owns the PGP tool. They also offer new products and version 8.0 of the PGP tool. See story.

Instant Messaging – Instant Headache

The following is a great article outlining the different security risks associated with instant messaging software and peer-to-peer file trading networks. Since IM technology works on PC's, PDA's, cell phones, and pagers Gartner predicts IM use at 70% in the corporate world by 2003. These instant messaging products introduce security

vulnerabilities to a network since they can bypass firewalls, bypass gateway anti-virus protection, have many hacker vulnerabilities, and most use no encryption. The article goes on to discuss the most popular IM programs and their features and then discusses proxying and SSL wrapping of the plain-text IM traffic.

Jared McLaren

Instant Headache
The rapidly expanding use of instant messaging is introducing new security challenges to enterprise networks. August 2002, InfoSecurityMag
http://www.infosecuritymag.com/2002/aug/cover.shtml

Hackers Can Turn Your Computer Into A Bomb

Many of us have already experienced what hackers and virus writers are capable of doing. We have heard of and seen viruses and worms that have knocked many of our own systems off-line. Hackers have defaced Web sites and stolen information, and have launched denial of service attacks against sites like eBay and Amazon. However, a recent article shows new research that suggests that hackers have greatly increased their hacking skills.

According to Arnold Yabenson, president of National CyberCrime Prevention Foundation (NCPF), hackers have now found a way to turn computers into a deadly weapon by just sending an email with an innocent-looking attachment. When the a user opens the attachment "the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade." This means that a hacker could write a CPU-exploding virus that spreads through email. The virus could first pass on the virus to everyone in the user's address book and then blow the computer up causing injury or even death to the user. The article states that the "sickos can wreak death and destruction from thousands of miles away!"

Yabenson believes that people close to hackers find this as no surprise as this is just the next step in the progression of horrors conceived by hackers. Yabenson cites specific attacks that hackers have already carried out. One of the more dangerous ones was when hackers came within two digits of cracking an 87 digit Russian code that would fire missiles aimed at five major U.S. cities.

Now to calm everyone's fear, the above narrative is a hoax. The "exploding-CPU" is not really possible, however, the information was taken from a real article that was posted in the Weekly World News (http://www.snpx.com/Images/computerbomb.jpg). Many people know that the Weekly World News will write up some fake articles, but some people do believe these stories. There are even posts to security and technical forums with people asking if the computer hand grenade was real. This hoax article also popped

up on other websites, but most never mentioned that it could be a fake. The point of my article is help users be aware that there are many hoaxes out there, and that it is important to recognize them for what they are when you come across them. Hoax writers love to use official sounding people and organizations for their quotes. For example, in the "exploding-CPU" article there is no evidence of the National CyberCrime Prevention Foundation ever existing.

If you want an idea of how many hoaxes have been discovered in the news just go to your favorite search engine and search for "hoax", or go to the following website: http://hoaxbusters.ciac.org/. Even websites that are well-respected news sites have been hacked and had bogus stories posted. Most recently USAToday.com was hacked and had many false stories placed on their sites (http://www.washingtonpost.com/wp-dyn/articles/A61049-2002Jul12.html). When reading news stories, remember to use common sense, and that you can't believe everything you read.

Paul Schmelzel

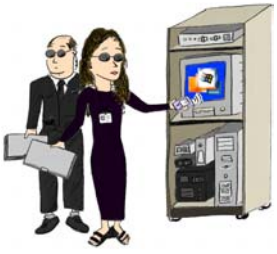
Return to Table of Contents

Current Activities

Charter security, Vulnerability Assessments, Incident Response, Awareness Projects, lots of things going on… Check out our website to see the latest additions, or just to refresh yourself on current guidelines and policies.

Information Security Office Service Offerings

Would you like to have a vulnerability assessment performed on your systems? Do you need help with an incident? Are you looking for security services? Check out the ISO Service Offerings!



Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates. (Security Services are listed in the last quarter of the web page.)

- Security Consulting
- Vulnerability Assessments
- Physical Security Vulnerability Assessments
- Network-Based Intrusion Detection System
- Enterprise Business Continuity
- Incident Response
- Test Lab
- Awareness Briefings
- Enterprise IT Business Continuity

Charter Project Transition

The ISO is currently working with other sections and departments to assist with the Charter Projects envisioned by Governor Vilsack. Want to know the latest on Charter Project Security Issues, Security Planning, and Security Status? Send your questions or concerns to Marie Hubbard.

Information Security Officer Distribution List

The Information Security Office has a distribution list with which we can easily send out security mailings to security contacts within the State of Iowa. Mailings include the Security Blanket, Security Quickies, Lunch & Learns, Security Alerts, Daily News and Virus Reports, security events, or other announcements. Some contacts also disseminate the ISO mailings to their departmental personnel. If you are interested in being included in this distribution list, drop a note to Security Awareness. If you would prefer to only get the Daily News, send to Security Awareness.

Security Awareness Tutorial

The new Security Awareness Tutorial (SAT) is complete and ready to use! Topics covered in the Security Awareness Tutorial include training on Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. The training course is available online and on CD-ROM, and will take up to 90 minutes to complete. It is divided into separate lessons, so you can complete the lessons at different times if needed.

The SAT is currently being used by ITD for security awareness training. Because the Information Security Office has Enterprise-wide responsibilities, **the SAT is also available to State of Iowa Enterprise agencies at no charge**. In addition, the SAT will be available to non-Enterprise agencies and non-State of Iowa organizations as well, for a licensing fee.

For more detailed information on the course you can visit http://www.itd.state.ia.us/security/education.html#tutorial. Contact William Hubbard if you have questions regarding the SAT content, and Justin Stone for access to the course.

UPCOMING SERVICES

Certification and Accreditation Process

C&A Process Update and Definition Phase

Developing a Certification and Accreditation process that will be both effective and practical for use in State government is a complex task. While there are many well documented and established programs in existence, they are all highly detailed and

require a great deal of resources to successfully complete. As I'm sure you are aware, the State has neither a great deal of unallocated money nor the extra manpower to devote to such extensive programs. Another influencing factor is the Charter process, in which the State is attempting to efficiently combine IT resources amongst enterprise agencies.

In light of these issues, we are developing a customized Certification and Accreditation process for State systems. This customized C&A process should both be simplified and decrease the actual time the C&A process takes for each system, application, network device or combination thereof. Toward that purpose, we are structuring the Definition phase around the completion of a Risk Analysis Form.

These forms will include requests for specific pieces of documentation on the system in question, as well as a Threat and Countermeasure checklist that covers a broad range of security issues. There will eventually be separate risk analysis forms developed for each operating system and many popular software systems. After an applicant completes the form, ITD staff would meet with the team designated as the primary contacts for that particular system and negotiate what the final configuration of the system should be. After a final configuration goal is reached and the agreed upon changes have been made and/or documentation provided, the system would be granted certification.

Marie Hubbard

Risk Assessment

A standard risk assessment methodology will be developed for use in Iowa state government. Training will be provided on how to best utilize the methodology, and staff assistance will be available for agency assessments. We're working on it, really.

OTHER ACTIVITIES

Enterprise Security Website

From this site you have access to tons of security information: Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's your free resource for Enterprise and ITD Security Information.

Educational Extras

Extra resources are available here for State security awareness efforts and home personal computer security. Newly added is a link to a home computer security series by Microsoft.

ITD Guidelines and Procedures

Go here to see new ITD ISO Guidelines and Procedures for Workstations and Servers, Tips on Malicious Code, and non-IT General Security issues:

Configuring a Windows 2000 Desktop	Preparing a Windows 2000 Server for Production
Windows IIS 5.0 Guide	IP Security Policies
Apache 2.0 for Windows NT/2000 Secure Installation Guideline	Enterprise Messaging System Protection Measures
Virus Detection and Prevention Tips	Virus Response Procedures
Travel Security Guidelines	Letter and Package Handling

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about…
Information Sharing!
Security Training!
Conferences!
Programs!
Security Vendor Announcements!

The Information Security Office's Lunch &Learn Program continues… These informal meetings cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. Change of location or time will be announced via e-mail, and sent to departmental Information Security Officer contacts. The past presentations (lots of them - in .pdf, .ppt, and/or video) and an updated schedule are available at the Lunch & Learn site.

Date and Time	Topic and Location
August 27 12:00pm-1:00pm	Security Awareness Grimes Bldg., South Conference Room
TBA (September)	Privacy vs. Open Access Forum

Questions regarding the Lunch & Learn program can be directed to William Hubbard.

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing information.

Security Vendors

SANS Offerings:
Each month SANS offers at least one training conference in a major U.S. city. In the next few months there are SANS GIAC Certification and Training programs in Detroit, St. Louis, Denver, Omaha and many other places. SANS also offers online security courses for those who are unable to travel much, but still wish to participate. Details and registration information: http://www.sans.org/newlook/home.php

SANS also offers a free First Wednesday Webcast series. This series is dedicated to sharing information on current security issues. http://www.sans.org/webcasts/

Microsoft: (Vendor Announcements)

Free MSDN Webcasts

The MSDN Webcasts team holds 90 minutes of deep, how to technical webcasts presented by knowledgeable Microsoft software design engineers, developer evangelists, and a host of others. This free event is held live, and it's interactive. Customers can see code and application demos online, and ask the presenter technical questions, or listen to their peers ask questions.
Register at: http://www.microsoft.com/usa/webcasts/upcoming/default.asp
Recorded sessions can be found at:
http://www.microsoft.com/usa/webcasts/ondemand/default.asp.

Microsoft Online Training
In an effort to meet the demands for training and certification on Microsoft products and platforms, Microsoft Government is sponsoring Online Training for selected courses for a limited time. These courses will be provided on a first come first served basis. Government employees can register for training at a reduced cost, as we have arranged for the Microsoft discount to be extended to our government customers. To register, Government technical professionals need to go to the web site:
http://www.msgovernmenttraining.com/offer/

Other Events:

McAfee - Extending Enterprise Security

Thursday, August 22, 2002

McAfee will be hosting a free seminar at the Des Moines Downtown Marriott on August 22nd. They will be discussing extending enterprise security. Details and registration information can be found by clicking on the attached link:
http://www.naiseminars.com/eb/3/MCA71228/inv

12th Annual Virus Bulletin International Conference (VB2002)
Date: September 26-27, 2002
Location: New Orleans, LA
VB 2002 is the only conference to focus exclusively on the threat of computer viruses and is an international meeting place for anti-virus professionals. More than 30 papers will be presented, with topics ranging from heuristics, computer viruses and the law,

Linux, Win32, Java and XP to best practices for corporate anti-virus. VB2002 offers parallel tracks of corporate and technical presentations.
http://security.ittoolbox.com/direct.asp?m=9&y=2002

BindView Insight 2002

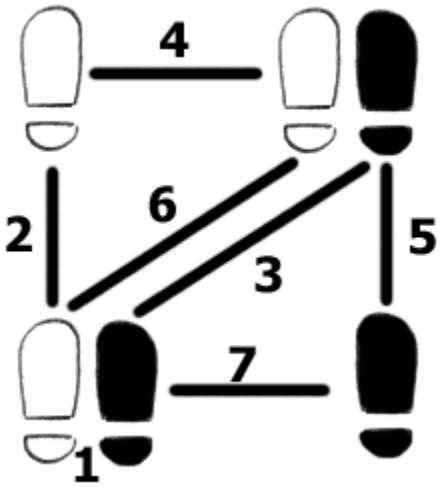
October 1-3, 2002, The Venetian Hotel, Las Vegas, Nevada

BindView invites you to attend its first user conference this fall. Join your fellow IT professionals, security experts, consultants, and partners for BindView Insight 2002.
http://www.bindview.com/userconf/

Return to Table of Contents

Helpful Hints

7 Steps to Personal Computing Security



Microsoft recently created a series of security guidelines for the Windows system home user. The articles are easy to understand and give useful information on what threats exist, how to protect home systems (including easy to follow checklists), and what products and services exist to help users. Remarkably enough, the articles note many non-Windows products and services in addition to their own products and services.

The topics covered in the series are as follows: Assess your risk, Use anti-virus software, Keep your software up-to-date, Check your security settings, Use a firewall, Create strong passwords, Conduct routine security maintenance.

7 Steps to Personal Computing Security

Please remember that security is everyone's responsibility, and that home systems can be compromised and used for Distributed Denial of Service Attacks, illegal file sharing, financial theft, or other illicit purposes. Be safe and keep your home systems secure.

William Hubbard

Return to Table of Contents

Linked Articles

Education

OECD publishes cybersecurity guidelines
In response to a U.S. call last October that it should update its principles on security of information systems and networks, the 30-member intergovernmental Organization for Economic Co-operation and Development (OECD) has made public its latest guidelines. August 08, 2002, ComputerWorld. Guidelines at: http://www.oecd.org/pdf/M00033000/M00033182.pdf.

Filling the INFOSEC ranks
With a little help from Uncle Sam, Carnegie Mellon University is helping colleges and universities train the next generation of information security professionals. Aug. 12, 2002, FCW

Can't Buy Security
The Bush administration's "National Strategy for Homeland Security" includes an idea to conduct background checks on private-sector employees who work in critical infrastructure areas. Frank Hayes argues that although that's a good step, what we really need is to make all workers security-conscious. July 29, 2002, ComputerWorld

Maximum Security Returns
Like a lot of other security professionals these days, Mike Hager, security chief at OppenheimerFunds Distributor Inc. in New York, is under excruciating pressure to provide top-notch protection of data, ensure privacy and manage user access—all on a drum-tight budget. (Editor's note: This article illustrates well the financial value of building security into new projects and products as opposed to adding on security aspects after completion.) July 15, 2002, ComputerWorld

Build a Response Team
A computer incident response team, or CIRT, is a lot like a firefighting crew - both are composed of individuals trained to respond quickly to specific incidents with the goal of limiting damage and reducing recovery time and costs. (Editor's note: Iowa is in the process of forming such a team for the State, the Iowa Crisis Action Team, or ICAT.) July 15, 2002, ComputerWorld

Let the Pros Investigate
Once thought of as the exclusive realm of violent-crime experts, forensics is fast becoming a mandatory skills set for companies that need to show that computer crimes don't go unsolved or unpunished. July 15, 2002, ComputerWorld

The Behaviors and Tools of Today's Hackers
These days, it doesn't take a computer expert to become a hacker. There are over 30,000 hacking-oriented sites on the Internet, offering easy to use click-and-hack programs and scripts for anyone to download. June 18, 2002, Symantec

Cracker Tools and Techniques – Faster, Stealthier… More Dangerous
From Web app manipulators to kernel-level rootkits, ingenious hacker tools challenge infosec's ability to thwart--or at least contain--attacks. July 2002, Information Security
Editors note: This is a good article on information security attack/defense tools and techniques (7 pages).

iDefense Pinpoints Top Wireless Vulnerabilities
They identify 10 easy steps to bolster wireless security. July 30, 2002, SNP

Getting Down and Dirty With Intrusion-Detection Systems
A security professional's independent look at the six-day Intrusion Detection In-Depth training class run by the SANS Institute in Cary, N.C. August 5, 2002, ComputerWorld

Trojan horse technology exploits Internet Explorer
A new technology could let a Trojan horse disguise itself as the Internet Explorer browser and allow hackers to steal data from PCs by fooling firewalls into thinking it's a trusted Microsoft Corp. application, say three security consultants. August 6, 2002, ComputerWorld

Security's part of big picture
For agencies, the enterprise defines most IT objectives--including systems security. "You need to have an agency-wide perspective on a lot of things associated with overall enterprise architecture," said French Caldwell, vice president and research director for Gartner Inc. of Stamford, Conn., and a former program analyst in the Office of the Secretary of the Navy. August 12, 2002, GNC

Expert: Simplicity Is Key To Keeping Code Secure
When it comes to writing secure code, less is more. August 9, 2002, ComputerWorld

Homeland Security

Ellen M. Gordon, the Iowa Homeland Security Advisor, has released the proposed Iowa Homeland Security Initiative. It covers many critical aspects of Homeland Security in Iowa, including critical infrastructure, program proposals, homeland security organization, and other items. To view the document, visit the Iowa Homeland Security Initiative page.

Sleuths Invade Military PCs With Ease
Security consultants entered scores of confidential military and government computers without approval this summer, exposing vulnerabilities that specialists say open the networks to electronic attacks and spying. August 15, Washington Post

Who's ready for cyber terror?
Like a doomsday asteroid, cyber attacks threaten to disrupt critical infrastructure services, causing billions of dollars in damage and loss of life. Awareness is critical, but now it's time to act. July 29, 2002, ZDNet

Report urges states to organize against cyber terror
The National Association of State Chief Information Officers (NASCIO) today issued a report urging government leaders in all 50 states to set aside political differences and make cybersecurity and critical-infrastructure protection a top priority. July 23, 2002, ComputerWorld

Deal struck for security alerts

The National Association of State Chief Information Officers today announced it has signed an agreement with the primary federal infrastructure security analysis and warning center so that individual states can receive alerts on cyber and physical threats. July 25, 2002, FCW

Cybersecurity strategy released
The Bush administration today unveiled the nation's first homeland and cybersecurity strategy, which calls for an unprecedented partnership between federal, state and local governments and the private sector to battle terrorism. July 16, 2002, ComputerWorld

The Strategy Document:
The National Strategy For Homeland Security: Office of Homeland Security

Final 'Blue Cascades' report cites infrastructure gaps
The report follows a high-level exercise last month called Blue Cascades that was sponsored by the Pacific Northwest Economic Region (PNWER). The exercise, the first regional, cross-border event held in North America, showed how entire regions can be to vulnerable to power outages and telecommunications failures. July 18, 2002, ComputerWorld

Cyber corps to extend to states
The White House's national strategy to protect cyberspace, scheduled for release in September, will contain a provision that extends a federal scholarship-for-service program to the state level, said Richard Clarke, cybersecurity adviser to President Bush. July 23, 2002, FCW

Cyber Crime

Update: NASA Investigating Hacker Theft Of Sensitive Documents
NASA cybercrime investigators are looking into the theft of militarily significant design documents pertaining to the next generation of reusable space vehicles. August 8, 2002, ComputerWorld

U.S. Aiding Asia-Pacific Anti-Cybercrime Efforts
U.S. law enforcement officials will meet with representatives from a host of Asia-Pacific countries this weekend as part of an international training program to help developing nations combat computer crime and cyberterrorism. August 15, 2002, SecurityFocus

FBI agent charged with hacking
Russia alleges agent broke law by downloading evidence. August 15, 2002, MSNBC

DOJ missing hundreds of laptops
The Justice Department's Office of the Inspector General released an audit report Aug. 5 revealing that more than 400 laptop computers have been reported lost or stolen from Justice agencies, including the FBI and the Drug Enforcement Administration. Aug. 6, 2002, FCW

Princeton demotes officer for hacking
Princeton University has demoted a top admission official for repeatedly entering the on-line admissions notification system of Yale University in an incident that marred the

prestige of two of the leading universities in the United States. Aug 14, 2002, GlobeTechnology

Five Israeli teenagers charged over Goner virus
According to reports in an Israeli newspaper, five teenagers have been charged in connection with the W32/Goner-A virus, which spread worldwide late last year. Aug. 6, 2002, SNP

Police, students combat cybercrime
In an unusual arrangement, Tulsa, Okla., police are teaming up with students at the University of Tulsa to help investigate and stop cybercrime. July 25, 2002, FCW

Bill with tougher penalties on cyber criminals passes House
The U.S. House of Representatives on July 15 voted overwhelmingly in favor of a bill that would significantly broaden the government's ability to go after and prosecute cyber criminals. July 16, 2002, ComputerWorld

Student charged with hacking university system to boost grades
A University of Delaware student broke into the school's computer system and gave herself passing grades in three courses, police said. July 17, 2002, MSNBC

Fighting piracy, entertainment industry is hunting down people who trade movies online
The movie industry is hunting down people who swap digital films online and demanding that their Internet service be cut off -- all part of an effort to stamp out piracy and avoid the online trading frenzy that has plagued the music business. July 19, 2002, Silicon Valley

Grades scam found at college
Two Florida Memorial College employees have been fired, three students expelled and 69 others face disciplinary action in connection with a cash-for-grade-change scandal at the private, four-year school in Northwest Miami-Dade, officials said. July 25, 2002, Miami Herald

Federal, state officials target cyber scams
Federal, state and local government officials yesterday announced 19 civil and criminal actions against scammers who have cheated tens of thousands of consumers out of millions of dollars. July 31, 2002, ComputerWorld

News

Microsoft releases Service Pack 3 for Windows 2000
The third collection of updates features security fixes, an automatic update feature, an application compatibility tool kit and a pop-up screen that lets users select the middleware they want to use. August 01, 2002, ComputerWorld

Security benchmarks being released for Windows 2000
To help companies create a first line of defense for their Windows 2000 Professional workstations, a group of security and government agencies is releasing a set of baseline

security settings that can be used as a starting point to protect corporate IT systems. July 17, 2002, ComputerWorld

Taking a Byte Out of Cybercrime
Evolving Crime Cyber forensics Challenge Privacy Rights. July 15, 2002, ABC
Accompanying story: ACLU commentary on Patriot Act

Security warning draws DMCA threat
Invoking both the controversial 1998 DMCA and computer crime laws, HP has threatened to sue a team of researchers who publicized a vulnerability in the company's Tru64 Unix operating system. July 30, 2002, CNet

Coming Soon: Attack Of The Super Worms
The threat to computer networks from worms is multiplying in both sophistication and potential for damage, according to security experts. July 25, 2002, ITToolbox

FBI Hobbled by Computer System, Officials Acknowledge
FBI Director Robert S. Mueller III has laid out an ambitious, three-year plan for overhauling the bureau's beleaguered system. But top FBI officials have long known the severity of the problem. July 29, 2002, ITToolbox

Stakes Higher for Hackers After Sept. 11
U.S. prosecutors and judges are cracking down on cyber crimes more aggressively than ever. August 11, 2002, CNet

Are Virus writers getting scared away?
Nobody has a bulletproof explanation, but theories range from the introduction of enhanced anti-virus software to stiffer anti-hacker laws to more vigilant computer users. August 12, 2002, ZDNet

Return to Table of Contents

Points of Contact

Kip Peters: Chief Information Security Officer (CISO), Enterprise Security Consulting, Enterprise Security, Policy, Standards, Overall Security Issues
515-725-0362

Marie Hubbard: Charter Projects: Transition Security Issues, Security Planning, Certification and Accreditation Process
515-725-0385

Paul Schmelzel: Security Operations: Vulnerability Assessments, Intrusion Detection, Incident Response, Test Lab
515-725-0410

Larry Brennan: Critical Infrastructure Assurance Coordinator, Iowa Crisis Action Team
515-725-0365

Wes Hunsberger: Business Continuity, Physical Security
515-725-0361

William Hubbard: Security Awareness
515-725-0452

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/
The awesome Enterprise Security website. You can find tons of state or ITD security information here. Policies, procedures, guidelines, educational resources, lists of services, useful links, and more!

http://www.cert.org/nav/index.html
Homepage for CERT (Computer Emergency Response Team)

http://www.sans.org/newlook/home.htm
SANS (System Administration, Networking, and Security)

FBI and SANS List Top Twenty Vulnerabilities and Free Scanner
Security leaders from 30 organizations, led by the FBI's NIPC and the SANS Institute published a list of the top twenty Internet security vulnerabilities along with instructions on how to fix them. (Updated May 2)

Iowa Homeland Security
This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more.

Homeland Defense Journal
This is the federal Homeland Defense journal homepage.

Return to Table of Contents

If you have questions or comments relating to this newsletter, or if there is a topic you would like to see an article on, please contact William Hubbard.
Cool artwork provided by Sam Wong.