Global Information Assurance Certification Paper

Mitigating the Risks of Laptop Data

Practical steps to reduce the threats to mobile computer data

Ryan Booton
March 10, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b option 1

Abstract

Mobile computers provide several advantages over desktop workstations. Because of this, over the years businesses have begun to rely on them more often. But as their use increases, a disturbing trend is also taking place. The amount of information available on how to bypass built-in security features is increasing dramatically. Hacking information has even made it to television, on programs such as TechTV.[1] Knowledge of how to break into computers can be obtained simply by surfing the Internet, watching a television program or reading a chapter of a book. In today's world, it must be assumed that laptop computer thieves can easily obtain the technical knowledge necessary to bypass many common security measures and obtain access to the data stored on a portable computer's hard drive.

Many companies and government organizations cannot afford to have their confidential information exposed to unauthorized individuals. Legislation currently exists which requires many agencies to disclose certain security breaches to customers and legal authorities. But actions such as this could place a business's security insufficiencies in the limelight.

This paper identifies some vulnerabilities specific to laptop computers running Windows, and suggests preventive measures to help mitigate risks. First, to help give a clear picture of the gravity of these threats, some of the intangible assets that are involved will be discussed. An overview of physical security will then provide the reader with a few suggestions on how to reduce the likelihood of theft. Advice is also offered to help minimize the chance of attacks through network or dial-up connections. The problem of unauthorized access by individuals with physical possession of a computer will then be discussed. This discussion will range from protecting against short-term unauthorized access of a computer left unattended for only a brief period of time, to the threat of a computer savvy thief with physical possession attempting to hack in. Ways of encrypting hard drive data will also be included. Assessing these risks individually can help to achieve multi-layered security, also known as Defense in-Depth.

Mitigating the Risks of Laptop Data

In November of 2003 Wells Fargo was faced with an embarrassing situation. A laptop computer used by one of their contractors was stolen. This computer contained the names, addresses and Social Security numbers of thousands of customers. Though Wells Fargo's security infrastructure may have been no different from many others in their industry, they had failed to ensure that this contractor adequately secured the laptop, and did not require the contractor to encrypt all sensitive information contained on its hard drive.[2]

Since this information could potentially be used to achieve identity theft, clearly the appropriate action was to promptly notify all individuals whose personal information had been compromised. Wells Fargo was even required to do so by law. A law in California, SB 1386, states:

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[3]

But notifying customers meant exposing security shortcomings to the public and damaging the company's reputation. Eventually, the media would even hear of it, spreading the story to countless other potential customers.

Since then, this story has made its way to dozens of banking and information systems security web sites and has been discussed widely. Though the story was highly publicized, because Wells Fargo handled the situation extremely well, their reputation was not hurt as much as it could have been. But as situations like this become well known, one could only assume that the public and legal authorities will have less tolerance. Information systems security personal should be expected to learn from examples such as this.

One of the first steps in assessing security risks is identifying the assets that are involved. Once assets are identified, monetary values can then be calculated in order to determine the amount of money to spend on countermeasures. However, the Wells Fargo incident shows that intangible assets such as a company's reputation are often involved. Assets such as this can be extremely hard to put a price on. Yet the cost of tangible equipment, such as hardware, is insignificant when compared

to the potential loss of customers, or legal action against a company because of negligence.

Since laptop computers are often used outside of an organization, they are not protected by many of the security measures guarding the rest of a company's systems. Most companies have a firewall to protect their network from hackers on the Internet. Many buildings have guards or security systems. Even a receptionist at the front door will help deter thieves from stealing the computers in an office.

But laptop computers are carried around in airports, left in cars and hotel rooms, used at many types of locations and are often connected to various dial-up Internet connections instead of to only one secure network at a main location. This makes them more vulnerable to theft, unauthorized access, viruses and hacking attempts.

Some companies have an option of storing confidential information at a centralized location. Roaming users can then connect to a server and access confidential data through a VPN or SSL connection. In these scenarios, data is encrypted until it is presented on the user's screen. However, many mobile computer users frequently work in locations where there is no Internet access. This is often the case for auditors or sales representatives, who cannot use a customer's phone line every time they need to access their data.

The Threat of Theft

One of the first threats that every organization should consider is the threat of theft. Perhaps the simplest yet most important thing that can be done to minimize this threat is to provide adequate physical security. Though physical possession is not necessarily required for an attacker to gain access to the data on a computer, if unauthorized users do not have physical access, they may have a tougher time accessing the data contained on a hard drive. According to law number 3 of a Microsoft article titled "The Ten Immutable Laws of Security":

> If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.[4]

Training is perhaps the most important thing that can be done to reduce the threat of computer theft. Laptop computer security guidelines and policies can be used to help teach the proper handling of portable computers. Some suggestions include instructing employees to not leave computers unattended in a vehicle. If this is not possible, another option is to have employees keep them out of site or in a vehicle's trunk. Portable computers should also not be checked as baggage on a plane. Some

organizations ask employees not to carry mobile computers in standard laptop carrying cases while traveling. This prevents thieves from realizing a person has one with them.

Hardware locks help prevent laptops from being stolen when they are left unattended. Cable locks are the most common type of hardware locks. Cable locks are wrapped around large heavy objects, such as desks, and are connected to laptop "security slots". Some have alarms that will sound if the cable is cut, which increases the chance that a thief will be caught immediately after stealing a laptop.

Though cable locks can provide a high amount of protection, users often have difficulty finding objects suitable to attach to. They frequently resort to looping the cable around a leg of a table, which can be easily lifted. Another common mistake that users often make is leaving the key to the lock in an obvious location.[5]

Hardware tracking systems locate laptops after they have been stolen, and act as a strong deterrent to theft. Products such as ComputracePlus report a PC's location the moment a stolen computer has access to the Internet. The ComputracePlus agent cannot be easily deleted from the hard drive can even survive a hard drive format. A "Data Delete" service is also offered to delete hard drive contents upon a customer's request.[6]

The Threat of Network or Internet Access

Since mobile computers are often connected to the Internet via dial-up connections and to networks of which security is unknown, extra care should be taken to ensure laptops are provided with software firewalls, strong operating system security policies and settings, and antivirus protection.

Software firewalls are inexpensive and are becoming simple to configure. Windows XP comes with a software firewall called the Internet Connection Firewall (ICF). To configure this, the majority of Windows XP users simply need to make sure it is enabled on all dial-up and network connections. Others will require information on which ports to leave open for various applications to work.

Though ICF works fine at blocking people on the outside from accessing your computer, it does not block outgoing communication. Many other firewall programs, have the ability to inform computer users when applications attempt to send information over the Internet. If a Trojan horse were embedded into an application, these types of firewalls would inform the user any time the Trojan horse attempted to send data to the internet. Users are then forced to decide whether or not to allow the

program to do so. When restricting outgoing communication is not provided, data is at the mercy of the developers of the applications that are installed.

Though ICF does not restrict outgoing communication, there is another way of looking at this issue. The software firewalls that monitor outgoing communication often display a somewhat illegible message, which asks the user to make a decision. They usually say that a specific program is attempting to access the Internet. At times this is a program that the user is familiar with, but other times it is Internet Explorer using a library file that even an experienced user would not have heard of. Often people are in a hurry to get their work done, and do not even take the time to read the messages.

Another way to protect computers from the risk of Trojan horse programs is to restrict users from installing programs. Since administrators have full control over their computers they can inadvertently install software as they surf the Internet. Administrators can also easily make system changes that could prevent their computers from working properly, or lower their security settings. Changing the group membership of user accounts, by having them only be members of the “Users” group, can prevent all of this. Though this may add a few support issues when employees need to install software updates, the added protection makes this worthwhile. Microsoft offers a good explanation of why you should not run your computer as an administrator:

> Running Windows 2000 or Windows XP as an administrator makes the system vulnerable to Trojan horses and other security risks. The simple act of visiting an Internet site can be extremely damaging to the system. An unfamiliar Internet site may have Trojan horse code that can be downloaded to the system and executed. If you are logged on with administrator privileges, a Trojan horse could do things like reformat your hard drive, delete all your files, create a new user account with administrative access, and so on.[7]

Operating system security policies and registry options should be set to further reduce the chance of unauthorized network access. Strong passwords should be required, with account lockout policies locking user accounts after a few invalid attempts. Guest accounts should be disabled. Enforce minimum password lengths and both maximum and minimum password ages. Remove or disable any unnecessary services. Become familiar with group policy security options. Also be sure to read articles specifically focused on hardening your operating system, which will go into security settings in more detail.

The Threat of Short-term Unauthorized Access

Even if it were possible to provide enough physical security to eliminate any chance of a laptop being stolen, there is more to consider. An unauthorized user could just as easily access the data on a laptop without stealing it. If one of your users were working off-site, and walked away from a laptop, even just for a few minutes, it may be easy for someone to gain access. This threat may exist every time an employee walks out to grab a can of pop. Every lunch hour, or even a bathroom break, could be an opportunity for an attacker to gain access to your data. When mobile users work off-site at customer locations where physical security is low, this threat increases.

Since an attacker may have only a short window of opportunity, any hurdle that can be put in place, may be enough of a barrier to prevent unauthorized access. Even though many of the measures presented here are easily overcome, they may slow down an attacker long enough. Many of these suggestions can be implemented very quickly, yet will go a long way towards preventing this type of access.

Password protected screen savers are a great example of a very simple security measure that can be initiated immediately, yet adds quite a bit of security. Without them, anyone could sit down at your desk and have access to your data whenever you are away from your workstation. An even better option would be to instruct users to lock their computers before taking a break, or leaving them for any reason. Though users might complain about being required to do this, it is as easy as pressing Ctrl-Alt-Delete, then Enter.

Windows NT, 2000 and XP all have the option of formatting hard drives with the NTFS file system. NTFS has built-in security features that file systems such as FAT and FAT32 do not offer. Even though a Windows 98 computer might ask a user for a password to log in, because the file system uses FAT32, a person could simply click cancel and still access everything on a drive. Because of the security features of NTFS, it provides a little protection in preventing attackers from simply booting a computer to a standard bootable floppy disk or CD, and obtaining access to your hard drive.

However, many operating systems and utilities are available that provide access to NTFS formatted hard drives. These totally bypass NTFS security. Knoppix, a GNU/Linux distribution that boots from a CD, allows easy access to NTFS partitions and will also conveniently allow someone to copy your data to a USB flash drive.[8] Other programs such as NTFSDOS (www.sysinternals.com) provide access to NTFS volumes by booting with a floppy disk. Operating systems such as these are freely

available, and do not require any special knowledge to run. Without other security measures in place, if a laptop were left unattended, even for just 15 minutes, a hacker could boot a computer to a CD, floppy disk, or USB flash drive and copy whatever he wished.

BIOS passwords further prevent short-term unauthorized access. Though most desktop and many laptop computers allow BIOS passwords to be cleared simply by removing a CMOS battery or resetting a jumper, many laptop computers offer enhanced security features, making clearing passwords difficult.[9] BIOS passwords can be set from a computer's CMOS configuration utility, usually by pressing either F2 or Delete when prompted while a computer boots. These are required to be entered before a computer's operating system begins to load. When implemented, a BIOS password must be entered regardless of the boot device, or the operating system being used.

While you're in the CMOS configuration utility, disable booting to anything other than the computer's hard drive. Also create a CMOS setup password to ensure that these settings cannot be changed. Be extremely careful to keep track of all BIOS passwords, since removing these may be difficult.

Now that we plan to ward off unauthorized access through password protected screen savers, locking the desktop, BIOS passwords, NTFS and disabling the ability to boot to compact and floppy disks, one might erroneously think that unauthorized individuals could not quickly obtain access to our data from our workstation. However, all of this security is absolutely child's play to many people, including anyone willing to spend a small amount of time learning how. Attackers could simply remove your laptop hard drive and access it from an operating system on a different computer. Since laptop computers have IDE hard drives, they can be connected to desktop computers using a 2.5" to 3.5" IDE hard drive cable adapter. Though this may sound a little time consuming, it could be easily done over a 15 minute coffee break.

Some laptop hard drive manufactures, such as Hitachi, provide hard drive passwords that will greatly reduce this threat. Laptop manufacturers, including Dell and IBM, have provided hard drives like this for years. Like BIOS passwords, these are set with a computer's CMOS configuration utility. However unlike BIOS password, they follow a hard drive, and must be entered, even when a hard drive is installed on another system.

Protecting laptop computers with the above suggestions will greatly reduce the chance of an attacker quickly accessing your data, when they have physical access to your computer for only a short period of time. But what if a computer was stolen, and a determined hacker had as much time

as he or she wanted to attempt to access your data? Would these measures help at all? If not, what else could be done?

The Threat of Long-term Physical Possession

As mentioned previously, the BIOS passwords of many portable computers are much harder to clear than most desktop computers. Since laptop manufacturers do not normally advertise the ways in which this can be done, it is somewhat difficult to determine the level of security many BIOS passwords actually provide.

However, with a little digging through newsgroups, one can learn that often laptops manufacturers store BIOS passwords in electrically erasable programmable read-only memory (EEPROM), located on a system board. Though removing CMOS batteries does not erase EEPROM, these chips can be erased by exposure to an electrical charge.[10] They can also simply be removed and replaced. If an attacker finds either of these methods a little too technical, the attacker has the option of sending the laptop to someone else for a chip replacement. Many companies provide this service. Password Crackers, Inc, a reputable company and one of the oldest commercial password recovery organizations in the world explains:

> Most laptop or notebook computers feature enhanced security. Password Crackers, Inc. offers a wide range of laptop security chips that can be used to replace the existing chips on a laptop or notebook and reset the security. Passwords can also be recovered from chips that have been removed from laptop or notebook systems. These passwords may be required to attempt to unlock protected hard disks.[9]

Like BIOS passwords, documentation detailing the degree of security provided by hard drive passwords can also be hard to find. According to IBM:

> If you forget your Supervisor password, there is no way to reset your password to enter the BIOS configuration. Setting a supervisor password automatically sets the hard drive password. If you do not remember your supervisor password you must have the system serviced to have the system board and hard drive replaced.[11]

This may lead someone to believe that some hard drive passwords might be extremely secure. However, Dell, a manufacturer who often uses the same hard drives as IBM, states:

> The password features provide a high level of security for the data in your computer or hard disk drive. However, they are not

> foolproof. If your data requires more security, you should obtain and use additional forms of protection…[12]

Many companies offer data recovery services, which can recover the data on password protected hard drives. Though many of these companies require proof of ownership, others may not.

While BIOS and hard drive passwords will help keep the uneducated out, they will only slow down a computer savvy hacker with physical possession of your computer, intent on accessing the data. Even though this is true, they will still greatly reduce the possibility of an unauthorized user obtaining access to the data on a laptop in a short period of time. Because they can be configured very quickly, they are a very good way to increase the security of your laptops immediately. However, to provide stronger protection to help ensure thieves cannot access the data on a stolen laptop, confidential information should also be encrypted.

Encrypting File System (EFS)

Encrypting the confidential data on laptop hard drives can go a long way towards ensuring that your data is not compromised in the event a computer is stolen. But all encryption methods are not equal. Microsoft provides a way to encrypt files and folders with their Encrypting File System (EFS). But before rushing out to use this, it would be wise to evaluate this type of encryption to determine whether or not it is right for your organization.

EFS is provided on Windows 2000 and XP computers and allows only the users who encrypt files and "data recovery agents" the ability to open encrypted files. EFS encrypts the files and folders chosen by a computer user. It goes beyond NTFS permissions, which only provides protection from those who log into the Windows operating system installed on your hard drive. EFS is not available on Windows XP Home Edition, and requires hard drive partitions to use NTFS. [13, 14]

Whenever any type of encryption is used, care should be taken to make sure users cannot lock themselves out of their encrypted data. On Windows XP computers, this can easily be done when a user forgets a password, and is required to have it changed by an administrator. Because of this risk, "data recovery agents" should be designated to provide an alternate method of accessing encrypted files. A password recovery disk can also help minimize this risk. However, be sure to keep all password recovery disks and the private keys of recovery agents locked up in a secure location. [13, 14]

Users of Windows 2000 whose computers are not members of a domain should either consider upgrading to Windows XP or look at third party encryption solutions. This is because Windows XP adds an additional level of protection, which affects the security of encrypted files. Since many utilities exist that can change passwords, an attacker could easily boot to a floppy disk containing a utility such as this, change a password and then simply sign in using the laptop user's new password. When passwords are changed this way on Windows XP computers, the certificates that are used in decrypting files become inaccessible.[13]

There are several things to keep in mind when using EFS:[13, 14]

- Every folder cannot be encrypted with EFS. There is no way to encrypt the %systemroot% folder and the pagefile.
- Since users determine which files to encrypt, there is no way for an administrator to ensure everything is encrypted that should be.
- Since word processing and other types of programs create unencrypted temporary files, be sure to encrypt the folders that these files are written to.
- Whenever possible, encrypt folders instead of files. When a folder is encrypted, all files contained in the folder become encrypted, as well along with all new files created in the folder.
- If your computer is stolen while it is in hibernation, open files could be seen by viewing the hiberfile.sys file from another operating system. Hibernation can be disabled to prevent this risk.
- Encrypted files copied to floppy disks, or other FAT volumes, are not encrypted at the destination. Use the Windows Backup utility to backup data. This will leave files encrypted, even when writing to FAT volumes.
- Microsoft provides a feature called SysKey to encrypt password hashes, making EFS encrypted files more secure. SysKey can be configured to have a password used as a key, or to have startup keys stored either on a floppy diskette or locally. By default, Windows XP computers have SysKey enabled and stores keys locally on a system's internal hard drive.

Two-factor Authentication

The use of third party products to provide two-factor authentication can greatly increase the degree of security provided by EFS. Two-factor authentication improves security by adding an additional process to verify the identity of a computer user. Since intruders, often can access a system by learning of a user's password, requiring an additional means to ensure the computer users are who they claim to be greatly increases security. Two-factor authentication is provided by any two of the following three factors:[15]

- Something a user knows. A password, passphrase or other piece of information known only to the user.
- Something a user has. A security token, smart card or other authentication device. Without possession of this piece of hardware, users can be disallowed access.
- Something a user is. This involves biometric technology such as fingerprint scanners and voice recognition.

Since most portable computers come with USB ports, USB tokens can provide an excellent way to achieve an additional authentication method. Because users are not granted access to a system until they authenticate, without this hardware device, files encrypted with EFS cannot be opened. This same benefit also applies to smartcards and biometric technology, which is integrated into several of today's laptop computers.[16]

Without an additional authentication method, it may be possible for hackers to recover passwords and access files encrypted by EFS, even on Windows XP computers. Kevin Rose demonstrated a very straight forward way of doing this on a television program that aired for TechTV on February 25, 2004. An overview of this demonstration is available at http://www.techtv.com/screensavers/darktips/story/0,24330,3625960,00.html. Even the encryption of password hashes provided by SysKey is shown to be vulnerable through a shareware program called SAMInside.[1]

Third Party Encryption

If EFS does not seem to be a good match for your organization, several third party products are available that provide strong encryption. These programs can be classified into three categories. [17]

- **File/folder based encryption** programs are similar to EFS in that they allow a user to select individual files or folders to be encrypted.
- **Virtual disk encryption** products create single encrypted files, which are presented to the operating system as a logical drive.
- **Full disk encryption** programs encrypt the entire contents of a drive.

Though each of these methods have their own benefits, since both file/folder based and virtual disk encryption programs do not encrypt all files, full disk encryption products may be preferred.

Since full disk encryption products encrypt all data on a hard drive, users cannot accidentally forget store a file in an encrypted folder. These programs are typically operating system independent. Encryption software vendors accomplish this by forcing users to authenticate to the encryption

software before an operating system begins to load. This prevents thieves from accessing a stolen hard drive through an operating system on another machine.

Though it is evident that many users have a need to go beyond the capabilities of EFS, third party encryption programs are not as commonplace as one would expect. Many computer security books explain EFS; however few provide information on third party encryption software. Reviews of these products are sparse. Only a relatively few number of disk encryption software companies have headquarters located in the United States. This is in contrast to other software products. Though this list is by no means comprehensive, here are a few third party full disk encryption products that you may wish to evaluate: [17]

- SafeBoot – SafeBoot Mobile Data Security - www.safeboot.com
- DriveCrypt Plus Pack (DCPP) – SecurStar Computer security - www.securstar.com
- Pointsec – Pointsec Mobile Technologies – www.pointsec.com
- Safeguard Easy - Utamaco Safeware AG – www.safeguardeasy.com
- SecureDoc - WinMagic Inc. – www.winmagic.com
- Encryption Plus Hard Disk - PC Guardian Technologies, Inc. - www.pcguardiantechnologies.com
- CompuSec - Global Technologies Group, Inc. – www.gtgi.com
- iT_SEC_datasafe – Secude it security GmbH - www.secude.com

When evaluating full disk encryption products there are several things that you may wish your chosen product to offer. Here are some suggestions of things that you might want to look for:

- Recognized secure encryption algorithms
- Pre-Boot Authentication
- Support for multiple users
- Integration with smartcards or security tokens to provide two-factor authentication
- Ability to prevent administrators from having access to data
- Support for encrypting data on removable drives (floppy disks, compact disks and USB flash drives)
- Centralized management features
- Auditing capabilities
- Encryption of backup files
- Single sign-on capability
- Federal Information Processing Standard (FIPS) certification or Common Criteria validation

Summary

Information on how to access data stored on laptop computers is everywhere. Many security features can easily be overcome. Because of this, companies that cannot afford to have their confidential data exposed must realize that anyone can easily learn how to access the data on their mobile computers unless they are adequately secured. Even though many security options can be undermined, they still will place barriers between unauthorized users and your data. Although no security measure will provide complete protection, there are many ways to encrypt data that will greatly add to the security of your confidential information.

This paper explained several security threats individually, and offered some suggestions on ways to reduce these risks. By assessing many risks separately, layers of security can be provided.

References

[1]Kevin Rose, TechTV Inc., "Dark Tip: Windows Password Hacking", February 2004
URL: http://www.techtv.com/screensavers/darktips/story/0,24330,3625960,00.html

[2] Mark Rasch, "The Wells Fargo Example", December 2003
URL: http://www.securityfocus.com/columnists/201

[3] Legislative Council of California, introduced by Senator Peace, principle coauthor: Assembly Member Simitian
Bill number: SB 1386, introduced in 2002, operative July 1, 2003
URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[4] Microsoft Corporation, Microsoft Security Response Center, "The Ten Immutable Laws of Security", Oct 2003
URL: http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx

[5] Ben Smith, Brian Komar, "Microsoft Windows Security Resource Kit", Microsoft Press, Mar 2003, p. 339-340

[6] Absolute Software Corp, "ComputracePlus: FAQs", 2004
URL: http://www.computrace.com/public/products/computraceplus/faqs.asp

[7] Microsoft Corporation, Windows XP Professional Product Documentation, "Why you should not run your computer as an administrator", 2004
URL: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_security_whynot_admin.mspx

[8] Knoppix.Net, "Knoppix", Date unknown
URL: http://www.knopper.net/knoppix/index-en.html

[9] Password Crackers Inc., "DELL - BIOS Password Security Chips", March 2004
URL: http://www.pwcrack.com/security_chips_dell.shtml

[10] Webopedia, "EEPROM", July 2003
URL: http://www.webopedia.com/TERM/E/EEPROM.html

[11] IBM Corporation, “TP General - How to change/remove/set a supervisor password”, August 2003
URL:
http://www-306.ibm.com/pc/support/site.wss/document.do?lndocid=YAST-3JZS7U

[12] Dell Inc., “Securing Your Computer: Dell™ Latitude™ LS Portable Computers User's Guide”, 2004
URL: http://support.jp.dell.com/docs/Systems/latls/en/ug/security.htm

[13] Ed Bott, Carl Siechert, “Windows Security Inside Out for Windows XP and Windows 2000”, Microsoft Press, June 2002, p. 624

[14] Chris Weber, Gary Bahadur, ”Windows XP Professional Security”, McGraw-Hill, 2002, p. 91-105

[15] Russell Kay, “Authentication”, March 2000
URL:
http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,44257,00.html

[16] Julian Ashbourne, “Two-factor Authentication”, Date unknown
URL:
http://www.scmagazine.com/products/index.cfm?fuseaction=GroupTestDetails&GroupId=6032

[17] Mike DeMaria, Network Computing, “Gone in 6.0 Seconds”, September 2002
URL: http://www.networkcomputing.com/1320/1320f43.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event