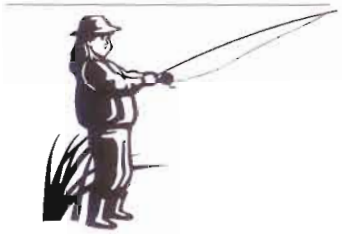
June 2009 NUREG/BR-0304 Volume 5, Number 4

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

OIG INFORMATION DIGEST

CYBER SECURITY OVERVIEW

INSIDE THIS ISSUE:



This issue of the *OIG Information Digest* focuses on cyber security. From one day to the next, computer technology advances by leaps and bounds. The information technology (IT) industry continues to make progress in the way information is processed and managed. The impact of IT on the business environment has been astounding; in a matter of seconds, billions of dollars are floating through cyberspace, changing the economy and wealth of companies and individuals. Furthermore, we can make financial transactions, perform research, and receive messages from friends, and business associates. IT is used for medical procedures and in automobiles; with it, we can make travel reservations, fly an airplane, and launch a satellite. Computers are used for almost everything in our daily lives. Along with those advancements has also come a new "language," and a need to protect our information, computers, and networks from misuse by unauthorized users.

There are dictionaries that explain and define "computer jargon." Here are some favorites; remember when:

- "Surfing" meant riding a board in the ocean?
- "Worm" was this wiggly, icky, brown creature in the dirt?
- "Wallpaper" was a way to decorate the walls in a room without painting?
- "Java" was a strong cup of coffee?
- "Cookie" was a favorite dessert?
- "Hardware" was a type of store to buy tools and other things to repair a house or use in a garden?
- "Firewall" was a brick partition connecting apartments or townhomes?
- "Virus" was a communicable illness?
- "Mouse" was this creepy little vermin who would come in your house when the weather turned cold?
- "Spam" was a great faux meat that came in a can with a twist key lock?
- "Windows" were panes of glass inside a house through which you could view the outdoors?
- "Fishing" (phishing) was a way to catch dinner by using a fishing pole and line and casting it into a shimmering pond surrounded by trees and grass...and the list goes on?

THE FIRST COMPUTERS

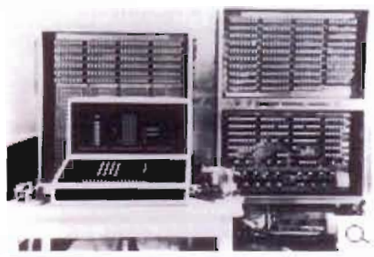
Some of the first "computers," such as the Complex Number Calculator (CNC), were invented as early as 1939. In 1939, Bell Telephone Laboratories completed this calculator, designed by researcher George Stibitz. In 1940, Stibitz demonstrated the CNC at an American Mathematical Society conference held at Dartmouth College. Stibitz stunned the group by performing calculations remotely on the CNC (located in New York City) using a Teletype connected via special telephone lines. This is considered to be the first demonstration of remote access computing.
(http://www.computerhistory.org)

The Complex Number Calculator - Image courtesy of Computer History Museum.

David Packard and Bill Hewlett founded Hewlett-Packard in a Palo Alto, CA, garage. Their first product was the HP 200A Audio Oscillator, which rapidly became a popular piece of test equipment for engineers. Walt Disney Pictures ordered eight of the 200B model to use as sound effect generators for the 1940 movie "Fantasia."
(http://www.computerhistory.org)

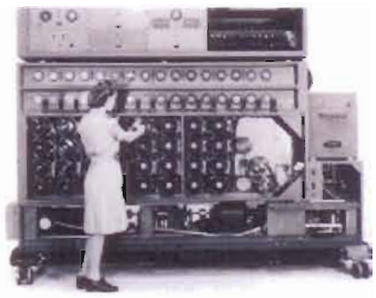
David Packard and Bill Hewlett in their Palo Alto, CA, garage - Image courtesy of Computer History Museum.

The Z3 was an early computer built by German engineer Konrad Zuse working in complete isolation from developments elsewhere. Using 2,300 relays, the Z3 used floating point binary arithmetic and had a 22-bit word length. The original Z3 was destroyed in a bombing raid of Berlin in late 1943. However, Zuse later supervised a reconstruction of the Z3 in the 1960s which is currently on display at the Deutsches Museum in Berlin.
(http://www.computerhistory.org)



The Zuse Z3 Computer - Image courtesy of Computer History Museum.

Based partly on the design of the Polish "Bomba," a mechanical means of decrypting Nazi military communications during WWII, the British Bombe design was greatly influenced by the work of computer pioneer Alan Turing and others. Many Bombes were built, and they dramatically improved the intelligence gathering and processing capabilities of Allied forces.
http://www.computerhistory.org)



The Bombe at Work - Image courtesy of Computer History Museum.

This amazing new technology brought numerous benefits for society, along with an assortment of challenges. Some of these challenges are described in the following pages.

DEFINING CYBER SECURITY

Cyber Security

The term 'cyber security' can be simply defined as security measures to protect information, computers, and their networks. However, putting these security measures into practice is not so simple. The more people rely on the Internet and Internet capable devices, the more complex the security measures need to be. Cyber security is needed for any computing device that is connected to a network, including the Internet. Implementing sound cyber security measures will prevent hacker intrusions, viruses, and other unwanted actions. Cyber security measures are not solely the responsibility of Government agencies or businesses; users must practice cyber security individually. Below are some examples of cyber security issues and helpful links to implement cyber security in your daily habits.

Hacking

When hacking first started, it was fueled by curiosity. The hacker wanted to learn how something worked, but did not want to cause harm. In recent years, hacker motivations seem to have changed. Now, many hackers are fueled by greed, ideological beliefs, and an interest in seeking revenge. A hacker is someone who gains unauthorized access to a computer or network, or is able to escalate their authority without authorization. A hacker's goal is to exfiltrate as much information as possible with minimal effort, similar to a thief breaking into an office and stealing company documents.

Sometimes, despite all security measures in place and caution practiced by computer users, information is stolen or destroyed. Therefore, it is a good security practice to create backups of all important information and store them apart from your computer. For example, if you save everything in your "My Documents" folder on your computer, it is important at least once a month to burn it onto a CD and store it in a secure file cabinet. Then, if your documents become corrupt or stolen, you will have a backup copy to resume business.

Passwords

Have you ever caught yourself asking, "Having multiple passwords with complex requirements is hard to remember, can I just write them all down?" Passwords are used to ensure that the user on the computer system is the correct user. The danger in answering "Yes" to the question above opens the door to online identity theft. Would you give someone else your PIN number and your ATM card? Leaving your password written down in your office allows someone to log onto the computer and pretend to be you.

When creating a password, try not to use common names or numbers. For example, your child's name followed by their birthday is a pattern that is fairly easy for a hacker to figure out and can be just as dangerous as writing down your password and leaving it in your office. It is a better idea to use words or phrases that do not appear in a standard dictionary. A good rule of thumb is to combine numbers, upper case and lower case letters, and special characters to create a complex password.

Hoaxes

Everyone has received a chain letter in their inbox explaining the newest computer virus with a link for the quick fix, but is it a real virus and is it a real fix?

The e-mail usually appears to be sent from a friend, so it must be true. Wrong! By clicking on the link or installing the quick fix, the user will instead install the virus that they were warned about. This can cause the virus to infect your computer and other computers on your network. To help prevent e-mail hoaxes such as this one, verify if the virus described is a real virus and do not forward the e-mail to anyone else. To verify the validity of the virus described in the e-mail, go to anti-virus Web sites such as:

- Symantec Security Response Hoaxes - http://www.symantec.com/avcenter/hoax.html
- McAfee Security Virus Hoaxes - http://vil.mcafee.com/hoax.asp

MODERN SOFTWARE & SOFTWARE CRACKING

Commercially available software programs frequently utilize protection mechanisms that require the input of a lengthy serial or registration number for the program to properly install and function. These software programs are frequently distributed in a compacted form and include subprograms to register aspects of the program with the computer's operating system. While in this compacted or uninstalled state, the numerous files that make up the program are frequently stored in one large file. Having all components of the uninstalled program in this one file enhances the transportability of the program and ensures that needed components are not lost. The program will not function until installed, which involves the automated extraction of the programs files from the large file and placement into various directories throughout the computer.

Software cracking, also known as cracked software, is the modification of software to remove, disable, or otherwise circumvent copyright protections and allow programs to function for unauthorized users. Keygens are created and distributed by software cracking groups and may be downloaded from various Web sites dedicated to software piracy (copying software without the permission of the copyright holder). A keygen is a small program, that uses algorithms to generate a key or functional serial number that allows a specific piece of software to operate.

NRC/OIG Cases

Misuse of NRC E-Mail by a Contractor Employee

OIG completed an investigation concerning misuse of NRC e-mail by an Office of Information Services contractor employee. The investigation was initiated based on information that the employee had placed a computer monitoring program on a computer owned by a private, local company and assigned to the NRC contractor's wife, who worked for the company. According to the information, the wife's e-mails and Web-browsing activity were captured by the monitoring program. The program then automatically and clandestinely sent reports, via e-mail, containing this information to the NRC contractor employee's NRC e-mail account. NRC's contract with the contractor company specifies that the contractor's employees are prohibited from engaging or using Government IT equipment, services, or access for any personal use, misuse, abuse, or any unauthorized usage. Through contact with the manufacturer of the computer monitoring software, OIG was able to verify that the NRC contractor employee had purchased, registered, and installed the software monitoring program. OIG's review of NRC computer e-mail and network logs confirmed the employee had received 288 e-mails, in his assigned NRC e-mail account, which contained the reports sent by the monitoring program. Interception and disclosure of wire, oral, or electronic communications is prohibited under Title 18, Section 2511, of the U.S. Code. The NRC was reimbursed for the amount of the time the employee spent on the computer. The contractor employee was issued a letter of reprimand.

Use of Illegal Software

This OIG investigation disclosed that an NRC contractor employee downloaded onto his assigned NRC computer two software programs that were illegally modified to allow the programs to function without an authorized license. Additionally, the contractor attempted to e-mail the two modified programs to a friend using his NRC e-mail account.

OIG also found that he had previously placed 27 software programs on his assigned NRC computer. These programs had not been activated but were improperly modified to override the internal copywrite protections of each. OIG also found that by virtue of his status as a computer administrator, he had installed and activated for use 20 software programs that were not NRC standard software.

OIG further found that he had used his assigned NRC computer to improperly copy five theatrical movies from DVDs. The contractor acknowledged that he knew that the downloading of cracked software programs was a violation of NRC's policies, and that NRC computers were only to be used for official business. The contractor employee was counseled, and the contractor reimbursed the NRC for the time the employee used the NRC computer.

DEPARTMENT OF JUSTICE CASES

Conspiracy to Intentionally Cause Damage to a Protected Computer

A California man pleaded guilty to Conspiracy to *Intentionally cause Damage to a Protected Computer and to Commit Computer Fraud, and Intentionally Causing or Intending to Cause Damage to a Protected Computer.*

His creation of what is called a "botnet" led to computer malfunctions at Seattle's Northwest Hospital in January, 2005. Further investigation revealed the computer intrusions also caused more than $135,000 of damage to military computers in the United States and overseas.

The creation and use of botnets is a growing problem in cyberspace. A botnet is created when a computer hacker executes a program over the Web that seeks out computers with a security weakness it can exploit. The program will then infect the computer with a malicious code so that it becomes essentially a robot drone for the hacker (also known as a "botherder") controlling the botnet. The computer is ordered to connect to the communications channel where the botherder issues commands. Botnets can range in size from just a few computers to tens of thousands of computers doing the botherder's bidding.

According to the plea agreement, three individuals created the botnet to fraudulently obtain commission income from private companies by installing adware on computers without the owner's permission. For example, by controlling someone's private computer, the botherder can remotely install the adware and collect commission without the computer owner's permission or knowledge. In this case, the Government alleged that the perpetrators earned $100,000 in fraudulent payments from companies that had their adware installed.

According to court filings, as the botnet searched for additional computers to compromise, it infected the computer network at Northwest Hospital in north Seattle. The increase in computer traffic as the botnet scanned the system interrupted normal hospital computer communications. These disruptions affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work, and computers in the intensive care unit shut down. By going to backup systems, the hospital was able to avoid any compromise in the level of patient care.

Following the indictment, the investigation revealed that the botnet had also damaged U.S. Department of Defense computer systems at the Headquarters 5th Signal Command in Manheim, Germany, and the Directorate of Information Management in Fort Carson, CO. More than 400 computers were damaged at a cost of $138,000 to repair.

Under the terms of the plea agreement the subject will be responsible for more than $252,000 in restitution to Northwest Hospital and the Department of Defense.

Conspiracy is punishable by up to 5 years in prison and a $250,000 fine. *Intentionally Causing or Intending to Cause Damage to an Infected Computer* is punishable by up to 10 years in prison and a $250,000 fine.

DEPARTMENT OF JUSTICE CASES (CONT. FROM PAGE 5)

Ex-Hostgator.com Employee Sentenced for Computer Intrusion

A former employee of Hostgator.com (a Web hosting company) has been sentenced following his conviction related to exceeding his access and intentionally causing damages to Hostgator.com. The support technician was indicted by a Federal grand jury in the Southern District of Texas on June 16, 2008. The case was transferred to the Northern District of Georgia following the employee's arrest on June 19, 2008, in Atlanta, GA. On November 16, 2008, he entered a formal plea of guilty to one count of committing computer intrusion.

In early October 2007, the former Hostgator employee moved to Atlanta and began working for a competitor company without ever notifying Hostgator he had ended his employment status. A Web-hosting company provides server space, Web services, and maintenance for Web sites of individuals or companies that do not have their own Web servers. Thereafter, he gained access into the Hostgator system and then knowingly executed several command and code functions to intentionally impair the integrity of the customer support network. Hostgator never authorized the execution or transmission of these commands. As a result of the intrusion, the defendant caused Hostgator to incur a loss in excess of $5,000 in value. Hostgator lost a significant amount of revenue and also incurred losses due to the damage assessments and restoration of the data and programs.

He was sentenced to 8 months imprisonment, a $100 special assessment and a 3-year term of supervised release for his involvement in the scheme to intentionally damage Hostgator, in violation of 18 U.S.C. §1030(a)(5)(A)(I).

Shadowcrew Organization Was Called 'One-Stop Online Marketplace For Identity Theft'

Six men who administered and operated Shadowcrew.com, one of the largest online centers for trafficking in stolen credit and bank card numbers and identity information, pleaded guilty in Federal court. The one-stop online marketplace operated by the defendants was taken down by the U.S. Secret Service, closing an illicit business that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses that exceeded $4 million.

The defendants admitted their respective roles in the online conspiracy to commit credit and bank card fraud, as well as identification document fraud. One person also pleaded guilty to a second count of unlawful transfer of identification to facilitate criminal conduct. He admitted his role in illegally obtaining approximately 18 million e-mail accounts with associated personally identifying information.

The Shadowcrew organization and its associated web site was a hub of online identity theft activity, facilitating online trafficking in stolen identity information and documents, as well as stolen credit and debit card numbers. A year-long Secret Service investigation led to the arrests of 21 individuals in the United States.

IT Security Tips

Desktop Security:

- Must be 12 characters long with at least one uppercase, lowercase, number and special character
- Don't share passwords
- Don't write down passwords
- Create passphrases for easy recall
- Lock your computer when not at your workstation
- Transport a laptop in a secure manner—don't leave it in the car
- Use the correct IT system for information such as: (SUNSI, SGI, and Classified)

For more information go to the NRC internal Web site: http://www.internal.nrc.gov/CSO.

DEPARTMENT OF JUSTICE CASES (CONT. FROM PAGE 6)

The indictment charged that the administrators, moderators, vendors, and others involved with Shadowcrew conspired to provide stolen credit and bank card numbers and identity documents through the Shadowcrew marketplace. The account numbers and other items were sold by approved vendors who had been granted permission to sell by administrators and moderators of the Shadowcrew site after completing a review process.

The main perpetrator admitted using techniques such as phishing and spamming to illegally obtain credit and bank card information which he then used to make purchases of merchandise online.

The illegally obtained goods were then sent to a "drop" or mailing address specifically set up to receive the stolen goods.

The defendants all acknowledged that Shadowcrew members sent and received payment for illicit merchandise and services via Western Union money transfers and digital currencies such as E-Gold and Web Money. In addition, they admitted that they illegally acquired via a computer, approximately 18 million e-mail accounts with associated usernames, passwords, dates of birth, and other personally identifying information — approximately 60,000 of which included first and last name, gender, address, city, state, country and telephone number.

To learn more about cyber security, visit: http://assets.opencrs.com/rpts/R40427_20090310.pdf.

Any time you suspect anyone is misusing a Government computer for any reason, please contact the Office of the Inspector General by mail, telephone, or the Web. You may request anonymity.

USNRC
Office of the Inspector General
Mail Stop O 5E13
11555 Rockville Pike
Rockville, MD 20852

We're on the Web! Click on the internal or external web site. Scroll to the bottom of the page. Click on Inspector General on the left. Click on Submit on-line form, type your complaint, and hit submit. The OIG does not try to find out where the e-mail came from. You may request anonymity.

HOTLINE

1-800-233-3497

TDD

1-800-270-2787