Global Information Assurance Certification Paper

David Wolfe
SANS GSEC - Track 1
Practical Assignment Version 1.4b
February 8, 2004

Psst! Your secrets are showing!

Eliminating the trail of breadcrumbs before an insider gets them.

> *Men are four:*
> *He who knows and knows not that he knows. He is asleep; wake him*
> *He who knows not and knows not that he knows not. He is a fool; shun him*
> *He who knows not and knows that he knows not. He is a child; teach him.*
> *He who knows and knows that he knows. He is a king; follow him.*
>
> Lady Burton[1]

Introduction

A critical step in planning military operations is developing a list of potential courses of action (COAs) that you believe your enemy may employ. After developing this list, it is customary to identify the *most likely* COA that your enemy will use against your forces, as well as the *most dangerous* COA. In practice, these are often not the same. With regard to computer security, although hackers are typically painted as the ultimate threat, if an organization is widely known to work on projects involving valuable proprietary and/or classified information, then malicious insiders are without a doubt both the most likely and most dangerous threats. Yet the vast majority of our defenses face outward to repel the external hackers, crackers and phreaks. In addition, detecting unauthorized actions by an insider is very difficult, because he or she is supposed to be in the workplace, and already has some degree of access.

In the future, security initiatives like the National Security Agency's *Voltaire* project[2] may provide tools to detect and prevent insider turncoats like Robert Hanssen from quietly sifting unseen through files and databases for sensitive information and leads to other, more closely held secrets. However, until such tools and capabilities are available and as affordable as current anti-virus software, protecting secrets from insiders will remain a difficult, but not impossible, task. Meeting this threat won't require draconian policies or Gestapo-like measures, either, because most users assigned to sensitive projects are conscientious about security--*if* they are aware of the threat and taught practical countermeasures. In this paper, the author will demonstrate how widely-used Microsoft Windows, Microsoft Internet Explorer, and Windows-based applications deposit unseen copies of documents on hard drives, and leave supposedly deleted information inside files and documents. Fortunately, a trained user can remove this information from a project workstation before quitting for the day. With a little more training, the user can quickly and effectively eliminate the accumulated browser files and data that allow an intruder to reconstruct the user's activities and follow this virtual trail of breadcrumbs to the organization's intellectual crown jewels. With the right training, checklists and utilities, the user can erase these telling traces long before the insider catches the scent.

The Threat

What makes the insider threat so compelling? As suggested earlier, malicious insiders are already past almost all of the organization's defenses. They are (until proven otherwise) trusted employees, not spies, and free to move about the organization, gathering clues to sensitive information by snooping through in-baskets, wastebaskets and desktops, looking over shoulders and listening to conversations in adjacent cubicles and hallways. Once cued to a target, they can return to harvest the most sensitive information straight from the project workstation by downloading it onto easily concealed removable media such as a USB drive, or even burn a CD if the workstation is so equipped. And chances are slim that anyone will notice, because the insider is not a stranger in a trench coat, but a familiar face.

The insider threat isn't new or trivial, and a growing body of evidence suggests these attacks are widespread even though most organizations are loath to admit it publicly. In a 2001 Carnegie-Mellon Software Engineering Institute survey, 71% of participating companies acknowledged insider attacks.[3] Since then, the Gartner Group and others have confirmed this growing threat, quoting numbers in the 70-90% range.[4] Clearly, the threat is real, and intrusion detection systems and other new technologies are just starting to look for bad actors already inside the traditional lines of defense. Like a fox inside the hen house, the insider is in position to steal sensitive information directly from co-workers' workstations and networked drives.

Because Microsoft's operating systems, web browser, and office applications have so many powerful features, they are widely used by government, business and industry. But for all their useful features, these software programs may also leave sensitive information on the user's hard drive and network drives, often without the user's knowledge. And since most organizations' workstations sit in unlocked offices and open cubicles, an insider can easily hop onto an unattended machine to quickly look for left-behind sensitive information, or remain after-hours for more in-depth snooping. The biggest challenge to the Information Assurance Team is to help users recognize where sensitive information has been deposited and remove it before the insider finds it. The following are some of the most common types of hidden information on Windows 2000 and Windows Millennium-based workstation:

1. Unseen Files. Unseen by the user, Windows and other applications constantly write information to hard drives as a normal by-product of handling files. This includes entire documents in their original formats.
2. Hidden Data Retained Inside Files. Supposedly deleted data is left within files and documents, and is often easily recovered without any special utilities.
3. Clues to Other Information. Convenience "features" in the operating system and browser continuously update lists of recently accessed files and record user actions, providing an electronic trail of breadcrumbs to the user's information.

Regrettably, too many users are unaware of this vulnerable information, and often lack the training and tools to effectively find and remove it. Hopefully this quick overview will fill that gap.

Unseen Files

Temporary (.tmp) Files. In its many versions, Windows and Windows-based applications have earned a reputation for consuming disk space by leaving temporary files on the hard drive after completing tasks. In the early DOS/Windows days when hard drives had limited capacity and a high cost, network administrators conserved precious workstation hard drive space by adding a couple commands at startup to automatically jump to the TEMP directory, then delete all temporary files. Back then, the focus was on resources, not security. According to Microsoft, "A temporary file is a file that is created to temporarily store information in order to free memory for other purposes, or to act as a safety net to prevent data loss when a program performs certain functions. For example, Word determines automatically where and when it needs to create temporary files. The temporary files only exist during the current session of Word. When Word is shut down in a normal fashion, all temporary files are first closed and then deleted."[5] However, when Word or other Windows applications shut down ***ab***normally (like when the application/system locks up for no apparent reason), a copy of the working file is often left behind on the hard drive as a temporary file. In general, temporary files result from poorly written programs, improper shutdowns, program hangs, and computer crashes.[6] These temporary files do, however, prove helpful when recovering the file being edited at the time of a lock-up, but when users habitually fail to open and close files in the way the application writers envisioned, the result is an ever-growing collection of temporary files scattered across the hard drive. For example, the author used Microsoft Word for Windows to draft a massive manuscript, working nightly over a period of months without bothering to clean up the temporary files. Not surprisingly, literally dozens of copies of the manuscript were automatically saved in the TEMP directory with a ***.tmp*** file extension or a temporary name beginning with the **~** symbol, each easily recoverably by anyone with access to the machine and the inclination to look. Fortunately, the user can easily find these temporary files on the hard drive by clicking the ***Start*** button, ***Search***, ***For Files And Folders***, and typing ***"*.tmp***" or "***~*.***". The files will be displayed in the results window, where cleanup is fast and easy by selecting all files and hitting delete (temporary files used by open applications can't be deleted while the apps are running). Unfortunately, ***Search*** doesn't identify temporary files stashed in Temporary Internet Files folders, so this clearly isn't the complete answer!

- **Complete copies of original files.** Deleting files with a ***.tmp*** file extension doesn't mean you've eliminated all files in the TEMP directory that might provide clues to the users' actions. Users downloading files from web sites often take shortcuts or perform other actions that cause the program to write the file to the TEMP directory. As shown in Figure 1, the TEMP directory of a networked Windows 2000 workstation (viewed with Windows Explorer) contains complete copies of previously downloaded documents, all left behind without the user's knowledge.

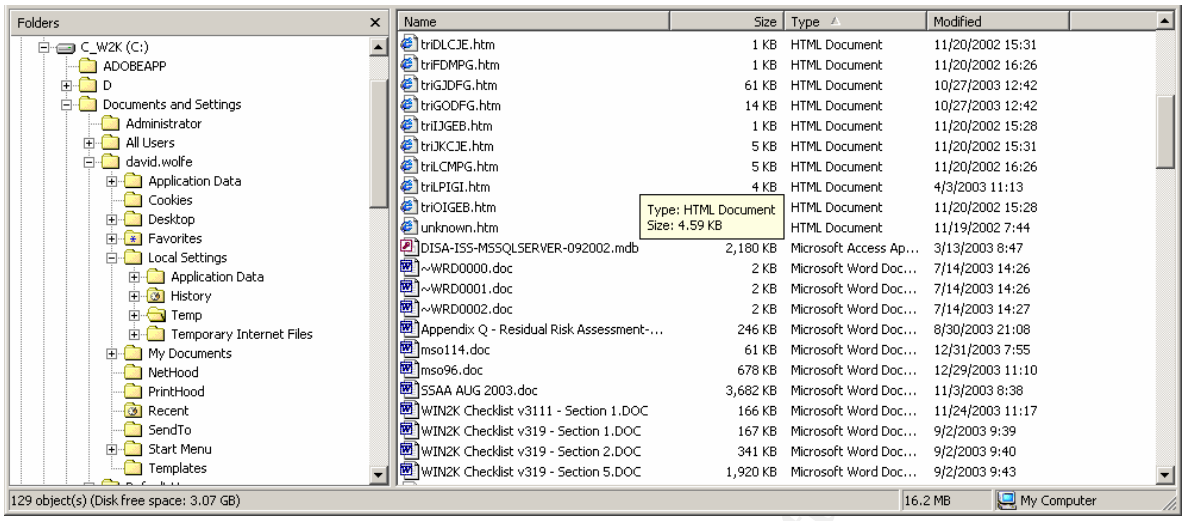

Figure 1

Cleanup of these files is a little more difficult, because the user has to visually search the TEMP folder for different types of files, recognize and delete the abandoned files.

- **E-mail Attachments in Temporary Internet Files.** While the files shown above were the result of downloads from web sites/portals, complete files are also left behind when working with E-mail. Unseen by the user, copies of files can be stashed on the hard drive just by opening an E-mail attachment. In Figure 2, the author E-mailed a draft paper home, then opened it and began editing before saving to another file folder under another title. Consequently, Windows saved copies of both document versions in a folder under Temporary Internet Files. How does the user know it's happening? During the "Save As" function, the temporary folder and its contents are revealed, and just as easily, the user can remove these unwanted copies by right-clicking on the unwanted file and deleting.

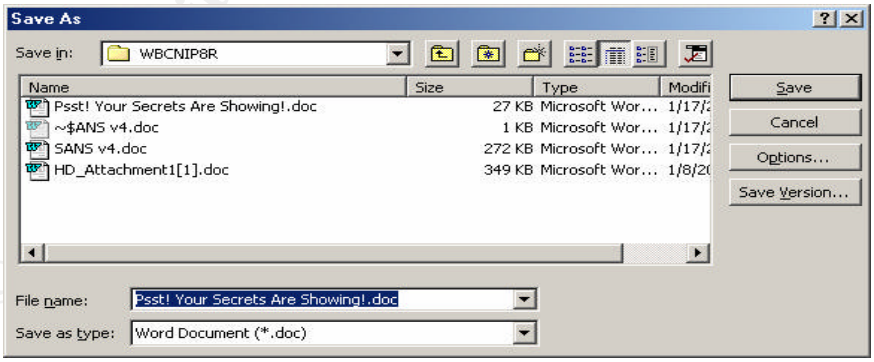

Figure 2

How does the user know where Windows put these files since they're not left in the root TEMP folder? Referring to Figure 3, click on the drop-down arrow of the "Save in:" box to display the complete path to the folder—and other folders created during previous sessions—then go clean them out.

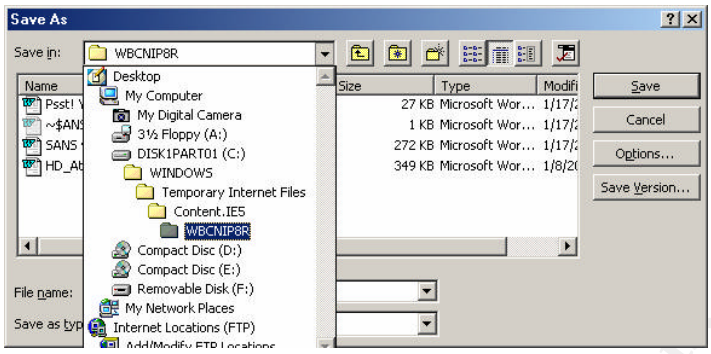

Figure 3

Looking into the other Temporary Internet Files folders in Figure 4 is also a wake-up call for the security-conscious user, as the author found when he followed his own advice and found copies of resumes E-mailed to friends months earlier.

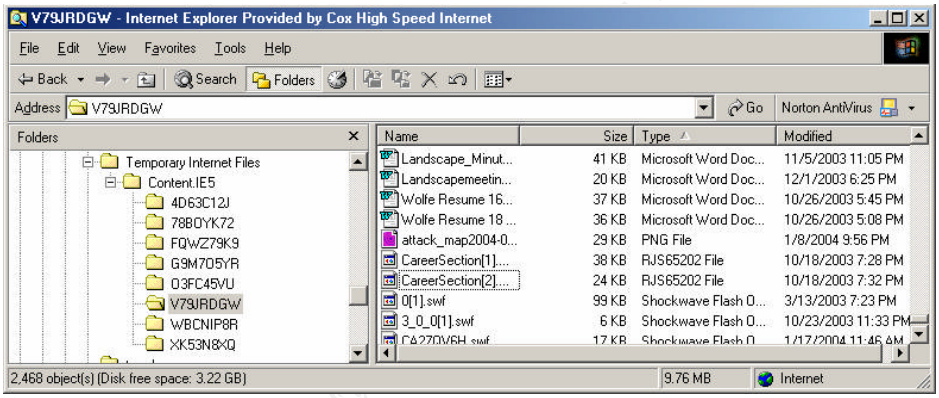

Figure 4

Clearly, once users understand how Windows and other common applications abandon files in unseen locations across the hard drive, they can prevent the build-up of sensitive information on project workstations and make it harder for the insider to zero in on sensitive information.

Hidden Data Retained Inside Files

How often have you heard someone say, “If it was a snake, it would have bitten me!” when learning that something was right in front of him or her? The same is unfortunately true of sensitive information, for it is hiding in plain sight in the very documents we use to accomplish the project. Because software applications are so powerful and complex with a wealth of functions and features, many new or inexperienced (or poorly trained) users aren’t even aware that some features are running in the background. Once again, if we show them where to look, users will be able to eliminate many of the most serious, and sometimes embarrassing, disclosures.

- **File Properties May Expose Document Source Information.** Can a single PowerPoint presentation or Word document found on a server tell the insider where to look for more sensitive information? Just click on ***File***, then ***Properties***, and the ***Summary*** tab will show the identity of the person who drafted the original

document—unless the writer used someone else's document as a template without modifying the properties data, which is especially embarrassing where resumes, homework assignments and proprietary projects are concerned! Unless document properties are sanitized, the insider's probability of learning who else is involved in a sensitive project improves significantly just by harvesting names from documents.

- **Retaining Deleted/Changed Information.** Watching documents grow inexplicably larger with each save during editing, even after large graphics are replaced with smaller ones, should be a big hint that something strange is going on inside the document. Some of this growth may be attributed to the ***Undo*** function, which records recent changes/deletions on a first-in, first-out basis. Unfortunately, this accumulation of unseen bits and bytes is a "normal" feature of Microsoft Word and other office applications, which hang onto deleted or replaced data until the ***Save As*** function is used. Forgetting this can lead to a sensitive information spillage if a harried action officer cuts sensitive information from a report and clicks on ***File***, ***Send To***, ***Mail Recipient as Attachment*** before using the ***Save As*** function. The document visually appears to be sanitized, but the E-mail recipient may be able to recover every detail of the original document, particularly if the originator neglected to turn off the ***Track Changes*** function under ***Tools***. Does it happen? Consider a resume this author recently received. After noting a different name in ***Properties*** and turning to ***Tools***, ***Track Changes***, ***Highlight Changes***, ***Highlight Changes on Screen***, the author noted two other individuals revised the same resume, replacing the original applicant's information with their own. All three versions were visible (in different colors). Although an insider may only have time or training to visually scan the document for such information left by change tracking and editing features, a more detailed examination by a trained IT professional can yield even more valuable information. In the case of a controversial British government dossier used to justify British participation in the 2003 Iraq War, an IT researcher downloaded a copy of the file in its original Word format from the government web site. After writing a small utility to extract the normally inaccessible revision log from the file, he was able to view the user and file names associated with the last 10 revisions, revealing the original authors.[7]

  Accepting all changes to the document before quitting, editing the properties tabs, and performing a final *Save As* before sending the document on will usually remove most of the easily viewed information. But as the Blair government learned, the only sure way to prevent exploitation is to use an application like Adobe Acrobat Distiller to convert the document into a file format that is basically an image, free of hidden or embedded information.

Clues to Other Information.

Finding valuable leads only takes a few moments, and failing to lock the workstation with a password protected screen saver may give the insider the time he or she needs to determine whether or not your workstation is a worthy target for a nocturnal visit. As shown in the following items, just a few mouse clicks reveals a tremendous amount of information about the user's activities and ongoing projects.

- **Recently Viewed Documents**. Right out of the box, Microsoft's word processor, spreadsheet and presentation applications are tattletales. If the user closes a Word document and walks away from the unlocked workstation, an insider can grab the mouse, click ***File***, and view a list of all documents recently opened—in order—at the bottom of the drop-down menu. It's a handy tool for users, allowing one to quickly click on the title of the last file or two and resume work. But it also reveals the project file name(s) and path to the file's location to the insider. Fortunately, it's also an option which can be turned off by clicking ***Tools***, ***Options***, select the ***General*** tab, and uncheck the box for ***Recently Used File List*** (See Figure 5).

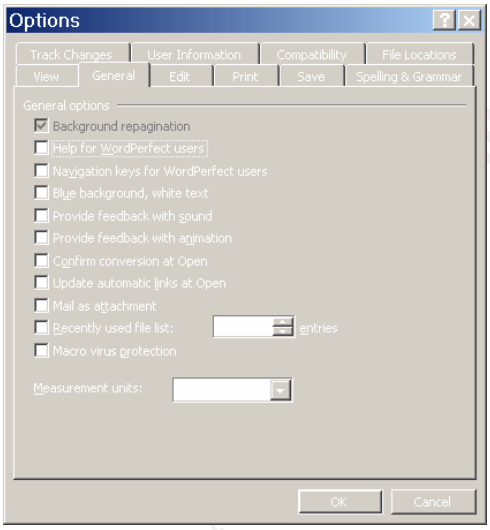

Figure 5

But the ***Recently Used Files List*** in each application isn't the only place your file use is being tracked. Clicking ***Start***, then ***Documents*** gives the insider a snapshot of all recently opened files of all types, not just Word or PowerPoint. Without hacking the workstation or installing keystroke loggers, an insider with 10 seconds alone with the workstation instantly knows whether the user is working on anything 'special.' Happily, a couple clicks clears this list, too—left-click ***Start***, ***Settings***, ***Taskbar and Start Menu***, then click the ***Advanced*** tab shown in Figure 6, and click ***Clear***. Not only does this clear the list of recently accessed documents, but it also clears the lists of recently accessed web sites and programs, too. On the down side, this has to be done every time before shut down to eliminate fresh accumulation.

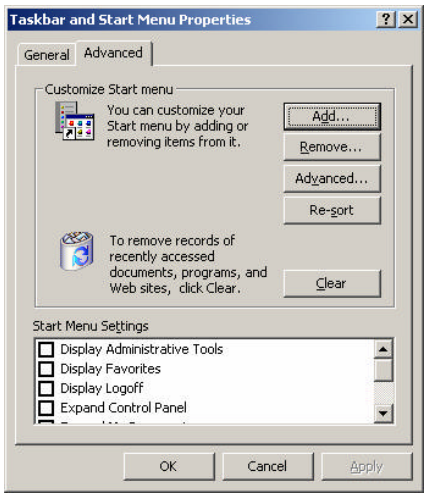

Figure 6

- **The *Recent* Folder.** If the insider has a few more moments on the workstation, a clean ***Documents*** list won't slow him or her down, for the unabridged listing of recently viewed files is stored in a hidden folder in the Windows directory, appropriately named Recent. Not only does the Recent folder give the insider an interesting list of file names to research, but the example in Figure 7 reveals a removable disk has been used with the workstation—a hint to snoop through the desk drawers!

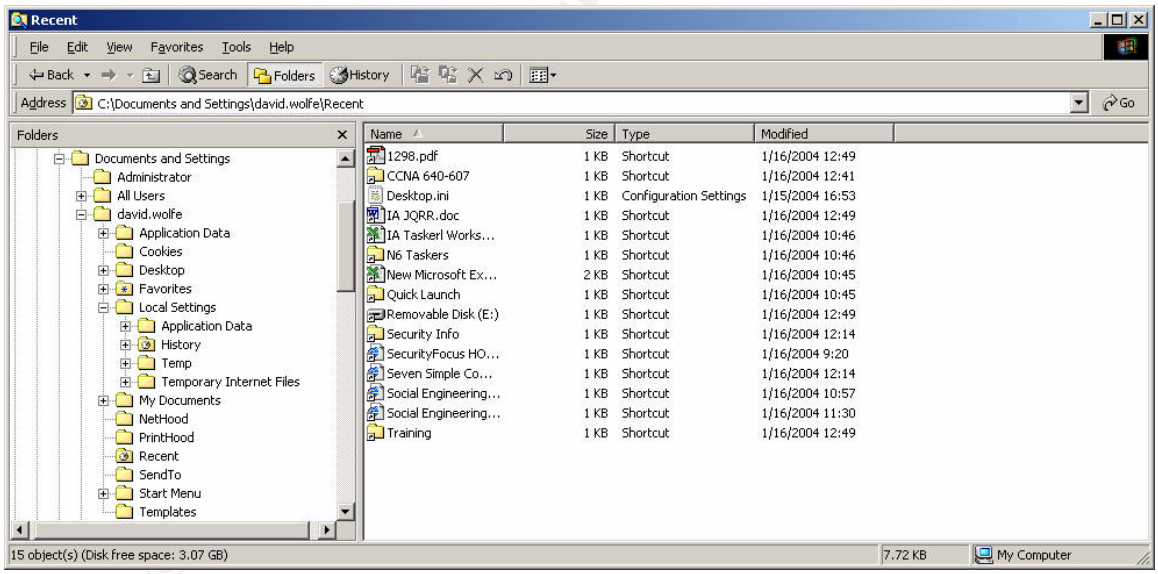

Figure 7

But wait, a folder named Recent isn't visible when using Windows Explorer—unless the user knows that Microsoft's default installation prevents users from seeing (and possibly deleting) certain folders and important system files (including Recent). This is easily rectified by clicking on ***Tools***, ***Folder Options***, ***View***, and clicking ***Show hidden files and folders***, as shown if Figure 8, below.[8]

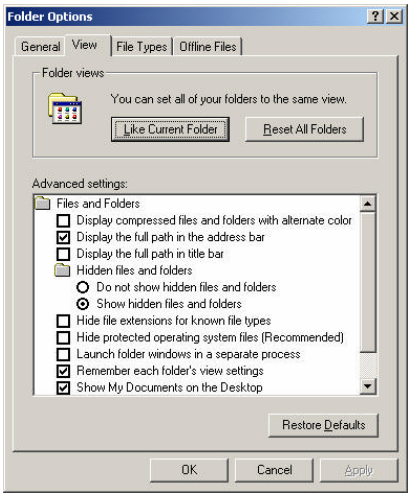

Figure 8

- **The Browser History Folder**. Just as the ***Documents*** tab and the Recent folder tell the insider where to focus his or her snooping, the History folder can also act as a roadmap to sensitive information. Using the same analytical skills as a concerned parent checking on a child's surfing habits, the insider can use the History folder to determine the focus of a sensitive project and even organizational relationships just by examining which web pages were accessed by the user. Depending on how the system administrator has configured the workstation, the accumulation of web site visits can span a period of days or weeks. The workstation in figure 9, for example, is set to record every URL visited throughout the month, giving the system administrator a powerful tool for recording unauthorized or improper surfing. Sadly, the insider reaps the same benefit.

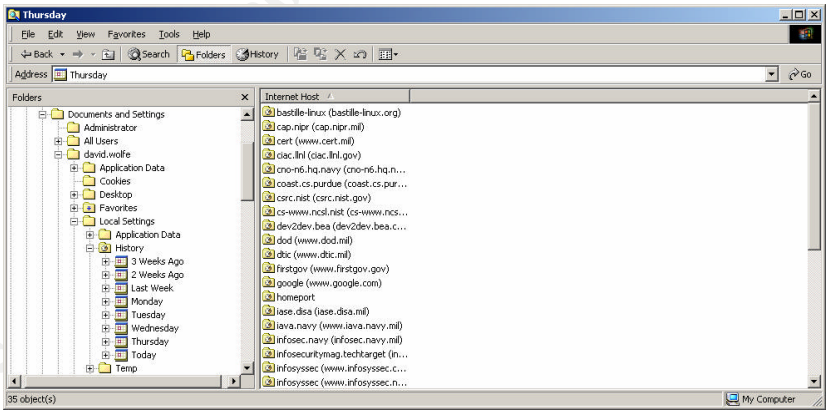

Figure 9

Taking this advantage away from an insider is quick and easy, provided the user has privileges to access and modify the History settings. In the Internet Explorer ***Tools*** menu, click ***Internet Options*****,** then click the ***General*** tab. Under ***History***, change the number of days History tracks the web pages visited to zero and click ***Clear History*** to delete anything already there.

- **Browser Favorites**. Keeping the History folder clear eliminates a hard record of when and where a user has been, but the Favorites folder can provide similar clues

to a determined insider. Users tend to collect and organize those links to web sites needed to do their job. By analyzing the Favorites folder names and the links within them, the insider may find clues leading to bigger pieces of the puzzle. Unfortunately, if the presence of certain URLs within Favorites compromises sensitive information, then there is no choice but to prohibit the use of Favorites, especially in a network environment where the user's system settings (and Favorites) are also mirrored on the network drive. Storing and running Favorites from a removable project drive is an option, but once again the browser also records recently accessed URLs for easy return access. However, there is a method for users to visit a site in a way that won't be recorded by the browser. In the browser, press ***Ctrl-O*** to bring up a dialog box, then type the URL (or paste it from a list on the project drive).[9] Now the browser's address drop-down will remain blank and deny the insider even that clue.

- **Cookies.** Cookies are yet another source of information for the insider. Just like the History and Favorites folders, the accumulated cookies with their embedded URLs give the insider a comprehensive listing of the user's on-line activities. How easily can an insider view the list of cookies? In the browser, Click ***Tools***, ***Internet Options***, and under the ***General*** tab click the ***Settings*** button in the ***Temporary Internet files*** area. In the ***Settings*** box, click the ***View Files*** button.[10] The insider now has the complete list of cookies and embedded URLs to research. Eliminating every cookie may be appealing, but isn't always practical, because some cookies are needed by some web sites to function effectively. However, if security is at stake, they must go. To quickly delete existing cookies, click the ***Tools*** menu in the browser, then ***Internet Options***. As shown in Figure 10, just click ***Delete Cookies***.

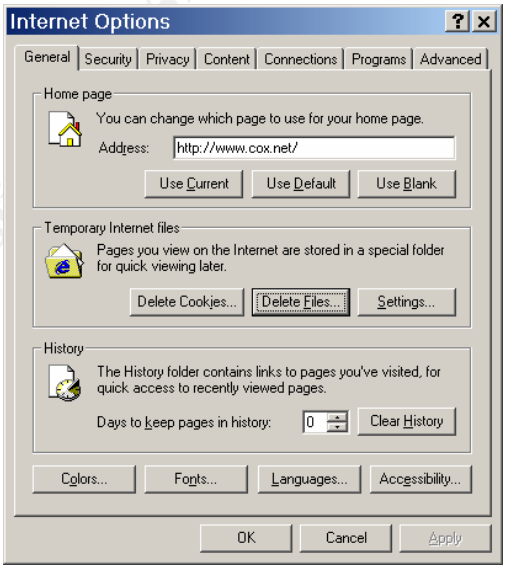

Figure 10

Rather than repeatedly deleting cookies, it may be easier to block them by increasing the ***Privacy*** setting within the browser (Figure 11).

Figure 11

If aggressively blocking cookies has unexpected consequences or is unacceptable because 'good' cookies must be allowed for web pages to function completely, experiment with the slide settings to determine where it starts impacting the user and stop there. Yet another cookie control can be pre-set in the browser (Figure 12) under ***Tools***, ***Internet Options***, click the ***Security*** tab, then the Custom Level button, and click to select to enable, disable or prompt when cookies are stored on the hard drive.

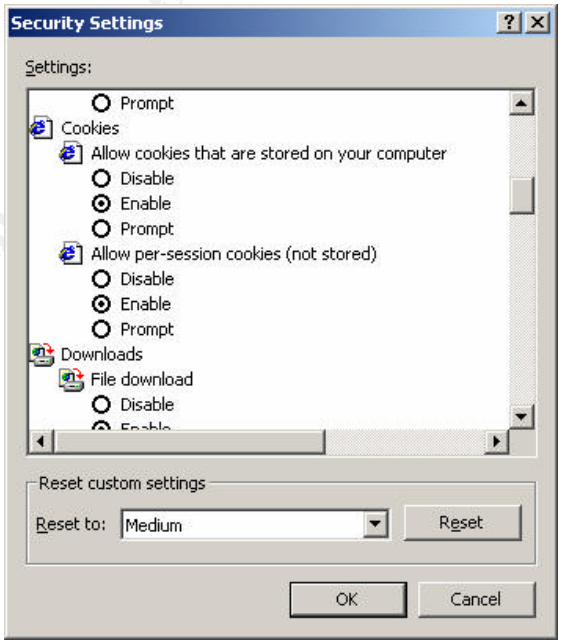

Figure 12

Utilities such as Norton System Works can also be used to clean out non-essential cookies; however, these utilities seem to err on the side of caution, and may leave

more cookies behind than desired. If the user isn't sure the settings provide adequate security, there are a number of reputable web sites that will provide a complimentary security scan.[11] In the end, the best option is the one that impacts the user least while protecting sensitive information.

- **Spyware.** Closely related to the cookie controversy is the issue of spyware, those nasty tracking cookies and unseen applications that often install themselves without the user's knowledge or consent while surfing web sites and downloading files. They record the user's actions and movements on the Internet and report back to their unseen masters without any indication to the user that the workstation is talking to strangers. In the case of an insider, placing spyware onto co-workers' workstations is simple, because he or she can secretly install it directly onto target workstations or shared network drives. Just as easily, he or she can pass it to the target user inside a copy of a music sharing program, all without having to fight through firewalls, intrusion detection systems or E-mail scanners. Since spyware is installed and collects information about the user invisibly, spyware detection and removal utilities like *AdAware* and *Spybot Search and Destroy* must be used regularly to ferret out tracking cookies, registry entries and spyware secretly hidden in downloaded applications or peer-to-peer file-sharing programs like Kazaa, BearShare and others.[12]
- **Temporary Internet Files**. In addition to the documents and cookies mentioned earlier, Temporary Internet Files folders accumulate virtually every object, image or photo (usually in jpg format) from visited web pages. The objects are automatically saved onto the local hard drive so they won't have to be download again when the user returns to the same web page, a time and bandwidth saving measure). As Figure 13 shows, the insider can retrieve the images stored in the Temporary Internet Files and quickly deduce the user is researching cameras, for example.

Figure 13

If the insider can view this information using common software applications already on the workstation, then clearly something must be done. Constantly deleting files from the workstation after every session could lead to an oversight, so why not just

turn off this feature? In the browser, click ***Tools***, then ***Internet Options*** to access the button to dump the accumulated files in the same way as Cookies. But going one step further, click ***Settings***, then move the ***Amount of disk space to use*** slide in Figure 14 to zero to effectively prevent the buildup of these files in the first place.

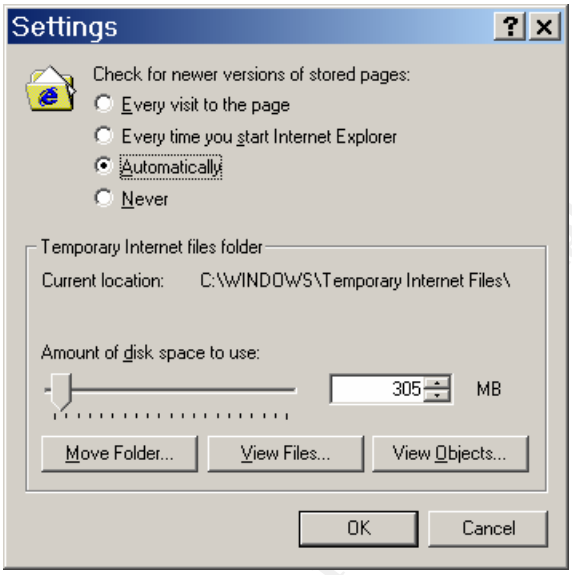

Figure 14

Conclusion

In a perfect world, software would be secure right out of the shrink-wrap, and leave the hard drive clear of any unseen information. But depending on the user's habits, operating environment and applications, these caches and more will always be found, particularly in the networked environment. Virtually every Windows-based application used in the modern office environment writes information onto the user's hard drive, often without the user's knowledge, and fails to remove it without operator intervention. That isn't meant as an indictment of the operating system and application developers, but as long as insiders operate freely inside traditional network defenses, finding and removing this unseen sensitive information remains an imperative whenever sensitive, proprietary or classified information is concerned. Effective training and practice can help users learn to prevent the buildup of sensitive information on their workstations, or at the very least find and remove it daily. But security isn't something that can be delegated solely to the user. Clear policies, coupled with standardized workstation/application configurations that prevent the buildup of unseen information in the first place, will help to eliminate a great deal of the complexity that frequently overwhelms inexperienced users. In the end, it takes a concerted effort by leadership, security managers, system administrators, trainers and users to eliminate clues to a sensitive project before the insider can find them. But it starts with educating the user to the threat.

Works Cited:

[1] Lady Burton, Source: *Given as an Arabian proverb.* http://www.worldofquotes.com/topic/Knowledge/1/

[2] Jackson, William. "Intelligence Community seeks Protection from Inside Threats," January 12, 2003. *Government Computer News*. http://www.gcn.com/vol1_no1/daily-updates/24622-1.html

[3] Pethia, Rich. "Internet Security Trends." February 16, 2001. Carnegie-Mellon Software Engineering Institute, **http://www.cert.org/present/internet-security-trends/**

[4] Gaudin, Sharon. "Security Begins From Within," Earthweb. August 4, 2003. http://itmanagement.earthweb.com/secu/article.php/2244131

[5]Microsoft Corp. "WD: How Word for Windows Uses Temporary Files." Microsoft Knowledge Base Article – 211632. http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q211/6/32.ASP&NoWebContent=1

[6] Berger, Sandy. "How to Eliminate Temp Files." AARP How To Guides. http://www.aarp.org/computers-howto/Articles/a2002-07-15-tempfiles.html

[7] Smith, Richard M. "Microsoft Word bytes Tony Blair in the butt." June 30, 2003. http://www.computerbytesman.com/privacy/blair.htm

[8] Bailes, Lenny. "Seek Out Hidden Files." *PC World*. August 08, 2000 http://www.pcworld.com/howto/article/0,aid,12834,00.asp

[9] Hewlett-Packard. "Snoop proof your PC." http://h71036.www7.hp.com/hho/cache/836-0-0-225-121.aspx;

[10] Spanbauer, Scott. "Internet Tips: Protect Yourself--Clear Your Cookies and History." January 2003. *PC World magazine*. http://www.pcworld.com/howto/article/0,aid,106715,00.asp

[11] Spanbauer, Scott. "Internet Tips: Play It Safe With the Right Browser Security Settings; Select the appropriate browser settings; improve wireless-network security with WPA." September 2003. *PC World magazine*. http://www.pcworld.com/howto/article/0,aid,111655,00.asp

[12] Spanbauer, Scott. "Escape the Spyware Nightmare, Spyware and adware are the newest threats to connected PCs. Here's how to get them off your machine--and keep them off." July 23, 2003. *PC World magazine*. http://www.pcworld.com/howto/article/0,aid,111630,00.asp