The Security Blanket

Issue 11, Sept./Oct. 2002
Helping you keep I.T. secure

In This Issue:

From the CISO

Information Security is something of a conundrum. It is important to create the best security policies, procedures, systems, checklists, backups, and behaviors we can, but we do so with the realization that security is an ongoing process, and is never absolutely attainable. Information security is rather like physical security in that we build walls, fences, access gates, locked storage areas, have identification cards, and hire guards to protect our systems and information, yet very different because the landscape is constantly changing. At best we can say our systems and information are as reasonably secure as we can make them, with the time and resources available to us.

The issues of information security touch on everyone who uses IT systems: users, managers, developers, and administrators alike. Thankfully, however, each of us can do a great deal to help keep State systems reasonably secure. By following good security practices (good passwords, acceptable email use, etc.) and following Enterprise and departmental security policies, we can all make a difference in keeping ourselves, and the State of Iowa, more secure. Be a good cyber citizen – do your part to protect the information and systems the citizens of Iowa depend upon.

Kip Peters

Return to Table of Contents

Feature Articles

Iowa Builds Plans to Protect Critical Assets

Larry Brennan, Information Technology Department,
AJ Mumm, Iowa Emergency Management Division

With respects to the recent one-year anniversary of the terrorist attacks upon our nation, this article will briefly address one of the Homeland Security accomplishments of the State since the September 11 attacks, the Iowa Critical Asset Protection Plan.

Calculator Lights on/off
Office Search Calendar
Note Pad Reception Desk Intercom

From the Desk of The Governor's Office

Monday, October 8, 2001

Vilsack Announces New Homeland Security Advisor

DES MOINES-Governor Tom Vilsack today announced the appointment of Ellen M. Gordon, Administrator of the Iowa Emergency Management Division, as Iowa's new Homeland Security Advisor. "We must ensure that all of Iowa's citizens are protected from terrorists," Vilsack said. "Ms. Gordon will help lead and coordinate security efforts to ensure the safety of Iowa families and businesses.

Gordon will work closely with the newly-created federal Homeland Security Office, headed be former Pennsylvania Governor Thomas Ridge.

After being named Homeland Security Advisor in October 2001, Ellen M. Gordon, Iowa Emergency Management Division Administrator, assembled an inter-agency

planning team to create an inventory of Iowa's most critical assets and recommend protective security measures for those assets. The core of the planning team was comprised of representatives from the Iowa Emergency Management Division, the Iowa National Guard and the Information Technology Department. The team met with representatives from each state agency and many private sector representatives.

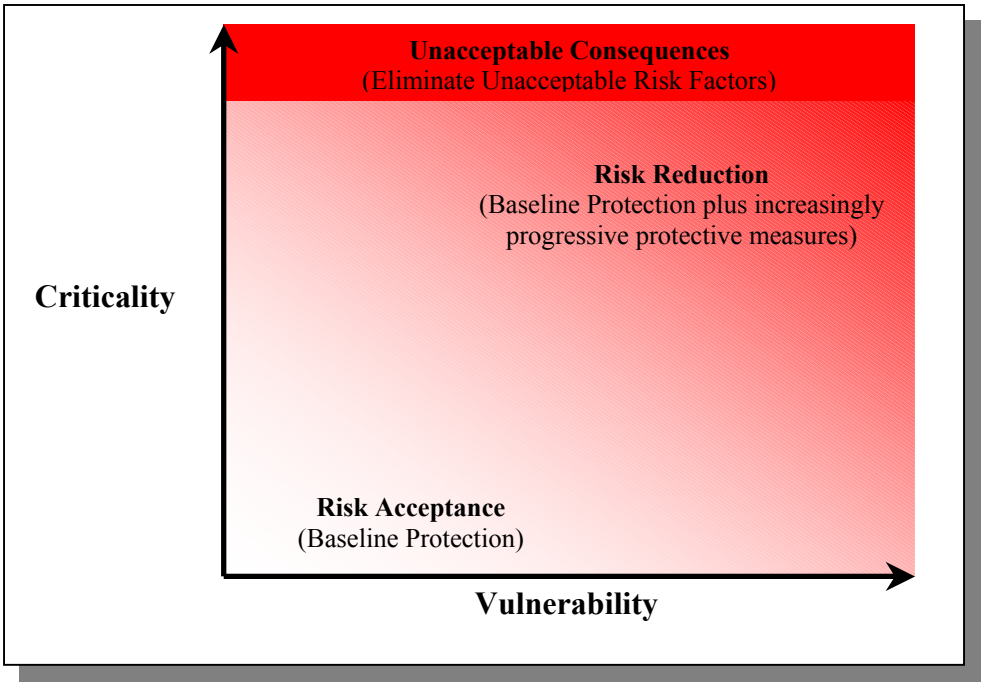
Purpose

The ability of responsible jurisdictions in the state to prevent, deter, defeat and respond decisively to terrorist attacks, domestic or international, against our citizens is one of the most critical and challenging priorities facing Iowa and the nation today. The State of Iowa regards all such terrorism, as well as a violent criminal act, as a potential threat to state and national security, and will apply all appropriate means to address exposure to such threats.

The purpose of the Iowa Critical Asset Protection Plan and the Iowa Critical Asset Assessment Model is to provide for the systematic identification, assessment, prioritization and recommendation of protective security actions of critical assets based on the assumption of future credible terrorism threats or the identification of an actual terrorist threat.

Methodology

To comprehensively address risk to an asset, the asset's criticality must be weighed against the asset's vulnerability. This is quantified by addressing 12 individual elements of any potential critical asset. Eight of these elements address the criticality associated with the asset, while the remaining four elements address the asset's vulnerability. While criticality remains fairly static over time, vulnerability is dynamic, being influenced by changing threat levels and implemented protective measures.



Results

By November 2001, approximately 12,000 public and private assets were identified that were deemed significant enough to qualify for further evaluation. At this time an inventory of highly critical assets has been isolated from the original list. This inventory represents Iowa's most critical political, social, and economic services and functions. Nearly 93% of these assets are either privately held or controlled by a non-governmental entity.

Iowa's most critical assets exhibit various levels of vulnerability when matched against a range of threat scenarios. The state's critical asset protection plan uses a series of draft graduated protective security measures to address the major vulnerabilities. These protective security measures are tied to the National Homeland Security Advisory System (HSAS) so they can be activated at the most appropriate threat level. At the baseline alert level of "Low" on HSAS we recommend policy enactments. An example of a policy could be that all employees are required to wear a picture ID. When the HSAS elevates to "High" there would be a check of all employees who enter the workplace for the photo ID.

What is Next?

This work is not a one-time effort that can sit on a shelf. Because the entire system (people, services, facilities, events, and information) is dynamic, the assessment work must be dynamic as well. Constant maintenance of the Iowa Critical Asset Protection Plan will better guarantee that decision makers have the most accurate and up-to-date information readily accessible to mitigate impacts from, prepare for, respond to, and recover from future terrorism threats. These efforts go far beyond terrorism. Critical assets are critical regardless of the hazard. Iowa will continue to maintain a multi-hazard approach and the work done with the Iowa Critical Asset Assessment Model advances efforts to mitigate impacts from all hazards ranging from terrorism to floods, tornadoes, blizzards, transportation and hazardous materials incidents.

No single asset is independent of other assets. Identifying interdependencies and the plethora of relationships will greatly enhance information available to emergency managers and other decision makers in today's environment. An interdependency model is currently under development to identify and trace these interdependencies for use in planning, preparedness, response, recovery, training, and exercising. Understanding these dynamic relationships will be a giant step forward in protecting our homeland. Yet securing our homeland and mitigating threats cannot be achieved solely through securing critical assets. Information security and the security of every citizen's information system must also be addressed.

What can you do?

"Homeland security begins at home. In this digital age, computer safety checks should be as routine as checking smoke detectors, the locks on your door, or the brakes in your car. Everyone needs to do their part,"

-Tatiana S. Gau, Senior Vice President, Integrity Assurance, America Online, Inc.

Each of us must also be responsible for securing our home systems. The National Cyber Security Alliance can help. The NCSA provides a Web site with information on how each of us can do our part to keep the nation and ourselves safer from cyber attacks. Their "Stay Safe Online" Web site is located at: http://www.staysafeonline.info/. Some of the security recommendations from the NCSA include:

- Use anti-virus software and keep it up to date.
- Don't open e-mail from unknown sources.
- Use hard-to-guess passwords.
- Protect your computer from Internet intruders -- use a firewall.
- Don't share access to your computers with strangers. Learn about file sharing risks.
- Disconnect from the Internet when not in use.
- Regularly download security protection updates and patches.
- Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.

The State of Iowa has made great strides in identifying, categorizing, and analyzing our critical assets through the Iowa Critical Asset Protection Plan. Citizens can be sure that this process will continue to help ensure the safety and security of the citizens of Iowa.

For more information regarding the ICAPP, or Iowa Homeland Security Initiatives, contact the Iowa Emergency Management Division, 515/281-3231.

Larry Brennan
AJ Mumm

Ready, Set, Crack!

Most 'best-practice' information security documents usually mention choosing good passwords as one of the primary ways everyday users can keep their system, accounts, and computers safer. They often give a minimum numbers of characters and note that users should use a blend of uppercase and lowercase letters (AaBbCc), numbers (123), and special characters (#>=*, etc.). Indeed, using a seemingly nonsensical mix supposedly can keep information safer. But is this diatribe of requirements really necessary? How much difference could different characters really make? Well… a lot, as it turns out.

Password cracking programs can attempt to guess passwords in three ways. The first way is a dictionary attack, in which they compare the unknown password to common words and names. This type of crack takes a few seconds for a dictionary containing tens of thousands of words. The second is a hybrid attack – the program checks for dictionary words and names and then adds from 1-3 characters (Iowa01, for example). It usually takes several minutes to run through the selected derivations. The third is a brute-force attack, which may utilize every combination of letters, numbers, and special characters selected

to try to guess the password. A brute force attack could try all combinations of numbers and letters, for example, or could try every keystroke possible on a keyboard – it would just take a lot longer. Generally, the greater the diversity of password characters, the greater the time it takes to crack the password.

The following is a list of test Windows account names, passwords, and the time it took to crack the password using a 600Mhz, 256KB of RAM laptop (a bit out-of-date now), and commonly available password auditing (password-cracking) programs such as LophtCrack and John the Ripper.

Account Name	**Password**	**Time to Crack**
User1	Iowa	1 second
User2	Iowa01	1 minute, 10 seconds
User3	Iowa#1	1 minute, 10 seconds
User4	"1LugP!"	5+ days

In Windows NT systems, each password is separated into 7 character sections or cryptographic hashes. (And with older NT LAN/MAN systems, all the characters are converted to uppercase – that's not good for security). Thus "1LugP!" is actually divided up and cracked in two separate sections: "1LugP!, and " (which was cracked 1 second). Shorter passwords, even ones such as %tg1 or Sa2# would fall fairly quickly to a brute-force attack simply because they are short – not too many derivations to crack. It is thus best to use all available characters (7) in the hash for maximum complexity. Some Unix systems can use a maximum of an 8-character length password so many security policies will often have 8 characters as a minimum password length to maximize complexity for all normal system passwords within an organization. Systems requiring higher levels of security might use a minimum of 14 characters (two full 7-character hashes), for instance, to necessitate a longer time to crack the system's full password.

As you can see from the table above, a 'word' oriented password gets cracked very quickly compared to a set of mixed characters: 70 seconds vs. 432000 seconds, or over 6,100 times longer. And I stopped after five days without successfully cracking it because it was starting to get *really* boring… The cracking program could have randomly found it in a couple hours, but that was extremely unlikely.

A long, seemingly random mix of characters is best to maximize the complexity and time to crack passwords. Those types of passwords may seem difficult to remember, but that's not necessarily true. User4's password looks nonsensical and hard to remember, but it's really not. It's actually a **pass-phrase** - "I like using good passwords!" converted to the password "1LugP!" and thus is fairly easy to remember. It is a strong password because it has a mix of all four character types: two upper case letters - LP, two lowercase letters - ug, one number – 1, and three special characters – "!", and in total has 8 or more characters. Of course if you can't remember it, even as a pass-phrase, it's not going to do you much good, and your system administrator will learn quickly to identify your call for help. Choose something that is easy to remember, but hard to guess.

Another way to greatly increase password complexity is to use ALT ANSI characters, if your system allows it. Most Microsoft systems do. Most password cracking programs won't even bother to check for these ALT special characters because they are very rarely

used for passwords, and they would vastly increase the time it takes to brute-force a password. (From hours or days to months, and then only if the special characters are configured into the cracking program…) Examples of these special characters include: ♣ (alt3333), ¼ (alt0188), and Þ (alt0222). Of course one must be extremely careful to accurately remember the password… (See the Helpful Hints section for more on ALT characters.)

If you create a strong password, why bother to change it? In reality, any password can be cracked. It just takes the correct character combination and a bit of time. Strong passwords take more time, but they can be cracked. It is thus best to change your password occasionally; ITD Security policy mandates every 60 days. If someone does manage to steal password files, it should take them awhile to crack the passwords. During that time the system administrator, security team, or you may find evidence of tampering and be able to detect or stop the intrusion. Changing your password on a regular basis also partially mitigates the threat of password theft, because if the stolen password gets changed it becomes worthless. Changing your password on occasion also helps mitigate the threat of curious onlookers – why bother stealing a password if you can just watch someone type it in? ☺

Lastly, passwords should also be memorized and not written down, whenever possible. Exceptions to this rule might include passwords to critical systems, when the password should be written down but locked away in a separate, secure location in case of emergency.

Remember, if someone uses your password to access a system, the system logs will record their activity as having been done by you, not the intruder. The moral of the story is: **Use good passwords and protect them, because it really does matter.**

William Hubbard

Instant Messaging Pitfalls

Nowadays instant messaging (IM) is found on just about every personal PC connected to the Internet as well as on many corporate desktops. The technology makes communication even easier than emails or phone calls. Just type a simple message, hit enter, and you and your buddy are up and chatting. With the ease of use and the benefits of simple communication, it's easy to overlook the large security holes introduced by these IM applications.

The infrastructure behind most of the popular IM clients is very similar. A central server maintains your user name, password, and a list of your buddies that you chat with online. When you log on, your computer contacts the central server farm to authenticate you and then grant you access to the IM system. From this point on, all normal text conversations are passed through this central server farm en route to the buddy you are talking with. This means that if I am sitting in my office chatting with AOL's Instant Messenger to a

friend in the office next to me, the text message goes all the way out to the Internet and through AOL's servers before it gets to my friend's computer that sits 10 feet away from me. By default, most IM applications also send this text-based chat in clear text. This brings up a question... do you trust that a clear text conversation passing across the Internet is secure? This means that if "administrator A" sends a password to "administrator B" through an IM application, it may pass through any number of insecure networks along the way. Many business secrets can be stolen through the foolish mistake of using such insecure transmissions.

Though most IM networks are insecure, there are some good encrypted clients on the market. Jabber is a popular encrypted IM application that takes the insecurity out of sensitive IM conversations. Since Jabber is encrypted, anyone on the Internet that may intercept your message will have a very difficult time ever finding out what you typed. Encryption is really the only way to overcome this most basic security flaw of default clear text data transmissions.

Another huge risk of instant messaging applications is their ability to bypass firewalls. For example, let's say that Bill wants to send Jane a picture of his new car, but Jane sits behind a firewall. Jane's firewall denies all incoming connection requests, but allows Jane to initiate a connection to anyone outside the network since the firewall trusts Jane. If they are both running any popular instant messaging software, they can transfer files with ease. Since Jane's computer sits behind the firewall, it initiates the conversation with Bill's PC to request the transfer, therefore bypassing the firewall's ability to stop incoming file transfers. This situation also introduces another problem. Email is one of the preferred methods of transferring documents back and forth between individuals. Email servers tend to have anti-virus software installed to stop viruses from entering your network. If people start sending documents back and forth through IM applications, there is no longer a choke point for anti-virus scanning. It leaves the scanning to your desktop alone and removes the extra layer of security of the email server's anti-virus scanning. This opens up a door to nasty IM-based viruses that have the ability to both bypass firewalls and bypass some anti-virus protection.

The last big point is that instant messaging is a relatively new technology. Many poorly designed products have been created that still have many security flaws being ironed out. Just head out to your favorite search engine and do a search on msn messenger vulnerabilities. You'll be surprised to see how many you find ranging anywhere from nuisances to vulnerabilities that can be used to control your computer. A buffer overflow in an IM application could be used to create a worm that could potentially spread to millions of people in very little time. Such a large audience of users is a tempting target for virus writers and hackers alike!

As you see, there are many things to think about when introducing instant messaging to your environment. If you deal with any kind of confidential information, it is best to go with an encrypted IM like Jabber or use add-on software such as Command Code's SpyShield plug-in for MSN Messenger. Also, policies against file transfers through instant messaging clients could help in stopping some viruses from entering your network. As always with new technology, do your research and be sure that your applications are implemented as securely as possible. Instant messaging can be a powerful and beneficial tool when implemented properly.

SpyShield encryption add-on for MSN Messenger
http://www.commandcode.com/download.html

Jabber Instant Messenger
http://www.jabber.org/

Jared McLaren

Return to Table of Contents

Current Activities

Policy development, Charter security, Vulnerability Assessments, Incident Response, Awareness Projects… 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

Information Security Office Certification Process

Work on the Certification and Accreditation process has continued, and draft documents are available on the Security web site at: http://www.itd.state.ia.us/security/ops.html, under Certification Process. One change that should be noted right away is a change in the name of the process. To reflect the fact that this process is being tailored for State of Iowa resources and simplified as much as possible, it will from now on be referred to as the Information Security Office Certification Process.

The first document being published is a broad outline of each step of the process. It includes a list of Certification team positions required for each certification process, a brief description of the kind of knowledge and/or authority each individual will need to possess, and the steps needed to develop the certification plan.

The certification plan will revolve around a document called the Certification Security Assessment, (CSA) which will be developed by the certification team members by adapting templates provided by the Certification Process Manager. Those templates will be published as they become available, and may be modified regularly if appropriate.

The initial results from completing the CSA will become the baseline security analysis of the system. The CSA will be finalized when all members of the Certification team agree that the system's security is acceptable and appropriate to the system. The final version of the CSA will then become the basis for the final document of this process, the Certification Authorization Agreement (CAA).

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 and Virus Report, which is sent out every business day, send the note with this subject heading: 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 such as system requirements and course content 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

Risk Assessment

A standard risk assessment methodology for Enterprise systems is under development. Training will be provided on how to best utilize the methodology, and staff assistance will be available for agency assessments.

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.

Information Security Outreach

In an effort to assist with the federal security awareness outreach effort and to aid state employees, security awareness materials are being disseminated to various departments and Capitol Complex public areas during the month of October. These materials include the ISO "Guidelines for Information Security and Internet Usage", the FTC "Safe at Any Speed" and "Identity Theft" guides, and password help sheets, and are designed to be beneficial both in the work place and at home. If you or your department would like to get more of these free documents contact Security Awareness.

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, Location, and Speaker
Wed., Nov. 20 12:00 – 1:00pm	An Introduction to TCP/IP Hoover B Level, Learning Center 1 and 2 Dave Rowen, Networking Guru

Please remember - we'll supply the place and the witty repartee, and maybe some cookies, but you will need to bring your own lunch. 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 info.

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 New York, Washington DC, Minneapolis and many other places. SANS also offers online and onsite security courses for those who are unable to travel much, but still wish to participate. SANS has also launched a **Win2K Gold Standard Tour**, a special one-day

course, which will take place in many cities around the nation. Details and registration information for the SANS programs: 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:

Iowa Technology Showcase
Date: October 23-24, 2002, Location: Polk County Convention Complex
Hear From Industry Leaders, Attend Free Educational Seminars, Test-Drive the Latest Technology, and Meet World-Class Providers. There are several seminars and presentations devoted to security issues at the Showcase, so it's a great opportunity for State personnel. Visit the ITEC Iowa Technology Showcase homepage for more information and registration procedures:
http://events.goitec.com/overview/default.asp?ec=IAT02

A few members of the Information Security Office will be participating at ITEC by giving presentations, hosting seminars, and joining in panel discussions. Come see them in action!

Information Sharing and Intelligence for Public Safety, Law Enforcement, and Military
Date: October 24, 2002, Location: Arlington, VA
By attending, you will learn how to implement real-time data sharing, interoperable communications, and detailed analysis between federal, state, emergency management, military and intelligence agencies. Hear tactics from such government agencies as the FBI, DOE, FEMA, NNSA, EPA, FCC, and more! To register or for more information, please call 1-800-647-7600, visit http://www.worldrg.com/fw261, or e-mail liz@worldrg.com

Cyber-Security in the Financial Services Sector Summit
Date: November 20-22, 2002, Location: New York, NY, Crowne Plaza
More than 30 individual breakout sessions and pre-summit workshops on topics ranging from the latest in enterprise security to the most current implementations of secure electronic commerce. Keynote Presentations from Government Policy-Makers and Industry Leaders such as: Ronald L. Dick, National Infrastructure Protection Center Director & Deputy Assistant Director, FBI Counter Terrorism Division Steve Malphrus, CIO, Board of Governors Federal Reserve System, The U.S.
Central Bank Ira Winkler, Chief Security Strategist, Hewlett-Packard

Return to Table of Contents

Helpful Hints

Using Alt Characters in Passwords

As noted in the article "Ready, Set, Crack!" above, ALT characters can be used in passwords in most Windows systems. This would greatly increase the complexity of the password, but necessitate having a really good memory, or writing the password down and keeping it in a locked, secure location.

Alternate characters can be viewed within Microsoft Word, by going to the Word Toolbar and selecting Insert, Symbol, then select Font (normal text). Then choose a symbol that has a numeric code (Alt+####). You can even create new shortcut keys (Alt codes) for symbols that have none.

To input characters in to a document or input field that are not on your keyboard:

1) Enable NumLock on the keyboard
2) Press and hold the ALT key
3) Press the keys on the numeric keypad that represent the decimal code value of the character you want to input
4) After you finish typing, release the ALT key.

Windows generates the character you specified and passes it to the foreground program, in this case the password text. Examples of this include: π (3555), ╣ (4022), and º (1447). Pretty cool, but if you forget the code, you'll be at the mercy of your system administrator or Help Desk personnel because someone will have to reset the password.

If you want to try this out, first create a test account. That way if something goes wrong you only lose the test account, and not a real one. Obviously users who are apt to forget passwords shouldn't use this technique. If a password really needs to be secure and can be written down and locked away, using an ALT character in the password is an option to consider.

William Hubbard

Return to Table of Contents

Linked Articles

Special: National Strategy to Secure Cyberspace

President Bush directed the development of a National Strategy to Secure Cyberspace to ensure that America has a clear roadmap to protect a part of its infrastructure so essential to our way of life. The draft of that road map was developed in close collaboration with key sectors of the economy that rely on cyberspace, State, and local governments, colleges and universities, and concerned organizations. It is an evolving document and comments are welcomed. September 18, 2002, President's Critical Infrastructure Protection Board
The Draft: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf

News Commentary on Report:
Cyber Security Report Spreads Burden
The plan advises everyone - home users and small business, large enterprises, higher education and government agencies - to do all they can to shore up security. September 18, 2002, CBS

Editor's note: There have been many news articles about the new NSSC, some positive, some not so positive. In any case, this effort is a beginning that with feedback from citizens, businesses, security professionals, and governmental agencies can be built upon and make a difference in helping our nation deal with security issues in our homes, places of work, and government. Hey, we need to start somewhere…

Education

Securing End Users from Attack
From malicious code to social engineers, corporate end users face a gamut of threats that endanger the network. Secure your users to secure your enterprise. October 5, 2002, Network Magazine
(Editor's note: The first two pages of this article discuss quite well the importance of ongoing user education in keeping a network secure.)

The Big Fix
Let's start where conversations about software usually end: Basically, software sucks. October 7, 2002, CSO Online
(Editor's note: Scott Berinato of CXO Media discusses the history and enormous security problems regarding software, and how a new stress on secure applications is taking shape. He gives a good overview of past and present of business concerns about application security, public issues surrounding it, and of a hopeful future course for software development.)

Linux Security How-To
This document is a general overview of security issues that face the administrator of Linux systems. It covers general security philosophy and a number of specific examples of how to better secure your Linux system from intruders. October 3, 2002, ITToolBox

Server clinic: Practical Linux security
Reduce risks and eliminate headaches through sensible account management. October 2002, IBM Developer Works

Design for security up front
A well-secured system has security designed during initiation--not during implementation or maintenance. The objectives of the initial phase are to define the need for the system, identify its purpose, and craft a system-specific security policy. Oct. 10, 2002, ZDNet

Who, What, Where
With the proliferation of Web-based applications, extranets, self-service portals, and heterogeneous enterprise systems, the development of automated identity management and provisioning systems is becoming a high priority. October 11, 2002, ITToolBox

Experts see ounce of prevention key to cyber cure
The increasing number of attacks on business computer networks means that organizations and government agencies should change their cybersecurity mindset to one of prevention, a panel of experts warned Thursday. August 22, 2002, GovExec

Strategies & Issues: Thwarting Insider Attacks
Many organizations fail to adequately protect against internal threats-often with calamitous consequences. September 5, 2002, Network Magazine

What are the real risks of cyber terrorism?
Ambiguity over its definition--and, therefore, which threats are real and which are not--has confused the public and given rise to countless myths. August 26, 2002, ZDNet
Editor's note: The author's criticisms regarding the perceived potential for cyber terrorism to cause or inflate mass casualties have merit. However, the potential for public damage will only increase as more and more of our nation's infrastructure becomes networked and interconnected. Though an increase in mass casualties deriving from a terrorist and cyber terrorist event is unlikely, it is possible. Also, the economic impact of cyber attacks from terrorist groups must be considered since the U.S. economy and infrastructure have been specifically noted as viable targets by terrorist organizations such as Al-Queda. Though terrorist cyber capabilities may be lacking now, they do have time to learn, and a target-rich environment to practice on.

Danger Within –Protecting your Company from Internal Security Attacks
The most damaging penetrations to an enterprise's security system often come with help from the inside. Gartner suggests ways for enterprises to keep a lid on sensitive information that could make the business vulnerable to an attack. August 21, 2002, CSO Online

The Weakest Link in Disaster Recovery

Much of the focus of disaster recovery planning is on creating redundant data sites and backup tapes. Very often, a crucial component is overlooked: that of keeping current documentation for all IT configuration settings. September 11, 2002, HNS

An Introduction to GNU Privacy Guard
David Scribner has penned an article introducing new users to GnuPG on GNU/Linux (and UNIX) systems. Scribner focuses on how this powerful encryption package can play a vital role in personal and business communications by increasing security. This very detailed article will be available in two parts this week on DesktopLinux.com. Sept., 23, 2002, Desktop Linux
Part 1: http://www.desktoplinux.com/articles/AT3341468184.html
Part 2: http://www.desktoplinux.com/articles/AT7966076367.html

Naked on the Net
Do you use a personal firewall to protect your home systems? (Editor's note: this short article covers Windows, Mac, and Linux personal firewalls.) Oct. 2002, Computer User

Digging the Dirt
Forensic investigation of computers is a relatively new industry. August 2002, SCMagazine

Is DRM Just a Dream?
The two sides of the digital rights fight. August 2002, RSA Security

Justifying the Expense of IDS, Part One: An Overview of ROIs for IDS
Justifying the Expense of IDS, Part Two: Calculating ROI for IDS
A positive return on investment (ROI) of intrusion detection systems (IDS) is dependent upon an organization's deployment strategy and how well the successful implementation and management of the technology helps the organization achieve the tactical and strategic objectives it has established. The second of a two-part series explores ways to justify the financial investment in IDS protection and discuss proactive and reactive management methodology and how this methodology affects their analysis of risk. July/August, 2002, Security Focus

Sniffing, war-chalking and more: A wireless vocabulary evolves
A new vocabulary has developed (with its roots in a 20-year-old movie) that enterprises would do well to learn. September 17, 2002, ComputerWorld

Cross-Site Scripting Vulnerabilities
This is a short three-page pdf tutorial on cross-site scripting. 2001, CERT

Who Are the Hackers?
As opportunities for hacking have increased, the ranks of hackers have grown, and their activities and motivations are more diverse than ever. September 17, 2002, Newsfactor

Detecting Cyberattacks By Profiling "Normal" Computer Habits
An early version of a new software system developed by University at Buffalo researchers that detects cyberattacks while they are in progress by drawing highly

personalized profiles of users has proven successful 94 percent of the time in simulated attacks. October 11, 2002, Space Daily

Security Spending: The Best Offense
While most security dollars go to technology, CIOs in our exclusive survey say investments in staff—and education efforts to guide them—must back up that robust firewall. September 15, 2002, CIO

Guide to Building Secure Web Applications
The Open Web Application Security Project (OWASP) has released an updated Guide to Building Secure Web Applications. The guide covers web application security topics from architecture to preventing attack specifics like cross-site scripting, cookie poisoning and SQL injection. September 23, 2002, Security Focus
The guide: http://www.owasp.org/guide/

Tips on protecting yourself from viruses
Good advice on how to protect your PC and what to look for in an AV product. October 18, 2002, HNS

Homeland Security

Protecting SCADA and the Vital Energy Infrastructure
Once it presents the basic threat scenarios against SCADA, this white paper recommends an assessment approach that is holistic, attentive to these threats, and mindful of the shifting agency roles. PDF file (Vigilinx Whitepaper)

Lack of cyber security specialists sparks concern
The United States is facing an alarming shortage in skilled workers to protect the nation's critical infrastructures from cyberterrorism and other threats, several homeland security and high-tech experts said Wednesday. September 4, 2002, GovExec

Clarke stumps for national Internet Operations Center
Presidential adviser Richard Clarke today asked the IT industry to support a proposed Internet Operations Center that could provide advance warning of cyber threats as they spread. October 8, 2002, GNC

White House Officials Debating Rules for Cyber warfare
The Bush administration is stepping up an internal debate on the rules of engagement for cyberwarfare as evidence mounts that foreign governments are surreptitiously exploring our digital infrastructure. August 22, 2002, ITToolBox

Cyber-attack fears stir security officers
Nearly half of corporate security officers expect terrorists to launch a major strike through computer networks in the next 12 months. August 29, 2002, IDG

National Guard builds out 54 SANs in consolidation project
The Army National Guard is spending about $10.5 million to deploy storage-area networks (SAN) in all 50 states and four territories where it has headquarters, in order to

consolidate servers and its personnel and logistics data onto SAN islands that are aimed at reducing the complexity and cost of management. August 22, 2002, ComputerWorld

U.S. vulnerable to data sneak attack
A group of hackers couldn't single-handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to U.S. systems, according to a recent war games simulation. August 13, 2002, CNet

Plans emerging for national security data sharing
They may not be the Continental Congress, but hundreds of IT experts from the defense and intelligence communities gathered here yesterday to share ideas and plans on emergency responses to a terrorist attack on the nation. August 20, 2002, ComputerWorld

Data security hinges on money, not technology, feds say
Government customers can foster information assurance by demanding it from vendors, said officials charged with overseeing the safety of the nation's critical infrastructure. August 21, 2002, GNC

Experts Fear Terrorists May Attack Through Cyberspace
To get an idea of what terrorists could do to hamper an emergency response, ABCNEWS asked Innerwall, a Colorado Springs-based computer security consulting firm, to hack into a police department in a different state and see how much disruption it could cause. September 16, 2002, ABCNews

Former FBI chief takes on encryption
Louis Freeh may have lost his battle against allowing encryption when he was at the FBI, but he is continuing the fight now he's left the federal agency. Oct. 15, 2002, ZDNet UK

Scientists protest information lock-down
Top US science advisers say that anti-terrorism security measures have caused scientific information to disappear from the Internet. Oct. 21, 2002, ZDNet UK

Cyber Crime

Cyber crime Victims Hit Back – Online
Fed up with complex procedures and surly customer service, savvy consumers are taking matters into their own hands by investigating and sharing information about online fraud. October 10, 2002, ITToolBox

New pop-up spam mail creeps onto desktop
A developer of bulk-mail software has figured out how to blast computers with pop-up spam over the Internet through a messaging function on many Windows operating systems. October 21, 2002, CNN

Web site defacements rise to all-time high in September
More than 9,000 Web sites were defaced in September, according to London security consultancy mi2g. The figure is 54% higher than for August's figure of 5,830 defacements, which was itself a record high. October 1, 2002, Computer Weekly

Massive credit card heist suspected
A Los Angeles-based Internet company said that 140,000 fake credit card charges, worth $5.07 each, were processed through its transaction system Thursday, in a computer scam that may have affected as many as 25 companies. September 13, 2002, MSNBC

Corporate saboteurs find hacking powerful weapon
Editor's note: This article brings to light a case of corporate espionage, the problems of international laws, and the far-reaching effects of the alleged espionage on the satellite smart-card industry. Most disturbing is the willingness to achieve financial gain through illegal, or as some would think, immoral means. September 3, 2002, Seattle Times

Internet abuse is top reason for workplace discipline
E-mail and Internet abuse is now the number one reason for disciplinary action in companies in the UK, according to a survey carried out by London law firm KLegal and *Personnel Today* magazine. September 3, 2002, ComputerWeekly

Secret Service expands cyber security task forces
Businesses in large cities across the U.S. will soon have a chance to send their IT specialists to quarterly government-sponsored meetings to compare notes with their peers on cybersecurity. August 22, 2002, ComputerWorld

Library hacker gets jail time
Hacking into the Monroe County (NY) Library System's Web site has earned a Philadelphia man 1-to-3-years in state prison. August 15, 2002, Democrat and Chronicle

DrinkOrDie member gets 33 months in prison
A 24-year-old member of DrinkOrDie, one of the oldest international piracy groups on the Internet, has been sentenced to 33 months in federal prison for conspiring to violate criminal copyright laws. August 21, 2002, ComputerWorld

News

Report: Hundreds of Navy PCs missing
The U.S. Pacific Fleet's warships and submarines were missing nearly 600 computers as of late July, including at least 14 known to have handled classified data, according to an internal Navy report obtained on Friday. October 18, 2002, C/Net

Heavy criticism of IT security
Companies are still not doing enough to protect themselves from viruses and hackers attacks, despite their unprecedented growth over the past year. October 08, 2002, VNUNet

Will Canada's ISPs become spies?
The Canadian government is considering a proposal that would force Internet providers to rewire their networks for easy surveillance by police and spy agencies. August 27, 2002, C/Net

Feds to clamp down on wireless LANs

National Institute of Standards and Technology (NIST) will recommend against the U.S. government using wireless LANs - except when applying a long, detailed list of security controls. August 19, 2002, Network World
The draft report: http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf

VA toughens security after PC disposal blunders
The Department of Veterans Affairs is tightening its policy on the disposal of old computers following disclosures that 139 computers containing sensitive personal information about veterans, including their medical records, were given away. August 26, 2002, FCW

E-terrorism: Liberty vs. Security
Since Sept. 11, databases containing information on tens of thousands of ordinary people have found their way into the hands of federal investigators hungry for any scraps of data that might serve as leads in terrorism investigations. August 27, 2002, ZDNet

Insecurity Plagues Emergency Alert System
The FCC-mandated network that lets officials interrupt radio and television broadcasts in an emergency is wide open to electronic tampering, and the government has no plans to fix it. September 10, 2002, Security Focus

Companies Snooze On Cyber-Security
Looking back on what should have been 12 months of big changes, computer-security experts report quite the opposite. To a shocking degree, top executives at most companies remain largely uninvolved with issues of computer security. September 10, ITToolBox

Getting in Front of Security
Two efforts—one public, one private—create diametrically opposed solutions. September 13, 2002, ESJ

Four agencies achieve interoperable PKI
After five years of work, the General Services Administration's Federal Bridge Certification Authority has made the public-key infrastructures of four agencies interoperable. September 18, 2002, GNC

Virginia disciplines 86 workers for misusing Internet
The Virginia Transportation Department last week disciplined 86 employees and contract workers for abuse and excessive use of the Internet. October 10, 2002, GNC

News Homepage links:
ABCNews: http://abcnews.go.com/index.html
C/Net: http://news.com.com/
CBS: http://www.cbsnews.com/sections/home/main100.shtml
CIO: http://www.cio.com/
ComputerUser: http://www.computeruser.com/articles/current_issue.html
ComputerWeekly: http://www.cw360.com
ComputerWorld: http://computerworld.com/
CSO Online: http://www.csoonline.com/
Democrat and Chronicle: http://www.democratandchronicle.com/news/
Desktop Linux: http://www.desktoplinux.com/
ESJ: http://www.esj.com/

FCW: http://www.fcw.com/fcw/
HNS: http://www.net-security.org/index.php
IDG: http://www.idg.net/
Infoconomy: http://www.infoconomy.com/pages/home-page/index.adp
GNC: http://www.gcn.com/
GovExec: http://www.govexec.com/
HNS: http://www.net-security.org/
ITToolbox: http://security.ittoolbox.com/news/
MSNBC: http://www.msnbc.com/news/default.asp
Network Magazine: http://www.networkmagazine.com/
Network World: http://www.nwfusion.com/news/
Newsfactor: http://www.newsfactor.com/
Reuters: http://www.reuters.com/
RSA Security: http://www.rsasecurity.com/newsletter/v3n2/
Seattle Times: http://seattletimes.nwsource.com/html/home/
SCMagazine: http://www.scmagazine.com/scmagazine/thismonth.html
Security Focus: http://online.securityfocus.com/
SNP: http://www.securitynewsportal.com/index.shtml
VNUNet: http://www.vnunet.com/
WhiteHouse: http://www.whitehouse.gov/
Yahoo! News: http://story.news.yahoo.com/news
ZDNet: http://www.zdnet.com/

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
515-281-5956

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 20 Vulnerabilities

Security leaders led by the FBI's NIPC and the SANS Institute published a revised list of the top twenty Internet security vulnerabilities along with instructions on how to fix them. (Updated Oct. 7, 2002)

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.

Stay Safe Online

A site dedicated to educating citizens and helping them secure their home systems. Sponsored by the National Cyber Security Alliance.

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.

The ISO Code:
Integrity…Service…Excellence