Global Knowledge™

Expert Reference Series of White Papers

Alternate Data Streams – What's Hiding in Your Windows NTFS?

Alternate Data Streams – What's Hiding in Your Windows NTFS?

Keith Palmgren, Global Knowledge Instructor, CISSP, Security+, TICSA

Introduction

Hackers and malware authors have a strong motivation to keep you from finding their malicious software on your system. If you find it, you can delete it. If you delete it, the malware author doesn't make money—yes, this is a for-profit business. Panda software, a respected anti-virus and anti-malware vendor, reports that from January – March of 2006, 70% of the malware released on the Internet was trying to make money for the authors in one way or another. For additional information on that report, visit http://www.pandasoftware.com/about_panda/press_room/Quarterly+PandaLabs+Report.htm.

The old ploy of "hide in plain site" isn't as reliable as it needs to be for the profit-minded malware author. For example, placing a malicious executable in a file called scsi.dll under the directory `c:\winnt\system32\os2\dll` might work fine in Windows 2000, since few people would be inclined to mess with that file. But that filename does not work in Windows XP because the `system32\os2` directory does not exist in XP. Malware authors want a more reliable means of hiding malicious files.

Enter Alternate Data Streams or ADSs (you will also find information referring to them as NTFS Streams). Every NTFS file system is capable of creating and maintaining ADSs. This is a feature added to the NTFS file system for compatibility with Macintosh computers. The Mac maintains certain information about a file that Windows does not. When you share files between a Mac and Windows, that additional information is kept in an ADS on the NTFS-based Windows system. Of course, anything that exists for a valid reason can be misused in an invalid, malicious way.

ADSs seem to be the best kept secret of the Microsoft world. Very few people, including those holding Microsoft certifications, are aware of them, although they are reasonably well understood in the computer forensics community. This is made worse by the fact that much of the information available about ADSs on the Internet is either out of date or simply wrong. Researching ADSs is extremely difficult. This paper will explain the issues with ADSs, as well as how they can be created, executed, found, and removed. Because of the amount of misinformation out there, everything in this paper has been verified on test systems.

The Details

With an ADS, one file is effectively hidden *behind* another file. The file in front is the only one visible in Windows Explorer or via the `dir` command. In fact, the only telltale sign is that the date-time stamp of the visible file changes to the time the ADS is created (even a one-way hash of the visible file using something like MD5 does not change). Here are some important points to remember throughout this discussion:

- You can put an ADS behind another file or behind a directory.

- You can put multiple files behind a single file or directory.

- Copying or moving a file within the NTFS file system does not affect the ADS. The stream copies/moves with the visible file to the new location. E-mailing the file as an attachment can destroy the ADS.

- The visible file is unaffected by the ADS. For example, placing an ADS behind the system calculator does not affect the operation of the calculator.

- All examples in this document show how ADSs can be created from the command line. Functions in various programming languages can also create and manipulate them, but we will not examine those functions here.

As noted above and demonstrated below, the date-time stamp on the visible file changes when an ADS is created behind it. However, utilities exist to manipulate those date-time stamps and make them say anything you want. If those utilities exist, then clearly the malware author could include similar functions in an install program to reset date-time stamps. Two utilities to manipulate date-time stamps are:

- Attribute Magic (http://www.elwinsoft.com/atm.html)

- File Tweak (http://www.febooti.com/products/filetweak/)

Creating an ADS is actually very simple. The command below will fork the system calculator behind a file in the root directory file called somefile.txt. The second command executes that copy of the calculator. (A much more detailed example follows below.) This command does not affect the original system calculator—it creates a copy of the calculator behind somefile.txt. Notice the use of the colon in these commands:

```
type c:\windows\system32\calc.exe>c:\somefile.txt:calc.exe
start c:\somefile.txt:calc.exe
```

The command below would place the Notepad executable into an ADS behind a directory c:\ads (the directory must already exist). You would execute the copy of notepad using the same start command syntax used above:

```
type c:\windows\system32\notepad.exe>c:\ads:notepad.exe
```

Unfortunately, until very recently, deleting ADSs was more of a problem. You had the following options:

- Move the file or directory to a FAT file system. This would destroy the stream. However, it would also remove any special file permissions, and that could be a problem, if the malicious file is hidden behind a critical directory such as system32.

- You could delete the visible file or directory. Again, if the malicious stream were hidden behind the system32 directory, that solution is less than desirable.

- You could use the commands below to get rid of an ADS behind a file named anyfile.txt in this example. Note that these commands do not work with a directory:

```
ren c:\anyfile.txt c:\temp.txt
type c:\temp.exe c:\anyfile.exe
del temp.exe
```

The Utilities

Fortunately, there is now a utility that will help you to delete Alternate Data Streams. If you visit http://www.spywareinfo.com/~merijn/downloads.html and scroll down the page, you will find the utility ADS Spy. This is a graphical tool that can show you ADSs and let you select which of those ADSs to delete. Versions 1.11 and later allow you to scan a single directory, the Windows base folder only, or your entire hard drive. A major advantage of ADS Spy is that it can delete ADSs from behind both files and directories.

A second utility, lads.exe is a command line utility. It does not delete ADSs, it only lists them. If you were to put lads.exe in the `C:\` directory, the command below creates a file containing a listing of all the ADS files on your system:

```
C:\lads.exe /S > C:\ads-list.txt
```

The /S tells lads to look in subdirectories. Without that, it only looks in the present directory. You can also specify a directory you want it to scan. Use `C:\lads /?` for all the options. You can download lads.exe from http://www.heysoft.de/Frames/f_sw_la_en.htm.

Further Discussion

The existence of an ADS on your system is not necessarily malicious. We have identified at least three times when an ADS will exist legitimately:

- Since they were invented for the purpose of tracking information on files shared between a Macintosh operating system and NTFS, this will obviously create them legitimately.

- When you use Microsoft Internet Explorer (at least through version 6) to download and save files from the Internet, the browser creates an ADS called Zone.Identifier. This file contains information about the Internet zone from which the file was downloaded. We have yet to discover why we might need that information, but that is what it does. Contents of such a file often look like the following:

  ```
  [ZoneTransfer]
  ZoneId=3
  ```

- In the Windows XP Windows Explorer, if you choose the View –> Thumbnails option for pictures, it appears to create the thumbnail as an ADS. These files have names similar to {4c8cc155-6c1e-11d1-8e41-00c04fb9386d}. Very informative, as you can see. Note that we are not certain that this is the thumbnail, since we've yet to find a way to open one of those files. However, using the utilities discussed above, we can clearly see that choosing View –> Thumbnails creates ADSs behind picture files.

Other applications may create legitimate ADSs. For example, saving files out of some versions of Microsoft Outlook reportedly creates them, though we have not been able to confirm that. The instances above are simply the ones we have definitely confirmed.

The Demonstration

Using a command line, it is possible to create and execute an ADS. Note that everything you see below is on a Windows XP SP2 system. If you are using something different, the paths and so forth may change (from `c:\windows` to `c:\winnt` on Windows 2000, for example). This demonstration is confirmed to work on Windows 2000, Windows XP, and Windows 2003.

First, we make a directory to work in for the test and cd into it. Then we copy the system calculator to that directory. When we make the copy, we give the file a new name to differentiate the copy we are working in from the actual system executable. Note that the new directory and copying the file is not required, we just don't want to take a chance on messing up the actual system executables.

Once we make the copy, we do a `dir` command and see that the date-time stamp on calc-ads.exe is 08/04/2004 03:00 AM and the size is 114,688 bytes.

We then do the `type` command to place the notepad.exe executable behind the calc-ads.exe file (notice the colon between the filenames). This creates the ADS. Note that we call the streamed file notepad-ads.exe to make sure we are using the copies and not the real system executables.

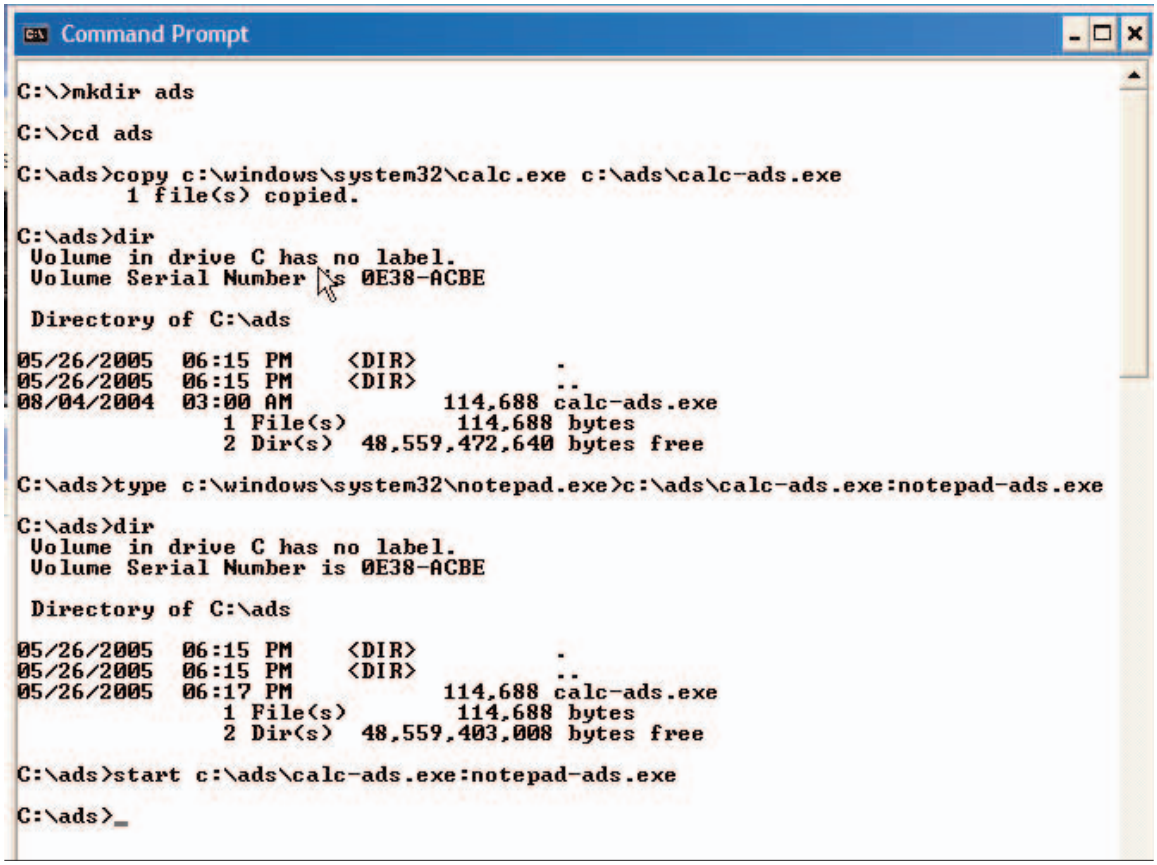

Figure 1. Command Line Demonstration

We do a `dir` again and see that the date/time stamp of calc-ads.exe has changed to 05/26/2005 06:17 PM. Note that it now shows the time we created the ADS; however, the file size is *unchanged* at 114,688 bytes.

(We will not demonstrate the date-time stamp changing utilities we mention above, but have tested them, and they do, indeed, work.)

With the ADS created, we are ready to execute it. In the command line window above, you see the `start` command, which is how you execute a file hidden as an ADS. The screen capture in Figure 2 was taken after pressing the enter key following that command, and then opening the Windows Task Manager and clicking the Processes tab. You can see that Notepad is open. In the Task Manager, you see calc-ads.exe:notepad-ads.exe, which shows that it is, indeed, the ADS that executed.

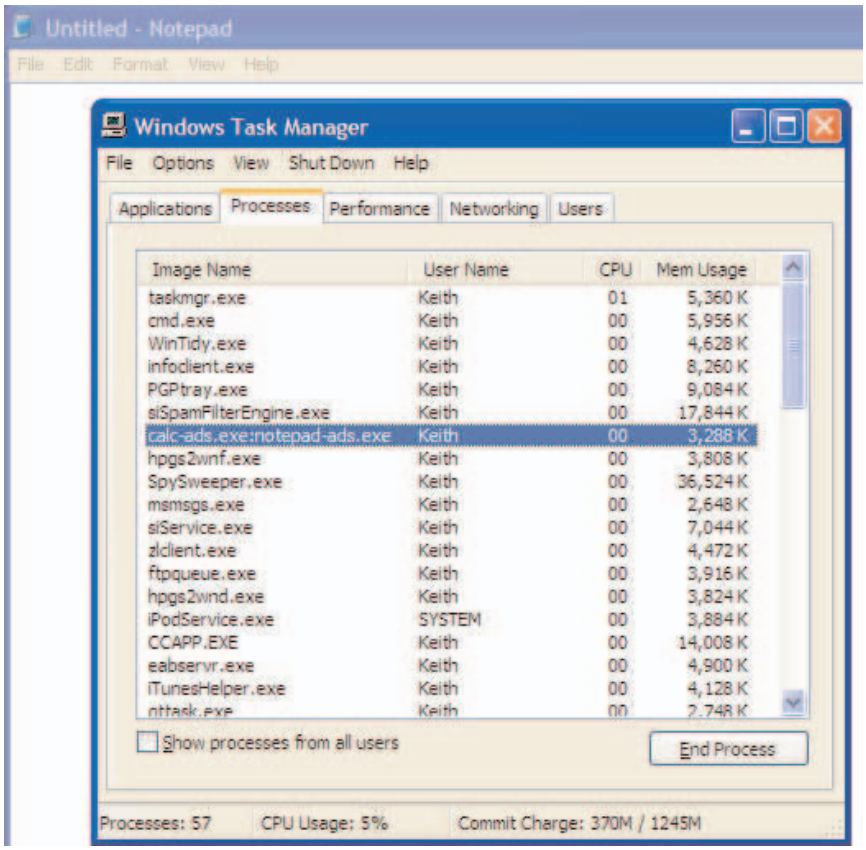

Figure 2. Notepad running and the Process shown

Note that the screen shot in Figure 2 is from Windows XP. If you do this on Windows 2000 or prior, the Task Manager process would show up as simply calc-ads.exe.

There is another point worth making regarding Task Manager, ADS, and malware. If an ADS executable is installing spyware on a system, the process would terminate before you can get logged in. Therefore, it would not show up in the process table at all, since it is already done running. Of course, something like a key logger would run continuously to capture all of your keystrokes. You should be able to see that type of program in the process table. In the latter case, you should expect the person who places the key logger on your system to be as creative and deceptive as possible in naming the executable in an attempt to make it look innocuous.

As we stated above, you can see the file size/date-time phenomenon in Windows Explorer, as well as the command line. Below are two screen captures. Figure 3 shows the calc-ads.exe before the ADS creation; note the file size and date-time stamp. Figure 4 shows the file after the ADS creation with the same size, but a different date-time. Again, the only telltale sign is the date-time stamp. The utilities mentioned above could erase even that clue.

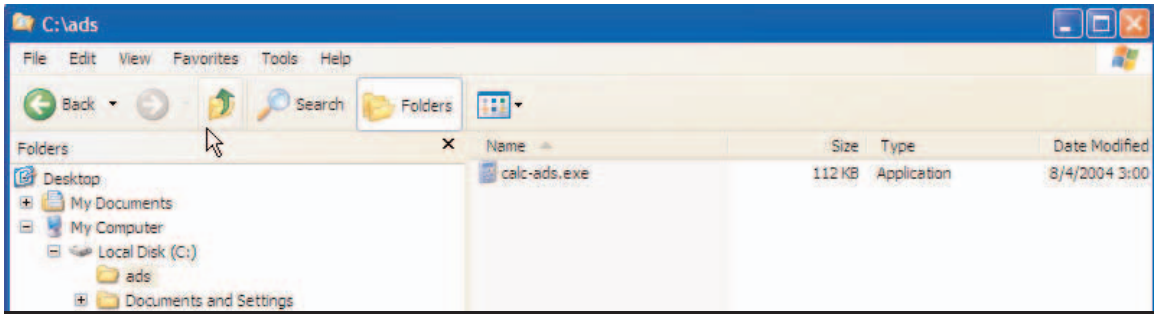

Figure 3. Windows Explorer before ADS creation

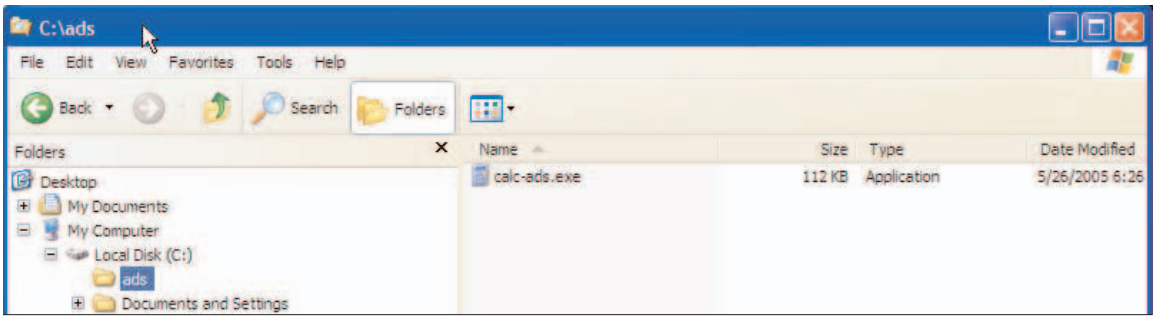

Figure 4: Windows Explorer after ADS creation

The Cleanup

We could clean up our test files by simply deleting them. Instead, we will use the utilities mentioned above as a continuation of the demonstration. We will use ADS Spy to delete the ADS, and LADS to check our progress. We begin by running the `lads` command with no command line switches so the program looks only in the present working directory, `c:\ads` in this case. In Figure 5, we can see the `lads` command finding the notepad-ads.exe ADS.

```
C:\ads>lads

LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\ads\

      size  ADS in file
----------  ------------------------------
     69120  C:\ads\calc-ads.exe:notepad-ads.exe

     69120 bytes in 1 ADS listed

C:\ads>
```

Figure 5. lads.exe showing the ADS

In Figure 6, we have run ADS Spy set to scan only the `c:\ads` folder. You can see that it also found the notepad-ads.exe hidden file. After it finds the ADS, we click to place a checkmark next to that file and then click the Remove Selected Streams button. We then see the warning in Figure 7.

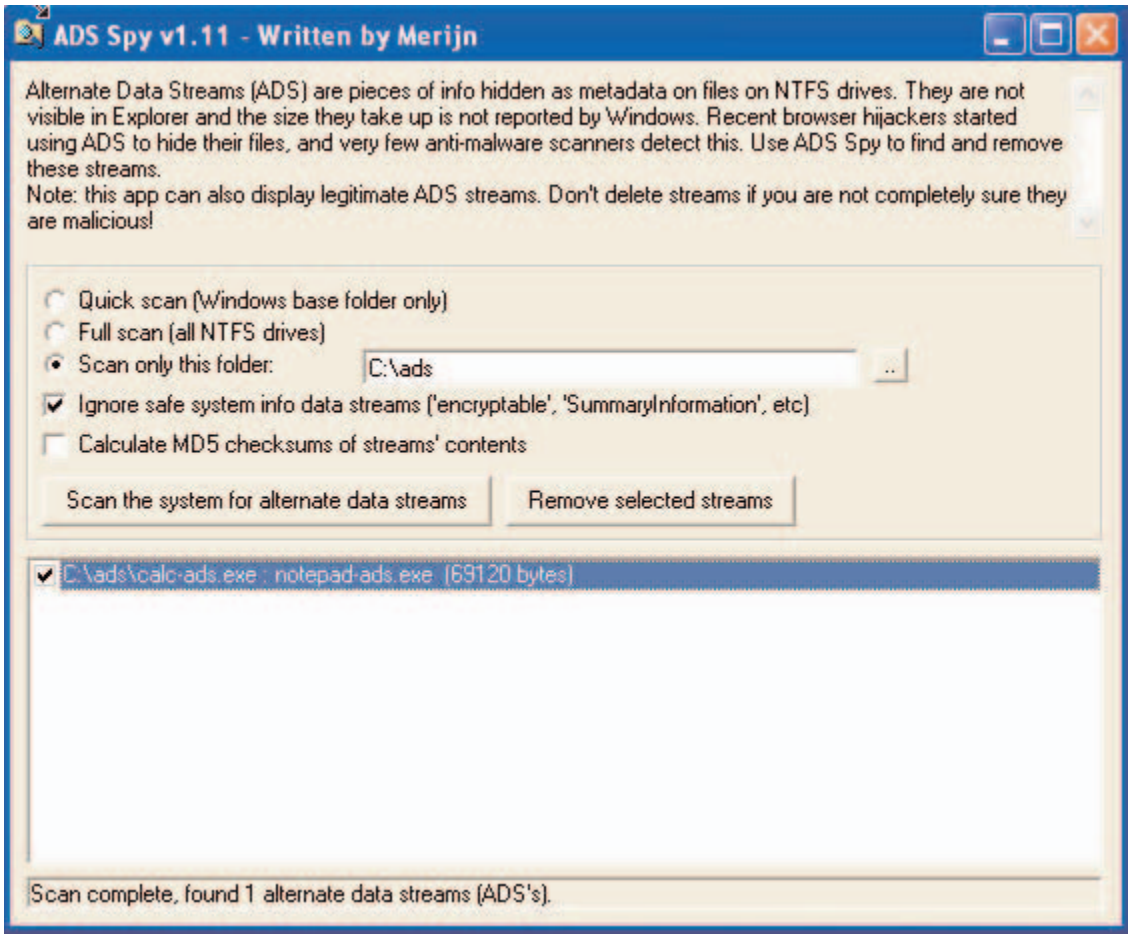

Figure 6. ADS Spy—deleting an ADS

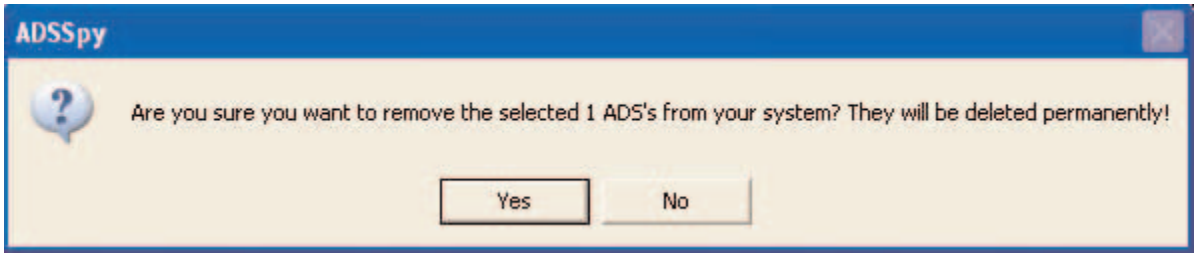

Figure 7. ADS Spy removal warning

Note that the warning in Figure 7 states, "They will be deleted permanently!" In other words, they will not be placed in the Recycle Bin for later recovery. In fact, so far as we have been able to determine, the files cannot be recovered by any means. Obviously, care should be used with ADS Spy.

Thus far, with care and common sense, we have been unable to cause serious damage with ADS Spy. It appears to work as advertised. Just ensure you use it wisely.

After clicking the Yes button in Figure 7, we again run the `lads` command and see that it finds no ADSs (incidentally, ADS Spy would not find any now either). Therefore, we see that removal of the ADS succeeded.

```
C:\ads>lads

LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\ads\

      size  ADS in file
----------  ------------------------------

         0 bytes in 0 ADS listed

C:\ads>
```

Figure 8. lads.exe confirming ADS removal

Summary

Alternate Data Streams exist for a perfectly valid reason. Unfortunately, like many valid features in the computer world, they can also be misused in invalid and malicious ways. When that occurs, it is important for systems administrators to understand ADSs as completely as possible. With that understanding, they can recognize the possibility that odd occurrences may be due to a hidden ADS file. They can then hunt down the hidden file and remove it—preferably in a safe and effective manner.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

Essentials of Network Security

CISSP Prep Course

Check Point NGX CCSA/CCSE
Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator (CHFI)

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Keith Palmgren has over 20 years of experience as a security professional and has held the CISSP certification since 1998. He spent the majority of his career as a security consultant for various firms, including starting and running Sprint's first International Security Consulting Practice. Currently, Keith is the president of NetIP, Inc.—A Knowledge Transfer Company. As such, he does freelance writing and teaching to share his knowledge with other IT professionals. Keith teaches a variety of courses in the Global Knowledge Security curriculum.